Digital Certificate Management for ATN/IPS

Timo Warns

AEEC IPS / January 2019

AIRBUS

Introduction

- ATN/IPS security will include some secure channels (e.g. sDS, DTLS, …)

- Secure channels rely on
  - digital certificates (with its associated public/private key pairs) and
  - related metadata (e.g. certificate signing requests, certificate chain information, revocation data, …).

- Secure management of digital certificates is essential for adequate security level.
  Confer ARINC 842 / ATA Spec 42.

- Agenda:
  - Selected concerns on digital certificate management
  - Selected Airbus security constraints on digital certificate management
  - Review of IPS gateway proposal
  - Proposal for PP858

Selected Concerns on Digital Certificate Management

- **Scope**: What is the scope of a digital certificate? (Authentication/Integrity/Encryption, sDS / DTLS / Link protection, ATC/AOC)
- **Generation**: Each private key should be generated in a way preventing that an attacker can guess the key.
- **Transport**: If a private key needs to be transported, disclosure to an attacker should be prevented.
- **Storage:** Each key should be stored in a way that prevents access by an attacker.
- **Metadata:** How to securely manage metadata?
  - *Certificate requests*
  - *Revocation information*
  - *Certificate chain information* (e.g. root or bridge CA certificates)

Further concerns

- **Cryptoperiods:** What is the lifetime of a key?
- **Certificate issuance:** How to validate certificate issuance requests?
- **Certificate validation:** How to validate a certificate?
- **Certificate revocation:** What are the triggers to revoke a certificate?
- **…**

Selected Airbus Security Constraints on Digital Certificate Management

- **Scope**: The scope of a cryptographic key should be as narrow as possible.
  For example, the A/C should not use the same certificate for sDS and for radio links.
  → Trade-off with number of needed certificates

- **Generation / Transport / Storage**:
  - The transport of valid A/C private keys outside the A/C should be avoided.
  - A/C private keys should be generated on-board.
  - If generated on-ground, the A/C private keys should be generated/transferred/stored by a hardware security module that prevents a disclosure of the keys.
  - Security controls should prevent unauthorized access to private keys stored on-board.
  - ATN/IPS should use a centralized on-aircraft key management system if available.

Selected Airbus Security Constraints on Digital Certificate Management (contd.)

- **Metadata**
  - *Certificate requests / revocation information:*
    Certificate signing requests / responses and revocation information should be manageable via electronic distribution.
    Alternative distribution via physical media should be possible as fall back.

    A maintenance action should trigger the generation of key pair / CSR.

  - *Certificate chain information:*
    Certificate chain information should be considered part of the aircraft configuration.
    Updates should be performed as maintenance actions (e.g. via data loading).

Review of IPS Gateway Proposal

- **Scope**: DTLS* (protecting management traffic and application traffic)
  → One certificate for ATN/IPS per A/C, authentication & symmetric key exchange, ATC & AOC

  Decision on appropriate scope needs agreement on secure channels first (sDS vs DTLS etc.)

- **Generation / Transport / Stored**:
  Public / private key is generated on-ground (by service provider on behalf of operator?).
  Private key is sent in-band via IPS GW to A/C (inside DTLS*).
  Private key is (at least temporarily) stored on ground, incl. IPS GW.

  Very strong dependence on IPS GW security. End-to-end security can be broken by IPS GW.

- **Metadata**
  - *Certificate requests:* Managed on-ground (by service provider on behalf of operator?)
    Electronic distribution likely feasible. Involvement of operator / MRO needs clarification.
  - *Revocation information:* Support for OCSP stapling, CRL could be retrieved as well
    Very good support for electronic distribution of revocation information
  - *Certificate chain information:* Updated on A/C via IPS GW (inside DTLS*)
    Unlikely to be considered a maintenance action.
    Strong dependence on IPS GW security. End-to-end security can be broken by IPS GW.

Proposal for Way Forward

- Put digital certificate management per se out-of-scope of PP858.

- Identify an interface to an on-aircraft cryptographic key management system.
  - For different implementations, this may be a centralized system or a local function integrated into the IPS router.

- Characterize the interface to the key management system as needed for ATN/IPS.
  - Description of principle services needed (and offered?) by ATN/IPS
  - Characterize the number / types of digital certificates to be used by ATN/IPS

Thank you

AIRBUS