SysD Onboarding Controller v1.0

16 april 2019

Contents

1 System Description Overview

Onboarding Controller system:

- A server at the edge of the Arrowhead local cloud, which is not part of the local cloud chain of trust
- It accepts all devices to connect via the OnboardingController service (*accept_ all* interface), thus it is the first entry point to the local cloud
- It has a server certificate for the *https* communication with the device
- (Optionally) the server certificate is provided by a public CA (e.g. verisign)

On success, the system provides:

- the endpoints of the DeviceRegistry, SystemRegistry and ServiceRegistry systems
- the Arrowhead CA (server) certificate
- an Arrowhead CA issued "onboarding" (client) certificate

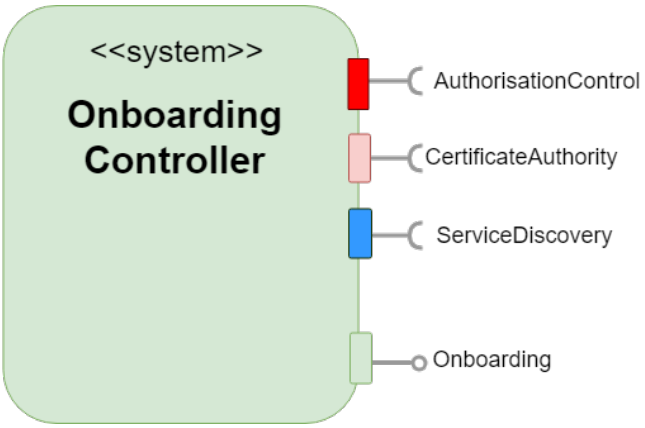

Figure 1: The Onboarding Controller system

The Onboarding Controller system consumes the ServiceDiscovery, AuthorizationControl and CertificateAuthority services and provides the OnboardingController service.

2 Use-cases

2.1 Onboarding Controller

This section provides the use cases that represent the actors and their interaction with the Onboarding Controller system. The actors can be devices with different credentials.

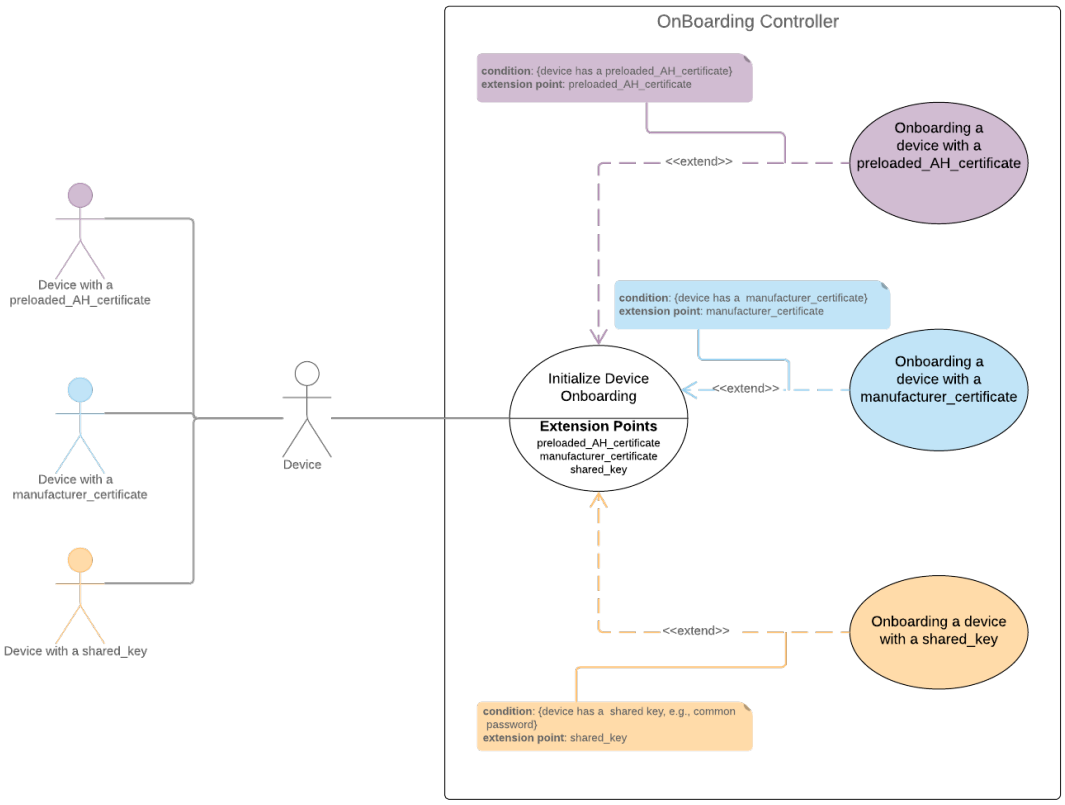

Figure 2: Onboarding Controller use cases

2.2 Onboarding Procedure

The onboarding procedure is needed when a new device produced by any vendor (e.g. Siemens, Infineon, Bosch, etc.), containing a security controller (e.g. TPM), wants to interact with the Arrowhead local cloud. To assure that the cloud is not compromised upon the arrival of this new device, it is important to establish a chain of trust from the new hardware device, to its hosted application systems and their services. Thus, the onboarding procedure makes possible that the device, systems and services are authenticated and authorized to connect to the Arrowhead local cloud.

The use cases in which the external actor interacts with the Arrowhead local cloud during onboarding include:

- Initialize Device Onboarding (via the Onboarding Controller system)
- Register a Device in the DeviceRegistry (via the DeviceRegistry system)

- Register a System in the SystemRegistry (via the SystemRegistry system)
- Register a Service in the ServiceRegistry (via the ServiceRegistry system)
- Start normal operation (e.g., service lookup, service consumption, etc.)

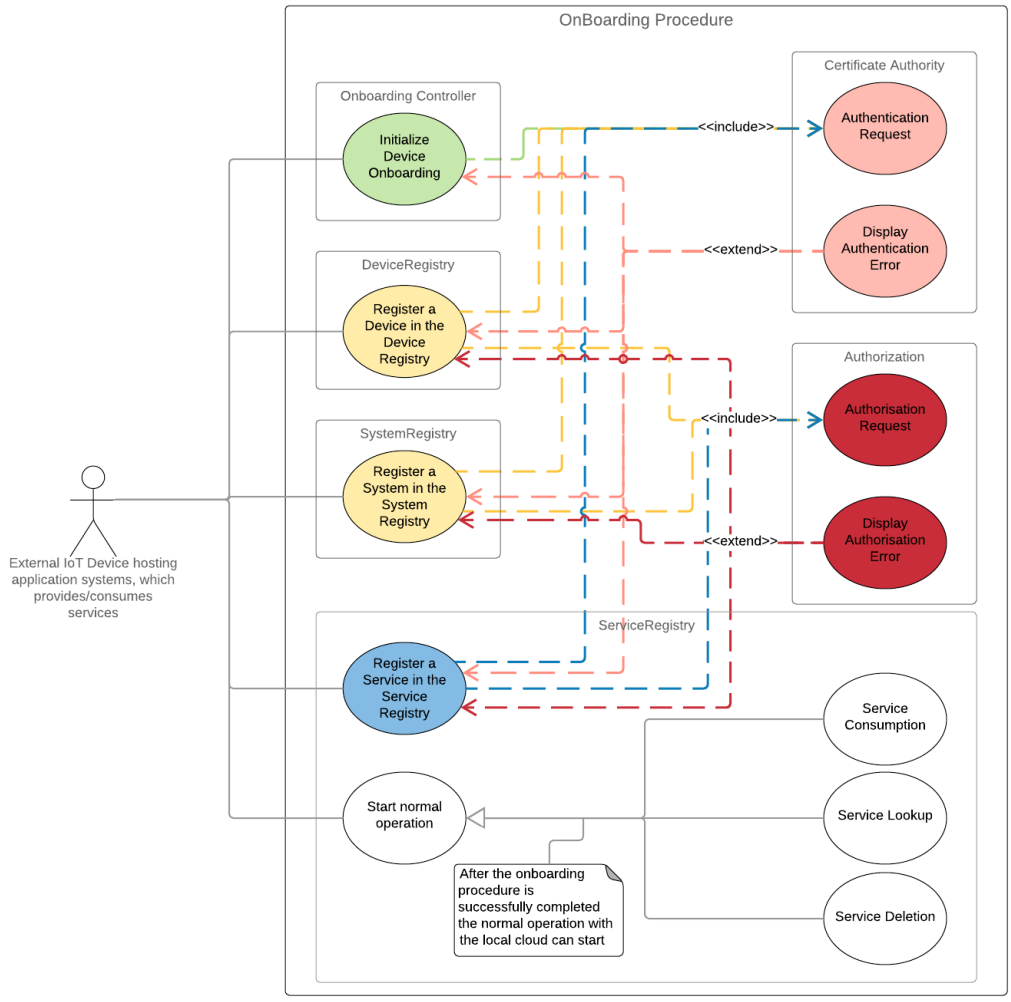

Figure 3: Onboarding Procedure use cases

3 Sequence Diagrams

The sequence diagrams show how a device interacts with the Arrowhead local cloud during the onboarding procedure. The device can have different credentials (e.g., a preloaded Arrowhead certificate, a manufacturer certificate or a shared key).

3.1 Onboarding a device with a preloaded Arrowhead certificate

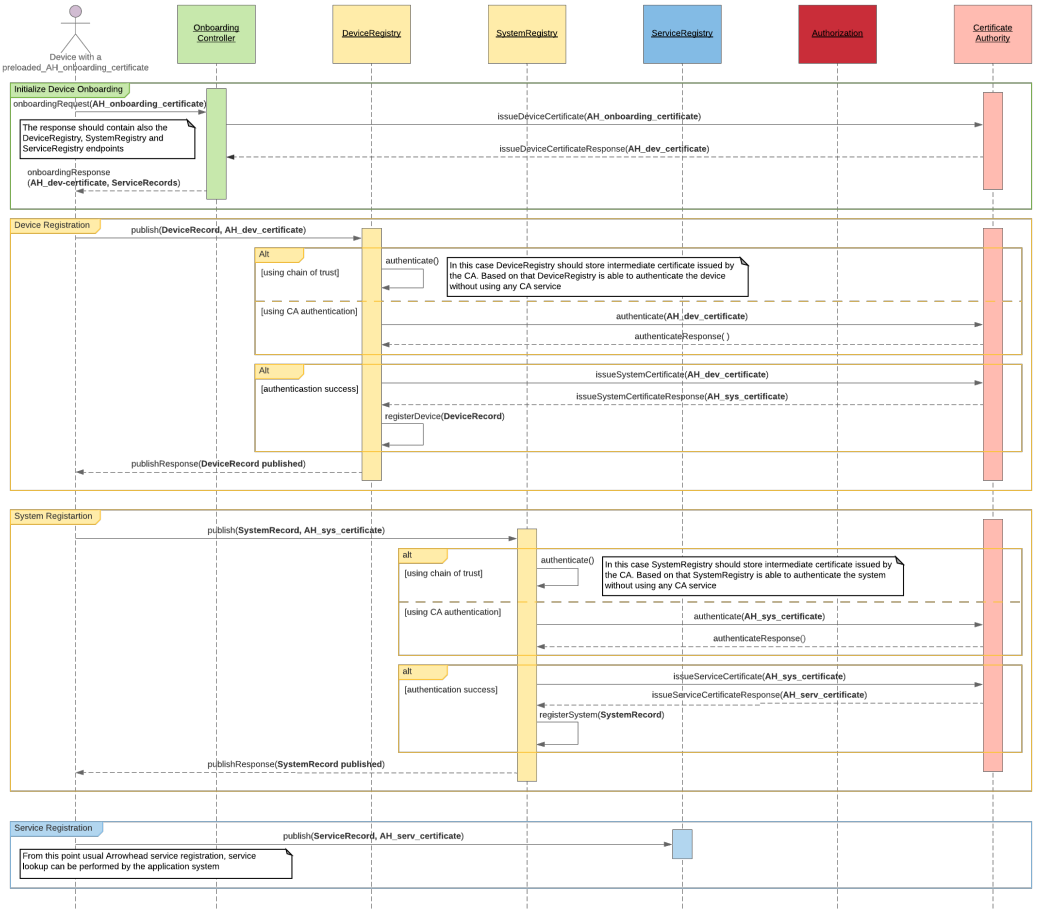

Figure 4: Onboarding a device with a preloaded Arrowhead certificate - Sequence Diagram

3.2 Onboarding a device with a manufacturer certificate

3.3 Onboarding a device with a shared key

4 Security

4.1 Authentication

4.1.1 Certificate based authentication

The certificate based authentication works through asymmetric cryptography. Each party needs to have a valid certificate which is signed by a trusted (and known) parent certificate. The trusted certificate confirms the identify of the presented certificate.

4.1.2 Chain of trust

The chain of trust is a concept where a certificate is signed by another certificate, which is more known and trusted. Figure 5 shows a chain of trust with three certificates. The certificate with the highest authority is known as root certificate. The root certificates signs its descending certificates, confirming their identity. Any certififcate between the root certificate and the end-entity certificate is called an intermediate certificate.

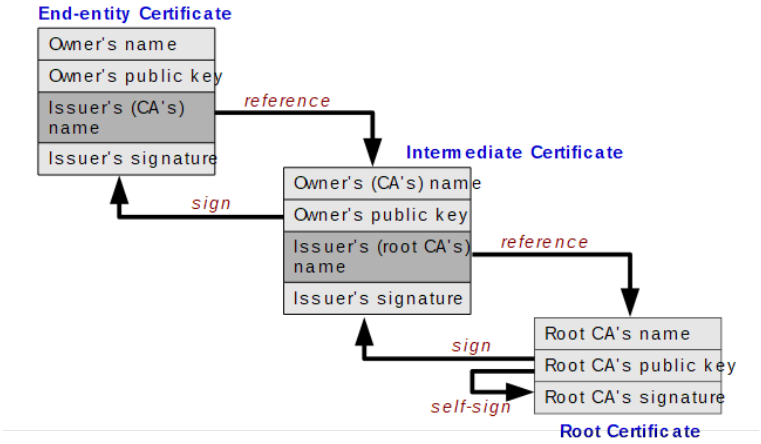

Figure 5: Chain of trust

Figure 6 shows the certificate hierarchy in the Arrowhead framework.

4.1.3 Arrowhead Certificate Authority

Arrowhead contains a core system called Certificate Authority (CA). The CA is the highest authority in the local cloud and responsible for signing any descending certificate. All services in the local cloud must trust the CA of the local cloud. The CA itself may be signed by a central arrowhead consortium, establishing a chain of trust and allowing different arrowhead clouds to interconnect with each other.

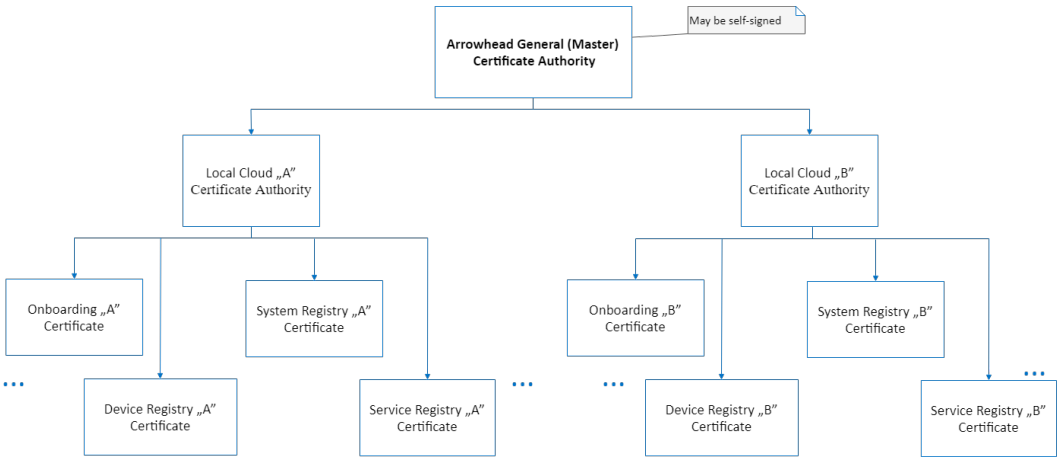

Figure 6: Certificate Hierarchy in Arrowhead

4.2 Authorization

Authorization is the function of allowing or disallowing specific actions. In the arrowhead system, the AuthorizationControl service is responsible for enforcing all authorization related policies. A policy may define that no systems with a specific OS may be allowed in the cloud. Another policy may define that a service (e.g., temperature collector service) may only query the service registry about existing temperature services but not e.g. power regulating services.

4.3 Assets

No defined yet.

4.4 Non-technical Security Requirements

No defined yet.

References

5 Revision history

5.1 Amendments

5.2 Quality Assurance

No.	Date	Version	Subject of Amendments	Author
1	07-12-2018	1.0	Initial Version	Silia Maksuti, Mario Zsilak
2	04-02-2019	1.1	Updated Version	Silia Maksuti
3				

No.	Date	Version	Approved by
1			
2			