eIDAS Standardisation
What are the Issues and Concerns?

Overview from CEN TC 224 WG 16 “ESIGN”
Gisela Meister
Table of contents

1. Status eIDAS Regulation and CEN TC 224 in the context of the Cyber security strategy
2. eIDAS and eIDAS Token Specification
3. eIDAS and CEN Standardisation on QSCDs
4. Do mobile ID solutions can be compliant to the eIDAS regulation?
5. Outlook / Summary
Strategy of the EU in the context of Cyber Security

The upcoming EU regulation

- EU Cyber security Strategy is a key point of the Digital Agenda for Europe
- Required compliance to the highest Security Assurance Levels
- Interoperability must be insured by referencing international standards
- Data and privacy protection from smart security solutions
- Innovative payment solutions must build on trusted foundations

To ensure a high level of cyber security across the EU:
- Reform of EU’s data protection rules
- Regulation on electronic Identification and Trusted Services
- Directive on Network and Information Security
- New Payment Services Directive

Giesecke & Devrient
The Legislation of the eIDAS regulation is i.e. to be performed by Implemented Acts

- which are not supposed for
- Harmonisation of the eID APIs, but for harmonisation of
  - Proxy Services respective Middleware APIs, supporting the same assurance level

The eIDAS Token Specification (TR 03110) provides harmonisation on SE level and is already

- cross-linked to European and international Security Standardisation (CEN; ETSI; ISO/IEC; GP)
- designed to reduce the complexity of the Service Software
- Intended for highest assurance level
  implemented as profile by German PA for millions of citizens
eIDAS Token Specification BSI & ANSSSI / ANTS References

- eIDAS Token
- Technical Guideline TR-03110-2
- Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token
- see www.bsi.bund.de/eIDAS

Backup: The Technical Guideline (BSI / ANSSI) contains profiles, protocols and APIs for eIDAS tokens, Service providers and Attribute Providers.

- Part 1 - relevant for MRTD documents
- Part 2 – Protocols for electronic IDentification, Authentication and Trust Services
- Part 3: Common Specifications,
- Part 4 – Applications and Document Profiles, including new enhanced privacy features as
  - Chip Authentication v3 for group-authentication
  - Pseudonymous Signatures for signing e.g. token stored attributes or commitment for remote signatures
  - Onntoken - Attribute Provider Functionality as Support of Enhanced Role Authentication (ERA)

Version 2.20 March 2015
The eIDAS Token Specification is cross-linked to current European and international security harmonisation activities on cyber security.
Part 1 - Introduction /Tutorial /Glossary

Part 2 – Basic signature services (w/o device auth.)

Part 3 – Device Authentication, Establishment of a secure channel

Part 4 – Privacy features (ERA, Age verification, …)

- including new enhanced privacy features as
  - On-token Attribute Provider Functionality as Support of Enhanced Role Authentication (ERA)
  - Age Verification…

Part 5 – Encipherment and Id mananagement services

- references the eIDAS Token Specification, whereever appropriate, but is designed for interindustry use
- is intended to be enhanced to be” technology neutral “ as the next step e.g. integration of mobile and remote services
Implementation Example 2 for eiDAS featuring the highest or moderate assurance level for eIDS:

Derived ID as short term for

Mobile ID, e.g. eID on a Mobile Phone,
- implemented in software and/or on a Secure Element e.g. SIM
- including derived credentials
  - derived by ID attribute(s) originated by a physical smart card
  - mapped logical data structure or subset or additional features (e.g. PKI applet e.g. Provided providing the same Interface as original)
- (limited) temporary validity e.g. credential may contain expiration date
- (enhanced) features e.g. may contain additional algorithms, protocols,...
Derived IDs may be implemented on a SE with / without a TEE
Backup: Security and Privacy requirements by Eurosmart are proven correct by current international cyber attacks. See German national federal assembly.

What could happen in the worst case?

eIDAS worst case for the smart security industry, in 8 steps

1. In the eIDAS regulation, levels «Substantial» and «high» are very close to each other.
2. Pushed by anglo-saxon lobby and European actors that will be acquired by internet giants, «substantial» has become the predominant requested level.
3. Member States make the statement that costs of «high» level electronic means are too high for too few use cases. They abandon the chip in the eID documents.
4. A new ecosystem appears: Solutions have doors to important attacks that cybersecurity new measures fight with delays. But insurance companies provide digital risk contracts and citizens/consumers bear the costs.
5. In the TTIP negotiations, EU solutions look quite similar to GAFAs, and European values (privacy, data protection) look old fashioned. Time will do its work (next step).
6. Society considers that data protection and privacy protection was a nice age, but now the new age is society 2.0.
7. Security of identity has become substantial; security of all access management and authentication means make the same move.
8. It is the decline of the smart security industry, with its consent.
<table>
<thead>
<tr>
<th>eIDAS</th>
<th>Success</th>
<th>Neutral</th>
<th>Concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part of Cyberstrategy of EU</td>
<td>Is linked and referred to other EU activities</td>
<td></td>
<td>Privacy concern are old aged , Society 2.0</td>
</tr>
<tr>
<td>moderate and high assurance level</td>
<td>software implementations are possible</td>
<td></td>
<td>moderate seems to be the mainstream in contradiction to cybersecurity goal</td>
</tr>
<tr>
<td>claims no reference to specific technology</td>
<td>Technology neutrality may win new implementations and use cases as remote/mobile</td>
<td>eIDAS token and CEN QSCD standards can be applied</td>
<td>no mandatory harmonisation on eID token level</td>
</tr>
<tr>
<td>Implemented Acts build on European Standards</td>
<td>Provides reference to CEN PPs /ETSI formats and EU projects</td>
<td></td>
<td>Harmonisation of eIDs are lacking , no reference to functional standards as eIDAS token or EN 419 212 /QSCD</td>
</tr>
<tr>
<td>New features as eSEAL</td>
<td></td>
<td>no need for new standard</td>
<td></td>
</tr>
</tbody>
</table>
Vielen Dank für Ihre Aufmerksamkeit!

Dr. Gisela Meister
Director
Head of Security Consulting / Standardisation

Secure Devices – Mobile Security
Giesecke & Devrient GmbH
Prinzregentenstrasse 159
81607 Munich, GERMANY
www.gi-de.com

Gisela. Meister@gi-de.com