KU LEUVEN

PKI and eIDAS

Bart Preneel

@bpreneel1 - preneel@infosec.exchange

4 June 2025

1

Part 1
PKI

2

Goals

- Understand how public keys can be distributed and revoked on a large scale
- Understand what a CA-based PKI is and what the problems are with their deployment
- Understand how multiple CAs can interoperate depending on their trust relationship
- Understand impact of eIDAS 2.0

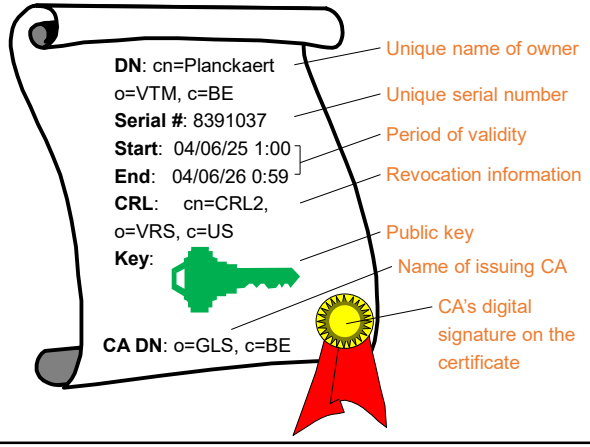
3

How to establish public keys?

- point-to-point on a trusted channel
  - *mail business card, phone*
- direct access to a trusted public file (registry or database)
  - *authentication trees*
- on-line trusted server (bottleneck)
  - OCSP*: Online Certificate Status Protocol*
- off-line servers and certificates
  - *PKI: Public Key Infrastructure*
- implicit guarantee of public parameters
  - *identity based and self-certified keys*

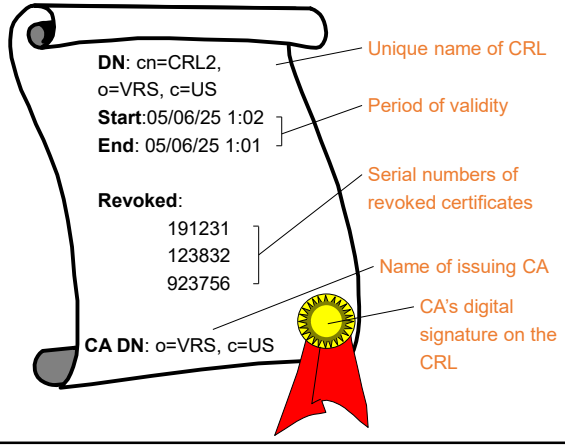
4

What is a Certificate?



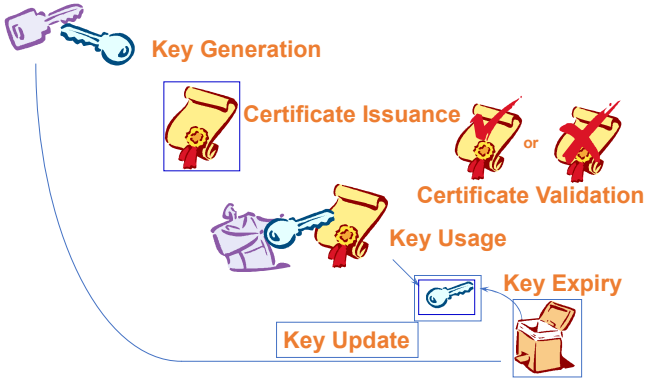
5

What is a Certificate Revocation List?



6

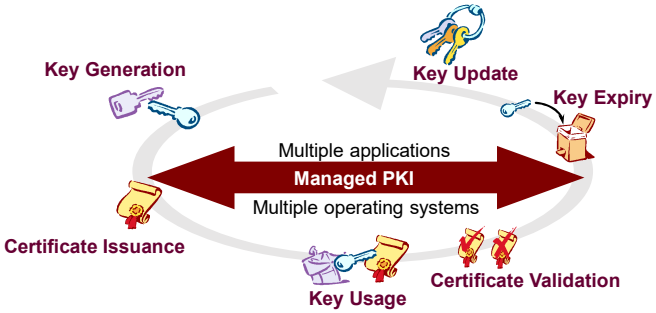
Key Lifecycle Management



7

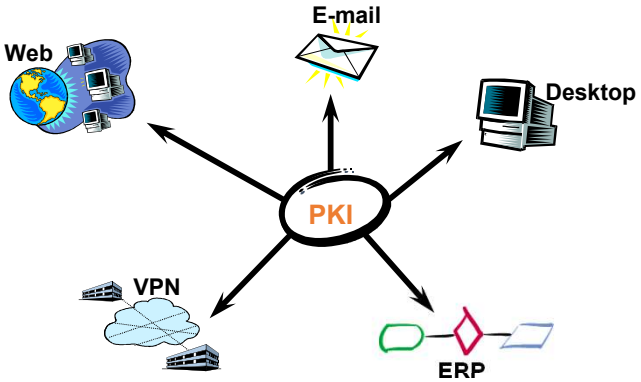
Fundamental PKI features

- Automated and transparent key and certificate lifecycle management
- Consistent behavior across applications



8

PKI should provide Unified Security



This vision from late 1990s has never materialized!

9

Certification Authority

- Issue certificates for all entities / devices (for multiple applications) from a single CA
  - single system saves h/w, s/w, training, personnel
- Flexible certificate policy / security policy
  - tailor to needs of environment, application or entity (e.g. certificate lifetime, crypto algorithms, keylengths, password rules, ...)

10

Certificate Repository

- LDAP-compliant directory stores certificates
  - standards-based for interoperability
- Directory products built specifically to address scalability issues
  - X.500 or proprietary schemes to replicate data (scales to millions of users)

11

Certificate Revocation

- Automated CRL publishing
  - when certificate revoked, CRL can be automatically published to directory providing near-immediate availability
  - automated CRL checking by application
  - want to avoid applications which require manual end-user actions to check CRLs for each application or certificate usage

March 2001: Verisign has issued 2 certs to fake Microsoft employees
- Problem: IE did not implement revocation checking

12

Automated Key Update & History

- Users should never even need to know they have their own certificates (password only)
- If key management is not automated or does not provide key history . . .
  - when certificate expires, lose access to all past encrypted data, e-mail, . . .
  - user must request new certificate and repeat entire registration process
- Should replace key, not just new expiry date
- Transparent triggering mechanism

13

Key Backup & Recovery

- Enterprise will lose valuable (stored) data if keys used to encrypt data are not backed up
  - 20-40% of users forget passwords / year
  - employees leave the organization
- Allows the enterprise to control the backup
  - not reliant on 3rd parties
  - should be configurable to require multiple administrators to authorize access

Key recovery/backup for storage keys should not be confused with **key escrow**; governments have tried to impose this for encryption keys used for communication

14

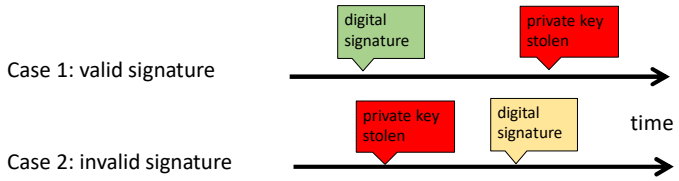
Support for Non-Repudiation

- Must use separate key pairs for digital signatures and encryption
  - want backup of encryption keys, **do not** want backup of signature private keys
- Separate key pairs allows lifecycles to be managed independently
- Different policy controls for each key pair
  - security requirements per pair may differ, e.g. valid lifetimes

15

Timestamping

- Legal requirement
- Business requirements related to fixing transactions in time
- Technical requirements related to certificate revocation (non-repudiation of origin)



Question: why is it not sufficient to include a timestamp in the signed text?

16

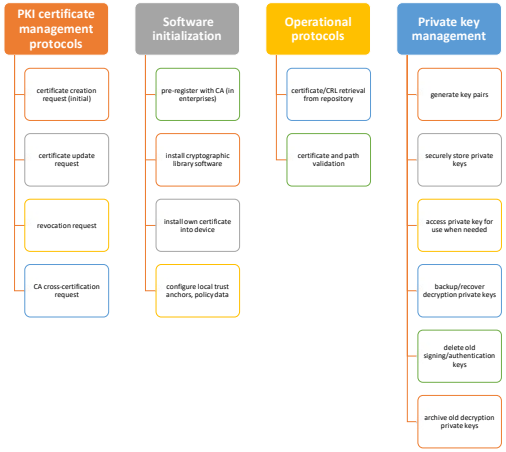
Summary - Essential PKI Components

Much more than a "certificate server" or set of toolkit calls

- Certification Authority
- Revocation system
- Certificate repository ("directory")
- Key backup and recovery system
- Support for non-repudiation
- Automatic key update
- Management of key histories
- Cross-certification
- PKI-ready application software

17

PKI Protocols [credit: Paul van Oorschot]



18

More info: IETF PKIX Working Group

www.ietf.org

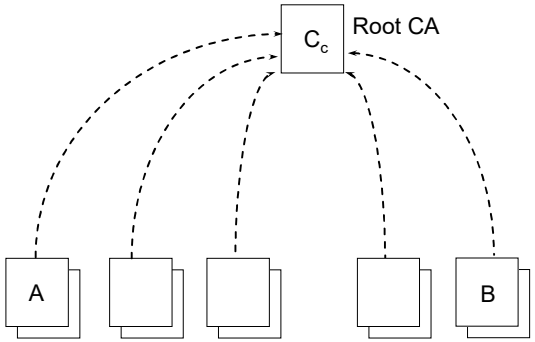
- de facto standards for Internet PKI, X.509-based
- Certificate & CRL Profile [PKIX-1]: RFC 2459
- Certificate Mgmt Protocols [PKIX-CMP, PKIX-3]: RFC 2510
- PKIX roadmap: www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-01.txt

19

Trust Models

20

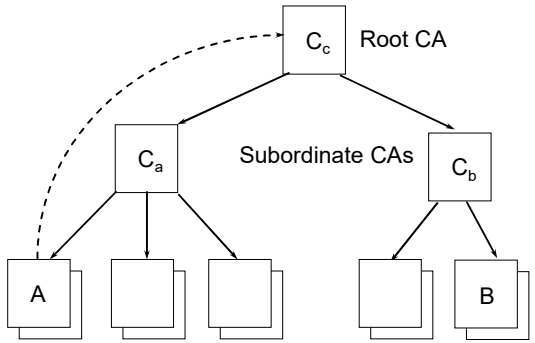
Hierarchical trust model



Relying parties transfer risk to the Root CA

21

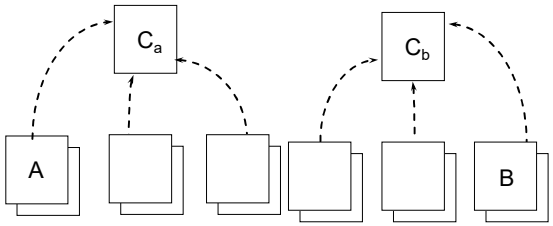
Hierarchical trust model



Root CA "deputizes" subordinate CAs, which issue certificates

22

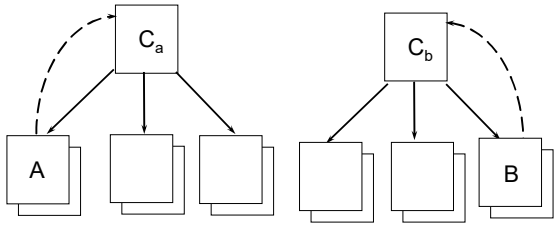
Enterprise trust model



Relying parties transfer risk to their local CA

23

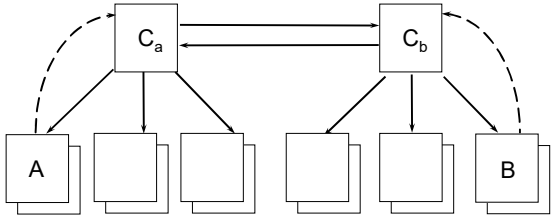
Enterprise trust model



The same local CA issues certificates to these parties

24

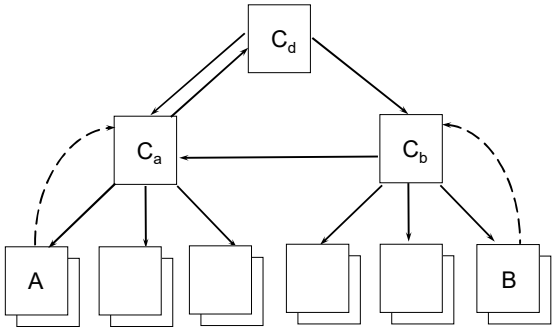
Enterprise trust model



Qualified relationships between CAs are established

25

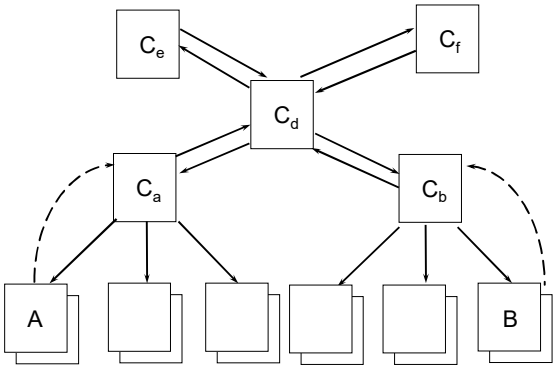
Enterprise trust model



Hierarchical relationships are a special case

26

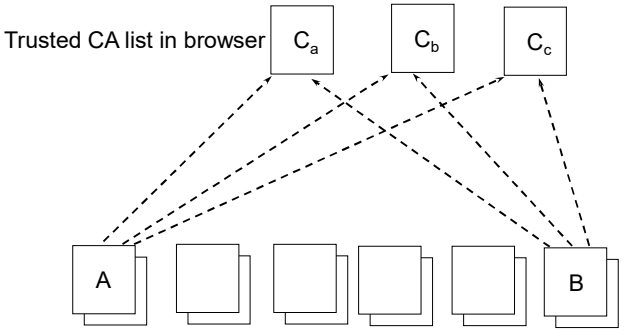
Enterprise trust model



Spoke-and-hub model is another special case

27

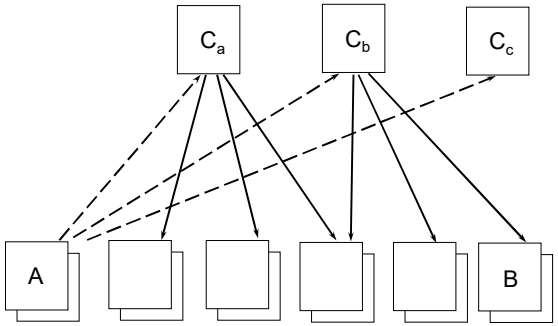
Browser trust model



All relying parties rely on public keys of same set of CAs

28

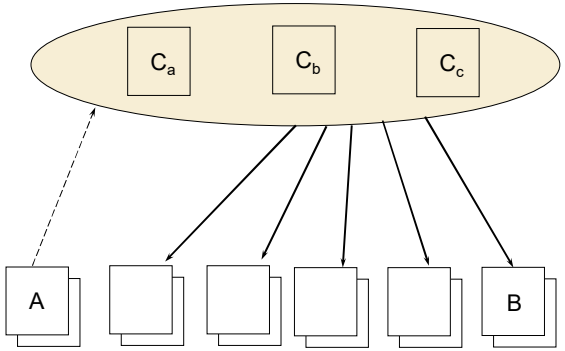
Browser trust model



Each of these CAs defines its own community of trust

29

Browser trust model

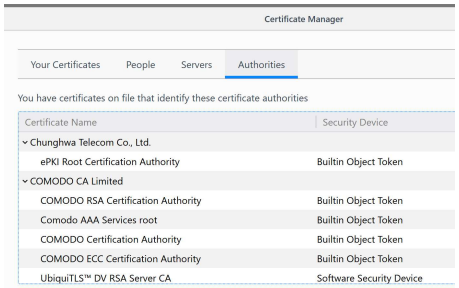


A relying party trusts the union of these communities

30

Browsers include about 650 self-signed CA certificates

- CA Browser forum (https://www.cabforum.org)
  - Voluntary
  - Industry guidelines w.r.t. CA behavior
- Common CA database (https://ccadb.org)
  - Information about CAs whose root and intermediate certificates are included in browsers



User of browser de facto trusts all these CAs

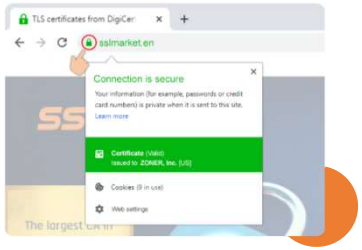
31

ACME: Automatic Certificate Management Environment

(simple version of CMP)

- Domain validation: can be automated
- Organization Validation: sloppy?
- Extended Validation

- But can users tell the difference?
- Mostly abandoned



32

The CA Mess on the web

[Eckersley10] "An observatory for the SSLiverse"

- 10.8M servers start SSL handshake
- 4.3M use valid certificate chains
- 650 CA certs trustable by Windows or Firefox (industry: only 65 main)
- 1.4M unique valid leaf certs
  - 300K signed by one GoDaddy cert
- 80 distinct keys used in multiple CA certs
- several CAs sign the IP address 192.168.1.2 (reserved by RFC 1918)
- 2 leaf certs have 508-bit keys
- Debian OpenSSL bug (2006-2008)
  - resulted in 28K vulnerable certs
  - fortunately only 530 validate
  - only 73 revoked

How can we fix this mess?

33

Selected CA incidents

- March'11 – Comodo: 9 fraudulent certs
  - via RA GlobalTrust.it/InstantSSL.it
- Summer'11 – DigiNotar: 500+ fraudulent certs
  - person-in-the-middle attack against Google users in Iran (300K unique IPs, 99% from Iran)
  - filed for bankruptcy 20 September 2011
- January'13 – Turktrust CA incident
- February'13 – Bit9 lost signing key
- CCA (India) ('14), CCNC and Lenovo (China), ANSSI (France), Kazakhstan ('19), Trustcor ('22)
- 2018: Industry-wide loss in root keys of Symantec
- Products adding trusted roots in trust store
  - Lenovo incident
  - Interception of social media usage by employers

34

Mobile CA

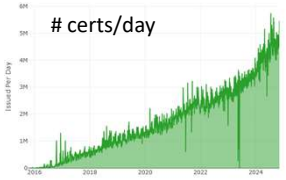
- O/S trust store
  - many Android phones run old versions and have old Trust Store
  - Android Pre-2.3 does not support SHA-256
  - still certs with MD5 and SHA-1
- Mobile Apps
  - ALLOW_ALL_HOSTNAME: 35% of apps; e.g., Facebook, Baidu
  - Custom Trust Store: not always better
- Source: https://bluebox.com/technical/trust-managers (no longer available)

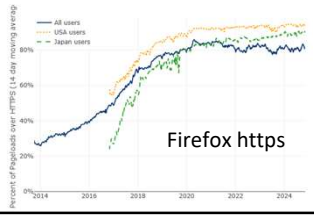
35

Let's Encrypt

live since November 2015
https://letsencrypt.org/stats/

> 550 M active certs
> 700 (fake) PayPal certs…
no revocation – 90-day validity





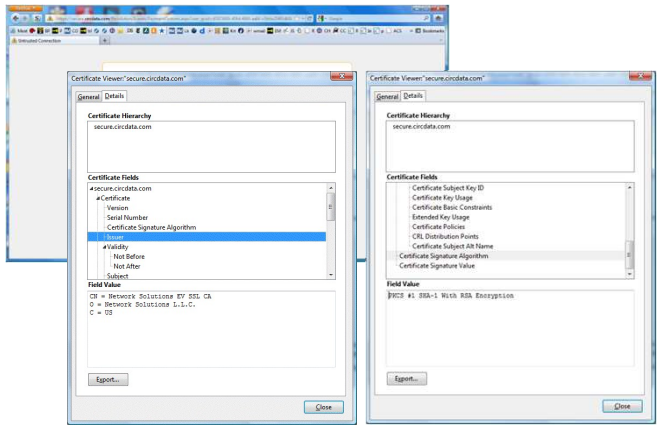
36

Attempted Improvements to CA ecosystem (first 3 mostly failed)

1. **DANE** – based on DNSSEC – specify restrictions for a given SSL/TLS server
   - would need hard fail
2. **CA Authorization** (RFC 6844): tell CA - if you are not one of the CAs on this list, don't issue certs for this domain (competition issue?) (2024: 15.4% of sites)
3. **Pinning:** tell clients - cert for this site look like this; if you detect something else, this may be a breach (more likely a misconfiguration)
   - not for "small" sites? (need bootstrap)
   - seems to work for Google/Chrome ecosystem
4. **Cert Transparency:** certs public in authenticated tree
   - suitable for audits after attack detection

37

CA common problem



38

Personal trust model (and related: "web-of-trust")

- all entities are end-users (CAs do not exist)
- keys are essentially self-guaranteed
- some end-users may also be *introducers*
- end-user imports public keys of others

CHARACTERISTICS

- suits individuals, not enterprise/corporations
- user-centric
- requires security-aware end-users
- poor scalability

39

PGP/GPG Key Servers

- Centralized support for web of trust: servers that hold huge public key rings
  - update to each other, accept and send updates from/to everyone
  - better than everyone keeping a huge key ring
  - server addresses included with PGP/GPG software
  - concerns: privacy, user registration/verification (are you Bill Gates?) and key revocation

Example: PGP Global Directory

40

Trust models & Revocation

- public-key systems are commonly engineered with long-life certificates
- certificates bind a key-pair to identity (and potentially privilege information)
- circumstances change over certificate life
  - keys may become compromised
  - identifying information may change
  - privilege may be withdrawn
- need ability to terminate the binding expressed in the certificate
- revocation: most difficult issue in practice

41

Revocation options

mechanisms indicating valid certificates
- short-lifetime certificates

mechanisms indicating invalid certificates
- certificate revocation lists - CRLs (v1 X.509)
- CRL fragments (v2 X.509), including ...
  - segmented CRLs (CRL distribution points)
  - delta CRLs
  - indirect CRLs

mechanisms providing a proof of status
- status-checking protocols (OCSP, ValiCert)
- iterated hash schemes (Micali)
- certificate revocation trees

42

CRL: properties

- basic CRL
  - simplicity
  - high communication cost from directory to user
- improved CRL
  - very flexible
  - more complex
  - reduced communication and storage

43

Online Certificate Status Protocol (OCSP) [RFC 2560]

- on-line query to
  - CA
  - or Trusted Responder
  - or CA designated responder
- containing
  - hash of public key CA
  - hash of public key in certificate
  - certificate serial number

44

OCSP: signed answer

- status
  - good: not revoked
  - revoked
  - unknown
- time
  - thisUpdate
  - nextUpdate
  - producedAt

45

OCSP: evaluation

- [+] positive and negative information
- [-] need to be on-line
  - risk for denial of service
  - not always possible
- ! OCSP may send you freshly signed but old information
- Worse if stapling (for performance)

If a browser gets **no answer** to an OCSP request, it just goes on as if nothing happened (usability is more important than security)
http://blog.spiderlabs.com/2011/04/certificate-revocation-behavior-in-modern-browsers.html

46

Revocation summary

- established standards for basic revocation
  - ITU-T X.509: 1997, ISO/IEC 9594-8: 1997
  - v2 CRLs
- more sophisticated solutions may be needed for specific applications
- revocation of higher level public keys is very hard (if not impossible)
  - e.g. requires browser patch
- even after 20 years of PKI history, revocation is problematic in practice

47

Characterizing questions for trust models

- what are the types/roles of entities involved
- who certifies public keys
- are trust relationships easily created, maintained, updated
- granularity of trust relationships
- ability of particular technology to support existing business models of trust
- how is revocation handled?
  . . . of end-users . . . of certification authorities

48

Trust model summary

Key idea: manageability of trust relationships

Each model has its place --

- personal trust model: okay for security-aware individuals working in small communities
- browser model: simple, large communities, everyone trusts all CAs defined by s/w vendor
- hierarchical model: best given an *obvious* global root and a *grand design* methodology
- enterprise trust model: best between peer organizations, where trust flexibility is required
- global PKI will include variety of trust models

49

PKI

- Public key cryptography and public keys are essential for large scale secure systems
- PKI as we know today is designed for an off-line world in 1978
- Global PKI is very hard
  - who is authoritative for a given namespace?
  - liability challenge
- Revocation is always hard

- Things are much easier if relying party is the same as issuing party: no certificates are needed

50

Part 2 eIDAS 2.0 regulation

51

eIDAS 1.0 (2014): limited uptake

- signatures
- seals
- time stamps
- registered delivery services
- dertificates for website authentication (QWACs)
- preservation of signatures & seals

But

- mostly public sector (limited use in private sector)
- few providers
- inflexible
- not cross-border: member state implementations

52

eIDAS 2.0 (announced June'21):

- certificates for website authentication update
- mobile identity wallet with government-issued identities
  - but also additional attributes (public and private issued)
  - selective disclosure of attributes
- electronic ledgers
- …

53

In force 20 May 2024

- **digital identity wallet** available and recognized by Nov. 2026
  - one per member state
- remains **voluntary** (avoid discrimination if non-use)
- **qualified website authentication certificates** (QWACs)

https://www.europarl.europa.eu/cmsdata/278103/eIDAS-4th-column-extract.pdf

- **Implementing regulations: 4 December 2024**
  - Integrity and core functionalities
  - Protocols and interfaces to be supported
  - Personal identification data and electronic attestations of attributes
  - Trust Framework
  - Certification

https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+milestone+reached+as+Commission+adopts+implementing+regulations

54

The Good

- interoperable at EU level (technical but not semantical)
  - Architecture Reference Framework https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.6.1/
  - https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/discussions
- open source implementation
- privacy focus:
  - no unique identifier for all applications
  - preclude tracking, profiling and discrimination
  - registration of relying parties

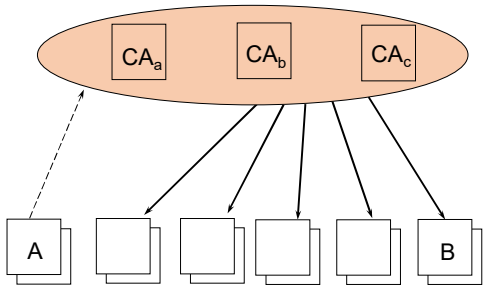
55

The Bad: linkability

- Server side likely not open source
  - member states are granted leeway so that, for justified reasons, specific components other than those installed on user devices need not be disclosed
- The technical framework of the European Digital Identity Wallet shall **not allow** providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, **to obtain data that allows for tracking**, linking, correlating or otherwise obtain knowledge of transactions or user behaviour unless explicitly authorised by the user.
- unlinkability and unobservability (w.r.t. service provider) **optional:** migration of service providers to weakest Member State
- ARF not up to date (public: 1.6)
  - technical implementation unclear
  - anonymous credentials (1985) seen as too innovative: only one-time use credentials

56

The Ugly: impact on WebPKI 1/5



Browser user trusts all 660 CAs in the browser
Adding CAs = at best not reducing security

57

The Ugly: impact on WebPKI 2/5

- eIDAS 2.0 further pushes for QWACS (Qualified Web Authentication Certificates) issued by QTSPs
- showing legal identity to user in a user-friendly way
- tried before (2008-2016) and abandoned in WebPKI: under the name Extended Validation
- problems
  - companies may have 5+ legal entities in Europe (BV, Srl, GmbH,…)
  - researchers registered a company with as name "Identity Verified"

Insanity Is Doing the Same Thing Over and Over Again and Expecting Different Results

58

The Ugly: QWACS/QTSPs last minute changes 3/5

- do the current 53 QTSPs comply with (free) certification processes? (data from Mozilla)
  - 23 YES
  - 17 never applied
  - 5 in queue
  - 8 failed and did not reapply
- what does eIDAS 2.0 say:
  - Root keys of accredited CAs of Member States need to be inserted in browser trust store
- Art. 45: "browsers to recognise any certificate that satisfies some criteria specified in regulation, *without any other requirements to be imposed by the browsers"*
- will certificate transparency be allowed? Other new ideas?
- opens door for
  - person-in-the-middle attack by EU Member states
  - similar attacks by other (less democratic) countries
- do we trust ETSI?

59

The Ugly: last minute changes 4/5

After 2nd open letter (Oct. 23): Recital 32 was updated (refusal to update Art. 45)

"Recognition of QWACs means that the providers of web-browsers should not deny the authenticity of qualified certificates for website authentication for the sole purpose of attesting the link between the website domain name and the natural or legal person to whom the certificate is issued and confirming the identity of that person.

The obligation of recognition, interoperability and support of QWACs is not to affect the freedom of web-browser providers to ensure web security, domain authentication and the encryption of web traffic in the manner and with the technology they consider most appropriate."

60

The Ugly
last minute changes 5/5

Mitigation of Art. 45

"By way of derogation to paragraph 1 and only in case of substantiated concerns related to breaches of security or loss of integrity of an identified certificate or set of certificates, web-browsers may take precautionary measures in relation to that certificate or set of certificates."

Supervisory authority and European Commission notified of concerns

Supervisory authority then decides whether or not the certificates have to be reinstated

Note: Article 4 of the Lisbon treaty allows for national security exception

61

Timeline

https://www.europarl.europa.eu/legislative-train/spotlight-JD22/file-eid

- Commission proposal: 3 June 2021
- EU Parliament ITRE: 9 February 2022
- First open letter (39 scientists): 2 March 2022
- EU Parliament ITRE: 16 March 2022
- Trilogue start: 21 March 2023
- Trilogue provisional agreement: June 2023 (secret)
- Second open letter (550+ scientists and 40+ NGOs) after leak: 2 November 2023
- End of trilogue: 8 November 2023
- Statement: still concerns (80+ scientists): 23 November 2023
  - Request for additional statement clarifying the recital and the unlinkability
- EU Parliament ITRE vote: 28 November 2023 but postponed till 7 December due to "technical error"
- Full Parliament vote: 29 February 2024
- Adoption by Council: 26 March 2024
- In force: 20 May 2024

62

European Council
Council of the European Union

Home > Press > Press releases

Council of the EU | Press release | 26 March 2024 10:30

European digital identity (eID): Council adopts legal framework on a secure and trustworthy digital wallet for all Europeans

63

Supplementary statement accepted by the Parliament and the Commission (not by the Council!)

'Statement by the Commission on Article 45 on the occasion of the adoption of Regulation 2024/...+

The Commission welcomes the agreement reached, which, in its view, clarifies that web browsers are required to ensure support and interoperability for the qualified website authentication certificates (QWACs) for the sole purpose of displaying the identity data of the owner of the website in a user-friendly manner. The Commission understands this obligation as not prejudging the methods used to display such identity data.

The Commission welcomes the agreement reached, which, in its view, clarifies that the requirement for the web browsers to recognise QWACs does not restrict browsers own security policies and that Article 45, as proposed, leaves it up to the web browsers to preserve and apply their own procedures and criteria in order to maintain and preserve the privacy of online communications using encryption and other proven methods. The Commission understands draft Article 45 as not imposing obligations or restrictions on how web browsers establish encrypted connections with websites or authenticate the cryptographic keys used when establishing those connections.

The Commission recalls that, in line with point 28 of the Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making of 13 April 2016, the Commission will make use of expert groups, consult targeted stakeholders and carry out public consultations, as appropriate.

64

Supplementary statement accepted by the Parliament and the Commission (not by the Councill)

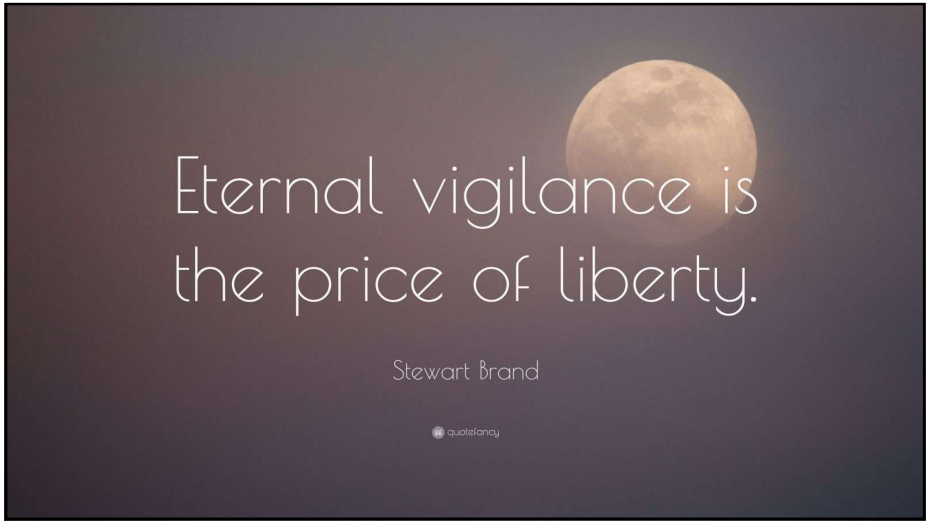
Statement by the Commission on unobservability on the occasion of the adoption of Regulation 2024/... +

The Commission welcomes the agreement reached, which in its view, confirms that this amending Regulation does not allow for the processing of personal data contained in or arising from the use of the European Digital Identity Wallet by the Wallet providers for other purposes than delivering wallet services.

The Commission also welcomes the inclusion of the concept of unobservability in Recital (11c) of the draft amending Regulation, which should prevent wallet providers from collecting and seeing the details of user's day-to-day transactions. The Commission is of the view that this concept means that there should not be correlation of data across different services for the purposes of user tracking or tracing or for determining, analysing and predicting personal behaviour, interests or habits.

At the same time, the Commission acknowledges that, in full compliance with Regulation (EU) 2016/679, the providers of European Digital Identity Wallets may access certain categories of personal data with the user's explicit consent, such as in order to ensure continuity in the provision of wallet services or to protect users from disruptions in their provision. That data should be limited to what is necessary for each specific purpose.'

65



66

Bart Preneel

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven
WEBSITE: homes.esat.kuleuven.be/~preneel/
EMAIL: Bart.Preneel@esat.kuleuven.be
MASTODON: bpreneel@infosec.exchange
TWITTER: @bpreneel1
TELEPHONE: +32 16 321148

KU LEUVEN COSIC
ArenBerg Crypto BV

67

67