Introduction and Goals

This document describes the architecture of **ZenZefi (*Zentrale Zertifikatsverwaltung*)**, henceforth termed *ZZ*, and **SigModul (*Signatur Modul*)**, henceforth termed *SM*, two applications which are developed during the project **Certificate-based Automotive Security (CeBAS)** by Daimler. The overall function of ZenZefi and SigModul (henceforth also termed *ZZSM*) is to serve certificates to inquiring software clients in the Daimler business divisions Research&Development, Production, Aftersales, but also to external Supplier engineers. Those certificates are requested by ZZSM on behalf of a user from the Daimler backend *CEBAS-PKI (PublicKeyInfrastructur)*. Depending on the user permissions ZZSM provides Diagnostic-, Coding-, EnhancedRights-, SecOC-, TimeReset-, and ECU-certificates to the requesting software client. The following provides a short recap how and where ZZSMM is used.

ZenZefi is a client software application and is deployed and operated/executed on diagnostic testing devices in the Daimler business divisions of Research&Development, Production, and Aftersales, and beyond that, is also provided to external supplier engineers for developing. ZZ mainly manages certificates and computes signatures for coding data on the diagnostic testing device. To query certificates from the PKI, ZZ enables Open ID Connect (using *Authorization-Code Grant*) and authenticates a user against the Daimler GAS-OIDC infrastructure.

SigModul is a backend system and is deployed and operated in the Daimler business divisions Production (assembly-, aggregate-, and battery-plants). Aftersales (VCS and MRS), as well as in Research&Development (CSB@RD). Depending on the business divions SM either computes signature for coding data or distributes diagnostic certificates. SM is hosted on the following environments

- Production-Assembly: plant specific data centers, operated on a Docker run-time infrastructure (SLES based Docker image)
- Production-Aggregate/-Battery: plant specific Windows machine, operated natively on Windows OS
- Aftersales-VCS: European Data Center, operated on a Kubernetes run-time infrastructure
- Aftersales-MRS: European Data Center
- R&D: Daimler Hybrid Cloud, operated on a CloudFoundry infrastructure

SigModul authenticates with a OIDC *Client-Credential Grant* against the PKI to query certificates from the PKI.

Requirements Overview

ZenZefi

ZenZefi is operable on Windows and Linux-based diagnostic testing devices, which run different vehicle diagnostic applications, like Monaco in R&D, ISService+ in production and Xentry Diagnose in Afterssales, depending on the business area.
Due to the heterogenous user communites, like Daimler internal engineers, production workers, AfterSales workshop workers, and external Supplier engineers (Bosch, Continental etc.), the runtime environments range from full-fledged computers to small handheld testing devices (which are provided by different vendors). Therefore, ZZ requirements differ and might even be conflicting. But overall, ZZ must be OS independant and therefore executable on any operating system.

R&D

This chapter describes the requirements for ZenZefi in the Daimler R&D business, where Daimler engineers typically use ZenZefi.

1. **Web-based user interface for certificate management**
   ZenZefi provides a web-based user interface for R&D engineers within the Daimler organisation, which allows the requesting of different certificate types, the importing of certificate of different type as well as the management of the imported certificates and certification requests like deleting and viewing of the certificate details. ZenZefi also provides a system integrity check so that the engineers can get visual feedback if their

installation is correct while executing various tests against the electronic control unit. ZenZefi also provides functionality to the engineer for simulating working with certificates which give him increased or decreased rights to perform certain action thus being able to simulate other roles in the organization like that of assembly line worker.

2. **Authentification to CorpDir**
   In order to be able to request certificates from the PKI ZenZefi needs to provide functionality that integrates with the Daimler corporate directory for authenticating and authorizing the current user.

3. **User management**
   In Daimler business area of R&D it is possible that multiple users will share the same diagnostic testing device and as such the same ZenZefi instance. Therefore ZenZefi supports a registration and login process for multiple users, so that the users can manage their own certificates in their user certificate store. A ZenZefi instance runs on behalf of the currently logged in users and all requests to a ZenZefi instance will be processed using the configuration and the certificate store of the currently logged in user.

4. **Requesting of Certificates**
   ZenZefi provides functionality for requesting of certification requests on behalf of the current user to the PKI. In the business area of R&D ZenZefi will access the PKI infrastructure directly via a RESTful interface.

Production

This chapter describes the requirements for ZenZefi in the Daimler Production business area, where typically assembly line workers use ZenZefi.

1. **Handling of invalid user certificates**
   ZenZefi intermittently checks the validity of diagnostic certificates and requests new certificates if required. ZenZefi will contact the SigModul indirectly via the application ISService+ which also runs locally on the diagnostic testing device.'

2. **Requesting of Certificates**
   ZenZefi provides functionality for requesting of certification requests on behalf of the current user to the PKI.
   In the business area of production ZenZefi will not access the PKI directly. Instead ZenZefi will invoke the diagnostic application ISService+ which will delegate the call further to the ISServer which then contacts the SigModul to retrieve the certificates.
   The SigModul is responsible for retrieving certificates from the PKI and distributing these to the tester devices where ZenZefi will run.

AfterSales

This chapter describes the requirements for ZenZefi in the Daimler AfterSales business area, where typically workshop staff will use ZenZefi.

1. **Requesting of Certificates**
   ZenZefi provides functionality for requesting of certification requests on behalf of the current user to the PKI.
   In the business area of AfterSales, ZenZefi will request the application Xentry Diagnose to retrieve certificates from the PKI.

Supplier

This chapter describes the requirements for ZenZefi in the Daimler-external business area of the supplier, where typically supplier-employed engineers will use ZenZefi.

1. **Requesting of Certificates**
   ZenZefi provides functionality for requesting of certification requests on behalf of the current user to the PKI.
   In the business area of supplier, i.e. when ZenZefi runs on devices of employees of supplier companies like Bosch or Continental, ZenZefi will access the PKI directly.

2. **Authentication to SupplierDir**
   In order to be able to request certificates from the PKI ZenZefi needs to provide functionality that integrates with the Daimler supplier directory for authenticating and authorizing the current user.

3. **Highly configurable**
   ZenZefi has a distinct configuration for every business area where ZenZefi runs in.
   ZenZefi will be delivered as a standalone jar file which contains all initial configuration that is suitable to successfully run in the target business area.
   At build time it is specified with what set of configurations ZenZefi should be built depending on the target business area, where the build artifact should be executed later.
   ZenZefi will contain the root and backend certificates - these form the trust anchor - for the target business area.
   A UI is required only in the business areas of R&D, so only the build that builds the artifact for the business area of R&D will also package the resources required for the UI into the standalone jar.
   The file logback.xml contains the logging configuration for ZenZefi.
   Additionally ZenZefi contains two configuration files: the mandatory "zenzefi.properties" and the optional "zenzefi-general.properties". During application startup the mandatory "zenzefi.properties" will be read first.
   While all files within the build artifact will be signed in order to protect them from manipulation, the signature of the file "zenzefi-general.properties" will not be checked at startup time of ZenZefi. The main goal for the file "zenzefi-general.properties" is to have a location where the user can edit configurations(e.g. the port ZenZefi will locally run on) in order to resolve major configuration issues(e.g. due to a local port conflict) without having to wait for an additional release.
   If a file is detected at startup time by ZenZefi where the signature does not match, except for "zenzefi-general.properties" where manipulation is allowed, ZenZefi will exit.
   After a successful startup ZenZefi will derive the configuration options for the default user. After completing the registration process for a new user, ZenZefi will also derive the configuration options for this new user automatically.
   ZenZefi_Properties.xlsx contains the configuration options for ZenZefi and specifies the default values for each business area as well as the way how ZenZefi handles these properties at the initial system startup, subsequent system startup, user registration, update of ZenZefi.

4. **Single User Mode**
   ZenZefi supports an arbitrary number of users. However, ZenZefi will always only run on behalf of a single user. After startup, ZenZefi will always run as default user. After a user logs in ZenZefi will run on behalf of that user, no matter over which interface(UI, REST, UI) the interaction with ZenZefi is triggered.

5. **REST interface for certificate management**
   ZenZefi exposes a set of restful webservice endpoints for applications running on the diagnostic testing device, which allows the testing device to retrieve certificates, sign coding data or manage the certificate in the user certificate store. Additionally ZenZefi also provides endpoints that can be used for retrieving meta information(version, system integrity, relevant log entries) about the current instance.

6. **Command-line interface for certificate management**
   The rest interface provided by ZenZefi can also be invoked using a command-line interface.

7. **Administration of certificates**
   ZenZefi provides functionality for the importing, verifying, deleting, viewing and persisting of certificates in the user certificate store.

8. **Signing of Coding Data**
   ZenZefi provides a web service which allows the signing of coding data. Signing of coding data comprises the computation of a hash value and the subsequent encrypting of the hashed value with private key that belongs to the secure variant coding certificate of the current user. As a result ZenZefi will return the signature for the coding data as well as the secure variant coding certificate, so that the ECU can verify if it trusts the secure variant coding certificate of the user by performing a chain-of-trust validation using its backend certificate and additionally verifying the signature using the public key in the secure variant coding certificate.
   ZenZefi does not implement cryptography, ZenZefi uses cryptography providers like BouncyCastle or other cryptography providers made available by Daimler. The main reason for this is to rely on publicly reviewed cryptographic functionality in order to avoid any kind of security-by-obscurity issues and possible vulnerabilities.

9. **Logging**
   Logging in ZenZefi is highly configurable via the logback.xml which specifies the logrotation strategy, the maximum size of a log file, the age for which log files should be kept as well as the maximum amount of disk space the log files can use before being deleted considering their age.

   Additionally to the logging of the complete application stack via logback to the file system all log messages programmatically generated by ZenZefi Java classes will also be logged to the database including a checksum, so that nobody can manipulate the log entry content. In the database the log entries will also be connected to each other on the relational level, so that missing log entries can also be detected.

10. **Monitoring**
    ZenZefi provides monitoring of the application mainly relying on the SpringBoot production-ready endpoints(see http://docs.spring.io/spring-boot/docs/current/reference/html/production-ready-endpoints.html) "health".

SigModul

The **SigModul** will be deployed in the backend systems within the business fields of AfterSales (one operation center) and MRS (Mercedes Remote Services), Production (one operating center per factory) and aggregate plants, as well as, in R&D (CSB@RD). SigModul signs coding data (which represents a specific configuration) with a coding certificate. SigModul generates the required keys by itself and also triggers certificate signing requests (CSRs) to the Daimler PKI (Registration and Certification Authority).

Production

This chapter describes the requirements in the Production environment.

Aftersales

This chapter describes the requirements in the AfterSales environment.

1. **High availability**
   In both business areas Production as well as AfterSales SigModul needs to be ready to be used in an environment where availability is crucial.
   In Production, where SigModul is operated in the operating center of the plant, outages of SigModul will have a negative impact on the availability of the ISServer and possibly ZenZefi, thus potentially disturbing the vehicle production process.
   In AfterSales, where SigModul is operated in the European DataCenter, outages of the SigModul will have a negative impact on the availability of the Vehicle Coding Service and thus on the processes in the garage which need to be available 24x7.
   High availability for SigModul will be considered after Phase 4 of the CeBAS project, when empirical data will be available to determine if the availability reached up to this point is sufficient.

2. **High scalability**
   In both business areas Production as well as AfterSales SigModul needs to be ready to be used in an environment where scalability is crucial.
   In Production, where SigModul is operated in the operating center of the plant, lack of scalability can have a throttling impact on the performance of the ISServer thus potentially disturbing the vehicle production process. In production the SigModul will typically need to sign a huge amount of coding data in a relatively short period of time(~1hour). This is due to the fact that SigModul will need to compute the signatures for all coding data to be transferred to the electronic control units in the vehicle and the actual vehicle production process will start shortly thereafter in the assembly line.
   In AfterSales, where SigModul is operated in the European DataCenter, lack of scalability can have a negative impact on the performance of the Vehicle Coding Service and thus on the processes in the garage which need to be available 24x7.
   Scalability for SigModul will be considered after Phase 4 of the CeBAS project, when empirical data will be available to determine if the scalability reached is sufficient.
   SigModul will implement a thread-pooling in order to parallelize processing of inbound coding data signing requests from ISServer.

3. **High configurability**
   SigModul has a distinct configuration for the business areas of Production and AfterSales where it will be used.

4. **Provides a command line interface**
   SigModul will provide a command-line interface that allows the administration of the current instance.

5. **Signing of Coding Data**
   SigModul provides a web service which allows the signing of coding data. Signing of coding data comprises the computation of a hash value and the subsequent encrypting of the hashed value with private key that belongs to the secure variant coding certificate of the current user. As a result SigModul will return the signature for the coding data as well as the secure variant coding certificate, so that the ECU can verify, if it trusts the secure variant coding certificate of the user by performing a chain-of-trust validation using its backend certificate and additionally verifying the signature using the public key in the secure variant coding certificate.
   SigModul does not implement cryptography, SigModul uses cryptography providers like BouncyCastle or other cryptography providers made available by Daimler. The main reason for this is to rely on publicly reviewed cryptographic functionality in order to avoid any kind of security-by-obscurity issues and possible vulnerabilities.

6. **Logging**
   Logging in SigModul is highly configurable via the logback.xml which specifies the logrotation strategy, the maximum size of a log file, the age for which log files should be kept as well as the maximum amount of disk space the log files can use before being deleted considering their age.

7. **Monitoring**
   SigModul provides monitoring of the application mainly relying on the SpringBoot production-ready endpoints(see http://docs.spring.io/spring-boot/docs/current/reference/html/production-ready-endpoints.html) "health".

Quality Goals

This is described in chapter 10.

Testability

ZenZefi and SigModul are designed so as to ease testability and achieve a high grade in test automation.

Stakeholders

These stakeholders are involved during project phase and afterwards in operations.

R&D

The business area R&D comprises the diagnostic hardware and software used by Daimler. In this business area R&D engineers use ZenZefi for testing and development tasks they perform on the electronic control unit using and diagnostic applications.

R&D Engineers

R&D engineers are users of the application "Monaco". They typically have extensive knowledge about the diagnosis and the bus systems within the car as well as the CeBAS project itself.
ZenZefi is not only yet another system in their toolchain R&D engineers already have to use in order to get diagnostic data from the vehicle and in order to perform their test, but instead they also use ZenZefi as a means of testing special use cases they need to cover.
Daimler engineers work from networks inside the Daimler organisation and authenticate against the Corporate Directory.

Production

The business area production comprises all plants including their IT infrastructure like the diagnostic testing device hardware and software, the ISServer etc. Plants have decentralized operating centers which can operate autnomously and as such can be considered self-contained units.

IT-/Functional Responsible IS-Servcie/-Server

This role is responsible for operating the server systems in the decentralized operating centers of the plants. As such users that belong to this role are responsible for operating and monitoring SigModul.

Production Workers

Production workers are the actual people working on the assembly line who use applications like ISService+ on the testing device and as such also indirectly use ZenZefi and the SigModul.
This group of people is focused on their tasks at hand and possesses little to no knowledget about IT systems in general as well as the authentication or authorization mechanisms and processes provided by the CeBAS project.

Test Sequence Developer

Users who belong to this role are responsible for the diagnostic processes in production. They use ZenZefi in a similar way like the R&D engineer, i.e. they have multiple certificates which they manage. They also authenticate against the CorpDir and receive personalized certificates. In contrast to the R&D engineers they will always work with the role "production".

AfterSales

The business area AfterSales comprises the workshops, which use software provided by Daimler in order to perform diagnostic operations on Daimler vehicles as well as the centrally hosted Daimler backend systems which allow the management of customer and vehicle data.

IT-/Functional Responsible AS-Backend Systems

This group is responsible for operating the AfterSales backend systems. Consequently this user group is also responsible for operating and monitoring applications provided by the CeBAS project i.e. ZenZefi and SigModul

Workshop Workers

This group consists of the workshop staff which uses XENTRY and consequently indirectly also ZenZefi. This user group is involved with practical activities and does not possess knowledge about IT-systems and authentication and requirements and processes related to the Daimler backend systems.

Supplier

The business area Supplier comprises the diagnostic hardware and software used by supplier companies like Bosch or Continental. In this business area supplier engineers use ZenZefi for testing and development tasks they perform on the electronic control unit using and diagnostic applications.

Supplier Engineers

Supplier engineer identity data is managed in the supplier directory. Supplier engineers work from networks outside the Daimler organisation and authenticate against the Supplier Portal.