

Accommodating EST in the ATN/IPS Stack

Follow-up on Feedback

Timo Warns

08 December 2021

Reminder: EST for IPS

- EST: protocol for certificate management
- ARINC 858 Part 1 identifies the potential need for adaptation of RFC 7030 (EST) to support transport using DTLS/UDP rather than TLS/TCP.
⇒ Need to assess options, agree on an approach/approaches, and document requirements in appropriate IPS standards.
- Four identified options:
 - EST over HTTPS (RFC 7030, TCP-based)
 - EST over HTTP/3 (RFC 7030 profiling, UDP-based)
 - EST over COAP (RFC draft, UDP-based)
 - Aviation-specific adaption of EST over UDP

IPS – Options for Enrollment over Secure Transport (EST)

Option	Description	Pros	Cons
1	EST over HTTPS	<ul style="list-style-type: none"> Compliant with RFC 7030 No impact on COTS SW No impact on EST server implementation 	<ul style="list-style-type: none"> Requires TLS / TCP in Airborne IPS System
2a	EST over HTTP/3	<ul style="list-style-type: none"> UDP-only solution Straightforward adaptation since HTTP semantics do not change with HTTP/3 	<ul style="list-style-type: none"> Not strictly RFC 7030 compliant Currently, no COTS SW support for DAL C
2b	EST over COAP	<ul style="list-style-type: none"> UDP-only solution Leverage standards under development https://datatracker.ietf.org/doc/draft-ietf-ace-coap-est/ 	<ul style="list-style-type: none"> COAP stack at CA level Standards completion risk Currently, no COTS SW support for DAL C
2c	Aviation-specific EST over UDP	<ul style="list-style-type: none"> UDP-only solution 	<ul style="list-style-type: none"> Aviation-specific stack at CA level Lack of COTS SW support Standards acceptance risk

Received Feedback

- **Aviation-specific accommodation should be avoided if possible**
- Feasibility of TCP-based EST client
 - If the EST client could be implemented as a native IP application at lower DAL (DAL D/E), then a TCP-based solution may be the most easy approach.
 - Note that EST client would only be needed on-ground.

⇒ **Need for UDP-only solution to be confirmed.**
- Currently, embedded COTS SW not obvious for EST over HTTP/3 or COAP.
- However, some embedded COTS SW support available for COAP.

⇒ **EST over HTTP/3 should not be preferred over COAP without further evaluation.**

Thank you

© Copyright Airbus (Specify your Legal Entity YEAR) / Presentation title runs here

This document and all information contained herein is the sole property of Airbus. No intellectual property rights are granted by the delivery of this document or the disclosure of its content. This document shall not be reproduced or disclosed to a third party without the expressed written consent of Airbus. This document and its content shall not be used for any purpose other than that for which it is supplied.

Airbus, its logo and product names are registered trademarks.