



eIDAS-Node Installation and Configuration Guide

Version 1.4.2

Document history

Version	Date	Reason for modification	Modified by
1.0	26/11/2015	Modifications to align with the eIDAS technical specifications.	DIGIT
1.1	09/09/2016	<ul style="list-style-type: none"> Configuration improvements including support for Tomcat 8. Removal of Attribute Provider. Documentation of improvements included in Release 1.1 (see Release notes for eIDAS-Node version 1.1). 	DIGIT
1.2	20/01/2017	<ul style="list-style-type: none"> Configuration and stability improvements. Documentation of improvements included in Release 1.2.0 (see Release notes for eIDAS-Node version 1.2.0). 	DIGIT
1.3	08/06/2017	<ul style="list-style-type: none"> Modifications to align with changes in Technical Specifications version 1.1. Bug fixes and configuration improvements (for details please see the Version 1.3.0 Release Notes). Documentation improvements to remove eIDAS-Nodes error codes and place in separate document <i>eIDAS Error Codes</i>. 	DIGIT
1.4	06/10/2017	<ul style="list-style-type: none"> Restructuring of reference documentation Modifications to remove support for JBoss6. Support WebLogic 12.2 family of servers. Amend filename conventions to change '\' to '/'. 	DIGIT
1.4.1	15/06/2018	Document Version changed to correspond with the release. Reuse of document policy updated.	DIGIT
1.4.2	06/08/2018	Installation manual updated to correspond with the release.	DIGIT

Disclaimer

This document is for informational purposes only and the Commission cannot be held responsible for any use which may be made of the information contained therein. References to legal acts or documentation of the European Union (EU) cannot be perceived as amending legislation in force or other EU documentation.

The document contains a brief overview of technical nature and is not supplementing or amending terms and conditions of any procurement procedure; therefore, no compensation claim can be based on the contents of the present document.

© European Union, 2018

Reuse of this document is authorised provided the source is acknowledged. The Commission's reuse policy is implemented by Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents.

Table of contents

DOCUMENT HISTORY	1
TABLE OF CONTENTS	3
LIST OF FIGURES	5
LIST OF TABLES	6
LIST OF ABBREVIATIONS	7
LIST OF DEFINITIONS	8
REFERENCES	10
1. INTRODUCTION	11
1.1. Document structure	11
1.2. Purpose	11
1.3. Document aims	12
1.4. Other technical reference documentation	12
1.5. eIDAS Technical specifications and software provided	13
1.5.1. Further information	13
2. PRODUCT OVERVIEW	14
2.1. Package	14
2.2. Modules	14
3. PREPARING THE INSTALLATION	17
3.1. Configuring the JVM	17
3.1.1. Oracle Java JCE Unlimited Strength Jurisdiction Policy	17
3.1.2. IBM SDK Java	17
3.2. Configuring the application server	18
3.2.1. Configuring Tomcat 7	18
3.2.2. Configuring Tomcat 8	19
3.2.3. Configuring JBoss AS 7	19
3.2.4. Configuring GlassFish V3	19
3.2.5. Configuring GlassFish V4	19
3.2.6. Configuring WebLogic	20
3.2.7. Configuring WebSphere	20
3.2.8. Configuring WebSphere Liberty Profile	20
3.3. Enabling logging	20
3.3.1. Configuring audit logging	21
3.4. Configuring application server security	25
3.4.1. Security constraints for WebSphere	25
4. CONFIGURING THE SOFTWARE	26
4.1. Configuring the project	26
4.1.1. Setup configuration directories	26
4.1.2. Setting up your Keystore	27
4.1.3. Configuring with Basic Setup	28
4.2. eIDAS-Node configuration files	28

4.2.1.	General purpose parameters	29
4.2.2.	Attribute registry	30
4.2.3.	eIDAS-Node Connector configuration	30
4.2.4.	eIDAS-Node Proxy Service configuration	34
4.2.5.	Additional configuration — Security	38
4.2.6.	Specific properties	45
4.2.7.	Demo Service Provider	45
4.2.8.	Demo Identity Provider	45
5.	BUILDING AND DEPLOYING THE SOFTWARE	46
5.1.	Tomcat/GlassFish server deployment	46
5.2.	JBoss7 Server deployment	48
5.3.	WebLogic Server deployment	49
5.4.	WebSphere Server deployment	50
6.	VERIFYING THE INSTALLATION	52
6.1.	Tomcat 7, 8	52
6.2.	JBoss 7	52
6.3.	GlassFish V3, V4	52
6.3.1.	GlassFish V3	52
6.3.2.	GlassFish V4	52
6.4.	WebLogic	53
6.5.	WebSphere Application Server	53
6.6.	Configuration files	53
7.	ADVANCED CONFIGURATION FOR PRODUCTION ENVIRONMENTS	55
7.1.	Clustering environment	55
7.1.1.	Load balancer	55
7.1.2.	Load balancer with Hazelcast	56
7.2.	Configuring Tomcat	56
7.2.1.	Setting AJP ports	56
7.2.2.	Apache HTTPD	56
7.3.	Set up Hazelcast	57
7.4.	Check your installation	58
7.5.	eIDAS-Node compliance	59
7.6.	eIDAS-Node configuration recommendations check list for production	60
APPENDIX A.	EIDAS LEVELS OF ASSURANCE	61
APPENDIX B.	USER CONSENT	62
APPENDIX C.	HAZELCAST PROPOSED CONFIGURATION	63
C.1	Network configuration	63
C.1.1	Multicast	63
C.1.2	Discovery by TCP/IP Cluster	64
C.1.3	Discovery by AWS (EC2 auto discovery)	64
C.1.4	Eviction	65
APPENDIX D.	INSTALLATION FREQUENTLY ASKED QUESTIONS	67

List of figures

Figure 1: Dependencies between modules	15
Figure 2: Communication flows between modules during authentication of citizens	16
Figure 3: Enabling application security on WebSphere AS	25
Figure 4: Default Hazelcast instance name	42
Figure 5: Default Hazelcast instance provider been	43
Figure 6: Anti-replay cache configuration — Hazelcast — applicationContext.xml ...	43
Figure 7: Correlation map cache configuration — Hazelcast — applicationContext.xml	44
Figure 8: Correlation map cache configuration — Hazelcast — specificApplicationContext.xml	44
Figure 9: Clustering environment — Load balancer	55
Figure 10: Clustering environment — Load Balancer with Hazelcast	56
Figure 11: Apache status page	58
Figure 12: Apache status page (continued)	59
Figure 13: Example Hazelcast multicast declarative configuration	64
Figure 14: Example Hazelcast configuration for TCP/IP discovery	64
Figure 15: Hazelcast eviction policy configuration	66

List of tables

Table 1: List of modules	14
Table 2: Supported servers	18
Table 3: General purpose parameters	29
Table 4: eIDAS-Node Connector and SP validation	31
Table 5: eIDAS-Node Connector dedicated information	33
Table 6: Adding eIDAS-Node Proxy Service to Connector	34
Table 7 : eIDAS-Node Proxy Service setup	34
Table 8: Activating the Proxy Service.....	37
Table 9: Security policies	38
Table 10: Security HTTP header parameters	38
Table 11: Check on certificate security parameter	39
Table 12: Configuring encryption algorithm	40
Table 13: Signature algorithm	41
Table 14: SAML binding parameters	41
Table 15: Parent project build for Tomcat/GlassFish Server deployment.....	46
Table 16: Module-based build for Tomcat/GlassFish Server deployment	47
Table 17: Project build for JBoss7 Server deployment	48
Table 18: Module-based build for JBoss7 Server deployment	48
Table 19: Parent project build for WebLogic Server deployment	49
Table 20: Module-based build for WebLogic Server deployment	49
Table 21: Parent project build for WebSphere Server deployment	50
Table 22: Module-based build for WebSphere Server deployment.....	51
Table 23: eIDAS-Node compliance.....	59

List of abbreviations

The following abbreviations are used within this document.

Abbreviation	Meaning
eIDAS	electronic Identification and Signature. The Regulation (EU) N°910/2014 governs electronic identification and trust services for electronic transactions in the internal market to enable secure and seamless electronic interactions between businesses, citizens and public authorities.
IdP	Identity Provider. An institution that verifies the citizen's identity and issues an electronic ID.
LoA	Level of Assurance (LoA) is a term used to describe the degree of certainty that an individual is who they say they are at the time they present a digital credential.
MW	Middle Ware. Architecture of the integration of eIDs in services, with a direct communication between SP and the citizen's PC without any central server. The term also refers to the piece of software of this architecture that executes on the citizen's PC.
MS	Member State
SAML	Security Assertion Markup Language
SP	Service Provider

List of definitions

The following definitions are used within this document.

Term	Meaning
Audit	A function which seeks to validate that controls are in place, adequate for their purposes, and which reports inadequacies to appropriate levels of management.
Audit log	An audit log is a chronological sequence of audit records, each of which contains evidence directly as a result of the execution of a business process or system function
Audit trail	A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.
Auditable event	An auditable event is generated by any activity in a system that is capable of being audited. An auditable event could lead to the compromise of the integrity and/or security of an information system and therefore indirectly compromise a business process
Basic Setup	The basic configuration and Demo tools provided in a package to setup and run an eIDAS-Node strictly for demo purposes only.
Demo tools	Demo tools comprise the Demo SP and Demo IDP included in the package. These components are not production ready and should not be deployed or used in production environments.
eIDAS-Node	An eIDAS-Node is an application component that can assume two different roles depending on the origin of a received request. See eIDAS-Node Connector and eIDAS-Node Proxy Service.
eIDAS-Node Connector	The eIDAS-Node assumes this role when it is located in the Service Provider's Member State. In a scenario with a Service Provider asking for authentication, the eIDAS-Node Connector receives the authentication request from the Service Provider and forwards it to the eIDAS-Node of the citizen's country. This was formerly known as S-PEPS.

eIDAS-Node Service	Proxy	The eIDAS-Node assumes this role when it is located in the citizen's Member State. The eIDAS-Node Proxy Service receives authentication requests from an eIDAS-Node of another MS (their eIDAS-Node Connector). The eIDAS-Node Proxy-Service also has an interface with the national eID infrastructure and triggers the identification and authentication for a citizen at an identity and/or attribute provider. This was formerly known as C-PEPS.
Encryption		Any procedure used in cryptography to convert plain text into cipher text in order to prevent anyone but the intended recipient from reading that data.
Hashing		The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.
Security event		See Auditable event

References

- [1] ISO/IEC 27002 - Information technology -- Security techniques -- Code of practice for information security management, section 10.10, 2005 (www.iso.org)
- [2] BSI PD008: Legal Admissibility and Evidential Weight of Information Stored Electronically, British Standards Institution, 1999
- [3] COBIT (Control Objectives for Information and related Technology) from Information Systems Audit and Control Association (<http://www.isaca.org/cobit.htm>)
- [4] ICT-PSP/2007/1 – STORK 1 : D5.7.3 Functional Design for PEPS, MW models and interoperability
- [5] K. Kent, M. Souppaya. Guide to Computer Security Log Management. Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-92, September 2006
- [6] SANS Consensus Policy Resource Community - Information Logging Standard, <http://www.sans.org/security-resources/policies/server-security>
- [7] NIST: An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12, December 1997, <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>
- [8] Common Criteria: Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 4, September.2012 Part 2: Security Functional Components, <http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf>
- [9] ENISA: Privacy Features of European eID Card Specification, Version 1.0.1, January 2009, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_features_eID.pdf
- [10] EC council - The use of audit trails in security systems <http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/the-use-of-audit-trails-in-security-systems-guidelines-for-european-banks/>
- [11] AUDIT Trails - NIST publication <http://csrc.nist.gov/publications/nistbul/itl97-03.txt>

1. Introduction

This document is intended for a technical audience consisting of developers, administrators and those requiring detailed technical information on how to configure, build and deploy the eIDAS-Node application.

The document describes the steps involved when implementing a Basic Setup and goes on to provide detailed information required for customisation and deployment.

1.1. Document structure

This document is divided into the following sections:

- Chapter 1 – Introduction: this section.
- Chapter 2 – *Product overview* describes the binaries and source code to be installed plus the configuration files.
- Chapter 3 – *Preparing the installation* describes the pre-requisites for a successful installation, including the correct Java version, supported application servers, environmental variables to be set, keystores etc.
- Chapter 4 – *Configuring the software* describes all configuration settings.
- Chapter 5 – *Building and deploying the software* describes the steps to build and then to deploy the software on the supported servers. There are two main types of eIDAS-Node: Connector and Proxy Service.
- Chapter 6 – *Verifying the installation* shows the final structure of your application server relevant directories, so that you can confirm that you have made the proper configurations.
- Chapter 7 – *Advanced configuration for production environments* provides detailed descriptions of the configurations to enable you to change specific aspects as required.
- Appendix A – *eIDAS Levels of Assurance* provides information on the three Levels of Assurance described in the Implementing Regulation.
- Appendix B – *User consent* provides a brief overview of the meaning of 'user consent' in the context of privacy legislation.
- Appendix C – *Hazelcast proposed configuration* provides specific information related to configuration of a cluster environment using Hazelcast.
- Appendix D – *Installation Frequently Asked Questions* provides answers to questions that may arise during your installation.

1.2. Purpose

The purpose of this document is to give a comprehensive view on the product and its components s that the user is about to install (in terms of binaries and/or source code, as well as in terms of configuration files).

1.3. Document aims

The aims of this document are to:

- guide you through the preliminary steps involved when setting up your servers;
- guide you through setting up, compiling and running a project for a basic configuration with one instance of your Application Server;
- cover detailed configuration of eIDAS-Nodes;
- provide a check list of files for each application server;
- show how to ensure eIDAS regulation compliance and provide a check list of recommendations;
- describe the HTTP response headers that the eIDAS-Node can send in order to increase its security;
- describe the technologies and configurations used for testing the eIDAS-Node in cluster mode.

1.4. Other technical reference documentation

We recommend that you also familiarise yourself with the following eID technical reference documents which are available on **CEF Digital Home > eID > All eID services > eIDAS Node integration package > View latest version:**

- *eIDAS-Node Installation, Configuration and Integration Quick Start Guide* describes how to quickly install a demo Service Provider, eIDAS-Node Connector, eIDAS-Node Proxy Service and demo IdP from the distributions in the release package. The distributions provide preconfigured eIDAS-Node modules for running on each of the supported application servers.
- *eIDAS-Node National IdP and SP Integration Guide* provides guidance by recommending one way in which eID can be integrated into your national eID infrastructure.
- *eIDAS-Node Demo Tools Installation and Configuration Guide* describes the installation and configuration settings for Demo Tools (SP and IdP) supplied with the package for basic testing.
- *eIDAS-Node and SAML* describes the W3C recommendations and how SAML XML encryption is implemented and integrated in eID. Encryption of the sensitive data carried in SAML 2.0 Requests and Assertions is discussed alongside the use of AEAD algorithms as essential building blocks.
- *eIDAS-Node Error and Event Logging* provides information on the eID implementation of error and event logging as a building block for generating an audit trail of activity on the eIDAS Network. It describes the files that are generated, the file format, the components that are monitored and the events that are recorded.
- *eIDAS-Node Security Considerations* describes the security considerations that should be taken into account when implementing and operating your eIDAS-Node scheme.
- *eIDAS-Node Error Codes* contains tables showing the error codes that could be generated by components along with a description of the error, specific behaviour and, where relevant, possible operator actions to remedy the error.

1.5. eIDAS Technical specifications and software provided

This software package is provided as a reference implementation in accordance with the *eIDAS Technical Specifications* v1.1.

1.5.1. Further information

For further information on the practical implementation of the features listed above, please refer to section 7.5 — *eIDAS-Node compliance* which describes the production mode for ensuring eIDAS regulation compliance.

2. Product overview

2.1. Package

The main product deliverable is `EidasNode.war` which is a web application that can be deployed to most Java web containers on the market. Both the eIDAS-Node Connector and the eIDAS-Node Proxy Service are implemented in this package. The actual functionality is activated by configuration.

2.2. Modules

The software is composed of several modules. This section describes the binaries and source code to be installed plus the configuration files.

Table 1: List of modules

Module Name	Folder	Description
Parent	EIDAS-Parent	Module containing a consolidated and consistent location of the libraries and their version number to be used across the different modules.
Light Commons	EIDAS-Light-Commons	Light Common application component and utility classes used for implementing as basis for the EIDAS-Commons and MS Specific module.
Commons	EIDAS-Commons	Common Applications components and utility classes for implementing functionality of authentication service.
Encryption	EIDAS-Encryption	Encryption and signature dedicated module. Contains libraries, including OpenSAML, provided for the build as Maven local repository.
ConfigModule	EIDAS-ConfigModule	Configuration management module dedicated to facilitate eIDAS-Node configuration.
SAMLEngine	EIDAS-SAMLEngine	Implementation of EIDAS SAML ProtocolEngine used in the eIDAS-Node.
Specific Communication Definition	EIDAS-SpecificCommunicationDefinition	The exchange definition (interfaces) used to formalise the exchange definition between the node and the specific module.
MS specific	EIDAS-Specific	Sample of Member State (MS) specific module. Not to be used in production.
Updater	EIDAS-Updater	Module used to change configuration of a running eIDAS-Node in testing environment. (To enable, web.xml must be updated.)

Module Name	Folder	Description
EidasNode	EIDAS-NODE	eIDAS-Node module (Proxy Service, Connector).
Service provider	EIDAS-SP	Sample of Service Provider module
Identity provider	EIDAS-IdP-1.0	Sample of Identity Provider module
Basic Setup configuration	EIDAS-Config	Sample configuration as in 6.6

The figure below shows the dependencies between the installed modules.

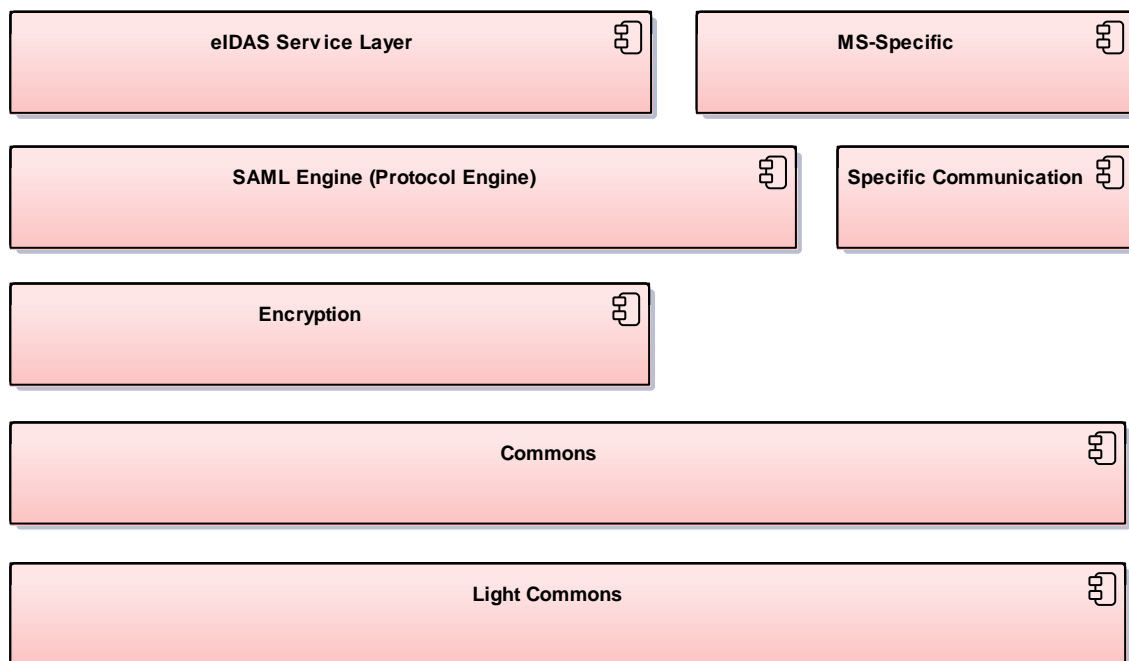


Figure 1: Dependencies between modules

The figure below shows the communications flows between modules during authentication of citizens.

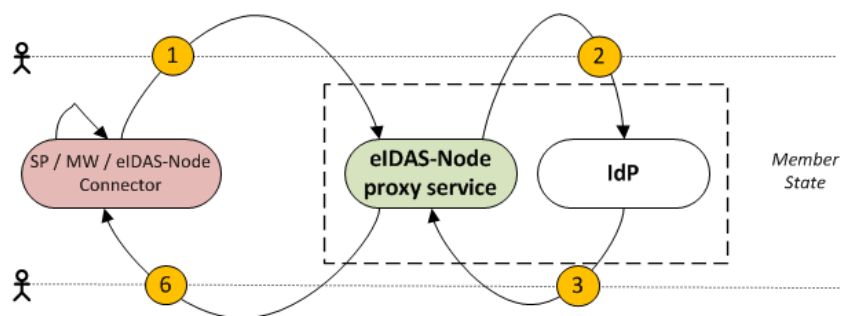


Figure 2: Communication flows between modules during authentication of citizens

3. Preparing the installation

This section provides instructions on how to deploy the project on Tomcat, JBoss, GlassFish, WebLogic or WebSphere servers.

The appropriate JVM needs to be installed and configured first. If the selected application server includes an embedded JVM, the configuration still needs to be changed.

3.1. Configuring the JVM

The project is built by default using the **Java SDK** version **1.7** (and can also be built in Java 1.8).

In order to avoid a possible XML External Entity attack (XXE), the OWASP guidelines advise to use Java 7 update 67, Java 8 update 20 or above. For more details, please refer to:

[https://www.owasp.org/index.php/XML_External_Entity_\(XXE\)_Prevention_Cheat_Sheet](https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Prevention_Cheat_Sheet).

3.1.1. Oracle Java JCE Unlimited Strength Jurisdiction Policy

If Oracle provided JVM is going to be used, then it is necessary to apply the JCE Unlimited Strength Jurisdiction Policy Files, which contain no restriction on cryptographic strengths:

1. Download the Java Cryptography Extension (JCE) Unlimited Strength Policy Files from Oracle (subject to be moved by Oracle to different URI):
 - For Java 7: <http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>
 - For Java 8: <http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html>
2. Uncompress and extract the downloaded zip file (it contains README.txt and two jar files).
3. For the installation, please follow the instructions in the README.txt file.

3.1.2. IBM SDK Java

If the IBM provided JVM is going to be used for the eIDAS-Node, it is necessary to upgrade at least version 7.

IBM WebSphere Application Server V8.5 comes by default with IBM SDK Java 6. Using IBM Installation Manager, you can install IBM SDK Java 7 as an optional feature. SDK Java 7 can be added at any time to the WAS installation by following the IBM installation procedure described at http://www-01.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/com.ibm.websphere.installation.base.doc/aetins_installation_jdk7_gui.html (possibly subject to relocation by IBM).

Once this is complete, both IBM SDK Java versions 6 and 7 will coexist. To switch the SDK used by server profiles, you can use the `managesdk` command described at http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_managesdk.html (possibly subject to relocation by IBM).

3.1.2.1. Configuring encryption support

The default IBM security provider bundled with JVM does not support the default encryption algorithm used by eIDAS (<http://www.w3.org/2009/xmlenc11#aes256-gcm>). One option is to use BouncyCastleProvider instead of default IBM JVM default provider:

1. Place the bouncycastle jar in \$IBM_JRE/lib/ext directory.
2. Copy the IBM unrestricted JCE policy files provided in AdditionalFiles directory and put them under \$IBM_JRE/lib/security to erase the existing ones. **Note that those jars are signed.**
3. Add BouncyCastleProvider to the list of providers in the \$IBM_JRE/lib/security/java.security file before the default provider, e.g.

```
security.provider.1=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
security.provider.2=org.bouncycastle.jce.provider.BouncyCastleProvider
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.jsse2.IBMJSSEProvider2
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.security.cmskeystore.CMSProvider
security.provider.8=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.9=com.ibm.security.sasl.IBMSASL
security.provider.10=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.11=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.12=org.apache.harmony.security.provider.PolicyProvider
```

3.2. Configuring the application server

The following is a list of the supported servers.

Table 2: Supported servers

Application Server	Supported version(s)
Tomcat	7, 8
GlassFish	3, 4
JBoss	7
WebLogic	12.1.2, 12c
WebSphere/WebSphere Liberty Profile	8.5.5/8.5.5.4

3.2.1. Configuring Tomcat 7

1. Create a folder named endorsed in \$TOMCAT_HOME.
2. Create a folder named shared in \$TOMCAT_HOME.
3. Edit the file \$TOMCAT_HOME/conf/catalina.properties and change the property `shared.loader` so that it reads:

```
shared.loader=${catalina.home}/shared/lib/*.jar
```

4. Extract from the binary zip file (under AdditionalFiles/endorsed) the following libs to \$TOMCAT_HOME/shared/lib:

```
xml-apis-1.4.01.jar  
resolver-2.9.1.jar  
serializer-2.7.2.jar  
xalan-2.7.2.jar  
xercesImpl-2.11.0.jar
```

3.2.2. Configuring Tomcat 8

Extract from the binary zip file (under AdditionalFiles/endorsed) the following libs to \$TOMCAT_HOME/lib:

```
xml-apis-1.4.01.jar  
resolver-2.9.1.jar  
serializer-2.7.2.jar -> rename this file to serializer.jar  
xalan-2.7.2.jar  
xercesImpl-2.11.0.jar
```

3.2.3. Configuring JBoss AS 7

Install the modules found under AdditionalFile/JBOSS7. These modules contain BouncyCastle JCE provider and xml-apis. They should be copied under \$JBoss_HOME/modules directory.

3.2.4. Configuring GlassFish V3

Extract from the binary zip file (under AdditionalFiles/endorsed) the following libs to \$GLASSFISH_HOME/glassfish/lib/endorsed

```
endorsed/resolver-2.9.1.jar  
endorsed/serializer-2.7.2.jar  
endorsed/xalan-2.7.2.jar  
endorsed/xercesImpl-2.11.0.jar  
endorsed/xml-apis-1.4.01.jar
```

where \$GLASSFISH_HOME is the base directory of your GlassFish server (e.g. /home/user/apps/glassfishv3).

3.2.5. Configuring GlassFish V4

Under \$GLASSFISH_DOMAIN/lib/ext/ copy xml-apis-1.4.01.jar

3.2.6. Configuring WebLogic

Under `$DOMAIN_HOME/lib/` copy `xml-apis-1.4.01.jar`

Note: For WebLogic 12c only:

The 'resources' folder containing javascripts, images and stylesheets has been renamed to 'resource';

the EIDAS-SP weblogic.xml file contains all references to the OpenSAML libraries.

3.2.7. Configuring WebSphere

The web applications should be deployed using the WAS Admin Console.

If your WAS installation is using IBM supplied Java SDK, please be sure to execute steps described in section 3.1.2.

3.2.8. Configuring WebSphere Liberty Profile

The `xml-apis-1.4.01.jar` file should be placed under `$SERVER_HOME/lib/global`.

The application may be deployed by copying the war files under `$SERVER_HOME/dropins` directory.

The IBM Installation Manager can be used to install the IBM SDK Java 7 for Liberty Profile (please refer to the IBM official documentation at: http://www.ibm.com/support/knowledgecenter/SSD28V_8.5.5/com.ibm.websphere.wlp.core.doc/a_e/twlp_ins_installation_jdk7.html - subject to be moved by IBM).

3.3. Enabling logging

To enable audit logging of the communications between eIDAS-Node Proxy Service and eIDAS-Node Connector, you should make the following configuration changes. This is part of EIDAS Audit log, for further information please see the *eIDAS-Node Error and Event Logging* guide.

The locations of the audit files are by default configured to use a Java system properties variable called `LOG_HOME`.

A value can be assigned to this variable by using: `-DLOG_HOME="<myDirectoryName>"` at server start-up.

If modification of the environment variable is not possible, the value of this variable could also be assigned by adding the following line in the `logback.xml` file

```
<property name="LOG_HOME" value = "<myDirectoryName>" />
```

Note: The eIDAS-Node logs may contain person identification data, hence these logs should be handled and protected appropriately in accordance with the European privacy regulations [Dir. 95/46/EC] and [Reg. 2016/679].

[Reg. 2016/679] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[Dir. 95/46/EC] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

3.3.1. Configuring audit logging

Edit the project eIDAS-Node file: `logback.xml` (located in the resource directory) and add the following lines:

```
<?xml version="1.0" encoding="UTF-8" ?>

<!--
    NOTE :
        the environment variable LOG HOME could be set to indicate the directory
        containing the log files
        the log configuration files will be scanned periodically each 30 minutes
        LOG level is defined as below :
            Default level : INFO
                Console appender (STDOUT)      : inherits from default
                eIDASNodeDetail appender        : INFO
                eIDASNodeSystem appender        : INFO
                eIDASNodeSecurity appender      : INFO
-->

<configuration scan="true" scanPeriod="30 minutes">

    <!--
        This define the CONSOLE appender - the level of the console appender is based on
        the root level
    -->
    <appender name="STDOUT" class="ch.qos.logback.core.ConsoleAppender">
        <encoder>
            <pattern>%d{yyyy-MM-dd; HH:mm:ss.SSS} [%thread] %-5level %logger{66} %marker -
%X{sessionId} -%X{remoteHost} -%msg%n</pattern>
        </encoder>
    </appender>

    <!--
        This define the FULL Detailed log file appender - the level of the console
        appender is INFO by default
    -->
    <appender name="eIDASNodeDetail"
class="ch.qos.logback.core.rolling.RollingFileAppender">
        <file>${LOG_HOME}/eIDASNodeDetail.log</file>

        <filter class="ch.qos.logback.classic.filter.ThresholdFilter">
            <level>INFO</level>
        </filter>
        <encoder class="eu.eidas.node.logging.logback_integrity.HashPatternLayoutEncoder">
            <pattern>%d{yyyy-MM-dd; HH:mm:ss.SSS} [%thread] %-5level %logger{66} %marker -
%X{sessionId} -%X{remoteHost} -%msg%n</pattern>
        </encoder>
```

```

    <param name="Append" value="true" />
    <triggeringPolicy class="ch.qos.logback.core.rolling.SizeBasedTriggeringPolicy">
        <maxFileSize>500KB</maxFileSize>
    </triggeringPolicy>
    <!-- Support multiple-JVM writing to the same log file -->
    <prudent>true</prudent>
    <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
        <fileNamePattern>${LOG_HOME}/eIDASNodeDetail.%d{yyyy-MM-dd}.log</fileNamePattern>
        <maxHistory>14</maxHistory>
    </rollingPolicy>
</appender>

<!--
    This define the SYSTEM Detailed log file appender - the default Filter is
    inherited from root level
-->
    <appender name="eIDASNodeSystem"
class="ch.qos.logback.core.rolling.RollingFileAppender">
        <file>${LOG_HOME}/eIDASNodeSystem.log</file>

        <filter class="ch.qos.logback.core.filter.EvaluatorFilter">
            <evaluator class="ch.qos.logback.classic.boolex.OnMarkerEvaluator">
                <marker>SYSTEM</marker>
            </evaluator>
            <onMismatch>DENY</onMismatch>
            <onMatch>ACCEPT</onMatch>
        </filter>
        <encoder class="eu.eidas.node.logging.logback_integrity.HashPatternLayoutEncoder">
            <pattern>%d{yyyy-MM-dd; HH:mm:ss.SSS} [%thread] %-5level %logger{66} %marker -
%X{sessionId} -%X{remoteHost} -%msg%n</pattern>
        </encoder>
        <param name="Append" value="true" />
        <!-- Support multiple-JVM writing to the same log file -->
        <prudent>true</prudent>
        <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
            <fileNamePattern>${LOG_HOME}/eIDASNodeSystem.%d{yyyy-MM-dd}.log</fileNamePattern>
            <maxHistory>14</maxHistory>
        </rollingPolicy>
    </appender>

<!--
    This define the SECURITY Detailed log file appender - the default Filter is
    inherited from root level
-->
    <appender name="eIDASNodeSecurity"
class="ch.qos.logback.core.rolling.RollingFileAppender">
        <file>${LOG_HOME}/eIDASNodeSecurity.log</file>

        <filter class="ch.qos.logback.core.filter.EvaluatorFilter">
            <evaluator class="ch.qos.logback.classic.boolex.OnMarkerEvaluator">
                <marker>SECURITY_SUCCESS</marker>
                <marker>SECURITY_WARNING</marker>
                <marker>SECURITY_FAILURE</marker>
            </evaluator>
            <onMismatch>DENY</onMismatch>
            <onMatch>ACCEPT</onMatch>
        </filter>

```

```

        <encoder class="eu.eidas.node.logging.logback_integrity.HashPatternLayoutEncoder">
            <pattern>%d{yyyy-MM-dd; HH:mm:ss.SSS} [%thread] %-5level %logger{66} %marker -
%X{sessionId} -%X{remoteHost} -%msg%n</pattern>
        </encoder>
        <param name="Append" value="true" />
        <!-- Support multiple-JVM writing to the same log file -->
        <prudent>true</prudent>
        <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
            <fileNamePattern>${LOG_HOME}/eIDASNodeSecurity.%d{yyyy-MM-
dd}.log</fileNamePattern>
            <maxHistory>14</maxHistory>
        </rollingPolicy>
    </appender>

    <!--
        This define the SAML exchange Detailed log file appender - the default Filter is
        inherited from root level
    -->
    <appender name="eIDASNodeSAMLExchange"
class="ch.qos.logback.core.rolling.RollingFileAppender">
        <file>${LOG_HOME}/eIDASNodeSAMLExchange.log</file>

        <filter class="ch.qos.logback.core.filter.EvaluatorFilter">
            <evaluator class="ch.qos.logback.classic.boolex.OnMarkerEvaluator">
                <marker>SAML_EXCHANGE</marker>
            </evaluator>
            <onMismatch>DENY</onMismatch>
            <onMatch>ACCEPT</onMatch>
        </filter>
        <encoder class="eu.eidas.node.logging.logback_integrity.HashPatternLayoutEncoder">
            <pattern>%d{yyyy-MM-dd; HH:mm:ss.SSS} [%thread] %-5level %logger{66} %marker -
%X{sessionId} -%X{remoteHost} -%msg%n</pattern>
        </encoder>
        <param name="Append" value="true" />
        <!-- Support multiple-JVM writing to the same log file -->
        <prudent>true</prudent>
        <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
            <fileNamePattern>${LOG_HOME}/eIDASNodeSAMLExchange.%d{yyyy-MM-
dd}.log</fileNamePattern>
            <maxHistory>14</maxHistory>
        </rollingPolicy>
    </appender>

    <!--
        This define the API fine grained level
    -->
    <logger name="org.opensaml">
        <level value="ERROR" />
        <appender-ref ref="STDOUT"/>
        <appender-ref ref="eIDASNodeDetail"/>
    </logger>
    <logger name="com.opensymphony.xwork2">
        <level value="WARN"/>
        <appender-ref ref="STDOUT"/>
        <appender-ref ref="eIDASNodeDetail"/>
    </logger>
    <logger name=" org.apache.struts2">
        <level value="WARN"/>

```



```

        <appender-ref ref="STDOUT"/>
        <appender-ref ref="eIDASNodeDetail"/>
    </logger>
    <logger name="org.springframework">
        <level value="WARN" />
        <appender-ref ref="STDOUT"/>
        <appender-ref ref="eIDASNodeDetail"/>
    </logger>
    <logger name="org.apache.xml.security">
        <level value="WARN" />
        <appender-ref ref="STDOUT"/>
        <appender-ref ref="eIDASNodeDetail"/>
    </logger>

    <logger name="eu.eidas.communication.requests">
        <level value="info" />
        <appender-ref ref="STDOUT"/>
        <appender-ref ref="eIDASNodeDetail"/>
    </logger>

    <logger name="eu.eidas.communication.responses">
        <level value="info" />
        <appender-ref ref="STDOUT"/>
        <appender-ref ref="eIDASNodeDetail"/>
    </logger>

    <!--
        The root level is set to debug for development purposes, for production
        environment it could be set to INFO
    -->
    <root level="DEBUG">
        <appender-ref ref="STDOUT" />
        <appender-ref ref="eIDASNodeSystem" />
        <appender-ref ref="eIDASNodeSecurity" />
        <appender-ref ref="eIDASNodeDetail" />
        <appender-ref ref="eIDASNodeSAMLExchange" />
    </root>
</configuration>

```

Notes:

- The root level of logging defines the detail of logged events, for testing and development purposes, this level should be set to DEBUG; in production environment, it should be INFO.
- Four different log files are generated by the application, depending on the context of the event to log (please refer to the *eIDAS-Node Error and Event Logging* guide for more details)
 - the Application System log (eIDASNodeSystem),
 - the Application Security log (eIDASNodeSecurity),
 - the Message Exchange log (eIDASNodeSAMLExchange),
 - the Application Detailed log (eIDASNodeDetail)
- `${FILENAME_FULL_PATH}` is the location of the file which will contain the logs.

(e.g.: /opt/eidaslogs/eIDASNodeDetail.log)

For further information on logging please refer to the *eIDAS-Node Error and Event Logging* and the *eIDAS-Node Security Considerations* guides.

3.4. Configuring application server security

3.4.1. Security constraints for WebSphere

WebSphere AS is configured by default to not observe security constraints in web applications. To enforce these constraints WebSphere should be configured as shown below.

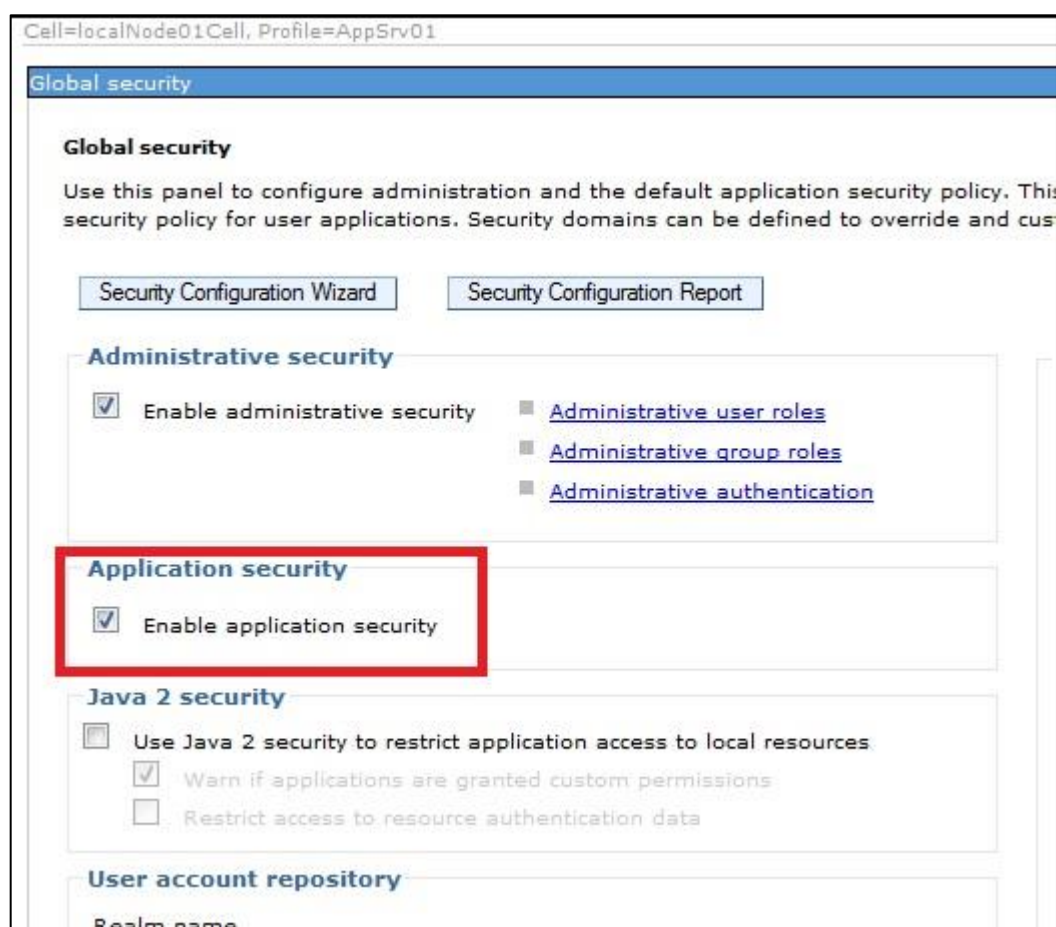


Figure 3: Enabling application security on WebSphere AS

4. Configuring the software

This section describes the configuration settings. Before proceeding with these steps your server must be configured, as described in section 3 — *Preparing the installation*.

Note: For information on implementing the eIDAS-Node Protocol Engine, please refer to the *CEF eID eIDAS-Node and SAML* document.

4.1. Configuring the project

To configure the project in the Basic Setup, follow the steps shown below.

4.1.1. Setup configuration directories

There are two different environment variables used to locate the eIDAS-Node's directories of configuration files. These can be defined as OS environment variables or setting it to the runtime environment (by `-D` switch to JVM or on the AS admin console):

- `$EIDAS_CONFIG_REPOSITORY` – used in `applicationContext.xml` and points to the configuration directory of the application (e.g. `file:/C:/PGM/projects/configEidas/`).
- `$SPECIFIC_CONFIG_REPOSITORY` – used in `applicationContext.xml` and points to the configuration directory of the supplied sample specific application (e.g. `file:/C:/PGM/projects/configEidas/specific/`). This one is used by the supplied sample MS-Specific part.

By default `EIDAS_CONFIG_REPOSITORY` and `SPECIFIC_CONFIG_REPOSITORY` (for the supplied sample MS-Specific) OS environment or JVM command line arguments (`-D` option) must be set in order to specify the location of configuration files. It is possible to change or hardcode these variables in `environmentalContext.xml`.

Note: a sample of this file is located in the EIDAS-config module.

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans-4.1.xsd">

    <!--

        Configuration repository path either from ENVIRONMENT variable or
        COMMAND LINE -D option of
            EIDAS_CONFIG_REPOSITORY and
            SPECIFIC_CONFIG_REPOSITORY
        For any other option - like hard-coded values - modify this
        file.

        Hard coding example:

    <bean id="eidasConfigRepository" class="java.lang.String">
```

```

        <constructor-arg value="c:/PGM/projects/configEidas/glassfish/"
/>
    </bean>

    <bean id="eidasSpecificConfigRepository" class="java.lang.String">
        <constructor-arg
value="c:/PGM/projects/configEidas/glassfish/specific/" />
    </bean>

    -->

    <bean id="eidasConfigRepository" class="java.lang.String">
        <constructor-arg value="#{
systemProperties['EIDAS_CONFIG_REPOSITORY'] ?:
systemEnvironment['EIDAS_CONFIG_REPOSITORY'] }" />
    </bean>

    <bean id="eidasSpecificConfigRepository" class="java.lang.String">
        <constructor-arg value="#{
systemProperties['SPECIFIC_CONFIG_REPOSITORY'] ?:
systemEnvironment['SPECIFIC_CONFIG_REPOSITORY'] }" />
    </bean>

</beans>

```

4.1.2. Setting up your Keystore

Copy your `eidaskeystore.jks` (the key store with your eIDAS-Node keys, alternatively you can use the example key store provided with the application) into a directory of your own choice, and make sure that:

- the property `keyStorePath` on file: `$EIDAS_CONFIG_REPOSITORY/SignModule_Service.xml` reflects the relative location of your Proxy Service `eidaskeystore.jks`;
- the property `keyStorePath` on file: `$EIDAS_CONFIG_REPOSITORY/SignModule_Connector.xml` reflects the relative location of your eIDAS-Node Connector `eidaskeystore.jks`;
- the property `keyStorePath` on file: `$SPECIFIC_CONFIG_REPOSITORY/SignModule_SP-Specific.xml` reflects the relative location of your MS-Specific Connector to your national infrastructure `eidaskeystore.jks`;
- the property `keyStorePath` on files: `$SPECIFIC_CONFIG_REPOSITORY/SignModule_Specific-IdP.xml` reflects the relative location of your MS-Specific sample Proxy Service to your national infrastructure `eidaskeystore.jks`.

If the eIDAS-Node is configured to use encryption, also ensure that:

- the property `keyStorePath` on file: `$EIDAS_CONFIG_REPOSITORY/EncryptModule_Service.xml` reflects the relative location of your Proxy Service `eidaskeystore.jks`;
- the property `keyStorePath` on file: `$EIDAS_CONFIG_REPOSITORY/EncryptModule_Connector.xml` reflects the relative location of your eIDAS-Node Connector `eidaskeystore.jks`;
- the property `keyStorePath` on file: `$SPECIFIC_CONFIG_REPOSITORY/EncryptModule_SP_Connector.xml`

reflects the relative location of your MS-Specific sample Connector to your national infrastructure `eidaskeystore.jks`;

- the property `keyStorePath` on files:
`$SPECIFIC_CONFIG_REPOSITORY/EncryptModule_Specific-IdP.xml`
reflects the relative location of your MS-Specific Proxy Service to your national infrastructure `eidaskeystore.jks`.

For more information see the *CEF eID eIDAS-Node and SAML* manual.

4.1.3. Configuring with Basic Setup

The Basic Setup allows you to use predefined configuration supplied with the software package, only for demo purposes. Copy the provided configuration files to the predefined `EIDAS_CONFIG_REPOSITORY` and `SPECIFIC_CONFIG_REPOSITORY`, then edit the file `eidas.xml` to specify the following eIDAS-Node Connector and eIDAS-Node Proxy Service configuration properties.

```
connector.assertion.url=
http://insert.your.ip.here:portGoesHere/EidasNode/ColleagueResponse
connector.destination.url=
http://insert.your.ip.here:portGoesHere/EidasNode/ServiceProvider
service1.url=
http://insert.your.ip.here:portGoesHere/EidasNode/ColleagueRequest
service.specificidredirect.url=
http://insert.your.ip.here:portGoesHere/EidasNode/IdpResponse
```

The supplied sample MS-Specific Proxy Service is ready made to connect one IdP. The URL of the IdP must be specified in `eidas_specific.xml`:

```
idp.url=
http://insert.your.ip.here:portGoesHere/IdP/AuthenticateCitizen
```

Demo SP reads the configuration from file `SP_CONFIG_REPOSITORY/sp.properties` so the `SP_CONFIG_REPOSITORY` environment variable / command line parameter should be set up. Change the following in `sp.properties`:

- `sp.url=http://your.ip.goes.here:portGoesHere/SP/ReturnPage`
- `countryX.url=http://your.ip.goes.here:portGoesHere/EidasNode/ServiceProvider`

For more information on settings for the Basic Setup please read *eIDAS-Node Demo Tool Installation and Configuration Guide*.

4.2. eIDAS-Node configuration files

This section provides a detailed description of the eIDAS-Node configuration files and their properties.

The `eidas.xml` file contains the properties to configure:

- General purpose parameters
- eIDAS-Node Connector

- eIDAS-Node Proxy Service

4.2.1. General purpose parameters

Table 3 lists general purpose parameters which include additional checks and security configurations.

Table 3: General purpose parameters

Key	Description
<code>metadata.activate</code>	Allows activation/deactivation of SAML metadata (this parameter activates/deactivates metadata publishing and requesting on both Connector and Proxy Service (see also the <i>eIDAS-Node and SAML</i> manual)
<code>node.metadata.not.signed.descriptors</code>	List of URLs corresponding to entity descriptors whose signatures have not to be checked. The format to use is <code>http://descriptorurl1; https://descriptorurl2</code> etc.
<code>response.encryption.mandatory</code>	When set to 'true' the node will try to encrypt assertions in the generated SAML responses (provided that the encryption related configuration is in place). Note: this parameter is used by both Proxy Service and Connector nodes.
<code>disable.check.mandatory.eidas.attributes</code>	When set to 'true' the node will check if at least one set of mandatory attributes is included in the request or in the response. Note: this parameter is used by both Proxy Service and Connector nodes
<code>disable.check.representative.attributes</code>	When set to false, the <code>ILightRequest</code> is checked if there are Representative attributes requested, and reject the authentication request. Default is false.
<code>distributedMaps</code>	When set to 'true' the node will use Hazelcast implementation for request-reply map correlations and anti-replay cache.
<code>nonDistributedMetadata.retention</code>	Retention period for simple metadata cache in seconds. (Note: for distributed environment it's not used, set it up in <code>hazelcast.xml</code> instead)
<code>eidas.protocol.version</code>	Value of eIDAS protocol version followed by the node, e.g. "1.1". When not empty, the value will be published in the node's metadata URLs.
<code>eidas.application.identifier</code>	Value of eIDAS protocol's application identifier relative to the node's code and version number, e.g. "CEF:eIDAS-ref:1.4.1". When not empty, the value will be published in the node's metadata URLs.

4.2.2. Attribute registry

Attribute registry holds and supplies information of types, value format and namespace for creating and validating requests and responses. The registry basically contains Attribute Definition objects built from custom XML files and hard coded lists of supported core attributes in `LegalPersonSpec`, `NaturalPersonSpec`, `RepresentativeLegalPersonSpec`, and `RepresentativeNaturalPersonSpec` collected together in `EidasSpec` class, found in the `SAMLEngine` module.

Each Protocol Engine has its own configuration files, specified by `SamLEngine.xml` files.

The following is an example code to introduce a new attribute to the XML configuration:

```
<entry
key="19.NameUri">http://eidas.europa.eu/attributes/natural/NewSomething</entry>
  <entry key="19.FriendlyName">NEW_SOMETHING</entry>
  <entry key="19.PersonType">NaturalPerson</entry>
  <entry key="19.Required">false</entry>
  <entry
key="19.XmlType.NamespaceUri">http://eidas.europa.eu/attributes/naturalperson</e
ntry>
    <entry key="19.XmlType.LocalPart">NewSomethingType</entry>
    <entry key="19.XmlType.NamespacePrefix">eidas-natural</entry>
```

For the `key` prefix number, take the last one and increment it. For eIDAS protocol the person type (natural or legal) must be specified and aligned with namespace.

4.2.2.1. Attribute registry validation and metadata support

Besides the Attribute Registry XML files there is a hard coded list of supported core attributes in `LegalPersonSpec`, `NaturalPersonSpec`, `RepresentativeLegalPersonSpec`, and `RepresentativeNaturalPersonSpec` collected together in `EidasSpec` class, can be found in the `SAMLEngine` module. This is necessary to get a reference of attribute definitions to perform business rule-based validations on requests and replies.

Supported attributes are published in the Metadata of the eIDAS-Node Proxy Service.

4.2.3. eIDAS-Node Connector configuration

The eIDAS-Node Connector configuration is composed of the following parts:

- Service Provider configuration
- eIDAS-Node Connector dedicated information
- Configuration of the recognised Connector

4.2.3.1. Service Provider configuration

To configure the Service Provider, you must provide a value for the properties.

Table 4: eIDAS-Node Connector and SP validation

Key	Description
<code>[SP-ID].qaalevel</code>	QAA level of the Id of the Service Provider e.g. <code>ES-SP.qaalevel=3</code> . Compared against the LightRequest's QAA level, which cannot be higher than this value.
<code>sp.default.parameters</code>	NOT USED
<code>SP-ID</code>	NOT USED
<code>sp.authorized.parameters</code>	NOT USED
<code>[SP-ID].validation</code>	The SP's keystore alias. This must match the SP's keystore alias or use "none" to bypass this validation e.g. <code>ES-SP.validation=ES-SP-CERT</code> . If you need to configure the same certificate for several SPs, then just add once the Certificate and put the keystore alias in this property for each SP e.g. <code>ES-SP1.validation= ES-SP-CERT;</code> <code>ES-SP2.validation= ES-SP-CERT;</code> <code>ES-SPn.validation= ES-SP-CERT</code>
<code>connector.spInstitution</code>	NOT USED
<code>connector.spApplication</code>	NOT USED
<code>connector.spCountry</code>	NOT USED
<code>connector.spSector</code>	NOT USED
<code>active.module.connector</code>	Allows deactivating eIDAS-Node Connector functionality: when setting this parameter to false, eIDAS-Node Connector will answer with an error message to incoming requests. The default value is true.
<code>sp.metadata.location.whitelist</code>	Example: <pre><entry key="sp.metadata.location.whitelist"> http://sp_1:8080/SP/metadata; http://sp_2:8888/SP/metadata; </entry></pre> semicolon separated urls of the SP's that the Connector is allowed to connect to obtain metadata/certificate to verify signature of SAML requests. Note: Non-existent or empty whitelist will prevent the node from retrieving any metadata from any SP.
<code>service1.metadata.url</code> ... <code>Service8.metadata.url</code>	urls of the service proxy's that the Connector is allowed to connect to obtain metadata/certificate to verify signature of SAML responses. Example: <pre><entry key="service2.name">LOCAL-EIDAS-CB</entry> <!-- URL of the first Service --> <entry key="service2.url">http://localhost:8080/EidasNode/ColleagueRequest</entry> <entry key="service2.skew.notbefore">0</entry> <entry key="service2.skew.notonorafter">0</entry> <entry key="service2.metadata.url"> http://localhost:8080/EidasNode/ServiceMetadata </entry></pre>

4.2.3.2. eIDAS-Node Connector dedicated information

To identify the eIDAS-Node Connector, the following information needs to be provided.

Table 5: eIDAS-Node Connector dedicated information

Key	Description
<code>connector.id</code>	NOT USED
<code>connector.assertion.url</code>	URL of the Action to be called when returning from eIDAS-Node Proxy Service. (This used as AssertionConsumerServiceURL in the Request also)
<code>connector.destination.url</code>	NOT USED
<code>saml.sp</code>	Name of the SAML ProtocolEngine instance to use between SP and eIDAS-Node Connector. Used by the supplied MS-Specific implementation.
<code>saml.connector</code>	Name of the SAML ProtocolEngine instance used by the eIDAS-Node Connector in the eIDAS Network (between Connector and Proxy Service).
<code>connector.node.url</code>	NOT USED
<code>connector.contact.support.email</code>	Email address of the support contact (for metadata)
<code>connector.contact.support.company</code>	Company name of the support contact (for metadata)
<code>connector.contact.support.givenname</code>	Given name of the support contact (for metadata)
<code>connector.contact.support.surname</code>	Surname of the support contact (for metadata)
<code>connector.contact.support.phone</code>	Phone number of the support contact (for metadata)
<code>connector.contact.technical.email</code>	Email address of the technical contact (for metadata)
<code>connector.contact.technical.company</code>	Company of the technical contact (for metadata)
<code>connector.contact.technical.givenname</code>	Given name of the technical contact (for metadata)
<code>connector.contact.technical.surname</code>	Surname of the technical contact (for metadata)
<code>connector.contact.technical.phone</code>	Phone number of the technical contact (for metadata)
<code>connector.metadata.url</code>	The URL at which the metadata of eIDAS-Node Connector will be made available, e.g. <code>http://server:port/EidasNode/ConnectorMetadata</code> Will be used as Issuer in the requests that eIDAS-Node Connector sends, but does not set or validate the physical listener binding, therefore can be a custom value, like a reverse proxy external URL.
<code>connector.organization.name</code>	Name of the organization displayed in metadata
<code>connector.organization.displayname</code>	Localised display name of the organization for metadata
<code>connector.organization.url</code>	URL of the organisation for metadata containing information
<code>ssos.connectorMetadataGeneratorIDP.post.location</code>	The URL for the metadata <code><md:SingleSignOnService></code> location attribute of the <code>SingleSignOnService</code> related to <code>Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"</code> . e.g. <code>http://localhost:8080/EidasNode/ServiceProvider</code> It does not set or validate the physical listener binding, therefore can be a custom value, like a reverse proxy external URL.
<code>ssos.connectorMetadataGeneratorIDP.redirect.location</code>	The URL for the metadata <code><md:SingleSignOnService></code> location attribute of the <code>SingleSignOnService</code> related to <code>Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"</code> . e.g. <code>http://localhost:8080/EidasNode/ServiceProvider</code> It does not set or validate the physical listener binding, therefore can be a custom value, like a reverse proxy external URL.

Key	Description
<code>connector.responder.metadata.url</code>	The URL at which the metadata of the eIDAS-Node Connector (presenting itself as an IdP) will be made available, e.g. <code>http://server:port/EidasNode/ConnectorResponderMetadata</code> Will be used as Issuer in the responses that eIDAS-Node Connector sends to SP. This setting is for the sample Specific.

If you are running tests across the network you must change the `connector.assertion.url` to reflect the IP address of the machine running the eIDAS-Node Connector:

`http://connector.ip.address:connector.port.number/node.deployment.name/ColleagueResponse.`

4.2.3.3. Configuring the recognised eIDAS-Node Proxy Service

The eIDAS-Node Connector recognises the eIDAS-Node Proxy Services listed in `eidas.xml`. Increment the `service.number`, add their keys and respective values. The URL must be in the format:
`http://service.ip.address:service.port.number/service.deployment.name/ColleagueRequest`

Table 6: Adding eIDAS-Node Proxy Service to Connector

Key	Description
<code>service.number</code>	Number of known eIDAS-Node Proxy Service
<code>serviceX.id</code>	Id of the eIDAS-Node Proxy Service X(=unique positive integer)
<code>serviceX.name</code>	Name of the eIDAS-Node Proxy Service X(=unique positive integer)
<code>serviceX.url</code>	URL of the eIDAS-Node Proxy Service X(=unique positive integer)
<code>serviceX.metadata.url</code>	URL where the eIDAS-Node Proxy Service X publishes its metadata
<code>serviceX.skew.notbefore</code>	Time skew in milliseconds to adjust <code>notBefore</code> SAML condition in Connector. The actual value is added to the received time condition, negative value is possible.
<code>serviceX.skew.notonorafter</code>	Time skew in milliseconds to adjust <code>notOnOrAfter</code> SAML condition in Connector. The actual value is added to the received time condition. A negative value is possible.

4.2.4. eIDAS-Node Proxy Service configuration

To activate an eIDAS-Node Proxy Service the following properties need to be provided:

Table 7 : eIDAS-Node Proxy Service setup

Key	Description
<code>service.id</code>	NOT USED
<code>service.countrycode</code>	The eIDAS-Node Proxy Service country ID in ISO 3166-1 alpha-3 format e.g. PT is the ISO 3166 code for Portugal. Used when the eIDAS-Node Proxy Service constructs the unique identifier attributes .

Key	Description
<code>service.maxQAALevel</code>	Max QAA Level that eIDAS-Node Proxy Service can authenticate (see Appendix A — <i>eIDAS Levels of Assurance</i>). If the request QAA level is higher, it will be denied.
<code>service.askconsent.type</code>	If set to "true", the Consent Page will be displayed to the user when processing the request from the eIDAS-Node Connector. Attributes without consent will be removed from the Response by the eIDAS-Node Proxy Service.
<code>service.askconsent.value</code>	If set to "true", the Value Consent Page (CV) will be displayed by the eIDAS-Node Proxy Service before sending the Response to the eIDAS-Node Connector. The user is able to cancel the forwarding of authentication data, resulting in an authentication failure.
<code>service.askconsent.all.attributes</code>	If set to "true", the Value Consent Page (CV) will display all the Response attributes/values, including additional (specified in XML file) ones. On "false" only the Core eIDAS attributes/values will be displayed.
<code>service.askconsent.attribute.names.only</code>	If set to "true", the Value Consent Page (CV) will display attribute names only for the Response, "false" will result in attribute values also.
<code>service.specificidredirect.url</code>	URL of the Action to be called when returning from IdP, this is used in the provided sample MS-Specific part, useful only with Demo setup.
<code>service.citizenConsentUrl</code>	The URL where the user provides the Citizen Consent (for information on citizen consent see Appendix B)
<code>service.node.url</code>	NOT USED
<code>service.contact.support.email</code>	Email address of the support contact (for metadata)
<code>service.contact.support.company</code>	Company of the support contact (for metadata)
<code>service.contact.support.givenname</code>	Given name of the support contact (for metadata)
<code>service.contact.support.surname</code>	Surname of the support contact (for metadata)
<code>service.contact.support.phone</code>	Phone number of the support contact (for metadata)
<code>service.contact.technical.email</code>	Email address of the technical contact (for metadata)
<code>service.contact.technical.company</code>	Company name of the technical contact (for metadata)
<code>service.contact.technical.givenname</code>	Given name of the technical contact (for metadata)
<code>service.contact.technical.surname</code>	Surname of the technical contact (for metadata)
<code>service.contact.technical.phone</code>	Phone number of the technical contact (for metadata)
<code>service.organization.name</code>	Name of the organisation displayed in the metadata
<code>service.organization.displayname</code>	Localised display name of the organisation for metadata
<code>service.organization.url</code>	URL of the organisation for Metadata containing information
<code>service.metadata.url</code>	<p>The URL under which the metadata of Proxy Service will be made available, e.g. <code>http://server:port/EidasNode/ServiceMetadata</code></p> <p>Will be used as Issuer in the requests that eIDAS-Node Proxy Service sends, but does not set or validate the physical listener binding, therefore can be a custom value, like a reverse proxy external URL.</p>

Key	Description
<code>service.LoA</code>	<p>Sets the Level of Assurance for the service. The following values are accepted:</p> <p><code>http://eidas.europa.eu/LoA/low</code> <code>http://eidas.europa.eu/LoA/substantial</code> <code>http://eidas.europa.eu/LoA/high</code></p> <p>Checked against the Request.</p>
<code>service.requester.metadata.url</code>	<p>The URL where the metadata of Proxy Service (presenting itself as an SP) will be made available, e.g. <code>http://EidasNode:8888/EidasNode/ServiceRequesterMetadata</code>.</p> <p>It will be used as Issuer in the requests that eIDAS-Node Connector sends to IdP, so this belongs to the provided sample MS-Specific part.</p>
<code>ssos.serviceMetadataGeneratorIDP.redirect.location</code>	<p>The URL for the metadata <code><md:SingleSignOnService></code> location attribute of the <code>SingleSignOnService</code> related to <code>Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"</code>.</p> <p>e.g. <code>http://EidasNode:8888/EidasNode/ColleagueRequest</code></p> <p>Does not come with physical binding check, so it can be set up for a reverse proxy external endpoint.</p>
<code>ssos.serviceMetadataGeneratorIDP.post.location</code>	<p>The URL for the metadata <code><md:SingleSignOnService></code> location attribute of the <code>SingleSignOnService</code> related to <code>Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"</code>.</p> <p>e.g. <code>http://EidasNode:8888/EidasNode/ColleagueRequest</code></p> <p>Does not come with physical binding check, so it can be set up for a reverse proxy external endpoint.</p>
<code>idp.metadata.location.whitelist</code>	<p>Example:</p> <pre><entry key="idp.metadata.location.whitelist"> http://idp_1:8080/IdP/metadata; http://idp_2:8888/IdP/metadata; </entry></pre> <p>semicolon separated urls of the IdP's that the Service Proxy is allowed to connect to obtain metadata/certificate to verify signature of SAML responses.</p> <p>Non-existent or empty whitelist will prevent the node from retrieving any metadata from any IdP.</p>

Key	Description
<code>connector.metadata.location.whitelist</code>	<p>semicolon separated urls of the Node Connectors that the ServiceProxy is allowed to connect to obtain metadata/certificate to verify signature of SAML requests.</p> <p>Example:</p> <pre><entry key="connector.metadata.location.whitelist"> http://localhost:8080/EidasNode/ConnectorMetadata; http://eidasnode:8888/EidasNode/ConnectorMetadata; </entry></pre> <p>Non-existent or empty whitelist will prevent the node from retrieving any metadata from any Connector.</p>

4.2.4.1. eIDAS-Node Proxy Service activation/deactivation

Table 8: Activating the Proxy Service

Key	Description
<code>active.module.service</code>	Whether to activate the Proxy Service module or not. Possible values: true, false. Default value: true.

4.2.4.2. Additional Configuration — Skew Time

It is possible for clocks to be out of synchronisation between eIDAS-Node instances (Proxy Service / Connector). To prevent validation errors occurring in the Connector you can configure a skew time for each Proxy Service. The skew time gives the Connector an additional tolerance window for validating the timestamps in the SAML Responses that are sent by the Proxy Service.

Please refer to Table 6: Adding eIDAS-Node Proxy Service to Connector for more information.

4.2.5. Additional configuration — Security

Table 9: Security policies

Key	Description
<code>max.requests.ip</code>	Maximum limit of requests per IP within the time frame of <code>max.time.ip</code> (-1 = unlimited)
<code>max.requests.sp</code>	Maximum limit of requests per SP within the time frame of <code>max.time.sp</code> (-1 = unlimited)
<code>max.time.ip</code>	Time frame for IP requests (seconds)
<code>max.time.sp</code>	Time frame for SP requests (seconds)
<code>trusted.sp.domain</code>	Allowed SPs to communicate with the eIDAS-Node Connector (none all list;Of;Domains)
<code>validation.bypass</code>	Bypass all SP validations (true false)
<code>validation.method</code>	Validate the Service Provider by domain or by domain and SPID (domain SPID)
<code>min.qaaLevel.value</code>	Minimum valid QAA level.
<code>max.qaaLevel.value</code>	Maximum valid QAA level.

Table 10: Security HTTP header parameters

Key	Description
<code>security.header.CSP.enabled</code>	Enable/disable sending the Content Security Policy (CSP) header. CSP protects against the injection of foreign content (refer to the <i>eIDAS-Node Security Considerations</i> guide for more information about the security features).
<code>security.header.CSP.includeMozillaDirectives</code>	In the CSP, this additional directive can be added for backward compatibility with old Mozilla browsers (refer to the <i>eIDAS-Node Security Considerations</i> guide for more information about the security features).
<code>security.header.XXssProtection.block</code>	This header enables the cross-site-scripting (XSS) filter built into most recent web browsers (refer to the <i>eIDAS-Node Security Considerations</i> guide for more information about the security features).
<code>security.header.XContentTypeOptions.noSniff</code>	The only defined value 'nosniff' prevents Internet Explorer and Google Chrome from 'MIME-sniffing' by inspecting the content of a response (refer to the <i>eIDAS-Node Security Considerations</i> guide for more information about the security features).

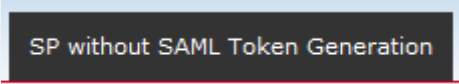
Key	Description
security.header.XFrameOptions.sameOrigin	<p>Prevents the application from being propagated in a frame or iframe, which in turns protects against key logging, clickjacking and similar attacks. Setting this option to true will prevent the eIDAS-Node from being framed in another application.</p> <p>If the SP needs to frame the eIDAS-Node, the option has to be set to 'false' (such as on the second tab of the SP Demo where the SAML request is generated by the eIDAS-Node).</p>  <p>(refer to the <i>eIDAS-Node Security Considerations</i> guide for more information about the security features).</p>
security.header.HSTS.includeSubDomains	<p>HTTP Strict-Transport-Security (HSTS) instructs browsers to prefer secure connections to the server (HTTP over SSL/TLS) over insecure ones (refer to the <i>eIDAS-Node Security Considerations</i> guide for more information about the security features).</p>
security.header.CSP.fallbackCheckMode	<p>If enabled, CSP fallback check mode includes an enforced CSP violation in JSP pages in order to check browser CSP feature. The included script displays a warning message in client browsers if CSP is not supported. However with CSP enabled browsers it may result in flood of warning messages logged by CSP report servlet. Disabled by default.</p>

Table 11: Check on certificate security parameter

Key	Description
check.citizenCertificate.serviceCertificate	<p>Checks that the country code stored in the eIDAS-Node Proxy Service SAML signing certificate is the same as the citizen country code in the SAML authentication request.</p>

4.2.5.1. Encryption

Table 12: Configuring encryption algorithm

Key	Description
<code>data.encryption.algorithm</code>	<p>This is an override setting for values set in SAMLEngine configuration. Contains the encryption algorithm to be used by Proxy Service and Connector. Possible value must be :</p> <pre><entry key="data.encryption.algorithm"></entry> <!-- List of Encryption algorithms</pre> <p> http://www.w3.org/2009/xmlenc11#aes128-gcm; http://www.w3.org/2009/xmlenc11#aes256-gcm; http://www.w3.org/2009/xmlenc11#aes192-gcm </p>
<code>encryption.algorithm.whitelist</code>	<p>This is an override setting for values set in SAMLEngine configuration. Contains the encryption algorithms allowed in the responses received by eIDAS-Node components. As per specification, this should be:</p> <p> http://www.w3.org/2009/xmlenc11#aes128-gcm; http://www.w3.org/2009/xmlenc11#aes256-gcm; http://www.w3.org/2009/xmlenc11#aes192-gcm </p>
<code>check_certificate_validity_period</code>	<p>Boolean value (true false), which indicates if the application will disallow the use of obsolete certificates. Applies to the signature check also (see Table 13).</p>
<code>disallow_self_signed_certificate</code>	<p>Boolean value (true false), which indicates if the application will disallow of the use of self-signed certificates. Applies to the signature check also (see Table 13).</p>
<code>response.encryption.mandatory</code>	<p>Boolean value (true/false), which indicates if the application will force the encryption of the SAML Response.</p>

4.2.5.2. Signature

Table 13: Signature algorithm

Key	Description
<code>signature.algorithm</code>	<p>This is an override setting for values set in SAMLEngine configuration. The signing algorithm (SHA2 based) used by the default signer for outgoing requests.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <code>http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</code> <code>http://www.w3.org/2001/04/xmldsig-more#rsa-sha384</code> <code>http://www.w3.org/2001/04/xmldsig-more#rsa-sha512</code> <code>http://www.w3.org/2001/04/xmldsig-more#rsa-ripemd160</code> <code>http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256</code> <code>http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384</code> <code>http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512</code> <code>http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1</code> <p>The default value is:</p> <ul style="list-style-type: none"> <code>http://www.w3.org/2001/04/xmldsig-more#rsa-sha512</code> <p>If another value is set, eIDAS-Nodes will use RSA-SHA512 algorithm and an error will be logged.</p>
<code>signature.algorithm.whitelist</code>	<p>This is an override setting for values set in SAMLEngine configuration. The list of allowed signature algorithms (in incoming requests). It contains OpenSAML's supported signing algorithms, separated by ;. Currently the elements of the list s may be picked from the following:</p> <ul style="list-style-type: none"> <code>http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</code> <code>http://www.w3.org/2001/04/xmldsig-more#rsa-sha384</code> <code>http://www.w3.org/2001/04/xmldsig-more#rsa-sha512</code> <code>http://www.w3.org/2001/04/xmldsig-more#rsa-ripemd160</code> <code>http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256</code> <code>http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384</code> <code>http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512</code> <code>http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1</code>
<code>Response.sign.assertions</code>	<p>When set to true, the SAML Responses (generated in Proxy Service and Connector) will have the attribute assertion signed</p>

4.2.5.3. SAML Binding method

Table 14: SAML binding parameters

Key	Description
<code>allow.redirect.binding</code>	<p>Whether to allow the HTTP Redirect binding. Possible values are true/false. (this was only applicable for STORK 1 message format and for testing purposes). For eIDAS, there are no bindings in the request.</p>
<code>validate.binding</code>	<p>Whether to validate the actual binding (POST or GET/Redirect) against <code>ProtocolBinding</code> attribute value of the SAML request. Possible values are true/false.</p>

By default, eIDAS-Nodes operate using SAML POST Binding. The parameter `allow.redirect.binding` (set to true) instructs the eIDAS-Node to accept HTTP Redirect Binding SAML requests, normally coming as HTTP GET requests. When HTTP Redirect Binding is used the following items should be considered:

- Most browsers have low limit for the size of GET request.
- Most servers have low limit for the size for HTTP header (e.g. in Apache Tomcat v7 this limit is about 8k; in order to increase this limit, the connector element in `server.xml` should contain a `maxHttpHeaderSize` element with the new limit);
- When this binding is activated, an HTTP redirect binding request received by Connector will be forwarded also as a redirect to Proxy Service and further (to IdP);
- The response is always sent back through a HTTP Post operation.

4.2.5.4. Additional Configuration — `SignModule_Service.xml` and `SignModule_Connector.xml`

It may be necessary to change the `keyStorePath` to reflect the location of your `eidasKeyStore.jks` file, please see the *eIDAS-Node and SAML* manual for more information.

4.2.5.5. Additional Configuration — Anti-replay Cache and Correlation Map Configuration

To prevent a replay of SAML requests an anti-replay cache is implemented at the eIDAS-Node Connector and eIDAS-Node Proxy Service level. We provide two different implementations for these caches, which can be configured. By default, the eIDAS-Node is set up to use a distributed cache with expiration.

This implementation is provided for correlating request and reply pairs both for `AuthenticationRequests` and `LightRequests`.

Hazelcast-backed caches are intended to be used in production environments. Development environment may use lighter cache implementations (simple `ConcurrentHashMap` based), which are activated by setting the parameter `distributedMaps` to **false** in `eidas.xml`.

By default there is one Hazelcast instance used by the Node for both correlation and anti-replay map purposes.

```
<!-- production environment hazelcast instance name -->
<bean id="defaultHazelcastInstance" class="java.lang.String">
  <constructor-arg value="eidasHazelcastInstance"/>
</bean>
```

Figure 4: Default Hazelcast instance name

The default instance is provided by the `eidasHazelcastInstanceInitializer` bean.

```
<!-- production environment hazelcast initializer bean - injected into map
providers -->
<bean id="eidasHazelcastInstanceInitializer" class="
eu.eidas.auth.commons.cache.HazelcastInstanceInitializer" init-
method="initializeInstance" lazy-init="true">
  <property name="hazelcastConfigfileName" value="hazelcast.xml"/>
  <property name="hazelcastInstanceName" ref="defaultHazelcastInstance"/>
</bean>
```

Figure 5: Default Hazelcast instance provider bean

This bean is to be injected into `ConcurrentMapServiceDistributedImpl` and `ConcurrentMapServiceDistributedImpl` beans. If the distributed environment requires setup of multiple Hazelcast instances, the configuration can be done simply adding more of the above beans to `applicationContext` and `specificApplicationContext` files.

```
<bean id="springServiceCMapAntiReplayProviderProd"
class="eu.eidas.auth.commons.cache.ConcurrentMapServiceDistributedImpl"
lazy-init="true">
  <property name="hazelcastInstanceInitializer"
ref="eidasHazelcastInstanceInitializer"/>
  <property name="cacheName" value="antiReplayCacheService"/>
</bean>
<bean id="springConnectorCMapAntiReplayProviderProd"
class="eu.eidas.auth.commons.cache.ConcurrentMapServiceDistributedImpl"
lazy-init="true">
  <property name="hazelcastInstanceInitializer"
ref="eidasHazelcastInstanceInitializer"/>
  <property name="cacheName" value="antiReplayCacheConnector"/>
</bean>
```

Figure 6: Anti-replay cache configuration — Hazelcast — `applicationContext.xml`

For correlation maps, there are three `AuthRequest` type maps in `ApplicationContext`, one for the Connector, two for the Proxy Service one of which is for the Specific.

```
<bean id="springServiceCMapsSpecificSpCorProviderProd"
class="eu.eidas.auth.commons.cache.ConcurrentMapServiceDistributedImpl" lazy-
init="true">
  <property name="hazelcastInstanceInitializer"
ref="eidasHazelcastInstanceInitializer"/>
  <property name="cacheName" value="specificSpRequestCorrelationCacheService"/>
</bean>
<bean id="springConnectorCMapCorProviderProd"
class="eu.eidas.auth.commons.cache.ConcurrentMapServiceDistributedImpl" lazy-
init="true">
  <property name="hazelcastInstanceInitializer"
ref="eidasHazelcastInstanceInitializer"/>
  <property name="cacheName" value="connectorRequestCorrelationCacheService"/>
</bean>
<bean id="springServiceCMapCorProviderProd"
class="eu.eidas.auth.commons.cache.ConcurrentMapServiceDistributedImpl" lazy-
init="true">
```

```
<property name="hazelcastInstanceInitializer"
ref="eidasHazelcastInstanceInitializer"/>
<property name="cacheName"
value="proxyServiceRequestCorrelationCacheService"/>
</bean>
```

Figure 7: Correlation map cache configuration — Hazelcast — applicationContext.xml

For the Specific part, `specificSpRequestCorrelationMap`, the map instance must be the same as used in the eIDAS-Node (`springServiceCMapsSpecificSpCorProvider`). `LightRequest` map types are defined here.

```
<bean id="springServiceCMapsSpecificIdpCorProviderProd"
class="eu.eidas.auth.commons.cache.ConcurrentMapServiceDistributedImpl" lazy-
init="true">
  <property name="hazelcastInstanceInitializer"
ref="eidasHazelcastInstanceInitializer"/>
  <property name="cacheName" value="specificIdpRequestCorrelationCacheService"/>
</bean>
<!-- LightRq correlation maps -->
<bean id="springConnectorCMapsSpecificLightCorProviderProd"
class="eu.eidas.auth.commons.cache.ConcurrentMapServiceDistributedImpl" lazy-
init="true">
  <property name="hazelcastInstanceInitializer"
ref="eidasHazelcastInstanceInitializer"/>
  <property name="cacheName"
value="specificConnectorLtRequestCorrelationCacheService"/>
</bean>
<bean id="springServiceCMapsSpecificLightCorProviderProd"
class="eu.eidas.auth.commons.cache.ConcurrentMapServiceDistributedImpl" lazy-
init="true">
  <property name="hazelcastInstanceInitializer"
ref="eidasHazelcastInstanceInitializer"/>
  <property name="cacheName"
value="specificServiceLtRequestCorrelationCacheService"/>
</bean>
```

Figure 8: Correlation map cache configuration — Hazelcast — specificApplicationContext.xml

For more information about the Hazelcraft product, please refer to section 7.3 — *Set up Hazelcast* and Appendix C.

4.2.5.6. Error Codes and Error Messages

The full list of eIDAS-Node error codes and related error messages is shown in the *eIDAS-Node Error Codes* document. Each error message must be used to match the error to present to the citizen (`errors.properties` file), to present to `sysadmin` (`sysadmin.properties`) and to translate in the Connector the errors from the Proxy Service.

For each error message a new property should exist in the following files:

- EIDAS-NODE/src/main/resources/error.properties
- EIDAS-NODE/src/main/resources/sysadmin.properties
- EIDAS-NODE/src/main/resources/eidastranslation.properties

For example, for the following `eidasErrors.properties` property:

```
connectorSAMLResponse.message=error.gen.connector.saml
```

you must add the following in the `error.properties`:

```
authenticationFailed.code=003002
authenticationFailed.message=authentication.failed
```

You must also add the following property to `sysadmin.properties` in the native Proxy Service language:

```
authentication.failed={0} - Authentication Failed.
```

Note: This format is mandatory: `{0} - Error Message.`

Using the same format, you must add the following property to `eidastranslation.properties` in the native eIDAS-Node Connector language:

```
authentication.failed={0} - A autenticação falhou.
```

Bear in mind that you must have as many `error.properties` files as the required languages. The file name follows the standards:

- `error_pt.properties` (i.e. Portuguese language)
- `error_es.properties` (i.e. Spanish language)
- `error_en.properties` (i.e. English language)

4.2.6. Specific properties

For the Basic Setup, you might need to reconfigure MS-Specific module Configuration for that application as detailed in the *eIDAS-Node Demo Tool Installation and Configuration Guide*.

4.2.7. Demo Service Provider

For the Basic Setup, you might need to reconfigure Demo Service Provider. Configuration for that application is detailed in the *eIDAS-Node Demo Tool Installation and Configuration Guide*.

4.2.8. Demo Identity Provider

In order to proceed with Basic Setup, you might need to modify the configuration of Demo Identity Provider. The procedure and settings are detailed in the *eIDAS-Node Demo Tool Installation and Configuration Guide*.

5. Building and deploying the software

This section describes the steps to build and then to deploy the software on the supported servers. There are two main types of eIDAS-Node: Connector and Proxy Service.

The project build files are in **Maven3** format, so you need to install Maven. Download instructions are provided at <http://maven.apache.org/run-maven/index.html>). Recommended versions of Maven are 3.3.9 and above. Lower versions can result in exceptions.

There are two ways to build the binaries from sources:

1. **Parent build:** the pom.xml file in the EIDAS-Parent module is a common reference for all dependent module/external Maven artifact versions, and able to build all binaries including Demo Tools. Issuing Maven "install" command with the appropriate activation profile (e.g.: -P weblogic for WebLogic) will result in a full build.
2. **Module-based build:** it is possible to build the artifacts one-by-one, which can be helpful if there is a need to build just one module. In this case please don't forget the dependencies between them. There is a certain order that needs to be followed.

The next sections detail the above two methods for supported application servers.

5.1. Tomcat/GlassFish server deployment

You must compile, install and deploy the projects, either by compiling the parent project or by compiling each module separately in the order shown below. At a command prompt, navigate to the folder shown below and enter the corresponding command line.

- **Note:** \$GLASSFISH_HOME refers to the base directory of your GlassFish server (e.g. /home/user/apps/glassfishv3).

Table 15: Parent project build for Tomcat/GlassFish Server deployment

Step	Folder	Command line
1	EIDAS-Parent	<code>mvn clean install -P tomcat</code>
2	EIDAS-Node	Tomcat: <code>copy target/EidasNode.war \$TOMCAT_HOME/webapps/EidasNode.war</code> GlassFish: <code>copy target/EidasNode.war \$GLASSFISH_DOMAIN/autodeploy/EidasNode.war</code>
3	EIDAS-SP	Tomcat: <code>copy target/SP.war \$TOMCAT_HOME/webapps/SP.war</code> GlassFish: <code>copy target/SP.war \$GLASSFISH_DOMAIN/autodeploy/SP.war</code>

Step	Folder	Command line
4	EIDAS-IdP-1.0	<p>Tomcat: copy target/IdP.war \$TOMCAT_HOME/webapps/IdP.war</p> <p>GlassFish: copy target/IdP.war \$GLASSFISH_DOMAIN/autodeploy/IdP.war</p>

Table 16: Module-based build for Tomcat/GlassFish Server deployment

Step	Folder	Command line
1	EIDAS-Parent	mvn clean install
2	EIDAS-Light-Commons	mvn clean install
3	EIDAS-Commons	mvn clean install
4	EIDAS-SpecificCommunicationDefinition	mvn clean install
5	EIDAS-Encryption	mvn clean install
6	EIDAS-ConfigModule	mvn clean install
7	EIDAS-SAMLEngine	mvn clean install
8	EIDAS-Updater	mvn clean install
9	EIDAS-Specific	mvn clean install
10	EIDAS-Node	<p>a. mvn clean package -P tomcat</p> <p>b.</p> <p>Tomcat: copy target/EidasNode.war \$TOMCAT_HOME/webapps/EidasNode.war</p> <p>GlassFish: copy target/EidasNode.war \$GLASSFISH_DOMAIN/autodeploy/EidasNode.war</p>
11	EIDAS-SP	<p>a. mvn clean package -P tomcat</p> <p>b.</p> <p>Tomcat: copy target/SP.war \$TOMCAT_HOME/webapps/SP.war</p> <p>GlassFish: copy target/SP.war \$GLASSFISH_DOMAIN/autodeploy/SP.war</p>

Step	Folder	Command line
12	EIDAS-IdP-1.0	a. <code>mvn clean package -P tomcat</code> b. Tomcat: <code>copy target/IdP.war \$TOMCAT_HOME/webapps/IdP.war</code> GlassFish: <code>copy target/IdP.war \$GLASSFISH_DOMAIN/autodeploy/IdP.war</code>

5.2. JBoss7 Server deployment

You must compile, install and deploy the projects, either by compiling the parent project or by compiling each module separately in the order shown below. At a command prompt, navigate to the folder shown below and enter the corresponding command line.

Note: The `$SERVER_CONFIG` variable refers to JBoss server configuration name (e.g. default)

If you want to use the 'default' configuration server, your full path will be:
`/home/user/apps/jboss-7.4.0.GA/server/default`

Table 17: Project build for JBoss7 Server deployment

Step	Folder	Command line
1	EIDAS-Parent	<code>mvn clean install -P jBoss7</code>
2	EIDAS-Node	<code>copy target/EidasNode.war \$JBoss_HOME/standalone/deployments/EidasNode.war</code>
3	EIDAS-SP	<code>copy target/SP.war \$JBoss_HOME/standalone/deployments/SP.war</code>
4	EIDAS-IdP-1.0	<code>copy target/IdP.war \$JBoss_HOME/standalone/deployments/IdP.war</code>

Table 18: Module-based build for JBoss7 Server deployment

Step	Folder	Command line
1	EIDAS-Parent	<code>mvn clean install</code>
2	EIDAS-Light-Commons	<code>mvn clean install</code>
3	EIDAS-Commons	<code>mvn clean install</code>
4	EIDAS-SpecificCommunicationDefinition	<code>mvn clean install</code>
5	EIDAS-Encryption	<code>mvn clean install</code>

Step	Folder	Command line
6	EIDAS-ConfigModule	mvn clean install
7	EIDAS-SAMLEngine	mvn clean install
8	EIDAS-Updater	mvn clean install
9	EIDAS-Specific	mvn clean install
10	EIDAS-Node	a. mvn clean package -P jBoss7 b. copy target/EidasNode.war \$JBASS_HOME/ standalone/deployments/EidasNode.war
11	EIDAS-SP	a. mvn clean package -P jBoss7 b. copy target/SP.war \$JBASS_HOME/ standalone/deployments/SP.war
12	EIDAS-IdP-1.0	a. mvn clean package -P jBoss7 b. copy target/IdP.war \$JBASS_HOME/ standalone/deployments/IdP.war

5.3. WebLogic Server deployment

You must compile, install and deploy the projects, either by compiling the parent project or by compiling each module separately in the order shown below. At a command prompt, navigate to the folder shown below and enter the corresponding command line.

Table 19: Parent project build for WebLogic Server deployment

Step	Folder	Command line
1	EIDAS-Parent	mvn clean install -P weblogic
2	EIDAS-Node	copy target/EidasNode.war \$WLS_HOME/DOMAIN/ autodeploy/EidasNode.war
3	EIDAS-SP	copy target/SP.war \$WLS_HOME/DOMAIN/ autodeploy/SP.war
4	EIDAS-IdP-1.0	copy target/IdP.war \$WLS_HOME/DOMAIN/ autodeploy/IdP.war

Table 20: Module-based build for WebLogic Server deployment

Step	Folder	Command line
1	EIDAS-Parent	mvn clean install
2	EIDAS-Light-Commons	mvn clean install

Step	Folder	Command line
3	EIDAS-Commons	mvn clean install
4	EIDAS-SpecificCommunicationDefinition	mvn clean install
5	EIDAS-Encryption	mvn clean install
6	EIDAS-ConfigModule	mvn clean install
7	EIDAS-SAMLEngine	mvn clean install
8	EIDAS-Updater	mvn clean install
9	EIDAS-Specific	mvn clean install
10	EIDAS-Node	a. mvn clean package -P weblogic b. copy target/EidasNode.war \$WLS_HOME/DOMAIN/autodeploy/EidasNode.war
11	EIDAS-SP	a. mvn clean package -P weblogic b. copy target/SP.war \$WLS_HOME/DOMAIN/autodeploy/SP.war
12	EIDAS-IdP-1.0	a. mvn clean package -P weblogic b. copy target/IdP.war \$WLS_HOME/DOMAIN/autodeploy/IdP.war

5.4. WebSphere Server deployment

You must compile, install and deploy the projects, either by compiling the parent project or by compiling each module separately in the order shown below using WebSphere's Admin Console. At a command prompt, navigate to the folder shown below and enter the corresponding command line:

Table 21: Parent project build for WebSphere Server deployment

Step	Folder	Command line
1	EIDAS-Parent	mvn clean install -P websphere After the build has been done, deploy EidasNode.war, IdP.war and SP.war.

Table 22: Module-based build for WebSphere Server deployment

Step	Folder	Command line
1	EIDAS-Parent	mvn clean install
2	EIDAS-Light-Commons	mvn clean install
3	EIDAS-Commons	mvn clean install
4	EIDAS-SpecificCommunicationDefinition	mvn clean install
5	EIDAS-Encryption	mvn clean install
6	EIDAS-ConfigModule	mvn clean install
7	EIDAS-SAMLEngine	mvn clean install
8	EIDAS-Updater	mvn clean install
9	EIDAS-Specific	mvn clean install
10	EIDAS-Node	mvn clean package -P websphere
11	EIDAS-SP	mvn clean package -P websphere
12	EIDAS-IdP-1.0	mvn clean package -P websphere

6. Verifying the installation

This section shows the final structure of your application server relevant directories, so that you can confirm that you have made the proper configurations. The structure of the application's 'war' files is also shown so you can verify that your applications were built successfully.

6.1. Tomcat 7, 8

```
$TOMCAT_HOME/endorsed
  resolver-2.9.1.jar
  serializer-2.7.2.jar
  xalan-2.7.2.jar
  xercesImpl-2.11.0.jar
  xml-apis-1.4.01.jar

$TOMCAT_HOME/webapps/
  IdP.war
  EidasNode.war
  SP.war
(server specific directories were not included)
```

6.2. JBoss 7

- Check modules directory for the presence of BouncyCastle and xml-apis modules.
- Copy war files under \$JBASS_HOME/standalone/Deployments.

6.3. GlassFish V3, V4

6.3.1. GlassFish V3

```
$GLASSFISH_HOME/glassfish/lib/endorsed/
  resolver-2.9.1.jar
  serializer-2.7.2.jar
  xalan-2.7.2.jar
  xercesImpl-2.11.0.jar
  xml-apis-1.4.01.jar

$GLASSFISH_HOME/glassfish/domains/domain1/autodeploy/
  IdP.war
  EidasNode.war
  SP.war
(server specific directories were not included)
```

6.3.2. GlassFish V4

```
$GLASSFISH_DOMAIN/lib/ext/
  xml-apis-1.4.01.jar

$GLASSFISH_DOMAIN/autodeploy/
  IdP.war
  EidasNode.war
  SP.war
```

(server specific directories were not included)

6.4. WebLogic

```
$WLS_HOME/domain/autodeploy/
    IdP.war
    EidasNode.war
    SP.war
    (server specific directories were not included)

$DOMAIN_HOME/lib/
    xml-apis-1.4.01.jar
```

6.5. WebSphere Application Server

WebSphere Application Server 8.5.5 has no requirement to add/replace endorsed libraries. The deployment of the WAR files may be done using the admin console.

Note: for WebSphere Liberty Profile deployment see section 3.2.8 — *Configuring WebSphere Liberty Profile*.

6.6. Configuration files

The below configuration and keystore files are needed for the full installation with Demo Tools. The layout itself can be different, depending on the environment variables, so this is just an example of Basic Setup:

```
server/eidas.xml
server/encryptionConf.xml
server/EncryptModule_Connector.xml
server/EncryptModule_Service.xml
server/hazelcast.xml
server/saml-engine-additional-attributes.xml
server/SamlEngine.xml
server/SamlEngine_Connector.xml
server/SamlEngine_Service.xml
server/SignModule_Connector.xml
server/SignModule_Service.xml
server/idp/EncryptModule_IdP.xml
server/idp/idp.properties
server/idp/IdPSamlEngine.xml
server/idp/saml-engine-additional-attributes.xml
server/idp/saml-engine-eidas-attributes.xml
server/idp/SamlEngine_IdP.xml
server/idp/SignModule_IdP.xml
server/idp/user.properties
server/sp/EncryptModule_SP.xml
server/sp/saml-engine-additional-attributes.xml
server/sp/saml-engine-eidas-attributes.xml
server/sp/SamlEngine_SP.xml
server/sp/SignModule_SP.xml
server/sp/sp.properties
server/sp/SPSamlEngine.xml
server/specific/eidas_Specific.xml
server/specific/EncryptModule_SP-Specific.xml
server/specific/EncryptModule_Specific-IdP.xml
server/specific/saml-engine-additional-attributes.xml
server/specific/SamlEngine_SP-Specific.xml
```

```
server/specific/SamlEngine_Specific-IdP.xml
server/specific/SignModule_SP-Specific.xml
server/specific/SignModule_Specific-IdP.xml
server/specific/SpecificSamlEngine.xmlkeystore/demokeys.jks
keystore/eidasKeyStore.jks
keystore/eidasKeyStore_Connector_CA.jks
keystore/eidasKeyStore_Connector_CB.jks
keystore/eidasKeyStore_Connector_CC.jks
keystore/eidasKeyStore_Connector_CD.jks
keystore/eidasKeyStore_Connector_CF.jks
keystore/eidasKeyStore_IDP_CA.jks
keystore/eidasKeyStore_IDP_CB.jks
keystore/eidasKeyStore_IDP_CC.jks
keystore/eidasKeyStore_IDP_CD.jks
keystore/eidasKeyStore_IDP_CF.jks
keystore/eidasKeyStore_METADATA.jks
keystore/eidasKeyStore_Service_CA.jks
keystore/eidasKeyStore_Service_CB.jks
keystore/eidasKeyStore_Service_CC.jks
keystore/eidasKeyStore_Service_CD.jks
keystore/eidasKeyStore_Service_CF.jks
keystore/eidasKeyStore_SP_CA.jks
keystore/eidasKeyStore_SP_CB.jks
keystore/eidasKeyStore_SP_CC.jks
keystore/eidasKeyStore_SP_CD.jks
keystore/eidasKeyStore_SP_CF.jks
```

7. Advanced configuration for production environments

This section provides detailed descriptions of the configurations to enable you to change specific aspects as required.

7.1. Clustering environment

This section describes the technologies and configurations used for testing the eIDAS-Node in cluster mode. The choice of technologies is proposed for testing purpose.

7.1.1. Load balancer

The configuration adopted is the following:

- One load balancer composed of two Tomcat 7 (version 7.0.55) servers including the eIDAS-Node;
- One Apache Http server to isolate SP/IDP request.

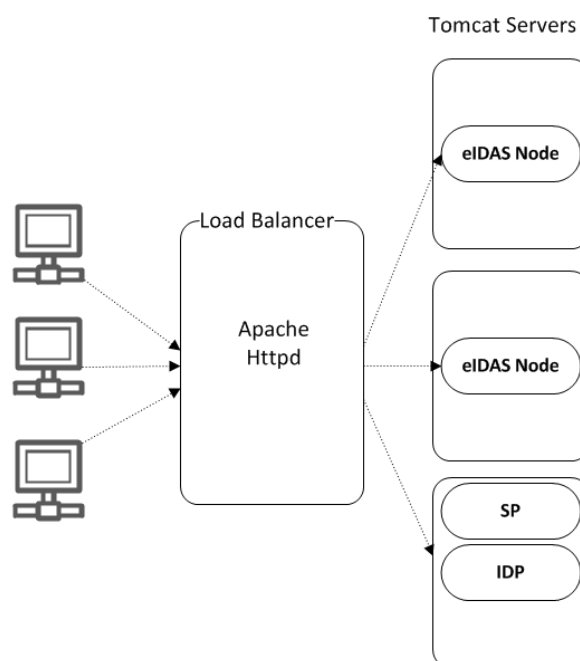


Figure 9: Clustering environment — Load balancer

The solution is to add one server in-front of all tomcat clusters to accept all the requests and distribute to the cluster. So this server acts as a **load balancer**.

There are several servers available with load balancing capability. Here we are going to use **Apache httpd** web server as a load balancer. With **mod_jk** module.

If one of the Tomcat instances fails then the load balancer dynamically reacts by ceasing to forward requests to that failed Tomcat instances. Other Tomcat instances continue as normal.

If the failed Tomcat is recovered from the failed state to normal state the load balancer will include it in the cluster to receive requests.

7.1.2. Load balancer with Hazelcast

Hazelcast gives **High availability and full fail-over capability** to our clustering environment.

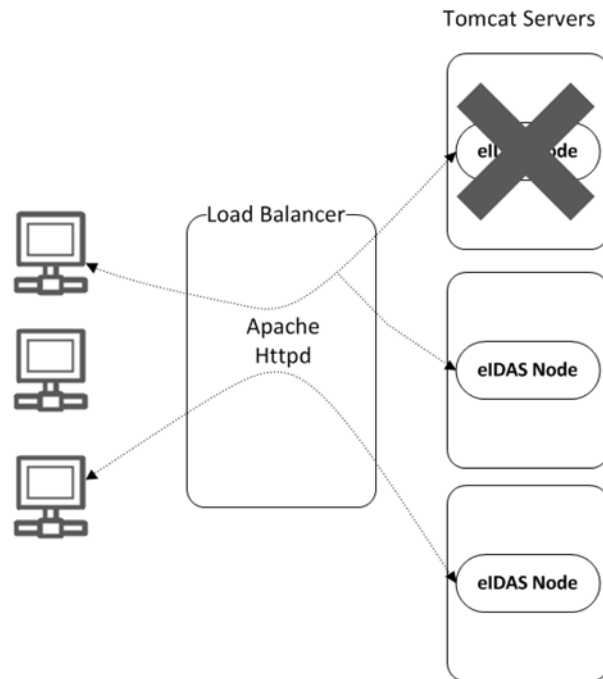


Figure 10: Clustering environment — Load Balancer with Hazelcast

For Hazelcast, replication of message exchange states (in correlation maps) needs to be set up (see section 7.3 — *Set up Hazelcast*).

7.2. Configuring Tomcat

7.2.1. Setting AJP ports

Traffic is passed between Apache and Tomcat(s) uses the binary AJP 1.3 protocol

Application Server	Http port	AJP port	Requests
Tomcat 7 – instance 1	Tomcat 1 port	8209	Connector, Proxy Service
Tomcat 7 – instance 2	Tomcat 2 port	8309	Connector, Proxy Service
Tomcat 7 - instance 3	Tomcat 3 port	8409	SP, IDP

7.2.2. Apache HTTPD

In this section we will use **Apache httpd** web server as a Load Balancer.

To provide the load balancing capability to Apache httpd server we need to include the module **mod_jk**.

7.2.2.1. Install and configure mod_jk

The **mod_jk** module is downloaded from <http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/>.

mod_jk is the Apache HTTPD module that will be used to provide our cluster with its load balancing and proxy capabilities, by default it uses the 'round robin' algorithm to distribute the requests. It uses the AJP protocol to facilitate fast communication between Tomcat servers and the Apache Web Server that will receive the client requests.

Configuration consists of adding a few lines to the main Apache HTTPD configuration file `httpd.conf`:

```
JkMount /status stat
JkMount /EidasNode/* balancer
JkMount /SP/* tomcat3
JkMount /IdP/* tomcat3
```

7.2.2.2. Configure the cluster workers

'Workers' is a blanket term used within **mod_jk** to refer to both real Tomcat servers that will process requests, and virtual servers included in the module to handle load balancing and monitoring.

File: workers.properties

By default, **mod_jk** includes three additional load balancing algorithms, some of which are more appropriate for certain situations, and can be configured with the 'method' directive:

```
worker.list=balancer,stat,tomcat3
worker.tomcat1.type=ajp13
worker.tomcat1.port=8209
worker.tomcat1.host=localhost
worker.tomcat2.type=ajp13
worker.tomcat2.port=8309
worker.tomcat2.host=localhost
worker.tomcat3.type=ajp13
worker.tomcat3.port=8409
worker.tomcat3.host=localhost
worker.balancer.type=lb
worker.balancer.balance_workers=tomcat1,tomcat2
```

7.3. Set up Hazelcast

To replicate required information between cluster members, all nodes need to be configured with Hazelcast. Please refer to section 4.2.5.5 — *Additional Configuration*

— *Anti-replay Cache and Correlation Map Configuration* and Appendix C for information on how to implement the required configuration.

7.4. Check your installation

Open the Apache status page: <http://localhost/status> and check that each node is up and running.

The screenshot shows the Apache status page in a web browser. The address bar displays vs-cis-12/status. The page content includes:

[\[Read Only\]](#) [\[Dump\]](#) [S=Show only this worker, E=Edit worker, R=Reset worker state, T=Try worker recovery]

Listing Load Balancing Worker (1 Worker) [\[Hide\]](#)

[\[S\]](#)[\[E\]](#)[\[R\]](#) Worker Status for balancer

Type	Sticky Sessions	Force Sticky Sessions	Retries	LB Method	Locking	Recover	Wait Time	Error Escalation	Time	Max Reply Timeouts
lb	True	False	2	Request	Optimistic	60	30	0		

Good Degraded Bad/Stopped Busy Max Busy Next Maintenance Last Reset [\[Hide\]](#)

2	0	0	0	0	19/81	279
---	---	---	---	---	-------	-----

Balancer Members [\[Hide\]](#)

Name	Type	Hostname	Address:Port	Connection Pool	Timeout	Connect	Timeout	Prepost	Timeout	Reply	Timeout	Retries	Recovery	Options	Max Packet Size
tomcat1	ajp13	localhost	127.0.0.1:8209	0	0	0	0	0	0	0	0	2	0		65536
tomcat2	ajp13	localhost	127.0.0.1:8309	0	0	0	0	0	0	0	0	2	0		65536

Name	Act	State	D	F	M	V	Acc	Sess	Err	CE	RE	Wr	Rd	Busy	Max	Con	Route	RR	Cd	Rs	LR	LE	
[S] [E] [R] tomcat1	ACT	OK/IDLE	0	1	1	0	0	0 (0/sec)	0	0 (0/sec)	0	0	0	0 (0/sec)	0	0 (0/sec)	0	0	0	0	0	0	279
[S] [E] [R] tomcat2	ACT	OK/IDLE	0	1	1	0	0	0 (0/sec)	0	0 (0/sec)	0	0	0	0 (0/sec)	0	0 (0/sec)	0	0	0	0	0	0	279

Edit this attribute for all members:

URI Mappings for balancer (1 maps) [\[Hide\]](#)

Server	URI	Match	Type	Source	Reply	Timeout	Sticky	Ignore	Stateless	Fail on	Status	Active	Disabled	Stopped	Use	Server	Errors
VS-CIS-K2.net1.ccc.eu.int:80	/PEPS/*	Wildchar	JkMount	-1	0	0	-	-	-	-	-	-	-	-	0		

Listing AJP Worker (1 Worker) [\[Hide\]](#)

[\[S\]](#)[\[E\]](#)[\[R\]](#) Worker Status for tomcat3

Figure 11: Apache status page

SER

Worker Status for tomcat3

Type

Hostname

Address:Port

Connection Pool

Timeout

Connect

Timeout

Prepost

Timeout

Reply

Timeout

Retries

Recovery

Options

Max Packet Size

[Hide]

ajp13

localhost

127.0.0.1:8409

0

0

0

0

2

0

State

Acc

Err

CE

RE

Wr

Rd

Busy

Max

Con

LR

LE

OK/IDLE

0

(0/sec)

0

0

0

(0/sec)

0

(0/sec)

0

0

0

279

URI Mappings for tomcat3

(3 maps)

[Hide]

Server

URI

Match

Type

Source

Reply

Timeout

Sticky

Ignore

Stateless

Fail on

Status

Active

Disabled

Stopped

Use

Server

Errors

VS-CIS-K2.net1.cec.eu.int:80

/IdP/*

Wildchar

JkMount

-1

0

0

-

-

-

-

-

-

0

VS-CIS-K2.net1.cec.eu.int:80

/AP/*

Wildchar

JkMount

-1

0

0

-

-

-

-

-

-

0

VS-CIS-K2.net1.cec.eu.int:80

/SP/*

Wildchar

JkMount

-1

0

0

-

-

-

-

-

-

0

Legend

[Hide]

Name

Worker name

Type

Worker type

Route

Worker route

Act

Worker activation configuration

ACT=Active, DIS=Disabled, STP=Stopped

State

Worker error status

OK=OK, ERR=Error with substates

IDLE=No requests handled, BUSY=All connections busy,

REC=Recovering, PRB=Probing, FRC=Forced Recovery

D

Worker distance

F

Load Balancer factor

M

Load Balancer multiplicity

V

Load Balancer value

Acc

Number of requests

Sess

Number of sessions created

Err

Number of failed requests

Figure 12: Apache status page (continued)

7.5. eIDAS-Node compliance

To ensure the eIDAS compliance, there is a list of parameters to specifically set. Those parameters are listed below.

Table 23: eIDAS-Node compliance

Parameter	Resulting value
disallow_self_signed_certificate	True: do not allow self-signed and expired certificates
check_certificate_validity_period	True: do not allow expired certificates
metadata.activate	True: specifies that metadata is generated by the Connector
metadata.restrict.http	True : metadata must be only available via HTTPS
tls.enabled.protocols	TLSv1.1,TLSv1.2: SSL/TLS enabled protocols
metadata.check.signature	True : metadata received from a partner must be signed
metadata.validity.duration	Metadata validity period in seconds. Default=86400 (i.e. one day)

Parameter	Resulting value
<code>response.encryption.mandatory</code>	True: do not allow response not encrypted
<code>Validate.binding</code>	True: the bindings are validated
<code>security.header.csp.enabled</code>	True: the content-security and security checks are enabled (HSTS, Mozilla directives, X-content-Type-Options, X-frame-options,
<code>disable.check.mandatory.eidas.attributes</code>	False: check the eIDAS minimum dataset constraint. Note: this parameter is used by both Proxy Service and Connector.
<code>disable.check.representative.attributes</code>	False: check the existence of Representative attributes in requests. Note: this parameter is used by both eIDAS-Node Proxy Service and eIDAS-Node Connector.
<code>disable.check.representative.attributes</code>	False: check the eIDAS Request representative rule (must not contain representative attributes). Note: this parameter is used by both Proxy Service and Connector.
<code>response.encryption.mandatory</code>	True : check if the response payload is encrypted
<code>check.citizencertificate.serviceCertificate</code>	True : check if the CN of the certificate used for signing the response is the same than the citizen country of the SamlRequest

To ensure compliance, the following checks are made:

- the Level of Assurance indicated in the Assertion matches or exceeds the requested Level of Assurance;
- the Response will not be transmitted to a URL other than the AssertionConsumerServiceURL in the metadata of the eIDAS-Node Connector.

Remark: To improve the resilience of the application, we strongly recommend using the cache instances used for request anti-replay and SAML metadata using Hazelcast services. (please see Appendix C for further details)

7.6. eIDAS-Node configuration recommendations check list for production

To be compliant with the eIDAS regulation, there are things to consider when installing the software in a production environment.

Appendix A. eIDAS Levels of Assurance

Level of Assurance (LoA) is a term used to describe the degree of certainty that an individual is who they say they are at the time they present a digital credential.

The eIDAS implementing regulation determines three Levels of Assurance:

- **Low** (service.LoA=http://eid.as.europa.eu/LoA/**low**)
- **Substantial** (service.LoA=http://eid.as.europa.eu/LoA/**substantial**)
- **High** (service.LoA=http://eid.as.europa.eu/LoA/**high**)

(The eIDAS-Node Proxy Service `service.LoA` key is described in Table 7.)

At the SAML Request level, the level of assurance will limit the comparison attribute to 'minimum':

- `<saml2p:RequestedAuthnContext Comparison="minimum">`

Validations made:

At the eIDAS-Node Proxy Service, if the requested (or higher) Level of Assurance cannot be fulfilled, the Request **MUST** be rejected.

The eIDAS-Node Connector verifies that the Level of Assurance indicated in the Assertion matches or exceeds the requested Level of Assurance, and sends the received authenticated person identification data to the requesting relying party.

The legal definitions of the Level of Assurance can be found at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_235_R_0002&from=EN.

Appendix B. User consent

In most Member States (MS), the privacy legislation requires that the user gives consent to the use of personal data. But the explanation of this requisite, and thus its implementation may be very different from one MS to another MS. So this general objective to request the consent of the user to send his/her attributes to a Service Provider in another Member State leads to the following consent-schemes. The consent is requested by the eIDAS-Node or by the Middleware of the user's MS.

There are three possible cases:

- The requested attributes are displayed and the user's consent is given by choosing only the attributes that he/she allows to transfer;
- The obtained values of the requested attributes are displayed and the user's consent is given by choosing only the attributes that he/she allows to transfer;
- The requested attributes are not displayed because the user's consent is not required as it was given (for example) when the user registered to the ID Provider.

Appendix C. Hazelcast proposed configuration

To correlate between request/response messages, and to prevent a replay of SAML requests, a caching mechanism is implemented at the eIDAS-Node Connector and Proxy Service level.

For clustered production mode (see section 7.5 — *eIDAS-Node compliance*), the application needs to be configured using Hazelcast product, which will provide a reliable solution based on a distributed hashmap, cluster-ready and with expiration of requests. The configuration of the product is done via its configuration file `hazelcast.xml` located by `EIDAS_CONFIG_REPOSITORY`. A default configuration is provided with the application. It is also possible to implement other clustering solutions by enriching the provided code. Please note, the provided configuration does not cover persistence. If persistence is required, a central database and MapStore interface must be implemented. Spring injection of map provider makes it possible on an entry level.

Hazelcast maps are activated by setting `distributedMaps` to "true" in `eidas.xml`.

C.1 Network configuration

The join configuration element is used to enable the Hazelcast instances to form a cluster, i.e. to join the members. Three ways can be used to join the members:

- multicast;
- discovery by TCP/IP;
- discovery by AWS (EC2 auto discovery).

C.1.1 Multicast

In the default configuration, we recommend the multicast configuration for clustering use.

With the multicast auto-discovery mechanism, Hazelcast allows cluster members to find each other using multicast communication. The cluster members do not need to know the concrete addresses of the other members, they just multicast to all the other members for listening. It depends on your environment whether multicast is possible or allowed.

The following is an example declarative configuration.

```
<network>
  <join>
    <multicast enabled="true">
      <multicast-group>224.2.2.3</multicast-group>
      <multicast-port>54327</multicast-port>
      <multicast-time-to-live>32</multicast-time-to-live>
      <multicast-timeout-seconds>2</multicast-timeout-seconds>
      <trusted-interfaces>
        <interface>192.168.1.102</interface>
      </trusted-interfaces>
    </multicast>
    <tcp-ip enabled="false">
    </tcp-ip>
    <aws enabled="false">
  </join>
</network>
```



```

    </aws>
  </join>
</network>

```

Figure 13: Example Hazelcast multicast declarative configuration

Note: The `multicast-timeout-seconds` element is significant. This specifies the time in seconds that a node should wait for a valid multicast response from another node running in the network before declaring itself as the leader node (the first node joined to the cluster) and creating its own cluster. This only applies to the startup of nodes where no leader has yet been assigned. If you specify a high value to `multicast-timeout-seconds`, such as 60 seconds, it means that until a leader is selected, each node will wait 60 seconds before moving on. Be careful when providing a high value. Also be careful to not set the value too low, or the nodes may give up too early and create their own cluster.

C.1.2 Discovery by TCP/IP Cluster

If multicast is not preferred as the way of discovery for your environment, then you can configure Hazelcast for full TCP/IP cluster. As the configuration in Figure 14 shows, when the `enable` attribute of `multicast` is set to `false`, `tcp-ip` has to be set to `true`. For the none-multicast option, all or a subset of nodes' hostnames and/or IP addresses must be listed. Note that not all of the cluster members have to be listed there but at least one of them has to be active in the cluster when a new member joins. The `tcp-ip` tag accepts an attribute called `connection-timeout-seconds` (default value = 5). Increasing this value is recommended if you have many IPs listed and members cannot properly build up the cluster.

```

<hazelcast>
  ...
  <network>
    <port auto-increment="true">5701</port>
    <join>
      <multicast enabled="false">
        <multicast-group>224.2.2.3</multicast-group>
        <multicast-port>54327</multicast-port>
      </multicast>
      <tcp-ip enabled="true">
        <member>machine1</member>
        <member>machine2</member>
        <member>machine3:5799</member>
        <member>192.168.1.0-7</member>
        <member>192.168.1.21</member>
      </tcp-ip>
    </join>
    ...
  </network>
  ...
</hazelcast>

```

Figure 14: Example Hazelcast configuration for TCP/IP discovery

C.1.3 Discovery by AWS (EC2 auto discovery)

Hazelcast supports EC2 auto discovery. For information on this configuration please refer to the Hazelcast documentation at <http://docs.hazelcast.org/docs/3.2/manual/html-single/>.

C.1.4 Eviction

Hazelcast also supports policy based eviction for distributed maps. Currently supported eviction policies are LRU (Least Recently Used) and LFU (Least Frequently Used). This feature enables Hazelcast to be used as a distributed cache. If `time-to-live-seconds` is not 0, entries older than `time-to-live-seconds` value will be evicted, regardless of the eviction policy set. In the application, for anti-replay/reply request-pair correlation cache we set by default the `time-to-live-seconds` to 300 (five minutes) and for the cache of metadata to one day.

```
<hazelcast>
...
<map name="antiReplayCacheService">
<time-to-live-seconds>300</time-to-live-seconds> <!-- 5 minutes -->
<eviction-policy>LRU</eviction-policy>
<max-size policy="PER_NODE">500</max-size>
</map>
<map name="antiReplayCacheConnector">
<time-to-live-seconds>300</time-to-live-seconds><!-- 5 minutes -->
<eviction-policy>LRU</eviction-policy>
<max-size policy="PER_NODE">500</max-size>
</map>
<map name="eidasmetadata">
<in-memory-format>BINARY</in-memory-format>
<time-to-live-seconds>86400</time-to-live-seconds><!-- 1 day -->
<eviction-policy>LRU</eviction-policy>
</map>
</hazelcast>
<map name="specificSpRequestCorrelationCacheService">
<in-memory-format>BINARY</in-memory-format>
<time-to-live-seconds>86400</time-to-live-seconds><!-- 1 day -->
<eviction-policy>LRU</eviction-policy>
</map>
<map name="connectorRequestCorrelationCacheService">
<in-memory-format>BINARY</in-memory-format>
<time-to-live-seconds>86400</time-to-live-seconds><!-- 1 day -->
<eviction-policy>LRU</eviction-policy>
</map>
<map name="proxyServiceRequestCorrelationCacheService">
<in-memory-format>BINARY</in-memory-format>
<time-to-live-seconds>86400</time-to-live-seconds><!-- 1 day -->
<eviction-policy>LRU</eviction-policy>
</map>
<map name="specificIdpRequestCorrelationCacheService">
<in-memory-format>BINARY</in-memory-format>
<time-to-live-seconds>86400</time-to-live-seconds><!-- 1 day -->
<eviction-policy>LRU</eviction-policy>
</map>
<map name="specificConnectorLtRequestCorrelationCacheService">
<in-memory-format>BINARY</in-memory-format>
<time-to-live-seconds>86400</time-to-live-seconds><!-- 1 day -->
<eviction-policy>LRU</eviction-policy>
</map>
<map name="specificServiceLtRequestCorrelationCacheService">
<in-memory-format>BINARY</in-memory-format>
```

```
<time-to-live-seconds>86400</time-to-live-seconds><!-- 1 day -->  
<eviction-policy>LRU</eviction-policy>  
</map>
```

Figure 15: Hazelcast eviction policy configuration

For more information on the features of this product, please refer to the Hazelcast official documentation (<http://docs.hazelcast.org/docs/3.2/manual/html-single/>).

Appendix D. Installation Frequently Asked Questions

Q: How can I use my SPECIFIC jar?

A: Just replace the `eidas-specific.1.0.jar`, found in the `EidasNode.war`, by your own.

Q: How can I compile the project using external properties (Tomcat)?

A: First you compile EIDAS-NODE and EIDAS-Specific without the `"-P embedded"` argument. This will generate the packages without specific properties. Now you need to place all the properties files in one folder and tell Tomcat to lookup that folder.

If in Linux:

Edit `$TOMCAT_HOME/bin/catalina.sh` and change

```
"CLASSPATH="$CLASSPATH""$CATALINA_HOME"/bin/bootstrap.jar" to
"CLASSPATH="$CLASSPATH""$CATALINA_HOME"/bin/bootstrap.jar:/path/to/
config/folder/"
```

If in Windows:

Edit `$TOMCAT_HOME/bin/catalina.bat` and change

```
"CLASSPATH="$CLASSPATH""$CATALINA_HOME"/bin/bootstrap.jar" to
"CLASSPATH="$CLASSPATH""$CATALINA_HOME"/bin/bootstrap.jar:/path/to/
config/folder/"
```

Q: I'm getting an error that says "Failed to load class org.slf4j.impl.StaticLoggerBinder" .

A: This error is reported when the `org.slf4j.impl.StaticLoggerBinder` class could not be loaded into memory. In this case, you should recompile your projects to ensure that Maven includes the appropriate jars.

Q: I'm getting an error that says "com.opensymphony.xwork2.DefaultActionInvocation.invokeAction (DefaultActionInvocation.java)" .

A: The `DefaultActionInvocation` class is responsible for calling the user action, if an error occurs, generally due to missing libraries or missing properties file, the struts framework will not be able to render the result of the action, thus producing that error message.

However, in the logs or the stack trace you can usually find another exception. That exception is the reason for this error, perhaps you can solve it by making sure:

- you have the properties files in the right place
- you have the right privileges to access jks file (you may need to install JCE and allow Java to read the file outside the webapp context)
- you have all the required libraries.