**System Description (SysD) Certificate Consumer**

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

* 1. System Description Overview [3](#_heading=h.30j0zll)

1. Use-cases [3](#_heading=h.3znysh7)
   1. Behaviour Diagrams [4](#_heading=h.2et92p0)
2. System services 4
   1. Consumed Services [5](#_heading=h.1t3h5sf)
3. Security 5
4. References [6](#_heading=h.lnxbz9)
5. Revision history [6](#_heading=h.35nkun2)
   1. Amendments [6](#_heading=h.1ksv4uv)
   2. Quality Assurance [7](#_heading=h.44sinio)
   3. **System Description Overview**

In the IoT structures the devices used can come from many different places and different manufacturers, as of today all of these devices come with their certificates in order to be used inside a particular structure.

In this case we analyze the arrowhead system and how it makes the onboarding process.

In this project we look at a different view in how to perform the onboarding process.

This document aims to explain the behaviour of the Certificate consumer, this system creates a mock contract proxy request to the Certificate provider. This allows the systems to have a control over what systems use each device and be able to deny or allow the use of them.

1. **Use-cases**

**Table 1 Use-case description**

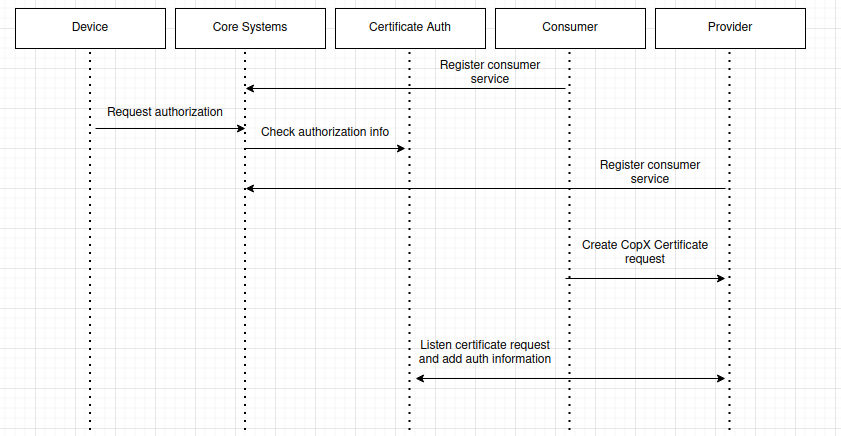
|  |
| --- |
| Name of the Use-case: On Boarding with CoPx |
| **Brief description**:  The objective is to implement a Certificate Synchronization (CS) system that together with a contract proxy stucture allows for provisioning of on-boarding certificate for a external device |
| **Primary actors**:  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 device consumer sends a CoPx request to the provider in order for the certificate to be created.  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. **Behavior Diagrams**

**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.

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. **Consumed Services**

**Table 2 Consumed services reference docs**

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

**Certificate Provider:** This service provides to the consumer a CoPx response to the certificate request, and also triggers an event every time a certificate is requested.

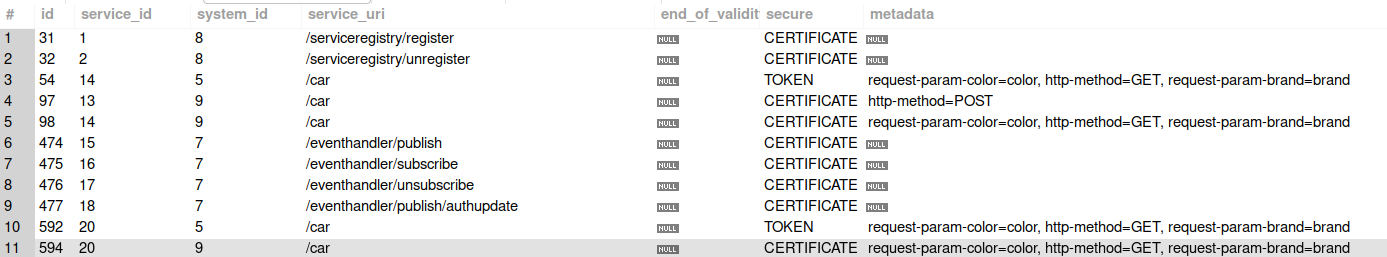
**ServiceRegistry:** This service is consumed to make sure that the Certificate Consumer system becomes accessible to other systems.

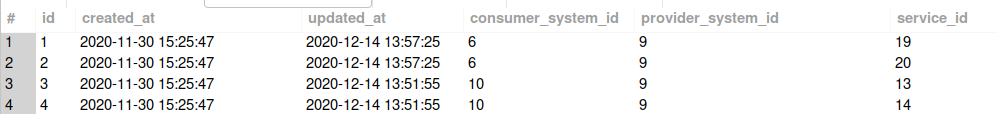
**Orchestration**: This service is used to determine what Authorization services to use.

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

1. **Security**

The authorization rules are the following:



****

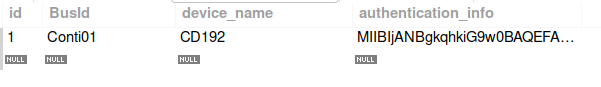
**Figure 2: Authorization rules for Certificate Consumer.**

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.

Consumer system 6 is this consumer system, it only consumes the provider that receives the certificate request.

This system availability is active, as it sends information by user input, the information that the Certificate\_consumer receives a response only after a request has been sent.

The certificate authority database structure is the following, it stores the information of the device entered, this allows the onboarding process to the AS (Arrowhead systems) to start.



* 1. **Amendments**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Date | Version | Subject of Amendments | Author |
| 1 | 2020-05-27 | 1.0 |  | Jerker Delsing |
|  | 2020-08-18 | 4.2 | Minor updates | Jerker Delsing |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |