enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TRUST SERVICES AND ELECTRONIC IDENTIFICATION: SUPPORTING POLICY

Dr. Andreas Mitrakas, Head of Unit Data security & standardisation,
ENISA

Trust Services Forum 2020

22 | 09 | 2020

Purpose of ENISA studies

- **Support the development and implementation** of Union policy in the field of electronic identity and trust services
- Promote **best practice in cybersecurity regarding (Q)TSPs and in eID schemes**
- Ensure that **secure electronic identification** and **authentication** can be used to access cross-border online services offered by Member States
- **Promote remote verification methods** to avoid face-to-face presence to a registration authority (Article 24 of eIDAS regulation) which creates burdensome and expensive physical presence procedures
- Support the fulfilment of requirements originating from the non-mandatory articles of eIDAS
- Harmonised adoption of the eIDAS regulation

A maturity model / remote identification

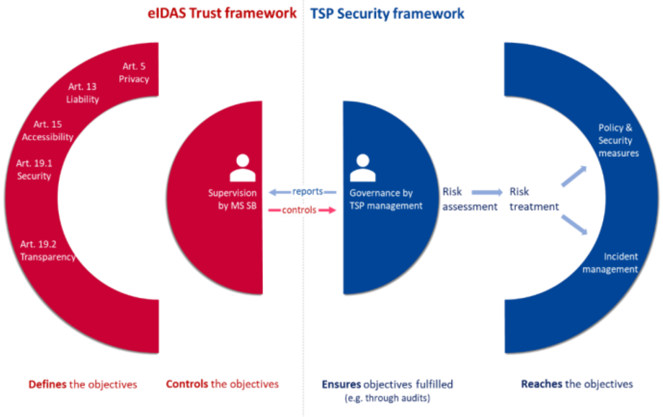
- A maturity model framework for eID schemes
  - ENISA is creating an eID **capacity maturity model** (CMM) in the form of a self-assessment questionnaire to measure the level of maturity of the eID schemes notified under eIDAS in EU Member States.
  - The aim of the project is to **promote best practices** on eID, relying on information provided in the context of the eID schemes notifications
- Analysis of methods to carry out identity verification remotely
  - To provide an **analysis of methods** to carry out identity verification remotely which varies at national level
  - **Propose best practices** for the eIDAS stakeholders taking into account the security requirements imposed by the eIDAS regulation.
  - The outcome will be a **risk analysis** and an **analysis of security measures** to check how compliance with the eIDAS regulation can be achieved

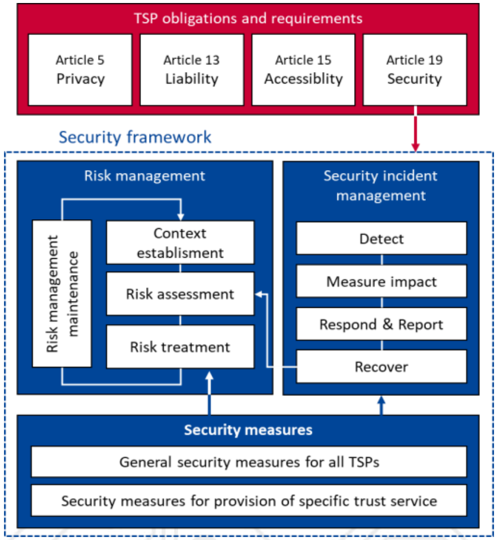
Review of recommendations for TSPs (and call for review/feedback)

- ## Objectives of the reviews:
  - update a set of ENISA prepared guidelines (so-called Set 2) , taking into account other documents published by ENISA (i.e. Set 1 of guidelines and further reports) ,
  - produce, based on the guidelines on a security framework for Qualified Trust Service Providers , a report on a security framework for non-qualified Trust Service Providers
- ## Targeted audiences:
  - TSPs, prospective QTSPs, and QTSPs looking for guidelines for fulfilling requirements originating from the eIDAS Regulation.
  - Service providers which may wonder if they are a TSP in the sense of eIDAS and which are interested in knowing their obligations as a consequence.
  - Relying parties wanting to evaluate how compliant a TSP they rely on is with the eIDAS (security) requirements, and how aware of his obligations their (prospective) TSP is.

Security framework for (Qualified) Trust Service Providers

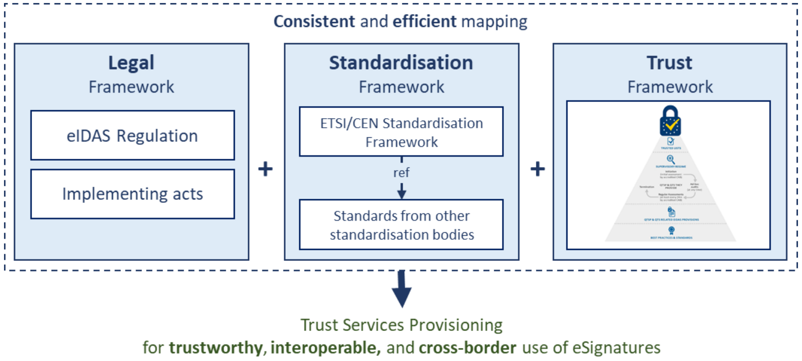
- In order to ensure due diligence, inclusion, transparency, and accountability of the operations and services, all TSPs (Qualified and non-Qualified) are subject to a common set of requirements, in particular on:
  - Data processing and protection, as defined in Article 5;
  - Liability, as defined in Article 13;
  - Accessibility for persons with disabilities, as defined in Article 15; and
  - Security, as defined in Article 19.1 and 19.2
- The studies target to “translate” these requirements:
  - In general for all TSPs (D4) as well as the specificities for QTSPs (D1)
  - Next to clarify the security measures, special attention is paid to risk management and security incident management as per specific attention for these topics under eIDAS.

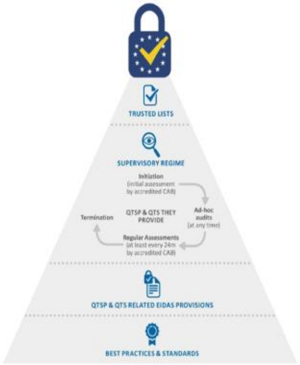


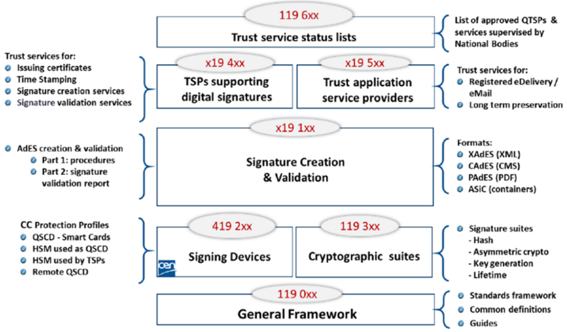


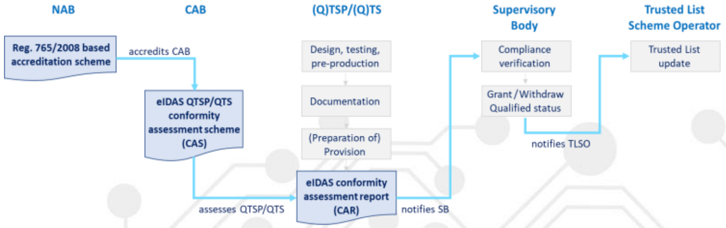
Recommendations for QTSPs based on Standards & Conformity Assessment of QTSPs

- “Recommendations for QTSPs based on standards”:
  - provides recommendations to help QTPSs and auditors understanding the expected mapping between the requirements / obligations and existing and updated standards, as well as provide guidance for their usage.
- “Conformity Assessment of QTSPs”:
  - discusses preparing and undertaking the conformity assessment as-well-as certification, surveillance and renewal in a process-oriented way.
  - covers frequently asked questions of parties involved.


Consistent and efficient mapping
Legal
Framework
eIDAS Regulation
Implementing acts
+
Standardisation
Framework
ETSI/CEN Standardisation Framework
ref
Standards from other standardisation bodies
+
Trust
Framework
Trust Services Provisioning
for trustworthy, interoperable, and cross-border use of eSignatures

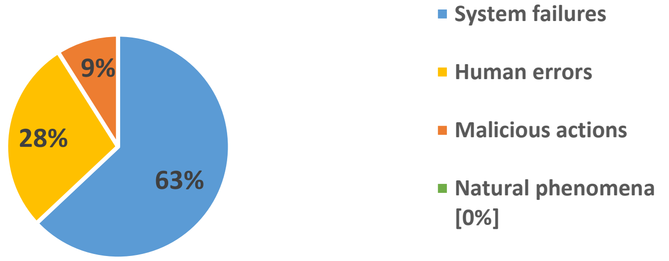

TRUSTED LISTS
SUPERVISORY REGIME
Initiation
(initial assessment by accredited CAB)
Ad-hoc audits
(at any time)
QTSP & QTS THEY PROVIDE
Termination
Regular Assessments
(at least every 24m by accredited CAB)
QTSP & QTS RELATED EIDAS PROVISIONS
BEST PRACTICES & STANDARDS



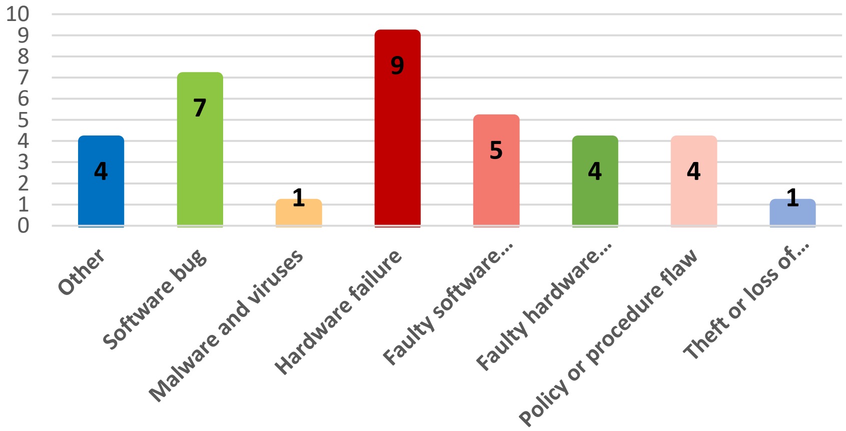

NAB
CAB
(Q)TSP/(Q)TS
Supervisory Body
Trusted List Scheme Operator
Reg. 765/2008 based accreditation scheme
accredits CAB
eIDAS QTSP/QTS conformity assessment scheme (CAS)
Design, testing, pre-production
Documentation
(Preparation of) Provision
eIDAS conformity assessment report (CAR)
assesses QTSP/QTS
notifies SB
Compliance verification
Grant / Withdraw Qualified status
notifies TLSO
Trusted List update

Art. 19 – incident reporting

Root causes Trust service security incidents - 2019



Detailed causes of trust services security incidents - 2019



- System failures dominate (63%, 20 incidents)
- Hardware failures and software bugs are the main causes
- Most incidents minor (almost a third had large impact)
- Most reported incidents concerned qualified trust services (78%)
- eSignature service most affected

ENISA strategy towards standardisation

- General
  - Maintain a comprehensive inventory of SDOs, their activities and products
  - Maintain a comprehensive inventory of industrial bodies, their activities and products
  - Development and maintenance of inventory of assurance protection profiles
- EU institutions
  - ENISA as a point of reference for EU institutions for cybersecurity
  - ENISA as a point of reference to EU research programs for cybersecurity
- Standards Developing Organisations
  - Influence European standardisation
  - Participate in relevant SDOs activities
  - Participate in relevant industry bodies activities
  - Contribution to development of relevant standards

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

☎ +30 28 14 40 9711

✉ info@enisa.europa.eu

🌐 www.enisa.europa.eu