**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

* 1. **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. |

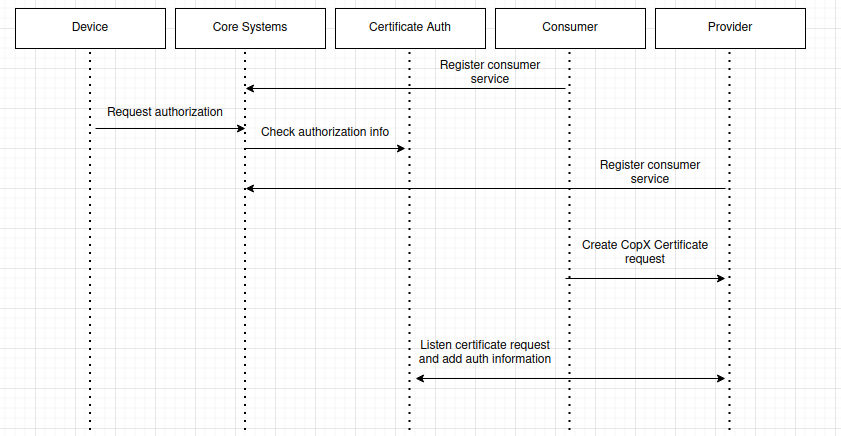
* 1. **Behaviour Diagrams**

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 db 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 if the auth info is available and it starts if so.

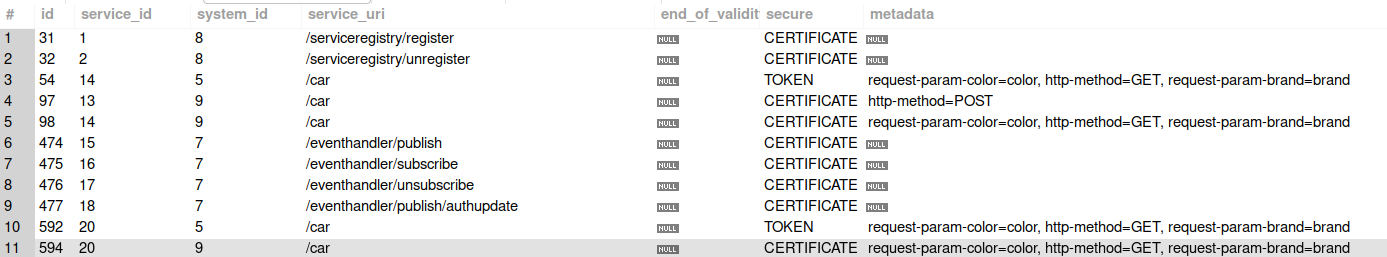


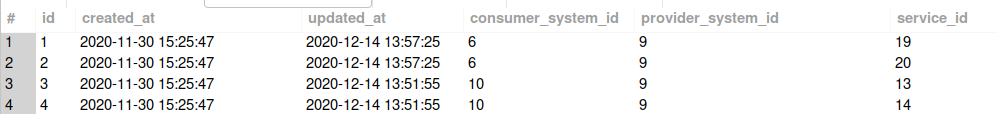
1. **System services**

This system does not provide any service rather it triggers events that are used by the CA.

1. **Security**

The authorization rules are the following:



****

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.

The provider used in this application is the one with system id 9

1. **References**

Any references must be placed here.

1. **Revision history**
   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 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* 1. **Quality Assurance**

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Date | Version | Approved by |
| 1 |  |  |  |
| 2 |  |  |  |