Dimitris Zacharopoulos

GUnet/HARICA, CA/B Forum Chair

Public Trust, CA/Browser Forum and PKI Industry Update

HARICA

CAB CA/BROWSER FORUM

A few words about HARICA

- HARICA (www.harica.gr), established in 2006, supported/funded by GUnet, a non-profit civil company
- Offers a variety of Publicly-Trusted Services
  - Certificates (eSignature, eSeal, QWAC, SSL/TLS, Code Signing, S/MIME, Client Authentication)
  - Qualified and non-Qualified Time-Stamps
  - Remote QSCD
  - …expanding to other Qualified Trust Services

What is the CA/Browser Forum?

- Global “Standards Defining Organization” (SDO)
- Collaboration of Certificate Issuers and Certificate Consumers
- SSL/TLS, Code Signing, S/MIME
- Produces “Guidelines” incorporated into audit schemes:
  - WebTrust
  - ETSI
- Guidelines are licensed under [Creative Commons Attribution 4.0]

CA/B Forum Governance

- CA/B Forum Plenary → https://cabforum.org/
  - Server Certificate Working Group
    - Validation Subcommittee
  - Code Signing Certificate Working Group
  - S/MIME Certificate Working Group
  - Network Security Working Group
- More Working Groups can be created

CAB CA/BROWSER FORUM

Server Certificate WG

- Update since September 2021
  - SC50: Remove the requirements from BRs section 4.1.1
  - SC53: OCSP SHA-1 sunset
  - SC51: Reduce and Clarify Log and Records Archival Retention Requirements
  - SC54: Onion Cleanup
  - SC58: Require distributionPoint in sharded CRLs
- Ballots under discussion
  - SC61: CRL Reason Codes
  - SC62: Certificate Profiles alignment
- Draft Ballots under consideration
  - Debian Weak keys
  - Make OCSP optional for Subscriber Certificates

Code Signing WG

- "Baseline Requirements for Code-Signing Certificate" v3.2 (2022-10-28)
- CSC-13: Update to Subscriber Private Key Protection Requirements
  - ALL Code Signing Certificates (OV/IV) **issued on or after 2022-11-15** need to be associated with a Key-Pair generated in a device that meets or exceeds FIPS 140-2 (level2).
- CSC-14: Convert Code Signing Baseline Requirements to RFC 3647
- CSC-15: Summer 2022 clean-up
- CSC-17: Subscriber Private Key Extension
  - postpones dates of CSC-13 to **2023-06-01**
- Next steps
  - Remote signing services
  - Time-stamping Authority issues
  - Import references from TLS Baseline Requirements

CAB CA/BROWSER FORUM

S/MIME Certificate WG

- Official S/MIME Baseline Requirements version 1.0.0
- Effective date **September 1, 2023**
- WebTrust Task Force and is already developing audit standards against SMBRs
- ETSI is planning a new standard for S/MIME
- Certificate Consumers are preparing updates to their Root Programs for S/MIME

Network Security WG

- NetSec Charter
- Prepare work for other WGs to include into their respective Guidelines

- Next steps:
  - Cloud Services Sub-Group Risk Assessment based on Threat Modelling (risk-based approach)
  - Air Gap Systems

CA/BROWSER FORUM

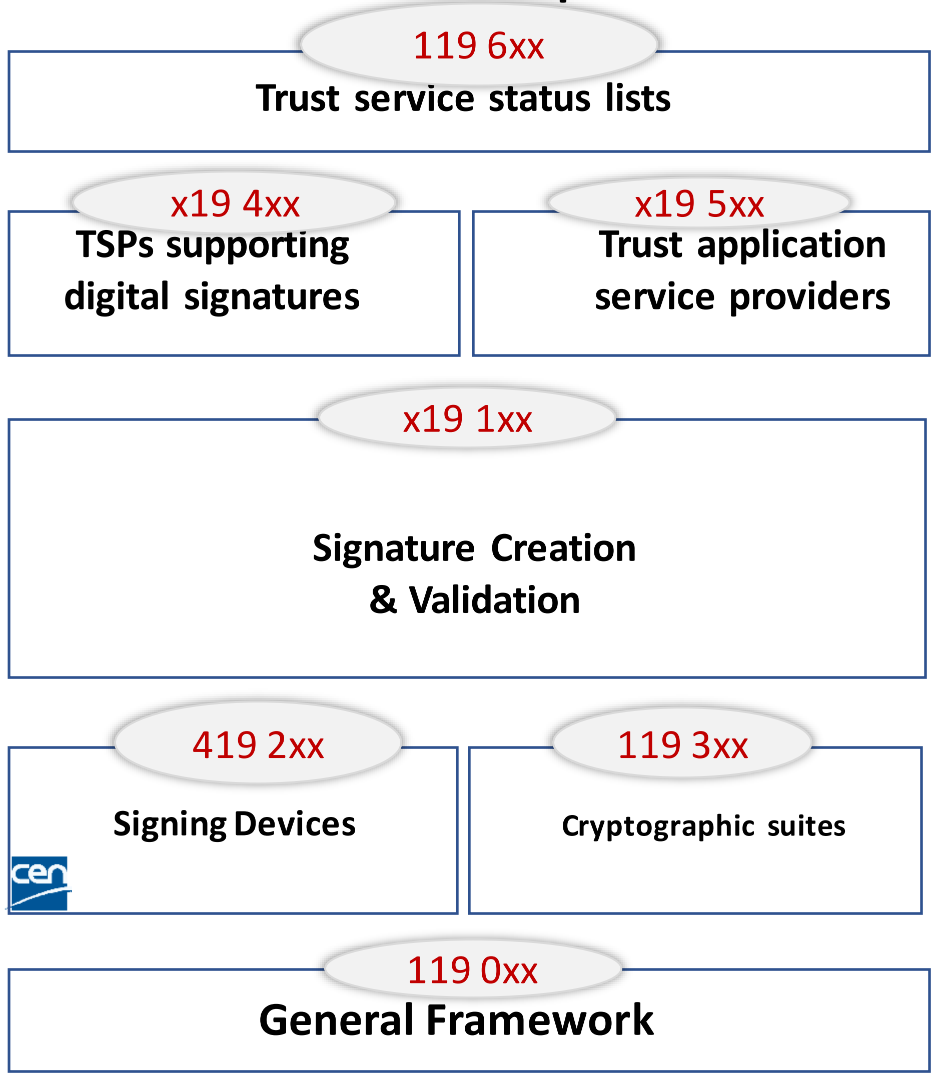
Other resources

- Meeting minutes (including F2F) https://cabforum.org/category/minutes/
- Mailing-list archives
  - CABF Plenary public list https://cabforum.org/pipermail/public/
  - Server Certificate WG public list https://cabforum.org/pipermail/servercert-wg/
    - Validation Subcommittee public list https://cabforum.org/pipermail/validation/
  - Code Signing Certificate WG public list https://cabforum.org/pipermail/cscwg-public/
  - S/MIME Certificate WG public list https://cabforum.org/pipermail/smcwg-public/
  - Network Security WG public list https://cabforum.org/pipermail/netsec/
- How to join the CA/B Forum
  - https://cabforum.org/information-for-potential-members

ETSI - ESI

- ETSI standards are publicly available for consultation
- Information on available standards and current activities
- ETSI standards are freely available for download

ETSI & CEN Standards supporting eIDAS the overall picture



119 6xx
Trust service status lists

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

x19 1xx
Signature Creation & Validation

419 2xx
Signing Devices

119 3xx
Cryptographic suites

119 0xx
General Framework

- Trusted list ✓
- Using & interpreting trusted list ✓
- Validation policy using trusted list ✓

Trust services for:
- Issuing certificates ✓*
- Time Stamping ✓
- Signature creation services ✓ *
- Signature validation services ✓
- Identity proofing (new) ✓
- Open Banking ✓

Trust services for:
- Registered eDelivery / eMail ✓*
- Long term preservation ✓

- AdES creation & validation
  - Part 1: procedures ✓*
  - Part 2: signature validation report ✓*

Formats:
- XAdES (XML) ✓*
- CAdES (CMS) ✓*
- PAdES (PDF) ✓
- ASiC (containers) ✓
- JAdES (JSON) ✓
- CB-AdES (CBOR) (new)

CC Protection Profiles
- QSCD - Smart Cards ✓
- HSM used as QSCD ✓
- HSM used by TSPs ✓
- Remote QSCD ✓

- Signature suites ✓
  - Hash
  - Asymmetric crypto
  - Key generation
  - Lifetime
- Schema for algorithm catalogues (new) ✓

- Standards framework ✓ *
- Common definitions ✓
- Guides ✓

✓ Completed
* Update in progress
(new) New

HARICA

Identity Proofing

- TS 119 461: Policy and security requirements for trust service components providing identity proofing of trust service subjects
  - Applicable to:
    - natural and legal persons
    - local and remote registration
    - range of EU trust services: certificate authorities, registered email, electronic IDs, “know your customer”
  - Publicly available
  - Working with other bodies to make this generally applicable

Trust Services Policy Requirements updates

- EN 319 401/411-1/411-2
- Change requests under discussion:
  - EN 319 401 -Update to align with new ISO 27002 and new NIS2 Directive (EU) 2022/2555
  - EN 319 411 – Various detailed updates including alignment with latest CA/B Forum documents and recommended use of TS 119 461
  - EN 319 412-1 & 2 & 4 – Proposals for detailed changes to certificate profiles

Guidelines for the coexistence of web browser and EU trust controls

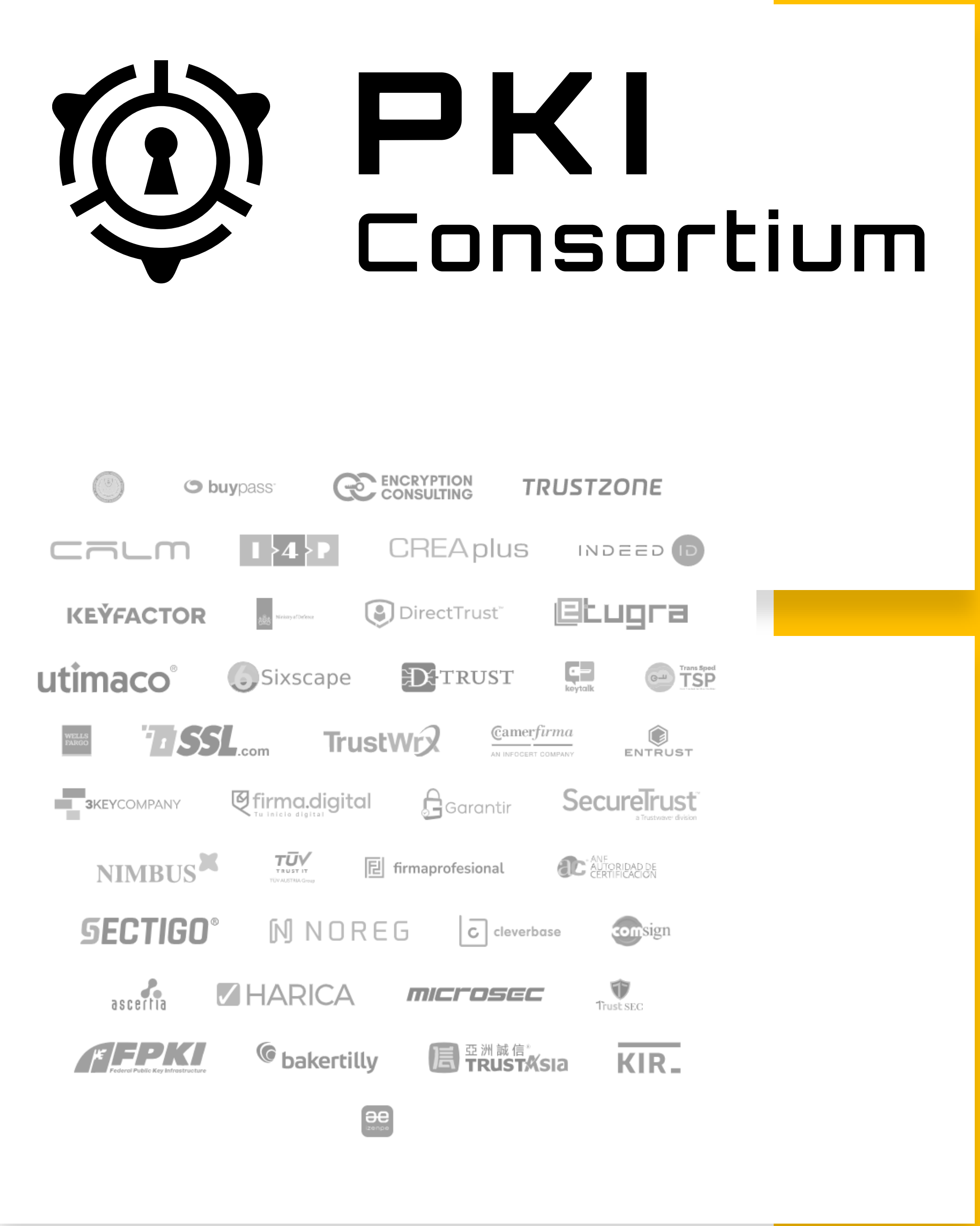
- TR 119 411-5
  - available at: https://www.etsi.org/standards-search#search=TR119411-5
- Certificate format:
  - Common certificate format following EN 319 412-4 and CA/B BRs
- Issued:
  - Based on EN 319 411-x and CA/B BRs
  - Browsers: Browser root store policy & EN 319 403-1 + TS 119 403-2 Audits
  - EU: EN 319 411-2 policies QNCP-w/QEVCP-w & EN 319 403-1 + TS 110 403-3 Audits
- Validated:
  - Browser: against browser root store
  - EU: Trusted lists as described in ETSI TS 119 615
- Display:
  - EU Trust Mark & EU Identity displayed if it passes both Browser and EU validation
  - Browser may continue to display website if it just passes Browser validation

ETSI working with CEN on eIDAS 2.0

- European Digital Identity Wallets (CEN)
  - securely request, obtain, store, select, combine, share legal person identification data and attestation to authenticate online and offline
- Qualified Trust Services (ETSI)
  - Considered “essential services” and must conform to the NIS2 Directive
- Qualified Website Authentication Certificates (ETSI)
  - shall be recognized by web-browsers which shall ensure that the identity data provided using any of the methods is displayed in a user friendly manner
- Qualified Electronic Ledgers (ETSI)
- Attestation of Attributes (ETSI)
- Possible Standards for eIDAS 2.0 (CEN & ETSI)

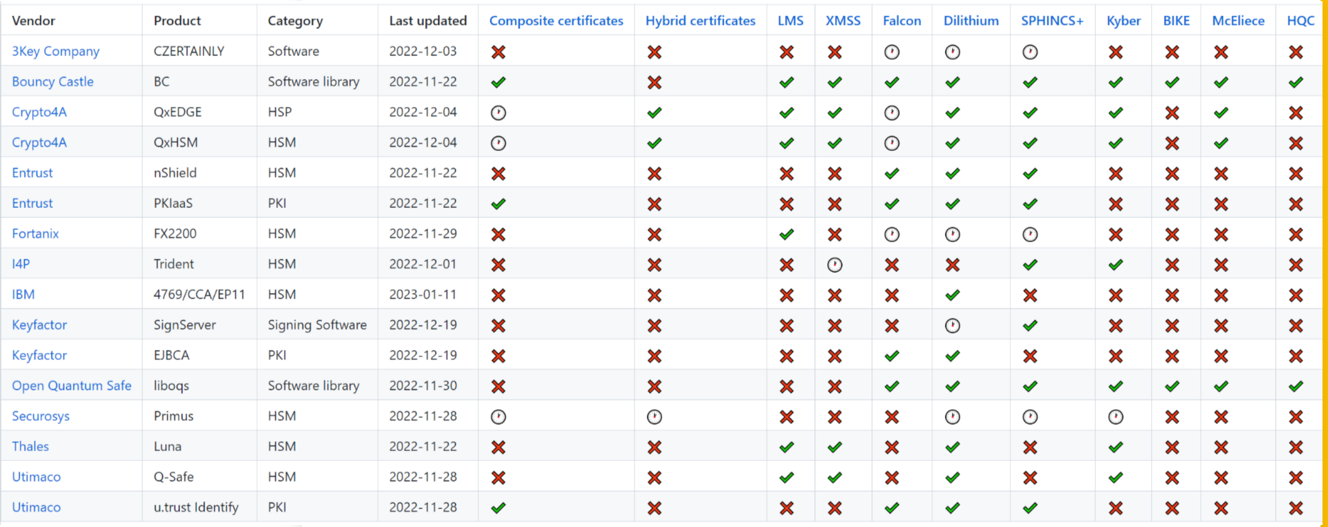
PKI Consortium

- Keep welcoming new members, now 64 in total, of which 5 governments
- Work is published on (pkic.org) and/or GitHub (github.com/pkic), everyone is welcome to contribute!
- No membership fees
- Focus is being shifted to engagement and participation



Recent updates

- PKI Maturity Model
- Remote Key attestation
- PQC Capabilities Matrix
- Post-Quantum Cryptography Conference (March 3, 2023 – Ottawa, Canada) – Hybrid event
  - Agenda, Registration
  - No cost
- Join here: https://pkic.org/join/



Vendor	Product	Category	Last updated	Composite certificates	Hybrid certificates	LMS	XMSS	Falcon	Dilithium	SPHINCS+	Kyber	BIKE	McEliece	HQC
3Key Company	CZERTAINLY	Software	2022-12-03	✗	✗	✗	✗	🕒	🕒	🕒	✗	✗	✗	✗
Bouncy Castle	BC	Software library	2022-11-22	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Crypto4A	QxEDGE	HSP	2022-12-04	🕒	✓	✓	✓	🕒	✓	✓	✓	✗	✓	✗
Crypto4A	QxHSM	HSM	2022-12-04	🕒	✓	✓	✓	🕒	✓	✓	✓	✗	✓	✗
Entrust	nShield	HSM	2022-11-22	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗
Entrust	PKIaaS	PKI	2022-11-22	✓	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗
Fortanix	FX2200	HSM	2022-11-29	✗	✗	✓	✗	🕒	🕒	🕒	✗	✗	✗	✗
I4P	Trident	HSM	2022-12-01	✗	✗	✗	🕒	✗	✗	✓	✓	✗	✗	✗
IBM	4769/CCA/EP11	HSM	2023-01-11	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
Keyfactor	SignServer	Signing Software	2022-12-19	✗	✗	✗	✗	✗	🕒	✓	✗	✗	✗	✗
Keyfactor	EJBCA	PKI	2022-12-19	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Open Quantum Safe	liboqs	Software library	2022-11-30	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓
Securosys	Primus	HSM	2022-11-28	🕒	🕒	✗	✗	✗	🕒	🕒	🕒	✗	✗	✗
Thales	Luna	HSM	2022-11-22	✗	✗	✓	✓	✗	✓	✗	✓	✗	✗	✗
Utimaco	Q-Safe	HSM	2022-11-28	✗	✗	✓	✓	✗	✓	✗	✓	✗	✗	✗
Utimaco	u.trust Identify	PKI	2022-11-28	✓	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗

Thank you

Dimitris Zacharopoulos

dzacharo@harica.gr