eIDAS Regulation –
eID and assurance levels –
Outcome of eIAS study

Dr. Marijke De Soete
Security4Biz (Belgium)
ETSI eIDAS Workshop
24 June 2015 – Sophia Antipolis
eIDAS Regulation

→ Regulation on electronic identification and trust services for electronic transactions in the internal market (sometimes referred to as e-IDAS – electronic identification and authentication services regulation) was published on 28 August 2014

→ **Goal:** “Strengthen the EU Single Market by boosting trust and convenience in secure and seamless cross-border electronic transactions”

→ **Most provisions take effect from 1 July 2016**
  - Repeals existing eSignature Directive 1999/93/EC
  - Replacing inconsistent national laws in Europe

→ **Regulation covers:**
  - Mutual recognition of e-identification means
  - Electronic trust services (e-signatures, e-seals, e-registered delivery services, time stamping, website authentication)
  - Electronic documents
eIDAS – Timeline of implementation

- **17.09.2014** - Entry into force of the Regulation
- **18.09.2015** - Voluntary recognition of eIDs
- **1.07.2016** - Date of application of rules for trust services:
- **18.09.2018** - Mandatory recognition of eIDs
eIDAS Regulation and e-Identification

→ Regulation establishes a legal framework to support the EU-wide recognition of eIDs used by Member States.
→ It mainly targets the public sector: Member States shall permit citizens from other Member States to use their own eIDs to access online services.
→ Private sector companies are not directly impacted – but voluntary alignment is expected to increase reach of their services.
→ eIAS Study Team provided input for building blocks for secondary legislation in the eID area covering:
  – Assurance levels
  – Cooperation
  – Notification
  – Interoperability framework
→ Implementing acts on interoperability framework and eID levels of assurance are due by 18 September 2015
eID Assurance levels

The Implementing act should define 3 assurance levels on the basis of the criteria enumerated in the Regulation:

a) the procedure to prove and verify the identity of a “Person” applying for the issuance of electronic identification means;

b) the procedure for the issuance of the requested electronic identification means;

c) the authentication mechanism, in which the natural or legal person uses the electronic identification means to confirm its identity to a relying party.

d) the entity issuing electronic identification means;

e) any other body involved in the application for the issuance of the electronic ID means; and

f) the technical and security specifications of the issued electronic identification means.

In terms of the Regulation, a Person can be a natural or legal person, or a natural person representing a legal person.
The Regulation specifies three assurance levels:

<table>
<thead>
<tr>
<th>Assurance level</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Low             | • *limited degree of confidence* in the claimed or asserted identity of a Person  
• reference to technical specifications, standards and procedures, including technical controls, the purpose of which is *to decrease the risk of misuse or alteration of the identity* |
| Substantial     | • *substantial degree of confidence* in the claimed or asserted identity of a Person  
• reference to technical specifications, standards and procedures, including technical controls, the purpose of which is *to decrease substantially the risk of misuse or alteration of the identity* |
| High            | • *higher degree of confidence* in the claimed or asserted identity of a Person  
• reference to technical specifications, standards and procedures, including technical controls, the purpose of which is *to prevent misuse or alteration of the identity* |
eID Assurance levels

To provide the required confidence in a person and the authentication, the implementing act should cover requirements for the following processes:

- Enrolment
- Credential management
- Authentication

and additional guidance for management and operational aspects (information security management, legal compliance, ...) which affect the identification and authentication of a “person”
eID Assurance Framework (eIDAF)

Enrolment phase
- Application and initiation
- Identity proofing and identity information verification
- Record-keeping

Credential management phase
- Credential creation
- Credential pre-processing
- Credential issuance
- Credential activation
- Credential storage
- Credential suspension, revocation, and/or destruction
- Credential renewal and/or replacement
- Record-keeping

Entity authentication phase
- Authentication
- Record-keeping

Electronic identification scheme

Management and Organisation
Actors in the eIDAF

- **Entity (Person)**
- **Electronic identification in an e-service**
- **Electronic identification means issuance (credential + token)**
- **Credential Service Provider**
- **Entity registration and identity proofing**
- **Relying Party (e-Service provider)**
- **Trusted Third Party (e.g., Authentication service)**
- **Registration Authority (RA)**
eID Assurance levels

• To define the requirements for the different levels in the different processes the Study team used input from:
  – STORK QAA
  – ISO 29115

• The IAS2 study team proposal for an eIDAF was delivered to the EC mid 2014:
  – Created an ISO compliant quality assurance specification while focusing on an outcome based approach
  – Draws on some normative requirements to integrate STORK experience
  – Filling in the identified gaps
eID Assurance levels

Comparison between eIDAF, STORK QAA and ISO/IEC 29115

<table>
<thead>
<tr>
<th>Assurance levels in Regulation</th>
<th>STORK-QAA</th>
<th>ISO 29115</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>QAA2</td>
<td>LoA2</td>
</tr>
<tr>
<td>Substantial</td>
<td>QAA3</td>
<td>LoA3</td>
</tr>
<tr>
<td>High</td>
<td>QAA4</td>
<td>LoA4</td>
</tr>
</tbody>
</table>
eID Assurance levels – Where are we now?

- Subsequent to the delivery of the draft eIDAF by the IAS2 team to the EC, the EC created an informal eIDAS expert group composed of Member States experts to provide support for the preparation of the secondary legislation.

- Challenges included
  - The development of assurance levels for the identification and identity proofing of legal person;
  - Identity proofing of a legal person in the enrolment phase – many forms exist with great variation among Member States;
  - Binding of a natural person acting on behalf of a legal person – make distinction between enrolment phase and subsequent use;
  - Development of different minimum data sets for natural and legal persons

- Implementing acts are discussed at the eIDAS Committee (under comitology procedure) on 23 and 24 June 2015.
Any questions or feedback?