Let's go eIDAS: building trust online

Towards Trustworthy Digital Identities in Europe
Brussels, 03/07/2019

Andrea Servida
DG CONNECT, European Commission
Unit R3 "Knowledge Management & Innovative Systems"
Andrea.Servida@ec.europa.eu
Building trust in the online world is crucial to accomplish the Digital Single Market. Coupling mobile authentication credentials, such as Mobile Connect, with the identity security provided by eIDs under the eIDAS Regulation, is the way towards this goal.

Andrus Ansip
Vice-President of the European Commission for Digital Single Market

#eIDAS
@eID_EU
eIDAS: boosting trust & supporting businesses!

Strengthen EU Single Market by boosting **TRUST** and **CONVENIENCE** in **secure** and **seamless** cross-border electronic transactions

Provide a consistent set of rules throughout the EU
eIDAS

- eID
- Electronic signatures
- Electronic seals
- Electronic time stamps
- Electronic registered delivery services
- Website authentication
- Electronic documents
- Validation Preservation

eIDAS
Achievements

- 172 QTSP in 29 countries (18 June 2019)
- 65% of the EU population covered by notified or pre-notified eIDs

Challenges

- Optimize the eIDAS trust model
- Efficient monitoring of the eIDAS enforcement in the MS
- Streamlining eIDAS and eGov principles in other relevant Commission initiatives & work closer with other DGs
- Promote incentives for better take-up of eIDAS by the private sector
- Promote internationalisation of eIDAS
- eIDAS Review: Getting the most data out of the eIDAS review to support the points above

### Notified eID schemes

<table>
<thead>
<tr>
<th>Country</th>
<th>Publication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>26 Sept 2017</td>
</tr>
<tr>
<td>Italy</td>
<td>10 Sept 2018</td>
</tr>
<tr>
<td>Spain</td>
<td>7 Nov 2018</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>7 Nov 2018</td>
</tr>
<tr>
<td>Estonia</td>
<td>7 Nov 2018</td>
</tr>
<tr>
<td>Croatia</td>
<td>7 Nov 2018</td>
</tr>
<tr>
<td>Belgium</td>
<td>27 Dec 2018</td>
</tr>
<tr>
<td>Portugal</td>
<td>28 Feb 2019</td>
</tr>
<tr>
<td>UK</td>
<td>2 May 2019</td>
</tr>
</tbody>
</table>

- CZ, IT and NL - peer-review -
- LV, BE and SK - pre-notified
Why eID is important

"The cross border use of trusted eID gives Europeans a **new freedom**: to rely on the eID they already use at national level and to securely access digital services provided everywhere across the EU.

Mariya Gabriel
Commissioner for Digital Economy and Society
#eIDAS
@eID_EU
What does eID under eIDAS do for you?

- "economic" drive
- "trust-building" drive
- Trusted assertions/credentials
- USER ENABLEMENT
- USER EMPOWERMENT

- Personal data = digital currency
- Personal data = private asset

eIDAS makes digital identity to speak for you and not about you!
EU vision: eID “speaks for us and not about us”

eIDAS gives the opportunity to citizens to:

- control and selectively disclose identity data when accessing online services cross border
- limit the collection of their identity data to those strictly needed for a transaction while ensuring always full accountability.

It reinforces:

**GDPR compliance**

Data minimisation; use of trusted attributes, credentials and entitlements (such as age verification, proof of residence, etc.), requirements regarding parental consent for the processing of personal data of children below a certain age ...

**Audiovisual Media Service Directive**

Protection of minors / Age verification and parental consent / Extension to video-sharing platforms / Emphasis on co-regulatory and self-regulatory instruments ...

**OOP**

Access to data based on “digital authentication” roaming / Consent / Proof of origin & integrity / ...

**Cybersecurity**

eID&TS are preventative security measures (e.g. access to platforms) / going beyond encryption (eg QWCAS) / support “need2know” (eg KYC) / promote risk management culture (e.g. audit, certification, SBN, etc.) / bring greater transparency and accountability online (fight disinformation) ...
Where eIDAS plays a role

**AMLD5 – Directive (EU) 2018/843**
Published on OJEU on 19/06/2018


**Once-Only Principle cross-border**
EU Regulation 2018/1724 on Single Digital Gateway of 02/10/2018

**Digital on-boarding and portability of KYC**
EC Expert Group on eID and remote KYC (5th meeting held on 23 May 2019) – jointly managed by CNECT, JUST and FISMA

**Company law**
Proposal to amend the Directive (EU) 2017/1132 adopted by EC on 25/04/2018 as regards the use of digital tools and processes in company law

**Tackling online disinformation / Fighting fake news**
COM(2018) 236 final adopted on 26/04/2018

**GDPR compliance**
Data minimisation; use of trusted attributes, credentials and entitlements (such as age verification, proof of residence, etc.)

**Audiovisual Media Service Directive**
Protection of minors / Age verification and parental consent

...
The building blocks of the Connecting Europe Facility promote the adoption of the same open standards and technical specifications, by the different sectors of the Union, for the most basic & common functionalities of any sectorial project/ platform.

These core commonalities will enable interoperability across borders and sectors.
How it started and where is it going?

**PILOTING**
- STORK
- PEPPOL
- SPOCS
- epSOS
- eCODEX

**SCALING UP**

**REGULATORY**
- EU Legislation e.g. eIDAS

**DEMAND CREATION**
- CEF Work Programmes
- eGovernment Action Plan
- DSM Catalogue of Standards

**SUPPLY CREATION**
- Grants (subsidies)

**SUSTAINING**
- e-SENS ecosystem

How it started and where is it going?
The eID ecosystem
The benefits of interoperable and recognised eID for the different actors:

- **Citizen**
  - Use eID
  - Cross-border online services
  - Ease of use
  - Cost saving
  - Increased assurance

- **Public administration**
  - Set up
  - National eIDAS Node
  - Cost saving
  - Compliance
  - Increased assurance
  - Financial support

- **Identity/Attribute providers**
  - Provide identity/attributes
  - New areas of application
  - Once only principle
  - Cost saving
  - Legal compliance
  - Increased security/assurance
  - Increase potential user base

- **Service providers**
  - Offer services using eID
  - Cost saving
  - Legal compliance
  - Increased security/assurance
  - Increase potential user base
Minimum set of person identification data **uniquely representing** a natural or a legal person

### Natural person

**Mandatory**
- Current family name(s)
- Current first name(s)
- Date of birth
- A unique identifier as persistent as possible in time

**Optional**
- First name(s) and family name(s) at birth
- Place of birth
- Current address
- Gender

[Sector specific attributes]
- [Social security number]
- [Student number]
- [Tax number]

### Legal person

**Mandatory**
- Current legal name
- A unique identifier as persistent as possible in time

**Optional**
- Current address
- VAT registration number
- Tax reference number
- Legal Entity Identifier (LEI) referred to in Commission Implementing Regulation (EU) No 1247/2012
- Economic Operator Registration and Identification (EORI) referred to in Commission Implementing Regulation (EU) No 1352/2013
- Excise number provided in Article 2(12) of Council Regulation (EC) No 389/2011

[Sector specific attributes]
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

Customer Due Diligence/Business Relationship

Check against fraud risk

Depend on bank/national applicable rules on CDD/KYC

How cross-border eID/authentication works

1. Identity verification
2. Notified eID under eIDAS
3. Minimum data set:
   • current family name
   • current first name
   • date of birth
   • unique identifier
4. Optional data in the MDS:
   • first and family name at birth
   • place of birth
   • current address
   • gender
5. Depend on bank/national applicable rules on CDD/KYC
6. Optional data in the MDS:
   • first and family name at birth
   • place of birth
   • current address
   • gender
7. Domain specific attributes:
   • Profession
   • Social Security Number
   • Politically Exposed Person
8. Attribute provider
What about eID in the EU?

On eID, EU is the first and only multi-jurisdictional region in the world having:
- **A policy** (i.e. Large scale pilots & CEF Building Block on eID and eSignature)
- **A predictable legal framework Regulation** (i.e. eIDAS Regulation)
- **Rules** (eIDAS Implementing Acts)
- **Technology** (i.e. national eIDs and CEF BBs)
- **Interoperability infrastructure** (eIDAS compatible "nodes/MW")

The EU has:
- World-class hardware, software and service providers, and administrations at the forefront of eGovernment
- 24 MS have eID means (4 planned) – 15 MS have eID cards (6 planned)
- Large Scale Pilot Projects to ensure interoperability
Update on UNCITRAL work

Creating a global standard for the recognition of eID and trust services in B2B for trade.

• 58th session of the Commission (8-12 April 2019, New York)

• Draft Provisions on the Cross-Border recognition of Identity Management and Trust Services”.
  ➢ Keeping a holistic approach embracing digital eIDs and trust services.
  ➢ Based on key principles and elements of eIDAS federating model

• Constructive approach of key countries (US/CAN/JP/RUS/CHINA/SGP)- Willingness to advance to concrete outcomes

• Revised text in the next session in Vienna (25-29 November 2019)
How eIDAS Regulation is relevant to blockchain: Inserting content in the blockchain

User decides to send some data to the blockchain (transaction record, DID, etc.)

Signed/sealed data

Data sent to the network are grouped into a block by validating nodes

The block is validated by the "validating nodes" of the network using a consensus algorithm

The block is timestamped and added to the chain of blocks (blockchain) which is accessible to all users
How eIDAS Regulation is relevant to blockchain: Content of the blockchain as an electronic document

**Article 3**
**Definitions**
For the purposes of this Regulation, the following definitions apply:

(35) ‘*electronic document*’ means *any content stored in electronic form*, in particular text or sound, visual or audiovisual recording;

**Article 46**
**Legal effects of electronic documents**
An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.
Identity in SSI

• Based on the use of Decentralised Identifiers (DIDs)
  • Fully under the control of the subject
  • Do not provide information about the subject
• Combined with the used of Verifiable Claims (VC)
  • Prove to third parties the attributes of the subject
  • Self-asserted / issued by others
• Trust on the issuer of the VC is established by trusting the issuer’s DID
How eIDAS Regulation is relevant to blockchain:
Blockchain for “identity”

- Issues signed attestation: Ensures identity of the issuer: trustworthiness of the attestation.
- User: Presents self-asserted data.
- Receiver: Ensures identity of the receiver: right to have access to the attestations.
- DID blockchain: eIDAS Observatory post: “SSI and eIDAS: a vision on how they are connected” Share your views!
The need for verified identities

- Three types of interactions in the digital world
  - Fully anonymous interaction
  - Anonymous identity, but verifiable under certain conditions
  - Fully disclosed real identity -> attributes allowing identifying uniquely the person
- Service providers / relying parties may impose requirements on the type of interaction allowed
- Users should be able to decide
  - SSI should, by design, support the three types of interactions
- The trustworthiness of verifiable claims is rooted on the authority of the issuer
  - Verifying the identity of the issuer is key
- Under DID / SSI, the trust on the actual identities of the parties is built out of the system
  - There is no binding of digital identifiers to real-world entities
- eIDAS can provide the trust framework for this binding
What's next

- Factors driving the evolution of electronic identity and trust services
  - Globalisation and connected society
  - Increasing demand for frictionless experiences
  - Increasing concerns about use of personal data
  - Increasing crowded and fragmented digital identity market
  - Growing dependency between public and private sectors
  - Increasing cybersecurity risks
  - Rise of exponential technology: cloud, DLT, IoT, AI, social media

- Trends
  - Mobile first
  - Biometrics: multimodal and behavioural
  - Analytics enabling real-time and continuous authentication
  - Blurring lines between the physical and the digital world – identity of things
  - Citizen-controlled data
  - Changing identity ecosystem
What's next

AN INTERNET OF HUMAN VALUES

The overall mission of the Next Generation Internet Initiative is to re-imagine and re-engineer the Internet for the third millennium and beyond. We envision the information age will be an era that brings out the best in all of us. We want to enable human potential, mobility and creativity at the largest possible scale - while dealing responsibly with our natural resources. In order to preserve and expand the European way of life, we shape a value-centric, human and inclusive Internet for all.

Resilient.

These important ambitions need a solid technological foundation to build on. The legendary robustness of the Internet must become actual reality in the Next Generation Internet. A massive global fleet of connected devices is on its way to enhance and control our homes, factories, offices and vehicles. Technology is entwined in concrete, circulating in space and is increasingly entering the intimacy of our human bodies. The Next Generation Internet has to be both highly adaptive and entertaining resilient. Whatever happens or parts of the network go down by some natural or other disaster, the effects on the rest of us should be close to zero.

Trustworthy.

There is another essential dimension to trust, which lies above physical availability. We need a transparent technological environment, that is completely trustworthy. The architecture, governance and policies structure how entire societies and economies interact. By design it should protect free speech and private enterprise and much more. The Next Generation Internet is to be designed to avoid any bias or systemic abuse of global trust in the Internet. It shall be a true global commons, rising above international politics and competition. It will guarantee the safety of citizens and strengthen the health and autonomy of our markets and societies across borders.

Sustainable.

The enduring success of the Internet lies in permission-free innovation, openness and interoperability. The Next Generation Internet is set up to empower, to unlock our choices. It fosters diversity and decentralisation, and grows the potential for disruptive innovation. This extends far beyond the technical realm. The Next Generation Internet will achieve a sustainably open environment for our cultures and economies, celebrating our values and promoting creativity and well-being.

Let's re-invent Internet to reach the full human potential, for all generations.

GET INVOLVED

NG1EU
CONSULTATION.NG1EU
@NG1EU

European Commission
For further information and feedback

Web page on eIDAS

eIDAS Observatory

Text of eIDAS Regulation in all languages
http://europa.eu/lux73KG

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

eIDAS twitter account
@EU_eIDAS

Andrea Servida
DG CONNECT, European Commission
Unit R3 “Knowledge Management & Innovative Systems"
andrea.servida@ec.europa.eu