Platform Security

This section provides an overview about the security architecture of CAP applications on different platforms.

Table of Contents

Platform Compliance

CAP applications run in a certain environment, that is, in the context of some platform framework that has specific characteristics. The underlying framework has a major impact on the security of the application, regardless of whether it runs a cloud environment or local environment. Moreover, CAP applications are tightly integrated with platform services, in particular with identity and persistence service.

> **End-to-end security necessarily requires compliance with all security policies of all involved components.**

> CAP application security requires consistent security configuration of the underlying platform and all consumed services. Consult the relevant security documentation accordingly.

CAP in Cloud Environment

Currently, CAP supports to run on two cloud runtimes of SAP Business Technology Platform :

- SAP BTP, Cloud Foundry Runtime
- SAP BTP, Kyma Runtime

Application providers are responsible to ensure a **secure platform environment**. In particular, this includes *configuring* platform services the application consumes. For instance, the provider (user) administrator needs to configure the identity service to separate platform users from business users that come from different identity providers. Likewise login policies (for example, multifactor authentication or single-sign-on) need to be aligned with company-specific requirements.

Note, that achieving production-ready security requires to meet all relevant aspects of the **development process** as well. For instance, source code repositories need to be protected and may not contain any secrets or personal data. Likewise, the **deployment process** needs to be secured. That includes not only setting up CI/CD pipelines running on technical platform users, but also defining integration tests to ensure properly secured application endpoints.

As part of **secure operations**, application providers need to establish a patch and vulnerability management, as well as a secure support process. For example, component versions need to be updated and credentials need to be rotated regularly.

> **WARNING**
>
> The application provider is responsible to **develop, deploy, and operate the application in a secure platform environment**. CAP offers seamless integration into platform services and tools to help to meet these requirements.

Find more about BTP platform security here:

↳ *SAP BTP Security*

↳ *SAP BTP Security Recommendations*

↳ *SAP BTP Security (Community)*

CAP in Local Environment

Security not only plays a crucial role in cloud environments, but also during local development. Apparently the security requirements are different from cloud scenario as local endpoints are typically not exposed for remote clients. But there are still a few things to consider because exploited vulnerabilities could be the basis for attacks on productive cloud services:

- Make sure that locally started HTTP endpoints are bound to `localhost`.
- In case you run your service in hybrid mode with bindings to cloud service instances, use cds bind instead of copying bindings manually to `default-env.json` file. `cds bind` avoids materialization of secrets to local disc, which is inherently dangerous.
- Don't write sensitive data to application logs, also not via debug logging.
- Don't test with real business data, for example, copied from a productive system.

SAP BTP Services for Security

SAP BTP provides a range of platform services that your CAP applications can utilize to meet production-grade security requirements. To ensure the security of your CAP applications, it's crucial to comply with the service level agreement (SLA) of these platform services. *As the provider of the application, you play a key role in meeting these requirements by correctly configuring and using these services.*

> **TIP**
>
> SAP BTP services and the underlying platform infrastructure hold various certifications and attestations, which can be found under the naming of SAP Cloud Platform in the SAP Trust Center .

The CAP framework offers flexible APIs that you can integrate with various services, including your custom services. If you replace platform services with your custom ones, it's important to ensure that the service level agreements (SLAs) CAP depends on are still met.

The most important services for security offered by the platform:

↳ *Webcast SAP BTP Cloud Identity and Security Services*

SAP Cloud Identity Services - Identity Authentication

The Identity Authentication service defines the user base for (CAP) applications and services, and allows to control access. Customers can integrate their 3rd party or on-premise identity provider (IdP) and harden security by defining multifactor authentication or by narrowing client IP ranges. This service helps to introduce a strict separation between platform users (provider) and business users (subscribers), a requirement of CAP. It supports various authentication methods, including SAML 2.0 and OpenID Connect , and allows for the configuration of single sign-on access.

↳ *Learn more in the security guide.*

SAP Authorization and Trust Management Service

The service lets customers manage user authorizations in technical roles at application level, which can be aggregated into business-level role collections for large-scale cloud scenarios. Obviously, developers must define application roles carefully as they form basic access rules to business data.

SAP Malware Scanning Service

This service can be used to scan transferred business documents for malware and viruses. Currently, there is no CAP integration. A scan needs to be triggered by the business application explicitly.

↳ *Learn more in the security guide.*

SAP Credential Store

Credentials managed by applications need to be stored in a secure way. This service provides a REST API for (CAP) applications to store and retrieve credentials at runtime.

↳ *Learn more in the security guide.*

SAP BTP Connectivity

The connectivity service allows SAP BTP applications to securely access remote services that run on the Internet or on-premise. It provides a way to establish a secure communication channel between remote endpoints that are connected via an untrusted network infrastructure.

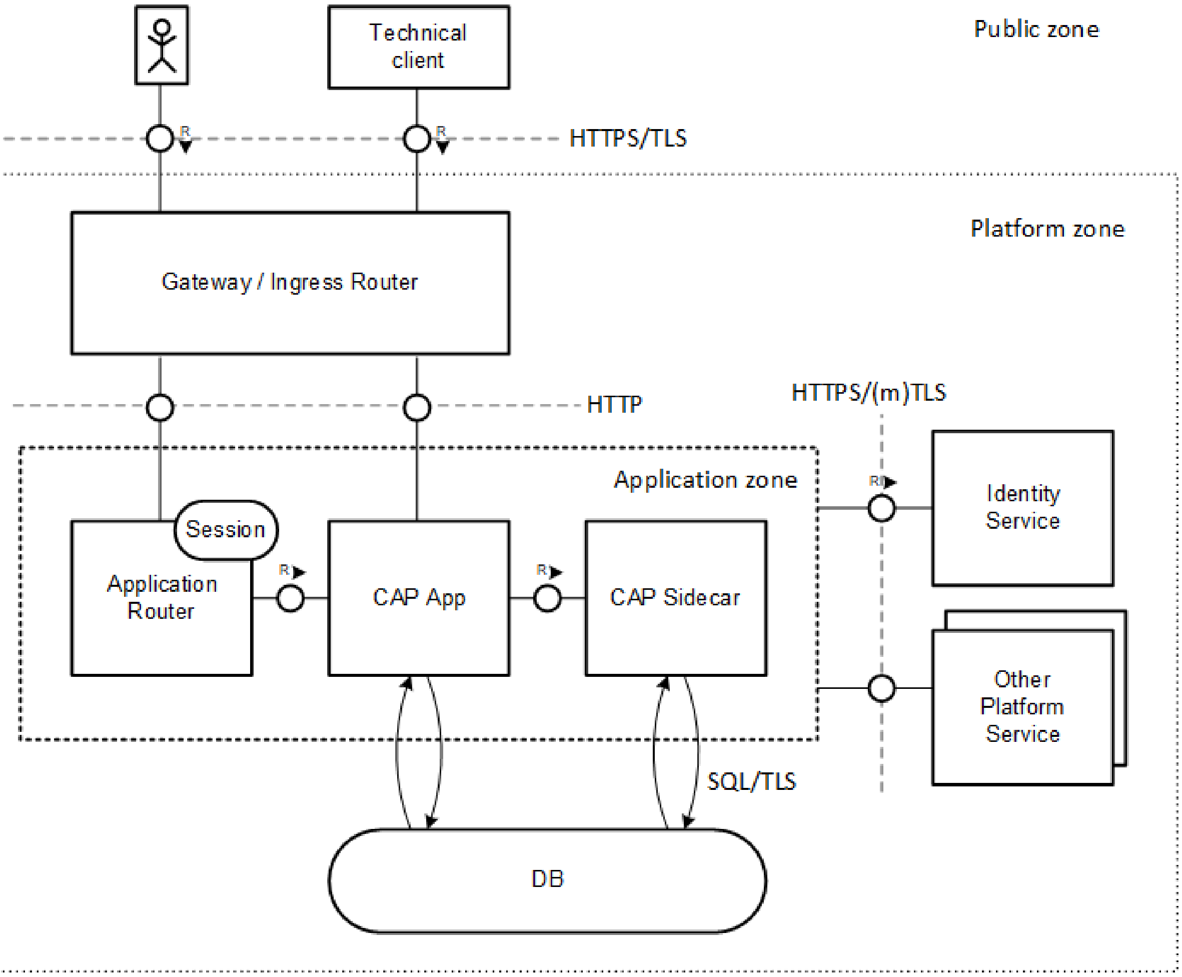
↳ *Learn more in the security guide.*

Architecture and Platform Requirements

As pointed out, CAP cloud applications run in a specific context that has a major impact on the security architecture. CAP requires a dedicated platform environment to integrate with, in order to ensure end-to-end security.

Architecture Overview

The following diagram provides a high-level overview about the security-relevant aspects of a deployed CAP application in a cloud environment:



To serve a business request, different runtime components are involved: a request, issued by a UI or technical client (public zone), is forwarded by a gateway or ingress router to the CAP application. In case of a UI request, an Application Router instance acts as a proxy. The CAP application might make use of a CAP sidecar. All application components (application zone) might make use of platform services such as database or identity service (platform zone).

Public Zone

From CAP's point of view, all components without specific security requirements belong to the public zone. Therefore, you shouldn't rely on the behavior or structure of consumer components like browsers or technical clients for the security of server components. The platform's gateway provides a single point of entry for any incoming call and defines the API visible to the public zone. As malicious users have free access to the public zone, these endpoints need to be protected carefully. Ideally, you should limit the number of exposed endpoints to a minimum, perhaps through proper network configuration.

Platform Zone

The platform zone contains all platform components and services that are *configured and maintained* by the application provider. CAP applications consume these low-level platform services to handle more complex business requests. For instance, persistence service to store business data and identity service to authenticate the business user play a fundamental role.

The platform zone also includes the gateway, which is the main entry point for external requests. Additionally, it may contain extra ingress routers.

Application Zone

The application zone comprises all microservices that represent a CAP application. They are tightly integrated and form a unit of trust. The application provider is responsible to *develop, deploy and operate* these services:

- The Application Router acts as as an optional reverse proxy wrapping the application service and providing business-independent functionality required for UIs. This includes serving UI content, providing a login flow as well as managing the session with the browser. It can be deployed as application (reusable module) or alternatively consumed as a service .

- The CAP application service exposes the API to serve business requests. Usually, it makes use of lower-level platform services. As built on CAP, a significant number of security requirements is covered either out of the box or by adding minimal configuration.

- The optional CAP sidecar (reusable module) is used to outsource application-independent tasks such as providing multitenancy and extension support.

Application providers, that is platform users, have privileged access to the application zone. In contrast, application subscribers, that is business users, are restricted to a minimal interface.

> **WARNING**
>
> ❗ Application providers **may not share any secrets from the application zone** such as binding information with other components or persons. In a productive environment, it is

> recommended to deploy and operate the application on behalf of a technical user.

> TIP
>
> Without limitation of generality, there may be multiple CAP services or sidecars according to common microservice architecture pattern .

Required Platform Environment

There are several assumptions that a CAP application needs to make about the platform environment it is deployed to:

1. Application and (platform) service endpoints are exposed externally by the API gateway via TLS protocol. Hence, the **CAP application can offer a pure HTTP endpoint** without having to enforce TLS and to deal with certificates.

2. The server certificates presented by the external endpoints are signed by a trusted certificate authority. This **frees CAP applications from the need to manage trust certificates.** The underlying runtimes (Java or Node) can validate the server certificates by default.

3. **Secrets** that are required to protect the application or to consume other platform services **are injected by the platform** into the application in a secure way.

All supported environments fulfill the given requirements. Additional requirements could be added in future.

> TIP
>
> Custom domain certificates need to be signed by trusted certificate authority.

> WARNING
>
> ❗ **In general, application endpoints are visible to public zone**. Hence, CAP can't rely on private endpoints. In particular, an application router does not prevent external access to the CAP application service. As a consequence, **all CAP endpoints must be protected in an appropriate manner**.

Previous page
CDS-based Authorization

Next page
Security Aspects