Certificate lifecycle management

Discussing a Potential IHE-ITI Profile Proposal

David Wikler, IHE-RO TC vendor co-chair, System Engineer at IBA
Krisha Howell, IHE-RO PC user co-chair, MD at Michigan Healthcare Professionals
Rex Cardan, RTSEC user co-chair, Medical Physicist at UAB Medicine

RTSEC Background

- Mission: To produce **position statements** on technology that enables **interoperability** of **RT systems**, with an **initial focus on cybersecurity**.

AAPM Newsletter. March/April 2026; 51(2):53–54

- Goal: Enable **secure DICOM communication** (DICOM TLS for DIMSE or HTTPS for DICOMweb) between RT systems from multiple vendors.
- Mean: Gather domain and security experts

RTSEC/IHE-RO Problem Statement

- Secure communication is standardized
  - DICOM Part 15 TLS Profile Secure Transport Connection Profiles
  - IHE-ITI ATNA
- Adoption remains very limited
- The barrier is Certificates Lifecycle Management
  - Clinics have diverse or non-existent Public Key Infrastructures (PKIs)
  - Certificates Enrollment and Renewal is manual
  - Certificate expiration jeopardizes continuity of care

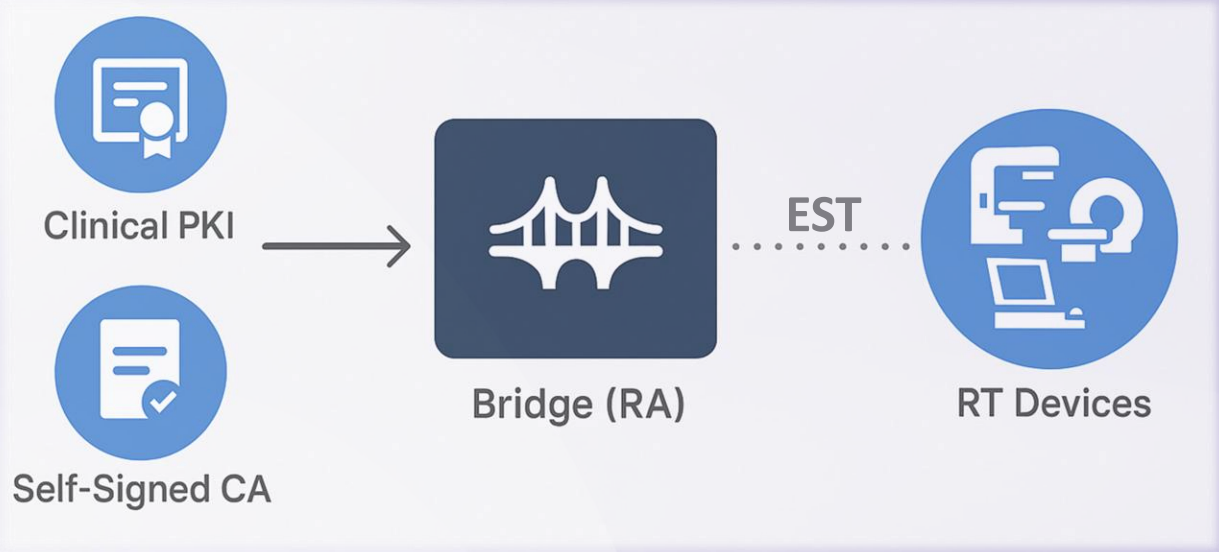
Current State

- **DICOM Part 15** TLS Secure Transport Connection require **X.509 certificates** with no further specifications.
- **IHE-ITI ATNA** favors **locally managed trust** (e.g., hospital CA) over public browser CAs with no further specifications.
- Existing protocols support **certificate lifecycle management**:
  - **EST (RFC 7030)** – IETF standard, limited deployment in enterprise PKI
  - **ACME (RFC 8555)** – widely adopted in web / cloud ecosystem)
  - **SCEP (RFC 8894)** – widely implemented in enterprise PKI, legacy

Gap

- Certificate management is **not profiled in IHE**
  - historically considered a **local infrastructure concern**
- No defined approach on how to:
  - Establish device identity
  - Obtain, renew, define lifetime, revoke certificates
  - Integrate with local PKI environments
- Result:
  - Poor adoption
  - reliance on **manual provisioning**
  - **repeated integration effort** across vendors for each deployment

Explored Solution: An EST-based RA



Concept:
A **bridge** that acts as a **Registration Authority (RA)** for a **clinical PKI**, or provides a **default self-signed CA** for simpler deployments.

- Standard: Utilizes the Enrollment over Secure Transport (**EST**) protocol, an **Internet Standard** from the IETF (RFC 7030).
- Benefit: Simplifies certificate management (enrollment, renewal) for RT devices, promoting interoperability and security.

OR.NET and IHE-DEV

Interoperability for Operating Room, ICU devices

- Develops **SDPi** (Service-oriented Device Point-of-care Interoperability) profiles **based on SDC** standards (developed by **IEEE 11073 PoCD WG**)
- Collaborates with **HL7 Devices** WG on SDC+FHIR integration within **FHIR/IHE Gemini** Project

- **Same Gap Identified**
  - Similar working group: Certificate infrastructure and security
    - develops a process for issuing and signing cryptographic certificates
      - See also Security Review of IEEE 11073 SDC Medical Device Standards · Alexander Dippel
  - Same EST protocol proposed
  - Different Authentication Mode (manufacturer certificate)
  - Wish for integration in IHE Profile

Opportunity for Alignment

- RTSEC and OR.NET are actively working in this area
  - RTSEC built a demonstrator
  - OR.NET preparing a specification draft
  - Both RTSEC and OR.NET independently converged on EST protocol
- discussion already spans RO, DEV, ITI and DICOM, HL7, SDC
- opportunity to avoid parallel specifications
- reusable profile could benefit multiple domain

Why ITI ?

- Problem extends beyond domains
  - Certificate lifecycle management is infrastructure, not modality-specific
- Applies to:
  - DICOM over TLS
  - DICOMweb over HTTPS
  - HL7 FHIR over HTTPS
  - HL7 v2 over MLLP/TLS
  - IEEE 11073 SDC over HTTP
- Potential for reuse across IHE domains