

Trust in a Digital Society



eID under eIDAS

Building trust in a digital society

Carlos Gómez
DG CONNECT
European Commission
Unit "eGovernment & Trust"

Part 1

What is eIDAS?

eIDAS – The Regulation in a nutshell

2 MAIN CHAPTERS SUBJECT TO DIFFERENT RULES AND REQUIREMENTS

Chapter II

Mutual recognition of e-identification means



Chapter IV

Electronic Documents

Chapter III

Electronic trust services

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

eID

17.09.2014

Entry into force of the eIDAS Regulation

29.09.2015

Voluntary cross-border recognition

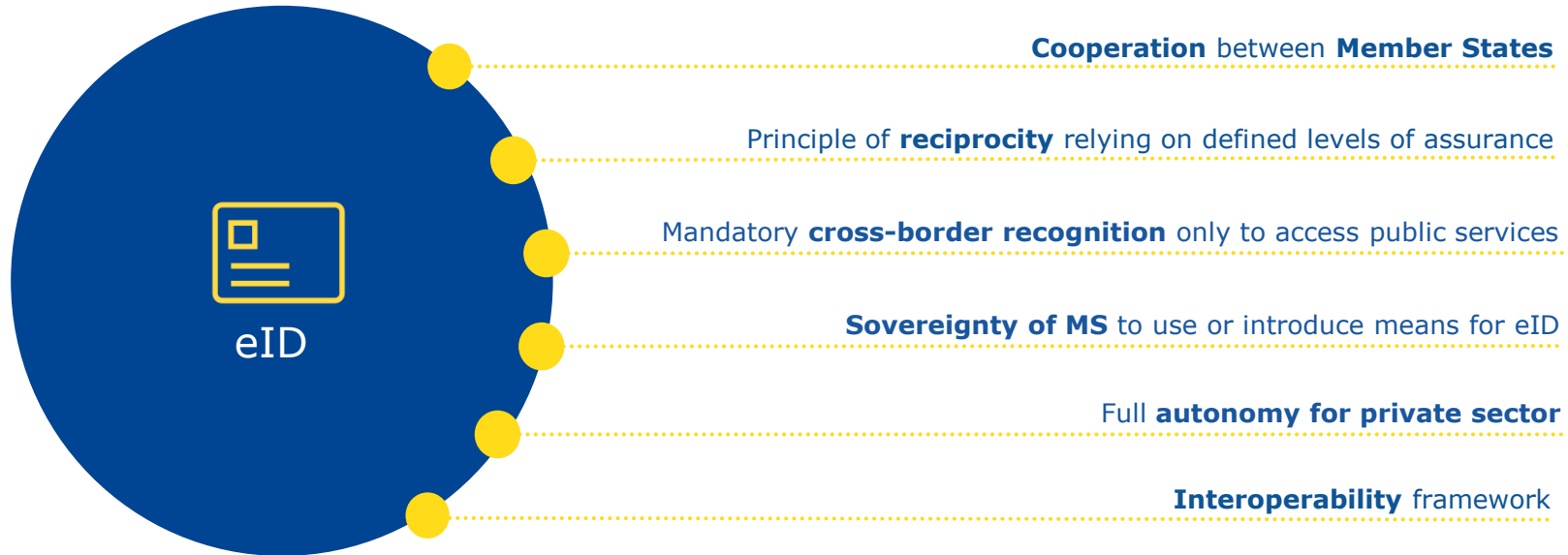
29.09.2018

Mandatory cross-border recognition

The eIDAS Legal Framework

	Legal Act	Reference	Adoption date	Entry into force
	eIDAS Regulation	910/2014	23.07.2014	17.09.2014 (1.07.2016 - application provisions on TS)
eID	ID on procedural arrangements for MS <u>cooperation</u> on eID (art. 12.7)	2015/296	24.02.2015	17.03.2015
	IR on <u>interoperability framework</u> (art. 12.8) Corrigendum C(2015) 8550 of 4.02.2016	2015/1501	8.09.2015	29.09.2015
	IR <u>assurance levels for electronic identification means</u> (art. 8.3)	2015/1502	8.09.2015	29.09.2015
	ID on circumstances, formats and procedures of <u>notification</u> (art. 9.5)	2015/1984	3.11.2015	5.11.2015 (notified to Ms)
Trust services	IR on <u>EU Trust Mark</u> for Qualified Trust Services (art.23.3)	2015/806	22.05.2015	12.06.2015
	ID on technical specifications and formats relating to <u>trusted lists</u> (art. 22.5)	2015/1505	8.09.2015	29.09.2015
	ID on <u>formats of advanced electronic signatures and seals</u> (art. 27.5 & 37.5)	2015/1506	8.09.2015	29.09.2015
	ID on <u>standards for the security assessment of qualified signature and seal creation devices</u> (art. 30.3 & 39.2)	2016/2303	25.04.2016	05.2016

eIDAS: Key principles for eID



*The Regulation does not impose the use of eID

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**

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

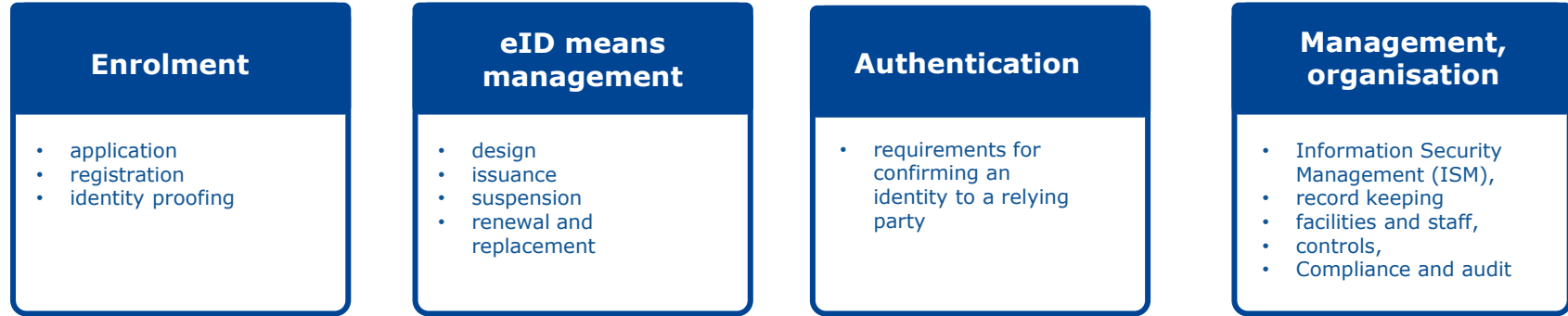
Only applicable to **schemes notified to the Commission** for cross border use

The **criteria** cover Identity Proof and Verification, the electronic means, issuance, authentication and information security management

Principles

Levels of Assurance - (EU) 2015/1502

Elements of Levels of Assurance



An example of differences between LoA: identity proofing

	<u>Level high:</u> substantial plus	<u>Level substantial:</u> low plus	<u>Level low</u>
Physical appearance at registration (including remote or at earlier stage)	<i>Required</i>	<i>Not required</i>	<i>Not required</i>
Verification of identity evidence	<i>Verified possession of valid identity evidence (like photo/bio)</i>	<i>Based on recognised evidence checked to be genuine. No direct verification of identity evidence assumed to be genuine</i>	<i>No direct verification of identity evidence assumed to be genuine</i>

Interoperability Framework - (EU)2015/1501, Corrigendum C(2015)8550

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")

eID schemes



EU MS and associated countries with nationally-issued eID schemes



Notified eID schemes

Germany

National ID card

40.000.000 registered users

26.09.2017

Pre-notified eID schemes

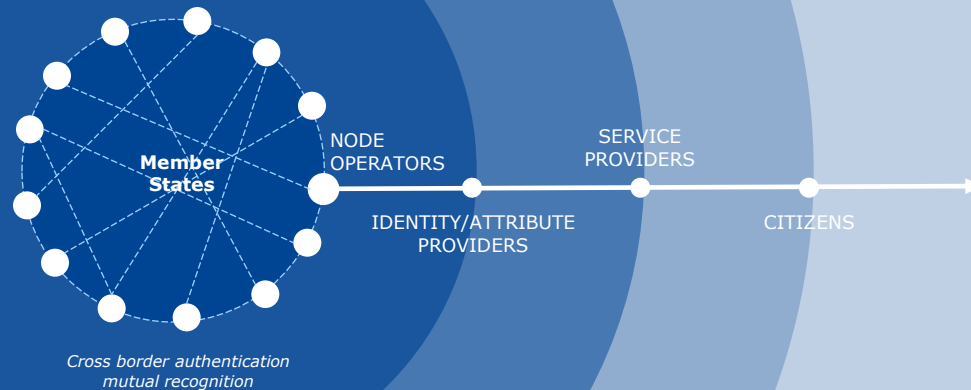
- Italy
- Spain
- Luxembourg
- Estonia
- Croatia

... and **10 more countries** are intending to pre-notify their schemes **by the end of 2018 !**

Part 2

How is eID under eIDAS implemented?

The eID ecosystem



The eID ecosystem



Node Operator

Entity responsible for ensuring that the eID node performs correctly and reliably its functions as a connection point.



Attribute Provider

Entity responsible for providing information about electronic identities (e.g. sector-specific information beyond the minimum dataset for natural and legal persons)



Identity Provider

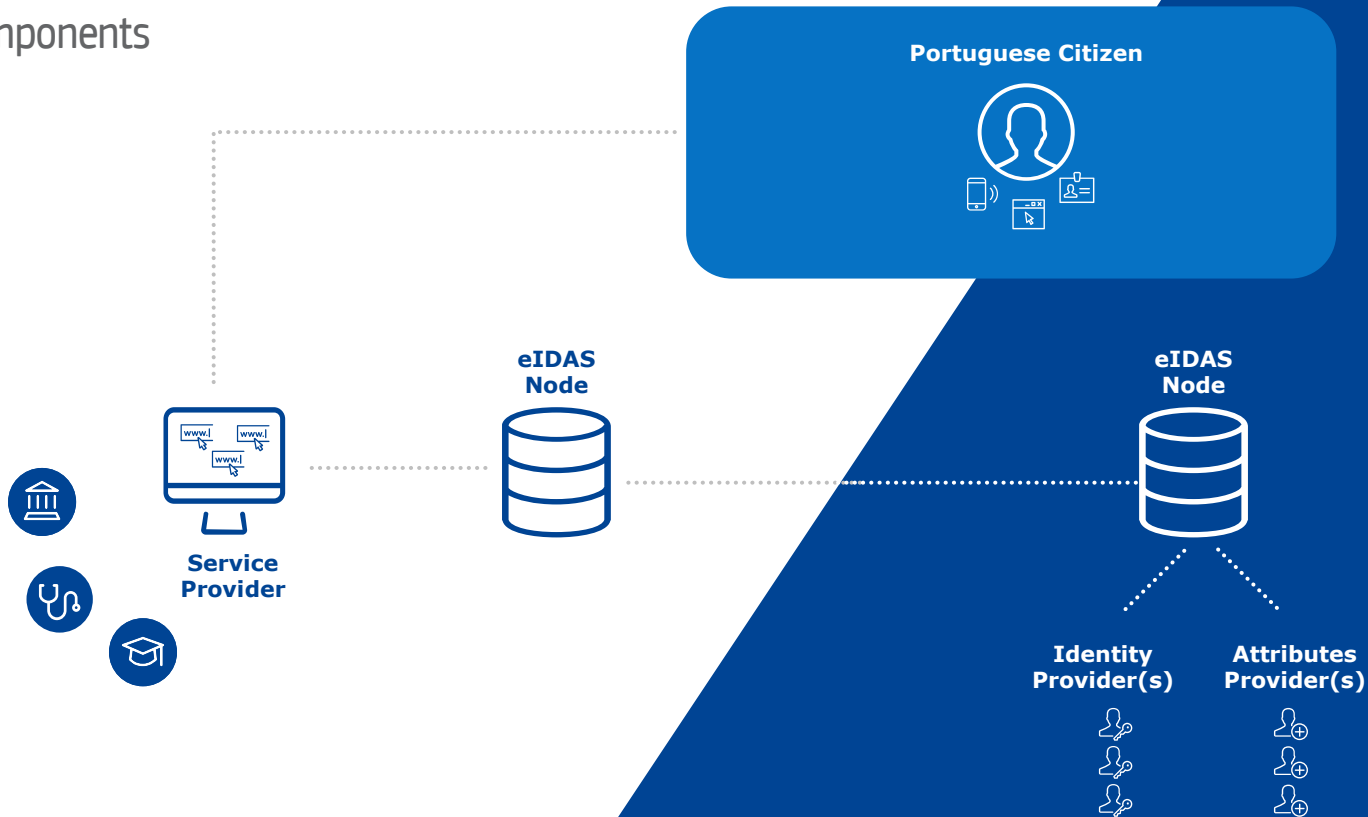
Entity responsible for verifying that a user is who they claim to be and assert verified data that identifies them to the relying party



Service Provider

Entity offering online services that rely on eID for cross-border authentication.

Components



FRANCE

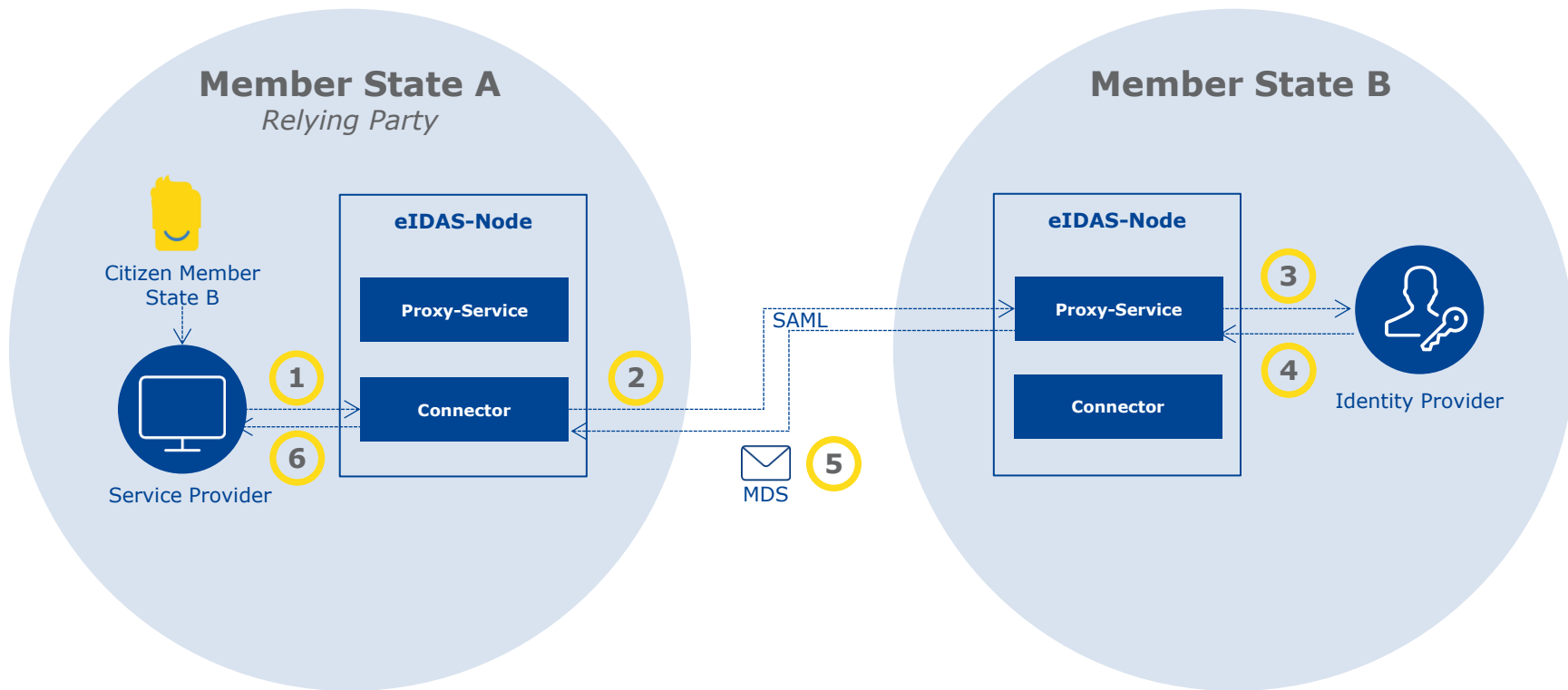
Portugal **issues** eID to its citizens for cross-border use

France **accepts*** eIDs issued by other Member States, like Portugal

PORTUGAL

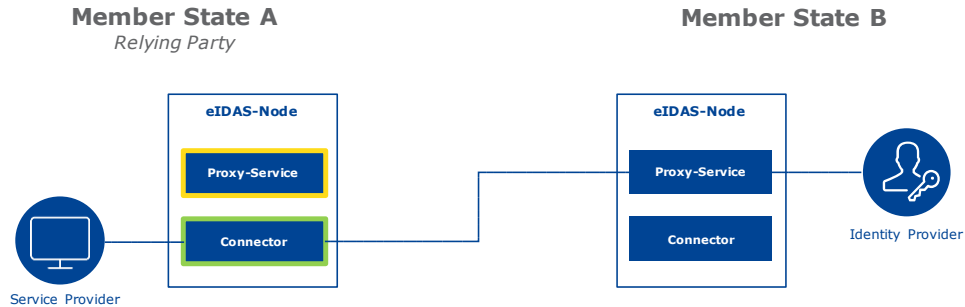
* Mandatory for eIDAS compliance

eIDAS Interoperability Architecture



eIDAS Compliance *for Node Operators (Member State)*

Interoperability Architecture



Connector

One or more connectors per Member State
(mandatory for mutual recognition of eID)

Proxy-Service

One Proxy-Service per Member State
(optional component operated when the MS notified one or more eID schemes)

Obligations

Legal

- ✓ Mutual recognition
- ✓ Liability of Member State

Organisational

- ✓ Notification of security breach
- ✓ Cooperation with other Member States
- ✓ ISO/IEC 27001 certification (or equivalent) or compliance with national legislation

Technical interoperability

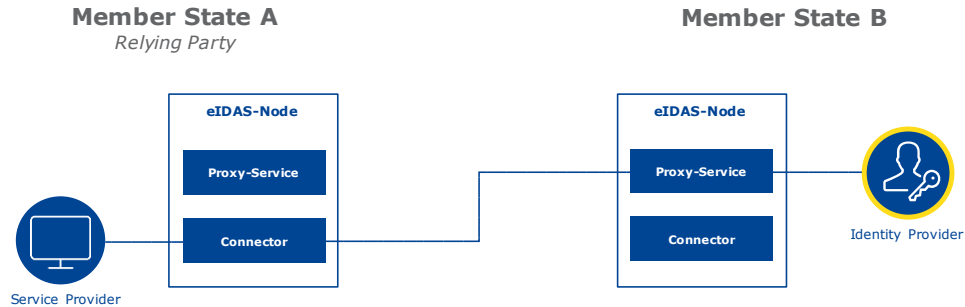
- ✓ eIDAS eID Profile

Operated by

- ✓ Public or private entities

eIDAS Compliance *for Identity Providers*

Interoperability Architecture



MDS – Minimum Data Set

Natural persons

Mandatory

Current Family Name
Current First Name
Date of birth
Unique Identifier

Optional: Name and family name at birth, current address, place of birth, gender

Legal persons

Mandatory

Current Legal Name
Unique Identifier

Optional: current address, VAT registration number, tax reference number, the identifier related to Article 3(1) of Directive 2009/101/EC , LEI, EORI, excise number

Obligations

Legal

- ✓ Liability of Member State

Organisational

- ✓ Notification of eID schemes
- ✓ Level of assurance based on enrolment, electronic identification, authentication and management/organisation of digital identities

Technical interoperability

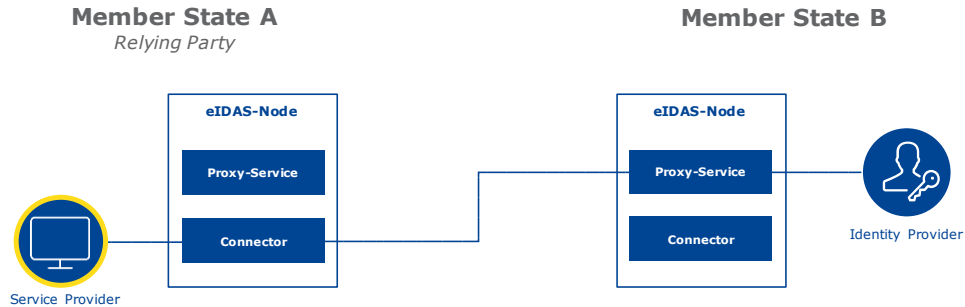
- ✓ At least MDS for natural and legal persons
- ✓ Member State specific interface with national infrastructure (proxy service)

Operated by

- ✓ Public or private entities

eIDAS Compliance *for Service Providers*

Interoperability Architecture



Obligations

Legal

- ✓ Mandatory for public entities offering online services to their citizens

Organisational

- ✓ Operational agreement with the responsible Member State

Technical interoperability

- ✓ Member State specific interface with national infrastructure (connector)
- ✓ Public and private service providers may need to connect to different connectors

Operated by

- ✓ Public or private entities

Countries in process of implementing an eIDAS compliant Node

- Countries setting-up an eIDAS compliant Node:
AT*, BE*, CZ*, DE, DK*, EE*, EL*, ES*, FR, HR*, HU, IR, IS, IT*, LT, LU*, LV*, MT*, NL*, NO*, PL*, PT, SI, SK, SE, UK*
- Countries planning national eIDAS Node implementation:
BG, CY, FI, RO, TR

** countries that expressed intent to use CEF eID sample implementation*



Connecting Europe Facility (CEF)



TRANSPORT
€26.25bn

ENERGY
€5.85bn

TELECOM

WiFi4EU
€120 m

Broadband
€170 m

Digital Service Infrastructures
€703m

2014 to 2020

Infrastructure programme to support the establishment of trans-European networks to reinforce an **interconnected Europe**

The deployment of **Digital Service Infrastructures** supports the development and smooth functioning of the **Digital Single Market** by :

- enabling the delivery of networked trans-European interoperable services for citizens, businesses and/or governments
- supporting the vision of public services being not only digital by default but also cross-border by default

What does CEF Digital finance?

DIGITAL SERVICE INFRASTRUCTURES (DSIs)

Funding for the
EUROPEAN COMMISSION

Funding for the
MEMBER STATES



CORE SERVICE PLATFORM

Services offered by the European Commission

SECTORIAL



eJustice Portal



EU Open Data Portal

...

BUILDING BLOCKS

eInvoicing



eSignature



eDelivery



eID



eTranslation



e Archiving



GRANTS

Projects in the Member States



Building block DSIs provide basic functionality and are reusable by sector-specific DSIs

2018 CEF eID and eSignature call

CEF eID: helps public administrations and private Service Providers to extend the use of their online services to citizens from other European countries, by allowing them to identify and authenticate using their national eID, according to the eIDAS regulation.

CEF eSignature: helps public administrations and businesses to accelerate the creation and verification of electronic signatures, facilitating the mutual recognition and cross-border interoperability of trust services, according to eIDAS.

- Budget: indicative 8 M euros
- 7,5 M eID, 0,5 M eSignature
- Co-funding rate: 75%
- Pre-financing: 50%
- Indicative duration of the actions: 18 months

More information about the calls?

- See the article on [CEF Digital](#) □
- For practical details of the calls, please check the [virtual info day page](#)
- Check regularly the Twitter account @inea_eu and [LinkedIn page](#) where updates of the calls are published.
- There is also a [LinkedIn group](#) that helps potential applicants find partners for their consortia.

2018 CEF eID and eSignature call

eID objectives



1. eID DSI integration:

Integrating the eID DSI (Digital Service Infrastructures) in existing e-services/systems/online platforms in various public or private sectors.



2. Attributes enablement:

Enabling attributes, mandates and authorities to be associated with electronic identities for cross-border use through the eIDAS node.



3. Student mobility:

Supporting student mobility by enabling students to identify themselves in a trusted manner across borders and thus benefit from the 'Once Only Principle' in higher education institutions, in line with European eStudent Card initiative

Part 3

How eIDAS is changing the eID
landscape?

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

AML5

5th Anti-Money Laundering Directive (**Agreed on 20 December 2017**)



An example: the financial sector

- On 27 November → adoption of [Delegated Regulation on Regulatory Technical Standards \(RTS\)](#) on strong customer authentication and common and secure communication for PSD2
 - **reference is made to both eIDAS notified eID means and trust services.**
 - **eIDAS notified eID means → possible solution for strong customer authentication**
 - **Qualified electronic seals or qualified website authentication certificates mandatory for the communication between payment providers.**
- On 14 December → adoption of [Commission Decision C\(2017\) 8405 final](#) setting up the Commission expert group on electronic identification and remote Know-Your-Customer processes
 - **Jointly managed by DG CNECT, DG FISMA and DG JUST**
 - **composed of up to 36 members comprising regulators, supervisors, identity experts, financial institutions and consumer organisations → Call for applications closed on 26.01**
 - **explore how to facilitate the cross-border use of eID and KYC portability based on identification and authentication tools under eIDAS to enable financial institutions to identify customers digitally for onboarding purposes**
- On 20 December → political agreement on revised text of the [Anti-Money Laundering Directive \(AMLD5\)](#)
 - **explicit reference to eIDAS notified eID means as a possible way to fulfil Know-Your-Customer/Customer Due Diligence requirements for non-face-to-face interactions**

Digital on-boarding

Customer initiates enrolment procedure

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



Notified eID under eIDAS →

1. Identity verification

2. Customer Due Diligence/Business Relationship

3. Check against fraud risk

Minimum data set:

- current family name
- current first name
- date of birth
- unique identifier

Depend on bank/national applicable rules on CDD/KYC

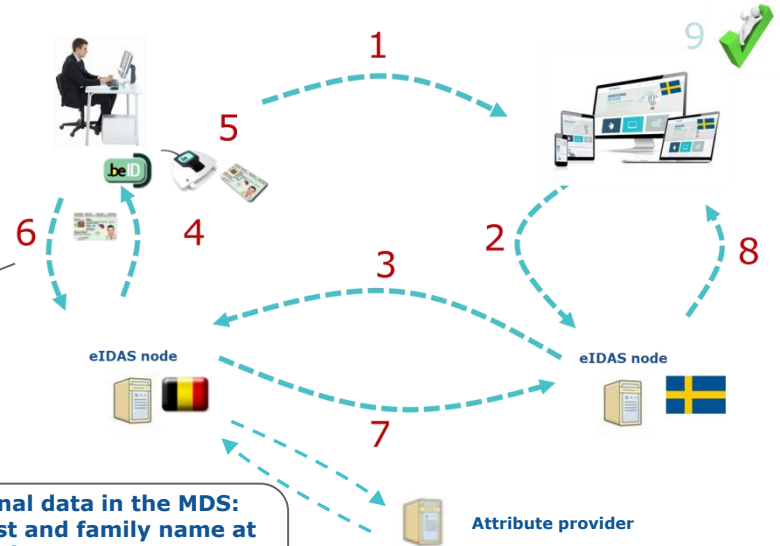
Optional data in the MDS:

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

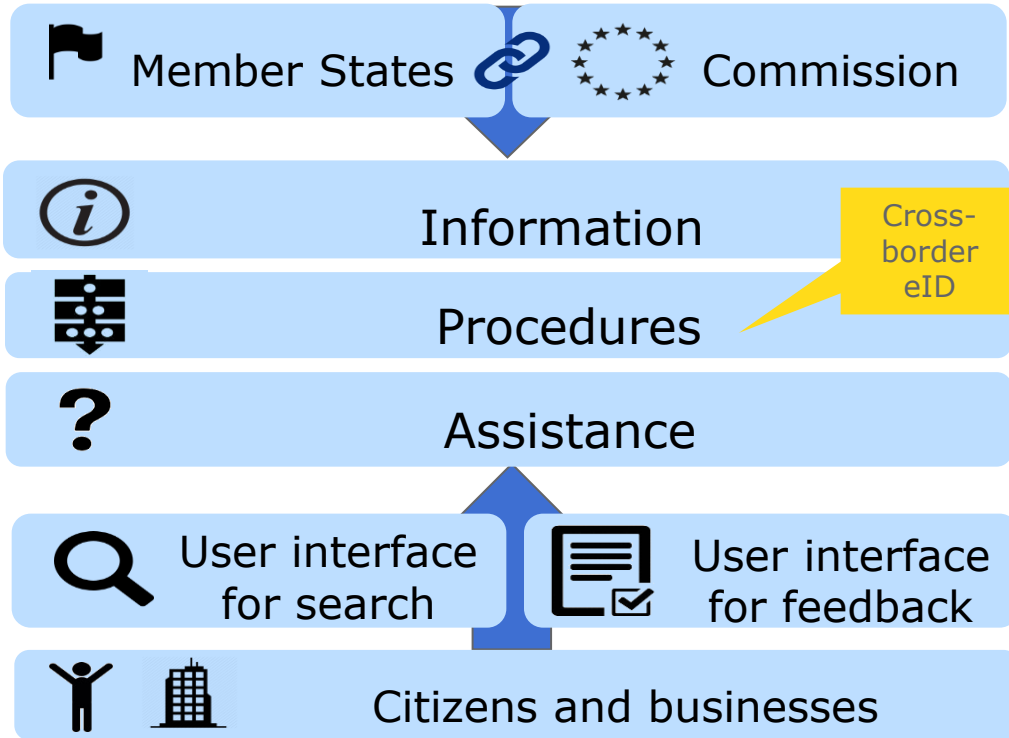
Domain specific attributes:

- Profession
- Social Security Number
- Politically Exposed Person

How cross-border eID/authentication works



Single digital gateway



What is the added value?

- ✓ Cross-silo approach
- ✓ Fully user-centric
- ✓ Non-duplication
- ✓ Fill online information gaps
- ✓ Fill quality gaps
- ✓ Improve findability
- ✓ Most used procedures online
- ✓ Full cross-border accessibility

eIDAS and GDPR

- **eIDAS Regulation**

- Article 5: Data processing and protection

1. Processing of personal data shall be carried out **in accordance with Directive 95/46/EC**.
2. Without prejudice to the legal effect given to pseudonyms under national law, **the use of pseudonyms in electronic transactions shall not be prohibited**.

- **eIDAS Interoperability Framework**

- Article 6: Data privacy and confidentiality

1. **Protection of privacy and confidentiality** of the data exchanged and the maintenance of data integrity between the nodes shall be ensured by using best available technical solutions and protection practices.
2. The **nodes shall not store any personal data, except** for the purpose set out in Article 9(3).

- Article 9(3): Management of security information and metadata

The node operator shall store data which, in the event of an incident, **enable reconstruction of** the sequence of the message exchange for establishing the **place and the nature of the incident**

- **GDPR**

- **Lawful processing:** Legitimate interest, explicit consent, executing an agreement, legal obligation, vital interest, general interest
- **Data minimisation**

Trusted eID

- eID notified under eIDAS as "trusted eID"
 - Strict procedures for identity verification
 - Strong authentication through more than one factor (LoA substantial and high)
- "Trusted eID" as the primary source of eID
 - Occasional access to services
 - Trust anchor for derived eID
- Data minimisation
 - Trusted eID for proving the age
- **Final draft principles and guidance on eID interoperability for online platforms**
 - To allow and facilitate online platforms users, if they wish so, to rely on their own government-issued/recognised eID means whenever the access to online platforms may require electronic identification or authentication steps



eID and mobile



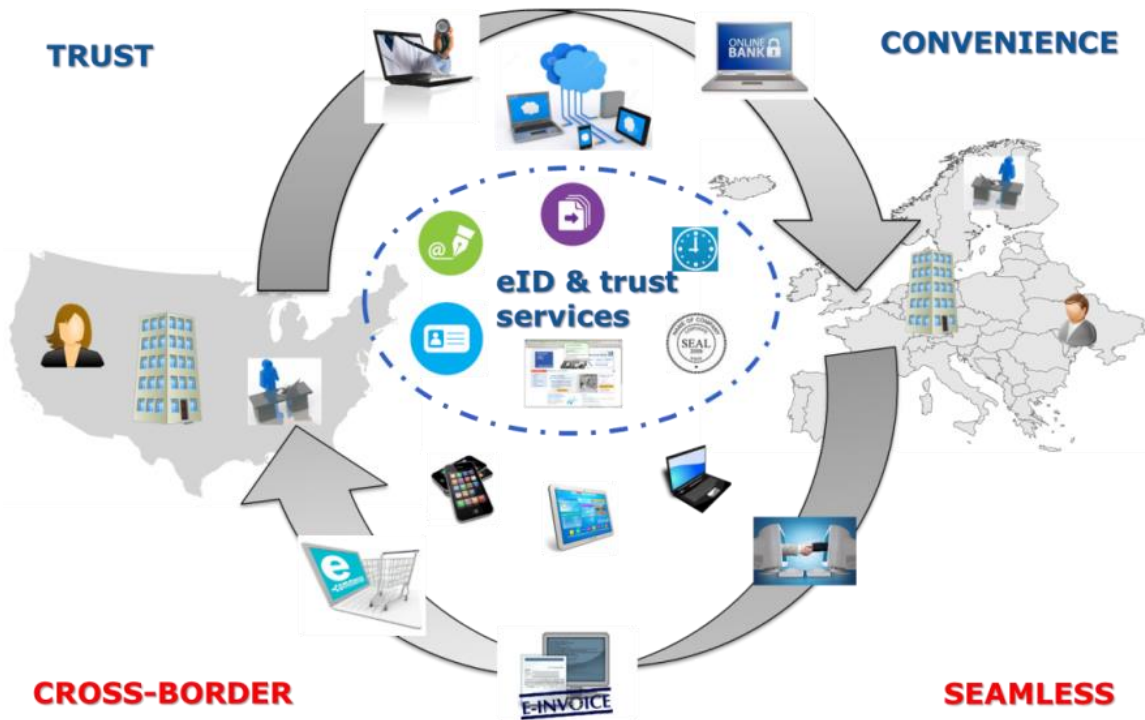
Building trust in the online world is crucial to accomplish the Digital Single Market. Coupling mobile authentication credentials, such as Mobile Connect, with the identity security provided by eIDs under the eIDAS Regulation, is the way towards this goal

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

#eIDAS
@eID_EU



eIDAS beyond EU



EU the first and only region in the world to have:

- Policy
- Regulation
- Rules
- Technology
- Interoperability infrastructure

Promote the eIDAS framework globally!

For further information and feedback

Web page on eIDAS

<http://ec.europa.eu/digital-agenda/en/trust-services-and-eid>

eIDAS Observatory

<https://ec.europa.eu/futurium/en/eidas-observatory>

Text of eIDAS Regulation in all languages

<http://europa.eu/!ux73KG>

eIDAS twitter account

[@EU_eIDAS](https://twitter.com/EU_eIDAS)

Connecting Europe Facility Catalogue of Building Blocks

The screenshot shows the 'eID' section of the CEF Digital website. The header includes the European Commission logo, 'CEF DIGITAL', and a search bar. The main navigation bar lists 'Home', 'Discover', 'How it works', 'Services', and 'Collaboration'. The content area is divided into three columns: 'About', 'Latest News', and 'Grants'. The 'About' section describes the CEF eID project's goal to help public administrations and private online service providers extend the use of their services to citizens from other EU Member States. It mentions funding of EUR 4 million over 4 years, with DG INTECT as the business owner and DIGIT as the solution provider. The 'Latest News' section lists three items: 'Live Webinar: eID under eIDAS: compliance, state of play and technology', 'Key Milestone Reached! First Cross-Border Connections Between technically compliant eIDAS Nodes in Production', and 'eIDAS Technical Specifications v. 1.1'. The 'Grants' section lists 'CEF-TO2017-1: eIdentification & eSignature' with an indicative budget of EUR 7 million and a call open to be confirmed. Below the news and grants are three yellow buttons: 'Discover eID >', 'All the latest >', and 'More information >'. A section titled 'Implementing eID' follows, stating that the implementation journey is divided into four steps. These steps are represented by icons and text: 1. 'Discover' (magnifying glass icon) - Understand what CEF eID is about, its legal context and how it can benefit public administrations. 2. 'How it works' (gears icon) - Evaluate the suitability of adopting CEF eID by understanding its IT architecture. 3. 'Services' (document icon) - Access and download the software, documentation and services provided to implement CEF eID. 4. 'Collaboration' (people icon) - Spaces to collaborate and discuss the CEF Building Blocks (Coming Soon).



ec.europa.eu/cefdigital