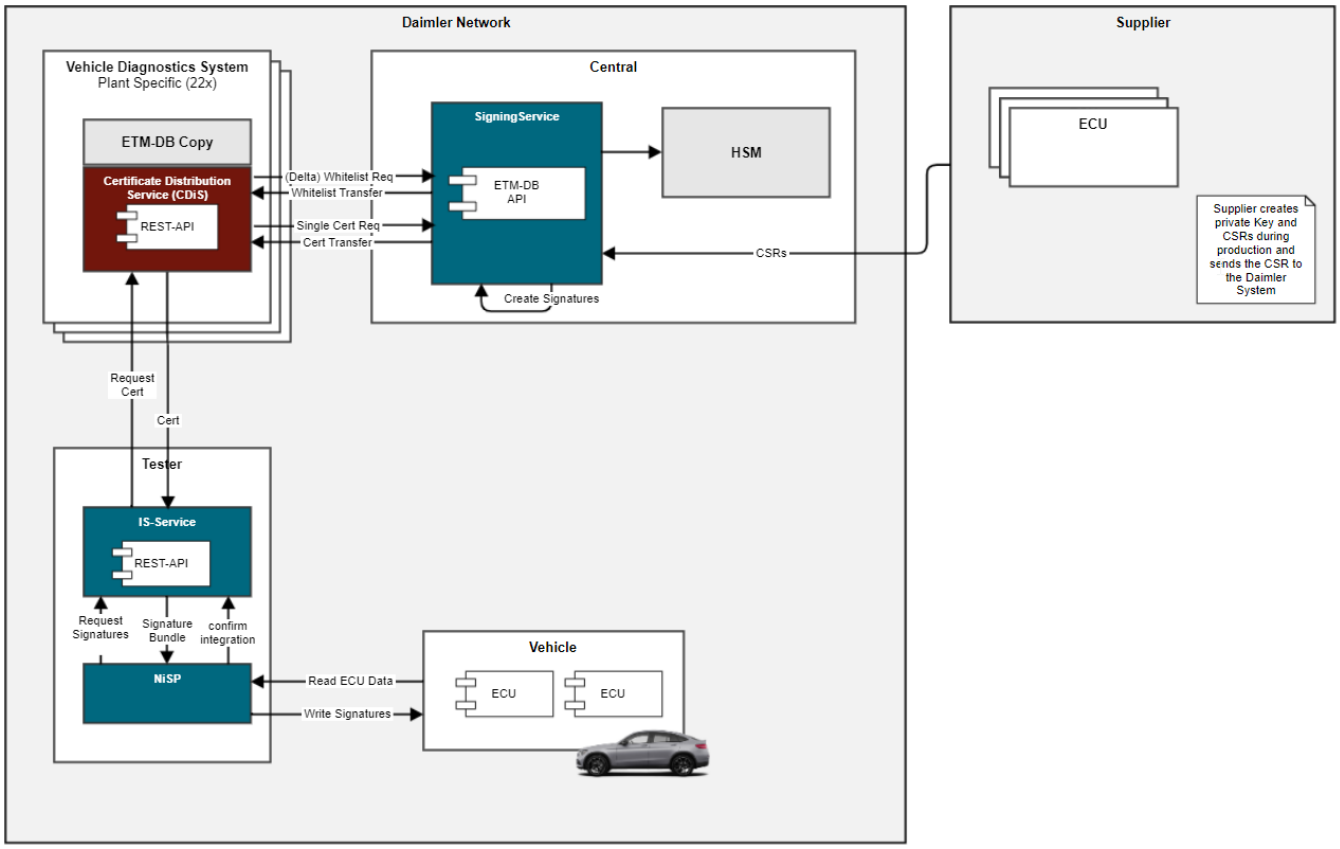
Processes

This diagram shows the systems involved and their interfaces (subject to change). Every process will be briefly described to outline a basic understanding.



Supplier PKI

Once an ECU is powered on at the supplier's production site it will generate a CSR that will be sent to Daimler PKI in order to generate an ECU trust model certificate. This certificate will not be sent back to the supplier, but get stored in a Whitelist DB where all certificates of all other suppliers are stored as well. Maximum certificates per car are 60 for S-class, lowest probably 40 for A-class with the other models somewhere in between.

PKI CDiS

From the PKIs Whitelist the certificates need to get distributed to the plants to be ready in time when they're needed during the production process (including rework). CDiS will have a copy of the Whitelist that needs to follow the "as small as possible - as big as needed" principle. Besides the certificates the certificate chains can be obtained from PKI.

CDiS IS-Tester

Once a car arrives at the final assembly and the ECUs were assembled and powered on, requests for the corresponding ECUs certificates will be generated and sent from IS-Tester to CDiS. Ideally, the certificate was already created by the initial suppliers CSR with enough lead time and retrieved by the plants CDiS, so it can be sent down immediately. If not a request is sent from CDiS to PKI in order to obtain the certificate or issue it on-the-fly if it doesn't exist yet, then send it back to the plants CDiS as soon as possible (approx. 30 sec max waiting time). A request from the plant can be trusted when the IS-Tester running device was authorized first.

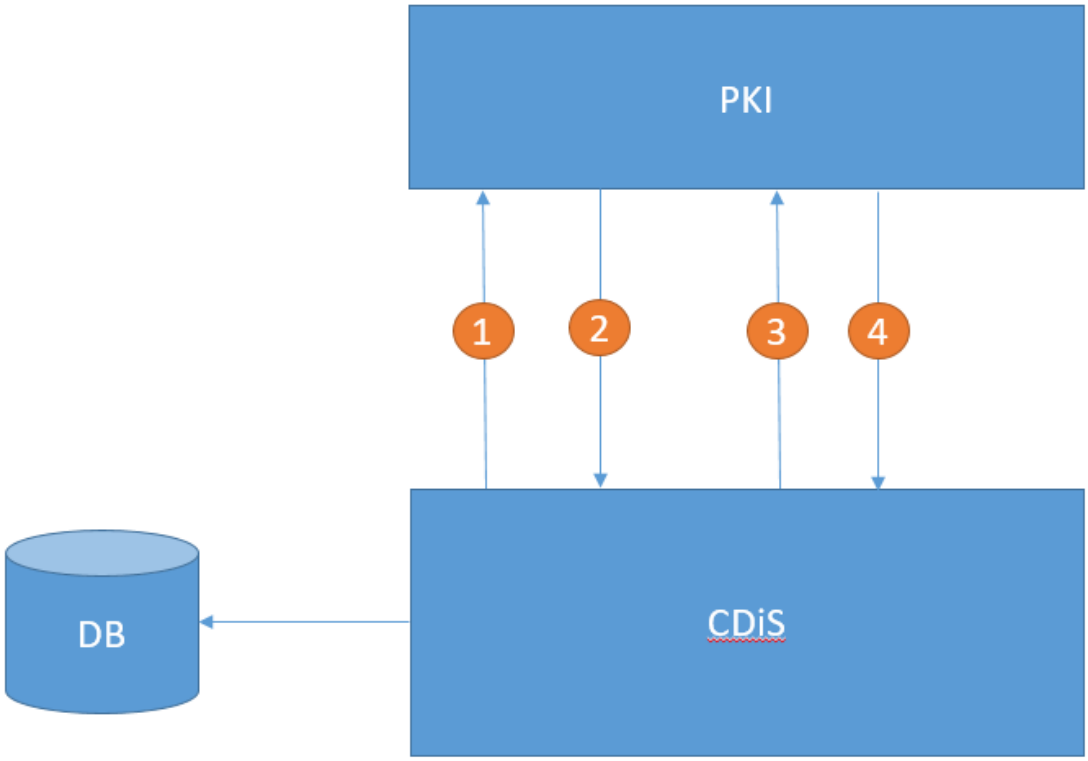
Processes (detailed)

PKI CDiS

Interfaces Overview:

1. Request list of public keys created within a timeframe (endpoint: /info)
2. Request single ECU TM certificate for a public key (endpoint: /cert)
3. Request certificate chains (endpoint: /exid)
4. Request certificate issuing for CSR (endpoint: /csr)

Requesting certificates



1. CDiS requests all certificates between <start> and <end>
2. PKI sends a list of public keys
3. CDiS requests the certificate for a public key
4. PKI submits the certificate

Potential error cases:

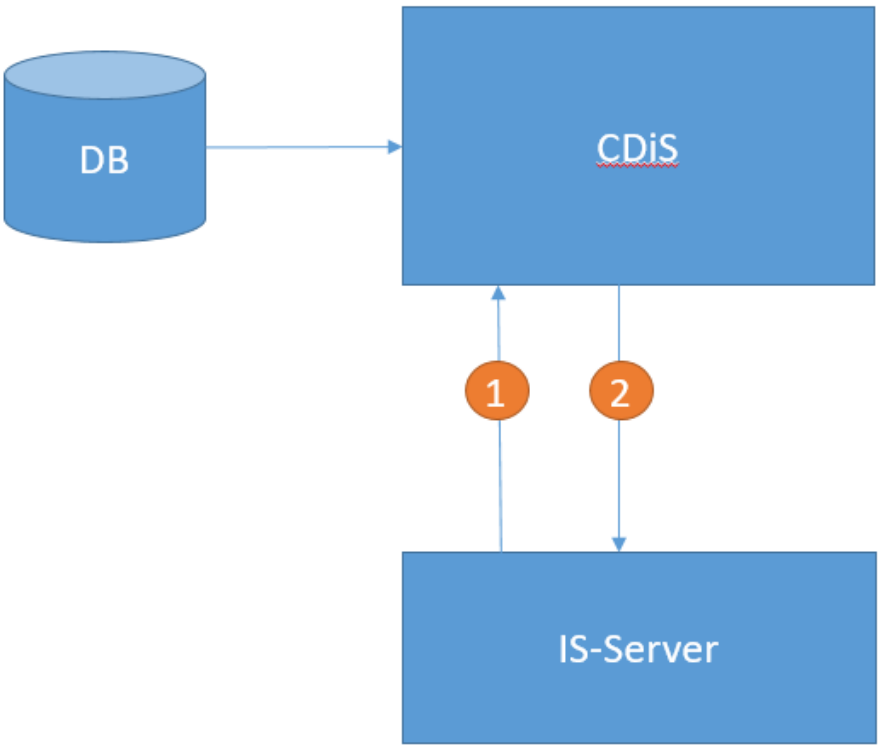
Error case	**Reaction**
IF1: No reply from PKI for update request (both public_key list and subsequent certificate request)	Retry after timeout, raise alarm after several failed attempts (first level support)
IF2: No certificate from PKI for an on-the-fly certificate request (emergency process)	How long shall CDiS try to get this certificate?
Certificate already inside Whitelist DB included in Delta Whitelist update.	Not a real error case. Update of previous certificate with new one.

CDiS IS-Tester

Interfaces overview:

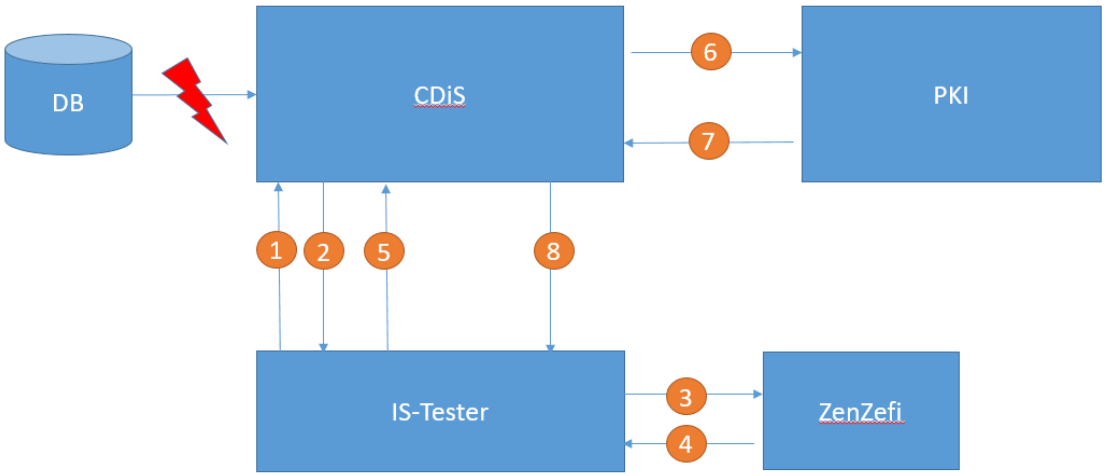
1. Request certificate for a CSR
2. Reply with certificate chain (ECU TM, intermediate, backend)
3. Confirm download of an ECU certificate

Requesting a certificate (standard case)



1. Request for certificate (single request for one ECU using the public key as ident)
2. Reply with ETM certificate

CDiS IS-Tester (emergency case)



1.Request for certificate Certificate not in DB!

2.Reply negative: Authorization request to IS-Tester to send signed CSR and HostID to authorize device.

3.Request to create signature over CSR and HostID

4.Reply with signature

5.Request: Signed CSR + HostID

6.Request to PKI to create the certificate on-the-fly (positive case)

7.Reply with certificate

8.Reply with certificate

// Unclear if emergency process (PKI certificate issuing triggered by plant) is allowed at all! 03.03.2022 still in discussion.

Further potential error cases that need to be considered and taken care of:

Error Case	**Reaction**
CDiS doesn't reply (downtime, internal error…)	IS-Tester sends several retries then gives up and raises an error to the user (via IS-Tester).
~~CDiS doesn't get an on-the-fly certificate from PKI (in-time?)~~	~~CDiS provides the certificate as soon as it is available. Meanwhile the IS-Tester runs into a timeout (and eventually requests the cert again).~~
Polling on all fronts takes forever (CDiS PKI, IS-Tester CDiS)	More and more threads that need to stop sometime. How to resume the processes? 16.06.: No polling. Synchronous communication with timeout.
Request for certificate already marked as "downloaded"	Provide again nevertheless
IS-Tester doesn't confirm "downloaded" for an ECU (maybe download procedure was canceled)	CDiS could mark it as "provided" to at least show the status and make it possible to investigate such issues.
CSR or certificate is corrupt	IS-Tester side: Request again CDiS side: Do we need to check a CSR / Certificate at all? Optional from my point of view. PKI: Does PKI do checks and only provide valid certificates?
ECU in plant provides a different CSR (public_key) than in the supplier request	Likely? No system in the process chain will be able to fix this I guess. • ECU SW buggy. Emergency process
Certificate is blacklisted	Info to IS-Tester to remove ECU from production. 16.06.: Still in discussion
Certificate already issued for another CSR (wrong certificate sent by PKI?)	Should CDiS double check if a certificate was already issued? NO
Part Number not part of the request for cert	IS-Tester will send a standard part number if NISP doesn't send it. Decline request otherwise.