Authentication in ATM

April 10, 2025

Per Erland Andersen – SESAR Deployment Manager

Funded by
the European Union

ICNS

Presentation Agenda

The Problem and The Objective

Application examples in the CNS domain

- Navigation – SBAS
- Surveillance – Radar

Secure communication
The Problem and The Objective

The situation and the problem:

*Communication is **not secured** on application level, relying on closed network or perimeter defences. Air-ground communication **also** suffers from **low security not using secure identification** (e.g., ADS-B)*

Secure communication is critical as aviation transitions to digital services.

From CP1:

*"To **achieve** the cyber security objectives **appropriate** for the service or services."*

Solusion

Identification and Authentication is key

Having this in place, several different cryptographic techniques can be used to ensure secure communication e.g. HMAC (Hash-based Message Authentication Code)

SBAS Authentication

SBAS Authentication

SBAS improves the accuracy and reliability of GNSS information by correcting signal measurement errors, but SBAS is subject to threads:

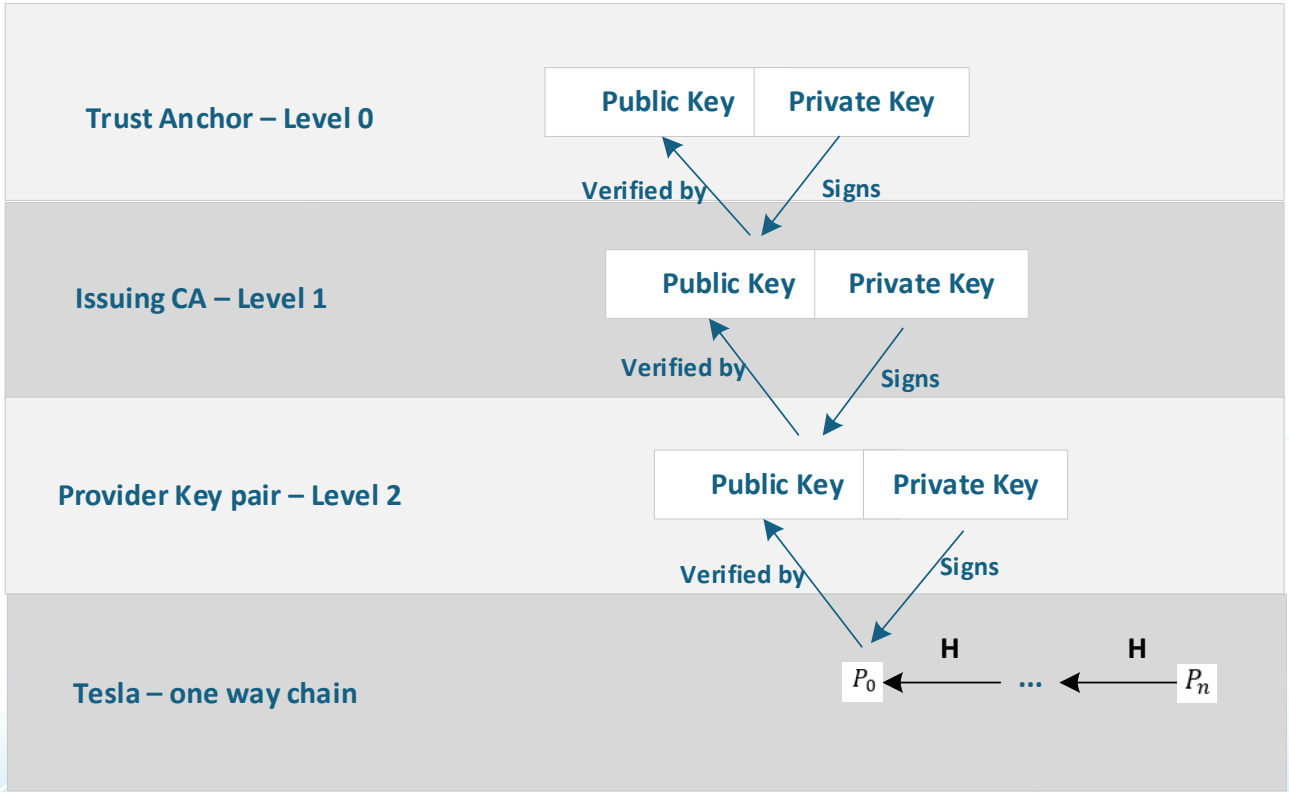
- Spoofing: an adversary masquerades SBAS satellites broadcasting erroneous signals. Example of this threat category includes:
  - Impact on the SBAS services, on correction and GNSS health status,
  - Mislead the position solution of receivers
- Tampering: unauthorized change of data or state: an adversary may intercept, manipulate and re-broadcast the signals

SBAS Authentication

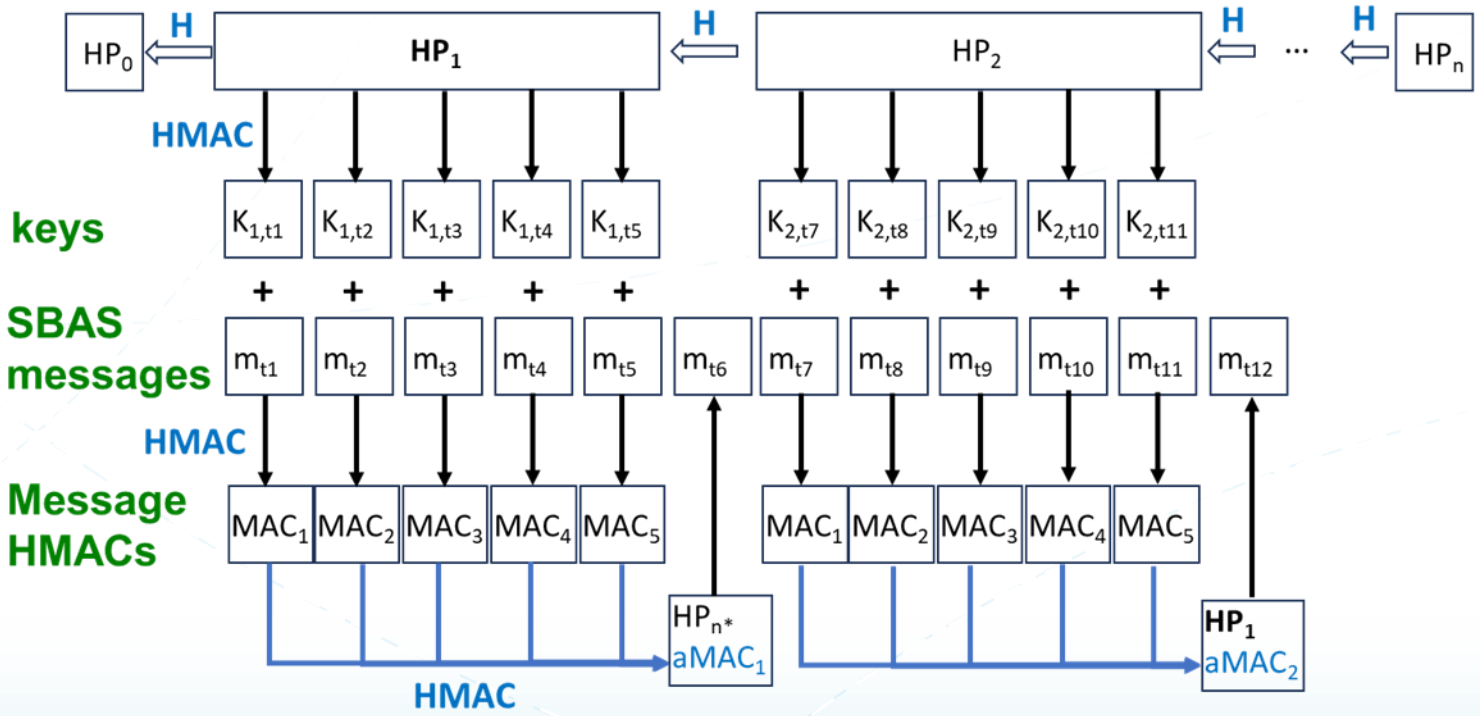
SBAS Authentication Trust Chain

SBAS message authentication implements a cryptographic protocol to protect the integrity and authenticity of SBAS messages:

- Relies on a combination of symmetric and asymmetric cryptographic keys used for the computation of Message Authentication Codes (MACs) and digital signatures.
- SBAS Keys are organised in a hierarchical model with four levels (Level 0 – Level 3).
  - Level 0 to Level 2 based on Digital certificates managed by PKI
  - Level 3 is based on the Timed-Efficient Stream Loss-Tolerant Authentication (TESLA) protocol

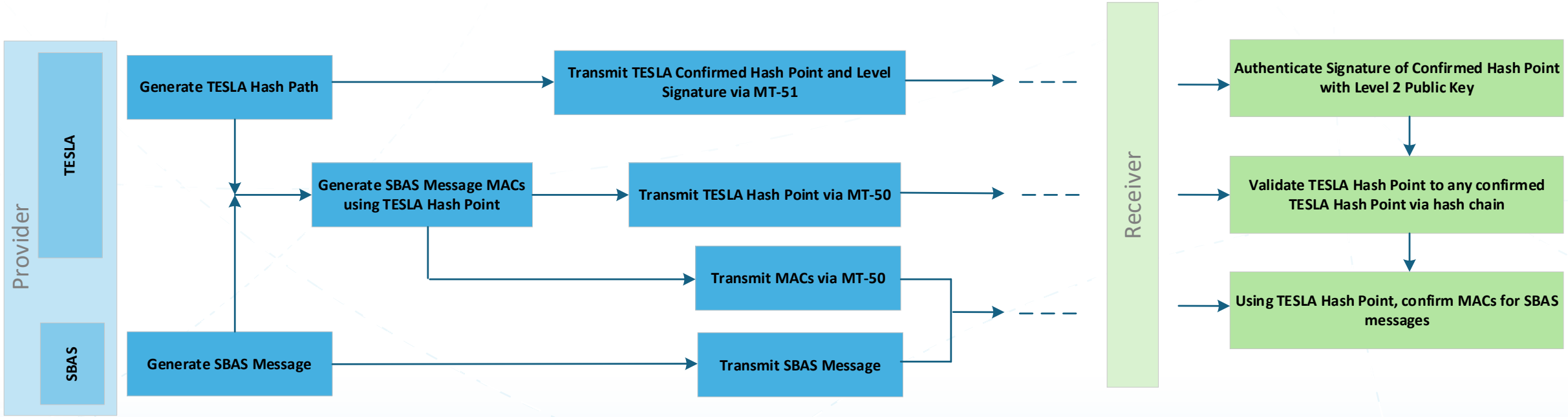


SBAS Authentication



SBAS Authentication

SBAS authentication key management data flows

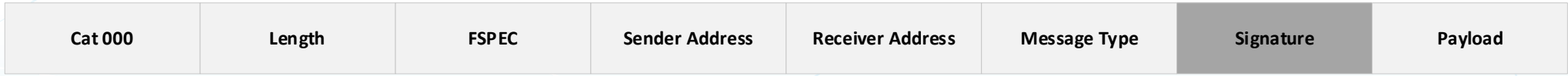


Securing ASTERIX

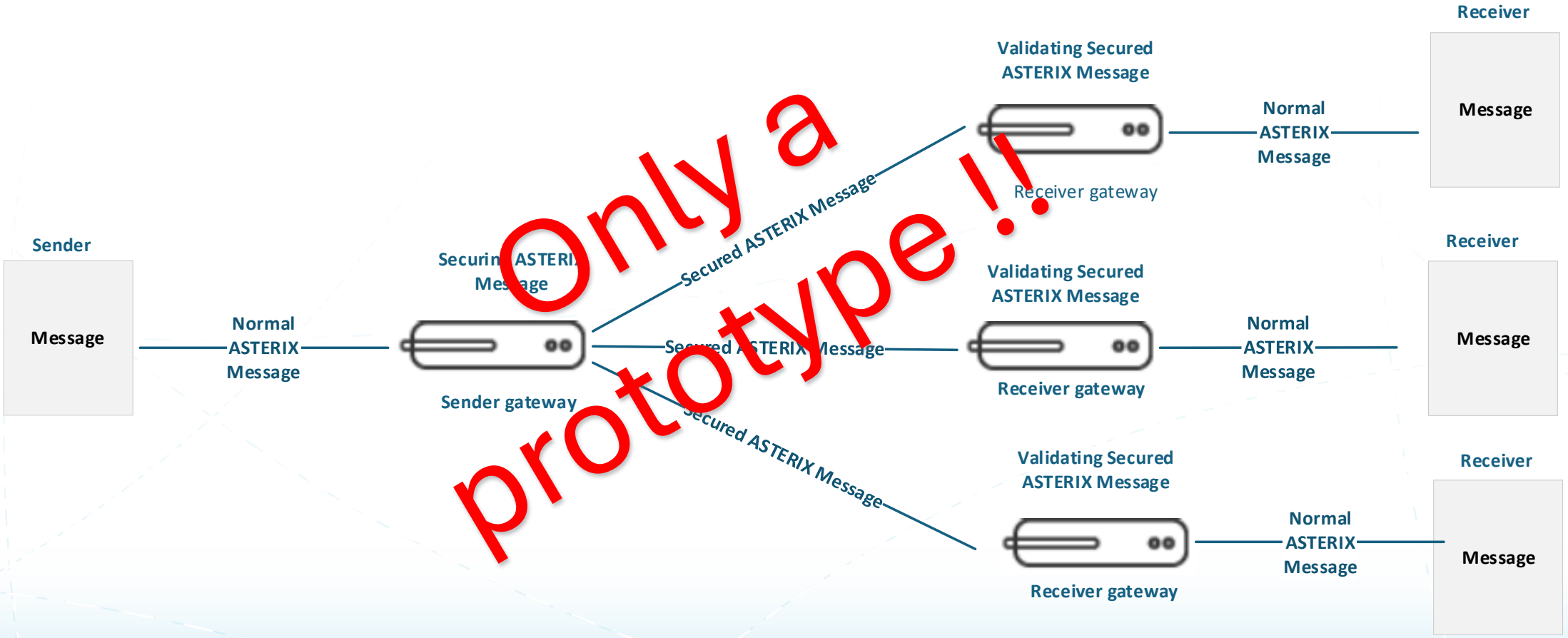
Securing ASTERIX

In Europe, Surveillance data is exchanged using ASTERIX protocol

- Surveillance data could be sensor data (radar, ADS-B, weather radar) or processed data from trackers
- ASTERIX does not have mechanism to provide integrity and authenticity of information, and is therefore vulnerable
- The "ASTERIX Maintenance Group" decided to include security extension in the ASTERIX Specification → Cat 000
  - Use of standardised cryptographic algorithm and open-source software



Prototype: Network Topology



Funded by
the European Union