Ministerie van Economische Zaken
en Klimaat

Building Trust, Empowering the Digital Economy
eIDAS Trust Services

CA Browser Forum 60

October 3, 2023

Rob Brand

Senior Policy Officer eIDAS

Ministry of Economic Affairs and Climate Policy

Directorate Digital Ecomomy

Background

Ministry of Economic Affairs and Climate Policy is responsible for the Telecommunications Law

- Political responsible for eIDAS Trust Services, Ministry of Interior and Kingdom Relations is responsible for eIDAS eID
- Currently involved in the eIDAS negotiations
- Member of EU Expert Group
- Member of ETSI
- Working on Large Scale Pilots for the EUDI Wallet

eIDAS and Trust Services can boost the Digital Single Market by increasing trust and user friendliness

Prehistory

- **Signature Directive 1999/93, introduction of qualified certificate for signatures**
  - → National legislation necessary; Wet elektronische handtekeningen (NL, 2002), Signaturgesetz (DE, 2001)
  - → No harmonization, no SB cooperation
  - → Management system audit, paper check only by SB-NL, SB-NL lack of relevant knowledge
- **PKIO, PKI for government communication**
  - 3 certificate model (CIA), based on ETSI 101456 requirements for CSPs
  - Root (Top CA) managed by the NL Government (“Staat der Nederlanden”)
  - Additional national interoperability requirements with supervision by government
  - Initial focus on B2G, G2B, G2G. First CSPs PinkRoccade, DigiNotar, CIBG, DoD
  - Services certificates (Websites, SSL), based on ETSI 102042 with same assurance level

Asteroid impact

DigiNotar hack in 2011

- man in the middle attack
- 500 false certificates issued
- caused by weak security practices (basic assurance level, PKIO certificates **NOT** affected)

→ Near complete shutdown of Dutch government traffic

→ DigiNator bankruptcy

Middle Ages (0)

DigiNotar resulted in a dramatic and substantial increase of

security awareness,

legal improvements and

organizational measures

Middle Ages (1)

- Report of the Dutch Safety Board Published in 2013 with a number of recommendations
- New Supervisory Body: Government Inspectorate Digital Infrastructure (RDI) with task of becoming knowledge center on Trust Services
- Ministerial crisis manual and yearly exercise
- Increase organization agility by requiring multiple vendor strategy

Middle Ages (2)

- eIDAS regulation (2014, effective July 1, 2016)
  - Direct effect so national laws obsolete
  - Harmonized requirements
  - **Product certification, based on ISO 17065**
  - **Autonomous responsibility and inspection right for national SBs after conformity assessment by accredited CAB**

Middle Ages (3)

- eIDAS regulation (2014, effective July 1, 2016)
  - Introduction of QWACs*
    - In NL QWACs required for Government organizations
  - **For DoD Qualified Certificates including QWACs essential for Trust within NATO communication**
  - Voluntary not-harmonized recognition of EV certificates (Green bar/lock)
    - Until another asteroid impact in 2018

Modern times (1)

- eIDAS 2 - Trust services (effective somewhere in 2024?!)
  - New Trust Services (rQES, Issuing of EAA, eArchiving, eLedgers)
  - Supervision of Trust Services even more strengthened
  - Enhanced governance and cooperation between SBs
  - Force recognition of QWACs by browsers (art 45.2)

Modern times (2)

- Recognition of QWACs by browsers
  - Weapon in the fight against internet fraud
  - Element in building trust in online services and digital economy
  - GDPR requires identification of the controller
  - Public authorities encouraged to use QWACs
  - QWACs required for PSD2
  - QWACs recommended for Relying Parties in the EUDI Wallet ecosystem

Modern times (3)

- Final legal text of article 45 will consist of elements of Commission proposal, Council compromise and EP amendment text

  → User-friendly display

  → No measures taken contrary to obligation to recognize

  → Precautionary measures by browsers in case of substantial and justified concerns

Modern times (4)

- Concerns about consistency and user friendliness of QWAC indication (UI)
- Concerns why high-trust certificates need extra requirements and audits
- Concerns on unilateral decision making for forced reduced life cycle for public and private services certificates (costs, resources, lack of automation) This also frustrates use of QWACs
- Concerns on implementation of two certificate approach with prediction of a new natural disaster

Future (0)

True cooperation is necessary

Future (1)

- Regulating trust instead of free market powers because of geopolitics
- More stress on digital autonomy/sovereignty
- EU looking for partners that comply
- Out of the box approach needed
  - Zoning certificate stores by browsers (cf Public Trust certificates and Private trust certificates, QWACs within PSD2)
  - Adjusted indication QWACs not in certificate store
  - EU representation in CA/Browser Forum as “root program operator” (EDIFB)
  - Taking services certificates like S/MIME outside WebPKI scope