

TeleTrust-EBCA "PKI-Workshop" 2026

Berlin, 08.10.2026

**Automatisierte richtliniengeprüfte Zertifikatsverwaltung
für isolierte Produktions- und kritische Infrastruktur
unter Verwendung des EST-Protokolls**

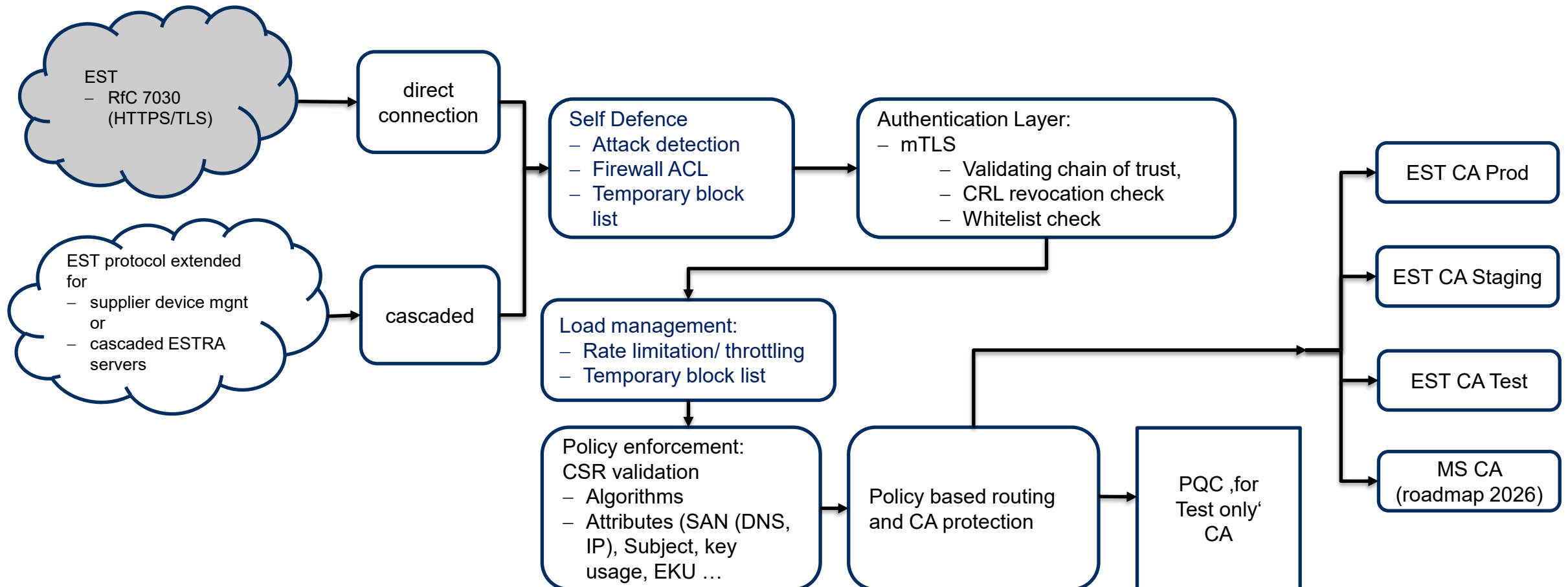
Harald Kaiblinger, Estra-Security GmbH

Holger Siegel, HST GmbH

- ESTRA
- EST – Warum und wie funktioniert es
 - SimpleEnrol und SimpleReEnrol
 - cacerts
- Geräte mit Zertifikaten ausstatten
- Umfeld
- EST – Lessons learned

- EST – das Protokoll + RA – Registration Authority
= ESTRA
- Vorteile
 - Verwendbar in „Kritis“ Umgebungen
 - Client-less
 - Algorithmus agnostisch
 - Open Source Plattform
 - PQC Ready

ESTRA Overview



EST

SimpleEnrol und SimpleReEnrol

- **/simpleenroll: Zertifikat beantragen**

- Der Client erzeugt ein Schlüsselpaar und einen PKCS#10-CSR.
- Er sendet POST /.well-known/est/simpleenroll mit Content-Type: application/pkcs10 und dem CSR base64-codiert im Body.
- Der Server authentifiziert und autorisiert den Client, die CA stellt das Zertifikat aus.
- Die Antwort enthält das Zertifikat.

- **Authentifizierung des Clients** (mindestens eine davon):

- TLS-Client-Zertifikat, zum Beispiel ein Hersteller-Zertifikat (IDevID) oder ein früher ausgestelltes Zertifikat

EST

cacerts

- /cacerts: CA-Zertifikate abholen

- Der Client holt sich hier die Vertrauensanker, also das CA-Zertifikat und gegebenenfalls die Kette.
- **Request:** GET /.well-known/est/cacerts, ohne Body und ohne Client-Authentifizierung.
- **Response:** 200 OK mit Content-Type: application/pkcs7-mime. Der Body ist eine base64-codierte PKCS#7-Struktur vom Typ "certs-only", also ein SignedData ohne Signatur, das nur Zertifikate enthält.
- **Inhalt:** das aktuelle CA-Zertifikat, eventuelle Zwischen-CAs und bei einem Root-Wechsel zusätzlich die Rollover-Zertifikate (OldWithOld, OldWithNew, NewWithOld).
- Beim allerersten Aufruf kann der Client das TLS-Zertifikat des Servers oft noch nicht prüfen, weil ihm der Vertrauensanker fehlt. Dafür sieht der RFC vor:
- **Implizite Trust Anchors:** Der Client prüft den Server gegen vorinstallierte Roots, zum Beispiel die des Herstellers.

- Geräte werden mit einer digitalen Identität vom Hersteller geliefert (Herstellerzertifikat).
 - Im Lieferschein der Geräte sind die Identitäten aufgelistet, die als ‚Whitelist‘ genutzt werden.
 - Die Geräte erhalten ‚Arbeitszertifikate‘ aus der ‚eigenen‘ PKI, die zur Authentifizierung und Verschlüsselung der Übertragung genutzt werden.
-
- ➔ Nur ‚eigene Geräte‘ dürfen sich authentifizieren.
 - ➔ Services dürfen nur der ‚eigenen PKI‘ vertrauen.
 - ➔ Die Identität des Gerätes kann über den gesamten LifeCycle sichergestellt werden.

EST-Protokoll (RFC 7030) Aufrufe:

Message type (per operation)	Request media type Response media type(s) Source(s) of types	Request section(s) Response section
Distribution of CA Certificates /cacerts	N/A application/pkcs7-mime [RFC5751]	Section 4.1 Section 4.1.1
Client Certificate Request Functions /simpleenroll /simplereenroll	application/pkcs10 application/pkcs7-mime [RFC5967] [RFC5751]	Sections 4.2/4.2.1 Section 4.2.2
Full CMC /fullcmc	application/pkcs7-mime application/pkcs7-mime [RFC5751]	Section 4.3.1 Section 4.3.2
Server-Side Key Generation /serverkeygen	application/pkcs10 multipart/mixed (application/pkcs7-mime & application/pkcs8) [RFC5967] [RFC5751] [RFC5958]	Section 4.4.1 Section 4.4.2
CSR Attributes /csrattrs	N/A application/csrattrs (This document)	Section 4.5.1 Section 4.5.2

CA-Verwaltung

und

Zertifikate verteilen

Message type (per operation)	Request media type Response media type(s) Source(s) of types	Request section(s) Response section
Distribution of CA Certificates /cacerts	N/A application/pkcs7-mime [RFC5751]	Section 4.1 Section 4.1.1
Client Certificate Request Functions /simpleenroll /simplereenroll	application/pkcs10 application/pkcs7-mime [RFC5967] [RFC5751]	Sections 4.2 /4.2.1 Section 4.2.2

- Kritische Infrastruktur
- Energie - Größter privater Energieversorger Europas! 
- Aufgabe: Digitalisierung deutscher Stromanschlüsse

In Deutschland gibt es rund 52,5 bis 52,9 Millionen Marktlösungen (Zählpunkte) bzw. Stromanschlüsse für Letztverbraucher

Der **Marktanteil der E.ON-Netzgesellschaften** am deutschen Stromverteilnetz liegt bei rund 32 Prozent. Damit betreiben die regionalen Tochtergesellschaften von E.ON (wie beispielsweise Westnetz, Bayernwerk Netz, Avacon oder Mitnetz) etwa **ein Drittel** des gesamten deutschen Stromnetzes.

Etwa **50 Prozent** aller deutschen Photovoltaikanlagen und rund **70 Prozent** aller Onshore-Windkraftanlagen sind an das Netz von E.ON-Tochtergesellschaften angeschlossen. Quelle: E.ON
- HST GmbH und ESTRA-Security GmbH

Systemintegratoren für automatisierte Zertifikatsverwaltung und -verteilung

- Erst-Rollout – SimpleEnrol
 - Abstimmung über CSR mit Herstellern erforderlich.
 - Einfache Probleme oder wenige bis keine Probleme!
- Zertifikatserneuerung - SimpleReEnrol
 - Vom ursprünglichen Ansatz eines reinen Re-Keying, musste abgewichen werden, da neue Einsatzfälle auch Erweiterungen an den Attributen benötigen. Zusätzliche Attribute und deren Validierung sollten auch beim Wiederausstellen eines Zertifikates unterstützt werden.

- Cacerts – Aktualisieren der vertrauenswürdigen CA-Zertifikate
 - Der Abruf ist einfach
 - Probleme ergaben sich die sich über den Lebenszyklus der Geräte ergebenden Änderungen und Updates der CA-Zertifikate. Insbesondere Cross-Signing und ‚Löschen‘ bedarf eines guten Prozesses, insbesondere in Verbindung mit ‚Secure-Elements‘, TPM oder Smartcard.

- Zurzeit sind bzw. werden mit 22 Herstellern Integrationen von diversen Geräten durchgeführt

Zusammenfassend:

DAS EST-PROTOKOLL eignet sich für diese Aufgaben sehr gut und ist EINE HERVORRAGENDE WAHL!

Danke für Ihre Aufmerksamkeit

Harald Kaiblinger

- Estra-Security GmbH
Stipcakgasse 9-17/27
1230 Wien
- www.estra-security.eu
- Mobil: +436706084202
- h.kaiblinger@estra-security.eu

Holger Siegel

- HST GmbH Technische Entwicklungen
Zweigstelle Wuppertal
Oberbergische Str 56
D-42285 Wuppertal
- Tel.: +49 202 3934616
Mobil: +49 170 7942828
holger.siegel@hsti.de