EUROPEAN COMMISSION
DIRECTORATE-GENERAL INFORMATICS

Directorate D - Digital Services
DIGIT D3 - Trans-European Services

eTrustEx WEB

Component Offering Description

Date : 3/07/2019

Document Status:

Status
Final

Document Approver(s):

Name	Role
POPGEORGIJEV Kristof	Project Officer - eTrustEx, DG DIGIT D3.002

Document Reviewer(s):

Name	Role
POPGEORGIJEV Kristof	Project Officer - eTrustEx, DG DIGIT D3.002

Summary of Changes:

Version	Date	Created by	Short Description of Changes
0.01	01/03/2019	Violeta POPESCU	First draft of the document
0.02	25/04/2019	Kristof POPGEORGIJEV	Review & comments
0.03	02/05/2019	Violeta POPESCU	Implement the suggested changes
0.04	01/07/2019	Kristof POPGEORGIJEV	Review & comments
0.05	02/07/2019	Violeta POPESCU	Implement the suggested changes
1.00	03/07/2019	Kristof POPGEORGIJEV	Finalisation of the document

Table of Contents

1. INTRODUCTION

The present document is the Component Offering Description (COD) of the eTrustEx Web secure message exchange application.

eTrustEx Web is a web application that can be used in any Policy Domain of the EU in order to enable secure and reliable exchange of documents and data, across borders and sectors, between Public Authorities and businesses at European, national and local level.

It allows the exchange of files between users, or users and systems via a user-friendly interface. Depending on the business needs and location of the parties involved in the exchange of messages, eTrustEx Web can be used by an organisation in combination with other interoperable components. The following scenarios are possible when using eTrustEx Web:

- used in combination with eTrustEx Node[1] in order to allow exchanges between users inside the same organisation, or between the organisation and external parties;

- used in combination with eTrustEx Node in order to allow exchanges between users (inside or outside an organisation) and systems located inside an organisation;

- used in combination with eTrustEx Node and CEF eDelivery Access Point[2] in order to allow the exchange of files from users to systems located outside an organisation by using the AS4 standardised message exchange protocol.

Regardless of the scenario chosen, TrustEx Web has to be hosted and maintained together with the central component of the platform, the eTrustEx Node, in charge of storing and exchanging messages between the sender and the receiver of the message.

---

[1] More information about the eTrustEx Node can be found in the eTrustEx Node Component Offering Description. See reference R1.

[2] More information about the eDelivery Access Point can be found in the CEF eDelivery Access Point Component Offering Description. See reference R2.

The below diagram summarizes the possible exchange interactions through eTrustEx Web.
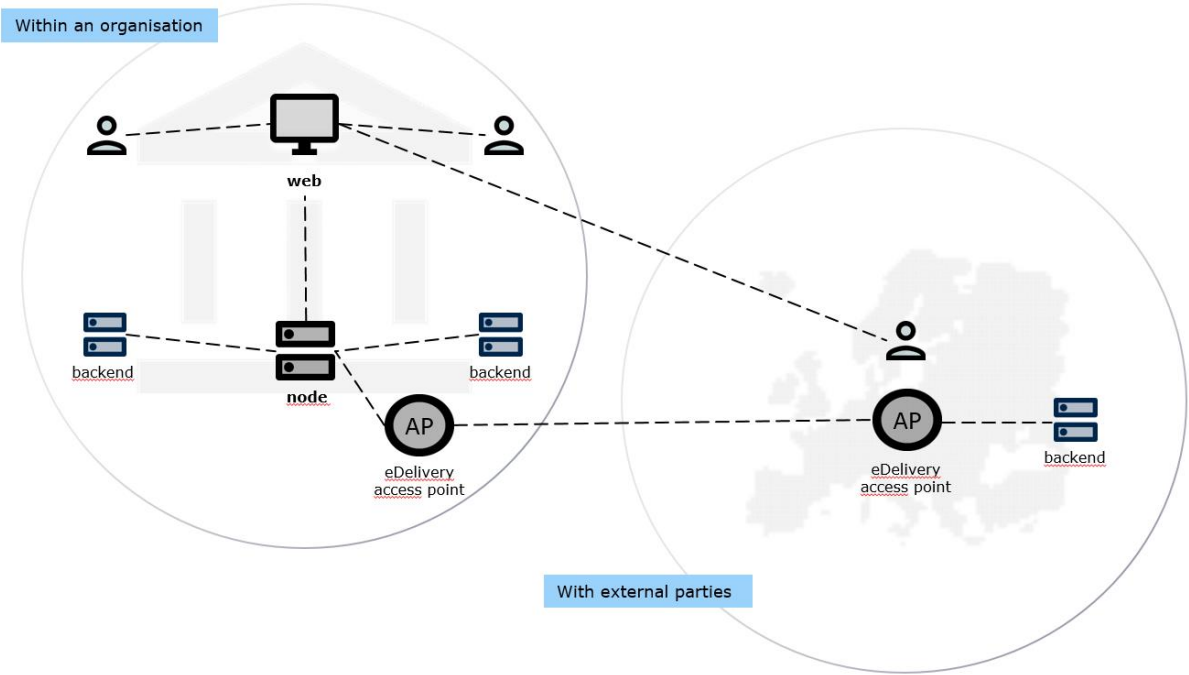

Figure 1 - Exchange interaction through eTrustEx Web

The development of the eTrustEx platform is funded by the ISA[2] programme. It is offered as an open source software tool via Joinup[3] and provided as a service to the EU Institutions and Agencies[4].

---

[3] https://joinup.ec.europa.eu/solution/open-e-trustex, or please see reference R3.

[4] EU Send web portal: https://europa.eu/!wp94dH

2. KEY FEATURES

Key feature	Description
Interoperability	Defined as an OASIS technical specification, which is built on top of existing technical specifications of proven interoperability: MIME, SOAP and WS-Security.
Reliable	Guarantees once-and-only-once delivery via the exchange of receipts and additional requirements on both Sender and Receiver side.
Check summing	All data transfers are verified with checksums in order to avoid data corruption during transfers.
Support of groups of files	The application allows the transfer of groups of linked files.
Confidentiality	The system ensures that the transferred documents are not viewed by anybody else than the Sender and the final recipient. It is guaranteed at transport level by the use of HTTPS connections, and supported at message level via public keys that can be used in end-to-end encryption.
Authentication	The system ensures that the users / systems involved in communication are really who they say they are.
Authorization	The system ensures that the users / systems only have access to the resources they are allowed to.
End-to-end encryption	Only the users involved in the communication can read the messages. In principle, it prevents potential eavesdroppers from being able to access the cryptographic keys needed to decrypt the conversation.
Integrity	The system guarantees the integrity of the transferred files using XML digital signatures.
Support of large files	The application allows the transfer of large files (up to 500 MB each) of any type.
Auditing	It is ensured by logging of all the calls and by storing the transactions in the system's database.
Retention policy	It supports automatic removal of messages that are too old and not relevant anymore to the business.
Notifications	It supports the sending of notifications to the Sender or Receiver of a message. eTrustEx Web can also send emails to personal email addresses whenever a new message is available for the Receiver.
Configurable	A number of the above-described key features are configurable in the system (e.g. retention policy, notifications, confidentiality etc.).
Authentication service	Open eTrustEx uses basic authentication and can be integrated with any custom authentication system. eTrustEx Web deployed within the European Commission premises is using the EU Login authentication.
Non-repudiation	It is ensured by the signed technical acknowledgements generated by eTrustEx Node, that can be used as a proof of submission (the party submitting the message is responsible for storing the acknowledgement).

3. KEY CONCEPTS

In eTrustEx Web, the transfer of files is done Party to Party. A **Party** represents an organization/part of an organization/project using the eTrustEx platform in order to exchange messages. A Party can have one or more **users**; all users of a Party have access to the same messages received/sent by that Party. In addition, a user can have access to multiple Parties.

In order to enable the communication between two Parties, the eTrustEx system administrator must create a logical communication channel, called Interchange Agreement (ICA). ICAs also define some attributes for the communication between the Parties, like the confidentiality (encryption) and integrity (signature) levels. The eTrustEx system administrator creates the Parties, the ICAs and one Party Administrator per Party. The Party Administrator can create and manage the users belonging to that Party. For more details regarding the key concepts used in eTrustEx Web, please consult the User Guide[5].

---

[5] See Reference R5

4. MESSAGE EXCHANGE FLOW
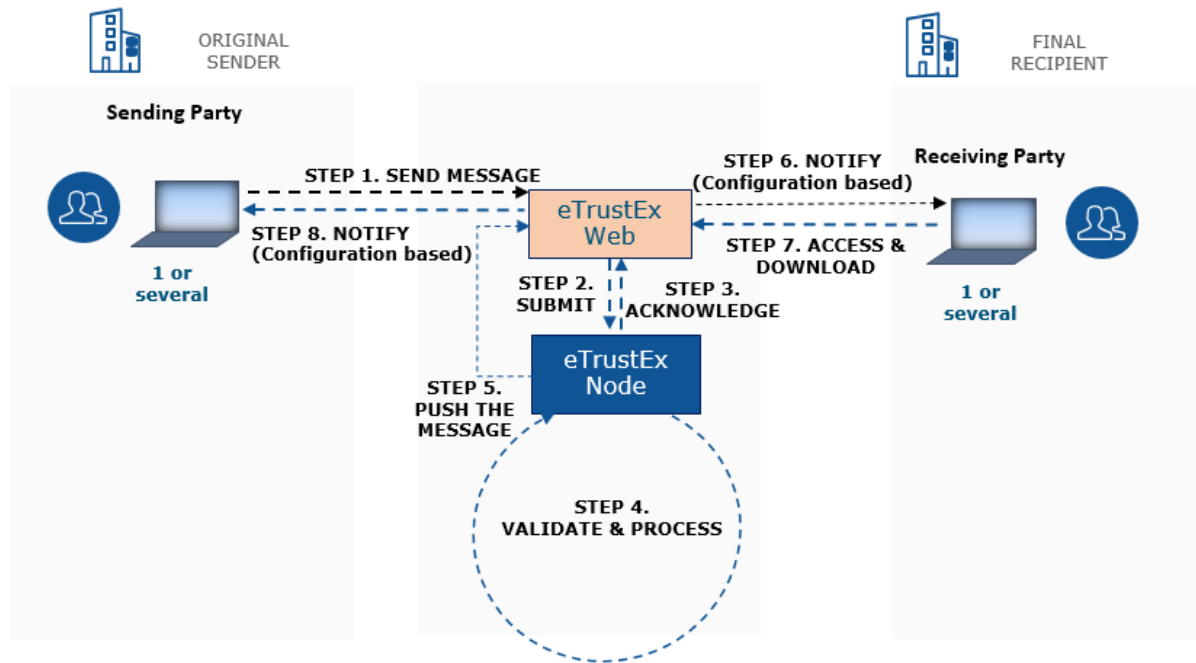
4.1. User to User

Figure 2 - Message Flow – user to user

Below is the conceptual description of the processing of a document submitted by a sender represented by a user to a receiver also represented by a user through eTrustEx Web. eTrustEx Web is used by the users in order to send / receive the message. However, eTrustEx Web always relies on eTrustEx Node for storing files and messages and for dispatching them to their receivers.

1) The sender starts by uploading the files and sending the message to the receiver by using eTrustEx Web;
2) eTrustEx Web converts the message to a format accepted by the eTrustEx Node web service interface and submits it to eTrustEx Node;
3) eTrustEx Node performs the synchronous processing and sends back to eTrustEx Web an acknowledgment of reception;
4) The message is further processed (asynchronously) by eTrustEx Node including extra validation where needed;
5) The message is pushed back to eTrustEx Web into the inbox of the receiving party;
6) eTrustEx Web may notify the receiver of the arrival of the new message via an e-mail notification;
7) The receiver can connect to eTrustEx Web in order to access the message and download the files;
8) eTrustEx Web may notify the sender regarding the status change of the message, if such configuration is in place.
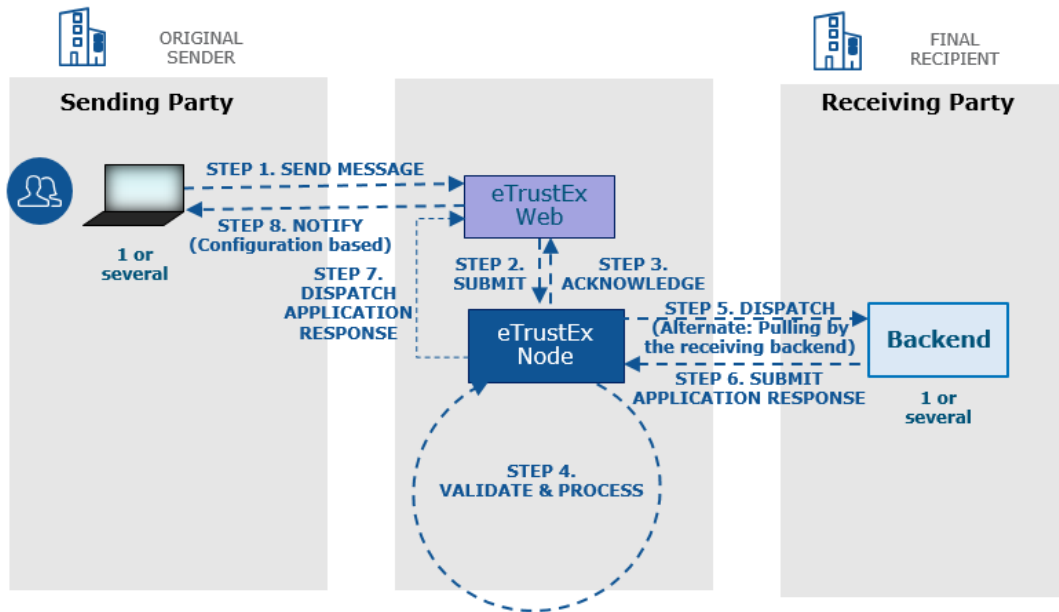
4.2. User to Machine

Figure 2 - Message Flow – user to machine

Below is the conceptual description of the processing of a document submitted by a Sender represented by a user to a Receiver System through eTrustEx Web and eTrustEx Node from start to finish. eTrustEx Web is used by the user in order to send the message.

1) The Sender starts by uploading the files and sending the message to the Receiver by using eTrustEx Web;

2) eTrustEx Web converts the message to a format accepted by the eTrustEx Node web service interface and submits it to eTrustEx Node;

3) eTrustEx Node performs the synchronous processing and sends back to eTrustEx Web an acknowledgment of reception;

4) The message is further processed (asynchronously) by eTrustEx Node including extra validation where needed;

5) The message may be forwarded to the Receiver's Backend System, or the Backend System of the Receiver may pull for the message;

6) Once the document processing is complete in the Backend System of the Receiver, its status[6] may be updated based on an Application Response sent by the Receiver to the Sender of the message;

7) eTrustEx Node dispatches the Application Response sent by the Receiver to eTrustEx Web;

8) eTrustEx Web may notify the user regarding the status change of the message, if such configuration is in place.

---

[6] Each message has a status that evolves based on a defined workflow. The status is transparent to the users and that becomes final once it is changed due to an application response sent by the receiver to the message sender.
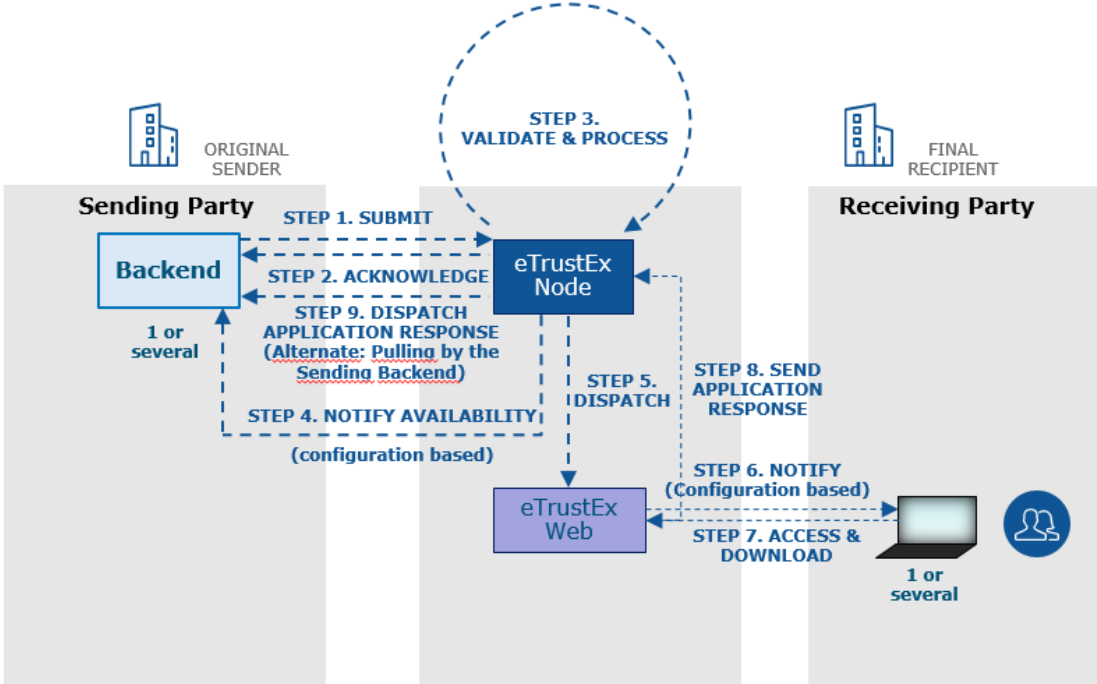
4.3. Machine to User

Figure 3 - Message Flow - machine to user

Below is the conceptual description of the processing of a document submitted by a Sender System to a Receiver represented by a user from start to finish. eTrustEx Web is used by the user in order to visualize the message and download the files.

1) The Sender starts by creating the electronic document using its Backend System, converts it to a format accepted by the eTrustEx interface and submits it to the Receiver via this web service interface;

2) An acknowledgment of reception is immediately sent back to the Sender;

3) Once successfully received, the message is processed by eTrustEx including extra validation where needed;

4) After the message is processed, the Sender's Backend System may be notified of the availability of the message;

5) The message is then dispatched to eTrustEx Web;

6) eTrustEx Web may notify the user regarding the arrival of the new message via an e-mail notification;

7) The user can connect to eTrustEx Web to access the message and download the files;

8) Once the user accessed the message, eTrustEx Web generates an Application Response and sends it to eTrustEx Node, changing the message status to READ;

9) eTrustEx Node may forward the Application Response to the Sender's Backend System, or the Backend System of the Sender may pull for the message.

5. NEEDED IMPLEMENTATIONS AND CONFIGURATIONS

As mentioned above, the message exchange flow in eTrustEx can be done in three ways: user to user, user to machine, or machine to user. Regardless of the scenario chosen, in order to exchange messages between two Parties, eTrustEx Web has to be hosted and maintained together with the central component of the platform, the eTrustEx Node, as it is in charge of storing and exchanging messages between the sender and the receiver. For information regarding the installations and configurations needed on the eTrustEx Node, please check the eTrustEx Node COD.[7]

Configurations on eTrustEx Web include inter alia the creation of a business domain, creation of Parties, importing the ICAs created in eTrustEx Node, creation of user accounts, etc. For more information about the implementations and configurations needed on eTrustEx Web, please follow the Open eTrustEx installation guide.[8]

As mentioned within the section "Key Concepts", Open eTrustEx uses basic authentication and can be integrated with any custom authentication system. For example, eTrustEx Web deployed within the European Commission premises is using the EU Login authentication.

---

[7] See reference R1.

[8] See reference R4.

6. LIST OF MAIN FUNCTIONALITIES

Functionality	Description
Send / receive encrypted messages	eTrustEx Web uses end-to-end encryption. Depending on the business needs, users can choose to encrypt or not the messages sent. The configuration is done when setting-up the overall architecture of the project.
Send/receive signed messages	Sender of a message has the option to sign or not the message. If the Sender signs the message, then he/she has to fill in the certificate and password for signature.
Exchange files of max 500 Mb/file	Users of eTrustEx Web can exchange individual files of max 500 Mb/file.
Exchange messages of max 5Gb	Maximum total size of a message is 5 Gb (within the limit of 5 Gb, max. 500 files and max. 500 Mb/file).
Exchange any type of files	Users of eTrustEx Web can exchange any type of files.
Send notifications by email to the Receiver of the message	When a new message is received by a Party, eTrustEx Web can send email notifications to personal email addresses of the user(s) belonging to that Party.
Access the message from the notification link received	The receiver of an email notification can access the message received by her/his Party directly from the link received by email.
Preview messages received	Users have a general view of their inbox. The preview of a message already includes important information about that message (e.g. subject, Sender Party, date and time, number of files received, etc.).
Download files directly from message preview	Users can download the files directly from message preview, without opening the message itself.
Send notifications to the Sender	eTrustEx can send message status notifications to the Sender of a message, informing about the status of the sent message.
Status of a sent message	The sender can see the status of a message from the "Sent" screen of eTrustEx Web (e.g. Read, Delivered, Failed, etc.)
Retention policy	Files received are not available for the download after a configurable period of time.
Support EU languages	Users can change the language from a drop-down button; the default language of the application is English.
PDF message summary available for the Sender	Sender of a message can choose to see a message summary from the "Sent" screen of eTrustEx Web.
Configurable functionalities	Business representatives of each project using eTrustEx Web can submit change requests, in order to customise the system according to their needs.

7. SUPPORTED ENVIRONMENTS AND INSTALLATION

The following table contains a list with the supported application servers and databases.

Application Server	Database
WebLogic version 12.1.3	Oracle 11g
WildFly version 10.1.0.Final	MySQL 5.5.x

For installing the open source version of the application, you can follow the installation guide provided in reference R4. The open source version of eTrustEx Web is using the second configuration: WildFly application server with MySQL database.

eTrustEx Web is compatible with all modern browsers, as shown below:

-   Chrome, v 64 (and above);
-   Firefox, v 59;
-   Edge, v 17.

Once the user is accessing eTrustEx Web, if the browser used is not compatible with the application, the user will be redirected to a page showing the compatible versions.

8. CONTACT INFORMATION

eTrustEx Support

- **By email: EC-ETRUSTEX-SUPPORT@ec.europa.eu**

9. REFERENCES

The table below gathers the list of documents referenced throughout the present Component Offering Description.

Ref	Document name	Document location
R1	eTrustEx Node COD	https://joinup.ec.europa.eu/solution/open-e-trustex/document/open-e-trustex-documentation
R2	CEF eDelivery Access Point Component Offering Description	https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+software
R3	eTrustEx One Pager	https://ec.europa.eu/isa2/sites/isa/files/etrustex-one-pager.pdf
R4	Open eTrustEx Web Installation Guide	https://joinup.ec.europa.eu/solution/open-e-trustex/document/open-e-trustex-documentation
R5	eTrustEx Web User Guide	https://joinup.ec.europa.eu/solution/open-e-trustex/document/open-e-trustex-documentation

10. Definitions, Acronyms and Abbreviations

Key	Description
Party	In eTrustEx Web, the transfer of files is done Party to Party. A **Party** represents an organization/part of an organization/project using the eTrustEx platform in order to exchange business documents.
Sender	A Party that is referred to as the origin of a message sent through eTrustEx Web.
Receiver	A Party that is referred to as the recipient of a message sent through eTrustEx Web.
eTrustEx Node	eTrustEx Node is the central component of the platform in charge of storing and exchanging messages between the Sender and the Receiver Party.
XML	XML (Extensible Mark-up Language) is the standard messaging format for business communication, allowing companies to connect their business systems with those of customers and partners using the existing Internet infrastructure.
XSD	XML schema definition language (XSD) describes the structure of an XML document.
Business Domain	A Business Domain represents the specific context of a business.
Interchange Agreement (ICA)	A logical communication channel, called interchange agreement is created in order to enable the communication between two Parties. This configuration is done by the eTrustEx system administrator.
Business Administrator, Party Administrator and Party Operator	In the context of eTrustEx GUI, each organization will have at least one Party Administrator per Party and more Party Operators. The **Party Administrators** of each organisation are set-up by the eTrustEx team at the set-up of the e-TrustEx data flow in Acceptance. The **Business Administrator** has the ability to grant Operator and Party Administrator roles to other users for all the Parties belonging to the organization. Once the Party Administrator role has been created for each Party, this person can administer the **Party Operators** independently from the services of eTrustEx. The Party Administrator can also create more Party Administrator roles for the same Party.
Party Operator	This role allows a user to view/send/receive the messages of a Party (or Parties) in the e-TrustEx application.
Party Administrator	This role allows a user to view/send/receive the messages of a Party (or Parties) in the e-TrustEx application and has the ability to grant Operator and Party Administrator roles to other users for a Party (or Parties) in the e-TrustEx Web application.

| **CEF eDelivery** | eDelivery is one of the CEF building blocks, which helps public administrations to exchange electronic data and documents with other public administrations, businesses and citizens, in an interoperable, secure, reliable and trusted way. It is a network of nodes for digital communications, based on a distributed model, where every participant becomes a node using standard transport protocols and security policies. |