eIDAS Regulation (EU) 910/2014

Boosting trust in the Digital Single Market: the role of eIDAS Regulation

International Workshop: Electronic identity without borders
7 December 2016 – Praha (CZ)

Andrea SERVIDA
DG CONNECT, European Commission
Head of Unit "eGovernment and Trust"
andrea.servida@ec.europa.eu
eIDAS: boosting trust & supporting businesses!

TRUST

CONVENIENCE

CROSS-BORDER

SEAMLESS
eIDAS – The Regulation in a nutshell

2 MAIN CHAPTERS SUBJECT TO DIFFERENT RULES AND REQUIREMENTS

Chapter II

Mutual recognition of e-identification means

Chapter III

Electronic trust services

• Electronic signatures
• Electronic seals
• Time stamping
• Electronic registered delivery service
• Website authentication

Chapter IV

Electronic Documents
The eIDAS Regulation provides for eID & TS:

- Technological neutrality
- Non-discrimination
- Interoperability
- Cross-border recognition
- Legal certainty
- Security
- Liability
Timeline

**eID**

- **17.09.2014** Entry into force of the eIDAS Regulation
- **29/09/2015** Voluntary cross-border recognition
- **26.11.15 - eID DSI v.1 eIDAS compliant**
- **29/09/2018** Mandatory cross-border recognition

**Trust services**

- **eSignature Directive rules**
- **1.07.2016** Date of application of eIDAS rules for trust services
<table>
<thead>
<tr>
<th>Legal Act</th>
<th>Reference</th>
<th>Adoption date</th>
<th>Entry into force</th>
</tr>
</thead>
<tbody>
<tr>
<td>eIDAS Regulation</td>
<td>910/2014</td>
<td>23.07.2014</td>
<td>17.09.2014 (1.07.2016 - application provisions on TS)</td>
</tr>
<tr>
<td>ID on procedural arrangements for MS cooperation on eID (art. 12.7)</td>
<td>2015/296</td>
<td>24.02.2015</td>
<td>17.03.2015</td>
</tr>
<tr>
<td>IR on interoperability framework (art. 12.8)</td>
<td>2015/1501</td>
<td>8.09.2015</td>
<td>29.09.2015</td>
</tr>
<tr>
<td>IR assurance levels for electronic identification means (art. 8.3)</td>
<td>2015/1502</td>
<td>8.09.2015</td>
<td>29.09.2015</td>
</tr>
<tr>
<td>ID on circumstances, formats and procedures of notification (art. 9.5)</td>
<td>2015/1984</td>
<td>3.11.2015</td>
<td>5.11.2015 (notified to Ms)</td>
</tr>
<tr>
<td>IR on EU Trust Mark for Qualified Trust Services (art.23.3)</td>
<td>2015/806</td>
<td>22.05.2015</td>
<td>12.06.2015</td>
</tr>
<tr>
<td>ID on technical specifications and formats relating to trusted lists (art. 22.5)</td>
<td>2015/1505</td>
<td>8.09.2015</td>
<td>29.09.2015</td>
</tr>
<tr>
<td>ID on formats of advanced electronic signatures and seals (art. 27.5 &amp; 37.5)</td>
<td>2015/1506</td>
<td>8.09.2015</td>
<td>29.09.2015</td>
</tr>
</tbody>
</table>
eIDAS: Key principles for eID

- **Cooperation** between Member States
- **Sovereignty of MS** to use or introduce means for eID
- **Interoperability** framework
- **Principle of reciprocity** relying on defined levels of assurance
- Mandatory **cross-border recognition** only to access public services
- **Full autonomy for private sector**

The Regulation does not impose the use of eID
Countries with nationally supported eID schemes

Nearly all Member States (will) have a nationally supported eID scheme in place

Preliminary data from the ongoing CEF eID Stakeholder Analysis Report by Deloitte

- Countries with eID schemes: AT, BE, DE, DK, EE, ES, FI, HR, HU, IT, IS, LT, LU, LV, MT, NL, NO, PT, RO, SE, SK, TR, UK
- Countries setting-up national eID schemes: BG, CY, CZ, EL, FR, SI
- Countries to be confirmed: IE, PL

Information provided by MSs (as of 1 January 2016):
eID cards in 15 MSs (6 planned), other eID means in 24 MSs
25 MSs having either an eID card or other eID means
Member States Cooperation in eID - (EU)2015/296

Key principles of the Cooperation

- Member States have the **obligation to cooperate**
- Main focus on achieving **interoperability** and **security**
- Common language

Elements of the Cooperation

- **Points of single contact** – exchange of information
- **Peer review**
  - Voluntary participation
  - Each Member State bears its own costs
  - Confidentiality of information obtained
  - Avoiding conflict of interest
- **Exchange of information, experience and good practices**
- **Request of information on interoperability and security**
- **Cooperation Network** - MS are members, meetings chaired by the COM
- **Tasks of the Cooperation Network** – some examples
  - adopt guidance on the scope of peer review and its arrangements
  - adopt opinions on developments relating to the interoperability framework
  - examine relevant developments in the eID sector
Levels of Assurance - (EU) 2015/1502

Inspiration from ISO 29115 and STORK QAA:
- Practical experience gained during STORK pilot
- Outcome-based approach in ISO 29115

Need for a **new set of criteria/procedures**:
- STORK too normative
- ISO 29115 does not take into account existing practice in MSs

Setting out **criteria** instead of **specifications**

**Principles**

- eIDs within MSs are **mapped** against **outcome based criteria** to determine which of the 3 LoA is applicable for both natural and legal persons
- The **mapping** is subject to **peer review by other MSs** to ensure understanding and consistency
- Only applicable to **schemes notified to the Commission** for cross border use
- The **criteria** cover IPV, the electronic means, issuance, authentication and information security management
Levels of Assurance - (EU) 2015/1502

Elements of Levels of Assurance

<table>
<thead>
<tr>
<th>Enrolment</th>
<th>eID means management</th>
<th>Authentication</th>
<th>Management, organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• application</td>
<td>• design</td>
<td>• requirements for confirming an identity to a relying party</td>
<td>• Information Security Management (ISM),</td>
</tr>
<tr>
<td>• registration</td>
<td>• issuance</td>
<td>• record keeping</td>
<td>• record keeping</td>
</tr>
<tr>
<td>• identity proofing</td>
<td>• suspension</td>
<td>• facilities and staff,</td>
<td>• facilities and staff,</td>
</tr>
<tr>
<td></td>
<td>• renewal and replacement</td>
<td>• controls,</td>
<td>• controls,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Compliance and audit</td>
<td>• Compliance and audit</td>
</tr>
</tbody>
</table>

An example of differences between LoA: *identity proofing*

<table>
<thead>
<tr>
<th>Physical appearance at registration (including remote or at earlier stage)</th>
<th>Level high: substantial plus</th>
<th>Level substantial: low plus</th>
<th>Level low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required</td>
<td>Not required</td>
<td>Not required</td>
<td></td>
</tr>
</tbody>
</table>

| Verification of identity evidence | Verified possession of valid identity evidence (like photo/bio) | Based on recognised evidence checked to be genuine | No direct verification of identity evidence assumed to be genuine |

**Principles**

- **Technological neutrality**

- **High level requirements** – further specifications being defined with MSs

- **Open source technical specifications and Reference implementation** available from Commission

- Option for MSs to directly implement the technical specifications provided **interoperability** is guaranteed

- **Disproportionate requirements** on other MSs flowing from an implementation are **not permitted**

- **The architecture is de-centralised**. The nodes or middleware components provide the interface translation between the different national solutions and does not impact them

- **Continuous development of technical specifications in cooperation with MS.** Cooperation Network ensures policy governance on specs (via formal "opinions")
Where does eIDAS have an impact?

**UMM&DS** - Uniform User Management and Digital Signatures  
**eHGI** - eHealth Governance Initiative  
**ECI** - European Citizens' Initiative  
**ESSN** - European Social Security Number  
**SUP** - Directive on single-member private limited liability companies  
**PSD2** – Revised Directive on Payment Services  
**AML4** - 4th Anti-Money Laundering Directive
Promoting eIDAS Regulatory fitness in other sector specific legislations

- **Better Regulation Toolbox** (Tool 23: ICT assessment, the digital economy and society) – explicit reference to eIDAS
- Close *bilateral cooperation* with other DGs on specific regulatory initiatives

Examples relevant to banking and financial sectors:
- Cooperation with FISMA and the European Banking Authority (EBA) on the role of notified eID and trust services to meet the requirements under the [PSD2](#):
  - EBA discussion paper (of 8/12/15) on strong customer authentication and secure communication under PSD2 - eIDAS is presented as a possible solution
  - EBA Consultation Paper (of 12/8/16) on draft regulatory technical standards on strong customer authentication and common and secure communication
  - Green paper (of 10/12/15) on retail financial services and related public consultation - eIDAS featured with respect to the cross border benefits of e-signature and eID.

- Cooperation with JUST on supporting the transposition of the [AMLD4 Directive](#) at national level, as well as on the recent proposal to amend AMLD4 (of 5/7/16), in order to ensure consistency with eIDAS.

Underlying principles:

| Digital by Default | Once only principle | Inclusiveness and accessibility | Openness and transparency | Cross-border by default | Interoperability by default | Trustworthiness and Security |

References to eIDAS: Policy priority 1 ("Modernise public administration with ICT, using key digital enablers") - actions:

- "Further efforts by all administrations are needed to accelerate the take up of electronic identification and trust services for electronic transactions in the internal market [...] actions to accelerate cross-border and cross-sector use of eID (including mobile ID) in digitally enabled sectors (such as banking, finance, eCommerce and sharing economy) and in the public sector namely on the European e-Justice Portal. The Commission will also explore the need to facilitate the usage of remote identification and secure authentication in the retail financial services"

- "The Commission will gradually introduce the 'digital by default' principle when interacting online with external stakeholders, using eIDAS services (in 2018), eInvoicing (in 2018) and eProcurement (in 2019)."
Banking in the Digital Age

• Round Table launched by Commissioner Oettinger on 5 April 2016
• The second and last meeting was held on 14 November in the presence also of VP Dombrovskis and saw the participation of 20 banks and associations.

• **Objective:** identify what should be done at EU level to help enhance banks' competitiveness and their ability better to serve citizens and firms
• **Attendance:** CEOs and Heads of Federations
• **Most important issues for banks in view of digital transformation**

**Priority areas identified:**
**Cybersecurity, data and cloud, eID and digital onboarding, platforms and online payments as well as some prudential and accounting issues related to technological developments and digital transformation**
Digital on-boarding

1. Customer initiates enrolment procedure

   Customer accesses bank website → website authentication ensures that website belongs to bank

   Identity verification

   Notified eID under eIDAS →

   Minimum data set:
   - current family name
   - current first name
   - date of birth
   - unique identifier

2. Customer Due Diligence/Business Relationship

   Depend on bank/national applicable rules on CDD/KYC

   Additional attributes:
   - first and family name at birth
   - place of birth
   - current address
   - gender

3. Fraud

How cross-border eID/authentication works:

1. Customer accesses bank website
2. Website authentication
3. Notified eID under eIDAS
4. Minimum data set
5. Additional attributes
6. Depend on bank/national applicable rules on CDD/KYC
7. Fraud
8. CustomerDue Diligence/Business Relationship
9. Customer initiates enrolment procedure
Sets a comprehensive strategic and political approach to standardisation for 5 priority ICT areas: 5G communications, cloud computing, the internet of things (IoT), (big) data technologies and cybersecurity.

Action in the area of Cybersecurity (section 3.1.4):

"The Commission will:

- Invite ESOs and other SDOs and relevant stakeholders to develop standards by the end of 2018 that support global interoperability and seamless trustworthy authentication across objects, devices and natural and legal persons based on comparable trust models. This work should be based on technical standards aligned with the eIDAS regulatory framework."

*Reference to eIDAS:*

**IMPLEMENTING MAIN PRINCIPLES FOR PLATFORM DEVELOPMENT IN THE EU:**

iii) Fostering trust, transparency and ensuring fairness

- "In order to empower consumers and to safeguard principles of competition, consumer protection and data protection, the Commission will further promote interoperability actions, including through issuing principles and guidance on eID interoperability at the latest by 2017. The aim will be to encourage online platforms to recognise other eID means — in particular those notified under the eIDAS Regulation — that offer the same reassurance as their own".
Stakeholder engagement - eIDAS Observatory

Purpose

• Help facilitate the use of cross-border electronic identification and trust services
• Foster transparency and accountability by identifying market hurdles and good practices, promoting knowledge-sharing and developing initiatives for innovation
• Contribute to the enhancement of trust and security of digital transactions thus to the building of the Digital Single Market
• Act as a virtual network of stakeholders to exchange ideas and good practices as well as recommend actions and initiatives to ease the uptake of eID and trust services

Launch

• Officially launched by VP Ansip during the event "A new leap in the eIDAS journey: new trust services for a Digital Single Market" on 30 June 2016
For further information and feedback

Web page on eIDAS

eIDAS Observatory

Text of eIDAS Regulation in all languages
http://europa.eu/!ux73KG

Connecting Europe Facility – Catalogue of Building Blocks
https://ec.europa.eu/cefdigital

eIDAS twitter account
@EU_eIDAS