Online Certificate Management for Aircraft Devices

ARINC 842 update

Ndrianina Randrianasolo

21 Jan 2021

AIRBUS

The need for Online Certificate management

Need Summary:

Current standard for certificate management makes it difficult to securely manage onboard certificates:
- It means one FLS per A/C.
- To be done every 1-3 years (minus a few weeks) for each A/C (depending on certificate lifetime).

As a result, less secure behaviour are seen in operation:
- Fallback to Pre-Shared Keys
- Using the same certificate for the entire Aircraft fleet
- In such case, the private key of the certificate is distributed as part of the LSAP. This further lowers the security level

The Online Certificate Provisioning feature aims at automating certificate provisioning on board:
- Aircraft system generates a key pair and a CSR when there's no valid certificate for the system
- Certificate is obtained online from PKI provider via Aircraft communication means

➔Security level is ensured
➔Airline avoids creating thousands of FLS and maintenance actions on Aircraft

Status and Way Forward Proposal

- This online certificate management feature greatly enhances operability and security of certificate usage on Aircraft
- Multiple solutions for this feature are starting to be implemented
- This feature has already been described at High Level in ATA DSWG Spec 42 - 2020
- Proposal to update ARINC 842 to provide implementation guidance, ensure consistency and allow compatibility
- Standardization also allows reuse of components (Ground and Board) across multiple vendors/manufacturers/suppliers/PKI

AIRBUS

Overall Principles

- The objective is to enable online maintenance workflows for certificate management

- The recommended certificate management should be centralized and remotely controllable from the ground
  - Requires Aircraft systems to be able to use Aircraft communication means to reach PKI provider servers
  - In some cases it implies that:
    - Devices need to have a local wired maintenance access
    - Or if via Wi-Fi, a network dedicated for device enrollment can be defined

- Maintenance actions on Aircraft for credential management should be avoided. Only necessary under “abnormal” conditions
  - Example of “abnormal” conditions:
    - A device is defect and needs to be replaced
    - A key has been compromised
  - Example of “normal” certificate management conditions:
    - A certificate is about to expire and a new certificate needs to be installed
    - A new key pair needs to be generated and a certificate signing request sent to the CA

AIRBUS

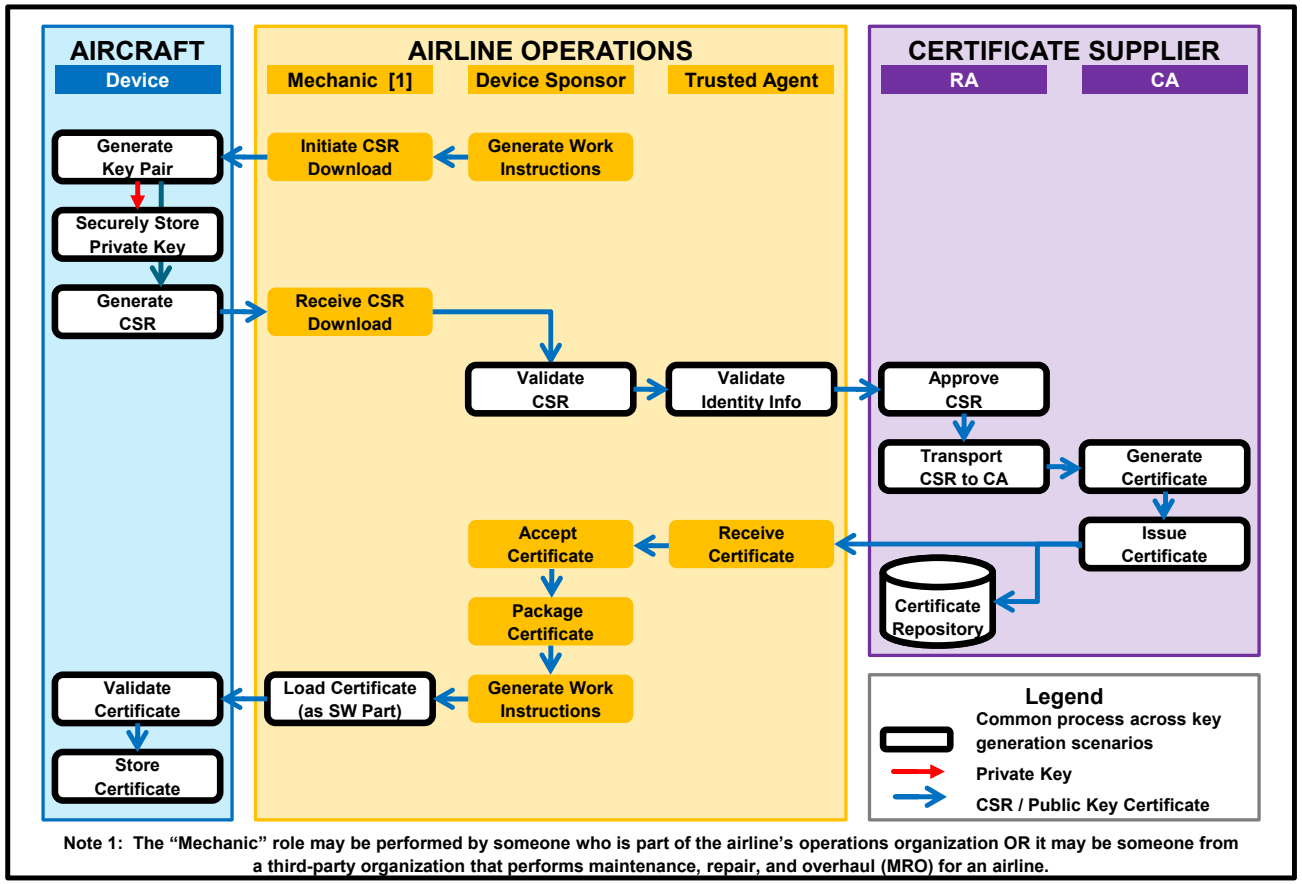
Online certificate management

- Aircraft devices has ground connectivity through a communication means
- Basic Workflow example:
  - Aircraft device determines that a new certificate is needed:
  - Aircraft device creates new keys and generates CSR (Certificate Signing Request)
  - Aircraft device sends CSR to PKI provider
  - Device sponsor is informed of certificate request
  - For medium or higher assurance levels: Device sponsor verifies device identity and authorizes CSR
  - CA issues certificate which is retrieved by Aircraft device
  - Aircraft device installs CSR
  - Device Sponsor verifies that certificate is correctly installed and in use on the Aircraft

AIRBUS

Standard on-aircraft key generation process flow

- This is a generic workflow for initial certificate installation and for re-keying
- Standardized in ARINC 842-2 (section 4) and ATA Spec 42 (section 5-7)
- The next slides will show how the online concept modifies the standard workflow



AIRBUS

Online Certificate Enrollment concept

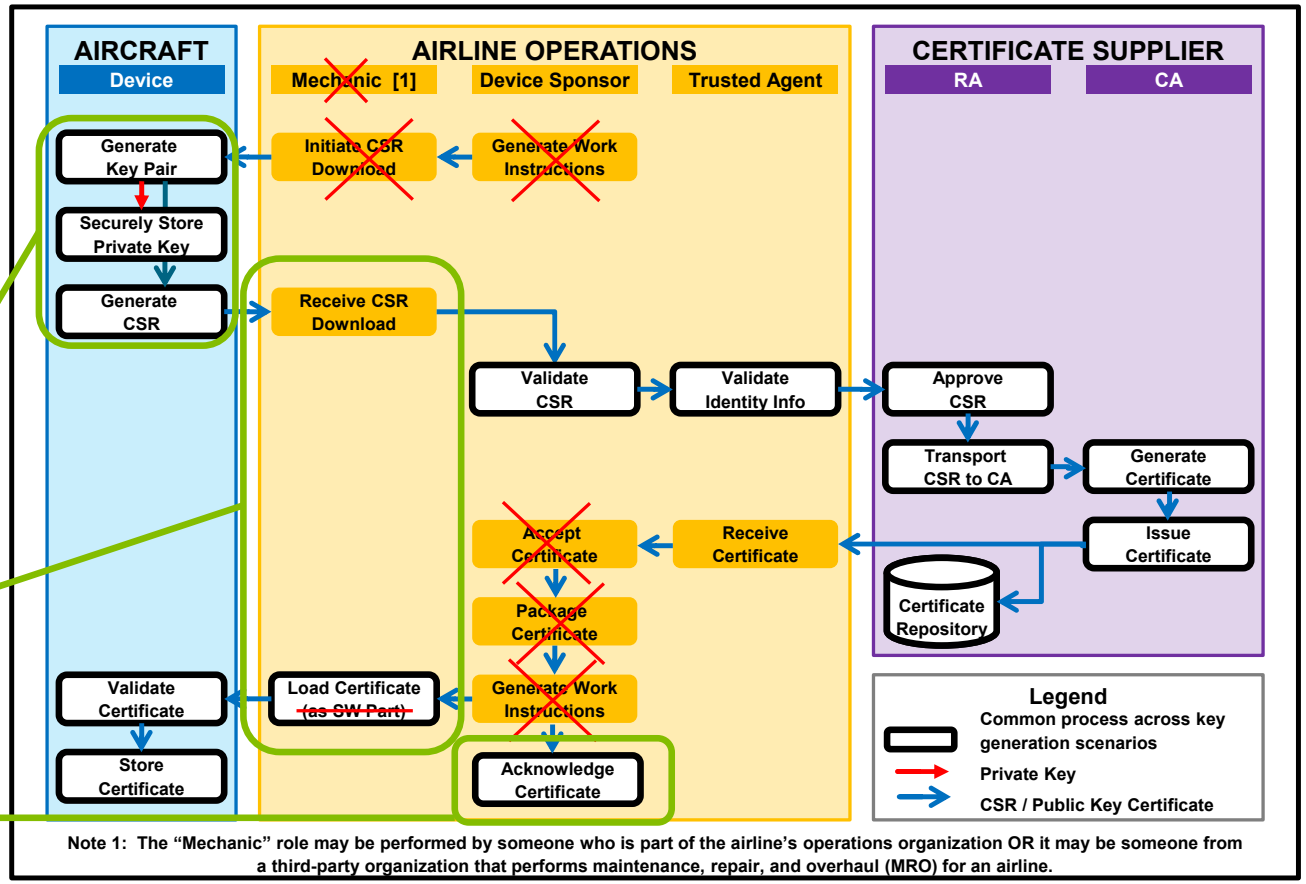
Online Certificate Enrollment principles:

- Simplify Non Security Airline Tasks
- Use Automatic Trigger when possible
- Device authentication to be ensured by the workflow (device and architecture)
- Standard protocol EST (Enrollment over Secure Transport, RFC 7030)
- Suitable for medium assurance

Automatic Trigger

EST via air-ground link
(inside or outside VPN)

Airbus process includes manual Acknowledgement step to confirm correct certificate installation on device



AIRBUS

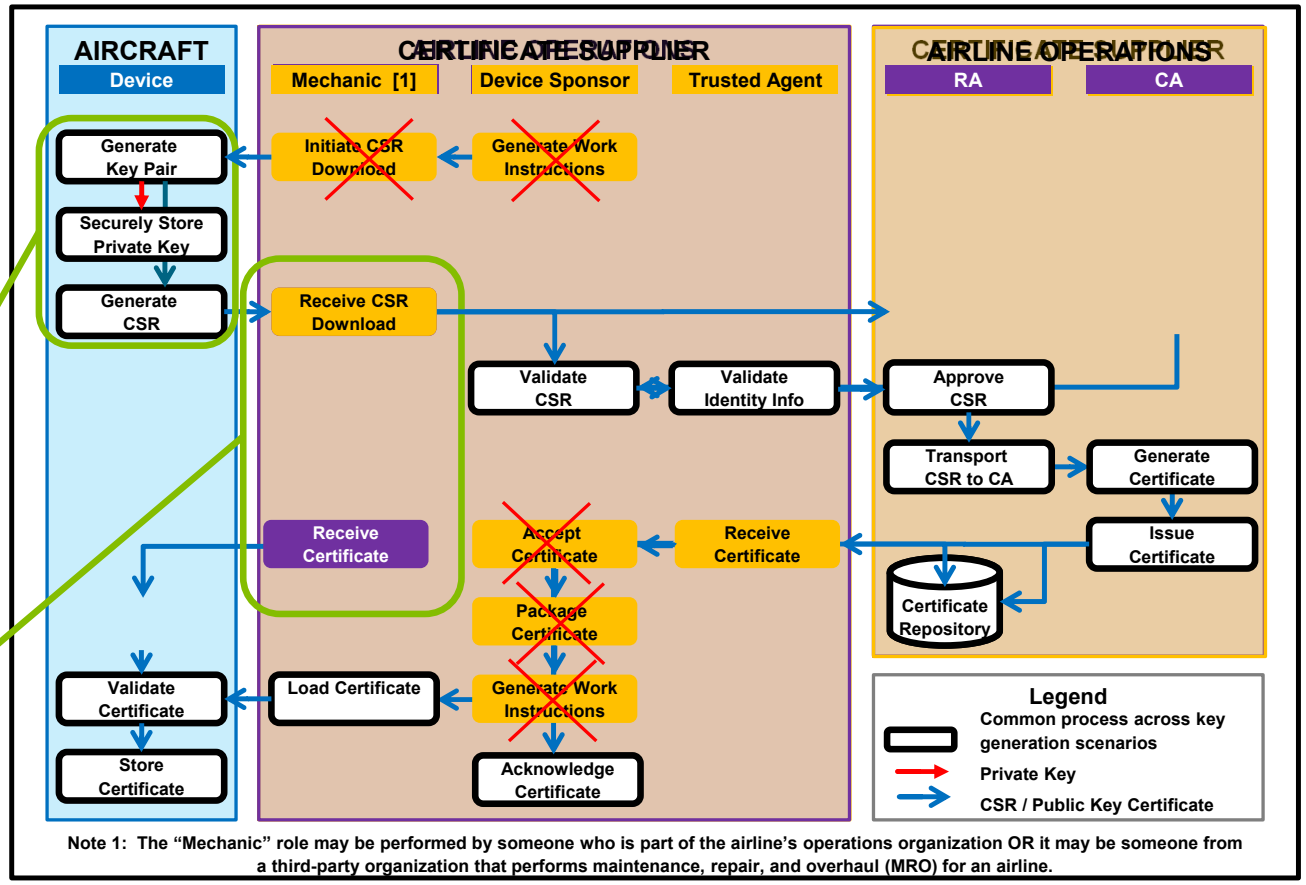
Device Initial Enrollment workflow

Device Initial Online Keying:

- Automatic certificate request to CA via EST protocol, includes device authentication (weak) to CA
- CSR Validation requires secure workflow (using process/architecture)
- Manual device sponsor approval

Automatic Trigger when no valid certificate for VPN

EST protocol



AIRBUS

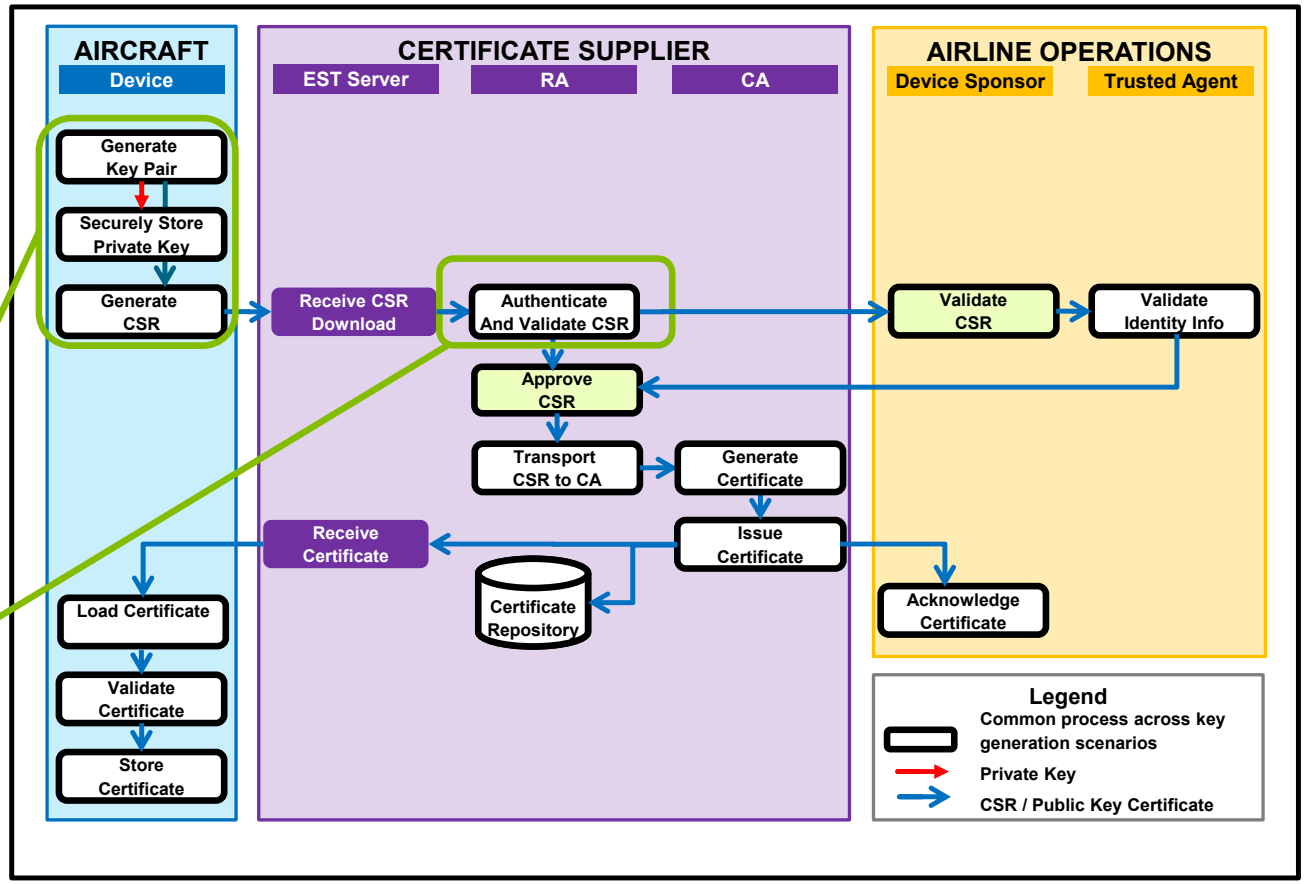
Device Reenrollment workflow

Device Reenrollment:

- Automatic Certificate reenrollment (Rekey) to CA via EST protocol, includes device authentication to CA
- Authentication using current certificate and certificate acknowledgement

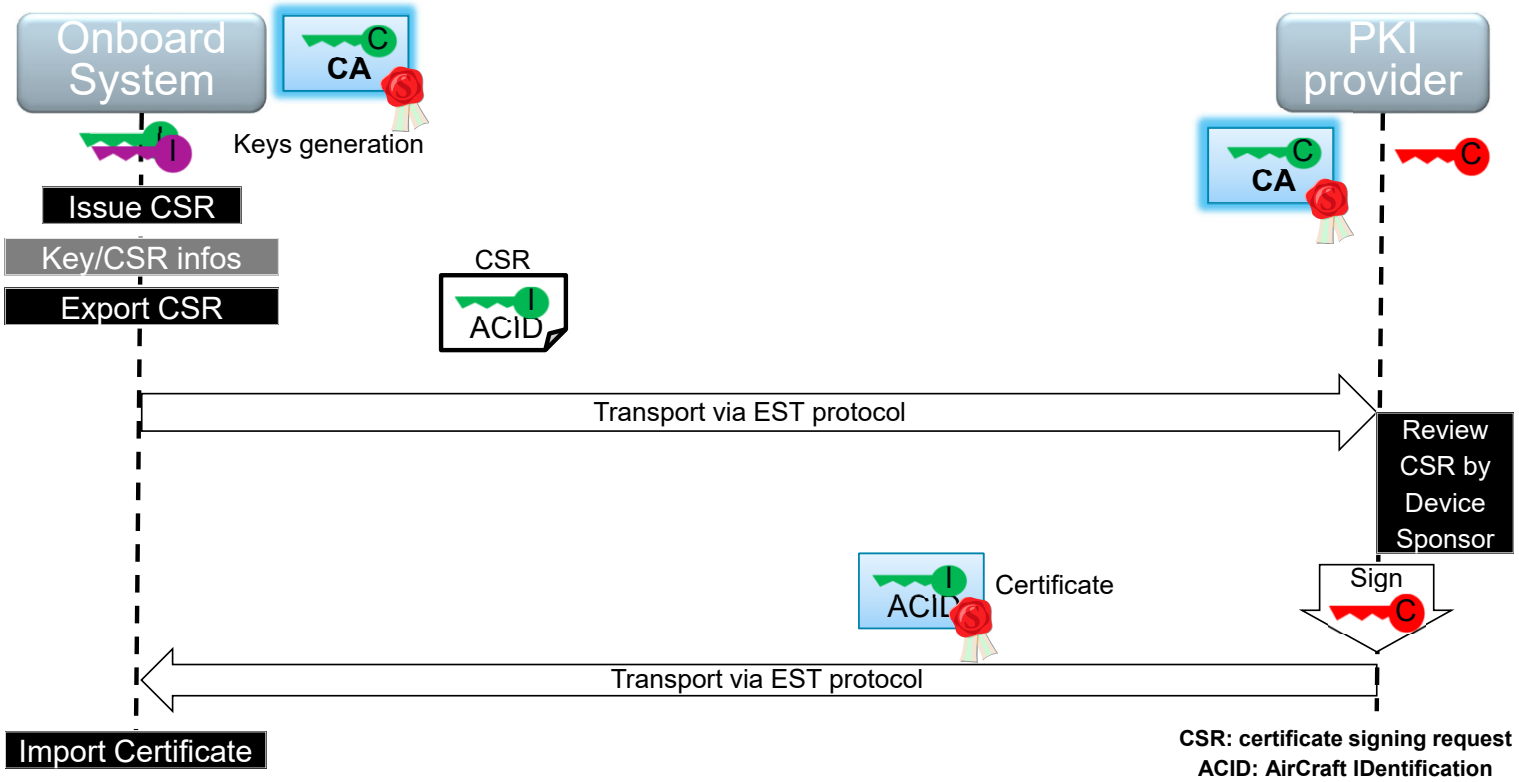
Automatic Trigger x days before current certificate expiration

EST protocol with authentication using currently valid certificate



AIRBUS

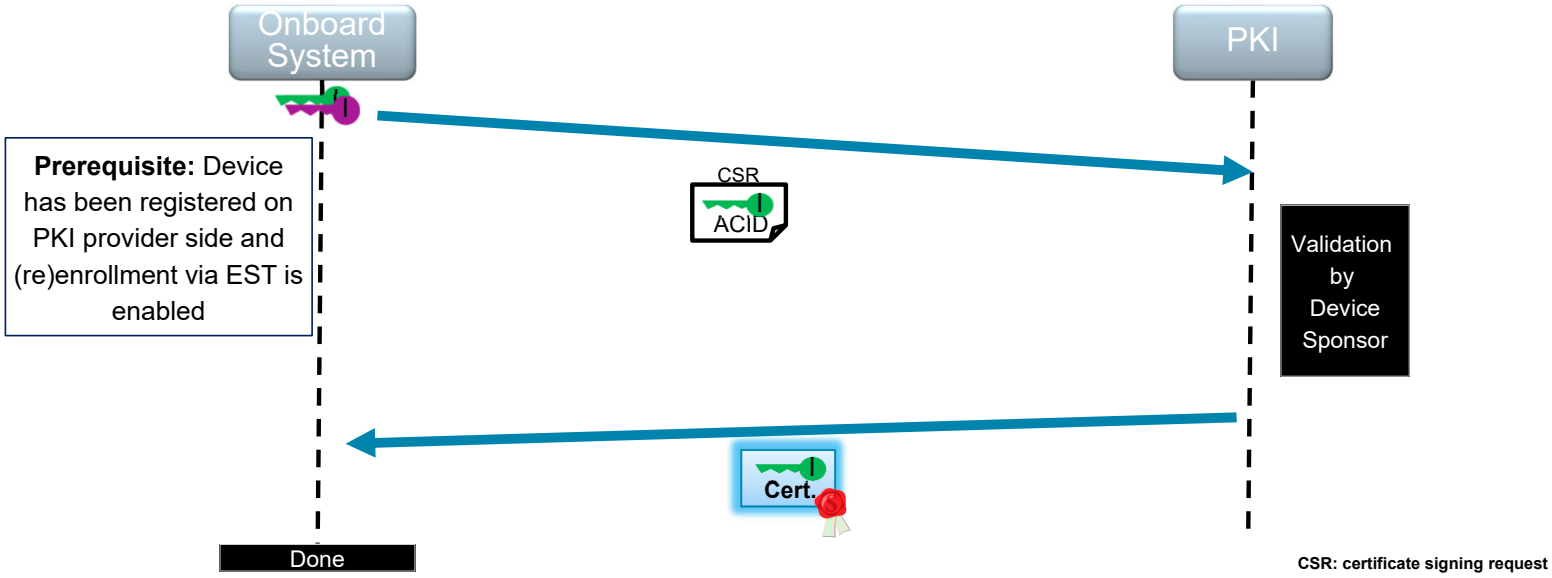
Keying with EST – Overall Principle



System Requests and Retrieves a Certificate to PKI Provider Server

AIRBUS

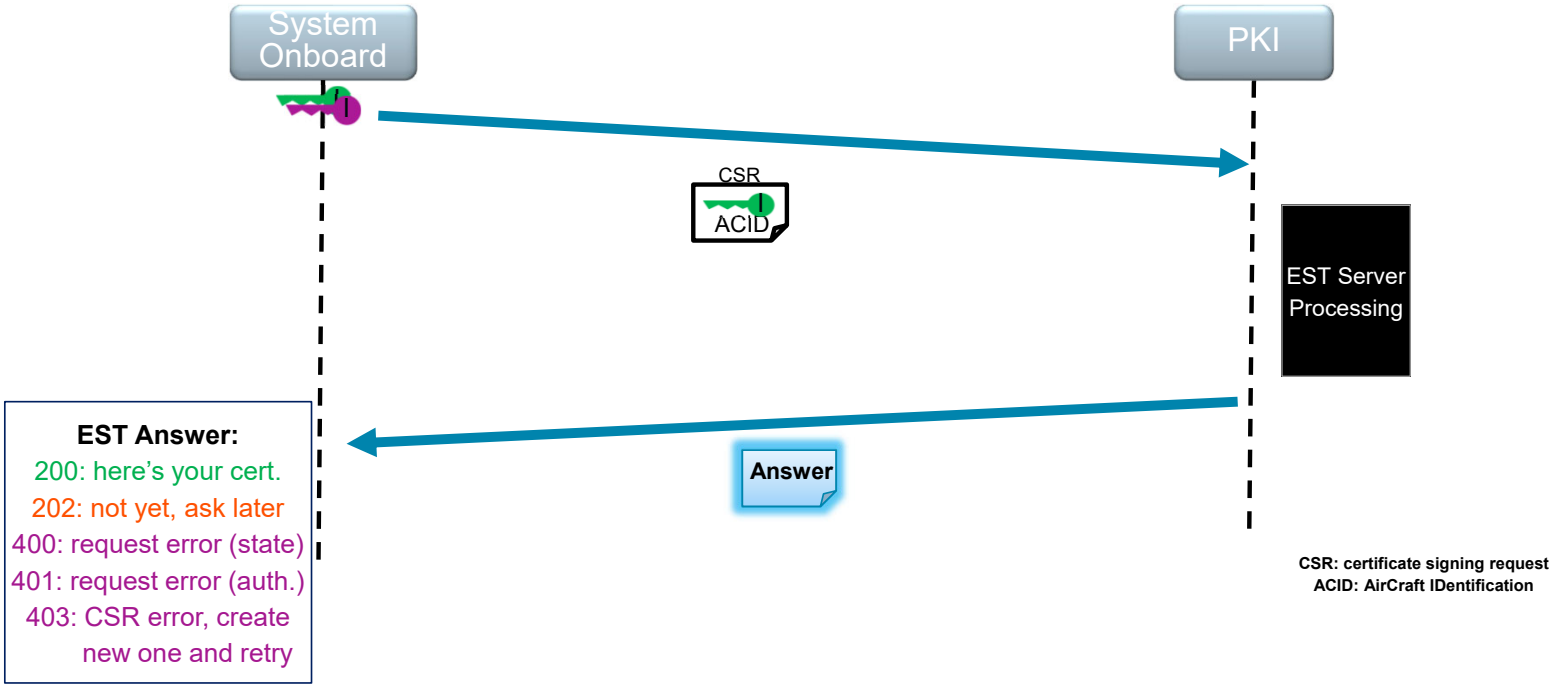
Keying with EST – Overall Principle



System Requests and Retrieves a Certificate to PKI Provider Server

AIRBUS

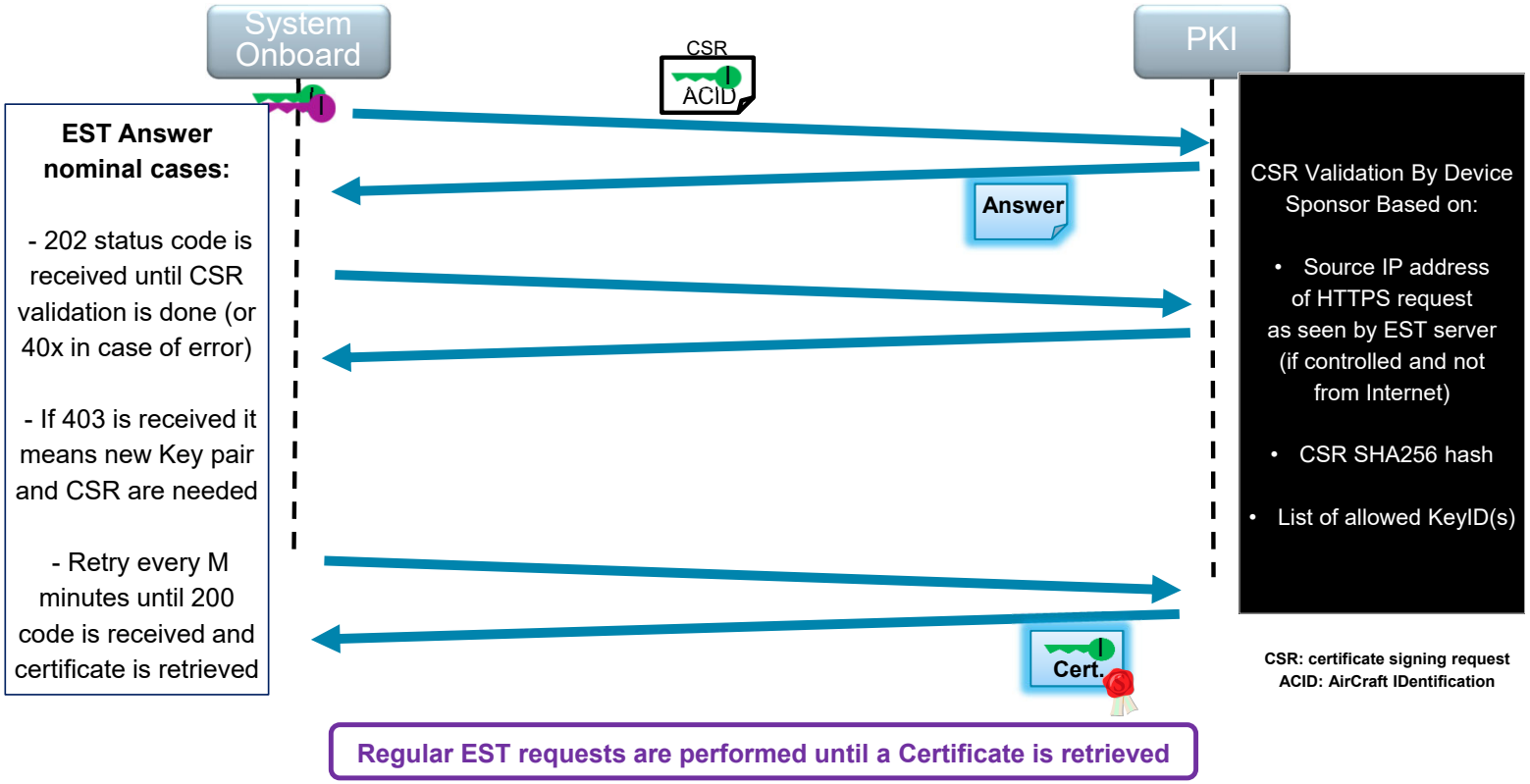
Keying with EST – Overall Principle



System Requests a Certificate for its CSR and Analyse the answer

AIRBUS

Keying with EST – Overall Principle



AIRBUS

Thank you

AIRBUS