EUROPEAN COMMISSION
DIRECTORATE-GENERAL INFORMATICS

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

eTrustEx Node

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	18/02/2019	Anamaria BATRINU	First draft of the document
0.02	22/02/2019	Anamaria BATRINU	Changed section 4 and added section for definitions, acronyms and abbreviations
0.03	26/02/2019	Kristof POPGEORGIJEV	Review
0.04	27/02/2019	Anamaria BATRINU	Implemented comments following review
0.05	01/03/2019	Anamaria BATRINU	Implemented new comments following discussion with Kristof
0.06	14/03/2019	Kristof POPGEORGIJEV	Review
0.07	24/05/2019	Anamaria BATRINU	Implemented comments from 14/03/2019
0.08	28/05/2019	Kristof POPGEORGIJEV	Review
0.09	29/05/2019	Anamaria BATRINU	Implemented comments from 28/05/2019
1.0	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 Node secure message exchange platform.

eTrustEx Node is a platform that can be used in any Policy Domain of the EU to enable secure and reliable exchange of documents and data (structured, non-structured and/or binary), both across borders and sectors between Public Authorities and businesses at European, national and local level.

The eTrustEx Node follows a centralised model and acts as a focal point in a star network topology. The platform is a mediator system handling document exchange requests from the connected systems. It is the enabler of information exchange in a loosely coupled fashion, so that the interconnected systems depend on each other to the least possible extent.

The eTrustEx Node platform can be used standalone or in combination with other interoperable components, depending on the business needs and the location of the parties involved in the exchange of messages. The following scenarios are possible when using eTrustEx Node:

- used standalone for exchanges between systems inside an organisation;
- used in combination with the eTrustEx Web application[1] when a user is involved (e.g. user to user, user to system and/or system to user) for exchanges inside the same organisation, or between an organisation and external parties;
- used in combination with a CEF eDelivery Access Point[2] based on the AS4[3] standardised message exchange protocol, between systems inside an organisation and systems of external parties.

[1] More information about the eTrustEx Web application can be found in the eTrustEx Web Component Offering Description. See reference R4.

[2] More information about the eDelivery Access Point can be found in the CEF eDelivery Access Point Component Offering Description. See reference R5.

[3] AS4: Applicability Statement 4. More info about AS4 can be found at http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html).

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

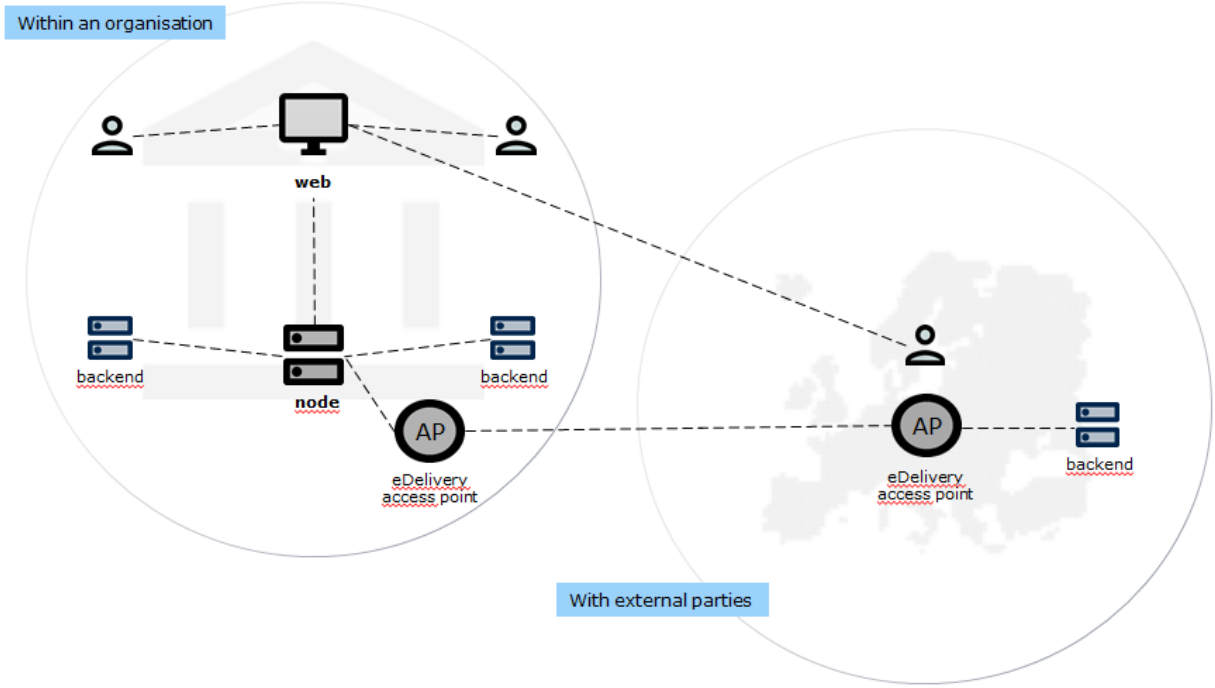

Figure 1 - Exchange Interaction through eTrustEx Node

The development of the eTrustEx platform is funded by the ISA[2] programme. It is offered as an open source software tool via Joinup[4] and provided as a service to the EU Institutions and Agencies[5].

[4] https://joinup.ec.europa.eu/solution/open-e-trustex
[5] EU Send web portal: https://europa.eu/!wp94dH

2. KEY FEATURES

Key feature	Description
Interoperability	Defined as an OASIS[6] technical specification, which is built on top of existing technical specifications of proven interoperability: MIME, SOAP and WS-Security[7].
Reliable	Guarantees once-and-only-once delivery via the exchange of receipts and additional requirements on both Sender and Receiver side.
Support of groups of files	The application allows the transfer of groups of linked files.
Confidentiality	The system allows ensuring that 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 users / systems only have access to the resources they are allowed to.
Integrity	The system allows guaranteeing integrity of the transferred files using XML digital signatures.
Storage security	A dedicated and secure file system to which only authorized users have access is used to store binaries. The databases that contain business data, logging information and audit trails is hosted in a secure environment where only authorized users have access.
Support of large files	The application allows the transfer of large files (up to 500 MB each) of any type.
Validity	The system allows guaranteeing the business validity of the messages stored in the system by supporting multiple types of validation: • Standard XSD validation; • Schematron validation (a rule-based validation language for making assertions about the presence or absence of patterns in XML messages); • Parent message validation; • Specific business rules implemented in the code of the eTrustEx Node itself.
Auditing	It is ensured by the logging of all the calls to eTrustEx Node and by storing the transactions in the system's database.
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).
Retention policy	It supports automatic removal of messages that are too old and not relevant anymore to the business.
Availability	It supports notification of availability to the message sender once the message is available to be retrieved by or dispatched to the recipient.

[6] https://www.oasis-open.org/

[7] WS-Security (WSS): Standard set of extensions to SOAP, used to apply security to Web services by specifying how to implement message content integrity and confidentiality

Key feature	Description
Advanced routing of documents	The system supports dispatching of the business documents to the recipient back-offices using standard interfaces (JMS, Web Service and AMQP).
Human readable generation	The System supports the generation of a human readable version of a document by applying a transformation template on the request, depending on the business needs.
Data extraction	The system supports message data extraction for easy searching of documents, by defining what information in the transmission will be extracted in order to be used for filtering by a specialized service.
Configurable	A number of the above-described key features are configurable in the System (e.g. retention policy, availability, validity, confidentiality etc.). eTrustEx Node component also includes an Administration Console that facilitates the configuration of the platform, allowing a business user to configure in a user friendly manner: • The parties exchanging the documents; • The access information used by the parties to communicate with eTrustEx Node; • The interchange agreements between the parties that need to exchange information; • The routing endpoints of the receiver parties; • Managing other users in their business domain. Other configurations, more technical, may be performed directly in the database by technical users.

All the above-mentioned features are described in detail in the *eTrustEx Node Interface Control Document*[8].

[8] See reference R1.

3. MESSAGE EXCHANGE FLOW

3.1. Machine to Machine

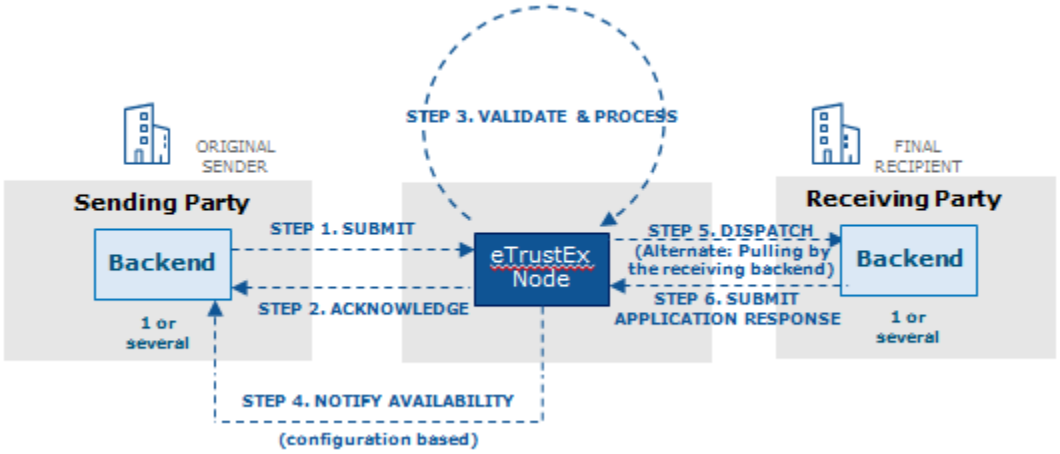

Figure 2 - Message Flow - machine to machine

Below is the conceptual description of the processing of a document submitted by a Sender System to a Receiver System through eTrustEx Node from start to finish:

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 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[9] may be updated based on an Application Response sent by the Receiver and made available to the Sender.

[9] 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.

3.2. User to Machine

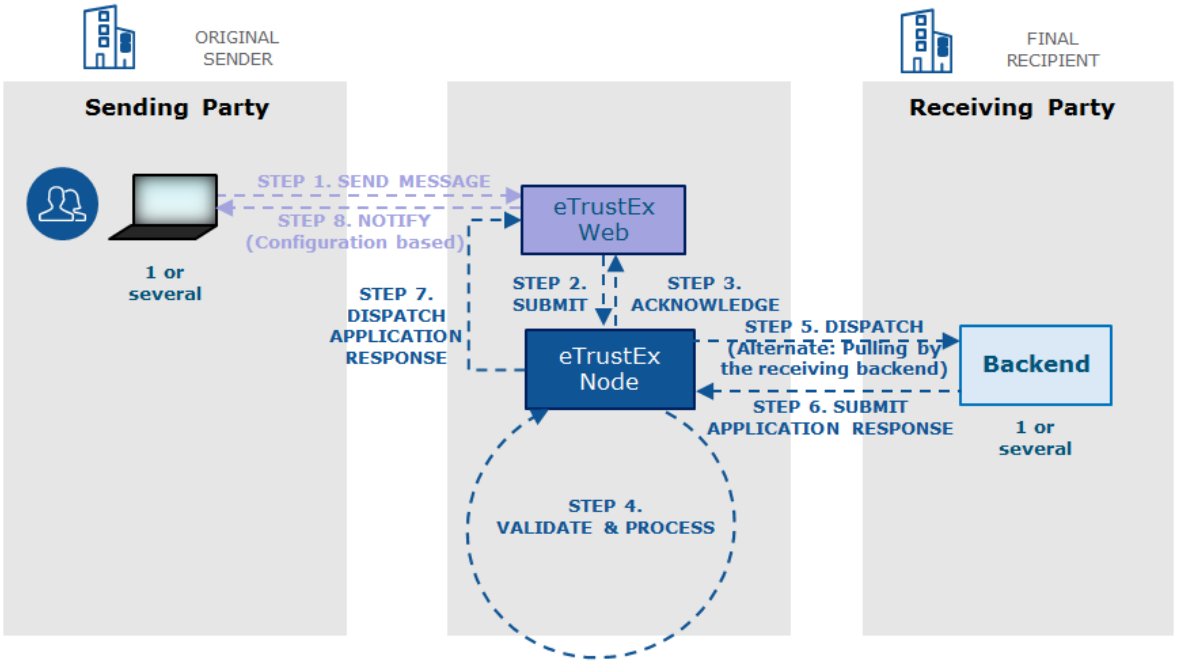

Figure 3 - Message Flow – user to machine

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 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[10] 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.

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

3.3. Machine to User

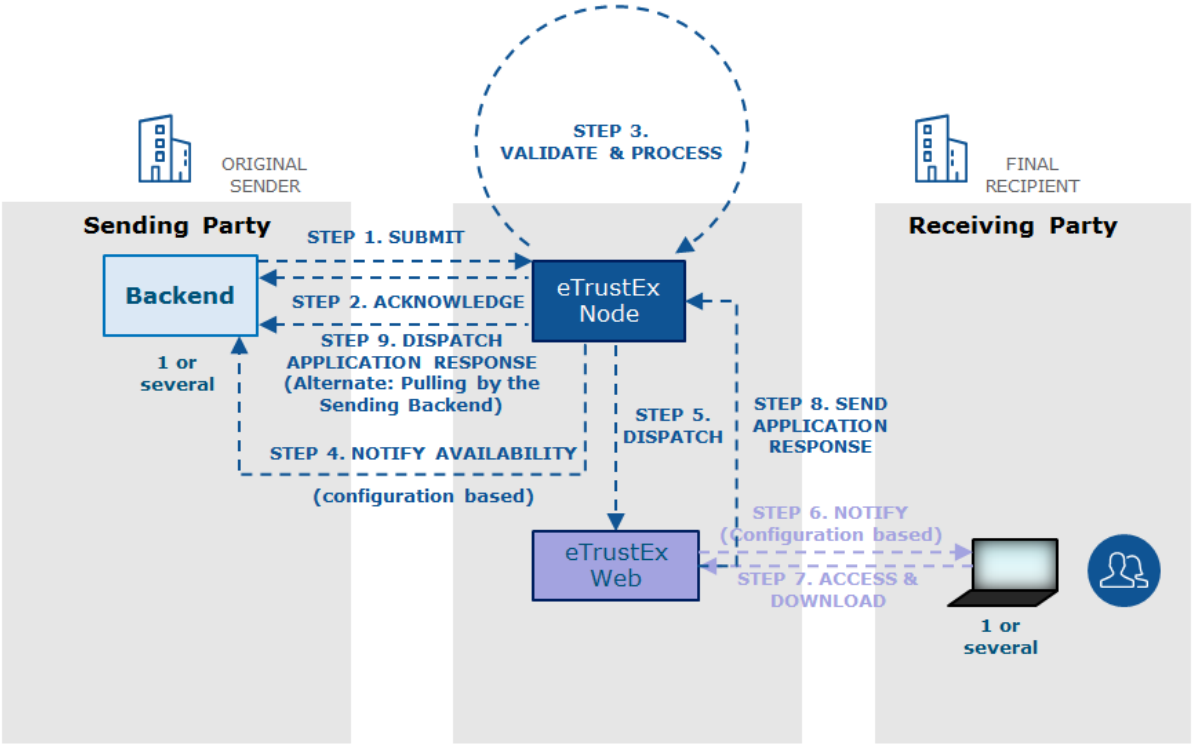

Figure 4 - Message Flow - machine to user

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.

4. NEEDED IMPLEMENTATIONS AND CONFIGURATIONS

4.1. Implementations on the Client Side

In order to use the services[11] exposed by the platform to exchange messages, the Systems of the parties involved in the exchange need to be adapted by implementing specific modules in order to communicate with the eTrustEx Node.

The modules that have to be implemented may vary on the business needs:

- There can be modules for sending messages to eTrustEx Node, that are able to communicate with the sending services like Submit Document Wrapper, Submit Document Bundle etc.
- There can be modules polling messages, in which case they will need to be able to communicate with the Inbox Request or Retrieve Request services.
- In case of dispatching, services will need to be exposed and modules implemented able to interpret the messages the eTrustEx Node is sending to these services.

4.2. Configurations of eTrustEx Node

In order for a System to connect to eTrustEx Node and send messages to another System, parties need to be defined for both Systems, as well as have unique business identifiers associated with them (e.g. GLN[12], VAT[13] etc.). The party credentials that will be used to connect to eTrustEx Node must also be defined as well as the encryption public key when needed.

To allow the exchange of messages between these parties, an interchange agreement needs to be defined on a profile allowing the exchange of a document of the type needed by the business.

If the messages need to be dispatched to the receiver, the corresponding JMS, AMQP or web service endpoints must also be configured.

All the above configurations can be performed through the graphical user interface of eTrustEx Node: the Administration Console.

[11] For a list of all services exposed by the eTrustEx Node, please see section 6 List of Services.
[12] Global Location Number. See https://www.gs1.org/standards/id-keys/gln for more details.
[13] Value Added Tax

5. COMMUNICATION MODE

Communication mode	Functional description
Synchronous	Allows the requester to quickly know the result of the requests requiring fast processing. When this communication mode is used, eTrustEx passes the results to the requester immediately.
Asynchronous	This communication mode is used for Requests for which eTrustEx needs a significant processing time or which require workflow steps performed by the back-office. Asynchronous Requests are services characterized by a two-step processing: a synchronous processing followed by an asynchronous one. While waiting for the asynchronous processing to be performed, the requester can use synchronous requests to periodically check the message status.
Technical Acknowledgement	A Technical Acknowledgment (Ack) is returned by eTrustEx Node in the case of Asynchronous requests, in the end of the synchronous processing part. In this case, it means that the message has been received and the processing of the message continues in the asynchronous part. The technical acknowledgment is digitally signed and must be saved and archived by the sender if proof of the message reception is required. Without this proof a sender cannot claim to have sent a message if it is not present in eTrustEx (e.g. due to technical issues in the connection between the sender and e-TrustEx).
Notification Available	For the asynchronous services, eTrustEx checks if an availability notification is required, and, if it is the case, it generates a specific application response (providing the document type code and having response code 1) and makes it available to the sender party. This way the sender is aware that the message has been correctly processed by eTrustEx and it is ready to be retrieved by or dispatched to the recipient(s).
Store and Forward	Base on the defined routing configurations, eTrustEx will dispatch the business documents to the recipient back-offices using standard interfaces (JMS, Web Service, and AMQP).

6. List of Services

Service Name	Communication type	Description
Submit Document Bundle	Asynchronous	This service allows a party to send a message.

Submit Application Response	Asynchronous	This service is used
		• either by the application to notify the sender regarding one of the following:
		  ○ an error in the message processing;
		  ○ the message has been correctly processed and is available to the receiver.
		• or by the receiver party of the message to trigger a message state change.

Submit Attached Document	Asynchronous	This service allows the sender party of a message to send a document that was missing from the initial message transmission.
Submit Event Notification	Asynchronous	This service is used by the application to notify the interested parties regarding specific events like document deletions, change in the configurations of parties and interchange agreements.
Retrieve Document Wrapper	Synchronous	This service allows a party to retrieve a specific binary file belonging to a message transmission.
Inbox Request	Synchronous	This service allows a party to check for all the received messages not yet retrieved.
Retrieve Request	Synchronous	This service allows a party to retrieve a specific message.
Query Request	Synchronous	This service allows a party to check for all the messages matching specific criteria.
View Request	Synchronous	This service allows a party to retrieve the human readable corresponding to a specific message transmission.
Status Request	Synchronous	This service allows a party to check the status of a specific message.
Retrieve Interchange Agreements	Synchronous	This service allows a party to retrieve specific interchange agreements.
Store Document Wrapper	Synchronous	This service allows a party to send a binary file that will be later on referenced in a message

Service Name	Communication type	Description
		transmission.
Delete Document Wrapper	Synchronous	This service allows a party to delete a binary file previously sent by this party, but not yet linked to a message transmission.
Delete Document	Synchronous	This service allows a party that has sent or received a document to delete this document.
Create Party	Synchronous	This service allows a party to configure a new party in the application.
Create Interchange Agreement	Synchronous	This service allows a party to configure a new interchange agreement in the application.

More details about each service can be found in the *eTrustEx Node Interface Control Document*[14].

[14] See reference R1.

7. Supported Environments and Installation

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

Application Servers	Databases
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 R3. The open source version of eTrustEx Node is using the second configuration: WildFly application server with MySQL database.

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 Interface Control Document	https://joinup.ec.europa.eu/solution/open-e-trustex/document/open-e-trustex-documentation
R2	eTrustEx Node Software Architecture Document	https://joinup.ec.europa.eu/solution/open-e-trustex/document/open-e-trustex-documentation
R3	Open eTrustEx Installation Guide	https://joinup.ec.europa.eu/solution/open-e-trustex/document/open-e-trustex-documentation
R4	eTrustEx Web Component Offering Description	https://joinup.ec.europa.eu/solution/open-e-trustex/document/open-e-trustex-documentation
R5	CEF eDelivery Access Point Component Offering Description	https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+software

10. Definitions, Acronyms and Abbreviations

Key	Description
HTTP	Hyper Text Transfer Protocol. A TCP-based application-layer protocol used for communication between Web servers and Web clients.
HTTPS	Secure version of the HTTP protocol. A different default port and an additional encryption/authentication layer between HTTP and TCP are used.
TCP	Transmission Control Protocol
Party	A Party is an entity that can exchange messages through eTrustEx Node. The entity can be an organization or a System used by an organization that wants to use eTrustEx Node for exchanging business documents.
Sender	A Party that is referred to as the origin of a message sent through eTrustEx Node.
Receiver	A Party that is referred to as the recipient of a message sent through eTrustEx Node.
SOAP	Simple Object Access Protocol: A lightweight XML-based messaging protocol used to encode the information in Web service request and response messages before sending them over a network.
WS (Web Service)	A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-process able format (specifically WSDL).
WSDL	WSDL (Web Service Description Language) is an XML-based service description on how to interface using a web service.
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 describes the structure of an XML document.
Schematron	Rule-based validation language for making assertions about the presence or absence of patterns in XML trees
MIME	Multipurpose Internet Mail Extensions
JMS	Java Message Service
AMQP	Advanced Message Queuing Protocol (https://www.amqp.org/)
Document Wrapper	A Document Wrapper is an entity composed of a binary file and its metadata, which can be exchanged through the eTrustEx Node

Key	Description
Bundle	Set of multiple document wrappers exchanged by the Parties playing a role in a data exchange scenario.
Business Domain	A Business Domain represents the specific context of a business.
Interchange Agreement (or ICA)	An Interchange Agreement represents a Contract between two or more Parties on the use of eTrustEx Node for the electronic exchange of information.
CEF	Connecting Europe Facility (https://ec.europa.eu/digital-single-market/en/connecting-europe-facility)
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.