



# Inverno Framework Documentation

Version: 1.5.3

Author: [Jeremy Kuhn](#)

# 1 Introduction

---

- 1.1 Design principles
- 1.2 Getting help

# 2 Overview

---

- 2.1 Inverno Core
  - 2.1.1 Creating an Inverno module
- 2.2 Inverno Modules
  - 2.2.1 Using a module
  - 2.2.2 Available modules
- 2.3 Inverno Tools
  - 2.3.1 Inverno Maven Plugin

# 3 Inverno Distribution

---

- 3.1 Requirements
- 3.2 Creating an Inverno project
  - 3.2.1 Developing a simple Inverno application
  - 3.2.2 Configuring logging
  - 3.2.3 Running the application
  - 3.2.4 Building the application image

# 4 Inverno Core

---

- 4.1 Motivation
- 4.2 Prerequisites
- 4.3 Overview
  - 4.3.1 Modules and Beans
  - 4.3.2 Java module system
- 4.4 Project Setup

- 4.4.1 Maven
  - 4.4.2 Gradle
- 4.5 Bean
  - 4.5.1 Module Bean
  - 4.5.2 Wrapper Bean
  - 4.5.3 Nested Bean
  - 4.5.4 Overridable
  - 4.5.5 Lifecycle
  - 4.5.6 Visibility
  - 4.5.7 Strategy
- 4.6 Module
  - 4.6.1 The module class
  - 4.6.2 Lifecycle
  - 4.6.3 Module as component
  - 4.6.4 Module as application
- 4.7 Dependency Injection
  - 4.7.1 Bean Socket
  - 4.7.2 Socket Bean
  - 4.7.3 Wiring
- 4.8 Modular application
  - 4.8.1 Composite module
  - 4.8.2 Provided type

## 5 Inverno Modules

---

- 5.1 Motivation
- 5.2 Prerequisites
- 5.3 Overview
- 5.4 Base
  - 5.4.1 Converter API
  - 5.4.2 Net API
  - 5.4.3 Reflection API
  - 5.4.4 Resource API
- 5.5 Boot
  - 5.5.1 Configuration
  - 5.5.2 Reactor
  - 5.5.3 Net service
  - 5.5.4 Media type service
  - 5.5.5 Resource service

- 5.5.6 Converters
  - 5.5.7 Worker pool
  - 5.5.8 Object mapper
- 5.6 Configuration
  - 5.6.1 Configuration source
  - 5.6.2 Configuration loader
- 5.7 HTTP Base
  - 5.7.1 HTTP base API
  - 5.7.2 HTTP header service
- 5.8 HTTP Server
  - 5.8.1 Configuration
  - 5.8.2 Server Controller
  - 5.8.3 HTTP Server API
  - 5.8.4 WebSocket
  - 5.8.5 Extending HTTP services
  - 5.8.6 Wrap-up
- 5.9 Web
  - 5.9.1 Web Routing API
  - 5.9.2 Web Server
  - 5.9.3 Web Controller
- 5.10 Reactive Template
  - 5.10.1 Creates an .irt template
  - 5.10.2 .irt syntax
  - 5.10.3 Pipes
  - 5.10.4 Modes
- 5.11 SQL Client
  - 5.11.1 SQL client API
  - 5.11.2 Vert.x SQL Client implementation
- 5.12 Redis Client
  - 5.12.1 Redis Client API
  - 5.12.2 Lettuce Redis Client implementation
- 5.13 LDAP
  - 5.13.1 Configuration
  - 5.13.2 LDAP Client API
  - 5.13.3 LDAP Client bean
- 5.14 Security
  - 5.14.1 Security Manager
  - 5.14.2 Security Context
- 5.15 Security HTTP

- 5.15.1 Security Interceptor
- 5.15.2 Access Control Interceptor
- 5.15.3 HTTP authentication
- 5.15.4 Cross-origin resource sharing (CORS)
- 5.15.5 Cross-site request forgery protection (CSRF)
- 5.16 Security LDAP
  - 5.16.1 LDAP authenticator
  - 5.16.2 Active Directory authenticator
  - 5.16.3 LDAP identity
- 5.17 JSON Object Signing and Encryption
  - 5.17.1 JWK Service
  - 5.17.2 JWS Service
  - 5.17.3 JWE Service
  - 5.17.4 JWT Service
  - 5.17.5 JOSE Media Type Converters

## 6 Inverno Maven Plugin

---

- 6.1 Usage
  - 6.1.1 Run a module application project
  - 6.1.2 Start and stop the application for integration testing
  - 6.1.3 Build a runtime image
  - 6.1.4 Build an application image
  - 6.1.5 Build a container image tarball
  - 6.1.6 Build and deploy a container image to a Docker daemon
  - 6.1.7 Build and deploy a container image to a remote repository
- 6.2 Goals
  - 6.2.1 Overview
  - 6.2.2 `inverno:build-app`
  - 6.2.3 `inverno:build-image`
  - 6.2.4 `inverno:build-image-docker`
  - 6.2.5 `inverno:build-image-tar`
  - 6.2.6 `inverno:build-runtime`
  - 6.2.7 `inverno:help`
  - 6.2.8 `inverno:run`
  - 6.2.9 `inverno:start`
  - 6.2.10 `inverno:stop`

## 7 Inverno OSS Parent

---

- 7.1 Dependencies
- 7.2 Maven Plugins

# 1

---

## Introduction

The **Inverno Framework** has been created with the objective of facilitating the creation of Java enterprise applications with maximum modularity, performance, maintainability and customizability.

New technologies are emerging all the time questioning what has been working for years, We strongly believe that we must instead recognize and preserve proven solutions and only provide what is missing or change what is no longer in line with widely accepted evolutions. The Java platform has proven to be resilient to change and offers features that make it an ideal choice to create durable and efficient applications in complex technical and organizational environments which is precisely what is expected in an enterprise world. The Inverno Framework is a fully integrated suite of modules built for the Java platform that fully embrace this philosophy by keeping things well organized, strict and explicit with clean APIs and comprehensive documentation.

The Inverno framework is open source and licensed under version 2.0 of the [Apache License](#).

## Design principles

A Inverno application is inherently modular, **modularity** is a key design principle which guarantees a proper separation of concerns providing flexibility, maintainability, stability and ease of development regardless of the lifespan of an application or the number of people involved to develop it. A Inverno module is built as a standard Java module extending the [Java module system](#) with [Inversion of Control](#) and [Dependency Injection](#) performed at compile time.

The Inverno Framework extends the Java compiler to generate code at compile time when it makes sense to do so which is strictly why annotations were initially created for. When done appropriately, **code generation** can be extremely valuable: issues can be detected ahead of time by analyzing the code during compilation, runtime footprint can be reduced by transferring costly processing like IoC/DI to the compiler improving runtime performance at the same time.

The framework uses a state of the art threading model and it has been designed from the ground up to be fully non-blocking and reactive in order to deliver very **high performance** while simplifying development of highly distributed applications requiring back pressure management.

The inherent modularity of the framework based on the Java module system guarantees a nice and clean project structure which prevents misuse and abuse by clearly separating the concerns and exposing **well designed APIs**.

Special attention has been paid to **configuration** and **customization** which are often overlooked and yet vital to create applications that can adapt to any environment or context.

## Getting help

We provide here a reference guide that starts by an overview of the Inverno core, modules and tools projects which gives a good idea of what can be done with the framework followed by a more comprehensive documentation that should guide you in the creation of an Inverno project using the Inverno distribution, the use of the core IoC/DI framework, the various modules including the configuration and the Web server modules and the tools to run, package and distribute Inverno components and applications.

The [API documentation](#) provides plenty of details on how to use the various APIs. The [getting started guide](#) is also a good starting point to get into it.

Feel free to report bugs and feature requests or simply ask questions using [GitHub](#)'s issue tracking system if you ran in any issue or wish to see some new functionalities implemented in the framework.



# 2

## Overview

---

### Inverno Core



The [Inverno core framework](#) project provides an Inversion of Control and Dependency Injection framework for the Java™ platform. It has the particularity of not using reflection for object instantiation and dependency injection, everything being verified and done statically during compilation.

This approach has many advantages over other IoC/DI solutions starting with the static checking of the bean dependency graph at compile time which guarantees that a program is correct and will run properly. Debugging is also made easier since you can actually access the source code where beans are instantiated and wired together. Finally, the startup time of a program is greatly reduced since everything is known in advance, such program can even be further optimized with ahead of time compilation solutions like [GraalVM](#)...

The framework has been designed to build highly modular applications using standard Java modules. An Inverno module supports encapsulation, it only exposes the beans that need to be exposed and it clearly specifies the dependencies it requires to operate properly. This greatly improves program stability over time and simplifies the use of a module. Since an Inverno module has a very small runtime footprint it can also be easily integrated in any application.

### Creating an Inverno module

An **Inverno module** is a regular Java module, that requires `io.inverno.core` modules, and which is annotated with `@Module` annotation. The following *hello* module is a simple Inverno module:

```
@io.inverno.core.annotation.Module
module io.inverno.example.hello {
    requires io.inverno.core;
}
```

An **Inverno bean** can be a regular Java class annotated with `@Bean` annotation. A bean represents the basic building block of an application which is typically composed of multiple interconnected beans instances. The following `HelloService` bean can be used to create a basic application:

```
package io.inverno.example.hello;

import io.inverno.core.annotation.Bean;

@Bean
public class HelloService {

    public HelloService() {}

    public void sayHello(String name) {
        System.out.println("Hello " + name + "!!!");
    }
}
```

At compile time, the Inverno framework will generate a module class named after the module, `io.inverno.example.hello.Hello` in our example. This class contains all the logic required to instantiate and wire the application beans at runtime. It can be used in a Java program to access and use the `HelloService`. This program can be in the same Java module or in any other Java module which requires module `io.inverno.example.hello`:

```
package io.inverno.example.hello;

import io.inverno.core.v1.Application;

public class Main {

    public static void main(String[] args) {
        Hello hello = Application.with(new Hello.Builder()).run();

        hello.helloService().sayHello(args[0]);
    }
}
```

## Building and running with Maven

The development of an Inverno module is pretty easy using [Apache Maven](#), you simply need to create a standard Java project that inherits from `io.inverno.dist:inverno-parent` project and declare a dependency to `io.inverno:inverno-core`:

```

<!-- pom.xml -->
<project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/maven-
4.0.0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <parent>
    <groupId>io.inverno.dist</groupId>
    <artifactId>inverno-parent</artifactId>
    <version>1.5.3</version>
  </parent>
  <groupId>io.inverno.example</groupId>
  <artifactId>hello</artifactId>
  <version>1.0.0-SNAPSHOT</version>

  <dependencies>
    <dependency>
      <groupId>io.inverno</groupId>
      <artifactId>inverno-core</artifactId>
    </dependency>
  </dependencies>
</project>

```

Java source files for `io.inverno.example.hello` module must be placed in `src/main/java` directory, the module can then be built using Maven:

```
$ mvn install
```

You can then run the application:

```

$ mvn inverno:run -Dinverno.run.arguments=John

[INFO] --- inverno-maven-plugin:1.3.1:run (default-cli) @ app-hello ---
[INFO] Running project: io.inverno.example.hello@1.0.0-SNAPSHOT...
Hello John!!!

```

## Building and running with pure Java

You can also choose to build your Inverno module using pure Java commands. Assuming Inverno framework modules are located under `lib/` directory and Java source files for `io.inverno.example.hello` module are placed in `src/io.inverno.example.hello` directory, you can build the module with the `javac` command:

```
$ javac --processor-module-path lib/ --module-path lib/ --module-source-path src/ -d jmods/ --module io.inverno.example.hello
```

The application can then be run as follows:

```

$ java --module-path lib/:jmods/ --module io.inverno.example.hello/io.inverno.example.hello.Main
John
Hello John!!!

```

# Inverno Modules



The [Inverno modules framework](#) project provides a collection of components for building highly modular and powerful applications on top of the [Inverno IoC/DI framework](#).

While being fully integrated, any of these modules can also be used individually in any application thanks to the high modularity and low footprint offered by the Inverno framework.

The objective is to provide a complete consistent set of high end tools and components for the development of fast and maintainable applications.

## Using a module

Modules can be used in a Inverno module by defining dependencies in the module descriptor. For instance you can create a Web application module using the *boot* and *web* modules:

```
@io.inverno.core.annotation.Module
module io.inverno.example.webApp {
    requires io.inverno.mod.boot;
    requires io.inverno.mod.web;
}
```

A simple microservice application can then be created in a few lines of code as follows:

```
import io.inverno.core.annotation.Bean;
import io.inverno.core.v1.Application;
import io.inverno.mod.base.resource.MediaTypees;
import io.inverno.mod.web.annotation.WebController;
import io.inverno.mod.web.annotation.WebRoute;

@Bean
@WebController
public class MainController {

    @WebRoute( path = "/message", produces = MediaTypees.TEXT_PLAIN)
    public String getMessage() {
        return "Hello, world!";
    }

    public static void main(String[] args) {
        Application.with(new WebApp.Builder()).run();
    }
}
```

Please refer to [Inverno distribution](#) for detailed setup and installation instructions.

Comprehensive reference documentations are available for [Inverno core](#) and [Inverno modules](#).

Several example projects showing various features are also available in the [Inverno example project](#). They can also be used as templates to start new Inverno application or component projects.

Feel free to report bugs and feature requests in GitHub's issue tracking system if you ran in any issue or wish to see some new functionalities implemented in the framework.

## Available modules

The framework currently provides the following modules.

### inverno-base

The foundational APIs of the Inverno framework modules:

- Conversion API used to convert objects from/to other objects
- Concurrent API defining the reactive threading model API
- Net API providing URI manipulation as well as low level network client and server utilities
- Reflect API for manipulating parameterized type at runtime
- Resource API to read/write any kind of resources (eg. file, zip, jar, classpath, module...)

### inverno-boot

The boot Inverno module provides base services to an application:

- the reactor which defines the reactive threading model of an application
- a net service used for the implementation of optimized network clients and servers
- a media type service used to determine the media type of a resource
- a resource service used to access resources based on URIs
- a basic set of converters to decode/encode JSON, parameters (string to primitives or common types), media types (text/plain, application/json, application/x-ndjson...)
- a worker thread pool used to execute tasks asynchronously
- a JSON reader/writer

### inverno-configuration

Application configuration API providing great customization and configuration features to multiple parts of an application (eg. system configuration, multitenant configuration, user preferences...).

This module also introduces the **.cprops** configuration file format which facilitates the definition of complex parameterized configuration.

In addition, it also provides implementations for multiple configuration sources:

- a command line configuration source used to load configuration from command line arguments
- a map configuration source used to load configuration stored in map in memory
- a system environment configuration source used to load configuration from environment variables
- a system properties configuration source used to load configuration from system properties

- a `.properties` file configuration source used to load configuration stored in a `.properties` file
- a `.cprops` file configuration source used to load configuration stored in a `.cprops` file
- a Redis configuration source used to load/store configuration from/to a Redis data store with supports for configuration versioning
- a composite configuration source used to combine multiple sources with support for smart defaulting
- an application configuration source used to load the system configuration of an application from a set of common configuration sources in a specific order, for instance: command line, system properties, system environment, local `configuration.cprops` file and `configuration.cprops` file resource in the application module

Configurations are defined as simple interfaces in a module which are processed by the Inverno compiler to generate configuration loaders and beans to make them available in an application with no further effort.

## inverno-http-base

The Inverno HTTP base module provides the foundational API as well as common services for HTTP client and server development, in particular an extensible HTTP header service used to decode and encode HTTP headers.

## inverno-http-server

The Inverno HTTP server module provides a fully reactive HTTP/1.x and HTTP/2 server implementation based on Netty.

It supports the following features:

- SSL
- HTTP compression/decompression
- Server-sent events
- HTTP/2 over cleartext upgrade
- URL encoded form data
- Multipart form data

## inverno-irt

The Inverno Reactive Template module provides a reactive template engine including:

- reactive, near zero-copy rendering
- statically types template generated by the Inverno compiler at compile time
- pipes for data transformation
- functional syntax inspired from XSLT and Erlang on top of the Java language that perfectly embraces reactive principles

## inverno-ldap

The Inverno LDAP module specifies a reactive API for querying [LDAP](#) servers. It also includes a basic LDAP client implementation based on the JDK. It supports bind and search operations.

## inverno-redis

The Inverno Redis client module specifies a reactive API for executing Redis commands on a [Redis](#) data store. It supports:

- batch queries
- transaction

## inverno-redis-lettuce

The Inverno Redis client Lettuce implementation module provides Redis implementation on top of [Lettuce](#) async pool.

It also exposes a Redis Client bean backed by a Lettuce client and created using the module's configuration. It can be used as is to send commands to a Redis data store.

## inverno-security

The Inverno Security module specifies an API for authenticating request to an application and controlling the access to protected services or resources. It provides:

- User/password authentication against a user repository (in-memory, Redis...).
- Token based authentication.
- Strong user identification against a user repository (in-memory, Redis...).
- Secured password encoding using message digest, Argon2, Password-Based Key Derivation Function (PBKDF2), BCrypt, SCrypt...
- Role-based access control.
- Permission-based access control.

## inverno-security-http

The Inverno Security HTTP module is an extension to the Inverno Security module that provides a specific API and base implementations for securing applications accessed via HTTP. It provides supports for:

- HTTP basic authentication scheme.
- HTTP digest authentication scheme.
- Form based authentication.
- Cross-origin resource sharing support CORS.
- Protection against Cross-site request forgery attack CSRF.

## inverno-security-ldap

The Inverno Security LDAP module is an extension to the Inverno Security module that provides support for authentication and identification against LDAP and Active Directory servers.

## inverno-security-jose

The Inverno Security JOSE module is a complete implementation of JSON Object Signing and Encryption RFCs. It provides:

- a JWK service used to manipulate JSON Web Key as specified by [RFC 7517](#) and [RFC 7518](#).
- a JWS service used to create and validate JWS tokens as specified by [RFC 7515](#).
- a JWE service used to create and decrypt JWE tokens as specified by [RFC 7516](#).
- a JWT service used to create, validate or decrypt JSON Web Tokens as JWS or JWE as specified by [RFC 7519](#).
- JWS and JWE compact and JSON representations support.
- JSON Web Key Thumbprint support as specified by [RFC 7638](#).
- support for JWS Unencoded Payload Option as specified by [RFC 7797](#).
- CFRG Elliptic Curve Diffie-Hellman (ECDH) and Signatures support as specified by [RFC 8037](#).
- CBOR Object Signing and Encryption (COSE) as specified by [RFC 8812](#).

## inverno-sql

The Inverno SQL client module specifies a reactive API for executing SQL statements on a RDBMS. It supports:

- prepared statement
- batch execution
- transaction

## inverno-sql-vertx

The Inverno SQL client Vert.x implementation module provides SQL Client implementations on top of [Vert.x](#) pool and pooled client.

It also exposes a pool based Sql Client bean created using the module's configuration that can be used as is to query a RDBMS.

## inverno-web

The Inverno Web module provides advanced features on top of the HTTP server module, including:

- request routing based on path, path pattern, HTTP method, request and response content negotiation including request and response content type and language of the response.
- path parameters
- interceptors



- transparent payload conversion based on the content type of the request or the response from raw representation (arrays of bytes) to Java objects
- transparent parameter (path, cookie, header, query...) conversion from string to Java objects
- static resource handler to serve static resources from various location based on the resource API
- a complete set of annotations for easy REST controller development

REST controllers can be easily defined using annotations which are processed by the Inverno compiler to generate the Web server configuration. The compiler also checks that everything is in order as for example that there are no conflicting routes.

## Inverno Tools



The Inverno framework provides tools for running and building modular Java applications and Inverno applications in particular. It allows for instance to create native runtime and application images providing all the dependencies required to run a modular application. It is also possible to build Docker and [OCI](#) images.

## Inverno Maven Plugin

The [Inverno Maven Plugin](#) provides specific goals to:

- run a modular Java application.
- start/stop a modular Java application during the build process to execute integration tests.
- build native a runtime image containing a set of modules and their dependencies creating a light Java runtime.
- build native an application image containing an application and all its dependencies into an easy to install platform dependent package (eg. `.deb`, `.rpm`, `.dmg`, `.exe`, `.msi`...).
- build docker or OCI images of an application into a tarball, a Docker daemon or a container image registry.

The plugin requires [JDK](#) 15+ and [Apache Maven](#) 3.6.0 or later.

# 3

## Inverno Distribution

---



The Inverno distribution provides a parent POM `io.inverno.dist:inverno-parent` and a BOM `io.inverno.dist:inverno-dependencies` for developing Inverno components and applications.

The parent POM inherits from the BOM which inherits from the [Inverno OSS parent](#) POM. It provides basic build configuration for building Inverno components and applications, including dependency management and plugins configuration. It especially includes configuration for the [Inverno Maven plugin](#).

The BOM specifies the [Inverno core](#) and [Inverno modules](#) dependencies as well as OSS dependencies.

The Inverno distribution thus defines a consistent sets of dependencies and configuration for developing, building, packaging and distributing Inverno components and applications. Upgrading the Inverno framework version of a project boils down to upgrade the Inverno distribution version which is the version of the Inverno parent POM or the Inverno BOM.

## Requirements

The Inverno framework requires [JDK](#) 15 or later and [Apache Maven](#) 3.6.0 or later.

## Creating an Inverno project

The recommended way to start a new Inverno project is to create a Maven project which inherits from the `io.inverno.dist:inverno-parent` project, we might also want to add a dependency to `io.inverno:inverno-core` in order to create an Inverno module with IoC/DI:

```

<project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/maven-
4.0.0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <parent>
    <groupId>io.inverno.dist</groupId>
    <artifactId>inverno-parent</artifactId>
    <version>1.5.3</version>
  </parent>
  <groupId>io.inverno.example</groupId>
  <artifactId>sample-app</artifactId>
  <version>1.0.0-SNAPSHOT</version>

  <dependencies>
    <dependency>
      <groupId>io.inverno</groupId>
      <artifactId>inverno-core</artifactId>
    </dependency>
  </dependencies>
</project>

```

That is all we need to develop, run, build, package and distribute a basic Inverno component or application. The Inverno parent POM provides dependency management and Java compiler configuration to invoke the Inverno compiler during the build process as well as Inverno tools configuration to be able to run and package the Inverno component or application.

If it is not possible to inherit from the Inverno parent POM, we can also declare the Inverno BOM `io.inverno.dist:inverno-dependencies` in the `<dependencyManagement/>` section to benefit from dependency management but loosing plugins configuration which must then be recovered from the Inverno parent POM.

```

<project>
  <dependencyManagement>
    <dependencies>
      <dependency>
        <groupId>io.inverno.dist</groupId>
        <artifactId>inverno-dependencies</artifactId>
        <version>1.5.3</version>
        <type>pom</type>
        <scope>import</scope>
      </dependency>
    </dependencies>
  </dependencyManagement>
</project>

```

Inverno modules dependencies can be added in the `<dependencies/>` section of the project POM. For instance the following dependencies can be added to develop a REST microservice application:

```

<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-boot</artifactId>
    </dependency>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-web</artifactId>
    </dependency>
  </dependencies>
</project>

```

Please refer to the [Inverno core documentation](#) and [Inverno modules documentation](#) to learn how to develop with IoC/DI and how to use Inverno modules.

## Developing a simple Inverno application

We can now start developing a sample REST application. An Inverno component or application is a regular Java module annotated with `@io.inverno.core.annotation.Module`, so the first thing we need to do is to create Java module descriptor `module-info.java` under `src/main/java` which is where Maven finds the sources to compile.

```

@io.inverno.core.annotation.Module
module io.inverno.example.sample_app {
  requires io.inverno.mod.boot;
  requires io.inverno.mod.web;
}

```

Note that we declared the `io.inverno.mod.boot` and `io.inverno.mod.web` module dependencies since we want to create a REST application, please refer to the [Inverno modules documentation](#) to learn more.

We then can create the main class of our sample REST application in `src/main/java/io/inverno/example/sample_app/App.java`:

```

package io.inverno.example.sample_app;

import io.inverno.core.annotation.Bean;
import io.inverno.core.v1.Application;
import io.inverno.mod.base.resource.MediaTypees;
import io.inverno.mod.web.annotation.WebController;
import io.inverno.mod.web.annotation.WebRoute;

@Bean
@WebController
public class App {

    @WebRoute( path = "/message", produces = MediaTypees.TEXT_PLAIN)
    public String getMessage() {
        return "Hello, world!";
    }

    public static void main(String[] args) {
        Application.with(new Sample_app.Builder()).run();
    }
}

```

## Configuring logging

Inverno framework is using [Log4j 2](#) for logging, Inverno application logging can be activated by adding the dependency to `org.apache.logging.log4j:log4j-core`:

```

<project>
  <dependencies>
    <dependency>
      <groupId>org.apache.logging.log4j</groupId>
      <artifactId>log4j-core</artifactId>
    </dependency>
  </dependencies>
</project>

```

If you don't include this dependency at runtime, Log4j falls back to the `SimpleLogger` implementation provided with the API and configured using `org.apache.logging.log4j.simplelog.*` system properties. The log level can then be configured by setting `-Dorg.apache.logging.log4j.simplelog.level=INFO` system property when running the application.

Log4j 2 provides a default configuration with a default root logger level set to `ERROR`, resulting in no info messages being output when starting an application. This can be changed by setting `-Dorg.apache.logging.log4j.level=INFO` system property when running the application.

However the recommended way is to provide a specific `log4j2.xml` logging configuration file in the project resources under `src/main/resources`:

```

<?xml version="1.0" encoding="UTF-8"?>
<Configuration xmlns="http://logging.apache.org/log4j/2.0/config"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://logging.apache.org/log4j/2.0/config
https://raw.githubusercontent.com/apache/logging-log4j2/rel/2.14.0/log4j-
core/src/main/resources/Log4j-config.xsd"
  status="WARN" shutdownHook="disable">

  <Appenders>
    <Console name="LogToConsole" target="SYSTEM_OUT">
      <PatternLayout pattern="%d{DEFAULT} %highlight{%-5level} [%t] %c{1.} - %msg%n%ex"/>
    </Console>
  </Appenders>
  <Loggers>
    <Root level="info">
      <AppenderRef ref="LogToConsole"/>
    </Root>
  </Loggers>
</Configuration>

```

Note that the Log4j shutdown hook must be disabled so as not to interfere with the Inverno application shutdown hook, if it is not disabled, application shutdown logs might be dropped.

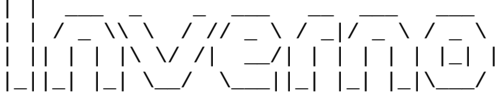
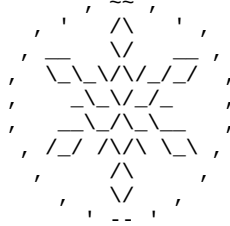
We could have chosen to provide a default logging configuration in the Inverno framework itself, but we preferred to stick to standard Log4j 2 configuration rules in order to keep things simple so please refer to the [Log4j 2 configuration documentation](#) to learn how to configure logging.

## Running the application

The application is now ready and can be run using the `inverno:run` goal:

```
$ mvn inverno:run
```

```
...
[INFO] --- inverno-maven-plugin:1.3.1:run (default-cli) @ sample-app ---
[INFO] Running project: io.inverno.example.sample_app@1.0.0-SNAPSHOT...
[===== 100 % =====]
2021-04-08 23:50:35,261 INFO [main] i.w.c.v.Application - Inverno is starting...
```

  
-- 1.5.1 --

Java runtime : OpenJDK Runtime Environment  
Java version : 16+36-2231  
Java home : /home/jkuhn/Devel/jdk/jdk-16  
  
Application module : io.inverno.example.sample\_app  
Application version : 1.0.0-SNAPSHOT  
Application class : io.inverno.example.sample\_app.App  
  
Modules :  
\* ...

```
2021-04-08 23:50:35,266 INFO [main] i.w.e.s.Sample_app - Starting Module
io.inverno.example.sample_app...
2021-04-08 23:50:35,266 INFO [main] i.w.m.b.Boot - Starting Module io.inverno.mod.boot...
2021-04-08 23:50:35,446 INFO [main] i.w.m.b.Boot - Module io.inverno.mod.boot started in 179ms
2021-04-08 23:50:35,446 INFO [main] i.w.m.w.Web - Starting Module io.inverno.mod.web...
2021-04-08 23:50:35,446 INFO [main] i.w.m.h.s.Server - Starting Module
io.inverno.mod.http.server...
2021-04-08 23:50:35,446 INFO [main] i.w.m.h.b.Base - Starting Module io.inverno.mod.http.base...
2021-04-08 23:50:35,450 INFO [main] i.w.m.h.b.Base - Module io.inverno.mod.http.base started in 3ms
2021-04-08 23:50:35,545 INFO [main] i.w.m.h.s.i.HttpServer - HTTP Server (nio) listening on
http://0.0.0.0:8080
2021-04-08 23:50:35,546 INFO [main] i.w.m.h.s.Server - Module io.inverno.mod.http.server started in
99ms
2021-04-08 23:50:35,546 INFO [main] i.w.m.w.Web - Module io.inverno.mod.web started in 99ms
2021-04-08 23:50:35,546 INFO [main] i.w.e.s.Sample_app - Module io.inverno.example.sample_app
started in 281ms
```

We can now test the application:

```
$ curl http://127.0.0.1:8080/message
Hello, world!
```

The application can be gracefully shutdown by pressing **Ctrl-c**.

## Building the application image

In order to create a native image containing the application and all its dependencies including JDK's dependencies, we can simply invoke the **inverno:build-app** goal:

```
$ mvn inverno:build-app
```

```
...
[INFO] Building application image: /home/jkuhn/Devel/git/frmk/io.inverno.example.sample-
app/target/maven-inverno/application_linux_amd64/sample-app-1.0.0-SNAPSHOT...
[===== 67 % =====>]
] Creating archive sample-app-1.0.0-SNAPSHOT-application_linux_amd64.zip...
```

This uses `jpackage` tool which is an incubating feature in JDK<16, if you intend to build an application image with an old JDK, you'll need to explicitly add the `jdk.incubator.jpackage` module in `MAVEN_OPTS`:

```
$ export MAVEN_OPTS="--add-modules jdk.incubator.jpackage"
```

This will create a ZIP archive containing a native application distribution `target/sample-app-1.0.0-SNAPSHOT-application_linux_amd64.zip` which will be deployed to the local Maven repository and eventually to a remote Maven repository.

Then in order to install the application on a compatible platform, we just need to download the archive corresponding to the platform, extract it to some location and run the application. Luckily for us this can be done quite easily with Maven dependency plugin:

```
$ mvn dependency:unpack -Dartifact=io.inverno.example:sample-app:1.0.0-SNAPSHOT:zip:application_linux_amd64 -DoutputDirectory=./
...
$ ./sample-app-1.0.0-SNAPSHOT/bin/sample-app
...
```

It is also possible to create platform specific package such as `.deb` or a `.msi` by defining particular formats in the Inverno Maven plugin configuration:

```
<project>
  <build>
    <plugins>
      <plugin>
        <groupId>io.inverno.tool</groupId>
        <artifactId>inverno-maven-plugin</artifactId>
        <executions>
          <execution>
            <id>build-app</id>
            <phase>package</phase>
            <goals>
              <goal>build-app</goal>
            </goals>
            <configuration>
              <formats>
                <format>zip</format>
                <format>deb</format>
              </formats>
            </configuration>
          </execution>
        </executions>
      </plugin>
    </plugins>
  </build>
</project>

$ mvn package
...
```

Note that there is no cross-platform support and a given platform specific format must be built on the platform it runs on.



Such platform-specific package can then be downloaded and installed using the right package manager:

```
$ mvn dependency:copy -Dartifact=io.inverno.example:sample-app:1.0.0-SNAPSHOT:deb:application_linux_amd64 -DoutputDirectory=./
...
$ sudo dpkg -i sample-app-1.0.0-SNAPSHOT-application_linux_amd64.deb
...
$ /opt/sample-app/bin/sample-app
...
```

The Inverno Maven plugin allows to create various application images including Docker or OCI container images, please refer to the [Inverno Maven plugin documentation](#) to learn more.

# 4

## Inverno Core

---

### Motivation

[Inversion of Control](#) and [Dependency Injection](#) principles are not new and many Java applications have been developed following these principles over the past two decades using frameworks such as Spring, CDI, Guice... However these recognized solutions might have some issues in practice especially with the way Java has evolved and how applications should be developed nowadays.

Dependency injection errors like a missing dependency or a cycle in the dependency graph are often reported at runtime when the application is started. Most of the time these issues are easy to fix but when considering big applications split into multiple modules developed by different people, it might become more complex. In any case you can't tell for sure if an application will start before you actually start it.

Most IoC/DI frameworks are black boxes, often considered as magical because one gets beans instantiated and wired altogether without understanding what just happened and it is indeed quite hard to figure out how it actually works. This is not a problem as long as everything works as expected but it can become one when you actually need to troubleshoot a failing application.

Beans instantiation and wiring are done at runtime using Java reflection which offers all the advantages of Java dynamic linking at the expense of some performance overhead. Classpath scanning, instantiation and wiring process indeed takes some time and prevents just-in-time compilation optimization making application startup quite slow.

Although IoC frameworks make the development of modular applications easier, they often require a rigorous methodology to make it the right way. For instance, you must know precisely what components are provided and/or required by all the modules composing an application and make sure one doesn't provide a component that might interfere with another.

These points are very high level, please have a look at this [article](#) if you like to learn more about the general ideas behind the Inverno framework. The Inverno framework proposes a new approach of IoC/DI principles consistent with latest developments of the Java™ platform and perfectly adapted to the development of modern applications in Java.

## Prerequisites

In this documentation, we'll assume that you have a working knowledge of [Inversion of Control](#) and [Dependency Injection](#) principles as well as [Object Oriented Programming](#).

## Overview

The Inverno framework is different in many ways and tries to address previous issues. Its main difference is that it doesn't rely on Java reflection at all to instantiate the beans composing an application (IoC) and wire them together (DI), this is actually done by a class generated by the Inverno compiler at compile time.

Since beans and their dependencies are determined at compile time, errors can be raised precisely when they make sense during development or at build time.

There is also no need for complex runtime libraries since the complexity is handled by the compiler which generates a readable class providing only what is required at runtime. This presents two advantages, first applications have a small footprint and start fast since most of the processing is already done and no reflection is involved. Secondly you will be able to actually debug all parts of your application since nothing is hidden behind a complex library, you can actually see when the beans are instantiated with the `new` operator opening rooms to other compile and runtime optimization as well.

The framework also fully embraces the modular system introduced in Java 9 which basically imposes to develop with modularity in mind. An Inverno module only exposes the beans that must be exposed to other modules and it clearly indicates the beans it requires to operate. All this makes modular development safer, clearer and more natural.

## Modules and Beans

Inversion of control and dependency injection principles have proven to be an elegant and efficient way to create applications in an Object Oriented Programming language. A Java application basically consists in a set of interconnected objects.

An Inverno application adds a modular dimension to these principles, the objects or the **beans** composing the application are created and connected in one or more isolated **modules** which are themselves composed in the **application**.

A **module** encapsulates several beans and possibly other modules. It specifies the dependencies it needs to operate and only exposes the beans that need to be exposed from the module perspective. As a result it is isolated from the rest of the application, it is unaware of how and where it is used and it actually doesn't care as long as its requirements are met. It really resembles a class which makes it very familiar to use.

A **bean** is a component of a module and more widely an application. It has required and optional dependencies provided by the module when a bean instance is created.

The **Inverno compiler** is an annotation processor which runs inside the Java compiler and generates module classes based on Inverno annotations found on the modules and classes being compiled.

## Java module system

Before you can create your first Inverno module, you must first understand what a Java module is and how it might change your life as a Java developer. If you are already familiar with it, you can skip that section and go directly to the [project setup](#) section.

The Java module system has been introduced in Java 9 mostly to modularize the overgrowing Java runtime library which is now split into multiple interdependent modules loaded when you need them at runtime or compile time. This basically means that the size of the Java runtime you need to compile and/or run your application now depends on your application's needs which is a pretty big improvement.

If you know OSGI or Maven already, you might say that modules have existed in Java for a long time but now they are fully integrated into the language, the compiler and the runtime. You can create a Java module, specify what packages are exposed and what dependencies are required and the good part is that both the compiler and JVM tell you when you do something wrong being as close as possible to the code, there's no more xml or manifest files to care about.

So how do you create a Java module? There is plenty of documentation you can read to have a complete and deep understanding of the Java module system, here we will only explain what you need to know to develop regular Inverno modules.

A Java module is specified in a `module-info.java` file located in the default package. Let's assume you want to create module `io.inverno.example.sample`, you can create the following file structure:

```
src
├── io.inverno.example.sample
│   ├── io
│   │   ├── inverno
│   │   │   ├── example
│   │   │   │   ├── sample
│   │   │   │   │   ├── internal
│   │   │   │   │   │   └── ...
│   │   │   │   └── ...
│   │   └── module-info.java
```

This is one way to organize the code, the only important thing is to put the `module-info.java` descriptor in the default package.

Now let's have a closer look at the module descriptor:

```
module io.inverno.example.sample {           // 1
    exports io.inverno.example.sample;      // 2
}
```

1. A module is declared using a familiar syntax starting with the `module` keyword followed by the name of the module which must be a valid Java name.
2. The `io.inverno.example.sample` module exports the `io.inverno.example.sample` package which means that other modules can only access public types contained in that package. Any type defined in another package within that module is only visible from within the module following usual Java visibility rules (default, public, protected, private). This basically defines a new level of encapsulation at module level. For instance, types in package `io.inverno.example.sample.internal` are not accessible to other modules regardless of their visibility.

Now let's say you need to use some external types defined and exported in another module `io.inverno.example.other`:

```
src
├── io.inverno.example.sample
│   ├── ...
│   └── module-info.java
└── io.inverno.example.other
    ├── ...
    └── module-info.java
```

If you try to reference any of these types in `io.inverno.example.sample` module as is the compiler will complain with explicit visibility errors unless you specify that `io.inverno.example.sample` module requires `io.inverno.example.other` module:

```
module io.inverno.example.sample {
    requires io.inverno.example.other;

    exports io.inverno.example.sample;
}
```

You should now be able to reference any public types defined in a package exported in `io.inverno.example.other` module.

The modular system has also changed the way Java applications are built and run. Before we used to specify a classpath listing the locations where the Java compiler and the JVM should look for application's classes whereas now we should specify a module path listing the locations of modules and forget about the classpath.

If we consider previous modules, they are compiled and run as follows:

```
> javac --module-source-path src -d jmods --module io.inverno.example.sample --module
io.inverno.example.other
> java --module-path jmods/ --module io.inverno.example.sample/io.inverno.example.sample.Sample
```

There are other subtleties like transitive dependencies, service providers or opened modules and cool features like jmod packaging and the `jlink` tool but for now that's pretty much all you need to know to develop Inverno modules which are basically instrumented Java modules.

You should now have a basic understanding of how an Inverno application is built and what Java technologies are involved. An Inverno application results from the composition of multiple isolated modules which create and wire the beans making up the application. Almost everything is done at compile time where module classes are generated.

# Project Setup

## Maven

The easiest way to setup an Inverno module project is to start by creating a regular Java Maven project which inherits from `io.inverno.dist:inverno-parent` project and depends on

`io.inverno:inverno-core`:

```
<project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/maven-
4.0.0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <parent>
    <groupId>io.inverno.dist</groupId>
    <artifactId>inverno-parent</artifactId>
    <version>1.5.3</version>
  </parent>
  <groupId>io.inverno.example</groupId>
  <artifactId>sample</artifactId>
  <version>1.0.0-SNAPSHOT</version>

  ...
  <dependencies>
    ...
    <dependency>
      <groupId>io.inverno</groupId>
      <artifactId>inverno-core</artifactId>
    </dependency>
    ...
  </dependencies>
  ...
</project>
```

Then you have to add a module descriptor to make it a Java module project. An Inverno module requires `io.inverno.core` and `io.inverno.core.annotation` modules. If you want your module to be used in other modules it must also export the package where the module class is generated by the Inverno compiler which is the module name by default. Remember that an Inverno module is materialized in a regular Java class subject to the same rules as any other class in a Java module.

```
module io.inverno.example.sample {
  requires io.inverno.core;
  requires io.inverno.core.annotation;

  exports io.inverno.example.sample;
}
```

If you do not want your project to inherit from `io.inverno.dist:inverno-parent` project, you'll have to explicitly specify compiler source and target version ( $\geq 9$ ), dependencies version and configure the Maven compiler plugin to invoke the Inverno compiler.

```

<project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/maven-
4.0.0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <groupId>io.inverno.example</groupId>
  <artifactId>sample</artifactId>
  <version>1.0.0-SNAPSHOT</version>

  <properties>
    <project.build.sourceEncoding>UTF-8</project.build.sourceEncoding>
    <maven.compiler.source>11</maven.compiler.source>
    <maven.compiler.target>11</maven.compiler.target>
    <version.inverno>1.5.1</version.inverno>
    <version.inverno.dist>1.5.3</version.inverno.dist>
  </properties>

  <dependencyManagement>
    <dependencies>
      <dependency>
        <groupId>io.inverno.dist</groupId>
        <artifactId>inverno-dependencies</artifactId>
        <version>${version.inverno.dist}</version>
        <type>pom</type>
        <scope>import</scope>
      </dependency>
    </dependencies>
  </dependencyManagement>

  <dependencies>
    <dependency>
      <groupId>io.inverno</groupId>
      <artifactId>inverno-core</artifactId>
    </dependency>
  </dependencies>

  <build>
    <plugins>
      ...
      <plugin>
        <artifactId>maven-compiler-plugin</artifactId>
        <configuration>
          <annotationProcessorPaths>
            <path>
              <groupId>io.inverno</groupId>
              <artifactId>inverno-core-compiler</artifactId>
              <version>${version.inverno}</version>
            </path>
          </annotationProcessorPaths>
        </configuration>
      </plugin>
      ...
    </plugins>
  </build>
</project>

```

An Inverno module is built just as a regular Maven project using maven commands (compile, package, install...). The module class is generated and compiled during the **compile** phase and included in the resulting JAR file during the **package** phase. If anything related to IoC/DI goes wrong during compilation, the compilation fails with explicit compilation errors reported by the Inverno compiler.

## Gradle

Since version 6.4, it is also possible to use [Gradle](#) to build Inverno module projects. Here is a sample **build.gradle** file:

```
plugins {
    id 'application'
}

repositories {
    mavenCentral()
}

dependencies {
    implementation 'io.inverno:inverno-core:1.5.1'
    annotationProcessor 'io.inverno:inverno-core-compiler:1.5.1'
}

java {
    modularity.inferModulePath = true
    sourceCompatibility = JavaVersion.VERSION_11
    targetCompatibility = JavaVersion.VERSION_11
}

application {
    mainModule = 'io.inverno.example.hello'
    mainClassName = 'io.inverno.example.hello.App'
}
```

## Bean

As you already know, a Java application can be reduced to the composition of objects working together. In an Inverno application, these objects are instantiated and injected into each other by one or more modules. Inside a module, a bean basically specifies what it needs to create a bean instance (DI) and how to obtain it (IoC).

A bean and a bean instance are two different things that should not be confused. A bean can result in multiple bean instances in the application whereas a bean instance always refers to exactly one bean. A bean is like a plan used to create instances.

A bean is fully identified by its name and the module in which it resides. The following notation is used to represent a bean qualified name: **[MODULE] : [BEAN]**. As a consequence, two beans with the same name cannot exist in the same module but it is safe to have multiple beans with the same name in different modules.



# Module Bean

Module bean is the primary type of beans you can create in an Inverno module. It is defined by a concrete class annotated with the `@Bean` annotation.

```
import io.inverno.core.annotation.Bean;
```

```
@Bean
public class SomeBean {
    ...
}
```

In the previous code we created a bean of type `SomeBean`. At compile time, the Inverno compiler will include it in the generated module class that you'll eventually use at runtime to obtain `SomeBean` instances.

By default, a bean is named after the simple name of the class starting with a lower case (eg. `someBean` in our previous example). This can be specified in the annotation using the `name` attribute:

```
@Bean(name="customSomeBean")
public class SomeBean {
    ...
}
```

# Wrapper Bean

A wrapper bean is a particular form of bean used to define beans whose code cannot be instrumented with Inverno annotations or that require more complex logic to create the instance. This is especially the case for legacy code or third party libraries.

A wrapper bean is defined by a concrete class annotated with both `@Bean` and `@Wrapper` annotations which basically wraps the actual bean instance and include the instantiation, initialization and destruction logic. It must implement the `Supplier<E>` interface which specifies the actual type of the bean as formal parameter.

```
@Bean
@Wrapper
public class SomeWrapperBean implements Supplier<SomeLegacyBean> {

    private SomeLegacyBean instance;

    public SomeWrapperBean() {
        // Creates the wrapped instance
        this.instance = ...
    }

    SomeLegacyBean get() {
        // Returns the wrapped instance
        return this.instance;
    }
    ...
}
```

In the previous code we created a bean of type `SomeLegacyBean`. One instance of the wrapper class is used to create exactly one bean instance and it lives as long as the bean instance is referenced.

Since a wrapper bean is annotated with `@Bean` annotation, it can be configured in the exact same way as a module bean except that it only applies to the wrapper instance which is responsible to configure the actual bean instance. The wrapper instance is never exposed, only the actual bean instance wrapped in it is exposed. As for module beans, `SomeLegacyBean` instances can be obtained using the generated Module class.

Note that since a new wrapper instance is created every time a new bean instance is requested, a wrapper class is not required to return a new or distinct result in the `get()` method. Nonetheless a wrapper instance is used to create, initialize and destroy exactly one instance of the supplied type and as a result it is good practice to have the wrapper instance always return the same bean instance. This is especially true and done naturally when initialization or destruction methods are specified.

When designing a prototype wrapper bean, particular care must be taken to make sure the wrapper does not hold a strong reference to the wrapped instance in order to prevent memory leak when a prototype bean instance is requested by the application. It is strongly advised to rely on `WeakReference<>` in that particular use case.

## Nested Bean

A nested bean is, as its name suggests, a bean inside a bean. A nested bean instance is obtained by invoking a particular method on another bean instance. Instances thus obtained participate in dependency injection but unlike other types of bean they do not follow any particular lifecycle or strategy, the implementor of the nested bean method is free to decide whether a new instance should be returned on each invocation.

A nested bean is declared in the class of a bean, by annotating a non-void method with no arguments with `@NestedBean` annotation. The name of a nested bean is given by the name of the bean providing the instance and the name of the annotated method following this notation:

`[MODULE] : [BEAN] . [METHOD_NAME]`.

```
@Bean
public class SomeBean {

    ...

    @NestedBean
    public SomeNestedBean nestedBean() {
        ...
    }
}
```

It is also possible to *cascade* nested beans.

## Overridable

A module bean or a wrapper bean can be declared as overridable which allows to override the bean inside the module by a socket bean of the same type.

An overridable bean is defined as a module bean or a wrapper bean whose class has been annotated with `@Overridable`. This basically tells the Inverno compiler to create an extra optional socket bean with the particular feature of being able to take over the bean when an instance is provided on module instantiation.

```
@Bean
@Overridable
public class SomeBean {

}
```

## Lifecycle

All bean instances follow the subsequent lifecycle in a module:

1. A bean instance is created
2. It is initialized
3. It is active
4. It is "eventually" destroyed

Let's examine each of these steps in details.

A bean instance is always created in a module, when a bean instance is created greatly depends on the context in which it is used, it can be created when a module instance is started or when it is required in the application. In order to create a bean instance the module must provide all the dependencies required by the bean. After that it sets any optional dependencies available on the instance thus obtained. This is actually when and where dependency injection takes place, this aspect will be covered more in details in following sections, for now all you have to know is that when requested the module creates a fully wired bean instance.

After that the module invokes initialization methods on the bean instance to initialize it. An initialization method is declared on the bean class using the `@Init` annotation:

```
@Bean
public class SomeBean {

    @Init
    public void init() {
        ...
    }
}
```

You can specify multiple initialization methods but the order in which they are invoked is undetermined. Inheritance is not considered here, only the methods annotated on the bean class are considered. Bean initialization is useful when you want to execute some code after dependency injection to make the bean instance fully functional (eg. initialize a connection pool, start a server socket...).

After that, the bean instance is active and can be used either directly by accessing it from the module or indirectly through another bean instance where it has been injected.

A bean instance is "eventually" destroyed, typically when its enclosing module instance is stopped. Just as you specified initialization methods, you can specify destruction methods to be invoked when a bean instance is destroyed using the `@Destroy` annotation:

```
@Bean
public class SomeBean {

    @Destroy
    public void destroy() {
        ...
    }
}
```

As for initialization methods, you can specify multiple destruction methods but the order in which they are invoked is undetermined and inheritance is also not considered. Bean destruction is useful when you need to free resources that have been allocated by the bean instance during application operation (eg. shutdown a connection pool, close a server socket...).

In case of wrapper beans, the initialization and destruction of a bean instance is delegated to the initialization and destruction methods specified on the wrapper bean which respectively initialize and destroy the actual bean instance wrapped in the wrapper bean.

```
@Bean
@Wrapper
public class SomeWrapperBean implements Supplier<SomeLegacyBean> {

    private SomeLegacyBean instance;

    public SomeWrapperBean() {
        // Creates the wrapped instance
        this.instance = ...
    }

    @Init
    public void init() {
        // Initialize the wrapped instance
        this.instance.start();
    }

    @Destroy
    public void destroy() {
        // Destroy the wrapped instance
        this.instance.stop();
    }
    ...
}
```

■

We stated here that all bean instances are eventually destroyed but this is actually not always the case. Depending on the bean strategy and the context in which it is used, it might not be destroyed at all, hopefully workarounds exist to make sure a bean instance is always properly destroyed. We'll cover this more in detail when we'll describe [bean strategies](#).

## Visibility

A bean can be assigned a public or private visibility. A public bean is exposed by the module to the rest of the application whereas a private bean is only visible from within the module.

Bean visibility is set in the `@Bean` annotation in the visibility attribute:

```
@Bean(visibility=Visibility.PUBLIC)
public class SomeBean {

}
```

## Strategy

A bean is always defined with a particular strategy which controls how a module should create a bean instance when one is requested, either during dependency injection when a module requires a bean instance to inject in another bean instance or during application operation when some application code requests a bean instance to a module instance.

## Singleton

The singleton strategy is the default strategy used when no explicit strategy is specified on a bean class. An Inverno module only creates one single instance for a singleton bean. That same instance is returned every time an instance of that bean is requested. It is then shared among all dependent beans through dependency injection and also the application if it has requested an instance.

A singleton bean is specified explicitly by setting the `strategy` attribute to `Strategy.SINGLETON` in the `@Bean` annotation:

```
@Bean(strategy = Strategy.SINGLETON)
public class SomeSingletonBean {

}
```

Modules easily support the bean lifecycle for singleton beans since a module instance holds singleton bean instances by design, they can then be properly destroyed when the module instance is stopped.

Particular care must be taken when a singleton bean instance is requested to a module instance by the application as the resulting reference will point to a *managed* instance which will be destroyed when the module instance is stopped leaving the instance referenced in the application in an unpredictable state.

A singleton bean is the basic building block of any application which explains why it is the default strategy. An application is basically made of multiple long living components rather than volatile disposable components. A server is a typical example of singleton bean, it is created when the application is started, initialized to accept requests and destroyed when the application is stopped.

A singleton instance is held by exactly one module instance, if you instantiate a module twice, you'll get two singleton bean instances, one in the first module instance and the other in the second module instance. This basically differs from the standard singleton pattern, you'll see more in detail why this actually matters when we'll describe [composite modules](#).

## Prototype

A prototype bean results in the creation of as many instances as requested. All dependent beans in the module get a different bean instance and each time a bean instance is requested to a module instance by the application a new instance is also created.

A prototype bean is specified by setting the `strategy` attribute to `Strategy.PROTOTYPE` in the `@Bean` annotation:

```
@Bean(strategy = Strategy.PROTOTYPE)
public class SomeBean {

}
```

Unlike singleton beans, modules can't always fully support the bean lifecycle for prototype beans. All prototype beans instances are kept in the module instance in order to destroy them when it is stopped. Modules use weak references to prevent memory leaks so that dereferenced instances are automatically removed from the internal registry when the garbage collector reclaims them. This works well for prototype bean instances injected into singleton bean instances since they are actually referenced until the module instance is stopped just like any singleton bean instance. It becomes tricky when a prototype bean instance is requested by the application. In that case, the prototype bean instance is removed from the module instance when it is dereferenced from the application and reclaimed by the garbage collector leaving no chance for the module instance to destroy it properly. The actual behavior is more subtle because a dereferenced prototype bean instance might actually be destroyed when a module is stopped before the instance is reclaimed by the garbage collector.

As a result, it is not recommended to define destruction methods on a prototype bean but if you really need to, you can make your bean implement `AutoCloseable`, specify the `close()` method as the unique destruction method and request prototype bean instances from the application using a try-with-resources block:

```
@Bean(strategy = Strategy.PROTOTYPE)
public class SomeBean implements AutoCloseable {

    @Destroy
    public void close() throws Exception {
        ...
    }
}
```

Then when requesting a prototype bean instance from the application:

```
try(SomeBean bean = module.someBean()) {
    ...
}
```

As soon as the program exits the try-with-resources block the bean instance is properly destroyed, then dereferenced and eventually reclaimed by the garbage collector and finally removed from the module instance. However you should make sure that the `close()` method can be called twice since it actually might.

Prototype beans should be used whenever there is a need to hold a state in a particular context. An HTTP client is a typical example of a stateful instance, different instances should be created and injected in singleton beans so they can deal with concurrency independently to make sure requests are sent only after a response to the previous request has been received.

That might not be the smartest way to use HTTP clients in an application but it gives you the idea.

Prototype beans can also be used to implement the factory pattern, just like a factory, you can request new bean instances on a module. Inverno framework makes this actually very powerful since there's no runtime overhead, modules can be created and used anywhere and you never have to worry about the boiler plate code that instantiates the bean since it is generated for you by the framework.

## Module

An Inverno module can be seen as an isolated collection of beans. The role of a module is to create and wire bean instances in order to expose logic to the application.

In practice, a module is materialized by the class generated by the Inverno compiler during compilation and which results from the processing of Inverno annotations.

A module is isolated from the rest of the application through its module class which clearly defines the beans exposed by the module and what it needs to operate. As a result, a module doesn't care when and how it is used in an application as long as its requirements are met.

Isolation is actually what makes the Inverno framework so special as it greatly simplifies the development of complex modular applications.

A module is defined as a regular Java module annotated with the `@Module` annotation:

```
@Module
Module io.inverno.sample.sampleModule {
    ...
}
```

## The module class

Java modules annotated with `@Module` will be processed by the Inverno compiler at compile time. The Inverno compiler generates one **module class** per module providing all the code required at runtime to create and wire bean instances.

This class is the entry point of a module and serve several purposes:

- encapsulate beans instances creation and wiring logic
- implement bean instance lifecycle
- specify required or optional module dependencies
- expose public beans
- hide private beans
- guarantee a proper isolation of the module within the application

This regular Java class can be instantiated like any other class. It relies on a minimal runtime library barely visible which makes it self-describing and very easy to use.

Let's see how it looks like for the `io.inverno.sample.sampleModule` module and `SomeBean` bean, the module class would be used as follows:

```
SampleModule module = new SampleModule.Builder().build(); // 1
module.start(); // 2

SomeBean someBean = module.someBean(); // 3
// Do something useful with someBean
module.stop(); // 4
```

1. The `SampleModule` class is instantiated
2. The module is started
3. The `SomeBean` instance is retrieved
4. Eventually the module is stopped



There are two important things to notice here, first you control when, where and how many times you want to instantiate a module, which brings great flexibility in the way modules are used in your application. For instance integrating an Inverno module in an existing code is pretty straightforward as it is plain old Java, it is also possible to create and use a module instance during application operation (eg. when processing a request). Secondly beans are exposed with their actual types through named methods which eventually produces more secure code because static type checking can (finally) be performed by the compiler.

Module classes provide dedicated builders to facilitate the creation of complex modules instances with multiple required and optional dependencies.

By default, the module class is named after the last identifier of the module name and generated in a package named after the module. The full class name can be specified in the annotation using the `className` attribute:

```
@Module(className="io.inverno.sample.CustomSampleModule")
Module io.inverno.sample.sampleModule {
    ...
}
```

The module class is like any other class in the module, if you want to use it outside the module you have to explicitly export its package in the module descriptor:

```
@Module
Module io.inverno.sample.sampleModule {
    exports io.inverno.sample.sampleModule;
}
```

Most of the time this is something you'll do especially if you want to create [composite modules](#), however if you only use the module class from within the module, typically in a main method or embedded in some other class, you won't have to do it.

Note that the Java compiler fails if you try to export a package which is empty before compilation, since the module class is generated this might actually happen, so you need to make sure the class will be generated in a package containing some code. This is not an ideal situation however a module usually defines and exports a package named after its name so this should solve the issue.

## Lifecycle

Just like a bean instance, a module follows a lifecycle:

1. A module instance is created
2. It is started
3. It is active
4. It is stopped

Let's examine each of these steps in details.

A module instance can be created directly in the application or indirectly inside a composite module. A module defines a dedicated `Builder` class that must be used to build the module instance. Relying on a builder is very helpful when considering complex modules with many required and optional dependencies.

The instance must then be started to make it operational. During this phase, all Inverno modules composed in the module are instantiated and started and all the beans defined in the module are created and initialized. Dependency injection is performed naturally as beans are created. Since everything has been validated at compile time, we know for sure that everything will work properly.

A module is actually composed by the beans it defines and the beans defined in the modules it composes. This is discussed in details in the [Modular application](#) section.

Once the module instance is active, beans are exposed to the application.

Finally, a module instance is stopped to release resources held by the beans instances. During this phase, beans are destroyed in the reverse order of their creation and composed Inverno modules are stopped.

## Module as component

Inverno modules are very flexible and can be used in many situations. You can for instance develop Inverno modules to create reusable software components. Such components would benefit from inversion of control and dependency injection capabilities offered by the framework without interfering with the applications that uses them. An Inverno module has also a very low runtime footprint since it creates objects and wires them in a fixed and deterministic way, it can then be created at any time in any situations.

## Standalone component

You can imagine a standalone module used to interface with an external system like a coffee maker module for example. From the outside a coffee maker is actually quite simple:

- it requires electricity to operate
- you have to fill it with coffee beans
- you have to supply some water as well
- then you can make some tasty coffee

From the inside on the other hand it can be much more complex than this, it is probably composed of multiple internal components that you actually don't care about as long as the coffee is good.

Let's try to imagine what kind of interface would be exposed by the `io.inverno.sample.coffeeMakerModule` module without anticipating any implementation.

First of all it would probably export the module's package as it is intended to be used from outside the module:

### module-info.java

```
@Module
Module io.inverno.sample.coffeeMakerModule {
    exports io.inverno.sample.coffeeMakerModule;
}
```

It might expose three singleton beans:

- `io.inverno.sample.coffeeMakerModule:coffeeBeansContainer` to be able to fill the coffee maker with beans
- `io.inverno.sample.coffeeMakerModule:waterReservoir` for water supply
- `io.inverno.sample.coffeeMakerModule:coffeeMaker` to actually make some coffee

### CoffeeBeansContainer

```
public interface CoffeeBeansContainer {
    void fill(CoffeeBean[] beans);
}
```

### WaterReservoir

```
public interface WaterReservoir {
    void fill(int waterQuantity);
}
```

### CoffeeMaker

```
public interface CoffeeMaker {
    Coffee make();
}
```

Inside a coffee shop application, you might instantiate several coffee maker modules used in the following way:

```

PowerSupply powerSupply = ... // Get some
power supply

CoffeeMakerModule coffeeMakerModule = new CoffeeMakerModule.Builder(powerSupply).build();
coffeeMakerModule.start();

ArabicaCoffeeBeans[] coffeeBeans = ... // Get some
tasty coffee beans
coffeeMakerModule.coffeeBeansContainer().fill(coffeeBeans); // fill the
coffee beans container
coffeeMakerModule.waterReservoir().fill(1.5); // fill the
water reservoir with 1.5 Liters

CoffeeMaker coffeeMaker = coffeeMakerModule.coffeeMaker(); // Get the
coffee maker instance

Coffee coffee_1 = coffeeMaker.make(); // Deliver some
tasty coffees
...
Coffee coffee_n = coffeeMaker.make();

coffeeMakerModule.stop();

```

The goal of this example was to show the benefits of using Inverno modules as standalone components in an application. As you can see:

- implementation details are completely hidden: you don't know and you don't have to know how the beans container, the water reservoir and the coffee maker are working together.
- dependencies are clearly exposed: you must provide some power supply to instantiate the module.
- only significant functionalities are exposed.
- if you look closely, you'll see that no particular technical framework is visible: from a code perspective, the application doesn't see and don't need to know it is using an Inverno module, everything is also statically typed and self-describing.

## Factory component

You can also create a module as a generic factory or builder to ease the creation of complex objects. If we consider previous example from a different perspective, we can imagine a factory module that could be used to build coffee makers from raw materials.

It would also probably export the module's package so it can be used from outside the module:

### module-info.java

```

@Module
Module io.inverno.sample.coffeeMakerFactoryModule {
    exports io.inverno.sample.coffeeMakerFactoryModule;
}

```

Then it would expose the `io.inverno.sample.coffeeMakerFactoryModule:coffeeMaker` prototype bean:

```

public interface CoffeeMaker {

    void fillWithCoffeeBeans(CoffeeBeans[] beans);

    void filleWithWater();

    Coffee makeCoffee();
}

```

Inside a cooking appliances factory application, you might instantiate one or more coffee maker factory module to produce coffee makers:

```

CoffeeMakerFactoryModule coffeeMakerFactoryModule = new
CoffeeMakerFactoryModule.Builder(rawMaterials...).build();
coffeeMakerFactoryModule.start();

CoffeeMaker coffeeMaker_1 = coffeeMakerFactoryModule.coffeeMaker(); // We can massively produce
coffee makers
...
CoffeeMaker coffeeMaker_n = coffeeMakerFactoryModule.coffeeMaker();

coffeeMakerFactoryModule.stop();

```

The context and the approach are clearly different here, the purpose of a factory component module is to enable developers to use IoC/DI to easily create complex objects.

## Processing component

Dependency Injection is mostly about interconnecting objects to form an application, but this is more a consequence of how IoC/DI frameworks are designed than an absolute fact. An Inverno module is cheap, it can also be created and used during the operation of an application to process requests. This makes it possible to have data objects or contextual objects injected and used in bean instances.

Let's say we have created a highly customizable coffee maker, capable of producing a coffee based on many parameters: steam pressure, temperature, grinding size... These parameters have to be used in various components of the coffee maker. These data have to be provided each time a customer orders a coffee

Propagating the right data to the right coffee maker component can be a tedious task. An Inverno module can be created to inject data where they are needed based on the dependencies of each beans composing the coffee maker module and eventually process the request.

```

public Coffee orderCoffee(Param_1 p1, Param_2 p2, ... Param_n pn) {
    // Receive a large amount of parameters to make a coffee

    try {
        CoffeeMakerModule coffeeMakerFactoryModule = new CoffeeMakerFactoryModule.Builder(p1, p2,
... pn).build(); // Parameters are injected only where they are needed
        coffeeMakerModule.start();

        return coffeeMakerModule.coffeeMaker().makeCoffee();
    }
    finally {
        coffeeMakerFactoryModule.stop();
    }
}

```

You can then benefit from dependency injection inside the business logic, performance shouldn't be impacted by bean instantiation or dependency injection logic because the creation of a module instance is no different than creating some objects with the **new** operator and invoking some setter methods. This is especially interesting when you have to process very complex requests with a lot of input data.

## Module as application

An Inverno module can also be used to bootstrap a whole application. In such situation one single Inverno module is started as an application in the main method of a class. This class can be defined in the same module but this is not mandatory as long as it has access to the application module. The role of an application module is to create and start all the components of the application.

```

public static void main(String[] args) {
    CoffeeMakerModule coffeeMakerModule = Application.with(new
CoffeeMakerModule.Builder(...)).run();
    ...
}

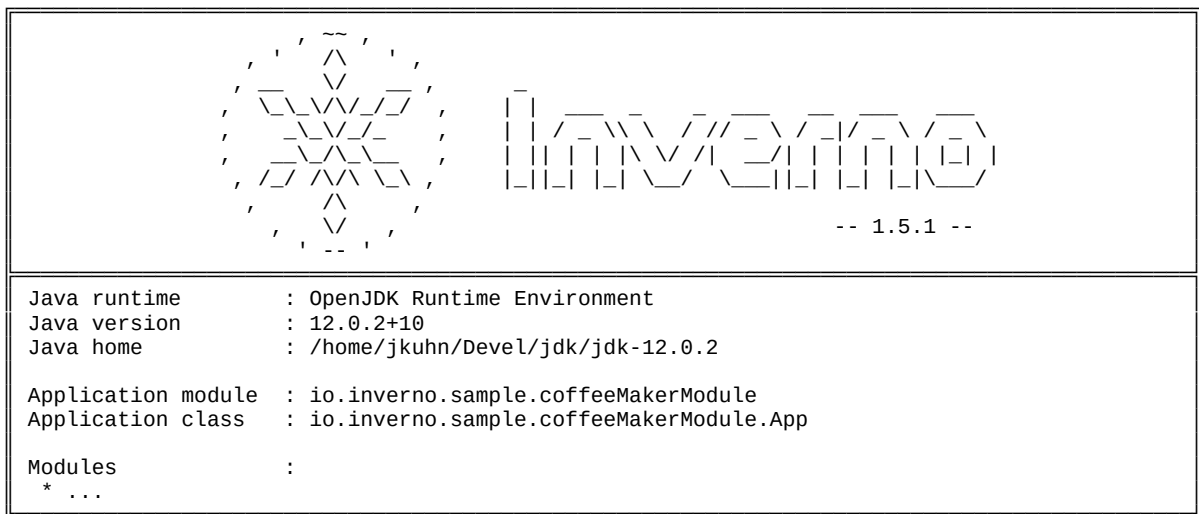
```

An application module is basically a regular module whose lifecycle is managed by the **Application** class. A module instance is created and started when the **run()** method is invoked and eventually stopped when the JVM shuts down.

Note that this involves a shutdown hook, as a consequence there is actually no guarantee that the module will be stopped especially if the JVM is not gracefully shut down.

Furthermore, an Inverno application outputs a customizable **Banner** on startup providing useful environment information in the application log.

```
mars 04, 2020 1:14:27 PM io.inverno.core.v1.Application run
INFO: Inverno is starting...
```



```
mars 04, 2020 1:14:27 PM io.inverno.core.v1.Module start
...
```

The **StandardBanner** is displayed by default but you can specify custom implementations as well:

```
public static void main(String[] args) {
    CustomBanner customBanner = ...
    CoffeeMakerModule coffeeMakerModule = Application.with(new
CoffeeMakerModule.Builder(...)).banner(customBanner).run();
    ...
}
```

## Dependency Injection

[Dependency Injection](#) principle is at the heart of the Inverno framework. Inside an Inverno module, beans instances are wired into each other based on their respective types and dependencies.

In order to understand how this works, you could imagine that each bean exposes multiple sockets and that multiple wires leave the bean, as many as necessary. After creating and initializing bean instances, the module has to plug these wires into compatible sockets. The type of the wire, which is the type of the bean, must match the type of the socket, which is the type of the dependency defined in the bean.

The result is modeled in a graph of beans built at compile time by the Inverno compiler which checks that it is a directed acyclic graph (ie. there's no cycles in the graph) and that there is a plug in each required socket. If everything is correct, a module class implementing the graph is created.

Dependency injection is validated and fully determined at compile time, the module class just instantiates and injects beans in a predetermined order without having to worry about missing dependencies or dependency cycles amongst others.

-

## Bean Socket

A **bean socket** designates a bean dependency. A bean can have two kinds of dependencies and then define two kinds of sockets: required and optional. Required dependencies must be resolved to create an operational bean instance whereas optional dependencies add extra capabilities to the bean instance. As a consequence, a module has to wire every required sockets, the Inverno compiler actually raises compilation errors on beans with unresolved required sockets.

The Inverno framework tries to be as less intrusive as possible, a bean specifies its sockets using standard Java as constructor arguments for required sockets and setter methods for optional sockets. Creating a bean is then very natural.

A bean socket is fully identified by its name, the name of the bean which defines it and the module in which the bean resides. The following notation is used to represent a bean socket qualified name: `[MODULE]:[BEAN]:[SOCKET_NAME]`. On a given bean in a given module, it is not possible to specify two sockets with the same name.

Let's go back to our coffee maker example and define the dependencies of the `CoffeeMaker` bean.

### CoffeeMakerImpl

`@Bean`

```
public class CoffeeMakerImpl implements CoffeeMaker {

    private PowerSupply powerSupply;

    private WaterReservoir waterReservoir;

    private CoffeeBeansContainer coffeeBeansContainer;

    public CoffeeMakerImpl(PowerSupply powerSupply, WaterReservoir waterReservoir,
CoffeeBeansContainer coffeeBeansContainer) {
        this.powerSupply = powerSupply;
        this.waterReservoir = waterReservoir;
        this.coffeeBeansContainer = coffeeBeansContainer;
    }

    public Coffee make() {
        ...
    }
}
```

The `io.inverno.sample.coffeeMakerModule:coffeeMakerImpl` bean then specifies three required sockets:

- `io.inverno.sample.coffeeMakerModule:coffeeMakerImpl:powerSupply`
- `io.inverno.sample.coffeeMakerModule:coffeeMakerImpl:waterReservoir`
- `io.inverno.sample.coffeeMakerModule:coffeeMakerImpl:coffeeBeansContainer`



There should be only one public constructor defined in a bean class, this is actually proper bean design. Defining multiple constructors means that there are probably some dependencies not really required by the bean to work properly. Only required dependencies should be specified in a single bean constructor and optional dependencies in multiple setter methods. However if for some reasons multiple public constructors are defined on a bean class, you can explicitly specify which constructor to consider using the `@BeanSocket` annotation.

```
@Bean
public class CoffeeMakerImpl implements CoffeeMaker {

    @BeanSocket
    public CoffeeMakerImpl(PowerSupply powerSupply, WaterReservoir waterReservoir,
        CoffeeBeansContainer coffeeBeansContainer) {
        ...
    }

    public CoffeeMakerImpl(PowerSupply powerSupply, WaterReservoir waterReservoir,
        CoffeeBeansContainer coffeeBeansContainer, SomeOptionalDependency dependency) {
        ...
    }
}
```

The coffee maker should now have everything it needs to make coffee but let's say we want the coffee maker to be able to make cappuccinos, it will then need a `MilkFrother`. The coffee maker can use a `MilkFrother` when available but it doesn't require a `MilkFrother` to make coffee, only to make cappuccinos, as a result it should be declared in an optional socket.

```
@Bean
public class CoffeeMakerImpl implements CoffeeMaker {

    ...
    private MilkFrother milkFrother

    ...
    public void setMilkFrother(MilkFrother milkFrother) {
        this.milkFrother = milkFrother;
    }

    public Coffee make() {
        ...
        if(this.milkFrother != null) {
            // Do something useful with the milk frother
            ...
        }
    }
}
```

The `io.inverno.sample.coffeeMakerModule:coffeeMakerImpl` bean now specifies one optional socket: `io.inverno.sample.coffeeMakerModule:coffeeMakerImpl:milkFrother`.

By convention, every setter method on a bean is considered an optional socket, this enforces proper bean design. However in some situations you might need to explicitly specify which setter methods are sockets. In order to do that, you need to annotate every socket setter method of the bean with the `@BeanSocket` annotation.

```

@Bean
public class CoffeMakerImpl implements CoffeMaker {

    ...
    @BeanSocket
    public void setMilkFrother(MilkFrother milkFrother) {
        ...
    }

    ...
    public void setSomethingElse() {
        ...
    }
}

```

Note that Inverno annotation are not inherited from ancestor class, the Inverno compiler only considers the bean class annotated with `@Bean` so you must explicitly override setter methods to specify optional sockets defined in a class ancestor. This might not be obvious but it is actually the safer way that gives a perfect control on the sockets you want to expose in your beans.

## Single and multiple

We can differentiate two kinds of bean socket: single socket and multiple socket. A single socket can be of any type except arrays, `java.util.List`, `java.util.Set` and `java.util.Collection` whereas the type of a multiple socket is necessarily an array, a `java.util.List`, a `java.util.Set` or a `java.util.Collection`. Multiple beans can be wired to a multiple socket whereas only one bean is wired to a single socket.

## Lazy

A socket can be annotated with the `@Lazy` to indicate that a bean instance supplier should be provided instead of an actual bean instance. A lazy socket must then be of type `Supplier<E>` which specifies the actual type of the socket as formal parameter. In order to lazily inject a list of beans, the socket must be of type `List<Supplier<E>>`.

A lazy socket allows a dependent bean to lazily retrieve a bean instance. This presents several advantages when prototype beans are wired into a lazy socket, it is then possible to create fully wired bean instances on demand during the operation of a module and use them when processing a request for instance.

## Socket Bean

Bean sockets designates the dependencies of a single bean. All beans in a module must be operational for a module to work properly as a consequence all beans required sockets must be resolved but what if one or more *plugs* are missing inside the module to match all these sockets? The dependency can then be declared at module level using a particular kind of bean: the **socket bean**.

From inside a module, a socket bean is considered as any regular beans as it takes part in the dependency injection process. From outside the module, it designates a module dependency that is provided when a module is instantiated.

Unlike other type of beans, a socket bean is not a concrete class, it must be an interface annotated with `@Bean` extending the `Supplier<E>` interface. The supplier's formal parameter designates the type of the dependency to provide.

Let's say the coffee maker module does not provide any `PowerSupply` bean internally, this makes sense since a power supply might be required to make coffee but it is clearly unrelated. We must then find a way to provide a `PowerSupply` inside the module to make it work. We can then create a `PowerSupplySocket` socket bean inside the coffee maker module.

```
@Bean
public interface PowerSupplySocket implements Supplier<PowerSupply> {}
```

This creates socket bean `io.inverno.sample.coffeeMakerModule:powerSupplySocket` in the module `io.inverno.sample.coffeeMakerModule`. As you can imagine, this bean can be injected in other module's beans just like any regular beans.

The module class generated by the Inverno compiler now defines an argument of type `PowerSupply` in the module's builder constructor, we must then provide a `PowerSupply` instance in order to instantiate the module.

```
PowerSupply powerSupply = ...
CoffeeMakerModule coffeeMakerModule = new CoffeeMakerModule.Builder(powerSupply).build();
...
```

A socket bean appears in the builder constructor when it is wired to a required bean socket inside the module. On the other hand, a socket bean wired to an optional bean socket appears in an extra method of the module's builder class.

We might want to be able to stick a brand sticker on the coffee maker, this is obviously completely optional and external to the coffee maker module. We can then define a `BrandStickerSocket` in the module.

```
BrandSticker brandSticker = ...
CoffeeMakerModule coffeeMakerModule = new
CoffeeMakerModule.Builder(powerSupply).brandSticker(brandSticker).build();
...
```

It is interesting to notice here that a Inverno module explicitly specifies its dependencies which is extremely valuable to create complex modular applications involving multiple people working together, one can easily understand how to use another one's module without mentioning the fact that the compiler can actually check that everything fits together since beans, modules and modules builder arguments are all statically typed.

# Wiring

The Inverno compiler wires beans together based on the sockets defined in the module. A viable module is a module that has:

- all its required sockets resolved, either internally with another bean in the module or externally through a socket bean
- no cycles in the resulting graph of beans

## Autowiring

By default, the Inverno compiler tries to automatically wire the beans in a module based on their respective types and the types of the sockets they expose.

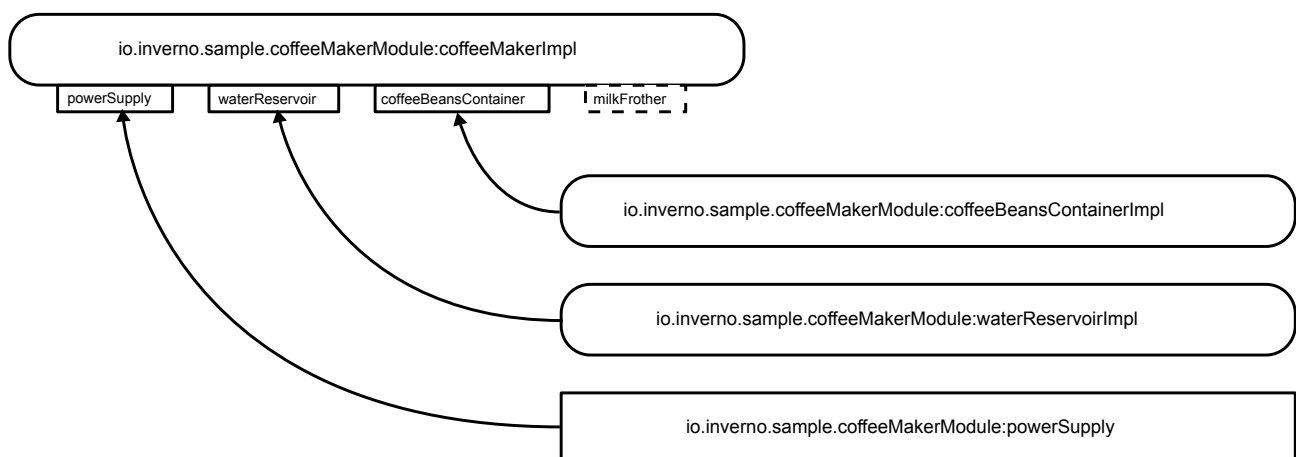
In the coffee maker module we have the following beans:

- `io.inverno.sample.coffeeMakerModule:coffeeMakerImpl`
- `io.inverno.sample.coffeeMakerModule:waterReservoirImpl`
- `io.inverno.sample.coffeeMakerModule:coffeeBeansContainerImpl`
- `io.inverno.sample.coffeeMakerModule:powerSupply` (socket bean)

The `io.inverno.sample.coffeeMakerModule:coffeeMakerImpl` bean defines the following sockets:

- `io.inverno.sample.coffeeMakerModule:coffeeMakerImpl:powerSupply`
- `io.inverno.sample.coffeeMakerModule:coffeeMakerImpl:waterReservoir`
- `io.inverno.sample.coffeeMakerModule:coffeeMakerImpl:coffeeBeansContainer`
- `io.inverno.sample.coffeeMakerModule:coffeeMakerImpl:milkFrother` (optional)

This configuration results in the following graph of beans:



The module is viable since all required beans sockets are resolved and the graph of beans is a directed acyclic graph. The Inverno compiler can then generate a module class containing the logic to instantiate the beans in the right order and the dependency injection logic. When an instance of the `io.inverno.sample.coffeeMakerModule` module is started, the `waterReservoirImpl` bean and the `coffeeBeansContainerImpl` are instantiated first then the `coffeeMakerImpl` bean is instantiated next using previously created instances and the `powerSupply` instance injected when the module was created.

In case one or more bean sockets cannot be resolved, the Inverno compiler outputs specific compilation errors for each one of them. When this happens, you must either define module beans or socket beans inside the module matching the unresolved sockets in order for the module to compile.

You'll learn in the [Modular application](#) section that there is another way to provide beans in a module by *composing* another Inverno module inside your module.

## Explicit wiring

It is not possible for the Inverno compiler to automatically wire module beans when more than one bean matching a socket exists in the module. In that case, the Inverno compiler outputs specific compilation errors on bean sockets presenting such conflicts. In order for the module to compile, these conflicts must be explicitly resolved.

Let's assume we actually have two beans of type `WaterReservoir` in the coffee maker module: `smallWaterReservoir` and `bigWaterReservoir`, the `coffeeMakerImpl` requires only one `WaterReservoir` since the `waterReservoir` socket is a single socket, we clearly have a conflict that the Inverno compiler cannot resolve on its own because it cannot decide for you which water reservoir bean is best suited. So you have to explicitly tell the Inverno compiler what to do using a `@Wire` annotation on the module definition:

```
@Module
@Wire(beans="smallWaterReservoir", into="coffeeMakerImpl:waterReservoir")
Module io.inverno.sample.coffeeMakerModule {
    ...
}
```

In the `@Wire` annotation the `beans` attribute is used to specify which beans must be wired into the socket specified in the `into` attribute.

The `beans` attribute is an array of bean qualified names of the form `([MODULE]:)?[BEAN]`. If the module name is omitted, the compiler will look for beans in the current module. When defining a wire for a single socket, only one bean qualified name is expected.

The `into` attribute is a bean socket qualified name of the form `([MODULE]|([MODULE]:)?[BEAN]):[SOCKET_NAME]`. When specifying a wire on a bean socket name which is necessarily defined in a bean in the current module, the module name can be omitted.

The module name is in fact only necessary when specifying a wire on a socket bean of a module composed in a [composite module](#).

Obviously, multiple `@Wire` annotations can be specified on a module definition. If a specified bean does not exist, if the specified socket does not exist, if the specified beans does not match the specified socket or if multiple beans were specified for a single socket, the Inverno compiler will raise compilation errors.

Resolving conflicts is one way of using explicit wiring, but in the case of a multiple socket, you can also use a wire to explicitly select which beans you want to inject using the `@Wire` annotation. For instance, let's say we have a module with four beans of type `SomeType`: `beanA`, `beanB`, `beanC`, `beanD` and another bean which defines a multiple socket of the same type (eg. `List<SomeType>`), if you do nothing, by default the Inverno compiler will automatically wire all four into the multiple socket, if you want to inject only `beanA` and `beanB` you can specify the following on the module definition:

```
@Module
@Wire(beans={"beanA", "beanB"}, into="someBean:multipleSomeType")
Module someModule {
    ...
}
```

It's interesting to see that it is not on the socket that the conflict is resolved but on the module that actually created that conflict. This is quite different than other DI frameworks that use qualifiers specified on the conflicting injection point. With these approaches, in order to properly separate the concerns a bean should not know the name of the actual bean that will be injected, as a result it is up to the bean to define the qualifiers and up to the other beans to be named or aliased after these qualifiers but this means the bean still know that a conflict exist otherwise it wouldn't need to specify any qualifier. The Inverno framework eliminates this issue to enforce proper separation of concerns.

## Selector

Beans are always wired to sockets based on their types, selectors provide another level of filtering. They are used to specify what compile time properties a bean type must have to be wired to a particular socket.

Selectors are annotations annotated with `@Selector` that can be specified on both bean sockets and socket beans. The framework currently supports the `@AnnotationSelector` that lets you filter beans based on a particular annotation.

Let's say, you finally decided to provide a milk frother to the coffee maker which is unfortunately only compatible with milk frothers of a particular brand. To do so, you can define a `@SuperSteam` annotation for the brand and tell the Inverno compiler to make sure the milk forther wired to the coffee maker is annotated with it.

```

public @interface SuperSteam {}

@Bean
public class CoffeMakerImpl implements CoffeMaker {

    ...
    public void setMilkFrother(@AnnotationSelector(SuperSteam.class) MilkFrother milkFrother) {
        ...
    }
}

```

If no bean of type `MilkFrother` annotated with `@SuperSteam` exists, a compilation error is raised.

It's important to understand here that the Inverno compiler considers the declared type of a bean which is not necessarily the actual type of the runtime instance. This is especially true when defining a [provided type](#) in a bean class, the selector annotation must then be specified on the provided type and not the actual bean class.

## Modular application

Modularity is at the heart of the Inverno framework, it has been built on the idea that flexibility, maintainability and stability, especially on large and complex applications can only be achieved through a proper modularization and strict [separation of concerns](#).

So far, we explored how to define and compose beans inside a module to implement a wider component or a standalone application but the Inverno framework also allows the composition of modules to create even more complex components and applications.

## Composite module

A **composite module** is literally a module composed of multiple Inverno modules. Concretely, all public beans exposed in a component module are considered for dependency injection in the composite module. In the same way, socket beans defined in a component module are resolved with the beans available in the composite module.

By default, any Inverno module required in the module descriptor of a Inverno module are composed by the Inverno compiler inside the module class. Component modules public beans are encapsulated in the composite module class and then only accessible from within that module. At runtime, component modules are instantiated and started along with the composite module which wires their public beans into the module's beans sockets or into other component modules socket beans.

Let's assume module `io.inverno.sample.milkFrotherModule` provides a `MilkFrother` bean compatible with the coffee maker. You can simply declare it as required in the module descriptor of the `io.inverno.sample.coffeeMakerModule` module to get the milk frother module created and started along with the coffee maker module and eventually wire the milk frother into the coffee maker.

```
@Module
Module io.inverno.sample.coffeeMakerModule {
    ...
    requires io.inverno.sample.milkFrotherModule;
    ...
}
```

The Inverno compiler will find out that the milk frother module provides a bean matching coffee maker optional milk frother socket and do the wiring in the module class.

In some situations, you might want to explicitly include or exclude required modules from the module composition, you can do this using **includes** and **excludes** attributes in the **@Module** annotation. This is useful when you just want to use types from another module without instantiating it.

```
@Module(includes={"moduleA", "moduleB"})
Module someModule {
    ...
    requires moduleA;
    requires moduleB;
    requires moduleC; // moduleC will be ignored by the Inverno compiler
    ...
}
```

In order for the module to compile, all required socket beans defined in component modules must be resolved. They can be resolved with any beans available in the composite module including beans, socket beans or any public beans provided in other component modules.

Explicit wiring can be used as described before using fully qualified names for component modules public beans or socket beans.

```
@Module
@Wire(beans="moduleA:bean1", into="someBean:socket") // Explicitly wire bean 'bean1' of
component module 'moduleA' into bean socket 'socket' in bean 'someBean' of module 'someModule'
@Wire(beans="moduleB:bean2", into="moduleC:socketBean") // Explicitly wire bean 'bean2' of
component module 'moduleB' into socket bean 'socketBean' of module 'moduleC'
Module someModule {
    ...
    requires moduleA;
    requires moduleB;
    requires moduleC;
    ...
}
```

Module composition offers greater flexibility when using or designing modules. A typical Inverno application module would be a simple composition of multiple Inverno modules implementing different aspects. Multiple modules inside an application can depend on the same module but with different instances which limits the possibility of collisions and increases reusability. Indeed when developing a module you don't have to worry about the context in which it will be used or executed, you can focus on the feature it provides, external dependencies can be provided internally through module composition or externally through socket beans.



## Provided type

By default, the type of a bean is given by the class defining the bean, for a module bean it is the annotated class and for a wrapper bean it is the formal parameter specified in the `Supplier<E>` interface.

This basically means that the type of a public bean must be accessible from outside the module, its package must then be exported in the module descriptor. However, you might, and probably will, need to hide bean implementations and only expose public API types.

You can control which type is actually provided by a bean using the `@Provide` annotation. A bean can only provide one type.

Let's see how it works for the `io.inverno.sample.coffeeMakerModule:coffeeMakerImpl` bean:

```
@Bean
public class CoffeMakerImpl implements @Provide CoffeMaker {
    ...
}
```

The `CoffeeMakerImpl` class can implement several types but it will be exposed as a `CoffeeMaker` in the module class.

The `@Provide` annotation is only useful on module bean, for w beans the implementation type is already hidden in the `Supplier#get()` method and the provided type is the formal parameter specified in the `Supplier<E>` interface.

The provided type is only considered outside the module when used in a composite module or in an application. Inside the module, the actual bean type is used for dependency injection unless the bean is also overridable in which case the provided type is also used internally.

Hiding implementation and only expose public API is very convenient when you developed a component module and it is a best practice in general if you want to enforce modularity inside an application. Most of the time modules should always depend on public API so from a dependency injection perspective it doesn't really matters whether a module expose implementation classes but you can't guarantee that nobody will ever create a dependency on an implementation class if that class is accessible which would be quite bad for maintainability. Being able to control the types actually exposed in a module enforces a proper isolation.

Particular care must be taken when using [selectors](#) in a composite module, the type of component modules beans considered by the Inverno compiler will be the provided types, so if you want to specify properties matching selectors, you have to specify them on the provided types and not the actual beans types.

# 5

## Inverno Modules

---

### Motivation

Built on top of the [Inverno core IoC/DI framework](#), Inverno modules suite aimed to provide a complete set of features to develop high end production-grade applications.

The advent of cloud computing and highly distributed architecture based on microservices has changed the way applications should be conceived, maintained, executed and operated. While it was perfectly fine to have application started in couple of seconds or even minutes some years ago with long release cycles, today's application must be highly efficient, agile in terms of development and deployment and start in a heart beat.

The Inverno framework was created to reduce framework overhead at runtime to the minimum, allowing to create applications that start in milliseconds. Inverno modules extend this approach to provide functionalities with low footprint, relying on the compiler when it makes sense to generate human-readable code for easy maintenance and improved performance.

An agile application is naturally modular which is the essence of the Inverno framework, but it must also be highly configurable and customizable in many ways using configuration data distributed in various data stores and that greatly depend on the context such as an execution environment: test, production..., a location: US, Europe, Asia..., a particular customer, a particular user... Advanced configuration capabilities are then essential to build modern applications.

Traditional application servers and frameworks used to be based on inefficient threading models that didn't make fair use of hardware resources which make them bad cloud citizens. Inverno applications are one hundred percent reactive making maximum use of the allocated resources.

The primary goals can be summarized as follows:

- provide a complete set of common features to build any kind of applications
- maintain a high level of performance...
- ...but always choose modularity and maintainability over performance to favor agility
- be explicit and consistent, there's nothing worse than ambiguity and disparateness, the *you have to know*s must be minimal and logical.
- provide advanced configuration and customization features

## Prerequisites

Before we can dig into the various modules provided in the framework, it is important to understand how to setup a modular Inverno project, so please have a look at the [Inverno distribution documentation](#) which describes in details how to create, build, run, package and distribute a modular Inverno component or application.

Inverno modules are built on top of the Inverno core IoC/DI framework, please refer to the [Inverno core documentation](#) to understand how IoC/DI is working in the framework.

The framework is fully reactive thanks to [Project Reactor Core library](#), it is strongly recommended to also look at [the reference documentation](#).

## Overview

The basic Inverno application is an Inverno module composing the *boot* module which provides common services. Other Inverno modules can then be added by defining the corresponding dependencies in the module descriptor.

```
@io.inverno.core.annotation.Module
module io.inverno.example.app {
    requires io.inverno.mod.boot;
    // Other modules...
}
```

Declaring a dependency to the *boot* module automatically includes core IoC/DI modules as well as *base* module, *configuration* module and reactive framework dependencies.

A basic application can then be created as follows:

```
import io.inverno.core.v1.Application;

public class Main {

    public static void main(String[] args) {
        Application.with(new App.Builder()).run();
    }
}
```

Inverno modules are fully integrated which means they have been designed to work together in an Inverno component or application but this doesn't mean it's not possible to embed them independently in any kind of application following the agile principle. For instance, the *configuration* module, can be easily used in any application with limited dependency overhead. More generally, an Inverno module can be created and started very easily in pure Java thanks to the Inverno core IoC/DI framework.

For instance, an application can embed a HTTP server as follows:

```
Boot boot = new Boot.Builder().build();
boot.start();

Server httpServer = new Server.Builder(boot.netService(), boot.resourceService())
    .setHttpServerConfiguration(HttpServerConfigurationLoader.load(conf -> conf.server_port(8080)))
    .setRootHandler(
        exchange -> exchange
            .response()
            .body()
            .raw()
            .value(Unpooled.unreleasableBuffer(Unpooled.copiedBuffer("Hello, world!",
Charsets.DEFAULT)))
    )
    .build();

httpServer.start();
...
httpServer.stop();
boot.stop();
```

Note that as for any Inverno module, dependencies are clearly specified and must be provided when creating a module, in the previous example the HTTP server requires a *NetService* and a *ResourceService* which are normally provided by the boot module but custom implementations can be provided. It is also possible to create an Inverno module composing the *boot* and *http-server* modules to let the framework deal with dependency injection.

## Base

The Inverno *base* module defines the foundational APIs used across all modules, it can be seen as an extension to the *java.base* module.

In order to use the Inverno *base* module, we need to declare a dependency in the module descriptor:

```
module io.inverno.example.app {
    requires io.inverno.mod.base;
    ...
}
```

The *base* module declares transitive dependencies to reactive APIs which don't need to be re-declared.

We also need to declare that dependency in the build descriptor:

Using Maven:

```
<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-base</artifactId>
    </dependency>
  </dependencies>
</project>
```

Using Gradle:

```
...
compile 'io.inverno.mod:inverno-base:1.5.3'
...
```

The *base* module is usually provided as a transitive dependency by other modules, mainly the *boot* module, so defining a direct dependency is usually not necessary at least for an application module.

## Converter API

The converter API provides interfaces and classes for building converters, decoders or encoders which are basically used to decode/encode objects of a given type from/to objects of another type.

## Scope

The `Scope` interface specifies a way to expose different bean instances depending on particular scope.

For instance, let's say we want to use different instances of a `Warehouse` bean based on a particular region, we can define a prototype bean for the `Warehouse` and create the following bean which extends `KeyScope`:

```
@Bean
public class WarehouseKeyScope extends KeyScope<Warehouse> {

    private final Supplier<Warehouse> storePrototype;

    public WarehouseKeyScope(@Lazy Supplier<Warehouse> storePrototype) {
        this.storePrototype = storePrototype;
    }

    @Override
    protected Warehouse create() {
        return this.storePrototype.get();
    }
}
```

We can then inject that bean where we need a `Warehouse` instance for a particular region:

```

@Bean
public class WarehouseService {

    private final KeyScope<Warehouse> warehouse;

    public WarehouseService(KeyScope<Warehouse> warehouse) {
        this.warehouse = warehouse;
    }

    public void store(Product product, String region) {
        Warehouse warehouse = this.warehouse.get(region);
        ...
    }
}

```

The base module expose three base **Scope** implementations:

- the **KeyScope** which binds an instance to an arbitrary key
- the **ThreadScope** which binds an instance to the current thread
- the **ReactorScope** which binds an instance to the current reactor's thread. This is very similar to the **ThreadScope** but this throws an **IllegalStateException** when used outside the scope of the reactor (ie. the current thread is not a reactor thread).

Particular care must be taken when using this technique in order to avoid resource leaks. For instance, when a scoped instance is no longer in use, it should be cleaned explicitly as references can be strongly reachable. The **KeyScope** exposes the **remove()** for this purpose. Also when using prototype bean instance, the destroy method, if any, may not be invoked if the instance is reclaimed before it can be destroyed, as a result you should avoid using such bean instances within scope beans.

## Basic converter

The **Converter** interface defines a basic converter. It simply extends **Decoder** and **Encoder** interfaces which defines respectively the basic decoder and the basic encoder.

A basic decoder is used to decode an object of a source type to an object of a target type. For instance, we can create a simple string to integer decoder as follows:

```

public class StringToIntegerDecoder {

    @Override
    public <T extends Integer> T decode(String value, Class<T> type) throws ConverterException {
        return (T)Integer.valueOf(value);
    }

    @Override
    public <T extends Integer> T decode(String value, Type type) throws ConverterException {
        return (T)Integer.valueOf(value);
    }
}
Decoder<String, Integer>

```

A basic encoder is used to encode an object of a source type to an object of a target type. For instance, we can create a simple integer to string encoder as follows:

```
public class IntegerToStringEncoder implements Encoder<Integer, String> {

    @Override
    public <T extends Integer> String encode(T value) throws ConverterException {
        return value.toString();
    }

    @Override
    public <T extends Integer> String encode(T value, Class<T> type) throws ConverterException {
        return value.toString();
    }

    @Override
    public <T extends Integer> String encode(T value, Type type) throws ConverterException {
        return value.toString();
    }
}
```

A string to integer converter can then be created by combining both implementations.

The previous example while not very representative illustrates the basic decoder and encoder API, you should now wonder how to use this properly in an application and what is the fundamental difference between a decoder and an encoder, the answer actually lies in the names. A decoder is meant to *decode* data formatted in a particular way into a representation that can be used in an application whereas an encoder is meant to *encode* an object in an application into data formatted in a particular way. From there, we understand that a converter can be used to read or write raw data (JSON data in an array of bytes for instance) to or from actual usable representations in the form of Java objects but it can also be used as an object mapper to convert from one representation to another (domain object to data transfer object for instance).

A more realistic example would then be a JSON string to object converter:

```

public class JsonToObjectConverter implements Converter<String, Object> {

    private ObjectMapper mapper = new ObjectMapper();

    @Override
    public <T> T decode(String value, Class<T> type) throws ConverterException {
        try {
            return this.mapper.readValue(value, type);
        }
        catch (JsonProcessingException e) {
            throw new ConverterException(e);
        }
    }

    @Override
    public <T> T decode(String value, Type type) throws ConverterException {
        ...
    }

    @Override
    public <T> String encode(T value) throws ConverterException {
        try {
            return this.mapper.writeValueAsString(value);
        }
        catch (JsonProcessingException e) {
            throw new ConverterException(e);
        }
    }

    @Override
    public <T> String encode(T value, Class<T> type) throws ConverterException {
        ...
    }

    @Override
    public <T> String encode(T value, Type type) throws ConverterException {
        ...
    }
}

```

The API provides other interfaces to create converters, decoders and encoders with more capabilities.

## Splittable decoder and Joinable encoder

A **SplittableDecoder** is a particular decoder which allows to decode an object of a source type into multiple objects of a target type. It specifies methods to decode one source instance into an array, a list or a set of target instances.

In the same way, a **JoinableEncoder** is a particular encoder which allows to encode multiple objects of a source type into one single object of a target type. It specifies methods to encode an array, a list or a set of source instances into a single target instance.

The **StringConverter** is a typical implementation that can decode or encode multiple parameters values.



```
StringConverter converter = new StringConverter();

// List.of(1, 2, 3)
List<Integer> l = converter.decodeToList("1,2,3", Integer.class);
// "1,2,3"
String s = converter.encodeList(List.of(1, 2, 3));
```

## Primitive decoder and encoder

A **PrimitiveDecoder** is fundamentally an object decoder which provides bindings to decode an object of a source type into an object of primitive (boolean, integer...) or common type (string, date, URI...).

In the same way, a **PrimitiveEncoder** is fundamentally an object encoder which provides bindings to encode an object of a primitive or common type to an object of a target type.

The **StringConverter** which is meant to convert parameter values is again a typical use case of primitive decoder and encoder.

```
StringConverter converter = new StringConverter();

// 123l
long l = converter.decodeLong("123");
// ISO-8601 date: "yyyy-MM-dd"
String s = converter.encode(LocalDate.now());
```

The **SplittablePrimitiveDecoder** and **JoinablePrimitiveEncoder** are primitive decoder and encoder that respectively extends **SplittableDecoder** and **JoinableEncoder**.

## Object converter

An **ObjectConverter** is a convenient interface for building **Object** converters. It extends **Converter**, **SplittablePrimitiveDecoder** and **JoinablePrimitiveEncoder**.

## Reactive converter

A **ReactiveConverter** is a particular converter which extends **ReactiveDecoder** and **ReactiveEncoder** for building reactive converters which are particularly useful to convert data from non-blocking I/O channels.

The **ReactiveDecoder** interface defines methods to decode one or many objects of a target type from a stream of objects of a source type. In the same way, the **ReactiveEncoder** interface defines methods to encode one or many objects of a source type into a stream of objects of target type.

The **ByteBufConverter** is a typical use case, it is meant to convert data from non-blocking channels like the request or response payloads in a network server or client, or the content of a resource read asynchronously.

```

ByteBufConverter converter = new ByteBufConverter(new StringConverter());

Publisher<ByteBuf> dataStream = ... // comes from a request or resource

// On subscription, chunk of data accumulates until a complete response can be emitted
Mono<ZonedDateTime> dateTimeMono = converter.decodeOne(dataStream, ZonedDateTime.class);

// On subscription, a stream of integer is mapped to a publisher of ByteBuf
Publisher<ByteBuf> integerStream = converter.encodeMany(Flux.just(1,2,3,4));

```

## Media type converter

A **MediaTypeConverter** is a particular kind of object converter which supports a specific format specified as a [media type](#) and converts object from/to raw data in the supported format. A typical example would be a JSON media type converter used to decode/encode raw JSON data.

The *web* module relies on such converters to respectively decode and encode HTTP request and HTTP response payloads based on the content type specified in the message headers.

## Composite converter

A **CompositeConverter** is an extensible object converter based on a **CompositeDecoder** and a **CompositeEncoder** which themselves rely on multiple **CompoundDecoder** and **CompoundEncoder** to extend or override respectively the decoding and encoding capabilities of the converter. In practical terms, it is possible to make a converter able to decode or encode any type of object by providing ad hoc compound decoders and encoders.

The **StringCompositeConverter** is a composite converter implementation which uses a default **StringConverter** to convert primitive and common types of objects, it can be extended to convert other types of object.

For instance, let's consider the following **Message** class:

```

public static class Message {

    private String message;

    // constructor, getter, setter
    ...
}

```

We can create specific compound decoder and encoder to respectively decode and encode a **Message** from/to a string as follows:

```

public static class MessageDecoder implements CompoundDecoder<String, Message> {

    @SuppressWarnings("unchecked")
    @Override
    public <T extends Message> T decode(String value, Class<T> type) throws ConverterException {
        return (T) new Message(value);
    }

    @SuppressWarnings("unchecked")
    @Override
    public <T extends Message> T decode(String value, Type type) throws ConverterException {
        return (T) new Message(value);
    }

    @Override
    public <T extends Message> boolean canDecode(Class<T> type) {
        return Message.class.equals(type);
    }

    @Override
    public boolean canDecode(Type type) {
        return Message.class.equals(type);
    }
}

public static class MessageEncoder implements CompoundEncoder<Message, String> {

    @Override
    public <T extends Message> String encode(T value) throws ConverterException {
        return value.getMessage();
    }

    @Override
    public <T extends Message> String encode(T value, Class<T> type) throws ConverterException {
        return value.getMessage();
    }

    @Override
    public <T extends Message> String encode(T value, Type type) throws ConverterException {
        return value.getMessage();
    }

    @Override
    public <T extends Message> boolean canEncode(Class<T> type) {
        return Message.class.equals(type);
    }

    @Override
    public boolean canEncode(Type type) {
        return Message.class.equals(type);
    }
}

```

And inject them into a string composite converter which can then decode/encode **Message** object:

```
CompoundDecoder<String, Message> messageDecoder = new MessageDecoder();
CompoundEncoder<Message, String> messageEncoder = new MessageEncoder();

StringCompositeConverter converter = new StringCompositeConverter();
converter.setDecoders(List.of(messageDecoder));
converter.setEncoders(List.of(messageEncoder));

Message decodedMessage = converter.decode("this is an encoded message", Message.class);
String encodedMessage = converter.encode(new Message("this is a decoded message"));
```

## Net API

The Net API provides interfaces and classes to manipulate basic network elements such as URIs or to create basic network clients and servers.

### URIs

A URI follows the standard defined by [RFC 3986](#), it is mostly used to identify resources such as file or more specifically a route in a Web server. The JDK provides a standard implementation which is not close to what is required by the *web* module to name just one.

The `URIs` utility class is the main entry point for working on URIs in any ways imaginable. It defines methods to create a blank URI or a URI based on a given path or URI. These methods return a `URIBuilder` instance which is then used to build a URI, a path, a query string or a URI pattern.

A simple URI can then be created as follows:

```
// http://localhost:8080/path/to/resource?parameter=value
URI uri = URIs.uri()
    .scheme("http")
    .host("localhost")
    .port(8080)
    .path("/path/to/resource")
    .queryParameter("parameter", "value")
    .build();
```

or from an existing URI as follows:

```
// https://test-server/path/to/resource
URI uri = URIs.uri(URI.create("http://localhost:8080/path/to?parameter=value"))
    .scheme("https")
    .host("test-server")
    .port(null)
    .segment("resource")
    .clearQuery()
    .build();
```

A URI can be normalized by enabling the `URIs.Option.NORMALIZED` option:

```
// path/to/other
URI uri = URIs.uri("path/to/resource", URIs.Option.NORMALIZED)
    .segment("..")
    .segment("other")
    .build();
```

A parameterized URI can be created by enabling the `URIs.Option#PARAMETERIZED` option and specifying parameters of the form `{{<name>[:<pattern>]}}` in the components of the URI. This allows to create URI templates that can be used to generate URIs from a set of parameters.

```
URIBuilder uriTemplate = URIs.uri(URIs.Option.PARAMETERIZED)
    .scheme("{scheme}")
    .host("{host}")
    .path("/path/to/resource")
    .segment("{id}")
    .queryParameter("format", "{format}");

// http://localhost/path/to/resource/1?format=text
URI uri1 = uriTemplate.build("http", "localhost", "1", "text");

// https://production/path/to/resource/32?format=json
URI uri2 = uriTemplate.build("https", "production", "32", "json");
```

The `URIBuilder` also defines methods to create string representations of the whole URI, the path component or the query component.

```
URIBuilder uriBuilder = URIs.uri()
    .scheme("http")
    .host("localhost")
    .port(8080)
    .path("/path/to/resource")
    .queryParameter("parameter", "value");

// http://localhost:8080/path/to/resource?parameter=value
String uri = uriBuilder.buildString();

// path/to/resource
String path = uriBuilder.buildPath();

// parameter=value
String query = uriBuilder.buildQuery();
```

It can also create `URIPattern` to match a given input against the pattern specified by the URI while extracting parameter values when the URI is parameterized.

```
URIPattern uriPattern = URIs.uri(URIs.Option.PARAMETERIZED)
    .scheme("{scheme}")
    .host("{host}")
    .path("/path/to/resource")
    .segment("{id}")
    .queryParameter("format", "{format}")
    .buildPattern();

URIMatcher matcher = uriPattern.matcher("http://localhost:8080/path/to/resource/1?format=text");
if(matcher.matches()) {
    // scheme=http, host=localhost, id=1, format=text
    Map<String, String> parameters = matcher.getParameters();
    ...
}
```

Path patterns are also supported by enabling the `URIs.Option#PATH_PATTERN` option and allows to create URI patterns with question marks or wildcards.

```
// Matches all .java files under /src path
URIPattern uriPattern = URIs.uri("/src/**/*.java", URIs.RequestTargetForm.ABSOLUTE,
    URIs.Option.PATH_PATTERN)
    .buildPathPattern();

// Matches test.jsp, tast.jsp, t1st.jsp...
uriPattern = URIs.uri("/t?st.java", URIs.RequestTargetForm.ABSOLUTE, URIs.Option.PATH_PATTERN)
    .buildPathPattern();
```

Note that the Path pattern option is not compatible with **ORIGIN** form request target, as a result the URI must be created using the **ABSOLUTE** request target form.

It is possible to determine whether a path pattern is included into another. A path pattern is said to be included into another path pattern if and only if the set of URIs matched by this pattern is included in the set of URIs matched by the other pattern.

```
```java URIPattern pathPattern1 = URIs.uri("/src/**", URIs.RequestTargetForm.ABSOLUTE,
    URIs.Option.PATH_PATTERN) .buildPathPattern();
```

```
URIPattern pathPattern2 = URIs.uri("/src/java/**/*.java", URIs.RequestTargetForm.ABSOLUTE,
    URIs.Option.PATH_PATTERN) .buildPathPattern();
```

```
URIPattern.Inclusion inclusion = uriPattern1.includes(uriPattern2); // returns
URIPattern.Inclusion.INCLUDED```
```

The proposed implementation is not exact which is why the `includes()` method returns **INCLUDED** when inclusion could be determined with certainty, **DISJOINT** when exclusion could be determined with certainty and **INDETERMINATE** when inclusion could not be determined with certainty.

Note that inclusion can only be determined when considering path patterns, ie. created using `buildPathPattern()` method and containing only a path component. The `includes()` method will always return **INDETERMINATE** for any other type of URI patterns.

## Network service

The **NetService** interface specifies a service for building optimized network clients and servers based on Netty. The *base* module doesn't provide any implementation, a base implementation is provided in the *boot* module.

This service especially defines methods to obtain **EventLoopGroup** instances backed by a root event loop group in order to reuse event loops across different network servers or clients running in the same application.

It also defines methods to create basic network client and server bootstraps.

# Reflection API

The reflection API provides classes and interfaces for building `java.lang.reflect.Type` instances in order to represent parameterized types at runtime which is otherwise not possible due to type erasure. Such `Type` instances are used when decoding data into objects of parameterized types.

The `Types` class is the main entry point for building any kind of Java types.

```
// java.util.List<? extends java.lang.Comparable<java.lang.String>>
Type type = Types.type(List.class)
    .wildcardType()
    .upperBoundType(Comparable.class)
    .type(String.class).and()
    .and()
    .build();
```

The reflection API is particularly useful to specify a parameterized type to an [object converter](#). For instance, let's imagine we have a `ByteBuffer` we want to decode to a `List<String>`, we can do:

```
ByteBuffer input = ...;
ObjectConverter<ByteBuffer> converter = ...;

Type listOfStringType = Types.type(List.class)
    .type(String.class).and()
    .build();
List<String> decode = converter.<List<String>>decode(input, listOfStringType);
```

# Resource API

The resource API provides classes and interfaces for accessing resources of different kinds and locations (file, zip, jar, classpath, module...) in a consistent way using a unique `Resource` interface.

A resource can be created directly using the implementation corresponding to the kind of resource. For instance, in order to access a resource on the class path, you need to choose the `ClasspathResource` implementation:

```
ClasspathResource resource = new ClasspathResource(URI.create("classpath:/path/to/resource"));
```

A resource is identified by a URI whose scheme specifies the kind of resources. The *base* module provides several implementations with a corresponding scheme.

Type	URI	Implementation
file	file:/path/to/resource	FileResource
zip	zip:/path/to/zip!/path/to/resource	ZipResource
jar	jar:/path/to/jar!/path/to/resource	JarResource
url	http https ftp://host/path/to/resource	URLResource
classpath	classpath:/path/to/resource	ClasspathResource
module	module://[MODULE_NAME]/path/to/resource	ModuleResource

The `ResourceService` interface specifies a service which provides a unified access to resources based only on the resource URI. The *base* module doesn't provide any implementation, a base implementation is provided in the *boot* module.

A typical use case is to get a resource from a URI without knowing the actual kind of the resource.

```
ResourceService resourceService = ...
```

```
Resource resource = resourceService.getResource(URI.create("classpath:/path/to/resource"));
```

The resource service can also be used to list resources at a given location. Nonetheless this actually depends on the implementation and the kind of resource, although it is clearly possible to list resources from a file location, it might not be supported to list resources from a class path or URL location.

The *boot* module [implementation](#) supports for instance the listing of resources that match a specific path pattern:

```
ResourceService resourceService = ...
```

```
Stream<Resource> resources =  
resourceService.getResources(URI.create("file:/path/to/resources/**/*"));
```

The `MediaTypeService` interface specifies a service used to determine the media type of a resource based on its extension, name, path or URI. As for the resource service, a base implementation is provided in the *boot* module.

```
MediaTypeService mediaTypeService = ...
```

```
// image/png  
String mediaType = mediaTypeService.getForExtension("png");
```



# Boot

The Inverno *boot* module provides basic services to applications including several base implementation for interfaces defined in the *base* module.

The Inverno *boot* module is the basic building block for any application and as such it must be the first module to declare in an application module descriptor.

```
@io.inverno.core.annotation.Module
module io.inverno.example.app {
    requires io.inverno.mod.boot;
    // Other modules...
}
```

The *boot* module declares transitive dependencies to the core IoC/DI modules as well as *base* and *configuration* modules. They don't need to be re-declared.

This dependency must also be declared in the build descriptor:

Using Maven:

```
<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-boot</artifactId>
    </dependency>
  </dependencies>
</project>
```

Using Gradle:

```
...
compile 'io.inverno.mod:inverno-boot:1.5.3'
...
```

## Configuration

The `BootConfiguration` is used to configure the beans exposed in the *boot* module, the `Reactor` and the `NetService` in particular.

Please refer to the [API documentation](#) to have an exhaustive description of the different configuration properties.

## Reactor

The module provides two `Reactor` implementations: one generic implementation which creates a regular Netty event loop group and a [Vert.x](#) core implementation which uses the event loops of a `Vert.x` instance. The Vert.x implementation is particularly suited when an Inverno application must integrate Vert.x services such as the PostgreSQL client.

The module exposes one or the other as bean depending on the *boot* module configuration, parameter `reactor_prefer_vertx` must be set to true, and whether or not the Vert.x core module is present on the module path.

## Net service

The module provides a base `NetService` implementation exposed as a bean for building network applications based on [Netty](#).

## Media type service

The module provides a base `MediaTypeService` implementation based on the JDK (see [Files.probeContentType\(Path\)](#)) and exposed as an overridable bean allowing custom implementations to be provided.

## Resource service

The module provides a base `ResourceService` implementation exposed as a bean for accessing resources.

This base implementation supports the following schemes: `file`, `zip`, `jar`, `classpath`, `module`, `http`, `https` and `ftp` and it allows to list resources for `file`, `zip` and `jar` schemes.

When supported, resources are listed from a base URI specifying a path pattern using the following rules:

- `?` matches one character
- `*` matches zero or more characters
- `**` matches zero or more directories in a path

For instance:

```
ResourceService resourceService = ...

// Return: '/base/test1/a', '/base/test1/a/b', '/base/test2/c'...
Stream<Resource> resources = resourceService.getResources(URI.create("file:/base/test?/**/*"));
```

It is also possible to resolve all resources with a specific name defined in all application modules by specifying `'*'` instead of the module name in a module URI:

```
ResourceService resourceService = ...

// all resources named '/path/to/resource' in all application modules
Stream<Resource> resources =
resourceService.getResources(URI.create("module://*/path/to/resource"));
```

This service can be extended by injecting custom `ResourceProvider` providing resources for a custom URI scheme. For instance, if we create a custom `Resource` and corresponding `ResourceProvider` implementations mapped to URI scheme `custom`, we can extend the resource service so it can create such custom resources.

```

Boot boot = new Base.Boot()
    .setResourceProviders(List.of(new CustomResourceProvider()))
    .build();

boot.start();

Resource customResource = boot.resourceService().get(URI.create("custom:..."));
...

boot.stop();

```

## Converters

The module exposes various **converter** implementations used across an application to convert parameter values or message payloads.

This includes the following also exposed as beans:

- a parameter converter for converting strings from/to objects, this converter can be extended by injecting specific compound decoders and encoders in the module as described in the [composite converter documentation](#).
- a JSON **ByteBuf** converter for converting raw JSON data in **ByteBuf** from/to objects in the application.
- an **application/json** media type converter for converting message payloads from/to JSON.
- an **application/x-ndjson** media type converter for converting message payloads from/to [Newline Delimited JSON](#)
- a **text/plain** media type converter for converting message payloads from/to plain text.

## Worker pool

An Inverno application must be fully reactive, most of the processing is performed in non-blocking I/O threads but sometimes blocking operations might be needed, in such cases, the worker thread pool should be used to execute these blocking operations without impacting the I/O event loop.

The default worker pool bean is a simple [cached Thread pool](#) which can be overridden by providing a different instance to the *boot* module.

## Object mapper

A standard JSON reader/writer based on Jackson **ObjectMapper** is also provided. This instance is used across the application to perform JSON conversion operations, a global configuration can then be applied to that particular instance or it can be overridden when creating the *boot* module.

The global object mapper is configured to use [JSR310](#) for dates which are serialized as timestamps following [ISO 8601](#) representation.

# Configuration

The Inverno *configuration* module defines a unified configuration API for building agile and highly configurable applications.

Configuration is one of the most important aspect of an application and sadly one of the most neglected. There are very few decent configuration frameworks and most of the time they relate to one part of the issue. It is important to approach configuration by considering it as a whole and not as something that can be solved by a property file here and a database there. Besides, it must be the first issue to tackle during the design phase as it will impact all aspects of the application. For instance, we can imagine an application where configuration is defined in simple property file, a complete configuration would probably be needed for each environment where the application is deployed, maintenance would be probably problematic even more when we know that configuration properties can be added, modified or removed over time.

In its most basic form, a configuration is not more than a set of properties associating a value to a key. It would be naive to think that this would be enough to build an agile and customizable application, but in the end, the property should always be considered as the basic building block for configurations.

Now, the first thing to notice is that any part of an application can potentially be configurable, from a server IP address to a color of a button in a user interface, there are multiple forms of configuration with different expectations that must coexist in an application. For instance, some parts of the configuration are purely static and do not change during the operation of an application, this is the case of a bootstrap configuration which mostly relates to the operating environment (eg. a server port). Some other parts, on the other hand, are more dynamic and can change during the operation of an application, this is the case of tenant specific configuration or even user preferences.

Following this, we can see that a configuration greatly depends on the context in which it is loaded. The definition of a configuration, which is basically a list of property names, is dictated by the application, so when the application is running, this definition should be fixed but the context is not. For instance, the bootstrap configuration is different from one operating environment to another, user preferences are not the same from one user to another...

We can summarize this as follows:

- a configuration is a set of configuration properties.
- the configuration of an application is actually composed of multiple configurations with their own specificities.
- the definition of a configuration is bound to the application as a result the only way to change it is to change the application.
- a configuration depends on a particular context which must be considered when setting or getting configuration properties.

The configuration API has been created to address previous points, giving a maximum flexibility to precisely design how an application should be configured.

In order to use the Inverno *configuration* module, we need to declare a dependency in the module descriptor:

```
module io.inverno.example.app {  
    ...  
    requires io.inverno.mod.configuration;  
    ...  
}
```

And also declare that dependency in the build descriptor:

Using Maven:

```
<project>  
  <dependencies>  
    <dependency>  
      <groupId>io.inverno.mod</groupId>  
      <artifactId>inverno-configuration</artifactId>  
    </dependency>  
  </dependencies>  
</project>
```

Using Gradle:

```
...  
compile 'io.inverno.mod:inverno-configuration:1.5.3'  
...
```

## Configuration source

A configuration source can be any data store that holds configuration data, the API abstracts configuration data sources to provide a unified access to configuration data through the `ConfigurationSource` interface. Specific implementations should be considered depending on the type of configuration: a bootstrap configuration is most likely to be static and stored in configuration files or environment variables whereas a tenant specific configuration is most likely to be stored in a distributed data store. But this is not a universal rule, depending on the needs we can very well consider any kind of configuration source for any kind of configuration. The configuration source abstracts these concerns from the rest of the application.

The `ConfigurationSource` is the main entry point for accessing configuration properties, it shall be used every time there's a need to retrieve configuration properties. It defines only one method for creating a `ConfigurationQuery` eventually executed in order to retrieve one or more configuration properties.

For instance, property `server.uri` can be retrieved as follows:

```

ConfigurationSource<?, ?, ?> source = ...

source.get("server.url") // 1
  .execute() // 2
  .single() // 3
  .map(queryResult -> queryResult
    .getResult() // 4
    .flatMap(ConfigurationProperty::asURI) // 5
    .orElse(URI.create("http://localhost"))) // 6
  )
  .subscribe(serverURI -> ...); // 7

```

In the preceding example:

1. create a configuration query to retrieve the `server.url` property
2. execute the query, the API is reactive so nothing will happen until a subscription is actually made on the resulting publisher of `ConfigurationQueryResult`
3. transform the `Flux` to a `Mono` since we expect a single result
4. get the resulting configuration property, a query result is always returned even if the property does not exist in the source therefore `getResult()` returns an `Optional` that lets you decide what to do if the property is missing
5. convert the property value to URI if present, a property can be defined in a source with a null value which explains why the property value is also an `Optional` and why we need to use `flatMap()`
6. return the actual value if it exists or the specified default value
7. subscribe to the `Mono` which actually runs the query in the source and return the property value or the default value if the property value is null or not defined in the source

This seems to be a lot of steps to simply retrieve one property value, but if you look closely you'll understand that each of them is actually necessary:

- we want to be able to retrieve multiple properties and/or create more complex queries in a batch so `.execute()` is required to mark the end of a batch of queries
- we want to be reactive so `.single().map()` and `subscribe()` are required
- we want to have access to the configuration query key at the origin of a property for troubleshooting as a result the query result must expose `getQueryKey()` and `getResult()` methods
- we want to be able to convert a property value and provide different behaviors when a property does not exist in a source or when it does exist but with a null value, as a result `.flatMap(property -> property.asURI()).orElse(URI.create("http://localhost"))` is required

As we said earlier, a configuration depends on the context: a given property might have different values when considering different contexts. The configuration API defines a configuration property with a name, a value and a set of parameters specifying the context for which the property is defined. Such configuration property is referred to as a **parameterized configuration property**.

Some configuration source implementations do not support parameterized configuration property, they simply ignore parameters specified in queries and return the value associated to the property name. This is especially the case of environment variables which don't allow to specify property parameters.

In order to retrieve a property in a particular context we can then parameterized the configuration query as follows:

```
source.get("server.url")
  .withParameters("environment", "production", "zone", "us")
  .execute()
  ...
```

In the preceding example, we query the source for property `server.url` defined for the production environment in zone US. To state the obvious, both the list of parameters and their values can be determined at runtime using actual contextual values. This is what makes parameterized properties so powerful as it is suitable for a wide range of use cases. This is all the more true when using [defaultable configuration sources](#) which use defaulting strategies to determine the best matching value corresponding to a given query.

As said before the API let's you fluently query multiple properties in a batch and map the results in a configuration object.

```
source
  .get("server.port", "db.url", "db.user", "db.password").withParameters("environment",
    "production", "zone", "us")
  .and()
  .get("db.schema").withParameters("environment", "production", "zone", "us", "tenant",
    "someCompany")
  .execute()
  .collectMap(queryResult -> queryResult.getQueryKey().getName(), queryResult ->
    queryResult.getResult())
  .map(properties -> {
    ApplicationConfiguration config = new ApplicationConfiguration();

    properties.get("server.port").flatMap(property ->
    property.asInteger()).ifPresent(config::setServerPort);
    properties.get("db.url").flatMap(property -> property.asURL()).ifPresent(config::setDbURL);
    properties.get("db.user").flatMap(property ->
    property.asString()).ifPresent(config::setDbUser);
    String dbPassword = properties.get("db.password").flatMap(property ->
    property.asString()).ifPresent(config::setDbPassword);
    String dbSchema = properties.get("db.schema").flatMap(property ->
    property.asString()).ifPresent(config::setDbSchema);

    return config;
  })
  .subscribe(config -> {
    ...
  });
```

The beauty of being reactive is that it comes with a lot of cool features such as the ability to re-execute a query or caching the result. A **Flux** or a **Mono** executes on subscriptions, which means we can create a complex query to retrieve a whole configuration, keep the resulting Reactive Streams **Publisher** and subscribe to it when needed. A Reactive Stream publisher can also cache configuration results.

```
Mono<ApplicationConfiguration> configurationLoader = ... // see previous example

// Query the source on each subscriptions
configurationLoader.subscribe(config -> {
    ...
});

// Cache the configuration for five minutes
Mono<ApplicationConfiguration> cachedConfigurationLoader =
configurationLoader.cache(Duration.ofMinutes(5));

// Query the source on first subscription, further subscriptions within a window of 5 minutes will
get the cached configuration
cachedConfigurationLoader.subscribe(config -> {
    ...
});
```

Although publisher caching is a cool feature, it might not be ideal for complex caching use cases and more solid solution should be considered.

A configuration source relies on a **SplittablePrimitiveDecoder** to decode property values. Configuration source implementations usually provide a default decoder but it is possible to inject custom decoders to decode particular configuration values. The expected decoder implementation depends on the configuration source implementation but most of the time a string to object decoder is expected.

```
SplittablePrimitiveDecoder<String> customDecoder = ...
```

```
PropertyFileConfigurationSource source = new PropertyFileConfigurationSource(new
ClasspathResource(URI.create("classpath:/path/to/configuration.properties")), customDecoder)
```

The regular and most efficient way to query a configuration source is to target specific configuration properties identified by a name and a set of parameters, however there are some cases that actually require to list all values defined for a particular property name and matching a particular set of parameters.

for instance, this is typically the case when configuring log levels, since we can hardly know the name of each and every loggers used in an application, it is easier, safer and more efficient in that case to list all the configuration properties defined for a **logging.level** property and apply the configuration to the loggers based on the parameters of the returned properties.

For instance, the following properties can be defined in the configuration:



```
logging.level[]=info
logging.level[logger="logger1"]=debug
logging.level[logger="logger2"]=trace
logging.level[logger="logger3"]=error
```

These configuration properties can then be listed in the application as follows:

```
// Returns all logging.level properties defined in the configuration source
List<ConfigurationProperty> result = source.list("logging.level")
    .executeAll()
    .collectList()
    .block();

// Apply logging configuration
for(ConfigurationProperty p : result) {
    Optional<String> loggerName = p.getKey().getParameter("logger");
    Level level = p.as(Level.class).get();
    // Configure logger...
}
```

The `executeAll()` method returns all the properties defined in the configuration source for a particular property name and matching the set of parameters defined in the query whether they are defined with extra parameters or not. For instance, if we extend our example by adding an `environment` parameter:

```
logging.level[]=info
logging.level[environment="dev", logger="logger1"]=debug
logging.level[environment="prod", logger="logger2"]=trace
logging.level[logger="logger3"]=error
```

The following list query will return all values that are defined with a `logger` parameter whether they are defined with an `environment` parameter or not. Please note how the `logger` parameter is specified in the query as a wildcard:

```
// Returns logging.level[environment="dev", logger="logger1"], logging.level[environment="prod",
// logger="logger2"] and logging.level[logger="logger3"]=error which are all defined with parameter
// logger
List<ConfigurationProperty> result = source.list("logging.level")
    .withParameters(Parameter.wildcard("logger"))
    .executeAll()
    .collectList()
    .block();
```

On the other hand, the `execute()` method is exact and returns all the properties defined in the configuration source for a particular property name and which parameters exactly match the set of parameters defined in the query, excluding those that are defined with extra parameters:

```
// Returns logging.level[logger="logger3"]=error which exactly defines parameter logger
List<ConfigurationProperty> result = source.list("logging.level")
    .withParameters(Parameter.wildcard("logger"))
    .execute()
    .collectList()
    .block();
```

## Configurable configuration source

A configurable configuration source is a particular configuration source which supports configuration properties updates. The [Redis configuration source](#) is an example of configurable configuration source.

The `ConfigurableConfigurationSource` interface is the main entry point for updating configuration properties, it shall be used every time there's a need to retrieve or set configuration properties.

It extends the `ConfigurationSource` with one method for creating a `ConfigurationUpdate` instance eventually executed in order to set one or more configuration properties in the configuration source.

For instance, a parameterized property `server.port` can be set in a configuration source as follows:

```
ConfigurableConfigurationSource<?, ?, ?, ?, ?> source = null;

source.set("server.port", 8080)
    .withParameters("environment", "production", "zone", "us")
    .execute()
    .single()
    .subscribe(
        updateResult -> {
            try {
                updateResult.check();
                // Update succeeded
                ...
            }
            catch(ConfigurationSourceException e) {
                // Update failed
                ...
            }
        }
    );
```

A configurable configuration source relies on a `JoinablePrimitiveEncoder` to encode property values. Implementations usually provide a default encoder but it is possible to inject custom encoders to encode particular configuration values. The expected encoder implementation depends on the configuration source implementation but most of the time an object to string encoder is expected.

```
RedisClient redisClient = ...
JoinablePrimitiveEncoder<String> customEncoder = ...
SplittablePrimitiveDecoder<String> customDecoder = ...
```

```
RedisConfigurationSource source = new RedisConfigurationSource(redisClient, customEncoder,
    customDecoder)
```

## Defaultable configuration source

By default, a configuration source returns the result that exactly match the configuration query. When considering parameterized configuration properties, this behaviour can quickly become quite restrictive and a defaulting mechanism that would allow to select the best matching value among those defined in the source could reveal their full potential.

A defaultable configuration source is a particular source that can rely on a defaulting strategy to determine the best matching value for a given configuration query. A defaultable configuration source implements `DefaultableConfigurationSource` which allows to choose the defaulting strategy to use by wrapping the original source:

```
DefaultableConfigurationSource<?, ?, ?, ?> source = ...
```

```
DefaultableConfigurationSource<?, ?, ?, ?> defaultingSource =  
source.withDefaultingStrategy(DefaultingStrategy.lookup());
```

```
DefaultableConfigurationSource<?, ?, ?, ?> originalSource = defaultingSource.unwrap();
```

A `DefaultingStrategy` provides two methods `#getDefaultingKeys(ConfigurationKey queryKey)` and `#getListDefaultingKeys(ConfigurationKey queryKey)` which respectively derives the actual keys to retrieve from the source ordered by priorities from the highest to the lowest to determine the best-matching value for the query (the first existing value shall be returned) and the actual keys that must be retained when listing properties. The configuration module provides three implementations: `DefaultingStrategy#noOp()` strategy, `DefaultingStrategy#lookup()` and `DefaultingStrategy#wildcard()`.

### noOp defaulting strategy

The noOp strategy is used to return exact results. This is the default behaviour for all configuration sources.

### lookup defaulting strategy

The lookup strategy prioritizes query parameters from left to right and is used to return the best matching property as the one matching the most continuous parameters from left to right.

If we consider query key `property[p1=v1, ...pn=vn]`, it supersedes key `property[p1=v1, ...pn-1=vn-1]` which supersedes key `property[p1=v1, ...pn-2=vn-2]`... which supersedes key `property[]`. It basically tells the source to lookup by successively removing the rightmost parameter if no exact result exists for a particular query.

For instance, if we consider a source with the following properties:

- `log.level[]=INFO`
- `log.level[environment = "prod"]=WARN`
- `log.level[environment = "prod", name = "test1"]=ERROR`

We can run the following queries with defaulting:

```

DefaultableConfigurationSource<?, ?, ?, ?> source = null;
source = source.withDefaultingStrategy(DefaultingStrategy.lookup());
source
    .get("log.level").withParameters("environment", "dev", "name", "test1") // 1
    .and().get("log.level").withParameters("environment", "prod", "name", "test2") // 2
    .and().get("log.level").withParameters("environment", "prod", "name", "test1") // 3
    .and().get("log.level").withParameters("name", "test1") // 4
    .and().get("log.level").withParameters("name", "test2", "environment", "prod") // 5
    .execute()
    ...

```

1. Returns **INFO** which corresponds to `log.level[]` property since properties `log.level[environment = "dev", name = "test1"]` and `log.level[environment = "dev"]` are not defined
2. Returns **WARN** which corresponds to `log.level[environment = "prod"]` since property `log.level[environment = "dev", name = "test2"]` is not defined
3. Returns **ERROR** which corresponds to the exact match
4. Returns **INFO** which corresponds to `log.level[]` property since property `log.level[name = "test1"]` is not defined
5. Returns **INFO** which corresponds to `log.level[]` properties since property `log.level[name = "test2", "environment", "prod"]` and `log.level[name = "test2"]` are not defined

Since parameters are prioritized from left to right, the order into which they are defined in the query is important. As you can see in see in above example querying `log.level[environment = "prod", name = "test2"]` is not the same as querying `log.level[name = "test2", environment = "prod"]`.

A query with `n` parameters results in at most `n+1` properties being retrieved from the source depending on the implementation.

## wildcard defaulting strategy

The wildcard strategy returns the best matching property as the one matching the most of the query parameters while prioritizing them from left to right.

If we consider query key `property[p1=v1, ...pn=vn]`, the most precise result is the one defining parameters `[p1=v1, ...pn=vn]`, it supersedes results that define `n-1` query parameters, which supersedes results that define `n-2` query parameters... which supersedes results that define no query parameters. Conflicts may arise when a source defines a property with different set of query parameters with the same cardinality (e.g. when it defines properties `property[p1=v1, p2=v2]` and `property[p1=v1, p3=v3]`). In such situation, priority is always given to parameters from left to right (therefore `property[p1=v1, p2=v2]` supersedes `property[p1=v1, p3=v3]`).

Considering previous example but with the wildcard strategy instead of the lookup strategy, some queries have different results:

```

DefaultableConfigurationSource<?, ?, ?, ?> source = null;
source = source.withDefaultingStrategy(DefaultingStrategy.wildcard());
source
    .get("log.level").withParameters("environment", "dev", "name", "test1") // 1
    .and().get("log.level").withParameters("environment", "prod", "name", "test2") // 2
    .and().get("log.level").withParameters("environment", "prod", "name", "test1") // 3
    .and().get("log.level").withParameters("name", "test1") // 4
    .and().get("log.level").withParameters("name", "test2", "environment", "prod") // 5
    .execute()
    ...

```

1. Returns **INFO** which corresponds to `log.level[]` property since properties `log.level[environment = "dev", name = "test1"]`, `log.level[environment = "dev"]` and `log.level[name = "test1"]` are not defined
2. Returns **WARN** which corresponds to `log.level[environment = "prod"]` since property `log.level[environment = "dev", name = "test2"]` is not defined and property `log.level[environment = "prod"]` is defined (it would also have superseded property `log.level[environment = "test2"]` if it had been defined)
3. Returns **ERROR** which corresponds to the exact match
4. Returns **INFO** which corresponds to `log.level[]` property since property `log.level[name = "test1"]` is not defined
5. Returns **WARN** which corresponds to `log.level[environment = "prod"]` since properties `log.level[name = "test2", environment = "prod"]` and `log.level[name = "test2"]` are not defined, but property `log.level[environment = "prod"]` is defined

As for the lookup strategy, the order into which they are defined in the query is important and querying `log.level[environment = "prod", name = "test2"]` is not the same as querying `log.level[name = "test2", environment = "prod"]`.

A query with  $n$  parameters results in at most  $2^n$  properties being retrieved from the source depending on the implementation.

## Map configuration source

The map configuration is the most basic configuration source implementation. It exposes configuration properties stored in a map in memory. It doesn't support parameterized properties, regardless of the parameters specified in a query, only the property name is considered when resolving a value.

```

MapConfigurationSource source = new MapConfigurationSource(Map.of("server.url", new
URL("http://localhost")));
...

```

This source is [defaultable](#) and it can be used for testing purpose in order to provide a mock configuration source.

## System environment configuration source

The system environment configuration source exposes system environment variables as configuration properties. As for the map configuration source, this implementation doesn't support parameterized properties.

```
$ export SERVER_URL=http://localhost
```

```
SystemEnvironmentConfigurationSource source = new SystemEnvironmentConfigurationSource();  
...
```

This implementation can be used to bootstrap an application using system environment variables.

## System properties configuration source

The system properties configuration source exposes system properties as configuration properties. As for the two previous implementations, it doesn't support parameterized properties.

```
$ java -Dserver.url=http://localhost ...
```

```
SystemPropertiesConfigurationSource source = new SystemPropertiesConfigurationSource();  
...
```

This implementation can be used to bootstrap an application using system properties.

## Command line configuration source

The command line configuration source exposes configuration properties specified as command line arguments of the application. This implementation supports parameterized properties.

Configuration properties must be specified as application arguments using the following syntax:

`--property[parameter_1=value_1...parameter_n=value_n]=value` where property and parameter names are valid Java identifiers and property and parameter values are Java primitives such as integer, boolean, string... A complete description of the syntax can be found in the [API documentation](#).

For instance the following are valid configuration properties specified as command line arguments:

```
$ java ... Main \  
--web.server_port=8080 \  
--web.server_port[profile="ssl"]=8443 \  
--db.url[env="dev"]="jdbc:oracle:thin:@dev.db.server:1521:sid" \  
--db.url[env="prod",zone="eu"]="jdbc:oracle:thin:@prod_eu.db.server:1521:sid" \  
--db.url[env="prod",zone="us"]="jdbc:oracle:thin:@prod_us.db.server:1521:sid"
```

```
public static void main(String[] args) {  
    CommandLineConfigurationSource source = new CommandLineConfigurationSource(args);  
    ...  
}
```

This implementation is [defaultable](#).

## .properties file configuration source

The **.properties** file configuration source exposes configuration properties specified in a **.properties** file. This implementation supports parameterized properties.

Configuration properties can be specified in a property file using a syntax similar to the command line configuration source for the property key. Some characters must be escaped with respect to the **.properties** file format. Property values don't need to follow Java's notation for strings since they are considered as strings by design.

```
web.server_port=8080
web.server_port[profile\="ssl"]=8443
db.url[env\="dev"]=jdbc:oracle:thin:@dev.db.server:1521:sid
db.url[env\="prod",zone\="eu"]=jdbc:oracle:thin:@prod_eu.db.server:1521:sid
db.url[env\="prod",zone\="us"]=jdbc:oracle:thin:@prod_us.db.server:1521:sid
```

```
PropertyFileConfigurationSource source = new PropertyFileConfigurationSource(new
ClasspathResource(URI.create("classpath:/path/to/file")));
...
```

This implementation is [defaultable](#).

## .cprops file configuration source

The **.cprops** file configuration source exposes configuration properties specified in a **.cprops** file. This implementation supports parameterized properties.

The **.cprops** file format has been introduced to facilitate the definition and reading of parameterized properties. In particular it allows to regroup the definition of properties with common parameters into sections and many more.

For instance:

```
### This is a comment
server.port=8080
db.url=jdbc:oracle:thin:@localhost:1521:sid
db.user=user
db.password=password
log.level=ERROR
application.greeting.message=""
=== Welcome! ===

    This is
    a formatted
    message.

=====
""

[ environment="test" ] {
    db.url=jdbc:oracle:thin:@test:1521:sid
    db.user=user_test
    db.password=password_test
```

```

}

[ environment="production" ] {
    db.url=jdbc:oracle:thin:@production:1521:sid
    db.user=user_production
    db.password=password_production

    [ zone="US" ] {
        db.url=jdbc:oracle:thin:@production.us:1521:sid
    }

    [ zone="EU" ] {
        db.url=jdbc:oracle:thin:@production.eu:1521:sid
    }

    [ zone="EU", node="node1" ] {
        log.level=DEBUG
    }
}

```

A complete [JavaCC grammar](#) is available in the source of the configuration module.

```

CPropsFileConfigurationSource source = new CPropsFileConfigurationSource(new
ClasspathResource(URI.create("classpath:/path/to/file"))));
...

```

This implementation is [defaultable](#).

## Redis configuration source

The [Redis](#) configuration source exposes configuration properties stored in a Redis data store. This implementation supports parameterized properties and it is also configurable which means it can be used to set configuration properties in the data store at runtime.

The following example shows how to set configuration properties for the **dev** and **prod** environment:

```

RedisClient<String, String> redisClient = ...
RedisConfigurationSource source = new RedisConfigurationSource(redisClient);

source
    .set("db.url", "jdbc:oracle:thin:@dev.db.server:1521:sid").withParameters("environment",
"dev").and()
    .set("db.url", "jdbc:oracle:thin:@prod_eu.db.server:1521:sid").withParameters("environment",
"prod", "zone", "eu").and()
    .set("db.url", "jdbc:oracle:thin:@prod_us.db.server:1521:sid").withParameters("environment",
"prod", "zone", "us")
    .execute()
    .blockLast();

```

This implementation is [defaultable](#).



## Versioned Redis configuration source

The versioned [Redis](#) configuration source exposes configuration properties stored in a Redis data store. This implementation supports parameterized properties and it is also configurable which means it can be used to set configuration properties in the data store at runtime.

The main difference with the [Redis configuration source](#) lies in the fact that it also provides a simple but effective versioning system which allows to set multiple properties and activate or revert them atomically. A global revision keeps track of the whole data store but it is also possible to version a particular branch in the tree of properties.

The following example shows how to set configuration properties for the **dev** and **prod** environment and activates them globally or independently:

```
RedisTransactionalClient<String, String> redisClient = ...
VersionedRedisConfigurationSource source = new VersionedRedisConfigurationSource(redisClient);

source
    .set("db.url", "jdbc:oracle:thin:@dev.db.server:1521:sid").withParameters("environment",
"dev").and()
    .set("db.url", "jdbc:oracle:thin:@prod_eu.db.server:1521:sid").withParameters("environment",
"prod", "zone", "eu").and()
    .set("db.url", "jdbc:oracle:thin:@prod_us.db.server:1521:sid").withParameters("environment",
"prod", "zone", "us")
    .execute()
    .blockLast();

// Activate working revision globally
source.activate().block();

// Activate working revision for dev environment and prod environment independently
source.activate("environment", "dev").block();
source.activate("environment", "prod").block();
```

It is also possible to fallback to a particular revision by specifying it in the **activate()** method:

```
// Activate revision 2 globally
source.activate(2).block();
```

This implementation is particularly suitable to load tenant specific configuration in a multi-tenant application, or user preferences... basically any kind of configuration that can and will be dynamically changed at runtime and might require atomic activation or fallback.

Parameterized properties and versioning per branch are two simple yet powerful features but it is important to be picky here otherwise there is a real risk of messing things up. You should thoughtfully decide when a configuration branch can be versioned, for instance the versioned sets of properties must be disjointed (if this is not obvious, think again), this is actually checked in the Redis configuration source and an exception will be thrown if you try to do things like this, basically trying to version the same property twice.

This implementation is [defaultable](#).

## Composite Configuration source

The composite configuration source is a configuration source implementation that allows to compose multiple configuration sources into one configuration source.

The property returned for a configuration query key then depends on the order in which configuration sources were defined in the composite configuration source, from the highest priority to the lowest.

The `CompositeConfigurationSource` resolves a configuration property by querying its sources in sequence from the highest priority to the lowest. It relies on a `CompositeConfigurationStrategy` to determine at each round which queries to execute and retain the best matching property from the results. The best matching property is the property whose key is the closest to the original configuration query key according to a `DefaultingStrategy`. The algorithm stops when an exact match is found or when there's no more configuration source to query.

A common defaulting strategy provided by the `CompositeConfigurationStrategy` is applied to all sources before executing a batch of queries, this allows to remain consistent and use a common defaulting strategy as well as optimizing the queries to execute on each source by keeping track of intermediate results.

For a composite configuration source using a `CompositeConfigurationStrategy#lookup()` strategy, which is the default, the best matching property for a given original query is determined by prioritizing query parameters from left to right as defined by the [lookup defaulting strategy](#). As a result, an original query with  $n$  parameters results in  $n+1$  queries being executed on a source if no property was retained in previous rounds and  $n-p$  queries if a property with  $p$  parameters ( $p < n$ ) was retained in previous rounds. Please remember that when using the lookup defaulting strategy the order into which parameters are specified in the original query is significant: `property[p1=v1,p2=v2]` is not the same as `property[p2=v2,p1=v1]`.

Let's consider two parameterized configuration sources: `source1` and `source2`.

`source1` holds the following properties:

- `server.url[]=null`
- `server.url[zone="US", environment="production"]="https://prod.us"`
- `server.url[zone="EU"]="https://default.eu"`

`source2` holds the following properties:

- `server.url[]="https://default"`
- `server.url[environment="test"]="https://test"`
- `server.url[environment="production"]="https://prod"`

We can compose them in a composite configuration source as follows:

```

ConfigurationSource<?, ?, ?> source1 = ...
ConfigurationSource<?, ?, ?> source2 = ...

CompositeConfigurationSource source = new CompositeConfigurationSource(List.of(source1, source2));

source
    .get("server.url").withParameters("zone", "US", "environment", "production") // 1
    .and().get("server.url").withParameters("environment", "test") // 2
    .and().get("server.url") // 3
    .and().get("server.url").withParameters("zone", "EU", "environment", "production") // 4
    .and().get("server.url").withParameters("environment", "production", "zone", "EU") // 5
    .subscribe(result -> ...);

```

In the example above:

1. `server.url[environment="production",zone="US"]` is exactly defined in `source1` => `https://prod.us` defined in `source1` is returned
2. `server.url[environment="test"]` is not defined in `source1` but exactly defined in `source2` => `https://test` defined in `source2` is returned
3. Although `server.url[]` is defined in both `source1` and `source2`, `source1` has the highest priority and therefore => `null` is returned
4. There is no exact match for `server.url[zone="EU", environment="production"]` in both `source1` and `source2`, the priority is given to the parameters from left to right, the property matching `server.url[zone="EU"]` shall be returned => `https://default.eu` defined in `source1` is returned
5. Here we've simply changed the order of the parameters in the previous query, again the priority is given to parameters from left to right, since there is no match for `server.url[environment="production", zone="EU"]`, `server.url[environment="production"]` is considered => `https://prod` defined in `source2` is returned

When considering multiple configuration sources, properties can be defined with the exact same key in two different sources, the source with the highest priority wins. In the last example we've been able to set the value of `server.url[]` to `null` in `source1`, however `null` is itself a value with a different meaning than a missing property, the `unset` value can be used in such situation to *unset* a property defined in a source with a lower priority.

For instance, considering previous example, we could have defined `server.url[]=unset` instead of `server.url[]=null` in `source1`, the query would then have returned an empty query result indicating an undefined property.

Prioritization and defaulting also apply when listing configuration properties on a composite configuration source. In case of conflict between two configuration sources, the default strategy retains the one defined by the source with the highest priority.

For instance, if we consider the following sources: `source1` and `source2`.

`source1` holds the following properties:

- `logging.level[environment="dev"]=info`
- `logging.level[environment="dev",name="test1"]=info`
- `logging.level[environment="prod",name="test1"]=info`
- `logging.level[environment="prod",name="test4"]=error`

- `logging.level[environment="prod",name="test5"]=info`
- `logging.level[environment="prod",name="test1",node="node-1"]=trace`

`source2` holds the following properties:

- `logging.level[environment="dev",node="node-1"]=info`
- `logging.level[environment="dev",name="test1"]=debug`
- `logging.level[environment="dev",name="test2"]=debug`
- `logging.level[environment="dev",name="test2",node="node-1"]=debug`
- `logging.level[environment="prod",name="test1"]=warn`
- `logging.level[environment="prod",name="test2"]=error`
- `logging.level[environment="prod",name="test3"]=info`

If we can compose them in a composite configuration source, we can list configuration properties as follows:

```
ConfigurationSource<?, ?, ?> source1 = ...
```

```
ConfigurationSource<?, ?, ?> source2 = ...
```

```
CompositeConfigurationSource source = new CompositeConfigurationSource(List.of(source1, source2));
```

```
source // 1
    .list("logging.level")
    .withParameters(
        Parameter.of("environment", "prod"),
        Parameter.wildcard("name")
    )
    .execute()
    .subscribe(result -> ...);
```

```
source // 2
    .list("logging.level")
    .withParameters(
        Parameter.of("environment", "dev"),
        Parameter.wildcard("name")
    )
    .executeAll()
    .subscribe(result -> ...);
```

In the example above:

1. `execute()` is exact and returns properties defined with parameters `environment` and `name`, with parameter `environment` only and with no parameter following defaulting rules implemented in the default strategy. As a result the following properties are returned:
  - `logging.level[environment="prod",name="test1"]=info` defined in `source1` and overriding the property defined in `source2`
  - `logging.level[environment="prod",name="test2"]=error` defined in `source2`
  - `logging.level[environment="prod",name="test3"]=info` defined in `source2`
  - `logging.level[environment="prod",name="test4"]=error` defined in `source1`
  - `logging.level[environment="prod",name="test5"]=info` defined in `source1`
2. `executeAll()` returns all properties defined with parameters `environment`, `name` and any other parameter, with parameter `environment` only and with no parameter following defaulting rules implemented in the default strategy. As a result the following properties are returned:

- `logging.level[environment="dev"]=info` defined in `source1` which is the property that would be returned when querying the source with an unspecified name (eg. `logging.level[environment="dev",name="unspecifiedLogger"]`)
- `logging.level[environment="dev",name="test1"]=info` defined in `source1` and overriding the property defined in `source2`
- `logging.level[environment="dev",name="test2"]=debug` defined in `source2`
- `logging.level[environment="dev",name="test2",node="node-1"]=debug` defined in `source2`

it is important to note that list operations, especially on a very large set of data can become quite expensive and impact performances, as a result they must be used wisely.

## Bootstrap configuration source

The bootstrap configuration source is a [composite configuration source](#) preset with configuration sources typically used when bootstrapping an application.

This implementation resolves configuration properties from the following sources in that order, from the highest priority to the lowest:

- command line
- system properties
- system environment variables
- the `configuration.cprops` file in `./conf/` or `${inverno.conf.path}/` directories if one exists (if the first one exists the second one is ignored)
- the `configuration.cprops` file in `/home/jkuhn/Devel/git/winter/inverno-apps/inverno-utilities/target/maven-inverno/application_linux_amd64/inverno-utilities-1.3.0-SNAPSHOT/lib/runtime/conf/` directory if it exists
- the `configuration.cprops` file in the application module if it exists

This source is typically created in a `main` method to load the bootstrap configuration on startup.

```
public class Application {

    public static void main(String[] args) {
        BootstrapConfigurationSource source = new
BootstrapConfigurationSource(Application.class.getModule(), args);

        // Load configuration
        ApplicationConfiguration configuration = ConfigurationLoader
            .withConfiguration(ApplicationConfiguration.class)
            .withSource(source)
            .load()
            .block();

        // Start the application with the configuration
        ...
    }
}
```

# Configuration loader

The API offers a great flexibility but as we've seen it might require some efforts to load a configuration in a usable explicit Java bean. Hopefully, this has been anticipated and the configuration module provides a configuration loader to smoothly load configuration objects in the application.

The `ConfigurationLoader` interface is the main entry point for loading configuration objects from a configuration source. It can be used in two different ways, either dynamically using Java reflection or statically using the Inverno compiler.

## Dynamic loader

A dynamic loader can be created by invoking static method `ConfigurationLoader#withConfiguration()` which accepts a single `Class` argument specifying the type of the configuration that must be loaded.

A valid configuration type must be an interface defining configuration properties as non-void no-argument methods whose names correspond to the configuration properties to retrieve and to map to the resulting configuration object, default values can be specified in default methods.

For instance the following interface represents a valid configuration type which can be loaded by a configuration loader:

```
public interface AppConfiguration {  
  
    // query property 'server_host'  
    String server_host();  
  
    // query property 'server_port'  
    default int server_port() {  
        return 8080;  
    }  
}
```

It can be loaded at runtime as follows:

```
ConfigurationSource<?, ?, ?> source = ...
```

```
ConfigurationLoader  
    .withConfiguration(AppConfiguration.class)  
    .withSource(source)  
    .withParameters("environment", "production")  
    .load()  
    .map(configuration -> startServer(configuration.server_host(), configuration.server_port()))  
    .subscribe();
```

In the above example, the configuration source is queried for properties `server_host[environment="production"]` and `server_port[environment="production"]`.

The dynamic loader also supports nested configurations when the return type of a method is an interface representing a valid configuration type.

```

public interface ServerConfiguration {

    // query property 'server_host'
    String server_host();

    // query property 'server_port'
    default int server_port() {
        return 8080;
    }
}

public interface AppConfiguration {

    // Prefix child property names with 'server_configuration'
    ServerConfiguration server_configuration();
}

```

In the above example, the configuration source is queried for properties `server_configuration.server_host[environment="production"]` and `server_configuration.server_port[environment="production"]`.

It is also possible to load a configuration by invoking static method `ConfigurationLoader#withConfigurator()` which allows to load any type of configuration (not only interface) by relying on a configurator and a mapping function.

A configurator defines configuration properties as void single argument methods whose names correspond to the configuration properties to retrieve and inject into a configurator instance using a dynamic configurer `Consumer<Configurator>`. The mapping function is finally applied to that configurer to actually create the resulting configuration object.

For instance, previous example could have been implemented as follows:

```

public class AppConfiguration {

    private String server_host;
    private String server_port = 8080;

    // query property 'server_host'
    public void server_host(String server_host) {
        this.server_host = server_host;
    }

    // query property 'server_port'
    public void server_port(int server_port) {
        this.server_port = server_port;
    }

    public String server_host() {
        return server_host;
    }

    public int server_port() {
        return server_port;
    }
}

```

```
ConfigurationSource<?, ?, ?> source = ...
```

```
ConfigurationLoader
    .withConfigurator(AppConfiguration.class, configurer -> {
        AppConfiguration configuration = new AppConfiguration();
        configurer.apply(configuration);
        return configuration;
    })
    .withSource(source)
    .withParameters("environment", "production")
    .load()
    .map(configuration -> startServer(configuration.server_host(), configuration.server_port()))
    .subscribe();
```

## Static loader

Dynamic loading is fine but it relies on Java reflection which induces extra processing at runtime and might cause unexpected runtime errors due to the lack of static checking. This is all the more true as most of the time configuration definitions are known at compile time. For these reasons, it is better to create adhoc configuration loader implementations. Fortunately, the configuration Inverno compiler plugin can generate these for us.

In order to create a configuration bean in an Inverno module, we simply need to create an interface for our configuration as specified above and annotates it with `@Configuration`, this will tell the configuration Inverno compiler plugin to generate a corresponding configuration loader implementation as well as a module bean making our configuration directly available inside our module.

```
@Configuration
public interface AppConfiguration {

    // query property 'server_host'
    String server_host();

    // query property 'server_port'
    int server_port();
}
```

The preceding code will result in the generation of class `AppConfigurationLoader` which can then be used to load configuration at runtime without resorting to reflection.

```
ConfigurationSource<?, ?, ?> source = ...
```

```
new AppConfigurationLoader()
    .withSource(source)
    .withParameters("environment", "production")
    .load()
    .map(configuration -> startServer(configuration.server_host(), configuration.server_port()))
    .subscribe();
```

A configuration can also be obtained *manually* as follows:



```
AppConfiguration defaultConfiguration = AppConfigurationLoader.load(configurator ->
configurator.server_host("0.0.0.0"));
```

```
AppConfiguration customConfiguration = AppConfigurationLoader.load(configurator ->
configurator.server_host("0.0.0.0"));
```

By default, the generated loader also defines an overridable module bean which loads the configuration in the module. This bean defines three optional sockets:

- **configurationSource** indicates the configuration source to query when initializing the configuration bean
- **parameters** indicates the parameters to consider when querying the source
- **configurer** provides a way to overrides default values

If no configuration source is present, a default configuration is created, otherwise the configuration source is queried with the parameters, the resulting configuration is then *patched* with the configurer if present. The bean is overridable by default which means we can inject our own implementation if we feel like it.

It is possible to disable the activation of the configuration bean or make it non overridable in the `@Configuration` interface:

```
@Configuration(generateBean = false, overridable = false)
public interface AppConfiguration {
    ...
}
```

Finally, nested beans can be specified in a configuration which is convenient when a module is composing multiple modules and we wish to aggregate all configurations into one single representation in the composite module.

For instance, we can have the following configuration defined in a component module:

```
@Configuration
public interface ComponentModuleConfiguration {
    ...
}
```

and the following configuration defined in the composite module:

```
@Configuration
public interface CompositeModuleConfiguration {

    @NestedBean
    ComponentModuleConfiguration component_module_configuration();
}
```

In the preceding example, we basically indicate to the Inverno framework that the `ComponentModuleConfiguration` defined in the `CompositeModuleConfiguration` must be injected into the component module instance.

# HTTP Base

The Inverno *http-base* module defines the foundational API for creating HTTP clients and servers. It also provides common HTTP services such as the header service.

In order to use the Inverno *http-base* module, we need to declare a dependency in the module descriptor:

```
module io.inverno.example.app {
    requires io.inverno.mod.http.base;
    ...
}
```

And also declare that dependency in the build descriptor:

Using Maven:

```
<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-http-base</artifactId>
    </dependency>
  </dependencies>
</project>
```

Using Gradle:

```
...
compile 'io.inverno.mod:inverno-http-base:1.5.3'
...
```

The *http-base* module is usually provided as a transitive dependency by other HTTP modules, the *http-server* module or the *web* module in particular, so this might not be necessary.

## HTTP base API

The base HTTP API defines common classes and interfaces for implementing applications or modules using HTTP/1.x or HTTP/2 protocols. This includes:

- HTTP methods and status enumerations
- Exception bindings for HTTP errors: `BadRequestException`, `InternalServerErrorException`...
- basic building blocks such as `Parameter` which defines the base interface for any HTTP component that can be represented as a key/value pair (eg. query parameter, header, cookie...)
- Cookie types: `Cookie` and `SetCookie`
- Common HTTP header names (`Headers.NAME_*`) and values (`Headers.VALUE_*`) constants
- Common HTTP header types: `Headers.ContentType`, `Headers.Accept...`
- HTTP header codec API for implementing HTTP header codec used to decode a raw HTTP header in a specific `Header` object
- A HTTP header service used to encode/decode HTTP headers from/to specific `Header` objects

# HTTP header service

The HTTP header service is the main entry point for decoding and encoding HTTP headers.

The `HeaderService` interface defines method to decode/encode `Header` object from/to `String` or `ByteBuf`.

For instance, a `content-type` header can be parsed as follows:

```
HeaderService headerService = ...

Headers.ContentType contentType = headerService.<Headers.ContentType>decode("content-type",
"application/xml;charset=utf-8");

// application/xml
String mediaType = contentType.getMediaType();
// utf-8
Charset charset = contentType.getCharset();
```

The `http-base` module provides a default implementation exposed as a bean which relies on a set of `HeaderCodec` objects to support specific headers. Custom header codecs can then be injected in the module to extend its capabilities.

For instance, we can create an `ApplicationContextHeaderCodec` codec in order for the header service to decode custom `application-context` headers to `ApplicationContextHeader` instances. The codec must be injected in the `http-base` module either explicitly when creating the module or through dependency injection.

```
Base httpBase = new Base.Builder()
    .setHeaderCodecs(List.of(new ApplicationContextHeaderCodec()))
    .build();

httpBase.start();

ApplicationContextHeaderCodec decodedHeader = httpBase.headerService().
<ApplicationContextHeaderCodec>.decode("...")
...

httpBase.stop();
```

Most of the time the `http-base` module is composed in a composite module and as a result dependency injection should work just fine, so we simply need to declare the codec as a bean in the module composing the `http-base` module to extend the header service.

By default, the `http-base` module provides codecs for the following headers:

- `accept` as defined by [RFC 7231 Section 5.3.2](#)
- `accept-language` as defined by [RFC 7231 Section 5.3.5](#)
- `authorization` as defined by [RFC 7235 Section 4.2](#)
- `content-disposition` as defined by [RFC 6266](#)
- `content-type` as defined by [RFC 7231 Section 3.1.1.5](#)
- `cookie` as defined by [RFC 6265 Section 4.2](#)
- `set-cookie` as defined by [RFC 6265 Section 4.1](#)

# HTTP Server

The Inverno *http-server* module provides fully reactive HTTP/1.x and HTTP/2 server based on [Netty](#).

It especially supports:

- HTTP/1.x pipelining
- HTTP/2 over cleartext
- WebSocket
- HTTP Compression
- TLS
- Interceptors
- Strongly typed contexts
- `application/x-www-form-urlencoded` body decoding
- `multipart/form-data` body decoding
- Server-sent events
- Cookies
- zero-copy file transfer when supported for fast resource transfer
- parameter conversion

The server is fully reactive, based on the reactor pattern and non-blocking sockets which means it requires a limited number of threads to supports thousands of connections with high end performances. This design offers multiple advantages starting with maximizing the usage of resources. It is also easy to scale the server up and down by specifying the number of threads we want to allocate to the server, which ideally corresponds to the number of CPU cores. All this makes it a perfect choice for microservices applications running in containers in the cloud.

This module lays the foundational service and API for building HTTP servers with more complex and advanced features, that is why you might sometimes find it a little bit low level but that is the price of performance. If you require higher level functionalities like request routing, content negotiation and automatic payload conversion please consider the [web module](#).

This module requires basic services like a [net service](#) and a [resource service](#) which are usually provided by the *boot* module, so in order to use the Inverno *http-server* module, we should declare the following dependencies in the module descriptor:

```
@io.inverno.core.annotation.Module
module io.inverno.example.app_http {
    requires io.inverno.mod.boot;
    requires io.inverno.mod.http.server;
}
```

The *http-base* module which provides the header service used by the HTTP server is composed as a transitive dependency in the *http-server* module and as a result it doesn't need to be specified here nor provided in an enclosing module.

We also need to declare these dependencies in the build descriptor:

Using Maven:

```
<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-boot</artifactId>
    </dependency>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-http-server</artifactId>
    </dependency>
  </dependencies>
</project>
```

Using Gradle:

```
...
compile 'io.inverno.mod:inverno-boot:1.5.3'
compile 'io.inverno.mod:inverno-http-server:1.5.3'
...
```

The resulting *app\_http* module, thus created, can then be started as an application as follows:

```
package io.inverno.example.app_http;

import io.inverno.core.v1.Application;

public class Main {

    public static void main(String[] args) {
        Application.with(new App_http.Builder()).run();
    }
}
```

The above example starts a HTTP/1.x server using default configuration and a default server controller.



The following configuration can then be created in the *app\_http* module:

```
package io.inverno.example.app_http;

import io.inverno.core.annotation.NestedBean;
import io.inverno.mod.boot.BootConfiguration;
import io.inverno.mod.configuration.Configuration;
import io.inverno.mod.http.server.HttpServerConfiguration;

@Configuration
public interface App_httpConfiguration {

    @NestedBean
    BootConfiguration boot();

    @NestedBean
    HttpServerConfiguration http_server();
}
```

This should be enough for exposing a configuration in the *app\_http* module that let us setup the server:

```
package io.inverno.example.app_http;

import io.inverno.core.v1.Application;

public class Main {

    public static void main(String[] args) {
        Application.with(new App_http.Builder()
            .setApp_httpConfiguration(
                App_httpConfigurationLoader.load(configuration -> configuration
                    .http_server(server -> server
                        .server_port(8081)
                        .h2c_enabled(true)
                    )
                    .boot(boot -> boot
                        .reactor_event_loop_group_size(4)
                    )
                )
            ).run();
    }
}
```

In the above code, we have set the server port to 8081, enabled HTTP/2 over cleartext and set the number of thread allocated to the reactor core IO event loop group to 4.

Please refer to the [API documentation](#) to have an exhaustive description of the different configuration properties. We can for instance configure low level network settings like TCP keep alive or TCP no delay as well as HTTP related settings like compression or TLS.

You can also refer to the [configuration module documentation](#) to get more details on how configuration works and more especially how you can from here define the HTTP server configuration in command line arguments, property files...

# Logging

The HTTP server can log access and error events at **INFO** and **ERROR** level respectively. They can be disabled by configuring `io.inverno.mod.http.server.Exchange` logger as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration xmlns="http://logging.apache.org/log4j/2.0/config"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://logging.apache.org/log4j/2.0/config
https://raw.githubusercontent.com/apache/logging-log4j2/rel/2.14.0/log4j-
core/src/main/resources/Log4j-config.xsd"
  status="WARN" shutdownHook="disable">

  <Appenders>
    <Console name="LogToConsole" target="SYSTEM_OUT">
      <PatternLayout pattern="%d{DEFAULT} %highlight{%5level} [%t] %c{1.} - %msg%n%ex"/>
    </Console>
  </Appenders>
  <Loggers>
    <!-- Disable HTTP server access and error logs -->
    <Logger name="io.inverno.mod.http.server.Exchange" additivity="false" level="off" />

    <Root level="info">
      <AppenderRef ref="LogToConsole"/>
    </Root>
  </Loggers>
</Configuration>
```

We can also create a more *production-like* logging configuration for a standard HTTP server that asynchronously logs access and error events in separate files in a JSON format for easy integration with log processing tools with a rolling strategy.



```

<?xml version="1.0" encoding="UTF-8"?>
<Configuration status="WARN" name="Website" shutdownHook="disable">
  <Appenders>
    <Console name="Console" target="SYSTEM_OUT">
      <PatternLayout pattern="%d{DEFAULT} %highlight{%5level} [%t] %c{1.} - %msg%n%ex"/>
    </Console>
    <!-- Error log -->
    <RollingRandomAccessFile name="ErrorRollingFile" fileName="logs/error.log"
filePattern="logs/error-%d{yyyy-MM-dd}-%i.log.gz">
      <JsonTemplateLayout/>
      <NoMarkerFilter onMatch="ACCEPT" onMismatch="DENY"/>
      <Policies>
        <TimeBasedTriggeringPolicy />
        <SizeBasedTriggeringPolicy size="10 MB"/>
      </Policies>
      <DefaultRolloverStrategy>
        <Delete basePath="logs" maxDepth="2">
          <IfFileName glob="error-*.log.gz" />
          <IfLastModified age="10d" />
        </Delete>
      </DefaultRolloverStrategy>
    </RollingRandomAccessFile>
    <Async name="AsyncErrorRollingFile">
      <AppenderRef ref="ErrorRollingFile"/>
    </Async>
    <!-- Access log -->
    <RollingRandomAccessFile name="AccessRollingFile" fileName="logs/access.log"
filePattern="logs/access-%d{yyyy-MM-dd}-%i.log.gz">
      <JsonTemplateLayout/>
      <MarkerFilter marker="HTTP_ACCESS" onMatch="ACCEPT" onMismatch="DENY"/>
      <Policies>
        <TimeBasedTriggeringPolicy />
        <SizeBasedTriggeringPolicy size="10 MB"/>
      </Policies>
      <DefaultRolloverStrategy>
        <Delete basePath="logs" maxDepth="2">
          <IfFileName glob="access-*.log.gz" />
          <IfLastModified age="10d" />
        </Delete>
      </DefaultRolloverStrategy>
    </RollingRandomAccessFile>
    <Async name="AsyncAccessRollingFile">
      <AppenderRef ref="AccessRollingFile"/>
    </Async>
  </Appenders>

  <Loggers>
    <Logger name="io.inverno.mod.http.server.Exchange" additivity="false" level="info">
      <AppenderRef ref="AsyncAccessRollingFile" level="info"/>
      <AppenderRef ref="AsyncErrorRollingFile" level="error"/>
    </Logger>

    <Root level="info" additivity="false">
      <AppenderRef ref="Console" level="info" />
      <AppenderRef ref="AsyncErrorRollingFile" level="error"/>
    </Root>
  </Loggers>
</Configuration>

```

Note that access and error events are logged by the same logger, they are differentiated by markers, `HTTP_ACCESS` and `HTTP_ERROR` respectively.

## Transport

By default, the HTTP server uses the Java NIO transport, but it is possible to use native [epoll](#) transport on Linux or [kqueue](#) transport on BSD-like systems for optimized performances. This can be done by adding the corresponding Netty dependencies with the right classifier in the project descriptor:

```
<project>
  <dependencies>
    <dependency>
      <groupId>io.netty</groupId>
      <artifactId>netty-transport-classes-epoll</artifactId>
    </dependency>
    <dependency>
      <groupId>io.netty</groupId>
      <artifactId>netty-transport-native-epoll</artifactId>
      <classifier>linux-x86_64</classifier>
    </dependency>
  </dependencies>
</project>
```

or

```
<project>
  <dependencies>
    <dependency>
      <groupId>io.netty</groupId>
      <artifactId>netty-transport-classes-kqueue</artifactId>
    </dependency>
    <dependency>
      <groupId>io.netty</groupId>
      <artifactId>netty-transport-native-kqueue</artifactId>
      <classifier>osx-x86_64</classifier>
    </dependency>
  </dependencies>
</project>
```

When these dependencies are declared on the JVM module path, the corresponding Java modules must be added explicitly when running the application. This is typically the case when the application is run or packaged as an application image using the Inverno Maven plugin.

This can be done by defining the corresponding dependencies in the module descriptor:

```
@io.inverno.core.annotation.Module
module io.inverno.example.app {
    ...
    requires io.netty.transport.unix.common;
    requires io.netty.transport.classes.epoll,
    requires io.netty.transport.epoll.linux.x86_64;
}
```

This approach is fine as long as we are sure the application will run on Linux, but in order to create a properly portable application, we should prefer adding the modules explicitly when running the application:

```
$ java --add-modules
io.netty.transport.unix.common,io.netty.transport.classes.epoll,io.netty.transport.epoll.linux.
x86_64 ...
```

When building an application image, this can be specified in the Inverno Maven plugin configuration:

```
<project>
  <build>
    <plugins>
      <plugin>
        <groupId>io.inverno.tool</groupId>
        <artifactId>inverno-maven-plugin</artifactId>
        <executions>
          <execution>
            <configuration>
              <vmOptions>--add-modules
io.netty.transport.unix.common,io.netty.transport.classes.epoll,io.netty.transport.epoll.linux.
x86_64</vmOptions>
            </configuration>
          </execution>
        </executions>
      </plugin>
    </plugins>
  </build>
</project>
```

## HTTP compression

HTTP compression can be activated by configuration for request and/or response. For instance:

```

public class Main {

    public static void main(String[] args) {
        Application.with(new App_http.Builder()
            .setApp_httpConfiguration(
                App_httpConfigurationLoader.load(configuration -> configuration
                    .http_server(server -> server
                        .decompression_enabled(true)
                        .compression_enabled(true)
                        .compression_level(6)
                    )
                )
            )
        ).run();
    }
}

```

Now if we send a request which accepts compression to the server, we should now receive a compressed response:

```

$ curl -i --compressed -H 'accept-encoding: gzip, deflate' http://localhost:8080
HTTP/1.1 200 OK
content-type: text/plain
server: inverno
content-encoding: gzip
content-length: 39

Hello

```

## TLS

In order to activate TLS, we need first to obtain a private key and a certificate stored in a keystore.

A self-signed certificate can be generated using `keytool`, the resulting keystore should be placed in `src/main/resources` to make it available as a module resource:

```

$ keytool -genkey -keyalg RSA -alias selfsigned -keystore keystore.jks -storepass password -validity
360 -keysize 2048

```

Then we need to configure the server to activate TLS using the certificate:

```

public class Main {

    public static void main(String[] args) {
        Application.with(new App_http.Builder()
            .setApp_httpConfiguration(
                App_httpConfigurationLoader.load(configuration -> configuration
                    .http_server(server -> server
                        .server_port(8443)
                        .tls_enabled(true)
                        .key_store(URI.create("module://io.inverno.example.app_http/keystore.jks"))
                        .key_alias("selfsigned")
                        .key_store_password("password")
                    )
                )
            )
        ).run();
    }
}

```

When an application using the *http-server* module is packaged as an application image, you'll need to make sure TLS related modules from the JDK are included in the runtime image otherwise TLS might not work. You can refer to the [JDK providers documentation](#) in the security developer's guide to find out which modules should be added depending on your needs. Most of the time you'll simply add `jdk.crypto.ec` module in the Inverno Maven plugin configuration:

```
<project>
  <build>
    <plugins>
      <plugin>
        <groupId>io.inverno.tool</groupId>
        <artifactId>inverno-maven-plugin</artifactId>
        <executions>
          <execution>
            <configuration>
              <addModules>jdk.crypto.ec</addModules>
            </configuration>
          </execution>
        </executions>
      </plugin>
    </plugins>
  </build>
</project>
```

## Server Controller

The server controller specifies how exchanges and errors are handled by the server. It also provides the exchange context created and attached to the exchange by the server.

The `ServerController` interface basically defines the following methods:

- `Mono<Void> defer(Exchange<ExchangeContext> exchange)` which is used to handle an exchange
- `Mono<Void> defer(ErrorExchange<ExchangeContext> errorExchange)` which is used to handle an error exchange
- `ExchangeContext createContext()` which provides the context attached to an exchange

Methods `void handle(Exchange<ExchangeContext> exchange)` and `void handle(ErrorExchange<ExchangeContext> errorExchange)` are also defined, they can be more convenient when the handling logic does not have to be reactive. Note that the server will always invoke `defer()` methods which must then be properly implemented.

As stated before, the *http-server* module provides a default `ServerController` implementation which returns `Hello` when a request is made to the root path `/` and (404) not found error otherwise. By default no context is created and `exchange.context()` returns `null`.

A custom server controller can be injected when creating the *app\_http* module. In the following code, a socket bean is defined to inject the custom server controller and starts an HTTP server which responds with **Hello from app\_http module!** to any request:

```
package io.inverno.example.app_http;

import io.inverno.core.annotation.Bean;
import io.inverno.core.v1.Application;
import io.inverno.mod.http.server.Exchange;
import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.http.server.ServerController;
import java.util.function.Supplier;

public class Main {

    @Bean
    public static interface Controller extends Supplier<ServerController<ExchangeContext,
Exchange<ExchangeContext>, ErrorExchange<ExchangeContext>>> {}

    public static void main(String[] args) {
        Application.with(new App_http.Builder()
            .setController(
                exchange -> exchange.response().body().string().value("Hello from app_http module!")
            )
        ).run();
    }
}
```

The **ServerController** interface also exposes static methods to easily create a server controller with custom exchange and error exchange handlers:

```

package io.inverno.example.app_http;

import io.inverno.core.annotation.Bean;
import io.inverno.core.v1.Application;
import io.inverno.mod.http.server.Exchange;
import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.http.server.ServerController;
import java.util.function.Supplier;

public class Main {

    @Bean
    public static interface Controller extends Supplier<ServerController<ExchangeContext,
Exchange<ExchangeContext>, ErrorExchange<ExchangeContext>>> {}

    public static void main(String[] args) {
        Application.with(new App_http.Builder()
            .setController(
                ServerController.from(
                    exchange -> {
                        exchange.response()
                            .body().string().value("Hello from app_http module!");
                    },
                    errorExchange -> {
                        errorExchange.response()
                            .headers(headers -> headers.status(Status.INTERNAL_SERVER_ERROR))
                            .body().string().value(errorExchange.getError().getMessage());
                    }
                )
            )
        ).run();
    }
}

```

It is also possible to provide a server controller bean in the *app\_http* module:

```

package io.inverno.example.app_http;

import io.inverno.core.annotation.Bean;
import io.inverno.mod.http.base.HttpException;
import io.inverno.mod.http.server.ErrorExchange;
import io.inverno.mod.http.server.Exchange;
import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.http.server.ServerController;

@Bean
public class App_httpServerController implements
ServerController<App_httpServerController.CustomContext,
Exchange<App_httpServerController.CustomContext>,
ErrorExchange<App_httpServerController.CustomContext>>{

    @Override
    public void handle(Exchange<CustomContext> exchange) throws HttpException {
        exchange.response().body().string().value("Hello " + exchange.context().getName() + " from
app_http module!");
    }

    @Override
    public CustomContext createContext() {
        return new CustomContext();
    }

    public static class CustomContext implements ExchangeContext {

        private String name = "anonymous";

        public String getName() {
            return name;
        }

        public void setName(String name) {
            this.name = name;
        }
    }
}

```

This bean is automatically wired to the server controller socket defined by the *http-server* module overriding the default server controller.

Note that above implementation still uses the default error handler.

With this approach there is no need for a server controller socket bean and the server can be simply started as before:



```

package io.inverno.example.app_http;

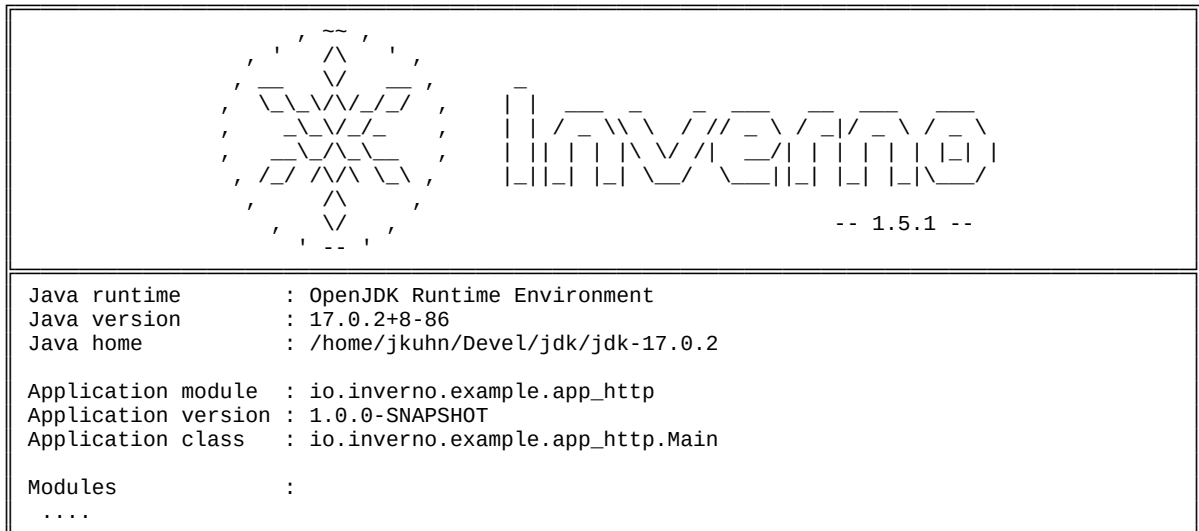
import io.inverno.core.v1.Application;

public class Main {

    public static void main(String[] args) {
        Application.with(new App_http.Builder()).run();
    }
}

```

```
2022-07-18 11:12:57,710 INFO [main] i.i.c.v.Application - Inverno is starting...
```



```

2022-07-18 11:12:57,713 INFO [main] i.i.e.a.App_http - Starting Module
io.inverno.example.app_http...
2022-07-18 11:12:57,713 INFO [main] i.i.m.b.Boot - Starting Module io.inverno.mod.boot...
2022-07-18 11:12:57,935 INFO [main] i.i.m.b.Boot - Module io.inverno.mod.boot started in 221ms
2022-07-18 11:12:57,935 INFO [main] i.i.m.h.s.Server - Starting Module
io.inverno.mod.http.server...
2022-07-18 11:12:57,935 INFO [main] i.i.m.h.b.Base - Starting Module io.inverno.mod.http.base...
2022-07-18 11:12:57,940 INFO [main] i.i.m.h.b.Base - Module io.inverno.mod.http.base started in 5ms
2022-07-18 11:12:57,994 INFO [main] i.i.m.h.s.i.HttpServer - HTTP Server (nio) listening on
http://0.0.0.0:8080
2022-07-18 11:12:57,995 INFO [main] i.i.m.h.s.Server - Module io.inverno.mod.http.server started in
59ms
2022-07-18 11:12:57,995 INFO [main] i.i.e.a.App_http - Module io.inverno.example.app_http started
in 283ms
2022-07-18 11:12:57,998 INFO [main] i.i.c.v.Application - Application io.inverno.example.app_http
started in 333ms

```

Now if we send a request to the server we should get the following response:

```

$ curl -i http://localhost:8080
HTTP/1.1 200 OK
content-length: 37

Hello anonymous from app_http module!

```

## HTTP Server API

The module defines classes and interfaces to handle HTTP requests sent by a client or errors raised during that process.

As we just saw, a `ServerController` must be provided to handle `Exchange` and `ErrorExchange`. An exchange represents an HTTP communication between a client and a server, it is composed of a `Request`, a `Response` and an `ExchangeContext`. An error exchange is created whenever an error is raised during the normal processing of an exchange and allows to report the error to the client. The API has been designed to be fluent and reactive in order for the request to be *streamed* down to the response.

## Exchange handler

An exchange handler is defined in a server controller and used to handle client-server exchanges. The `ReactiveExchangeHandler` is a functional interface defining method `Mono<Void> defer(Exchange<ExchangeContext> exchange)` which is used to handle server exchanges in a reactive way. It is for instance possible to execute non-blocking operations before actually handling the exchange.

Authentication is a typical example of a non-blocking operation that might be executed before handling the request.

Under the hood, the server first subscribes to the returned `Mono`, when it completes the server then subscribes to the response body data publisher and eventually sends a response to the client.

The `ExchangeHandler` extends the `ReactiveExchangeHandler` with method `void handle(Exchange<ExchangeContext> exchange)` which is more convenient than `defer()` when no non-blocking operation other than the generation of the client response is required.

A basic exchange handler can then be created as follows:

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {  
    exchange.response().body().string().value("Hello, world!");  
};
```

The above exchange handler sends a `Hello, world!` message in response to any request.

## Response body

A response body must be sent back to the client in order to terminate the exchange, the API exposes several ways to provide response data and therefore terminate the exchange.

## Empty

An exchange can be ended with no response body as follows:

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.response().body().empty();
};
```

## String

We already saw how to send a single string response but we might also want to send the response in a reactive way as a stream of data in case the entire response payload is not available right away, if it doesn't fit in memory or if we simply want to send a response in multiple parts as soon as they become available (e.g. progressive display).

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.response().body().string().stream(Flux.just("Hello", " ", "world!"));
};
```

## Raw

Raw data (i.e. bytes) can also be sent in response to a request. As for the string response, the response can be a single byte buffer or a stream of byte buffers:

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    Flux<ByteBuffer> dataStream = Flux.just(
        Unpooled.unreleasableBuffer(Unpooled.copiedBuffer("Hello", Charsets.DEFAULT)),
        Unpooled.unreleasableBuffer(Unpooled.copiedBuffer(" ", Charsets.DEFAULT)),
        Unpooled.unreleasableBuffer(Unpooled.copiedBuffer("world!", Charsets.DEFAULT))
    );

    exchange.response().body().raw().stream(dataStream);
};
```

Returned `ByteBuffer` are released as soon as they are sent to the client.

## Resource

A [resource](#) can be sent in a response body. When possible the server uses low-level ([zero-copy](#)) API for fast resource transfer.

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.response()
        .body().resource().value(new FileResource("/path/to/resource"));
};
```

The media type of the resource is resolved using a [media type service](#) and automatically set in the response `content-type` header field.

If a specific resource is created as in above example the media type service used is the one defined when creating the resource or a default implementation if none was specified. If the resource is obtained with the resource service provided in the *boot* module the media type service used is the one provided in the *boot* module.

## Server-sent events

[Server-sent events](#) provide a way to send server push notifications to a client. It is based on [chunked transfer encoding](#) over HTTP/1.x and regular streams over HTTP/2. The API provides an easy way to create SSE endpoints.

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.response().body().sse().from(
        (events, data) -> data.stream(Flux.interval(Duration.ofSeconds(1))
            .map(seq -> events.create(event -> event
                .id(Long.toString(seq))
                .event("seq")
                .comment("Some comment")
                .value(Unpooled.unreleasableBuffer(Unpooled.copiedBuffer("Event #" + seq,
Charsets.DEFAULT))))))
    );
};
```

In the above example, server-sent events are emitted every second and streamed to the response. This is done in a function accepting the server-sent event factory used to create events and the response data producer.

## Request body

Request body can be handled in a similar way. The reactive API allows to process the payload of a request as the server receives it and therefore progressively build and send the corresponding response.

A request body is however optional as not all HTTP request has a body.

## String

The request body can be consumed as `CharSequence` as follows:

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.response()
        .body().string().stream(exchange.request().body()
            .map(body -> Flux.from(body.string().stream()).map(s -> Integer.toString(s.length()))
            .orElse(Flux.just("0")))
    );
};
```

In the above example, if a client sends a payload in the request, the server responds with the number of characters of each string received or it responds 0 if the request payload is empty. As before, request body is processed as a flow of data.

## Raw

It can also be consumed as raw data as follows:

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.response()
        .body().raw().stream(exchange.request().body()
            .map(body -> Flux.from(body.raw().stream())
                .map(chunk -> {
                    try {
                        return
Unpooled.unreleasableBuffer(Unpooled.buffer(4).writeInt(chunk.readableBytes()));
                    }
                    finally {
                        chunk.release();
                    }
                })
            ))
        .orElse(Flux.just(Unpooled.unreleasableBuffer(Unpooled.buffer(4).writeInt(0))))
};
```

In the above example, if a client sends a payload in the request, the server responds with the number of bytes of each chunk of data it receives or it responds 0 if the request payload is empty. This simple example illustrates how we can process requests as flow of data.

Note that request's **ByteBuf** data must be released when they are consumed in the exchange handler.

## URL Encoded form

HTML form data are sent in the body of a POST request in the form of key/value pairs encoded in [application/x-www-form-urlencoded format](#). The resulting list of **Parameter** can be obtained as follows:

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.response()
        .body().string().stream(Flux.from(exchange.request().body().get().urlEncoded().stream())
            .map(parameter -> "Received parameter " + parameter.getName() + " with value " +
parameter.getValue())
        );
};
```

In the above example, for each form parameters the server responds with a message describing the parameters it just received. Again this shows that the API is fully reactive and form parameters can be processed as they are decoded.

A more traditional example though would be to obtain the map of parameters grouped by names (because multiple parameters with the same name can be sent):

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.response()
        .body().string().stream(Flux.from(exchange.request().body().get().urlEncoded().stream()))
        .collectMultimap(Parameter::getName)
        .map(formParameters -> "User selected options: " +
formParameters.get("options").stream().map(Parameter::getValue).collect(Collectors.joining(", ")))
        );
}
```

Here we may think that the aggregation of parameters in a map could *block* the I/O thread but this is actually not true, when a parameter is decoded, the reactive framework is notified and the parameter is stored in a map, after that the I/O thread can be reallocated. When the parameters publisher completes the resulting map is emitted to the mapping function which build the response. During all this process, no thread is ever waiting for anything.

## Multipart form

A [multipart/form-data](#) request can be handled in a similar way. Form parts can be obtained as follows:

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.response()
        .body().string().stream(Flux.from(exchange.request().body().get().multipart().stream()))
        .map(part -> "Received part " + part.getName())
        );
};
```

Multipart form data is most commonly used for uploading files over HTTP. Such handler can be implemented as follows using the [resource API](#) to store uploaded files:

```

ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.response().body().string().stream(
        Flux.from(exchange.request().body().get().multipart().stream())
// 1
        .flatMap(part -> part.getFilename()
// 2
            .map(fileName -> Flux.<CharSequence, FileResource>using(
// 3
                () -> new FileResource("uploads/" + part.getFilename().get()),
// 4
                file -> file.write(part.raw().stream()).map(Flux::from).get()
// 5
                    .reduce(0, (acc, cur) -> acc + cur)
                    .map(size -> "Uploaded " + fileName + "(" + part.headers().getContentType()
+ "): " + size + " Bytes\n"),
                    FileResource::close
// 6
                ))
            .orElseThrow(() -> new BadRequestException("Not a file part"))
// 7
        )
    );
};

```

The above code uses multiple elements and deserves a detailed explanation:

1. get the stream of parts
2. map the part to the response stream by starting to determine whether the part is a file part
3. if the part is a file part, map the part to the response stream by creating a Flux with a file resource
4. in this case the resource is the target file where the uploaded file will be stored
5. stream the part's payload to the target file resource and eventually provides the response in the form of a message stating that a file with a given size and media type has been uploaded
6. close the file resource when the publisher completes
7. if the part is not a file part respond with a bad request error

The `Flux.using()` construct is the reactive counterpart of a try-with-resource statement. It is interesting to note that the content of the file is streamed up to the file and it is then never entirely loaded in memory. From there, it is quite easy to stop the upload of a file if a given size threshold is exceeded. We can also imagine how we could create a progress bar in a client UI to show the progression of the upload.

In the above code we uploaded one or more file and stored their content on the local file system and during all that process, the I/O thread was never blocked.

Note that since part's `ByteBuffer` data are consumed by the target file resource, there is no need to release them in the exchange handler.

## Error exchange handler

An error exchange handler is defined in a server controller and used to handle errors raised during the normal processing of an exchange in the exchange handler.

It is basically an `ExceptionHandler` of `ErrorExchange`. An error exchange exposes the original error, it is then possible to implement different behaviours based on the type of error:

```
ExceptionHandler<ExchangeContext, ErrorExchange<ExchangeContext>> errorHandler = errorExchange -> {
    if(errorExchange.getError() instanceof BadRequestException) {

        errorExchange.response().body().raw().value(Unpooled.unreleasableBuffer(Unpooled.copiedBuffer("client sent an invalid request", Charsets.DEFAULT)));
    }
    else {

        errorExchange.response().body().raw().value(Unpooled.unreleasableBuffer(Unpooled.copiedBuffer("Unknown server error", Charsets.DEFAULT)));
    }
};
```

## Exchange interceptor

An exchange handler can be intercepted using an `ExchangeInterceptor`. An interceptor can be used to preprocess an exchange in order to check preconditions and potentially respond to the client instead of the handler, initialize a context (tracing, metrics...), decorate the exchange...

The `intercept()` method returns a `Mono` which makes it reactive and allows to invoke non-blocking operations before invoking the handler.

An intercepted exchange handler can be created as follows:

```
ExceptionHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {...};

ExchangeInterceptor<ExchangeContext, Exchange<ExchangeContext>> interceptor = exchange -> {
    LOGGER.info("Path: " + exchange.request().getPath());

    // exchange is returned unchanged and will be processed by the handler
    return Mono.just(exchange);
};

ReactiveExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> interceptedHandler =
    handler.intercept(interceptor);
```

An interceptor can also end an exchange, in which case it must return an empty `Mono` to stop the exchange handling chain.



```

ExchangeInterceptor<ExchangeContext, Exchange<ExchangeContext>> interceptor = exchange -> {
    // Check some preconditions...
    if(...) {
        // Do some processing and terminate the exchange
        exchange.response().body().empty();

        // the exchange has been processed by the interceptor and it won't be processed by the
handler
        return Mono.empty();
    }
    return Mono.just(exchange);
}

```

Multiple interceptors can be chained by invoking `intercept()` method multiple times:

```

// exchange handling chain: interceptor3 -> interceptor2 -> interceptor1 -> handler
handler.intercept(interceptor1).intercept(interceptor2).intercept(interceptor3);

```

## Exchange context

A strongly typed context is exposed in the `Exchange`, it allows to store or access data and to provide contextual operations throughout the process of the exchange. The server creates the context along with the exchange using the server controller. It is then possible to *customize* the exchange with a specific strongly types context.

The advantage of this approach is that the compiler can perform static type checking but also to avoid the usage of an untyped map of attributes which is less performant and provides no control over contextual data. Since the developer defines the context type, he can also implement logic inside.

A context can be used to store security information, tracing information, metrics... For instance, if we combine this with exchange interceptors:

```

ExchangeHandler<SecurityContext, Exchange<SecurityContext>> handler = exchange -> {
    if(exchange.context().isAuthenticated()) {
        exchange.response().body().string().value("Hello, world!");
    }
    else {
        exchange.response().body().empty();
    }
};

ExchangeInterceptor<SecurityContext, Exchange<SecurityContext>> securityInterceptor = exchange -> {
    // Authenticate the request
    if(...) {
        exchange.context().setAuthenticated(true);
    }
    return Mono.just(exchange);
}

ReactiveExchangeHandler<SecurityContext, Exchange<SecurityContext>> interceptedHandler =
handler.intercept(securityInterceptor);

```

The server relies on the [ServerController](#) in order to create the context. Please refer to the [Server Controller](#) section which explains this in details and describes how to setup the HTTP server.

## Misc

The API is fluent and mostly self-describing as a result it should be easy to find out how to do something in particular, even so here are some miscellaneous elements

### Request headers

Request headers can be obtained as string values as follows:

```
handler = exchange -> {
    // Returns the value of the first occurrence of 'some-header' as string or returns null
    String someHeaderValue = exchange.request().headers().get("some-header").orElse(null);

    // Returns all 'some-header' values as strings
    List<String> someHeaderValues = exchange.request().headers().getAll("some-header");

    // Returns all headers as strings
    List<Map.Entry<String, String>> allHeadersValues = exchange.request().headers().getAll();
};
```

It is also possible to get headers as [Parameter](#) which allows to easily convert the value using a parameter converter:

```
handler = exchange -> {
    // Returns the value of the first occurrence of 'some-header' as LocalDateTime or returns null
    LocalDateTime someHeaderValue = exchange.request().headers().getParameter("some-
header").map(Parameter::asLocalDateTime).orElse(null);

    // Returns all 'some-header' values as LocalDateTime
    List<LocalDateTime> someHeaderValues = exchange.request().headers().getAllParameter("some-
header").stream().map(Parameter::asLocalDateTime).collect(Collectors.toList());

    // Returns all headers as parameters
    List<Parameter> allHeadersParameters = exchange.request().headers().getAllParameter();
};
```

The *http-server* module can also use the [header service](#) provided by the *http-base* module to decode HTTP headers:

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    // Returns the decoded 'content-type' header or null
    Headers.ContentType contentType = exchange.request().headers().
<Headers.ContentType>getHeader(Headers.NAME_CONTENT_TYPE).orElse(null);

    String mediaType = contentType.getMediaType();
    Charset charset = contentType.getCharset();
    ...
};
```

The header service can be extended with custom HTTP `HeaderCodec`. Please refer to [Extending HTTP services](#) and the [http-base module](#) for more information.

## Query parameters

Query parameters in the request can be obtained as follows:

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    ...
    // get a specific query parameter, if there are multiple parameters with the same name, the
    first one is returned
    int someInteger = exchange.request().queryParameters().get("some-
integer").map(Parameter::asInteger).orElseThrow(() -> new BadRequestException("Missing some-
integer"));

    // get all query parameters with a given name
    List<Integer> someIntegers = exchange.request().queryParameters().getAll("some-
integer").stream().map(Parameter::asInteger).collect(Collectors.toList());

    // get all query parameters
    Map<String, List<Parameter>> queryParameters = exchange.request().queryParameters().getAll();
    ...
};
```

## Request cookies

Request cookie can be obtained in a similar way as follows:

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    ...
    // get a specific cookie, if there are multiple cookie with the same name, the first one is
    returned
    int someInteger = exchange.request().cookies().get("some-
integer").map(Parameter::asInteger).orElseThrow(() -> new BadRequestException("Missing some-
integer"));

    // get all cookies with a given name
    List<Integer> someIntegers = exchange.request().cookies().getAll("some-
integer").stream().map(Parameter::asInteger).collect(Collectors.toList());

    // get all cookies
    Map<String, List<CookieParameter>> queryParameters = exchange.request().cookies().getAll();
    ...
};
```

## Request components

The API also gives access to multiple request related information such as:

- the HTTP method:

```
exchange.request().getMethod();
```

- the scheme (`http` or `https`):

```
exchange.request().getScheme();
```

- the authority part of the requested URI (**host** header in HTTP/1.x and **:authority** pseudo-header in HTTP/2):

```
exchange.request().getAuthority();
```

- the requested path including query string:

```
exchange.request().getPath();
```

- the absolute path which is the normalized requested path without the query string:

```
exchange.request().getAbsolutePath();
```

- the **URIBuilder** corresponding to the requested path to build relative paths:

```
exchange.request().getPathBuilder().path("path/to/child/resource").build();
```

- the query string:

```
exchange.request().getQuery();
```

- the socket address of the client or last proxy that sent the request:

```
exchange.request().getRemoteAddress();
```

## Response status

The response status can be set in the response headers following HTTP/2 specification as defined by [RFC 7540 Section 8.1.2.4](#).

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.response()
        .headers(headers -> headers.status(Status.OK))
        .body().raw();
};
```

## Response headers/trailers

Response headers can be added or set fluently using a configurator as follows:

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.response()
        .headers(headers -> headers
            .contentType(MediaType.TEXT_PLAIN)
            .set(Headers.NAME_SERVER, "inverno")
            .add("custom-header", "abc")
        )
        .body().raw()....;
};
```

Response trailers can be set in the exact same way:

```

ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.response()
        .trailers(headers -> headers
            .add("some-trailer", "abc")
        )
        .body().raw()...;
};

```

## Response cookies

Response cookies can be set fluently using a configurator as follows:

```

ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.response()
        .cookies(cookies -> cookies
            .addCookie(cookie -> cookie.name("cookie1")
                .httpOnly(true)
                .secure(true)
                .maxAge(3600)
                .value("abc")
            )
            .addCookie(cookie -> cookie.name("cookie2")
                .httpOnly(true)
                .secure(true)
                .maxAge(3600)
                .value("def")
            )
        )
        .body().raw()...;
};

```

## WebSocket

An HTTP exchange can be upgraded to a WebSocket exchange as defined by [RFC 6455](https://tools.ietf.org/html/rfc6455).

The `websocket()` method exposed on the `Exchange` allows to upgrade to the WebSocket protocol, it returns an optional `WebSocket` which might be empty if the original exchange does not support the upgrade. This is especially the case when using HTTP/2 for which Websocket upgrade is not supported or if the state of the exchange prevents the upgrade (e.g. error exchange).

The resulting `WebSocket` allows specifying a `WebSocketExchangeHandler` and a default action in case the WebSocket opening handshake fails (e.g. the client did not provide the correct headers for the upgrade...). A WebSocket exchange handler is used to handle the resulting `WebSocketExchange` which exposes WebSocket inbound and outbound data.

In the following example, the original HTTP `Exchange` is upgraded to a `WebSocketExchange` and all inbound frames are sent back to the client. An internal server error (500) is returned if WebSocket upgrade is not supported and a bad request error (400) is returned if the opening handshake failed:

```

ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.webSocket()
        .orElseThrow(() -> new InternalServerErrorException("WebSocket not supported"))
        .handler(webSocketExchange -> {
            webSocketExchange.outbound().frames(factory -> webSocketExchange.inbound().frames());
        })
        .or(() -> {
            throw new BadRequestException("Web socket handshake failed");
        });
});

```

It is possible to specify the supported subprotocols when creating the `WebSocket`, an `UnsupportedProtocolException` shall be raised if the subprotocol negotiation fails (i.e. the client requested a protocol that is not supported by the server)

```

ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    // Indicates that the server supports the 'chat' subprotocol
    exchange.webSocket("chat")
        ...
};

```

The `WebSocketExchange` also exposes:

- the original HTTP request,

```
webSocketExchange.request();
```

- the exchange context:

```
webSocketExchange.context();
```

- the negotiated subprotocol:

```
webSocketExchange.getSubProtocol();
```

- multiple methods for closing the WebSocket:

```

webSocketExchange.close(WebSocketStatus.NORMAL_CLOSURE);
webSocketExchange.close((short)1000, "Goodbye!");

```

A WebSocket exchange finalizer can be specified to free resources once the WebSocket is closed:

```

webSocketExchange.finalizer(Mono.fromRunnable(() -> {
    // Release some resources
    ...
}));

```

The WebSocket protocol is bidirectional and allows sending and receiving data on both ends exposed by `inbound()` and `outbound()` methods in the WebSocket exchange.

## Inbound

In a WebSocket exchange, the **Inbound** exposes the stream of frames sent by the client to the server. It allows to consume WebSocket frames (text or binary) or messages (text or binary).

The following handler simply logs incoming frames:

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.webSocket()
        .orElseThrow(() -> new InternalServerErrorException())
        .handler(webSocketExchange -> {
            Flux.from(webSocketExchange.inbound().frames()).subscribe(frame -> {
                try {
                    LOGGER.info("Received WebSocket frame: kind = " + frame.getKind() + ", final = "
+ frame.isFinal() + ", size = " + frame.getBinaryData().readableBytes());
                }
                finally {
                    frame.release();
                }
            });
        });
};
```

As for request body **ByteBuf** data, WebSocket frames are reference counted and they must be released where they are consumed. In previous example, inbound frames are consumed in the handler which must release them.

The WebSocket protocol supports fragmentation as defined by [RFC 6455 Section 5.4](#), a WebSocket message can be fragmented into multiple frames, the final frame being flagged as final to indicate the end of the message. The **Inbound** can handle fragmented WebSocket messages and allows to consume corresponding fragmented data in multiple ways.

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.webSocket()
        .orElseThrow(() -> new InternalServerErrorException())
        .handler(webSocketExchange -> {
            Flux.from(webSocketExchange.inbound().messages()).subscribe(message -> {
                // The stream of frames composing the message
                Publisher<WebSocketFrame> frames = message.frames();

                // The message data as stream of ByteBuf
                Publisher<ByteBuf> binary = message.binary();

                // The message data as stream of String
                Publisher<String> text = message.text();

                // Aggregate all fragments into a single ByteBuf
                Mono<ByteBuf> reducedBinary = message.reducedBinary();

                // Aggregate all fragments into a single String
                Mono<String> reducedText = message.reducedText();

                ...
            });
        });
};
```

Note that the different publishers in previous example are all variants of the frames publisher, as a result they are exclusive and it is only possible to subscribe once to only one of them.

Unlike WebSocket frames, WebSocket messages are not reference counted, however message fragments, which are basically frames, must be released when consumed as WebSocket frames or `ByteBuffer`.

Messages can be filtered by type (text or binary) by invoking `WebSocketExchange.Inbound#textMessages()` and `WebSocketExchange.Inbound#binaryMessages()`.

## Outbound

In a WebSocket exchange, the `Outbound` exposes the stream of frames sent by the server to the client. It allows to specify the stream of WebSocket frames (text or binary) or messages (text or binary) to send to the client. WebSocket frames and messages are created using provided factories.

The following handler simply sends three text frames to the client. The WebSocket is closed automatically when the outbound publisher terminates.

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.webSocket()
        .orElseThrow(() -> new InternalServerErrorException())
        .handler(webSocketExchange -> {
            webSocketExchange.outbound().frames(factory -> Flux.just("ONE", "TWO",
"THREE")).map(factory::text));
        });
}
```

Likewise we can send messages to the client, in the following example three WebSocket frames are sent to the client per message: the constant `message:`, the actual message content and an empty final frame which marks the end of the message. Frames and messages publisher are exclusive, only one of them can be specified.

```
ExchangeHandler<ExchangeContext, Exchange<ExchangeContext>> handler = exchange -> {
    exchange.webSocket()
        .orElseThrow(() -> new InternalServerErrorException())
        .handler(webSocketExchange -> {
            webSocketExchange.outbound().messages(factory -> Flux.just("ONE", "TWO",
"THREE")).map(content -> factory.text(Flux.just("message: ", content))));
        });
}
```

## A simple chat server

Using the reactive API, a simple chat server can be implemented quite easily. The following exchange handler uses a sink to broadcast the frames received to every connected clients:



```

package io.inverno.example.app_http_websocket;

import io.inverno.core.annotation.Bean;
import io.inverno.core.annotation.Destroy;
import io.inverno.core.annotation.Init;
import io.inverno.mod.base.resource.MediaTypees;
import io.inverno.mod.base.resource.PathResource;
import io.inverno.mod.base.resource.Resource;
import io.inverno.mod.http.base.HttpException;
import io.inverno.mod.http.server.ErrorExchange;
import io.inverno.mod.http.server.Exchange;
import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.http.server.ServerController;
import io.inverno.mod.http.server.ws.WebSocketFrame;
import reactor.core.publisher.Flux;
import reactor.core.publisher.Sinks;

@Bean
public class ChatServerController implements ServerController<ExchangeContext,
Exchange<ExchangeContext>, ErrorExchange<ExchangeContext>> {

    private Sinks.Many<WebSocketFrame> chatSink;

    @Init
    public void init() {
        this.chatSink = Sinks.many().multicast().onBackpressureBuffer(16, false);
    }

    @Destroy
    public void destroy() {
        this.chatSink.tryEmitComplete();
    }

    @Override
    public void handle(Exchange<ExchangeContext> exchange) throws HttpException {
        exchange.webSocket().ifPresentOrElse(
            websocket -> websocket
                .handler(webSocketExchange -> {
                    Flux.from(webSocketExchange.inbound().frames())
                        .subscribe(frame -> {
                            try {
                                this.chatSink.tryEmitNext(frame);
                            }
                            finally {
                                frame.release();
                            }
                        });
                    webSocketExchange.outbound().frames(factory ->
this.chatSink.asFlux().map(WebSocketFrame::retainedDuplicate)); // 5
                })
                .or(() -> exchange.response()
                    .body().string().value("Web socket handshake failed")
                ),

```

```

        () -> exchange.response()
            .body().string().value("WebSocket not supported")
    );
}
}

```

0. Create a multicast chat sink with autocancel set to false to broadcast inbound frames to all connected clients.
1. When receiving a new connection, get the inbound frames stream.
2. Subscribe to the inbound frames stream.
3. For each frame received, broadcast the frame using the chat sink.
4. Release the inbound frame.
5. Set the WebSocket outbound using the chat sink: on each frame, retain and duplicate.

As stated before, WebSocket frames are reference counted and inbound WebSocket frames must be released since the handler is the one consuming them. Furthermore for each connected client, the frame must be duplicated, since it is written multiple times, and retained to increment the reference counter, since it must stay in memory until it has been sent to all connected clients.

This chat server could have been implemented more simply without bothering with reference counting by emitting string data instead of frames in the chat sink. But this would actually be far less optimal as it would involve memory copy. In above solution, the incoming data is never copied into memory, there is only one `ByteBuf` written to all connected client. As always, it is important to find the right balance between performance, simplicity and readability.

## Extending HTTP services

The `http-server` module also defines a socket to plug a custom parameter converter which is a basic `StringConverter` by default. Since we created the `app_http` module by composing `boot` and `http-server` modules, the parameter converter provided by the `boot` module should then override the default. This converter is a `StringCompositeConverter` which can be extended by injecting custom `CompoundDecoder` and/or `CompoundEncoder` instances in the `boot` module as described in the [composite converter documentation](#).

The `HeaderService` provided by the `http-basic` module composed in the `http-server` module can also be extended by injecting custom `HeaderCodec` instances used to encode/decode custom HTTP headers.

In practice, all we have to do to extend these services is to provide `HeaderCodec`, `CompoundDecoder` or `CompoundEncoder` beans in the `app_http` module.

## Wrap-up

If we put all we've just seen together, here is a complete example showing how to create a HTTP/2 server with HTTP compression using a custom server controller:

```

package io.inverno.example.app_http;

import io.inverno.core.annotation.Bean;
import io.inverno.core.v1.Application;
import io.inverno.mod.base.Charsets;
import io.inverno.mod.http.server.ErrorExchange;
import io.inverno.mod.http.server.Exchange;
import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.http.server.ServerController;
import io.netty.buffer.Unpooled;
import java.net.URI;
import java.util.function.Supplier;

public class Main {

    @Bean
    public static interface Controller extends Supplier<ServerController<ExchangeContext,
Exchange<ExchangeContext>, ErrorExchange<ExchangeContext>>> {}

    public static void main(String[] args) {
        // Starts the server
        Application.run(new App_http.Builder()
            // Setups the server
            .setApp_httpConfiguration(
                App_httpConfigurationLoader.load(configuration -> configuration
                    .http_server(server -> server
                        // HTTP compression
                        .decompression_enabled(true)
                        .compression_enabled(true)
                        // TLS
                        .server_port(8443)
                        .tls_enabled(true)
                        .key_store(URI.create("module:/keystore.jks"))
                        .key_store_password("password")
                        // Enable HTTP/2
                        .h2_enabled(true)
                    )
                )
            )
            // Sets the server controller
            .setController(ServerController.from(
                exchange -> {
                    exchange.response()
                        .body().raw().value(Unpooled.unreleasableBuffer(Unpooled.copiedBuffer("Hello
from main!", Charsets.DEFAULT)));
                },
                errorExchange -> {
                    errorExchange.response()
                        .headers(headers -> headers.status(500))

                    .body().raw().value(Unpooled.unreleasableBuffer(Unpooled.copiedBuffer("Error: " +
errorExchange.getError().getMessage(), Charsets.DEFAULT)));
                }
            ))
        );
    }
}

```

```
$ curl -i --insecure https://localhost:8443/
HTTP/2 200
content-length: 16

Hello from main!
```

## Web

The Inverno *web* module provides extended functionalities on top of the *http-server* module for developing high-end Web and RESTfull applications.

It especially provides:

- advanced HTTP request routing and interception
- content negotiation
- automatic message payload conversion
- path parameters
- static handler for serving static resources
- version agnostic [WebJars](#) support
- smooth Web/REST controller development
- [OpenAPI](#) specifications generation using Web/REST controllers JavaDoc comments
- SwaggerUI integration
- an Inverno compiler plugin providing static validation of the routes and generation of Web server controller configurers

The *web* module composes the *http-server* module and therefore starts a HTTP server. Just like the *http-server* module, it requires a net service and a resource service as well as a list of [media type converters](#) for message payload conversion. Basic implementations of these services are provided by the *boot* module which provides `application/json`, `application/x-ndjson` and `text/plain` media type converters. Additional media type converters can also be provided by implementing the `MediaTypeConverter` interface.

In order to use the Inverno *web* module, we should declare the following dependencies in the module descriptor:

```
@io.inverno.core.annotation.Module
module io.inverno.example.app_web {
    requires io.inverno.mod.boot;
    requires io.inverno.mod.web;
}
```

We also need to declare these dependencies in the build descriptor:

Using Maven:

```

<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-boot</artifactId>
    </dependency>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-web</artifactId>
    </dependency>
  </dependencies>
</project>

```

Using Gradle:

```

...
compile 'io.inverno.mod:inverno-boot:1.5.3'
compile 'io.inverno.mod:inverno-web:1.5.3'
...

```

## Web Routing API

The *web* module defines an API for routing HTTP requests to the right handlers.

A **router** is a server exchange handler as defined by the *http-server* module API which can be used to handle exchanges or error exchanges in the server controller of the HTTP server, its role is to route an exchange to an handler based on a set of rules applied to the exchange.

A **route** specifies the rules that an exchange must matched to be routed to a particular handler. A **route interceptor** specifies the rules that a route must match to be intercepted by a particular exchange interceptor.

A **route manager** is used to manage the routes in a router or, more explicitly, to list, create, enable or disable routes in a router. An **interceptor manager** is used to configure the route interceptors in an intercepted router.

The module defines a high level SPI in `io.inverno.mod.spi` package that can be used as a base to implement custom routing implementations in addition to the provided Web routing implementations. Nevertheless, it is more of a guideline, one can choose a totally different approach to implement routing, in the end the HTTP server expects a `ServerController` with an `ExchangeHandler<ExchangeContext>`, `Exchange<ExchangeContext>` to handle exchange and an `ExchangeHandler<ExchangeContext>`, `ErrorExchange<ExchangeContext>` to handle errors, what is done inside these handlers is completely opaque, the SPI only shows one way to do it.

A `WebRouter` is used to route a `WebExchange` to the right `ExchangeHandler`, it extends `ExchangeHandler` and it is typically used as the exchange handler in a the server controller of the HTTP server.

An `ErrorRouter` is used to route an `ErrorWebExchange` to the right `ExchangeHandler` when an exception is thrown during the normal processing of an exchange, it extends `ExchangeHandler` and it is typically used as the error exchange handler in a the server controller of the HTTP server.

## Web exchange

The *web* module API extends the [server exchange API](#) defined in the *http-server* module. It defines the server `WebExchange` composed of a `WebRequest`/`WebResponse` pair in a HTTP communication between a client and a server. These interfaces respectively extends the `Exchange`, `Request` and `Response` interfaces defined in the *http-server* module. A web exchange handler (i.e. `ExchangeHandler<ExchangeContext, WebExchange<ExchangeContext>>`) is typically attached to one or more Web routes defined in a `WebRouter`.

The Web exchange provides additional fonctionnalités on top of the exchange including support for path parameters, request/response body decoder/encoder based on the content type, WebSocket inbound/outbound data decoder/encoder based on the subprotocol.

### Path parameters

Path parameters are exposed in the `WebRequest`, they are extracted from the requested path by the [Web router](#) when the handler is attached to a route matching a parameterized path as defined in a [URI builder](#).

For instance, if the handler is attached to a route matching `/book/{id}`, the `id` path parameter can be retrieved as follows:

```
ExchangeHandler<ExchangeContext, WebExchange<ExchangeContext>> handler = exchange -> {
    exchange.request().pathParameters().get("id")
        .ifPresentOrElse(
            id -> {
                ...
            },
            () -> exchange.response().headers(headers ->
headers.status(Status.NOT_FOUND)).body().empty()
        );
};
```

### Request body decoder

The request body can be decoded based on the content type defined in the request headers.

```
ExchangeHandler<ExchangeContext, WebExchange<ExchangeContext>> handler = exchange -> {
    Mono<Result> storeBook = exchange.request().body().get()
        .decoder(Book.class)
        .one()
        .map(book -> storeBook(book));
    exchange.response().body()
        .string().stream(storeBook.map(result -> result.getMessage()));
};
```

When invoking the `decoder()` method, a [media type converter](#) corresponding to the request content type is selected to decode the payload. The `content-type` header MUST be specified in the request, otherwise (400) bad request error is returned indicating an empty media type. If there is no converter corresponding to the media type, a (415) unsupported media type error is returned indicating that no decoder was found matching the content type.

A decoder is obtained by specifying the type of the object to decode in the `decoder()` method, the type can be a `Class<T>` or a `java.lang.reflect.Type` which allows to decode parameterized types at runtime bypassing type erasure. Parameterized Types can be built at runtime using the [reflection API](#).

As you can see in the above example the decoder is fully reactive, a request payload can be decoded in a single object by invoking method `one()` on the decoder which returns a `Mono<T>` publisher or in a stream of objects by invoking method `many()` on the decoder which returns a `Flux<T>` publisher.

Decoding multiple payload objects is indicated when a client streams content to the server. For instance, it can send a request with `application/x-ndjson` content type in order to send multiple messages in a single request. Since everything is reactive the server doesn't have to wait for the full request and it can process a message as soon as it is received. What is remarkable is that the code is widely unchanged.

```
ExchangeHandler<ExchangeContext, WebExchange<ExchangeContext>> handler = exchange -> {
    Flux<Result> storeBook = exchange.request().body().get()
        .decoder(Book.class)
        .many()
        .map(book -> storeBook(book));
    exchange.response().body()
        .string().stream(storeBook.map(result -> result.getMessage()));
};
```

Conversion of a multipart form data request body is also supported, the payload of each part being decoded independently based on the content type of the part. For instance we can upload multiple books in multiple files in a `multipart/form-data` request and decode them on the fly as follows:

```
ExchangeHandler<ExchangeContext, WebExchange<ExchangeContext>> handler = exchange -> {
    exchange.response()
        .body().string().stream(Flux.from(exchange.request().body().get().multipart().stream()) // 1
        .flatMap(part -> part.decoder(Book.class).one()) // 2
        .map(book -> storeBook(book)) // 3
        .map(result -> result.getMessage()) // 4
    );
};
```

In the previous example:

1. A stream of files is received in a `multipart/form-data` request (note that we assume all parts are file parts).
2. Each part is decoded to a `Book` object, the media type must be specified in the `content-type` header field of the part.
3. The book object so obtained is processed.



4. The result for each upload is returned to the client.

All this process is done in a reactive way, the first chunk of response can be sent before all parts have been processed.

## Response body encoder

As for the request body, the response body can be encoded based on the content type defined in the response headers. Considering previous example we can do the following:

```
ExchangeHandler<ExchangeContext, WebExchange<ExchangeContext>> handler = exchange -> {
    Mono<Result> storeBook = exchange.request().body().get()
        .decoder(Book.class)
        .one()
        .map(book -> storeBook(book));
    exchange.response()
        .headers(headers -> headers.contentType(MediaType.APPLICATION_JSON))
        .body()
            .encoder(Result.class)
            .one(storeBook);
};
```

When invoking the `encoder()` method, a [media type converter](#) corresponding to the response content type is selected to encode the payload. The `content-type` header MUST be specified in the response, otherwise a (500) internal server error is returned indicating an empty media type. If there is no converter corresponding to the media type, a (500) internal server error is returned indicating that no encoder was found matching the content type.

A single object is encoded by invoking method `one()` on the encoder or multiple objects can be encoded by invoking method `many()` on the encoder. Returning multiple objects in a stream is particularly suitable to implement progressive display in a Web application, for example to display search results as soon as some are available.

```
ExchangeHandler<ExchangeContext, WebExchange<ExchangeContext>> handler = exchange -> {
    Flux<SearchResult> searchResults = ...;
    exchange.response()
        .headers(headers -> headers.contentType(MediaType.APPLICATION_X_NDJSON))
        .body()
            .encoder(SearchResult.class)
            .many(searchResults);
};
```

## WebSocket message decoder/encoder

A Web exchange can be upgraded to a Web WebSocket exchange. The `Web2SocketExchange` thus created extends `WebSocketExchange` and allows to respectively decode/encode WebSocket inbound and outbound messages based on the subprotocol negotiated during the opening handshake.

As for request and response payloads, a [media type converter](#) corresponding to the subprotocol is selected to decode/encode inbound and outbound messages. If there is no converter corresponding to the subprotocol, a `WebSocketException` is thrown resulting in a (500) internal server error returned to the client indicating that no converter was found matching the subprotocol.

The subprotocol must then correspond to a valid media type. Unlike request and response payloads which expect strict media type representation, compact `application/` media type representation can be specified as subprotocol. In practice, it is possible to open a WebSocket connection with subprotocol `json` to select the `application/json` media type converter.

As defined by [RFC 6455](#), a WebSocket subprotocol is not a media type and is registered separately, however using media type is very handy in this case as it allows to reuse the data conversion facility. Supporting compact `application/` media type representation allows to mitigate this specification violation as it is then possible to specify a valid subprotocol while still being able to select a media type converter. Let's consider the registered subprotocol `v2.bookings.example.net` (taken from [RFC 6455 Section 1.9](#)), we can then create a media type converter for `application/v2.bookings.example.net` that will be selected when receiving connection for that particular subprotocol.

The following example is a variant of the [simple chat server](#) which shows how JSON messages can be automatically decoded and encoded:

```
ExchangeHandler<ExchangeContext, WebSocketExchange<ExchangeContext>> handler = exchange -> {
    exchange.webSocket("json")
        .orElseThrow(() -> new InternalServerErrorException("WebSocket not supported"))
        .handler(webSocketExchange -> {

Flux.from(webSocketExchange.inbound().decodeTextMessages(Message.class)).subscribe(message ->
this.chatSink.tryEmitNext(message));
        webSocketExchange.outbound().encodeTextMessages(this.chatSink.asFlux());
    })
    .or(() -> exchange.response()
        .body().string().value("Web socket handshake failed")
    );
};
```

## Web route

A Web route specifies the routing rules and the exchange handler that shall be invoked to handle a matching exchange. It can combine the following routing rules which are matched in that order: the path, method and content type of the request, the media ranges and language ranges accepted by the client. For instance, a Web exchange is matched against the path routing rule first, then the method routing rule... Multiples routes can then match a given exchange but only one will be retained to actually process the exchange which is the one matching the highest routing rules.

If a route doesn't define a particular routing rule, the routing rule is simply ignored and matches all exchanges. For instance, if a route doesn't define any method routing rule, exchanges are matched regardless of the method.

The `WebRoutable` interface defines a fluent API for the definition of Web routes. The following is an example of the definition of a Web route which matches all exchanges, this is the simplest route that can be defined:

```
routable
    .route()                                // 1
        .handler(exchange -> {              // 2
            exchange.response()
                .headers(headers ->
                    headers.contentType(MediaType.TEXT_PLAIN)
                )
                .body()
                .encoder()
                .value("Hello, world!");
        });
```

1. A new `WebRouteManager` instance is obtained to configure a `WebRoute`
2. We only define the handler of the route as a result any exchange might be routed to that particular route unless a more specific route matching the exchange exists.

An exchange handler can be attached to multiple routes at once by providing multiple routing rules to the route manager, the following example actually results in 8 individual routes being defined:

```
routable
    .route()
        .path("/doc")
        .path("/document")
        .method(Method.GET)
        .method(Method.POST)
        .consumes(MediaType.APPLICATION_JSON)
        .consumes(MediaType.APPLICATION_XML)
        .handler(exchange -> {
            ...
        });
```

The Web routable also allows to select all routes that matches the rules defined in a Web route manager using the `findRoutes()` method. The following example select all routes matching `GET` method:

```
Set<WebRoute<ExchangeContext>> routes = router
    .route()
        .method(Method.GET)
        .findRoutes();
```

It is also possible to enable, disable or remove a set of routes in a similar way:

```
// Disables all GET routes
routable
    .route()
        .method(Method.GET)
        .disable();

// Enables all GET routes
routable
    .route()
        .method(Method.GET)
        .enable();

// remove all GET routes
routable
    .route()
        .method(Method.GET)
        .remove();
```

Individual routes can be enabled, disabled or removed as follows:

```
// Disables all GET routes producing 'application/json'
routable
    .route()
        .method(Method.GET)
        .findRoutes()
        .stream()
        .filter(route -> route.getProduce().equals(MediaType.APPLICATION_JSON))
        .forEach(WebRoute::disable);

// Enables all GET routes producing 'application/json'
routable
    .route()
        .method(Method.GET)
        .findRoutes()
        .stream()
        .filter(route -> route.getProduce().equals(MediaType.APPLICATION_JSON))
        .forEach(WebRoute::enable);

// Removes all GET routes producing 'application/json'
routable
    .route()
        .method(Method.GET)
        .findRoutes()
        .stream()
        .filter(route -> route.getProduce().equals(MediaType.APPLICATION_JSON))
        .forEach(WebRoute::remove);
```

Routes can also be configured as blocks in reusable `WebRoutesConfigurer` by invoking `configureRoutes()` methods:

```

WebRoutesConfigurer<ExchangeContext> public_routes_configurer = routable -> {
    routable
        .route()
        ...
};

WebRoutesConfigurer<ExchangeContext> private_routes_configurer = routable -> {
    routable
        .route()
        ...
};

routable
    .configureRoutes(public_routes_configurer)
    .configureRoutes(private_routes_configurer)
    .route()
    ...

```

## Path routing rule

The path routing rule matches exchanges whose request targets a specific path or a path that matches against a particular pattern. The path or path pattern of a routing rule must be absolute (ie. start with `/`).

We can for instance define a route to handle all requests to `/bar/foo` as follows:

```

routable
    .route()
        .path("/foo/bar")
        .handler(exchange -> {
            ...
        });

```

The route in the preceding example specifies an exact match for the exchange request path, it is also possible to make the route match the path with or without a trailing slash as follows:

```

routable
    .route()
        .path("/foo/bar", true)
        .handler(exchange -> {
            ...
        });

```

A path pattern following the parameterized or path pattern [URIs notation](#) can also be specified to create a routing rule matching multiple paths. This also allows to specify [path parameters](#) that can be retrieved from the `WebExchange`.

In the following example, the route will match all exchanges whose request path is `/book/1`, `/book/abc...` and store the extracted parameter value in path parameter `id`:

```

routable
    .route()
        .path("/book/{id}")
        .handler(exchange -> {
            exchange.request().pathParameters().get("id")...
        });

```

A parameter is matched against a regular expression set to `[^/]*` by default which is why previous route does not match `/book/a/b`. Parameterized URIs allow to specify the pattern matched by a particular path parameter using `{<name>[:<pattern>]}` notation, we can then put some constraints on path parameters value. For instance, we can make sure the `id` parameter is a number between 1 and 999:

```
routable
  .route()
    .path("/book/{id:[1-9][0-9]{0,2}}")
    .handler(exchange -> {
      ...
    });
```

If we just want to match a particular path without extracting path parameters, we can omit the parameter name and simply write:

```
routable
  .route()
    .path("/book/{}")
    .handler(exchange -> {
      ...
    });
```

## Method routing rule

The method routing rule matches exchanges that have been sent with a particular HTTP method.

In order to handle all `GET` exchanges, we can do:

```
routable
  .route()
    .method(Method.GET)
    .handler(exchange -> {
      ...
    });
```

## Consume routing rule

The consume routing rule matches exchanges whose request body content type matches a particular media range as defined by [RFC 7231 Section 5.3.2](#).

For instance, in order to match all exchanges with an `application/json` request payload, we can do:

```
routable
  .route()
    .method(Method.POST)
    .consumes(MediaType.APPLICATION_JSON)
    .handler(exchange -> {
      ...
    });
```

We can also specify a media range to match, for example, all exchanges with a `*/*json` request payload:

```

routable
  .route()
    .method(Method.POST)
    .consumes("*/json")
    .handler(exchange -> {
      ...
    });

```

The two previous routes are different and as a result they can be both defined, a content negotiation algorithm is used to determine which route should process a particular exchange as defined in [RFC 7231 Section 5.3](#).

Routes are sorted by consumed media ranges as follows:

- quality value is compared first as defined by [RFC7231 Section 5.3.1](#), the default quality value is 1.
- type and subtype wildcards are considered after:  $a/b > a/* > */b > */*$
- parameters are considered last, the most precise media range which is the one with the most parameters with matching values gets the highest priority (eg.

$application/json;p1=a;p2=2 > application/json;p1=b > application/json;p1$ )

The first route whose media range matches the request's **content-type** header field is selected.

If we consider previous routes, an exchange with an **application/json** request payload will be matched by the first route while an exchange with a **text/json** request will be matched by the second route.

A media range can also be parameterized which allows for interesting setup such as:

```

routable
  .route()
    .path("/document")
    .method(Method.POST)
    .consumes("application/json;version=1")
    .handler(exchange -> {
      ...
    })
  .route()
    .path("/document")
    .method(Method.POST)
    .consumes("application/json;version=2")
    .handler(exchange -> {
      ...
    })
  .route()
    .path("/document")
    .method(Method.POST)
    .consumes("application/json")
    .handler(exchange -> {
      ...
    });

```

In the above example, an exchange with a **application/json;version=1** request payload is matched by the first route, **application/json;version=2** request payload is matched by the second route and any other **application/json** request payload is matched by the third route.

If there is no route matching the content type of a request of an exchange matched by previous routing rules, a (415) unsupported media type error is returned.

As described before, if no route is defined with a consume routing rule, exchanges are matched regardless of the request content type, content negotiation is then eventually delegated to the handler which must be able to process the payload whatever the content type.

## Produce routing rule

The produce routing rule matches exchanges based on the acceptable media ranges supplied by the client in the `accept` header field of the request as defined by [RFC 7231 Section 5.3.2](#).

A HTTP client (eg. Web browser) typically sends an `accept` header to indicate the server which response media types are acceptable in the response. The best matching route is determined based on the media types produced by the routes matching previous routing rules.

We can for instance define the following routes:

```
routable
  .route()
    .path("/doc")
    .produces(MediaType.APPLICATION_JSON)
    .handler(exchange -> {
      ...
    })
  .route()
    .path("/doc")
    .produces(MediaType.TEXT_XML)
    .handler(exchange -> {
      ...
    });
```

Now let's consider the following `accept` request header field:

```
accept: application/json, application/xml;q=0.9, */xml;q=0.8
```

This field basically tells the server that the client wants to receive first an `application/json` response payload, if not available an `application/xml` response payload and if not available any `*/xml` response payload.

The content negotiation algorithm is similar as the one described in the [consume routing rule](#), it is simply reversed in the sense that it is the acceptable media ranges defined in the `accept` header field that are sorted and the route producing the media type matching the media range with the highest priority is selected.

Considering previous routes, a request with previous `accept` header field is then matched by the first route.

A request with the following `accept` header field is matched by the second route:



```
accept: application/xml;q=0.9, */xml;q=0.8
```

The exchange is also matched by the second route with the following `accept` header field:

```
accept: application/json;q=0.5, text/xml;q=1.0
```

If there is no route producing a media type that matches any of the acceptable media ranges, then a (406) not acceptable error is returned.

As described before, if no route is defined with a produce routing rule, exchanges are matched regardless of the acceptable media ranges, content negotiation is then eventually delegated to the handler which becomes responsible to return an acceptable response to the client.

## Language routing rule

The language routing rule matches exchanges based on the acceptable languages supplied by client in the `accept-language` header field of the request as defined by [RFC 7231 Section 5.3.5](#).

A HTTP client (eg. Web browser) typically sends a `accept-language` header to indicate the server which languages are acceptable for the response. The best matching route is determined based on the language tags produced by the routes matching previous routing rules.

We can defines the following routes to return a particular resource in English or in French:

```
routable
  .route()
    .path("/doc")
    .language("en-US")
    .handler(exchange -> {
      ...
    });
```

```
routable
  .route()
    .path("/doc")
    .language("fr-FR")
    .handler(exchange -> {
      ...
    });
```

The content negotiation is similar to the one described in the [produce routing rule](#) but using language ranges and language types instead of media ranges and media types. Acceptable language ranges are sorted as follows:

- quality value is compared first as defined by [RFC 7231 Section 5.3.1](#), the default quality value is 1.
- primary and secondary language tags and wildcards are considered after: `fr-FR > fr > *`

The route whose produced language tag matches the language range with the highest priority is selected.

As for the produce routing rule, if there is no route defined with a language tag that matches any of the acceptable language ranges, then a (406) not acceptable error is returned. However, unlike the produce routing rule, a default route can be defined to handle such unmatched exchanges.

For instance, we can add the following default route to the router:

```
routable
    .route()
        .path("/doc")
        .handler(exchange -> {
            ...
        });
```

A request with the following `accept-language` header field is then matched by the default route:

```
accept-language: it-IT
```

## WebSocket route

The `WebRoutable` interface also exposes `websocketRoute()` which returns a `WebSocketRouteManager` which allows defining WebSocket routes. A WebSocket route specifies the routing rules and the WebSocket exchange handler that shall be invoked after upgrading a matching exchange to a WebSocket exchange. It can combine the following routing rules which are matched in that order: the path of the request, the language ranges accepted by the client and the supported subprotocol. Unlike a regular Web route, a WebSocket exchange does not support method, consume and produce routing rules, this difference can be explained by the fact that a WebSocket upgrade request is always a `GET` request and that consumed and produced media types have just no meaning in the context of a WebSocket.

When an exchange matches a WebSocket route, the Web router automatically handles the upgrade and setups the WebSocket exchange handler specified in the route. If the WebSocket upgrade is not supported, a `WebSocketException` is thrown resulting in a (500) internal server error returned to the client.

A WebSocket endpoint can then be easily defined as follows:

```
routable
    .websocketRoute()
        .path("/ws")
        .subprotocol("json")
        .handler(webSocketExchange -> {
            webSocketExchange.outbound().messages(factory ->
webSocketExchange.inbound().messages());
        });
```

`WebSocketRoute` extends `WebRoute`, as a result, just like Web routes, WebSocket routes matching particular rules can be selected, enabled, disabled or removed:

```
// Disables all WebSocket routes supporting subprotocol 'json'
routable
  .webSocketRoute()
    .subprotocol("json")
    .findRoutes()
    .stream()
    .forEach(WebSocketRoute::disable);

// Enables all routes (including WebSocket routes) with path matching '/ws'
routable
  .route()
    .path("/ws")
    .enable();
```

## Subprotocol routing rule

The produce routing rule matches exchanges based on the supported subprotocols supplied by the client in the `sec-websocket-version` header field of the request as defined by [RFC 6455](https://tools.ietf.org/html/rfc6455).

A HTTP client (eg. Web browser) wishing to open a WebSocket connection typically sends a `sec-websocket-version` header to indicate the server which subprotocols it supports by order of preference. The best matching route is determined based on the subprotocol supported by the routes matching previous routing rules.

We can then define the following WebSocket routes that handle different subprotocols:

```
routable
  .webSocketRoute()
    .path("/ws")
    .subprotocol("json")
    .handler(webSocketExchange -> {
      ...
    })
  .webSocketRoute()
    .path("/ws")
    .subprotocol("xml")
    .handler(webSocketExchange -> {
      ...
    })
  .webSocketRoute()
    .path("/ws")
    .handler(webSocketExchange -> {
      ...
    });
```

Let's consider a request with the following `sec-websocket-version` header field:

```
sec-websocket-version: xml, json
```

This field basically tells the server that the client wants to open a WebSocket connection using the `xml` subprotocol and if not supported the `json` subprotocol. As a result the request is matched by the second route in above example.

If there is no route supporting any of the subprotocols provided by the client, an `UnsupportedProtocolException` is thrown resulting in a (500) internal server error returned to the client. The last route in above example is therefore not a default route, it is only matched when the client open a WebSocket connection with no subprotocol.

## Web route interceptor

A Web route interceptor specifies the rules and the exchange interceptor that shall be applied to a matching route. It can combine the same rules as for the definition of a route: the path and method of the route, media range matching the content consumed by the route, media range and language range matching the media type and language produced by the route.

Multiple web exchange interceptors (i.e. `ExchangeInterceptor<ExchangeContext, WebExchange<ExchangeContext>>`) can be applied to one or more web routes.

The `WebInterceptable` interface defines a fluent API similar to the `WebRoutable` for the definition of Web interceptors. The following is an example of the definition of a Web route interceptor that is applied to routes matching `GET` methods and consuming `application/json` payloads:

```
interceptable.  
    .intercept()  
        .method(Method.GET)  
        .consumes(MediaType.APPLICATION_JSON)  
        .interceptor(exchange -> {  
            LOGGER.info("Intercepted!");  
            return Mono.just(exchange);  
        });
```

As for an exchange handler, an exchange interceptor can be applied to multiple routes at once by providing multiple rules to the route interceptor manager, the following example is used to apply a route interceptor to `/doc` and `/document` routes consuming `application/json` or `application/xml` payloads:

```
interceptable  
    .intercept()  
        .path("/doc")  
        .path("/document")  
        .consumes(MediaType.APPLICATION_JSON)  
        .consumes(MediaType.APPLICATION_XML)  
        .interceptor(exchange -> {  
            ...  
        });
```

Multiple interceptors can be applied to a route at once using the `interceptors()` methods. The following example is equivalent as applying `interceptor1` then `interceptor2` on all routes matching `/some_path` (i.e. `interceptor2` is then invoked before `interceptor1`):

```
ExchangeInterceptor<ExchangeContext, WebExchange<ExchangeContext>> interceptor1 = ...;  
ExchangeInterceptor<ExchangeContext, WebExchange<ExchangeContext>> interceptor2 = ...;
```

```
interceptable  
    .intercept()  
        .path("/some_path")  
        .interceptors(List.of(interceptor1, interceptor2));
```

The list of exchange interceptors applied to a route can be obtained from a `WebRoute` instance:

```
// Use a WebRoutable to find a WebRoute
WebRoute<ExchangeContext> route = ...
```

```
List<? extends ExchangeInterceptor<ExchangeContext, WebExchange<ExchangeContext>>> routeInterceptors
= route.getInterceptors();
```

In a similar way, it is possible to explicitly set exchange interceptors on a specific `WebRoute` instance:

```
Set<WebRoute<ExchangeContext>> routes = router.getRoutes();
```

```
ExchangeInterceptor<ExchangeContext, WebExchange<ExchangeContext>> serverHeaderInterceptor =
exchange -> {
    exchange.response()
        .headers(headers -> headers.set(Headers.NAME_SERVER, "Inverno Web Server"));

    return Mono.just(exchange);
};
```

```
ExchangeInterceptor<ExchangeContext, WebExchange<ExchangeContext>> securityInterceptor = exchange ->
{...};
```

```
routes.stream().forEach(route -> route.setInterceptors(List.of(serverHeaderInterceptor,
securityInterceptor)));
```

Route interceptors can also be configured as blocks in reusable `WebInterceptorsConfigurer` by invoking `configureInterceptors()` methods:

```
WebInterceptorsConfigurer<ExchangeContext> public_interceptors_configurer = interceptable -> {
    interceptable
        .intercept()
        ...
};
```

```
WebInterceptorsConfigurer<ExchangeContext> private_interceptors_configurer = interceptable -> {
    interceptable
        .intercept()
        ...
};
```

```
interceptable
    .configureInterceptors(public_interceptors_configurer)
    .configureInterceptors(private_interceptors_configurer)
    .intercept()
    ...
```

The definition of an interceptor is very similar to the definition of a route, however there are some peculiarities. For instance, a route can only produce one particular type of content in one particular language that are matched by a route interceptor with matching media and language ranges.

For performance reasons, route interceptor's rules should not be evaluated each time an exchange is processed but once when a route is defined. Unfortunately, this is not always possible and sometimes some rules have to be evaluated when processing the exchange. This happens when the difference between the set of exchanges matched by a route and the set of exchanges matched by a route interceptor is not empty which basically means that the route matches more exchanges than the route interceptor.

In these situations, the actual exchange interceptor is wrapped in order to evaluate the problematic rule on each exchange. A typical example is when a route defines a path pattern (eg. `/path/*.jsp`) that matches the specific path of a route interceptor (eg. `/path/private.jsp`), the exchange interceptor must only be invoked on an exchange that matches the route interceptor's path. This can also happen with method and consumes rules.

Path patterns are actually very tricky to match *offline*, the `WebInterceptedRouter` implementation uses the `URIPattern#includes()` to determine whether a given URIs set is included into another, when this couldn't be determine with certainty, the exchange interceptor is wrapped. Please refer to the [URIs](#) documentation for more information.

Particular care must be taken when listing the exchange interceptor attached to a route as these are the actual interceptors and not the wrappers. If you set interceptors explicitly on a `WebRoute` instance, they will be invoked whenever the route is invoked.

When a route interceptor is defined with specific produce and language rules, it can only be applied on routes that actually specify matching produce and language rules. Since there is no way to determine which content type and language will be produced by an exchange handler, it is not possible to determine whether an exchange interceptor should be invoked prior to the exchange handler unless specified explicitly on the route. In such case, a warning is logged to indicate that the interceptor is ignored for the route due to missing produce or language rules on the route.

## Web router

The `WebRouter` extends both `WebRoutable` and `WebInterceptable` interfaces. As such routes and route interceptors are defined in the `WebRouter` bean exposed in the `web` module and used in the web server controller to handle web exchange. This internal web server controller is wired to the `http-server` module to override the default HTTP server controller.

In addition to `configureRoutes()` and `configureInterceptors()` methods defined by `WebRoutable` and `WebInterceptable`, the `WebRouter` interface provides `configure()` methods that accepts `WebRouterConfigurer` to fluently apply blocks of configuration.

```

WebRouter<ExchangeContext> router = ...

WebRouterConfigurer<ExchangeContext> configurer = ...
List<WebRouterConfigurer<ExchangeContext>> configurers = ...

router
    .configure(configurers)
    .configure(configurer)
    .route()
        .handler(exchange -> ...)

```

Please refer to the [Web Server documentation](#) to see in details how to properly configure Web server routes and interceptors.

Route interceptors are only applied to routes defined on a `WebInterceptedRouter` which is obtained by defining one or more route interceptor on the web router. The following example shows how it works:

```

router
    .route()
        .path("/public")
        .handler(exchange -> {
            ...
        })
    .intercept()
        .interceptor(exchange -> {
            ...
        })
    .route()
        .path("/private")
        .handler(exchange -> {
            ...
        })
    .getRouter()
    .route()
        .path("/static/**")
        .handler(new StaticHandler<>(resourceService.getResource(URI.create("file:/path/to/web-root/"))));

```

In the preceding example, only `/private` route is intercepted, both `/public` and `/static/**` routes are not intercepted since they are defined on the original Web router which is not intercepted. Note the call to `getRouter()` method which returns the original Web router instance and basically *rollbacks* the interceptors configuration.

A Web intercepted router can also be used to apply interceptors to all routes previously defined in a Web router.

```

router
    .intercept()
        .method(Method.GET)
        .interceptor(exchange -> {...})
    .applyInterceptors()

```

In the previous example, all **GET** routes previously defined in the Web router will be intercepted.

The Web router bean specifies default Web routes and error Web routes created when the router is initialized and therefore not intercepted. You must keep in mind that they exist and if you wish to intercept them, you'll have to explicitly invoke `applyInterceptors()`.

## Error web exchange

The *web* module API extends the [server exchange API](#) defined in the *http-server* module. It defines the server **WebExchange** composed of a **WebRequest/WebResponse** pair in a HTTP communication between a client and a server. These interfaces respectively extends the **Exchange**, **Request** and **Response** interfaces defined in the *http-server* module. A web exchange handler (i.e. `ExchangeHandler<ExchangeContext, WebExchange<ExchangeContext>>`) is typically attached to one or more Web routes defined in a **WebRouter**.

The Error Web exchange provides additional functionalities on top of the exchange such as path parameters and response body encoding based on the content type.

As the **WebExchange**, the **ErrorWebExchange** exposes a **WebResponse** which supports automatic response payload encoding based on the content type specified in the response headers. The usage is exactly the same as for the Web server exchange [response body encoder](#).

The following error Web route matches **IllegalArgumentException** errors for client accepting **application/json** media type in the response:

```
ExchangeHandler<ExchangeContext, ErrorWebExchange<ExchangeContext>> errorHandler = errorExchange ->
{
    errorExchange.response()
        .headers(headers -> headers.status(Status.INTERNAL_SERVER_ERROR))
        .body()
        .encoder(Message.class)
        .value(new Message(errorExchange.getError().getMessage()));
};
```

## Error Web route

An Error Web route specifies the routing rules and the error exchange handler that shall be invoked to handle a matching error exchange. Similar to a [Web route](#), it can combine the following routing rules which are matched in that order: the type of error, the path of the request, the media ranges and language ranges accepted by the client.

The **ErrorWebRoutable** interface defines a fluent API for the definition of Error Web routes. The following is an example of the definition of an Error Web route which matches **IllegalArgumentException** errors for client accepting **application/json** media type:



```

errorRoutable
    .route()
    .error(IllegalArgumentException.class)
    .produces(MediaType.APPLICATION_JSON)
    .handler(errorExchange ->
        errorExchange.response()
            .body()
            .encoder(Message.class)
            .value(new Message("IllegalArgumentException")))
    );

```

As with a Web routable, the Error Web routable allows to select routes matching specific rules defined in an `ErrorWebRouteManager` and enable, disable or remove specific routes.

The following example disable all routes matching `SomeCustomException` error type:

```

errorRoutable
    .route()
    .error(SomeCustomException.class)
    .disable();

```

## Error type routing rule

The error type routing rule matches error exchanges whose error is of a particular type.

For instance, in order to handle all error exchanges whose error is an instance of `SomeCustomException`, we can do:

```

errorRoutable
    .route()
    .error(SomeCustomException.class)
    .handler(exchange -> {
        ...
    });

```

## Produce routing rule

The produce routing rule, when applied to an error route behaves exactly the same as for a [Web route](#). It allows to define error handlers that produce responses of different types based on the set of media range accepted by the client.

This is particularly useful to returned specific error responses to a particular client in a particular context. For instance, a backend application might want to receive errors in a parseable format like `application/json` whereas a Web browser might want to receive errors in a human readable format like `text/html`.

## Language routing rule

The language routing rule, when applied to an error route behaves exactly the same as for a [Web route](#). It allows to define error handlers that produce responses with different languages based on the set of language range accepted by the client fallbacking to the default route when content negotiation did not give any match.

## Error Web route interceptor

Error Web routes can be intercepted in a similar way as for [Web route](#) by combining the same rules as for the definition of an Error Web route.

Multiple Error Web exchange interceptors (i.e. `ExchangeInterceptor<ExchangeContext, ErrorWebExchange<ExchangeContext>>`) can be applied to one or more Error Web routes.

The `ErrorWebInterceptable` interface defines a fluent API similar to the `ErrorWebRouteable` for the definition of Error Web interceptors. The following is an example of the definition of an Error Web route interceptor for intercepting Error Web exchange with `SomeCustomException` errors and `/some_path` path:

```
java errorInterceptable .intercept() .path("/some_path") .error(SomeCustomException.class)
.interceptor(errorExchange -> { ... });`
```

As for `WebRoute`, the `ErrorWebRoute` allows to list the Error interceptors applied to an Error route and explicitly set interceptors:

```
// Use an ErrorWebRouteable to find an ErrorWebRoute
ErrorWebRoute<ExchangeContext> errorRoute = ...

List<ExchangeInterceptor<ExchangeContext, ErrorWebExchange<ExchangeContext>>> errorRouteInterceptors
= new ArrayList<>(errorRoute.getInterceptors());
errorRouteInterceptors.add(errorExchange -> {
    ...
});

errorRoute.setInterceptors(errorRouteInterceptors);
```

The `ErrorWebInterceptable` offers the same features as the `WebInterceptable` and allows configuring error interceptors as blocks in reusable `ErrorWebInterceptorsConfigurer` by invoking `configureInterceptors()` methods:

```
ErrorWebInterceptorsConfigurer<ExchangeContext> public_error_interceptors_configurer =
errInterceptable -> {
    errInterceptable
        .intercept()
        ...
};

ErrorWebInterceptorsConfigurer<ExchangeContext> private_error_interceptors_configurer =
errInterceptable -> {
    errInterceptable
        .intercept()
        ...
};

errorInterceptable
    .configureInterceptors(public_error_interceptors_configurer)
    .configureInterceptors(private_error_interceptors_configurer)
    .intercept()
    ...
```

## Error Web router

The `ErrorWebRouter` extends both `ErrorWebRoutable` and `ErrorWebInterceptable` interfaces. As such Error routes and Error route interceptors are defined in the `ErrorWebRouter` bean exposed in the `web` module and used in the web server controller to handle Error Web exchange. This internal web server controller is wired to the `http-server` module to override the default HTTP server controller.

Just like the `WebRouter` interface, the `ErrorWebRouter` exposes the `configure()` method which accepts `ErrorWebRouterConfigurer` to fluently apply blocks of configuration. The same configuration rules as for the [Web router](#) applies:

```
ErrorWebRouter<ExchangeContext> errorRouter = ...

ErrorWebRouterConfigurer<ExchangeContext> configurer = ...
List<ErrorWebRouterConfigurer<ExchangeContext>> configurers = ...

router
    .configure(configurers)
    .configure(configurer)
    .intercept()
        .interceptor(errorExchange -> {
            ...
        })
    .applyInterceptors() // Apply interceptor to previously defined Error routes
    .route()
        .path("/intercepted")
        .handler(exchange -> {
            ...
        })
    .getRouter()
    .route()
        .path("/not_intercepted")
        .handler(exchange -> {
            ...
        });
```

Please refer to the [Web Server documentation](#) to see in details how to properly configure Web server error routes and interceptors.

## Web Server

The `web` module composes the `http-server` module and as a result it requires a `NetService` and a `ResourceService`. A set of [media type converters](#) is also required for message payload conversion. All these services are provided by the `boot` module, so one way to create an application with a Web server is to create an Inverno module composing `boot` and `web` modules.

```
@io.inverno.core.annotation.Module
module io.inverno.example.app_web {
    requires io.inverno.mod.boot;
    requires io.inverno.mod.web;
}
```

The resulting *app\_web* module, thus created, can then be started as an application as follows:

```
package io.inverno.example.app_web;

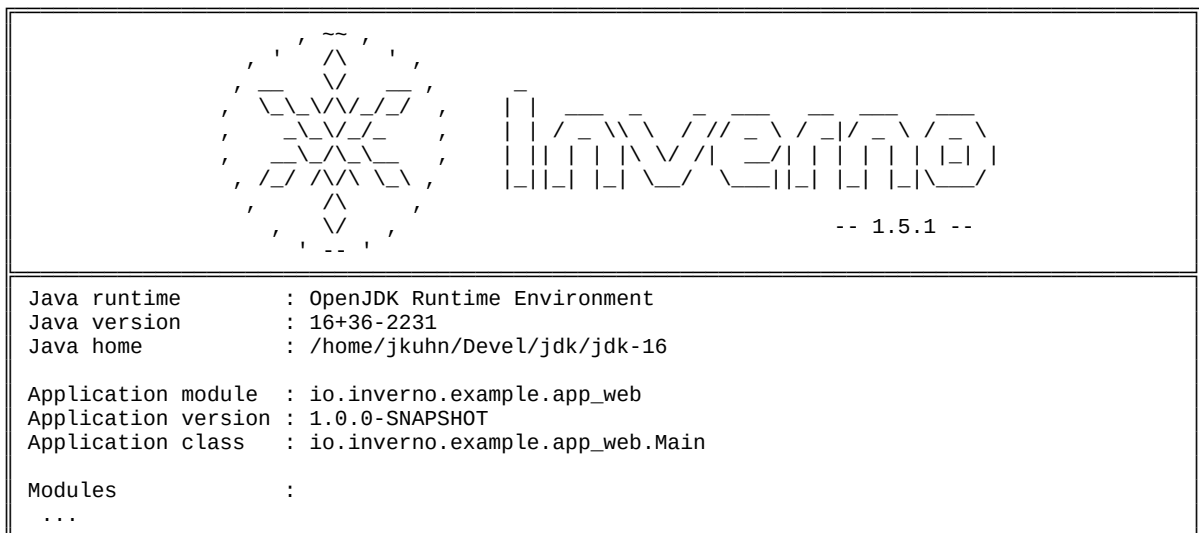
import io.inverno.core.v1.Application;

public class Main {

    public static void main(String[] args) {
        Application.with(new App_web.Builder()).run();
    }
}
```

The above example starts a Web server using default configuration which is a HTTP/1.x server with a Web router as root handler and an error router as error handler.

```
2021-04-14 11:00:18,308 INFO [main] i.w.c.v.Application - Inverno is starting...
```



```
2021-04-14 11:00:18,313 INFO [main] i.w.e.a.App_web - Starting Module io.inverno.example.app_web...
2021-04-14 11:00:18,313 INFO [main] i.w.m.b.Boot - Starting Module io.inverno.mod.boot...
2021-04-14 11:00:18,494 INFO [main] i.w.m.b.Boot - Module io.inverno.mod.boot started in 181ms
2021-04-14 11:00:18,494 INFO [main] i.w.m.w.Web - Starting Module io.inverno.mod.web...
2021-04-14 11:00:18,495 INFO [main] i.w.m.h.s.Server - Starting Module
io.inverno.mod.http.server...
2021-04-14 11:00:18,495 INFO [main] i.w.m.h.b.Base - Starting Module io.inverno.mod.http.base...
2021-04-14 11:00:18,499 INFO [main] i.w.m.h.b.Base - Module io.inverno.mod.http.base started in 4ms
2021-04-14 11:00:18,570 INFO [main] i.w.m.h.s.i.HttpServer - HTTP Server (nio) listening on
http://0.0.0.0:8080
2021-04-14 11:00:18,570 INFO [main] i.w.m.h.s.Server - Module io.inverno.mod.http.server started in
75ms
2021-04-14 11:00:18,571 INFO [main] i.w.m.w.Web - Module io.inverno.mod.web started in 76ms
2021-04-14 11:00:18,571 INFO [main] i.w.e.a.App_web - Module io.inverno.example.app_web started in
259ms
```

The Web router doesn't define any routes by default so if we hit the server, a (404) not found error is returned showing the default error Web router in action:

```
$ curl -i -H 'accept: application/json' http://localhost:8080
HTTP/1.1 404 Not Found
content-type: application/json
content-length: 47

{"status":"404","path":"/","error":"Not Found"}
```

Now if you open <http://localhost:8080> in a Web browser, you should see the following (404) whitelabel error page:

## 404 Not Found



## Configuration

The Web server configuration is done in the the *web* module configuration [WebConfiguration](#) which includes the *http-server* module configuration [HttpServerConfiguration](#). As for the *http-server* module, the net service configuration can also be considered to set low level network configuration in the *boot* module.

Let's create the following configuration in the *app\_web* module:

```
package io.inverno.example.app_web;

import io.inverno.core.annotation.NestedBean;
import io.inverno.mod.boot.BootConfiguration;
import io.inverno.mod.configuration.Configuration;
import io.inverno.mod.web.WebConfiguration;

@Configuration
public interface App_webConfiguration {

    @NestedBean
    BootConfiguration boot();

    @NestedBean
    WebConfiguration web();
}
```

The Web server can then be configured. For instance, we can enable HTTP/2 over cleartext, TLS, HTTP compression... as described in the [http-server module documentation](#).

```
package io.inverno.example.app_web;

import io.inverno.core.v1.Application;

public class Main {

    public static void main(String[] args) {
        Application.with(new App_web.Builder()
            .setApp_webConfiguration(
                App_webConfigurationLoader.load(configuration -> configuration
                    .web(web -> web
                        .http_server(server -> server
                            .server_port(8081)
                            .h2c_enabled(true)
                            .server_event_loop_group_size(4)
                        )
                    )
                )
            ).run();
    }
}
```

## Configuring the Web server controller

As explained before, the module specifies a `ServerController` bean as defined by the [http-server module](#) and wired to the HTTP server overriding the default server controller. It is composed of the Web router and the Error Web router beans which respectively route exchanges and error exchanges to the right handlers.

The Web server controller bean is private, its Web router and Error Web router are configured by defining a single `WebServerControllerConfigurer` bean. The `WebServerControllerConfigurer` interface extends both `WebRouterConfigurer` and `ErrorWebRouterConfigurer` and specifies a `createContext()` method used to initialize the exchange context as specified in [http-server module documentation](#). The Web server controller configurer is responsible for configuring routes in the Web server. It is invoked after default routes have been initialized but it doesn't replace them, they can however be overridden by defining routes matching the same rules.

### Web configurers

In a complex application with many route definitions sometimes dispatched into multiple modules and using complex interceptor setup, having a single configuration might not always be ideal and we should prefer defining multiple consistent configurers later aggregated into one Web server controller configurer bean. Following [Web routing API documentation](#), we know routes and interceptors can be configured using a combination of `WebRoutesConfigurer`, `WebInterceptorsConfigurer`, `WebRouterConfigurer`, `ErrorWebRoutesConfigurer`, `ErrorWebInterceptorsConfigurer` or `ErrorWebRouterConfigurer` beans. At compile time, the Inverno Web compiler plugin will then automatically generates a `WebServerControllerConfigurer` bean that aggregates all these beans into one single configuration. This way we don't have to create a Web server controller configurer bean and we can compose with above configurers which offer more flexibility, particularly in relation to the exchange context.

For instance, the Web router and the error Web router can be configured into separate configurer beans in the `app_web` module as follows:

```
package io.inverno.example.app_web;

import io.inverno.core.annotation.Bean;
import io.inverno.mod.base.resource.MediaTypees;
import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.web.WebRouter;
import io.inverno.mod.web.WebRouterConfigurer;

@Bean( visibility = Bean.Visibility.PRIVATE )
public class App_webWebRouterConfigurer implements WebRouterConfigurer<ExchangeContext> {

    @Override
    public void configure(WebRouter<ExchangeContext> router) {
        router
            .route()
                .path("/hello")
                .produces(MediaTypees.TEXT_PLAIN)
                .language("en-US")
                .handler(exchange -> exchange
                    .response()
                        .body()
                            .encoder(String.class)
                                .value("Hello!")
                )
            .route()
                .path("/hello")
                .produces(MediaTypees.TEXT_PLAIN)
                .language("fr-FR")
                .handler(exchange -> exchange
                    .response()
                        .body()
                            .encoder(String.class)
                                .value("Bonjour!")
                )
            .route()
                .path("/custom_exception")
                .handler(exchange -> {
                    throw new SomeCustomException();
                });
    }
}
```

```

package io.inverno.example.app_web;

import io.inverno.core.annotation.Bean;
import io.inverno.mod.base.resource.MediaTypees;
import io.inverno.mod.http.base.Status;
import io.inverno.mod.http.base.UnauthorizedException;
import io.inverno.mod.http.base.header.Headers;
import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.web.ErrorWebRouter;
import io.inverno.mod.web.ErrorWebRouterConfigurer;
import reactor.core.publisher.Mono;

@Bean( visibility = Bean.Visibility.PRIVATE )
public class App_webErrorWebRouterConfigurer implements ErrorWebRouterConfigurer<ExchangeContext> {

    @Override
    public void configure(ErrorWebRouter<ExchangeContext> errorRouter) {
        errorRouter
            .route()
                .error(SomeCustomException.class)
                .handler(errorExchange -> errorExchange
                    .response()
                    .headers(headers -> headers
                        .status(Status.BAD_REQUEST)
                        .contentType(MediaTypees.TEXT_PLAIN)
                    )
                    .body()
                    .encoder()
                    .value("A custom exception was raised")
                )
            .intercept()
                .error(UnauthorizedException.class)
                .interceptor(errorExchange -> {
                    errorExchange.response().headers(headers ->
headers.add(Headers.NAME_WWW_AUTHENTICATE, "basic realm=inverno"));
                    return Mono.just(errorExchange);
                })
            // We must apply interceptors to intercept error routes defined by default in the web
server module
            .applyInterceptors();
    }
}

```

After compilation, class `App_web_WebServerContollerConfigurer` aggregating the two configurer beans should have been generated and the corresponding bean wired into the Web server module.

Now we can test the application:

```

$ curl -i http://localhost:8080/
HTTP/1.1 404 Not Found
content-length: 0

$ curl -i http://localhost:8080/hello
HTTP/1.1 200 OK
content-type: text/plain
content-length: 6

Hello!

```



```
$ curl -i -H 'accept-language: fr' http://localhost:8080/hello
HTTP/1.1 200 OK
content-type: text/plain
content-length: 8

Bonjour!

$ curl -i -H 'accept: application/json' http://localhost:8080/hello
HTTP/1.1 406 Not Acceptable
content-type: application/json
content-length: 81

{"status":"406","path":"/hello","error":"Not Acceptable","accept":["text/plain"]}

$ curl -i http://localhost:8080/custom_exception
HTTP/1.1 400 Bad Request
content-type: text/plain
content-length: 29

A custom exception was raised
```

Since Web configurers are all defined as interfaces, you can easily centralize configuration by implementing one or more configurers. For instance, previous configurers could have been defined in one single bean implementing `WebRouterConfigurer<ExchangeContext>` and `ErrorWebRouterConfigurer<ExchangeContext>`.

Note that it is still possible to use a custom `WebServerControllerConfigurer` bean instead of the one generated by the Inverno Web compiler plugin. This basically requires to explicitly wire the custom bean into the `web` module using a `@Wire` annotation (otherwise compilation will fail indicating a dependency injection conflict as two beans can then be wired to the Web server controller configurer socket). This can be justified when there are specific needs regarding the exchange context. It is however recommended to use the generated configurer which greatly simplifies configuration.

When defining Web configurer beans, it is important to make them private inside the module in order to avoid side effects when composing the module as they may interfere with the generated server controller configurer, which already aggregates module's Web configurer beans, resulting in routes being configured twice. Compilation warnings shall be raised when a Web configurer is defined as a public bean.

Web configurers are applied by the generated Web server controller configurer in the following order starting by `WebInterceptorsConfigurer` beans, then `WebRouterConfigurer` beans and finally `WebRoutesConfigurer` beans. This basically means that the interceptors defined in `WebInterceptorsConfigurer` beans in the module will be applied to all routes defined in the module including those provided in component modules. Although it is possible to define multiple `WebInterceptorsConfigurer` beans, it is recommended to have only one because the order in which they are injected in the Web server controller configurer is not guaranteed which might be problematic under certain circumstances.

## Exchange context

The exchange context is global to all routes and interceptors, and basically specific to any application as it directly depends on what is expected by the routes and interceptors. Considering a complex application, this can quickly become very tricky. A safe approach would be to define a single global context type for the whole application and use it in all routes and interceptors definitions. Unfortunately we might have to include routes provided by third party modules that can't possibly use that context type. Besides, we might not want to expose the whole context to every routes and interceptors. The exchange context is unique and therefore necessarily global but ideally it should be possible to define different context types corresponding to the routes being defined. For instance, a secured route might require some kind of security context unlike a public route.

The exchange context is provided by the Web server controller which basically delegates to the `createContext()` method of the Web server controller configurer. Since it is generated by the Inverno Web compiler plugin, the plugin must also generate the global context based on the routes and interceptors definitions aggregated in the generated `WebServerControllerConfigurer` bean.

The fact that the `web` module only accepts one Web server controller configurer guarantees that there will be only one context provider.

Let's consider the case of an application which defines routes and interceptors that can use different exchange context depending on their functional area. For instance, we can imagine an application exposing front office and back office services using `FrontOfficeContext` and `BackOfficeContext` respectively.

Front office routes are then defined to handle exchanges exposing the `FrontOfficeContext` and back office routes, that may be specified in a completely different module, are defined to handle exchanges exposing the `BackOfficeContext`.

Let's start by defining these contexts and see how the global context is generated by the Inverno Web compiler plugin.

Exchange contexts must be defined as interfaces extending `ExchangeContext`:

```
package io.inverno.example.app_web.test;

import io.inverno.mod.http.server.ExchangeContext;

public interface FrontOfficeContext extends ExchangeContext {

    void setMarket(String market);

    String getMarket();
}
```

```

package io.inverno.example.app_web.test;

import io.inverno.mod.http.server.ExchangeContext;

public interface BackOfficeContext extends ExchangeContext {

    void setVar(double var);

    double getVar();
}

```

Then we can define different beans to configure front office and back office routers:

```

package io.inverno.example.app_web;

import io.inverno.core.annotation.Bean;
import io.inverno.mod.base.resource.MediaTypees;
import io.inverno.mod.http.base.Method;
import io.inverno.mod.web.WebInterceptable;
import io.inverno.mod.web.WebInterceptorsConfigurer;
import io.inverno.mod.web.WebRoutable;
import io.inverno.mod.web.WebRoutesConfigurer;
import reactor.core.publisher.Mono;

@Bean( visibility = Bean.Visibility.PRIVATE )
public class FrontOfficeRouterConfigurer implements WebRoutesConfigurer<FrontOfficeContext>,
WebInterceptorsConfigurer<FrontOfficeContext> {

    @Override
    public void configure(WebRoutable<FrontOfficeContext, ?> routes) {
        routes
            .route()
                .path("/frontOffice")
                .method(Method.GET)
                .handler(exchange -> {
                    exchange.response()
                        .headers(headers -> headers.contentType(MediaTypees.TEXT_PLAIN))
                        .body().string().value("I've done some stuff on market: " +
exchange.context().getMarket());
                });
    }

    @Override
    public void configure(WebInterceptable<FrontOfficeContext, ?> interceptors) {
        interceptors
            .intercept()
                .path("/frontOffice/**")
                .interceptor(exchange -> {
                    // Resolve the market from the request, session or else
                    exchange.context().setMarket("market");
                    return Mono.just(exchange);
                });
    }
}

```

```

package io.inverno.example.app_web;

import io.inverno.core.annotation.Bean;
import io.inverno.mod.base.resource.MediaTypees;
import io.inverno.mod.http.base.Method;
import io.inverno.mod.web.WebInterceptable;
import io.inverno.mod.web.WebInterceptorsConfigurer;
import io.inverno.mod.web.WebRoutable;
import io.inverno.mod.web.WebRoutesConfigurer;
import reactor.core.publisher.Mono;

@Bean( visibility = Bean.Visibility.PRIVATE )
public class BackOfficeRouterConfigurer implements WebRoutesConfigurer<BackOfficeContext>,
WebInterceptorsConfigurer<BackOfficeContext> {

    @Override
    public void configure(WebRoutable<BackOfficeContext, ?> routes) {
        routes
            .route()
                .path("/backOffice")
                .method(Method.GET)
                .handler(exchange -> {
                    exchange.response()
                        .headers(headers -> headers.contentType(MediaTypees.TEXT_PLAIN))
                        .body().string().value("VaR is: " + exchange.context().getVar());
                });
    }

    @Override
    public void configure(WebInterceptable<BackOfficeContext, ?> interceptors) {
        interceptors
            .intercept()
                .path("/backOffice/**")
                .interceptor(exchange -> {
                    // Resolve the VaR from the request, session or else
                    exchange.context().setVar(1234.5678);
                    return Mono.just(exchange);
                });
    }
}

```

Now if we compile the module, the Inverno Web compiler plugin generates interface `App_web_WebServerContollerConfigurer.Context` inside the generated `App_web_WebServerContollerConfigurer` which extends all context types encountered while aggregating the configurer beans. It will also implement method `createContext()` in order to return a concrete implementation of the context:

- Getter and setter methods (i.e. `T get*()` and `void set*(T value)` methods) are implemented in order be able to set and get data on the context as shown in above examples.
- Other methods with no default implementation gets a blank implementation (i.e. no-op).

If we open the generated `App_web_WebServerContollerConfigurer` we should see:

```

...
@Override
public Context createContext() {
    return new Context() {
        private String market;
        private double var;

        @Override
        public String getMarket() {
            return this.market;
        }

        @Override
        public void setMarket(String market) {
            this.market = market;
        }

        @Override
        public double getVar() {
            return this.var;
        }

        @Override
        public void setVar(double var) {
            this.var = var;
        }
    };
}

public static interface Context extends BackOfficeContext, FrontOfficeContext, ExchangeContext {}
...

```

Using such generated context guarantees that the context created by the Web server controller complies with what is expected by route handlers and interceptors. This allows to safely compose multiple Web modules in an application, developed by separate teams and using different context types.

This doesn't come without limitations. For instance, exchange context must be defined as interfaces since multiple inheritance is not supported in Java. If you try to use a class, a compilation error will be raised.

Another limitation comes from the fact that it might be difficult to define a route that uses many context types, using configurers the only way to achieve this is to create an intermediary interface that extends the required context types. Although this is acceptable, it is not ideal semantically speaking. Hopefully this issue can be mitigated, at least for route definition, when routes are defined in a declarative way in a [Web controller](#) which allows to specify context type using intersection types on the route method (e.g. `<T extends FrontOfficeContext & BackOfficeContext>`).

Finally, the Inverno Web compiler plugin only generates concrete implementations for getter and setter methods which might seem simplistic but actual logic can still be provided using default implementations in the context interface. For example, role based access control can be implemented in a security context as follows:

```

package io.inverno.example.app_web;

import io.inverno.mod.http.server.ExchangeContext;
import java.util.Set;

public interface SecurityContext extends ExchangeContext {

    void setRoles(Set<String> roles);

    Set<String> getRoles();

    default boolean hasRole(String role) {
        return this.getRoles().contains(role);
    }
}

```

Exposing `setRoles()` methods to actual services which should only be concerned by controlling access might not be ideal. There are two concerns to consider here: first resolving the roles of the authenticated user and set them into the context which is the responsibility of a security interceptor and then controlling the access to a secured service or resource which is the responsibility of a service or another security interceptor. Since we can compose multiple configurers using multiple context types automatically aggregated into one server controller configurer we can easily solve that issue by splitting previous security context:

```

package io.inverno.example.app_web;

import io.inverno.mod.http.server.ExchangeContext;
import java.util.Set;

public interface SecurityContext extends ExchangeContext {

    Set<String> getRoles();

    default boolean hasRole(String role) {
        return this.getRoles().contains(role);
    }
}

package io.inverno.example.app_web;

import java.util.Set;

public interface ConfigurableSecurityContext extends SecurityContext {

    void setRoles(Set<String> roles);
}

```

Particular care must be taken when declaring context types with generics (e.g. `Context<A>`), we must always make sure that for a given erased type (e.g. `Context`) there is one type that is assignable to all others which will then be retained during the context type generation. This basically follows Java language specification which prevents from implementing the same interface twice with different arguments as a result the generated context can only implement one which must obviously be assignable to all others. A compilation error shall be reported if inconsistent exchange context types have been defined.

In order to avoid any misuse and realize the benefits of the context generation, it is important to understand the purpose of the exchange context and why we choose to have it strongly typed.

The exchange context is mainly used to propagate contextual information across the routing chain composed by interceptors and the exchange handler, it is not necessarily meant to expose any logic.

Unlike many other frameworks which use untyped map, the exchange context is strongly typed which has many advantages:

- static checking can be performed by the compiler,
- an handler or an interceptor have guarantees over the information exposed in the context (`ClassCastException` are basically impossible),
- as we just saw it is also possible to expose some logic using default interface methods,
- actual services can be exposed right away in the context without having to use error prone string keys or explicit cast.

The generation of the context by the Inverno Web compiler plugin is here to reduce the complexity induced by strong typing as long as above rules are respected.

## Static handler

The `StaticHandler` is a built-in exchange handler that can be used to define routes for serving static resources resolved with the [Resource API](#).

For instance, we can create a route to serve files stored in a `web-root` directory as follows:

```
router
  .route()
    .path("/static/{path:.*}") // 1
    .handler(new StaticHandler<>(new FileResource("web-root/"))) // 2
```

1. The path must be parameterized with a `path` parameter which can include `/`, for the static handler to be able to determine the relative path of the resource in the `web-root` directory
2. The base resource is defined directly as a `FileResource`, although it is also possible to use a `ResourceService` to be more flexible in terms of the kind of resource

The static handler relies on the resource abstraction to resolve resources, as a result, these can be located on the file system, on the class path, on the module path...

The static handler also looks for a welcome page when a directory resource is requested. For instance considering the following `web-root` directory:

```
web-root/
├── index.html
└── snowflake.svg
```

A request to `http://127.0.0.1/static/` would return the `index.html` file.

## 100-continue interceptor

The `ContinueInterceptor` class which can be used to automatically handles `100-continue` as defined by [RFC 7231 Section 5.1.1](#).

```
router
    .intercept()
        .interceptor(new ContinueInterceptor())
    .route()
    ...
```

Note that in order to comply with RFC 7231, an HTTP server must respond with a (100) status to a request with a 100-continue expectation. The `ContinueInterceptor` allows to automatize this, otherwise it must be done explicitly:

```
...
if(exchange.request().headers().contains(Headers.NAME_EXPECT, Headers.VALUE_100_CONTINUE)) {
    exchange.response().sendContinue();
}
...
```

## WebJars

The `WebJarsRoutesConfigurer` is a `WebRoutesConfigurer` implementation used to configure routes to WebJars static resources available on the module path or class path. Paths to the resources are version agnostic: `/webjars/{webjar_module}/{path:. *}` where `{webjar_module}` corresponds to the *modularized* name of the WebJar minus `org.webjars`. For example the location of the Swagger UI WebJar would be `/webjars/swagger.ui/`.

The `WebJarsRoutesConfigurer` requires a `ResourceService` to resolve WebJars resources. WebJars routes can be configured as follows:



```

package io.inverno.example.app_web;

import io.inverno.core.annotation.Bean;
import io.inverno.mod.base.resource.ResourceService;
import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.web.WebJarsRoutesConfigurer;
import io.inverno.mod.web.WebRouter;
import io.inverno.mod.web.WebRouterConfigurer;

@Bean
public class App_webWebRouterConfigurer implements WebRouterConfigurer<ExchangeContext> {

    private final ResourceService resourceService;

    public App_webWebRouterConfigurer(ResourceService resourceService) {
        this.resourceService = resourceService;
    }

    @Override
    public void accept(WebRouter<ExchangeContext> router) {
        router
            .configureRoutes(new WebJarsRoutesConfigurer<>(this.resourceService))
            ...
    }
}

```

Then we can declare WebJars dependencies such as the Swagger UI in the build descriptor:

```

<project>
  <dependencies>
    <dependency>
      <groupId>org.webjars</groupId>
      <artifactId>swagger-ui</artifactId>
    </dependency>
  </dependencies>
</project>

```

The Swagger UI should be accessible at <http://localhost:8080/webjars/swagger-ui/>.

Sadly WebJars are rarely modular JARs, they are not even named modules which causes several issues when dependencies are specified on the module path. That's why when an application is run or packaged using [Inverno tools](#), such dependencies and WebJars in particular are *modularized*. A WebJar such as `swagger-ui` is modularized into `org.webjars.swagger.ui` module which explains why it is referred to by its module name: `swagger.ui` in the WebJars resource path (the `org.webjars` part is omitted since the context is known).

When running a fully modular Inverno application, *modularized* WebJars modules must be added explicitly to the JVM using the `--add-modules` option, otherwise they are not resolved when the JVM starts. For instance:

```
$ java --add-modules org.webjars.swagger.ui ...
```

Hopefully, the Inverno Maven plugin adds unnamed modules by default when running or packaging an application, so you shouldn't have to worry about it. The following command automatically adds the unnamed modules when running the JVM:

```
$ mvn inverno:run
```

This can be disabled in order to manually control which modules should be added:

```
$ mvn inverno:run -Dinverno.exec.addUnnamedModules=false -Dinverno.exec.vmOptions="--add-modules org.webjars.swagger.ui"
```

It might also be possible to define the dependency in the module descriptor, unfortunately since WebJars modules are unnamed, they are named after the name of the JAR file which is greatly unstable and can't be trusted, so previous approach is by far the safest. If you need to create a WebJar you should make it a named module with the `Automatic-Module-Name` attribute sets to `org.webjars.{webjar_module}` in the manifest file and with resources located under `META-INF/resources/webjars/{webjar_module}/{webjar_version}/`.

Note that when the application is run with non-modular WebJars specified on the class path, they can be accessed without any particular configuration as part of the UNNAMED module using the same path notation.

## OpenAPI specification

The `OpenApiRoutesConfigurer` is a `WebRoutesConfigurer` implementation used to configure routes to [OpenAPI specifications](#) defined in `/META-INF/inverno/web/openapi.yml` resources in application modules.

OpenAPI routes can be configured on the Web router as follows:

```
package io.inverno.example.app_web;

import io.inverno.core.annotation.Bean;
import io.inverno.mod.base.resource.ResourceService;
import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.web.OpenApiRoutesConfigurer;
import io.inverno.mod.web.WebRouter;
import io.inverno.mod.web.WebRouterConfigurer;

@Bean
public class App_webWebRouterConfigurer implements WebRouterConfigurer<ExchangeContext> {

    private final ResourceService resourceService;

    public App_webWebRouterConfigurer(ResourceService resourceService) {
        this.resourceService = resourceService;
    }

    @Override
    public void accept(WebRouter<ExchangeContext> router) {
        router
            .configureRoutes(new OpenApiRoutesConfigurer<>(this.resourceService))
            ...
    }
}
```

The configurer will scan for OpenAPI specifications files `/META-INF/inverno/web/openapi.yml` in the application modules and configure the following routes:

- `/open-api` returning the list of available OpenAPI specifications in `application/json`
- `/open-api/{moduleName}` returning the OpenAPI specifications defined for the specified module name or (404) not found error if there is no OpenAPI specification defined in the module or no module with that name.

By default the configurer also configures these routes to display OpenAPI specifications in a [Swagger UI](#) when accessed from a Web browser (ie. with `accept: text/html`) assuming the Swagger UI Webjar dependency is present:

```
<project>
  <dependencies>
    <dependency>
      <groupId>org.webjars</groupId>
      <artifactId>swagger-ui</artifactId>
    </dependency>
  </dependencies>
</project>
```

Swagger UI support can be disabled from the `OpenApiRoutesConfigurer` constructor:

```
router
  .configureRoutes(new OpenApiRoutesConfigurer<>(this.resourceService, false))
  ...
```

OpenAPI specifications are usually automatically generated by the Web Inverno compiler plugin for routes defined in a [Web controller](#) but you can provide manual or generated specifications using the tool of your choice, as long as it is not conflicting with the Web compiler plugin.

## Web Controller

The [Web routing API](#) provides a *programmatic* way of defining the Web routes of a Web server but it also provides a set of annotations for defining Web routes in a more declarative way.

A **Web controller** is a regular module bean annotated with `@WebController` which defines methods annotated with `@WebRoute` describing Web routes. These beans are scanned at compile time by the Inverno Web compiler plugin in order to include corresponding *programmatic* configuration in the generated Web server controller configurer.

For instance, in order to create a book resource with basic CRUD operations, we can start by defining a `Book` model in a dedicated `*.dto` package (we'll see later why this matters):

```

package io.inverno.example.app_web.dto;

public class Book {

    private String isbn;
    private String title;
    private String author;
    private int pages;

    // Constructor, getters, setters, hashCode, equals...
}

```

Now we can define a **BookResource** Web controller as follows:

```

package io.inverno.example.app_web;

import java.util.Set;

import io.inverno.core.annotation.Bean;
import io.inverno.example.app_web.dto.Book;
import io.inverno.mod.base.resource.MediaTypees;
import io.inverno.mod.http.base.Method;
import io.inverno.mod.web.annotation.Body;
import io.inverno.mod.web.annotation.PathParam;
import io.inverno.mod.web.annotation.WebController;
import io.inverno.mod.web.annotation.WebRoute;

@Bean( visibility = Bean.Visibility.PRIVATE ) // 1
@WebController( path = "/book" ) // 2
public class BookResource {

    @WebRoute( method = Method.POST, consumes = MediaTypees.APPLICATION_JSON ) // 3
    public void create(@Body Book book) { // 4
        ...
    }

    @WebRoute( path =("/{isbn}", method = Method.PUT, consumes = MediaTypees.APPLICATION_JSON )
    public void update(@PathParam String isbn, @Body Book book) {
        ...
    }

    @WebRoute( method = Method.GET, produces = MediaTypees.APPLICATION_JSON )
    public Set<Book> list() {
        ...
    }

    @WebRoute( path =("/{isbn}", method = Method.GET, produces = MediaTypees.APPLICATION_JSON )
    public Book get(@PathParam String isbn) {
        ...
    }

    @WebRoute( path =("/{isbn}", method = Method.DELETE )
    public void delete(@PathParam String isbn) {
        ...
    }
}

```

Implementations details have been omitted for clarity, here is what's important:

1. A Web controller must be a module bean because it will be wired into the generated Web router configurator and used to invoke the right handler method attached to a Web route. Besides this is convenient for implementation as it allows a repository to be wired into the `BookResource` bean for instance.
2. The `@WebController` annotation tells the Web compiler plugin to process the bean as a Web controller. The controller root path can also be specified in this annotation, if not specified it defaults to `/` which is the root path of the Web server.
3. The `@WebRoute` annotation on a method tells the Web compiler plugin to define a route whose handler should invoke that method. The set of routing rules (ie. path, method, consume, produce, language) describing the route can all be specified in the annotation.
4. Request Parameters and body are specified as method parameters annotated with `@CookieParam`, `@FormParam`, `@HeaderParam`, `@PathParam`, `@QueryParam` and `@Body` annotations.

Some other contextual objects like the underlying `WebExchange` or the exchange context can also be injected in the Web controller method.

Assuming we have provided proper implementations to create, update, list, get and delete a book in a data store, we can compile the module. The generated Web server controller configurator bean should configure the routes corresponding to the Web controller's annotated methods in the Web router. The generated class uses the same APIs described before, it is perfectly readable and debuggable and above all it eliminates the overhead of resolving Web controllers or Web routes at runtime.

Now let's go back to the `Book` DTO, we said earlier that it must be created in a dedicated package, the reason is actually quite simple. Since above routes consume and produce `application/json` payloads, the `application/json` media type converter will be invoked to convert `Book` objects from/to JSON data. This converter uses an `ObjectMapper` object from module `com.fasterxml.jackson.databind` which uses reflection to instantiate the objects and populate them from a parsed JSON tree. Unfortunately or hopefully the Java modular system prevents unauthorized reflective access and as a result the `ObjectMapper` can't access the `Book` class unless we explicitly export the package containing DTOs to module `com.fasterxml.jackson.databind` in the module descriptor as follows:

```
module io.inverno.example.app_web {  
    ...  
    exports io.inverno.example.app_web.dto to com.fasterxml.jackson.databind;  
}
```

Using a dedicated package for DTOs allows then to limit and control the access to the module classes.

If you're not familiar with the Java modular system and used to Java 8<, you might find this a bit distressing but if you want to better structure and secure your applications, this is the way.

We can now run the application and test the book resource:

```
$ curl -i http://localhost:8080/book
HTTP/1.1 200 OK
content-type: application/json
content-length: 2
```

```
[]
```

```
$ curl -i -X POST -H 'content-type: application/json' -d '{"isbn":"978-0132143011","title":"Distributed Systems: Concepts and Design","author":"George Coulouris, Jean Dollimore, Tim Kindberg, Gordon Blair","pages":1080}' http://localhost:8080/book
HTTP/1.1 200 OK
content-length: 0
```

```
$ curl -i http://localhost:8080/book
HTTP/1.1 200 OK
content-type: application/json
content-length: 163
```

```
[{"isbn":"978-0132143011","title":"Distributed Systems: Concepts and Design","author":"George Coulouris, Jean Dollimore, Tim Kindberg, Gordon Blair","pages":1080}]
```

```
$ curl -i http://localhost:8080/book/978-0132143011
HTTP/1.1 200 OK
content-type: application/json
content-length: 161
```

```
{"isbn":"978-0132143011","title":"Distributed Systems: Concepts and Design","author":"George Coulouris, Jean Dollimore, Tim Kindberg, Gordon Blair","pages":1080}
```

It is possible to separate the API from the implementation by defining the Web controller and the Web routes in an interface implemented in a module bean. For instance:

```
package io.inverno.example.app_web;
```

```
import io.inverno.example.app_web.dto.Book;
import io.inverno.mod.base.resource.MediaTypees;
import io.inverno.mod.http.base.Method;
import io.inverno.mod.web.annotation.Body;
import io.inverno.mod.web.annotation.PathParam;
import io.inverno.mod.web.annotation.WebController;
import io.inverno.mod.web.annotation.WebRoute;
import java.util.Set;
```

```
@WebController( path = "/book" )
```

```
public interface BookResource {
```

```
    @WebRoute( method = Method.POST, consumes = MediaTypees.APPLICATION_JSON )
    void create(@Body Book book);
```

```
    @WebRoute( path =("/{isbn}", method = Method.PUT, consumes = MediaTypees.APPLICATION_JSON )
    void update(@PathParam String isbn, @Body Book book);
```

```
    @WebRoute( method = Method.GET, produces = MediaTypees.APPLICATION_JSON )
    Set<Book> list();
```

```
    @WebRoute( path =("/{isbn}", method = Method.GET, produces = MediaTypees.APPLICATION_JSON )
    Book get(@PathParam String isbn);
```

```
    @WebRoute( path =("/{isbn}", method = Method.DELETE )
    void delete(@PathParam String isbn);
```

```
}
```

```

package io.inverno.example.app_web;

import io.inverno.core.annotation.Bean;
import io.inverno.example.app_web.dto.Book;
import io.inverno.mod.http.base.BadRequestException;
import io.inverno.mod.http.base.NotFoundException;
import io.inverno.mod.web.annotation.Body;
import io.inverno.mod.web.annotation.PathParam;
import java.util.HashSet;
import java.util.Map;
import java.util.Set;
import java.util.concurrent.ConcurrentHashMap;

@Bean( visibility = Bean.Visibility.PRIVATE )
public class BookResourceImpl implements BookResource {

    @Override
    public void create(@Body Book book) {
        ...
    }

    @Override
    public void update(@PathParam String isbn, @Body Book book) {
        ...
    }

    @Override
    public Set<Book> list() {
        ...
    }

    @Override
    public Book get(@PathParam String isbn) {
        ...
    }

    @Override
    public void delete(@PathParam String isbn) {
        ...
    }
}

```

This provides better modularity and allows defining the API in a dedicated module which can later be used to implement various server and/or client implementations in different modules. Another advantage is that it allows to split a Web controller interface into multiple interfaces.

Generics are also supported, we can for instance create the following generic **CRUD<T>** interface:

```

package io.inverno.example.app_web;

import io.inverno.mod.base.resource.MediaTypees;
import io.inverno.mod.http.base.Method;
import io.inverno.mod.web.annotation.Body;
import io.inverno.mod.web.annotation.PathParam;
import io.inverno.mod.web.annotation.WebRoute;
import java.util.Set;

public interface CRUD<T> {

    @WebRoute(method = Method.POST, consumes = MediaTypees.APPLICATION_JSON)
    void create(@Body T resource);

    @WebRoute(path =("/{id}", method = Method.PUT, consumes = MediaTypees.APPLICATION_JSON)
    void update(@PathParam String id, @Body T resource);

    @WebRoute(method = Method.GET, produces = MediaTypees.APPLICATION_JSON)
    Set<T> list();

    @WebRoute(path =("/{id}", method = Method.GET, produces = MediaTypees.APPLICATION_JSON)
    T get(@PathParam String id);

    @WebRoute(path =("/{id}", method = Method.DELETE)
    void delete(@PathParam String id);
}

```

And then create multiple specific resources using that interface:

```

package io.inverno.example.app_web;

import io.inverno.example.app_web.dto.Book;
import io.inverno.mod.web.annotation.WebController;

@WebController(path = "/book")
public interface BookResource extends CRUD<Book> {

}

```

The book resource as we defined it doesn't seem very reactive, this statement is both true and untrue: the API and the Web server are fully reactive, as a result Web routes declared in the book resource Web controller are configured using a reactive API in the generated Web server controller configurer, nonetheless the methods in the Web controller are not reactive.

Luckily, we can easily transform previous interface and make it fully reactive:



```

package io.inverno.example.app_web;

import io.inverno.mod.base.resource.MediaTypees;
import io.inverno.mod.http.base.Method;
import io.inverno.mod.web.annotation.Body;
import io.inverno.mod.web.annotation.PathParam;
import io.inverno.mod.web.annotation.WebRoute;
import reactor.core.publisher.Flux;
import reactor.core.publisher.Mono;

public interface CRUD<T> {

    @WebRoute(method = Method.POST, consumes = MediaTypees.APPLICATION_JSON)
    Mono<Void> create(@Body Mono<T> resource);

    @WebRoute(path =("/{id}", method = Method.PUT, consumes = MediaTypees.APPLICATION_JSON)
    Mono<Void> update(@PathParam String id, @Body Mono<T> resource);

    @WebRoute(method = Method.GET, produces = MediaTypees.APPLICATION_JSON)
    Flux<T> list();

    @WebRoute(path =("/{id}", method = Method.GET, produces = MediaTypees.APPLICATION_JSON)
    Mono<T> get(@PathParam String id);

    @WebRoute(path =("/{id}", method = Method.DELETE)
    Mono<Void> delete(@PathParam String id);
}

```

There is one remaining thing to do to make the book resource a proper REST resource. When creating a book we must return a 201 Created HTTP code with a **location** header as defined by [RFC7231 Section 7.1.2](#). This can be done by injecting the **WebExchange** directly in the **create()** method:

```

public interface CRUD<T> {

    @WebRoute(method = Method.POST, consumes = MediaTypees.APPLICATION_JSON, produces =
MediaTypees.APPLICATION_JSON)
    Mono<Void> create(@Body Mono<T> resource, WebExchange<?> exchange);
    ...
}

```

We can then do the following in the book resource implementation to set the status and **location** header:

```

package io.inverno.example.app_web;

import io.inverno.core.annotation.Bean;
import io.inverno.example.app_web.dto.Book;
import io.inverno.mod.http.base.Status;
import io.inverno.mod.http.base.header.Headers;
import io.inverno.mod.web.WebExchange;
import reactor.core.publisher.Mono;

@Bean
public class BookResourceImpl implements BookResource {

    @Override
    public Mono<Void> create(Mono<Book> book, WebExchange<?> exchange) {
        ...
        exchange.response().headers(headers -> headers
            .status(Status.CREATED)
            .add(Headers.NAME_LOCATION,
exchange.request().getPathBuilder().segment(b.getIsbn()).buildPath())
        );
        ...
    }
    ...
}

```

Now if we run the application and create a book resource we should get the following:

```

$ curl -i -X POST -H 'content-type: application/json' -d '{"isbn":"978-0132143011","title":"Distributed Systems: Concepts and Design","author":"George Coulouris, Jean Dollimore, Tim Kindberg, Gordon Blair","pages":1080}' http://localhost:8080/book
HTTP/1.1 201 Created
content-type: application/json
location: /book/978-0132143012
content-length: 0

```

Declarative routes are configured last in the generated Web server controller configurator which means they override any route previously defined in a Web configurator but above all they are intercepted by the interceptors defined in `WebInterceptorsConfigurer` beans in the module.

## Declarative Web route

So far, we have described a concrete Web controller use case which should already give a good idea on how to configure route in a declarative way. Now, let's examine in details how a Web route is declared in a Web controller.

A Web route or HTTP endpoint or REST endpoint... in short an HTTP request/response exchange is essentially defined by:

- An input, basically an HTTP request characterized by the following components: path, method, query parameters, headers, cookies, path parameters, request body.
- A normal output, basically a successful HTTP response and more precisely: a status (2xx or 3xx), headers and a response body.
- A set of error outputs, basically unsuccessful HTTP responses and more precisely: a status (4xx or 5xx), headers and a response body.

Web routes are defined as methods in a Web controller which match this definition: the Web route input is defined as method parameters, the Web route normal output is defined by the return type of the method and finally the exceptions thrown by the method define the Web route error outputs.

It then remains to bind the Web route semantic to the method, this is done using various annotations on the method and its parameters.

## Routing rules

Routing rules, as defined in the [Web routing API](#), are specified in a single `@WebRoute` annotation on a Web controller method. It allows to define paths, methods, consumed media ranges, produced media types and produced languages of the Web routes that route a matching request to the handler implemented by the method.

For instance, we can define multiple paths and/or multiple produced media types in order to expose a resource at different locations in various formats:

```
@WebRoute( path = { "/book/current", "/book/v1" }, produces = { MediaType.APPLICATION_JSON,
    MediaType.APPLICATION_XML } )
Flux<T> list();
```

The `matchTrailingSlash` parameter can be used to indicate that the defined paths should be matched taking the trailing slash into account or not.

Note that this exactly corresponds to the [Web routing API](#).

## Parameter bindings

As stated above, a `@WebRoute` annotated method must be bound to a Web exchange. In particular, method parameters are bound to the various elements of the request using `*Param` annotations defined in the Web routing API.

Such parameters can be of any type, as long as the parameter converter plugged into the *web* module can convert it, otherwise a `ConverterException` is thrown. The default parameter converter provided in the *boot* module is able to convert primitive and common types including arrays and collections. Please refer to the [HTTP server documentation](#) to learn how to extend the parameter converter to convert custom types.

In the following example, the value or values of query parameter `isbn` is converted to an array of strings:

```
@WebRoute( path = { "/book/byIsbn" }, produces = { MediaType.APPLICATION_JSON } )
Flux<T> getBooksByIsbn(@QueryParam String[] isbn);
```

If the above route is queried with `/book/byIsbn?isbn=978-0132143011,978-0132143012,978-0132143013&isbn=978-0132143014` the `isbn` parameter is then: `["978-0132143011", "978-0132143012", "978-0132143013", "978-0132143014"]`.

A parameter defined like this is required by default and a `MissingRequiredParameterException` is thrown if one or more parameters are missing from the request but it can be declared as optional by defining it as an `Optional<T>`:

In the following example, query parameter `limit` is optional and no exception will be thrown if it is missing from the request:

```
@WebRoute( path = { "/book" }, produces = { MediaType.APPLICATION_JSON } )
Flux<T> getBooks(@QueryParam Optional<Integer> limit);
```

### *Query parameter*

Query parameters are declared using the `@QueryParam` annotation as follows:

```
@WebRoute( path = { "/book/byIsbn" }, produces = { MediaType.APPLICATION_JSON } )
Flux<T> getBooksByIsbn(@QueryParam String[] isbn);
```

Note that the name of the method parameter actually defines the name of the query parameter.

This contrasts with other RESTful API, such as JAX-RS, which requires to specify the parameter name, again, in the annotation. Since the Inverno Web compiler plugin works at compile time, it has access to actual method parameter names defined in the source.

### *Path parameter*

Path parameters are declared using the `@PathParam` annotation as follows:

```
@WebRoute(path = "{id}", method = Method.GET, produces = MediaType.APPLICATION_JSON)
Mono<T> get(@PathParam String id);
```

Note that the name of the method parameter must match the name of the path parameter of the route path defined in the `@WebRoute` annotation.

### *Cookie parameter*

It is possible to bind cookie values as well using the `@CookieParam` annotation as follows:

```
@WebRoute(method = Method.POST, consumes = MediaType.APPLICATION_JSON)
Mono<Void> create(@CookieParam String book_store, @Body Mono<T> book, WebExchange exchange);
```

In previous example, the route must be queried with a `book_store` cookie which is not declared as optional:

```
$ curl -i -X POST -H 'cookie: book_store=store1' -H 'content-type: application/json' -d '...'
http://localhost:8080/book
...
```

### *Header parameter*

Header field can also be bound using the `@HeaderParam` annotation as follows:

```
@WebRoute(method = Method.GET, produces = MediaType.APPLICATION_JSON)
Flux<T> list(@HeaderParam Optional<Format> format);
```

In previous example, the `Format` type is an enumeration indicating how book references must be returned (eg. `SHORT`, `FULL`...), a `format` header may or may not be added to the request since it is declared as optional:

```
$ curl -i -H 'format: SHORT' http://localhost:8080/book
...
```

### Form parameter

Form parameters are bound using the `@FormParam` annotation as follows:

```
@WebRoute(method = Method.POST, consumes = MediaType.APPLICATION_X_WWW_FORM_URLENCODED)
Mono<Void> createAuthor(
    @FormParam String forename,
    @FormParam Optional<String> middlename,
    @FormParam String surname,
    @FormParam LocalDate birthdate,
    @FormParam Optional<LocalDate> deathdate,
    @FormParam String nationality);
```

Form parameters are sent in a request body following `application/x-www-form-urlencoded` format as defined by [living standard](#). They can be sent using a HTML form submitted to the server resulting in the following request body:

```
forename=Leslie,middlename=B.,surname=Lamport,birthdate=19410207,nationality=US
```

Previous route can then be queried as follows:

```
$ curl -i -X POST -H 'content-type:application/x-www-form-urlencoded' -d
'forename=Leslie,middlename=B.,surname=Lamport,birthdate=19410207,nationality=US'
http://localhost:8080/author
```

Form parameters results from the parsing of the request body and as such, `@FormParam` annotations can't be used together with `@Body` on route method parameters.

## Contextual parameters

A contextual parameter is directly related to the context into which an exchange is processed in the route method, it can be injected in the route method by specifying a method parameter of a supported contextual parameter type.

### WebExchange

The underlying Web exchange can be injected by specifying a method parameter of a type assignable from `WebExchange`.

```
@WebRoute(method = Method.POST, consumes = MediaType.APPLICATION_JSON)
Mono<Void> create(@Body Mono<T> resource, WebExchange<?> exchange) throws BadRequestException;
```

The exchange gives full access to the underlying request and response. Although it allows to manipulate the request and response bodies, this might conflict with the generated Web route and as a result the exchange should only be used to access request parameters, headers, cookies... or specify a specific response status, response cookies or headers...

The Web exchange also gives access to the exchange context, if a route handler requires a particular context type, it can be specified as a type parameter as follows:

```
@WebRoute(method = Method.POST, consumes = MediaType.APPLICATION_JSON)
Mono<Void> create(@Body Mono<T> resource, WebExchange<SecurityContext> exchange) throws
BadRequestException;
```

Context types declared in a declarative Web route are aggregated in the Web server controller configurator by the Inverno Web compiler plugin in the same way as for Web server [configurators](#). However declarative Web routes make it possible to use interaction types when multiple context types are expected using a type variable which brings more flexibility.

```
@WebRoute(method = Method.POST, consumes = MediaType.APPLICATION_JSON)
<E extends TracingContext & SecurityContext> Mono<Void> create(@Body Mono<T> resource,
WebExchange<E> exchange) throws BadRequestException;
```

When declaring generic context types, we must make sure they are all consistent (i.e. there is one type that is assignable to all others). When declaring a route using generic context type, it is then good practice to use upper bound wildcards as follows:

```
@WebRoute(method = Method.POST, consumes = MediaType.APPLICATION_JSON)
Mono<Void> create(@Body Mono<T> resource, WebExchange<SecurityContext<? extends PersonIdentity, ?
extends AccessController>> exchange) throws BadRequestException;
```

Previous code basically means that the route requires a `SecurityContext` with any `PersonIdentity` types and any `AccessController` types. This is quite different than if we defined it as `SecurityContext<PersonIdentity, AccessController>`, in the first case we can assign `SecurityContext<PersonIdentity, RoleBasedAccessController>` whereas in the second case we can only assign `SecurityContext<PersonIdentity, RoleBasedAccessController>`. Using upper bound wildcards then provides greater flexibility and more integration options: routes basically don't have to be defined using the same context type definition.

### *Exchange context*

The exchange context can also be injected directly by specifying a method parameter of a type assignable from `ExchangeContext`.

```
@WebRoute(path =("/{id}", method = Method.GET, produces = MediaType.APPLICATION_JSON)
Mono<T> get(@PathParam String id, WebContext webContext);
```

As for the Web exchange, it is possible to specify intersection types using a type variable:

```
@WebRoute(path =("/{id}", method = Method.GET, produces = MediaType.APPLICATION_JSON)
<E extends WebContext & InterceptorContext> Mono<T> get(@PathParam String id, E context);
```

As before, context types declared in a declarative Web route are aggregated in the Web server controller configurator by the Inverno Web compiler plugin.

## Request body

The request body can be bound to a route method parameter using the `@Body` annotation. Request body is automatically converted based on the media type declared in the `content-type` header field of the request as described in the [Web server exchange documentation](#). The body parameter method can then be of any type as long as there is a media type converter for the media type specified in the request that can convert it.

In the following example, the request body is bound to parameter `book` of type `Book`, it is then converted from `application/json` into a `Book` instance:

```
@WebRoute(method = Method.POST, consumes = MediaType.APPLICATION_JSON)
void create(@Body Book book);
```

Unlike parameters, the request body can be specified in a reactive way, the previous example can then be rewritten using a `Mono<T>`, a `Flux<T>` or more broadly a `Publisher<T>` as body parameter type as follows:

```
@WebRoute(method = Method.POST, consumes = MediaType.APPLICATION_JSON)
Mono<Void> create(@Body Mono<Book> book);
```

A stream of objects can be processed when the media type converter supports it. For instance, the `application/x-ndjson` converter can emit converted objects each time a new line is encountered, this allows to process content without having to wait for the entire message resulting in better response time and reduced memory consumption.

```
@WebRoute(method = Method.POST, consumes = MediaType.APPLICATION_X_NDJSON)
Mono<Void> create(@Body Flux<Book> book);
```

The `application/json` also supports such streaming capability by emitting converted objects while parsing a JSON array.

The `@Body` annotation can not be used together with the `@FormParam` annotation on route method parameters because the request body can only be consumed once.

## Multipart form data

Multipart form data request body can be bound by defining a body parameter of type `Mono<WebPart>` if one part is expected, `Flux<WebPart>` if multiple parts are expected or more broadly of type `Publisher<WebPart>`.

We can then rewrite the example described in [Web server exchange documentation](#) as follows:

```

@WebRoute( path = "/bulk", method = Method.POST, consumes = MediaType.MULTIPART_FORM_DATA)
Flux<Result> createBulk(@Body Flux<WebPart> parts) {
    return parts
        .flatMap(part -> part.decoder(Book.class).one())
        .map(book -> storeBook(book));
}

```

It is not possible to bind particular parts to a route method parameter. This design choice has been motivated by performance and resource consumption considerations. Indeed, this would require to consume and store the entire request body in memory before invoking the method. As a result, multipart data must still be handled *manually* using and processed in sequence (i.e. a part must be fully consumed before we can consume the next one).

## Response body

The response body is specified by the return type of the route method.

```

@WebRoute(path =("/{id}", method = Method.GET, produces = MediaType.APPLICATION_JSON)
Book get(@PathParam String id);

```

As for the request body, the response body can be reactive if specified as a `Mono<T>`, a `Flux<T>` or more broadly as a `Publisher<T>`:

```

@WebRoute(path =("/{id}", method = Method.GET, produces = MediaType.APPLICATION_JSON)
Mono<Book> get(@PathParam String id);

```

Depending on the media type converter, partial responses can be sent to the client as soon as they are complete. For instance a stream of responses can be sent to a client as follows:

```

@WebRoute(path = "/", method = Method.GET, produces = MediaType.APPLICATION_X_NDJSON)
Publisher<Book> list();

```

In the preceding example, as soon as a book is retrieved from a data store it can be sent to the client which can then process responses as soon as possible reducing the latency and resource consumption on both client and server. The response content type is `application/x-ndjson`, so each book is encoded in JSON before a newline delimiter to let the client detects partial responses as defined by [the ndjon format](#).

### Server-sent events

[Server-sent events](#) can be streamed in the response body when declared together with a server-sent event factory route method parameter. A server-sent event factory can be bound to a route method parameter using the `@SseEventFactory` annotation.

In the following example, we declare a basic server-sent events Web route producing events with a `String` message:

```

@WebRoute(path = "/event", method = Method.GET)
Publisher<WebResponseBody.SseEncoder.Event<String>> getBookEvents(@SseEventFactory
WebResponseBody.SseEncoder.EventFactory<String> events);

```



Server-sent event return type can be any of `Mono<WebResponseBody.SseEncoder.Event<T>>` if only one event is expected, `Flux<WebResponseBody.SseEncoder.Event<T>>` if multiple events are expected or more broadly `Publisher<WebResponseBody.SseEncoder.Event<T>>`.

By default, the media type of a server-sent event message is `text/plain` but it can be encoded using a specific media type converter as well by specifying a media type in the `@SseEventFactory` annotation.

We can rewrite previous example with messages of a custom type serialized in JSON as follows:

```
@WebRoute(path = "/event", method = Method.GET)
public Publisher<WebResponseBody.SseEncoder.Event<BookEvent>>
getBookEvents(@SseEventFactory(MediaType.APPLICATION_JSON)
WebResponseBody.SseEncoder.EventFactory<BookEvent> events) {
    return Flux.interval(Duration.ofSeconds(1))
        .map(seq -> events.create(
            event -> event
                .id(Long.toString(seq))
                .event("bookEvent")
                .value(new BookEvent("some book event"))
        ))
    );
}
```

## Declarative WebSocket route

Just like Web route, a WebSocket route can be declared using the `@WebSocketRoute` annotation with slightly different semantic and bindings. A WebSocket exchange is essentially defined by an inbound stream of messages and an outbound stream of messages.

WebSocket routes are defined as methods in a Web controller with the following rules:

- The WebSocket `Web2SocketExchange.Inbound` may be injected as method parameter.
- The WebSocket inbound may be injected as method parameter as a `Mono<T>`, a `Flux<T>` or more broadly as a `Publisher<T>`. When defined that way, the `Web2SocketExchange.Inbound` can not be injected as method parameter.
- The WebSocket `Web2SocketExchange.Outbound` may be injected as method parameter and if so the method must be `void`.
- The WebSocket `Web2SocketExchange.Outbound` may be specified as method's return type as a `Mono<T>`, a `Flux<T>` or more broadly as a `Publisher<T>` which closes the WebSocket when it terminates. When defined that way, the `Web2SocketExchange.Outbound` can not be injected as method parameter.
- The `Web2SocketExchange` may always be injected as method parameter.
- The exchange context may always be injected as method parameter just like for regular Web routes.

## Routing rules

WebSocket routing rules, as defined in the [Web routing API](#), are specified in a single `@WebSocketRoute` annotation on a Web controller method. It allows to define paths, produced languages, supported subprotocols and the message type consumed and produced by the WebSocket routes that route a matching request to the handler implemented by the method.

A basic WebSocket route consuming and producing JSON text messages can be declared as follows:

```
@WebSocketRoute( path = "/chat", subprotocol = { "json" } )
Flux<Message> chat(Flux<Message> inbound);
```

Note that this exactly corresponds to the [Web routing API](#).

## Contextual parameters

The `Web2SocketExchange` and the exchange context can be injected in the WebSocket route handler method just as for a regular [Web route](#).

```
@WebSocketRoute( path = "/chat", subprotocol = { "json" } )
Flux<Message> chat(Flux<Message> inbound, Web2SocketExchange<? extends ExchangeContext>
webSocketExchange);

@WebSocketRoute( path = "/chat", subprotocol = { "json" } )
<E extends SecurityContext & ChatContext> Flux<Message> chat(Flux<Message> inbound, E context);
```

## WebSocket inbound

The WebSocket inbound can be specified as method parameter in two ways, either by injecting the `Web2SocketExchange.Inbound` or by injecting a `Mono<T>`, a `Flux<T>` or more broadly as a `Publisher<T>`.

When specified as `Web2SocketExchange.Inbound` parameter, inbound frames or messages can be consumed as defined in the [Web Routing API documentation](#):

```
@WebSocketRoute( path = "/ws" )
public void webSocket(Web2SocketExchange.Inbound inbound) {
    Flux.from(inbound.messages()).flatMap(WebSocketMessage::reducedText).subscribe(LOGGER::info);
}
```

When specified as a `Publisher<T>` parameter, `<T>` can be basically a `ByteBuf`, a `String` or any types that can be converted using a converter matching the negotiated subprotocol.

For instance, raw inbound messages can be consumed as follows:

```

@WebSocketRoute( path = "/ws" )
public void websocket(Flux<ByteBuf> inbound) {
    inbound.subscribe(message -> {
        try {
            LOGGER.info(message.toString(Charsets.DEFAULT));
        }
        finally {
            // ByteBuf must be released where they are consumed
            message.release();
        }
    });
}

```

It is also possible to consume raw frame data composing inbound messages as follows:

```

@WebSocketRoute( path = "/ws" )
public void websocket(Flux<Flux<ByteBuf>> inbound) {

    inbound
        .doOnNext(message -> LOGGER.info("Message start"))
        .flatMap(message -> message.doOnComplete(() -> LOGGER.info("Message end")))
        .subscribe(message -> {
            try {
                LOGGER.info(message.toString(Charsets.DEFAULT));
            }
            finally {
                // ByteBuf must be released where they are consumed
                message.release();
            }
        });
}

```

Finally, inbound messages can also be automatically decoded using a converter matching the subprotocol negotiated during the opening handshake:

```

@WebSocketRoute( path = "/ws", subprotocol = { "json" } )
public void websocket(Flux<Message> inbound) {
    inbound.subscribe(message -> {
        LOGGER.info(message.getNickname() + ": " + message.getMessage());
    });
}

```

## WebSocket outbound

The WebSocket outbound can be specified in two ways, either as method parameter by injecting the `Web2SocketExchange.Outbound` or as method's return type as a `Mono<T>`, a `Flux<T>` or more broadly as a `Publisher<T>`.

When specified as `Web2SocketExchange.Outbound`, outbound frames or messages can be provided as defined in the [Web Routing API documentation](#):

```

@WebSocketRoute( path = "/ws" )
public void websocket(Web2SocketExchange.Outbound outbound) {
    outbound.messages(factory -> Flux.interval(Duration.ofSeconds(1)).map(ign ->
        factory.text(ZonedDateTime.now().toString())));
}

```

When specified as method's return type as a `Publisher<T>`, `<T>` can be basically a `ByteBuf`, a `String` or any types that can be converted using a converter matching the negotiated subprotocol.

For instance, `String` outbound messages can be provided as follows:

```
@WebSocketRoute( path = "/ws" )
public Flux<String> websocket() {
    return Flux.just("message 1", "message 2", "message 3");
}
```

It is also possible to produce fragmented raw messages as follows:

```
@WebSocketRoute( path = "/ws" )
public Flux<Flux<ByteBuf>> websocket() {
    return Flux.just(
        Flux.just(
            Unpooled.unreleasableBuffer(Unpooled.copiedBuffer("message", Charsets.DEFAULT)),
            Unpooled.unreleasableBuffer(Unpooled.copiedBuffer(" 1", Charsets.DEFAULT))
        ),
        Flux.just(
            Unpooled.unreleasableBuffer(Unpooled.copiedBuffer("message ", Charsets.DEFAULT)),
            Unpooled.unreleasableBuffer(Unpooled.copiedBuffer(" 2", Charsets.DEFAULT))
        ),
        Flux.just(
            Unpooled.unreleasableBuffer(Unpooled.copiedBuffer("message ", Charsets.DEFAULT)),
            Unpooled.unreleasableBuffer(Unpooled.copiedBuffer(" 3", Charsets.DEFAULT))
        )
    );
}
```

Finally, outbound messages can be automatically encoded using a converter matching the subprotocol negotiated during the opening handshake:

```
@WebSocketRoute( path = "/ws", subprotocol = { "json" } )
public Flux<Message> websocket() {
    return Flux.just(
        new Message("john", "message 1"),
        new Message("bob", "message 2"),
        new Message("alice", "message 3")
    );
}
```

Putting it all together, the [simple chat server](#) can be simply implemented as follows:

```

package io.inverno.example.app_web_websocket;

import io.inverno.core.annotation.Bean;
import io.inverno.core.annotation.Destroy;
import io.inverno.core.annotation.Init;
import io.inverno.example.app_web_websocket.dto.Message;
import io.inverno.mod.web.annotation.WebController;
import io.inverno.mod.web.annotation.WebSocketRoute;
import reactor.core.publisher.Flux;
import reactor.core.publisher.Sinks;

@Bean
@WebController
public class App_web_websocketWebController {

    private Sinks.Many<Message> chatSink;

    @Init
    public void init() {
        this.chatSink = Sinks.many().multicast().onBackpressureBuffer(16, false);
    }

    @Destroy
    public void destroy() {
        this.chatSink.tryEmitComplete();
    }

    @WebSocketRoute(path = "/ws", subprotocol = "json")
    public Flux<Message> ws2(Flux<Message> inbound) {
        inbound.subscribe(message -> this.chatSink.tryEmitNext(message));
        return this.chatSink.asFlux();
    }
}

```

## Composite Web module

The Web Inverno compiler plugin generates a single Web server controller configurer bean aggregating all route definitions and context types specified in Web configurers or Web controllers beans in the module. When a module composes the *web* module, this bean is then wired to the *web* module to configure the Web server controller.

Now when a module doesn't compose the *web* module, the Web router configurer bean is simply exposed by the module waiting for the module to be composed within other modules until a top module eventually composes the *web* module.

This raises two issues:

- First if multiple Web modules are composed together with the *web* module, dependency injection conflicts will be reported since multiple Web server controller configurer beans can be wired to the *web* module.
- Then if such module is composed in another module defining other Web controllers, we still need to expose one Web router configurer providing all route definitions to a top module composing the *web* module.

Hopefully, the `WebServerControllerConfigurer` interface extends `WebRouterConfigurer` and `ErrorWebRouterConfigurer` which are automatically aggregated in a generated Web server controller configurer bean by the Inverno Web compiler plugin. Then all we have to do to compose Web modules is to explicitly wire the top `WebServerControllerConfigurer` bean to the *web* module.

A generated Web server controller configurer is always annotated with a `@WebRoutes` annotation specifying the Web routes it configures. For instance, the configurer generated for the module defining the book Web controller looks like:

```
@WebRoutes({
    @WebRoute(path = { "/book/{id}" }, method = { Method.GET }, produces = { "application/json"
    }),
    @WebRoute(path = { "/book" }, method = { Method.POST }, consumes = { "application/json" }),
    @WebRoute(path = { "/book/{id}" }, method = { Method.PUT }, consumes = { "application/json"
    }),
    @WebRoute(path = { "/book" }, method = { Method.GET }, produces = { "application/json" }),
    @WebRoute(path = { "/book/{id}" }, method = { Method.DELETE })
})
@Bean( name = "webServerControllerConfigurer" )
@Generated(value="io.inverno.mod.web.compiler.internal.WebServerControllerConfigurerCompilerPlugin",
    date = "2022-07-20T14:10:14.100988902+02:00[Europe/Paris]")
public final class App_web_WebServerControllerConfigurer implements
WebServerControllerConfigurer<App_web_WebServerControllerConfigurer.Context> {
    ...
}
```

These information are used by the compiler plugin to statically check that there is no conflicting routes when generating the Web server controller configurer. It is a good practice to explicitly define the `@WebRoutes` annotation when defining routes programmatically in a Web configurer, otherwise the compiler can not determine conflict as it does not know the actual routes configured.

Now let's imagine we have created a modular Web application with a *book* module defining the book Web controller, an *admin* module defining some admin Web controllers and a top *app* module composing these modules together with the *web* module.

The module descriptors for each of these modules should look like:

```
@io.inverno.core.annotation.Module( excludes = { "io.inverno.mod.web" } )
module io.inverno.example.web_modular.admin {
    requires io.inverno.core;
    requires io.inverno.mod.web;

    exports io.inverno.example.web_modular.admin to io.inverno.example.web_modular.app;
}

@io.inverno.core.annotation.Module( excludes = { "io.inverno.mod.web" } )
module io.inverno.example.web_modular.book {
    requires io.inverno.core;
    requires io.inverno.mod.web;

    exports io.inverno.example.web_modular.book to io.inverno.example.web_modular.app;
    exports io.inverno.example.web_modular.book.dto to com.fasterxml.jackson.databind;
}
```

```
@io.inverno.core.annotation.Module
module io.inverno.example.web_modular.app {
    requires io.inverno.mod.boot;
    requires io.inverno.mod.web;

    requires io.inverno.example.web_modular.admin;
    requires io.inverno.example.web_modular.book;
}
```

The first thing to notice is that the *web* module is excluded from *admin* and *book* modules since we don't want to start a Web server in these modules, we only need the Web routing API to define Web controllers and generate Web server controller configurer beans. As a consequence, the *boot* module which provides converters and net service required to create and start the *web* module is also not required but the *io.inverno.core* module is still required. Finally we must export packages containing the generated module classes to the *app* module so it can compose them.

The *admin* and *book* modules should compile just fine resulting in two Web server controller configurer beans being generated and exposed in each module. But the compilation of *app* module should raise some dependency injection errors since multiple Web server controller configurer beans exist whereas only one can be wired to the *web* module. There are actually three Web server controller configurer beans, how so? There are those exposed by the *admin* and *book* modules and one generated in the *app* module and aggregating the previous two. In order to solve the conflict, we should then define the following explicit wire in the *app* module:

```
@io.inverno.core.annotation.Module
@io.inverno.core.annotation.Wire(beans="io.inverno.example.web_modular.app:webServerControllerConfigurer", into="io.inverno.mod.web:controllerConfigurer")
module io.inverno.example.web_modular.app {
    ...
}
```

One could rightfully argue that this explicit wiring is useless and cumbersome, but it is consistent with the IoC/DI core framework principles. Keeping things simple and explicit limits possible side effects induced by the fact that what's happening with *automatic* conflict resolution is often specific and might not be obvious. This is all the more true when such behavior is manually overridden.

The same principles applies if multiple modules like *admin* or *book* are cascaded into one another: Web server controller configurer beans at a given level are aggregated in the Web server controller configurer bean in the next level.

## Automatic OpenAPI specifications

Besides facilitating the development of REST and Web resources in general, Web controllers also simplify documentation. The Web Inverno compiler plugin can be setup to generate [Open API](#) specifications from the Web controller classes defined in a module and their JavaDoc comments.

Writing JavaDoc comments is something natural when developing in the Java language, with this approach, a REST API can be documented just as you document a Java class or method, documentation is written once and can be used in both Java and other languages and technologies using the generated Open API specification.

In order to activate this feature the `inverno.web.generateOpenApiDefinition` annotation processor option must be enabled when compiling a Web module. This can be done on the command line: `java -Ainverno.web.generateOpenApiDefinition=true ...` or in the Maven compiler plugin configuration in the build descriptor:

```
<project>
  <build>
    <pluginManagement>
      <plugins>
        <plugin>
          <groupId>org.apache.maven.plugins</groupId>
          <artifactId>maven-compiler-plugin</artifactId>
          <configuration>
            <compilerArgs combine.children="append">
              <arg>-Ainverno.web.generateOpenApiDefinition=true</arg>
            </compilerArgs>
          </configuration>
        </plugin>
      </plugins>
    </pluginManagement>
  </build>
</project>
```

The compiler then generates an Open API specification in `META-INF/inverno/web/openapi.yml` for any module defining one or more Web controllers.

The previous [book resource](#) could then be documented as follows:



```

/**
 * The book resource.
 */
@Bean
@WebController(path = "/book")
public class BookResource {

    /**
     * Creates a book resource.
     *
     * @param book a book
     * @param exchange the web exchange
     *
     * @return the book resource has been successfully created
     * @throws BadRequestException A book with the same ISBN reference already exist
     */
    @WebRoute(method = Method.POST, consumes = MediaType.APPLICATION_JSON)
    public Mono<Void> create(@Body Mono<Book> book, WebExchange exchange) throws BadRequestException
    { ... }

    /**
     * Updates a book resource.
     *
     * @param isbn the reference of the book resource to update
     * @param book the updated book resource
     *
     * @return the book resource has been successfully updated
     * @throws NotFoundException if the specified reference does not exist
     */
    @WebRoute(path =("/{isbn}", method = Method.PUT, consumes = MediaType.APPLICATION_JSON)
    public Mono<Void> update(@PathParam String isbn, @Body Mono<Book> book) throws NotFoundException
    { ... }

    /**
     * Returns the list of book resources.
     *
     * @return a list of book resources
     */
    @WebRoute(method = Method.GET, produces = MediaType.APPLICATION_JSON)
    public Flux<Book> list();

    /**
     * Returns the book resource identified by the specified ISBN.
     *
     * @param isbn an ISBN
     *
     * @return the requested book resource
     * @throws NotFoundException if the specified reference does not exist
     */
    @WebRoute(path =("/{isbn}", method = Method.GET, produces = MediaType.APPLICATION_JSON)
    public Mono<Book> get(@PathParam String isbn) throws NotFoundException { ... }

    /**
     * Deletes the book resource identified by the specified ISBN.
     *
     * @param isbn an ISBN
     *
     * @return the book resource has been successfully deleted

```

```

    * @throws NotFoundException if the specified reference does not exist
    */
    @WebRoute(path = "{isbn}", method = Method.DELETE)
    public Mono<Void> delete(@PathParam String isbn) { ... }
}

```

Note that just like the `javadoc` tool, the Web compiler plugin takes inheritance into account when resolving JavaDoc comments and as a result, it is possible to define JavaDoc comments in an interface and enrich or override them in the implementation classes.

By default, the normal HTTP status code responded by a route is assumed to be `200` but it is possible to specify a custom status code using the `@inverno.web.status` tag. For instance the book creation route which actually responds with a `201` status should be documented as follows:

```

public class BookResource {

    /**
     * Creates a book resource.
     *
     * @param book a book
     * @param exchange the web exchange
     *
     * @return {@@inverno.web.status 201} the book resource has been successfully created
     * @throws BadRequestException A book with the same ISBN reference already exist
     */
    @WebRoute(method = Method.POST, consumes = MediaType.APPLICATION_JSON)
    public Mono<Void> create(@Body Mono<Book> book, WebExchange exchange) throws BadRequestException
    { ... }

    ...
}

```

Multiple `@return` statements can be specified if multiple response statuses are expected, however this might raise issues during the generation of the JavaDoc, you can bypass this by disabling the linter with `-Xdoclint:none` option.

This tag can also be used to specify error status code in `@throws` statements, but this is usually not necessary since the Web compiler plugin automatically detects status code for regular `HttpException` such as `BadRequestException` (400) or `NotFoundException` (404).

The Web compiler plugin generates, per module, one Open API specification and one Web server controller configurator bean aggregating all routes from all Web controllers and Web configurers. As a result the general API documentation corresponds to the general documentation of the module which is defined in the module descriptor JavaDoc comment.

For instance, we can describe the API exposed by the *book* module in the module descriptor including the API version which should normally match the module version:

```

/**
 * This is a sample Book API which demonstrates Inverno Web module capabilities.
 *
 * @author <a href="mailto:jeremy.kuhn@inverno.io">Jeremy Kuhn</a>
 *
 * @version 1.2.3
 */
@io.inverno.core.annotation.Module( excludes = { "io.inverno.mod.web" } )
module io.inverno.example.web_modular.book {
    requires io.inverno.core;
    requires io.inverno.mod.web;

    exports io.inverno.example.web_modular.book to io.inverno.example.web_modular.app;
    exports io.inverno.example.web_modular.book.dto to com.fasterxml.jackson.databind;
}

```

These specifications can also be exposed in the Web server using the [OpenApiRoutesConfigurer](#) as described in the [Web server documentation](#).

If we build and run the [modular book application](#) and access <http://localhost:8080/open-api> in a Web browser we should see a Swagger UI loaded with the Open API specifications of the *admin* and *book* modules:

The screenshot displays the Swagger UI for the **io.inverno.example.web\_modular.book** API. At the top, there's a header with the Swagger logo and a dropdown menu showing the selected definition: `io.inverno.example.web_modular.book`. Below the header, the API title **io.inverno.example.web\_modular.book** is prominently displayed, followed by the version **1.2.3** and the specification type **OAS3**. A brief description states: "This is a sample Book API which demonstrates Inverno Web module capabilities." and provides a contact link for Jeremy Kuhn.

The main section, titled **bookResource** (The book resource.), lists five endpoints:

- POST** `/book`: Creates a book resource.
- GET** `/book`: Returns the list of book resources.
- GET** `/book/{isbn}`: Returns the book resource identified by the specified ISBN.
- PUT** `/book/{isbn}`: Updates a book resource.
- DELETE** `/book/{isbn}`: Deletes the book resource identified by the specified ISBN.

At the bottom, there is a section for **Schemas** with a right-pointing arrow.

It is also possible to target a single specification by specifying the module name in the URI, for instance [http://localhost:8080/open-api/io.inverno.example.web\\_modular.book](http://localhost:8080/open-api/io.inverno.example.web_modular.book):

# io.inverno.example.web\_modular.book 1.2.3 OAS3

[/open-api/io.inverno.example.web\\_modular.book](/open-api/io.inverno.example.web_modular.book)

This is a sample Book API which demonstrates Inverno Web module capabilities.

[Contact Jeremy Kuhn](#)

## bookResource The book resource.

**POST** **/book** Creates a book resource.

**GET** **/book** Returns the list of book resources.

**GET** **/book/{isbn}** Returns the book resource identified by the specified ISBN.

**PUT** **/book/{isbn}** Updates a book resource.

**DELETE** **/book/{isbn}** Deletes the book resource identified by the specified ISBN.

Schemas



Finally, Open API specifications formatted in [YAML](#) can be retrieved as follows:

```
$ curl http://localhost:8080/open-api/io.inverno.example.web_modular.admin
```

```
openapi: 3.0.3
info:
  title: 'io.inverno.example.web_modular.admin'
  version: ''
...
```

## Reactive Template

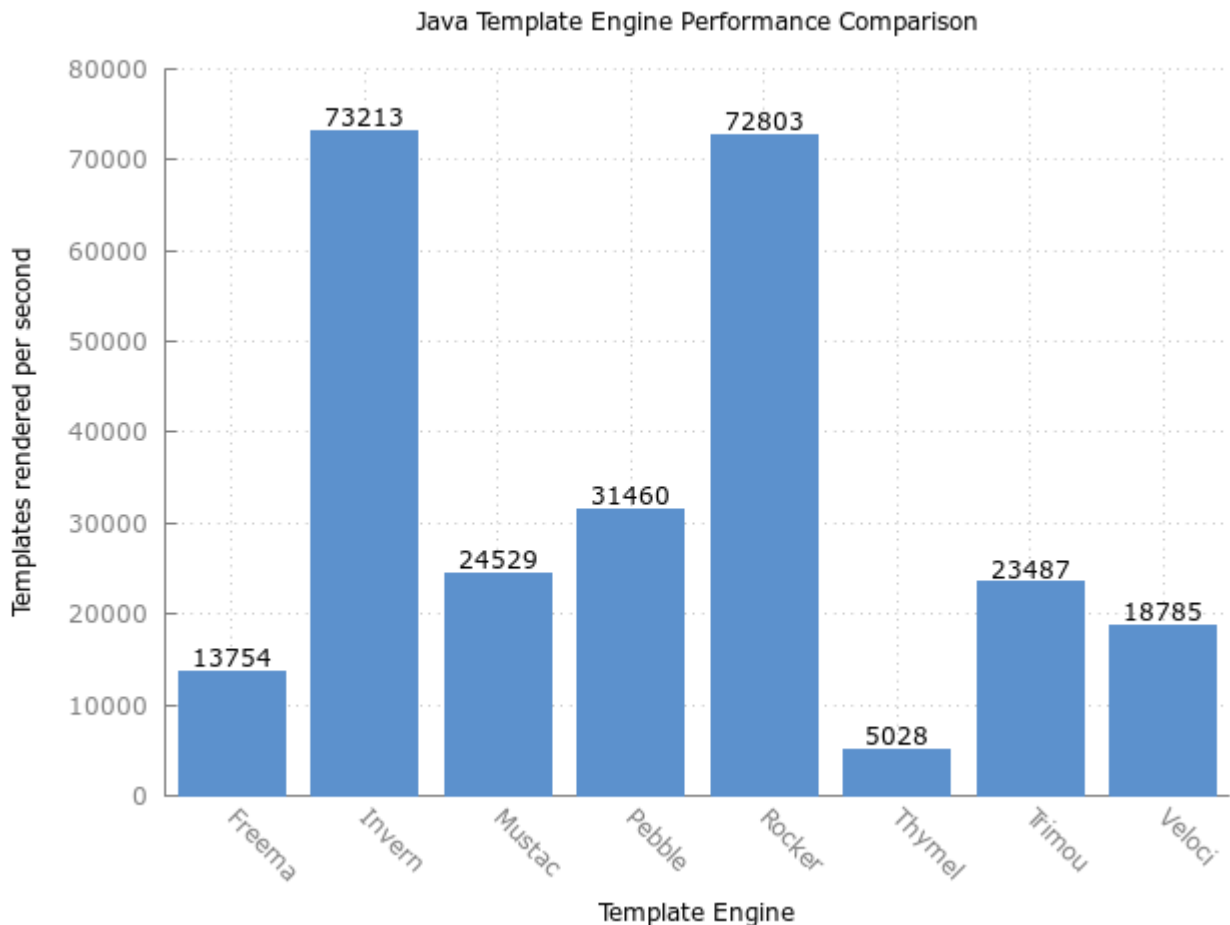
The Inverno *irt* module provides a template engine for efficient reactive data rendering.

Data are basically rendered by templates which are regrouped in template sets and applied based on the type of data to render. A template set is statically typed and generated by an Inverno compiler plugin which compiles *.irt* template set source files along with the Java sources of a module.

The template sets classes thus obtained support reactive rendering, data are rendered as a flow of events for efficient usage of resources. For instance, the complete set of data doesn't have to be available or loaded into memory, the rendering being reactive the output can be generated incrementally by processing each piece of data individually one after the other when they become available. Since the rendering process never blocks it is also possible to lazily load data when/if they need to be rendered.

The syntax of `.irt` template set is inspired from functional language such as [XSLT](#) and [Erlang](#) which are particularly suited for reactive rendering. Since a template is a generated Java class, the Java language is also widely used in a template source file, especially for the dynamic parts of a template.

In terms of raw performance, Inverno templates processing is faster than most Java template engines by an order of magnitude and with lower memory usage. The following [benchmark project](#) compares performances of various template engines rendering a list of stock items into an HTML document as a String.



Please keep in mind that outcomes might be different considering different scenarios, especially reactive rendering which might appear slower but addresses different concerns such as stream processing and optimized usage of resources.

In order to use the Inverno `irt` module, we need to declare a dependency in the module descriptor:

```
module io.inverno.example.app {  
    ...  
    requires io.inverno.mod.irt;  
    ...  
}
```

And also declare that dependency in the build descriptor:

Using Maven:

```
<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-irt</artifactId>
    </dependency>
  </dependencies>
</project>
```

Using Gradle:

```
...
compile 'io.inverno.mod:inverno-irt:1.5.3'
...
```

Dependencies to `io.netty.common` and `io.netty.buffer` are also required when using `BYTEBUF` or `PUBLISHER_BYTEBUF` [modes](#) which require Netty's `ByteBuf`. They are defined as optional in the `irt` module and won't be included by default. In order to use `ByteBuf` based generation modes, the following dependencies must be declared as well in the module descriptor:

```
module io.inverno.example.app {
  ...
  requires io.netty.common;
  requires transitive io.netty.buffer;
  ...
}
```

And the corresponding dependency to `io.netty:netty-buffer` must be declared in the the build descriptor:

Using Maven:

```
<project>
  <dependencies>
    <dependency>
      <groupId>io.netty</groupId>
      <artifactId>netty-buffer</artifactId>
    </dependency>
  </dependencies>
</project>
```

Using Gradle:

```
...
compile 'io.netty:netty-buffer:4.1.79.Final'
...
```

## Creates an .irt template

A template can be created along with other Java source files in the source directory of an Inverno module. At compile time, the Inverno reactive template compiler plugin will scan the module source folder for `.irt` files and compiles them to generate template set classes that can be used in your module to render data.

The following `Simple.irt` template set is a simple example containing one template that renders a `Message` object as String:

```
package io.inverno.example.app_irt.templates;

import io.inverno.example.app_irt.model.Message;

option modes = {"STRING"};
option charset = "utf-8";

(Message message) -> {The message is: {@message.message}}

package io.inverno.example.app_irt.model;

public class Message {

    private final String message;

    private final boolean important;

    public Message(String message, boolean important) {
        this.message = message;
        this.important = important;
    }

    public String getMessage() {
        return message;
    }

    public boolean isImportant() {
        return important;
    }
}
```

As for any Java source file, the preceding template source must be created in the same package as the one it declares in a module source folder. The name of the template corresponds to the name of the file.

After compiling the module, a new Java class `Simple.java` should have been created in the generated source folder in package `io.inverno.example.app_irt.templates`.

A `Message` object can then be rendered as follows:

```
CompletableFuture<String> rendered = Simple.string().render(new Message("Hello, world!"));
System.out.println(rendered.get()); // The message is: Hello, world!
```

# .irt syntax

## Package and imports

An `.irt` template always starts with the declaration of the Java package containing the template, followed by the list of imported Java types or static methods used within the template. This is exactly the same as any Java source file.

```
package io.inverno.example.app_irt.templates;

import io.inverno.example.app_irt.model.Message;
...
```

## Includes

Then you can specify external template sets to include in the template set using the `include` keyword. This allows to include templates from an external template set in a template set using the same precedence. For instance, in the following example, template set `io.inverno.example.app_irt.templates.Misc` is included in the template set which means that its templates can be applied in the including template.

```
include io.inverno.example.app_irt.templates.Misc;
```

Note that this can lead to conflicts when two included templates defines a template using the same signature (same name and same input parameters), such conflict can be resolved by explicitly overriding the conflicting template in the including template set.

## Options

Rendering options are specified after that using the `option` keyword. You can for instance declare the charset to use for rendering which defaults to `utf-8` if not specified:

```
option charset = "utf-8";
```

or the template rendering modes supported by the generated template set. There are five template rendering modes, you can choose to specify one or more modes depending on your needs:

- **STRING** to expose methods to render data in a `String`, this is the default behavior
- **BYTEBUF** to expose methods to render data in a `ByteBuf`
- **STREAM** to expose methods to render data in an `OutputStream`
- **PUBLISHER\_STRING** to expose methods to render data in a `Publisher<String>`
- **PUBLISHER\_BYTEBUF** to expose methods to render data in a `Publisher<ByteBuf>`

The last two modes are particularly suitable for reactive rendering.

```
option modes = {"STRING", "STREAM", "PUBLISHER_STRING"};
```



# Templates

Templates are specified last. A template is a function that defines how a particular input must be rendered, a template can have a name in which case it is referred as a named template. In a template set, there can't be two templates with the same signature (ie. defining the same input parameters) unless they have different names.

A template is declared as follows:

```
(Message message) -> {...}
```

A named template is declared as follows:

```
name(Message message) -> {...}
```

A template can be defined with zero or more parameters. No parameter templates can be useful to create static templates such as headers or footers, they are usually named:

```
header() -> {...}
```

The body of a template is a combination of static content and statements which define how the template input should be rendered. Template statements are specified within braces `{...}` which must be escaped within static content using `\`.

A template can also be specified without a body in order to create aliases or resolve conflicts.

For instance the following template defines alias `apple` for template `fruit` (assuming `Apple` is an instance of `Fruit`):

```
apple(Apple fruit) -> this::fruit
fruit(Fruit fruit) -> {...}
```

And the following template resolves a conflict induced by the inclusion of template set `Include1` and `Include2` which both defines template `conflicting` with the same input parameters:

```
...
include io.inverno.example.app_irt.templates.Include1;
include io.inverno.example.app_irt.templates.Include2;
...

conflicting(String input) -> Include1
```

## Static content

Static contents are specified directly in the template body and are rendered as is:

```
(...) -> {
This is a static content, braces: \{ and \} must be escaped.
}
```

## Comment

The syntax supports two kinds of comments which can be either outside or inside the body of a template.

Outside the body of a template, comments are regular Java comments:

```
/*
 * This a comment to explain that the following import is commented
 */
// import java.util.List;
```

Inside the body of a template, comments are statements starting with `{%` and ending with `}`:

```
(Message message) -> {
Hello {% this is a comment} World.
}
```

## Value of

A value can be rendered directly in a synchronous way within a statement starting with `{@` and ending with `}` as follows:

```
(Message message) -> {
The message is: {@message.message}
}
```

In the preceding example, we used a syntactic sugar to navigate into the message object hierarchy and access the `message` properties but it is also possible to evaluate a raw Java expression specified between `(` and `)` to get the same result:

```
(Message message) -> {
The message is: {@(message.getMessage())}
}
```

It is then possible to evaluate any Java expression:

```
(Message message) -> {
The message is: {@(5+8)}
}
```

Note that this can be dangerous when you the origin of a template set can't be trusted.

## If

An if statement can be used to render different contents based on one or more conditions. An if statement starts with `{@if` and ends with `}`, it contains one or more branches separated by `;` defining a condition and a corresponding body, a default branch with an empty condition can be specified last. Each condition is specified as a raw Java if expression between `(` and `)`:

```

(Message message, String lang) -> {
    @if
    (lang.equals("fr")) -> {
        Le message est: {@message.message}
    };
    (lang.equals("de")) -> {
        Die Nachricht ist: {@message.message}
    };
    () -> {
        The message is: {@message.message}
    }
}

```

## Apply template

Templates can be applied on data using an apply template statement starting with `{` and ending with `}`. The template to apply is selected among the ones available in the template set based on the type of data to render following Java's rules for function overloading.

As for the value of statement, it is possible to use a syntactic sugar notation or a raw Java expression between `(` and `)` to select the data on which a template should be applied. A template set provides a default template for object which simply renders the `toString()` representation of the input. Considering previous examples, the content of a message object can then also be rendered as follows:

```

(Message message) -> {
    The message is: {message.message}
}

```

Unlike the value of statement which renders data synchronously, applying a template can be an asynchronous operation depending on the type of data to render. Indeed when the data to render is an array, an `Iterable`, a `Stream` or a `Publisher`, the template is applied on each element and in the case of a `Publisher` the operation is reactive, non-blocking and therefore asynchronous.

For instance, a list of messages can be rendered synchronously as follows:

```

(List<Message> messages) -> {
    Messages are:
    {messages}
}

(Message message) -> {@message.message}
}

```

resulting in:

```

Messages are:
message 1
message 2
message 3
message 4
message 5
...

```

Now if we consider a `Publisher`, a message is rendered to the output when it is emitted by the publisher following reactive principles.

As you can see the apply template statement is extremely powerful, it is used to render data based on their types which facilitates composition but it can also be used as a for loop statement to render a list of elements.

By default, an apply template statement will select the unnamed template within the template set matching the type of data to render, but it is also possible to select a named templates as follows:

```
(List<Message> messages) -> {
Messages are:
{messages;bullet}
}

(Message message) -> {@message.message}

bullet(Message message) -> {* {@message.message}
}
```

resulting in:

```
Messages are:
* message 1
* message 2
* message 3
* message 4
* message 5
...
```

Extra parameters can also be passed to a template in which case we have to explicitly specify the inputs:

```
(List<Message> messages) -> {
Messages are:
{messages; message -> bullet(message, "-")}
}

bullet(Message message, String marker) -> {@marker} {@message.message}
}
```

resulting in:

```
Messages are:
- message 1
- message 2
- message 3
- message 4
- message 5
...
```

It is also possible to specify guard expressions as raw Java expressions and choose to apply different templates based on certain conditions. For instance, let's say we want to render important messages in a specific way, we can do as follows:

```
(List<Message> messages) -> {
Messages are:
{messages;(message) -> important(message) when (message.isImportant());(message)}
}

(Message message) -> {@message.message}

important(Message message) -> {**{@message.message}**
}
```

In the previous example, the **important** template is applied when a message is important and the unnamed template is applied otherwise. Assuming message 3 is important, this will result in:

```
Messages are:
- message 1
- message 2
- **message 3**
- message 4
- message 5
...
```

The index of an item in a list is made available when selecting the target template. For instance, a numbered list of messages can be rendered as follows:

```
(List<Message> messages) -> {
Messages are:
{messages;(index, message) -> (index, message)}
}

(long index, Message message) -> {@index}. {@message.message}
}
```

resulting in:

```
Messages are:
0. message 1
1. message 2
2. message 3
3. message 4
4. message 5
...
```

A no-arg named template can be applied by omitting the data part in the statement:

```
(Message message) -> {
    {;header}
    The message is: {@message.message}
    {;footer}
}

header() -> {==== HEADER ====
}

footer() -> {==== FOOTER ====
}
```

resulting in:

```
==== HEADER ====
The message is: {@message.message}
==== FOOTER ====
```

## Pipes

A pipe can be used to transform data before they are rendered or before a template is applied, as a result they can be specified in value of and apply template statements. In practice, a pipe is a simple function that accepts a data and transform it into another data. Pipes can be chained to sequentially apply multiple transformations.

A pipe can be specified as a lambda expression and applied using a `|` in a value of or apply template statement as follows:

```
(Message message) -> {
The message is: {@message.message|((String content) -> content.toUpperCase())}
}
```

Lambdas are handy when there's a need for very specific pipes, however the recommended way to create pipes is to define them in Java as static methods returning the `Pipe` implementation in order to keep the template readable. Above pipe can be defined in a Java class as follows:

```
package io.inverno.example.app_irt.pipes;

import io.inverno.mod.irt.Pipe;

public final class SamplePipes {

    public static Pipe<String, String> uppercase() {
        return String::toUpperCase;
    }
}
```

We can then statically import that class in the template set and simplify above example:

```
import static io.inverno.example.app_irt.pipes.SamplePipes.*;

(Message message) -> {
    The message is: {@message.message|uppercase}
}
```

Several built-in pipes are provided in the module in the `Pipes`, `StreamPipes` and `PublisherPipes` classes. The `Pipes` class provides pipes used to transform simple data object before rendering such as strings, dates and numbers. The `StreamPipes` and `PublisherPipes` provide pipes used to transformed streams and publishers typically in an apply template statement.

For instance the following example sort a list of items and map them to their datetime before applying templates:

```
import static io.inverno.mod.irt.Pipes.*;
import static io.inverno.mod.irt.PublisherPipes.*;

import java.time.format.DateTimeFormatter;

(Publisher<Item> items) -> {
    {items|sort|map(Item::getDateTime)}
}

(ZonedDateTime datetime) -> {
    {@datetime|dateTime(DateTimeFormatter.ISO_DATE_TIME)}
}
```

## Modes

Template set classes are generated by the Inverno reactive template compiler plugin. Depending on the modes specified in the template set options, the resulting class will expose different `render()` methods with different outputs.

## STRING

The **STRING** mode is the default resulting in the generation of `render()` methods that return a `CompletableFuture<String>` which completes once the input data has been fully rendered into the resulting String. For instance, assuming we have created a `Simple.irt` template set containing a template to render `Message` object, we can render a `Message` to a String as follows:

```
String result = Simple.string().render(new Message("some important message", true)).get();
```

The rendering process start as soon as the `render()` method is invoked, the `get()` operation on the resulting `CompletableFuture` waits until the message has been fully rendered. In this particular example, the whole process is synchronous since the input data is available from the start but keep in mind that this might not always be the case especially when `Publisher` objects are rendered in the process.

## BYTEBUF

The **BYTEBUF** has a similar behavior except that data are rendered in a **ByteBuffer**:

```
ByteBuffer result = Simple.bytebuf().render(new Message("some important message", true)).get();
```

It is possible to provide the `ByteBuffer` instance into which data should be rendered by defining a factory:

```
ByteBuffer result = Simple.bytebuf(() -> Unpooled.unreleasableBuffer(Unpooled.buffer())).render(new Message("some important message", true)).get();
```

This can be useful to optimize memory as it allows to reuse `ByteBuffer` instances or specify direct or pooled `ByteBuffer`.

Note that the **BYTEBUF** requires `io.netty.common` and `io.netty.buffer` modules which must be declared explicitly in the module descriptor.

## STREAM

The **STREAM** mode is used to render data in an `OutputStream`:

```
ByteArrayOutputStream result = Simple.stream(() -> new ByteArrayOutputStream()).render(new Message("some important message", true)).get();
```

## PUBLISHER\_\*

Finally the **PUBLISHER\_STRING** and **PUBLISHER\_BYTEBUF** modes are used to generate fully reactive rendering methods which return `Publisher<String>` and `Publisher<ByteBuffer>` respectively. Unlike previous modes, the rendering process starts when a subscription is made on the returned `Publisher` which can emits partial rendering result whenever a partial data is rendered.

```
String result = Flux.from(Simple.publisherString().render(new Message("some important message", true))).collect(Collectors.joining()).block();
```

If you consider small data set and require very high performance, you should prefer non-reactive modes. If your concern is more about resources, considering a large amount of data that you do not want to load into memory at once or progressive rendering you should prefer reactive modes which might have a slight decrease in performance.

Note that the `BYTEBUF` requires `io.netty.common` and `io.netty.buffer` modules which must be declared explicitly in the module descriptor.

## SQL Client

The Inverno SQL client module specifies a reactive API for executing SQL statement on a RDBMS.

This module only exposes the API and a proper implementation module must be considered to obtain `SqlClient` instances.

In order to use the Inverno *SQL client* module, we need to declare a dependency to the API and at least one implementation in the module descriptor:

```
module io.inverno.example.app {
    ...
    requires io.inverno.mod.sql; // this is actually optional since implementations should already
    define a transitive dependency
    requires io.inverno.mod.sql.vertx; // Vert.x implementation
    ...
}
```

And also declare these dependencies in the build descriptor:

Using Maven:

```
<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-sql</artifactId>
    </dependency>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-sql-vertx</artifactId>
    </dependency>
  </dependencies>
</project>
```

Using Gradle:

```
...
compile 'io.inverno.mod:inverno-sql:1.5.3'
compile 'io.inverno.mod:inverno-sql-vertx:1.5.3'
...
```



# SQL client API

The Sql client API defines the `SqlClient` interface which provides reactive methods to execute SQL statements on a RDBMS.

## Query and update

The `SqlClient` extends the `SqlOperations` interface which defines methods for common RDBMS operations such as query or update in addition to the more general statements and prepared statements.

We can query a database as follows:

```
SqlClient client = ...

Flux<Person> persons = Flux.from(
    client.query("SELECT * FROM person")
)
.map(row -> new Person(row.getString("firstname"), row.getString("name"),
row.getLocalDate("birthdate"))); // Map the resulting rows

persons.subscribe(...); // The query is executed on subscribe following reactive principles
```

Prepared queries are also supported:

```
Publisher<Row> results = client.query("SELECT * FROM person WHERE name = $1", "John");
```

A row mapping function can be specified directly in the query as well

```
Publisher<Person> results = client.query(
    "SELECT * FROM person WHERE name = $1",
    row -> new Person(row.getString("firstname"), row.getString("name"),
row.getLocalDate("birthdate")),
    "Smith"
);
```

A single result can also be queried as follows:

```
Mono<Person> person = client.queryForObject( // only consider the first row in the results
    "SELECT * FROM person WHERE name = $1",
    row -> new Person(row.getString("firstname"), row.getString("name"),
row.getLocalDate("birthdate")),
    "Smith"
);
```

The two previous examples are actually optimizations of the first one which enable implementations to optimize the query, resulting in faster execution.

The database can be updated as follows:

```
client.update(
    "UPDATE person SET birthdate = $1 WHERE id = $2",
    LocalDate.of(1970, 1, 1), 123
);
```

It can also be updated in a batch as follows:

```
client.batchUpdate(
    "UPDATE person SET birthdate = $1 WHERE id = $2",
    List.of(
        new Object[]{ LocalDate.of(1970, 1, 1), 123 },
        new Object[]{ LocalDate.of(1980, 1, 1), 456 },
        new Object[]{ LocalDate.of(1990, 1, 1), 789 }
    )
);
```

Note that all these operations use prepared statements which protect against SQL injection attacks.

## Statements

The `SqlClient` also defines methods to create more general statements and prepared statements.

A static statement can be created and executed as follows:

```
SqlClient client = ...

Publisher<SqlResult> results = client.statement("SELECT * FROM person").execute();

// The statement is executed on subscribe following reactive principles
results.subscribe(...);
```

The execution of a statement returns `SqlResult` for each SQL operations in the statement in a publisher.

The `SqlResult` exposes row metadata and depending on the operation type either the number of rows affected by the operation (`UPDATE` or `DELETE`) or the resulting rows (`SELECT`).

Following preceding example:

```
Flux<Person> persons = Flux.from(client.statement("SELECT * FROM person").execute())
    .single() // Make sure we have only one result
    .flatMapMany(SqlResult::rows)
    .map(row -> new Person(row.getString("firstname"), row.getString("name"),
        row.getLocalDate("birthdate")))

persons.subscribe(...);
```

Queries can also be fluently appended to a statement as follows:

```
Publisher<SqlResult> results = client
    .statement("SELECT * FROM person")
    .and("SELECT * FROM city")
    .and("SELECT * FROM country")
    .execute();
```

Unlike prepared statements, static statements are not pre-compiled and do not protect against SQL injection attacks which is why prepared statements should be preferred when there is a need for performance, dynamic or user provided queries.

A prepared statement can be created and executed as follows:

```
SqlClient client = ...
```

```
Publisher<SqlResult> results = client.preparedStatement("SELECT * FROM person WHERE name = $1")
    .bind("Smith") // bind the query argument
    .execute();
```

```
// The statement is executed on subscribe following reactive principles
results.subscribe(...);
```

As for a static statement, a prepared statement returns `SqlResult` for each SQL operations in the statement, however it is not possible to specify multiple operation in a prepared statement. But it is possible to transform it into a batch which will result in multiple operations and therefore multiple `SqlResult`.

In order to create a batch statement, we must bind multiple query arguments as follows:

```
Publisher<SqlResult> results = client.preparedStatement("SELECT * FROM person WHERE name = $1")
    .bind("Smith")           // first query
    .and().bind("Cooper")    // second query
    .and().bind("Johnson")  // third query
    .execute();
```

```
// Returns 3 since we have created a batch statement with three queries
long resultCount = Flux.from(results).count().block();
```

## Transactions

The API provides two ways to execute statement in a transaction which can be managed explicitly or implicitly.

We can choose to manage transaction explicitly by obtaining a `TransactionalSqlOperations` which exposes `commit()` and `rollback()` methods that we must invoke explicitly to close the transaction:

In the following example we perform a common `SELECT/UPDATE` operation within a transaction:

```

SqlClient client = ...

final float debit = 42.00f;
final int accountId = 1;

Mono<Integer> affectedRows = Mono.usingWhen(
    client.transaction(),
    tops -> tops
        .queryForObject("SELECT balance FROM account WHERE id = $1", row -> row.getFloat(0),
accountId)
        .flatMap(balance -> ops
            .update("UPDATE account SET balance = $1 WHERE id = $2", balance - debit, accountId)
            .doOnNext(rowCount -> {
                if(balance - debit < 0) {
                    throw new IllegalStateException();
                }
            })
        )
    ,
    tops -> {
        // Complete
        // extra processing before commit
        // ...

        return tops.commit();
    },
    (tops, ex) -> {
        // Error
        // extra processing before roll back
        // ...

        return tops.rollback();
    },
    tops -> {
        // Cancel
        // extra processing before commit
        // ...

        return tops.rollback();
    }
);

// On subscribe, a transaction is created, the closure method is invoked and the transaction is
explicitly committed or rolled back when the publisher terminates.
affectedRows.subscribe(...);

```

The following example does the same but with implicit transaction management:

```

SqlClient client = ...

final float debit = 42.00f;
final int accountId = 1;

Publisher<Integer> affectedRows = client.transaction(ops -> ops
    .queryForObject("SELECT balance FROM account WHERE id = $1", row -> row.getFloat(0), accountId)
    .flatMap(balance -> ops
        .update("UPDATE account SET balance = $1 WHERE id = $2", balance - debit, accountId)
        .doOnNext(rowCount -> {
            if(balance - debit < 0) {
                throw new IllegalStateException();
            }
        })
    )
);

// Same as before but the transaction is implicitly committed or rolled back
affectedRows.subscribe(...);

```

Note that transactions might not be supported by all implementations, for instance the Vert.x pooled client implementation does not support transactions and an **UnsupportedOperationException** will be thrown if you try to create a transaction.

## Connections

Some **SqlClient** implementations backed by a connection pool for instance can be used to execute multiple SQL statements on a single connection released once the resulting publisher terminates (either closed or returned to the pool).

For instance we can execute multiple statements on a single connection as follows:

```

SqlClient client = ...

final int postId = 1;

client.connection(ops -> ops
    .queryForObject("SELECT likes FROM posts WHERE id = $1", row -> row.getInteger(0), postId)
    .flatMap(likes -> ops.update("UPDATE posts SET likes = $1 WHERE id = $2", likes + 1, postId))
);

```

## Vert.x SQL Client implementation

The Inverno Vert.x SQL client module is an implementation of the SQL client API on top of the [Vert.x Reactive SQL client](#).

It provides multiple **SqlClient** implementations that wrap Vert.x SQL pooled client, pool or connection and exposes a **SqlClient** bean created from the module's configuration and backed by a Vert.x pool. It can be used to execute SQL statements in an application.

In order to use the Inverno *Vert.x SQL client* module, we need to declare a dependency in the module descriptor:

```
module io.inverno.example.app {  
    ...  
    requires io.inverno.mod.sql.vertx;  
    ...  
}
```

And also declare this dependency as well as a dependency to the Vert.x implementation corresponding to the RDBMS we are targeting in the build descriptor:

Using Maven:

```
<project>  
  <dependencies>  
    <dependency>  
      <groupId>io.inverno.mod</groupId>  
      <artifactId>inverno-sql-vertx</artifactId>  
    </dependency>  
    <dependency>  
      <groupId>io.vertx</groupId>  
      <artifactId>vertx-pg-client</artifactId>  
    </dependency>  
  </dependencies>  
</project>
```

Using Gradle:

```
...  
compile 'io.inverno.mod:inverno-sql-vertx:1.5.3'  
compile 'io.vertx:vertx-pg-client:4.1.2'  
...
```

## Configuration

The `VertxSqlClientConfiguration` is used to create and configure the SQL client bean exposed by the module.

Please refer to the [API documentation](#) to have an exhaustive description of the different configuration properties.

## Sql Client bean

The module exposes a `SqlClient` bean which is backed by a Vert.x pool. It is created using the configuration and especially the `db_uri` property whose scheme indicates the RDBMS system and therefore the Vert.x pool implementation to use.

For instance, the following configuration can be used to connect to a PostgreSQL database:

```
db_uri="postgres://user:password@localhost:5432/sample_db"
```

If you want to connect to a particular RDBMS, don't forget to add a dependency to the corresponding Vert.x SQL client implementation. Vert.x currently supports DB2, MSSQL, MySQL, PostgreSQL and Oracle.

The connection pool can be configured as well:

```
pool_maxSize=20
```

Please refer to the [Vert.x database documentation](#) to get the options supported for each RDBMS implementations.

The Vert.x SQL client requires a `Vertx` instance which is provided in the Inverno application reactor when using a `VertxReactor`, otherwise a dedicated `Vertx` instance is created. In any case, this instance can be overridden by providing a custom one to the module.

## Vert.x wrappers

Depending on our needs, we can also choose to create a custom `SqlClient` using one the Vert.x SQL client wrappers provided by the module.

The `ConnectionSqlClient` wraps a Vert.x SQL connection, you can use to transform a single connection obtained via a Vert.x connection factory into a reactive `SqlClient`.

The `PooledClientSqlClient` wraps a Vert.x pooled SQL client that supports pipelining of queries on a single configuration for optimized performances. This implementation doesn't support transactions.

```
SqlClient client = new PooledClientSqlClient(PgPool.client(...));
```

Finally, the `PoolSqlClient` wraps a Vert.x SQL pool. This is a common implementation supporting transactions and result streaming, it is used to create the module's SQL client bean.

```
SqlClient client = new PoolSqlClient(PgPool.pool(...));
```

## Redis Client

The Inverno Redis client module specifies a reactive API for executing commands on a [Redis](#) data store.

This module only exposes the API and a proper implementation module must be considered to obtain `RedisClient` instances.

In order to use the Inverno *Redis client* module, we need to declare a dependency to the API and at least one implementation in the module descriptor:

```

module io.inverno.example.app {
    ...
    requires io.inverno.mod.redis; // this is actually optional since implementations should already
    define a transitive dependency
    requires io.inverno.mod.redis.lettuce; // Lettuce implementation
    ...
}

```

And also declare these dependencies in the build descriptor:

Using Maven:

```

<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-redis</artifactId>
    </dependency>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-redis-lettuce</artifactId>
    </dependency>
  </dependencies>
</project>

```

Using Gradle:

```

...
compile 'io.inverno.mod:inverno-redis:1.5.3'
compile 'io.inverno.mod:inverno-redis-vertx:1.5.3'
...

```

## Redis Client API

The Redis client API defines the `RedisClient` and `RedisTransactionalClient` interfaces which provide reactive methods to create and execute [Redis commands](#).

The `RedisTransactionalClient` interface extends the `RedisClient` interface with Redis transactional support (ie. `MULTI`, `DISCARD`, `EXEC`...).

## Redis Operations

The API exposes multiple `*Operations` interfaces which are all extended by the `RedisClient` and which allows to fluently send commands to a Redis data store.

There are currently ten such interfaces that exposes the >200 commands supported in Redis:

- `RedisHashReactiveOperations`
- `RedisKeyReactiveOperations`
- `RedisScriptingReactiveOperations`
- `RedisSortedSetReactiveOperations`
- `RedisStringReactiveOperations`
- `RedisGeoReactiveOperations`
- `RedisHLLReactiveOperations`



- `RedisListReactiveOperations`
- `RedisSetReactiveOperations`
- `RedisStreamReactiveOperations`

The API is pretty straightforward and provides guidance on how to create and send commands to the Redis data store. For instance a simple string value can be queried as follows:

```
RedisClient<String, String> client = ...

Mono<String> getSomeKey = client.get("someKey");

// The command is sent on subscribe following reactive principles
getSomeKey.subscribe(...);
```

Complex commands are created using builders, for instance command `ZRANGE mySortedSet 0 +inf BYSCORE REV LIMIT 0 1 WITHSCORES` can be created and executed as follows:

```
RedisClient<String, String> client = ...

Flux<SortedSetScoredMember<String>> zrangeWithScores = client.zrangeWithScores()
    .reverse()
    .byScore()
    .limit(0, 1)
    .build("mySortedSet", Bound.inclusive(0), Bound.unbounded());

// The command is sent on subscribe following reactive principles
zrangeWithScores.subscribe(...);
```

## Keys and Values codecs

The `RedisClient` supports encoding and decoding of Redis keys and values, as a result the `RedisClient` client is a generic type which allows to specify the types of key and values.

The actual encoding/decoding logic is implementation specific.

## Connections

Commands can be executed directly on the client instance in which case a connection is obtained each time an operation method is invoked on the client and released once the resulting publisher terminates. This might not be an issue when a single command is issued or when using an implementation based on a single connection, However if there's a need to execute multiple commands or when using an implementation backed by a connection pool, it is often better to execute multiple SQL statements on a single connection released once the resulting publisher terminates (the connection can be either closed or returned to the pool).

Multiple commands can be executed on a single connection as follows:

```

RedisClient<String, String> client = ...

Flux<String> results = Flux.from(client.connection(operations ->
    Flux.concat(
        operations.get("key1"),
        operations.get("key2"),
        operations.get("key3")
    )
));

// Commands are sent on subscribe following reactive principles
results.subscribe(...);

```

## Batch

Commands can also be executed in batch, delaying the network flush so that multiple commands are sent to the server in one shot. This can have a significant positive impact on performances as the client doesn't have to wait for a response to send the next command.

A batch of commands can be executed as follows:

```

RedisClient<String, String> client = ...

Flux<String> results = Flux.from(client.batch(operations ->
    Flux.just(
        operations.get("key1"),
        operations.get("key2"),
        operations.get("key3")
    )
));

// Commands are sent on subscribe following reactive principles
results.subscribe(...);

```

## Transactions

Redis supports transactions through **MULTI**, **EXEC** and **DISCARD** commands which is a bit different than traditional begin/commit/rollback we can find in RDBMS. Please have a look at [Redis transactions documentation](#) to have a proper understanding on how transactions work in Redis.

Commands can be executed within a transaction using a **RedisTransactionalClient**, a transaction can be managed implicitly or explicitly by obtaining a **RedisTransactionalOperations** and explicitly invoke **exec()** or **rollback()**.

In the following example, two **SET** commands are executed within a transaction, when subscribing to the returned **Mono<RedisTransactionResult>**, the two set publishers are subscribed on and the transaction is executed implicitly and a **RedisTransactionResult** is eventually emitted and holds transaction results:

```

RedisClient<String, String> client = ...

Mono<RedisTransactionResult> transaction = client
    .multi(operations ->
        Flux.just(
            operations.set("key_1", "value_1"),
            operations.set("key_2", "value_2")
        )
    );

// Commands are sent on subscribe following reactive principles
RedisTransactionResult result = transaction.block();

if(!result.wasDiscarded()) {
    Assertions.assertEquals("OK", result.get(0));
    Assertions.assertEquals("OK", result.get(1));
}
else {
    // Report error
}

```

If any error is raised during the processing, typically when the client subscribes to the returned command publishers, the transaction is discarded.

The same transaction can be explicitly managed as follows:

```

RedisClient<String, String> client = ...

Mono<RedisTransactionResult> transaction = client
    .multi()
    .flatMap(operations -> {
        operations.set("key_1", "value_1").subscribe();
        operations.set("key_2", "value_2").subscribe();

        return operations.exec();
    });

// Commands are sent on subscribe following reactive principles
RedisTransactionResult result = transaction.block();

```

In above example, it is important to subscribe to command publishers explicitly otherwise they won't be part of the transaction.

Redis uses optimistic locking using check-and-set through the **WATCH** command which is used to indicate which keys should be monitored for changes during a transaction. When creating a transaction, it is possible to specified watches that would discard the transaction if any change is detected.

For instance, the following transaction will be discarded if the value of key **key\_3** is changed after the transaction begin:

```

RedisClient<String, String> client = ...

Mono<RedisTransactionResult> transaction = client
    .multi("key_3") // watch 'key_3'
    // let's change the value of 'key_3' using another connection to get the transaction discarded
    .doOnNext(ign -> client.set("key_3", "value_3").block())
    .flatMap(operations -> {
        operations.set("key_3", "value_3").subscribe();

        return operations.exec();
    });

RedisTransactionResult result = transaction.block();

// Transaction was discarded since 'key_3' changed before the transaction after the start of the
// transaction and before it ended
Assertions.assertTrue(result.wasDiscarded());

```

## Lettuce Redis Client implementation

The Inverno Lettuce Redis client module is an implementation of the Redis client API on top of the [Lettuce client](#).

It provides `PoolRedisClient` and `PoolRedisClusterClient` implementations that wrap a Lettuce `AsyncPool` used to acquire `StatefulRedisConnection` and `StatefulRedisClusterConnection` respectively. The `PoolRedisClusterClient` doesn't implement `RedisTransactionalClient` since transactions are not supported by Redis in a clustered environment.

The module also exposes a `RedisClient<String, String>` bean created from the module's configuration and backed by a Lettuce `BoundedAsyncPool<StatefulRedisConnection<String, String>>` instance.

SQL pooled client, pool or connection and exposes a `RedisClient` bean created from the module's configuration and backed by a Vert.x pool. It can be used to execute SQL statements in an application.

In order to use the Inverno *Lettuce Redis client* module, we need to declare a dependency in the module descriptor:

```

module io.inverno.example.app {
    ...
    requires io.inverno.mod.redis.lettuce;
    ...
}

```

And also declare this dependencies in the build descriptor:

Using Maven:

```

<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-redis-lettuce</artifactId>
    </dependency>
  </dependencies>
</project>

```

Using Gradle:

```

...
compile 'io.inverno.mod:inverno-redis-lettuce:1.5.3'
...

```

## Configuration

The `LettuceRedisClientConfiguration` is used to create and configure the Redis client bean exposed by the module.

Please refer to the [API documentation][inverno-javadoc] to have an exhaustive description of the different configuration properties.

## Redis Client bean

The module exposes a `RedisClient<String, String>` bean which is backed by a `Lettuce BoundedAsyncPool<StatefulRedisConnection<String, String>>` instance. It is created using the configuration and especially the `uri` property which specified the Redis server to connect to which is `redis://localhost:6379` by default

For instance, the following configuration can be used to connect to a remote Redis server:

```
uri="redis://remoteRedis"
```

The connection pool can be configured as well:

```
pool_max_active=8
pool_min_idle=0
pool_max_idle=8
```

Secured connection using TLS and/or authentication can also be configured as follows:

```
tls=true
username=user
password=password
```

By default, this Redis client relies on a dedicated event loop group but it can also rely on Inverno's reactor when a `Reactor` instance is available. This is transparent when assembling an application with the `boot` module which exposes Inverno's reactor.

## Lettuce wrappers

Depending on our needs, we can also choose to create a custom `RedisClient` using one the Lettuce Redis client wrappers provided by the module.

The `PoolRedisClient` implementation wraps a Lettuce `AsyncPool<StatefulRedisConnection<K, V>>`, it is then possible to create a `RedisClient` client instance using specific key/value codecs:

```
BoundedAsyncPool<StatefulRedisConnection<byte[], byte[]>> pool =
AsyncConnectionPoolSupport.createBoundedObjectPool(
    () -> this.client.connectAsync(ByteArrayCodec.INSTANCE,
RedisURI.create("redis://localhost"),
    BoundedPoolConfig.create()
);
RedisClient<byte[], byte[]> byteArrayClient = new PoolRedisClient<>(pool, byte[].class,
byte[].class);
```

The `PoolRedisClusterClient` implementation should be used to connect to a Redis cluster, it wraps a Lettuce `AsyncPool<StatefulRedisClusterConnection<K, V>>`

## LDAP

The Inverno LDAP client module specifies a basic reactive API for interacting with an LDAP or Active Directory server.

It also provides a default JDK based implementation of the `LDAPClient` exposed in the module.

This module requires an `ExecutorService` used to execute JDK blocking operations in separate thread. The `boot` module provides a global worker pool which is ideal in such situations, so in order to use the Inverno `ldap` module, we should declare the following dependencies in the module descriptor:

```
@io.inverno.core.annotation.Module
module io.inverno.example.app {
    ...
    requires io.inverno.mod.boot;
    requires io.inverno.mod.ldap;
    ...
}
```

And also declare these dependencies in the build descriptor:

Using Maven:

```

<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-boot</artifactId>
    </dependency>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-ldap</artifactId>
    </dependency>
  </dependencies>
</project>

```

Using Gradle:

```

...
compile 'io.inverno.mod:inverno-boot:1.5.3'
compile 'io.inverno.mod:inverno-ldap:1.5.3'
...

```

## Configuration

The `LDAPClientConfiguration` is used to create and configure the JDK based LDAP client bean exposed by the module.

Please refer to the [API documentation](#) to have an exhaustive description of the different configuration properties.

## LDAP Client API

The LDAP client API defines the `LDAPClient` interface which provides reactive methods to bind, search and get LDAP entries in an LDAP server.

## LDAP Operations

The API exposes `LDAPOperations` interface which is extended by the `LDAPClient` and which allows to fluently send commands to the LDAP server.

### Bind

The `bind()` method exposed on the `LDAPClient` allows to authenticate a user and obtain an `LDAPOperations` instance bound to that user.

The following is a complete example where user `jsmith` is authenticated and multiple operations are executed on the bound `LDAPOperations` instance.

```

String uid = "jsmith";
String userDN = "cn=jsmith,ou=users,dc=inverno,dc=io";
User user = Mono.from(client.bind(
    "cn={0},ou=users,dc=inverno,dc=io",
    new Object[] {uid},
    "password",
    ops -> ops.search(userDN, new String[] {"uid"}, "(&(objectClass=inetOrgPerson)(uid={0}))",
uid)
    .flatMap(userEntry -> ops.search("dc=inverno,dc=io", new String[] { "cn" }, "(&
(objectClass=groupOfNames)(member={0}))", userEntry.getDN())
        .map(groupEntry -> groupEntry.getAttribute("cn").map(LDAPAttribute::asString).get())
        .collectList()
        .map(groups -> new User(userEntry.getDN(),
userEntry.getAttribute("uid").map(LDAPAttribute::asString).get(), groups)))
    )
    .block();

```

As stated before, the `LDAPClient` extends `LDAPOperations` and any operations can then be directly invoked on the client instance. Whether an LDAP client instance is authenticated or not on the LDAP server is implementation specific.

## Get a single entry

A single entry identified by a specific `DN` can be retrieved as follows:

```
LDAPOperations operations = ...
```

```
LDAPEntry jsmithEntry = operations.get("cn=jsmith,ou=users,dc=inverno,dc=io").block();
```

The `DN` can also be specified as a templated expression using `{i}` notation and a list of arguments:

```
LDAPOperations operations = ...
```

```
LDAPEntry jsmithEntry = operations.get("cn={0},ou=users,dc=inverno,dc=io", "jsmith").block();
```

It is also possible to specify which attributes must be retrieved:

```
LDAPOperations operations = ...
```

```
LDAPEntry jsmithEntry = operations.get("cn={0},ou=users,dc=inverno,dc=io", new String[] {"cn",
"uid", "mail", "userPassword"}, "jsmith").block();
```

LDAP Attributes are exposed on the resulting `LDAPEntry`, raw attribute values can be obtained as follows:

```

// Gets the value of attribute 'mail' or null
// if multiple 'mail' attributes are defined, one of them is returned in a non-deterministic way
Object mail = jsmithEntry.get("mail").orElse(null);

// Gets all values for attribute 'mail' or an empty list
List<Object> allMail = jsmithEntry.getAll("mail");

// Get all attributes
List<Map.Entry<String, Object>> all = jsmithEntry.getAll();

```



It is also possible to get attributes as convertible `LDAPAttribute` as follows:

```
// Gets the value of attribute 'birthDate' as a local date or null
// if multiple 'birthDate' attributes are defined, one of them is returned in a non-deterministic
way
LocalDate birthDate =
jsmithEntry.getAttribute("birthDate").map(LDAPAttribute::asLocalDate).orElse(null);

// Gets all values for attribute 'address' as strings or an empty list
List<String> addresses =
jsmithEntry.getAllAttribute("address").stream().map(LDAPAttribute::asString).collect(Collectors.toList());

// Get all attributes
List<LDAPAttribute> allAttribute = jsmithEntry.getAllAttribute();
```

## Search

We can search for entries using a base context and a filter expression. In the following example we search for `inetOrgPerson` class entries with `CN` and `UID` attributes in the `users` organizational unit:

```
List<LDAPEntry> result = client.search("ou=users,dc=inverno,dc=io", new String[] {"cn", "uid"}, "(objectClass=inetOrgPerson)"
    .collectList()
    .block());
```

The filter can be templated using the `{i}` notation. In the following we search for the groups user `jsmith` belongs to:

```
List<LDAPEntry> result = client.search("dc=inverno,dc=io", new String[]{ "cn" }, "(&
(objectClass=groupOfNames)(member={0}))", "cn=jsmith,ou=users,dc=inverno,dc=io")
    .collectList()
    .block());
```

Complex queries can be created using a `SearchBuilder` which allows specifying a search scope among other things:

```
List<LDAPEntry> result = client.search()
    .scope(LDAPOperations.SearchScope.WHOLE_SUBTREE)
    .build("ou=users,dc=inverno,dc=io", new String[] {"cn", "uid"}, "(objectClass=inetOrgPerson)"
    .collectList()
    .block());
```

## LDAP Client bean

The module exposes an `LDAPClient` bean implemented using JDK `DirContext` to access the LDAP server. The client is created using the module's configuration which specifies:

- the LDAP server URI (e.g. `ldap://remoteLDAP:1389`)
- the authentication choice (`simple` by default)
- the referral policy (follow referrals by default)
- the admin user `DN` which shall be used by default to connect to the server
- the admin user credentials, typically a password

If no admin user **DN** and credentials are specified the client connects to the server anonymously unless operations are executed inside a `bind()` invocation.

For instance, the following configuration can be used to connect to a remote LDAP server using an admin **DN**:

```
uri="ldap://remoteLDAP:1389"  
admin_dn="cn=admin,ou=users,dc=inverno,dc=io"  
admin_credentials="admin_password"
```

Since the JDK directory service interface uses blocking operations, the client also requires an **ExecutorService** to make it reactive by executing blocking operations in separate threads and make sure no blocking operation is ever run in a reactor I/O thread. The *boot* module typically provides a global worker pool that must be used in such situations but it is also possible to use a specific **ExecutorService** as well when this makes sense.

## Security

The Inverno *security* module defines an API for securing access to protected services or resources in an application.

Securing an application is a complex topic which involves multiple concerns such as authentication, identification, access control, cryptography... Over the years, many techniques and specifications were created to address these concerns and protect against always more complex attacks. Defining a generic security API that is consistent with all these aspects is therefore a tedious task.

The Inverno security API has been designed to follow a clear security model with the aim of simplifying security setup inside an application by relying on simple concepts in order to keep things manageable and understandable.

The Inverno security model, which basically defines application security, is based on three main concepts:

- **Authentication** which relates to the authentication of a request made to the application.
- **Identification** which relates to the identification of the entity accessing the application.
- **Access Control** which relates to the control of access to protected services or resources in the application.

The authentication process is about authenticating credentials (e.g. user/password, token...) provided in a request in order to assess whether access to the application is granted to a requesting entity. It is very important to understand that authentication is not about authenticating the entity but really the credentials. The entity represents the originator of a request to the application, it can be external or internal, it can be an application, a device, a proxy or an actual person but as far as the application is concerned, access can only be granted when valid credentials have been authenticated which is more related to the request than the actual entity behind that request. When referring to the *authenticated entity*, we simply refer to that entity behind a request which provided credentials that has been authenticated during the authentication process.

This is actually an important point so let's take a concrete example to better understand what it means. Let's consider a prepaid card which allows for ten entries to a roller coaster, you can buy one and at the entrance pass it to your friends one after the other so you can all enjoy the ride. When passing the gates, it is the pass that is being authenticated not the person holding that pass.

The identification process is about identifying the authenticated entity accessing the application. This goes beyond authentication whose role is, and we insisted on that, to validate that provided credentials are valid and which does not necessarily give any information about who or what is actually accessing the application.

The access control process is about controlling whether an authenticated entity has the proper clearance (e.g. roles, permissions...) to access specific services or resources within the application.

From these definitions, it is important to notice that although authentication, identification and access control are all related to an entity accessing the application, they are not necessarily related to each others. For instance [OAuth2](#) is a perfect example of authentication without identification. Then we can surely conceive multiple cases where we have authentication without access control, for example an opaque token can be authenticated which gives us no information about the roles or permissions of the authenticated entity. To sum up, a requesting entity can be authenticated, then maybe identified and we may be able to control the access to protected services or resources based on other information (e.g. roles, permissions...)

Let's consider a more practical example to illustrate the theory. Let's assume our secured application is actually a secured facility:

- a person can only enter the facility if he authenticates at the entrance by showing proper credentials:
  - it can be a blank badge that gives him access to the facility but does not strongly identify him.
  - it can be a badge with identification information which is actually useless to properly identify the person unless he can prove he is the actual owner of the badge (e.g. using biometric information).

- it can be some kind of ID registered in the facility security system like a driver's license or an ID card. From there he can receive a temporary badge to access the rest of the facility (e.g. a visitor badge). In this case we might have some identification information but not necessarily what is needed to fully use the services offered inside the facility. Let's say the facility is a bank and the person is here to make a withdrawal, once inside the bank the ID card authenticated at the entrance does not give any information about the person's bank account and whether he is actually the owner of that bank account. These might be considered as identification information which require additional identification process.
- it can be a registered fingerprint or any kind of biometric information which might also provide identification information assuming they are securely stored inside the facility security system.
- the person can then enter the facility and access areas or use services inside:
  - there can be unsecured services, like a coffee machine in the lobby which anybody within the facility can use.
  - there can be restricted areas or services that require proper clearance to access. The person must then re-authenticate using the same credentials he used to enter the facility or using temporary credentials received at the entrance (e.g. visitor badge). Access control must then be performed and requires to have the person's clearances securely stored in the facility security system or inside the temporary credentials in which case they should ideally be signed and encrypted to guarantee both integrity (we don't want to let him forge his own clearances) and privacy (we don't want to let him know how access control works in the system).
  - there can be services that require further identification information which can be already available following the person's authentication or which require some additional verification. For instance, the facility can be a casino, anybody can access the restaurant area but the casino area is restricted to adults over 18.
- finally when leaving the facility, the person must return any temporary credentials he received (e.g. visitor badge in exchange from his ID card) or we can just let him go if those credentials have an expiration time and/or can be revoked anytime when we don't want him to use the facility anymore.

An Inverno application is secured by composing authentication with identity and access controller inside a **Security Context** that implements application security requirements.

The *security* module defines the core security API and several extensions modules provide specific security features:

- the *security-http* module provides exchange interceptors and handlers to secure Web applications.
- the *security-jose* module provides services to manipulate JSON Object Signing and Encryption token as specified by [RFC 7515](#), [RFC 7516](#), [RFC 7517](#), [RFC 7518](#) and [RFC 7519](#).
- the *security-ldap* module provides authenticators and identity resolvers to authenticate and identify an entity against an [LDAP](#) server or an [Active Directory](#) server.

The complete security API including extension modules currently supports:

- User/password authentication against a user repository (in-memory, Redis...).
- Token based authentication.

- Strong user identification against a user repository (in-memory, Redis...).
- Secured password encoding using message digest, [Argon2](#), [Password-Based Key Derivation Function](#), [BCrypt](#), [SCrypt](#)...
- [Role-based access control](#).
- Permission-based access control.
- JSON Object Signing and Encryption (provided in the *security-jose* module).
- LDAP/Active Directory authentication and identification (provided in the *security-ldap* module).
- HTTP [basic](#) authentication scheme (provided in the *security-http* module).
- HTTP [digest](#) authentication scheme (provided in the *security-http* module).
- Form based authentication (provided in the *security-http* module).
- Cross-origin resource sharing support ([CORS](#)) (provided in the *security-http* module).
- Protection against Cross-site request forgery attack ([CSRF](#)) (provided in the *security-http* module).

In order to use the Inverno *security* module, we need to declare a dependency in the module descriptor:

```
module io.inverno.example.app {
    ...
    requires io.inverno.mod.security;
    ...
}
```

And also declare that dependency in the build descriptor:

Using Maven:

```
<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-security</artifactId>
    </dependency>
  </dependencies>
</project>
```

Using Gradle:

```
...
compile 'io.inverno.mod:inverno-security:1.5.3'
...
```

Before looking into details of the security API, let's see how to secure a simple standalone application composed of a single *HelloService* bean exposing *sayHello()* method. Initially the application might look like:

```

package io.inverno.example.app_hello_security;

import io.inverno.core.annotation.Bean;

@Bean
public class HelloService {

    public void sayHello() {
        StringBuilder message = new StringBuilder();
        message.append("Hello world!");
        System.out.println(message.toString());
    }
}

package io.inverno.example.app_hello_security;

import io.inverno.core.v1.Application;

public class Main {

    public static void main(String[] args) {
        Application.run(new App_hello_security.Builder()).helloService().sayHello();
    }
}

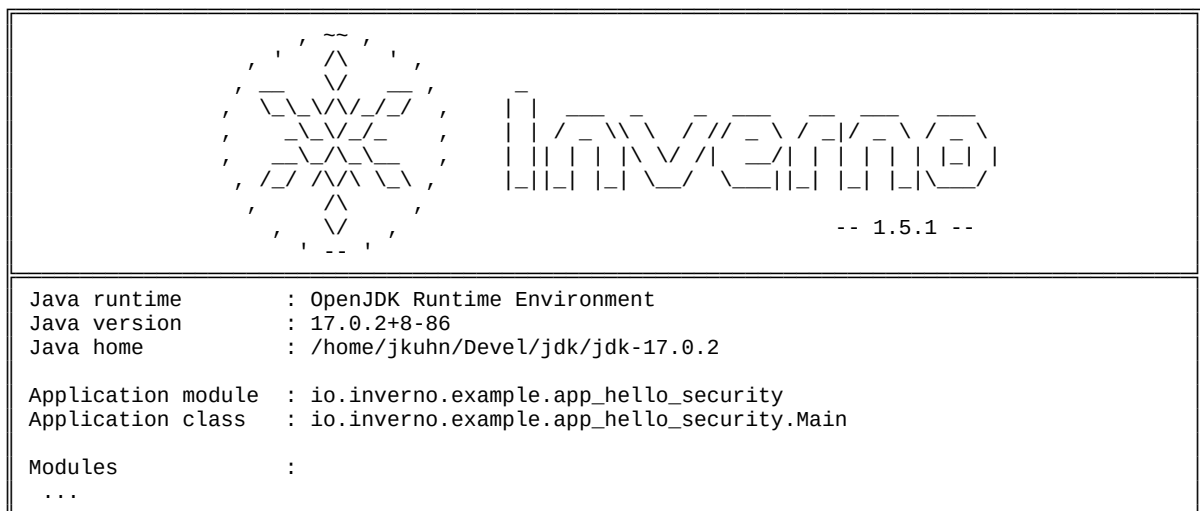
```

Running the application would return the following output:

```

$ mvn inverno:run
...
[INFO] Running project: io.inverno.example.app_hello_security@1.0.0-SNAPSHOT...
[=====] 100 %
=====
15:59:29.395 [main] INFO io.inverno.core.v1.Application - Inverno is starting...

```



```

15:59:29.400 [main] INFO io.inverno.example.app_hello_security.App_hello_security - Starting Module
io.inverno.example.app_hello_security...
15:59:29.402 [main] INFO io.inverno.example.app_hello_security.App_hello_security - Module
io.inverno.example.app_hello_security started in 3ms
15:59:29.405 [main] INFO io.inverno.core.v1.Application - Application
io.inverno.example.app_hello_security started in 23ms
Hello world!
15:59:29.411 [Thread-0] INFO io.inverno.example.app_hello_security.App_hello_security - Stopping
Module io.inverno.example.app_hello_security...

```

We want to protect the whole application so basically exit the application if the user could not be authenticated using login/password credentials specified on the command line.

In order to authenticate a user against an in-memory repository, we must create a **security manager** as follows:

```

package io.inverno.example.app_hello_security;

import io.inverno.core.annotation.Bean;
import io.inverno.core.v1.Application;
import io.inverno.mod.security.SecurityManager;
import io.inverno.mod.security.accesscontrol.AccessController;
import io.inverno.mod.security.authentication.LoginCredentials;
import io.inverno.mod.security.authentication.LoginCredentialsMatcher;
import io.inverno.mod.security.authentication.password.RawPassword;
import io.inverno.mod.security.authentication.user.InMemoryUserRepository;
import io.inverno.mod.security.authentication.user.User;
import io.inverno.mod.security.authentication.user.UserAuthenticator;
import io.inverno.mod.security.context.SecurityContext;
import io.inverno.mod.security.identity.Identity;
import java.util.List;
import java.util.function.Supplier;
import org.apache.logging.log4j.LogManager;
import org.apache.logging.log4j.Logger;

public class Main {

    private static final Logger LOGGER = LogManager.getLogger(Main.class);

    public static void main(String[] args) {
        if(args.length != 2) {
            System.out.println("Usage: hello <user> <password>");
            return;
        }

        // The security manager uses a user authenticator with an in-memory user repository and a
        // login credentials (i.e. login/password) matcher
        SecurityManager<LoginCredentials, Identity, AccessController> securityManager =
        SecurityManager.of(
            new UserAuthenticator<>((
                InMemoryUserRepository
                    .of(List.of(
                        User.of("jsmith")
                            .password(new RawPassword("password"))
                            .build()
                    ))
                .build(),
            new LoginCredentialsMatcher<>()
        )
    );

    securityManager.authenticate(LoginCredentials.of(args[0], new RawPassword(args[1])))
        .subscribe(securityContext -> {
            if(securityContext.isAuthenticated()) {
                LOGGER.info("User has been authenticated");
                Application.run(new App_hello_security.Builder()).helloService().sayHello();
            }
            else {
                securityContext.getAuthentication().getCause().ifPresentOrElse(
                    error -> LOGGER.error("Failed to authenticate user", error),
                    () -> LOGGER.error("Unauthorized anonymous access")
                );
            }
        });
    }
}

```



Now if we run the application with valid or invalid credentials we should get the following outputs:

```
$ mvn inverno:run -Dinverno.run.arguments="jsmith password"
16:08:24.078 [main] INFO io.inverno.example.app_hello_security.Main - User has been authenticated
16:08:24.090 [main] INFO io.inverno.core.v1.Application - Inverno is starting...
...
16:08:24.108 [main] INFO io.inverno.example.app_hello_security.App_hello_security - Starting Module
io.inverno.example.app_hello_security...
16:08:24.111 [main] INFO io.inverno.example.app_hello_security.App_hello_security - Module
io.inverno.example.app_hello_security started in 4ms
16:08:24.115 [main] INFO io.inverno.core.v1.Application - Application
io.inverno.example.app_hello_security started in 21ms
Hello world!
16:08:24.116 [Thread-0] INFO io.inverno.example.app_hello_security.App_hello_security - Stopping
Module io.inverno.example.app_hello_security...

$ mvn inverno:run -Dinverno.run.arguments="jsmith invalid"
...
16:08:49.442 [main] ERROR io.inverno.example.app_hello_security.Main - Failed to authenticate user
io.inverno.mod.security.authentication.InvalidCredentialsException: Invalid credentials
    at
io.inverno.mod.security.authentication.AbstractPrincipalAuthenticator.lambda$authenticate$1(Abstract
PrincipalAuthenticator.java:74) ~[io.inverno.mod.security-1.5.0-SNAPSHOT.jar:?]
    at reactor.core.publisher.MonoErrorSupplied.subscribe(MonoErrorSupplied.java:55)
[reactor.core-3.4.14.jar:?]
    at reactor.core.publisher.Mono.subscribe(Mono.java:4400) [reactor.core-3.4.14.jar:?]
    at
reactor.core.publisher.FluxSwitchIfEmpty$SwitchIfEmptySubscriber.onComplete(FluxSwitchIfEmpty.java:8
2) [reactor.core-3.4.14.jar:?]
    at
reactor.core.publisher.FluxMapFuseable$MapFuseableSubscriber.onComplete(FluxMapFuseable.java:150)
[reactor.core-3.4.14.jar:?]
    at
reactor.core.publisher.FluxFilterFuseable$FilterFuseableSubscriber.onComplete(FluxFilterFuseable.jav
a:171) [reactor.core-3.4.14.jar:?]
    at reactor.core.publisher.Operators$MonoSubscriber.complete(Operators.java:1817)
[reactor.core-3.4.14.jar:?]
    at reactor.core.publisher.MonoSupplier.subscribe(MonoSupplier.java:62) [reactor.core-
3.4.14.jar:?]
    at reactor.core.publisher.Mono.subscribe(Mono.java:4400) [reactor.core-3.4.14.jar:?]
    at reactor.core.publisher.Mono.subscribeWith(Mono.java:4515) [reactor.core-3.4.14.jar:?]
    at reactor.core.publisher.Mono.subscribe(Mono.java:4371) [reactor.core-3.4.14.jar:?]
    at reactor.core.publisher.Mono.subscribe(Mono.java:4307) [reactor.core-3.4.14.jar:?]
    at reactor.core.publisher.Mono.subscribe(Mono.java:4279) [reactor.core-3.4.14.jar:?]
    at io.inverno.example.app_hello_security.Main.main(Main.java:71) [classes/:?]
...

```

We can change the `HelloService` in order to display a personalized greeting message to the authenticated user. This requires to resolve the identity of the user and inject the security context into the `HelloService`.

The identity of the user can be stored in the user repository and resolved using a `UserIdentityResolver` in the security manager as follows:

```

package io.inverno.example.app_hello_security;

import io.inverno.core.annotation.Bean;
import io.inverno.core.v1.Application;
import io.inverno.mod.security.SecurityManager;
import io.inverno.mod.security.accesscontrol.AccessController;
import io.inverno.mod.security.authentication.LoginCredentials;
import io.inverno.mod.security.authentication.LoginCredentialsMatcher;
import io.inverno.mod.security.authentication.password.RawPassword;
import io.inverno.mod.security.authentication.user.InMemoryUserRepository;
import io.inverno.mod.security.authentication.user.User;
import io.inverno.mod.security.authentication.user.UserAuthenticator;
import io.inverno.mod.security.context.SecurityContext;
import io.inverno.mod.security.identity.PersonIdentity;
import io.inverno.mod.security.identity.UserIdentityResolver;
import java.util.List;
import java.util.function.Supplier;
import org.apache.logging.log4j.LogManager;
import org.apache.logging.log4j.Logger;

public class Main {

    private static final Logger LOGGER = LogManager.getLogger(Main.class);

    @Bean
    public static interface App_hello_securitySecurityContext extends
Supplier<SecurityContext<PersonIdentity, AccessController>> {}

    public static void main(String[] args) {
        ...
        // The security manager now uses a user identity resolver to resolve the identity of the
authenticated user
        SecurityManager<LoginCredentials, PersonIdentity, AccessController> securityManager =
SecurityManager.of(
            new UserAuthenticator<>() {
                InMemoryUserRepository
                    .of(List.of(
                        User.of("jsmith")
                            .password(new RawPassword("password"))
                            .identity(new PersonIdentity("jsmith", "John", "Smith",
"jsmith@inverno.io")))
                    .build()
            })
            .build(),
            new LoginCredentialsMatcher<>()
        ),
        new UserIdentityResolver<>()
    );

        // The security context is now injected in the App_hello_security module
        securityManager.authenticate(LoginCredentials.of(args[0], new RawPassword(args[1])))
            .subscribe(securityContext -> {
                if(securityContext.isAuthenticated()) {
                    LOGGER.info("User has been authenticated");
                    Application.run(new
App_hello_security.Builder(securityContext)).helloService().sayHello();
                }
                else {
                    securityContext.getAuthentication().getCause().ifPresentOrElse(
                        error -> LOGGER.error("Failed to authenticate user", error),

```

```

        () -> LOGGER.error("Unauthorized anonymous access")
    );
    }
    });
}
}

```

In above code, we also declared a socket bean in order to inject the `SecurityContext` in the module and eventually in the `HelloService` bean:

```

package io.inverno.example.app_hello_security;

import io.inverno.core.annotation.Bean;
import io.inverno.mod.security.accesscontrol.AccessController;
import io.inverno.mod.security.context.SecurityContext;
import io.inverno.mod.security.identity.PersonIdentity;

@Bean
public class HelloService {

    private final SecurityContext<PersonIdentity, AccessController> securityContext;

    public HelloService(SecurityContext<PersonIdentity, AccessController> securityContext) {
        this.securityContext = securityContext;
    }

    public void sayHello() {
        StringBuilder message = new StringBuilder();
        message.append("Hello
").append(this.securityContext.getIdentity().map(PersonIdentity::getFirstName).orElse("whoever you
are")).append("!");
        System.out.println(message.toString());
    }
}

```

If we run the application, we should now get a personalized greeting message using the user identity:

```

$ mvn inverno:run -Dinverno.run.arguments="jsmith password"
...
Hello John!

```

A `PersonIdentity` has been attached to the user in the repository but the repository may also contain users with no defined identity which is why `SecurityContext#identity()` returns an `Optional`.

Now let's say we want some privileged users to be greeted with an extra polite message. We can assign roles to users in the repository and resolve a `RoleBasedAccessController` to check privileges in the `HelloService`:

```

package io.inverno.example.app_hello_security;

import io.inverno.core.annotation.Bean;
import io.inverno.core.v1.Application;
import io.inverno.mod.security.SecurityManager;
import io.inverno.mod.security.accesscontrol.GroupsRoleBasedAccessControllerResolver;
import io.inverno.mod.security.accesscontrol.RoleBasedAccessController;
import io.inverno.mod.security.authentication.LoginCredentials;
import io.inverno.mod.security.authentication.LoginCredentialsMatcher;
import io.inverno.mod.security.authentication.password.RawPassword;
import io.inverno.mod.security.authentication.user.InMemoryUserRepository;
import io.inverno.mod.security.authentication.user.User;
import io.inverno.mod.security.authentication.user.UserAuthenticator;
import io.inverno.mod.security.context.SecurityContext;
import io.inverno.mod.security.identity.PersonIdentity;
import io.inverno.mod.security.identity.UserIdentityResolver;
import java.util.List;
import java.util.function.Supplier;
import org.apache.logging.log4j.LogManager;
import org.apache.logging.log4j.Logger;

public class Main {

    private static final Logger LOGGER = LogManager.getLogger(Main.class);

    @Bean
    public static interface App_hello_securitySecurityContext extends
Supplier<SecurityContext<PersonIdentity, RoleBasedAccessController>> {}

    public static void main(String[] args) {
        ...
        // The security manager now uses a groups RBAC Resolver to resolve the RBAC access controller
of the authenticated user
        SecurityManager<LoginCredentials, PersonIdentity, RoleBasedAccessController> securityManager
= SecurityManager.of(
            new UserAuthenticator<>() {
                InMemoryUserRepository
                    .of(List.of(
                        User.of("jsmith")
                            .password(new RawPassword("password"))
                            .identity(new PersonIdentity("jsmith", "John", "Smith",
"jsmith@inverno.io"))
                            .groups("vip")
                            .build(),
                        User.of("adoe")
                            .password(new RawPassword("password"))
                            .identity(new PersonIdentity("adoe", "Alice", "Doe", "adoe@inverno.io"))
                            .build()
                    ))
                    .build(),
                new LoginCredentialsMatcher<>()
            ),
            new UserIdentityResolver<>(),
            new GroupsRoleBasedAccessControllerResolver()
        );
        ...
    }
}

```

```

package io.inverno.example.app_hello_security;

import io.inverno.core.annotation.Bean;
import io.inverno.mod.security.accesscontrol.RoleBasedAccessController;
import io.inverno.mod.security.context.SecurityContext;
import io.inverno.mod.security.identity.PersonIdentity;
import reactor.core.publisher.Mono;

@Bean
public class HelloService {

    private final SecurityContext<PersonIdentity, RoleBasedAccessController> securityContext;

    public HelloService(SecurityContext<PersonIdentity, RoleBasedAccessController> securityContext)
    {
        this.securityContext = securityContext;
    }

    public void sayHello() {
        this.securityContext.getAccessController()
            .map(rbac -> rbac.hasRole("vip"))
            .orElse(Mono.just(false))
            .subscribe(isVip -> {
                StringBuilder message = new StringBuilder();
                if(isVip) {
                    message.append("Hello my dear friend
").append(this.securityContext.getIdentity().map(PersonIdentity::getFirstName).orElse("whoever you
are")).append("!");
                }
                else {
                    message.append("Hello
").append(this.securityContext.getIdentity().map(PersonIdentity::getFirstName).orElse("whoever you
are")).append("!");
                }
                System.out.println(message.toString());
            });
    }
}

```

We can now run the application using **jsmith** and **adoc** credentials and see the results:

```

$ mvn clean inverno:run -Dinverno.run.arguments="jsmith password"
...
Hello my dear friend John!

$ mvn clean inverno:run -Dinverno.run.arguments="adoc password"
...
Hello Alice!

```

As for the identity, we can not assume that an access controller is present in the security context which only proves that an entity has been authenticated.

# Security Manager

Now let's take a closer look at the API starting by the `SecurityManager` which is the main entry point to secure an application.

Note that when securing a Web application, the role of the `SecurityManager` is actually handled by a `SecurityInterceptor` intercepting secured Web route and populating the exchange context with the security context to make it accessible to route handlers and interceptors. Please refer to the *security-http* module documentation for detailed information.

The security manager is used to authenticate credentials and create a security context exposing the actual authentication result and the authenticated entity's identity and access controller if any. A `SecurityManager` instance is created by composing an `Authenticator` with optional `IdentityResolver` and `AccessControllerResolver` which are respectively used to resolve the `Identity` and the `AccessController` of the authenticated entity based on the `Authentication` object resulting from the authentication of input `Credentials` by the `Authenticator`.

The `SecurityManager` interface basically chains the authentication, the identity resolution and the access controller resolution in a single method `authenticate()` returning the resulting `SecurityContext`.

```
Authenticator<Credentials, Authentication> authenticator = ...
IdentityResolver<Authentication, Identity> identityResolver = ...
AccessControllerResolver<Authentication, AccessController> accessControllerResolver = ...
```

```
// Create a security manager with authentication only
SecurityManager<Credentials, Identity, AccessController> securityManager =
SecurityManager.of(authenticator);
```

```
// Create a security manager with identity resolution
SecurityManager<Credentials, Identity, AccessController> securityManager =
SecurityManager.of(authenticator, identityResolver);
```

```
// Create a security manager with access control resolution
SecurityManager<Credentials, Identity, AccessController> securityManager =
SecurityManager.of(authenticator, accessControllerResolver);
```

```
// Create a security manager with both identification and access control resolution
SecurityManager<Credentials, Identity, AccessController> securityManager =
SecurityManager.of(authenticator, identityResolver, accessControllerResolver);
```

Note how generics are used to specify what `Credentials` can be authenticated, what `Authentication` object are returned by the authenticator and used by identity and access controller resolvers to resolve specific `Identity` and `AccessController` objects. This basically allows the compiler to check that the security manager is created with consistent `Authenticator`, `IdentityResolver` and `AccessControllerResolver`.

A security context can then be obtained by authenticating appropriate credentials as defined by the selected authenticator.

```
SecurityManager<LoginCredentials, PersonIdentity, RoleBasedAccessController> securityManager = ...

SecurityContext<PersonIdentity, RoleBasedAccessController> securityContext =
securityManager.authenticate(LoginCredentials.of("user", new RawPassword("password"))).block();
```

A security manager shall always return a security context even in case of security errors. For instance it returns:

- an **anonymous** security context when authenticating **null** credentials. An anonymous security context only expose an unauthenticated **Authentication** object with no cause.
- an **denied** security context when authentication or identity or access controller resolutions failed with error.
- an **granted** security context when authentication and identity and access controller resolutions were successful.

The following shows a proper way to handle a security context:

```
if(securityContext.isAuthenticated()) {
    // Successful authentication
    ...
}
else if(securityContext.isAnonymous()) {
    // Anonymous access
    ...
}
else {
    // Failed authentication
    ...
}
```

## Credentials

Credentials must be provided to the application to get access to protected services or resources inside the application. In practice, **Credentials** must be authenticated by the **Authenticator** of a **SecurityManager** which eventually creates the application's **SecurityContext** used accross the application to determine whether the authenticated entity can invoke services or access resources.

There are many forms of credentials which depend on the actual authentication process. The most common is a username/password pair, but we can also think about tokens, an X.509 certificates... The security API exposes several basic type of credentials.

### TokenCredentials

Token credentials are composed of a single token usually easy to authenticate, temporary, revocable or renewable. They are typically obtained by an entity following other stronger authentication processes using sensitive credentials (e.g. username/password with or without multi-factor authentication...) in order to avoid exposing these sensitive data or to use a cheaper authentication process each time the application is accessed by the authenticated entity.

The `TokenCredentials` class is a basic token credentials implementation exposing an opaque token.

## PrincipalCredentials

Principal credentials represents generic credentials for a principal entity identified using a username. The `PrincipalCredentials` interface is actually a base type which is simply exposing the username, it does not presume of any particular authentication method (e.g. password, multi-factor, biometric...).

## LoginCredentials

Login credentials are specific principal credentials with a password which is used to authenticate a principal entity identified by a username.

The `LoginCredentials` interface extends `PrincipalCredentials` and simply exposes a `Password` in addition to the username. Login credentials can be created with a username and a password as follows:

```
LoginCredentials loginCredentials = LoginCredentials.of("jsmith", new RawPassword("password"));
```

Login credentials provided by a user in a login form for instance usually contain a raw password in clear text, however it is completely possible to define them using an encoded password and therefore secure the password all the way to the authenticator.

## Password

Password can be used in an authentication based on a shared secret, namely the password. The API defines the `Password` interface which is used to represent a password and allows it to be stored in a secured encoded form, for instance in a user repository. It can also be used to match a password provided in a password based credentials, for instance when authenticating `LoginCredentials` against other password based credentials resolved from a secured repository.

The `Password` interface exposes an encoded password value, the actual `Password.Encoder` that was used to encode the password and `matches()` methods used to match a raw password or another `Password` instance.

A simple message digest password can be created from a raw password value as follows:



```
// password -> bta60AntIvI9YWRfsFFSRBocTW-4xSzmI...
MessageDigestPassword password = new MessageDigestPassword.Encoder().encode("password");
```

or from an encoded value as follows:

```
MessageDigestPassword password = new MessageDigestPassword("bta60AntIvI9YWRfsFFSRBocTW-4xSzmI...",
new MessageDigestPassword.Encoder());
```

Using the password instance, it is then possible to match a provided raw password value:

```
if(password.matches("password")) {
    // passwords match
    ...
}
```

In order to properly match passwords, it is important to use the same encoder as the one that was used to encode the password. Password encoders can be configured in various ways to reach a proper level of protection. As a result, when encoding password, it is important to always use constant encoder's settings to be able to recover the exact same password instance from a given encoded password. One way to do that is to hardcode these settings in the application but then they shall never be changed or all passwords must be renewed. Another more reliable way would be to store encoder's settings next to the encoded password. This can be done by serializing the password as JSON.

```
ObjectMapper mapper = new ObjectMapper();

MessageDigestPassword password = new MessageDigestPassword.Encoder("SHA-512", "secret".getBytes(),
16).encode("password");

// {"@c":".MessageDigestPassword","value":"R3IF7VY7Trxh4slRRVF4Yk0_JNicaAtUZ...", "encoder":
{"@c":".MessageDigestPassword$Encoder","algorithm":"SHA-512","secret":"c2VjcmV0","saltLength":16}}
String serializedPassword = mapper.writeValueAsString(password);

// Returns a MessageDigestPassword instance
Password<?, ?> readPassword = mapper.readValue(jsonPassword, Password.class);
```

The API currently provides the following **Password** implementations:

- **Argon2Password** which uses [Argon2](#) key derivation function.
- **BCryptPassword** which uses [BCrypt](#) hashing function.
- **MessageDigestPassword** which uses a **MessageDigest** with salt.
- **PBKDF2Password** which uses [Password-Based Key Derivation Function 2](#).
- **SCryptPassword** which uses [SCrypt](#) hashing function.
- The **RawPassword** implementation does not encode passwords, it is typically used to represent in-memory and volatile passwords submitted to a running application for authentication. They are usually matched against stored and secured password credentials. A **RawPassword** instance can't be serialized as JSON as other password implementations, it shall not be stored or communicated under any circumstances.

# Authenticator

In a security manager, an authenticator is responsible for authenticating `Credentials` and returning a resulting `Authentication` which represents a proof that credentials have been authenticated.

The `Authenticator` interface is a functional interface defining one `authenticate()` method. It is then easy to create *inline* authenticator implementations for testing purposes or else. A simplistic authenticator for authenticating login credentials (i.e. username/password) can be created as follows:

```
Authenticator<LoginCredentials, Authentication> authenticator = credentials -> Mono.fromSupplier(()  
-> {  
    if(credentials.getUsername().equals("user") && credentials.getPassword().equals("password")) {  
        return Authentication.authenticated();  
    }  
    return Authentication.denied();  
});
```

An authenticator might not always be able to authenticate provided credentials, this basically means that the authenticator is unable to determine whether specified credentials are valid because it does not manage or understand them. For instance, we can imagine defining different authenticators targeting different user realms or authentication systems, credentials could only be authenticated by the authenticator targeting the same realm or authentication system.

In such situations, an authenticator can decide to return an empty `Mono` instead of returning a denied authentication or throwing an `AuthenticationException` which would terminate the authentication process. This would allow other authenticators to try to authenticate the credentials.

Multiple authenticators can be chained using the `or()` operator. In the following example, `authenticator1` is implemented in such a way that it only tries to authenticate users it knows, returning an empty `Mono` for those it doesn't know in order to delegate authentication to `authenticator2` which is terminal and always returns an `Authentication` instance:

```

Authenticator<LoginCredentials, Authentication> authenticator1 = credentials -> Mono.fromSupplier(()
-> {
    if(credentials.getUsername().equals("user1")) {
        if(credentials.getPassword().matches("password")) {
            return Authentication.granted();
        }
        // Claim the credentials and terminate the chain
        return Authentication.denied();
    }
    // Delegate to next authenticator in the chain
    return null;
});

Authenticator<LoginCredentials, Authentication> authenticator2 = credentials -> Mono.fromSupplier(()
-> {
    if (credentials.getUsername().equals("user2") && credentials.getPassword().matches("password"))
    {
        return Authentication.granted();
    }
    return Authentication.denied();
});

Authenticator<LoginCredentials, Authentication> compositeAuthenticator =
authenticator1.or(authenticator2);

// A granted authentication is returned by authenticator1
compositeAuthenticator.authenticate(LoginCredentials.of("user1", new RawPassword("password")));

// A denied authentication is returned by authenticator2 which claimed the credentials
compositeAuthenticator.authenticate(LoginCredentials.of("user1", new RawPassword("invalid")));

// A granted authentication is returned by authenticator2
compositeAuthenticator.authenticate(LoginCredentials.of("user2", new RawPassword("password")));

// A denied authentication is returned by authenticator2 which is terminal
compositeAuthenticator.authenticate(LoginCredentials.of("user2", new RawPassword("invalid")));

// A denied authentication is returned by authenticator2 which is terminal
compositeAuthenticator.authenticate(LoginCredentials.of("unknown", new RawPassword("password")));

```

This approach might be very usefull when there is a need to authenticate credentials against multiple authentication systems. However you must be aware that some authenticator might not be *chainable* since, as **authenticator2** they can be implemented to claim all credentials peventing further authenticator to be invoked. Let's consider a **LoginCredentials** authenticator, it could rightfully consider that any username/password pair that it is unable to validate should be denied.

It is also possible to transform the resulting authentication which can be useful to adapt it for further processing (e.g. identity resolver, access controller resolver, login forms...). In the following example, we transform the authentication returned by a login credentials authenticator into a **TokenAuthentication**:

```
Authenticator<LoginCredentials, Authentication> authenticator = ...
```

```
authenticator.map(authentication -> {  
    final String token = UUID.randomUUID().toString();  
    return new TokenAuthentication() {  
        @Override  
        public String getToken() {  
            return token;  
        }  
  
        @Override  
        public boolean isAuthenticated() {  
            return authentication.isAuthenticated();  
        }  
  
        @Override  
        public Optional<SecurityException> getCause() {  
            return authentication.getCause();  
        }  
    };  
});
```

A proper authentication implementation shall always return an authentication whether authentication succeeds or fails, however there might be use cases where we simply want to fail and propagate the authentication error. This can be desirable when handling denied authentications is not required and must be delegated to a higher level typically the security manager.

Considering previous example, we can make sure only authenticated authentication will be transformed by using the `failOnDenied()` operator which can be invoked to avoid having to handle denied authentications when transforming the authentication output:

```
Authenticator<LoginCredentials, Authentication> authenticator = ...
```

```
authenticator  
    // Fail when an denied authentication is returned and propagate the underlying SecurityException  
    .failOnDenied()  
    // Only transform successful authentication  
    .map(authentication -> {  
        final String token = UUID.randomUUID().toString();  
        return new TokenAuthentication() {  
            @Override  
            public String getToken() {  
                return token;  
            }  
  
            @Override  
            public boolean isAuthenticated() {  
                return authentication.isAuthenticated();  
            }  
  
            @Override  
            public Optional<SecurityException> getCause() {  
                return authentication.getCause();  
            }  
        };  
    });
```

It is also possible to fail on both denied or anonymous authentications using the `failOnDeniedAndAnonymous()` operator.

The API was designed to provide the most flexibility to the application which can decide how denied or anonymous authentications should be handled, unauthenticated authentications actually exist to still be able to create a security context and do things inside the application from an unauthenticated authentication. You should however take particular care when transforming authentication instances using `map()` or `flatMap()` operators, remember that an authentication represents proof that credentials were authenticated and as a result always make sure the authentication state is taken into account all the way. In previous example, we could have quite easily ignored the authentication in the mapper and always returned an authenticated authentication. Using `failOnDenied()` or `failOnDeniedAndAnonymous()` can prevent you from doing such mistakes.

The API provides several base implementations that facilitate the authentication setup in an application.

Please refer to *security-jose* and *security-ldap* modules documentations for JOSE tokens authenticators (i.e. JWS, JWE, JWT), LDAP and Active Directory authenticators.

## PrincipalAuthenticator

The principal authenticator is a generic authenticator for `PrincipalCredential` which returns `PrincipalAuthentication`. Authentication is done by matching provided credentials against trusted credentials using a `CredentialsMatcher`. Trusted credentials are resolved by username using a `CredentialsResolver`. A `PrincipalAuthenticator` is then created with a `CredentialsResolver` and a `CredentialsMatcher` as follows:

```
// Resolves trusted credentials by username (e.g. from a trusted store...)
CredentialsResolver<LoginCredentials> credentialsResolver = ...

// Matches provided credentials against trusted credentials
CredentialsMatcher<LoginCredentials, LoginCredentials> credentialsMatcher = ...

PrincipalAuthenticator<LoginCredentials, LoginCredentials> authenticator = new
PrincipalAuthenticator<>(credentialsResolver, credentialsMatcher);

authenticator.authenticate(LoginCredentials.of("user", new RawPassword("password")));
```

A principal authenticator is terminal by default and terminates the authentication by returning a denied authentication on `AuthenticationException` due to unresolvable credentials (`CredentialsNotFoundException`) or unmatched credentials (`InvalidCredentialsException`). A principal authenticator can be made non-terminal in order to chain other authenticators:

```
PrincipalAuthenticator<LoginCredentials, LoginCredentials> authenticator = new
PrincipalAuthenticator<>(credentialsResolver, credentialsMatcher);

LoginCredentials invalidCredentials = LoginCredentials.of("user", new RawPassword("invalid"));

// Returns a denied authentication
PrincipalAuthentication authentication = authenticator.authenticate(invalidCredentials).block();

// Returns null
PrincipalAuthentication authentication = authenticator.authenticate(invalidCredentials).block();
```

## UserAuthenticator

The user authenticator extends the principal authenticator, it is used to authenticate actual users. As for the `PrincipalAuthenticator`, the `UserAuthenticator` authenticates `PrincipalCredentials`, but it matches them against trusted `User` credentials instead of generic credentials. A user is a specific kind of credentials to represent actual users with `Identity` and groups. The resulting authentication is a `UserAuthentication` which exposes the `Identity` and the set of groups of the authenticated entity. A user is typically used to represent credentials for a physical person accessing the application.

Since the `User` interface exposes both identity and groups, the `UserAuthenticator` can actually authenticate and resolve data required to resolve the user's `Identity` and `AccessController` at once. In a security manager, it can be associated with a `UserIdentityResolver` which extracts the identity from the authentication and a `GroupsRoleBasedAccessControllerResolver` which uses the groups from the authentication as roles to create a `RoleBasedAccessController`.

```
// Resolves system users by username (e.g. from a user repository...)
CredentialsResolver<User<PersonIdentity>> credentialsResolver = ...

// Matches provided credentials against trusted users which are also LoginCredentials
CredentialsMatcher<LoginCredentials, LoginCredentials> credentialsMatcher = ...

UserAuthenticator<LoginCredentials, PersonIdentity, User<PersonIdentity>> authenticator = new
UserAuthenticator<>(credentialsResolver, credentialsMatcher);

UserAuthentication<PersonIdentity> authentication =
authenticator.authenticate(LoginCredentials.of("user", new RawPassword("password"))).block();

// first name, last name, email...
PersonIdentity identity = authentication.getIdentity();

// user belongs to groups sales, admin...
Set<String> groups = authentication.getGroups();
```

As for the [principal authenticator](#), a user authenticator is terminal by default but can be made non-terminal by setting the `terminal` flag to `false`.

## Credentials resolver

A credentials resolver is usually used within `Authenticator` implementations for resolving trusted credentials based on some id provided with the credentials in order to match them against trusted credentials. Both `PrincipalAuthenticator` and `UserAuthenticator` uses this technique to authenticate `LoginCredentials` identified by the username.

The `CredentialsResolver` interface is a functional interface defining one `resolveCredentials()` method. A simplistic implementation can then be created as follows:

```
CredentialsResolver<LoginCredentials> credentialsResolver = username -> Mono.fromSupplier(() -> {
    switch(username) {
        case "user1": return LoginCredentials.of("user1", new
BCryptPasswordEncoder().encode("password1"));
        case "user2": return LoginCredentials.of("user2", new
BCryptPasswordEncoder().encode("password2"));
        default: return null;
    }
});

// Returns user1's trusted credentials
LoginCredentials user1Credentials = credentialsResolver.resolveCredentials("user1").block();

// Returns null
LoginCredentials user3Credentials = credentialsResolver.resolveCredentials("user3").block();
```

The API provides several implementations that facilitate the authentication setup in an application.

## InMemoryLoginCredentialsResolver

An in-memory login credentials resolver can be used to create dynamic and volatile `LoginCredentials` resolvers which are particularly suited for testing and prototyping. The `InMemoryLoginCredentialsResolver` basically looks for `LoginCredentials` stored in a `ConcurrentHashMap` and allows to add or remove credentials as needed.

```
InMemoryLoginCredentialsResolver inMemoryLoginCredentialsResolver = new
InMemoryLoginCredentialsResolver(List.of(LoginCredentials.of("user1", new
RawPassword("password"))));
inMemoryLoginCredentialsResolver.put("user2", new RawPassword("password"));
inMemoryLoginCredentialsResolver.remove("user1");
```

## UserRepository

A user repository is a user credentials resolver that provides CRUD operations to a data store in order to securely store and manage application users.

```

userRepository<PersonIdentity, User<PersonIdentity>> userRepository = null;

// Create a user with identity and groups
userRepository.createUser(new User<>("jsmith", new PersonIdentity("jsmith", "John", "Smith",
"jsmith@inverno.io"), new RawPassword("password"), "group1", "group2"));

// Update user email
userRepository.getUser("jsmith")
    .doOnNext(user -> user.getIdentity().setEmail("jsmith1@inverno.io"))
    .map(userRepository::updateUser)
    .block();

// Password change requires current credentials
userRepository.changePassword(LoginCredentials.of("jsmith", new RawPassword("password")),
"newPassword");

// Delete user
userRepository.deleteUser("jsmith").block();

```

A proper `UserRepository` implementation shall rely on a `PasswordPolicy` and a `PasswordEncoder` to respectively control the level of protection offered by passwords and securely store them in the datastore.

The `PasswordPolicy` interface defines the `verify()` method which evaluates the strength of a password in a login credentials against some rules. A `PasswordPolicy.PasswordStrength` provides qualitative and quantitative marks used to evaluate the password strength, it is returned when the password follows the policy and included in a `PasswordPolicyException` thrown when the password does not follow the policy.

The `SimplePasswordPolicy` is a simple implementation that allows to control password's minimum and maximum length:

```

PasswordPolicy<LoginCredentials, SimplePasswordPolicy.SimplePasswordStrength> passwordPolicy = new
SimplePasswordPolicy<>(4, 8);

// Throws a PasswordPolicyException since 'newPassword' is too long (> 8)
SimplePasswordPolicy.SimplePasswordStrength passwordStrength =
passwordPolicy.verify(LoginCredentials.of("jsmith", new RawPassword("password")), "newPassword");

// Returns the strength of the password
SimplePasswordPolicy.SimplePasswordStrength passwordStrength =
passwordPolicy.verify(LoginCredentials.of("jsmith", new RawPassword("password")), "newPassword");

// WEAK, MEDIUM, STRONG...
passwordStrength.getQualifier();

// 10, 42, 100... The higher the better
passwordStrength.getScore();

```

Please consider [NIST Digital Identity Guidelines Section 5.1.1.2](#) if you need to create more elaborate implementations.

The `PasswordEncoder` was covered previously in this documentation, it is used to evenly encode passwords before they are stored in the repository.



The API currently provides two `UserRepository` implementations:

- the `InMemoryUserRepository` which stores users in a `ConcurrentHashMap`.
- the `RedisUserRepository` which stores users in a `Redis` datastore.

By default, they both use a default `SimplePasswordPolicy` as password policy and a `PBKDF2Password.Encoder` as password encoder. Custom password policy and encoder can be specified as follows:

```
// Required to access Redis datastore
RedisClient<String, String> redisClient = null;

// Required to serialize/deserialize users to/from JSON strings
ObjectMapper mapper = null;

// Use BCrypt hashing function and enforce passwords between 10 and 20 characters
UserRepository<PersonIdentity, User<PersonIdentity>> redisUserRepository = new RedisUserRepository<>
(redisClient, mapper, new BCryptPassword.Encoder(8, 32), new SimplePasswordPolicy<>(10,20) );
```

A `UserRepository` can be typically exposed in a REST interface consumed by an admin UI in order to manage application's users.

## Credentials matcher

A credentials matcher is usually used in conjunction with a credentials resolver within `Authenticator` implementations to match credentials against trusted credentials resolved using the credentials resolver. Both `PrincipalAuthenticator` and `UserAuthenticator` uses this technique to authenticate `LoginCredentials` identified by the username.

The `CredentialsMatcher` interface is a functional interface defining one `matches()` method which must be reflexive, symmetric and transitive. A simplistic implementation can then be created as follows:

```
CredentialsMatcher<LoginCredentials, LoginCredentials> credentialsMatcher = (credentials,
trustedCredentials) -> {
    return credentials.getPassword().matches(trustedCredentials.getPassword());
};
```

### LoginCredentialsMatcher

The API provides `LoginCredentialsMatcher` implementation which basically check that usernames are equal and that passwords are matching.

```
// Match user provided login credentials against trusted user credentials
CredentialsMatcher<LoginCredentials, User<PersonIdentity>> credentialsMatcher = new
LoginCredentialsMatcher();
```

## Identity resolver

In a security manager, an identity resolver is responsible for resolving the `Identity` of an authenticated entity based on the `Authentication` returned by an `Authenticator`.

The `IdentityResolver` interface is a functional interface defining one `resolveIdentity()` method which makes it easy to create inline implementations:

```
IdentityResolver<PrincipalAuthentication, PersonIdentity> identityResolver = authentication -> {  
    // The authentication is a proof of authentication, we can assume valid credentials have been  
    provided  
    String authenticatedUsername = authentication.getUsername();  
  
    // Retrieve user identity from a reactive data source using the authenticated username  
    Mono<PersonIdentity> identity = ...  
  
    return identity;  
};
```

A security manager may or may not use an identity manager depending on what is needed by the application. Identity resolution is also not exclusive to the identity resolver, there might be cases where identity information can actually be resolved during the authentication process, these information can then be exposed in an specific authentication and used in an identity resolver to create the actual identity exposed in the security context.

We can also think of various use cases where the identity can not or should not be resolved during the authentication process. For instance, in token based authentication, a token can be authenticated using cryptographic techniques (e.g. signature) without requiring to communicate with an external system which might have provided identity information, identity can then be resolved next by the identity resolver if the application needs it. Again, it is important to understand that authentication and identity are not necessarily correlated, the `LDAPIdentityResolver` provided in the `security-ldap` module is a good example that can be used after another authenticator than the `LDAPAuthenticator`.

## UserIdentityResolver

The `UserAuthenticator` is a good example of identity information resolved during authentication. The identity is resolved with trusted credentials used for authentication in order to save resources. However a security manager still requires an identity resolver in order to expose the identity in the security context. In this particular case, the `UserIdentityResolver` can be used to simply extract the identity from the `UserAuthentication` and returns it to the security manager.

```
// Simply returns the identity resolved during authentication  
IdentityResolver<UserAuthentication<PersonIdentity>, PersonIdentity> identityResolver = new  
UserIdentityResolver<UserAuthentication<PersonIdentity>, PersonIdentity>();
```

## AccessController resolver

In a security manager, an access controller resolver is responsible for resolving the authorizations granted to the authenticated entity based on the `Authentication` returned by an `Authenticator` in order to control its access to protected services and resources using an `AccessController`.

The `AccessControllerResolver` interface is a functional interface defining method `resolveAccessController()`, a simple inline implementation can be created as follows:

```
AccessControllerResolver<PrincipalAuthentication, RoleBasedAccessController>
accessControllerResolver = authentication -> {
    // The authentication is a proof of authentication, we can assume valid credentials have been
    provided
    String authenticatedUsername = authentication.getUsername();

    // Retrieve the role of the authenticated entity from a reactive data source using the
    authenticated username
    Mono<Set<String>> roles = ...

    return roles.map(RoleBasedAccessController::of);
};
```

As for the [identity resolver](#), a security manager may or may not use an access controller resolver depending on application's needs. As for identity resolution, access control information (e.g. roles, permissions...) can be resolved during authentication. For instance, the `UserAuthenticator` resolves user's groups along with trusted credentials used for authentication. These information can then be passed in the authentication and used within the access controller resolver to create the `AccessController` used to control the access to protected service and resources for the authenticated entity.

## GroupsRoleBasedAccessControllerResolver

The `GroupsRoleBasedAccessControllerResolver` uses the set of groups exposed in a `GroupAwareAuthentication` (e.g. `UserAuthentication`) to create a [role-based access controller](#).

```
AccessControllerResolver<GroupAwareAuthentication, RoleBasedAccessController>
accessControllerResolver = new GroupsRoleBasedAccessControllerResolver();
```

## ConfigurationSourcePermissionBasedAccessControllerResolver

The `ConfigurationSourcePermissionBasedAccessControllerResolver` creates a [permission-based access controller](#) for the authenticated entity identified by a username. The resulting access controller is backed by a [configuration source](#) which defines permissions by username.

```
// The configuration source defining permissions by user
ConfigurationSource<?, ?, ?> configurationSource = null;

ConfigurationSourcePermissionBasedAccessControllerResolver accessControllerResolver = new
ConfigurationSourcePermissionBasedAccessControllerResolver(configurationSource);
```

# Security Context

The security context is the central component used to secure an application. It is obtained from a [security manager](#) after credentials authentication. It is composed of the following sub-components:

- an **Authentication** which results from the authentication of credentials and proves that there was an authentication.
- an **Identity** which provides information about the identity of the authenticated entity.
- an **AccessController** which provides services to determine whether the authenticated entity has the right to access protected services or resources within the application.

These basically correspond to the three main concepts composing the Inverno security model as described in the [introduction](#) of the *security* module.

A **SecurityContext** instance should be distributed in the application anywhere there is a need to protect services and resources (i.e. authentication and access control) or a need for information about the authenticated entity (i.e. identification). It is usually obtained from a security manager but it is also possible to create a security context from previous components as follows:

```
Authentication authentication = Authentication.granted();
PersonIdentity identity = new PersonIdentity("jsmith", "John", "Smith", "jsmith@inverno.io");
RoleBasedAccessController accessController = RoleBasedAccessController.of("reader", "writer");

SecurityContext<PersonIdentity, RoleBasedAccessController> securityContext =
    SecurityContext.of(authentication, identity, accessController);
```

This construct can be useful for testing but it is important to remember that the API specifies that an authentication must represent the proof that credentials were authenticated which basically guarantees that the security context can be trusted. As a result, the security manager should always be preferred to create the security context.

## Authentication

An authentication results from an authentication process and represents the proof that [credentials](#) were authenticated, typically by an [authenticator](#). In other words, it guarantees that the entity accessing the application has provided credentials and that they have been authenticated successfully or not.

An **Authentication** is always present in a security context but this does not mean credentials have been successfully authenticated, it simply means that there was an authentication. It can then take three forms:

- **anonymous** which corresponds to an authentication which is not authenticated with no cause of error and indicates that authentication was bypassed and application is accessed anonymously.
- **denied** which corresponds to an authentication which is not authenticated with a cause of error (e.g. invalid credentials...) and indicates a failed authentication.

- **granted** which corresponds to an authenticated authentication and indicates a successful authentication.

From there, it is up to the application to authorize anonymous access and decide what to do in case of denied access. The following example shows how to fully handle authentication in a security context:

```
SecurityContext<PersonIdentity, RoleBasedAccessController> securityContext = ...

if(securityContext.getAuthentication().isAuthenticated()) {
    // Application is accessed by an authenticated entity:
    // - use access controller to secure services and resources
    // - use identity to get information about the authenticated entity
    ...
}
else if(securityContext.getAuthentication().isAnonymous()) {
    // Application is accessed anonymously: we can grant partial access or deny access
    ...
}
else {
    // Authentication failed: we should deny access and report the error
    LOGGER.error(securityContext.getAuthentication().getCause().get());
    ...
}
```

By extension, a security context can be anonymous, denied or granted as described in the [security manager](#). A denied or anonymous security context always returns empty identity and access controller. Previous code can then be rewritten as follows:

```
SecurityContext<PersonIdentity, RoleBasedAccessController> securityContext = ...

if(securityContext.isAuthenticated()) {
    // Application is accessed by an authenticated entity:
    // - use access controller to secure services and resources
    // - use identity to get information about the authenticated entity
    ...
}
else if(securityContext.isAnonymous()) {
    // Application is accessed anonymously: we can grant partial access or deny access
    ...
}
else {
    // Authentication failed: we should deny access and report the error
    LOGGER.error(securityContext.getAuthentication().getCause().get());
    ...
}
```

You might have notice that, unlike identity and access controller types, the authentication type is not defined as formal parameter in the `SecurityContext` interface. The authentication type is important in the security manager which uses specific identity and access controller resolvers for which the actual authentication type is important, however it is no longer useful in the security context which only needs to determine whether authentication is anonymous, denied or granted.

# Identity

The identity exposes information that identifies that authenticated entity, it is resolved by the security manager using an [identity resolver](#).

A security context may or may not expose an identity depending on several elements such as whether identity is required by the application or whether an identity can be resolved based on the credentials provided to the security manager. In any case, the application must be prepared to handle security context with no identity.

```
SecurityContext<PersonIdentity, RoleBasedAccessController> securityContext = ...
```

```
securityContext.getIdentity().ifPresentOrElse(  
    identity -> {  
        // Send an email to the authenticated user  
        String email = identity.getEmail();  
        ...  
    },  
    () -> {  
        LOGGER.warn("Unable to send email: missing identity");  
        ...  
    }  
);
```

## Access Controller

The access controller provides services used to determine whether access to protected service or resource should be granted to the authenticated entity, it is resolved by the security manager using an [access controller resolver](#).

As for the identity, the application should not assume that a security context exposes an access controller for an authenticated entity and it must be prepared to deal with a missing access controller.

```
SecurityContext<PersonIdentity, RoleBasedAccessController> securityContext = ...
```

```
Mono<String> protectedReactiveService = securityContext.getAccessController()  
    .map(accessController2 -> accessController2  
        .hasRole("reader")  
        .map(hasRole -> {  
            if(!hasRole) {  
                throw new ForbiddenException();  
            }  
            // User is authorized: do something useful  
            return "User is a reader";  
        })  
    )  
    .orElseThrow(() -> new InternalServerErrorException("Missing access controller"));
```

The API provides **AccessController** implementations to get [role-based access control](#) or permission-based access control.

## RoleBasedAccessController

A role-based access controller defines services used to determine whether an authenticated entity has a particular set of roles. [Role-based access control](#) is used to protect access to services or resources based on the roles that were assigned to the authenticated user.

A `RoleBasedAccessController` is ideally obtained from an authentication by a security manager using a specific access controller resolver, but a simple instance can also be created from a collection of roles as follows:

```
RoleBasedAccessController accessController = RoleBasedAccessController.of("reader", "writer");
```

This construct can be useful for `AccessControllerResolver` implementations and testing purposes.

The `RoleBasedAccessController` interface basically defines three methods: `hasRole()` used to determine whether the authenticated entity has a specific role, `hasAnyRole()` used to determine whether the authenticated entity has any of the roles in a set of roles and `hasAllRole()` used to determine whether the authenticated entity has all the roles in a set of roles.

```
SecurityContext<PersonIdentity, RoleBasedAccessController> securityContext = ...
```

```
securityContext.getAccessController()
    .ifPresent(accessController2 -> {
        // Returns true if the authenticated user has role 'reader'
        Mono<Boolean> canRead = accessController2.hasRole("reader");

        // Returns true if the authenticated user has any of the roles: 'writer', 'admin'
        Mono<Boolean> canWrite = accessController2.hasAnyRole("writer", "admin");

        // Returns true if the authenticated user has all of the roles: 'reader', 'writer'
        Mono<Boolean> canReadAndWrite = accessController2.hasAllRoles("reader", "writer");
    });
```

These methods are reactive to support implementations using non-blocking operations.

## PermissionBasedAccessController

A permission-based access controller defines services used to determine whether an authenticated has the required permissions to access a protected service or resource. Access to services or resources is then controlled based on the permissions granted to the authenticated user for a particular context. Permissions are evaluated in a context defined by a set of parameters, such permissions are referred as **parameterized permissions**.

The `PermissionBasedAccessController` interface basically defines three kind of methods: `hasPermission()` used to determine whether the authenticated user has a particular permission in a particular context, `hasAnyPermission()` used to determine whether the authenticated entity has any of the permissions in a set of permissions in a particular context and `hasAllPermissions()` used to determine whether the authenticated entity has all the permissions in a set of permissions in a particular context.

```

SecurityContext<PersonIdentity, PermissionBasedAccessController> securityContext = null;

securityContext.getAccessController()
    .ifPresent(accessController -> {
        // Returns true if the authenticated user has permission read
        Mono<Boolean> canRead = accessController.hasPermission("read");

        // Returns true if the authenticated user has permission read on 'contract' documents
        Mono<Boolean> canReadContracts = accessController.hasPermission("read",
PermissionBasedAccessController.Parameter.of("documentType", "contract"));

        // Returns true if the authenticated user has permission 'manage' or 'admin'
        Mono<Boolean> canManagePrinter = accessController.hasAnyPermission(Set.of("manage",
"admin"));

        // Returns true if the authenticated user has permission can manage printer 'lp1200'
        Mono<Boolean> canManagePrinterLP1200 = accessController.hasAnyPermission(Set.of("manage",
"admin"), PermissionBasedAccessController.Parameter.of("printer", "lp1200"));

        // Returns true if the authenticated user can book and modify 'AF' flights from 'Only'
airport
        Mono<Boolean> canBookAndModify = accessController.hasAllPermissions(Set.of("book",
"modify"), PermissionBasedAccessController.Parameter.of("company", "AF"),
PermissionBasedAccessController.Parameter.of("origin", "ORY"));
    });

```

Parameterized permissions are very powerful and offer the most flexibility to control access to protected services and resources by taking the operational context into account. They are very similar to parameterized configuration properties as described in the *configuration* module. It is then no surprise that the API provides the `ConfigurationSourcePermissionBasedAccessController` implementation which is backed by a `ConfigurationSource` to resolve permissions as configuration properties defined as follows:

- the property name can be either a username or a role name prefixed with a role prefix to differentiate them from users (defaults is `ROLE_`)
- the property parameters are the permissions parameters defining the context into which permissions are defined
- the property value is a comma separated list of permissions defined using the following rules:
  - `permission` to indicates a granted permission
  - `!permission` to indicates that a permission must not be granted
  - `*` to indicate that all permissions are granted

The configuration source can be configured to use various defaulting strategies depending on the needs, it is however common to use a `DefaultingStrategy.wildcard()` strategy as it is more adapt than the `DefaultingStrategy.lookup()` strategy in that particular context.

Considering the following permissions defined in a `CPropsFileConfigurationSource`:



```
[ domain = "printer" ] {
    # jsmith has role 'user' and therefore permission to query to any printer in the printer
domain
    ROLE_user="query"
    ROLE_admin="*"
}

[ domain = "printer", printer = "lp1200" ] {
    # jsmith has permission to query and print to printer lp1200
    jsmith="query,print"
}

[ printer="epsoncolor" ] {
    # jsmith has permission to manage printer epsoncolor across all domains
    # when querying with (domain=printer,printer=epsoncolor) the permission is actually 'query'
because domain parameter has the highest priority
    jsmith="manage"
    ROLE_user="query,print"
}

[ domain = "printer", printer = "XP-4100" ] {
    # jsmith has all permission on printer XP-4100
    jsmith="*"
}

[ domain = "printer", printer = "HL-L6400DW" ] {
    ROLE_user="query,print"
}

[ domain = "printer", printer = "C400V-DN" ] {
    jsmith="*,!manage"
}
}
```

We can then control permissions for user `jsmith` as follows:

```
CPropsFileConfigurationSource src = new CPropsFileConfigurationSource(new
ClasspathResource(URI.create("classpath:/permissions.cprops")))
    .withDefaultingStrategy(DefaultingStrategy.wildcard());

PermissionBasedAccessController pbac = new ConfigurationSourcePermissionBasedAccessController(src,
"jsmith", Set.of("user"));

// true: 'jsmith' has role 'user' for which permission query is granted in domain 'printer'
pbac.hasPermission("query", "domain", "printer").block();

// true: 'jsmith' has role 'user' for which permission query is granted in domain 'printer'
pbac.hasPermission("query", "domain", "printer", "printer", "TM-C3500").block();

// false: 'jsmith' only have permission query in domain 'printer'
pbac.hasPermission("query").block();

// true: 'jsmith' has all permissions on printer 'XP-4100' in domain 'printer'
pbac.hasPermission("manage", "domain", "printer", "printer", "XP-4100").block();

// true: 'jsmith' has all permissions but 'manage' permission on printer 'C400V-DN' in domain
'printer'
pbac.hasPermission("print", "domain", "printer", "printer", "C400V-DN").block();

// false: 'jsmith' has all permissions but 'manage' permission on printer 'C400V-DN' in domain
'printer'
pbac.hasPermission("manage", "domain", "printer", "printer", "C400V-DN").block();
```

It is important to remember that when using a defaulting strategy, the order into which parameters are specified in the query can impact results. For instance, the wildcard strategy gives priority to the permission defined with the most parameters and in case of conflict to parameters defined from left to right in the query.

■

*With great power comes great responsibility.* As you can imagine, this particular permission-based access controller implementation is quite complex and requires rigor to be used properly. The more parameters are considered, the more difficult it is to define permissions. This might also have an impact on performances, especially when a defaulting strategy is used (wildcard defaulting may require  $2^n$  queries on the configuration source where  $n$  is the number of parameter). As a guideline, you should try to consider limited number of parameters (ideally two and not more than three) and consider caching permissions.

As of now, the impact on performances that might be introduced by the `ConfigurationSourcePermissionBasedAccessController` is still unclear due to limited real-life feedbacks which is why no big decision was taken yet to provide caching solutions. Possible solutions include using multiple dedicated Redis replicas when using a `RedisConfigurationSource` or caching the complete list of permissions by user in an in-memory configuration source.

## Security HTTP

The Inverno *security-http* module extends the security API and the HTTP server API respectively defined in the *security* module and the *http-server* module in order to secure access to an HTTP server or a Web application.

It defines a complete API for authenticating HTTP requests and exposing the resulting security context in the exchange context which can then be used in exchange interceptors and handlers to secure the application.

Base implementations for various HTTP and Web security standards are also provided. The module currently supports the following features:

- HTTP [basic](#) authentication scheme.
- HTTP [digest](#) authentication scheme.
- Form based authentication.
- Token based authentication.
- Cross-origin resource sharing support ([CORS](#)).
- Protection against Cross-site request forgery attack ([CSRF](#)).

In order to use the Inverno *security-http* module, we need to declare a dependency in the module descriptor:

```
module io.inverno.example.app {  
    ...  
    requires io.inverno.mod.security.http;  
    ...  
}
```

And also declare that dependency in the build descriptor:

Using Maven:

```
<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-security-http</artifactId>
    </dependency>
  </dependencies>
</project>
```

Using Gradle:

```
...
compile 'io.inverno.mod:inverno-security-http:1.5.3'
...
```

Let's quickly see how to secure a simple Web application exposing a single hello world service using basic authentication. The application might initially look like:

```
package io.inverno.example.app_web_security;

import io.inverno.core.annotation.Bean;
import io.inverno.core.v1.Application;
import io.inverno.mod.http.base.Method;
import io.inverno.mod.web.annotation.WebController;
import io.inverno.mod.web.annotation.WebRoute;

@Bean
@WebController
public class Main {

    @WebRoute( path = "/hello", method = Method.GET)
    public String hello() {
        return "Hello world!";
    }

    public static void main(String[] args) {
        Application.run(new App_web_security.Builder());
    }
}
```

We can run and test the application which should respond with **Hello world!** when requesting `http://localhost:8080/hello`:

• • •

[===== 100 %  
=====]

```
|      , ~~, |  
|    , ' ^ ' ,  
|   , _ V _ ,  
|  , \\\V\\// / ,  
|   , _\V/_ ,  
|  , _\^/\_ ,  
|   , // ^\^ \\  
|    , ^ ,  
|   , V ,  
|    ' - - '
```

```
|      -  
| | | _ _ _ _ _  
| | / _ \\ \ / // _ \ / _ / _ \ / \  
| | | | | \ V / | _ / | | | | | | |  
|_|_| |_| \ / \ _||_| |_| |_| \ /
```

```
|                                     -- 1.5.1 --
```

---

```
| Java runtime       : OpenJDK Runtime Environment  
| Java version      : 18+36-2087  
| Java home         : /home/jkuhn/Devel/jdk/jdk-18  
|  
| Application module : io.inverno.example.app_web_security  
| Application class  : io.inverno.example.app_web_security.Main  
|  
| Modules           :  
| ...
```

```
$ curl -i http://localhost:8080/hello
HTTP/1.1 200 OK
content-length: 12

Hello world!
```

From there, let's say we want to protect the access to all routes requiring [HTTP basic authentication](#). In order to do this we must authenticate basic credentials provided within requests and reject requests (401) on denied authentication in which case a basic authentication challenge must also be sent to the client.

A Web configurer must be created to define a **security interceptor** that will authenticate requests and use a **BasicAuthenticationErrorInterceptor** to intercept unauthorized (401) errors and return the basic authentication challenge to the client.

```

package io.inverno.example.app_web_security;

import io.inverno.core.annotation.Bean;
import io.inverno.mod.http.base.UnauthorizedException;
import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.security.accesscontrol.AccessController;
import io.inverno.mod.security.authentication.LoginCredentialsMatcher;
import io.inverno.mod.security.authentication.password.RawPassword;
import io.inverno.mod.security.authentication.user.InMemoryUserRepository;
import io.inverno.mod.security.authentication.user.User;
import io.inverno.mod.security.authentication.user.UserAuthenticator;
import io.inverno.mod.security.http.AccessControlInterceptor;
import io.inverno.mod.security.http.SecurityInterceptor;
import io.inverno.mod.security.http.basic.BasicAuthenticationErrorInterceptor;
import io.inverno.mod.security.http.basic.BasicCredentialsExtractor;
import io.inverno.mod.security.http.context.InterceptingSecurityContext;
import io.inverno.mod.security.identity.Identity;
import io.inverno.mod.web.ErrorWebRouter;
import io.inverno.mod.web.ErrorWebRouterConfigurer;
import io.inverno.mod.web.WebInterceptable;
import io.inverno.mod.web.WebInterceptorsConfigurer;
import java.util.List;

@Bean( visibility = Bean.Visibility.PRIVATE )
public class SecurityConfigurer implements
WebInterceptorsConfigurer<InterceptingSecurityContext<Identity, AccessController>>,
ErrorWebRouterConfigurer<ExchangeContext> {

    @Override
    public void configure(WebInterceptable<InterceptingSecurityContext<Identity, AccessController>,
?> interceptors) {
        interceptors
            .intercept()
                .interceptors(List.of(SecurityInterceptor.of(
                    new BasicCredentialsExtractor(), // 1
                    new UserAuthenticator<>( // 2
                        InMemoryUserRepository // 3
                            .of(List.of(
                                User.of("jsmith")
                                    .password(new RawPassword("password"))
                                    .build()
                            ))
                        .build(),
                    new LoginCredentialsMatcher<>()
                ))
            ),
            AccessControlInterceptor.authenticated() // 4
        );
    }

    @Override
    public void configure(ErrorWebRouter<ExchangeContext> errorRouter) {
        errorRouter
            .intercept()
                .error(UnauthorizedException.class)
                .interceptor(new BasicAuthenticationErrorInterceptor<>("inverno-basic")) // 5
            // We must apply interceptors to intercept white labels error routes
            .applyInterceptors(); // 6
    }
}

```

The Web configurer implements `WebInterceptorsConfigurer` in order to configure route interceptors and `ErrorWebRouterConfigurer` in order to configure error route interceptors and apply them to all error routes (including default ones). It declares the `InterceptingSecurityContext` exchange context type which is required by the `SecurityInterceptor` to set the security context. Interceptors are defined to intercept all routes.

In above code, there are several things that deserve further explanation:

1. The `SecurityInterceptor` is the Web counterpart of the `SecurityManager`, it is used to authenticate credentials provided in HTTP requests and create the security context which is then exposed in the exchange context and accessible to exchange interceptors and handlers.
2. In addition to the authenticator and optional identity and access controller resolvers, it requires a credentials extractor used to extract `Credentials` from the request. The `BasicCredentialsExtractor` basically extracts `LoginCredentials` (username/password) from the `authorization` HTTP header of the request.
3. The security interceptor can then use any authenticator that is able to authenticate login credentials such as the `UserAuthenticator`.
4. An access control interceptor is added next in order to limit the access to authenticated users. Just like the security manager, the security interceptor authenticates credentials and creates the security context. But that does not mean authentication was successful, the resulting security context can be anonymous, denied or authenticated.
5. The `BasicAuthenticationErrorInterceptor` intercepts unauthorized (401) errors and set the basic authentication scheme challenge in the `www-authenticate` HTTP header of the response with the `inverno-basic` realm.
6. The Web server provides white labels error routes by default which must be explicitly intercepted since they have been created before on an unintercepted router.

Having to explicitly apply interceptors on default routes can be a source of errors and misunderstanding but there is unfortunately no other way if we want to make them overridable. A systematic and safe approach to this issue would be to always override default error routes.

We should now receive an unauthorized (401) error with a basic authentication challenge when requesting `http://localhost:8080/hello` (or any other endpoint) without credentials:

```
$ curl -i http://127.0.0.1:8080/hello
HTTP/1.1 401 Unauthorized
www-authenticate: basic realm="inverno-basic"
content-length: 0
```

In order to access the service, we must provide valid credentials in the `authorization` HTTP header. Basic authentication scheme specifies that credentials are obtained by encoding in base64 the concatenation of the username, a single colon and the password. In our example credentials for user `jsmith` are then `anNtaXR0OnBhc3N3b3Jk`:

```
$ curl -i -H 'authorization: basic anNtaXR0OnBhc3N3b3Jk' http://127.0.0.1:8080/hello
HTTP/1.1 200 OK
content-length: 12

Hello world!
```

We can change the `/hello` route handler to respond with a personalized message. This requires to resolve the identity of the user and use it in the handler.

We use a user repository which can provide user's identity, a `UserIdentityResolver` can then be used in the security interceptor to resolve it and make it available in the security context:



```

package io.inverno.example.app_web_security;

import io.inverno.core.annotation.Bean;
import io.inverno.mod.http.base.UnauthorizedException;
import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.security.accesscontrol.AccessController;
import io.inverno.mod.security.authentication.LoginCredentialsMatcher;
import io.inverno.mod.security.authentication.password.RawPassword;
import io.inverno.mod.security.authentication.user.InMemoryUserRepository;
import io.inverno.mod.security.authentication.user.User;
import io.inverno.mod.security.authentication.user.UserAuthenticator;
import io.inverno.mod.security.http.AccessControlInterceptor;
import io.inverno.mod.security.http.SecurityInterceptor;
import io.inverno.mod.security.http.basic.BasicAuthenticationErrorInterceptor;
import io.inverno.mod.security.http.basic.BasicCredentialsExtractor;
import io.inverno.mod.security.http.context.InterceptingSecurityContext;
import io.inverno.mod.security.identity.PersonIdentity;
import io.inverno.mod.security.identity.UserIdentityResolver;
import io.inverno.mod.web.ErrorWebRouter;
import io.inverno.mod.web.ErrorWebRouterConfigurer;
import io.inverno.mod.web.WebInterceptable;
import io.inverno.mod.web.WebInterceptorsConfigurer;
import java.util.List;

@Bean( visibility = Bean.Visibility.PRIVATE )
public class SecurityConfigurer implements
WebInterceptorsConfigurer<InterceptingSecurityContext<PersonIdentity, AccessController>>,
ErrorWebRouterConfigurer<ExchangeContext> {

    @Override
    public void configure(WebInterceptable<InterceptingSecurityContext<PersonIdentity,
AccessController>, ?> interceptors) {
        interceptors
            .intercept()
                .interceptors(List.of(SecurityInterceptor.of(
                    new BasicCredentialsExtractor(),
                    new UserAuthenticator<>()
                        .InMemoryUserRepository
                            .of(List.of(
                                User.of("jsmith")
                                    .password(new RawPassword("password"))
                                    .identity(new PersonIdentity("jsmith", "John", "Smith",
"jsmith@inverno.io")))
                            .build()
                        ))
                    .build(),
                    new LoginCredentialsMatcher<>()
                ),
                new UserIdentityResolver<>()
            ),
            AccessControlInterceptor.authenticated()
        );
    }

    @Override
    public void configure(ErrorWebRouter<ExchangeContext> errorRouter) {
        errorRouter
            .intercept()
                .error(UnauthorizedException.class)
    }
}

```

```

        .interceptor(new BasicAuthenticationErrorInterceptor<>("inverno-basic"))
        // We must apply interceptors to intercept white labels error routes
        .applyInterceptors();
    }
}

```

The `PersonIdentity` type is now declared in the `InterceptingSecurityContext` exchange context type and the identity is resolved from user's identity.

We can now inject the exchange security context in the route handler and get the identity to provide the personalized message:

```

package io.inverno.example.app_web_security;

import io.inverno.core.annotation.Bean;
import io.inverno.core.v1.Application;
import io.inverno.mod.http.base.Method;
import io.inverno.mod.security.accesscontrol.AccessController;
import io.inverno.mod.security.http.context.SecurityContext;
import io.inverno.mod.security.identity.PersonIdentity;
import io.inverno.mod.web.annotation.WebController;
import io.inverno.mod.web.annotation.WebRoute;

@Bean
@WebController
public class Main {

    @WebRoute( path = "/hello", method = Method.GET)
    public String hello(SecurityContext<? extends PersonIdentity, ? extends AccessController>
securityContext) {
        return "Hello " +
securityContext.getIdentity().map(PersonIdentity::getFirstName).orElse("whoever you are") + "!";
    }
}

```

Here we injected `io.inverno.mod.security.http.context.SecurityContext` which extends both `io.inverno.mod.security.context.SecurityContext` and `ExchangeContext`. This interface is not mutable and exposes the exact same components as the regular security context, it should be used in application's route interceptors and handlers. On the other hand, the `InterceptingSecurityContext` is mutable and should only be used by security related interceptors and the `SecurityInterceptor` in particular.

User `jsmith` should now receive a personalized message when requesting `http://localhost:8080/hello`:

```

$ curl -i -H 'authorization: basic anNtaXRoOnBhc3N3b3Jk' http://127.0.0.1:8080/hello
HTTP/1.1 200 OK
content-length: 11

Hello John!

```

Let's create another endpoint for VIP users responding with an extra polite message. VIP users can be placed into the `vip` group and a `RoleBasedAccessController` can be resolved using a `GroupsRoleBasedAccessControllerResolver`.

Let's start by creating the `/vip/hello` route:

```
package io.inverno.example.app_web_security;

import io.inverno.core.annotation.Bean;
import io.inverno.core.v1.Application;
import io.inverno.mod.http.base.ForbiddenException;
import io.inverno.mod.http.base.Method;
import io.inverno.mod.security.accesscontrol.AccessController;
import io.inverno.mod.security.accesscontrol.RoleBasedAccessController;
import io.inverno.mod.security.http.context.SecurityContext;
import io.inverno.mod.security.identity.PersonIdentity;
import io.inverno.mod.web.annotation.WebController;
import io.inverno.mod.web.annotation.WebRoute;
import reactor.core.publisher.Mono;

@Bean
@WebController
public class Main {

    ...
    @WebRoute( path = "/vip/hello", method = Method.GET)
    public Mono<String> hello_vip(SecurityContext<? extends PersonIdentity, ? extends
RoleBasedAccessController> securityContext) {
        return securityContext.getAccessController()
            .orElseThrow(() -> new ForbiddenException())
            .hasRole("vip")
            .map(isVip -> {
                if(!isVip) {
                    throw new ForbiddenException();
                }
                return "Hello my dear friend " +
securityContext.getIdentity().map(PersonIdentity::getFirstName).orElse("whoever you are") + "!";
            });
    }
    ...
}
```

You may have notice that we did not have to change the `/hello` route definition which can still declare `SecurityContext<? extends PersonIdentity, ? extends AccessController>` since it is assignable from the actual context type `SecurityContext<PersonIdentity, RoleBasedAccessController>` declared in the security configurer. Note that a compilation error would have been raised to report inconsistent exchange context types if we had not used upper bound wildcards.

We can now change the Web configurer to resolve the role-based access controller using a `GroupsRoleBasedAccessControllerResolver`.

```

package io.inverno.example.app_web_security;

import io.inverno.core.annotation.Bean;
import io.inverno.mod.http.base.UnauthorizedException;
import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.security.accesscontrol.GroupsRoleBasedAccessControllerResolver;
import io.inverno.mod.security.accesscontrol.RoleBasedAccessController;
import io.inverno.mod.security.authentication.LoginCredentialsMatcher;
import io.inverno.mod.security.authentication.password.RawPassword;
import io.inverno.mod.security.authentication.user.InMemoryUserRepository;
import io.inverno.mod.security.authentication.user.User;
import io.inverno.mod.security.authentication.user.UserAuthenticator;
import io.inverno.mod.security.http.AccessControlInterceptor;
import io.inverno.mod.security.http.SecurityInterceptor;
import io.inverno.mod.security.http.basic.BasicAuthenticationErrorInterceptor;
import io.inverno.mod.security.http.basic.BasicCredentialsExtractor;
import io.inverno.mod.security.http.context.InterceptingSecurityContext;
import io.inverno.mod.security.identity.PersonIdentity;
import io.inverno.mod.security.identity.UserIdentityResolver;
import io.inverno.mod.web.ErrorWebRouter;
import io.inverno.mod.web.ErrorWebRouterConfigurer;
import io.inverno.mod.web.WebInterceptable;
import io.inverno.mod.web.WebInterceptorsConfigurer;
import java.util.List;

@Bean( visibility = Bean.Visibility.PRIVATE )
public class SecurityConfigurer implements
WebInterceptorsConfigurer<InterceptingSecurityContext<PersonIdentity, RoleBasedAccessController>>,
ErrorWebRouterConfigurer<ExchangeContext> {

    @Override
    public void configure(WebInterceptable<InterceptingSecurityContext<PersonIdentity,
RoleBasedAccessController>, ?> interceptors) {
        interceptors
            .intercept()
                .interceptors(List.of(SecurityInterceptor.of(
                    new BasicCredentialsExtractor(),
                    new UserAuthenticator<>()
                        .InMemoryUserRepository
                            .of(List.of(
                                User.of("jsmith")
                                    .password(new RawPassword("password"))
                                    .identity(new PersonIdentity("jsmith", "John", "Smith",
"jsmith@inverno.io"))
                                .groups("vip")
                                    .build(),
                                User.of("adoe")
                                    .password(new RawPassword("password"))
                                    .identity(new PersonIdentity("adoe", "Alice", "Doe",
"adoe@inverno.io"))
                                    .build()
                            ))
                    ))
                .build(),
                new LoginCredentialsMatcher<>()
            ),
        new UserIdentityResolver<>(),
        new GroupsRoleBasedAccessControllerResolver()
    ),

```

```

        AccessControlInterceptor.authenticated()
    ));
}
...
}

```

The `RoleBasedAccessController` type is now declared in the `InterceptingSecurityContext` exchange context type, we also added another normal user and a role-based access controller based on users' groups is now resolved.

Accessing route `/hello` and `/vip/hello` with different users should provide the following results:

```

$ curl -i -H 'authorization: basic anNtaXRoOnBhc3N3b3Jk' http://127.0.0.1:8080/hello
HTTP/1.1 200 OK
content-length: 11

Hello John!

$ curl -i -H 'authorization: basic anNtaXRoOnBhc3N3b3Jk' http://127.0.0.1:8080/vip/hello
HTTP/1.1 200 OK
content-length: 26

Hello my dear friend John!

$ curl -i -H 'authorization: basic YWRvZTpwYXNzd29yZA==' http://127.0.0.1:8080/hello
HTTP/1.1 200 OK
content-length: 12

Hello Alice!

$ curl -i -H 'authorization: basic YWRvZTpwYXNzd29yZA==' http://127.0.0.1:8080/vip/hello
HTTP/1.1 403 Forbidden
content-length: 0

```

Here we have decided to control access inside the `/vip/hello` route handler but we could have also globally restrict access to `/vip/**` routes to VIP users using an `AccessControlInterceptor` in the security configurer:

```

package io.inverno.example.app_web_security;

import io.inverno.core.annotation.Bean;
import io.inverno.mod.http.base.ForbiddenException;
import io.inverno.mod.http.base.UnauthorizedException;
import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.security.accesscontrol.GroupsRoleBasedAccessControllerResolver;
import io.inverno.mod.security.accesscontrol.RoleBasedAccessController;
import io.inverno.mod.security.authentication.LoginCredentialsMatcher;
import io.inverno.mod.security.authentication.password.RawPassword;
import io.inverno.mod.security.authentication.user.InMemoryUserRepository;
import io.inverno.mod.security.authentication.user.User;
import io.inverno.mod.security.authentication.user.UserAuthenticator;
import io.inverno.mod.security.http.AccessControlInterceptor;
import io.inverno.mod.security.http.SecurityInterceptor;
import io.inverno.mod.security.http.basic.BasicAuthenticationErrorInterceptor;
import io.inverno.mod.security.http.basic.BasicCredentialsExtractor;
import io.inverno.mod.security.http.context.InterceptingSecurityContext;
import io.inverno.mod.security.identity.PersonIdentity;
import io.inverno.mod.security.identity.UserIdentityResolver;
import io.inverno.mod.web.ErrorWebRouter;
import io.inverno.mod.web.ErrorWebRouterConfigurer;
import io.inverno.mod.web.WebInterceptable;
import io.inverno.mod.web.WebInterceptorsConfigurer;
import java.util.List;

@Bean( visibility = Bean.Visibility.PRIVATE )
public class SecurityConfigurer implements
WebInterceptorsConfigurer<InterceptingSecurityContext<PersonIdentity, RoleBasedAccessController>>,
ErrorWebRouterConfigurer<ExchangeContext> {

    @Override
    public void configure(WebInterceptable<InterceptingSecurityContext<PersonIdentity,
RoleBasedAccessController>, ?> interceptors) {
        interceptors
            ...
            .intercept()
                .path("/vip/**")
                .interceptor(AccessControlInterceptor.verify(securityContext ->
securityContext.getAccessController()
                    .orElseThrow(() -> new ForbiddenException())
                    .hasRole("vip")
                ));
    }
    ...
}

```

The `/vip/hello` route handler can then be simplified while still being only accessible by VIP users:

```

package io.inverno.example.app_web_security;

import io.inverno.core.annotation.Bean;
import io.inverno.core.v1.Application;
import io.inverno.mod.http.base.Method;
import io.inverno.mod.security.accesscontrol.AccessController;
import io.inverno.mod.security.accesscontrol.RoleBasedAccessController;
import io.inverno.mod.security.http.context.SecurityContext;
import io.inverno.mod.security.identity.PersonIdentity;
import io.inverno.mod.web.annotation.WebController;
import io.inverno.mod.web.annotation.WebRoute;

@Bean
@WebController
public class Main {

    ...
    @WebRoute( path = "/vip/hello", method = Method.GET)
    public String hello_vip(SecurityContext<? extends PersonIdentity, ? extends
RoleBasedAccessController> securityContext) {
        return "Hello my dear friend " +
securityContext.getIdentity().map(PersonIdentity::getFirstName).orElse("whoever you are") + "!";
    }
    ...
}

```

If you followed the *security* module documentation, and you should have, you might have noticed how the *SecurityInterceptor* is similar to the *SecurityManager*, they basically have the same role which is to authenticate a request and provide a security context which, although we had to create an exchange security context, is still the central component used to secure the application. As a result, securing a Web application is no different than securing a regular application and it should therefore be easy to create secured components and libraries that can be integrated in both.

## Security Interceptor

The *SecurityInterceptor* is the main entry point for securing an HTTP server or a Web application, it is the counterpart of the *SecurityManager* for regular applications. Its role is to extract *Credentials* from HTTP requests and just like the *SecurityManager*, to authenticate them and possibly resolve an *Identity* and/or an *AccessController*. It then sets the resulting security context in the exchange. Exchange interceptors and handlers can then access the security context anytime for securing services and resources.

A *SecurityInterceptor* instance is created by composing a *CredentialsExtractor* used to extract *Credentials* from the request in addition to the *Authenticator* and optional *IdentityResolver* and *AccessControllerResolver*. It should be used to intercept request targeting services or resources that must be secured or require identity information.

Although it is completely possible to use it on the global exchange handler in the HTTP server controller, we will focus on securing Web routes in a Web server in the rest of this documentation as it covers more interesting use cases.

As for the `SecurityManager`, the `SecurityInterceptor` basically chains the extraction of credentials, the authentication, the identity resolution and the access controller resolution and sets the resulting `SecurityContext` in the exchange context declared as a `InterceptingSecurityContext`.

A `SecurityInterceptor` is created as follows:

```
CredentialsExtractor<Credentials> credentialsExtractor = ...
Authenticator<Credentials, Authentication> authenticator = ...
IdentityResolver<Authentication, Identity> identityResolver = ...
AccessControllerResolver<Authentication, AccessController> accessControllerResolver = ...

SecurityInterceptor<Credentials, Identity, AccessController, InterceptingSecurityContext<Identity,
AccessController>, Exchange<InterceptingSecurityContext<Identity, AccessController>>>
securityInterceptor = SecurityInterceptor.of(credentialsExtractor, authenticator, identityResolver,
accessControllerResolver);
```

It can be applied to Web routes just like any other exchange interceptor by defining a Web configurer implementing `WebInterceptorsConfigurer` or `WebRouterConfigurer`. The following example shows how to secure access by applying the security interceptor to all `/vip/**` routes:

```
package io.inverno.example.app_web_security;

import io.inverno.mod.security.accesscontrol.AccessController;
import io.inverno.mod.security.accesscontrol.AccessControllerResolver;
import io.inverno.mod.security.authentication.Authenticator;
import io.inverno.mod.security.identity.Identity;
import io.inverno.mod.security.identity.IdentityResolver;
import io.inverno.mod.security.http.CredentialsExtractor;
import io.inverno.mod.security.http.SecurityInterceptor;
import io.inverno.mod.security.http.context.InterceptingSecurityContext;
import io.inverno.mod.web.WebInterceptable;
import io.inverno.mod.web.WebInterceptorsConfigurer;

public class SecurityConfigurer implements
WebInterceptorsConfigurer<InterceptingSecurityContext<Identity, AccessController>> {

    @Override
    public void configure(WebInterceptable<InterceptingSecurityContext<PersonIdentity,
AccessController>, ?> interceptors) {
        CredentialsExtractor<Credentials> credentialsExtractor = ...
        Authenticator<Credentials, Authentication> authenticator = ...
        IdentityResolver<Authentication, Identity> identityResolver = ...
        AccessControllerResolver<Authentication, AccessController> accessControllerResolver = ...

        interceptors
            .intercept()
            .path("/vip/**")
            .interceptor(SecurityInterceptor.of(credentialsExtractor,
authenticator, identityResolver, accessControllerResolver));
    }
}
```



By combining various implementations of `CredentialsExtractor`, `Authenticator`, `IdentityResolver` and `AccessControllerResolver`, it is possible to implement any kind of HTTP authentication methods (e.g. basic, digest, token...). It is still good to remember that the role of the security interceptor is to authenticate credentials and create a resulting security context which can be anonymous, denied or authenticated, actual access control must be done in subsequent interceptors or within the route handler.

Since the security interceptor is a regular exchange interceptor, it is possible to define various instances applied to different routes. We can for instance imagine using different security interceptors implementing different authentication methods or targeting different user repositories based on the path, the language... basically any routing criteria exposed by the `WebRouteManager`.

## CredentialsExtractor

A credentials extractor is used in a security interceptor to extract `Credentials` from an HTTP request. The `CredentialsExtractor` interface is a functional interface defining method `extract()`. The following example shows a simple inline implementation that extract `LoginCredentials` from HTTP headers returning no credentials if either username or password is missing:

```
CredentialsExtractor<LoginCredentials> credentialsExtractor = exchange -> {  
    return Mono.fromSupplier(() -> exchange.request().headers().get("username")  
        .flatMap(username -> exchange.request().headers().get("password")  
            .map(RawPassword::new)  
            .map(password -> LoginCredentials.of(username, password))  
        )  
        .orElse(null)  
    );  
};
```

When no credentials are returned, the security interceptor creates an anonymous security context.

Multiple credentials extractor can be chained in order to extract credentials from different location within the request by order of preference. For instance, we can create a credentials extractor to extract `TokenCredentials` from an HTTP header, a cookie, or a query parameter in that order.

```

CredentialsExtractor<TokenCredentials> headerTokenCredentialsExtractor = exchange -> {
    return Mono.fromSupplier(() ->
exchange.request().headers().get("token").map(TokenCredentials::new).orElse(null));
};

CredentialsExtractor<TokenCredentials> cookieTokenCredentialsExtractor = exchange -> {
    return Mono.fromSupplier(() -> exchange.request().cookies().get("token").map(cookie -> new
TokenCredentials(cookie.asString()))).orElse(null));
};

CredentialsExtractor<TokenCredentials> queryTokenCredentialsExtractor = exchange -> {
    return Mono.fromSupplier(() -> exchange.request().queryParameters().get("token").map(parameter -
> new TokenCredentials(parameter.asString()))).orElse(null));
};

CredentialsExtractor<TokenCredentials> credentialsExtractor = headerTokenCredentialsExtractor
    .or(cookieTokenCredentialsExtractor)
    .or(queryTokenCredentialsExtractor);

```

## SecurityContext vs HTTP SecurityContext vs InterceptingSecurityContext

The *security-http* module provides `io.inverno.mod.security.http.context.SecurityContext` which extends both `ExchangeContext` and `io.inverno.mod.security.context.SecurityContext` defined in the *security* module. Although the security context semantic remains unchanged, this was necessary to be able to expose it as an exchange context. The `io.inverno.mod.security.http.context.SecurityContext` can be seen as a security exchange context, it must be used to secure HTTP endpoints as it can be accessed from the `Exchange` and injected in Web route handlers.

It also provides the `io.inverno.mod.security.http.context.InterceptingSecurityContext` which extends `io.inverno.mod.security.http.context.SecurityContext` and exposes a single `setSecurityContext()` method. This is a mutable version of the `io.inverno.mod.security.http.context.SecurityContext` which enables security related interceptors or handlers, such as the `SecurityInterceptor`, to set the `io.inverno.mod.security.context.SecurityContext` in the security exchange context.

In the end, every `ExchangeContext` types should be implemented in the generated global `ExchangeContext` type which will basically implements both `io.inverno.mod.security.http.context.SecurityContext` and `io.inverno.mod.security.http.context.InterceptingSecurityContext`. However making sure `io.inverno.mod.security.http.context.SecurityContext` is used in applicative interceptors and handlers and only allow the `io.inverno.mod.security.http.context.InterceptingSecurityContext` in specific trusted security interceptors and handlers is a good way to control and protect the security context against untrustful modifications.

# Access Control Interceptor

As we just saw, the role of the security interceptor is to authenticate credentials and provides a security context but it does not actually control access. The security context can be anonymous, denied or authenticated, actual access control must then be done in a subsequent interceptors and/or directly in the route handler. An `AccessControlInterceptor` can be applied on secured routes to control access globally.

In the following example, `AccessControlInterceptor.authenticated()` is used to create an interceptor that restricts access to authenticated users.

```
package io.inverno.example.app_web_security;

import io.inverno.mod.security.accesscontrol.AccessController;
import io.inverno.mod.security.accesscontrol.AccessControllerResolver;
import io.inverno.mod.security.authentication.Authenticator;
import io.inverno.mod.security.identity.Identity;
import io.inverno.mod.security.identity.IdentityResolver;
import io.inverno.mod.security.http.AccessControlInterceptor;
import io.inverno.mod.security.http.CredentialsExtractor;
import io.inverno.mod.security.http.SecurityInterceptor;
import io.inverno.mod.security.http.context.InterceptingSecurityContext;
import io.inverno.mod.web.WebInterceptable;
import io.inverno.mod.web.WebInterceptorsConfigurer;
import java.util.List;

public class SecurityConfigurer implements
WebInterceptorsConfigurer<InterceptingSecurityContext<Identity, AccessController>> {

    @Override
    public void configure(WebInterceptable<InterceptingSecurityContext<PersonIdentity,
AccessController>, ?> interceptors) {
        CredentialsExtractor<Credentials> credentialsExtractor = ...
        Authenticator<Credentials, Authentication> authenticator = ...
        IdentityResolver<Authentication, Identity> identityResolver = ...
        AccessControllerResolver<Authentication, AccessController> accessControllerResolver = ...

        interceptors
            .intercept()
            .path("/vip/**")
            .interceptors(List.of(
                SecurityInterceptor.of(credentialsExtractor, authenticator, identityResolver,
accessControllerResolver),
                AccessControlInterceptor.authenticated()
            ));
    }
}
```

We can use `AccessControlInterceptor.anonymous()` to restrict access to anonymous users or we can also provide custom access control using `AccessControlInterceptor.verify()` as follows:

```

package io.inverno.example.app_web_security;

import io.inverno.mod.http.base.ForbiddenException;
import io.inverno.mod.security.accesscontrol.AccessControllerResolver;
import io.inverno.mod.security.accesscontrol.RoleBasedAccessController;
import io.inverno.mod.security.authentication.Authentication;
import io.inverno.mod.security.authentication.Authenticator;
import io.inverno.mod.security.authentication.Credentials;
import io.inverno.mod.security.http.AccessControlInterceptor;
import io.inverno.mod.security.http.CredentialsExtractor;
import io.inverno.mod.security.http.SecurityInterceptor;
import io.inverno.mod.security.http.context.InterceptingSecurityContext;
import io.inverno.mod.security.identity.Identity;
import io.inverno.mod.security.identity.IdentityResolver;
import io.inverno.mod.web.WebInterceptable;
import io.inverno.mod.web.WebInterceptorsConfigurer;
import java.util.List;

public class SecurityConfigurer implements
WebInterceptorsConfigurer<InterceptingSecurityContext<Identity, RoleBasedAccessController>> {

    @Override
    public void configure(WebInterceptable<InterceptingSecurityContext<Identity,
RoleBasedAccessController>, ?> interceptors) {
        CredentialsExtractor<Credentials> credentialsExtractor = null;
        Authenticator<Credentials, Authentication> authenticator = null;
        IdentityResolver<Authentication, Identity> identityResolver = null;
        AccessControllerResolver<Authentication, RoleBasedAccessController> accessControllerResolver
= null;

        interceptors
            .intercept()
                .path("/vip/**")
                .interceptors(List.of(
                    SecurityInterceptor.of(credentialsExtractor, authenticator, identityResolver,
accessControllerResolver),
                    AccessControlInterceptor.verify(securityContext ->
securityContext.getAccessController()
                        .orElseThrow(() -> new ForbiddenException())
                        .hasRole("vip")
                    )
                ));
    }
}

```

## HTTP authentication

By combining `CredentialsExtractor` with `Authenticator`, it is possible to implement various HTTP authentication methods. The security HTTP API provides credentials extractors as well as exchange interceptors and handlers that facilitate the configuration of standard HTTP authentication methods in Web applications.

# HTTP Basic authentication

The [basic HTTP authentication scheme](#) is, as its name suggests, a basic authentication method on top of HTTP in which credentials are provided in the [authorization](#) HTTP header in the form `basic Base64(username ":" password)`. Basic authentication can be requested to the client (e.g. a Web browser) by specifying a `www-authenticate` HTTP header in an unauthorized (401) response sent when a protected resource is requested without credentials or with invalid credentials.

A security context implementing HTTP basic authentication is obtained by combining the [BasicCredentialsExtractor](#) which extracts [LoginCredentials](#) with a compatible [Authenticator](#) implementation. The following example uses a basic [PrincipalAuthenticator](#) with an in-memory login credentials resolver in order to secure `/basic/**` routes:

```
package io.inverno.example.app_web_security;

...
import io.inverno.mod.security.http.basic.BasicCredentialsExtractor;
...

...
public class SecurityConfigurer implements
WebInterceptorsConfigurer<InterceptingSecurityContext<Identity, AccessController>> {

    @Override
    public void configure(WebInterceptable<InterceptingSecurityContext<Identity, AccessController>,
?> interceptors) {
        interceptors
            .intercept()
                .path("/basic/**")
                .interceptor(SecurityInterceptor.of(
                    new BasicCredentialsExtractor(),
                    new PrincipalAuthenticator<>()
                        .new InMemoryLoginCredentialsResolver(List.of(
                            LoginCredentials.of("john", new
MessageDigestPassword.Encoder().encode("password")),
                            LoginCredentials.of("alice", new
MessageDigestPassword.Encoder().encode("password")),
                            LoginCredentials.of("bob", new
MessageDigestPassword.Encoder().encode("password"))
                        )),
                    new LoginCredentialsMatcher<LoginCredentials, LoginCredentials>()
                )
            );
    }
}
```

In order to fully implement HTTP basic authentication scheme as defined by [RFC 7617](#), we also need to send a basic authentication challenge on unauthorized (401) errors. This can be done by intercepting [UnauthorizedException](#) on secured routes using a [BasicAuthenticationErrorInterceptor](#):

```

package io.inverno.example.app_web_security;

...
import io.inverno.mod.security.http.basic.BasicAuthenticationErrorInterceptor;
...

...
public class SecurityConfigurer implements
WebInterceptorsConfigurer<InterceptingSecurityContext<Identity, AccessController>>,
ErrorWebRouterConfigurer<ExchangeContext> {

    ...
    @Override
    public void configure(ErrorWebRouter<ExchangeContext> errorRouter) {
        errorRouter
            .intercept()
                .error(UnauthorizedException.class)
                .path("/basic/**")
                .interceptor(new BasicAuthenticationErrorInterceptor<>("inverno-basic"))
                // We must apply interceptors to intercept white labels error routes which are
already defined
            .applyInterceptors();
    }
}

```

Using above configuration, unauthorized (401) error response corresponding to unauthenticated access will be augmented with a **www-authenticate** HTTP header requesting for basic authentication in the **inverno-basic** realm. In practice, this results in a login prompt being displayed in a Web browser.

The following shows an unauthorized (401) HTTP response with a basic authentication challenge generated by the **BasicAuthenticationErrorInterceptor**:

```

$ curl -i http://127.0.0.1:8080/basic/hello
HTTP/1.1 401 Unauthorized
www-authenticate: basic realm="inverno-basic"
content-length: 0

```

Sending a basic authentication challenge to the client has actually nothing to do with authentication, it simply gives indication to the client on what credentials are expected by the server to access a protected resource. If you don't need to strictly abide to the specification or if your HTTP resources will only be consumed by backend applications you might choose not to use the **BasicAuthenticationErrorInterceptor**.

## HTTP Digest authentication

The [HTTP digest access authentication](#) is a more secured HTTP authentication method in which login credentials (username/password) are sent digested by the client using a nonce previously sent by the server in a **www-authenticate** HTTP header. As for basic authentication, digest credentials are provided in the **authorization** HTTP header. The nonce is built using a secret, the current timestamp and a validity period which allows to expire digest credentials.

A security context implementing HTTP digest authentication is obtained by combining the `DigestCredentialsExtractor` which extracts `DigestCredentials` with a compatible `Authenticator` implementation. The `DigestCredentialsMatcher` can be used within a `PrincipalAuthenticator` or a `UserAuthenticator` to match digest credentials against trusted login credentials (digest credentials basically represent digested login credentials). The following example uses a `UserAuthenticator` with an in-memory user repository and a `DigestCredentialsMatcher` in order to secure `/digest/**` routes:

```
package io.inverno.example.app_web_security;

...
import io.inverno.mod.security.http.digest.DigestCredentialsExtractor;
import io.inverno.mod.security.http.digest.DigestCredentialsMatcher;
...

...
public class SecurityConfigurer implements
WebInterceptorsConfigurer<InterceptingSecurityContext<Identity, AccessController>> {

    @Override
    public void configure(WebInterceptable<InterceptingSecurityContext<Identity, AccessController>,
?> interceptors) {
        interceptors
            .intercept()
                .path("/digest/**")
                .interceptor(SecurityInterceptor.of(
                    new DigestCredentialsExtractor(),
                    new UserAuthenticator<>(
                        InMemoryUserRepository
                            .of(List.of(
                                User.of("jsmith")
                                    .password(new RawPassword("password"))
                                    .build(),
                                User.of("adoe")
                                    .password(new RawPassword("password"))
                                    .build()
                            ))
                    ))
                .build(),
                new DigestCredentialsMatcher<>("secret")
            )
        );
    }
}
```

As previously mentioned, digest credentials expire at a fixed datetime specified in the nonce, this is checked in the `DigestCredentialsMatcher` which fails authentication with a `ExpiredNonceException` when this happens.

The HTTP digest access authentication is based on a challenge-response mechanism as a result a digest authentication challenge must be generated server-side on an unauthorized access or expired nonce errors and sent to the client prior to authentication. This is done using a `DigestAuthenticationErrorInterceptor` on secured routes to intercept `UnauthorizedException` errors:

```

package io.inverno.example.app_web_security;

...
import io.inverno.mod.security.http.basic.BasicAuthenticationErrorInterceptor;
...

...
public class SecurityConfigurer implements
WebInterceptorsConfigurer<InterceptingSecurityContext<Identity, AccessController>>,
ErrorWebRouterConfigurer<ExchangeContext> {

    ...
    @Override
    public void configure(ErrorWebRouter<ExchangeContext> errorRouter) {
        errorRouter
            .intercept()
                .error(UnauthorizedException.class)
                .path("/digest/**")
                .interceptor(new DigestAuthenticationErrorInterceptor<>("inverno-digest", "secret"))
                // We must apply interceptors to intercept white labels error routes which are
already defined
            .applyInterceptors();
    }
}

```

Using above configuration, an unauthorized (401) error response corresponding to unauthenticated access will be augmented with a **www-authenticate** HTTP header containing the digest authentication challenge requesting for digest credentials in the **inverno-digest** realm. The interceptor basically generates a nonce using the specified secret, the nonce validity period (defaults to 300 seconds) and the message digest algorithm (defaults to **MD5**). In practice, this results in a login prompt being displayed in a Web browser.

The following shows an unauthorized (401) HTTP response with a digest authentication challenge generated by the **DigestAuthenticationErrorInterceptor**:

```

$ curl -i http://localhost:8080/digest/hello
HTTP/1.1 401 Unauthorized
www-authenticate: digest realm="inverno-
digest", qop="auth", nonce="0Dg20Tk2MzI3NjcwMzAwOjAyZmIxNWY0ZTAyMTA0NzMzMzdjYmU4YmY4NWRhOGI4", algorithm=MD5
content-length: 0

```

## Token based authentication

Token based authentication is a simple authentication method based on the authentication of a token which was usually previously issued to the client by the server.

A token must be ideally difficult to forge and easy to validate which is why cryptographic methods are often used to generate secured token but solution based on random numbers stored in a trusted data store (like a session store) can also be considered.



A security context implementing token based authentication can be obtained by combining a `TokenCredentials` extractor with a compatible `Authenticator` implementation. The following example uses a `CookieTokenCredentialsExtractor` to extract `TokenCredentials` from a specific cookie and a simplistic highly unsecure authenticator which validates tokens against an hardcoded list of authorized tokens:

```
package io.inverno.example.app_web_security;

...
import io.inverno.mod.security.http.token.CookieTokenCredentialsExtractor;
...

...
public class SecurityConfigurer implements
WebInterceptorsConfigurer<InterceptingSecurityContext<Identity, AccessController>> {

    @Override
    public void configure(WebInterceptable<InterceptingSecurityContext<Identity, AccessController>,
?> interceptors) {
        interceptors
            .intercept()

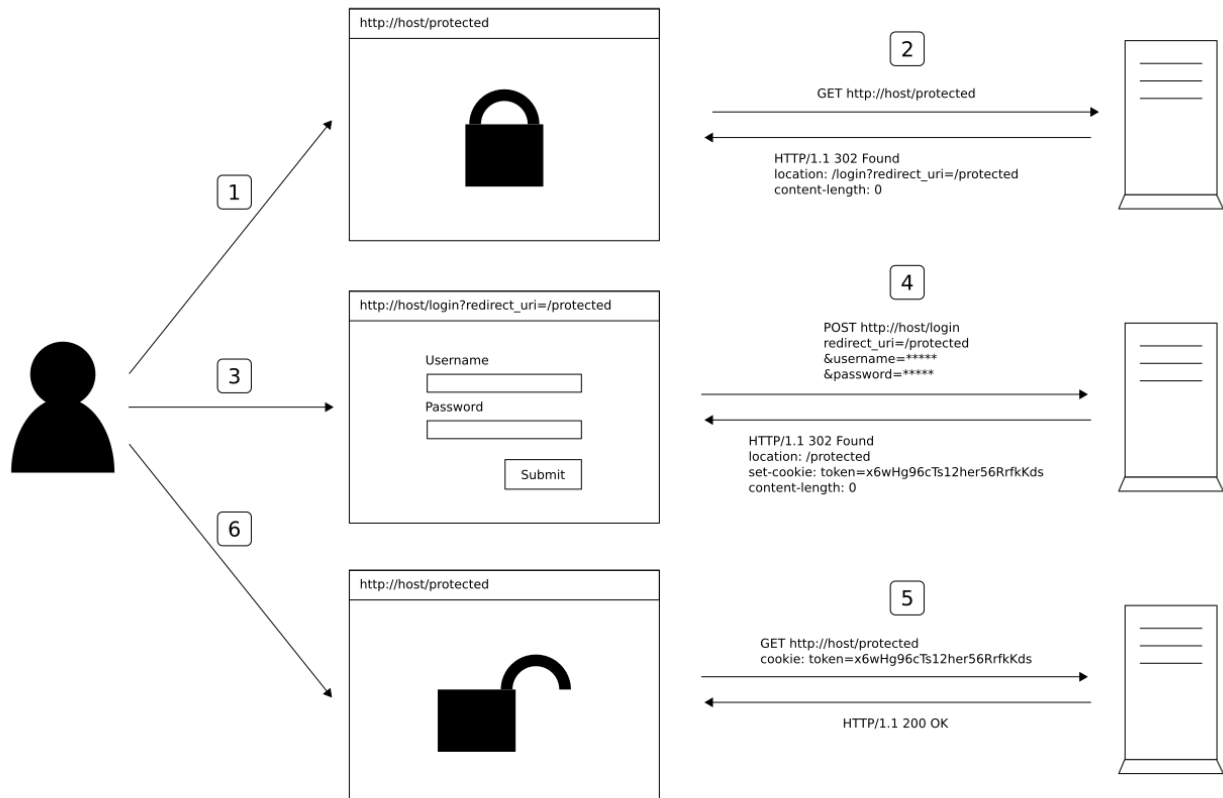
                .path("/token/**")
                .interceptor(SecurityInterceptor.of(
                    new CookieTokenCredentialsExtractor(),
                    credentials -> Mono.fromSupplier(() -> {
                        if(Set.of("token1", "token2",
"token3").contains(credentials.getToken())) {
                            return Authentication.granted();
                        }
                        return Authentication.denied();
                    })
                ));
    }
}
```

As already mentioned, a proper token must be ideally hard to forge and using cryptographic solution such as [JWS](#), [JWE](#) or [JWT](#) are highly recommended.

## Form based login

Form based login is meant to be used to log physical users in an application using a login page in a Web browser. This is slightly more complex than a basic authentication as it usually involves the use of multiple authentication methods.

The login flow is started when a user tries to access a protected resource (1) in a Web browser without credentials or with invalid credentials, an unauthorized (401) is then raised and the user is redirected to the login page prompting for credentials (2), usually a username/password pair. The user then fills the input fields and submits the form (3) to the login action whose role is to authenticate the credentials and generate temporary credentials, usually token credentials, sent back to the client, usually in a cookie, in a found (302) response (4). The client is then redirected to the page initially requested which is now accessed with valid token credentials (5). The user can then access the protected page (6).



Form based login then requires two authentication methods: one to authenticate credentials provided by the user to a login action which should generate the actual credentials that are authenticated by the second method to grant access to protected resources.

Let's start by configuring Web routes to the login page and the login action.

The API provides the `FormLoginPageHandler` which renders a white label login page containing the login form using an Inverno reactive template. The actual login action URI can be configured when creating the handler (defaults to `/login`). The login form sends three parameters: `username`, `password` and `redirect_uri`.

```

package io.inverno.example.app_web_security;

...

public class SecurityConfigurer implements WebRoutesConfigurer<SecurityContext<Identity,
AccessController>> {

    @Override
    public void configure(WebRoutable<SecurityContext<Identity, AccessController>, ?> routes) {
        routes
            .route()
                .method(Method.GET)
                .path("/login")
                .produces(MediaType.TEXT_HTML)
                .handler(new FormLoginPageHandler<>("/login"));
    }
}

```

The login page is not different than a standard route and a custom login page can be easily used instead of the white label login page.

The `LoginActionHandler` is a route handler that must be targeted by the login form to authenticate the user credentials. It relies on a `CredentialsExtractor` to extract credentials from the login request and a compatible `Authenticator` to authenticate them. Finally, it uses a `LoginSuccessHandler` and a `LoginFailureHandler` to determine what to do in case of successful or failed authentication. If no `LoginSuccessHandler` is defined, a blank response is returned on successful authentication. If no `LoginFailureHandler` is defined, a unauthorized (401) error is returned on failed authentication.

In the following example, we decided to generate a [JWS](#) on successful authentication which requires to inject a `JWKSService` to generate a JSON Web Key and a `JWSService` to create JWS tokens.

Please refer to the [security-jose module documentation](#) to learn how to create and validate [JWS](#), [JWE](#) or [JWT](#).

```

package io.inverno.example.app_web_security;

...

public class SecurityConfigurer implements WebRoutesConfigurer<SecurityContext<Identity,
AccessController>> {

    private final Mono<? extends OCTJWK> jwsKey;
    private final JWSService jwsService;

    public SecurityConfigurer(JWKService jwkService, JWSService jwsService) {
        this.jwsKey = jwkService.oct().generator()
            .algorithm(OCTAlgorithm.HS256.getAlgorithm())
            .generate()
            .cache();
        this.jwsService = jwsService;
    }

    @Override
    public void configure(WebRoutable<SecurityContext<Identity, AccessController>, ?> routes) {
        routes
            ...
            .route()
                .method(Method.POST)
                .path("/login")
                .handler(new LoginActionHandler<>(
// 1
                    new FormCredentialsExtractor(),
// 2
                    new PrincipalAuthenticator<>(
// 3
                        new InMemoryLoginCredentialsResolver(List.of(
                            LoginCredentials.of("john", new
MessageDigestPassword.Encoder().encode("password")),
                            LoginCredentials.of("alice", new
MessageDigestPassword.Encoder().encode("password")),
                            LoginCredentials.of("bob", new
MessageDigestPassword.Encoder().encode("password"))
                        )),
                        new LoginCredentialsMatcher<LoginCredentials, LoginCredentials>()
                    )
                )
                .failOnDenied()
// 4
                .flatMap(authentication ->
this.jwsService.builder(PrincipalAuthentication.class, this.jwsKey) // 5
                    .header(header -> header
                        .algorithm(OCTAlgorithm.HS256.getAlgorithm())
                    )
                    .payload(authentication)
                    .build(MediaType.APPLICATION_JSON)
                    .map(JWSAuthentication::new)
                ),
                LoginSuccessHandler.of(
                    new CookieTokenLoginSuccessHandler<>("/form"),
// 6
                    new RedirectLoginSuccessHandler<>()
// 7
                ),
    }

```

```

        new RedirectLoginFailureHandler<>("/login")
// 8    ));
    }
}

```

1. The `LoginActionHandler` is used to handle `POST` request submitted in the login form.
2. The `FormCredentialsExtractor` is used to extract user credentials submitted in the login form as `LoginCredentials`, the actual username and password form parameter names can be set in the credentials extractor (defaults to `username` and `password`).
3. A simple `PrincipalAuthenticator` is then used to authenticate the credentials.
4. The authentication shall fail if the principal authenticator returns a denied authentication.
5. The resulting `PrincipalAuthentication` is then wrapped into a `JWSAuthentication`. We don't have to check whether the authentication is authenticated before creating the JWS token since we used `failOnDenied()`.
6. The `CookieTokenLoginSuccessHandler` is used to set the compact representation of the JWS token in a response cookie. The cookie name and the cookie path can be set when creating the login success handler (defaults to `AUTH-TOKEN` and `/`).
7. The `RedirectLoginSuccessHandler` is then chained to redirect the user to the the page initially requested.
8. The `RedirectLoginFailureHandler` is used to redirect the user to the login page in case of failed authentication, the actual authentication error is specified in a query parameter (defaults to `error`) so it can be displayed in the login form.

The login page and the login action handler are all set, we can now move on and configure a token based authentication to secure `/form/**` routes and restrict access to authenticated users. Since the login action handler sets a JWS token in a cookie we need to use a `CookieTokenCredentialsExtractor` to extract the `TokenCredentials` and a `JWSAuthenticator` to validate the JWS. The JWS actually wraps the original `PrincipalAuthentication` we can then unwrap it in order to restore the original authentication.

```

package io.inverno.example.app_web_security;

...

public class SecurityConfigurer implements WebRoutesConfigurer<SecurityContext<Identity,
AccessController>>, WebInterceptorsConfigurer<InterceptingSecurityContext<Identity,
AccessController>> {

    ...
    @Override
    public void configure(WebInterceptable<InterceptingSecurityContext<Identity, AccessController>,
?> interceptors) {
        interceptors
            .intercept()
                .path("/form/**")
                .interceptors(List.of(
                    SecurityInterceptor.of(
                        new CookieTokenCredentialsExtractor(),
                        new JWSAuthenticator<>(this.jwsService, PrincipalAuthentication.class,
this.jwsKey)
                            .failOnDenied()
                            .map(jwsAuthentication -> jwsAuthentication.getJws().getPayload())
                    ),
                    AccessControlInterceptor.authenticated()
                ));
    }
}

```

In above code, the JWS authenticator uses the JWS service to parse and validate the JWS token. A denied `JWSAuthentication` with an `InvalidCredentialsException` cause is returned on invalid tokens.

Using a JWS token allows to restore the original authentication which can be very useful for resolving identity and/or access controller using regular authentication types (e.g. `PrincipalAuthentication`, `UserAuthentication`...).

Accessing a protected resource with no token or an invalid token results in an `UnauthorizedException` error since the access is restricted to authenticated users. the client should then be redirected to the login page. This can be done applying the `FormAuthenticationErrorInterceptor` on `UnauthorizedException` errors on `/form/**` routes.

```

package io.inverno.example.app_web_security;

...

public class SecurityConfigurer implements WebRoutesConfigurer<SecurityContext<Identity,
AccessController>>, WebInterceptorsConfigurer<InterceptingSecurityContext<Identity,
AccessController>>, ErrorWebRouterConfigurer<ExchangeContext> {

    ...
    @Override
    public void configure(ErrorWebRouter<ExchangeContext> errorRouter) {
        errorRouter
            .intercept()
                .error(UnauthorizedException.class)
                .path("/form/**")
                .interceptor(new FormAuthenticationErrorInterceptor<>("/login"))
            // We must apply interceptors to intercept white labels error routes which
are already defined
            .applyInterceptors();
    }
}

```

Finally, a `/logout` route can also be defined using a `LogoutActionHandler` which uses an `AuthenticationReleaser` to release the security context and a `LogoutSuccessHandler` to handle successful logout and respond to the client. In the following example, a `CookieTokenLogoutSuccessHandler` is used to delete the token cookie and a `RedirectLogoutSuccessHandler` is used to redirect the user after a successful logout to the root of the server (`/`).

```

package io.inverno.example.app_web_security;

...

public class SecurityConfigurer implements WebRoutesConfigurer<SecurityContext<Identity,
AccessController>>, WebInterceptorsConfigurer<InterceptingSecurityContext<Identity,
AccessController>>, ErrorWebRouterConfigurer<ExchangeContext> {

    ...
    @Override
    public void configure(WebRoutable<SecurityContext<Identity, AccessController>, ?> routes) {
        routes
            ...
            .route()
                .method(Method.GET)
                .path("/logout")
                .handler(new LogoutActionHandler<>() {
                    authentication -> Mono.empty(),
                    LogoutSuccessHandler.of(
                        new CookieTokenLogoutSuccessHandler<>("/form"),
                        new RedirectLogoutSuccessHandler<>()
                    )
                })
            );
    }
    ...
}

```

Here is the complete code of the `SecurityConfigurer` used to configure form login flow:

```

package io.inverno.example.app_web_security;

import io.inverno.core.annotation.Bean;
import io.inverno.mod.base.resource.MediaTypees;
import io.inverno.mod.http.base.Method;
import io.inverno.mod.http.base.UnauthorizedException;
import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.security.accesscontrol.AccessController;
import io.inverno.mod.security.authentication.InMemoryLoginCredentialsResolver;
import io.inverno.mod.security.authentication.LoginCredentials;
import io.inverno.mod.security.authentication.LoginCredentialsMatcher;
import io.inverno.mod.security.authentication.PrincipalAuthentication;
import io.inverno.mod.security.authentication.PrincipalAuthenticator;
import io.inverno.mod.security.authentication.password.MessageDigestPassword;
import io.inverno.mod.security.http.AccessControlInterceptor;
import io.inverno.mod.security.http.SecurityInterceptor;
import io.inverno.mod.security.http.context.InterceptingSecurityContext;
import io.inverno.mod.security.http.context.SecurityContext;
import io.inverno.mod.security.http.form.FormAuthenticationErrorInterceptor;
import io.inverno.mod.security.http.form.FormCredentialsExtractor;
import io.inverno.mod.security.http.form.FormLoginPageHandler;
import io.inverno.mod.security.http.form.RedirectLoginFailureHandler;
import io.inverno.mod.security.http.form.RedirectLoginSuccessHandler;
import io.inverno.mod.security.http.form.RedirectLogoutSuccessHandler;
import io.inverno.mod.security.http.login.LoginActionHandler;
import io.inverno.mod.security.http.login.LoginSuccessHandler;
import io.inverno.mod.security.http.login.LogoutActionHandler;
import io.inverno.mod.security.http.login.LogoutSuccessHandler;
import io.inverno.mod.security.http.token.CookieTokenCredentialsExtractor;
import io.inverno.mod.security.http.token.CookieTokenLoginSuccessHandler;
import io.inverno.mod.security.http.token.CookieTokenLogoutSuccessHandler;
import io.inverno.mod.security.identity.Identity;
import io.inverno.mod.security.jose.jwa.OCTAlgorithm;
import io.inverno.mod.security.jose.jwk.JWKService;
import io.inverno.mod.security.jose.jwk.oct.OCTJWK;
import io.inverno.mod.security.jose.jws.JWSAuthentication;
import io.inverno.mod.security.jose.jws.JWSAuthenticator;
import io.inverno.mod.security.jose.jws.JWSService;
import io.inverno.mod.web.ErrorWebRouter;
import io.inverno.mod.web.ErrorWebRouterConfigurer;
import io.inverno.mod.web.WebInterceptable;
import io.inverno.mod.web.WebInterceptorsConfigurer;
import io.inverno.mod.web.WebRoutable;
import io.inverno.mod.web.WebRoutesConfigurer;
import java.util.List;
import reactor.core.publisher.Mono;

@Bean( visibility = Bean.Visibility.PRIVATE )
public class SecurityConfigurer implements WebRoutesConfigurer<SecurityContext<Identity,
AccessController>>, WebInterceptorsConfigurer<InterceptingSecurityContext<Identity,
AccessController>>, ErrorWebRouterConfigurer<ExchangeContext> {

    private final Mono<? extends OCTJWK> jwsKey;
    private final JWSService jwsService;

    public SecurityConfigurer(JWKService jwkService, JWSService jwsService) {
        this.jwsKey = jwkService.oct().generator()
            .algorithm(OCTAlgorithm.HS256.getAlgorithm())
            .generate()
            .cache();
    }

```



```

        this.jwsService = jwsService;
    }

    @Override
    public void configure(WebRoutable<SecurityContext<Identity, AccessController>, ?> routes) {
        routes
            .route()
                .method(Method.GET)
                .path("/login")
                .produces(MediaType.TEXT_HTML)
                .handler(new FormLoginPageHandler<>("/login"))
            .route()
                .method(Method.POST)
                .path("/login")
                .handler(new LoginActionHandler<>({
                    new FormCredentialsExtractor(),
                    new PrincipalAuthenticator<>({
                        new InMemoryLoginCredentialsResolver(List.of(
                            LoginCredentials.of("john", new
                                MessageDigestPassword.Encoder().encode("password")),
                            LoginCredentials.of("alice", new
                                MessageDigestPassword.Encoder().encode("password")),
                            LoginCredentials.of("bob", new
                                MessageDigestPassword.Encoder().encode("password"))
                        )),
                        new LoginCredentialsMatcher<LoginCredentials, LoginCredentials>()
                    })
                })
                .failOnDenied()
                .flatMap(authentication ->
                    this.jwsService.builder(PrincipalAuthentication.class, this.jwsKey)
                        .header(header -> header

                            .algorithm(OCTAlgorithm.HS256.getAlgorithm())
                                )
                        .payload(authentication)
                        .build(MediaType.APPLICATION_JSON)
                        .map(JWSAuthentication::new)
                    ),
                LoginSuccessHandler.of(
                    new CookieTokenLoginSuccessHandler<>("/form"),
                    new RedirectLoginSuccessHandler<>()
                ),
                new RedirectLoginFailureHandler<>("/login")
            ))
            .route()
                .method(Method.GET)
                .path("/form/logout")
                .handler(new LogoutActionHandler<>({
                    authentication -> Mono.empty(),
                    LogoutSuccessHandler.of(
                        new CookieTokenLogoutSuccessHandler<>("/form"),
                        new RedirectLogoutSuccessHandler<>()
                    )
                })
            ));
    }

    @Override
    public void configure(WebInterceptable<InterceptingSecurityContext<Identity,
        AccessController>, ?> interceptors) {
        interceptors
    }

```

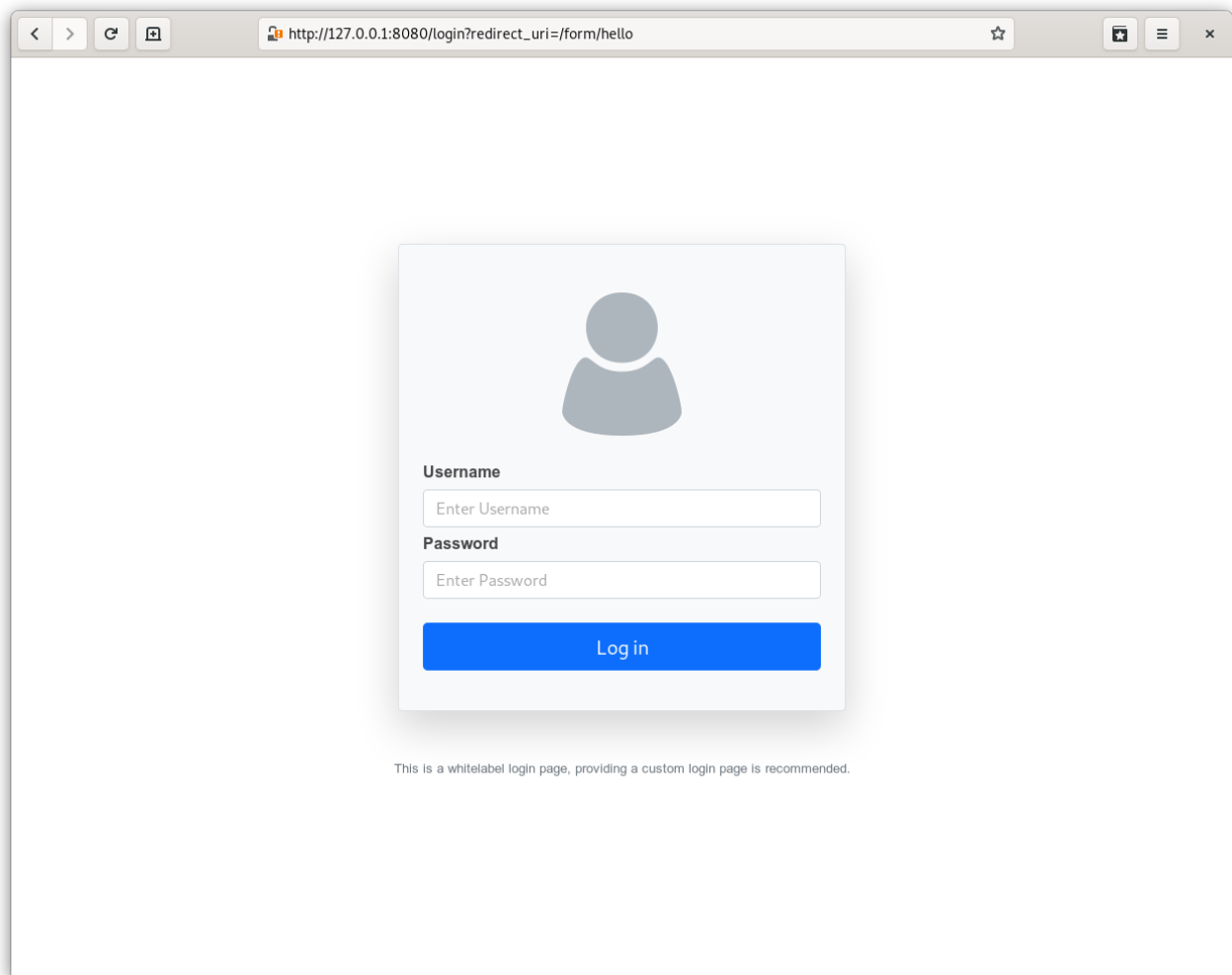
```

        .intercept()
        .path("/form/**")
        .interceptors(List.of(
            SecurityInterceptor.of(
                new CookieTokenCredentialsExtractor(),
                new JWSAuthenticator<>(this.jwsService,
PrincipalAuthentication.class, this.jwsKey)
            ),
            .failOnDenied()
            .map(jwsAuthentication ->
jwsAuthentication.getJws().getPayload())
        ),
        AccessControlInterceptor.authenticated()
    ));
}

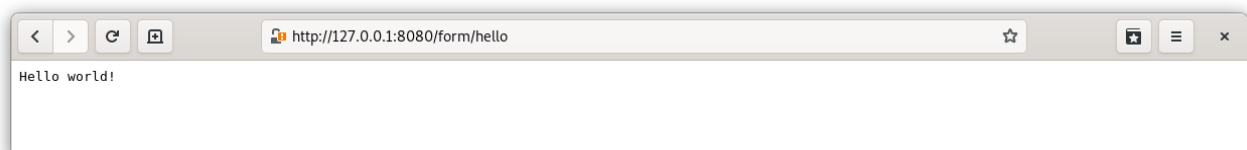
@Override
public void configure(ErrorWebRouter<ExchangeContext> errorRouter) {
    errorRouter
        .intercept()
        .error(UnauthorizedException.class)
        .path("/form/**")
        .interceptor(new FormAuthenticationErrorInterceptor<>("/login"))
        // We must apply interceptors to intercept white labels error routes which
are already defined
        .applyInterceptors();
}
}

```

After defining routes `/form/hello` and `/`, we can run the application and test the login flow by accessing <http://localhost:8080/form/hello> which should redirect the Web browser to the white label login page:



After filling valid login credentials in the login form, we should be redirected to the protected resource which is now accessible.



We described a basic form login flow but it can be extended to match more complex or specific security requirements.

For instance, two-factors authentication could be implemented quite easily by providing a custom login form that would include a second authentication factor in addition to the login credentials and a specific login credentials authenticator that would check that factor as well, it is even possible to use the standard `UserAuthenticator` and just chain another authenticator to validate the second factor.

# Cross-origin resource sharing (CORS)

Cross-origin resource sharing is a mechanism that allows for cross-domain requests where a resource is requested in a Web browser from a page in another domain. Cross-domain requests are usually forbidden by Web browsers following the [same-origin policy](#). CORS defines a protocol that allows the Web browser to communicate with the server and determine whether a cross-origin request can be authorized.

The `CORSInterceptor` can be used to configure the CORS policy, it can be applied to routes that might be accessed from different domain than the server or globally to apply the policy to all routes.

Assuming the HTTP server runs locally on port `8080`, the following example shows how to authorize all requests from `http://127.0.0.1:9090`:

```
package io.inverno.example.app_web_security;

import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.security.http.cors.CORSInterceptor;
import io.inverno.mod.web.WebInterceptable;
import io.inverno.mod.web.WebInterceptorsConfigurer;

public class SecurityConfigurer implements WebInterceptorsConfigurer<ExchangeContext> {

    @Override
    public void configure(WebInterceptable<ExchangeContext, ?> interceptors) {
        interceptors
            .intercept()
                .interceptor(CORSInterceptor.builder("http://127.0.0.1:9090").build());
    }
}
```

The `CORSInterceptor` fully supports the CORS protocol, it allows to define allowed origins (static or using a pattern), methods, headers with max age allowing credentials or private network. Please refer to the [HTTP CORS protocol specification](#) for further details in order to create more complex configuration

# Cross-site request forgery protection (CSRF)

Cross-site request forgery attack consists for an attacker to make the Web browser of a victim perform unwanted action on a trusted Web site when the user is authenticated. This is made possible by the use of cookies holding authentication credentials and which are automatically included in the requests by the Web browser. As far as the server is concerned, it can not make the difference between a legitimate and a malicious request as long as it contains valid credentials.

The `CSRFDoubleSubmitCookieInterceptor` can be used to protect against CSRF attacks, it implements the double submit cookie method advised by [OWASP](#).

The following example shows how to configure the Web server in order to prevent CSRF attacks:

```

package io.inverno.example.app_web_security;

import io.inverno.mod.http.server.ExchangeContext;
import io.inverno.mod.security.http.csrf.CSRFDoubleSubmitCookieInterceptor;
import io.inverno.mod.web.WebInterceptable;
import io.inverno.mod.web.WebInterceptorsConfigurer;

public class SecurityConfigurer implements WebInterceptorsConfigurer<ExchangeContext> {

    @Override
    public void configure(WebInterceptable<ExchangeContext, ?> interceptors) {
        interceptors
            .intercept()

        .interceptor(CSRFDoubleSubmitCookieInterceptor.builder().httpOnly(false).build());
    }
}

```

The name of the reference cookie token is set to **XSRF-TOKEN**, on a **POST**, **PUT**, **PATCH** or **DELETE** request, the interceptor tries to compare its value to a header (**X-CSRF-TOKEN** by default) or, if missing, to a query parameter (**\_csrf\_token** by default). If the two values are matching, which basically means the client was able to read the cookie, the request can be safely authorized otherwise a forbidden (403) error shall be return to the client.

When using the **CSRFDoubleSubmitCookieInterceptor** with a Web application developped with [Angular](#) or other any other framework that support double submit cookie, the **httpOnly** flag of the reference cookie must be set to **false**.

## Security LDAP

The Inverno *security-ldap* module provides authenticators used to authenticate login credentials against [LDAP](#) or [Active Directory](#) servers.

It also provides an identity resolver for resolving user identity from the LDAP attributes of a user entry.

The LDAP client provided in module *ldap* is therefore required, in order to use the the Inverno *securiy-ldap* module we need then to declare the following dependencies in the module descriptor:

```

module io.inverno.example.app {
    ...
    requires io.inverno.mod.ldap;
    requires io.inverno.mod.security.ldap;
    ...
}

```

And also declare these dependencies in the build descriptor:

Using Maven:

```

<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-ldap</artifactId>
    </dependency>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-security-ldap</artifactId>
    </dependency>
  </dependencies>
</project>

```

Using Gradle:

```

...
compile 'io.inverno.mod:inverno-security-http:1.5.3'
compile 'io.inverno.mod:inverno-security-ldap:1.5.3'
...

```

The following example shows how to configure a security manager to authenticate login credentials against an LDAP server, resolving the authenticated user's identity from the LDAP server and a role-based access controller from user's groups.

```

// Provided by the ldap module
LDAPClient ldapClient = null;

SecurityManager<LoginCredentials, LDAPIdentity, RoleBasedAccessController> securityManager =
SecurityManager.of(
  new LDAPAuthenticator(ldapClient, "dc=inverno,dc=io"),
  new LDAPIdentityResolver(ldapClient),
  new GroupsRoleBasedAccessControllerResolver()
);

```

## LDAP authenticator

The `LDAPAuthenticator` can authenticate `LoginCredentials` (username/password) against a standard LDAP server.

When the password specified in the credentials is a `RawPassword`, authentication is made by a binding operation to the LDAP server. If the password is an encoded password, authentication is made by comparing the encoded value to the password attribute (`userPassword` by default) of the LDAP user entry.

The user `DN` is obtained using username template (defaults to `cn={0},ou=users`) formatted with the username specified in the credentials. User groups are resolved by searching for groups using a search filter set to `(&(objectClass=groupOfNames)(member={0}))` by default.

An `LDAPAuthenticator` is created using an `LDAPClient` and a base `DN` which identifies the organization where to look for entries. The following example shows how to create an `LDAPAuthenticator` to authenticate users in the `dc=inverno,dc=io` organization:

```
// Provided by the ldap module
LDAPClient ldapClient = ...
```

```
LDAPAuthenticator ldapAuthenticator = new LDAPAuthenticator(ldapClient, "dc=inverno,dc=io");
```

```
LDAPAuthentication authentication = ldapAuthenticator.authenticate(LoginCredentials.of("jsmith", new
RawPassword("password"))).block();
```

The `LDAPAuthentication` returned by the `LDAPAuthenticator` is a specific principal authentication that exposes the user's DN, it also extends `GroupAwareAuthentication` since LDAP users can be organized in groups (i.e. `groupOfNames` class). These information are resolved when authenticating credentials in the LDAP authenticator. A

`GroupsRoleBasedAccessControllerResolver` can then be used in a security manager or security interceptor to resolve a role-based access controller using users groups as roles.

## Active Directory authenticator

The `ActiveDirectoryAuthenticator` is a similar implementation used to authenticate `LoginCredentials` against an [Active Directory](#) server and returning `LDAPAuthentication`.

Although Active Directory can be accessed using LDAP, the internal semantic is quite different than standard LDAP server like [OpenLDAP](#) which is why we needed a specific implementation.

Unlike the `LDAPAuthenticator`, authentication using password comparison is not supported and therefore it can only authenticate credentials specified with raw passwords using a bind operation. User groups are resolved from the `memberOf` attribute of the user entry which is resolved using a search user filter set to `(&(objectClass=user)(userPrincipalName={0}))` by default.

An `ActiveDirectoryAuthenticator` is created using an `LDAPClient` and a domain. The following example shows how to create an `ActiveDirectoryAuthenticator` to authenticate users in `inverno.io` domain:

```
// Provided by the ldap module
LDAPClient ldapClient = ...
```

```
ActiveDirectoryAuthenticator adAuthenticator = new ActiveDirectoryAuthenticator(ldapClient,
"inverno.io");
```

```
LDAPAuthentication authentication = adAuthenticator.authenticate(LoginCredentials.of("jsmith", new
RawPassword("password"))).block();
```

## LDAP identity

An LDAP server is basically a directory service which can provide any kind of information about a user such as email addresses, postal addresses, phone numbers... The `LDAPIdentity` exposes standard LDAP attributes of `person`, `organizationalPerson` and `inetOrgPerson` classes as defined by [RFC 2256](#) and [RFC 2798](#).

The LDAP identity is resolved in a security manager or a security interceptor from an `LDAPAuthentication` using an `LDAPIdentityResolver` which basically look up the LDAP user entry with specific attributes in the LDAP server using the user DN and a search user filter set to `(&(objectClass=inetOrgPerson)(uid={0}))` by default.

An `LDAPIdentityResolver` is created using an `LDAPClient`. The following example shows how to create a simple `LDAPIdentityResolver` for resolving common identity attributes:

```
// Provided by the ldap module
LDAPClient ldapClient = ...

LDAPIdentityResolver ldapIdentityResolver = new LDAPIdentityResolver();
```

It is possible to specify which attributes must be queried as follows:

```
// Provided by the ldap module
LDAPClient ldapClient = ...

LDAPIdentityResolver ldapIdentityResolver = new LDAPIdentityResolver(ldapClient, "uid", "mail",
"mobile");
```

## JSON Object Signing and Encryption

The Inverno *security-jose* module is a complete implementation of JSON Object Signing and Encryption RFC specifications.

It allows to create, load or manipulate JSON Web Keys used to sign and verify JWS tokens or encrypt and decrypt JWE tokens. It also allows to manipulate so-called JSON Web Tokens (JWT) which are basically a set of claims wrapped inside a JWS or JWE token.

JWS and JWE tokens are using cryptographic signature and encryption algorithms which offer both payload integrity and/or privacy. The fact that they can be easily validated makes them an ideal choice for token credentials which do not necessarily require external systems for authentication.

Here is the complete list of RFCs implemented in the *security-jose* module:

- [RFC 7515](#) JSON Web Signature (JWS)
- [RFC 7516](#) JSON Web Encryption (JWE)
- [RFC 7517](#) JSON Web Key (JWK)
- [RFC 7518](#) JSON Web Algorithms (JWA)
- [RFC 7519](#) JSON Web Token (JWT)
- [RFC 7638](#) JSON Web Key (JWK) Thumbprint
- [RFC 7797](#) JSON Web Signature (JWS) Unencoded Payload Option
- [RFC 8037](#) CFRG Elliptic Curve Diffie-Hellman (ECDH) and Signatures in JSON Object Signing and Encryption (JOSE)
- [RFC 8812](#) CBOR Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms



The Inverno *security-jose* module requires media type converters to be able to convert JWS and JWE payloads (e.g. object to JSON...), media type converters are usually provided in the *boot* module, as a result in order to use the module, we need to declare the following dependencies in the module descriptor:

```
@io.inverno.core.annotation.Module
module io.inverno.example.app {
    ...
    requires io.inverno.mod.boot;
    requires io.inverno.mod.security.jose;
    ...
}
```

And also declare these dependencies in the build descriptor:

Using Maven:

```
<project>
  <dependencies>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-boot</artifactId>
    </dependency>
    <dependency>
      <groupId>io.inverno.mod</groupId>
      <artifactId>inverno-security-jose</artifactId>
    </dependency>
  </dependencies>
</project>
```

Using Gradle:

```
...
compile 'io.inverno.mod:inverno-security-jose:1.5.3'
...
```

The *security-jose* module is an Inverno module which exposes four services:

- the **jwkService** used to manage JSON Web Keys.
- the **jwsService** used to sign and verify JSON Web signature tokens.
- the **jwsService** used to encrypt and decrypt JSON Web signature tokens.
- the **jwtService** used to create JSON Web tokens as JWS or JWE.

It also provides JOSE object media type converters (e.g. *application/jose*, *application/jose+json*, *application/jwk+json*...) which can be used to decode (parse, verify, decrypt) JWS, JWE or JWK.

It can be easily composed in another Inverno module, as shown above, to get these services injected where they are needed but it can also be used in any other application which requires JOSE support. Media type converters might however be required to automatically convert payloads inside JWS or JWE token based on the content type, they can be provided explicitly when creating the module.

Explicit encoders and decoders can also be used to convert payloads, it is then completely possible to run the module without specifying media type converters.

A **Jose** module instance embeddable in any Java application and able to handle **application/json** or **text/plain** payloads can be obtained as follows:

```
// Exported in the 'boot' module
JsonStringMediaTypeConverter jsonConverter = new JsonStringMediaTypeConverter(new
JacksonStringConverter(new ObjectMapper()));
TextStringMediaTypeConverter textConverter = new TextStringMediaTypeConverter(new
StringConverter());

// Build Jose module
Jose jose = new Jose.Builder(List.of(jsonConverter, textConverter)).build();

// Initialize Jose module
jose.start();

// Create, load or store JSON Web keys
JWKService jwkService = jose.jwkService();
...

// Create, sign and verify JSON Web Signature tokens
JWSService jwsService = jose.jwsService();
...

// Create, encrypt and decrypt JSON Web encryption tokens
JWEService jweService = jose.jweService();
...

// Create JSON Web Token as JWS or JWE
JWTService jwtService = jose.jwtService();
...

// Destroy Jose module
jose.stop();
```

Although it is recommended to compose the *security-jose* module with the *boot* module inside an Inverno application so as not to have to deal with dependency injection or module's lifecycle, it is completely feasible to use JOSE services in any Java application as shown above, even those which do not use the Java module system.

The API is quite complete and supports advanced features such as automatic key resolution by JWK key id or X.509 thumbprints (from a Java key store or other trusted repositories), a JWK store to store frequently used keys, JWK certificate path validation, JWK Set resolution, JWE compression... Before seeing all this in details, let's quickly see how to create JSON Web Keys and use them to create and read JWS, JWE or JWT tokens.

A JSON Web Key (JWK) represents a cryptographic key used to sign/verify or encrypt/decrypt JWS or JWE tokens. The following example shows how to create a simple symmetric octet key using HS256 signature algorithm:

```
// Injected or obtained from a 'Jose' instance
JWKSService jwkService = ...

/*
 * {
 *   "alg": "HS512",
 *   "k": "h92UNTmd5NpTl5UUalbp03z4AygilZrDYH0aSjwjYQ_fma8_a06A8Mw0UjJGJyFEGPLJ46ujcTLlKo0_AjK3UQ",
 *   "kty": "oct",
 *   "kid": "octKey"
 * }
 */
Mono<? extends OCTJWK> octKey = jwkService.oct().generator()
    .keyId("octKey")
    .algorithm(OCTAlgorithm.HS512.getAlgorithm())
    .generate()
    .cache();
```

The API is fully reactive, subscribing multiple times to the `Mono` returned by the key generator would result in multiple keys being generated which is why `cache()` was used to make sure one single key is generated and returned. The key thus obtained can then be used to sign or verify JWS tokens.

A JSON Web Signature token (JWS) is composed of a header, a payload and a payload signature. The header basically specifies the information needed to verify the payload signature. A JWS token then provides integrity protection since although it is possible to read the content of the payload, it is not possible to modify it without breaking the signature.

The following example shows how to create a JWS token with a simple text payload using previous symmetric key:

```
// Injected or obtained from a 'Jose' instance
JWSService jwsService = ...

/*
 * {
 *   "header": {
 *     "alg": "HS512",
 *     "cty": "text/plain",
 *     "kid": "octKey"
 *   },
 *   "payload": "This is a simple payload",
 *   "signature": "mwq--Ke20m3zA2y1F9cQlw5SyFPzhkvwoRaaezbzqifL5joJWuJEddPbtFDKLaBUD9Ufwi6R6IFbb0e-nxkr4w"
 * }
 */
Mono<JWS<String>> jws = jwsService.builder(String.class, octKey)
    .header(header -> header
        .keyId("octKey")
        .algorithm(OCTAlgorithm.HS512.getAlgorithm())
        .contentType(MediaTypes.TEXT_PLAIN)
    )
    .payload("This is a simple payload")
    .build();

//
eyJjdHkiOiJ0ZXh0L3BsYWluIiwia2lkIjoib2N0S2V5IiwiaWxnIjoisFM1MTIifQ.VGhpcyBpcyBhIHNpbXBsZSBwYXlsb2FkLmwq--Ke20m3zA2y1F9cQlw5SyFPzhkvwoRaaezbzqifL5joJWuJEddPbtFDKLaBUD9Ufwi6R6IFbb0e-nxkr4w
String jwsCompact = jws.block().toCompact();
```

The JWS content type must be set in order to determine which media type converters to use to convert the payload. If you don't want to include the content type property (`cty`) in the resulting JWS, the content type can also be specified on the `build()` method. An explicit `Function<T, Mono<String>>` payload encoder can also be specified on the `build()` method in order to bypass media type converters.

The compact representation of the JWS token can then be used to communicate integrity protected data to a recipient sharing the same symmetric key. A JWS token compact representation is parsed and validated as follows:

```
Mono<JWS<String>> jws = jwsService.reader(String.class, octKey)
    .read(compactJWS);

// Returns "This is a simple payload" or throw a JWSReadException if the token is invalid
jws.block().getPayload();
```

A JSON Web Encryption token (JWE) provides privacy in addition to integrity by encrypting the payload. It is composed of a header which specifies how to decrypt and verify the cipher text, an encrypted key (used for digital signature and encryption), an initialization vector, the cipher text and an authentication tag.

The following example shows how to load an RSA key pair into a JWK, use it to create a JWE token and read its compact representation:

```
// Injected or obtained from a 'Jose' instance
JWEService jweService = ...

/*
 * From RFC7516 Section A.1:
 * {
 *   "n": "oahUIoWw0K0usKNu0R6H4wkf4oBUXHTxRvGb48E-
BVvxkeDNjbC4he8rUwcJoZmds2h7M70imEVhRU5djINxtqlLXI4DFqcI1DgjT9LewND8MW2Krf3Spsk_ZkoFnilakGygTwpZ3ues
H-PFABNIUYp0iN15dsQRkgr0vEhxN92i2asb0enSZeyaxziK72UwxrrKoExv6kc5twXTq4h-
QChL0ln0_mtUZwfsRaMStPs6mS6XrgxnxbWhojf663tuEQueGC-
FCMfra36C9knDFGzKsNa7LZK2djYgyD3JR_MB_4NUJW_Tq0QtwHYbxevoJArm-L5StowjzGy-_bq6Gw",
 *   "e": "AQAB", "d": "kLdtIj6GbDks_ApCSTYQtelcNttlKi0yPzMrXHeI-yk1F7-kpDxY4-
WY5NWV5KntaEeXS1j82E375xxhWMHXyvjYecPT9fpwR_M9gV8n9Hrh2anTpTD93Dt62ypw3yDsJzBnTnrYu1iwwRgBKrEYY46qAZ
IrA2xAwnm2X7uGR1hghkqDp0Vqj3kbSCz1XyfCs6_LehBwtXHIyh8Ripy40p24mo0AbgxVw3rxT_vlt3Uve4W03JkJOzlpUf-
KTVI2Ptgm-dARxTetE-id-40Jr0h-K-VFs3VsndVTIznSxfyrj8ILL6MG_Uv8YAu7VILSB3l0W085-4qE3DzgrTjgyQ",
 *   "p": "1r52Xk46c-LsfB5P442p7atdPurxQSy4mti_tZI3Mgf2EuFVbUoDBvaRQ-
SWxkbkmoEzL7JXroSBjSrK3YIQgYdMgyAEPTpjXv_hI2_1eTSPVzfzL0lffNn03IXqWF5MDFu0UYE0hzb2vhrln_rKrbfDIwUbTr
jjgieRbwc6Cl0",
 *
"q": "wLb35x7hmQWZswJmB_vle87ihgZ19S8lBEROLIsZG4ayZVe9Hi9gDVC0BmUDdaDYVTSNx_8Fyw1YYa9XGrGnDew00J28cRU
oeBB_jKI1oma0Orv1T9aXIwxKwd4gvxFImOwr3QRL9KEBRzk2RatUBnmDZJTIAfWts0g68UZHvtc",
 *   "dp": "ZK-YwE7diUh0qR1tr7w8WHtoLdx3MZ_OTowIFvgfeQ3SiresXjm9gZ5KLhMXvo-uz-
KUJWdxS5pFQ_M0evdo1dKiRtjVw_x4NyqyXPM5nULPkcpU827rnpZzAJKpdhWAgqrXGKAECQH0xt4taznjnd_zVpAmZZq60WPMBM
fKcuE",
 *
"dq": "Dq0gfgJ1DdFGXiLvQEznuKEN0UumsJBxkjydc3j4ZYdBiMRay86x0vHCjywcMlYYg4yoC4YZa9hNVcsjqA3FeiL19rk8g6
Qn29Tt0cj8qqyFpz9vNDBUfCAiJVeS0jJDZPYHdHY8v1b-o-Z2X5tvLx-TCekf7oxyeKDUqKwjis",
 *   "qi": "VIMPMYbPf47dT1w_zDUXfPimsSegnM0A1zTaX7aGk_8urY6R8-
ZW1FXU7AlwAyLWybqq6t16Vfd7hQd0y6fLUK4SLOydb61gwan0sXG0A0v82cHq0E3eL4HrtZkUuKvnPrMnsUUFfUdybVzxyjz9J
F_XyaY14ardLSjf4L_FNY",
 *   "kty": "RSA",
 *   "kid": "rsaKey"
 * }
 */
Mono<? extends RSAJWK> rsaKey = jwkService.rsa().builder()
    .keyId("rsaKey")
    .modulus("oahUIoWw0K0usKNu0R6H4wkf4oBUXHTxRvGb48E-
BVvxkeDNjbC4he8rUwcJoZmds2h7M70imEVhRU5djINxtqlLXI4DFqcI1DgjT9LewND8MW2Krf3Spsk_ZkoFnilakGygTwpZ3ues
H-PFABNIUYp0iN15dsQRkgr0vEhxN92i2asb0enSZeyaxziK72UwxrrKoExv6kc5twXTq4h-
QChL0ln0_mtUZwfsRaMStPs6mS6XrgxnxbWhojf663tuEQueGC-
FCMfra36C9knDFGzKsNa7LZK2djYgyD3JR_MB_4NUJW_Tq0QtwHYbxevoJArm-L5StowjzGy-_bq6Gw")
    .publicExponent("AQAB")
    .privateExponent("kLdtIj6GbDks_ApCSTYQtelcNttlKi0yPzMrXHeI-yk1F7-kpDxY4-
WY5NWV5KntaEeXS1j82E375xxhWMHXyvjYecPT9fpwR_M9gV8n9Hrh2anTpTD93Dt62ypw3yDsJzBnTnrYu1iwwRgBKrEYY46qAZ
IrA2xAwnm2X7uGR1hghkqDp0Vqj3kbSCz1XyfCs6_LehBwtXHIyh8Ripy40p24mo0AbgxVw3rxT_vlt3Uve4W03JkJOzlpUf-
KTVI2Ptgm-dARxTetE-id-40Jr0h-K-VFs3VsndVTIznSxfyrj8ILL6MG_Uv8YAu7VILSB3l0W085-4qE3DzgrTjgyQ")
    .firstPrimeFactor("1r52Xk46c-LsfB5P442p7atdPurxQSy4mti_tZI3Mgf2EuFVbUoDBvaRQ-
SWxkbkmoEzL7JXroSBjSrK3YIQgYdMgyAEPTpjXv_hI2_1eTSPVzfzL0lffNn03IXqWF5MDFu0UYE0hzb2vhrln_rKrbfDIwUbTr
jjgieRbwc6Cl0")

    .secondPrimeFactor("wLb35x7hmQWZswJmB_vle87ihgZ19S8lBEROLIsZG4ayZVe9Hi9gDVC0BmUDdaDYVTSNx_8Fyw1YYa9X
GrGnDew00J28cRUoeBB_jKI1oma0Orv1T9aXIwxKwd4gvxFImOwr3QRL9KEBRzk2RatUBnmDZJTIAfWts0g68UZHvtc")
    .firstFactorExponent("ZK-YwE7diUh0qR1tr7w8WHtoLdx3MZ_OTowIFvgfeQ3SiresXjm9gZ5KLhMXvo-uz-
KUJWdxS5pFQ_M0evdo1dKiRtjVw_x4NyqyXPM5nULPkcpU827rnpZzAJKpdhWAgqrXGKAECQH0xt4taznjnd_zVpAmZZq60WPMBM
fKcuE")

    .secondFactorExponent("Dq0gfgJ1DdFGXiLvQEznuKEN0UumsJBxkjydc3j4ZYdBiMRay86x0vHCjywcMlYYg4yoC4YZa9hNV
csjqA3FeiL19rk8g6Qn29Tt0cj8qqyFpz9vNDBUfCAiJVeS0jJDZPYHdHY8v1b-o-Z2X5tvLx-TCekf7oxyeKDUqKwjis")
    .firstCoefficient("VIMPMYbPf47dT1w_zDUXfPimsSegnM0A1zTaX7aGk_8urY6R8-
ZW1FXU7AlwAyLWybqq6t16Vfd7hQd0y6fLUK4SLOydb61gwan0sXG0A0v82cHq0E3eL4HrtZkUuKvnPrMnsUUFfUdybVzxyjz9J
```

```

F_XyaY14ardLSjf4L_FNY")
    .build()
    .cache();

/*
 * {
 *   "header":{
 *     "enc":"A256GCM",
 *     "alg":"RSA-OAEP",
 *     "cty":"text/plain",
 *     "kid":"rsaKey"
 *   },
 *   "payload":"This is a simple payload",
 *   "initializationVector":"97ZuhWEQ0ygN7T3g",
 *   "authenticationTag":"_e-vSUwj5LawcnXR0qKvmQ",
 *
 *   "encryptedKey":"V0k1HQDwucfkljliz8RzxvuKXX_B6sTMwZbwKJztZjL0Ga8i3yrRl_4jumBTkBIyWMDdZYxcbHtkzZQhQDFJ
VpvNcf1QxEryhe30nFOEF2BGJDPwSYc-
AVmAtQ01gHrUaTF02xvWntfvzu3ePq5vVHl4eiL72P0VdoN9w8ck4Ha0jeoooYcrkaV8l15cYurXsJ8oo_KQ40SBmKnK99CRrqR1Q
ggPscTpE1QeVj2Z9tw5A3rqYGbCX2d2QwP-
zc7w501bsuB5qE99i0iAKtMwEdaz6iC97nDry8Vo2uSPf3YviwpmzmlbbwJlb_bHhl1aeTZaNL9JLvxvqCDQehdAx7g",
 *   "cipherText":"YFPMGQXbmI5ZWZxkpH04vEwsBLCmBJ4G"
 * }
 */
Mono<JWE<String>> jwe = jweService.builder(String.class, rsaKey)
    .header(header -> header
        .keyId("rsaKey")
        .algorithm("RSA-OAEP")
        .encryptionAlgorithm("A256GCM")
    )
    .payload("This is a simple payload")
    .build(MediaTypes.TEXT_PLAIN);

//
eyJlbmMiOiJBbmJ0R0NNIiwiaWxnIjoiaUlNBLU9BRVAiLCJjdHkiOiJ0ZXh0L3BsYWluIiwia2lkIjoicnNhS2V5In0.EG3dFsn0
MAXWRadls1UHpmfNFspczXldNTwr9Lf08BZXsliEJJ8J9-
Z25oFnpaI7q3lXazNg06C9upJW2ZiDg2hmmqoCzYD7xdFEz_Ykg07_92tPxcm0XSGZJUtx1d8gpJBoIQWmPCm06vVveoCds-
kmtTQEigokSewKmkIQy0QcyAhLT5y_gkL0JrKLTPjTKGept7dl9uTzuZenWi-5apdVynDh0kra0kCSu8ahVPPPSf5s9aHUS8th-
pjWatS70FwM0rjLzYXmcqdNPAYM0Pcg88Fw_uI8J7I6tzDInV31rVZ9pDlVarmVSYhS9Rfa91gZaba-
onCiFURceUae0g.im9v2BnFnFp_uGtX.VItNFUA2xtrgr0-Fs-LukV0RZbRURNkv.eFgbb8i10lfIkSHFM8IkXA
String jweCompact = jwe.block().toCompact();

Mono<JWE<String>> jwe = jweService.reader(String.class, rsaKey)
    .read(jweCompact);

// Returns "This is a simple payload" or throw a JWReadException if the token is invalid
jwe.block().getPayload();

```

In above example, the RSA public key was used to encrypt a generated symmetric key (using RSA-OAEP algorithm) which is used to encrypt the payload (using A256GCM algorithm) and the RSA private key was used to decrypt that encryption key and use it to decrypt and validate the token.

A JSON Web Token (JWT) can be a JWS or a JWE with a JWT Claims Set as payload.

The following example shows how to create and validate a JWT expiring in ten minutes from now using previous symmetric key:

```
// Injected or obtained from a 'Jose' instance
JWTService jwtService = ...

/*
 * {
 *   "header":{
 *     "typ":"JWT",
 *     "kid":"octKey",
 *     "alg":"HS512"
 *   },
 *   "payload":{
 *     "iss":"john",
 *     "exp":1659346862,
 *     "http://example.com/is_root":true
 *   },
 *   "signature":"hX_m668usLB1DHGW4cD2NJ1UzCs3T6sGCa0ctvGTkresiZ87iIeKnY0-
EoIvWmDy3SY69rGLMsbsEjsru1QdZw"
 * }
 */
Mono<JWS<JWTClaimsSet>> jwt = jwtService.jwsBuilder(octKey)
    .header(header -> header
        .keyId("octKey")
        .algorithm("HS512")
        .type("JWT")
    )
    .payload(JWTClaimsSet.of("john", ZonedDateTime.now().plusMinutes(10).toEpochSecond())
        .addCustomClaim("http://example.com/is_root", true)
        .build()
    )
    .build();

//
eyJ0eXAiOiJKV1QiLCJraWQiOiJvY3RLZXkiLCJhbGciOiJIUzUxMiJ9.eyJpc3MiOiJqb2huIiwiaXNwIjoxNjU5MzQ2ODYyLCJodHRwOi8vZXhhbXBsZS5jb20vaXNfcm9vdCI6dHJ1ZX0.hX_m668usLB1DHGW4cD2NJ1UzCs3T6sGCa0ctvGTkresiZ87iIeKnY0-
EoIvWmDy3SY69rGLMsbsEjsru1QdZw
String jwtCompact = jwt.block().toCompact();

Mono<JWS<JWTClaimsSet>> jwt = jwtService.jwsReader(octKey)
    .read(compactJWT);

// Throw a JWSReadException if the signature is invalid or an InvalidJWTException if the JWT Claims
set is invalid (e.g. expired, inactive...)
jwt.block().getPayload().ifInvalidThrow();
```

Note that here we didn't have to specify the content type since a JWT payload is always `application/json`.

## JWK Service

The JWK service is used to build, generate or read JSON Web Keys (JWK) which represent cryptographic keys as specified by [RFC 7517](#). A `JWK` is meant to be used to sign or verify the signature part in a JWS, derive, encrypt/decrypt or wrap/unwrap the content encryption key in a JWE or encrypt or decrypt a JWE. It is characterized by a set of properties:

- **key type** (`key_type`) which identifies the cryptographic algorithm family used with the key (e.g. RSA, EC...).
- **public use** (`public_use`) which identifies the intended use of the public key (signature or encryption).
- **key operations** (`key_ops`) which identifies the operations for which the key is intended to be used (e.g. sign, verify, encrypt, decrypt...).
- **algorithm** (`alg`) which identifies the algorithm intended for use with the key (e.g. HS256).
- **key id** (`kid`) which identifies the key in issuer and recipient systems.
- **X.509 URL** (`x5u`) which is a URI pointing to a resource for an X.509 public key certificate or certificate chain (the public key when considering asymmetric JWK).
- **X.509 certificate chain** (`x5c`) which contains a chain of one or more PKIX certificates (the public key when considering asymmetric JWK).
- **X.509 thumbprints** (`x5t` and `x5t#S256`) which are Base64 encoded X.509 certificate thumbprint used to uniquely identifies a key (the public key when considering asymmetric JWK).

Depending on the key type and more particularly the cryptographic algorithm family, additional properties may be required (e.g. the name of an elliptic curve, the modulus of an RSA public key...).

A JWK can be symmetrical or asymmetrical composed of a public and private key pair and respectively used in symmetrical (e.g. HMAC, AES...) or asymmetrical (e.g. Elliptic Curve, RSA...) cryptographic algorithms as specified by [RFC 7518](#). The specification differentiates three types of algorithms:

- *Digital Signatures and MACs* which are used to digitally sign or create a MAC of a JWS.
- *Key Management* which are used to derive or encrypt/decrypt the Content Encryption Key (CEK) used to encrypt a JWE.
- *Content Encryption* which are used to encrypt and identity-protect a JWE using a CEK.

The **JWK** interface exposes common JWK properties and provides **JWASigner**, **JWAKeyManager** or **JWACipher** instances for any of these cryptographic operations assuming they are supported by the JWK. For instance, an **ECJWK** which supports Elliptic-Curve algorithms cannot be used for content encryption but it can be used to digitally sign content and decrypt or derive keys, a **JWKProcessingException** shall be thrown when trying to obtain a signer, a key manager or a cipher when the JWK does not support it, when JWK properties are not consistent with the requested algorithm or if the requested algorithm is not of the requested type.



```

ECJWK ecJWK = jwkService.ec().generator()
    .curve(ECCurve.P_256.getCurve())
    .generate()
    .block();

// Throw a JWKProcessingException since Elliptic-curve algorithms cannot be used to encrypt data
ecJWK.cipher();

// Throw a JWKProcessingException since no algorithm was specified in the JWK
ecJWK.signer();

// Throw a JWKProcessingException since ES512 algorithm is not a key management algorithm
ecJWK.keyManager(ECAAlgorithm.ES512.getAlgorithm());

// Throw a JWKProcessingException since ES512 algorithm is not consistent with curve P_256 (P_512 is
expected)
ecJWK.signer(ECAAlgorithm.ES512.getAlgorithm());

// Return a key manager using ECDH ES algorithm on curve P_256
ecJWK.keyManager(ECAAlgorithm.ECDH_ES.getAlgorithm());

OCTJWK octJWK = jwkService.oct().generator()
    .algorithm(OCTAlgorithm.HS512.getAlgorithm())
    .generate()
    .block();

// Throw a JWKProcessingException since HS256 algorithm is requested which is not consistent with
HS512 algorithm specified in the JWK
octJWK.signer(OCTAlgorithm.HS256.getAlgorithm());

// Return a signer using HS512 algorithm
octJWK.signer();

```

A **SymmetricJWK** exposes a symmetric secret key whereas an **AsymmetricJWK** exposes a public and private key pair.

A **JWK** can be minified using method **minified()** which returns a **JWK** containing required minimal properties as specified by [RFC 7638](#). A JWK thumbprint can be created using method **toJWKThumbprint()** which allows to specify the message digest (defaults to SHA-256) to use to digest the minified **JWK**. A JWK thumbprint can be used as key id to uniquely identify a **JWK**.

A **JWK** can be converted to a public **JWK** using method **toPublicJWK()** which removes any sensitive properties: in case of a **SymmetricJWK** the secret key value is removed and in case of an **AsymmetricJWK** the private key value and any related information are removed.

Private **JWK** containing sensitive data shall never be communicated unprotected, most of the time the public representation shall be enough for a recipient to resolve the key to use to verify or decrypt a JWS or a JWE.

A **JWK** can be trusted or untrusted depending on how the key was resolved by the JWK service. For instance, a **JWK** built from an X.509 certificate chain (**x5c** or **x5u**) whose path could not be validated will be considered untrusted. Digital signature or content decryption will eventually fail in JWS and JWE services when using an untrusted key. It is possible to explicitly trust a key using method **trust()** when its authenticity could be determined using external means.

The **JWKService** bean uses **JWKFactory** implementations to generate, build or read JWKs, they are injected into the service when the module is initialized. Standard implementations supporting Elliptic-curve, RSA, Octet, Edward-Curve, extended Elliptic-Curve and PBES2 keys are provided and injected by default as defined by [RFC 7518](#) and [RFC 8037](#). Additional **JWKFactory** implementations can be added when building the module to extend the module's capabilities and support extra signature, encryption or key management algorithms.

Standard built-in factories are directly exposed on the **JWKService** in order to quickly generate or build specific JWK:

```
// Return the ECJWKFactory
jwkService.ec()...

// Return the RSAJWKFactory
jwkService.rsa()...

// Return the OCTJWKFactory
jwkService.oct()...

// Return the EdECJWKFactory
jwkService.edec()...

// Return the XECJWKFactory
jwkService.xec()...

// Return the PBES2JWKFactory
jwkService.pbes2()...
```

External factories cannot be exposed explicitly by the **JWKService** interface. When reading or generating a **JWK**, The JWK service basically retains all factories that supports the requested key type and algorithm, including external ones. Multiple JWKs built by different factories might then be returned by **read()** and **generate()** methods.

The **JWKService** interface also exposes methods for reading JWK JSON representations. For instance the following example shows how to resolve and read a JWK Set JSON resource located at a specific URIs as defined by [RFC 7517 Section 5](#):

```
// Return one or more JWKs
Publisher<? extends JWK> read = jwkService.read(URI.create("https://host/jwks.json"));
```

## JWK Factory

A `JWKFactory` allows to generate a `JWK` using a `JWKGenerator`, build a `JWK` using a `JWKBuilder` and read a `JWK` from a JSON representation.

### Generating JWK

A `JWKGenerator` is used to generate a new `JWK`. Depending on the type (symmetric or asymmetric) this results in the creation of a secret key or a public and private key pair matching the key type and algorithm specified in the generator instance.

For instance, a symmetric octet key can be generated as follows:

```
JWKSService jwkService = ...

OCTJWK mySymmetricKey = jwkService.oct().generator()
    .keyId("mySymmetricKey")
    .algorithm(OCTAlgorithm.HS512.getAlgorithm())
    .keySize(24)
    .generate()
    .block();
```

An asymmetric RSA key pair can be generated as follows:

```
JWKSService jwkService = ...

Mono<? extends RSAJWK> myAsymmetricKey = jwkService.rsa().generator()
    .keyId("myAsymmetricKey")
    .algorithm(RSAAlgorithm.PS256.getAlgorithm())
    .generate()
    .cache();
```

Note how `cache()` was used to transform the resulting `Mono` into a hot source and prevent generating a new key each time it is being subscribed.

### Building JWK

A `JWKBuilder` is used to build a `JWK` from a set of properties as defined by [RFC 7517](#). A JWK builder does not simply create a `JWK` instance filled with the provided properties, it can also directly resolve the JWK from a `JWKStore` or resolve keys (secret, public or private) using a `JWKKeyResolver` and determines whether the resulting `JWK` is consistent and can be trusted.

The default `JWKKeyResolver` implementation uses a Java Key Store to resolve keys corresponding to the key id or X.509 thumbprints properties in that order. The Java Key Store location is specified in the module's configuration (`JOSEConfiguration`).

In practice, a `JWK` is resolved as follows:

1. The builder first tries to get a matching `JWK` in the module's `JWKStore` from the key id, the X.509 SHA-1 or the X.509 SHA-256 thumbprints in that order. If a matching `JWK` is found the process stops and the `JWK` returned.
2. If no matching `JWK` was found, it tries to resolve the secret key or the public and private key pair from the key id, X.509 SHA-1 or X.509 SHA-256 thumbprints in that order using the module's `JWKKeyResolver`.
3. X.509 certificates chain (`x5c`), if any, is validated using module's `X509JWKCertPathValidator` and corresponding public key value is extracted.
4. X.509 certificates chain URI (`x5u`), if any, is resolved using module's `JWKURLResolver` and validated using module's `X509JWKCertPathValidator` and corresponding public key value is extracted.
5. It then checks that all information are consistent (i.e. specified key values match the ones resolved with the `JWKKeyResolver`, and the ones extracted from X.509 certificates).
6. It finally returns a consistent `JWK` which is trusted when key values were resolved with the `JWKKeyResolver` (which is assumed to be trusted) or when the X.509 certificate path have been validated (i.e. a certificate in the chain is trusted).

Any issue detected during that process results in a `JWKProcessingException`. X.509 certificates chain resolution as well as certificate path validation are disabled by default (`x5c` and `x5u` are simply ignored) and can be activated by setting properties `resolve_x5u` and `validate_certificate` to `true` in the module's configuration (`JOSEConfiguration`).

Automatic resolution of X.509 certificates URI can be dangerous and might be considered as a threat which is why this is disabled by default.

The following example shows how to build an `RSAJWK` with a public and private key pair by specifying each properties:

```

RSAJWK rsaKey = jwkService.rsa().builder()
    .keyId("rsaKey")
    .modulus("oahUIoWw0K0usKNuOR6H4wkf4oBUXHTxRvGb48E-
BVvxkeDNjbC4he8rUwcJoZmds2h7M70imEVhRU5djINXtqlLXI4DFqcI1DgjT9LewND8MW2Krf3Spsk_ZkoFniLakGygTwpZ3ues
H-PFABNIUYp0iN15dsQRkgr0vEhxN92i2asb0enSZeyaxziK72UwxrrKoExv6kc5twXTq4h-
QChL0ln0_mtUZwfsRaMStPs6mS6XrgxnxbWohjf663tuEQueGC-
FCMfra36C9knDFGzKsNa7LZK2djYgyD3JR_MB_4NUJW_Tq0QtwHYbxevoJArm-L5StowjzGy-_bq6Gw")
    .publicExponent("AQAB")
    .privateExponent("kLdtIj6GbDks_ApCSTYQtelcNttlKi0yPzMrXHeI-yk1F7-kpDxY4-
WY5NWV5KntaEeXS1j82E375xxhWMHXyvjYecPT9fpwR_M9gV8n9Hrh2anTpTD93Dt62ypW3yDsJzBnTnrYu1iwwRgBKrEYY46qAZ
IrA2xAwnm2X7uGR1hghkqDp0Vqj3kbSCz1XyfcS6_LehBwtXHIyh8Ripy40p24mo0AbgxVw3rxT_vlt3Uve4W03JkJOzlpUf-
KTVI2Ptgm-dARxTetE-id-40Jr0h-K-VFs3VsndVTIznSxfyrj8ILL6MG_Uv8YAu7VILSB3l0W085-4qE3DzgrTjgyQ")
    .firstPrimeFactor("1r52Xk46c-LsfB5P442p7atdPurxQSy4mti_tZI3Mgf2EuFVbUoDBvaRQ-
SWxkbkmoEzL7JXroSBjSrK3YIQgYdMgyAEPTpjXv_hI2_1eTSPVzfzL0lffNn03IXqWF5MDFuoUYE0hzb2vhrln_rKrbfDIwUbTr
jjgieRbwC6Cl0")

    .secondPrimeFactor("wLb35x7hmQwZsWjMB_vle87ihgZ19S8lBEROLIsZG4ayZVe9Hi9gDVC0BmUDdaDYVTSNx_8Fyw1YYa9X
GrGnDew00J28cRUoeBB_jKI1oma00rv1T9aXIwXkd4gvxFIm0Wr3QRL9KEBRzk2RatUBnmDZJTIAfwTs0g68UZHvtc")
    .firstFactorExponent("ZK-YwE7diUh0qr1tR7w8WHtoLDx3MZ_0TowiFvgfeQ3SiresXjm9gZ5KLhMXvo-uz-
KUJWDxS5pFQ_M0evdo1dKiRTjVw_x4NyqyXPM5nULPkcpU827rnpZzAJKpdhWAgqrXGKAECQH0Xt4taznjnd_zVpAmZZq60WPMBM
fKcuE")

    .secondFactorExponent("Dq0gfgJ1DdFGXiLvQEZNuKEN0UumsJBxkjydc3j4ZYdBiMRAY86x0vHCjywcMlYYg4yoC4YZa9hNV
csjqA3Feil19rk8g6Qn29Tt0cj8qqyFpz9vNDBUfCAiJVeES0jJDZPYHdHY8v1b-o-Z2X5tvLx-TCekf7oxyeKDUqKWjis")
    .firstCoefficient("VIMpMYbPf47dT1w_zDUXfPimsSegnM0A1zTaX7aGk_8urY6R8-
ZW1FxU7AlwAyLWybqq6t16Vfd7hQd0y6fLUK4S10ydB61gwan0sXG0A0v82cHq0E3eL4HrtZkUuKvnPrMnsUUFUdybVzxyjz9J
F_XyaY14ardLSjf4L_FNY")
    .build()
    .block();

```

If we assumed that `rsaKey` is not stored in the module's `JWKStore` and that public and private keys are also not stored in the module's Java Key Store, the resulting `RSAPublicKey` is therefore untrusted since the provided information could not be authenticated.

An untrusted `JWK` cannot be used to digitally sign, encrypt or derive keys. If we know by external means that the provided information can be trusted after all, we can explicitly trust the `JWK` as follows:

```

rsaKey.trust();

// The JWK is now trusted
...

```

Note that this can be considered unsafe and should be used with extra care.

Now if we assume that `rsaKey` is stored in the module's `JWKStore`, the key can be built, or in that case simply loaded, as follows:

```

RSAJWK rsaKey = jwkService.rsa().builder()
    .keyId("rsaKey")
    .build()
    .block();

```

In that case, the returned `JWK` is trusted as it comes from a trusted `JWKStore`.

Finally, if the `rsaKey` is not stored in the module's `JWKStore`, but a public and private key pair is stored in the module's Java Key Store, the `JWK` can be loaded in the exact same way:

```
RSAJWK rsaKey = jwkService.rsa().builder()
    .keyId("rsaKey")
    .build()
    .block();
```

There is however a noticeable difference between the two, when a `JWK` is resolved from the module's `JWKStore`, properties specified in the builder other than the key id or X.509 thumbprints are simply ignored and no further consistency check is performed. On the other hand, when keys are resolved using the module's `JWKKeyResolver`, the properties specified in the builder must be consistent. The purpose of the `JWKStore` is to optimize the resolution of frequently used keys which is incompatible with systematic consistency check.

Please refer to [JWK Store](#) and [JWK Key Resolution](#) to better understand how JWK and key resolution work.

## Reading JWK

A `JWK` is read from a JSON representation in a similar way as the one described for the JWK builder. The JSON object is basically parsed in a map of properties which are then injected in a `JWKBuilder` which is used to build the resulting `JWK`.

The following example shows how to parse the JSON representation of the `RSAJWK` built in previous section:

```

String rsaJwkJSON = "{\n"
    + "    \"n\": \"oahUIoWw0K0usKNuOR6H4wkf4oBUXHTxRvgb48E-  

BVvxkeDNjbC4he8rUwcJoZmds2h7M70imEVhRU5djINXtqlLXI4DFqcI1DgjT9LewND8MW2Krf3Spsk_ZkoFni lakGygTwpZ3ues  

H-PFABNIUYp0iN15dsQRkgr0VEhxN92i2asb0enSZeyaxziK72UwxrrKoExv6kc5twXTq4h-  

QChL0ln0_mtUZwfsRaMStPs6mS6XrgxnxbWhojf663tuEQueGC-  

FCMfra36C9knDFGzKsNa7LZK2djYgyD3JR_MB_4NUJW_Tq0QtWHybxevoJArm-L5StowjzGy-_bq6Gw\", \"n\"  

    + "    \"e\": \"AQAB\", \"d\": \"kLdtIj6GbDks_ApCSTYQtelcNttlKi0yPzMrXHeI-yk1F7-kpDxY4-  

WY5NWV5KntaEeXS1j82E375xxhWMHXyvjYecPT9fpwR_M9gV8n9Hrh2anTpTD93Dt62ypW3yDsJzBnTnrYu1iwwRgBKREYY46qAZ  

IrA2xAwnm2X7uGR1hghkqDp0Vqj3kbSCz1XyfcS6_LehBwtxHIyh8Ripy40p24mo0AbgxVw3rxT_vlt3Uve4W03JkJ0zlpUf-  

KTVI2Ptgm-dARxTetE-id-40Jr0h-K-VFs3VsndVTIznSxfyrj8ILL6MG_Uv8YAu7VILSB3l0W085-4qE3DzgrTjgyQ\", \"n\"  

    + "    \"p\": \"1r52Xk46c-LsfB5P442p7atdPurxQSy4mti_tZI3Mgf2EuFVbUoDBvaRQ-  

SWxkbbkmoEzL7JXroSBjSrK3YIQYdMgyAEPTpjXv_hI2_1eTSPVZfzL0lffNn03IXqWF5MDFu0UYE0hzb2vhr lN_rKrbfDIwUbTr  

jjgieRbwC6Cl0\", \"n\"  

    + "  

    \"q\": \"wLb35x7hmQWZsWjMB_vle87ihgZ19S8lBER0LIsZG4ayZVe9Hi9gDVC0BmUDDaDYVTSNx_8Fyw1YYa9XGrGnDew00J28  

cRUoeBB_jKI1oma00rv1T9aXIwXKwd4gvxFIm0Wr3QRL9KEBRzK2RatUBnmDZJTIAfWts0g68UZHvtc\", \"n\"  

    + "    \"dp\": \"ZK-Ywe7diUh0qR1tR7w8WhtolDx3MZ_OTowiFvgfeQ3SiresXjm9gZ5KLhMXvo-uz-  

KUJWdX5SpFQ_M0evdo1dKiRtjVw_x4NyqyXPM5nULPkcpU827rnpZzAJKpdhwAgqrXGKAECQH0Xt4taznjnd_zVpAmZZq60WPMBM  

fKcuE\", \"n\"  

    + "  

    \"dq\": \"Dq0gfgJ1DdFGXiLvQEznuKEN0UumsJBxkjydc3j4ZYdBimRAY86x0vHCjywcMlYYg4yoC4YZa9hNVcsjqA3FeiL19rk  

8g6Qn29Tt0cj8qqyFpz9vNDBUfCAiJVeES0jJDPYHdHY8v1b-o-Z2X5tvLx-Tcekf7oxyeKDUqKwjis\", \"n\"  

    + "    \"qi\": \"VIMpMYbPf47dT1w_zDUXfPimsSegnMOA1zTaX7aGk_8urY6R8-  

ZW1FXU7AlwAyLWybqq6t16Vfd7hQd0y6fLUK4SLOydb61gwan0sXG0A0v82cHq0E3eL4HrtZkUuKvnPrMnsUUFUdybVzxyjz9J  

F_XyaY14ardLSjf4L_FNY\", \"n\"  

    + "    \"kty\": \"RSA\", \"n\"  

    + "    \"kid\": \"rsaKey\\\"\\n\"  

    + "}\"";

```

```
RSAJWK rsaKey = jwkService.rsa().read(rsaJwkJSON).block();
```

The same rules as the ones described for the JWK builder apply. In above code the resulting **JWK** is untrusted. Assuming a **rsaKey** JWK is stored in the module's **JWKStore**, the following code shall return a workable **JWK**:

```

String rsaJwkJSON = "{\n"
    + "    \"kid\": \"rsaKey\\\"\\n\"  

    + "}\"";

```

```
RSAJWK rsaKey = jwkService.rsa().read(rsaJwkJSON).block();
```

Note that we did not have to specify the key type here since we are directly using the **RSAJWKFactory** to read the JSON representation. We could have invoked the **read()** method on the **JWKService** instead but the key type would then have been required in order to determine which JWK factory to use.

## JWK Store

The *security-jose* module uses a **JWKStore** to store and load frequently used keys. By default the module uses a no-op implementation but more effective implementations can be injected when creating the module.

The purpose of the `JWKStore` is optimize key resolution when loading keys while creating or reading JWS or JWE. As soon as a key is matched by a key id, an X.509 SHA-1 or X.509 SHA-256 thumbprint, the key shall be returned and no further processing performed, including consistency checks.

Note that this actually goes a bit against [RFC 7517](#) for which inconsistent JWK must be rejected but this is a fair optimization as the returned `JWK` shall always be consistent.

The `JWKStore` interface exposes methods `getByKeyId()`, `getBy509CertificateSHA1Thumbprint()` and `getByX509CertificateSHA256Thumbprint()` which are respectively used by `JWKBuilder` implementation to resolve `JWK` by key id, X.509 SHA-1 and X.509 SHA-256 thumbprints. The `set()` and `remove()` methods are used to add or remove `JWK` instances.

The `InMemoryJWKStore` is a simple implementation that stores keys in concurrent hash maps, the following wrapper bean can be defined in a module to override the default no-op implementation:

```
@Wrapper
@Bean
public class JWKStoreWrapper implements Supplier<JWKStore> {

    @Override
    public JWKStore get() {
        return new InMemoryJWKStore();
    }
}
```

Or it can be injected directly in the module's builder if the module is created and initilized explicitly:

```
Jose jose = new Jose.Builder(List.of(jsonConverter, textConverter)).setJwkStore(new
InMemoryJWKStore()).build();

jose.start();
...
jose.stop();
```

The `JWKStore` is exposed in the `JWKService`, a `JWK` can be stored as follows:

```
jwkService.oct().generator()
    .keyId("octKey")
    .algorithm(OCTAlgorithm.HS512.getAlgorithm())
    .generate()
    .map(JWK::trust)
    .flatMap(jwkService.store()::set)
    .block();
```

Since keys resolved from the `JWKStore` are usually used when validating or decrypting JWS or JWE, they should all be trusted to avoid errors.



The `InMemoryJWKStore` is a basic implementation that does not check this condition before storing an instance but more advanced implementations should definitely consider rejecting untrusted keys. Whatever the solution, processing will eventually fail when using an untrusted key.

## JWK Key resolution

When building or reading a `JWK`, actual keys (secret, public and private) can be resolved by key id, X.509 SHA-1 or X.509 SHA-256 thumbprints in a `JWKBuilder` implementation using the module's `JWKKeyResolver`.

The module provides a default implementation that look up keys in a Java Key Store whose location is specified in the module's configuration. Key resolution will be disabled if the key store configuration is missing.

Let's assume we have a Java Key Store `keystore.jks` accessible with password `password`, the following configuration allows the default `JWKKeyResolver` implementation to resolve keys from that key store:

```
### configuration.cprops
io.inverno.example.app_jose.appConfiguration {
    jose {
        key_store = "file:/path/to/keystore.jks"
        key_store_password = "password"
    }
}
```

Unlike the `JWKStore`, a `JWKProcessingException` is thrown when resolved keys are not consistent with the properties specified in the JWK builder.

Custom `JWKKeyResolver` implementation can be provided to override the default behaviour by defining a bean in the module or by directly injecting the instance in the module's builder when the module is created and initialized explicitly:

```
Jose jose = new Jose.Builder(List.of(jsonConverter, textConverter)).setJwkKeyResolver(new
CustomJWKKeyResolver()).build();
```

## JWK Set resolution

The `JWKService` can be used to resolve multiple keys from a URI pointing to a JWK Set resource as defined by [RFC 7517 Section 5](#).

For instance, the keys defined in a JWK Set at location `https://server.example.com/keys.jwks` can be resolved as follows:

```
Publisher<? extends JWK> read = jwkService.read(URI.create("https://server.example.com/keys.jwks"));
```

The `JWKService` delegates to the module's `JWKURLResolver` to resolve the resource as a map of properties, the default implementation uses a `ResourceService` which must be injected into the module for the feature to be activated.

A complete `ResourceService` implementation supporting common URI schemes (`file://`, `http://`, `classpath:...`) is provided in the `boot` module.

JWK set resolution is also used as a last resort to resolve keys when building or reading JWS or JWE with property `jku`, this behaviour is disabled by default and must be activated explicitly in the module's configuration (`JOSEConfiguration`) by setting `resolve_jku` property to `true`:

```
### configuration.cprops
io.inverno.example.app_jose.appConfiguration {
    jose {
        resolve_jku = true
    }
}
```

Automatic resolution of JWK Set URL can be dangerous and might be considered as a threat which is why this is disabled by default.

`JWK` instances obtained that way from external JWK Set resources are considered untrusted by default, and therefore cannot be used to build or read JWS or JWE, unless locations (i.e. URIs) are explicitly as a trusted listed in the module's configuration (`JOSEConfiguration`) in `trusted_jku` property.

For instance, the following configuration can be set to trust keys resolved from `https://server.example.com/keys.jwks`:

```
### configuration.cprops
io.inverno.example.app_jose.appConfiguration {
    jose {
        trusted_jku = "https://server.example.com/keys.jwks"
    }
}
```

## Certificate path validation

When building or reading a `JWK` with an X.509 certificates chain or X.509 certificates chain URI, it is possible to validate the certificates chain in order to determine whether the resulting `JWK` can be trusted.

An X.509 certificate is considered trusted if any of the certificate in the chain is trusted. An `X509JWKCertPathValidator` is used in `JWKBuilder` implementations to validate resolved certificates chains.

The default implementation uses a PKIX `CertPathValidator` with `PKIXParameters` defining the trusted certificates, these parameters are provided by the `JWKPKIXParameters` wrapper bean which uses the trust store of the JDK by default. This bean is overridable and custom `PKIXParameters` can be provided as well by defining a bean in the module or by directly injecting the instance in the module's builder when the module is created and initialized explicitly:

```
CertStore customTrustStore = ...
```

```
Jose jose = new Jose.Builder(List.of(jsonConverter, textConverter)).setJwkPKIXParameters(new  
JWKPKIXParameters(customTrustStore).get()).build();
```

Certificate path resolution is disabled by default and must be activated explicitly in the module's configuration ([JOSEConfiguration](#)) by setting `validate_certificate` property to `true`:

```
### configuration.cprops  
io.inverno.example.app_jose.appConfiguration {  
    jose {  
        validate_certificate = true  
    }  
}
```

## JSON Web Algorithms

The *security-jose* module fully supports algorithms specified in [RFC 7518 JSON Web Algorithm \(JWA\)](#), [RFC 8037](#) and [RFC 8812](#) and used to sign/verify, encrypt/decrypt and derive content encryption keys. They are grouped into categories with associated `JWK` implementations and `JWAAlgorithm` enum listing the algorithms and defining the parameters required to create corresponding `JWASigner`, `JWACipher` and `JWAKeyManager`.

The `JWA` interface is the base type extended by all JWA algorithms including `JWASigner` for digital signature algorithms, `JWACipher` for encryption algorithms and `JWAKeyManager` for key management algorithms.

The `JWASigner` interface exposes methods `sign()` and `verify()` used to respectively sign and verify some arbitrary data.

```
byte[] payload = "This is a payload".getBytes();  
  
JWASigner signer = ...  
  
byte[] signature = signer.sign(payload);  
  
if(signer.verify(payload, signature)) {  
    ...  
}
```

The `JWACipher` interface exposes methods `encrypt()` and `decrypt()` to respectively encrypt and decrypt some arbitrary data. Encryption requires additional authentication data and a `SecureRandom` for random number generation and returns encrypted data composed of a cipher text, an initialization vector and an authentication tag. Decryption requires the additional authentication data, the cipher text, the initialization vector and the authentication tag (which are basically the components of a JWE).

```
byte[] payload = "This is a payload".getBytes();
// Specified in RFC 7516
byte[] aad = ...

JWACipher cipher = ...

JWACipher.EncryptedData encryptedData = cipher.encrypt(payload, aad);

byte[] decryptedPayload = cipher.decrypt(encryptedData.getCipherText(), aad,
encryptedData.getInitializationVector(), encryptedData.getAuthenticationTag());
```

Key management algorithms are used to determine the Content Encryption Key (CEK) used to encrypt a JWE, they are further divided into **DirectJWAKeyManager** for algorithms that derives the content encryption key which is not encrypted, **EncryptingJWAKeyManager** for algorithms that encrypt/decrypt the content encryption key and **WrappingJWAKeyManager** for algorithms that wrap/unwrap the content encryption key.

Key management algorithm usually requires specific parameters passed in the JOSE header, as a result methods exposed by key managers usually require the algorithm and a map of parameters.

A **DirectJWAKeyManager** is used to derive the CEK on both ends using parameters specified in a JOSE header.

```
// e.g. Ephemeral public key (epk), Agreement PartyUInfo (apu), Agreement PartyVInfo (apv) when
using ECDH-ES algorithm
Map<String, Object> parameters = ...

DirectJWAKeyManager directKeyManager = ...

DirectJWAKeyManager.DirectCEK directCEK = directKeyManager.deriveCEK("ECDH-ES", parameters);
OCTJWK cek = directCEK.getEncryptionKey();
```

When using a direct key management algorithm, the encrypted key part of the JWE is empty since the CEK is derived and not encrypted or wrapped.

An **EncryptingJWAKeyManager** is used to encrypt and decrypt the CEK.

```
// e.g. PBES2 Salt Input (p2s), PBES2 Count (p2c) when using PBES2-HS256+A128KW algorithm
Map<String, Object> parameters = ...
// Generated when building a JWE
JWK cek = ...

EncryptingJWAKeyManager encryptingKeyManager = ...

EncryptingJWAKeyManager.EncryptedCEK encryptedCEK = encryptingKeyManager.encryptCEK(cek,
parameters);
byte[] encryptedKey = encryptedCEK.getEncryptedKey();

JWK decryptedCEK = encryptingKeyManager.decryptCEK(encryptedKey, "PBES2-HS256+A128KW", parameters);
```

A **WrappingJWAKeyManager** is used to wrap and unwrap the CEK.

```

Map<String, Object> parameters = ...
// Generated when building a JWE
JWK cek = ...

WrappingJWKeyManager wrappingKeyManager = ...

WrappingJWKeyManager.WrappedCEK wrappedCEK = wrappingKeyManager.wrapCEK(cek, parameters);
byte[] wrappedKey = wrappedCEK.getWrappedKey();

JWK unwrappedCEK = wrappingKeyManager.unwrapCEK(wrappedKey, "A192KW", parameters);

```

Although signers, ciphers and key managers are usually used indirectly when building or reading JWS or JWE but they can also be used directly as shown above.

## Octet

Octet algorithms are based on a shared secret key, they are listed in the `OCTAlgorithm` enum.

The following example shows how to obtain an A128GCM `JWACipher` from a generated `OCTJWK`:

```

JWACipher cipher = jwkService.oct().generator()
    .algorithm(OCTAlgorithm.A128GCM.getAlgorithm())
    .generate()
    .block()
    .cipher();

```

## Elliptic Curve

Elliptic-curve algorithms are based on a public and private key pair and using a specific Elliptic curve (P-256, P-384, P-521 defined in `ECCurve` enum), they are listed in the `ECAAlgorithm` enum.

Elliptic-curve cryptography has the advantage of producing smaller signatures than RSA for the same level of protection.

The following example shows how to obtain an ES384 `JWASigner` from a generated `ECJWK` using default P-256 curve:

```

JWASigner signer = jwkService.ec().generator()
    .algorithm(ECAAlgorithm.ES384.getAlgorithm())
    .generate()
    .block()
    .signer();

```

## RSA

RSA algorithms are based on a public and private key pair, they are listed in the `RSAAAlgorithm` enum.

The following example shows how to obtain an RSA\_OAEP `JWKeyManager` (`EncryptingJWKeyManager`) from a generated `RSAWK`:

```
JWAKeYManager keyManager = jwkService.rsa().generator()
    .algorithm(RSAAlgorithm.RSA_OAEP.getAlgorithm())
    .generate()
    .block()
    .keyManager();
```

## PBES2

PBES2 algorithms are based on a shared secret key, namely a password, they are listed in the `PBES2Algorithm` enum.

They are usually used for the password-based encryption of the CEK in a JWE.

The following example shows how to obtain a PBES2-HS256+A128KW `JWAKeYManager` (`EncryptingJWAKeYManager`) from a generated `PBES2JWK`:

```
JWAKeYManager keyManager = jwkService.pbes2().generator()
    .algorithm(PBES2Algorithm.PBES2_HS256_A128KW.getAlgorithm())
    .length(32) // generate a 32 characters long password
    .generate()
    .block()
    .keyManager();
```

## Edward-Curve

Edward-curve algorithms are based on a public and private key pair and using a specific Edward-curve (Ed25519, Ed448, X25519, X448 defined in `OKPCurve`), they are listed in the `EdECAlgorithm` enum.

The following example shows how to obtain an Ed25519 `JWASigner` from a generated `EdECJWK`:

```
JWASigner signer = jwkService.edec().generator()
    .algorithm(EdECAlgorithm.EDDSA_ED25519.getAlgorithm())
    .generate()
    .block()
    .signer();
```

## Extended Elliptic Curve

Extended elliptic-curve algorithms are based on a public and private key pair, they are listed in the `XECAlgorithm` enum.

These algorithms basically combine ECDH\_ES algorithms with elliptic-curve algorithms to wrap the CEK in a JWE.

The following example shows how to obtain an ECDH-ES+A128KW `JWAKeYManager` (`WrappingJWAKeYManager`) from a generated `XECJWK`:

```
java jwkService.xec().generator() .algorithm(XECAlgorithm.ECDH_ES_A128KW.getAlgorithm())
    .curve(OKPCurve.X25519.getCurve()) .generate() .block() .keyManager();`
```

# JWS Service

The JWS service is used to build or read JWS represented using the compact or the JSON notation as defined by [RFC 7515](#).

The `JWSService` bean is used to create `JWSBuilder` or `JsonJWSBuilder` instances to build JWS using the compact or the JSON notation and `JWSReader` or `JsonJWSReader` instances to read JWS serialized using the compact or JSON notation.

A JWS allows to communicate integrity protected content using digital signatures or message authentication codes (MACs). It is composed of three parts:

- a JOSE header which specifies how to understand (i.e. type, content type...), sign or verify the JWS.
- a payload which is digitally signed in the JWS.
- a signature which is essentially the digital signature of the concatenation of the header and the payload.

A `JWS` is obtained from a `JWSBuilder` or a `JWSReader`, the `JWS` interface exposes the header, the payload and the signature. It can be serialized using the compact notation as follows:

```
JWS<?> jws = ...

// <header>.<payload>.<signature>
// e.g.
eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJqb2UiLA0KICJleHAiOiJleMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlIiwibmVkbS9pc19yb290Ijp0cnVlfQ.dBjftJeZ4CVP-mB92K27uhbUJU1p1r_ww1gFWFOEjXk
String jwsCompact = jws.toCompact();
```

A `JsonJWS` is obtained from a `JsonJWSBuilder` or a `JsonJWSReader`, the `JsonJWS` interface exposes the payload and the list of signatures. It can be serialized using the JSON notation as follows:

```
JsonJWS<?, ?> jsonJWS = ...
```

```
/*
 * RFC 7515 Appendix A.6
 *
 * {
 *   "payload":
"eyJpc3MiOiJqb2UiLA0KICJleHAiOiJlZMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ",
 *   "signatures": [
 *     {
 *       "protected": "eyJhbGciOiJSUzI1NiJ9",
 *       "header": {
 *         "kid": "2010-12-29"
 *       },
 *       "signature": "cC4hiUPoj9Eetdgtv3hF80EGrhuB__dzERat0XF9g2VtQgr9PJbu3X0iZj5RZ
 *         mh7AAuHIm4Bh-0Qc_lF5YKt_08W2Fp5jujGbdS9uJdbF9CUAr7t1dnZcAcQjb
 *         KBYNX4BAynRFdiuB--f_nZLgrnbyTyWz075vRK5h6xBARLIARNPvkSjtQBMHl
 *         b1L07Qe7K0GarZRmB_eSN9383Lc0Ln6_d0--xi12jzDwusC-e0kHWEsqtfZES
 *         c6BfI7no0PqvhJ1phCnvWh6IeYI2w9Q0YEUipUTI8np6LbgGY9Fs98rqVt5AX
 *         LIhWkWywLVmtVrBp0igcN_IoypGLUPQGe77Rw"
 *     },
 *     {
 *       "protected": "eyJhbGciOiJFUzI1NiJ9",
 *       "header": {
 *         "kid": "e9bc097a-ce51-4036-9562-d2ade882db0d"
 *       },
 *       "signature": "DtEhU3ljbEg8L38VWAfUAq0yKAM6-Xx-F4GawxaePMXFCgfTjDxw5dJxLa8IS
 *         lSAPmWQxfKTUJqPP3-Kg6NU1Q"
 *     }
 *   ]
 * }
 */
String jwsJson = jsonJWS.toJson();
```

The detached compact representation as specified by [RFC 7797](#) is also supported and can be used when large payloads communicated by external means are considered.

```
JWS<?> jws = ...
```

```
// <header>..<signature>
// e.g. eyJhbGciOiJFUzUxMiJ9..AdwMgeerwtHoh-l192l60hp9wAHZfVJbLfD_UxMi70cwnZOYaRI1bKPWROc-
mZZqwqT2SI-
KGDKB34X00aw_7XdtaG8GaSwFKdCAPZgoXD2YBJZCPEx3xKpRwcd008KpEHwJjyq0gzD07iKvU8vcnwNrmxYbSw9ERBXuk0XoLLz
e0_Jn
String jwsDetachedCompact = jws.toDetachedCompact();
```

The most common representation is by far the compact representation which can be safely used in URLs. On the other hand, the JSON notation can be used to target multiple systems with various JWKs.

A JWS offers integrity protection of its content using a digital signature, as a result, building or reading a JWS requires a [JWK](#) supporting digital signature algorithms.



## Building JWS

A `JWSBuilder` is used to create `JWS`, it is obtained by invoking one of the `builder()` methods on the `JWSService` bean. The actual payload type can be specified explicitly in the method as well as the `JWK` to use to digitally sign the `JWS`.

The `builder()` method actually accepts a publisher of `JWK` which means multiple keys can be considered when building the JWS. If keys are not specified, they are resolved from the JOSE header parameters using the `JWK service`. When building a JWS, the `JWSBuilder` basically retains the first trusted `JWK` that was able to sign the JWS. The retained `JWK` is exposed in the resulting `JWSHeader`. It is important to note that untrusted `JWK` are filtered out. A `JOSEObjectBuildException` is thrown if no suitable keys could be found.

A `JWSbuilder` uses media type converters injected in the module to encode the JWS payload based on the content type which can be either specified in the JOSE header (`cty`), or when invoking the `build()` method. An explicit `Function<T, Mono<String>>` encoder can also be specified in order to bypass media type converters.

A specific encoder basically overrides the content type specified in `build()` method which overrides the content type specified in the JOSE header.

The digital signature is computed by applying a signature algorithm to the JWS signing input composed of the JWS header and the serialized payload.

The following example shows how to build a `JWS` with a generated `JWK` and a payload serialized as `application/json` using corresponding media type converter:

```
// Injected or obtained from a 'Jose' instance
JWKService jwkService = ...
JWSService jwsService = ...

Mono<? extends OCTJWK> key = jwkService.oct().generator()
    .keyId("keyId")
    .algorithm(OCTAlgorithm.HS256.getAlgorithm())
    .generate()
    .cache();

JWS<Message> jws = jwsService.builder(Message.class, key)
    .header(header -> header
        .keyId("keyId")
        .algorithm(OCTAlgorithm.HS256.getAlgorithm())
    )
    .payload(new Message("John", "Hello world!"))
    .build(MediaTypes.APPLICATION_JSON)
    .block();

//
eyJhbGciOiJIUzI1NiIsImtpZCI6ImtleUlkIn0.eyJhdXRob3IiOiJkb2huIiwibWVzc2FnZSI6IkhlbGxvIHRvcmxkISJ9.aSR
mKH3ZiTGM2MrKBLqBJH-d-rBEt5bWPY6TEC15B7s
String jwsCompact = jws.toCompact();
```

Assuming the `JWK` can be resolved by the `JWKService` using the key id (from module's `JWKStore` or `JWKKeyResolver`), the key can be omitted when creating the builder:

```
// Using an 'InMemoryJWKStore', we can store the key so it can be resolved by key id by the
// 'JWKService'
key.map(JWK::trust).map(jwkService.store()::set).block();

// Key 'keyId' is then automatically resolved
JWS<Message> jws = jwsService.builder(Message.class)
    ...
```

The JWS JSON representation as defined by [RFC 7515 Section 7.2](#) is a JWS representation that is neither optimized nor URL-safe. This notation can hardly be compared to the compact notation and it shall be used for very different purposes, for instance to communicate digitally signed or MACed content in JSON using different keys and algorithms to one or more recipients.

A `JsonJWSBuilder` is used to create `JsonJWS` with multiple signatures following the JSON representation specification, it is obtained by invoking one of the `jsonBuilder()` methods on the `JWSService` bean. Since a `JsonJWS` might have multiple signatures using different keys and algorithms, only the payload type can be specified when creating the builder, keys will be provided or resolved later in the process.

A `JsonJWS` is created in a similar way as for a `JWS` with one payload but multiple JOSE headers to create multiple signatures. The JOSE header is then divided into an unprotected header and a protected headers which, unlike the unprotected header, is included in the digital signature. Protected and unprotected headers must be disjoint and content related parameters such as the type (`typ`) or the content type (`cty`) must be consistent across all signature headers. Some sensitive parameters such as the algorithm (`alg`) must also be integrity protected and therefore specified exclusively in the protected header. A `JWSBuildException` shall be thrown in case of invalid or inconsistent signature headers. Keys must be provided explicitly or resolved automatically for each signature to be able to compute the digital signature.

The following example shows how to build a `JsonJWS` with two signatures using generated keys and a payload encoded using an explicit encoder:

```

// Injected or obtained from a 'Jose' instance
JWKSService jwkService = ...
JWSService jwsService = ...

Mono<? extends OCTJWK> key1 = jwkService.oct().generator()
    .keyId("key1")
    .algorithm(OCTAlgorithm.HS256.getAlgorithm())
    .generate()
    .cache();

Mono<? extends RSAJWK> key2 = jwkService.rsa().generator()
    .keyId("key2")
    .algorithm(RSAAlgorithm.RS256.getAlgorithm())
    .generate()
    .cache();

JsonJWS<Message, BuiltSignature<Message>> jsonJWS = jwsService.jsonBuilder(Message.class)
    .signature(
        protectedHeader -> protectedHeader
            .keyId("key1")
            .algorithm(OCTAlgorithm.HS256.getAlgorithm()),
        unprotectedHeader -> {},
        key1
    )
    .signature(
        protectedHeader -> protectedHeader
            .keyId("key2")
            .algorithm(RSAAlgorithm.RS256.getAlgorithm()),
        unprotectedHeader -> {},
        key2
    )
    .payload(new Message("Alice", "Hi John!"))
    .build(message -> Mono.just(message.getAuthor() + " > " + message.getMessage()))
    .block();

/*
 * {
 *   "signatures": [
 *     {
 *       "header": {
 *         "kid": "key1",
 *         "cty": "text/plain"
 *       },
 *       "signature": "u38wYs0v1M-zgw0lr2Gw3PKRALPxwH6I4wfpLFF_E3I",
 *       "protected": "eyJhbGciOiJIUzI1NiJ9"
 *     },
 *     {
 *       "header": {
 *         "kid": "key2",
 *         "cty": "text/plain"
 *       },
 *       "signature": "X6J77kf7sXW_7j7tLvGwJR2hy2kvDjuEGdT-1WU_Po2Z0sMPvHJd9LRdgYWUCn10V6
 *         xgNatDQuwEnegOrIOVTI2yN6_T74rQY1-VW08kESg_MyGRoieC3s6beQAt0JdwKgSs
 *         xNZjCbRLTu_bxTpIl90j2MgPNHiL8ox2uDwA3pg-6cgEzswMQx6x_KQ-e3VPuqdiSd
 *         6PNeFNiYN-s9xBTlN_m-0k8MDHSzQ612Ms3Q1ox2gONdpVG3wcoIPX63zaRmt-a3r6
 *         KReL9bPBs1hCRHxp6ermxwJRf0yjkfo2KH2fwV_wMiPsCdbJSIL3MPrer0yi5iVDu
 *         iXK-yWoJ2X0g",
 *       "protected": "eyJhbGciOiJIUzI1NiJ9"
 *     }
 *   ]
 * }

```

```

*   },
*   "payload": "QWxpY2UgPiBIaSBKb2huIQ"
* }
*/
String jwsJson = jsonJWS.toJson();

```

In above code, we can see that the payload is common to all signatures which explains why content related parameters must be consistent across all signatures and to make this clear the content type was specified in the common unprotected header. Each resulting unprotected headers then contain the key id and the JWS content type whereas protected headers, encoded in Base64, contain the algorithms that were used to digitally sign the JWS.

The `JsonJWS` interface exposes the payload as well as the `JWS` instances corresponding to each signature.

```

Message message = jsonJWS.getPayload();

List<JWS> jwsSignatures = jsonJWS.getSignatures().stream()
    .map(signature -> signature.getJWS())
    .collect(Collectors.toList());

```

Note that the `JWS` instances thus obtained are deduced from the JSON representation which makes a difference between protected and unprotected headers, as a result the actual header used in the signature corresponds to the protected header but the `JWSHeader` exposed in the `JWS` results from the merge of the protected and unprotected headers.

## Reading JWS

A `JWSReader` is used to read JWS compact representations, it is obtained by invoking one of the `reader()` methods on the `JWSService` bean. The expected payload type must be specified explicitly in the method and the `JWK` to use to verify the JWS signature can be specified as well.

As for the `JWSBuilder`, a `JWSReader` can consider multiple keys to verify a JWS signature. If keys are not specified, they are resolved from the JOSE header parameters using the [JWK service](#). When reading a `JWS`, the `JWSReader` basically uses provided or resolved trusted `JWK` in sequence to verify the signature and stops when the signature could be verified. As for the `JWSBuilder`, untrusted `JWK` are filtered out and a `JOSEObjectReadException` is thrown if no suitable keys could be found. A `JWSReadException` with aggregated errors (`getSuppressed()`) is thrown when reading an invalid JWS.

A `JWSReader` also uses media type converters injected in the module to decode the JWS payload based on the JWS content type defined in the JOSE header (`cty`) or explicitly specified when invoking the `read()` method. An explicit `Function<String, Mono<T>>` decoder can also be specified in order to bypass media type converters.

A specific decoder basically overrides the content type specified in `read()` method which overrides the content type in the JOSE header.



```
// Injected or obtained from a 'Jose' instance
JWKSService jwkService = ...
JWSService jwsService = ...

Mono<? extends OCTJWK> key = jwkService.oct().builder()
    .keyId("keyId")
    .algorithm(OCTAlgorithm.HS256.getAlgorithm())
    .keyValue("xqf1haCsSJGuueZivcq4YafdWw6n5CH2BTT6vDwUSaM")
    .build()
    .cache();

String jwsCompact = "eyJhbGciOiJIUzI1NiIsImtpZCI6ImtleUlkIiwia3R5IjoiaXBwbGljYXRpb24vanNvbiJ9."
    + "eyJhdXRob3IiOiJCawxsIiwibWVzc2FnZSI6IkhleSEifQ."
    + "pNS2tZmB20ezMA-twec0hobDk3H5AgWyh-m5eV5xE14";

JWS<Message> jws = jwsService.reader(Message.class, key)
    .read(jwsCompact)
    .block();

// Bill says Hey!
Message message = jws.getPayload();
```

Assuming the `JWK` can be resolved by the `JWKS` using the key id (from module's `JWKStore` or `JWKKeyResolver`), the key can be omitted when creating the reader:

```
// Using an 'InMemoryJWKStore', we can store the key so it can be resolved by key id by the
// 'JWKSService'
key.map(JWK::trust).map(jwkService.store()::set).block();

// Key 'keyId' is then automatically resolved
JWS<Message> jws = jwsService.reader(Message.class)
    .read(jwsBytes);
```

A `JsonJWSReader` is used to read JWS JSON representations as defined by [RFC 7515 Section 7.2](#), it is obtained by invoking one of the `jsonReader()` methods on the `JWSService` bean. Since a `JsonJWS` might have multiple signatures using different keys and algorithms, only the payload type must be specified when creating the reader. A `JsonJWS` is basically read without verifying signatures which must later be verified individually, keys can then be specified explicitly or automatically resolved. A `JsonJWS` can be considered valid if one signature could be verified.

The `JsonJWS` instance returned by a `JsonJWSReader` actually differs from the one returned by a `JsonJWSBuilder`, a built `JsonJWS` exposes `JsonJWS.BuiltSignature` which exposes a valid `JWS` whereas a read `JsonJWS` exposes `JsonJWS.ReadSignature` which exposes `readJWS()` methods to actually verify the signature and return the corresponding `JWS`.

The following example shows how to read and verify a JWS JSON representation with two signatures, the payload being decoded using an explicit decoder:

```

// Injected or obtained from a 'Jose' instance
JWKSService jwkService = ...
JWSService jwsService = ...

Mono<? extends ECJWK> key2 = jwkService.ec().builder()
    .keyId("key2")
    .algorithm(ECAAlgorithm.ES256.getAlgorithm())
    .curve(ECCurve.P_256.getCurve())
    .xCoordinate("f830J3D2xF1Bg8vub9tLe1gHMzV76e8Tus9uPHvRVEU")
    .yCoordinate("x_FEzRu9m36HLN_tue659LNpXW6pCyStikYjKIWI5a0")
    .eccPrivateKey("jpsQnnGQmL-YBIffH1136cspYG6-0iY7X1fCE9-E9LI")
    .build()
    .cache();

String jwsJson = "{"
    + "  \"signatures\": ["
    + "    {"
    + "      \"header\": {"
    + "        \"cty\": \"text/plain\", \"
    + "        \"kid\": \"key1\""
    + "      }, \"
    + "      \"signature\": \"PxhpMkmTep5obGFZv500sRGA-e7-fxhUmWdUyLC74ms\", \"
    + "      \"protected\": \"eyJhbGciOiJIUzI1NiJ9\""
    + "    }, \"
    + "    {"
    + "      \"header\": {"
    + "        \"cty\": \"text/plain\", \"
    + "        \"kid\": \"key2\""
    + "      }, \"
    + "      \"signature\": \"KqjGSxiBD5GhwFhLs8H_RBg8nXsKtp4nj5PsdxCzd0ZqMed874ZAxTgnyd0KmQEZwmYvvgM-o8NC9VdIWaIMvw\", \"
    + "      \"protected\": \"eyJhbGciOiJFUzI1NiJ9\""
    + "    }, \"
    + "  ], \"
    + "  \"payload\": \"T6luZGEgPiBTaGFsbCB3ZSBiZWdpbj8\""
    + "}";

JsonJWS<Message, ReadSignature<Message>> jsonJWS = jwsService.jsonReader(Message.class)
    .read(jwsJson, p -> {
        Mono.fromSupplier(() -> {
            int separatorIndex = p.indexOf(">");
            return new Message(p.substring(0, separatorIndex - 1), p.substring(separatorIndex + 2));
        })
    })
    .block();

// Return as soon as one of the signatures could have been verified with key2
JWS<Message> verifiedJWS = Flux.fromIterable(jsonJWS.getSignatures())
    .flatMap(signature -> signature.readJWS(key2).onErrorResume(e -> Mono.empty()))
    .blockFirst();

if(verifiedJWS != null) {
    // Linda says Shall we begin?
    Message message = verifiedJWS.getPayload();
}

```

In above code, the verified **JWS** should correspond to the second signature since we used **key2** to verify the **JsonJWS** signatures.

defined by [RFC 7515](#), custom parameters listed in the critical header parameter (`crit`) and present in the JOSE header must be fully understood by the application for the JWS to be valid. The parameters actually processed by an application and therefore understood can be specified on the `JWSReader` which throws a `JOSEObjectReadException` when encountering unknown critical parameters.

the following example, the `JWSReader` is setup to understand custom parameter `http://example.com/application_parameter` which allows it to read the specified JWS:

```

no<? extends OCTJWK> key = jwkService.oct().builder()
    .keyId("keyId")
    .algorithm(OCTAlgorithm.HS256.getAlgorithm())
    .keyValue("xqf1haCsSJGuueZivcq4YafdWw6n5CH2BTT6vDwUSaM")
    .build()
    .cache();

{
    "header": {
        "alg": "HS256",
        "kid": "keyId",
        "crit": [
            "http://example.com/application_parameter"
        ],
        "http://example.com/application_parameter": true
    },
    "payload": "Lorem ipsum",
    "signature": "aQMwOhoxZW0cpYVm04FBJwGc7fB04xzUKVJz9qfjpxc"
}

String jwsCompact =
    yJhbGciOiJIUzI1NiIsImtpZCI6ImtleUlkIiwiaWY3JpdCI6WyJodHRwOi8vZXhhbXBsZS5jb20vYXBwGljYXRpb25fcGFyYW1yGyIl0sImh0dHA6Ly9leGFtcGxlLmNvbS9hcHBsaWNoZGlvdGl9wYXJhbWV0ZXIiOnRydWV9."
    + "TG9yZW0gaXBzdW0."
    + "aQMwOhoxZW0cpYVm04FBJwGc7fB04xzUKVJz9qfjpxc";

String> jws = jwsService.reader(String.class, key)
    .processedParameters("http://example.com/application_parameter")
    .read(jwsCompact, MediaType.TEXT_PLAIN)
    .block();

```

## WE Service

The JWE service is used to build or read JWE represented using the compact or the JSON notation as defined by [RFC 7516](#).

The `JWEService` bean is used to create `JWEBuilder` or `JsonJWEBuilder` instances to build JWE using the compact or the JSON notation and `JWEReader` or `JsonJWEReader` instances to read JWE serialized using the compact or JSON notation.

WE allows to communicate encrypted content using cryptographic algorithms that arantees both integrity and confidentiality. It is composed of five parts:

- a JOSE header which specifies how to understand (i.e. type, content type...), encrypt or decrypt the JWE content.

- an encrypted key which corresponds to the content encryption key used to encrypt the JWE content.
- an initialization vector used when encrypting the JWE content.
- a cipher text which results from the authenticated encryption of the JWE content.
- an authentication tag which ensures the integrity of the cipher text.

A **JWE** is obtained from a **JWEBUILDER** or a **JWEREADER**, the **JWE** interface exposes the header, the encrypted key, the initialization vector, the cipher text, the authentication tag and the payload. It can be serialized using the compact notation as follows:

```
JWE<?> jwe = ...
```

```
// <header>.<encrypted_key>.<initialization_vector>.<cipher_text>.<authentication_tag>
// e.g.
eyJhbGciOiJBMTI4S1ciLCJlbmMiOiJBMTI4Q0JDLUhTMjU2In0.6KB707dM9YTigHtLvtgWQ8mKwboJW3of9locizkDTHzBC2Il
rT1o0Q.AxY8DCtDaGlsbGljb3RoZQ.KDlTtXchhZTGufMYmOYGS4HffxPSUrFmqCHXaI9wOGY.U0m_YmjN04DJvceFICbCVQ
String jweCompact = jwe.toCompact();
```

A **JsonJWE** is obtained from a **JsonJWEBUILDER** or a **JsonJWEREADER**, the **JsonJWE** interface exposes protected and unprotected headers, the initialization vector, the additional authentication data, the cipher text, the authentication tag and the list of recipients. It can be serialized using the JSON notation as follows:



```
JsonJWE<?, ?> jsonJWE = ...
```

```
/*
 * RFC 7516 Appendix A.4
 *
 * {
 *   "protected": "eyJlbmMiOiJBMTI4Q0JDLUhTMjU2In0",
 *   "unprotected": {
 *     "jku": "https://server.example.com/keys.jwks"
 *   },
 *   "recipients": [
 *     {
 *       "header": {
 *         "alg": "RSA1_5",
 *         "kid": "2011-04-29"
 *       },
 *       "encrypted_key": "UGhIOguC7IuEvf_NPVaXsGMOl0mwvc1GyqlIKOK1nN94nHPoltGRhWhw7Zx0-
 *         kFm1NjN8LE9XShH59_i8J0PH5ZZyNfGy2xGdULU7sHNF6Gp2vPLgNZ__deLKx
 *         GHZ7PcHALUzo0egEI-8E66jX2E4zyJKx-YxzZIItrZC5hlRirb6Y5CL_p-ko3
 *         YvkkysZIFNPccxRU7qve1WYPxqbb2Yw8kZqa2rMWI5ng80tvzLV7elprCbuPh
 *         cCdZ6XDP0_F8rkXds2vE4X-nc0IM8hAYHHi29NX0mcKiRaD0-D-ljQTP-cFPg
 *         wCp6X-nZZd90HBv-B3oWh2TbqmScqXMR4gp_A"
 *     },
 *     {
 *       "header": {
 *         "alg": "A128KW",
 *         "kid": "7"
 *       },
 *       "encrypted_key": "6KB707dM9YTIgHtLvtgWQ8mKwboJW3of9locizkDTHzBC2IlrT1o0Q"
 *     }
 *   ],
 *   "iv": "AxY8DctDaGlsbGljb3RoZQ",
 *   "ciphertext": "KDLtTxchhZTGufMYmOYGS4HffxPSUrFmqCHXaI9wOGY",
 *   "tag": "Mz-VPPyU4RlcuYv1IwIvzw"
 * }
 */
```

```
String jweJson = jsonJWE.toJson();
```

The most common representation is by far the compact representation which can be safely used in URLs. On the other hand, the JSON notation can be used to target multiple systems with various JWKS.

A JWE offers integrity and confidentiality of its content using authenticated encryption, it requires two algorithms:

- the algorithm (**alg**) used to encrypt/decrypt, wrap/unwrap or derive a content encryption key (CEK)
- the encryption algorithm used to actually encrypt/decrypt the content using the CEK.

The CEK is either generated or derived when building a JWE and resolved when reading a JWE using a key management algorithm. As a result, building or reading a JWE requires a **JWK** supporting key management algorithms.

## Building JWE

A `JWEBuilder` is used to create `JWE`, it is obtained by invoking one of the `builder()` methods on the `JWEService` bean. The actual payload type can be specified explicitly in the method as well as the `JWK` to use to encrypt, wrap or derive the content encryption key used to encrypt the `JWE`.

The `builder()` method actually accepts a publisher of `JWK` which means multiple keys can be considered when building the JWE. If keys are not specified, they are resolved from the JOSE header parameters using the `JWK service`. When building a JWE, the `JWEBuilder` basically retains the first trusted `JWK` that was able to encrypt the content encryption key. The retained `JWK` is exposed in the resulting `JWEHeader`. It is important to note that untrusted `JWK` are filtered out. A `JOSEObjectBuildException` is thrown if no suitable keys could be found.

A `JWEBuilder` uses media type converters injected in the module to encode the JWE payload based on the content type which can be either specified in the JOSE header (`cty`), or when invoking the `build()` method. An explicit `Function<T, Mono<String>>` encoder can also be specified in order to bypass media type converters.

A specific encoder basically overrides the content type specified in `build()` method which overrides the content type specified in the JOSE header.

The JWE content are encrypted using a generated content encryption key (CEK) or directly using the provided or resolved `JWK` in case of direct encryption (i.e. `alg=dir`). The CEK (if any) is encrypted, wrapped or derived using the provided or resolved `JWK` and included in the resulting JWE with the initialization vector that was generated and used during the authenticated encryption and the resulting authentication tag so that a recipient has all the information required to decrypt the CEK and eventually verify and decrypt the JWE.

The following example shows how to build a `JWE` with a generated `JWK` and a payload serialized as `application/json` using corresponding media type converter:

```

// Injected or obtained from a 'Jose' instance
JWKSService jwkService = ...
JWEService jweService = ...

Mono<? extends OCTJWK> key = jwkService.oct().generator()
    .keyId("keyId")
    .algorithm(OCTAlgorithm.A256GCMKW.getAlgorithm())
    .generate()
    .cache();

JWE<Message> jwe = jweService.builder(Message.class, key)
    .header(header -> header
        .keyId("keyId")
        .algorithm(OCTAlgorithm.A256GCMKW.getAlgorithm())
        .encryptionAlgorithm(OCTAlgorithm.A128CBC_HS256.getAlgorithm())
    )
    .payload(new Message("John", "Hello world!"))
    .build(MediaType.APPLICATION_JSON)
    .block();

//
eyJlbnMiOiJBMTI4Q0JDLUhTMjU2IiwiaWxnIjoia2V5SWQiLCJ0YwciOiJ3b2RkcDJScThPOEdG
WG9PUWZvaTdnIiwiaXYiOiJpYmFfaklzSDRyWUdfcUQtIn0.Barv9ju_JgIBugTD3TtKGA60yqadZ635rkw6rfpeR7s.QH1HhZKh
KWrPzJtfSLRjuQ.gUXtGvVzvwpFh0ZgULZGB2z0dsFjUG0u2Rih_JNsryDIAkpD_LMDDNYTh2ZRgm1.EgQt9XxCfFDRho5mPAXQ
RQ
String jweCompact = jwe.toCompact();

```

Assuming the **JWK** can be resolved by the **JWKSService** using the key id (from module's **JWKStore** or **JWKKeyResolver**), the key can be omitted when creating the builder:

```

// Using an 'InMemoryJWKStore', we can store the key so it can be resolved by key id by the
// 'JWKSService'
key.map(JWK::trust).map(jwkService.store()::set).block();

// Key 'keyId' is then automatically resolved
JWE<Message> jwe = jweService.builder(Message.class)
    ...

```

The JWE JSON representation as defined by [RFC 7516 Section 7.2](#) is a JWE representation that is neither optimized nor URL-safe. This notation can hardly be compared to the compact notation and it shall be used for very different puposes, for instance to communicate encrypted content in JSON using different keys and algorithms to one or more recipients.

A **JsonJWEBuilder** is used to create **JsonJWE** with multiple recipients following the JSON representation specification, it is obtained by invoking one of the **jsonBuilder()** methods on the **JWEService** bean. Since a **JsonJWE** might have multiple recipients with different encrypted content using different keys and algorithms, only the payload type can be specified when creating the builder, keys will be provided or resolved later in the process.

A `JsonJWE` is created from common protected and unprotected headers, one payload and multiple recipients with unprotected headers used to encrypt the JWE using different keys. Unlike unprotected headers, the common protected header is included in the additional authentication data used during the authenticated encryption of the JWE. Common headers and per recipient header must be disjoint and content related parameters such as the type (`typ`) or the content type (`cty`) must be consistent across all recipient headers. A `JWEBuildException` shall be thrown in case of invalid or inconsistent recipient headers. The encryption algorithm parameter (`enc`) must also be consistent across all recipients since the cipher text, the initialization vector, the authentication tag and the content encryption key used to encrypt the JWE are common to all recipients (the JWE is actually encrypted once), it is however encrypted, wrapped or derived per recipient using different keys explicitly provided or automatically resolved for each recipient. In case of a direct encryption or direct key agreement algorithm, the algorithm parameter (`alg`) must also be consistent across all recipients.

In the particular case of a direct encryption, a `JsonJWE` is really not different than a regular JWE since all recipients have then to share the same encryption key.

The following example shows how to build a `JsonJWE` with two recipients using generated keys and a payload encoded as `text/plain` using an explicit encoder:

```

// Injected or obtained from a 'Jose' instance
JWKSService jwkService = ...
JWEService jweService = ...

Mono<? extends RSAJWK> key1 = jwkService.rsa().generator()
    .keyId("key1")
    .algorithm(RSAAlgorithm.RSA1_5.getAlgorithm())
    .generate()
    .cache();

Mono<? extends OCTJWK> key2 = jwkService.oct().generator()
    .keyId("key2")
    .algorithm(OCTAlgorithm.A128KW.getAlgorithm())
    .generate()
    .cache();

JsonJWE<Message, BuiltRecipient<Message>> jsonJWE = jweService.jsonBuilder(Message.class)
    .headers(
        protectedHeader -> protectedHeader
            .encryptionAlgorithm(OCTAlgorithm.A128CBC_HS256.getAlgorithm()),
        unprotectedHeader -> {}
    )
    .payload(new Message("Alice", "Hi John!"))
    .recipient(
        header -> header
            .keyId("key1")
            .algorithm(RSAAlgorithm.RSA1_5.getAlgorithm()),
        key1
    )
    .recipient(
        header -> header
            .keyId("key2")
            .algorithm(OCTAlgorithm.A128KW.getAlgorithm()),
        key2
    )
    .build(message -> Mono.just(message.getAuthor() + " > " + message.getMessage()))
    .block();

/*
 * {
 *   "unprotected": {
 *   },
 *   "ciphertext": "n8hpXBhxZ9brlm465Ipey9kpCHy0xDfR-qNzRh32KQM",
 *   "recipients": [
 *     {
 *       "header": {
 *         "alg": "RSA1_5",
 *         "kid": "key1"
 *       },
 *       "encrypted_key": "ItwxvAJqMh_kGeJ9jmHPm1NJ1Kod-TmAwsM5IbZDy54uB6U1eGQZKQzzLTMGMM
 *         UUf6G96kT35Vv__L2fr6k8INlG0i3ae5YDnRmVwOpD74pffQn3FFcoxx68_xSu
 *         DWDHMRbyEqHFur-DZy20-yb00dna7qg7kmAz0wv9VS0HpFRwj8wB4w7g4zg4jI
 *         5IztiTX587fCtw7YuiBYnNEUzCrddUoBAAPHWHiilez25lv0dhjvyyMNAT-j_5
 *         8FDIQGgqUY0uLE48-gKF2alnRikjk_9H9Cg_99mBEyls5EAnRq3aGiJz7wPJR3
 *         1Qt154c8IUDLtqNXKaB8qsk5taYV5hlQ"
 *     },
 *     {
 *       "header": {
 *         "alg": "A128KW",
 *         "kid": "key2"
 *       }
 *     }
 *   ]
 * }
 */

```

```

*         },
*         "encrypted_key": "srvZC3EPaEYkfHkTp21-mzBHA17gjuof6-NTWdg7unHsPK1rnp1eFQ"
*     }
* },
* "iv": "bBb7jcsxoRcPpKahEPCvwA",
* "tag": "u7dD-MwLkfA4SfuRjvVmdQ",
* "protected": "eyJlbmMiOiJBMTI4Q0JDLUhTMjU2In0"
* }
*/
String jweJson = jsonJWE.toJson();

```

In above code, we can see that the cipher text is common to all recipients which explains why content related parameters and the encryption algorithm must be consistent across all recipients and to make this clear the encryption algorithm was specified in the common protected header, encoded in Base64. Unprotected headers in each recipient then specify the key id and the algorithm to use to resolve the content encryption key in order to decrypt the JWE.

The `JsonJWE` interface exposes the common protected and unprotected headers, the cipher text, the initialization vector, the additional authentication data and the authentication tag as well as the `JWE` instances corresponding to each recipient.

```

List<JWE<Message>> jweRecipients = jsonJWE.getRecipients().stream()
    .map(recipient -> recipient.getJWE())
    .collect(Collectors.toList());

```

Note that the `JWE` instances thus obtained are deduced from the JSON representation which makes a difference between protected and unprotected headers, as a result the actual header used in the additional authentication data corresponds to the protected header but the `JWEHeader` exposed in the `JWE` results from the merge of the common protected and unprotected headers and the recipient unprotected header.

## Reading JWE

A `JWEReader` is used to read JWE compact representations, it is obtained by invoking one of the `reader()` methods on the `JWEService` bean. The expected payload type must be specified explicitly in the method and the `JWK` to use to decrypt, unwrap or derive the content encryption key, actually used to decrypt the `JWE`, can be specified as well.

As for the `JWEBuilders`, a `JWEReader` can consider multiple keys to decrypt, unwrap or derive the content encryption key used to encrypt the JWE. If keys are not specified, they are resolved from the JOSE header parameters using the [JWK service](#). When reading a `JWE`, the `JWEReader` basically uses provided or resolved trusted `JWK` in sequence to resolve the content encryption key and stops when the CEK could be resolved. As for the `JWEBuilders`, untrusted `JWK` are filtered out and a `JOSEObjectReadException` is thrown if no suitable keys could be found. A `JWEReadException` with aggregated errors (`getSuppressed()`) is thrown when reading an invalid JWE.

A **JWReader** also uses media type converters injected in the module to decode the JWE payload based on the JWE content type defined in the JOSE header (**cty**) or explicitly specified when invoking the **read()** method. An explicit **Function<String, Mono<T>>** decoder can also be specified in order to bypass media type converters.

A specific decoder basically overrides the content type specified in **read()** method which overrides the content type in the JOSE header.

The following example shows how to read a JWE compact representation by decoding the **application/json** payload as specified in the JOSE header using the corresponding media type converter:

```
// Injected or obtained from a 'Jose' instance
JWKService jwkService = ...
JWEService jweService = ...

Mono<? extends OCTJWK> key = jwkService.oct().builder()
    .keyId("keyId")
    .algorithm(OCTAlgorithm.A256GCMKW.getAlgorithm())
    .keyValue("GkilETj3L4jpinuRiaNq6zd7-_1JPbfU9DY3xHl9HEE")
    .build()
    .cache();

String jweCompact =
"eyJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiaWxnIjoia2V5SWQiLCJhdHkiOiJhcHBsawNhdGlvbi9qc29uIiwidGFnIjoiaWUtlc2VBelZoenh5Vk9pRVNvVEdoQSIslmI2IjoieEJFSTlYeHBDVTZwcVVSaCJ9."
+ "MNYqpQCQPrUSZTwP-C7kUCG0FqFGGciUU2qW54jc3NM."
+ "_nfKSroUwjzJcPETt-ow."
+ "1dL8rLmhKF7hqVNzQf5owPOSZN7Z_V46w0UvIBDuFjh5pqvhbs4ltrTsk6E_NF-y."
+ "RJ8Q0GLuT2fz5VrzG1EHbg";

JWE<Message> jwe = jweService.reader(Message.class, key)
    .read(jweCompact)
    .block();

// Bill says Hey!
Message message = jwe.getPayload();
```

Assuming the **JWK** can be resolved by the **JWKService** using the key id (from module's **JWKStore** or **JWKKeyResolver**), the key can be omitted when creating the reader:

```
// Using an 'InMemoryJWKStore', we can store the key so it can be resolved by key id by the
'JWKService'
key.map(JWK::trust).map(jwkService.store()::set).block();

// Key 'keyId' is then automatically resolved
JWE<Message> jwe = jweService.reader(Message.class)
    ...
```

A `JsonJWEReader` is used to read JWE JSON representations as defined by [RFC 7516 Section 7.2](#), it is obtained by invoking one of the `jsonReader()` methods on the `JWEService` bean. Since a `JsonJWE` might have multiple recipients using different keys and algorithms, only the payload type must be specified when creating the reader. A `JsonJWE` is basically read without decrypting the JWE content which must be decrypted for each recipient individually, keys can then be specified explicitly or automatically resolved. A `JsonJWE` can be considered valid if the content could be verified and decrypted for at least one recipient.

The `JsonJWE` instance returned by a `JsonJWEReader` actually differs from the one returned by a `JsonJWEBuilder`, a built `JsonJWE` exposes `JsonJWE.BuiltRecipient` which exposes a valid `JWE` whereas a read `JsonJWE` exposes `JsonJWE.ReadRecipient` which exposes `readJWE()` methods to actually verify and decrypt the JWE content and return the corresponding `JWE`.

The following example shows how to read and decrypt a JWE JSON representation with two recipients, the payload being decoded using an explicit decoder:



```

// Injected or obtained from a 'Jose' instance
JWKSService jwkService = ...
JWEService jweService = ...

Mono<? extends OCTJWK> key2 = jwkService.oct().builder()
    .keyValue("GawgggFyGrWKav7AX4VKUg")
    .build()
    .cache();

String jweJson = "{"
    + "  \"unprotected\": {"
    + "    },"
    + "  \"ciphertext\": \"2jtWSZdL-TJGyktUwldH4sphYuz2VbseUS9eL_vh_tU\", "
    + "  \"recipients\": ["
    + "    {"
    + "      \"header\": {"
    + "        \"alg\": \"RSA1_5\", "
    + "        \"kid\": \"key1\""
    + "      }, "
    + "      \"encrypted_key\": \"kIHuM-OZU1wvmb6ocdDsn1ljF11kIbfvv9y7XpTPGfdYez2AhJvpHfPZ6LKK5-
yDfHAVWTXz_RbgjPATURNKy0hdogfWBWxEpQE8WaBafI8kSk0GzhJrR2tcXhrxs0xwPMthjfZ38zNql1oZuL9pzUZ3PicNhcCX
D2XN52kw7VGMvPus8r89orY4q2l_xA65wkxHtG3JDG9Je_CidYuX_PXHqMkrbszsUPbyCspPIRTP5yWMeFmMp8KiEnyGaQITt0vZ
uea4u3tWuhX0wa2AN74quesArMhx81NwxaMnuDNrF6eQFIQw4QJ41MqVchHRAoXYKQvB8DYce9fHhPQ\""
    + "    }, "
    + "    {"
    + "      \"header\": {"
    + "        \"alg\": \"A128KW\", "
    + "        \"kid\": \"key2\""
    + "      }, "
    + "      \"encrypted_key\": \"OSMIf3Elx-NmfzP1Y_aZbae6k6yU2rl7o2uHd7v3lHgS4UjJURVYTQ\""
    + "    }"
    + "  ], "
    + "  \"iv\": \"vrCX8Yr9o0s--KiBtkQ6kw\", "
    + "  \"tag\": \"gHpLPXRRDjUNJ1HDivaSTg\", "
    + "  \"protected\": \"eyJlbmMiOiJBMTI4Q0JDLUhTMjU2In0\""
    + "}";

JsonJWE<Message, ReadRecipient<Message>> readJsonJWE = jweService.jsonReader(Message.class)
    .read(jweJson, payload -> {
        Mono.fromSupplier(() -> {
            int separatorIndex = payload.indexOf(">");
            return new Message(payload.substring(0, separatorIndex - 1),
payload.substring(separatorIndex + 2));
        })
    })
    .block();

// Return as soon as one of the recipients could have been verified and decrypted with key2
JWE<Message> decryptedJWE = Flux.fromIterable(readJsonJWE.getRecipients())
    .flatMap(recipient -> recipient.readJWE(key2).onErrorResume(e -> Mono.empty()))
    .blockFirst();

if(decryptedJWE != null) {
    // Linda says Shall we begin?
    Message message = decryptedJWE.getPayload();
}

```

In above code, the decrypted **JWE** should correspond to the second recipient since we used **key2** to resolve the content encryption key.

As defined by [RFC 7516](#), custom parameters listed in the critical header parameter (**crit**) and present in the JOSE header must be fully understood by the application for the JWE to be valid. The parameters actually processed by an application and therefore understood can be specified on the **JWEReader** which throws a **JOSEObjectReadException** when encountering unknown critical parameters.

In the following example, the **JWEReader** is setup to understand custom parameter [http://example.com/application\\_parameter](http://example.com/application_parameter) which allows it to read the specified JWE:

```
Mono<? extends OCTJWK> key = jwkService.oct().builder()
    .keyId("keyId")
    .algorithm(OCTAlgorithm.A256GCMKW.getAlgorithm())
    .keyValue("GkilETj3L4jpinuRiaNq6zd7-_1JPbfU9DY3xHl9HEE")
    .build()
    .cache();

/*
 * {
 *   "header": {
 *     "enc": "A128CBC-HS256",
 *     "alg": "A256GCMKW",
 *     "kid": "keyId",
 *     "crit": [
 *       "http://example.com/application_parameter"
 *     ],
 *     "http://example.com/application_parameter": true,
 *     "tag": "pq10ChvU6GZcMDLZqTEo0Q",
 *     "iv": "VcuwU871tvGMGOHB"
 *   },
 *   "payload": "Lorem ipsum",
 *   "initializationVector": "i1GTQ9xy0L89vza7hNCiAQ",
 *   "authenticationTag": "5EiKTUS272wTHd978Q0uHQ",
 *   "encryptedKey": "Aq7Nwm_h4LmGjJynbUY00709juKlUMFWXS_HMpAAR1g",
 *   "cipherText": "mDeuwt3Q0199_h6diPwu_w"
 * }
 */
String jweCompact =
"eyJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiaWxnIjoiaQTI1NkdDTUtXIiwia2lkIjoia2V5SWQiLCJjcml0IjpbImh0dHA6Ly9leGFiG6FtcGx1LmNvbS9hcHBsaWNhdGlvb19wYXJhbWV0ZXIiXSwiaHR0cDovL2V4YW1wbGUuY29tL2FwcGxpY2F0aW9uX3BhbmFtZXRLciI6dHJ1ZSwidGFuIjoicHEXt0NodLU2R1pjTURMwnFURW8wUSIsImI2IjoiaWVmn1d1U4NzF0dkdNR09IQiJ9."
+ "Aq7Nwm_h4LmGjJynbUY00709juKlUMFWXS_HMpAAR1g."
+ "i1GTQ9xy0L89vza7hNCiAQ."
+ "mDeuwt3Q0199_h6diPwu_w."
+ "5EiKTUS272wTHd978Q0uHQ";

JWE<String> jwe = jweService.reader(String.class, key)
    .processedParameters("http://example.com/application_parameter")
    .read(jweCompact, MediaType.TEXT_PLAIN)
    .block();
```

## JWT Service

The JWT service is used to build or read JWT represented using a URL-safe compact notation as defined by [RFC 7519](#). A JSON Web Token is a particular type of JWS or JWE that is used to securely transfer claims between two parties.

In practice, a JWT is created or read just like a **JWS** or a **JWE** with type **JWT** and a JSON payload of type **JWTClaimsSet** representing a set of claims.

The **JWTService** bean is used to create specific **JWSBuilder** or **JWEBUILDER** instances for building JWT as **JWS** or **JWE** and specific **JWSReader** or **JWEReader** instances for reading **JWS** and **JWE** with **JWTClaimsSet** payloads serialized using the compact notation.

## JWT claims set

A JWT claims set represents a JSON object whose members are the claims conveyed by the JWT as defined by [RFC 7519](#) which also specifies registered claim names. For instance, the issuer (**iss**) claim identifies the principal that issued the JWT, the expiration time claim (**exp**) identifies the expiration time on or after which the JWT must not be accepted for processing... A JWT is therefore validated by first verifying or decrypting the enclosing JWS or JWE and then by validating the JWT claims set, a JWT must be rejected if for instance the expiration time has passed.

The **JWTClaimsSet** interface is used to represent the JWT payload in a JWS or a JWE, it exposes the registered claims and allows to specify custom claims.

The following example shows how to create a **JWTClaimsSet** with an issuer and a custom claim and which expires in a day:

```
JWTClaimsSet jwtClaimsSet = JWTClaimsSet.of("joe", ZonedDateTime.now().plusDays(1).toEpochSecond())
    .addCustomClaim("http://example.com/is_root", true)
    .build();
```

A **JWTClaimsSet** can be validated in multiple ways:

```
if(jwtClaimsSet.isValid()) {

}

// Run an action only if the JWT claims set is valid
jwtClaimsSet.isValid(() -> {
    ...
});

// Run an action the JWT claims set is valid and another action if it is not
jwtClaimsSet.isValidOrElse(
    () -> {
        // Valid
        ...
    },
    () -> {
        // Invalid
        ...
    }
);

// Throws an InvalidJWTException if the JWT claims set is invalid
jwtClaimsSet.invalidateThrow();

// Throws the provided exception if the JWT claims set is invalid
jwtClaimsSet.invalidateThrow(() -> new CustomException("Invalid credentials"));
```

A `JWTClaimsSet` validates expiration time and not before claims by default, additional `JWTClaimsSetValidator` can be added as well by invoking `validate()` or `setValidators()` methods.

In the following example, a validator is added to check that the issuer is `iss`, an `InvalidJWTException` is thrown if the issuer claim does not match:

```
jwtClaimsSet.validate(JWTClaimsSetValidator.issuer("iss"));

// Throws an InvalidJWTException since issuer 'joe' does not match the expected 'iss'
jwtClaimsSet.ifInvalidThrow();
```

It is then possible to provide custom validation logic using multiple `JWTClaimsSetValidator`, but the `JWTClaimsSet` interface can also be itself extended to better reflect application specificities by exposing application specific claims or specific validation logic.

## Building JWT

The `JWTService` bean exposes `jwsBuilder()` and `jweBuilder()` methods used to obtain specific `JWSBuilder` or `JWEBBuilder` for creating JWT as `JWS` or `JWE` with `JWTClaimsSet` payloads. The builders thus obtained follow the exact same rules as defined by the [JWS service](#) and the [JWE service](#) with the following exceptions: the type (`typ`) and the content type (`cty`) are always considered to be `JWT` and `application/json` since the JWT claims set is defined as a JSON object. A `JWTBuildException` is thrown when a type other than `JWT` (the type can be omitted) or a content type (no content type is allowed) are specified in the JOSE header.

The following example shows how to create a JWT as a `JWS` using a generated key:

```

// Injected or obtained from a 'Jose' instance
JWKSService jwkService = ...
JWTService jwtService = ...

Mono<? extends OCTJWK> key = jwkService.oct().generator()
    .generate()
    .cache();

/*
 * {
 *   "iss": "joe",
 *   "exp": 1691133731,
 *   "http://example.com/is_root": true
 * }
 */
JWTClaimsSet claims = JWTClaimsSet.of("joe", ZonedDateTime.now().plusYears(1).toEpochSecond())
    .addCustomClaim("http://example.com/is_root", true)
    .build();

JWS<JWTClaimsSet> jwt = jwtService.jwsBuilder(key)
    .header(header -> header
        .algorithm(OCTAlgorithm.HS256.getAlgorithm())
        .type("JWT")
    )
    .payload(claims)
    .build()
    .block();

//
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJqb2UiLCJleHAiOiJlE20TEzMzNzQsImh0dHA6Ly9leGFtcGxlLnNvbS9pc19yb290Ijp0cnVlfQ.4fEhUpbK4aNhgZB0XL_UiJV9k5pLw35MT1zIjq4oCro
String jwtCompact = jwt.toCompact();

```

The following example shows how to create a JWT as a **JWE** using a generated key:

```
// Injected or obtained from a 'Jose' instance
JWKSService jwkService = ...
JWTService jwtService = ...

Mono<? extends ECJWK> key = jwkService.ec().generator()
    .keyId("keyId")
    .algorithm(ECAAlgorithm.ECDH_ES.getAlgorithm())
    .curve(ECCurve.P_256.getCurve())
    .generate()
    .cache();

/*
 * {
 *   "iss": "joe",
 *   "exp": 1691133731,
 *   "http://example.com/is_root": true
 * }
 */
JWTClaimsSet claims = JWTClaimsSet.of("joe", ZonedDateTime.now().plusYears(1).toEpochSecond())
    .addCustomClaim("http://example.com/is_root", true)
    .build();

JWE<JWTClaimsSet> jwte = jwtService.jweBuilder(key)
    .header(header -> header
        .algorithm(ECAAlgorithm.ECDH_ES.getAlgorithm())
        .encryptionAlgorithm(OCTAlgorithm.A256GCM.getAlgorithm())
        .type("JWT")
    )
    .payload(claims)
    .build()
    .block();

//
eyJlbmMiOiJBbmJ0R0NNIiwidHlwIjoiSldUIiwiaWwiOiJYXnIjoiR0NESC1FUyIsImVwayI6eyJjcnyYiOiJQLTI1NiIsIngia0iIxdVc4
VlAxVzhDazZ6dERIMWRjYnk3NzRfVXU4X1RvalNKZEJSMVpRaFRNIiwieSI6InBGRG1KZDJXTS1jZGcxVHdMR0FkalduSURrRW1x
c2lmMWJfV0tKMWRWSnciLCJrdHkiOiJFQyJ9fQ..zhYytTdGNvPajvU.j-
Edyx9DpIdHGrCYiH20cjLkORhw95bXBJSEQPVjDe7wRfYFUVfch43X4HI3fKYSxIWgjIACM3ynqQwu7Ta3cQ.3PDS0t-
SdNyCEqYRD8P0hA
String jwteCompact = jwte.toCompact();
```

By default, the JWT service creates **JWSBuilder** and **JWEBuilder** for building JWT with **JWTClaimsSet** payload type, in order to obtain builders for custom **JWTClaimsSet** types, the type must be explicitly specified when creating the builder.

## Reading JWT

The **JWTService** bean exposes **jwsReader()** and **jweReader()** methods used to obtain specific **JWSReader** or **JWEReader** for reading JWT as **JWS** or **JWE** with **JWTClaimsSet** payloads. The builders thus obtained follow the exact same rules as defined by the [JWS service](#) and the [JWE service](#) with the following exceptions: the type (**typ**) must be **JWT** and no content type (**cty**) is allowed. A **JWTReadException** is thrown when a type other than **JWT** or a content type are specified in the JOSE header.

The following example shows how to read a JWT as a **JWS**:

```
// Injected or obtained from a 'Jose' instance
JWKService jwkService = ...
JWTService jwtService = ...

Mono<? extends OCTJWK> key = jwkService.oct().builder()
    .keyId("keyId")
    .algorithm(OCTAlgorithm.HS256.getAlgorithm())
    .keyValue("xqf1haCsSJGuueZivcq4YaafdWw6n5CH2BTT6vDwUSaM")
    .build()
    .cache();

String jwtCompact = "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9."
    + "eyJpc3MiOiJqb2UiLCJleHAiOjE2OTExMzMzMjE0MDA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijpb0cnVlQ."
    + "4p0_3W8DBRjTPw2e2KI1__v-6QOT_5dWIMKbfsSvTo0";

JWTClaimsSet validClaims = jwtService.jwsReader(key)
    .read(jwtCompact)
    .map(JWS::getPayload)
    .filter(JWTClaimsSet::isValid)
    .block();
```

The following example shows how to read a JWT as a **JWE**:

```
// Injected or obtained from a 'Jose' instance
JWKService jwkService = ...
JWTService jwtService = ...

Mono<? extends ECJWK> key = jwkService.ec().builder()
    .keyId("keyId")
    .algorithm(ECAAlgorithm.ECDH_ES.getAlgorithm())
    .curve(ECCurve.P_256.getCurve())
    .xCoordinate("a9HrKi7kwXR0EumziK_B5ZRlsk7QbXGPJfx_c30GoZs")
    .yCoordinate("fixJ3kr2abu0huetFyhs00Mqd3_M6xMIKE8hr3FggOM")
    .eccPrivateKey("VCSeZseVoZ1E4TyWmRqD0nt5I_ipSbkfXCRHQSTPqUw")
    .build()
    .cache();

// The encrypted key is empty since ECDH_ES is a direct key agreement
jwteCompact =
"eyJlbmMiOiJBMjU2R0NNIiwidHlwIjoiSldUIiwiaWxnIjoiRUNESCI1FUYiImVwayI6eyJjcnYiOiJQLTI1NiIsIngiOiJ6bEc"
zQzVwUetZVG4yVhpiZlZJYm5K0TZTai0yNDJG6TlwVVRmUWN0M0UzIiwieSI6IkUyeE9hNnNlb0dJVHpkRHdxVjZlT2Nlc2dzNmI"
2M082NlJWVXlsV2N6LTgiLCJrdHkiOiJFQyJ9fQ."
    + "."
    + "_1eQRi8ukFZDwa27."
    + "WjPLHYGHu1zpg3QSbhB9ciraoRU7UXpeJJXz76UZAkWJ-rxEXwkimnflTnEymG_oK1i7hKwCANRhgWwr22GqNg."
    + "Zos43NFBxdh_br01ae-7vA";

JWTClaimsSet validClaims = jwtService.jweReader(key)
    .read(jwteCompact)
    .map(JWE::getPayload)
    .filter(JWTClaimsSet::isValid)
    .block();
```

By default, the JWT service creates **JWSReader** and **JWEReader** for reading JWT with **JWTClaimsSet** payload type, in order to obtain readers for custom **JWTClaimsSet** types, the type must be explicitly specified when creating the reader.

## JOSE Media Type Converters

The module also exposes a set of `MediaTypeConverter<String>` for converting JOSE media types as defined by [RFC 7515 Section 9.2](#), [RFC 7517 Section 8.5](#) and [RFC 7519 Section 10.3](#). It currently supports: `application/jose`, `application/jose+json`, `application/jwk+json`, `application/jwk-set+json` and `application/jwt`.

JOSE media type converters are basically used to convert JWK, JWS, JWE or JWT serialized using the compact or the JSON notation. They rely on the module's services to decode an input into corresponding JOSE object (`JWK`, `JWS`, `JWE` or `JWT`), as a result a JWS or a JWE are verified and decrypted by the converters which throw `ConverterException` in case of invalid inputs. In the specific case of a JWT, the validation of the decoded `JWTClaimsSet` is not performed and left to the application.

These media types converters are also used by module services when converting JOSE payloads. It is then possible to wrap any JOSE object in a `JWS` or a `JWE` using compact or JSON serialization. A typical use cases consist in wrapping a `JWK` or a `JWKSet` in a `JWE` to securely communicate keys.

The following example shows how to create a `JWE` conveying multiple `JWK`:



```
// Injected or obtained from a 'Jose' instance
JWKService jwkService = ...
JWEService jweService = ...

OCTJWK key1 = jwkService.oct().builder()
    .keyId("key1")
    .algorithm(OCTAlgorithm.A256GCMKW.getAlgorithm())
    .keyValue("GkilETj3L4jpinuRiaNq6zd7-_1JPbfU9DY3xHl9HEE")
    .build()
    .block();

OCTJWK key2 = jwkService.oct().builder()
    .keyId("key2")
    .algorithm(OCTAlgorithm.HS256.getAlgorithm())
    .keyValue("xqf1haCsSJGuueZivcq4YafdWw6n5CH2BTT6vDwUSaM")
    .build()
    .block();

JWKSet jwkSet = new JWKSet(key1, key2);

Mono<? extends ECJWK> key = jwkService.ec().builder()
    .keyId("keyId")
    .algorithm(ECAAlgorithm.ECDH_ES.getAlgorithm())
    .curve(ECCurve.P_256.getCurve())
    .xCoordinate("a9HRKi7kwXR0EumziK_B5ZRlsk7QbXGPJfx_c30GoZs")
    .yCoordinate("fixJ3kr2abu0huetFyhS00Mqd3_M6xMIKE8hr3FGgOM")
    .eccPrivateKey("VCSeZseVoZ1E4TyWmRqD0nt5I_ipSbKfXCxRHQPQuw")
    .build()
    .cache();

JWE<JWKSet> jwe = jweService.builder(JWKSet.class, key)
    .header(header -> header
        .algorithm(ECAAlgorithm.ECDH_ES.getAlgorithm())
        .encryptionAlgorithm(OCTAlgorithm.A128GCM.getAlgorithm())
        .contentType(MediaType.APPLICATION_JWK_SET_JSON)
    )
    .payload(jwkSet)
    .build()
    .block();

//
eyJlbmMiOiJBMTI4R0NNIiwiaXNjaXBPbmGljYXRpb24vandrlXNldCtqc29uI
cnYiOiJQLTI1NiIsIngia0iJPCw5Nb3BKcDNQcGZ6VlFCQW1ZanU2MVewWUNKUHJuM
S1QzX2QzaGQ2VVNRSm1zSjV5blBtaDN5QmRkZVdHbEs5ZDgiLCJrdHkiOiJFYyJ9f
epA4DaoWAD84EyYqFnaFv2HtQJlNF33jwSIuxHaMG0nK1Cm6yKcdzzC4e1pG1FNY7
aaEx7j0t5nbGNrvzBZJddDWQbhLZomXL7cKzLfypv8Y4SWPzcua6FJMSh7DoZWUZ
y2QS1tu5R4hY5E9EW5QIWC06IErtldHF_y_oZIy7iSxf55GjgBVsoRoFKA.OujlTS
String jweCompact = jwe.toCompact();
```

The resulting compact JWE containing encrypted keys can then be conveyed to a recipient which can decrypt the keys with the shared secret key.

```
// Injected or obtained from a 'Jose' instance
JWEService jweService = ...

jweCompact =
"eyJlbmMiOiJBMTI4R0NNIiwia3R5IjoiaXBwbGljYXRpb24vandrLXNldCtqc29uIiwiaWxnIjoiaRUNCSC1FUyIsImVwayI6eyJ
jcnYiOiJQLTI1NiIsIngjOiJPcw5NbJBKcDNQcGZ6VlFCQW1ZanU2MVEwWUNkUHJuMkI3ew5ZdlRLN3FJIiwieSI6ImhZXzI2am9
tS1QzX2QzaGQ2VVNRSm1zSjV5blBtaDN5QmRkZVdHbEs5ZDgiLCJrdHkiOiJFQyJ9fQ."
+ "."
+ "Xvp00GyH44d8Gwc."
+ "5aV-
epA4DaowAD84EyYqFnaFv2HtQJlNF33jwSIuxHaMG0nK1Cm6yKcdzzC4e1pG1FNY7wg9SI_JlkFDYqjp6EuMe64vFU0iPCj28QtP
aafEx7j0t5nbGNRvzBZJdDWQbhlZomXL7cKzLjfYpv8Y4SWPzcua6FJMSH7DoZwUZfKZDzDk_-2fpXvE_LLw7rTbi8Vltm9AClzm
y2QS1tu5R4hY5E9Ew5QIWC06IErtldHF_y_oZIy7iSxf55GjgBVs0roFkA."
+ "0ujlTScT9q0M6wWsFJMULa";

jwkSet = jweService.reader(JWKSet.class, key)
    .read(jweCompact)
    .map(JWE::getPayload)
    .block();
```

The following example shows how to wrap a received **JWS** in a **JWE** in order to add confidentiality protection:



```
// Injected or obtained from a 'Jose' instance
JWSService jwsService = null;
JWEService jweService = null;

jweCompact =
"eyJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiTl1kdTUtXlIiwia2lkIjoiaWV3R5IjoiaXBwGljYXRpb24vam9zZSIsInRhZyI6IlBjT2tjZWNSNUSwaW92a2hnMEhwUEEiLCJpdjI6InFNMUtteHhIcmZocXFuRmIifQ."
+ "LLn2scpDiAdRRSFirvTXTXsVwQp9mSH4dPv1I-IruFM."
+ "LfCNkDe5r3eE2Kjadmpkww."
+ "5AjCbDExRhRsLy-
iXX2RAavfXVWFECinKxU3t_B0bnC4mzgXmaqvfWUC8QM8K3gjt36Qa89nqajVYmJwRrZ0ZMoH68JgXvp2npIEdJSrL3CqT
Hm30bK5-7TbYLP1K3t9v995w0IAajUsXaHfpNODqAsFlc83A6wwxv37WVq4mWy-
WZ7ZwIpwHY5semqMxv0FbpNMPtkLaG0JzqYLnzH7yaT2DSBQKIXlCZ0hc."
+ "ZML3thQjah7dtXdv17LJXA";

/// Here we assume keys 'jwsKey' and 'jweKey' can be resolved by the 'JWSService' and the
'JWEService'

// Marcel says Finally!
Message message = jweService.
<JWS<Message>>reader(Types.type(JWS.class).type(Message.class).and().build())
    .read(jweCompact)
    .map(JWE::getPayload)
    .map(JWS::getPayload)
    .block();
```

# 6

## Inverno Maven Plugin

---

The Inverno Maven Plugin is used to run, package and distribute modular applications and Inverno applications in particular. It relies on a set of Java tools to build native runtime or application images as well as Docker or OCI images for modular Java projects.

### Usage

The Inverno Maven plugin can be used to run a modular application project or build an image for a modular project. There are three types of images that can be build using the plugin:

- **runtime image** is a custom Java runtime containing a set of modules and their dependencies.
- **application image** is a native self-contained Java application including all the necessary dependencies to run the application without the need of a Java runtime.
- **container image** is a Docker or CLI container image that can be packaged as a TAR archive or directly deployed on a Docker daemon or container registry.

### Run a module application project

The `inverno:run` goal is used to execute the modular application defined in the project from the command line.

```
$ mvn inverno:run
```

The application is first *modularized* which means that any non-modular dependency is modularized by generating an appropriate module descriptor using the `jdeps` tool in order for the application to be run with a module path and not a class path (and certainly not both).

The application is executed in a forked process, application arguments can be passed on the command line:

```
$ mvn inverno:run -Dinverno.run.arguments='--some.configuration=\"hello\"'
```

Actual arguments are determined by splitting the parameter value around spaces. There are several options to declare an argument which contains spaces:

- it can be escaped: `Hello\ World`
- it can be quoted: `"Hello World"` or `'Hello World'`

Since quotes or double quotes are used as delimiters, they might need to be escaped as well to declare an argument that contains some: `I\'m\ happy`, `"I'm happy"`, `'I\'m happy'`.

In order to debug the application, we need to specify the appropriate options to the JVM:

```
$ mvn inverno:run -Dinverno.exec.vmOptions="-Xdebug -Xrunjdp:transport=dt_socket,server=y,suspend=y,address=8000"
```

By default the plugin will detect the main class of the application, but it is also possible to specify it explicitly in case multiple main classes exist in the project module.

```
$ mvn inverno:run -Dinverno.exec.mainClass=io.inverno.example.Main
```

A pidfile is created when the application is started under `${project.build.directory}/maven-inverno` directory, it indicates the pid of the process running the application. If the build exits while the application is still running or if the pidfile was not properly removed after the application has exited, it might be necessary to manually kill the process and/or remove the pidfile.

## Start and stop the application for integration testing

The `inverno:start` and `inverno:stop` goals are used together to start and stop the application while not blocking the Maven build process which can then execute other goals targeting the running application such as integration tests.

They are bound to the `pre-integration-test` and `pre-integration-test` phases respectively:

```

<project>
  <build>
    <plugins>
      <plugin>
        <groupId>io.inverno.tool</groupId>
        <artifactId>inverno-maven-plugin</artifactId>
        <executions>
          <execution>
            <id>start</id>
            <phase>pre-integration-test</phase>
            <goals>
              <goal>start</goal>
            </goals>
          </execution>
          <execution>
            <id>stop</id>
            <phase>post-integration-test</phase>
            <goals>
              <goal>stop</goal>
            </goals>
          </execution>
        </executions>
      </plugin>
    </plugins>
  </build>
</project>

```

## Build a runtime image

A runtime image is a custom Java runtime distribution containing specific modules and their dependencies. Such image is used as a base for generating application image but it can also be distributed as a lightweight Java runtime.

The `inverno:build-runtime` goal uses `jlink` tool to assemble the project module and its dependencies.

```

<project>
  <build>
    <plugins>
      <plugin>
        <groupId>io.inverno.tool</groupId>
        <artifactId>inverno-maven-plugin</artifactId>
        <executions>
          <execution>
            <id>build-project-runtime</id>
            <phase>package</phase>
            <goals>
              <goal>build-runtime</goal>
            </goals>
            <configuration>
              <vm>server</vm>
              <addModules>jdk.jdwp.agent,jdk.crypto.ec</addModules>
              <vmOptions>-Xms2G -Xmx2G -XX:+UseNUMA -XX:+UseParallelGC</vmOptions>
              <formats>
                <format>zip</format>
                <format>tar.gz</format>
                <format>tar.bz2</format>
              </formats>
            </configuration>
          </execution>
        </executions>
      </plugin>
    </plugins>
  </build>
</project>

```

By default, the project module and its dependencies are included in the resulting image, this include JDK's modules such as `java.base`, in the previous example we've also explicitly added the `jdk.jdwp.agent` to support remote debugging and `jdk.crypto.ec` to support TLS communications.

The resulting image is packaged to the formats defined in the configuration and attached, by default, to the Maven project.

## Build an application image

An application image is built using the `inverno:build-app` goal which basically generates a runtime image and uses `jpakege` tool to generate a native platform-specific application package.



```

<project>
  <build>
    <plugins>
      <plugin>
        <groupId>io.inverno.tool</groupId>
        <artifactId>inverno-maven-plugin</artifactId>
        <executions>
          <execution>
            <id>build-application</id>
            <phase>package</phase>
            <goals>
              <goal>build-app</goal>
            </goals>
            <configuration>
              <vm>server</vm>
              <addModules>jdk.jdwp.agent,jdk.crypto.ec</addModules>
              <launchers>
                <launcher>
                  <name>app</name>
                  <vmOptions>-Xms2G -Xmx2G -XX:+UseNUMA -
XX:+UseParallelGC</vmOptions>
                </launcher>
              </launchers>
              <formats>
                <format>zip</format>
                <format>deb</format>
              </formats>
            </configuration>
          </execution>
        </executions>
      </plugin>
    </plugins>
  </build>
</project>

```

The `inverno:build-app` goal is very similar to the `inverno:build-runtime` goal except that the resulting image provides an application launcher and it can be packaged in a platform-specific format. For instance, we can generate a `.deb` on a Linux platform or a `.exe` or `.msi` on a Windows platform or a `.dmg` on a MacOS platform. The resulting package can be installed on these platforms in a standard way.

This goal uses `jpackage` tool which is an incubating feature in JDK<16, if you intend to build an application image with an old JDK, you'll need to explicitly add the `jdk.incubator.jpackage` module in `MAVEN_OPTS`:

```
$ export MAVEN_OPTS="--add-modules jdk.incubator.jpackage"
```

## Build a container image tarball

A container image can be built in a TAR archive using the `inverno:build-image-tar` goal which basically build an application package and package it in a container image.

```

<project>
  <build>
    <plugins>
      <plugin>
        <groupId>io.inverno.tool</groupId>
        <artifactId>inverno-maven-plugin</artifactId>
        <executions>
          <execution>
            <id>build-image-tar</id>
            <phase>package</phase>
            <goals>
              <goal>build-image-tar</goal>
            </goals>
            <configuration>
              <vm>server</vm>
              <addModules>jdk.jdwp.agent,jdk.crypto.ec</addModules>
              <executable>app</executable>
              <launchers>
                <launcher>
                  <name>app</name>
                  <vmOptions>-Xms2G -Xmx2G -XX:+UseNUMA -
XX:+UseParallelGC</vmOptions>
                </launcher>
              </launchers>
              <repository>example</repository>
            </configuration>
          </execution>
        </executions>
      </plugin>
    </plugins>
  </build>
</project>

```

The resulting image reference is defined by `${registry}/${repository}/${name}:${project.version}`, the registry and the repository are optional and the name default to the project artifact id.

The resulting image can then be loaded in a docker daemon:

```
$ docker load --input target/example-1.0.0-SNAPSHOT-container_linux_amd64.tar
```

As for `build-app` goal, this goal uses `jpackage` tool so if you intend to use a JDK<16 you'll need to explicitly add the `jdk.incubator.jpackage` module in `MAVEN_OPTS`:

```
$ export MAVEN_OPTS="--add-modules jdk.incubator.jpackage"
```

## Build and deploy a container image to a Docker daemon

The `inverno:build-image-docker` goal is used to build a container image and deploy it to a Docker daemon using the Docker CLI.

```

<project>
  <build>
    <plugins>
      <plugin>
        <groupId>io.inverno.tool</groupId>
        <artifactId>inverno-maven-plugin</artifactId>
        <executions>
          <execution>
            <id>build-image-docker</id>
            <phase>package</phase>
            <goals>
              <goal>build-image-docker</goal>
            </goals>
            <configuration>
              <vm>server</vm>
              <addModules>jdk.jdpw.agent,jdk.crypto.ec</addModules>
              <executable>app</executable>
              <launchers>
                <launcher>
                  <name>app</name>
                  <vmOptions>-Xms2G -Xmx2G -XX:+UseNUMA -
XX:+UseParallelGC</vmOptions>
                </launcher>
              </launchers>
              <repository>example</repository>
            </configuration>
          </execution>
        </executions>
      </plugin>
    </plugins>
  </build>
</project>

```

By default the `docker` command is used but it is possible to specify the path to the Docker CLI in the `inverno.container.docker.executable` parameter.

As for `build-app` goal, this goal uses `jpackage` tool so if you intend to use a JDK<16 you'll need to explicitly add the `jdk.incubator.jpackage` module in `MAVEN_OPTS`:

```
$ export MAVEN_OPTS="--add-modules jdk.incubator.jpackage"
```

## Build and deploy a container image to a remote repository

The `inverno:build-image` goal builds a container image and deploy it to a remote repository.

```

<project>
  <build>
    <plugins>
      <plugin>
        <groupId>io.inverno.tool</groupId>
        <artifactId>inverno-maven-plugin</artifactId>
        <executions>
          <execution>
            <id>build-image-docker</id>
            <phase>package</phase>
            <goals>
              <goal>build-image-docker</goal>
            </goals>
            <configuration>
              <vm>server</vm>
              <addModules>jdk.jdwp.agent,jdk.crypto.ec</addModules>
              <executable>app</executable>
              <launchers>
                <launcher>
                  <name>app</name>
                  <vmOptions>-Xms2G -Xmx2G -XX:+UseNUMA -
XX:+UseParallelGC</vmOptions>
                </launcher>
              </launchers>
              <registryUsername>user</registryUsername>
              <registryPassword>password</registryPassword>
              <registry>gcr.io</registry>
              <repository>example</repository>
            </configuration>
          </execution>
        </executions>
      </plugin>
    </plugins>
  </build>
</project>

```

By default the registry points to the Docker hub [registry-1.docker.io](https://registry-1.docker.io) but another registry can be specified, [gcr.io](https://gcr.io) in our example.

As for [build-app](#) goal, this goal uses [jpackage](#) tool so if you intend to use a JDK<16 you'll need to explicitly add the [jdk.incubator.jpackage](#) module in [MAVEN\\_OPTS](#):

```
$ export MAVEN_OPTS="--add-modules jdk.incubator.jpackage"
```

## Goals

### Overview

- [inverno:build-app](#) Builds the project application package.
- [inverno:build-image](#) Builds a container image and publishes it to a registry.
- [inverno:build-image-docker](#) Builds a Docker container image to a local Docker daemon.
- [inverno:build-image-tar](#) Builds a container image to a TAR archive that can be later loaded into Docker:

- [inverno:build-runtime](#) Builds the project runtime image.
- [inverno:help](#) Display help information on inverno-maven-plugin.
- [inverno:run](#) Runs the project application.
- [inverno:start](#) Starts the project application without blocking the Maven build.
- [inverno:stop](#) Stops the project application that has been previously started using the start goal.

## inverno:build-app

### Full name:

io.inverno.tool:inverno-maven-plugin:1.3.1:build-app

### Description:

Builds the project application package.

A project application package is a native self-contained Java application including all the necessary dependencies. It can be used to distribute a complete application.

### Attributes:

- Requires a Maven project to be executed.
- Requires dependency resolution of artifacts in scope: compile+runtime.
- Requires dependency collection of artifacts in scope: compile+runtime.
- Since version: 1.0.
- Binds by default to the lifecycle phase: package.

## Required parameters

Name	Type	Description
<a href="#">attach</a>	boolean	Attach the resulting image archives to the project to install them in the local Maven repository and deploy them to remote repositories. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.attach</li> <li>• <i>Default</i> : true</li> </ul>
<a href="#">formats</a>	Set	A list of archive formats to generate (eg. zip, tar.gz...) <ul style="list-style-type: none"> <li>• <i>Default</i> : zip</li> </ul>

## Optional parameters

Name	Type	Description
<a href="#">addModules</a>	String	The modules to add to the resulting image <ul style="list-style-type: none"> <li><i>User property</i> : inverno.image.addModules</li> </ul>
<a href="#">addOptions</a>	String	The options to prepend before any other options when invoking the JVM in the resulting image. <ul style="list-style-type: none"> <li><i>User property</i> : inverno.image.addOptions</li> </ul>
<a href="#">automaticLaunchers</a>	boolean	Enables the automatic generation of launchers based on the main classes extracted from the application module. If enabled, a launcher is generated for all main classes other than the main launcher. <ul style="list-style-type: none"> <li><i>User property</i> : inverno.app.automaticLaunchers</li> <li><i>Default</i> : false</li> </ul>
<a href="#">bindServices</a>	boolean	Link in service provider modules and their dependencies. <ul style="list-style-type: none"> <li><i>User property</i> : inverno.image.bindServices</li> <li><i>Default</i> : false</li> </ul>
<a href="#">compress</a>	String	The compress level of the resulting image 0=No compression, 1=constant string sharing, 2=ZIP. <ul style="list-style-type: none"> <li><i>User property</i> : inverno.image.compress</li> </ul>
<a href="#">configurationDirectory</a>	File	A directory containing user-editable configuration files that will be copied to the resulting image. <ul style="list-style-type: none"> <li><i>User property</i> : inverno.image.configurationDirectory</li> <li><i>Default</i> : \${project.basedir}/src/main/conf/</li> </ul>
<a href="#">copyright</a>	String	The application copyright. <ul style="list-style-type: none"> <li><i>User property</i> : inverno.app.copyright</li> </ul>

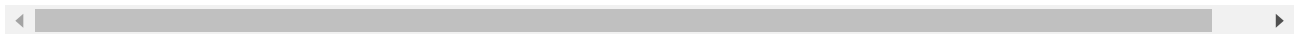
<a href="#">description</a>	String	The description of the application. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.description</code></li> <li>• <i>Default</i> : <code>\${project.description}</code></li> </ul>
<a href="#">excludeArtifactIds</a>	String	Comma separated list of Artifact names to exclude. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.excludeArtifactIds</code></li> </ul>
<a href="#">excludeClassifiers</a>	String	Comma Separated list of Classifiers to exclude. Empty String indicates don't exclude anything (default). <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>excludeClassifiers</code></li> </ul>
<a href="#">excludeGroupIds</a>	String	Comma separated list of GroupId Names to exclude. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.excludeGroupIds</code></li> </ul>
<a href="#">excludeScope</a>	String	Scope to exclude. An Empty string indicates no scopes (default). <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.excludeScope</code></li> </ul>
<a href="#">ignoreSigningInformation</a>	boolean	Suppress a fatal error when signed modules JARs are linked in the image. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.ignoreSigningInformation</code></li> <li>• <i>Default</i> : <code>false</code></li> </ul>
<a href="#">includeArtifactIds</a>	String	Comma separated list of Artifact names to include. Empty String indicates include everything (default). <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.includeArtifactIds</code></li> </ul>
<a href="#">includeClassifiers</a>	String	Comma Separated list of Classifiers to include. Empty String indicates include everything (default). <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.includeClassifiers</code></li> </ul>
<a href="#">includeGroupIds</a>	String	Comma separated list of GroupIds to



		<p>include. Empty String indicates include everything (default).</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.includeGroupIds</li> </ul>
<a href="#">includeScope</a>	String	<p>Scope to include. An Empty string indicate all scopes (default). The scopes being interpreted are the scopes as Maven sees them, not as specified in the pom. In summary:</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.includeScope</li> </ul>
<a href="#">installDirectory</a>	String	<p>Absolute path of the installation directory the application on OS X or Linux. Relative sub-path of the installation location of the application such as 'Program Files' or 'AppData' on Windows.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.app.installDirectory</li> </ul>
<a href="#">jmodsOverrideDirectory</a>	File	<p>A directory containing module descriptors use to modularize unnamed dependency modules and which override the ones that are otherwise generated.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.jmodsOverrideDirector</li> <li>• <i>Default</i> : \${project.basedir}/src/jmod</li> </ul>
<a href="#">launchers</a>	List	<p>A list of extra launchers to include in the resulting application.</p>
<a href="#">legalDirectory</a>	File	<p>A directory containing legal notices that w be copied to the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.legalDirectory</li> <li>• <i>Default</i> : \${project.basedir}/src/main/legal/</li> </ul>
<a href="#">licenseFile</a>	File	<p>The path to the application license file.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.app.licenseFil</li> <li>• <i>Default</i> : \${project.basedir}/LICENSE</li> </ul>
<a href="#">linuxConfiguration</a>	LinuxConfiguration	<p>Linux specific configuration.</p>

<a href="#">macOSConfiguration</a>	MacOSConfiguration	MacOS specific configuration.
<a href="#">manDirectory</a>	File	<p>A directory containing man pages that will be copied to the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.manDirectory</li> <li>• <i>Default</i> : \${project.basedir}/src/main/man/</li> </ul>
<a href="#">overWritelfNewer</a>	boolean	<p>Overwrite dependencies that don't exist or are older than the source.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.overWritelfNewer</li> <li>• <i>Default</i> : true</li> </ul>
<a href="#">projectMainClass</a>	String	<p>The main class in the project module to use when building the project JMOD package.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.runtime.projectMainClass</li> </ul>
<a href="#">resolveProjectMainClass</a>	boolean	<p>Resolve the project main class when not specified explicitly.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.runtime.projectMainClass</li> <li>• <i>Default</i> : false</li> </ul>
<a href="#">resourceDirectory</a>	File	<p>The path to resources that override resulti package resources.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.app.resourceDirectory</li> </ul>
<a href="#">skip</a>	boolean	<p>Skips the generation of the application.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.app.skip</li> </ul>
<a href="#">stripDebug</a>	boolean	<p>Strip debug information from the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.stripDebug</li> <li>• <i>Default</i> : true</li> </ul>
<a href="#">stripNativeCommands</a>	boolean	Strip native command (eg. java...) from th

		resulting image. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.stripNativeCommands</li> <li>• <i>Default</i> : true</li> </ul>
<a href="#">vendor</a>	String	The application vendor. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.app.vendor</li> <li>• <i>Default</i> : \${project.organization.name}</li> </ul>
<a href="#">verbose</a>	boolean	Enables verbose logging. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.verbose</li> <li>• <i>Default</i> : false</li> </ul>
<a href="#">vm</a>	String	Select the HotSpot VM in the output image defined as: 'client' / 'server' / 'minimal' / 'a <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.vm</li> </ul>
<a href="#">windowsConfiguration</a>	WindowsConfiguration	Windows specific configuration.



## Parameter details

### <addModules>

The modules to add to the resulting image.

- **Type**: java.lang.String
- **Required**: no
- **User property**: inverno.image.addModules

### <addOptions>

The options to prepend before any other options when invoking the JVM in the resulting image.

- **Type**: java.lang.String
- **Required**: no
- **User property**: inverno.image.addOptions

### <attach>

Attach the resulting image archives to the project to install them in the local Maven repository and deploy them to remote repositories.

- **Type**: boolean

- **Required:** yes
- **User property:** invernno.image.attach
- **Default:** true

### <automaticLaunchers>

Enables the automatic generation of launchers based on the main classes extracted from the application module. If enabled, a launcher is generated for all main classes other than the main launcher.

- **Type:** boolean
- **Required:** no
- **User property:** invernno.app.automaticLaunchers
- **Default:** false

### <bindServices>

Link in service provider modules and their dependencies.

- **Type:** boolean
- **Required:** no
- **User property:** invernno.image.bindServices
- **Default:** false

### <compress>

The compress level of the resulting image: 0=No compression, 1=constant string sharing, 2=ZIP.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.compress

### <configurationDirectory>

A directory containing user-editable configuration files that will be copied to the resulting image.

- **Type:** java.io.File
- **Required:** no
- **User property:** invernno.image.configurationDirectory
- **Default:** \${project.basedir}/src/main/conf/

### <copyright>

The application copyright.

- **Type:** java.lang.String
- **Required:** no

- **User property:** invernno.app.copyright

## <description>

The description of the application.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.app.description
- **Default:** \${project.description}

## <excludeArtifactIds>

Comma separated list of Artifact names to exclude.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.excludeArtifactIds

## <excludeClassifiers>

Comma Separated list of Classifiers to exclude. Empty String indicates don't exclude anything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** excludeClassifiers

## <excludeGroupIds>

Comma separated list of GroupId Names to exclude.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.excludeGroupIds

## <excludeScope>

Scope to exclude. An Empty string indicates no scopes (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.excludeScope

## <formats>

A list of archive formats to generate (eg. zip, tar.gz...)

- **Type:** java.util.Set
- **Required:** yes
- **Default:** zip

## <ignoreSigningInformation>

Suppress a fatal error when signed modular JARs are linked in the image.

- **Type:** boolean
- **Required:** no
- **User property:** invernno.image.ignoreSigningInformation
- **Default:** false

## <includeArtifactIds>

Comma separated list of Artifact names to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.includeArtifactIds

## <includeClassifiers>

Comma Separated list of Classifiers to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.includeClassifiers

## <includeGroupIds>

Comma separated list of GroupIds to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.includeGroupIds

## <includeScope>

Scope to include. An Empty string indicates all scopes (default). The scopes being interpreted are the scopes as Maven sees them, not as specified in the pom. In summary:

- runtime scope gives runtime and compile dependencies,
- compile scope gives compile, provided, and system dependencies,
- test (default) scope gives all dependencies,
- provided scope just gives provided dependencies,
- system scope just gives system dependencies.
- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.includeScope

## <installDirectory>

Absolute path of the installation directory of the application on OS X or Linux. Relative sub-path of the installation location of the application such as 'Program Files' or 'AppData' on Windows.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.app.installDirectory

## <jmodsOverrideDirectory>

A directory containing module descriptors to use to modularize unnamed dependency modules and which override the ones that are otherwise generated.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.image.jmodsOverrideDirectory
- **Default:** \${project.basedir}/src/jmods/

## <launchers>

A list of extra launchers to include in the resulting application.

- **Type:** java.util.List
- **Required:** no

## <legalDirectory>

A directory containing legal notices that will be copied to the resulting image.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.image.legalDirectory
- **Default:** \${project.basedir}/src/main/legal/

## <licenseFile>

The path to the application license file.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.app.licenseFile
- **Default:** \${project.basedir}/LICENSE

## <linuxConfiguration>

Linux specific configuration.

- **Type:** io.inverno.tool.maven.internal.task.CreateProjectApplicationTask\$LinuxConfiguration
- **Required:** no

## <macOSConfiguration>

MacOS specific configuration.

- **Type:**  
io.inverno.tool.maven.internal.task.CreateProjectApplicationTask\$MacOSConfiguration
- **Required:** no

## <manDirectory>

A directory containing man pages that will be copied to the resulting image.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.image.manDirectory
- **Default:** \${project.basedir}/src/main/man/

## <overWritelfNewer>

Overwrite dependencies that don't exist or are older than the source.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.image.overWritelfNewer
- **Default:** true



### <projectMainClass>

The main class in the project module to use when building the project JMOD package.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.runtime.projectMainClass

### <resolveProjectMainClass>

Resolve the project main class when not specified explicitly.

- **Type:** boolean
- **Required:** no
- **User property:** invernno.runtime.projectMainClass
- **Default:** false

### <resourceDirectory>

The path to resources that override resulting package resources.

- **Type:** java.io.File
- **Required:** no
- **User property:** invernno.app.resourceDirectory

### <skip>

Skips the generation of the application.

- **Type:** boolean
- **Required:** no
- **User property:** invernno.app.skip

### <stripDebug>

Strip debug information from the resulting image.

- **Type:** boolean
- **Required:** no
- **User property:** invernno.image.stripDebug
- **Default:** true

### <stripNativeCommands>

Strip native command (eg. java...) from the resulting image.

- **Type:** boolean
- **Required:** no
- **User property:** invernno.image.stripNativeCommands
- **Default:** true

## <vendor>

The application vendor.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.app.vendor
- **Default:** \${project.organization.name}

## <verbose>

Enables verbose logging.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.verbose
- **Default:** false

## <vm>

Select the HotSpot VM in the output image defined as: 'client' / 'server' / 'minimal' / 'all'

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.vm

## <windowsConfiguration>

Windows specific configuration.

- **Type:**  
io.inverno.tool.maven.internal.task.CreateProjectApplicationTask\$WindowsConfiguration
- **Required:** no

# inverno:build-image

### Full name:

io.inverno.tool:inverno-maven-plugin:1.3.1:build-image

### Description:

Builds a container image and publishes it to a registry.

### Attributes:

- Requires a Maven project to be executed.
- Requires dependency resolution of artifacts in scope: compile+runtime.
- Requires dependency collection of artifacts in scope: compile+runtime.
- Since version: 1.0.

- Binds by default to the lifecycle phase: install.

## Required parameters

Name	Type	Description
<a href="#">attach</a>	boolean	Attach the resulting image archives to the project to install them in the local Maven repository and deploy them to remote repositories. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.attach</li> <li>• <i>Default</i> : true</li> </ul>
<a href="#">executable</a>	String	The executable in the application image to use as image entry point. The specified name should correspond to a declared application image launchers or the project artifact id if no launcher was specified. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.app.executable</li> <li>• <i>Default</i> : \${project.artifactId}</li> </ul>
<a href="#">formats</a>	Set	A list of archive formats to generate (eg. zip, tar.gz...) <ul style="list-style-type: none"> <li>• <i>Default</i> : zip</li> </ul>
<a href="#">from</a>	String	The base container image. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.container.from</li> <li>• <i>Default</i> : debian:buster-slim</li> </ul>

## Optional parameters

Name	Type	Description
<a href="#">addModules</a>	String	The modules to add to the resulting image <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.addMo</code></li> </ul>
<a href="#">addOptions</a>	String	The options to prepend before any other o invoking the JVM in the resulting image. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.addOp</code></li> </ul>
<a href="#">automaticLaunchers</a>	boolean	Enables the automatic generation of launc on the main classes extracted from the ap module. If enabled, a launcher is generate main classes other than the main launcher <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.app.automatic</code></li> <li><i>Default</i> : <code>false</code></li> </ul>
<a href="#">bindServices</a>	boolean	Link in service provider modules and their dependencies. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.bindSe</code></li> <li><i>Default</i> : <code>false</code></li> </ul>
<a href="#">compress</a>	String	The compress level of the resulting image compression, 1=constant string sharing, 2 <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.compre</code></li> </ul>
<a href="#">configurationDirectory</a>	File	A directory containing user-editable config that will be copied to the resulting image. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.configurationDirectory</code></li> <li><i>Default</i> : <code>\${project.basedir}/src/main,</code></li> </ul>
<a href="#">copyright</a>	String	The application copyright. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.app.copyright</code></li> </ul>
<a href="#">description</a>	String	The description of the application. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.app.descriptio</code></li> <li><i>Default</i> : <code>\${project.description}</code></li> </ul>
<a href="#">environment</a>	Map	The container's environment variables.
<a href="#">excludeArtifactIds</a>	String	Comma separated list of Artifact names to <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.exclud</code></li> </ul>

<a href="#">excludeClassifiers</a>	String	Comma Separated list of Classifiers to exclude. An Empty String indicates don't exclude anything (default). • <i>User property</i> : excludeClassifiers
<a href="#">excludeGroupIds</a>	String	Comma separated list of GroupId Names to exclude. An Empty String indicates include everything (default). • <i>User property</i> : invernno.image.excludeGroupIds
<a href="#">excludeScope</a>	String	Scope to exclude. An Empty string indicates include everything (default). • <i>User property</i> : invernno.image.excludeScope
<a href="#">ignoreSigningInformation</a>	boolean	Suppress a fatal error when signed modules are not found or linked in the image. • <i>User property</i> : invernno.image.ignoreSigningInformation • <i>Default</i> : false
<a href="#">imageFormat</a>	ImageFormat	The format of the container image. • <i>User property</i> : invernno.container.imageFormat • <i>Default</i> : Docker
<a href="#">includeArtifactIds</a>	String	Comma separated list of Artifact names to include. An Empty String indicates include everything (default). • <i>User property</i> : invernno.image.includeArtifactIds
<a href="#">includeClassifiers</a>	String	Comma Separated list of Classifiers to include. An Empty String indicates include everything (default). • <i>User property</i> : invernno.image.includeClassifiers
<a href="#">includeGroupIds</a>	String	Comma separated list of GroupIds to include. An Empty String indicates include everything (default). • <i>User property</i> : invernno.image.includeGroupIds
<a href="#">includeScope</a>	String	Scope to include. An Empty string indicates include everything (default). The scopes being interpreted are as Maven sees them, not as specified in the pom file. • <i>User property</i> : invernno.image.includeScope
<a href="#">installDirectory</a>	String	Absolute path of the installation directory for the application on OS X or Linux. Relative sub-

		<p>installation location of the application such as 'Program Files' or 'AppData' on Windows.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.installDir</code></li> </ul>
<a href="#">jmodsOverrideDirectory</a>	File	<p>A directory containing module descriptors that will be used to modularize unnamed dependency module and override the ones that are otherwise generated.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.jmodsOverrideDirectory</code></li> <li>• <i>Default</i> : <code>\${project.basedir}/src/jmodsOverride</code></li> </ul>
<a href="#">labels</a>	Map	The labels to apply to the container image.
<a href="#">launchers</a>	List	A list of extra launchers to include in the resulting application.
<a href="#">legalDirectory</a>	File	<p>A directory containing legal notices that will be included in the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.legalDirectory</code></li> <li>• <i>Default</i> : <code>\${project.basedir}/src/main/legal</code></li> </ul>
<a href="#">licenseFile</a>	File	<p>The path to the application license file.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.licenseFile</code></li> <li>• <i>Default</i> : <code>\${project.basedir}/LICENSE</code></li> </ul>
<a href="#">linuxConfiguration</a>	LinuxConfiguration	Linux specific configuration.
<a href="#">macOSConfiguration</a>	MacOSConfiguration	MacOS specific configuration.
<a href="#">manDirectory</a>	File	<p>A directory containing man pages that will be included in the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.manDirectory</code></li> <li>• <i>Default</i> : <code>\${project.basedir}/src/main/man</code></li> </ul>
<a href="#">overWriteIfNewer</a>	boolean	<p>Overwrite dependencies that don't exist on the target platform than the source.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.overWriteIfNewer</code></li> <li>• <i>Default</i> : <code>true</code></li> </ul>
<a href="#">ports</a>	Set	The ports exposed by the container at runtime as: <code>port_number [ '/' udp/tcp ]</code>

<a href="#">projectMainClass</a>	String	The main class in the project module to use building the project JMOD package. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.runtime.proje</code></li> </ul>
<a href="#">registry</a>	String	The registry part of the target image referred as: <code>\${registry}/\${repository}/\${name}:\${pr}</code> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.container.regi</code></li> </ul>
<a href="#">registryPassword</a>	String	The password to use to authenticate to the <ul style="list-style-type: none"> <li>• <i>User property</i> :  <code>inverno.container.registry.password</code></li> </ul>
<a href="#">registryUsername</a>	String	The user name to use to authenticate to the <ul style="list-style-type: none"> <li>• <i>User property</i> :  <code>inverno.container.registry.username</code></li> </ul>
<a href="#">repository</a>	String	The repository part of the target image referred as: <code>\${registry}/\${repository}/\${name}:\${pr}</code> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.container.repo</code></li> </ul>
<a href="#">resolveProjectMainClass</a>	boolean	Resolve the project main class when not specified explicitly. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.runtime.proje</code></li> <li>• <i>Default</i> : <code>false</code></li> </ul>
<a href="#">resourceDirectory</a>	File	The path to resources that override resulting resources. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.resource[</code></li> </ul>
<a href="#">skip</a>	boolean	Skips the generation of the application. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.skip</code></li> </ul>
<a href="#">stripDebug</a>	boolean	Strip debug information from the resulting <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.stripDe</code></li> <li>• <i>Default</i> : <code>true</code></li> </ul>
<a href="#">stripNativeCommands</a>	boolean	Strip native command (eg. <code>java...</code> ) from the image. <ul style="list-style-type: none"> <li>• <i>User property</i> :  <code>inverno.image.stripNativeCommands</code></li> </ul>

		<ul style="list-style-type: none"> <li>• <i>Default</i> : true</li> </ul>
<a href="#">user</a>	String	The user and group used to run the container as: user / uid [ ':' group / gid ]
<a href="#">vendor</a>	String	The application vendor. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.app.vendor</li> <li>• <i>Default</i> : \${project.organization.name}</li> </ul>
<a href="#">verbose</a>	boolean	Enables verbose logging. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.verbose</li> <li>• <i>Default</i> : false</li> </ul>
<a href="#">vm</a>	String	Select the HotSpot VM in the output image: 'client' / 'server' / 'minimal' / 'all' <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.vm</li> </ul>
<a href="#">volumes</a>	Set	The container's mount points.
<a href="#">windowsConfiguration</a>	WindowsConfiguration	Windows specific configuration.



## Parameter details

### <addModules>

The modules to add to the resulting image.

- **Type**: java.lang.String
- **Required**: no
- **User property**: inverno.image.addModules

### <addOptions>

The options to prepend before any other options when invoking the JVM in the resulting image.

- **Type**: java.lang.String
- **Required**: no
- **User property**: inverno.image.addOptions



## <attach>

Attach the resulting image archives to the project to install them in the local Maven repository and deploy them to remote repositories.

- **Type:** boolean
- **Required:** yes
- **User property:** inverno.image.attach
- **Default:** true

## <automaticLaunchers>

Enables the automatic generation of launchers based on the main classes extracted from the application module. If enabled, a launcher is generated for all main classes other than the main launcher.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.app.automaticLaunchers
- **Default:** false

## <bindServices>

Link in service provider modules and their dependencies.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.image.bindServices
- **Default:** false

## <compress>

The compress level of the resulting image: 0=No compression, 1=constant string sharing, 2=ZIP.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.compress

## <configurationDirectory>

A directory containing user-editable configuration files that will be copied to the resulting image.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.image.configurationDirectory
- **Default:** \${project.basedir}/src/main/conf/

## <copyright>

The application copyright.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.app.copyright

## <description>

The description of the application.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.app.description
- **Default:** \${project.description}

## <environment>

The container's environment variables.

- **Type:** java.util.Map
- **Required:** no

## <excludeArtifactIds>

Comma separated list of Artifact names to exclude.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.excludeArtifactIds

## <excludeClassifiers>

Comma Separated list of Classifiers to exclude. Empty String indicates don't exclude anything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** excludeClassifiers

## <excludeGroupIds>

Comma separated list of GroupId Names to exclude.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.excludeGroupIds

### <excludeScope>

Scope to exclude. An Empty string indicates no scopes (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.excludeScope

### <executable>

The executable in the application image to use as image entry point. The specified name should correspond to a declared application image launchers or the project artifact id if no launcher was specified.

- **Type:** java.lang.String
- **Required:** yes
- **User property:** inverno.app.executable
- **Default:** \${project.artifactId}

### <formats>

A list of archive formats to generate (eg. zip, tar.gz...)

- **Type:** java.util.Set
- **Required:** yes
- **Default:** zip

### <from>

The base container image.

- **Type:** java.lang.String
- **Required:** yes
- **User property:** inverno.container.from
- **Default:** debian:buster-slim

### <ignoreSigningInformation>

Suppress a fatal error when signed modular JARs are linked in the image.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.image.ignoreSigningInformation
- **Default:** false

## <imageFormat>

The format of the container image.

- **Type:** com.google.cloud.tools.jib.api.buildplan.ImageFormat
- **Required:** no
- **User property:** invernno.container.imageFormat
- **Default:** Docker

## <includeArtifactIds>

Comma separated list of Artifact names to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.includeArtifactIds

## <includeClassifiers>

Comma Separated list of Classifiers to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.includeClassifiers

## <includeGroupIds>

Comma separated list of GroupIds to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.includeGroupIds

## <includeScope>

Scope to include. An Empty string indicates all scopes (default). The scopes being interpreted are the scopes as Maven sees them, not as specified in the pom. In summary:

- runtime scope gives runtime and compile dependencies,
- compile scope gives compile, provided, and system dependencies,
- test (default) scope gives all dependencies,
- provided scope just gives provided dependencies,
- system scope just gives system dependencies.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.includeScope

### <installDirectory>

Absolute path of the installation directory of the application on OS X or Linux. Relative sub-path of the installation location of the application such as 'Program Files' or 'AppData' on Windows.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.app.installDirectory

### <jmodsOverrideDirectory>

A directory containing module descriptors to use to modularize unnamed dependency modules and which override the ones that are otherwise generated.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.image.jmodsOverrideDirectory
- **Default:** \${project.basedir}/src/jmods/

### <labels>

The labels to apply to the container image.

- **Type:** java.util.Map
- **Required:** no

### <launchers>

A list of extra launchers to include in the resulting application.

- **Type:** java.util.List
- **Required:** no

### <legalDirectory>

A directory containing legal notices that will be copied to the resulting image.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.image.legalDirectory
- **Default:** \${project.basedir}/src/main/legal/

## <licenseFile>

The path to the application license file.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.app.licenseFile
- **Default:** \${project.basedir}/LICENSE

## <linuxConfiguration>

Linux specific configuration.

- **Type:** io.inverno.tool.maven.internal.task.CreateProjectApplicationTask\$LinuxConfiguration
- **Required:** no

## <macOSConfiguration>

MacOS specific configuration.

- **Type:**  
io.inverno.tool.maven.internal.task.CreateProjectApplicationTask\$MacOSConfiguration
- **Required:** no

## <manDirectory>

A directory containing man pages that will be copied to the resulting image.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.image.manDirectory
- **Default:** \${project.basedir}/src/main/man/

## <overWritelfNewer>

Overwrite dependencies that don't exist or are older than the source.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.image.overWritelfNewer
- **Default:** true

## <ports>

The ports exposed by the container at runtime defined as: port\_number [ '/' udp/tcp ]

- **Type:** java.util.Set
- **Required:** no

## <projectMainClass>

The main class in the project module to use when building the project JMOD package.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.runtime.projectMainClass

## <registry>

The registry part of the target image reference defined as:

`${registry}/${repository}/${name}:${project.version}`

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.container.registry

## <registryPassword>

The password to use to authenticate to the registry.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.container.registry.password

## <registryUsername>

The user name to use to authenticate to the registry.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.container.registry.username

## <repository>

The repository part of the target image reference defined as:

`${registry}/${repository}/${name}:${project.version}`

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.container.repository

## <resolveProjectMainClass>

Resolve the project main class when not specified explicitly.

- **Type:** boolean
- **Required:** no
- **User property:** invernno.runtime.projectMainClass
- **Default:** false

## <resourceDirectory>

The path to resources that override resulting package resources.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.app.resourceDirectory

## <skip>

Skips the generation of the application.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.app.skip

## <stripDebug>

Strip debug information from the resulting image.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.image.stripDebug
- **Default:** true

## <stripNativeCommands>

Strip native command (eg. java...) from the resulting image.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.image.stripNativeCommands
- **Default:** true

## <user>

The user and group used to run the container defined as: user / uid [ ':' group / gid ]

- **Type:** java.lang.String
- **Required:** no

## <vendor>

The application vendor.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.app.vendor
- **Default:** \${project.organization.name}



### <verbose>

Enables verbose logging.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.verbose
- **Default:** false

### <vm>

Select the HotSpot VM in the output image defined as: 'client' / 'server' / 'minimal' / 'all'

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.vm

### <volumes>

The container's mount points.

- **Type:** java.util.Set
- **Required:** no

### <windowsConfiguration>

Windows specific configuration.

- **Type:**  
io.inverno.tool.maven.internal.task.CreateProjectApplicationTask\$WindowsConfiguration
- **Required:** no

## inverno:build-image-docker

### Full name:

io.inverno.tool:inverno-maven-plugin:1.3.1:build-image-docker

### Description:

Builds a Docker container image to a local Docker daemon.

### Attributes:

- Requires a Maven project to be executed.
- Requires dependency resolution of artifacts in scope: compile+runtime.
- Requires dependency collection of artifacts in scope: compile+runtime.
- Since version: 1.0.
- Binds by default to the lifecycle phase: install.

## Required parameters

Name	Type	Description
<a href="#">attach</a>	boolean	Attach the resulting image archives to the project to install them in the local Maven repository and deploy them to remote repositories. <ul style="list-style-type: none"><li>• <i>User property</i> : inverno.image.attach</li><li>• <i>Default</i> : true</li></ul>
<a href="#">executable</a>	String	The executable in the application image to use as image entry point. The specified name should correspond to a declared application image launchers or the project artifact id if no launcher was specified. <ul style="list-style-type: none"><li>• <i>User property</i> : inverno.app.executable</li><li>• <i>Default</i> : \${project.artifactId}</li></ul>
<a href="#">formats</a>	Set	A list of archive formats to generate (eg. zip, tar.gz...) <ul style="list-style-type: none"><li>• <i>Default</i> : zip</li></ul>
<a href="#">from</a>	String	The base container image. <ul style="list-style-type: none"><li>• <i>User property</i> : inverno.container.from</li><li>• <i>Default</i> : debian:buster-slim</li></ul>

## Optional parameters

Name	Type	Description
<a href="#">addModules</a>	String	The modules to add to the resulting image <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.addMo</code></li> </ul>
<a href="#">addOptions</a>	String	The options to prepend before any other o invoking the JVM in the resulting image. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.addOp</code></li> </ul>
<a href="#">automaticLaunchers</a>	boolean	Enables the automatic generation of launc on the main classes extracted from the ap module. If enabled, a launcher is generate main classes other than the main launcher <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.automatic</code></li> <li>• <i>Default</i> : <code>false</code></li> </ul>
<a href="#">bindServices</a>	boolean	Link in service provider modules and their dependencies. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.bindSe</code></li> <li>• <i>Default</i> : <code>false</code></li> </ul>
<a href="#">compress</a>	String	The compress level of the resulting image compression, 1=constant string sharing, 2 <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.compre</code></li> </ul>
<a href="#">configurationDirectory</a>	File	A directory containing user-editable config that will be copied to the resulting image. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.configurationDirectory</code></li> <li>• <i>Default</i> : <code>\${project.basedir}/src/main,</code></li> </ul>
<a href="#">copyright</a>	String	The application copyright. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.copyright</code></li> </ul>
<a href="#">description</a>	String	The description of the application. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.descriptio</code></li> <li>• <i>Default</i> : <code>\${project.description}</code></li> </ul>
<a href="#">dockerEnvironment</a>	Map	The Docker environment variables used by CLI executable.
<a href="#">dockerExecutable</a>	File	The path to the Docker CLI executable use

		<p>image in the Docker daemon.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.container.docker.executable</li> </ul>
<a href="#">environment</a>	Map	The container's environment variables.
<a href="#">excludeArtifactIds</a>	String	<p>Comma separated list of Artifact names to</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.exclude</li> </ul>
<a href="#">excludeClassifiers</a>	String	<p>Comma Separated list of Classifiers to exc String indicates don't exclude anything (de</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : excludeClassifiers</li> </ul>
<a href="#">excludeGroupIds</a>	String	<p>Comma separated list of GroupId Names t</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.exclude</li> </ul>
<a href="#">excludeScope</a>	String	<p>Scope to exclude. An Empty string indicate (default).</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.exclude</li> </ul>
<a href="#">ignoreSigningInformation</a>	boolean	<p>Suppress a fatal error when signed module linked in the image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.ignoreSigningInformation</li> <li>• <i>Default</i> : false</li> </ul>
<a href="#">imageFormat</a>	ImageFormat	<p>The format of the container image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.container.ima</li> <li>• <i>Default</i> : Docker</li> </ul>
<a href="#">includeArtifactIds</a>	String	<p>Comma separated list of Artifact names to Empty String indicates include everything</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.include</li> </ul>
<a href="#">includeClassifiers</a>	String	<p>Comma Separated list of Classifiers to incl String indicates include everything (default</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.include</li> </ul>
<a href="#">includeGroupIds</a>	String	<p>Comma separated list of GroupIds to inclu String indicates include everything (default</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.include</li> </ul>

<a href="#">includeScope</a>	String	<p>Scope to include. An Empty string indicate (default). The scopes being interpreted are as Maven sees them, not as specified in the summary:</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.include</code></li> </ul>
<a href="#">installDirectory</a>	String	<p>Absolute path of the installation directory application on OS X or Linux. Relative sub-installation location of the application such as 'Files' or 'AppData' on Windows.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.installDir</code></li> </ul>
<a href="#">jmodsOverrideDirectory</a>	File	<p>A directory containing module descriptors modularize unnamed dependency module override the ones that are otherwise generated.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.jmodsOverrideDir</code></li> <li>• <i>Default</i> : <code>\${project.basedir}/src/jmod</code></li> </ul>
<a href="#">labels</a>	Map	The labels to apply to the container image
<a href="#">launchers</a>	List	A list of extra launchers to include in the resulting application.
<a href="#">legalDirectory</a>	File	<p>A directory containing legal notices that will be included in the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.legalDir</code></li> <li>• <i>Default</i> : <code>\${project.basedir}/src/main</code></li> </ul>
<a href="#">licenseFile</a>	File	<p>The path to the application license file.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.licenseFile</code></li> <li>• <i>Default</i> : <code>\${project.basedir}/LICENSE</code></li> </ul>
<a href="#">linuxConfiguration</a>	LinuxConfiguration	Linux specific configuration.
<a href="#">macOSConfiguration</a>	MacOSConfiguration	MacOS specific configuration.
<a href="#">manDirectory</a>	File	<p>A directory containing man pages that will be included in the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.manDir</code></li> <li>• <i>Default</i> : <code>\${project.basedir}/src/main</code></li> </ul>

<a href="#">overWritelfNewer</a>	boolean	<p>Overwrite dependencies that don't exist on the target image than the source.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.overWrite</li> <li>• <i>Default</i> : true</li> </ul>
<a href="#">ports</a>	Set	<p>The ports exposed by the container at runtime as: port_number [ '/' udp/tcp ]</p>
<a href="#">projectMainClass</a>	String	<p>The main class in the project module to use when building the project JMOD package.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.runtime.projectMainClass</li> </ul>
<a href="#">registry</a>	String	<p>The registry part of the target image reference is defined as:</p> <p><code>\${registry}/\${repository}/\${name}:\${projectVersion}</code></p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.container.registry</li> </ul>
<a href="#">repository</a>	String	<p>The repository part of the target image reference is defined as:</p> <p><code>\${registry}/\${repository}/\${name}:\${projectVersion}</code></p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.container.repository</li> </ul>
<a href="#">resolveProjectMainClass</a>	boolean	<p>Resolve the project main class when not specified explicitly.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.runtime.projectMainClass</li> <li>• <i>Default</i> : false</li> </ul>
<a href="#">resourceDirectory</a>	File	<p>The path to resources that override result image resources.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.app.resourceDirectory</li> </ul>
<a href="#">skip</a>	boolean	<p>Skips the generation of the application.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.app.skip</li> </ul>
<a href="#">stripDebug</a>	boolean	<p>Strip debug information from the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.stripDebug</li> <li>• <i>Default</i> : true</li> </ul>
<a href="#">stripNativeCommands</a>	boolean	<p>Strip native command (eg. java...) from the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.stripNativeCommands</li> </ul>

		<ul style="list-style-type: none"> <li>• <i>Default</i> : true</li> </ul>
<a href="#">user</a>	String	The user and group used to run the container as: user / uid [ ':' group / gid ]
<a href="#">vendor</a>	String	The application vendor. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.app.vendor</li> <li>• <i>Default</i> : \${project.organization.name}</li> </ul>
<a href="#">verbose</a>	boolean	Enables verbose logging. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.verbose</li> <li>• <i>Default</i> : false</li> </ul>
<a href="#">vm</a>	String	Select the HotSpot VM in the output image: 'client' / 'server' / 'minimal' / 'all' <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.vm</li> </ul>
<a href="#">volumes</a>	Set	The container's mount points.
<a href="#">windowsConfiguration</a>	WindowsConfiguration	Windows specific configuration.



## Parameter details

### <addModules>

The modules to add to the resulting image.

- **Type**: java.lang.String
- **Required**: no
- **User property**: inverno.image.addModules

### <addOptions>

The options to prepend before any other options when invoking the JVM in the resulting image.

- **Type**: java.lang.String
- **Required**: no
- **User property**: inverno.image.addOptions

## <attach>

Attach the resulting image archives to the project to install them in the local Maven repository and deploy them to remote repositories.

- **Type:** boolean
- **Required:** yes
- **User property:** inverno.image.attach
- **Default:** true

## <automaticLaunchers>

Enables the automatic generation of launchers based on the main classes extracted from the application module. If enabled, a launcher is generated for all main classes other than the main launcher.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.app.automaticLaunchers
- **Default:** false

## <bindServices>

Link in service provider modules and their dependencies.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.image.bindServices
- **Default:** false

## <compress>

The compress level of the resulting image: 0=No compression, 1=constant string sharing, 2=ZIP.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.compress

## <configurationDirectory>

A directory containing user-editable configuration files that will be copied to the resulting image.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.image.configurationDirectory
- **Default:** \${project.basedir}/src/main/conf/



### <copyright>

The application copyright.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.app.copyright

### <description>

The description of the application.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.app.description
- **Default:** \${project.description}

### <dockerEnvironment>

The Docker environment variables used by the Docker CLI executable.

- **Type:** java.util.Map
- **Required:** no

### <dockerExecutable>

The path to the Docker CLI executable used to load the image in the Docker daemon.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.container.docker.executable

### <environment>

The container's environment variables.

- **Type:** java.util.Map
- **Required:** no

### <excludeArtifactIds>

Comma separated list of Artifact names to exclude.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.excludeArtifactIds

### <excludeClassifiers>

Comma Separated list of Classifiers to exclude. Empty String indicates don't exclude anything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** excludeClassifiers

### <excludeGroupIds>

Comma separated list of GroupId Names to exclude.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.excludeGroupIds

### <excludeScope>

Scope to exclude. An Empty string indicates no scopes (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.excludeScope

### <executable>

The executable in the application image to use as image entry point. The specified name should correspond to a declared application image launchers or the project artifact id if no launcher was specified.

- **Type:** java.lang.String
- **Required:** yes
- **User property:** invernno.app.executable
- **Default:** \${project.artifactId}

### <formats>

A list of archive formats to generate (eg. zip, tar.gz...)

- **Type:** java.util.Set
- **Required:** yes
- **Default:** zip

## <from>

The base container image.

- **Type:** java.lang.String
- **Required:** yes
- **User property:** inverno.container.from
- **Default:** debian:buster-slim

## <ignoreSigningInformation>

Suppress a fatal error when signed modular JARs are linked in the image.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.image.ignoreSigningInformation
- **Default:** false

## <imageFormat>

The format of the container image.

- **Type:** com.google.cloud.tools.jib.api.buildplan.ImageFormat
- **Required:** no
- **User property:** inverno.container.imageFormat
- **Default:** Docker

## <includeArtifactIds>

Comma separated list of Artifact names to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.includeArtifactIds

## <includeClassifiers>

Comma Separated list of Classifiers to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.includeClassifiers

## <includeGroupIds>

Comma separated list of GroupIds to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.includeGroupIds

## <includeScope>

Scope to include. An Empty string indicates all scopes (default). The scopes being interpreted are the scopes as Maven sees them, not as specified in the pom. In summary:

- runtime scope gives runtime and compile dependencies,
- compile scope gives compile, provided, and system dependencies,
- test (default) scope gives all dependencies,
- provided scope just gives provided dependencies,
- system scope just gives system dependencies.
- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.includeScope

## <installDirectory>

Absolute path of the installation directory of the application on OS X or Linux. Relative sub-path of the installation location of the application such as 'Program Files' or 'AppData' on Windows.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.app.installDirectory

## <jmodsOverrideDirectory>

A directory containing module descriptors to use to modularize unnamed dependency modules and which override the ones that are otherwise generated.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.image.jmodsOverrideDirectory
- **Default:** \${project.basedir}/src/jmods/

## <labels>

The labels to apply to the container image.

- **Type:** java.util.Map
- **Required:** no

## <launchers>

A list of extra launchers to include in the resulting application.

- **Type:** java.util.List
- **Required:** no

## <legalDirectory>

A directory containing legal notices that will be copied to the resulting image.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.image.legalDirectory
- **Default:** \${project.basedir}/src/main/legal/

## <licenseFile>

The path to the application license file.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.app.licenseFile
- **Default:** \${project.basedir}/LICENSE

## <linuxConfiguration>

Linux specific configuration.

- **Type:** io.inverno.tool.maven.internal.task.CreateProjectApplicationTask\$LinuxConfiguration
- **Required:** no

## <macOSConfiguration>

MacOS specific configuration.

- **Type:**  
io.inverno.tool.maven.internal.task.CreateProjectApplicationTask\$MacOSConfiguration
- **Required:** no

## <manDirectory>

A directory containing man pages that will be copied to the resulting image.

- **Type:** java.io.File
- **Required:** no
- **User property:** invernno.image.manDirectory
- **Default:** \${project.basedir}/src/main/man/

## <overWritelfNewer>

Overwrite dependencies that don't exist or are older than the source.

- **Type:** boolean
- **Required:** no
- **User property:** invernno.image.overWritelfNewer
- **Default:** true

## <ports>

The ports exposed by the container at runtime defined as: port\_number [ '/' udp/tcp ]

- **Type:** java.util.Set
- **Required:** no

## <projectMainClass>

The main class in the project module to use when building the project JMOD package.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.runtime.projectMainClass

## <registry>

The registry part of the target image reference defined as:

`${registry}/${repository}/${name}:${project.version}`

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.container.registry

## <repository>

The repository part of the target image reference defined as:

`${registry}/${repository}/${name}:${project.version}`

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.container.repository

## <resolveProjectMainClass>

Resolve the project main class when not specified explicitly.

- **Type:** boolean
- **Required:** no
- **User property:** `inverno.runtime.projectMainClass`
- **Default:** false

## <resourceDirectory>

The path to resources that override resulting package resources.

- **Type:** `java.io.File`
- **Required:** no
- **User property:** `inverno.app.resourceDirectory`

## <skip>

Skips the generation of the application.

- **Type:** boolean
- **Required:** no
- **User property:** `inverno.app.skip`

## <stripDebug>

Strip debug information from the resulting image.

- **Type:** boolean
- **Required:** no
- **User property:** `inverno.image.stripDebug`
- **Default:** true

## <stripNativeCommands>

Strip native command (eg. `java...`) from the resulting image.

- **Type:** boolean
- **Required:** no
- **User property:** `inverno.image.stripNativeCommands`
- **Default:** true

## <user>

The user and group used to run the container defined as: `user / uid [ ':' group / gid ]`

- **Type:** `java.lang.String`
- **Required:** no

## <vendor>

The application vendor.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.app.vendor
- **Default:** \${project.organization.name}

## <verbose>

Enables verbose logging.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.verbose
- **Default:** false

## <vm>

Select the HotSpot VM in the output image defined as: 'client' / 'server' / 'minimal' / 'all'

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.vm

## <volumes>

The container's mount points.

- **Type:** java.util.Set
- **Required:** no

## <windowsConfiguration>

Windows specific configuration.

- **Type:**  
io.inverno.tool.maven.internal.task.CreateProjectApplicationTask\$WindowsConfiguration
- **Required:** no

# inverno:build-image-tar

## Full name:

io.inverno.tool:inverno-maven-plugin:1.3.1:build-image-tar

## Description:

Builds a container image to a TAR archive that can be later loaded into Docker:



```
$ docker load --input target/{@literal<image>.tar }
```

### Attributes:

- Requires a Maven project to be executed.
- Requires dependency resolution of artifacts in scope: compile+runtime.
- Requires dependency collection of artifacts in scope: compile+runtime.
- Since version: 1.0.
- Binds by default to the lifecycle phase: package.

## Required parameters

Name	Type	Description
<a href="#">attach</a>	boolean	Attach the resulting image archives to the project to install them in the local Maven repository and deploy them to remote repositories. <ul style="list-style-type: none"><li>• <i>User property</i> : inverno.image.attach</li><li>• <i>Default</i> : true</li></ul>
<a href="#">executable</a>	String	The executable in the application image to use as image entry point. The specified name should correspond to a declared application image launchers or the project artifact id if no launcher was specified. <ul style="list-style-type: none"><li>• <i>User property</i> : inverno.app.executable</li><li>• <i>Default</i> : \${project.artifactId}</li></ul>
<a href="#">formats</a>	Set	A list of archive formats to generate (eg. zip, tar.gz...) <ul style="list-style-type: none"><li>• <i>Default</i> : zip</li></ul>
<a href="#">from</a>	String	The base container image. <ul style="list-style-type: none"><li>• <i>User property</i> : inverno.container.from</li><li>• <i>Default</i> : debian:buster-slim</li></ul>

## Optional parameters

Name	Type	Description
<a href="#">addModules</a>	String	The modules to add to the resulting image <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.addMo</code></li> </ul>
<a href="#">addOptions</a>	String	The options to prepend before any other o invoking the JVM in the resulting image. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.addOp</code></li> </ul>
<a href="#">automaticLaunchers</a>	boolean	Enables the automatic generation of launc on the main classes extracted from the ap module. If enabled, a launcher is generate main classes other than the main launcher <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.app.automatic</code></li> <li><i>Default</i> : <code>false</code></li> </ul>
<a href="#">bindServices</a>	boolean	Link in service provider modules and their dependencies. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.bindSe</code></li> <li><i>Default</i> : <code>false</code></li> </ul>
<a href="#">compress</a>	String	The compress level of the resulting image compression, 1=constant string sharing, 2 <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.compre</code></li> </ul>
<a href="#">configurationDirectory</a>	File	A directory containing user-editable config that will be copied to the resulting image. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.configurationDirectory</code></li> <li><i>Default</i> : <code>\${project.basedir}/src/main,</code></li> </ul>
<a href="#">copyright</a>	String	The application copyright. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.app.copyright</code></li> </ul>
<a href="#">description</a>	String	The description of the application. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.app.descriptio</code></li> <li><i>Default</i> : <code>\${project.description}</code></li> </ul>
<a href="#">environment</a>	Map	The container's environment variables.
<a href="#">excludeArtifactIds</a>	String	Comma separated list of Artifact names to <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.exclud</code></li> </ul>

<a href="#">excludeClassifiers</a>	String	Comma Separated list of Classifiers to exclude. An Empty String indicates don't exclude anything (default). • <i>User property</i> : excludeClassifiers
<a href="#">excludeGroupIds</a>	String	Comma separated list of GroupId Names to exclude. An Empty String indicates include everything (default). • <i>User property</i> : invernno.image.excludeGroupIds
<a href="#">excludeScope</a>	String	Scope to exclude. An Empty string indicates include everything (default). • <i>User property</i> : invernno.image.excludeScope
<a href="#">ignoreSigningInformation</a>	boolean	Suppress a fatal error when signed modules are not found or linked in the image. • <i>User property</i> : invernno.image.ignoreSigningInformation • <i>Default</i> : false
<a href="#">imageFormat</a>	ImageFormat	The format of the container image. • <i>User property</i> : invernno.container.imageFormat • <i>Default</i> : Docker
<a href="#">includeArtifactIds</a>	String	Comma separated list of Artifact names to include. An Empty String indicates include everything (default). • <i>User property</i> : invernno.image.includeArtifactIds
<a href="#">includeClassifiers</a>	String	Comma Separated list of Classifiers to include. An Empty String indicates include everything (default). • <i>User property</i> : invernno.image.includeClassifiers
<a href="#">includeGroupIds</a>	String	Comma separated list of GroupIds to include. An Empty String indicates include everything (default). • <i>User property</i> : invernno.image.includeGroupIds
<a href="#">includeScope</a>	String	Scope to include. An Empty string indicates include everything (default). The scopes being interpreted are as Maven sees them, not as specified in the pom file. • <i>User property</i> : invernno.image.includeScope
<a href="#">installDirectory</a>	String	Absolute path of the installation directory for the application on OS X or Linux. Relative sub-

		<p>installation location of the application such as 'Program Files' or 'AppData' on Windows.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.installDir</code></li> </ul>
<a href="#">jmodsOverrideDirectory</a>	File	<p>A directory containing module descriptors that will be used to modularize unnamed dependency module descriptors that will override the ones that are otherwise generated.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.jmodsOverrideDirectory</code></li> <li>• <i>Default</i> : <code>\${project.basedir}/src/jmodsOverrideDirectory</code></li> </ul>
<a href="#">labels</a>	Map	The labels to apply to the container image.
<a href="#">launchers</a>	List	A list of extra launchers to include in the resulting application.
<a href="#">legalDirectory</a>	File	<p>A directory containing legal notices that will be included in the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.legalDirectory</code></li> <li>• <i>Default</i> : <code>\${project.basedir}/src/main/legal</code></li> </ul>
<a href="#">licenseFile</a>	File	<p>The path to the application license file.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.licenseFile</code></li> <li>• <i>Default</i> : <code>\${project.basedir}/LICENSE</code></li> </ul>
<a href="#">linuxConfiguration</a>	LinuxConfiguration	Linux specific configuration.
<a href="#">macOSConfiguration</a>	MacOSConfiguration	MacOS specific configuration.
<a href="#">manDirectory</a>	File	<p>A directory containing man pages that will be included in the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.manDirectory</code></li> <li>• <i>Default</i> : <code>\${project.basedir}/src/main/man</code></li> </ul>
<a href="#">overWriteIfNewer</a>	boolean	<p>Overwrite dependencies that don't exist on the target platform than the source.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.overWriteIfNewer</code></li> <li>• <i>Default</i> : <code>true</code></li> </ul>
<a href="#">ports</a>	Set	The ports exposed by the container at runtime as: <code>port_number [ '/' udp/tcp ]</code>

<a href="#">projectMainClass</a>	String	The main class in the project module to use when building the project JMOD package. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.runtime.projectMainClass</code></li> </ul>
<a href="#">registry</a>	String	The registry part of the target image reference as: <code>\${registry}/\${repository}/\${name}:\${project.version}</code> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.container.registry</code></li> </ul>
<a href="#">repository</a>	String	The repository part of the target image reference defined as: <code>\${registry}/\${repository}/\${name}:\${project.version}</code> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.container.repository</code></li> </ul>
<a href="#">resolveProjectMainClass</a>	boolean	Resolve the project main class when not specified explicitly. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.runtime.projectMainClass</code></li> <li>• <i>Default</i> : <code>false</code></li> </ul>
<a href="#">resourceDirectory</a>	File	The path to resources that override result image resources. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.resourceDirectory</code></li> </ul>
<a href="#">skip</a>	boolean	Skips the generation of the application. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.skip</code></li> </ul>
<a href="#">stripDebug</a>	boolean	Strip debug information from the resulting image. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.stripDebug</code></li> <li>• <i>Default</i> : <code>true</code></li> </ul>
<a href="#">stripNativeCommands</a>	boolean	Strip native command (eg. java...) from the image. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.image.stripNativeCommands</code></li> <li>• <i>Default</i> : <code>true</code></li> </ul>
<a href="#">user</a>	String	The user and group used to run the container as: <code>user / uid [ ':' group / gid ]</code>
<a href="#">vendor</a>	String	The application vendor. <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.app.vendor</code></li> <li>• <i>Default</i> : <code>\${project.organization.name}</code></li> </ul>

<a href="#">verbose</a>	boolean	Enables verbose logging. <ul style="list-style-type: none"><li>• <i>User property</i> : inverno.verbose</li><li>• <i>Default</i> : false</li></ul>
<a href="#">vm</a>	String	Select the HotSpot VM in the output image 'client' / 'server' / 'minimal' / 'all' <ul style="list-style-type: none"><li>• <i>User property</i> : inverno.image.vm</li></ul>
<a href="#">volumes</a>	Set	The container's mount points.
<a href="#">windowsConfiguration</a>	WindowsConfiguration	Windows specific configuration.



## Parameter details

### <addModules>

The modules to add to the resulting image.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.addModules

### <addOptions>

The options to prepend before any other options when invoking the JVM in the resulting image.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.addOptions

### <attach>

Attach the resulting image archives to the project to install them in the local Maven repository and deploy them to remote repositories.

- **Type:** boolean
- **Required:** yes
- **User property:** inverno.image.attach
- **Default:** true

## <automaticLaunchers>

Enables the automatic generation of launchers based on the main classes extracted from the application module. If enabled, a launcher is generated for all main classes other than the main launcher.

- **Type:** boolean
- **Required:** no
- **User property:** `inverno.app.automaticLaunchers`
- **Default:** false

## <bindServices>

Link in service provider modules and their dependencies.

- **Type:** boolean
- **Required:** no
- **User property:** `inverno.image.bindServices`
- **Default:** false

## <compress>

The compress level of the resulting image: 0=No compression, 1=constant string sharing, 2=ZIP.

- **Type:** `java.lang.String`
- **Required:** no
- **User property:** `inverno.image.compress`

## <configurationDirectory>

A directory containing user-editable configuration files that will be copied to the resulting image.

- **Type:** `java.io.File`
- **Required:** no
- **User property:** `inverno.image.configurationDirectory`
- **Default:** `${project.basedir}/src/main/conf/`

## <copyright>

The application copyright.

- **Type:** `java.lang.String`
- **Required:** no
- **User property:** `inverno.app.copyright`

## <description>

The description of the application.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.app.description
- **Default:** \${project.description}

## <environment>

The container's environment variables.

- **Type:** java.util.Map
- **Required:** no

## <excludeArtifactIds>

Comma separated list of Artifact names to exclude.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.excludeArtifactIds

## <excludeClassifiers>

Comma Separated list of Classifiers to exclude. Empty String indicates don't exclude anything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** excludeClassifiers

## <excludeGroupIds>

Comma separated list of GroupId Names to exclude.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.excludeGroupIds

## <excludeScope>

Scope to exclude. An Empty string indicates no scopes (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.excludeScope



## <executable>

The executable in the application image to use as image entry point. The specified name should correspond to a declared application image launchers or the project artifact id if no launcher was specified.

- **Type:** java.lang.String
- **Required:** yes
- **User property:** inverno.app.executable
- **Default:** \${project.artifactId}

## <formats>

A list of archive formats to generate (eg. zip, tar.gz...)

- **Type:** java.util.Set
- **Required:** yes
- **Default:** zip

## <from>

The base container image.

- **Type:** java.lang.String
- **Required:** yes
- **User property:** inverno.container.from
- **Default:** debian:buster-slim

## <ignoreSigningInformation>

Suppress a fatal error when signed modular JARs are linked in the image.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.image.ignoreSigningInformation
- **Default:** false

## <imageFormat>

The format of the container image.

- **Type:** com.google.cloud.tools.jib.api.buildplan.ImageFormat
- **Required:** no
- **User property:** inverno.container.imageFormat
- **Default:** Docker

### <includeArtifactIds>

Comma separated list of Artifact names to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.includeArtifactIds

### <includeClassifiers>

Comma Separated list of Classifiers to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.includeClassifiers

### <includeGroupIds>

Comma separated list of GroupIds to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.includeGroupIds

### <includeScope>

Scope to include. An Empty string indicates all scopes (default). The scopes being interpreted are the scopes as Maven sees them, not as specified in the pom. In summary:

- runtime scope gives runtime and compile dependencies,
- compile scope gives compile, provided, and system dependencies,
- test (default) scope gives all dependencies,
- provided scope just gives provided dependencies,
- system scope just gives system dependencies.
- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.includeScope

## <installDirectory>

Absolute path of the installation directory of the application on OS X or Linux. Relative sub-path of the installation location of the application such as 'Program Files' or 'AppData' on Windows.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.app.installDirectory

## <jmodsOverrideDirectory>

A directory containing module descriptors to use to modularize unnamed dependency modules and which override the ones that are otherwise generated.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.image.jmodsOverrideDirectory
- **Default:** \${project.basedir}/src/jmods/

## <labels>

The labels to apply to the container image.

- **Type:** java.util.Map
- **Required:** no

## <launchers>

A list of extra launchers to include in the resulting application.

- **Type:** java.util.List
- **Required:** no

## <legalDirectory>

A directory containing legal notices that will be copied to the resulting image.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.image.legalDirectory
- **Default:** \${project.basedir}/src/main/legal/

## <licenseFile>

The path to the application license file.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.app.licenseFile
- **Default:** \${project.basedir}/LICENSE

## <linuxConfiguration>

Linux specific configuration.

- **Type:** io.inverno.tool.maven.internal.task.CreateProjectApplicationTask\$LinuxConfiguration
- **Required:** no

## <macOSConfiguration>

MacOS specific configuration.

- **Type:**  
io.inverno.tool.maven.internal.task.CreateProjectApplicationTask\$MacOSConfiguration
- **Required:** no

## <manDirectory>

A directory containing man pages that will be copied to the resulting image.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.image.manDirectory
- **Default:** \${project.basedir}/src/main/man/

## <overWritelfNewer>

Overwrite dependencies that don't exist or are older than the source.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.image.overWritelfNewer
- **Default:** true

## <ports>

The ports exposed by the container at runtime defined as: port\_number [ '/' udp/tcp ]

- **Type:** java.util.Set
- **Required:** no

## <projectMainClass>

The main class in the project module to use when building the project JMOD package.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.runtime.projectMainClass

## <registry>

The registry part of the target image reference defined as:  
`${registry}/${repository}/${name}:${project.version}`

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.container.registry

## <repository>

The repository part of the target image reference defined as:  
`${registry}/${repository}/${name}:${project.version}`

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.container.repository

## <resolveProjectMainClass>

Resolve the project main class when not specified explicitly.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.runtime.projectMainClass
- **Default:** false

## <resourceDirectory>

The path to resources that override resulting package resources.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.app.resourceDirectory

## <skip>

Skips the generation of the application.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.app.skip

## <stripDebug>

Strip debug information from the resulting image.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.image.stripDebug

- **Default:** true

## <stripNativeCommands>

Strip native command (eg. java...) from the resulting image.

- **Type:** boolean
- **Required:** no
- **User property:** invernno.image.stripNativeCommands
- **Default:** true

## <user>

The user and group used to run the container defined as: user / uid [ ':' group / gid ]

- **Type:** java.lang.String
- **Required:** no

## <vendor>

The application vendor.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.app.vendor
- **Default:** \${project.organization.name}

## <verbose>

Enables verbose logging.

- **Type:** boolean
- **Required:** no
- **User property:** invernno.verbose
- **Default:** false

## <vm>

Select the HotSpot VM in the output image defined as: 'client' / 'server' / 'minimal' / 'all'

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.vm

## <volumes>

The container's mount points.

- **Type:** java.util.Set
- **Required:** no

## <windowsConfiguration>

Windows specific configuration.

- **Type:**  
io.inverno.tool.maven.internal.task.CreateProjectApplicationTask\$WindowsConfiguration
- **Required:** no

# inverno:build-runtime

### Full name:

io.inverno.tool:inverno-maven-plugin:1.3.1:build-runtime

### Description:

Builds the project runtime image.

A runtime image is a custom Java runtime containing a set of modules and their dependencies.

### Attributes:

- Requires a Maven project to be executed.
- Requires dependency resolution of artifacts in scope: compile+runtime.
- Requires dependency collection of artifacts in scope: compile+runtime.
- Since version: 1.0.
- Binds by default to the lifecycle phase: package.

## Required parameters

Name	Type	Description
<a href="#">attach</a>	boolean	Attach the resulting image archives to the project to install them in the local Maven repository and deploy them to remote repositories. <ul style="list-style-type: none"><li>• <i>User property</i> : inverno.image.attach</li><li>• <i>Default</i> : true</li></ul>
<a href="#">formats</a>	Set	A list of archive formats to generate (eg. zip, tar.gz...) <ul style="list-style-type: none"><li>• <i>Default</i> : zip</li></ul>

## Optional parameters



Name	Type	Description
<a href="#">addModules</a>	String	The modules to add to the resulting image. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.addModules</code></li> </ul>
<a href="#">addOptions</a>	String	The options to prepend before any other options when invoking the JVM in the resulting image. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.addOptions</code></li> </ul>
<a href="#">bindServices</a>	boolean	Link in service provider modules and their dependencies. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.bindServices</code></li> <li><i>Default</i> : <code>false</code></li> </ul>
<a href="#">compress</a>	String	The compress level of the resulting image: 0=No compression, 1=constant string sharing, 2=ZIP. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.compress</code></li> </ul>
<a href="#">configurationDirectory</a>	File	A directory containing user-editable configuration files that will be copied to the resulting image. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.configurationDirectory</code></li> <li><i>Default</i> : <code>\${project.basedir}/src/main/conf/</code></li> </ul>
<a href="#">excludeArtifactIds</a>	String	Comma separated list of Artifact names to exclude. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.excludeArtifactIds</code></li> </ul>
<a href="#">excludeClassifiers</a>	String	Comma Separated list of Classifiers to exclude. Empty String indicates don't exclude anything (default). <ul style="list-style-type: none"> <li><i>User property</i> : <code>excludeClassifiers</code></li> </ul>
<a href="#">excludeGroupIds</a>	String	Comma separated list of GroupId Names to exclude. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.excludeGroupIds</code></li> </ul>
<a href="#">excludeScope</a>	String	Scope to exclude. An Empty string indicates no scopes (default). <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.excludeScope</code></li> </ul>
<a href="#">ignoreSigningInformation</a>	boolean	Suppress a fatal error when signed modular JARs are linked in the image. <ul style="list-style-type: none"> <li><i>User property</i> : <code>inverno.image.ignoreSigningInformation</code></li> </ul>

		<ul style="list-style-type: none"> <li>• <i>Default</i> : false</li> </ul>
<a href="#">includeArtifactIds</a>	String	<p>Comma separated list of Artifact names to include. Empty String indicates include everything (default).</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.includeArtifactIds</li> </ul>
<a href="#">includeClassifiers</a>	String	<p>Comma Separated list of Classifiers to include. Empty String indicates include everything (default).</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.includeClassifiers</li> </ul>
<a href="#">includeGroupIds</a>	String	<p>Comma separated list of GroupIds to include. Empty String indicates include everything (default).</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.includeGroupIds</li> </ul>
<a href="#">includeScope</a>	String	<p>Scope to include. An Empty string indicates all scopes (default). The scopes being interpreted are the scopes as Maven sees them, not as specified in the pom. In summary:</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.includeScope</li> </ul>
<a href="#">jmodsOverrideDirectory</a>	File	<p>A directory containing module descriptors to use to modularize unnamed dependency modules and which override the ones that are otherwise generated.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.jmodsOverrideDirectory</li> <li>• <i>Default</i> : \${project.basedir}/src/jmods/</li> </ul>
<a href="#">launchers</a>	List	<p>A list of launchers to include in the resulting runtime.</p>
<a href="#">legalDirectory</a>	File	<p>A directory containing legal notices that will be copied to the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.legalDirectory</li> <li>• <i>Default</i> : \${project.basedir}/src/main/legal/</li> </ul>
<a href="#">manDirectory</a>	File	<p>A directory containing man pages that will be copied to the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.manDirectory</li> <li>• <i>Default</i> : \${project.basedir}/src/main/man/</li> </ul>
<a href="#">overWritelfNewer</a>	boolean	<p>Overwrite dependencies that don't exist or are older than the source.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.overWritelfNewer</li> </ul>

		<ul style="list-style-type: none"> <li>• <i>Default</i> : true</li> </ul>
<a href="#">projectMainClass</a>	String	<p>The main class in the project module to use when building the project JMOD package.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.runtime.projectMainClass</li> </ul>
<a href="#">resolveProjectMainClass</a>	boolean	<p>Resolve the project main class when not specified explicitly.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.runtime.projectMainClass</li> <li>• <i>Default</i> : false</li> </ul>
<a href="#">skip</a>	boolean	<p>Skips the generation of the runtime.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.runtime.skip</li> </ul>
<a href="#">stripDebug</a>	boolean	<p>Strip debug information from the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.stripDebug</li> <li>• <i>Default</i> : true</li> </ul>
<a href="#">stripNativeCommands</a>	boolean	<p>Strip native command (eg. java...) from the resulting image.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.stripNativeCommands</li> <li>• <i>Default</i> : true</li> </ul>
<a href="#">verbose</a>	boolean	<p>Enables verbose logging.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.verbose</li> <li>• <i>Default</i> : false</li> </ul>
<a href="#">vm</a>	String	<p>Select the HotSpot VM in the output image defined as: 'client' / 'server' / 'minimal' / 'all'</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.image.vm</li> </ul>

## Parameter details

### <addModules>

The modules to add to the resulting image.

- **Type**: java.lang.String
- **Required**: no
- **User property**: inverno.image.addModules

## <addOptions>

The options to prepend before any other options when invoking the JVM in the resulting image.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.addOptions

## <attach>

Attach the resulting image archives to the project to install them in the local Maven repository and deploy them to remote repositories.

- **Type:** boolean
- **Required:** yes
- **User property:** inverno.image.attach
- **Default:** true

## <bindServices>

Link in service provider modules and their dependencies.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.image.bindServices
- **Default:** false

## <compress>

The compress level of the resulting image: 0=No compression, 1=constant string sharing, 2=ZIP.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.compress

## <configurationDirectory>

A directory containing user-editable configuration files that will be copied to the resulting image.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.image.configurationDirectory
- **Default:** \${project.basedir}/src/main/conf/

### <excludeArtifactIds>

Comma separated list of Artifact names to exclude.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.excludeArtifactIds

### <excludeClassifiers>

Comma Separated list of Classifiers to exclude. Empty String indicates don't exclude anything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** excludeClassifiers

### <excludeGroupIds>

Comma separated list of GroupId Names to exclude.

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.excludeGroupIds

### <excludeScope>

Scope to exclude. An Empty string indicates no scopes (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.excludeScope

### <formats>

A list of archive formats to generate (eg. zip, tar.gz...)

- **Type:** java.util.Set
- **Required:** yes
- **Default:** zip

### <ignoreSigningInformation>

Suppress a fatal error when signed modular JARs are linked in the image.

- **Type:** boolean
- **Required:** no
- **User property:** invernno.image.ignoreSigningInformation
- **Default:** false

### <includeArtifactIds>

Comma separated list of Artifact names to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.includeArtifactIds

### <includeClassifiers>

Comma Separated list of Classifiers to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.includeClassifiers

### <includeGroupIds>

Comma separated list of GroupIds to include. Empty String indicates include everything (default).

- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.includeGroupIds

### <includeScope>

Scope to include. An Empty string indicates all scopes (default). The scopes being interpreted are the scopes as Maven sees them, not as specified in the pom. In summary:

- runtime scope gives runtime and compile dependencies,
- compile scope gives compile, provided, and system dependencies,
- test (default) scope gives all dependencies,
- provided scope just gives provided dependencies,
- system scope just gives system dependencies.
- **Type:** java.lang.String
- **Required:** no
- **User property:** invernno.image.includeScope

## <jmodsOverrideDirectory>

A directory containing module descriptors to use to modularize unnamed dependency modules and which override the ones that are otherwise generated.

- **Type:** java.io.File
- **Required:** no
- **User property:** invernno.image.jmodsOverrideDirectory
- **Default:** \${project.basedir}/src/jmods/

## <launchers>

A list of launchers to include in the resulting runtime.

- **Type:** java.util.List
- **Required:** no

## <legalDirectory>

A directory containing legal notices that will be copied to the resulting image.

- **Type:** java.io.File
- **Required:** no
- **User property:** invernno.image.legalDirectory
- **Default:** \${project.basedir}/src/main/legal/

## <manDirectory>

A directory containing man pages that will be copied to the resulting image.

- **Type:** java.io.File
- **Required:** no
- **User property:** invernno.image.manDirectory
- **Default:** \${project.basedir}/src/main/man/

## <overWritelfNewer>

Overwrite dependencies that don't exist or are older than the source.

- **Type:** boolean
- **Required:** no
- **User property:** invernno.image.overWritelfNewer
- **Default:** true

## <projectMainClass>

The main class in the project module to use when building the project JMOD package.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.runtime.projectMainClass

## <resolveProjectMainClass>

Resolve the project main class when not specified explicitly.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.runtime.projectMainClass
- **Default:** false

## <skip>

Skips the generation of the runtime.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.runtime.skip

## <stripDebug>

Strip debug information from the resulting image.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.image.stripDebug
- **Default:** true

## <stripNativeCommands>

Strip native command (eg. java...) from the resulting image.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.image.stripNativeCommands
- **Default:** true

## <verbose>

Enables verbose logging.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.verbose



- **Default:** false

<vm>

Select the HotSpot VM in the output image defined as: 'client' / 'server' / 'minimal' / 'all'

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.image.vm

## inverno:help

### Full name:

io.inverno.tool:inverno-maven-plugin:1.3.1:help

### Description:

Display help information on inverno-maven-plugin. Call `mvn inverno:help -Ddetail=true -Dgoal=<goal-name>` to display parameter details.

### Attributes:

## Optional parameters

Name	Type	Description
<a href="#">detail</a>	boolean	If true, display all settable properties for each goal. <ul style="list-style-type: none"> <li>• <i>User property</i> : detail</li> <li>• <i>Default</i> : false</li> </ul>
<a href="#">goal</a>	String	The name of the goal for which to show help. If unspecified, all goals will be displayed. <ul style="list-style-type: none"> <li>• <i>User property</i> : goal</li> </ul>
<a href="#">indentSize</a>	int	The number of spaces per indentation level, should be positive. <ul style="list-style-type: none"> <li>• <i>User property</i> : indentSize</li> <li>• <i>Default</i> : 2</li> </ul>
<a href="#">lineLength</a>	int	The maximum length of a display line, should be positive. <ul style="list-style-type: none"> <li>• <i>User property</i> : lineLength</li> <li>• <i>Default</i> : 80</li> </ul>

## Parameter details

### <detail>

If true, display all settable properties for each goal.

- **Type:** boolean
- **Required:** no
- **User property:** detail
- **Default:** false

### <goal>

The name of the goal for which to show help. If unspecified, all goals will be displayed.

- **Type:** java.lang.String
- **Required:** no
- **User property:** goal

### <indentSize>

The number of spaces per indentation level, should be positive.

- **Type:** int
- **Required:** no
- **User property:** indentSize
- **Default:** 2

### <lineLength>

The maximum length of a display line, should be positive.

- **Type:** int
- **Required:** no
- **User property:** lineLength
- **Default:** 80

## inverno:run

### Full name:

io.inverno.tool:inverno-maven-plugin:1.3.1:run

### Description:

Runs the project application.

### Attributes:

- Requires a Maven project to be executed.

- Requires dependency resolution of artifacts in scope: compile+runtime.
- Requires dependency collection of artifacts in scope: compile+runtime.
- Since version: 1.0.
- Binds by default to the lifecycle phase: validate.

## Optional parameters

Name	Type	Description
<a href="#">addUnnamedModules</a>	boolean	Adds the unnamed modules when executing the application. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.exec.addUnnamedModules</li> <li>• <i>Default</i> : true</li> </ul>
<a href="#">arguments</a>	String	The arguments to pass to the application.
<a href="#">commandLineArguments</a>	String	The command line arguments to pass to the application. This parameter overrides AbstractExecMojo.arguments when specified. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.run.arguments</li> </ul>
<a href="#">configurationDirectory</a>	File	A directory containing user-editable configuration files that will be copied to the image to execute. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.exec.configurationDirectory</li> <li>• <i>Default</i> : \${project.basedir}/src/main/conf/</li> </ul>
<a href="#">jmodsOverrideDirectory</a>	File	A directory containing module descriptors to use to modularize unnamed dependency modules and which override the ones that are otherwise generated. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.exec.jmodsOverrideDirectory</li> <li>• <i>Default</i> : \${project.basedir}/src/jmods/</li> </ul>
<a href="#">mainClass</a>	String	The main class to use to run the application. If not specified, a main class is automatically selected. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.exec.mainClass</li> </ul>
<a href="#">overWritelfNewer</a>	boolean	Overwrites dependencies that don't exist or are older than the source. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.exec.overWritelfNewer</li> <li>• <i>Default</i> : true</li> </ul>
<a href="#">skip</a>	boolean	Skips the execution. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.exec.skip</li> </ul>
<a href="#">verbose</a>	boolean	Enables verbose logging. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.verbose</li> <li>• <i>Default</i> : false</li> </ul>

<a href="#">vmOptions</a>	String	The VM options to use when executing the application. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.exec.vmOptions</li> <li>• <i>Default</i> : - Dorg.apache.logging.log4j.simplelog.level=INFO - Dorg.apache.logging.log4j.level=INFO</li> </ul>
<a href="#">workingDirectory</a>	File	The working directory of the application. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.run.workingDirectory</li> <li>• <i>Default</i> : \${project.build.directory}/maven-inverno/working</li> </ul>

## Parameter details

### <addUnnamedModules>

Adds the unnamed modules when executing the application.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.exec.addUnnamedModules
- **Default:** true

### <arguments>

The arguments to pass to the application.

- **Type:** java.lang.String
- **Required:** no

### <commandLineArguments>

The command line arguments to pass to the application. This parameter overrides AbstractExecMojo.arguments when specified.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.run.arguments

### <configurationDirectory>

A directory containing user-editable configuration files that will be copied to the image to execute.

- **Type:** java.io.File

- **Required:** no
- **User property:** `inverno.exec.configurationDirectory`
- **Default:** `${project.basedir}/src/main/conf/`

### <jmodsOverrideDirectory>

A directory containing module descriptors to use to modularize unnamed dependency modules and which override the ones that are otherwise generated.

- **Type:** `java.io.File`
- **Required:** no
- **User property:** `inverno.exec.jmodsOverrideDirectory`
- **Default:** `${project.basedir}/src/jmods/`

### <mainClass>

The main class to use to run the application. If not specified, a main class is automatically selected.

- **Type:** `java.lang.String`
- **Required:** no
- **User property:** `inverno.exec.mainClass`

### <overWriteIfNewer>

Overwrites dependencies that don't exist or are older than the source.

- **Type:** `boolean`
- **Required:** no
- **User property:** `inverno.exec.overWriteIfNewer`
- **Default:** `true`

### <skip>

Skips the execution.

- **Type:** `boolean`
- **Required:** no
- **User property:** `inverno.exec.skip`

### <verbose>

Enables verbose logging.

- **Type:** `boolean`
- **Required:** no
- **User property:** `inverno.verbose`
- **Default:** `false`

## <vmOptions>

The VM options to use when executing the application.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.exec.vmOptions
- **Default:** -Dorg.apache.logging.log4j.simplelog.level=INFO -Dorg.apache.logging.log4j.level=INFO

## <workingDirectory>

The working directory of the application.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.run.workingDirectory
- **Default:** \${project.build.directory}/maven-inverno/working

## inverno:start

### Full name:

io.inverno.tool:inverno-maven-plugin:1.3.1:start

### Description:

Starts the project application without blocking the Maven build.

This goal is used together with the stop goal in the pre-integration-test and post-integration-test phases to run integration tests.

### Attributes:

- Requires a Maven project to be executed.
- Requires dependency resolution of artifacts in scope: compile+runtime.
- Requires dependency collection of artifacts in scope: compile+runtime.
- Since version: 1.0.
- Binds by default to the lifecycle phase: pre-integration-test.

## Optional parameters

Name	Type	Description
<a href="#">addUnnamedModules</a>	boolean	Adds the unnamed modules when executing the application. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.exec.addUnnamedModules</li> <li>• <i>Default</i> : true</li> </ul>
<a href="#">arguments</a>	String	The arguments to pass to the application.
<a href="#">configurationDirectory</a>	File	A directory containing user-editable configuration files that will be copied to the image to execute. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.exec.configurationDirectory</li> <li>• <i>Default</i> : \${project.basedir}/src/main/conf/</li> </ul>
<a href="#">jmodsOverrideDirectory</a>	File	A directory containing module descriptors to use to modularize unnamed dependency modules and which override the ones that are otherwise generated. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.exec.jmodsOverrideDirectory</li> <li>• <i>Default</i> : \${project.basedir}/src/jmods/</li> </ul>
<a href="#">mainClass</a>	String	The main class to use to run the application. If not specified, a main class is automatically selected. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.exec.mainClass</li> </ul>
<a href="#">overWritelfNewer</a>	boolean	Overwrites dependencies that don't exist or are older than the source. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.exec.overWritelfNewer</li> <li>• <i>Default</i> : true</li> </ul>
<a href="#">skip</a>	boolean	Skips the execution. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.exec.skip</li> </ul>
<a href="#">timeout</a>	long	The amount of time in milliseconds to wait for the application to start. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.start.timeout</li> <li>• <i>Default</i> : 60000</li> </ul>
<a href="#">verbose</a>	boolean	Enables verbose logging. <ul style="list-style-type: none"> <li>• <i>User property</i> : inverno.verbose</li> <li>• <i>Default</i> : false</li> </ul>



<a href="#">vmOptions</a>	String	<p>The VM options to use when executing the application.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.exec.vmOptions</code></li> <li>• <i>Default</i> : -  <code>Dorg.apache.logging.log4j.simplelog.level=INFO</code> -  <code>Dorg.apache.logging.log4j.level=INFO</code></li> </ul>
<a href="#">workingDirectory</a>	File	<p>The working directory of the application.</p> <ul style="list-style-type: none"> <li>• <i>User property</i> : <code>inverno.run.workingDirectory</code></li> <li>• <i>Default</i> : <code>\${project.build.directory}/maven-inverno/working</code></li> </ul>

## Parameter details

### <addUnnamedModules>

Adds the unnamed modules when executing the application.

- **Type:** `boolean`
- **Required:** no
- **User property:** `inverno.exec.addUnnamedModules`
- **Default:** `true`

### <arguments>

The arguments to pass to the application.

- **Type:** `java.lang.String`
- **Required:** no

### <configurationDirectory>

A directory containing user-editable configuration files that will be copied to the image to execute.

- **Type:** `java.io.File`
- **Required:** no
- **User property:** `inverno.exec.configurationDirectory`
- **Default:** `${project.basedir}/src/main/conf/`

### <jmodsOverrideDirectory>

A directory containing module descriptors to use to modularize unnamed dependency modules and which override the ones that are otherwise generated.

- **Type:** `java.io.File`
- **Required:** no

- **User property:** `inverno.exec.jmodsOverrideDirectory`
- **Default:** `${project.basedir}/src/jmods/`

### <mainClass>

The main class to use to run the application. If not specified, a main class is automatically selected.

- **Type:** `java.lang.String`
- **Required:** no
- **User property:** `inverno.exec.mainClass`

### <overWriteIfNewer>

Overwrites dependencies that don't exist or are older than the source.

- **Type:** `boolean`
- **Required:** no
- **User property:** `inverno.exec.overWriteIfNewer`
- **Default:** `true`

### <skip>

Skips the execution.

- **Type:** `boolean`
- **Required:** no
- **User property:** `inverno.exec.skip`

### <timeout>

The amount of time in milliseconds to wait for the application to start.

- **Type:** `long`
- **Required:** no
- **User property:** `inverno.start.timeout`
- **Default:** `60000`

### <verbose>

Enables verbose logging.

- **Type:** `boolean`
- **Required:** no
- **User property:** `inverno.verbose`
- **Default:** `false`

## <vmOptions>

The VM options to use when executing the application.

- **Type:** java.lang.String
- **Required:** no
- **User property:** inverno.exec.vmOptions
- **Default:** -Dorg.apache.logging.log4j.simplelog.level=INFO -Dorg.apache.logging.log4j.level=INFO

## <workingDirectory>

The working directory of the application.

- **Type:** java.io.File
- **Required:** no
- **User property:** inverno.run.workingDirectory
- **Default:** \${project.build.directory}/maven-inverno/working

# inverno:stop

### Full name:

io.inverno.tool:inverno-maven-plugin:1.3.1:stop

### Description:

Stops the project application that has been previously started using the start goal.

This goal is used together with the start goal in the pre-integration-test and post-integration-test phases to run integration tests.

### Attributes:

- Requires a Maven project to be executed.
- Since version: 1.0.
- Binds by default to the lifecycle phase: post-integration-test.

## Optional parameters

Name	Type	Description
<a href="#">skip</a>	boolean	Skips the execution. <ul style="list-style-type: none"> <li><i>User property</i> : inverno.stop.skip</li> </ul>
<a href="#">timeout</a>	long	The amount of time in milliseconds to wait for the application to stop. <ul style="list-style-type: none"> <li><i>User property</i> : inverno.stop.timeout</li> <li><i>Default</i> : 60000</li> </ul>
<a href="#">verbose</a>	boolean	Enables verbose logging. <ul style="list-style-type: none"> <li><i>User property</i> : inverno.verbose</li> <li><i>Default</i> : false</li> </ul>

## Parameter details

### <skip>

Skips the execution.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.stop.skip

### <timeout>

The amount of time in milliseconds to wait for the application to stop.

- **Type:** long
- **Required:** no
- **User property:** inverno.stop.timeout
- **Default:** 60000

### <verbose>

Enables verbose logging.

- **Type:** boolean
- **Required:** no
- **User property:** inverno.verbose
- **Default:** false



## Inverno OSS Parent

---



The Inverno OSS parent POM provides OSS dependencies and plugin management to Inverno components and applications.

### Dependencies

GroupId	ArtifactId	Version
com.aayushatharva.brotli4j	brotli4j	1.7.1
com.aayushatharva.brotli4j	native-linux-x86_64	1.7.1
com.aayushatharva.brotli4j	native-osx-x86_64	1.7.1
com.aayushatharva.brotli4j	native-windows-x86_64	1.7.1
com.fasterxml.jackson.core	jackson-core	2.13.3
com.fasterxml.jackson.core	jackson-databind	2.13.3
com.fasterxml.jackson.datatype	jackson-datatype-jsr310	2.13.3
com.google.cloud.tools	jib-core	0.21.0
commons-codec	commons-codec	1.15
io.lettuce	lettuce-core	6.2.0.RELEASE
io.netty	netty-all	4.1.79.Final
io.netty	netty-buffer	4.1.79.Final
io.netty	netty-codec-http	4.1.79.Final
io.netty	netty-codec-http2	4.1.79.Final
io.netty	netty-common	4.1.79.Final
io.netty	netty-handler	4.1.79.Final
io.netty	netty-handler-proxy	4.1.79.Final
io.netty	netty-resolver	4.1.79.Final
io.netty	netty-resolver-dns	4.1.79.Final
io.netty	netty-tcnative-boringssl-static	2.0.54.Final
io.netty	netty-transport	4.1.79.Final
io.netty	netty-transport-classes-epoll	4.1.79.Final
io.netty	netty-transport-classes-kqueue	4.1.79.Final
io.netty	netty-transport-native-epoll	4.1.79.Final
io.netty	netty-transport-native-epoll	4.1.79.Final

io.netty	netty-transport-native-epoll	4.1.79.Final
io.netty	netty-transport-native-epoll	4.1.79.Final
io.netty	netty-transport-native-kqueue	4.1.79.Final
io.netty	netty-transport-native-kqueue	4.1.79.Final
io.netty.incubator	netty-incubator-transport-classes-io_uring	0.0.14.Final
io.netty.incubator	netty-incubator-transport-native-io_uring	0.0.14.Final
io.netty.incubator	netty-incubator-transport-native-io_uring	0.0.14.Final
io.netty.incubator	netty-incubator-transport-native-io_uring	0.0.14.Final
io.projectreactor	reactor-core	3.4.21
io.vertx	vertx-core	4.3.2
io.vertx	vertx-db2-client	4.3.2
io.vertx	vertx-mssql-client	4.3.2
io.vertx	vertx-mysql-client	4.3.2
io.vertx	vertx-pg-client	4.3.2
io.vertx	vertx-sql-client	4.3.2
net.java.dev.javacc	javacc	7.0.12
org.apache.commons	commons-compress	1.21
org.apache.commons	commons-lang3	3.12.0
org.apache.commons	commons-text	1.9
org.apache.logging.log4j	log4j-api	2.17.2
org.apache.logging.log4j	log4j-core	2.17.2
org.apache.logging.log4j	log4j-jul	2.17.2
org.apache.logging.log4j	log4j-layout-template-json	2.17.2
org.apache.maven	maven-artifact	\${maven.version}

org.apache.maven	maven-compat	\${maven.version}
org.apache.maven	maven-core	\${maven.version}
org.apache.maven	maven-model	\${maven.version}
org.apache.maven	maven-plugin-api	\${maven.version}
org.apache.maven.plugin-tools	maven-plugin-annotations	3.6.4
org.apache.maven.shared	maven-common-artifact-filters	3.3.1
org.bouncycastle	bcjmail-jdk18on	1.71
org.bouncycastle	bcmail-jdk18on	1.71
org.bouncycastle	bcpg-jdk18on	1.71
org.bouncycastle	bcpkix-jdk18on	1.71
org.bouncycastle	bcprov-jdk18on	1.71
org.bouncycastle	bctls-jdk18on	1.71
org.bouncycastle	bcutil-jdk18on	1.71
org.junit	junit-bom	5.9.0
org.mockito	mockito-core	4.6.1
org.ow2.asm	asm	9.3
org.webjars	swagger-ui	4.11.1

## Maven Plugins



<b>GroupId</b>	<b>ArtifactId</b>	<b>Version</b>
org.apache.maven.plugins	maven-antrun-plugin	3.1.0
org.apache.maven.plugins	maven-assembly-plugin	3.4.2
org.apache.maven.plugins	maven-clean-plugin	3.2.0
org.apache.maven.plugins	maven-compiler-plugin	3.10.1
org.apache.maven.plugins	maven-dependency-plugin	3.3.0
org.apache.maven.plugins	maven-deploy-plugin	3.0.0
org.apache.maven.plugins	maven-gpg-plugin	3.0.1
org.apache.maven.plugins	maven-install-plugin	3.0.1
org.apache.maven.plugins	maven-jar-plugin	3.2.2
org.apache.maven.plugins	maven-javadoc-plugin	3.4.0
org.apache.maven.plugins	maven-plugin-plugin	3.6.4
org.apache.maven.plugins	maven-resources-plugin	3.3.0
org.apache.maven.plugins	maven-source-plugin	3.2.1
org.apache.maven.plugins	maven-surefire-plugin	3.0.0-M7
org.codehaus.mojo	exec-maven-plugin	3.1.0
org.javacc.plugin	javacc-maven-plugin	3.0.3
org.sonatype.plugins	nexus-staging-maven-plugin	1.6.13

The Inverno Framework is released under version 2.0 of the [Apache License](#).

Copyright © 2021, The Inverno Framework