EUROPEAN COMMISSION

DIGIT | DG CNECT
Digital Europe Programme

eDelivery Building Block

Version 1.20

Security Controls

Linking eIDAS (Q)ERDS & eDelivery

Document Status:

Status
Final

Document Approver(s):

Name	Role
Joao Rodrigues Frade	CEF eDelivery Project and Architecture Office
Bogdan DUMITRIU	Project Manager

Document Reviewer(s):

Name	Role
Filipe Beato	PwC EU Services
Dusko Karaklajic	PwC EU Services
Adrien Ferial	CEF eDelivery Technical Office
Ioana Dragusanu	CEF eDelivery Technical Office
Maarten Daniels	CEF eDelivery Technical Office
Marco Fernandez-Gonzalez	eIDAS Task Force
Susanne Wigard	DIGIT (ISA)

Summary of Changes:

Version	Date	Created by	Short Description of Changes
0.01	2016-05-04	PwC EU Services	Definition of Trust Zones
1.00	2017-02-25	European Commission	For Review
1.10	2018-12-13	CEF Support	Contact information updated
1.20	22-04-2022	Caroline AEBY	Remove CEF references and update links

Table of Contents

APPROACH AND PURPOSE OF THE DOCUMENT

This document assumes that readers are familiar with the eDelivery building block of the Digital Europe Programme (DEP) and the eIDAS regulation. Readers not familiar with these topics are recommended to consult:

- The eDelivery introduction document [1] to learn about its technical specifications, software and services;
- The eIDAS regulation (Regulation (EU) N°910/2014) [2] on electronic identification and trust services for electronic transactions in the internal market;
- The technical guidelines by ENISA [3] on how to implement the specific provisions of eIDAS.

This document addresses the security controls and recommendations applicable to eDelivery's message exchange Use Case which uses the AS4 messaging protocol without dynamic discovery, i.e. without the Service Metadata Publisher (SMP) and the Service Metadata Locator (SML). As it will be further detailed in this document, the message exchange Use Case is closely linked to the Electronic Registered Delivery Service (ERDS), a trust service under the eIDAS regulation.

The eIDAS regulation [2] defines **E**lectronic **R**egistered **D**elivery **S**ervice (ERDS) as a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including the proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.

As for all other trust services under eIDAS, ERDS can be provided by a non-qualified Trust Service Provider (TSP) or a Qualified TSP (QTSP). Whereas TSPs provide ERDS, QTSPs provide Qualified ERDS (QERDS). This is because non-qualified TSPs are only subject to light touch and reactive ex post supervisory activities and QTSPs are subject to both ex ante and ex post requirements / obligations by national supervisory bodies. As a result of these more stringent requirements, only QTSPs are part of national trusted lists and can make use of the EU trust mark. As laid out in Article 43 of the regulation, both qualified and non-qualified ERDS benefit from a non-discrimination clause as evidence in legal proceedings but only QERDS enjoys the presumption of "*the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the QERDS*". The QERDS requirements are specified in Article 44 of the regulation. The next chapters will show how eDelivery is aligned with these technology-neutral requirements. Even though this document is a good starting point for TSPs to understand how eDelivery can help them become qualified (i.e. QTSPs), the use of eDelivery by itself does not grant, or ensures, the qualified status. It is worth highlighting that this decision can only be made by the national supervisory bodies. Key content of this document includes the following information:

- The description of the security controls of the message exchange Use Case of eDelivery and, in particular, of the controls embedded in the AS4 profile[1] created within the e-SENS Large Scale Pilot;
- Mapping of QERDS requirements to the security controls of eDelivery;
- A set of recommendations for Businesses and Public Authorities intending to use eDelivery and to potentially go through the process of becoming a QTPSP providing QERDS.

[1] http://wiki.ds.unipi.gr/display/ESENS/PR+-+AS4

This document targets any organisation, Public or Private, intending to use the eDelivery building block in the provision of ERDS or similar service. The following figure summarises the objectives, target audience and main outputs of this document.

OBJECTIVES

Extract the QERDS requirements from the eIDAS regulation.

Understand the security controls of eDelivery and map them to the QERDS requirements.

Suggest and recommend a list of security controls to be implemented when using eDelivery, possibly, as a QTSP.

AUDIENCE

Policy officers involved in the roll-out of EU-wide or national policies that require an eDelivery messaging infrastructure.

IT Architects (mainly Security Experts) involved in the design and operation of eDelivery messaging infrastructures that implement the AS4 profile of the eDelivery building block.

Service providers (TSPs and QTSPs) involved in the implementation and roll-out of eDelivery.

OUTPUT

A **LIST OF QERDS REQUIREMENTS** extracted from the eIDAS regulation **(CHAPTER 2)**

A **POLL OF SECURITY CONTROLS** addressing the QERDS Requirements **(CHAPTER 3)**

A **SET of RECOMMENDATIONS** of security controls to implement when using the eDelivery building block **(CHAPTER 4)**

Figure 1. Summary of the objectives, audience and outputs of this document

GLOSSARY

The key terms used in this **document** are defined in Table 1. The key acronyms used in the eDelivery Building Block are defined in the Glossary on the Digital Web Portal:

Table 1. Security controls and recommendations key terms

Term	Description
Access Point	The Access Point (AP) of eDelivery implements the AS4 message exchange protocol according to the e-SENS profile [4]. This ensures standardised, interoperable, secure and reliable data exchange. For more information, please refer to the Digital Portal [5].
AS4	The AS4 profile of eDelivery is the AS4 Usage Profile/ implementation guidelines defined by e-SENS based on the AS4 specification of OASIS, itself a profile of OASIS ebXML Messaging Services Version 3.0, which in turn is based on various Web Services specifications of OASIS.
Backend system	In the context of eDelivery, the Backend systems represent the IT systems used by the business and public administrations, which are the origin of the documents and data to be exchanged through eDelivery. In order to do so, Backend systems must be connected to a eDelivery Access Point, directly or through a connector component.
Business Domain owners	In this context, it represents the owners of the projects that use eDelivery. These are usually businesses and public administrations that benefit from one or more Access Points (AP) in a given policy domain. They typically use eDelivery to create a secure messaging infrastructure for the exchange of data and documents within their domain.
eDelivery	The eDelivery building block helps public administrations to exchange electronic data and documents with other public administrations, businesses and citizens (usually through web-portals), in an interoperable, secure, reliable and trusted way.
Connector	The connector component of eDelivery is an optional component that facilitates the interoperability and integration between the systems implemented by the Backend systems and the Access Points.
Electronic Seal	According to the eIDAS regulation, “electronic seal means 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”. Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document’s origin and integrity. An advanced electronic seal means an electronic seal that meets the requirements of Article 36. For qualified status the electronic seal requires to be an advanced electronic seal which is created by a qualified electronic seal creation device and is based on a qualified certificate for electronic seals.
Electronic Signature	According to the eIDAS regulation, “electronic signature means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign”. Where relying upon certificates, the latter are issued to a natural person. An advanced electronic signature means an electronic signature that meets the requirements of Article 26. For qualified status the electronic signature requires to be an advanced electronic signature which is created by a qualified electronic signature creation device and is based on a qualified certificate for electronic signatures.
Electronic Registered Delivery Service (ERDS)	According to Article 3(36) of the eIDAS regulation, ERDS is a service that makes possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.
Electronic Time stamp	According to Article 3(33) of the eIDAS regulation, an ‘electronic time stamp’ means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time. Article 3(34) defines ‘qualified electronic time stamp’ as an electronic time

	stamp which meets the requirements laid down in Article 42.
e-SENS	The electronic Simple European Networked Services (e-SENS) is a large-scale pilot project with the aim of consolidating, improving, and extending technical solutions based around common building blocks, in order to foster digital interactions among public administrations across the EU.
FTP	File Transfer Protocol (FTP) is a standard network protocol used to transfer files between different end-systems using a computer network.
JMS	Java Messaging Service is a messaging standard that allows Java EE application components to create, send, receive and read messages.
Message Encryption	Message encryption is the process of converting a plaintext message into a ciphertext for the purpose of confidentiality. The message encryption can be computed with symmetric key algorithms, where the same key is used for encryption and decryption, or with asymmetric key algorithms, where different keys are used for encryption and decryption (a private and public key pair are used) [6].
Messaging Layer Security	Messaging Layer Security considers the security of the messages transferred using the AS4 message exchange protocol e.g. documents, emails, files.
Organisation	In the context of this document, organisation refers to businesses and public administrations that operate or benefit from one or more Access Points in a given policy domain. Organisations may provide or benefit from non-qualified or qualified electronic registered delivery services.
PMode	A PMode (Processing Mode) is a collection of parameters that determine how AS4 messages (e.g. User Messages and Signal Messages) are exchanged between a pair of Access Points with respect to Quality of Service, Transmission Mode and Error Handling.
Policy domain	Policy domains are typically linked to the Directorate-Generals of the European Commission, e.g. DG Justice and DG SANTE that are the business owners of domains such as the eJustice domain and eHealth domain respectively. Policy domains use eDelivery to create a secure messaging infrastructure for the exchange of data and documents.
Public Administration	According to eIDAS regulation a Public Administration means a state, a regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate.
Qualified Electronic Registered Delivery Service (QERDS)	According to the eIDAS regulation, Article 3(37) a 'qualified electronic registered delivery service' means an electronic registered delivery service which meets the requirements laid down in Article 44 ("Requirements for qualified electronic registered delivery service").
Qualified Trust Service Provider (QTSP)	According to the eIDAS regulation, Article 3(20) a 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body, according to the requirements laid down in Article 24 ("Requirements for qualified trust service providers.
Security control	According to ISO 27001 [7], controls are any administrative, managerial, technical, or legal methods that are used as safeguards and countermeasures to modify or manage information security risks. In this document, security controls represent the technical mechanisms to be put in place to ensure confidentiality and integrity and consequently address the security requirements extracted from the eIDAS regulation.
Security domain	A security domain is a set of security controls implemented and managed by a responsible entity in different communication areas in the eDelivery four-corner model.
Service Provider	Service provider means a natural or a legal person who provides services integrating and implementing eDelivery.
Transport Layer Security	The transport layer security defines security for the protocols that are responsible to transparently transfer data between end systems, or hosts, ensuring a complete data transfer from host to host communication.
Trust	Trust is the characteristic that one organisation is willing to rely upon a second entity to execute a set of actions and/or to make a set of assertions about a set of subjects and/or scopes) [6].
Trust Service	According to eIDAS regulation a trust service' means an electronic service normally provided for remuneration which consists of:

	a. the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or b. the creation, verification and validation of certificates for website authentication; or c. the preservation of electronic signatures, seals or certificates related to those services
Trust Service Provider (TSP)	According to Article 3(19) of the eIDAS regulation, a TSP means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified TSP;

CONVENTIONS USED IN THE DOCUMENT

The conventions regarding qualified and non-qualified status used in this **document** are defined in Table 2.

Table 2. Description of the used conventions

Convention	Description
ERDS	Used when the ERDS is not qualified.
QERDS	Used when the ERDS holds qualified status.
(Q)ERDS	Used when the ERDS is qualified or not.
TSP	Used when the TSP is not qualified.
QTSP	Used when the TSP holds qualified status.
(Q)TSP	Used when the TSP is qualified or not.

REFERENCES

[1] "Introduction to the Digital Europe Programme, eDelivery building block," [Online]. Available: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery

[2] "eIDAS Regulation," [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&rid=2.

[3] ENISA, "Guidelines implementing eIDAS," [Online]. Available: https://www.enisa.europa.eu/topics/trust-services/guidelines/.

[4] "e-SENS AS4 Profile," [Online]. Available: https://ec.europa.eu/cefdigital/wiki/x/AwFfAQ.

[5] "eDelivery Access Point," [Online]. Available: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Access+Point+software.

[6] "OASIS Trust," [Online]. Available: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html.

[7] "ISO/IEC 27001," [Online]. Available: http://www.iso27001security.com/html/27001.html.

[8] "Digital Portal- eDelivery," [Online]. Available: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery.

[9] "ENISA Algorithms and Key Sizes," [Online]. Available: https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report.

[10] "BSI Technical Guidelines," [Online]. Available: https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TechnicalGuidelines_node.html.

[11] "TLS Protocol," [Online]. Available: https://tools.ietf.org/html/rfc5246.

[12] ENISA, "Standardisation in the field of Electronic Identities and Trust Service Providers," [Online]. Available: https://www.enisa.europa.eu/publications/standards-eidas.

[13] "eDelivery PKI Service," [Online]. Available: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/PKI+Service.

[14] ETSI, "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview," [Online]. Available: http://www.etsi.org/deliver/etsi_tr/119000_119099/119000/01.01.01_60/tr_119000v010101p.pdf.

1. INTRODUCTION

The eDelivery building block of the Digital Europe Programme (DEP) enables Businesses and Public Administrations (both are hereinafter referred to as 'organisations'), to exchange electronic data and documents in digital format in an interoperable, secure, reliable and trusted way [8], with other organisations (and indirectly with citizens). The eDelivery building block prescribes the use of Access Points implementing the AS4 Messaging Protocol according to the guidelines defined in the e-SENS profile/ implementation guidelines. Access Points may be operated and offered as a service by (Q)TSPs to enable heterogeneous systems to interact with each other in a secure way over the internet. This document recommends a list of security controls to be put in place by organisations when interconnecting their systems through AS4 Access Points to transmit data according to the definition of Electronic Registered Delivery Services (hereinafter referred to as 'ERDS') in article 3(36) of the eIDAS regulation, (EU) N°910/2014. The security controls recommended in this document facilitate the provision of Qualified ERDS (hereinafter referred to as 'QERDS') according to the requirements in article 44 of the eIDAS regulation. Compliance to these technological-neutral requirements enables common legal effect when documents and data are exchanged in digital format across borders [2]. The recommended security controls do not grant or ensure the qualified status, service providers must refer to the national supervisory body in their respective country.

1.1. The four-corner Model

Most eDelivery Messaging Infrastructures are based on a simple messaging topology known as the four-corner model, as illustrated in Figure 2. This means that the information exchanged between the original sender in corner one (C1) and the final recipient in corner four (C4) goes via Access Points, corners two and three (C2 and C3) respectively. These Access Points are interoperable with each other because they implement the same message exchange protocol and implementation guidelines, i.e. the AS4 message protocol as defined in the e-SENS profile [4]. In more detail, Figure 2 illustrates the message exchange Use Case of the eDelivery building block where organisations operating C1 and C4 use (Q)ERDS provided by C2 and C3, both of them (Q)TSPs (or comparable).

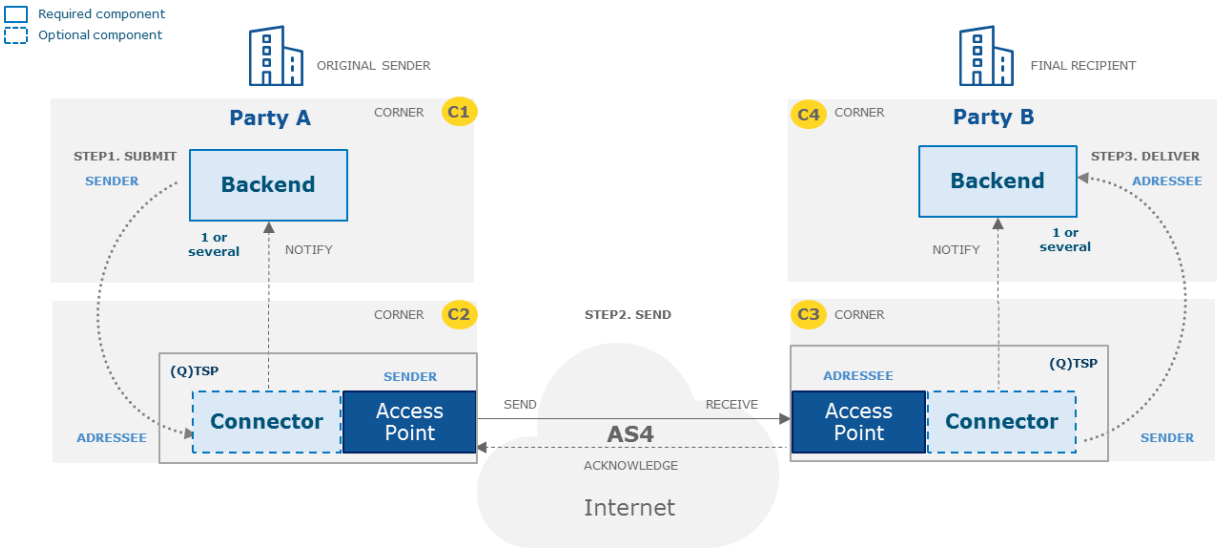

Figure 2 The eDelivery four-corner model

The elements of a four-corner model are:

- The **original sender (C1)** and the **final recipient (C4)**. Both of these corners are organisations, i.e. legal persons (businesses and public administrations). These organisations use IT systems (herewith referred to as **Backend systems**) to connect to the (Q)ERDS. It's important to notice that the Backend systems can be of any type e.g. an Enterprise Resource Planning system, a Document Management system, a Case Management system, a Base Registry system, a Portal, etc. As Backend systems are external to the (Q)ERDS, the authentication mechanism(s) used to authenticate natural persons/ end-users is left to these systems. This means that in a four-corner model:

    - **C1** is the original sender of a message. Hence, C1's **Backend** system produces and **submits** the message to the Access Point playing the sender role (C2) of the (Q)ERDS.

    - **C4** is the addressee of the message. Hence, C4's **Backend** system processes and consumes the message **delivered** by the Access Point playing the receiver role (C3) of the (Q)ERDS.

    It's important to clarify that the Backend system can use any technology (e.g. JMS, FTP, Polling or Web Services) to transmit and receive information from an Access Point. The choice of the authentication mechanism(s) used between [C1 and the (Q)ERDS via C2] and [C4 and the (Q)ERDS via C3] is left to the (Q)TSPs. These (Q)TSPs should use technical solutions that comply with the (Q)ERDS requirements. The message itself can be packaged in any format (e.g. XML, JSON, PDF or binary data).

- The **sender Access Point (C2)** and the **receiver Access Point (C4)** are implementations of the AS4 message exchange protocol according to the e-SENS AS4 profile [4]. These corners ensure the secure and reliable exchange of data between the message's sender (C1) and the message's addressee (C4). These corners are the boundaries of the (Q)ERDS. In the event of data being transferred between two or more (Q)TSPs, the ERDS service is qualified, i.e. QERDS, if both C2 and C3 comply with the QERDS requirements. It's also worth noticing that connectors can be put in place to facilitate the integration between Backend systems and Access Points.

The reader is invited to visit the Digital Portal [8] to know more about any of the above elements.

1.2. Scope of the eDelivery building block

As summarised in the table below, the data exchanged in a four-corner model is transferred among several communication layers. The eDelivery building block mainly focuses on the messaging and transport communication layer and is neutral in relation to the others.

Table 3. Communication layers

Layers	Role
Application Layer **(Out of scope)**	Responsible for the interactions between end-users and the Backend system.
Messaging and Transport Layer	Provides the protocols along with functional and procedural means of packaging and transferring messages, such as electronic data, documents and binary files. The eDelivery uses the AS4 message protocol according to the e-SENS Profile [4].
Networking Layer **(Out of scope)**	Typically this layer is the public internet. It contributes to the functional and procedural means of transferring message sequences between network nodes.

In addition to the communication layers, three security domains are defined in order to delimit the security controls present in a four-corner model. The eDelivery building block mainly focuses on the Cross-party Security domain and is neutral in relation to the others. Hence, this security domain is tightly linked to the AS4 messaging protocol [4].

Table 4. Security domains

Security Domain	Role
Cross-party Security (C2-C3)	Focuses on securing the exchange of information between Access Points.
Inner Security (C1-C2 and C3-C4)	Focuses on securing the exchange of information between Backend systems and Access Points.
End-to-end Security (C1-C4)	Focuses on securing the exchange of information between the original sender (C1) and the final recipient (C4). This domain contains is a result of the aggregation of the choices made in the Cross-party Security and the Inner Security domains.

As a result of the above, Figure 3 shows the scope of the eDelivery building block, i.e. the Cross-party Security domain and the Messaging and Transport Layer. This scope is aligned to the (Q)ERDS scope.

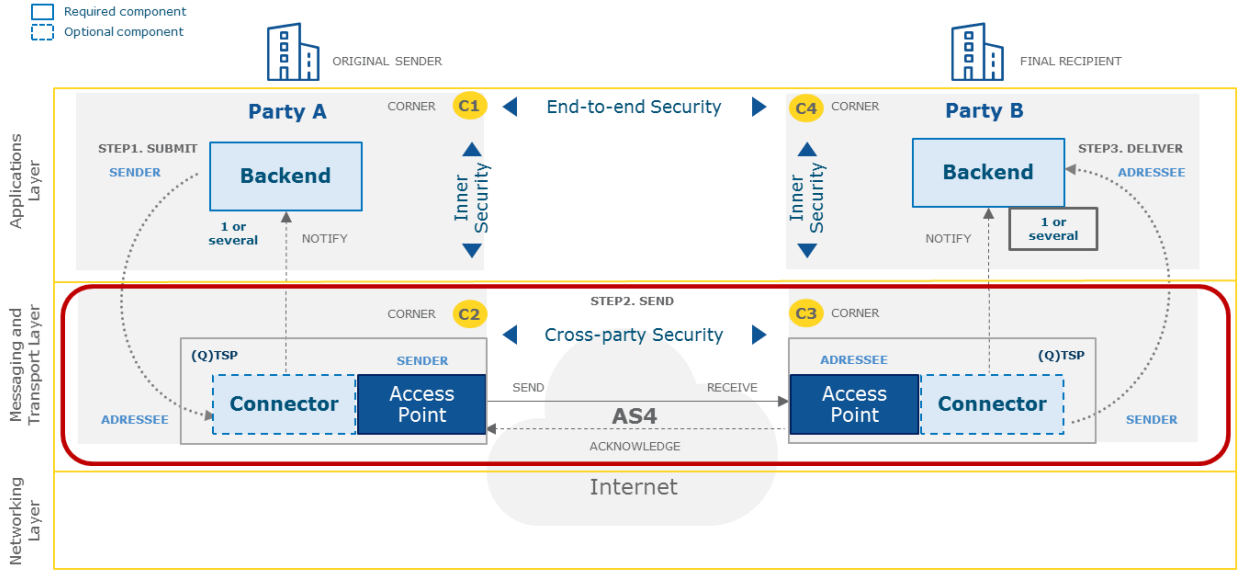

Figure 3. Communication layers and security domains of a four-corner eDelivery infrastructure

The set of recommended security controls for each of the security domains is described in Section 4 of this document. A more detailed description for each of the domains is available in Annex I.

2. QERDS REQUIREMENTS

The QERDS requirements are specified, in a technology-neutral way, in Article 44 of the eIDAS regulation. Table 5[2] below shows how the QERDSs requirements relate to the different Security Domains of eDelivery's four-corner model and in which of them the requirements apply.

Table 5. Summary of QERDS requirements from the eIDAS regulation

QERDS requirement	eIDAS reference	Interpretation for the purposes of eDelivery	Security domain
REQ1: Message Integrity	Article 3 (36) Article 19 Article 24 Article 44, *(d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;* *(e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;*	Messages should be secured against any illegitimate and unauthorised manipulation during transmission. This should be ensured via an advanced electronic signature/seal.	End-to-end Security (C1-C4)
REQ2: Message Confidentiality	Article 5 Article 19 Article 24	Messages should be encrypted during transmission.	End-to-end Security (C1-C4)
REQ3: Sender Identification	Article 24 Article 44 *(b) they ensure with a high level of confidence the identification of the sender;*	The identity of the sender should be verified with a high level of confidence, via an authentication process and/or the use of an advanced electronic signature/seal.	Inner Security (C1-C2)[3]
REQ4: Addressee Identification	Article 24 Article 44 *(c) they ensure the identification of the addressee before the delivery of the data;*	The identity of the addressee should be ensured before the delivery of the message, via an authentication process and/or the advanced electronic signature/seal.	Inner Security (C3-C4)[4]
REQ5: Time-Reference	Article 44 *(f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.*	The date and time of sending and receiving a message should be indicated via a qualified electronic timestamp ensured by an advanced electronic signature/seal.	Cross-party Security (C2-C3)
REQ6: Proof of Send/Receive	Article 3 (36) "… provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data…"	Sender and receiver of the message should be provided with evidence of message sending and receiving. This should be linked to the date and time of send/delivery via a timestamp or a qualified electronic timestamp for qualified status.	Cross-party Security (C2-C3)

[2] More details about requirements in the scope of the eIDAS regulation are presented in Annex II.

[3] [4] Technically, identification of the sender is performed between C1-C2 and of the recipient is between C3-C4. Legally, both parties (C2 and C3) are involved in meeting both requirements: according to article 44(1) (a) together with article 44(1) second subparagraph of the eIDAS regulation; QERDS can be provided by multiple qualified trust service providers meeting each of them article 44(1) (b) to (f). In other words, each qualified trust service providers will have to demonstrate to the Supervisory Body that it identifies the sender and the recipient. In the context of multiple qualified trust service providers, it cannot be done directly but upon relying and (and describing to the SB) the identification done by the other qualified trust service providers (and conversely).

Figure 4 maps the QERDS requirements described in Table 5 to the corners in a four-corner model, demonstrating how the eDelivery building block facilitates article 44 of the eIDAS regulation.

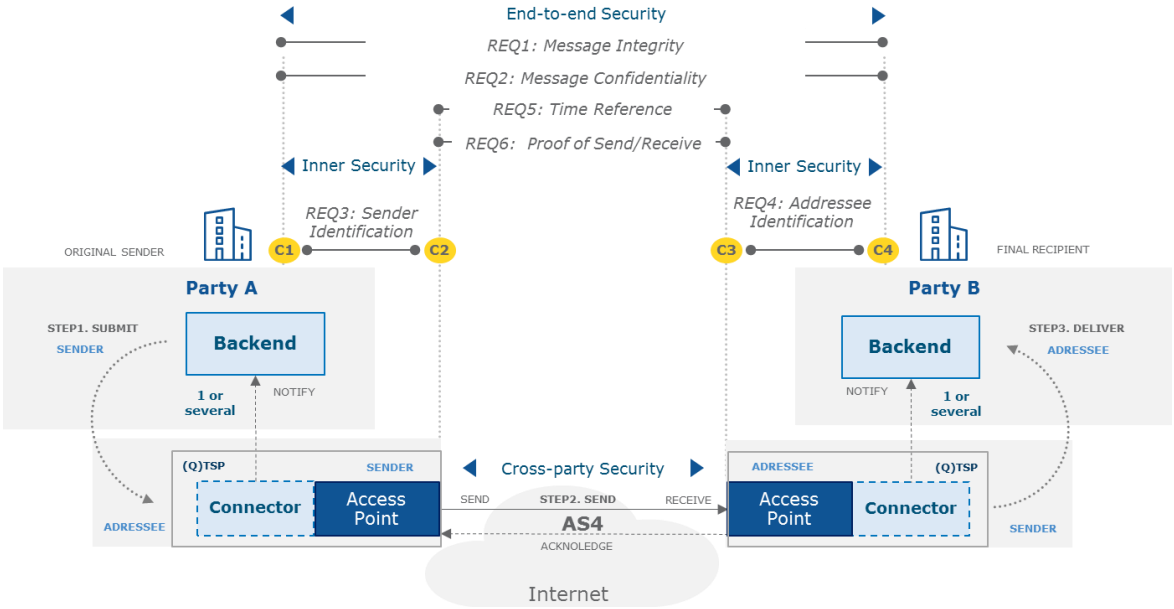

Figure 4. QERDS requirements from eIDAS applied to the four-corner model

In addition to the requirements listed in Table 5, in the case that the service is provided by two or more organisations then, according to Article 44, "*the requirements in points (a) to (f) shall apply to all qualified trust service providers*".

3. SECURITY CONTROLS

The security controls represent the technical mechanisms to be put in place to secure the eDelivery's message exchange Use Case on each of the security domains. These security controls were derived from the e-SENS AS4 Profile (used by eDelivery C2-C3) and best practice documents from ENISA [9] and BSI [10]. In this document there are two types of security controls:

- **Normative controls:** denote the controls required to address the requirements from the eIDAS regulation.
- **Non-normative controls:** denote recommended controls that are not, according to the analysis made by the authors of this document, necessary to address the requirements from the eIDAS regulation but should be put in place to enhance security.

The table below provides a brief description of the type of security control per security domain. It is important to highlight that it's up to the supervisory bodies in the EU Member States to grant the qualified status. Hence, this list is by no means exhaustive or complete as supervisory authorities may apply a different set of controls.

Table 6. Security domains in the four-corner model

Security domain	Responsible entity	Type of security controls at a glance
C2-C3 (Cross-party) Security	(Q)TSP	Set of primarily normative security controls to secure the exchanges between C2 and C3. These controls are defined based on the e-SENS AS4 profile. They are therefore implemented by default and covered by the eDelivery specifications. More information about this security domain can be found in Section 4.1.
C1-C2 (Inner) Security **C3-C4 (Inner) Security**	Sending Business Domain Owner Receiving Business Domain Owner	Set of security controls implemented to secure the exchanges between Backend systems and Access Points. These security controls should be implemented and managed by the organisations responsible for the Backend systems (C1 and C4) that use or intend to use eDelivery. Section 4.2 recommends a list of controls that should be implemented in this security domain.
C1-C4 (End-to-end) Security	Aggregation of all others	Set of security controls put in place to the secure the exchanges between C1 and C4. This domain is an aggregation of the security on the Cross-party and Inner security domains, thus requires the security controls, on both domains, to be in place. Section 4.3 describes the controls that should be implemented in this security domain.

Table 7 shows the security controls linked to the QERDS requirements from Section 2 and their respective legal implications. It should be noted that, for the process of granting the qualified status, TSPs must refer to their national supervisory body. As the trusted lists indicate the qualified status of TSPs, they can be used to bootstrap trust between corners, alone or in combination with other trust models such as PKI or mutual key exchange. The selection of trust model should be done taking into consideration the needs of the domain and a risk analysis.

Electronic signature/seal as used in this document are a form of advanced electronic signature/seal as defined by the eIDAS regulation and the eSignature Directive (Directive 1999/93/EC). Advanced electronic signatures/seals give higher security and trust guarantees as they must be based on qualified certificates and are created by a secure signature/seal creation device. For an advanced signature/seal to be qualified it must be created by a qualified signature/seal creation device. The qualified status of the signature/seal provides legal effect for integrity and correctness as well as higher security and trust levels.

Table 7. Overview of the security controls[5]

Security control	QERDS requirement	Legal implications
CTR1: Transport Layer Security protocol (TLS) Transport Layer Security (TLS) protocols provide authenticity and integrity of the message, by applying cryptographic mechanisms from host to host. Server (addressee) authentication is required and achieved using a server certificate, allowing the client (sender) to make sure the TCP connection is set up with the right server. The identification of the sender (client) is optional, and can be additionally achieved through configurable client authentication[6] using the different mechanisms: • *Mutual authentication (two-way TLS)*: This is done using the digital certificate of client (sender), allowing the server (receiver) to verify the connecting client (sender). Mutual certificate exchange rely on trust models, such as PKI or Trust lists; • *Basic authentication*: The client (sender) uses username/password to authenticate to the server (addressee). In this case, proper password management, including secure storage, sufficient complexity and regular updates need to be ensured by the client. TLS should follow ENISA security [9] and BSI [10] guidelines. Current version is 1.2 [11].	**REQ1**: Message Integrity **REQ2**: Message Confidentiality **REQ3**: Sender Identification **REQ4**: Addressee Identification	European General Data Protection Regulation (GDPR), in case of applicability.
CTR2: Message Encryption Message encryption ensures the confidentiality of the message, so that only the correct recipient of the message can access it. The message encryption protocols should follow ENISA security **[9]** and BSI **[10]** guidelines.	**REQ2:** Message Confidentiality	European General Data Protection Regulation (GDPR), in case of applicability.
CTR3: Electronic Seal of the message 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. From a technical perspective, electronic seal ensures integrity of the message, as well as the identity of the origin. Its legal effect is defined by the eIDAS regulation, Article 35. *(1) "An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals."* *(2) "A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked."* For advanced electronic seals the requirements are defined by eIDAS regulation, Article 36, while the standard algorithms and cipher suites are defined in the ENISA Standardisation for eID and TSPs [12] and follow ETSI TR 119 000 [14].	**REQ1:** Message Integrity **REQ3**: Sender Identification	**Non-qualified:** ensures integrity and origin of the data, in other words authentication of the data. **Qualified**: eIDAS regulation, Article 35. "A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked" **Both:** Non-discrimination in legal proceedings
CTR4: Electronic Seal of the evidence Serve as evidence to the sender of a message that the message was sent, and delivered to the intended recipient.	**REQ6:** Proof of send/receive	
CTR5: Electronic Time Stamp Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time. Its legal effect is defined by the eIDAS regulation, Article 41. *(1) "An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp"* *(2) "A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound."* The qualified time stamp requirements are defined in eIDAS regulation, Article 42, while the standard algorithms and cipher suites are defined in the ENISA Standardisation for eID and TSPs [11] and follow ETSI TR 119 000 [14].	**REQ5:** Time-Reference	**Non-qualified:** establishes existence of the data at a given time. In other words, ensures date and time of the data. **Qualified:** eIDAS regulation, Article 41. "A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound." **Both:** Non-discrimination in legal proceedings
CTR6: Electronic Signature of the message Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. Its legal effect is defined by the eIDAS regulation, Article 25. *(1) "An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures."* *(2) "A qualified electronic signature shall have the equivalent legal effect of a handwritten signature"* The advanced electronic signature requirements are defined by eIDAS regulation, Article 26, while the standard algorithms and cipher suites are defined in the ENISA Standardisation for eID and TSPs [12] and follow ETSI TR 119 000 [14].	**REQ1:** Message Integrity **REQ3:** Sender Identification	**Non-qualified:** used by a natural person to sign. In other words express consent (or any other functional equivalence that the signature might bear for a given transaction) **Qualified:** eIDAS regulation, Article 25. "A qualified electronic signature shall have the equivalent legal effect of a handwritten signature" **Both:** Non-discrimination in legal proceedings

[5] The list of security controls is not exhaustive and does not suggest specific algorithms, for that the reader is referred to the best practises guidelines, such as ENISA [10], BSI [11], and list of example standards that could be used as defined by ENISA standardisation for eID and TSPs [13], ENISA guidelines implementing eIDAS [3] and ETSI TR 119 000 [15].

[6] Authentication is the process used to establish the confidence in digital identities based on single or multiple authenticators, that can be based on some entity knowledge (username/password), possession (e.g. digital certificates or tokens), or inherence (e.g. biometrics).

4. RECOMMENDATIONS

This section presents recommendations of normative and non-normative security controls to be put in place on each one of the security domains of a four-corner model. A more in depth description of the security controls, technical and legal implications is available in Annex I.

4.1. Cross-party Security (C2-C3)

This section documents the security controls that are implemented by default in the Cross-party Security domain, by the eDelivery Access Points, to meet the QERDS requirements. Figure 5 illustrates these normative security controls in yellow between C2 and C3. These controls are prescribed in the e-SENS AS4 Profile.

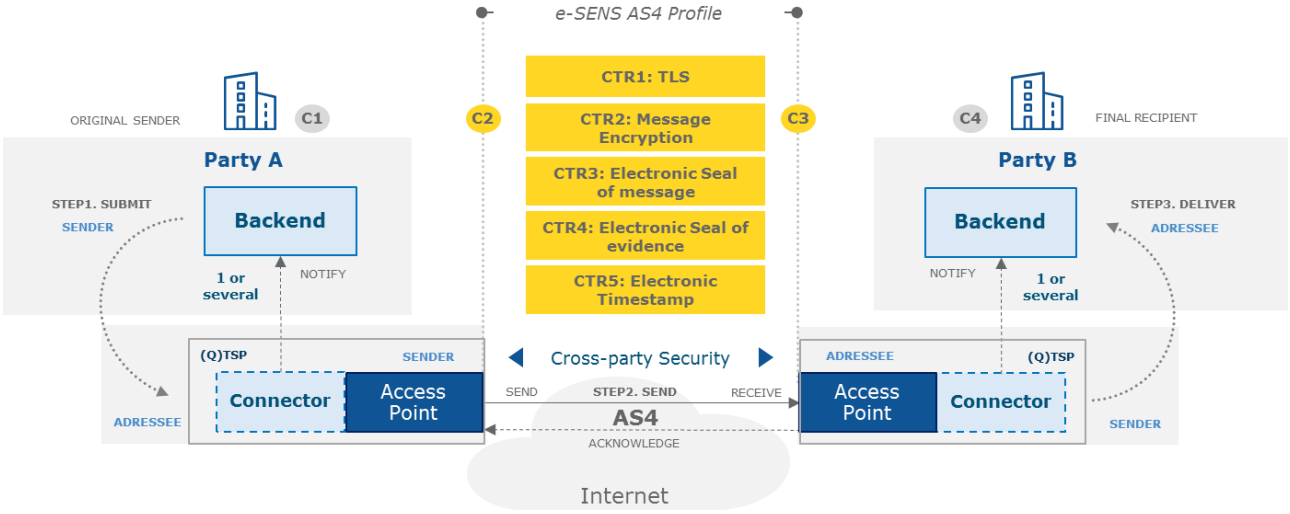

Figure 5. The implemented (yellow) security controls at Cross-party security domain

Table 8 presents a summary of the normative security controls in the Cross-party Security domain (C2-C3) and also their mapping to the QERDS requirements. The table shows:

- X for normative security controls that are implemented by default in the Access Points. In this case cells are greyed out to mark that these controls are available by default in the eDelivery building block according to the e-SENS AS4 profile (C2-C3).
- O for non-normative security controls that are optionally configurable through the Access Point's PMode parameters.

The technical and legal implications of the security controls of this domain are available in Annex I.1.

Table 8. Cross-party domain security controls[7]

	C2 – C3						Description
	REQ1	REQ2	REQ3	REQ4	REQ5	REQ6	
CTR1: Transport Layer Security protocol (TLS)	X	X	O	X			TLS guarantees message confidentiality and integrity between C2-C3, hence meeting REQ1, REQ2, and REQ4. REQ3 is currently optional and can be defined on the Access Point's configuration, through mutual authentication (as shown in Section 2), as defined by the AS4 profile. Note that TLS ensures that REQ1 and REQ2 are met during the message transfer between C2-C3 but not while the message is provisionally stored at C2 and C3.
CTR2: Message Encryption		X					The message is encrypted (CTR2) by C2 to C3. This ensures REQ2, by guaranteeing that only C3 is able to open the message.
CTR3: Electronic Seal of message	X		X				To meet REQ1 and REQ3, C2 applies an electronic seal to the message. This enables C3 to verify the integrity and sender of the message. As the (advanced) electronic seal is attached to the message, it can be verified at any time by any entity using C2's public certificate, thus ensuring the non-repudiation from the sender (C2).
CTR4: Electronic Seal of evidence						X	To meet REQ6, the receiver Access Point (C3) applies an electronic seal to the receipt of the message. This receipt is stored to be made available upon request. This not only guarantees non-repudiation from the receiver (C£) but also that it received 'that' message.
CTR5: Electronic Timestamp					X		To meet REQ5 (non-qualified), the eDelivery Access Points (C2 and C3) use a time stamp to testify the time of sending and a time stamp for the time of receipt. For qualified time stamp the accuracy of the date should be based on the Coordinated Universal Time and signed using an advanced electronic seal of a QTSP (Article 42).

Legend:

REQ1: Message Integrity	REQ4: Addressee Identification	☐: Not Applicable
REQ2: Message Confidentiality	REQ5: Time-Reference	X: Normative controls by default
REQ3: Sender Identification	REQ6: Proof Send/Receive	O: Non-normative control

4.2. Inner Security (C1-C2, C3-C4)

This section recommends a list of security controls that C1 and C4 should implement for connecting Backend systems to the Access Points in a four-corner model. As shown in Figure 6, their number is kept to a minimum. This figure also shows the QERDS requirements linked to the recommended security controls.

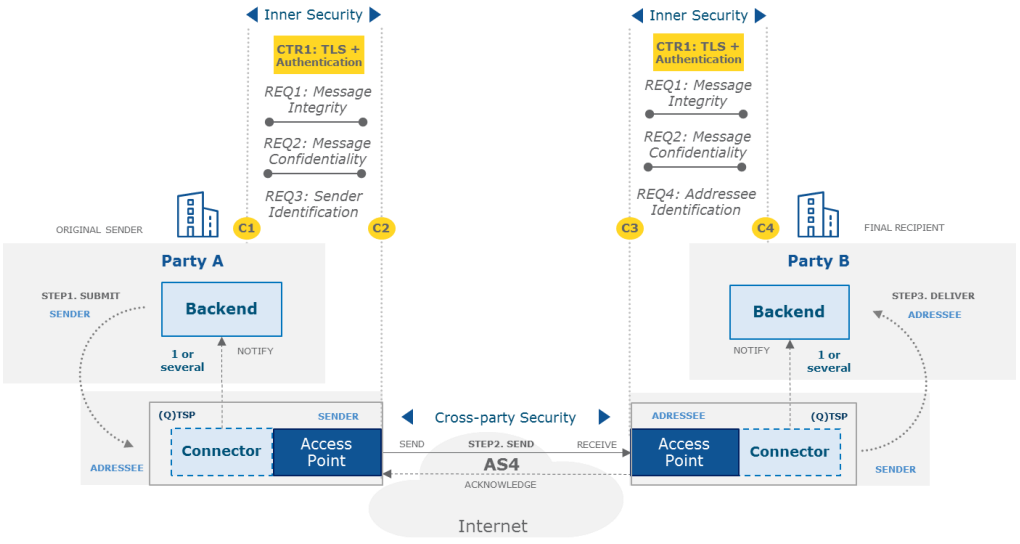

Figure 6. Recommended security controls (yellow) for the Inner Security domain

[7] Authentication is defined in the eIDAS regulation, Article 3(5) as "an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed", thus representing REQ4, which between C2 and C3 is met via the use of an electronic seal (CTR3). The definition of the access rights of organisations by means of attributes or access control lists is configurable at Access Point level and specified in the PMode configuration by the (Q)TSPs. Access Rights are not expressed in Table 6 as access control represents a non-normative control.

Table 9 provides an overview of the minimum security controls to be put in place by organisations when connecting their Backend systems to eDelivery Access Points. This security domain is the same between **C1-C2** and **C3-C4**. The **X** represents the normative security controls of this domain. In this case, there are no additional non-normative controls (**O**). It should be noted that REQ5 (Time-reference) and REQ6 (Proof of send/receive) are implemented by C2 and C3 and are therefore not present in this domain. Nonetheless, any evidences generated by the Access Points should become available to C1 and C4 on request. The technical and legal implications of the security controls of this domain are available in Annex I.2.

Table 9. Inner Security domain security controls

	C1 – C2				C3 – C4				Description
	REQ1	REQ2	REQ3	REQ3	REQ1	REQ2	REQ3	REQ4	
CTR1: Transport Layer Security protocol (TLS) with Client Authentication	X	X	X		X	X		X	TLS guarantees message confidentiality and integrity between C1 - C2, and C3 - C4. TLS between C1 - C2 meets REQ1 and REQ2 also REQ3 in the case that TLS adds client authentication (i.e. C1 and C4 when connecting to C2 and C3 respectively). This can be done using basic authentication (e.g. username/password) or, alternatively, two-way TLS (mutual authentication). The same holds for the TLS sessions between C3-C4. Note that TLS ensures that REQ1 and REQ2 are met during the message transfer between C1-C2 and C3-C4 but not while the message is provisionally stored at C2 and C3.

Legend

REQ1: Message Integrity REQ2: Message Confidentiality REQ3: Sender Identification	REQ4: Addressee Identification REQ5: Time-Reference REQ6: Proof of Send/Receive	X: Normative controls O: Non-normative controls

4.3. End-to-end Security (C1-C4)

This domain is composed by the aggregation of the security controls to be put in place by the organisations operating C1 and C4 (Inner Security), alongside with the controls implemented by the eDelivery Access Points i.e. C2 and C3 (Cross-party Security domain). As a result, Figure 7 illustrates that End-to-end Security is achieved transitively.

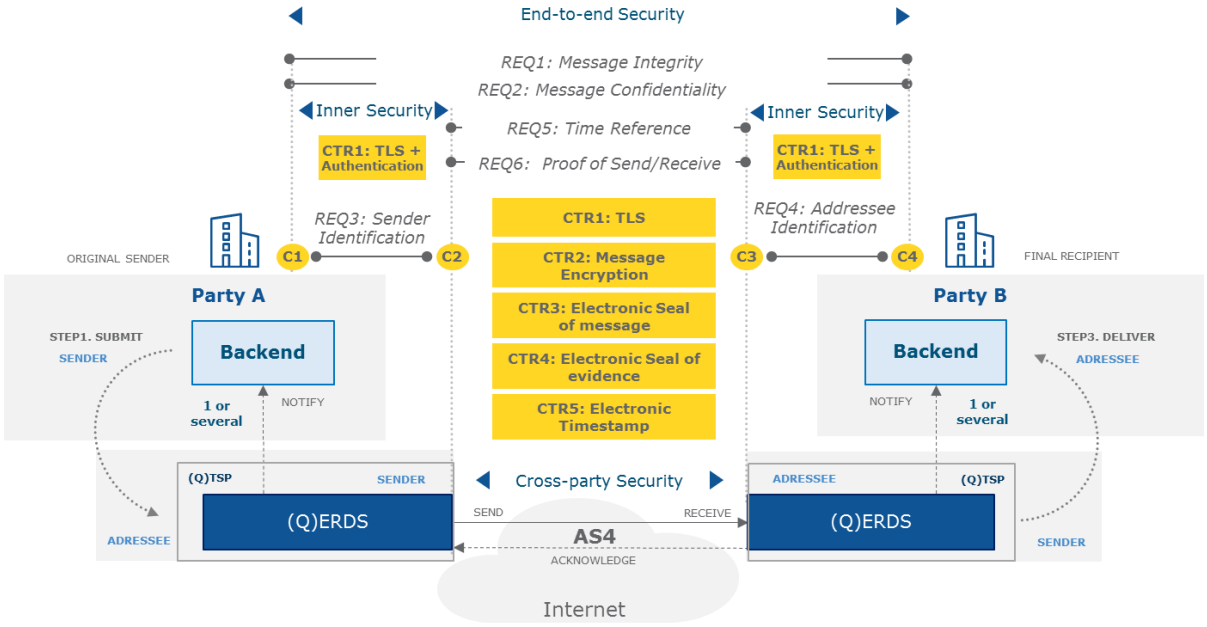

Figure 7. Recommended security controls (yellow) for End-to-end Security domain

According to the ERDS definition in the eIDAS regulation, ERDS provides evidence relating to the handling of the transmitted data (Article 3 (36)). Furthermore, as stated in article 24(2)(h), it is the responsibility of the (Q)TSPs that provide trust services to record and deliver evidences. Hence, the legal evidences described in this document (REQ6) are provided by the (Q)TSPs (i.e. operating C2 and C3) to the original sender (C1) and final recipient (C4) upon request.

The End-to-end Security domain requires security from the original sender (C1) to the final recipient (C4). Both communicate with Access Points (C2-C3) that comply with the QERDS requirements. Table 10 summarises the normative and non-normative security controls required for End-to-end Security (C1-C4) to be achieved **transitively**. This table also shows the mapping to the respective QERDS requirements. As in the previous chapters, X marks the security controls required to fulfil the requirement, while the greyed out cells mark the controls that are available by default in the eDelivery building block according to the e-SENS AS4 profile. To further enhance the level of confidentiality and integrity of their eDelivery messaging infrastructure, organisations can implement additional non-normative security controls (these are marked with O). These should be selected according to business needs and security policies. A more detailed description of End-to-end Security domain is available in Annex I.3.

Table 10. Recommended security controls for End-to-end Security domain to connect C1 and C4 to the eDelivery

	C1			C2 – C3						C4			Description
	REQ1	REQ2	REQ3	REQ1	REQ2	REQ3	REQ4	REQ5	REQ6	REQ1	REQ2	REQ4	
CTR1: Transport Layer Security protocol (TLS) with Authentication	X	X	X	X	X					X	X	X	TLS guarantees message confidentiality and integrity between corners, such as between C1-C2 and C3-C4. In particular, TLS meets REQ1 and REQ2 for C1-C2 and C3-C4. The identification of the original sender (C1) and final recipient (C4) are the responsibility of C2 and C3 respectively. Hence, REQ3 is met between C1-C2 and REQ4 between and C3-C4 by TLS with authentication (either two-way TLS or basic authentication). The authentication mechanism(s) used to authenticate natural persons/ end-users is left to backend systems (i.e. C1 and C4).
CTR2: Message Encryption		O			X								To meet REQ2, C2 encrypts the message for C3 (CTR2). Optionally, C1 can encrypt for C4, ensuring that that REQ2 is met during the entire path C1-C4 (transfer, storage, processing).
CTR3: Electronic Seal of message	O		O	X		X							To meet REQ1 and REQ3, C2 applies an electronic seal to the message header and payload, and C3 verifies the integrity and the sender of the message. Optionally, C1 can seal the message payload, thus identifying itself to C2 (REQ3) and ensuring that REQ1 is met (more information about this possibility is available in the extended security scenario in Annex I.3).
CTR4: Electronic Seal of evidence									X				To meet REQ6, C2 and C3 as (Q)TSPs apply an electronic seal to the sending and receipt of each message and the time and date (as an electronic time stamp), store it and make it available upon request to C1 and C4.
CTR5: Electronic Timestamp								X					The recommended configuration to meet REQ5 is that C2 and C3 use a (qualified) time stamp to testify the time of sending and reception of the message. For qualified time stamp the accuracy of the date should be based on the Coordinated Universal Time and signed using an advanced electronic seal of a QTSP (Article 42).
CTR6: Electronic Signature	O		O										CTR6 can be used for identification of natural persons towards C2 (REQ3) and fulfilling REQ1 up to C4. (more information about this possibility is available in the extended security scenario in Annex I.3).

Legend:

REQ1: Message Integrity	REQ4: Addressee Identification	: Not Applicable
REQ2: Message Confidentiality	REQ5: Time-Reference	X : Normative controls by default
REQ3: Sender Identification	REQ6: Proof send/Receive	X : Normative controls to be implemented
		O : Non-normative controls

5. Summary and Conclusion

The eIDAS regulation provides a common reference for (Q)ERDS with the common legal effect across Europe. The eDelivery building block facilitates meeting the (Q)ERDS requirements from the eIDAS regulation by putting in place a set of security controls at the messaging and transport layer.

This document provided an overview of the requirements from the eIDAS regulation along with a list of recommended security controls that can assist in meeting these requirements in order to securely exchange messages from the original sender to the final recipient. In addition, it described the security controls implemented by eDelivery, and a list of security controls recommended to be put in place by organisations that connect, or intend to connect to, via eDelivery messaging infrastructure.

As described in the document, the implementation of the security controls in the Inner Security domain, are the entire responsibility of the organisations using (Q)ERDS (i.e. Businesses and Public Administrations). It is important to note that the implementation of the security controls listed in this document does not guarantee the 'qualified' status. It is up to the supervisory bodies in the EU Member States to grant it to the (Q)TSPs [2].

6. CONTACT INFORMATION

eDelivery Support Team

By email: CEF-EDELIVERY-SUPPORT@ec.europa.eu

Standard Service: 8am to 6pm (Normal EC working Days)

Annex I. SECURITY DOMAINS DETAILED DESCRIPTION

This section describes the security controls implemented in the eDelivery building block and presents some security guidelines for organisations to perform a trustworthy connection to eDelivery.

Electronic signature/seal as used in this document are a form of advanced electronic signature/seal, hence based on qualified certificates and created by a secure signature/seal creation device. Qualified status provides a higher security level and legal support, however qualified status is provided only by the supervisory bodies upon the accreditation of the conformity assessment body[8].

I.1. CROSS-PARTY (C2-C3) SECURITY DOMAIN

This section presents a detailed description of the normative security controls implemented in the eDelivery building block, as well as the communication flow between Access Points as depicted in Figure 8.

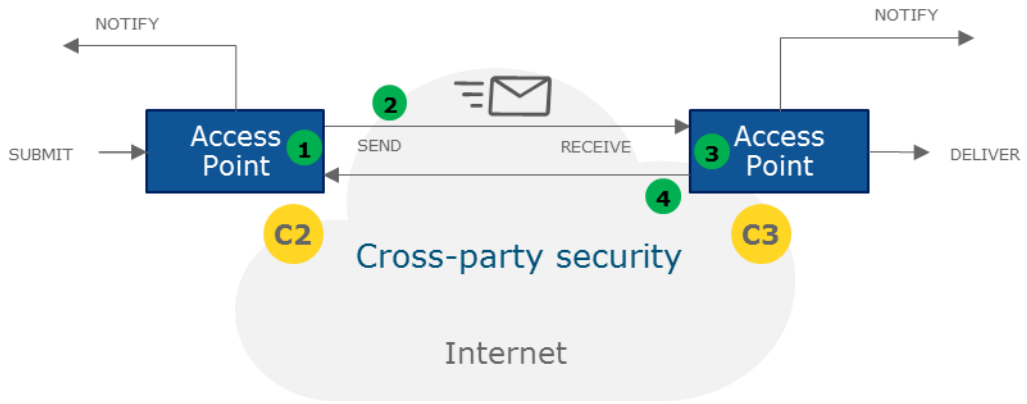

Figure 8. Cross-party Security (C2-C3)

The eDelivery components ensure security between C2 and C3 by using several security controls conformant with the e-SENS AS4 Profile at the transport and messaging layer.

The message exchange between C2 (sender) and C3 (receiver) is described by the following four steps (Figure 8).

1. Access Point (C2) creates an AS4 message composed of a SOAP **header, SOAP body and one or more payloads** (i.e. attachments) with C3 as a recipient, as illustrated in Figure 9. The encrypted and electronic sealed content is included in an attachment. The electronic seal is performed using the RSA-SHA256 cipher suite with the private key of C2. For the encryption of the content AES symmetric encryption on the GCM authenticated mode of operation is used with a randomly generated key, which is encrypted with the public key of C3 using RSA-OAEP. In addition, the header containing the message metadata details, such as message ID, original sender and final recipient information, is also sealed by C2. The electronic seal digest

[8] The conformity assessment body assesses the state of QTSP/QTS against the eIDAS regulation under the Regulation (EC) 765/2008. The conformity assessment body is accredited by the national accreditation body at Member States.

of the header and the content payload, along with the encryption information are included in the WS-Security header, whereas the SOAP body is sent empty as described in the e-SENS AS4 profile.

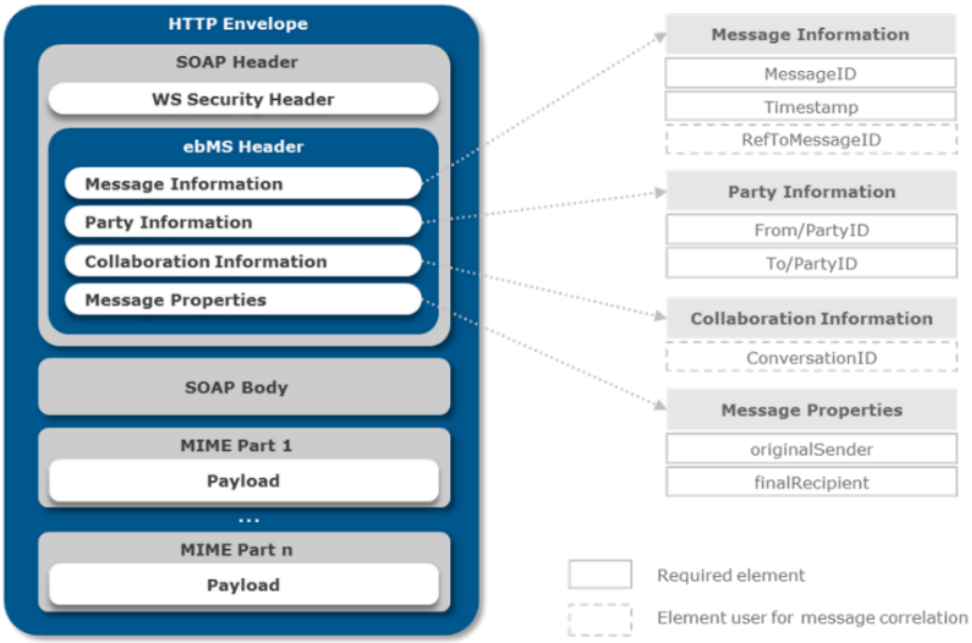

Figure 9. The e-SENS AS4 eDelivery message structure (SOAP envelope)

2. The message is sent through a TLS connection, providing message confidentiality and authenticity at the transport layer. During the TLS connection establishment, C2 (sender) identifies C3 (addressee) using the digital certificate of C3 while C2 is optionally (configurable in the PMode settings) identified using mutual authentication. As the message is secure at the messaging layer, the use of TLS can been seen are redundant, however it adds an extra layer of security and impacts performance depending on the message transfer sensitivity level. The TLS cipher suites are configurable and the recommended cipher suites for future use of TLS should follow the ENISA guidelines [9].

3. C3 decrypts the message using its private key and verifies the integrity and authenticity of the message according to the digital certificate (public key) of C2. This assures C3 that C2 was the sender of the message, and that the message was not tampered with during communication. The digital certificates exchange and the trust model of C2 and C3 is defined in the eDelivery PKI service [13].

4. Upon reception and verification, C3 generates an evidence receipt based on the message information received, electronic seals it using its digital certificate and sends it to C2 as proof of receipt. The electronic seal provides integrity and authenticity of the evidence as C2 can verify that the message has been received by C3.

A summary of the security controls implemented at the Cross-party Security domain, between C2 and C3, is presented in Table 11, along with the mapping to the security requirements based on the eIDAS regulation, and the technical (security) and legal implications.

Table 11. Technical and legal implications of the security controls at Cross-party Security domain, between sending Access Point (C2) and receiving Access Point (C3)[9]

Security control	Description	Requirements	Implications	
			Technical	Legal
CTR1: Transport Layer Security (TLS)	The Transport Layer Security (TLS 1.2 [11]) protocol is used, following ENISA security [9] and BSI [10] guidelines. C2 establishes a TLS connection with C3 for confidentiality and authenticity of the message at transport layer. The sender (C2) identification is provided as following: • *Mutual authentication*: This is done using the digital certificate (TLS/SSL certificate) of C2, allowing C3 to identify C2. For qualified status a qualified certificate should be used.	REQ1: Message Integrity	Authenticity of the message while transmitted between C2 and C3.	European General Data Protection Regulation (GDPR), in case of applicability.
		REQ 2: Message Confidentiality	Confidentiality of the message while transmitted between C2 and C3.	
		REQ3: Sender Identification	If two-way TLS is used, the Sender (C2) is identified by the Addressee (C3) using website authentication certificates (machine to machine or TLS certificate).	
		REQ4: Addressee Identification	The Addressee (C3) is identified by the Sender (C2) using website authentication certificates (machine to machine or TSL/SSL certificate) before message transmission. This is optional and should be configured in the PMode settings.	
CTR2: Message Encryption	C2 encrypts the payload of the message using AES-GCM with a random secret key, and the random key with the public key of C3 using RSA-OAEP. Message encryption follows WS-Security using W3C XML Encryption. The used cipher suite for symmetric encryption is AES GCM-mode, and for asymmetric is RSA-OAEP. This is following the ENISA security [9] and BSI [10] guidelines.	REQ2: Message Confidentiality	The message payload is encrypted by C2 for the addressee C3.This guarantees that only the addressee C3 is able to open the message during transmission, storage, and processing.	European General Data Protection Regulation (GDPR), in case of applicability.
CTR3: Electronic Seal of message	An electronic seal is applied to the message**.** C2 applies an electronic seal to the message header and payload using its own private key which guarantees integrity protection. The seal is verified by C3 using C2's public key for authenticity and non-repudiation of origin of the message payload and headers. Electronic sealing follows WS-Security with W3C XML Signing. The used cipher suite is RSA-SHA256. Other recommended standards for advanced seals are described in the ENISA standardisation for eID and TSPs [11] and follow ETSI TR 119 000 [14].	REQ1: Message Integrity	The message payload and header are electronic sealed. This allows C3 to verify that the message payload and header were not tampered with, and the message sender is C2. As the electronic seal is attached to the message, it can be verified at any time by any entity holding the C2 public certificate and within the same trust domain. Hence, the electronic seal assures non-repudiation with C2 as the sender, during transmission, storage, and processing.	Non-qualified: ensures integrity and origin of the data, in other words authentication of the data. Qualified: eIDAS regulation, Article 35. "A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked."
		REQ3: Sender Identification		
CTR4: Electronic Seal of evidence	An electronic seal is applied to the receipt. Upon reception and verification of a message from C2, C3 generates an evidence receipt based on message identification information (e.g. message identifier, timestamp, and sender metadata) with a new timestamp and a reference to the received message, applies an electronic seal and returns the sealed evidence to C2. The receipt is sent automatically to C2 as a "signal" message response to the initial message. Electronic sealing follows WS-Security with W3C XML Signing. The used cipher suite is: RSA-SHA256. Other recommended standards for advanced signature are described in the ENISA standardisation for eID and TSPs [11] and follow ETSI TR 119 000 [14].	REQ6: Proof of send/receive	Guarantees to C2 that C3 received the correct message and non-repudiation. The seal can be verified during transmission, storage, and processing.	Both: Non-discrimination in legal proceedings.
CTR5: Electronic Timestamp	A metadata (System) Timestamp is placed at the WS-Security header, and it is electronically sealed for integrity protection. The currently used time stamp relies on the system clock, hence is not qualified. For qualified timestamp extra measures should be employed after approval from a supervisory body. Other recommended standards for advanced timestamps are described in the ENISA standardisation for eID and TSPs [11].	REQ5: Time-Reference	The timestamp of the response evidence receipt guarantees that the message was processed by C3 at a given time. Whereas the timestamp of original AS4 message guarantees that the message was sent by C2 at a given time.	Non-qualified: establishes existence of the data at a given time. In other words, ensures date and time of the data. Non-discrimination in legal proceedings

[9] All the legal effects defined and steamed by the eIDAS regulation are applicable to all Member State countries within EU-28.

I.2. INNER (C1-C2, C3-C4) SECURITY DOMAIN

This section presents a detailed description of the normative security controls to be implemented in the Inner Security domain by organisations operating the Backend systems in order to secure the communication between the Backend systems and the Access Points according to the ERDS requirements.

In order to comply with the ERDS requirements the organisations controlling the Backend systems are recommended to implement TLS to guarantee the message confidentiality and integrity as well as the authentication of the connecting corners, i.e. C1 and C2, or C3 and C4.

The technical and legal implications related to using TLS are depicted in Table 12 for each of the connecting corners.

I.3. END-TO-END (C1-C4) SECURITY DOMAIN

The communication C1-C4 embodies the Backend (C1) to Backend (C4) communications between the original sender and the final recipient. The three following scenarios have been identified by the eDelivery stakeholders, with the **default** scenario representing the common use of the eDelivery building block, where C2 and C3 represent (Q)TSPs.

1. Delegation scenario **(default)**, where an organisation operating the original sender C1 connects to the C2 system, but delegates the message security (e.g. sealing and encryption) to C2. The sealing is performed using the credentials from the C2's certificate, while C1 is still identified as the original sender.

2. Extended delegation scenario, where an organisation controlling the original sender C1 delegates the right to C2 to seal the message with the digital certificate issued to C1. The legal aspects in this case are handled contractually between the organisations operating C1 and C2.

3. Extended security scenario, where the communicating organisations (original sender C1 and final recipient C4) take responsibility for the significant part of the security controls, e.g. message signing/sealing and message encryption, depending on the different sensitivity levels of the message and business requirements. Hence, organisations implement extra non-normative security controls using an electronic seal/signature (CTR3 and CTR4). This scenario requires mutual trust between C1 and C4, and C2-C3 to relay the message exchange in an interoperable way.

Table 12 provides a detailed description of the security controls, the requirements they meet, as well as their technical and legal implications.

I.3.1. DELEGATION SCENARIO

The delegation scenario (default) considers the scenario where an organisation corresponding to the original sender C1 explicitly delegates the message processing rights to the communication partner C2 which represents a (Q)TSP, as illustrated in Figure 10. In this case, C2 seals the messages with its own digital certificate (i.e. the corresponding private key), while still keeping the reference to the original sender C1 in the metadata. On the recipient side, C4 can verify that the original sender of the message is C1 through the metadata and C3 can verify that C2 digitally sealed the message using its certificate.

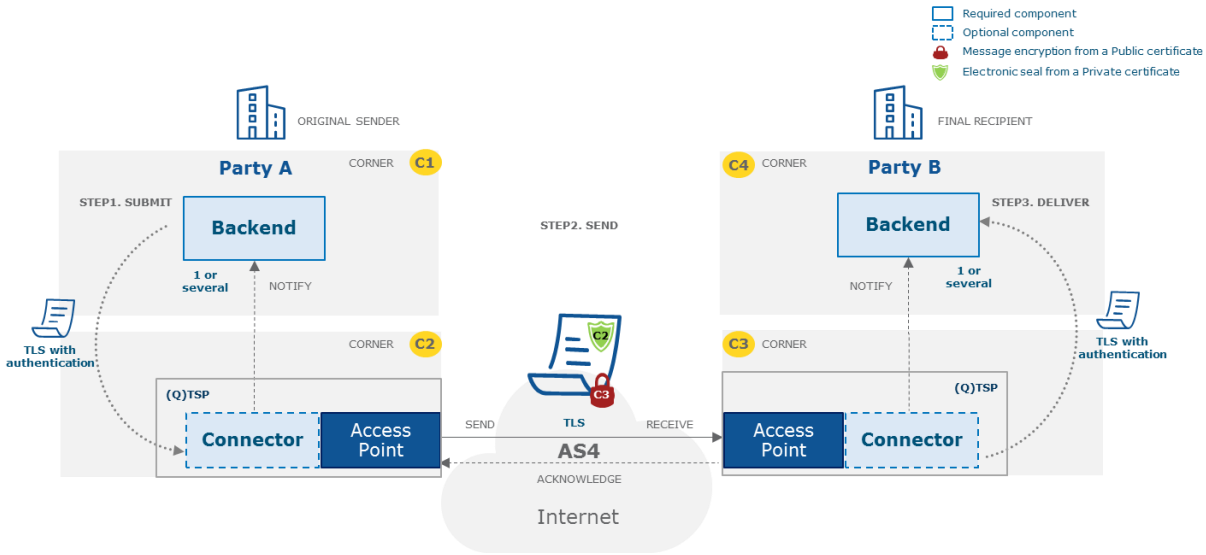

Figure 10. eDelivery delegation scenario (i.e. default scenario) on a four-corner model

To implement this scenario, C2 needs to authenticate C1 before sealing the message. As shown in Table 10, in addition to the existing security controls provided by the eDelivery building block, the TLS protocol needs to be implemented between C1-C2 and C3-C4. The C1 to C4 authentication is performed by the trusted service provided by C2 – C3.

As the message is sealed by C2, the legal implications related to electronic sealing (Table 12) are related to a legal person that operates C2.

Note: This case contains some security implications. As TLS secures the message in transit between C1 and C2, but not when the message is stored and processed by C2 Additional organisation and technical measures need to be put in place by the organisation operating C2 to mitigate the risk of tampering with the message while processed in its environment. In addition, the (Q)TSP Access Points need to under the same trust model for example the use of trust lists, through a specific PKI or mutual trust. The legal aspects associated to this scenario should be handled contractually between the organisations operating C1 and C2.

I.3.2. EXTENDED DELEGATION SCENARIO

Similar to the delegation scenario, this scenario occurs when the business entity (original sender C1) delegates the message processing to the communication partner (C2), as illustrated in Figure 11. However, in this specific scenario, C2 also stores and holds the digital certificate and associated private key of C1, and thus uses it to electronically seal the message. In this way, C1 can be identified as the original sender during process, transport and storage of the message by the receiving party. This scenario is eventually more suitable when C1 and C2 are in the same organisation and legal person. In any case, the legal aspects associated to this scenario should be handled contractually between the organisations operating C1 and C2.

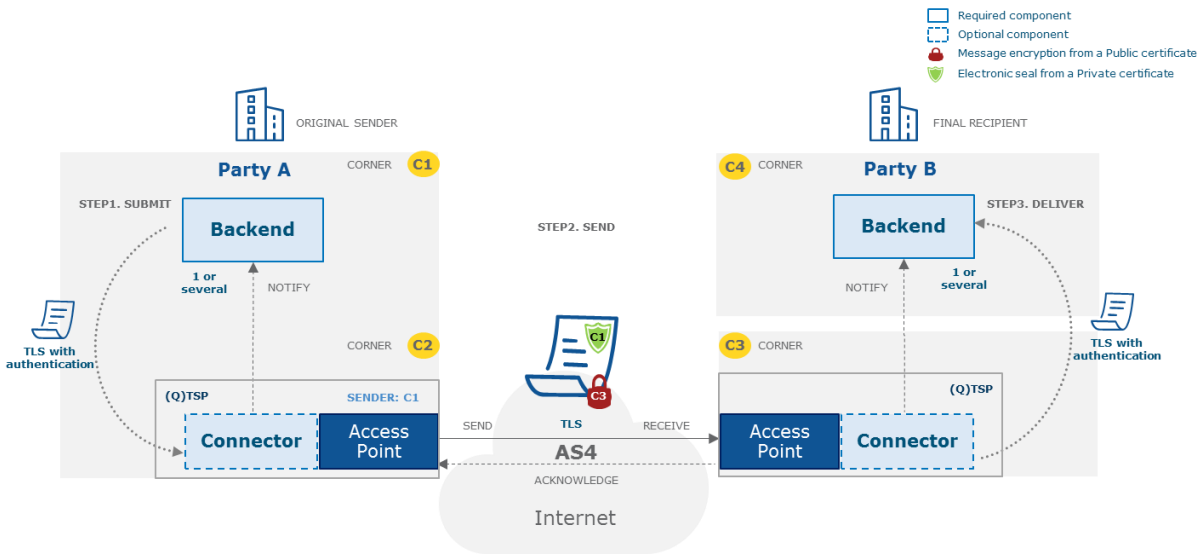

Figure 11. eDelivery extended delegation scenario on a four-corner model

As the message is sealed by C2 as C1, the legal implications related to electronic sealing (Table 12) are related to a legal person that operates C1.

Note. This case contains security implications. As C2 holds the digital certificate of C1, additional organisation and technical measures need to be put in place by the organisation operating C1 to mitigate the risk of C2 of tampering with the message. In fact, as the message is sealed by C2 with the digital certificate of C1, the legal implications of such scenario need to be addressed by the contractual agreements between C1 and C2. **This scenario is suitable when C1 and C2 are the same organisation and legal person.**

I.3.3. EXTENDED SECURITY SCENARIO

Depending on specific business needs and security policies, organisations responsible for the Backend systems can perform different configurations and implement additional security controls. This scenario (Figure 12) is suitable when C1 and C4 exchange highly sensitive data and have the necessary security means and capabilities.

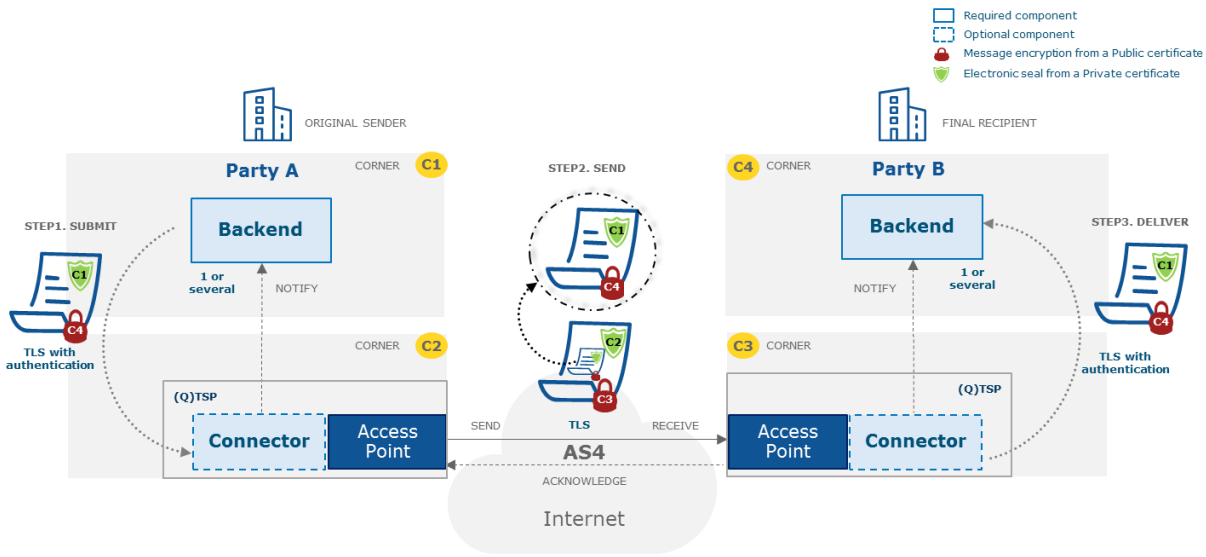

Figure 12. eDelivery extended security scenario on a four-corner model

In this scenario, the C1 and C4 take the technical and legal responsibility to implement the correct security controls to guarantee security in the different domains. For instance, as depicted in Figure 12 the original sender (C1) can chose to apply the electronic seal or signature to the message, so that the final recipient (C4) is able to verify the message using C1's public digital certificate. In addition, C1 can encrypt the message (using the public digital certificate of C4) to enhance the confidentiality of the message from C1 to C4 and add an extra layer of security. In both cases C1 and C4 are required to mutually exchange digital certificates in order to correctly verify and encrypt the exchanged messages, and be under the same trust model: a specific PKI, trust lists or mutual trust. Usually, organisations following this scenario are required to agree on the necessary security provisions prior to the exchange of sensitive, possibly classified, information and to hold full control of the security of the messages. The legal aspects associated to this scenario should be handled contractually between the organisations operating C1 and C2.

The technical and legal implications of the security controls when applied for this scenario in the End-to-end domain are summarised in Table 10.

Note. This case contains some security implications, as the communicating organisations are required to establish trust and perform a secure digital certificate exchange needed for verification and encryption of messages. Different trust models can be used to guarantee a secure and trusted mutual exchange of the digital certificates, such as the use of trust lists or through a specific PKI. Also, these organisations take full responsibility to comply or not with the eIDAS regulation.

Table 12. Technical and legal implications of the security controls at the End-to-end (and Inner) **S**ecurity domain, between the original sender (C1) and the final recipient (C4)

Security control	Description	Requirements	Implications	
			Technical	Legal
CTR1: Transport Layer Security (TLS) with authentication ***from C1 to C2 (and C3 to C4)***	The Transport Layer Security (TLS 1.2 [11]) protocol, following ENISA security [9] and BSI [10] guidelines protects the transmission of the message between C1 and C2. For the sender (C1) identification, organisations can opt for the two following options (the same applies for C4 – C3 connection) • *Mutual authentication*: This is done using the digital certificate (TLS/SSL certificate) of C1, allowing C2 to identify C1. For qualified status a qualified certificate should be used. • *Basic authentication:* C1 uses for example a username/password combination to authenticate to C2. In this case, proper password management, including secure storage, sufficient complexity and regular updates need to be ensured by C1; For	REQ1: Message Integrity	Authenticity of the message while transmitted from C1 to C2, and from C3 to C4.	European General Data Protection Regulation (GDPR), in case of applicability.
		REQ2: Message Confidentiality	Confidentiality of the message while transmitted from C1 to C2, and from C3 to C4.	
		REQ3: Sender Identification	The Sender (C1) is identified by C2 using website authentication certificates (machine to machine or TSL/SSL certificate), or identified through basic authentication, before message transmission Similar for C3 and C4.	
		REQ4: Addressee Identification	The Addressee (C4) is identified by C3 using website authentication certificates (machine to machine or TSL/SSL certificate) before message transmission.	
CTR2: Message Encryption ***from C1 and C4***	For the *extended security scenario:* the original sender C1 encrypts the payload of the message to the final recipient C4 using cryptographic mechanism that should follow the ENISA security [9] and BSI [10] guidelines ENISA Standardisation for eID and TSPs.	REQ2: Message Confidentiality	The message payload is encrypted by the original sender C1 for the final recipient C4. This guarantees that only the final recipient C4 is able to open the message during transmission, storage, and processing of the message. Hence, any component with no access (e.g. C2 and C3) is unable to open and read the payload of the message.	European General Data Protection Regulation (GDPR), in case of applicability.
CTR3: Electronic Seal of message ***by C1***	For the *extended security scenario*: an electronic seal should be applied to the message**.** The original sender C1 should apply an electronic seal to the message header and payload using the digital certificate issued to a legal entity. The seal can then be verified by C2, C3 and C4 using C1's public key for authenticity and non-repudiation of the message payload and headers. The electronic seal algorithm and cipher suite should follow the ENISA security [9] and BSI [10] guidelines. Recommended standards for advanced seals are described in the ENISA standardisation for eID and TSPs [11] and follow ETSI TR 119 000 [14].	REQ1: Message Integrity	The message payload and header are electronic sealed. This allows final recipient (C4) and any other component (C2 or C3) to verify that the message payload and header have not been tampered with, and the message original sender is C1. As the electronic seal is attached to the message, it can be verified at any time. Hence, the electronic seal assures authenticity of C1 as the sender during transmission, storage, and processing of the message.	Non-qualified: ensures integrity and origin of the data, in other words authentication of the data Qualified: eIDAS regulation, Article 35. "A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked." Both: Non-discrimination in legal proceedings
		REQ3: Sender Identification		
CTR6: Electronic Signature ***by C1***	For the *extended security scenario*: The electronic signature considers C1 as a natural person electronically signs the message with the personal digital certificate. Technically similar to Electronic seal, however, this requires the use of a digital certificate issues to a natural person instead of a legal entity (Electronic Seal). Hence, this should be applied to the message by C1. Recommended standards for advanced seals are described in the ENISA standardisation for eID and TSPs [11] and follow ETSI TR 119 000 [14].	REQ1: Message Integrity	From technical perspective, the same effect as CTR3: electronic seal of the message.	Non-qualified: used by a natural person to sign. In other words express consent (or any other functional equivalence that the signature might bear for a given transaction) Qualified: eIDAS regulation, Article 25. "A qualified electronic signature shall have the equivalent legal effect of a handwritten signature" Both: Non-discrimination in legal proceedings
		REQ3: Sender Identification		
CTR5: Electronic Time Stamp (Qualified) ***by C1***	For the *extended security scenario*: A qualified electronic timestamp should be created at the moment when the original sender C1 submits the message, and when the final recipient C4 retrieves it, by applying an electronic seal to time reference of the message. Recommended configuration to meet REQ5on default scenario: C2 uses a (qualified) time stamp to testify the time of sending; C3 uses a (qualified) time stamp on the receipt, in the case that C2 and C3 are (Q)TSPs. The electronic time stamp algorithm should follow the ENISA security [9] and BSI [10] guidelines. Other recommended standards for advanced seals are described in the ENISA standardisation for eID and TSPs [11] and follow ETSI TR 119 000 [14].	REQ5: Time-Reference	Guarantees to C1 and C4 that the message was created, processed and transmitted at a given time.	Non-qualified: establishes existence of the data at a given time. In other words, ensures date and time of the data. Qualified: eIDAS regulation, Article 41. "A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound." Non-discrimination in legal proceedings

Annex II. eIDAS REGULATION- REQUIREMENTS

This section is divided into two parts. The first one addresses the general provisions applicable to trust service providers, while the second one deals with the requirements specific for the electronic registered delivery service.

A service provider which intends to use the eDelivery to provide qualified or non-qualified trust services needs to comply with the full list of requirements mandated by the eIDAS regulation. For the requirements for the initiation of a qualified trust service, the reader is referred to Article 21 of the regulation.

The remainder of this section presents an overview of the general requirements following the eIDAS regulation within the scope of the eDelivery.

II.1. GENERAL PROVISIONS

Article 5 (Data processing and protection), paragraph 1:

1. *Processing of personal data shall be carried out in accordance with Directive 95/46/EC.*

Note: DIGIT should perform data protection and privacy analysis by documenting the information lifecycle of the eDelivery and ensuring that the processing of personal is in accordance to the Regulation (EC) No 45/2001.

Each service provider using the eDelivery Messaging Infrastructure needs to perform the data protection and privacy analysis in accordance to the applicable legislation. As a starting point, the information lifecycle of the eDelivery Messaging provided by DIGIT can be used.

Article 12 (Accessibility for persons with disabilities)

Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.

Recital 29

In line with the obligations under the United Nations Convention on the Rights of Persons with Disabilities, approved by Council Decision 2010/48/EC (1), in particular Article 9 of the Convention, persons with disabilities should be able to use trust services and end-user products used in the provision of those services on an equal basis with other consumers. Therefore, where feasible, trust services provided and end-user products used in the provision of those services should be made accessible for persons with disabilities. The feasibility assessment should include, inter alia, technical and economic considerations.

Note: In any case, trust service providers implementing the eDelivery Access Points need to respect the *United Nations Convention on the Rights of Persons with Disabilities.*

Article 13 (Liability and burden of proof), paragraph 2:

Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.

Note: In any case, service providers implementing the eDelivery Access Points are **solely responsible** for informing their customers about any limitations on the use of their services.

Article 19 (Security requirements applicable to trust service providers)

*Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the **level of security is commensurate to the degree of risk**. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.*

Note: To determine appropriate security measures, service providers can use the information security risk assessment of the eDelivery provided by DIGIT as a starting point for a "holistic" risk assessment of the services it provides.

Article 24 (Requirements for qualified trust service providers), paragraph 2, including the following items:

A qualified trust service provider providing qualified trust services shall:

e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;

f) use trustworthy systems to store data provided to it, in a verifiable form so that:

a. they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,

b. only authorised persons can make entries and changes to the stored data,

c. the data can be checked for authenticity;

g) take appropriate measures against forgery and theft of data;

h) record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;

Note: Trust service providers are solely responsible for keeping these records for a period of time defined in the applicable legislation.

i) ensure lawful processing of personal data in accordance with Directive 95/46/EC;

II.2. REQUIREMENTS DIRECTLY RELATED TO ELECTRONIC REGISTERED DELIVERY

The eIDAS regulation defines electronic registered delivery as *"a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the* ***risk of loss, theft, damage or any unauthorised alterations***" (art.3 (36)).

Article 44 (Requirements for qualified electronic registered delivery services):

a) they are provided by one or more qualified trust service provider(s);

Note: (Qualified) trust service providers are **solely responsible** for ensuring that they meet all the requirements to be granted the qualified status.

b) they ensure with a high level of confidence the identification of the sender;

Note: End user **authentication** needs to be addressed by a provider of qualified electronic registered delivery service.

c) they ensure the identification of the addressee before the delivery of the data;

d) *the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably*;

Note*:* End-to-end trust and signature generation/validation by the end participants is the responsibility of a qualified trust service provider(s) and it is not in scope of the eDelivery DSI.

e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;

f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.

In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers."

The IAS2 Project, which provides inputs for the secondary legislation stresses the sensitivity of privacy protection:

"Attention should be given to the processing of privacy-sensitive information, particularly with regard to selling and re-selling transaction related information that might disclose behaviour or preferences"

Annex III. e-SENS Comparison mapping

The following table (Table 13) summarises the mapping between the e-SENS AS4 functionalities and controls to the ERDS requirements and security controls presented in this document.

Table 13. e-SENS AS4 Profile functionalities mapping with ERDS requirements and security controls

Functionality	e-SENS AS4 Profile	Security Control	ERDS Requirements
Transport Layer Integrity, Sender Authentication, Receiver Authentication and Message Confidentiality (Non-Persistent)	• Transport Layer (SSL / TLS) Security	• TLS with basic or mutual authentication (CTR1)	• Message Integrity (REQ1) • Message Confidentiality (REQ2) • Sender Identification (REQ3) • Addressee Identification (REQ4)
Message Identification	• ebMS3 MessageId	• Electronic seal (CTR3) • Electronic signature (CTR5) • Electronic Timestamp (CTR5)	• Message Integrity (REQ1)
Message Correlation	• ebMS3 RefToMessageId and ConversationId	• NA	• NA
Message Timestamp	• ebMS3 Timestamp and WS-Security Timestamp	• Electronic Timestamp (CTR5)	• Time-Reference (REQ5)
Party Identification	• ebMS 3.0 "From" and "To" party identifiers.	• Electronic seal (CTR3) • Electronic signature (CTR6)	• Addressee Identification (REQ4)
Non-Repudiation of Origin	• WS-Security 1.1 using XML Signature	• Electronic seal (CTR3) • Electronic signature (CTR6) • Electronic Timestamp (CTR5)	• Message Integrity (REQ1) • Proof of send/receive (REQ6)
Message Confidentiality	• WS-Security 1.1 using XML Encryption	• TLS (CTR1) • Message Encryption (CTR2)	• Message Confidentiality (REQ2)
Non-Repudiation of Receipt	• Signed Receipt Signal Message	• Electronic seal (CTR3) • Electronic signature (CTR6) • Electronic Timestamp (CTR5)	• Message Integrity (REQ1) • Proof of send/receive (REQ6)
Reliable Message	• AS4 reception awareness feature for lightweight, interoperable reliable messaging	• Electronic seal (CTR3) • Electronic signature (CTR6) • Electronic Timestamp (CTR5)	• Message Integrity (REQ1) • Proof of send/receive (REQ6)