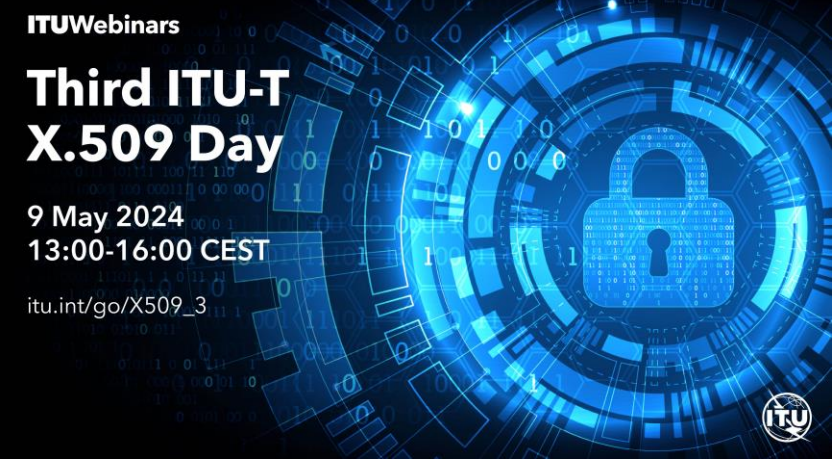


V1.1

SESSION 1: Latest advances in X.509 from organizations and industries across the world

Today's emerging X.509 implementations

Anthony M. Rutkowski, ETSI-ITU-T liaison,
mailto:tony.rutkowski@cisecurity.org

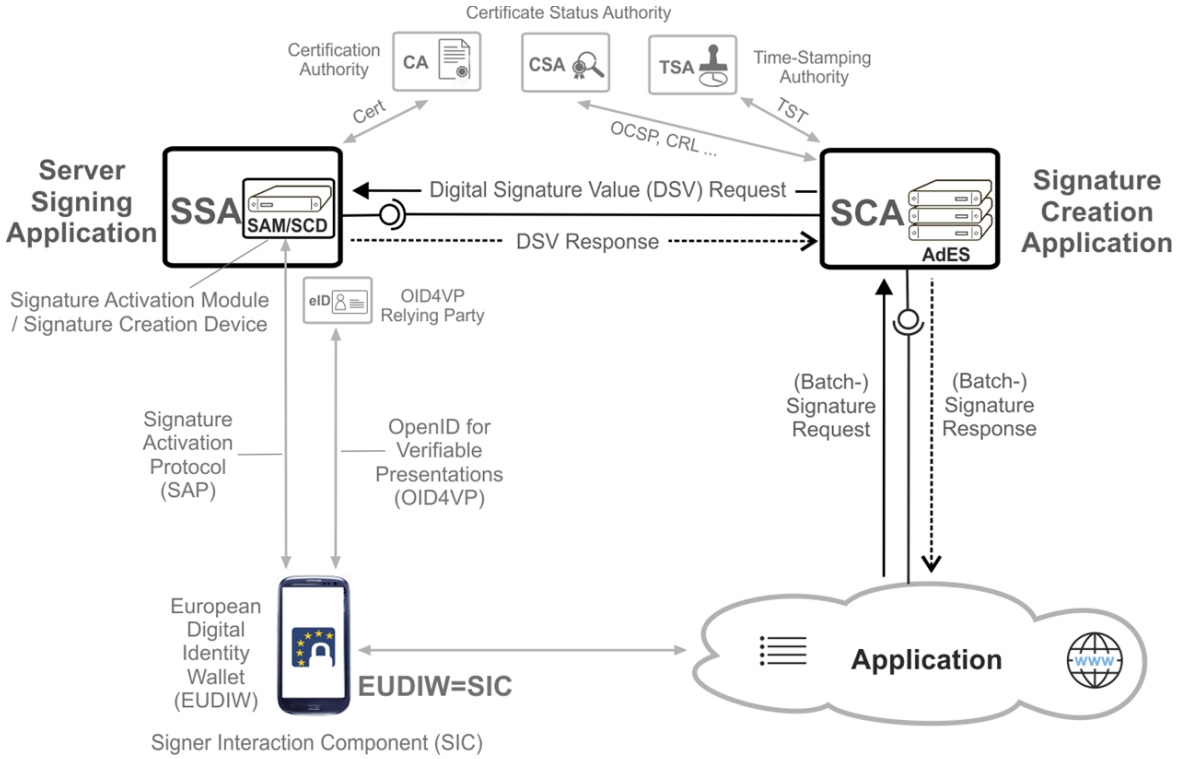
X.509 implementation metrics

- Requirement articulated by Paul Baran at RAND in Aug 1964
- Dedicated industry standards bodies arose – ETSI TC ESI, CA/B Forum
- 42,102 patents
- 42,100 scholarly articles
- 811 finds for 3GPP
- 4,840 finds for ITU
- 2,480 finds for ETSI
- 16,700 finds for IETF
- 19,900 finds for .gov
- 34,900 finds for Google
- 35,100 finds for Microsoft
- 24,900 finds for Amazon
- 11,700 finds for Cisco
- 1971 CVE X.509 related vulnerability finds

ETSI Electronic Signatures and Infrastructures (TC ESI)

- Designated European Standards Organisation (ESO)
- All standards and publications are freely available at permanent URIs and well versioned
- CABF Auditor status TC ESI standards
- EU eIDAS framework for European Digital Identity and Digital Identity Wallet (EUDIW)
- TS 119 412, Electronic Signatures and Infrastructures (ESI); Certificate Profiles, Jul 2020
- EN 319 411, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates
- TS 119 102, Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures, Aug 2018
- Workshop on EU Digital Identity Framework Standards, 10-12 Sep 2024, Sophia Antipolis
- Interoperability Plugtests held Oct-Dec 2023 included 190 participants from 121 organisations from 38 countries for five digital signature formats XML (XAdES), PDF (PAdES), CMS (CAdES), Container (ASiC), and Java (JAdES)

A revision to EU Regulation 910/2014 on electronic identities, authentication and signatures (eIDAS) is expected to be published in the Official Journal of the European Union in spring 2024. This revision establishes an ambitious European Digital Identity Framework with digital identity wallets and a number of new trust services.



Requirements of Trust Service Providers

- In Sep 2023, ETSI published a new standard on “Requirements for trust service providers issuing publicly trusted S/MIME certificates” (ETSI TS 119 411-6) helping Trust Service Providers comply with new standards for S/MIME certificates that are enforced since 1 September 2023
- Since the 1st of September 2023, all TSPs issuing digital certificates used for S/MIME that are publicly trusted in certain operating systems and root certificate programs must comply with the S/MIME Baseline Requirements published by the CA/Browser Forum
- The new ETSI standard
  - Assists Trust Service Providers in asserting their compliance, when required
  - Will enable the same public key certificate used for signing electronic mail accepted by major IT solution providers (e.g., Microsoft, Apple, Google) to be also recognized as meeting the EU requirements for electronic signatures, issued to individual persons, and electronic seals, issued to organizations
  - Supports the EU regulation for electronic identities, authentication, and signatures (eIDAS – Regulation (EU) 910/2014) and builds on the policy requirements for Trust Service Providers (TSPs), the ETSI EN 319 411 series of standards used for eIDAS audits

EU Digital Identity Wallet and beyond

- The eIDAS regulation recognises the following types of trust service providers:
  - Certification Authorities issuing certificates for digital signatures supporting electronic signatures and seals (see ETSI page on digital signatures)
  - Certification Authorities issuing certificates to support website authentication, aligned with the requirements of the CA/Browser Forum as recognised by all the major Web Browser Vendors
  - Time-stamping authorities providing proof of existence of a data object (including signed documents) at a given time
  - Providers of services for the validation and preservation of signed data
  - Providers of services for registered electronic delivery including registered electronic mail
- This has been extended in eIDAS 2 with the definition of a new form of national electronic identifier, equivalent to national identity card, called the EU Digital Identity Wallet
- eIDAS also supports the provision of trust services for:
  - Electronic Attestation of Attributes relating attributes and credentials to identified persons
  - Creation of electronic signatures and seals using removte signing devices held in the cloud, as opposed to, for example, locally held smart card
  - Electronic Archiving
  - Electronic Ledgers
- ETSI is developing standards for interfacing to the EU Digital Identity Wallet and support of the other new trust services.

CA/Browser Forum

Minutes of F2F 61 Meeting, Feb 2024

- Building Trust, Empowering the Digital Economy: eIDAS Trust Services (F2F 60)
- Mozilla Root Program Update
- Google Root Program Update
- Apple Root Program Update
- Microsoft Root Program Update
- Common CA Database Update
- ETSI Update
- Accredited Conformity Assessment Bodies Council Update
- WebTrust Update
- Proof-of-Concept for Baseline Requirement of Baseline Requirements

Working Groups: Server Cert, Code Signing Cert, SMIME Cert, Validation + network security

Note by Stephen Davidson

- Ballot SC-067 before the CA /Browser Forum (CABF) seeks to require CAs to implement Multi-Perspective Issuance Corroboration (or MPIC) in the way they conduct domain validation and CAA checks
- Will require CAs to perform their checking using multiple Network Perspectives, making it more difficult for adversaries to launch attacks (such as DNS cache poisoning and BGP hijacking) on some of the methods defined in the TLS Baseline Requirements
- The technique has been demonstrated at scale in implementations including by Let's Encrypt and Google Trust Services
- If successful, the ballot will presumably be carried into other CABF standards, such as the S/MIME Baseline Requirements
- As this will require significant investment in validation infrastructure by CAs, which may be a challenge for smaller issuers including European Qualified TSPs, the ballot includes a phased implementation schedule in 2024-2026

- Created a Definitions and Glossary working group (DGWG)
- 11 April 2024 Telecon meeting minutes

Toward more trusted X.509 implementations

- USDOD Instruction (NSA/CISA)
- UK NCSC Guidance
- Google Certificate Authority Service
- Let's Encrypt New Issuance Chains
- AWS Operation Best Practices for NCSC Cloud
- Apple PKI
- Microsoft Build
- Huawei Cloud

Ref: IEEE, A Survey on X.509 Public-Key Infrastructure, Certificate Revocation, and Their Modern Implementation on Blockchain and Ledger Technologies