Delegated Certificate Validation for Federated Space Public Key Infrastructure

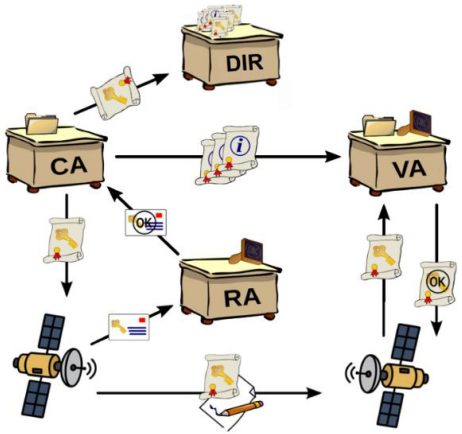
Alin-Petru Roșu
(Delft University of Technology)

Oana-Alexandra Graur
(European Space Agency)

Security for Space Systems (3S) 2025
ESTEC, The Netherlands
November 05, 2025

Context

- Space missions increasingly require **international collaboration** (e.g., Artemis)
- ECSS & CCSDS key management limited to **symmetric cryptography** which **lacks scalability**
- **PKI** deployment in space is challenging; **federated PKI**, even more
- **Certificate validation remains an open problem** under limited connectivity and multi-agency trust models

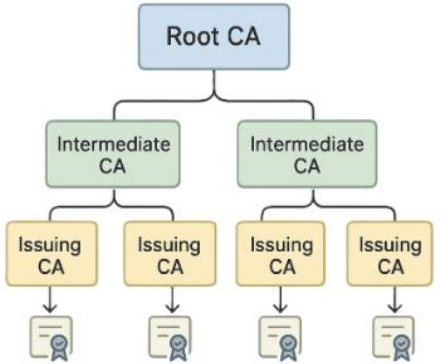


Single CA PKI. Adapted from [1] under CC BY-SA 3.0

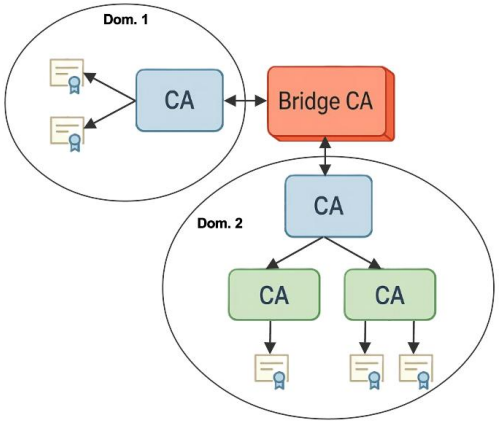
https://commons.wikimedia.org/wiki/File:Public-Key-Infrastructure.svg [1]

Problem Statement

- Path construction is challenged by intermittent connectivity and limited bandwidth
- Classical revocation mechanisms (CRLs, OCSP) are hard to adopt in space
- Potential lack of reliable time source (validity check)
- Validation in federated PKIs requires policy mappings and constraint extensions processing
- Post-Quantum Cryptography (PQC) further complicates validation



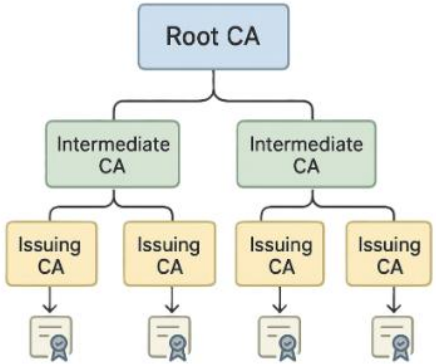
Layered PKI Architecture



Bridge PKI Model

Mitigation

- Delegated Path Validation (**DPV**) and Discovery (**DPD**) – RFC 3379
- Protocol to achieve DPV/DPD: **Server-Based Certificate Validation Protocol (SCVP)** – RFC 5055
- *"applications are burdened with the overhead of constructing and validating the certification paths"*
- *"delegating path discovery and/or validation processing to a server, and to **allow central administration of validation policies within an organization**"*
- SCVP servers can be trusted or not for full validation



Layered PKI Architecture

SCVP and Validation Policies

- **Request-response model** under a specified **validation policy:**
  - Defines the **list of trust anchors**
  - Configures the sources and type of **revocation information**
  - Check if certificates strictly adhere to predefined profiles (e.g., specific extensions and algorithm sets)
- High configurability (e.g., policies can be parametrized, clients can specify time for validation or trust server's time)

SCVP Security Considerations

- **Trust scope:** DPV clients can trust different servers
- **Integrity protection:** Requests and responses protected with digital signatures or MACs
- **Trust implication:** Trusting a server is equivalent to trusting local validation software.
- **Security requirement:** An SCVP server must be secured at least as strongly as its trusted anchors
- **No confidentiality:** SCVP does not provide encryption
- **Replay protection:** Nonce extensions prevent replay attacks

Advantages

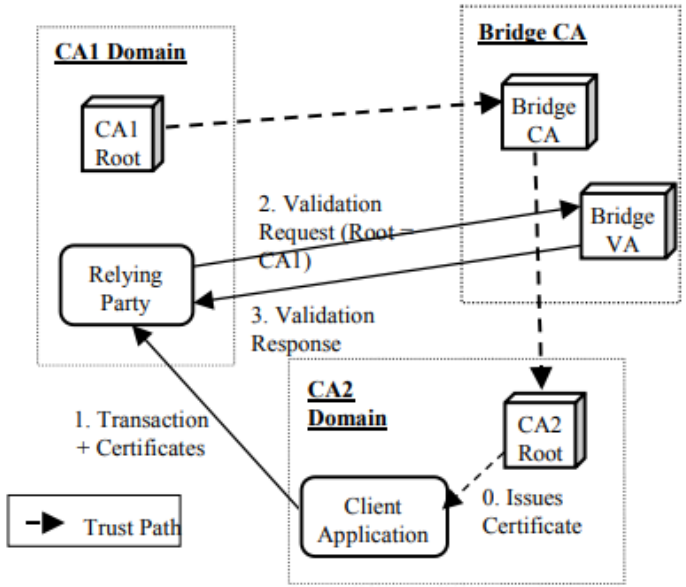
- Relayed requests
- Simplified software on constrained assets
- Centralized policy management (auditability)
- Lowers computational and network load on client side
- Stapling-like mechanisms are possible (but not standard)

Disadvantages

- Complex server implementation and management
- Complex PKI architecture
- Single point of failure
- Limited commercial adoption (*SCVP providers:* HID, Axway, Ascertia ADSS, Trusted Hub SCVP Appliance)

Proposal

- PoC SCVP implementation
- For this demonstration, the server will be deployed on the ground and compare with local validation
- SCVP can be deployed as part of a Bridge VA
- Future architectures can explore in-orbit SCVP relays



Architecture with a Bridge VA

https://csrc.nist.rip/archive/pki-twg/y2002/presentations/twg-02-08.pdf

THANK YOU!

Questions?

Contact