|  |
| --- |
|  |
| EDSSI  Milestone 1.7: Usability Report for other CEF Building Blocks in relation to the European Digital Student Service infrastructure |
|  |

| Document title | **EDSSI MS1.7 - Usability Report for other CEF Building Blocks** |
| --- | --- |
| Version | **1.0** |
| Status | **Final** |
| Activity | **1** |
| Date of delivery | **October 2021** |
| Author | **Francisco Aragó, José Traver (Universitat Jaume I)** |

Table of Contents

[**Executive Summary 2**](#_heading=h.1fob9te)

[**1.**](#_heading=h.3znysh7) **Introduction 2**

[1.1.](#_heading=h.2et92p0) Methodology 3

[1.2.](#_heading=h.3dy6vkm) About the Document 3

[**2.**](#_heading=h.1t3h5sf) **Analysis of the CEF Building Blocks 4**

[2.1.](#_heading=h.4d34og8) eID 4

[2.2.](#_heading=h.2s8eyo1) eSignature 5

[2.3.](#_heading=h.1ksv4uv) eDelivery 8

[2.4.](#_heading=h.1y810tw) eArchiving 13

[2.5.](#_heading=h.3whwml4) eInvoicing 17

[2.6.](#_heading=h.1pxezwc) eTranslation 19

[2.7.](#_heading=h.3o7alnk) European Blockchain Service Infrastructure (EBSI) 21

[2.8.](#_heading=h.1hmsyys) Big Data Test Infrastructure (BDTI) 30

[2.9.](#_heading=h.3fwokq0) Context Broker 31

[2.10.](#_heading=h.19c6y18) Only Once Principle (OOP) 34

[**3.**](#_heading=h.37m2jsg) **Analysis of Other Relevant European Digital Infrastructures 36**

[3.1.](#_heading=h.1mrcu09) Single Digital Gateway (SDG) 36

[**4.**](#_heading=h.3l18frh) **References 38**

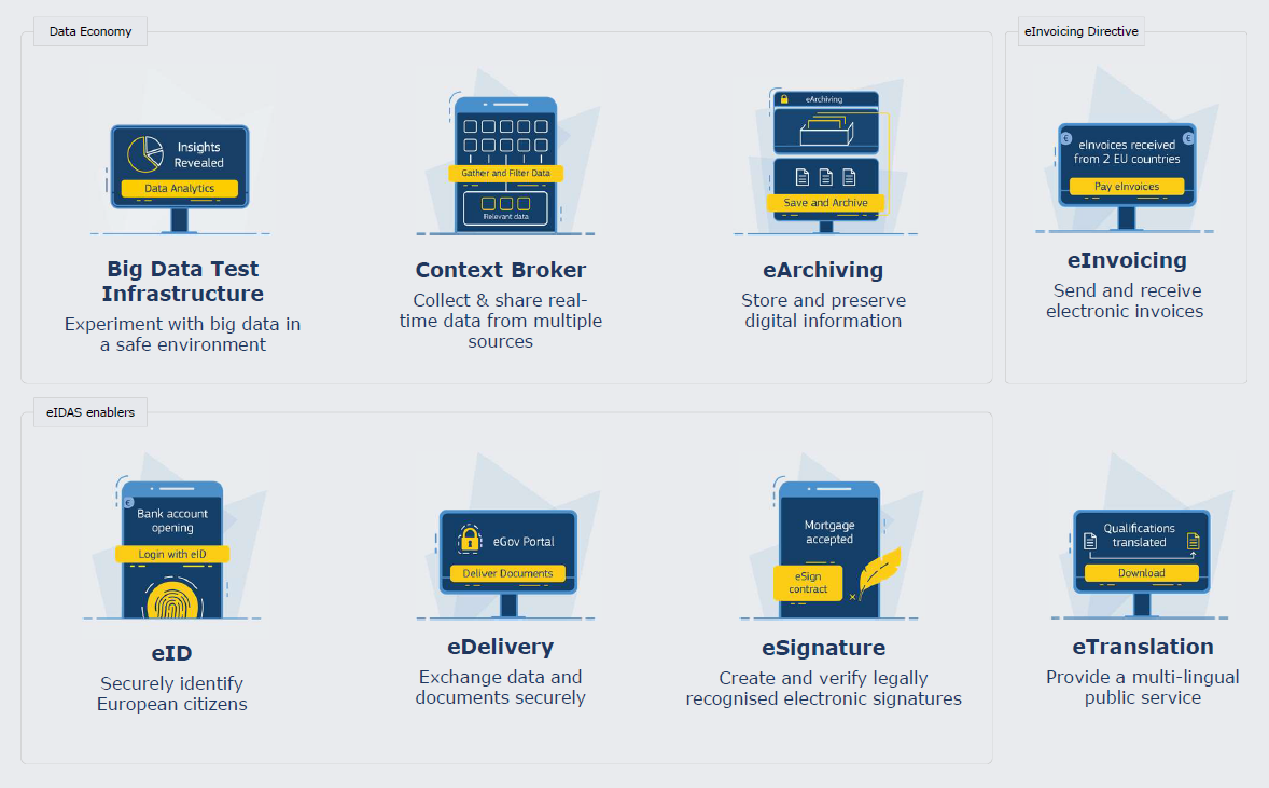
# Executive Summary

The present document provides a comprehensive analysis of the mission and functionalities of the CEF Building Blocks, and an overall analysis of the potentials they can offer for the future evolution of the European Student Digital Service Infrastructure. The present document will be used by the project Steering Committee to help in decision making but can be used as well as a short introduction to the CEF building blocks by any other stakeholder.

# Introduction

European Commission’s Connecting Europe Facility (CEF) Programme is a funding programme run by the EU Innovation and Networks Executive Agency (INEA). The programme aims at investing in the development and deployment of European infrastructures (in all relevant fields, such as transport and energy but in this document the focus is on digital service infrastructures) to support cross-border interaction between public administrations, businesses, and citizens, in pursuit of more efficiency and growth, and the accomplishment of the European Single Digital Market.

The CEF Building Blocks are a series of initiatives promoted, adopted or developed (some are directly promoted by the EUROPEAN COMMISSION, some are identified from funded initiatives as having the potential to become relevant and reusable key strategic components) by the CEF programme to obtain a set of components to offer basic capabilities in many fields of the digital activity that can be reused by any European public entity to facilitate the delivery of digital services across borders and sectors (including private sector entities) of the digital market scene. These Building Blocks are then reusable specifications, software and services that can potentially form part of a wide variety of IT systems in different policy domains of the EU. The building blocks help promote the adoption of the same open standards and technical specifications across different sectors of the EU, for basic and common functionalities to many digital services, thus helping achieve the effective interoperability across borders and sectors. Due to all of this, the Building Blocks receive special treatment and adoption by INEA, centring an important part of the funding strategy around their promotion and adoption. INEA ceased operations on 31 March 2021 and the portfolio of solutions, including the CEF Building Blocks was taken over by the newly established European Climate, Infrastructure and Environment Executive Agency (CINEA). 5 Building Blocks were selected in the initial phase, which have been extended to 9. All of them will be analysed in this document.



*Figure 1: Currently Launched CEF Building Blocks*

EDSSI project aims at producing another component to be adopted by CINEA, in this case not a building block, but a Digital Service Infrastructure (DSI) for the European Students. A component that will provide direct service to stakeholders of a sector in support of specific procedures centred around mobility and especially the Erasmus+ programme. This does not mean that parts of it can be reused or extended to new use cases, users, or even different sectors. With this in mind, EDSSI has a strong commitment with the reuse of pre-existing components, to minimise attack and error vectors through the use of solid and solvent existing solutions, and to minimise costs associated with scalability and extensibility. A proof of this is the fact that EDSSI builds strongly around the CEF eID Building Block. But to deepen on this commitment, the project included in its planning the execution of a task devoted to analysing the potential benefits of integrating the rest of the existing Building Blocks. The outcome would be the present report, which will be used by the project Steering Committee as a support tool to analyse and plan the evolution and sustainability of the European Student DSI. It might also even serve as a comprehensive guide to the Building Blocks and a general assessment tool for any other independent stakeholders that could benefit from this outcome.

## Methodology

The development of this document was followed by an extensive research phase. The pre-existing knowledge on the matter led to the search for additional sources (seminars, presentation, documents, technical documentation) to help complete and structure all the information needed to provide a clear picture of the scope, goals, and functionalities of each analysed Building Block. This information was shared with the rest of the partners and through discussions, the potential usages over EDSSI and their feasibility was analysed and registered on the document.

This analysis will be an input for the project Steering Committee, to help determine the future strategy and development of EDSSI, as some of the building blocks could facilitate solving existing requirements or even help discover potential improvements or opportunities not envisaged before the Building Block was considered.

## About the Document

Besides this introduction, the document presents two main sections: One referring to the analysis of the CEF Building Blocks, and another one referencing other EU infrastructures that, not being Building Blocks, are still relevant for EDSSI and the stakeholders in the academia sector. Each subsection will have the same structure and will cover one Building Block, presenting three differentiated points.

First, we will introduce a short description of the block, it’s mission and the use cases it tries to solve. We will introduce all the relevant context information on the technical and business levels, to provide a good general overview of the Building Block, what it was created for and what it can do, to help the decision-making process. With the information above, and considering the business goals, functionalities and use cases of EDSSI project, the second point will analyse how EDSSI could benefit from integrating this Building Block and how it could be done, by presenting an approximated potential architectural blueprint, and the use cases it could cover. Finally, the third point will develop an approximative cost-benefit analysis with the information from the section above, by doing a rough estimation of the effort required to implement the sketched use cases - individual use cases can be evaluated and analysed for feasibility separately -, and compared to the estimated benefits - a rough estimation of the overall benefits, considering all domains benefits can appear on -, assert a few recommendations on whether they should be implemented or not, and whether it should be implemented on the short, mid or long term; as well as under what conditions it should happen.

This analysis does not have the ambition of being full nor detailed, and even less to suppose any final decision or positioning of the EDSSI project towards the integration of the Building Blocks or the sustainability plan, as only a reduced set of the partners are participating on it. The goal of this document is to become a helpful decision-making tool. A starting point and guide for the discussions regarding the sustainability and future evolution of the EDSSI that will happen towards the end of the project.

# Analysis of the CEF Building Blocks

This section will provide an analysis of the CEF Building Blocks as described in the introduction. For each one of them, all relevant context information at business and technical levels will be provided, as well as any further references needed to understand the reason and purpose the BB was developed for, or how it can be used, and what it can be used for.

Then, from the EDSSI point of view, the potential use cases the Building Block can help solve will be analysed, as well as any new use cases it could open for the EDSSI future evolution and improvement.

Finally, a basic cost-benefit analysis will be performed to get some preliminary assessment on the viability of integrating the Building Block in EDSSI to fulfil the potential use cases formerly identified.

## eID

This building block is already an integral part and a core component of EDSSI, so it is listed here only for the sake of completeness.

Imagen que contiene medidor, reloj

Descripción generada automáticamente

*Figure 2: CEF eID Proxy Model*

Authentication lies in the middle of each process involving the Student Digital Life, and CEF eID identities provide a leap forward in the trust and quality of the identity lifecycle, from the enrolment to the authentication and credential renewal. In other words: CEF eID facilitates the mutual recognition of student identities between institutions without the need of in-person registration procedures and enables academic institutions to advance on the digitalisation of especially critical student management procedures by ensuring the bind between the digital identity and the real-world identity. Moreover, as has been observed during the project, CEF eID offers a strong solution to the credential management issue, especially for small higher education institutions that can’t support an advanced IT team and service catalogue.

Many service providers can’t handle the security requirements of managing user authentication credentials, so they resort to identity federation. In many cases, and for the sake of usability, they even resort to social network authentication. This, despite its convenience for the provider and for the user, has a lot of strategic, legal and security implications that strongly limit the trust of the service offering and the sensitivity of the processes it can deliver. CEF eID becomes a key element in this scenario, as a potential contender to substitute the social authentication. CEF eID, by design - for example, thanks to the different supported levels of assurance - offers a strong and flexible framework to cover many needs in the authentication field. That is why ensuring a successful rollout of the CEF eID infrastructure in all the member states, as well as promoting the notification of as many supported eID schemes as possible in each country and ensuring citizens own and know how to use their credentials is a strategic effort that will pay off in the long-term.

EDSSI can still take more advantage of CEF eID in the future, but the details and plans strongly depend on how the consolidation of the CEF eID infrastructure and the notified schemas evolve, but the main points of growth can be identified in the following:

* General availability of eIDAS across the EU Member States. Today from the Swedish National Node only 12 Member States are available (Belgium, Croatia, Czech Republic, Denmark, Estonia, Germany, Italy, Latvia, Luxembourg, Portugal, Slovakia, Spain)
* The general availability of eIDs to European citizens. Today we see that only a very small portion of the student population has an eID that can be used through eIDAS.
* The general availability of low and substantial level of assurance Id schemas
* The growth of the offered attribute set, beyond the Minimum Data Set.

## eSignature

eSignature building block is a mix of elements: standard definitions, tools to be deployed, and supporting services for public administrations (also private sector, but not mandatorily) in the enforcement of the eIDAS regulation, that establishes the obligation of being able to create and verify electronic signatures legally valid in all European Member States.

### Description

The CEF eSignature Building Block provides the tools to allow electronically signing any digital document across Europe; and allows the proper verification of the signature and to validate the trust chain, in line with the eIDAS Regulation (910/2014) for e-signatures, e-seals and related services offered by Trust Service Providers. This way, the mission of the [eSignature Building Block](https://ec.europa.eu/cefdigital/wiki/x/9gTvB) is to provide the tools to facilitate achieving compliance with the eIDAS Regulation by helping deliver the required technical and legal cross-border interoperability between the electronic signature services of different member states. It does this for the eSignature part of the regulation, the same way the eID Building Block does so for the identity part.

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja

*Figure 3: Electronic Signature Process*

The goal of Electronic Signature is signatory identification (that is, binding the identity of the signatory to the document), with the requirement of providing document integrity preservation mechanisms (any modification after being signed can be detected) and permit non-repudiation of the signature (the signatory cannot, to a certain degree, reject that the signature was consciously and voluntarily issued).

The eIDAS Regulation defines three e-signature levels: basic or simple (checks the integrity and issuer), advanced (allows timestamping, preservation, etc.) and qualified signatures (additional guarantees on the trust chain across the operative). The latter meets the highest standards of security, and the regulation considers them legally equivalent to handwritten signatures, as well as mandating any European Public Administration to be able to verify and accept it. Of course, the requirements of each signature level are built on the requirements of the level below it, so a qualified electronic signature meets the requirements of an advanced signature, and the advanced signature meets the requirements of a basic electronic signature.

Imagen que contiene Gráfico

Descripción generada automáticamente

*Figure 4: eIDAS eSignature Levels*

The eIDAS Regulation also distinguishes between signatures issued by natural persons (citizens) and those issued by legal persons (companies, organisations). Although both are intended to ensure the document’s origin and integrity, it defines two separate concepts: the electronic signature and electronic seal. An electronic seal is defined as “data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity, where the creator of a seal is a legal person”, whereas the electronic signature is issued by a natural person. Electronic seals can be used as evidence that an electronic document was issued by a legal person, but the regulation also considers valid, at the qualified level, the signature from the authorised representative of the legal person.

The [tools and services](https://ec.europa.eu/cefdigital/wiki/x/9gTvB) provided by [CEF eSignature Building Block](https://ec.europa.eu/cefdigital/wiki/x/9gTvB) to support eSignature are described below:

* **List of Trusted Lists**: It is a list of lists, the root element of the trust model for eSignatures defined by the eIDAS regulation. The list can be (and should be) automatically processed by any service provider that aims at verifying an eSignature. Each entry of the list points to the list of trusted certificate providers by a Member State. This way, any valid signature will only be trusted if the issuer of the used certificate appears on the lists in this list[[1]](#footnote-0).
* **ETSI Signature Conformance Checker**: It is an online service aimed at service providers in the process of integrating a signature provider service. It allows checking that a generated signature can be validated and is compliant with the regulation. The developer uploads the generated signature, and the service analyses it.
* **Validation Tests**: A compilation of test cases have been set up to help in the development of robust eSignature validation implementations. The test cases currently focus on the validation of the 'qualification part' of qualified electronic signatures and seals based on trusted lists (that is excluding the specific test cases related to the validation of an advanced electronic signature or seal according to ETSI EN 319 102-1).
* **Digital Signature Service library**: It is an open-source library, written in Java, that implements the primitive operations required to create and validate digital signatures. It is a basic component to facilitate the development of eIDAS-compliant eSignature solutions. Digital signatures are the set of standard cryptographic operations performed with public key systems and standard specifications like XML Digital Signatures, JSON signatures, etc. This must be noted, because eIDAS regulation differentiates electronic signatures from digital signatures being the latter only a subset of the former. That is: not all eIDAS compliant electronic signature schemes need to be PKI based.
* **Service Offering Canvas eSignature**: it is a stakeholder-oriented online service, including resources and documentation to guide all the stakeholder profiles to the information or support service they need. It includes the reference to a personalised support help desk. Its aim is to facilitate the onboarding process for stakeholders interested in implementing and using electronic signatures and electronic seals.
* **TLSO Community management**: The Trusted List Scheme Operator Community management service is another stakeholder-oriented to provide hands-on support to the TLSOs (the entities in each member state that manage the Trusted Lists). It allows access to materials, helpdesk and regular contact and support to all the TLSOs. On top of that, regular interactive TL error-reduction campaigns are upheld for the TLSO Community.
* **Trusted List Browser**: An online tool, aimed at any stakeholder, especially not trained citizens, that lets them search the entities that can be trusted, as they appear on the Trusted Lists.
* **Standards and specifications**: A compilation of all the relevant resources on standards around electronic signatures, digital signature standards and representations.
* **EU Trust Services Dashboard**: The EU Trust Services Dashboard unifies and centralizes many of the above-described tools, for the purpose of augmenting existing features and gradually implementing new initiatives into a continuous improvement approach. It is some sort of single-entry point for all the eSignature related needs.

During the development of this Building Block, changes in the policy of web browsers provoked the obsolescence of Java applets launched by the browser. This had a disabling effect on the signature solutions. Most member states have developed their own solutions to overcome this limitation, but it is worth noting that the building block example services use an open software solution (developed by a private company, which also has a professional solution and provides support services) called NexU[[2]](#footnote-1). This is the main reason for the promotion of remote signing solutions. On these, private keys are managed by trusted third parties (in the cloud). They must be Qualified Trust Service Providers. This way, the applications communicate with signing platforms which communicate with the TSP managing the keys. This allows for a seamless, more mobile friendly user experience, not requiring any effort or configuration requirement on the user’s side.

Developing and deploying an in-house signing solution comprises roughly the following phases:

* Integrate CEF’s DSS library on your signing service, which provides eIDAS compliance.
* Test the interoperability using ETSI signature Conformance Checker and the Qualified electronic signature validation test cases.
* Obtain a digital signature for eSignature, eSeal or website authentication from a Trust Service Provider, using the Trusted List Browser to choose from.

So, the final goal is to create a pan-European environment where citizens and organisations are able to sign and verify documents regardless of the signing tool used, trust provider, and service accessed, and the Building Block provides an array of tools and services to facilitate and reduce costs to all the involved stakeholders. Besides, achieving interoperability with third countries outside the EU is another task in progress.

### Usability Analysis

As in many procedures, EDSSI procedures require the issuing of signed data by different parties (Institution representatives that sign the Erasmus+ charter, International Relations Officers signing Inter-Institutional Agreements, Students signing the Learning Agreement, DG-EAC officials...). Although not all procedures require the same assurance or legal validity on the signatures, this is the most obvious potential usage of the eSignature Building Block on EDSSI, but integration needs to be analysed case by case as they are designed.

Besides this, and only partially inside of the scope of EDSSI, each institution might have the need to deploy a signature server. The eSignature building block can help on this (and this signature server can be a component used in upcoming EDSSI procedures). Also, depending on the liability model, EDSSI could also provide a centralised signature server for all the participants, acting as a central notarisation service (the role of an EC-owned DSI would be a source of trust for all the participants), and used to sign the Learning Agreements, Inter-Institutional Agreements and Charters.

If we focus on the available tools in the Building Block, there are not many, and they are very basic and primitive, so any integration requires big effort. For example, no out-of-the-box client-side signature solution is provided, which is one of the major needs by most integrators, but as it also is the most effort-consuming component and the most difficult to adapt to all the use cases (and thus manage incidences and bug reports), it is not considered to be offered on the Building Block (the demo implementation uses an existing generic free solution offered by a company that sells its integration services). Another potential use of the Building Block in EDSSI would be to use the library to develop a client-side signature system for the student integrated in the Erasmus+ app, but as it will be discussed later, it is not a cost-effective task.

### Feasibility Analysis

The first barrier here is the cost of development, maintenance, and operation of digital signature solutions. There are not enough popular and easy to deploy solutions yet for an easy integration, so cost-benefit must be analysed carefully before taking over such a task.

The first aspect to consider would be if there is a poignant need in EDSSI to issue legally valid signatures. The analysts must ask a series of questions, such as: can the participation in the Erasmus+ programme have legal consequences on any of the involved parties? Can any of the issued administrative documents become potential evidence in a lawsuit? Is there a need for legal acceptance and recognition of the issued documents? How is the liability managed in the programme? Does the charter-signing bind to a specific legal framework? How are conflicts between HEIs managed there? In summary: is there a legal framework that limits the liability and the legal actions stakeholders (students, institutions, the EC) can undertake?

Depending on the trust model and legal liability model accepted by all the participating parties, and the specific procedure, the importance of the signatures varies. For example, currently the Learning Agreement is signed with a digitalised hand signature by the student, and the institutions exchange it over a secure trusted network where the acceptance of the LA by both parties is not represented by any kind of electronic signature, but by the execution of the process itself, following the specifications of the network and the participant Student Information Systems. It also holds a detailed log of who did what in a learning agreement at any point in time, complying with the full-trail audit proof requirements. Other procedures might require more cryptographically secure signatures, but the point is that the need for legally accepted and cryptographically secure signatures is relative and depends on the needs and agreements of all parties involved. Due to this, most of the potential integrations described above fall short on a cost-benefit analysis, and will almost surely be dismissed, because in all the cases, most probably establishing relaxed liability rules is indeed a possibility which helps save dramatic amounts of effort and money on the development, maintenance, and user-support of a client-side signature solution.

Some of the highest-level procedures in EDSSI might indeed require legally valid signatures aligned with the eIDAS regulation but depending on the frequency and volume of signatures produced, integrating them on EDSSI would be counterproductive, and they should be relayed to the signature facilities of each institution. That is, each institution would have to procure their own eIDAS-compatible signature infrastructure issuing and validation, and just use EDSSI procedures to exchange the signed documents, not to sign nor validate them. This would leave room for member states to organise properly and converge on their signature solutions without causing impact on EDSSI.

In conclusion: EDSSI could benefit from trusted and legally signed documents, but currently, the cost of integration and operation of the Building Block greatly outweighs the benefits, especially as more cost-effective alternatives exist.

## eDelivery

eDelivery is a set of tools to allow building a distributed network of nodes for the exchange of electronic data and documents or messages between public administrations, businesses, and citizens. It is based on standard transport protocols and security policies to ensure interoperable, secure, reliable, and trusted communications.

### Description

This building block provides the technical specifications, software, and support services to allow projects to build a network of nodes for secure digital data exchange through a safe and interoperable channel to transfer documents and messages between all the involved participants with heterogeneous information systems.

eDelivery is designed as well to ensure a proper scalability of the network, offering performance and maintainability as the number of participants grows. But the main characteristic is how it ensures security and accountability of the transactions: data integrity and confidentiality are granted through the use of digital signatures and encryption, but also accountability (for an enhanced legal assurance) is achieved by the fact that the recipient of a message must send a digitally signed acknowledgement of receipt for every received message. eDelivery is content agnostic and supports multiple types of data exchange models; it is a flexible solution that can be easily adapted to the needs of any use case with no additional development requirements, only through parameterisation of the deployment.

To ensure the above-described goals, it is critical to use open standards, which allows any vendor using any development platform to develop a compliant solution. This is necessary to boost adoption and to cover the needs of all stakeholders, which in the end will produce a more solid and tested ecosystem of solutions. A list of compliant solutions is maintained by the EC[[3]](#footnote-2).

The eDelivery building block communications are based on the OASIS open standard AS4 messaging protocol. Given that the standard is very extensive, eDelivery uses a specific profile of the protocol, and guidelines developed by the Member States during the e-SENS Pilot. This standardized protocol lays the foundations to achieve pan-European and cross-domain interoperability. The messages are exchanged through secure connections (generally HTTP transport), in the form of a multipart-related MIME message. The first element of the multipart is a standard XML AS4 message, which is contained in a SOAP envelope, which provides the security elements, and the exchanged documents, referred and hashed inside the AS4 message payload, are included through references as attachments on the multipart.

eDelivery is intended primarily for policy domain owners involved in the roll out of EU or national policies that require the secure exchange of documents and data across borders. It is also intended for service and software vendors in the eDelivery domain, helping them to upgrade their solutions so they are fully interoperable and conformant

An eDelivery network is composed of a set of Access Points (nodes) that are interconnected, trust themselves and can exchange information with the AS4 messaging protocol. Each one of them has a unique identifier. Organisations willing to send or accept messages need either to install an Access Point, or to connect to an Access Point managed by a sector authority. Each organisation (or even each application) could deploy its own access point, but usually it’s more cost-efficient that a single AP serves many organisations/applications inside a domain (for example, a ministry in a country). In that case, the organisation connects to the Connector of the AP, which is a specific interface to interact with the AP which does not require using AS4 protocol (usually a use-case specific API). This model of proxied communication between two communicating parties that relay their messages through the APs is what is called the four-corner model in eDelivery. This model is flexible enough to lead to the deployment of multiple topologies. For example, to a mesh of trust, where each organisation deploys an AP and decides which APs to trust; or a proxy network, where each organisation trusts its area node, and the node operator trusts all other nodes (the nodes share a common trust domain), so by extension, an organisation trusts the organisation the other nodes trust.

Interfaz de usuario gráfica, Texto, Chat o mensaje de texto

Descripción generada automáticamente

*Figure 5: eDelivery Four Corner Model*

As can be seen on the above model, Party A, the sender, already knows how to communicate with Party B, the receiver. To reach this point, a routing service is needed. In eDelivery this is represented by the Service Metadata Provider (SMP) and the Service Metadata Locator (SML). When a sender needs to discover where the information about a receiver is stored, it queries the SML, which guides the sender towards the location of the receiver metadata (address, protocol, endpoints...), which is stored on the SMP (the SML will return a URL that points to the SMP).

The SMP is the component in charge of publishing the routing and messaging capabilities for every participant (APs, Receiving Parties) in the data exchange network. Every participant must be given a unique ID in the form of a URL. It is a decentralized component, so at any point in time there can be several SMPs (a centralised one, one per MS, etc.). The information is published following the eDelivery Profile based on the OASIS BDX SMP standard. The published information includes:

* The receiving AP lookup information (IP address, URL, transport protocol).
* The communication protocol (AS4).
* The available and possible business processes.
* The message types supported and required.
* The security setup (public key used for the encryption of the message, etc.).
* Any other information relevant for the message exchange (extensions).

The SML is a centralised component that stores the locations of every SMP in the network and manages the resource records of the participants and SMPs in the DNS Server. The SMPs register on the SML prior to being discovered. The SML stores the unique identifier (URL) of all receiving parties and SMPs on the network in the DNS Server. eDelivery's SML enables the sending AP to dynamically discover the address of the receiving AP’s SMP. The service is queried using the eDelivery Profile based on the OASIS BDXL Specification; The IDs follow the eDelivery ebCore Party ID Profile specification.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

*Figure 6: eDelivery solution components*

So, in a nutshell, components of an eDelivery network are:

* **Access Point**: The node of the eDelivery network, the connector where the consumers and producers connect to exchange the messages. Communication protocol is eDelivery AS4 profile of the ebMS3/AS4 OASIS Standard.
* **Service Metadata Publisher** (SMP): The component that enables a party to notify its own specific access parameters to allow receiving messages.
* **Service Metadata Locator** (SML): The component that a party can query to discover where to find the contact data of the receiving party.
* **Connector**: An eDelivery Connector may also be used to facilitate the integration between backend systems and Access Points. It implements a case-specific and easy to use API, instead of requiring AS4 support on all the backend services.

It is important to notice that there is not a single eDelivery network (that is, there is not a network of nodes, one node per MS). The design of the network can adjust to each use case needs. Each trust domain usually manages its own network for sectoral operation of specific use cases and configured to fit their own needs. It is currently used in more and more domain-specific use cases across-Europe. Different partners from different MS agree on building a base info exchange infrastructure on eDelivery to fit a purpose: connection of business registers, secure interconnection of justice and civil security organisations to obtain evidence, send orders, background checks (E-CODEX), etc.; e-Invoicing (Peppol); exchange of reports from medical devices (European Database on Medical Devices, EUDAMED); European e-Justice Portal. In the education domain it is not yet in use, but as we’ll see later, the first initiatives in using eDelivery for academic workflows are on the way (Single Digital Gateway, DE4A).

Below is a list of all the services and elements offered by the building block:

* **Technical specifications**: the profile restricting the AS4 standard
* **Public Key Infrastructure (PKI)**: CEF, as a service, offers a fully functional trust infrastructure based on the public keys required by eDelivery APs to securely exchange the data. It includes a set of roles, policies, procedures, and systems addressed to create, manage, distribute, store and revoke digital certificates, which are then used to build trust over the deployed eDelivery Access Points (AP) and Service Metadata Publishers (SMP). The participants trust the root of trust of the PKI and then automatically they trust the APs and the SMPs they need to. Of course, using this service is not mandatory, and each eDelivery network can develop and use its own trust model and infrastructure.
* **Service Metadata Locator (SML)**: A central instance of the metadata service, to facilitate the deployment of eDelivery networks that don't want or can’t afford managing one.
* **Connectivity testing**: Allows checking if a deployed Access Point complies with the CEF eDelivery profile and can successfully communicate with the test Access Point hosted by the EC.
* **Conformance testing**: Allows verifying that an implementation of the CEF eDelivery Access Point and/or the SMP specifications complies with the CEF eDelivery specifications: eDelivery AS4 Profile, and eDelivery SMP Profile. This is achieved through provided test cases, a testing platform, and personalised support during the entire testing process.
* **Reference Software Implementations**: Standard software implementations of the technical specifications, maintained by the EC and available to freely reuse. Stakeholders can help define the evolution of these solutions, by suggesting features that are then developed by the CEF's team. The following components are provided:
  + **Access Point**: Domibus is the CEF-maintained implementation in Java, but there are many more (Holodeck being one of the most used), supported by multiple programming languages.
  + **Service Metadata Publisher**: SMP software, in Java[[4]](#footnote-3)
  + **Service Metadata Locator**: SML software, in Java[[5]](#footnote-4)
* **Community and support helpdesk**: As usual, CEF offers mechanisms to provide personalised support and to receive feedback from the users.

### Usability Analysis

eDelivery is another Building Block that has a direct and evident potential usage, but with a discussable feasibility. It could be used as the base infrastructure for the Erasmus Without Papers message exchange, substituting the currently existing infrastructure of peer API call communications coordinated by a common central registry of participants. This could be achieved by converting the API calls into parameterised operations represented in a common message structure. Instead of calling an API over the target, a peer would send a message to the target party specifying the operation and parameters, over a common eDelivery network. The trust model would pass from a central registry of mutually accepted peers to a network of MS-operated APs that trust themselves, and a MS delegated management of the trust on institutions. Each institution would only communicate with its local AP instead of with all peers and the institution would trust all the institutions trusted by all the APs on the network. This would suppose a complete change of paradigm, and the implications will be analysed in the next section.

The European Student Card part of EDSSI would neither fit the role of eDelivery, as it is composed of a centralised service for e-Cards (the ESC Router) accessed by terminal clients directly.

### Feasibility Analysis

As introduced above, integrating eDelivery would suppose a complete paradigm-shift on the design of the Erasmus Without Papers (EWP) network which from a theoretical perspective could be open for discussion, but which presents many more difficulties from a practical point of view, as we will see.

The first aspect of the design that would need to be examined is the communication model: the current case-specific REST/SOAP APIs vs a generic message passing system. They are two different conceptions, each one of them with pros and cons: to extend the functionality, the latter would require only to modify the message content values, so it would not require architectural changes, which in principle is a more flexible approach, but if the new requirements need to extend the message syntax, it may affect other existing services and consumers. The API approach, which is the one chosen by EWP requires a bigger effort to extend, but the exported functionalities are more solid and easier to version (to support multiple versions of the API). Also, tracking the issues in a direct AP connection is quicker and easier than using a message passing system with intermediate nodes.

From the topological point of view, EWP is designed as a peer-to-peer network, whereas eDelivery acts as a proxy network. This is not a random decision: the underlying idea is to minimise the governance effort and distribute the maintenance and user support efforts. Scalability on proxy networks is easier but puts much stress on the proxies. That is, they need to be operated by some entity that is trusted by the other participants and also can invest the necessary effort to maintain the node (this also includes managing issues which are directly correlated to the number of transactions), as a failure would affect all participants behind the node. In this aspect, peer to peer communications distribute the load and risk evenly to all the participants, avoiding these central and trusted entities. The only central element of trust here is the registry, but its tasks and responsibilities are completely minimised. Considering only this aspect, the task could be feasible, but as we will later see, it doesn’t seem so. It must be noted that eDelivery, thanks to its flexible design, could be used as a peer-to-peer mesh network, just like EWP, but changing the underlying technology (adding layers of complexity) to achieve the same logical design doesn’t seem to be a cost-effective decision.

But the most important argument here is that EWP is an already developed and established infrastructure. It is currently adopted by a growing number of institutions and is on the verge of becoming mandatory. The humongous effort of redesigning the APIs and making all the participants adapt would not be a feasible task even if the benefits of using eDelivery were notable.

## eArchiving

eArchiving building block is another set of tools, specifications, software, and documentation aimed at the establishment of data preservation infrastructures. The goal is to keep large amounts of digital documents accessible and reusable for long periods of time, regardless of the system used to store it, and facilitating the migration to future technologies.

### Description

CEF eArchiving is a building block designed to help organisations tackle the issues of long-term accessibility of information, to which end it offers a set of components:

* Open and platform independent specifications, based on international standards, for creating information packages to preserve and reuse data.
* Open-source software components that demonstrate the application of specifications to the preservation and access to information.
* Documentation, training, and guidance to potential adopters on issues around data management and digital archiving lifecycle, as well as a community of users and experts built around the digital archiving tasks, to help in sharing and preserving the knowledge.

The three stakeholder groups eArchiving targets are the following:

* **Data Producers**: Anyone with information that needs to be preserved and reused. They can use eArchiving to develop standardised archival export interfaces and workflows into their business cases.
* **Archives**: Organizations responsible for digital archiving activities. They can use eArchiving to keep standard interoperable and secure data storages, by following the specifications on their ingest, preservation and access interfaces.
* **Solution provider:** Software and service providers. They can use eArchiving to make sure their development of components or end-to-end solutions do preserve data safely and in line with European standards, to align with client expectations.

The main component of the eArchiving building block is formed by the Information Package specifications, which describe a common format for storing bulk data and metadata in a platform-independent way, providing authenticity, integrity, and long-term understandability.

Tabla

Descripción generada automáticamente

*Figure 7: Information Package Structure Diagram*

These specifications facilitate migrating long-term valuable data between successive generations of information storage systems. It also allows moving data to dedicated long-term repositories or preserving and reusing data over shorter periods of time on specific information systems. The latest initiative from the eArchiving Building Block is the specification of a Reference Architecture, a holistic general design aimed to support multiple business cases, covering all the common needs of data management and preservation. It is aimed at supporting institutions by raising awareness on the importance of having a strategy, and on the necessary business components of digital preservation. Besides, following international standards and specifications for packaging digital information enables organisations to transmit documents and information across borders, for short, medium, and long-term storage, access, and reuse, regardless of the software platform, and promoting a high level of transparency and confidence among all participants in the information lifecycle. The main standard is the Reference model for an Open Archival Information System (OAIS) (OAIS Reference model[[6]](#footnote-5)) which has Information Packages as its basis. The main standard for transmitting Information Packages is the Metadata Encoding and Transmission Standard (METS), and the main standard for preserving Information Packages is Preservation Metadata Implementation Strategies (PREMIS). The OAIS Reference Model is designed as a conceptual framework of a digital archive. The model defines three types of information packages (an information package contains the archival content along with descriptive and technical metadata):

* Submission Information Package (SIP): the input of the archive, from the data producer.
* Dissemination Information Package (DIP): the output of the archive to the data consumer.
* Archival Information Package (AIP): the internal format used by the archive for long-term preservation.

And a set of electronic archival processes: Ingest, Archival Storage, Preservation Planning, Data Management, Access, Administration.

Diagrama

Descripción generada automáticamente

*Figure 8: OAIS Reference Model*

eArchiving building block offers a set of software components, to demonstrate how the eArchiving technical specifications might be used in various stages of the archival workflow (Ingest, Preservation, Access) and in different legal and organisational contexts. They can be used as well to be installed and used for specific digital archiving tasks, where no in-house developments exist, when there is a need to integrate eArchiving specifications in systems and workflows. Below is the list of provided software components[[7]](#footnote-6).

Interfaz de usuario gráfica

Descripción generada automáticamente

*Figure 9: eArchiving lifecycle and components*

* **E-ARK Web** (eArchiving Reference Implementation): The reference implementation of eArchiving specifications. It offers basic functions for ingest management and dissemination of information packages.
* **eArchiving ToolBox** (eATB): A Python library with a suite of tools for the creation of information packages for archival purposes, according to the specification. The library can also be used as a standalone component from the command line and can therefore be employed as an independent test case generator for the validation component.
* **Commons-ip**: A Java Library that provides an API to create or process Submission and Archival Information Packages, and to validate them. Can be used for custom integrations of information systems in order to automate the process of transfer of information to an archive.
* **ESSArch**: An open-source digital preservation platform covering the whole eArchiving process and workflow. It can prepare any content information to be packaged, validated, and submitted to a digital repository, receive, and validate packages and prepare for further transfer into a digital repository. Supports the receival (ingest), storage (storage) and reuse (access) of the packages, as well as the preservation planning/actions, policy/profile management and archival descriptions (data management) procedures.
* **RODA-in**: A tool for producers and archivists to create Submission Information Packages (SIP) ready to be submitted to an Open Archival Information System (OAIS). The tool creates SIPs from files and folders available on the local file system.
* **RODA**: A digital repository solution that delivers functionalities for all the main units of the OAIS reference model. RODA is capable of ingesting, managing, and providing access to the various types of produced digital objects. Supports existing standards such as the Open Archival Information System (OAIS), Metadata Encoding and Transmission Standard (METS), Encoded Archival Description (EAD), Dublin Core (DC) and PREMIS (Preservation Metadata).
* **Database Preservation Toolkit** (DBPTK): Set of tools to store and access relational databases in a standardised archival format (SIARD).
* **Python E-ARK Information Package Validator**: Validation for information packages (SIP, DIP, AIP) provided as a REST web service, command line application and software library (a Python API). The validation process checks: if the package is well formed (conforms with the appropriate specification), valid (package metadata is syntactically correct) and keeps integrity (the package contents are consistent with those declared in the package's manifest metadata: file names, sizes, checksums, etc.)
* **Java E-ARK Information Package Validator**: Same as the one above, but in Java instead of Python.

### Usability Analysis

Although EDSSI processes include some document management, they have a limited volume and lifespan. Participating HEIs have other processes more suited for an eArchiving deployment, but they are usually internal or, at most, country specific needs. No long-term needs related to mobility programmes or EDSSI processes requiring centralised eArchiving seem to be identified. HEIs could use eArchiving on generic MS centred deployments, but outside the scope EDSSI.

The only convergence would be for EDSSI to have interfaces to generate SIPs and be able to consume DIPs for the managed evidence, but this would need a careful analysis.

### Feasibility Analysis

As described above, it seems not worth to deploy an eArchiving infrastructure for EDSSI: there are no long-term preservation needs that are not covered by the institutions themselves (or their MS). EDSSI by design decentralises storage and management needs into all the participating HEIs, and already has its own common interface to manage all the required data from them, which is not generic nor compatible with eArchiving. As described above, the capacity of EDSSI to generate the evidences in the form of information packages as an alternative could be considered in the future, to be interoperable with other systems, but this investment would need to have a proper justification which currently does not exist, as no EDSSI process needs to consume or feed data of an eArchiving system, and if some HEI does it, it does it behind the common APIs of EDSSI. High levels of adoption of eArchiving would be needed before potential use cases could be identified.

## eInvoicing

eInvoicing Building Block is a digital solution that enables public sector contractors and companies to receive and process electronic invoices, according to the European standard, to reduce operational costs and times to facilitate cross-border trade operations and public procurement procedures.

### Description

This is an important but very case-specific building block, as it aims at offering a common way of issuing and accepting invoices in commercial transactions across Europe, in an electronic format. On 16 April 2014, the European Parliament voted on the 2014/55/EU directive on electronic invoicing in public procurement. Electronic invoicing is the exchange of an electronic invoice document between a supplier and a buyer (in this case, a public administration), issued, transmitted, and received in a structured data format which allows for its automatic and electronic processing, as defined in the directive. Electronic Invoices can generally be classified as visual invoices (PDF, JPG files) or structured data invoices (XML, JSON data structures). Also, both aspects can be combined (for example, with XML embedded on a PDF). The directive mandates all public sector bodies to have the capability to receive structured data invoices.

The Directive, then, called for the definition of a common European standard on electronic invoicing (materialised in the EN 16931 standard) at the semantic level, and additional standardisation deliverables which will enhance interoperability at the syntax level. It is important to notice that the standard is a semantic specification for the content of an invoice, not a specific syntax. Therefore, several syntaxes (technical specifications, XML schemas, etc.) might be used by different entities. When an invoice document is created in a syntax, that document must comply with the semantic specifications on EN 16931 and to the syntax binding for the relevant syntax (how the syntax elements match the semantic elements). That is, Member States can use international syntax standards, or their own internal syntax standards, as long as they can be unambiguously translated to other syntaxes, all of them following EN 16931. It doesn’t matter which are the tag names, or whether they use XML, JSON or any other representation syntax: the contents of the invoice and their meaning will be the same for all MS public bodies. The free-access documents obtained from this standardisation process are the following ones:

* The semantic data model: EN 16931-1: 2017[[8]](#footnote-7)
* The list of mandatory syntaxes that comply with the standard (the document has updates with the result of evaluation of compliance of different syntaxes): CEN/TS 16931-2: 2017[[9]](#footnote-8)

The CEF eInvoicing building block aims at promoting the uptake and accelerating the use of eInvoicing, according to the European standard, amongst public and private entities established in the EU (and participating EEA countries). Despite being usable for private transactions (Business to Business, Government to Citizen or Business to Consumer), they are not addressed in the context of the building block, so the solution is mainly (primarily) oriented to public sector administrations (when contracting services) in complying with EU eInvoicing legislation; and their related private sector counterparts involved in the invoicing process: suppliers for the awarded contracts and software solution and service providers (invoicing and accounting) in adapting their services to be able to communicate with the public bodies. So, the eInvoicing building block is therefore primarily designed to enable Business to Government and Government to Government transactions.

The two compliant syntaxes declared as mandatory to be accepted are the following:

* **OASIS UBL 2.1 (ISO/IEC 19845:2015)**[[10]](#footnote-9).
* **CII UN/CEFACT** Cross Industry Invoice (D16B, SCRDM - CII)[[11]](#footnote-10)

Other popular invoice syntaxes not compliant or compliant but not mandatory:

* **UN/EDIFACT (and ISO 26025 based XML version)**: It is a B2B oriented standard. Despite it is backed by the European Commission through the 94/820/CE agreement, it is not accepted by many public administrations, so it has not been considered to be added to the mandatory list, but is recommended to be accepted
* **Financial Invoice (based on ISO 20022)**: It has been analysed and lacks support for some essential components of the semantic model, so for this reason cannot be considered compliant.

The current scene shows that there exist many country-specific syntax standards, but no information on their compliance is provided. What can be observed is that not all of them list supporting the two mandatory syntaxes, so the displayed status by the MS shows that adoption is not yet in a final stage, and effective semantic interoperability cannot be guaranteed by now.

The most promising initiative in terms of interoperability is Peppol. The base syntax used for the implementation of the PEPPOL BIS 3.0 BILLING[[12]](#footnote-11) is the OASIS UBL 2.1, so compliance is guaranteed. But data compliance is not the only requirement for an effective interoperability, common access interfaces and gateways on a trusted common security domain are necessary to facilitate the exchange of data. To this end, Peppol has reused the eDelivery Building Block to deploy the Peppol network. This way, each Ms has a single gateway for receiving and sending invoices to other MS, and each MS is responsible for managing its own sender and receiver entities. Unfortunately, this network is not yet adopted by all MS.

The building block offers a set of tools to facilitate the compliance of the electronic invoice services with the directive, both at semantic and at syntax level (both for the mandatory and recommended syntaxes).

* **Implementation Checklist**: a guide with the key points for implementing compliant eInvoicing solutions (for public administrations, suppliers, and software service providers) and transposing the eInvoicing Directive into MS legislation (for the competent MS governance bodies).
* **Conformance testing**: A test infrastructure that allows software service providers and public administrations to check conformance of their eInvoicing solution against the semantic standard in a specific syntax from the ones described above. It provides a ready to use platform, and user support during the entire testing process.
* **Code Lists**: A set of lists of codes for fields with closed values (country, currency, etc.), as the standard defines which code lists may be used for each business term that has the data type "code". Some code lists are managed by external standards organisations and some others have been developed for the building block and are managed by CEF.
* **Validation Artefacts**: The semantic standard defines rules that go beyond the syntax, so to check that an invoice is compliant is not enough to test against the schemas of the syntax (what happens, for example, if an invoice has an issue date in the future?). CEF has developed a set of examples and validation artefacts (written in the Schematron language), so any invoice can be tested against the rules for compliance.

### Usability Analysis

EDSSI currently does not implement any invoice-related processes, and although chances exist, it currently has very limited potential in that sense, as no student-mobility related invoicing process between HEIs or between HEIs and EDSSI exist, and any other invoicing processes related to the stakeholders fall out of the scope of EDSSI (for example, between HEIs and students or providers).

In any case, the best approach to fulfil any invoice related process that might appear goes through integration with Peppol, given the circumstance that all MS join the Peppol network, and its use tends to generalise.

### Feasibility Analysis

As no use-case fits in the scope of this Building Block, the feasibility of implementing it cannot be analysed.

## eTranslation

CEF eTranslation Building Block is a set of user services to provide machine translation of texts and documents in the EU official languages and beyond, to EC officials, public administrations and lately to private small and medium business owners.

### Description

It is a free (for now, as changes on the service demand and on the goals of the new Digital Europe Programme might require charging fees), easy and secure translation tool to help in breaking language barriers in the EU. It serves three core user groups: officials working in European public administrations and on the EUROPEAN COMMISSION, small and medium-sized enterprise and University language faculty in all EU countries, Iceland, and Norway. Using eTranslation is safe (uploaded data is deleted at most 24h after) and the user keeps the ownership of the data at all times.

The tool is designed to translate from and to the official languages of the EU, and some others like Russian and simplified Chinese (work in progress)[[13]](#footnote-12)

Tabla

Descripción generada automáticamente

*Figure 10: Languages Supported on eTranslation*

The main component is a user web application with an interface. EU Login account registration is required, and then a self-registration on the service. The user can write text for translation or upload documents, to obtain the translated version. Document structure will be preserved on the translated version, and it can translate multiple documents to multiple languages in a single operation. It also supports different language domains (colloquial, formal, legal, EU related, etc.). Not all combinations of languages are supported in all domains.

Public administrations can also integrate eTranslation into their own information systems to add machine translation capabilities to their digital public services and their content to make them multilingual through the CEF eTranslation API. eTranslation provides an API for machine-to-machine request of translations (no information on whether text only is accepted or also documents can be submitted, but probably both will be supported). European and national public administrations, or cross-border EU projects supported from the CEF programme can integrate eTranslation in their digital services to enable users to use them in their own language in a simple and effective way. No public documentation on the API capabilities or security model are available. The only entry point for information referred is the helpdesk address: [help@cefat-tools-services.eu](mailto:help@cefat-tools-services.eu)

CEF eTranslation is built using neural network and machine learning algorithms that examine the full context of a sentence to produce highly fluent, readable translations. The service is continuously improved through the European Language Resource Coordination (ELRC) initiative, which identifies and gathers language and translation data relevant to national public services, administrations, and governmental institutions across all 30 European countries participating in the programme, to improve the service and the translation engines. An important role here is that of the contributors: those who wish to provide language resources to the system. eTranslation engine requires being fed, so it is continuously looking for language resources, such as translations, translation memories and bilingual (or multilingual) corpora of texts in machine readable format.

This effort is coordinated through the European Language Resource Coordination group. Any document generated and translated by a European public administration is a potential candidate to be submitted. Selection is done per-domain. Each MS has a national contact point, which is part of the ELCR that will coordinate the contribution efforts (funding is available to enforce contributions). All contributions are classified under the European Language Resource Coordination repository (ELRC-SHARE), which is used for documenting, storing, browsing, and accessing language resources that are collected through the ELRC.

User tools offered by the building block:

* **Translation service web front end**: Allows the user to input text and translate it to another of the supported languages. It also allows users to upload a series of documents (in the most common office document formats[[14]](#footnote-13)), which will be translated by a background process and the user can get them emailed or downloaded.
* **Multilingual Tweet**: A web application that facilitates publishing on twitter in multiple languages. From an input text, it allows marking multiple target languages. It generates a translation (with a disclaimer stating it is an automated translation) and allows editing and tweeting (with the embedded Twitter web snippet) each translation individually.
* **Natural Language Processing tool**: A web application that, given a document, can be asked to recognise and mark all named entities (locations, people, etc) and/or to catalogue the contained text in a category.
* **Speech-to-Text**: Speech recognition web application that converts audio or video files to text (only English supported for now).
* **Catalogue of Translation resources**: contains a huge compilation of translation and translation support tools, both from public administrations and from private companies.
* **Service helpdesk**: personal support service for users and integrators

### Usability Analysis

This building block is mainly user oriented. There is no service integration option as such for many of the translation tools, just being user applications (which any EDSSI participant can use for their own needs). The only tool with capability to be integrated is translator, but although an API is mentioned, no technical information is publicly available (only accessible on demand by requesting it on the support email), as it doesn’t seem to be the main goal of the service and the scalability is probably a big issue.

In any case, it is not advisable to do live machine-translation of legally sensitive documents like the Learning Agreement, or the Inter institutional agreements. They require human specialist translators. Also, being standard documents, translations can be provided beforehand.

In general, it is not advisable in general to depend on a live service for content translation. Translation is a heavy process, and can generate lag, so it is not worth it for most content, and even less for the cases in EDSSI, where content is mostly static. It can be of use to display human input when it needs to be read by another human that might not know the language of origin (for example, the IROs reading the OLA and similar), but careful analysis would be needed to discover opportunities in this sense. In any case, it is always important to present the original text along with the translation, as machine translation should always be an aid, never be allowed to override the original information. A future potential application for it could be developing a multilingual support chatbot for Erasmus+. Information of various student services (like housing, insurance, or posts on happenings during a student's staying) are also a target for this automated translation.

### Feasibility Analysis

The Building Block is easy to be used out of the box individually by the EDSSI personnel for all translation needs (it is, indeed, encouraged), but no feasible integration use-cases can be envisaged on the short or mid-term. A more mature integration API and translation infrastructure would be needed before it can be considered for live automated translation as a service. Also, the potential cost of this service would need to be considered on the cost-benefit analysis.

## European Blockchain Service Infrastructure (EBSI)

The European Blockchain Services Infrastructure Building Block is a set of efforts, coordination initiatives and infrastructures to support the adoption of blockchain-based technologies in public services

### Description

In 2018, All EU Member States, Norway and Liechtenstein formed the [European Blockchain Partnership (EBP)](https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership), with the common goal of exploring the potentials of blockchain-based services. This developed into the creation of the European Blockchain Services Infrastructure (EBSI). The basic goal is to leverage blockchain for the creation of cross-border services for public administrations in a trusted manner and reducing the dependency on centralised services. In 2020 began the deployment of the network of distributed blockchain nodes by public entities in many of the involved MS and the EC (currently 25 fully deployed and 11 in process), to support blockchain-based applications on a restricted set of use cases.

The main goal of this infrastructure is to enforce the design and deployment of public services taking advantage of the distributed capacities of the blockchain to:

* Avoid single points of failure which, on failure, bring down other public and private consumer service providers that depend on these critical services. Blockchain is redundant, and a node failure will not deny the access to data.
* Reduce the workload on these public services, by allowing trusted offline data transactions between the user and the consumer service, skipping the critical services except for the initial issuing of the data.
* Empower citizens to take control of their own data and move around online services using it, in the same trusted and secure way as if the data was in control of the public service (well, almost as trusted, because offline transactions must rely as well on the non-revocation of compromised or obsolete claims, and there can be a window of time where revoked data is still accepted by offline consumers if their revocation-check policy is not fully online).

Diagrama

Descripción generada automáticamente

*Figure 11: EBSI ledger access logic*

EBSI is a private consensus (permissioned, only the verification of entities with permission to do so are considered to reach the consensus) network with public data ledgers (it can be read by anyone). This means that no Proof of Work algorithm is used to allow a block write (dramatically reducing the computational time and energy consumption and avoiding the complexity of dimensioning the proof to the demand). Instead, only selected, well known, and authorised writers are allowed to do so (they provide a proof of authority). But access to ledger data is still public, which means that the data written on the ledger must be accessible by all (not any kind of secret, private or sensible data), no personal data (as the right to data deletion and the privacy cannot be granted), nor data that can be used to extract personal data (for example, hashed data, but be careful, as sometimes, using known data, unwanted information can be extracted from hashed data, so always use salting). Since applications need to store private data, EBSI offers traditional off-chain distributed storage. Both for blockchain and off-chain storage, multiple underlying technologies are supported (see figure)

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

*Figure 12: EBSI Supported Storage Technologies*

EBSI does not (in principle) provide direct and unrestricted access to the blockchain content for consumers or readers (as said above, it supports only selected use cases). It offers an abstraction layer with a set of case-specific standard APIs. This way, the node is agnostic to the underlying blockchain technology, and the end user applications are abstracted from the storage and access technologies. The architecture of an EBSI node is divided on three layers:

* **Infrastructure layer**: generic capabilities and connectivity to Blockchain network. Supports multiple underlying technologies ()
* **Chain and storage layer**: modules to handle all the blockchain and off-chain storage protocols supported by EBSI
* **Core services**: the standardised APIs which consumer services integrate to develop EBSI supported applications.

Interfaz de usuario gráfica, Diagrama

Descripción generada automáticamente

*Figure 13: EBSI Node Architecture*

Below is a detailed list of the APIs and tools offered on the core services:

* Identity
  + Verifiable Presentation API/Library
  + Verifiable Credential API/Library
  + Identity Hub API
  + DID Authentication Library
  + DID Registry API
* Trusted Registries
  + Trusted Apps Registry API
  + Trusted Issuers Registry API
  + Trusted SC Registry API
  + Trusted Schemas Registry API
  + Trusted IAM Registry API
* Wallet Libraries
  + Signing blockchain transactions
  + Reference implementations
  + Key management
* API Security Management
  + Reverse Proxy
* Integration API
  + Timestamp API
  + Storage API
  + Ledger API
  + Authorization API
  + Notification API
  + Revocation API
* Integration tools
  + API Catalogue
  + EBSI Generic Libraries
  + Apps Onboarding
  + User onboarding
  + EBSI Trusted App Store

As an alternative to using the Core Services APIs, applications may be integrated to native APIs where developers choose to create additional functionality to the ones available. The following figure is a breakdown of the available storage APIs (blockchain and off-chain)

Implementing a procedure over EBSI implies at least two parts: the issuing (by public entities) of trusted data (documents used as evidence in different situations), and the verifier (consumer, a public or private entity). The issuer will generate a Verifiable Credential, associated with verifiable data written on the ledger, and the verifier will request the Verifiable Credential, will verify it, and check the trust on the verification as stored on the ledger (and will also probably check for revocation). We’ll introduce these concepts:

* **Verifiable Credential** (VC, also verifiable claim): is a digital credential, to assert a set of data (in the form of a data structure or a list of attributes), and the necessary metadata to allow an entity (the verifier, a natural person, or a legal entity) to check the integrity and trust on the origin (authorship) of the data as coming from another entity (the issuer) using a cryptographic-based standard procedures.
* **Decentralised Identifier** (DID): is an opaque identifier that can uniquely identify a party (issuer, holder, verifier, see role table) in the data exchange and is fully under this party's control and used for referring to it. It can be anywise (one DID for all communications, could allow tracing the owner’s activity), pairwise or n-wise (each communication or domain can use a single identifier, preventing or limiting tracing).
* **Wallet**: is the user application that represents the holder. That is, it can negotiate the retrieval and delivery of VCs from the issuer and verifier respectively and keep them in a secure way under the user’s control. Wallet applications are needed in EBSI to handle the different VCs, because they can have a generic structure or very specific structures, that for an optimised user experience, need to be able to interpret and represent easily. Not all wallets will be able to support all kinds of VCs, so probably different use cases will have independent wallet apps. A sample implementation as a web app (most common use is as a mobile app) is provided by EBSI[[15]](#footnote-14).
* **Verifiable ID** (V-ID): V-IDs are a form of a Verifiable Credentials, used only for identification/authentication in a narrow sense (like a passport or national ID), includes personal data like the family name, first name, birth date, place of birth, unique identifier...
* **Verifiable Attestation**: a special form of a Verifiable Credential that a Natural Person or Legal Entity can put forward as evidence of certain properties or as evidence of an obtained permit/attestation/authorization.
* **Verifiable Presentation**: a structure that represents the data from one or more VCs which is passed from the holder to a Verifier. Its main goal is to minimise the amount of data revealed to verifiers (in pursuit of zero-knowledge proofing). Holders construct and share a Verifiable Presentation based on a "Verifiable Presentations Request" from a verifier. A Verifiable Presentation contains information from one or more VCs for the purpose of sharing this data with a Verifier. After creating a Verifiable Presentation EBSI states that “*a Holder signs the respective Verifiable Presentation using cryptographic keying material, particularly using the keys associated with their Decentralized Identifiers (DIDs), which are stored in a secure data store, including so-called Wallets*” and “*Verifiable Presentations will be submitted using the “technical signature” of the Holder for authenticity/integrity-purposes. However, ESSIFv2 does not consider the signing of presentations with legal binding value/effect*”. This assertion needs to be clarified: if the presentation is built by the holder and does not include any proof of integrity generated by the issuer (the original signature of the data extracted from the VC), the contained data can be tampered by the holder and shall not be trusted by the verifier. No EBSI case uses presentations for now, but this needs to be properly designed to avoid holes in the trust model.

In these concept definitions, we introduce the roles of the self-sovereign data interaction model, which EBSI implements and promotes. The following table shows the in detail:

| * Roles | |
| --- | --- |
| Issuer | The party that creates and issues Verifiable Credentials to Holders (a university, a public administration). |
| Holder | The party (the citizen wallet app) storing Verifiable Credentials that have been issued to them by an Issuer. |
| Verifier | The party who requests and verifies a Verifiable Credential from the holder as a condition to provide a service (a private company, for example). |
| Relying Party | Equivalent to “Verifier”. |
| ESSIF Onboarding Service (EOS) | Service that can onboard Natural Persons and Legal Entities to the EBSI ESSIF ledger (DID Registry, creates a did for the holder and registers it on the ledger) with authorization based on classical identification means (requests eIDAS authentication, and associates the eIDAS credential to the DID) |
| Trusted Issuer (TI) | The party that is authorised to issue certain types of VC (trust on TIs will depend on accreditation by a TAO listed in a relevant Trusted Issuer Registry). |
| Trusted Accreditation Organisation (TAO) | An organisation authorised to accredit other entities as issuers of VCs (it is listed in a relevant Trusted Accreditation Organisation Registry). |

*Table 1: Roles EBSI data interaction model*

Gráfico

Descripción generada automáticamente

*Table 2: EBSI Data Interaction Model*

In the classic pattern of information sharing, the user (citizen), or the verifier of the information, receives the information directly from the authentic source in real time. This pattern can include several intermediaries to ensure the trust. EBSI proposes a different pattern for exchanging information, distributed, and decentralized, as opposed to the classic pattern which is based on a centralized information exchange protocol. The Blockchain acts as the point of truth (information written there cannot be modified and is checked by many nodes), supporting the verification of the entities involved in the transaction (the DIDs and the authority that avails it are written there) and ensuring the authenticity of information without requiring real-time access to the information source. As explained before, no personal data must be written on the Blockchain. The Verifiable Credentials and personal information are kept in an application (the wallet), and only the proofs of trust on the issuer and the access points of the verifier are on the ledger. On the diagrams below, the general business logic of EBSI use cases is visually and sequentially explained, and then the logic sequence inside the EBSI node.

Aplicación

Descripción generada automáticamente con confianza baja

*Table 3: EBSI stack business flow*

Diagrama

Descripción generada automáticamente

*Table 4: EBSI Ecosystem Functional Overview*

Despite being mentioned in several spots above, now we will introduce all the use cases supported in EBSI, for the creation of cross-border services for citizens to manage their own identity, educational credentials, register documents, etc.

**Identity (SSI), ESSIF**

The goal is implementing a Self-Sovereign Identity model across Europe, combining the strength of eIDAS infrastructure with the EBSI capability to grant the users capability to create and control their own identity that will be accepted across borders. That is, the citizen will use the eIDAS Bridge API Service to authenticate in eIDAS and obtain an e-sealed VC (the above define Verifiable-ID) with the attributes in the eIDAS security assertion.

The VC structure contains:

* the issuance and expiration date
* the DID of the issuer (public institution, a MS trusted identity provider)
* the DID of the citizen (the holder)
* the personal details of the citizen (the attributes of the eIDAS assertion, at least the minimum dataset)
* the signature of the public institution (eIDAS e-sealing for the maximum acceptance and trust)

Below, an example of the implemented Verifiable ID (the eID specific VC structure):



*Figure 14: Example of eIDAS identity VC*

**Diploma**

Citizens gain control of their educational credentials by carrying them around in their wallet and not depending on the issuer to use them at will once obtained (to apply for a job, for a master’s degree, etc.).

Diagrama

Descripción generada automáticamente

*Figure 15: EBSI Diploma Use Case*

**Traceability (notarisation)**

Allows creating trusted digital audit trails, to automate compliance checks and prove data integrity. Its goal is to allow storing immutable reference data of documents or other digital artefacts that can be used at a later stage as proof of their authenticity/integrity and can be linked together to build a trusted, time-stamped audit trail (for example, for grant procedures).

**Trust data sharing**

Allows to securely share data (such as VAT identification numbers) among customs and tax authorities in the EU.

In the future, three new use cases will be deployed: Small and Medium Enterprise Financing, Asylum Process Management, European Social Security Pass

EBSI has developed the Early Adopters Programme to engage with external stakeholders to be the first to integrate with the infrastructure, an incubator to help early adopters imagine, build, and launch their EBSI pilot projects. 22 projects were selected in 2021 each partner has been given early access to the pre-production environment of EBSI and invited to develop their own pilot project to address a specific business or government online procedure involving the exchange of verifiable credentials (basically develop and integrate wallets, verifier, or issuer services), among the supported use cases. This is intended to test the strength of the core services and help improve them and converge with the needs of Europe's businesses and public administrations. All current pilots are on the diploma use case.

### Usability Analysis

Decentralised identity solutions are on the rise, and EBSI aims at becoming a reference in the European Public Sector scenario. It can reduce load and dependency on central components like the myAcademicID Hub.

The main synergy with EDSSI would be to develop a wallet integrated on the Erasmus+ app to carry student’s documentation and credentials (might require creating new core service APIs) like the OLA, entitlements, eIDAS auth, student card, etc. These user assertions and documents could be presented to the desired consumers (destination HEI, origin HEI, myAcademicID Hub, EC services) to fulfil almost all user-centred services, and many others could be redesigned to become user centred. A list of the potential services that this could support would be:

* Decentralised eIDAS authentication. It can be implemented per service provider or try a less-decentralised approach: integration on the myAcademicID hub, which would be a compromise solution between centralisation and full decentralisation.
* VC-based EduGAIN authentication.
* VC-based affiliation and entitlement providing.
* Decentralised transfer of academic records as a Verifiable Claim.
* OLA as a Verifiable Claim.
* European Student Card as a Verifiable Claim. Strong in-person authentication of the identity with a validation functionality on the app.

All of these new use cases would require extended analysis and planning, and if implemented, should be alternative to the existing procedures, not substitutes.

### Feasibility Analysis

Decentralised ledger technologies (DLTs) have potential and are advancing quickly, which is both an opportunity and a threat. They are fairly new and so far, the proof-of-concept implementations have been focusing on specific scenarios, therefore the adoption of these technologies requires further maturing along with proper cost-benefits analysis, also in relation to existing infrastructures. EBSI tries to create a unified infrastructure, not only at ledger level, but to offer unified service APIs, although at this point in time these APIs are specific to EBSI, not generic services across well-established solutions. EDSSI project builds on existing and well deployed infrastructures, such as EduGAIN and eIDAS, which are based on mature protocols (SAML and OIDC). This allowed the project to progress rather quickly also because trust models and privacy aspects are well-defined. The adoption of decentralised identities would require significant changes, that involves APIs, the definition of new trust models, the introduction of wallets etc. Whilst these aspects are very interesting and worth exploring, they go beyond the scope of this project. Tools like the wallet are also a limitation: you need a wallet app to be able to handle your VCs, but despite some standards exist, each wallet is open to handle any kind of data structure inside the VCs, so effective interoperability is still far away, and wallet apps tend to multiply, each one of them covering a very narrow set of use cases.

Also, it must be noted that EBSI use cases are, per infrastructure needs, fully user-centric, and despite EDSSI contemplates user-centric parts (like the federated authentication), most are business-to-business processes where the user interaction is fully specific to each participating institution (EWP, ESC). These use cases are extremely difficult and inefficient to redesign in an interoperable user-centric manner, as this would involve all stakeholders, including HEIs to change their basic processes in a coordinated way, so an effort of this dimension cannot easily be considered worth, and even less for a still emerging technology. We must also take into account the existing technological gap, as not all the potential users, mainly students, own a smartphone, which is the most usual platform for wallet applications, despite some existing as browser extensions or even as remote wallet agents.

Finally, we must take into account the knowledge gap. Despite the huge growth in digital alphabetisation in the latest years and in the usability of applications development, many potential users still find difficulties in understanding the implication of certain processes. This is even more concerning in regard to processes involving the management and custody of sensible personal data. The growing occurrence of phishing campaigns shows how lucrative and (still, after all) easy is to steal personal information. Decentralised identity processes usually require the user to coordinate the use of their mobile device with the desktop computer, through the reading of QR codes, which makes the process more complex and adds additional failure points. As not all students are familiar with this paradigm, forcing the common user into taking custody of his own data, through processes he is not familiar with, is something that will for sure raise the number of security incidents and support requests from confused users as well. EDSSI, as one of its driver goals, is designed to minimise and streamline the GUI displayed to the user, to optimise user’s experience and minimise incidences and support requests.

In summary: the potential and growth rate of EBSI make it attractive to leverage, but the emerging technology state is a risk that needs to be balanced. The best approach with this Building block is to explore the potentials of new side-services, or to do redundant pilot implementations of pre-existing processes using decentralised ledger technologies with the EBSI infrastructure (like, for example, the decentralised eIDAS auth at the MyAcademicID hub), but the technology is not mature enough to substitute existing processes. The NREN community and GEANT are already exploring how eduGAIN and the national Identity Federation could take advantage of DLTs and EBSI in particular.

## Big Data Test Infrastructure (BDTI)

This building block provides a set of services to assist public administrations to start experimenting with big data analysis. Through the provision of a catalogue with many sources of data to analyse, a catalogue of software products and methodologies for big data analysis, and a support test Infrastructure in a safe cloud environment to work with data, BDTI helps collect useful insights contributing to better public decisions.

### Description

Big data refers to the raw data or information that is available in big volumes, changes or grows at a high speed, and covers a wide variety of fields, often cross-sector. This requires new forms of processing, to be able to extract valuable information which will enable enhanced decision-making, insight discovery and process optimisation to the institutions. Big Data Test Infrastructure facilitates public administrations to be able to take their first steps in this field, without the need of provisioning the tools, the data, or the infrastructure by themselves. Only European Public Administrations can access the service. Policymakers, Data scientists and IT practitioners are the target profiles.

BDTI offers three major tools:

* **BDTI Test Infrastructure**: A virtual testing environment built on the Amazon AWS stack that provides pre-configured and ready to use tools for analytics experiments. The mission of this service is to allow users to play around with the big data software tools without wasting time on installation and settings and supporting public entities that do not have initial access to big infrastructures. European Public Administrations that would like to experiment with data analytics can apply to run a pilot project on the BDTI test infrastructure service. They will have to provide some background information about the planned pilot and on the size of the required infrastructure. Based on this, the BDTI team will assess the request and provide the virtual environment that is best suited for their needs, as well as documentation and introductory guidelines on how to use the environment, which is Linux based. Supported programming languages are Python, Java, Scala, and R. The maximum duration of a project is six months. After the end of this time window, the instance will be frozen and BDTI will provide the user with guidance on how to deploy their own analytics environment.
* **Data Sources Catalogue**: a centralised repository with a list of reliable and accessible sources of big amounts of data in different domains (mainly sources of open data) that will help the users to find reusable data for the execution of their experiments and data analytics use cases on the infrastructure. Each entry as well contains guidelines on how to access the data (how to develop technical interfaces using the APIs of the source). The catalogue is maintained and updated regularly; suggestions are accepted through the helpdesk.
* **Big Data and Analytics Software Catalogue**: a centralised repository with a list of open-source analytical software tools useful for implementing big data solutions[[16]](#footnote-15). They are classified by functional categories. Most of the tools in the catalogue come already pre-installed in the pilot instance that is created over the test infrastructure for the user to run the experiments, but any of them can be requested to be included.

### Usability Analysis

This building block is just a playground infrastructure, not designed to support any production services, nor to offer supporting services for other services. It presents a limited usage schedule (any work in progress gets deleted after 6 months), after which, the user is invited and assisted to deploy its own playground.

It can be a help in exploratory tasks, but no strong needs can be identified related to this Building Block. Also, many partners in EDSSI already have big infrastructure support and deal with huge amounts of data, so they most probably already have their own big data exploitation environments and processes (usually for logging and statistics).

### Feasibility Analysis

As no use-case fits in the scope of this Building Block, the feasibility of implementing it cannot be analysed.

## Context Broker

The CEF Context Broker is a component built to collect data from different sources and support smart decisions (such as in Smart Cities projects).

### Description

The Context Broker is a digital platform that enables the integration of gathered data and includes insights for further exploitation of the data. In 2016, the European Commission promoted the definition of a standard Context Information Management system (CIM) API, using FIWARE NGSI as a base. The result was NGSI-LD9, supporting JSON Linked Data (JSON-LD). The NGSI-LD API specification is compatible with the FIWARE NGSIv2 API specifications.

Diagrama

Descripción generada automáticamente

*Figure 16: Fiware ecosystem and related software*

The Context Broker (Orion being the reference implementation) is a generic enabler for sensor and context data management, and one of the central elements of the Fiware Ecosystem (Fiware supports other use cases beyond context brokering). Orion is designed to facilitate coordination between a set of sensors (or “actuators”, because some sensing devices can react to context modifications performed by the consumer apps) and the consumers of the data (control dashboards, event registries, event processors, etc.) through the implementation of a standard generic central broker. The broker implements a generic management system and protocol that allows to model any kind of sensor entity, with any arbitrary structure of internal properties through a recursive data model (the attributes can be of attribute type and so on) and providing built-in types for basic data items. At an infrastructure level, the multiple level brokers can be deployed in a tree structure, to abstract the handling of sets of sensors. This is what is called “context broker federation”, and allows two ways of acting: push federation, where changes in a context broker are notified to another context broker, and pull federations, where a context broker forwards queries down to other context brokers.

So, the system is modelled through the creation of entities (the sensors, which are of a type and have a unique identifier), that have a set of attributes (that can be read, modified, or deleted, or even new properties can be added on runtime). Any attribute can hold a property of the entity (identified by a name), of a type (a basic type or a sub-object), with a specific value, and a set of metadata items referring to this property (each metadata item has the same form)

The first version of the model used JSON as the representation language, but the newest version commissioned by the EC includes a JSON-LD specification, which provides built-in data schema validation support and stronger type and content validation mechanisms.

The context broker, besides the common entity representation model, also provides a management API (NGSI-LD), which is the one that allows the consumer applications to interact with the entities on the system, and the entities to provide their data. The API allows the sensors to register (by creating an entity) and update their data (the entity can be updated as a whole, or each attribute or metadata item can be updated individually), and consumer services to exploit the registered sensor data and extract event information, individual or grouped by logical areas, physical areas, or any other attribute. The query API allows for a rich query parameter specification, as it enables the clients to do updates, queries or subscribe changes on the context information (on the entities and their properties).

Diagrama

Descripción generada automáticamente con confianza media

*Figure 17: Fiware Context Data Model*

This model offers a powerful and standard way of modelling IoT networks within a common security domain. It must be noted that modelling is not limited to a single security domain. Fiware provides an Identity Manager (Keyrock) that integrates with the Context Broker to provide Oauth2 based access control, supporting even Attribute Based Access Control, so, it allows to define a rich and fine-grained security and access control model.

The importance of the generic API and model design of the Context Broker is a key point, as it enables any software or hardware manufacturer to build Fiware compliant sensors that can be easily integrated. But to even facilitate this task further, Fiware offers another standard component that interfaces between the context broker and the specific sensors, implementing modules to deal with specific IoT protocols, the Backend Device Management Generic Enabler (DCA-IDAS being the reference implementation).

Diagrama

Descripción generada automáticamente

*Figure 18: Schema of the Fiware Backend Device Management*

Same happens for the apps that exploit the sensor data: The generic model and standard query/registration/modification API allows the software to be easily portable and adaptive. Topology can be modified and rearranged on runtime, new sensors from new manufacturers, or new consumer apps can be added whilst reusing all the infrastructure in the middle and with no hard changes on the APP, which will only change at a semantic level if new requirements appear (if new properties are added on the sensors or new query needs appear).

Diagrama

Descripción generada automáticamente

*Figure 19: Example of a Fiware Smart Cities deployment with IoT sensors*

As a final note, it is worth mentioning that Fiware has adopted the CEF eDelivery Building Block as another generic enabler on its ecosystem.

### Usability Analysis

Despite being one of the most mature and useful Building blocks, the use cases EDSSI implements can hardly fit on it. The component is designed to be a central broker mainly in IoT contexts. That is, the entities represented there are mainly state-based sensors or actuators over an open world environment, that need to be controlled and exploited over a control network by consumer applications. EDSSI components are more complex, and their operations do not fall in the context described, as they fulfil advanced business flow beyond basic sensing/acting on an environment. For the machine-to-machine communications, EDSSI has for the EWP part, although using the context broker could be an option, the already existing solution is a better fit. The arguments for this are better described in the eDelivery section, which is another Building Block that covers this need, and is much better fit for purpose than the Context Broker could be.

### Feasibility Analysis

As described above, no use case in EDSSI can be identified to fit the usage of the Context Broker. It is neither feasible to use the Context Broker for the machine to machine communications, as it does not provide any additional benefit (in fact, using it would require a forced design, very negative for EDSSI), and would add an immense overhead to the development, management and maintenance of the solution, as it does not allow to directly model the needed APIs and the security model is not even close to the EDSSI needs (it could be modelled with additional components, but to a cost that cannot be even considered).

## Only Once Principle (OOP)

The Once-Only Principle will enable public entities to share citizen data between themselves, so that the citizen accessing a public service just will need to deliver data once, and just ask the data to be transferred from the original recipient to the new recipient in subsequent public service accesses requiring that data.

### Description

This building block is still in progress (to be launched in 2023), so the available information and the analysis we can perform is limited and may be subject to change. The OOP is a basic abstract goal for the EC: to avoid citizens having to provide the same data over and over to each public service it interacts with. This principle applies to many funded projects (among them, EDSSI), but the building block originates from the outcomes of two projects: TOOP[[17]](#footnote-16) (more infrastructure-centred) and SCOOP4C[[18]](#footnote-17) (more on the citizen dimension of the principle). As we will see later, SDG regulation is the next step in the application of the principle, and the pilots are converging to help define the requirements of the implementation act for the regulation. In the last year and a half, DE4A[[19]](#footnote-18) project has launched a serious piloting initiative, with the goal of setting up production services aligned with the SDG regulation and providing assessment to the SDG implementation act developers.

Both TOOP and DE4A projects are pilots that explore the application of the once-only principle on a cross-border pan-European scale, focusing on reducing the administrative burden of businesses by digitalising common administrative procedures and developing an infrastructure to facilitate the exchange of citizen data among public bodies. The infrastructure of choice in both cases is an eDelivery network (in the case of DE4A, multiple exchange paradigms are being implemented, through the development of rich eDelivery connectors).

TOOP focused on connecting the MS specific data exchange systems to eDelivery, and doing some synthetic piloting on these fields:

* Cross-border business data exchange: interconnect business-registers to exchange company data, certifications, licenses, etc.
* Cross-border public procurement: exchange the required documentation from the applying company, for the awarded contractor, etc.
* Cross-border exchange of maritime crew and ship certificates.

DE4A will do live piloting of some of the SDG procedures:

* Cross-border application for higher education studies, recognition of diplomas and request of grants.
* Change the residence address for a citizen in a cross-border environment, request birth/marriage certificates, request pension information.
* Businesses applying for online public procedures across-borders, registration in business register

OOP Building Block states that it contributes to the Single Digital Gateway Regulation (which promotes online access to a set of common online procedures in EU Countries). It is still to be known how the CEF Building Blog relates to the implementation of the SDG technical solution, but most probably, the architecture blueprint, specifications and software will be part of it. All the above-mentioned pilots use eDelivery. This is a key point, as it shows that eDelivery could take up a central role in the data exchange strategy of the EC.

### Usability Analysis

Mostly, and given the lack of any more solid data, the eDelivery analysis applies here. Only the new regulatory and strategic dimensions of future convergence and interoperability add some benefit to the adoption of eDelivery: Erasmus+ procedures could be redefined to be compatible with the technical solution for the SDG

### Feasibility Analysis

First point to be established here is that OOP Is not yet a Building Block, so it is impossible to evaluate and plan over what is not yet properly defined, so for the moment, the conclusions resort to those drawn on the eDelivery section. As explained there, the effort of converging with SDG would be huge. A very well-established solution and enough resources would be needed to even consider taking this effort pays off. In any case, it is a very long-term plan, with a very long-term return of investment period.

# Analysis of Other Relevant European Digital Infrastructures

Despite not being a Building Block, the closeness to them and to the business objectives of EDSSI makes it necessary to include some analysis on the following initiatives.

## Single Digital Gateway (SDG)

Single Digital Gateway technical solution is an upcoming infrastructure managed by the EC and the MS, that will enforce the application of the SDG regulation that promotes public procedure interoperability across-borders, to pursue the effective application of the Only Once Principle.

### Description

Regulation (EU) 2018/1724 of the European Parliament[[20]](#footnote-19) establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services is what we know as the SDG regulation. Paper-based procedures, scattered information, non-harmonised public procedures, etc. are situations that hold back the concept of a real single market, as freedom of goods, services, capital, and people is not fully ensured due to these barriers. SDG regulation attempts to address these problems.

The single digital gateway aims at facilitating online access to information, administrative procedures, and assistance services required by EU citizens and legal entities in other EU countries. The principle behind this is facilitating the accomplishment of the Only Once Principle across-borders in Europe.

Following the approval of the regulation, a committee, composed of working groups of MS experts have been formed to design the detailed aspects of the technical solution to enforce the SDG. The outcomes of this analysis will be included in an implementing act for the SDG technical system (due June 2021 according to article 14.9). The DE4A project, having as partners key MS officials, plays an important role in the collaboration with these working groups: DE4A outcomes influence the working groups and the decisions taken by the groups are included in DE4A, to seek the maximum alignment with the future technical system.

By the end of 2023 access to 21 online procedures (registering a car or claiming a pension, HEI enrolment)[[21]](#footnote-20) is due in all EU countries. The most important administrative procedures for cross-border users will be mandatorily available online in all EU countries. A system to transfer documents needed for these procedures between national authorities in different EU countries will also be included (i.e., a diploma obtained in one country shall be shared with the national authorities of another, where it is needed to enrol, or to take a job).

The setting up of a technical system for the cross-border automated exchange of evidence and application of the Once Only Principle will allow citizens and businesses to request any official evidence, required by an administration as part of several key online procedures (see ANNEX II of the regulation), to be exchanged directly between administrations, even in different Member States, and not requiring the citizen to provide that data multiple times.

As the regulation foresees, the procedures at the MS shall not change due to the regulation. The evidence requirements will be the same, and only the option to retrieve them through the SDG technical system will be added. This is an important detail, as the use of SDG must be optional for the citizen, who has the right to provision the data in the former way the service implemented and can decide to stop the SDG use at any time of the process the user decides to, resorting to the old procedure and evidence provision. The data being transferred must be minimal for the purpose, and the citizen has the right to preview the data before it is transferred, so it can decide to stop the transfer.

### Usability Analysis

The situation described in the OOP section applies here. Only thing that can be added is that some generic SDG procedures could be reused for Erasmus+.

### Feasibility Analysis

The only thing SDG adds to this analysis from what has already been said on the OOP section is the mandatory aspect of the regulation. At some point in the future the HEIs will need to implement the SDG procedures. Since they will have an established infrastructure, that might be the window of opportunity to consider migrating the EWP services to the SDG technical solution. But this is a very long-term sustainability decision. For now, it just requires following the developments of SDG and consider collaborating with them to ensure that EDSSI requirements are covered by the solution.

# References

1. "Once Only Principle." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Principle. Accessed October 26, 2021.
2. "CEF OOP is progressing on the SDG Once Only Technical System | TOOP.EU." TOOP Project, https://toop.eu/node/420. Accessed October 26, 2021.
3. "Domibus." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus. Accessed October 26, 2021.
4. "EBSI." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI. Accessed October 26, 2021.
5. "Learn - EBSI Documentation." CEF Digital, https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/Learn. Accessed October 26, 2021.
6. "EBSI project overview." CEF Digital Code Server, https://ec.europa.eu/cefdigital/code/projects/EBSI. Accessed October 26, 2021.
7. "Big data test infrastructure." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/big+data+test+infrastructure. Accessed October 26, 2021.
8. "eArchiving Knowledge centre." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eArchiving+Knowledge+centre. Accessed October 26, 2021.
9. "Technical Specifications." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Technical+Specifications. Accessed October 26, 2021.
10. "eInvoicing." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eInvoicing. Accessed October 26, 2021.
11. "Obtaining a copy of the European standard on eInvoicing." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Obtaining+a+copy+of+the+European+standard+on+eInvoicing. Accessed October 26, 2021.
12. "GitHub." Connecting Europe / eInvoicing-EN16931: Validation artefacts for the European eInvoicing standard EN 16931, https://github.com/ConnectingEurope/eInvoicing-EN16931. Accessed October 26, 2021.
13. "The Peppol eDelivery Network Specifications - Peppol." Peppol, http://peppol.eu/downloads/the-peppol-edelivery-network-specifications/. Accessed October 26, 2021.
14. "eSignature Overview." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature+Overview. Accessed October 26, 2021.
15. "What is eSignature." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+eSignature. Accessed October 26, 2021.
16. "Digital Signature Service." DSS, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Digital+Signature+Service+-++DSS. Accessed October 26, 2021.
17. "How does it work?" European Commission, https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773030. Accessed October 26, 2021.
18. "Context Broker." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Context+Broker. Accessed October 26, 2021.
19. "Documentation Context Broker." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Documentation+Context+Broker. Accessed October 26, 2021.
20. "eTranslation." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eTranslation. Accessed October 26, 2021.
21. "CET-AT Service Catalogue." European Commission, https://cef-at-service-catalogue.eu/catalogue/browse/c4fbb39f-e441-4bfe-abca-e39a2a0238ba/. Accessed October 26, 2021.
22. "All CEF services." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/All+CEF+services. Accessed October 26, 2021.
23. "CEF Digital Home." European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home. Accessed October 26, 2021.
24. "Developers Catalogue." FIWARE, https://www.fiware.org/developers/catalogue/. Accessed October 26, 2021.
25. "Getting Started with NGSI-v2." Step-by-Step, https://fiware-tutorials.readthedocs.io/en/latest/getting-started.html. Accessed October 26, 2021.
26. "Swagger UI." Fiware, https://swagger.lab.fiware.org/?url=https://raw.githubusercontent.com/Fiware/specifications/master/OpenAPI/ngsiv2/ngsiv2-openapi.json. Accessed October 26, 2021.
27. "API Walkthrough." Fiware-Orion, https://fiware-orion.readthedocs.io/en/master/user/walkthrough\_apiv2/index.html. Accessed October 26, 2021.
28. “FIWARE Enablers” Fimac, https://fimac.m-iti.org/5a.php. Accessed October 26, 2021.
29. "Documentation Home." Fiware-IdM, https://fiware-idm.readthedocs.io/en/latest/. Accessed October 26, 2021.

| [**www.edssi.eu**](https://edssi.eu/) |
| --- |

1. <https://ec.europa.eu/tools/lotl/eu-lotl.xml> [↑](#footnote-ref-0)
2. <https://nowina.lu/solutions/java-less-browser-signing-nexu/> [↑](#footnote-ref-1)
3. <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+conformant+solutions> [↑](#footnote-ref-2)
4. <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP> [↑](#footnote-ref-3)
5. <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML> [↑](#footnote-ref-4)
6. <https://public.ccsds.org/pubs/650x0m2.pdf> [↑](#footnote-ref-5)
7. Software can be found at <https://github.com/E-ARK-Software> [↑](#footnote-ref-6)
8. <https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:71870,1883209&cs=18AD38D91FB33B5CBD300B5C8FC9AB681> [↑](#footnote-ref-7)
9. <https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:60603,1883209&cs=123AC2047CD007B80B02109216D18F76A> [↑](#footnote-ref-8)
10. UBL Website:<https://www.oasis-open.org/committees/ubl/>, Used XML Schemas:<http://docs.oasis-open.org/ubl/os-UBL-2.1/UBL-2.1.zip> [↑](#footnote-ref-9)
11. XML Schemas overview:<http://www.unece.org/cefact/xml_schemas/index.html>, Used XML Schemas: <http://www.unece.org/fileadmin/DAM/cefact/xml_schemas/D16B_SCRDM__Subset__CII.zip> [↑](#footnote-ref-10)
12. <https://docs.peppol.eu/poacc/billing/3.0/bis/> [↑](#footnote-ref-11)
13. The currently supported 27 languages are Bulgarian (BG), French (FR), Italian (IT), Romanian (RO), Croatian (HR), Finnish (FI), Latvian (LV), Russian (RU), Czech (CS), German (DE), Lithuanian (LT), Spanish (ES), Danish (DA), Greek (EL), Maltese (MT), Slovak (SK), Dutch (NL), Hungarian (HU), Norwegian Bokmål (NB), Slovenian (SL), English (EN), Icelandic (IS), Polish (PL), Swedish (SV), Estonian (ET), Irish (GA), Portuguese (PT) [↑](#footnote-ref-12)
14. .txt, .doc, .docx, .odt, .ott, .rtf, .xls, .xlsx, .ods, .ots, .ppt, .pptx, .odp, .otp, .odg, .otg, .htm, .html, .xhtml, .h, .xml, .xlf, .xliff, .sdlxliff, .rdf, .tmx and pdf [↑](#footnote-ref-13)
15. To use it, the test user needs to create an EBSI Wallet account: open the EBSI Wallet and authenticate via your EU Login, then setup your EBSI account to follow the user journey. In your wallet, you will create your own Decentralised ID and a set of public-private keys Open a request on the Sample Verifiable ID Issuer website to receive your verifiable ID. The Sample Verifiable ID Issuer verifies the request and issues the ID Verifiable Credential, which will be stored in your wallet. With your digital ID, you will have access to other services on the EBSI platform. [↑](#footnote-ref-14)
16. Hadoop, Ganlgia, Hive, Hue, JupyterHub, Livy, Mahout, MXNet, Pig, Spark, Tensorflow, Zeppelin, RStudio, Solr [↑](#footnote-ref-15)
17. https://toop.eu/ [↑](#footnote-ref-16)
18. https://www.scoop4c.eu/ [↑](#footnote-ref-17)
19. https://www.de4a.eu/ [↑](#footnote-ref-18)
20. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\_.2018.295.01.0001.01.ENG [↑](#footnote-ref-19)
21. See Article 6 and ANNEX II of the regulation [↑](#footnote-ref-20)