European Commission

Introduction to the Connecting Europe Facility

eID building block

DIGIT
Directorate-General for Informatics

DG CONNECT
Directorate-General for Communications Networks, Content and Technology

March 2016

eID connecting europe

DISCLAIMER

This document is for informational purposes only and the Commission cannot be held responsible for any use which may be made of the information contained therein. References to legal acts or documentation of the European Union (EU) cannot be perceived as amending legislation in force or other EU documentation.

The document contains a brief overview of technical nature and is not supplementing or amending terms and conditions of any procurement procedure; therefore, no compensation claim can be based on the contents of the present document.

Introduction to the Connecting Europe Facility eID building block

Created by: CEF eID

DOCUMENT HISTORY

Version	Date	Modified by	Short Description of Changes
1.04	30/03/2016	CEF eID	Published

Table of contents

Audience

This document describes the Electronic Identification (eID) building block which is one of the Connecting Europe Facility (CEF) Digital programme's essential digital services. These essential digital services, called building block Digital Service Infrastructures (DSIs) will play a vital role in the flow of data across borders and sectors.

The document will help Service Providers, Service Operators and Implementers who are interested to better understand the CEF eID facility. In particular it provides information on the background, terminology, concepts, roles, components, connectivity, features and architecture of the CEF eID.

This document is intended for the following audiences:

SERVICE PROVIDERS

interested in integrating in an existing online platform of this eID DSI in order to enable citizens from any Member State to use its national eID to access a public service

SERVICE OPERATORS

interested in operating the Pan-European Proxy Services (eIDAS-Nodes) at national level in order to guarantee the availability of the service for the first years of operation

IMPLEMENTORS

interested in setting-up Pan-European Proxy Services (eIDAS-Nodes) at national level in order to link the national eID service to the core platform.

Whilst every effort has been made to ensure that the information contained in the document is correct, any comments on it should be submitted to the European Commission: *CEF-BUILDING-BLOCKS@ec.europa.eu*

1 Introduction

What is CEF eID?

Introduction to CEF eID

The CEF eID building block helps public administrations and private online service providers to easily extend the use of their online services to citizens from other EU Member States. It allows cross-border authentication, in a secure, reliable and trusted way, by making national electronic identification systems interoperable.

Once this building block is deployed in a Member State, the mutual recognition of national eIDs becomes possible between participating Member States, in line with the eIDAS (electronic Identification and Signature) legal framework (see eIDAS Regulation (EU) 910/2014) and with the privacy requirements of all the participating countries. Mutual recognition of national eIDs allows citizens of one Member State to access online services provided by public and private organisations from other participating EU Member States, using their own national eID.

Following the successful completion of the STORK pilot programme (as described in section 2 of this document), CEF has taken on the role to 'productise' and support roll-out of eID connectivity to other Member States. This has included the development of open-source software components, documentation, training and support. Member States can leverage their electronic ID systems to provide access to the services of other Member States with confidence in the levels of assurance provided by secure means of authentication linked to qualified identities.

More information about the CEF Telecom policy background, its Work Programmes and related information is available on the Digital Agenda website.

More information about eID is available on the CEF Digital Single Web Portal.

For information on the governance structure of CEF eInvoicing, please see the Non-paper on the IT Governance of CEF Building Blocks

The technical management of the eID building block DSI is done by the Directorate-General for Informatics (DIGIT) of the European Commission.

Implementation of the EU policy directly related to eID and Trust Services is the responsibility of the Directorate-General for Communications Networks, Content and Technology (DG CNECT) of the European Commission.

The Innovation and Networks Executive Agency (INEA) is responsible for the implementation of the CEF Telecom programme grants in cooperation with the Commission.

Introduction to CEF eID

Electronic identification (eID) and electronic Trust Services (eTS) are key enablers for secure cross-border electronic transactions and central building blocks of the Digital Single Market.

The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (**eIDAS Regulation**) adopted by the co-legislators on 23 July 2014 is a milestone to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. The eIDAS Regulation, which is based on the Commission Communication (COM(2012)238 final of 4 June 2012), will increase the effectiveness of public and private online services, eBusiness and electronic commerce in the EU.

eID and eTS - namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication - are inseparable by essence when analysing the requirements needed to ensure legal certainty, trust and security in electronic transactions.

In this regard, the eIDAS Regulation:

ensures that people and businesses can use their own nationally issued electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available.

creates a European internal market for eTS by ensuring that they will work across borders and benefit from a specific legal effect as well ads will not be discriminated with regard to their equivalent paper based processes. Only by providing certainty on the legal validity of all these services will businesses and citizens use these digital interactions as their natural way of interaction.

Benefits of CEF eID

Below is an overview of the expected **benefits** to the individual Projects and Policy Domains:

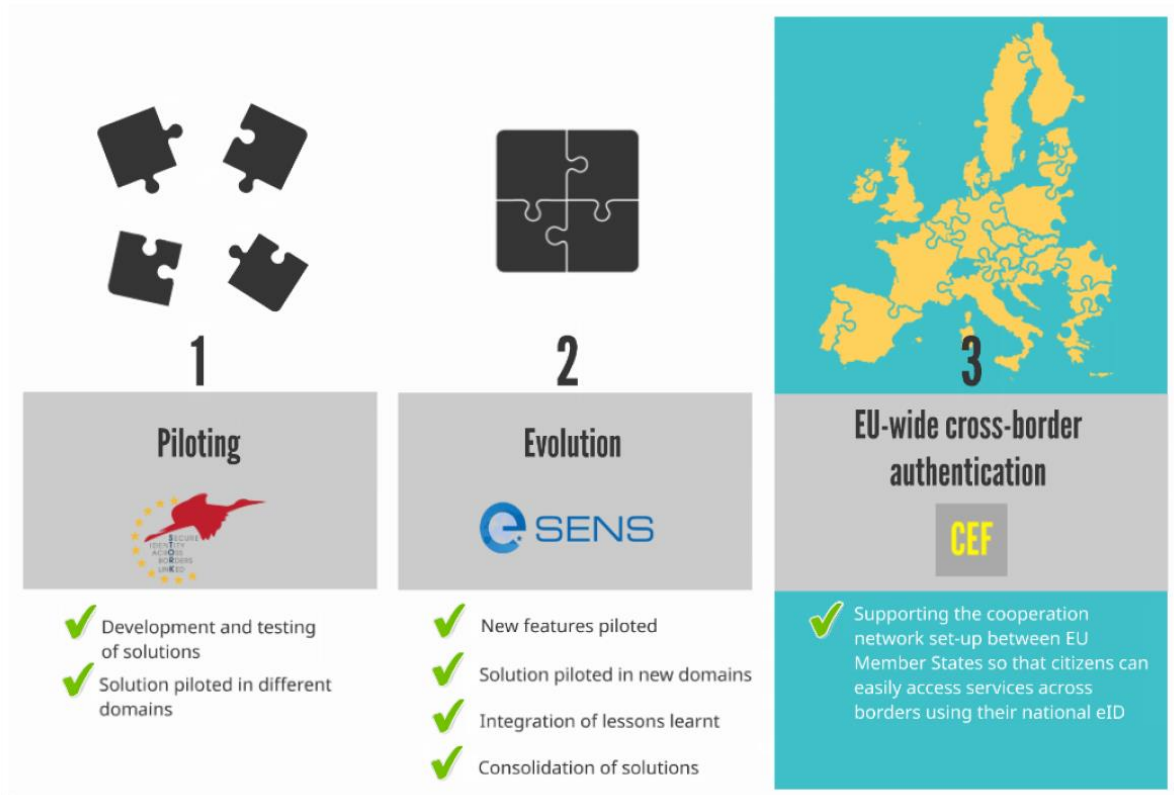
2 Context

What is CEF Digital?

Context

The story of cross-border eID authentication can be viewed in the context of a number of Large Scale Pilots (LSPs), the work, results and lessons of which play an important role in CEF eID.

This section will explore these Large Scale Pilots in some more detail (see Section 9 of this document for eID Success Stories).



Context – STORK beginnings

Cross-border eID interoperability is a complex and multi-disciplinary issue covering legal, operational, semantical and technical aspects.

To meet this challenge the European Commission initiated and co-funded an eID Large Scale Pilot under the Competitiveness and Innovations Framework Programme, ICT Policy Support Programme (CIP, ICT-PSP). This initiative resulted in STORK – which stands for Se-cure identiTy acrOss boRders linKed.

STORK was a Large Scale Pilot aiming at solving the issues of cross-border interoperability of eID. The basic assumption was to build a modular technological infrastructure on top of national eID infrastructures.

Two models are used by countries involved with STORK:

- proxy
- middleware

The decision of which model to follow depends on the country. It may be based on weighing a number of considerations, including:

- liability
- scalability
- data protection
- legal requirements
- end-to-end security

Context - e-SENS & CEF

e-SENS (Electronic Simple European Networked Services) is a large-scale project with the aim of consolidating, improving, and extending technical solutions based around the building block DSIs to foster digital interaction with public administrations across the EU.

e-SENS will facilitate cross-border processes within the EU by:

- making it easier for companies to set up business electronically;
- enabling electronic procurement procedures for businesses;
- creating seamless access to EU legal systems;
- making it easier to use healthcare services abroad in cases of emergency.

e-SENS is piloting the use of building blocks including eID to develop the digital infrastructure for improving the quality of public services in the EU.

CEF incorporates improvements resulting from the pilots, and packages the solution with documentation, training and support, before making it available for deployment by Member States.

For more information on how e-SENS and CEF work together, please refer to the CEF Digital Single Web Portal.

Context – CEF eID

The eID DSI met the eligibility criteria of the CEF in 2014 and was, as a result, included in the CEF Telecom Work Programme 2014. The operation of the eID core service platform is therefore ensured for 4 years, until 2018, with a budget of EUR 4 million.

Parts of the funding under CEF have been made available in the form **of grants allocated following competitive Calls for Proposals**. Proposals shall be **submitted by one or more Member States or**, with the agreement of the Member States concerned, by **international organisations, joint undertakings, or public or private undertakings or bodies established in Member States.**

According to the CEF regulation, the grants should not exceed 75% of the eligible costs. These calls will be published on the website of the Innovation and Networks Executive Agency (INEA).

3 Motivation

Why should you reuse eID?

Motivation

CEF eID is based on a mature eID solution (see Chapter 2) tested in a cross-border scenario.

The CEF eID solution can assist **compliance with the eIDAS Regulation** (which ensures legal interoperability by providing a clear regulatory framework).

While the eIDAS regulation provides the basis for **Legal Interoperability**, the CEF Operational Management Board provides **Organisational Interoperability**, the CEF solution also ensures **Semantic** and **Technical Interoperability**, including the technical and operational security requirements coming from the eIDAS Implementing acts.

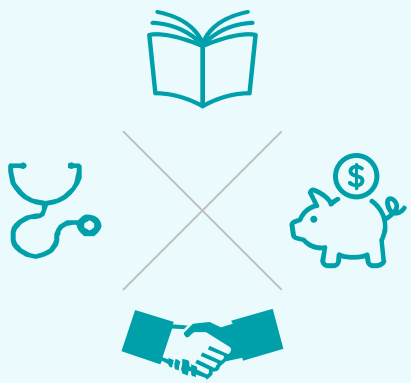
But what does this mean in reality? Below we look at some real life examples of where an eID solution could be used.

eLearning

As more and more Europeans learn, study and teach across national borders, an interoperable eID solution allows academic services to be provided to students, even if the services concern an individual in one Member State, using services in another.

eHealth

Little information is more sensitive than that concerning our health. An interoperable eID solution ensures that patient's medical records and personal information is securely exchanged when required to across national borders. Such a solution will also support in the verification of a Health Care Professional's identity and professional credentials.



eBanking

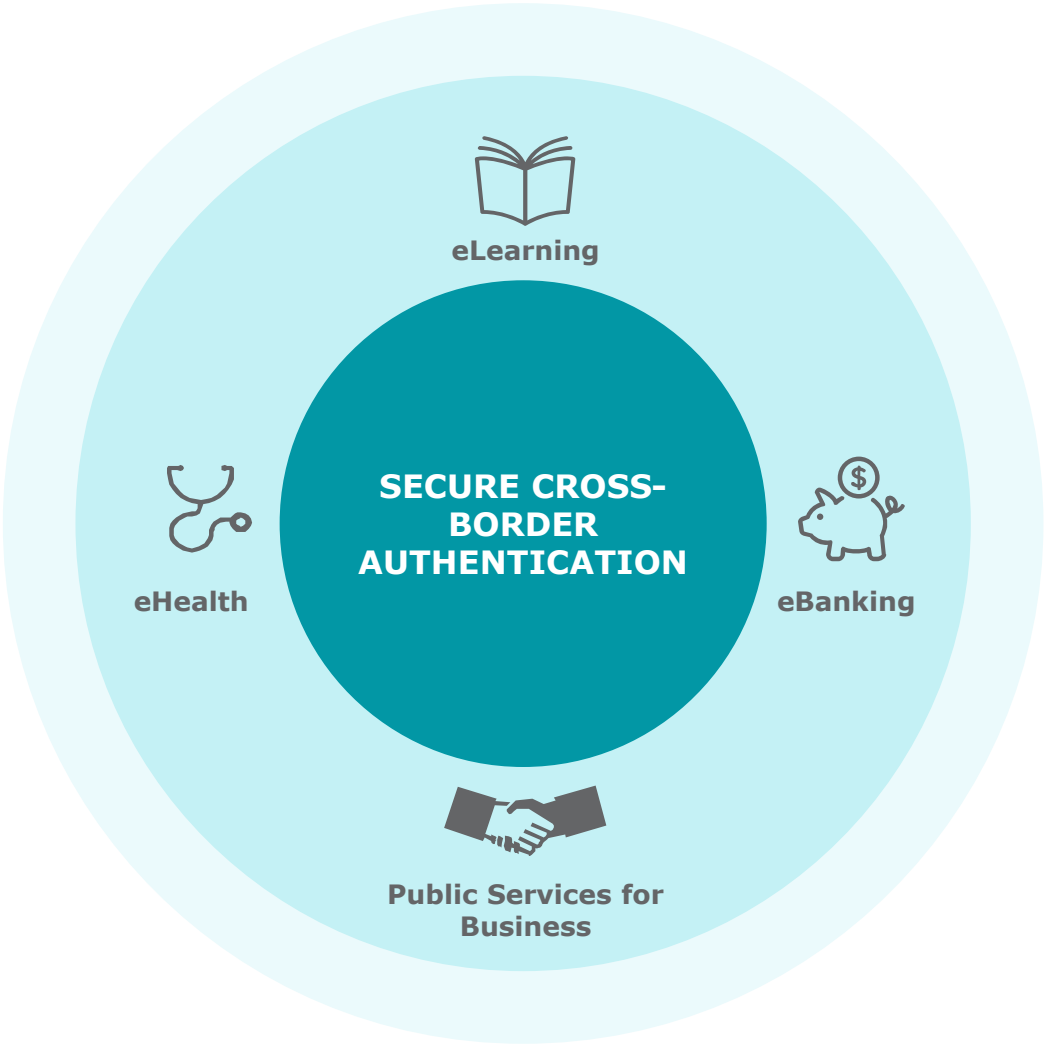
When moving as a citizen or as a business to a new country, setting up bank accounts remains a significant burden. An interoperable eID solution facilitates the identification process when opening new bank accounts.

Public Services for Business

Public administrations, from European to local level, provide various services to businesses. An interoperable eID solution allows national eID schemes to be used by business and legal representatives in the validation of information concerning Business Registers or Single Points of Contact.

Motivation – Goal

These domain-specific examples – and the many more beyond – all have one key requirement, the **overarching goal of the eID solution**.



Secure cross-border authentication is then achieved by **Legal** Interoperability (eIDAS), **Organisational** Interoperability, **Semantic** Interoperability and and **Technical** interoperability (provided by CEF).

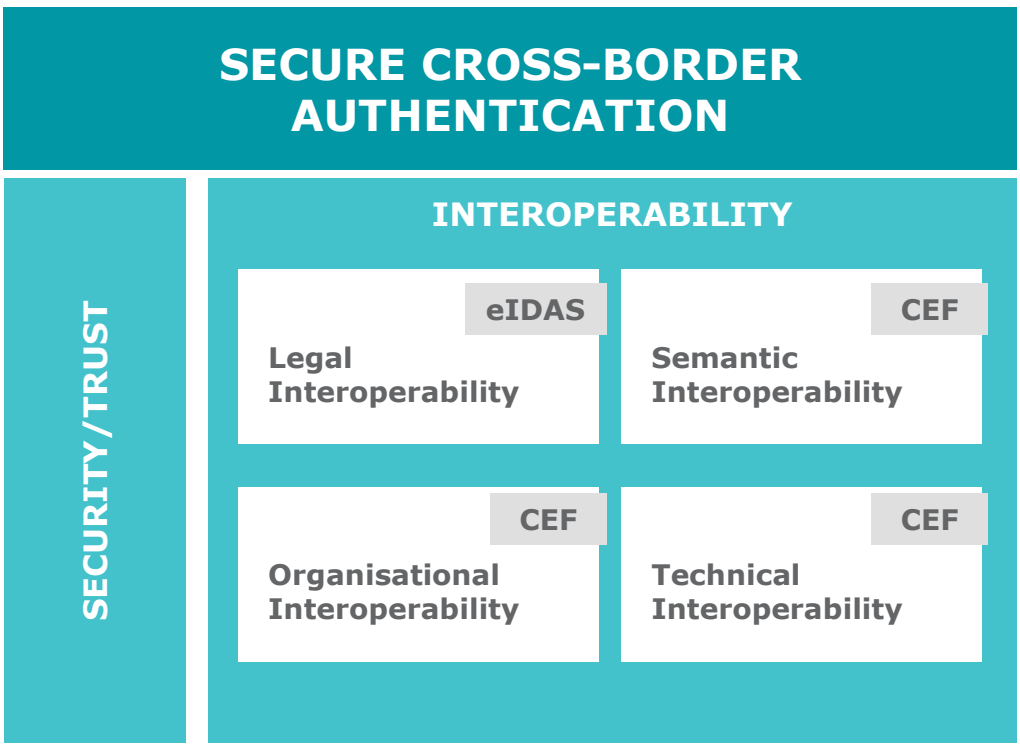
Motivation

In addition to the overarching goal of CEF eID, there are the specific business needs that it helps to achieve.

More than twenty European countries currently have eID systems in place. These systems protect electronic services mostly pertaining to the public sector, but in some cases also covering commercial applications. They all have varying security mechanisms for identification and authentication, and are based on different philosophies which lack cross-border recognition and validation, thereby fragmenting the Single Market.

In this context, and aligned with the efforts to strengthen the digital single market, the trans-European availability of widespread and secure access to the internet and digital services is essential if Europe is to reap the full benefits of this technological revolution.

Below are the **business needs** that eID helps to tackle:



eIDAS
Interoperability level provided by eIDAS

CEF
Interoperability level provided by CEF

Motivation

In details, here are the goals that eID helps achieve:

Goal	**Secure Cross-Border Authentication**			
Business Needs	**Legal Interoperability**	**Organisational Interoperability**	**Semantic Interoperability**	**Technical Interoperability**
What it's about	**Providing a legal basis, and therefore legal obligation, for the recognition of eIDs across boarders (respecting data protection legislation in both originating and receiving countries)**	**Clarifying and detailing the organisational relationship between the different Member States and the necessary operational management related process**	**Ensuring that the electronic identification information exchanged in a cross-border scenario is transmitted in a meaningful way to and from external sources to ensure that the precise meaning of exchanged information is understood and preserved throughout exchanges between parties**	**Ensuring that the technical elements of cross-border eID authentication are compatible - when interconnecting the different national eID solutions, it should be technically possible to link the different eID information systems**
Example	*National eID solutions have been developed following the national legislation. Cross-border legal validity cannot foster trust across borders without the possibility to use nationally issued eIDs across incompatible legal frameworks.*	*Once the national eID solutions have been interconnected, without compatibility between the organisational elements between Member States (such as change management, release management)* cross-border authentication cannot be guaranteed.	*National eID solutions have developed the message format and independently*	*It should be possible to guarantee the unambiguous identification of users of online services.*

Motivation

What are the technical use cases?

Having established the goal of the eID solution and the related business needs, the technical use cases (i.e. user centric views of what CEF eID can offer / how it can help) must be examined.

The 'eIDAS-Network' consists of eIDAS-Nodes, which can either **request (via an eIDAS-Connector)** or **provide (via an eIDAS-Service)** a cross-border authentication.

In the case of the eIDAS-Service Node, this may be operated in two different ways:

- **eIDAS-Proxy-Service**: an eIDAS-Service operated by the Sending Member State and providing personal identification data.
- **eIDAS-Middleware-Service**: an eIDAS-Service running Middleware provided by the Sending Member State, operated by the Receiving Member State and providing personal identification data.

1

User from a **proxy country** accessing a service in another **proxy country**

2

User from a **Middleware country** accessing a service in a **proxy country**

3

User from a **proxy country** accessing a service in a **Middleware country**

4

User in a **Middleware country** accessing a service in another **Middleware country**

4 Technical Use Cases

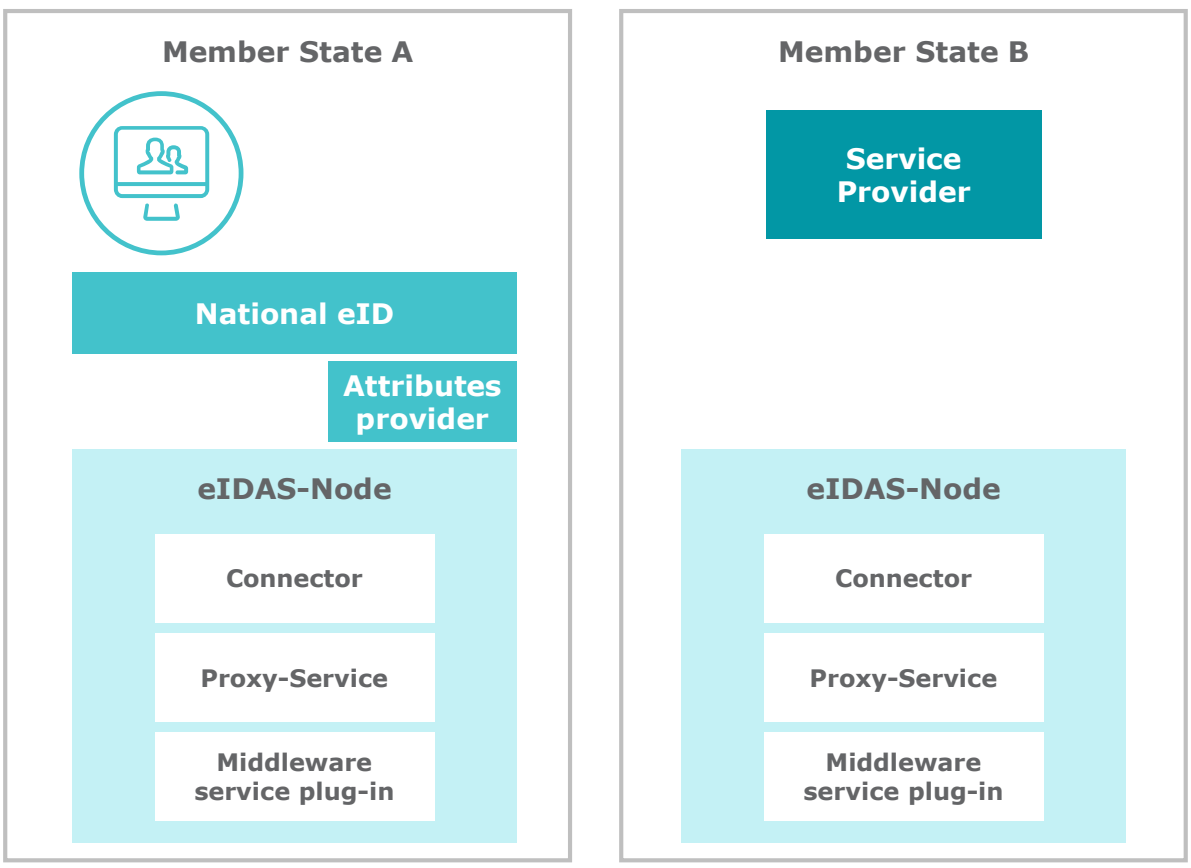
A deep-dive into CEF eID

Use cases

The eIDAS solution has been developed to accommodate a variety of national/international schemes to maximise interoperability. The following sections contain scenarios of flows in certain use cases. Before deep diving into the 4 use cases, it is important to mention which are the components that come into play.

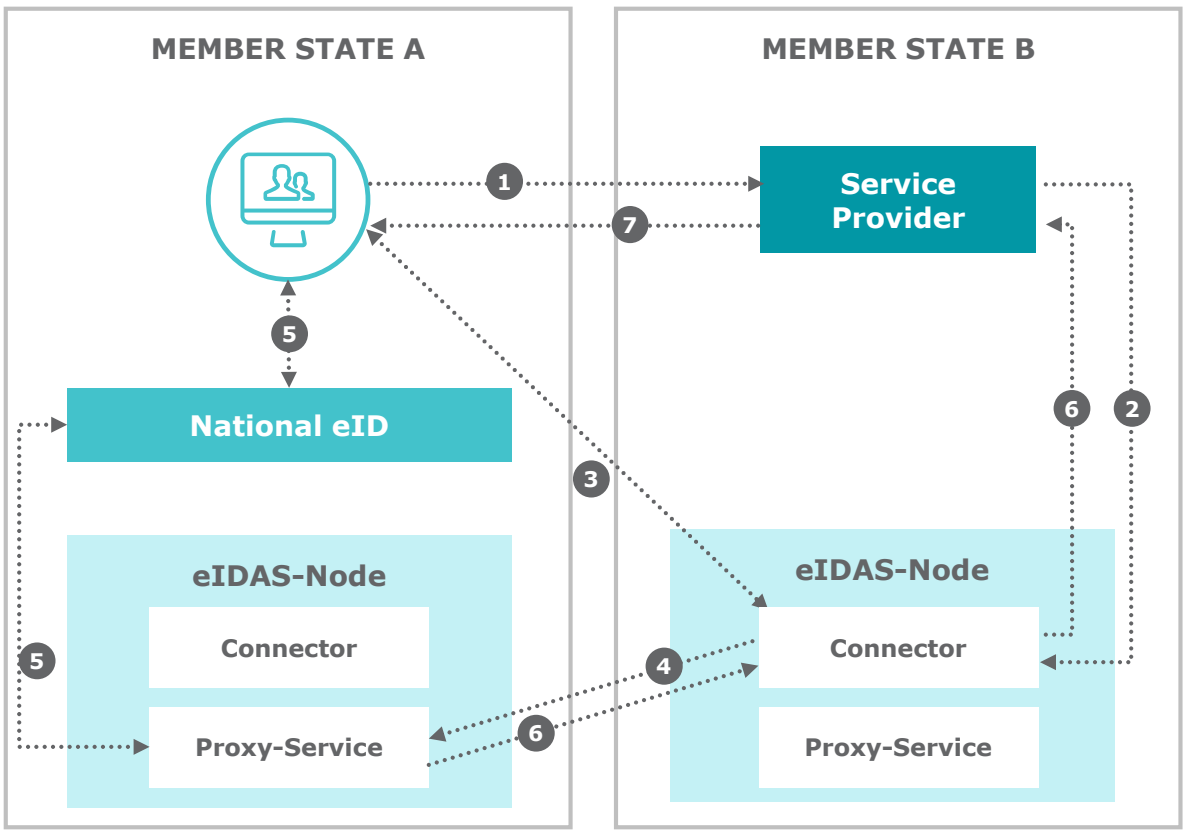
The diagram below illustrates the main components in an eIDAS solution. It shows:

- Two **Member States**, **MS** A and MS B both of which are 'proxy countries', i.e. they do not operate their own Middleware.
- A user (citizen).
- A Service Provider (SP) (public administrations and private online service providers).
- The eIDAS-Node in the Member State of the target Service Provider.
- The eIDAS-Node in the Member State of the user. Conceptually, each eIDAS-Node consists of:
    - four interfaces.
    - a Connector (formerly known as an S-PEPS).
    - a Proxy Service (formerly known as a C-PEPS).
    - one or more MS middleware service plugins (optional) for communication with middleware countries (formerly known as VIDP).
- The National electronic Identity Provider of the user's Member State.
- The Attributes Provider of the user's Member State.



User from a proxy country accessing a service in another proxy country

1 2 3 4



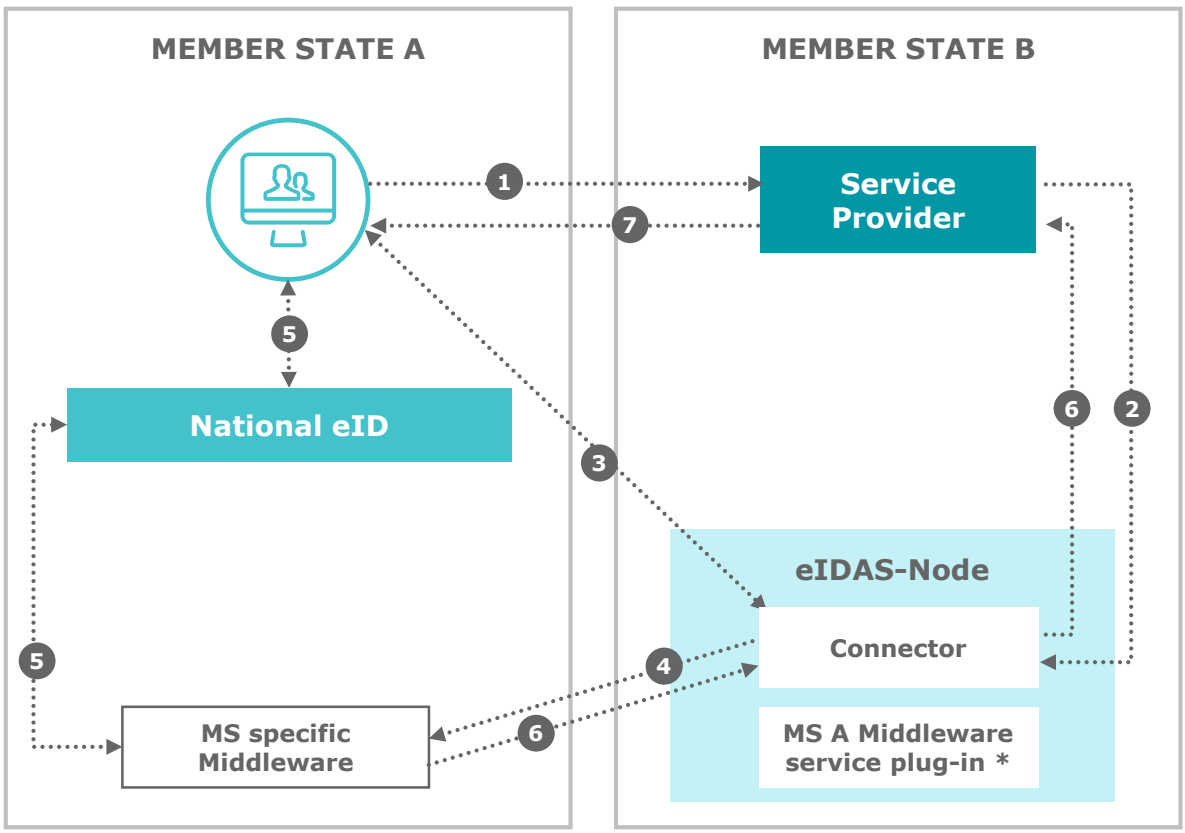
1. The user in MS A requests access to a Service Provider in MS B, both proxy countries.
2. The Service Provider in MS B sends the request to its own eIDAS-Node (Connector).
3. On receipt of the request, the eIDAS-Node Connector asks the user for their country of origin (TLS protocol).
4. When the country of origin is selected by the user, the SAML Request is forwarded by the eIDAS-Node Connector to the eIDAS-Node Proxy-Service of the user's Member State.
5. The eIDAS-Node Proxy-Service sends the SAML Request to the Identity Provider for authentication.
   The user authenticates using their electronic identity. Once authenticated, this identity is returned to the eIDAS-Node Proxy-Service.
   Depending on the implementation there may be two additional steps within step 5:
   - for the user to select the attributes to be provided (therefore giving consent)
   - for the user to agree the values of the attributes to be given.
6. The eIDAS-Node Proxy-Service sends a SAML Assertion to the requesting eIDAS-Node Connector, which forwards the response to the Service Provider.
7. The Service Provider grants access to the user.

Interaction with the user only happens in stages 1, 3, 5 and 7. The remainder of the process is automated and invisible to the user.

The Identity Provider and the Attribute Provider would be in MS A.

User from a Middleware country accessing a service in a proxy country

1 2 3 4



1. The user in MS A requests access to a Service Provider in MS B (a proxy country).
2. The Service Provider sends a request to the eIDAS-Node (Connector) in its own country.
3. On receipt of the request, the eIDAS-Node Connector asks the user for their country of origin (using TLS protocol).
4. When the country of origin is selected by the user, the request is forwarded by the eIDAS-Node Middleware Service plugin to the MS Specific Middleware of the user's Member State (SAML Request).
5. The user authenticates using their national electronic identity and the Middleware infrastructure in his/her country. Depending on the implementation there may be two additional steps within step 5:
   - for the user to select the attributes to be provided (therefore giving consent)
   - for the user to agree the values of the attributes to be given.
6. Once authenticated, the MS Specific Middleware sends a response back to the eIDAS-Node Middleware Client, which passes the response to the eIDAS-Node Connector (SAML Assertion). The eIDAS-Node then sends the electronic identity information to the Service Provider.
7. The Service Provider grants access to the user.

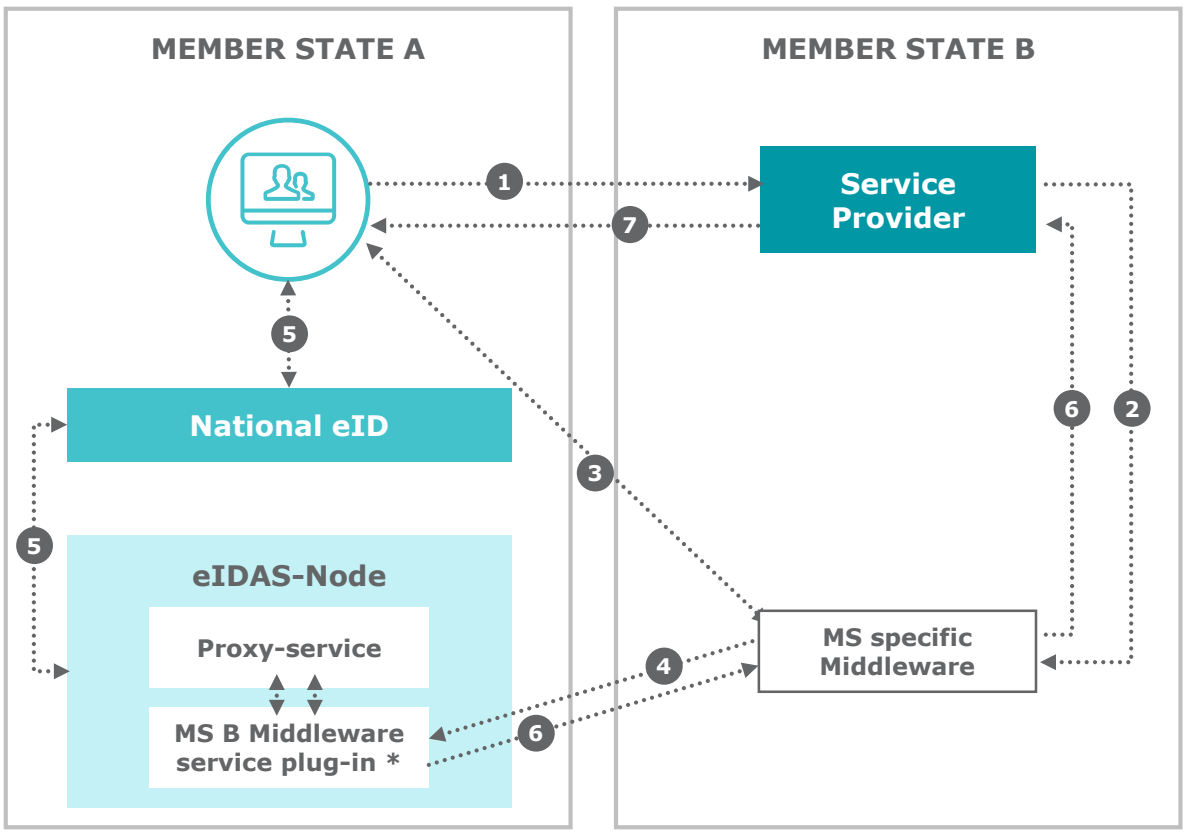
Interaction with the user only happens in stages 1, 3, 5 and 7. The remainder of the process is automated and invisible to the citizen.

The Identity Provider and the Attribute Provider would be in MS A. Note that the Middleware Service can be running in the domain of the Service Provider. However, the authentication process remains the same.

(*) For a proxy country to authenticate to a middleware country, the proxy country must have integrated the middleware country's Middleware Service plugin in its eIDAS-Node.

User from a proxy country accessing a service in a Middleware country

1 2 3 4



1. The user in MS A (a proxy country) requests access to a Service Provider in MS B (a Middleware country).
2. The Service Provider sends a request to the MS Specific Middleware in its country.
3. On receipt of the request, the MS Specific Middleware asks the user for their country of origin (using TLS protocol).
4. When the user selects their country of origin, the request is forwarded by the MS Specific Middleware to the eIDAS-Node Middleware Service plugin of the user's Member State (MS A).
5. The user authenticates using their national electronic identity. Once authenticated, this identity is forwarded to the Member State's eIDAS-Node (eIDAS-Node Proxy-Service).
6. The eIDAS-Node passes the eID information to the requesting Middleware Service plugin, which forwards the response to the MS Specific Middleware in MS B which passes it on to the Service Provider.
7. The Service Provider grants access to the user.

Interaction with the user only happens in stages 1, 3, 5 and 7. The remainder of the process is automated and invisible to the user.

The Identity Provider and the Attribute Provider would be in MS A.

User in a Middleware country accessing a service in another Middleware country

1 2 3 4

As the two Middleware countries authenticate via their own MS Specific Middleware, the eIDAS-Node does not play a role, therefore this scenario is out of scope of this document.

5 Technical specifications

What are the technical foundations of CEF eID?

eID Technical specifications

Regulation (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market – technical specifications

The technical specifications for the eIDAS interoperability framework have been developed by the European Commission with the help of member states collaborating in a technical sub-committee of the eIDAS Expert Group. A further role of the Commission has been to provide a sample implementation of the technical specifications which member states are free to adopt as an "off the shelf" implementation should they wish to do so.

More information about the CEF Telecom policy background, its Work Programmes and related information is available on the Digital Agenda website.

More information about eID technical specifications is available on the CEF Digital Single Web Portal.

In line with Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, and with COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 of 8 September 2015 on the interoperability framework, in particular with regard to Article 12 thereof, in order to implement the interoperability framework, technical specifications could be developed. The present technical specifications may serve as the basis of further details of the technical requirements contained by COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501

The specifications based on the Interoperability Framework Implementing Regulation posted here as versions 1.0 represent a stable eIDAS compliant set of technical specifications which Member States can use if they are providing their own implementation. These technical specifications will be subject to further development in the normal course of events and any subsequent changes will form part of the timed release management process.

6 Implementations

What are the existing CEF eID implementations?

Your options

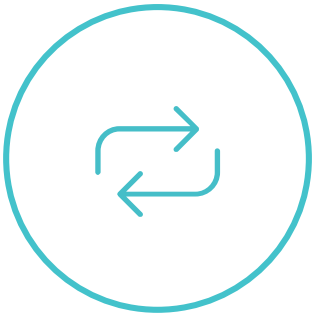
While considering a CEF eID project, three alternative implementation scenarios can be considered:

BUILD

You **build** and **test** your own components according to the specifications of the eID DSI. This can be done using an in-house development team or by an external contractor.

BUY

You **buy** a product(s) that implements the specifications of the eID DSI. This can be a Commercial or Open Source software product. Additional services can be involved.



RE-USE

You **reuse** the sample software of the eID DSI or one of its stand-alone services.

Software Implementations

eIDAS Sample Implementation v1.0

Member States may implement this version directly, or use it as a sample when testing other implementations of the technical specifications.

Release 1.0 of the eIDAS sample implementation for Member States is an all-in-one package for the Java platform including binary distributions for Glassfish, JBoss, Tomcat, WebLogic, WebSphere and the source code (Maven project).

The next and subsequent releases will be timed in accordance with the release schedule as part of the operational management of the eID building block.

With each re-release, the CEF eID Team are striving to improve a users' CEF eID experience. In a future release, CEF Digital therefore intends to provide a major architectural improvement involving the Specific module. The Specific module is inherited from the STORK PEPS Pilot 1 application and provides a sample implementation of a Member State Specific module to customise the communication between the Identity Provider and the eIDAS-Node Proxy Service. These improvements will provide abstraction and a correct placeholder for Member States specific implementation, remove dependencies and further extend the scope of the Specific module.

Sample software maintained by the European Commission

DISCLAIMER

These lists are for informational purposes only and the Commission cannot be held responsible for any use which may be made of the information contained therein.

7

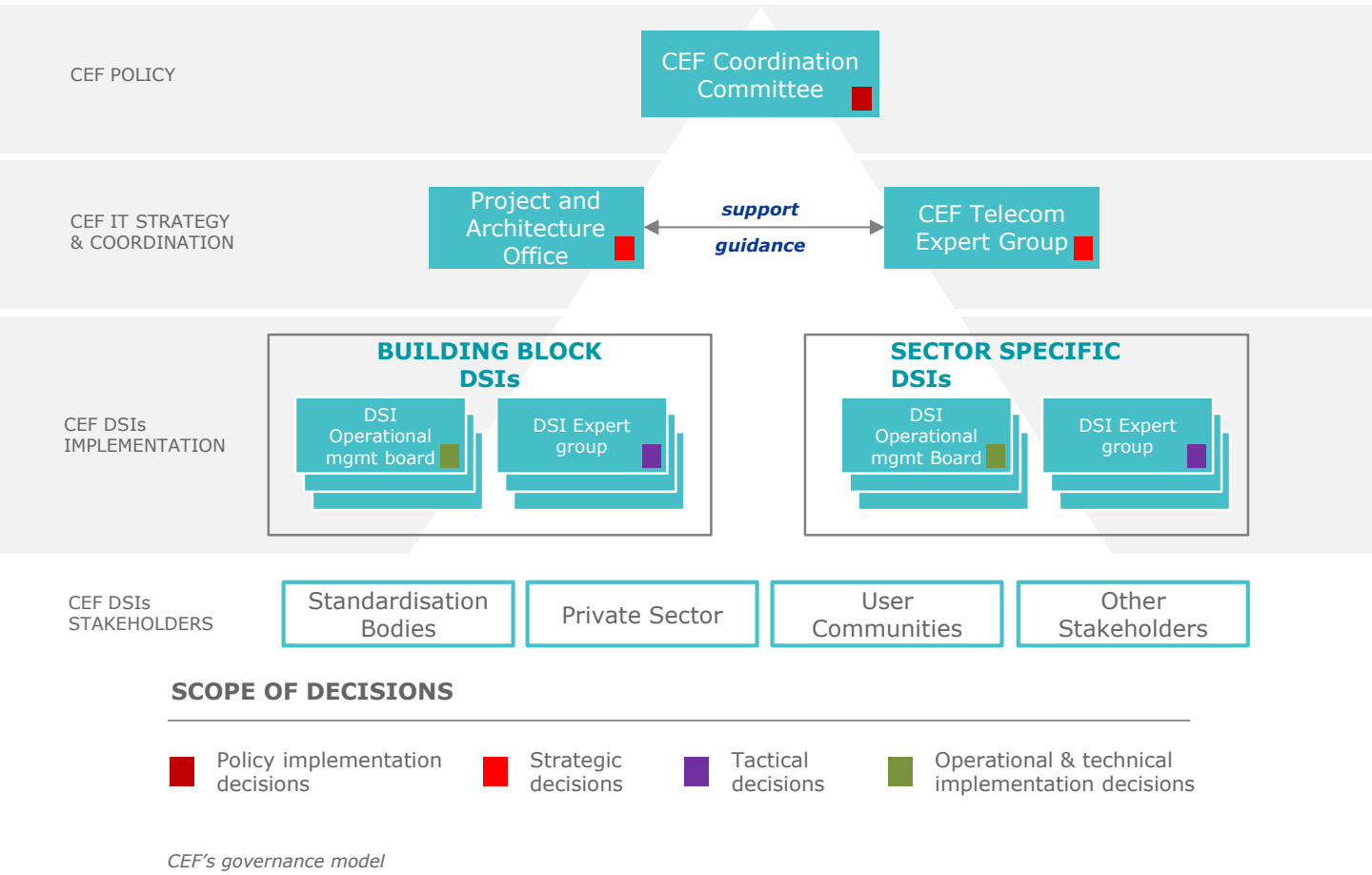
Governance

What is the CEF IT governance model?

Governance

CEF has a governance model in place to ensure that eID's reusable components correspond to user needs and expectations and that stakeholders can influence their evolution over time.

As shown below, the proposed model is multi-layered, designed according to guiding principles stemming from the CEF regulations.



CEF's governance model

Governance

The eID Operational Management Board (OMB) is organised every month to discuss all types of operational matters (change requests, release planning, etc.). This governance body brings together:

- The eID DSI (Policy) Owner, accountable for its policy and its translation into the functionality of the building block: this role is currently played by DG CNECT
- The DSI Solution Provider, accountable for the delivery side of eID's components and related services: this role is currently played by DIGIT
- The Directorate Generals of the Commission that have decided to reuse, or are interested in reusing, eID

The OMB works in close collaboration with, and is advised by, the eIDAS technical subgroup (composed of Member State representatives). Consultation processes ensure that standardisation bodies, the private sector, user communities and other stakeholders are involved as required. In case of issues, these can be escalated to the 'CEF Telecom Expert Group' (also composed of Member State Representatives). The CEF Telecom Committee is mostly involved in the formulation of the CEF Telecom Work Programmes and less in their implementation.

3

CEF Services to Service Providers

How can I get help?

CEF Services to Service Providers

Service Provider support

Service Providers themselves can be in need of support regarding the eID infrastructure. This can happen in several situations, of which some examples are:

- The Service Provider cannot resolve/answer the issue or question raised by a user.
- The Service Provider encounters trouble when integrating with the eID infrastructure.
- The Service Provider encounters trouble using the eID infrastructure.

It is the responsibility of each Member State to set up a support structure for their own country. In this context, the Member State appoints a local eID representative and country representative to offer support to Service Providers.

Service Providers should always contact the local representative when support is needed. In case this representative is not able to solve/answer the issue, he will get support from the country representative.

End-user support

When an end-user (e.g. citizen) encounters problems when trying to authenticate and use the services of a Service Provider, the user should contact the support function of the Service Provider. It is the responsibility of each Service Provider to set up such a support function for users in need of eID support in their application.

Member State support

To support new or already integrated Member States with the use of the eID infrastructure, functional mailboxes are provided by DIGIT CEF eID. These mailboxes are a contact point for:

Additional information about the eID infrastructure

Feedback on the services provided by the CEF eID building block DSI team

Technical support questions

For generic CEF related comments and queries use:

CEF-BUILDING-BLOCKS@ec.europa.eu

For specific eID related comments and queries use:

DIGIT-CEF-EID@ec.europa.eu

9 Success stories

Success Stories – STORK

During the pilots the technical infrastructure was developed and deployed to prove that the technology is feasible and sustainable to meet the needs of legacy eID systems and those of the future.

As a result of the STORK pilots:

- In 6 Member States a framework has been developed for an interoperable service allowing foreign citizens (using their eID credentials) to notify all relevant entities of an address change. This was achieved without modifying current procedures in each Member State.
- 12 Member States have integrated STORK with the European Commission Authentication Service (ECAS). This integration allowed citizens from those Member States to use their national eIDs to access electronic services of the European Commission.
- 5 Member States are currently using the STORK solution in their eDelivery applications, allowing citizens from other Member States to access the service with their own eID credentials.
- In 5 Member States foreign students can access online administrative and academic services offered by European Universities with their eID.
- 10 Member States allow foreign citizens to register for social security with their eID credentials.

Success Stories – e-SENS

e-SENS

e-SENS was launched to consolidate, improve, and extend the technical solutions developed by the thematic LSPs

The objective of the e-SENS building block e-ID is to establish cross border recognition and e-identification validation that meets the requirements set for e-Government applications in different domains. Thus e-SENS permits businesses, citizens and government employees to use the presently widespread (national) identities in cross-border public and private services. The solution includes the know-how gained in STORK which is developed to provide infrastructure for cross-border use of government-endorsed electronic identities and exchange of attributes, including roles and mandates as needed by various on-line services.

The e-ID building block implemented under e-SENS develops integrated framework to handle e-ID by benefiting from experience gained in this area by other LSPs. In addition, several other issues, which were outside the scope of the previous projects will be addressed in e-SENS: e.g. the possibility to use self-managed user-centric on-line identities (based on cloud ID or other types of consumer ID) are likely to be investigated within the context of public services.

In the first cycle the e-ID building block of e-SENS focused on inventorying the previous LSPs, determining the requirements for e-SENS cross-border recognition and e-ID verification as well as determining a set of architectural building blocks and standards for targeted software products. The e-ID group identified 2 areas for the first cycle, namely Cross-border e-ID Interoperability Architecture and Attribute Provider.

10 Definitions

Definitions

A **Building Block** offers basic capabilities and services that can be combined with other building blocks or sector-specific applications to deliver architectures, solutions and sector-specific services.

Source: TOGAF® 9.1 and Regulation (EU) No 283/2014

Interoperability is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.

Source: European Interoperability Framework 2.0

e-SENS (Electronic Simple European Networked Services) is a large-scale pilot project with the aim of consolidating, improving, and extending technical solutions based around the building block DSIs to foster digital interaction with public administrations across the EU.

Regulation (EU) N°910/2014 on eID and trust services for electronic transactions in the internal market (**eIDAS Regulation**) adopted by the co-legislators on 23 July 2014 is a milestone to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities.

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

The **electronic identity (eID) building block** helps public administrations and private online service providers to easily extend the use of their online services to citizens from other EU Member States. It allows cross-border authentication, in a secure, reliable and trusted way, by making existing national electronic identification systems

A Digital Service Infrastructure (DSI) enables networked services to be delivered electronically, typically over the internet, providing cross-border interoperable services for citizens, businesses and/or public authorities.

Source: Regulation (EU) No 283/2014

According to the eIDAS regulation a **Public Administration** means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate

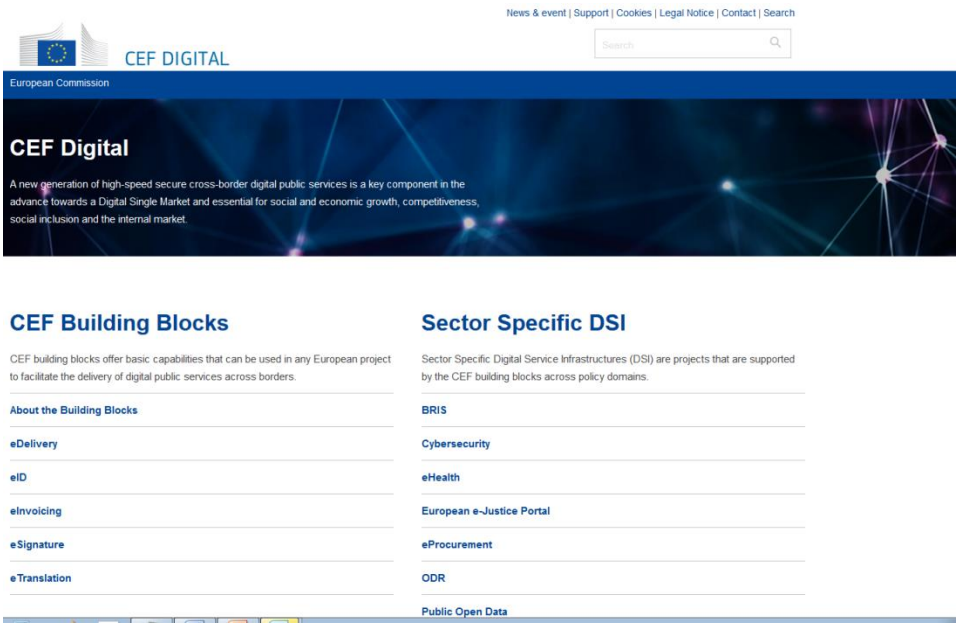
Source: http://ec.europa.eu/digital-agenda/en/trust-services-and-eid

According Directive 2000/31/EC (eCommerce Directive), "**service provider**" is defined as any natural or legal person providing an information society service

Source: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031

eID connecting europe

Visit the catalogue of building blocks on CEF Digital Single Web Portal
https://ec.europa.eu/cefdigital



DIGIT
Directorate-General for Informatics
DG CONNECT
Directorate-General for Communications Networks, Content and Technology

Contact us
CEF-BUILDING-BLOCKS@ec.europa.eu