SCVP Validation Request (D)TLS 1.3 Extension

Rob Segers (FAA)

Ashley Kopman (Concepts Beyond)

7/25/2022

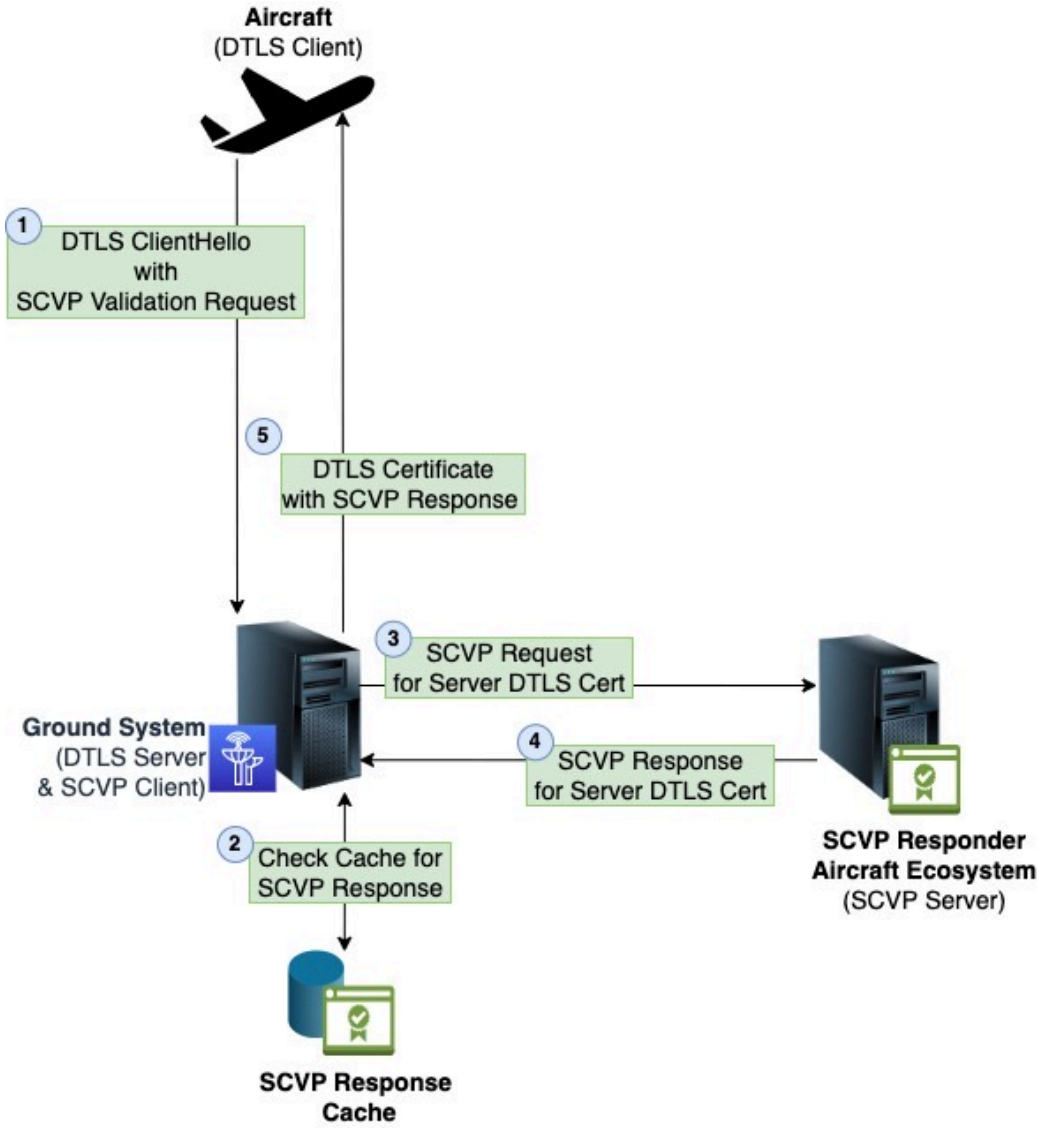
Use Case – Global Aviation

- In global aviation there is a need for information security interoperability and resiliency
- ICAO is developing a trust framework using PKI to harmonize and map commercial aviation identity and access requirements to a common set of operating rules
- Server-based Certificate Validation Protocol (SCVP) RFC 5055 is used to validate identity and trust
  - No centralized way to proliferate trust lists throughout aviation
  - Software developed/owned/operated/managed independently
  - ICAO operates on the principle of state sovereignty
  - Interoperability is key, can only be done using standardized protocols

Air-To-Ground DTLS Communications

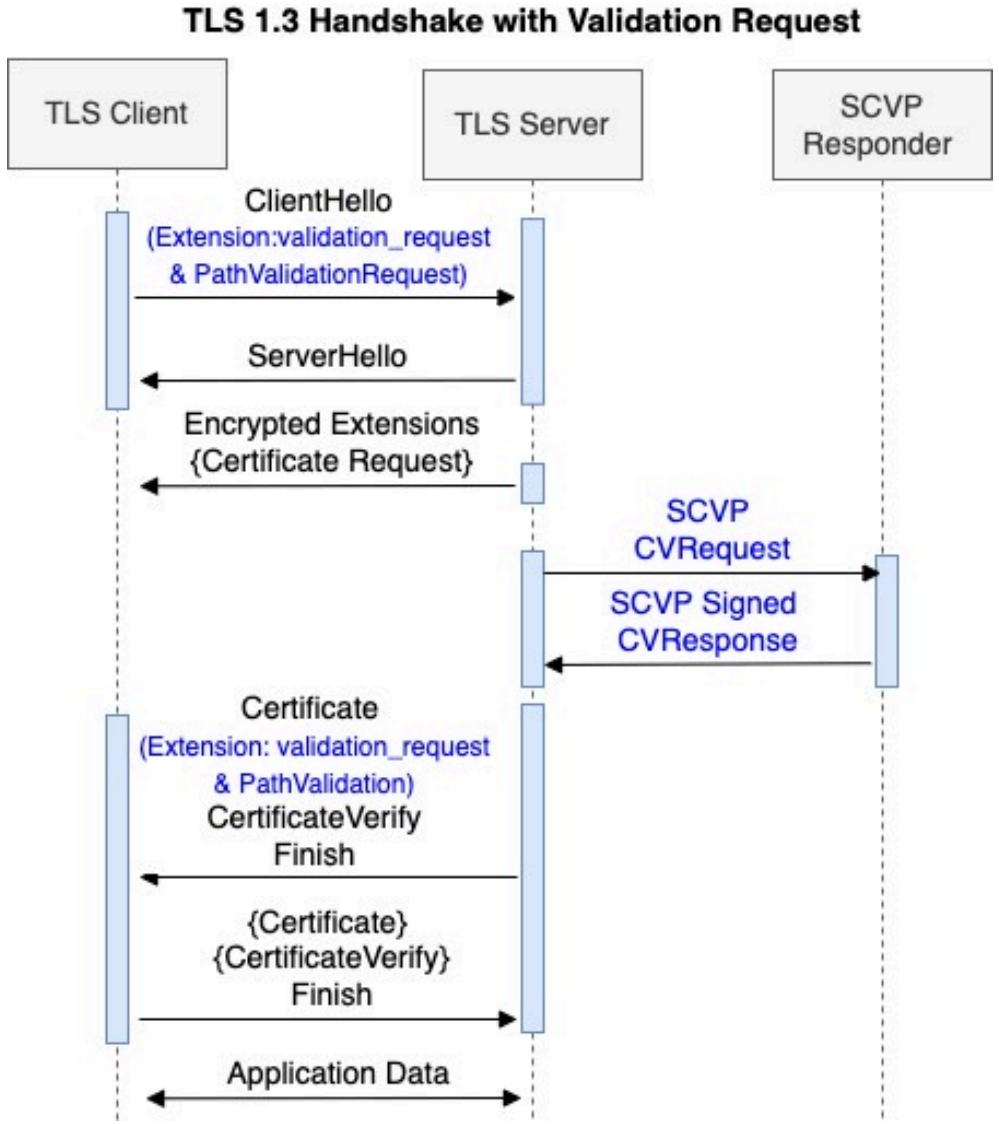
- Trend in Aviation Industry to move away from custom protocols to internet standards
  - Feed any customization necessary back into internet standards where possible
  - Obtain IETF stamp of approval for aviation industry adoption
  - Data communication evolution: ACARS -> OSI -> IP
- Ground certificate validation on the aircraft using trust lists and CRLs
  - Requires loading each aircraft with all trust anchors in use by ground servers communicating with aircraft
    - Airlines(>5,000) + ANSPs(193) + OEMs(~100) = +/- 5,500 ground entitles ~25,000 Commercial Aircraft worldwide
  - Requires regular uploading of CA CRLs to aircraft at least every 24 hours
- Ground certificate validation on the aircraft using SCVP Validation
  - Requires only a single (or small set) of trust anchors onboard the aircraft
  - Propose new SCVP Validation Request TLS 1.3 Extension to remove burden of SCVP request from the aircraft client by having ground system server make the SCVP request and provide the result to the client

SCVP Validation Request in Aviation



1. The Aircraft initiates the DTLS Connection and includes an SCVP Validation Request DTLS extension
   - Optionally includes URIs of the SCVP Responders trusted in the aircraft ecosystem
   - Optionally includes Trust Anchor to use for Certificate path construction and validation
   - Optionally includes SCVP Request settings
2. The Ground System (DTLS Server) receives the SCVP Validation Request and checks the Cache for a matching SCVP Response
3. If no response is 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 specified by the Aircraft
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 in the response to the Aircraft

Proposed (D)TLS 1.3 Extension Validation Request

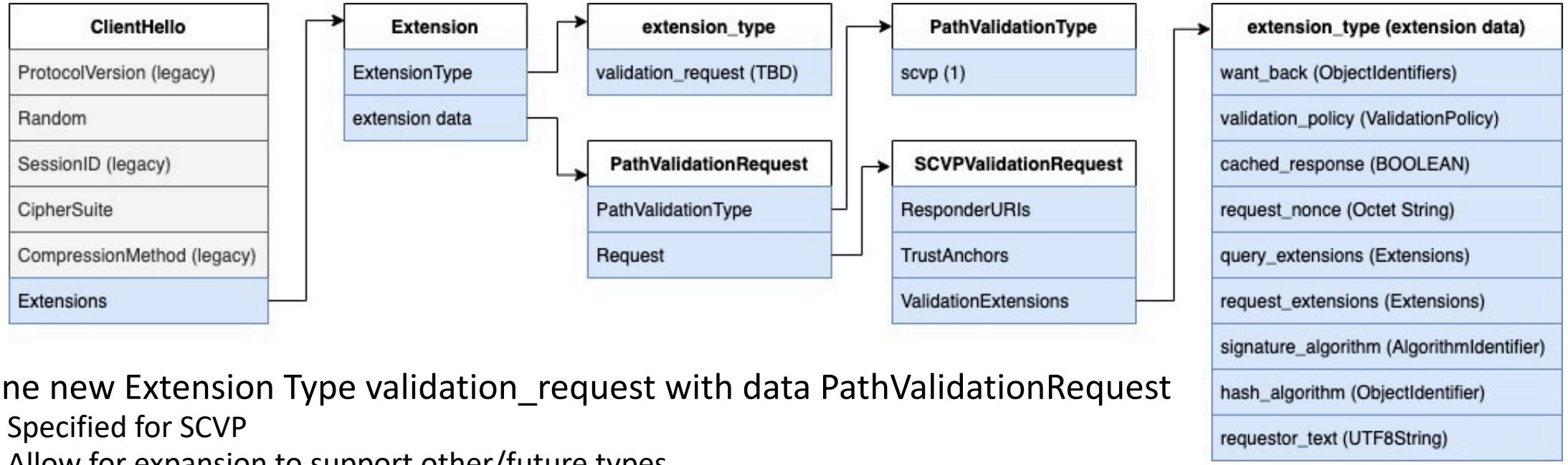


Allow (D)TLS clients to request that the (D)TLS server sends the client certificate path validation information during a (D)TLS handshake

- Based on status_request extension for sending OCSP information in (D)TLS handshake
- Define new Extension type to (D)TLS 1.3 called validation_request
- Define new PathValidationRequest structure for ClientHello extension
  - Defined for type Server-based Certificate Validation Protocol (SCVP)
- Define mapping of SCVPValidationRequest extensions to SCVP Request
- Define new PathValidation structure for Certificate extension
  - Defined for type SCVP

Back up

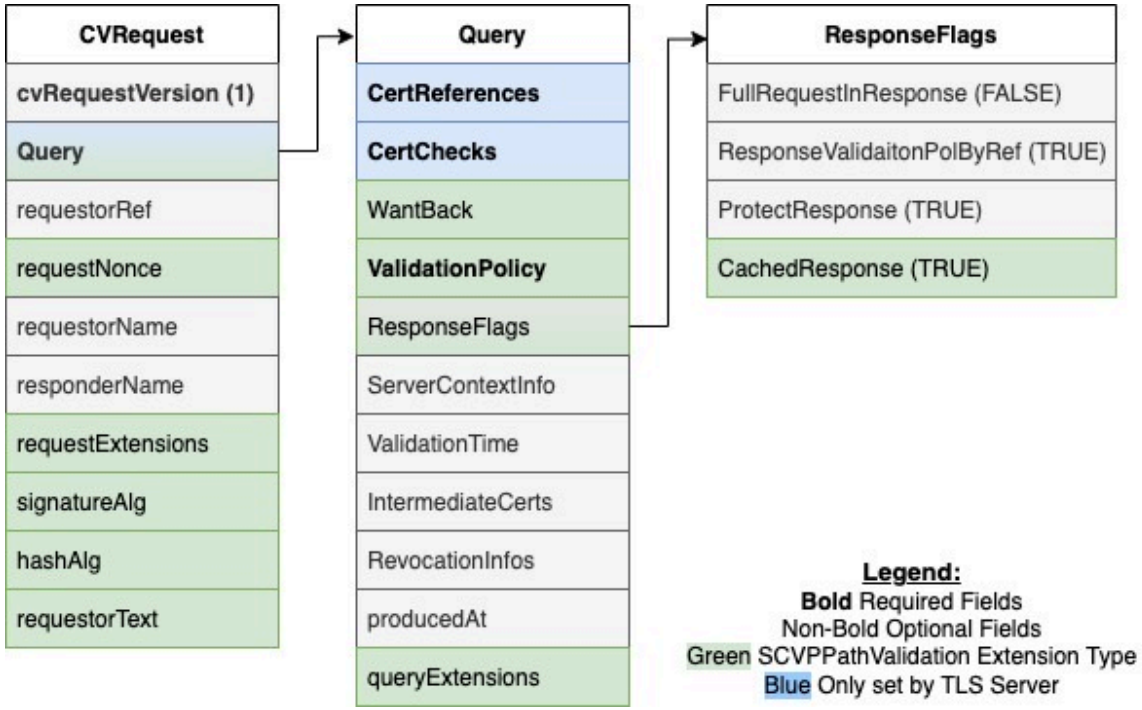
TLS 1.3 ClientHello Extension



- Define new Extension Type validation_request with data PathValidationRequest
  - Specified for SCVP
  - Allow for expansion to support other/future types
- SCVPValidationRequest
  - ResponderURIs – ASN.1 SEQUENCE of IA5String
    - SCVP Responder(s) the Client Trusts, zero length if trusted responders are known by TLS Server
  - TrustAnchors – ASN.1 SEQUENCE of PKCReference
    - TrustAnchors at which certificate path must terminate, zero length if known by the TLS Server OR the SCVP Responder trust anchors should be used
  - ValidationExtensions
    - Allow client to specify value in SCVP RFC 5055 CVRequest
    - Extension data types map directly to CVRequest

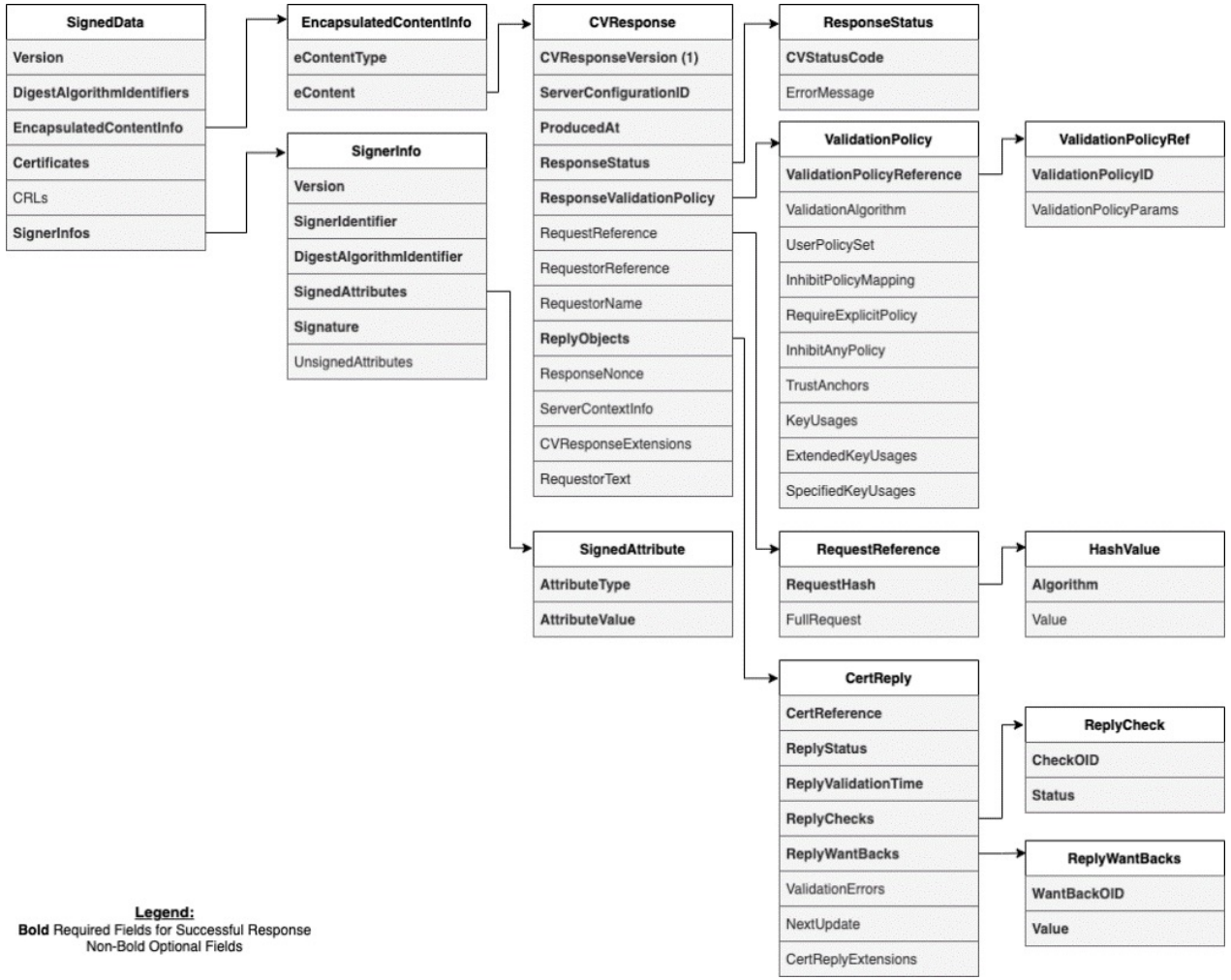
SCVP Request

- SCVP Request (CVRequest) has only a few required fields with lots of configurable values
  - Propose to define ValidationExtension Types for the fields in Green
  - Blue Fields will only be set by the Server
- SCVP Request will always contain a single CertificateReference with the X.509v3 Certificate of the (D)TLS Server
- If no ValidationExtensions are specified, (D)TLS Server will default required fields
  - ValidationPolicy = id-svp-defaultValPolicy
  - All optional fields will be left blank
- To minimize bandwidth usage, it is recommended that (D)TLS Clients minimize ValidationExtension used

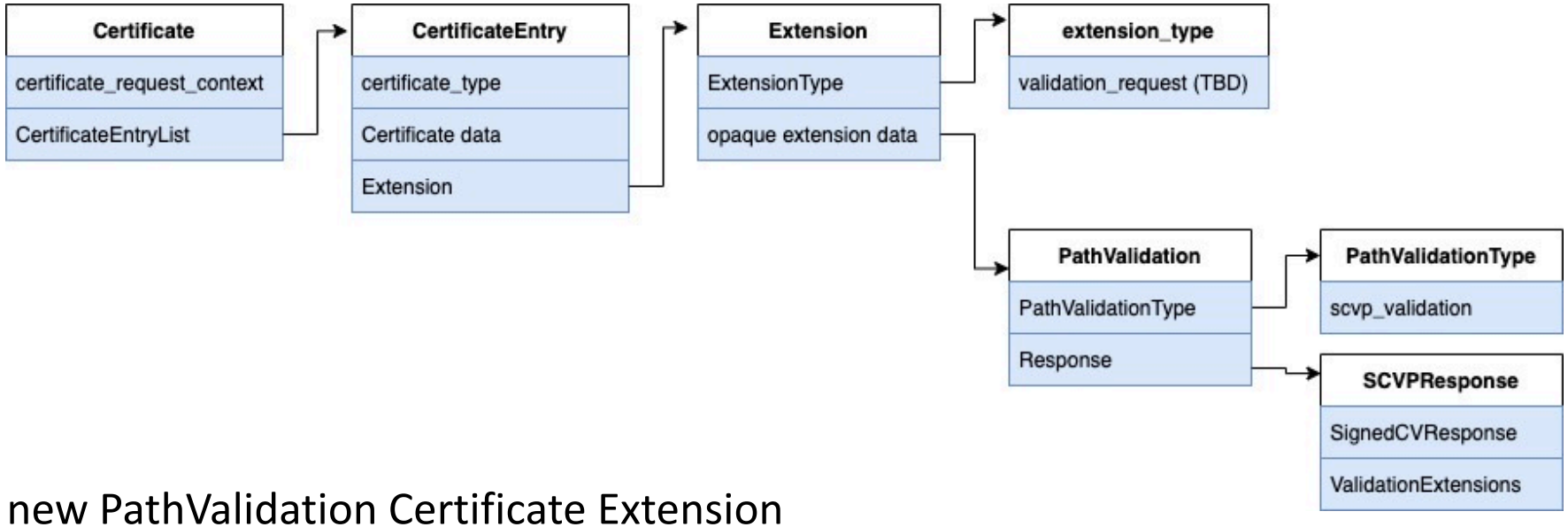


SCVP Response

- SCVP Response will be signed by the Client specified SCVP Responder
- Digital Signature on the SCVP Response is used to ensure the Response is provided by the trusted SCVP Responder and has not been altered
- Size of SCVP Response will vary based on the SCVP Request settings
  - By keeping SCVP Request options to a minimum SCVP Response can be small



PathValidation Certificate Extension



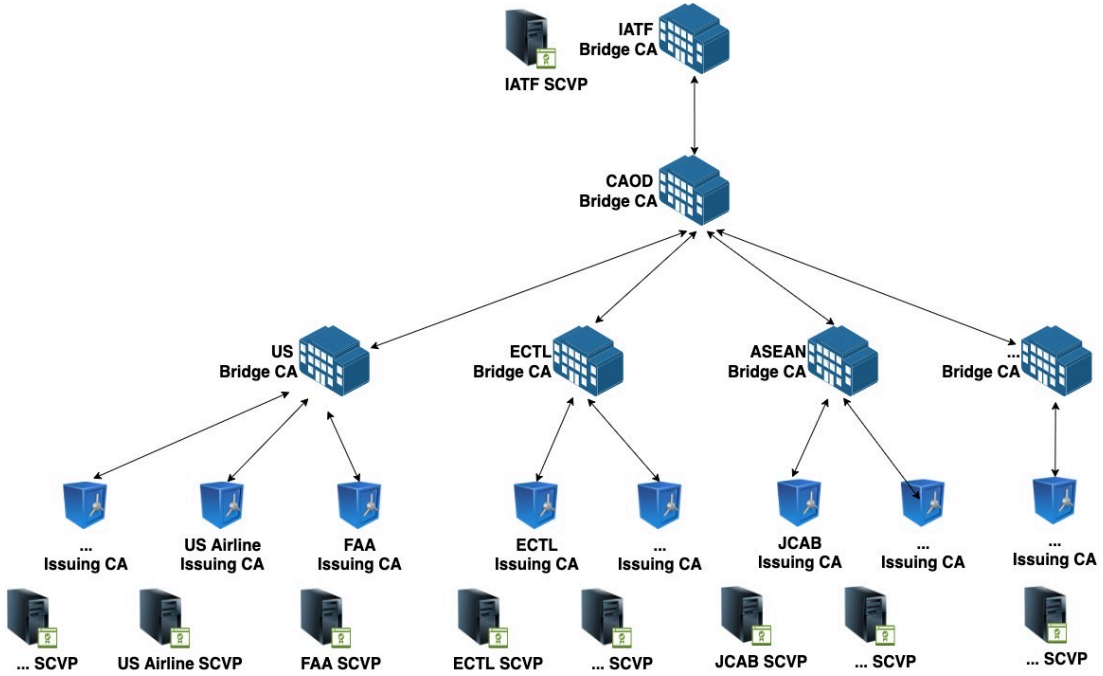
- Propose new PathValidation Certificate Extension
- Like PathValidationRequest, PathValidation type is defined for scvp_validation and allows expansion to future types
- For type scvp_validation, the Response contains:
  - SignedCVResponse: a Single DER-encoded SCVP Response (CVResponse defined in RFC 5055), signed by the Client specified SCVP Responder
  - ValidationExtensions: list of validation extensions from the SCVPValidationRequest that were used in the CVRequest to indicate to the TLS Client which validation extensions were honored

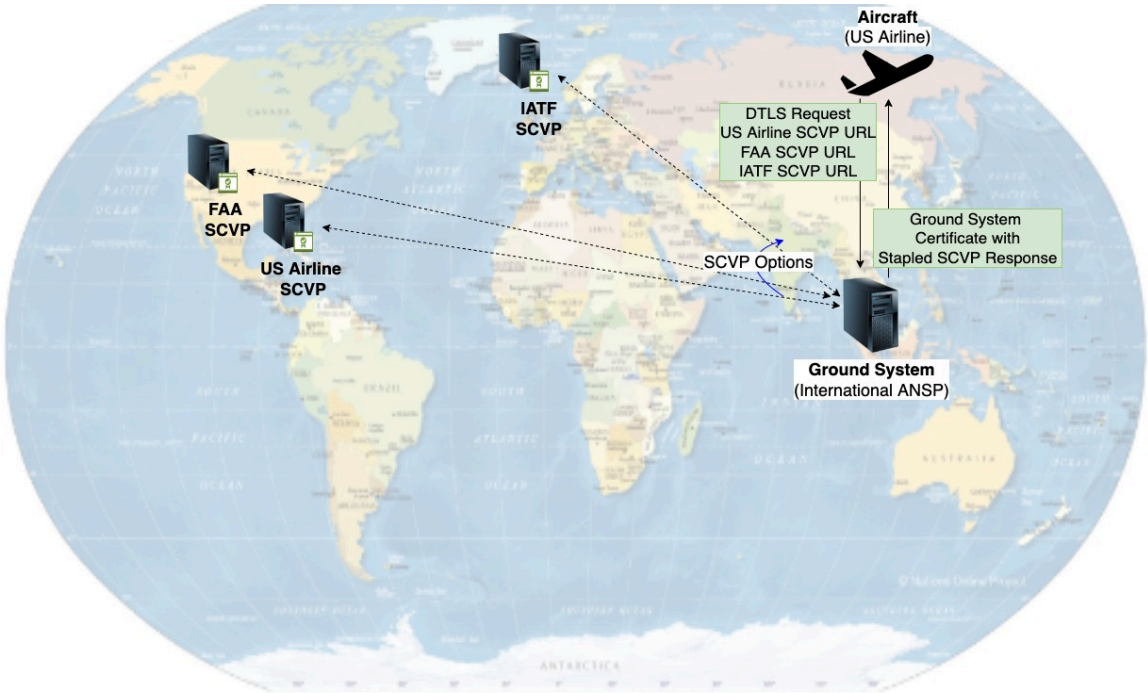
SCVP Validation Request Extension

- 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 (D)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
- Propose definition of new (D)TLS extensions for SCVP Validation Request

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