Concepts Beyond

SCVP Validation with TLS/DTLS in an air to ground communication

May, 2022

Ashley Kopman (Concepts Beyond)
Rob Segers (FAA)

Set the Stage

- In a digital global aviation ecosystem there is a need for interoperability and cyber resilience
  - To support this, a globally harmonized trust framework is in development
  - This framework will enable trusted digital ground-to-ground, air-to-ground and air-to-air communications
- The ICAO trust framework is based on Public Key Infrastructure (PKI) to harmonize and map commercial aviation identity and access requirements to a common set of operating rules
  - The cross-certified Certificate Authority (CA) hierarchy governed by the trust framework Certificate Policy (CP) is used to establish trust
- Server-based Certificate Validation Protocol (SCVP) can be leveraged to delegate path discovery and validation, reducing load on the client and resulting in consistent application of validation policies

Air-To-Ground Communications

- Air-to-ground communications are switching from voice communication to digital data communications
  - Improves performance and reduces errors
  - These safety-critical messages must be secured to ensure the messages can be trusted
- Current IATF work has largely focused on interoperable infrastructure for integrity and identity validation in ground-to-ground data exchange
  - Cross certificates and validation using SCVP are key components in a flexible PKI hierarchy
  - Air-to-ground communications are limited bandwidth and sometimes high latency
  - Limit the number of round trips and bandwidth involved
  - To extend the work done to air-to-ground communication need to enable validation without requiring direct aircraft communication with SCVP Server

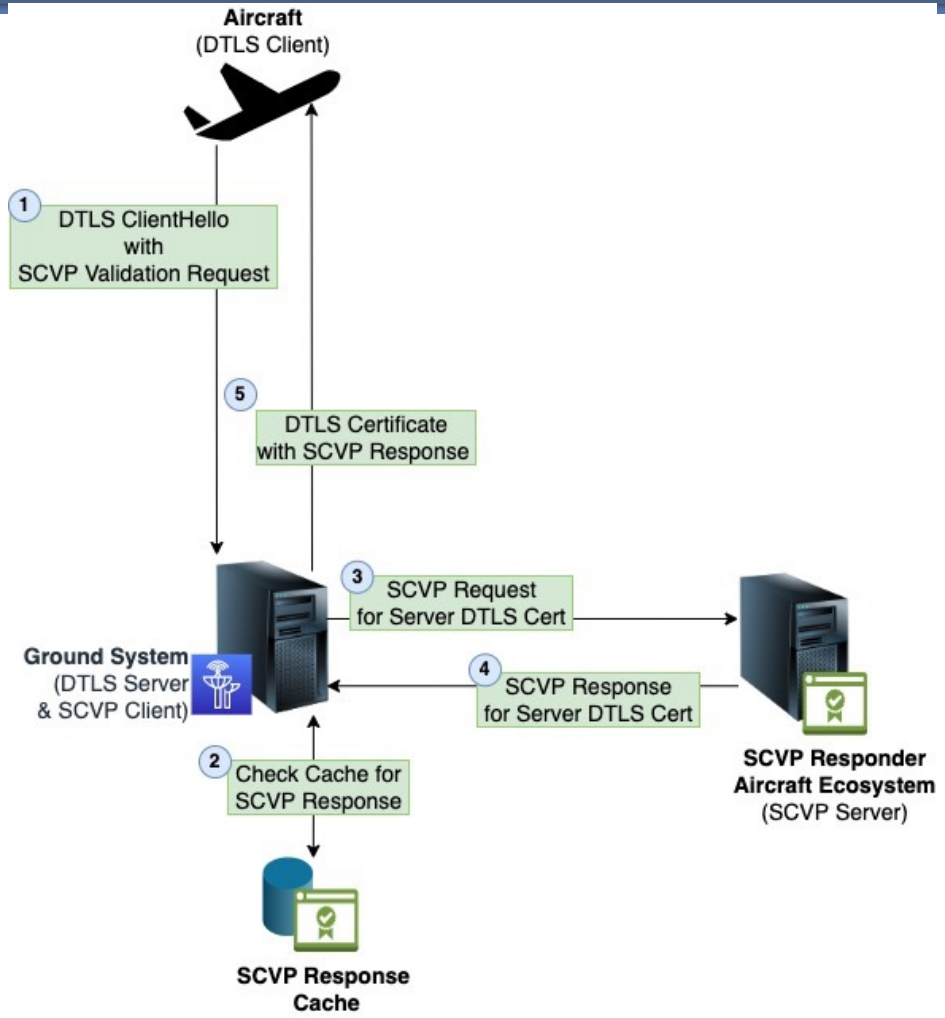
Validating Ground Server Identity

- This can be done by either:
  - Implementing certificate path building and validation on the aircraft
    - Requires loading each aircraft with all trust anchors in use by ground servers communicating with aircraft
    - Requires regular uploading of CA Certificate Revocation Lists (CRLs) to aircraft at least every 24 hours
  - Utilize SCVP Validation Request Extension to establish trust
    - Requires only a single trust anchor onboard the aircraft

SCVP Validation Request Extension

- Online Certificate Status Protocol (OCSP) Status Request Extension has been proven effective means to provide OCSP response to Transport Layer Security (TLS) client
- OCSP Status Request has limitations in the cross-certified PKI hierarchy
  - Requires the OCSP Response and certificate for each step in the path which makes the OCSP Certificate Status Request quite large
  - SCVP provides single response for the server certificate with full path validation without providing full details in the Validation Response, signed by an SCVP server that can be verified against the aircraft trust anchor
- Leverage the OCSP Status Request Extension idea to create similar TLS extensions for SCVP Validation Request
  - Eliminates need for client to reach the SCVP Responder
  - Increases performance, decreases bandwidth
- Removes burden of SCVP request from the aircraft client by having ground system server make the SCVP request and provide the result to the client
- TLS / Datagram Transport Layer Security (DTLS) 1.2 and 1.3 have extensions for OCSP Status Request, propose definition of similar extensions for SCVP Validation Request

SCVP Validation Request in Aviation

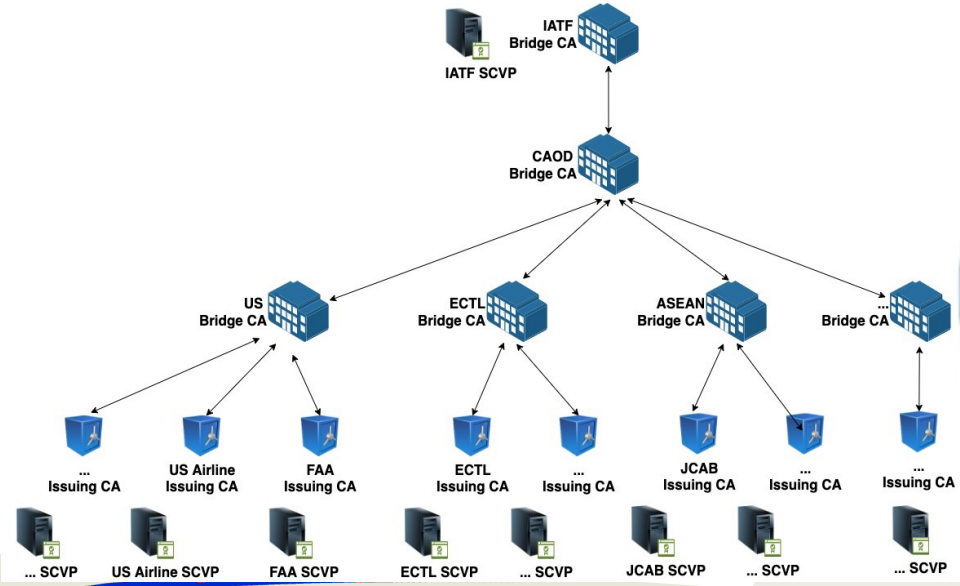


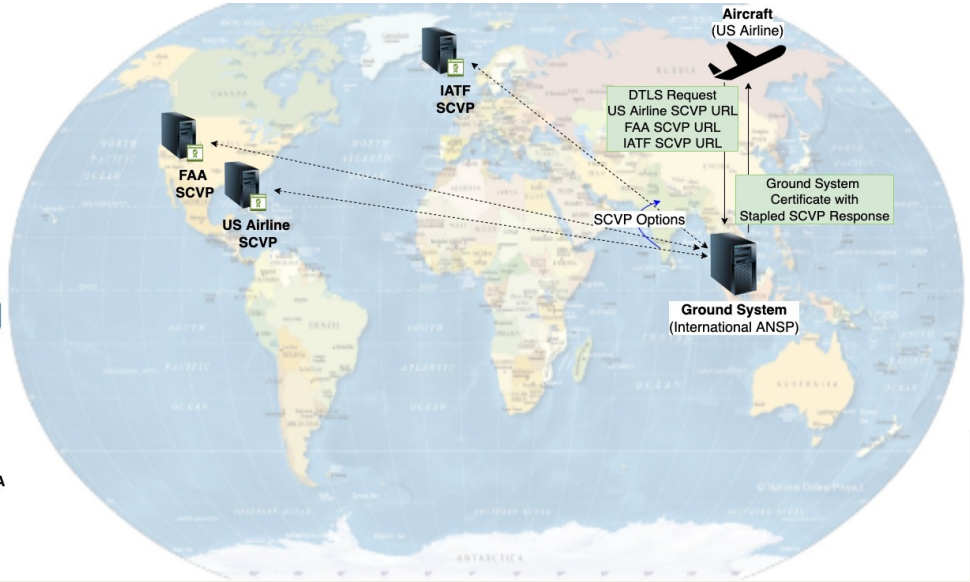
1. The Aircraft initiates the DTLS Connection and includes an SCVP Validation Request DTLS extension
   - Includes either:
     - URIs of the SCVP Responders trusted in the aircraft ecosystem (Including an IATF SCVP Responder)
     - Trust Anchor to use for Certificate path construction and validation
   - Optionally includes SCVP Request settings
2. The Ground System (DTLS Server) receives the ClientHello with the SCVP Validation Request and checks the Cache for an SCVP Response from the specified SCVP Responder
3. If no response if found in the cache, the Ground System generates a SCVP Request
   - The Request to validate the DTLS Server's certificate is sent to the SCVP Responder at the specified URL
4. The SCVP Responder processes the request and generates an SCVP response
   - The Response is sent back to the Ground System
   - The Ground System adds the response to the cache
5. The Ground System includes the SCVP response to the server certificate in the response to the Aircraft

Concepts Beyond

SCVP in International Aviation

- In international aviation there is a potential for many Certificate Authorities and SCVP Servers
- SCVP could be provided at any or all levels in the PKI hierarchy
  - At the Airspace User (AU), Air Navigation Service Provider (ANSP), Regions and/or Internationally
- By allowing the aircraft to specify the SCVP Responders, ensure trust can be established from anywhere in the world
  - The IATF SCVP required as a neutral fallback reachable by any member of the trust framework
  - Alternatively, support use of Trust Anchor with Ground System known SCVP Responder





SCVP Validation Request for Short Lived certificates

- Short lived certificates can be used to reduce the size of CRLs and therefore mitigate many issues with revocation checking
- Establishing trust in short lived certificates is still needed
  - To establish trust, a path from the end-entity certificate to a Trust Anchor must be constructed and policy validated
  - Certificate validation is a complex process
  - SCVP can offload the complexity of certificate path construction and validation to a server
  - SCVP can centralize the administration of validation policies, ensuring that policies are consistently enforced across clients
- When utilizing SCVP, short-lived and long-lived certificates have same security posture and maintenance strategy from an aircraft perspective
  - Revocation checking is performed by SCVP server
- Consider using short-lived certificates for the SCVP server to sign responses

Conclusions

- SCVP should be used to enable validation of certificates in a complex International Aviation PKI Ecosystem
  - This has been shown in ground-to-ground communications
- SCVP Validation Request is proposed as a mechanism
  - To reduce overhead for TLS/DTLS Clients
  - To reduce the path validation and CRL downloads necessary onboard the aircraft
- Use of short-lived certificates do not fulfill the need to validate trust
  - SCVP Validation Request extension can be used in combination with short-lived or long-lived certificates to establish trust