**System Description (SysD) Certificate Provider**

System Description (SysD) Template – Black Box Design [1](#_heading=h.gjdgxs)

* 1. System Description Overview 3

1. Use-cases 3
   1. Behaviour Diagrams 4
2. System services 4
   1. Provided Services 5
3. Security 5
4. References 6
5. Revision history 6
   1. Amendments 6
   2. Quality Assurance 7
   3. **System Description Overview**

The IoT systems were created with the purpose of allowing interoperability and connectivity between systems and devices, these systems as of today rely on certificates that are provisioned manually. In this system we propose a way to facilitate this onboarding process.

The certificate provider takes certificate CoPx requests from a consumer (that wants to register a new device) and returns a response which then triggers an event used to update the authorization information.

1. **Use-cases**

**Table 1 Use-case description**

|  |
| --- |
| Name of the Use-case: On Boarding with CoPx |
| **Brief description**:  The objective is to implement a Certificate Synchronization (CS) system that together with a contract proxy structure allows for provisioning of on-boarding certificates for an external device.  The certificate provider does not provide the certificate itself, it rather provides the authorization for the authentication info to be created by the Certificate Authority. |
| **Primary actors**:  Device Manufacturer |
| **Secondary actors**:  Device consumers |
| **Preconditions**:  To begin the process a device consumer attempts to start a device into the arrowhead services, but he finds himself unable to start as it is not registered in the certificate authority system, which stores device certificates. |
| **Main flow**:  Present in a sequence of steps the interactions among the actors  1- The provider receives a CoPx request and sends a response.  2- When the request is created an **event is triggered** which is listened by the certificate authority.  3- The certificate authority then updates the database with the authorization info.  4- Then the device is able to begin the onboarding process in the arrowhead systems. |

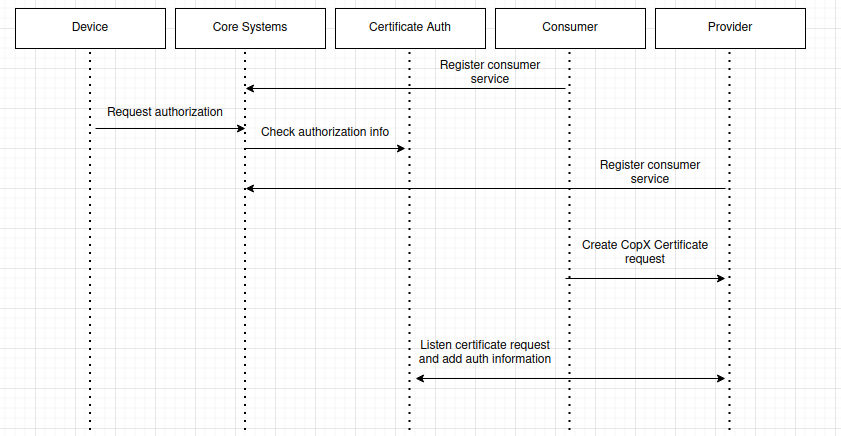
* 1. **Behaviour Diagrams**

This section provides the behavior diagrams of how the system in the arrowhead network interacts with the other actors.

**2.1.1. Certificate request diagram:**

The device system attempts to connect to the arrowhead systems, in this process a certificate authority system is involved, it stored in a database every external device auth info and checks if the device is authorized, as it is unable to start the consumer creates a contract proxy request that is based in json key values, the provider then returns and answer and an CERTIFICATE\_REQUEST event is created, the certificate authority purpose is to listen to those events, when one of those events is created the certificate authority updates its database, as seen in figure 1.

Then the device is started again, it checks with the CA (Certificate Authority) if the auth info is available and it starts if so.



**Figure 1: Certificate consumer diagram, it shows the flow that the consumer follows while requesting a certificate.**

1. **System services**
   1. Produced Services:

**Table 2 Produced services reference docs**

|  |  |  |
| --- | --- | --- |
| Service | SD Document Reference | IDD Document Reference |
| Certificate Service | Arrowhead-Assignment/Doc arrowhead/Doc arrowhead/Cert Provider/IDD\_CertPr.docx | Arrowhead-Assignment/Doc arrowhead/Doc arrowhead/Cert Provider/IDD\_CertPr.docx |

The Certificate Provider is a passive service as it waits for a certificate request, the system then validates the request and triggers an event which is listened by the Certificate Authority and sends a response to the consumer of the service, table 2 provider routes for reference documents.

3.2. Consumed Services:

**ServiceRegistry:** This service is consumed to make sure that the Certificate Consumer system becomes accessible to other systems.

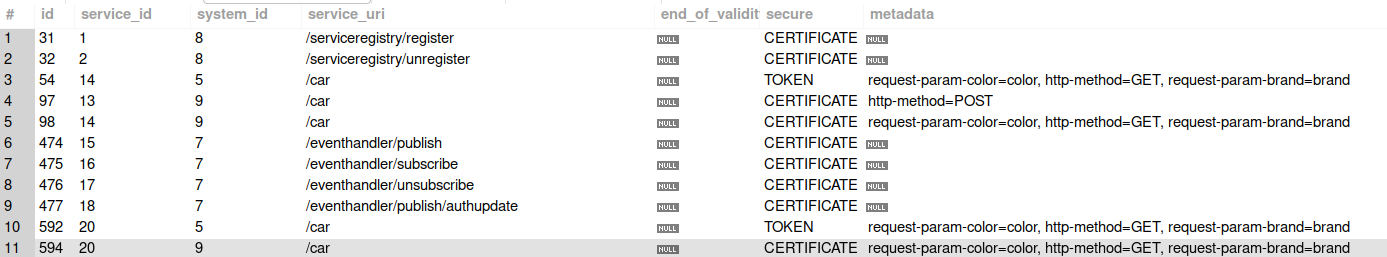
**Orchestration**: This service is used to determine what Authorization services to use.

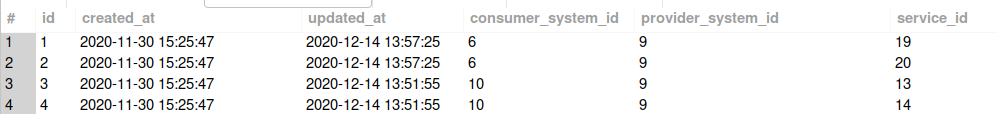
**Authorization**: This service is used to determine if calls to produced services are authorized or not.

**Certificate Authority**: This service listens to the events triggered by the Certificate Provider and updates authentication data for the requested device.

1. **Security**

The authorization rules are the following:



****

**Figure 2: Authorization rules for Certificate Consumer**

In order to simplify the process and not focus on creating new certificates in this particular project the names and certificates from examples were used.

As can be seen in figure 2, the provider with system\_id 9 is connected with 2 consumer systems, consumer\_system\_id 6 is the one that serves as this service consumer, it sends certificate requests and expects responses, consumer\_system\_id 10 is the certificate authority whose listen to the provider events.

The Certificate Provider is passively waiting for request from the consumer, after the arrowhead systems authorization systems clear the interactions no further checks are required.

The interaction between the provider and the Certificate Authority is only trough the event handler system as it manages the requests made to the Certificate Provider.