Security guidelines on the appropriate use of qualified electronic registered delivery services

Guidance for users

VERSION 2.0

FINAL

DECEMBER 2016

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use trust@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

ISBN 978-92-9204-214-1, DOI 10.2824/985945

Table of Contents

Executive Summary

On July 1st 2016, Regulation (EU) 910/2014 (hereafter called the eIDAS Regulation), which lays down the rules on electronic identification and trust services for electronic transactions in the internal market came into force covering across Europe in all 28 Member States. It defines trust services for supporting electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services and website authentication.

The eIDAS Regulation represented a big step forward in building a digital single market as it provides one common legal framework for all parties relying or providing on those kinds of services. Indeed, various sectors of the economy (e.g. finance, banking, transport, insurance, health, sharing economy, trading, etc.) where obligations exist for security, reliable identification, strong authentication, legal certainty of evidences, will clearly be positively affected by the eIDAS Regulation. This latter will indeed allow citizens, businesses and public administrations to meet such obligations for any (cross-border) electronic transaction as they will now be able to use the recognised eID means and (qualified) trust services. In particular, data sent and received using a qualified electronic registered delivery service shall enjoy 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 qualified electronic registered delivery service.

This document addresses qualified electronic registered delivery services and is one out of a series of five documents which aim to assist parties wishing to use qualified electronic signatures, seals, time stamps, eDelivery or website authentication certificates to understand the subject correctly as-well-as the potential benefits, amongst others, by giving examples of possible applications. This series of documents also aims to give those parties some advice on how to correctly use the related qualified trust services.

After explaining what a qualified electronic registered delivery service is and what properties/function it does and does not provide, the following concrete examples of use are given for inspiration to the readers:

- Enabling electronic registered mail;
- Supporting official submissions in eGovernment services;
- Accessing sensitive data;
- Exchanging (sensitive) data;
- Notarization of events.

Next to the above, and as even the most secure / trusted service becomes insecure and unreliable if not being integrated or used correctly, some key recommendations are given for correct integration and use. This is expressed in three levels for relying parties:

- Basic/Minimum recommended level of implementation to be followed by entities or in processes dealing with normal levels of criticality of data and therefor can live with a lower maturity in implementing trust services (technology).
- (Standard) Recommended level of implementation to be followed by entities or in processes dealing with important business data and therefor need to be able to rely on a medium to higher maturity of implementation of trust services (technology).
- Enhanced recommended level of implementation to be followed by entities or in processes dealing with data of sensitive/high level of criticality and therefor need to be able to rely on a (very) high maturity of implementation of trust services (technology).

1. Introduction

1.1 General context/the eIDAS regulation on eID and trust services

Regulation (EU) No 910/2014[1] (hereafter the **eIDAS**[2] Regulation), on electronic identification and trust services for electronic transactions in the internal market, provides a predictable regulatory environment for electronic identification and a set of electronic trust services, namely electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication.

It is possible to use these trust services as well as electronic documents as evidence in legal proceedings in all EU Member States contributing to their general cross-border use. Courts (or other bodies in charge of legal proceedings) cannot discard them as evidence only because they are electronic but have to assess these electronic tools in the same way they would do for their paper equivalent.

Whether you are a large company, a SME or a citizen willing to complete an electronic transaction in another EU country, e.g. submit a call for tender or register as a student in another EU Member State (MS), besides reducing time and costs, the eIDAS Regulation will ensure cross-border recognition of national eID and electronic trust services supporting your electronic transaction. Hence it will boost trust, security and convenience.

Since 1 July 2016, most provisions of the eIDAS Regulation are directly applicable in the 28 EU Member States' legal framework overcoming problems of fragmented national regimes. It provides legal certainty and fosters the usage of eID means and electronic trust services for online access and online transactions at EU level.

The eIDAS Regulation will ensure that people and businesses can use their national eIDs to access public services in other EU countries where eIDs are required for such an access at national level. It also creates an EU wide internal market for electronic trust services by ensuring their recognition and workability across borders and are considered equivalent to traditional paper based processes.

1.2 Opportunities brought by the eIDAS Regulation

The opportunities reside in leveraging eID and electronic trust services as key enablers for making national and cross-border electronic transactions more secure, more convenient, trustworthy and benefiting from legal certainty.

The broader adoption of EU-wide recognised eID means and of electronic trust services will facilitate and boost the digital transformation of organisations, be it public administrations or businesses, enhance customer experience, improve the security of electronic transactions and stimulate the provisioning of new and innovative services.

[1] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
[2] See Glossary.

To this end, a large number of sectors (e.g. finance, banking, transport, insurance, health, sharing economy, trading, etc.) where obligations exist for security, reliable identification, strong authentication, legal certainty of evidences, will be positively affected. The eIDAS Regulation will indeed allow citizens, businesses and public administrations to conveniently meet such obligations for any cross-border electronic transaction using the recognised eID means and (qualified) trust services of their choice. Without undergoing identity verification based on physical presence, but by using MS notified eID means of a level "high", one should for example be able to use public services in another country or banks may accept such eID to open a bank account[3]. By relying on a qualified electronic time stamp, one shall enjoy, all over the EU, 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. By relying on a qualified electronic registered delivery service, one will benefit, all over the EU, from the presumption of the integrity of the registered 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 that qualified trust service.

1.3 Specific Role of the qualified trust services

To further enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, the eIDAS Regulation introduces the notions of qualified trust service and qualified trust service provider with a view to indicating requirements and obligations that ensure high-level security of whatever qualified trust service or product is used or provided and, as a consequence, are granted a higher presumption of their legal effect.

Therefore, when looking for trust services, selecting qualified ones ensures benefiting from a high level of security and legal certainty of trust services. E.g., qualified electronic time stamp shall enjoy, all over the EU, 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.

1.4 Initiation and supervision of qualified trust services

In order to ensure high-level security of qualified trust services, the eIDAS Regulation foresees an active supervision scheme of qualified trust service providers (QTSP) and qualified trust services (QTS) they

[3] National legislations on prevention of money laundering may currently may force identity verification to be based on physical presence. Furthermore, the use by the private sector of electronic identification means under a notified scheme is on a voluntarily basis only (see Recital 17 of the eIDAS Regulation).

provide (hereafter referred to as a QTSP/QTS) by the national competent supervisory body (SB) that supervises, ex ante and ex post, fulfilment of the **QTSP/QTS requirements and obligations**[4].

All those requirements must be met by the QTSP/QTS before providing the very first qualified trust service output, e.g. before issuing the very first qualified time stamp in the case of QTSP providing qualified time stamping services.

Before a TSP/TS is granted a qualified status (QTSP/QTS), it will be subject to a pre-authorisation process – the so-called initiation process. QTSPs may only begin to provide the qualified trust service after the qualified status has been granted by the competent supervisory body and indicated in the national **trusted list**[5]. From there, the supervision scheme covers the full life cycle of each QTS and each QTSP, from its genesis until its termination.

In practice, where TSPs, without qualified status, intend to start providing qualified trust services, they shall submit to the supervisory body a notification of their intention together with a conformity assessment report issued by an "eIDAS" accredited conformity assessment body. Before notifying the competent supervisory body of their intention to start providing qualified trust services, the future QTSP/QTS must hence successfully pass an external assessment (audit) to confirm it fulfils the eIDAS requirements. That audit must be conducted by a conformity assessment body specifically accredited to carry out assessments of QTSP/QTS. The audit results in a formal conformity statement confirming - if such is the case - that the QTSP/QTS meets all the applicable requirements of the eIDAS Regulation. Based on the notified information including the report of such an audit, the competent SB will formally verify that the candidate QTSP/QTS meets the applicable eIDAS requirements and, in case of positive verification, it will undertake the publication of the grant of the qualified status for that QTSP/QTS in the national trusted list.

It is only when its qualified status is published in the corresponding national trusted list that the QTSP/QTS is authorised to provide the corresponding QTS.

Note: A TSP cannot be deemed as qualified without providing at least one type of a qualified trust service (cfr Art.3.20 of the eIDAS Regulation). A TSP is granted a qualified status separately for each type of qualified trust service covered by the eIDAS Regulation. E.g. a QTSP qualified for the provisioning of qualified certificates for electronic signatures is not per se granted a qualified status for the issuance of qualified time stamps; it must first complete the full pre-authorisation process and have its granted qualified status for the provision of qualified time stamp published explicitly in the national trusted list before issuing qualified time stamps in addition to the provision of qualified certificates for electronic signatures. There are nine different types of QTSs defined by the eIDAS Regulation for which a qualified status is granted separately: provision of qualified certificates for electronic signatures, provision of qualified certificates for electronic seals, provision of qualified certificates for website authentication, qualified preservation service for qualified electronic signatures, qualified preservation service for qualified electronic seals, qualified validation service for qualified electronic signatures, qualified validation service for qualified electronic seals, qualified electronic time stamps services, and qualified electronic registered delivery services.[6]

[4] See glossary
[5] See glossary.
[6] See Annex A.7 for further details.

For marketing purposes, once qualified, a QTSP/QTS may use the EU Trust Mark for qualified trust services when promoting its QTS. That trust mark shown in Figure 1 can only be used by a QTSP to "label" its QTS. It can be used on any support provided it meets requirements from Art.23 of the eIDAS Regulation (e.g. a link to the corresponding national trusted list where consumers may verify the granted qualified status must be displayed on the QTSP's website) and rules of Commission Implementing Regulation (EU) 2015/806.[7] Basically, this secondary legislation sets the form, colour and size of the EU trust mark, sets the obligation to clearly indicate the qualified services that the EU trust mark pertains to, and allows association with other graphical or textual elements provided that certain conditions are met. [8]

Figure 1: EU trust mark for qualified trust services

The use of the EU trust mark, which is voluntary, aims to foster transparency of the market and help consumers distinguishing between qualified trust services and non-qualified ones.

Once granted a qualified status, QTSPs and their QTSs have the obligation to pass, and submit the competent supervisory body with a two-yearly conformity assessment report (CAR) issued by an accredited CAB confirming that the QTSP and the QTSs it provides fulfil the requirements laid down in the Regulation. Competent supervisory bodies are also allowed, at their own discretion and at any time, to audit themselves any QTSP/QTS for which they are competent or to request an accredited CAB to perform an ad hoc audit.

QTSPs and their QTSs are supervised for their entire lifecycle, from their genesis to their termination. In particular, in order to ensure sustainability and durability of QTSs, as well as to ensure proper termination and user's confidence in their provision, QTSPs must maintain, at all times, an up-to-date termination plan. That plan is to be agreed by the SB upon initiation and regularly checked for compliance during the life of the QTSP/QTS.

1.5 A focus on qualified electronic registered delivery services

The eIDAS Regulation establishes the principle that an electronic document should not be denied legal effect on the grounds that it is in an electronic form.

This regulation also defines an electronic registered delivery service, hereafter called eDelivery service, 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*

[7] Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services (Text with EEA relevance). OJ L 128, 23.5.2015, p. 13–15.
[8] See https://ec.europa.eu/digital-single-market/en/news/eu-trust-mark for more guidance on the use of that trust mark, downloadable images, user manual and answers to frequently asked questions.

data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations" (Art.3.36).

In practice the data referred to by that definition as being transmitted under such an eDelivery service from a sender to a receiver can be of any type, including electronic documents (initially created in electronic form or dematerialised documents), structured or not. The transmission means can be of any kind as well including but not limited to the well-known email system.

By relying on a qualified electronic registered delivery service, one will benefit, all over the EU, from the presumption of the integrity of the registered 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 that qualified trust service.

1.6 Scope of the present document and relationship with the other recommendations

This document proposes **security guidelines on the appropriate use of qualified electronic registered delivery services**. It aims to support relying parties and end users of qualified electronic registered delivery services to securely use these services.

The target audience of the document are end users and relying parties of qualified electronic registered delivery services. This could comprise individuals, businesses and public administrations. For example, it could be a public administration that wishes to formalize electronic interactions with citizens to benefit from the legal guarantees provided by such qualified trust services, and which would like to ensure it is utilizing these services:

- In compliance with the eIDAS Regulation.
- In a proper and secure manner that guarantees that the security properties of the service are being maintained.

The present document is organised to provide information and guidance with regards to the following aspects of qualified electronic registered delivery services:

- What is it?
- What key properties it provides?
- What properties can it not provide?
- What are the potential use cases?
- What are the usage best practices?
- Example of tools & practical usage aspects.

Four other linked documents propose security guidelines on the appropriate use respectively of qualified electronic signatures, qualified electronic seals, qualified electronic time stamps and qualified website authentication certificates.[9]

Although each of these qualified trust services share some technical backgrounds or tools and thus provide some common functionalities, such as illustrated below, each of them has its own objectives and core functionalities as summarised in the following table:

[9] See *https://www.enisa.europa.eu/topics/trust-services/qualified-trust-services*.

TRUST SERVICE	Data Integrity	Confidentiality	Authenticates Origin *(NATURAL PERSON)*	Authenticates Origin *(LEGAL PERSON)*	Authenticates Time
QTS	✓	✗	✗	✗	✓
QES	✓	✗	✓	✗	✗
QESeal	✓	✗	✗	✓	✗
QWAC	✓	✓	✓	✓	✗
QeDel	✓	✓*	✓	✓	✓

*not a core functionality but is usually provided as part of a greater solution

Table 1: Comparative table of functionalities offered by the various types of qualified trust services

If each (qualified) trust service can be used as a stand-alone service, some (qualified) trust services may support other (qualified) trust services.

2. Qualified electronic registered delivery – what is it?

2.1 Electronic registered delivery service

The eIDAS Regulation establishes the principle that an electronic document should not be denied legal effect on the grounds that it is in electronic form.

This regulation also defines an electronic registered delivery service, hereafter called eDelivery service, 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).

In practice the data referred to by that definition as being transmitted under such an eDelivery service from a sender to a receiver can be of any type, including electronic documents (initially created in electronic form or dematerialised documents), structured or not. The transmission means can be of any kind as well including but not limited to email.

Usually the data referred to by the definition as being transmitted under such an eDelivery service from a sender to a receiver is generally called a message.

eDelivery can be used by all kinds of entities willing to share electronic documents securely, such as public administrations, business organisations, and citizens. The following figure illustrates the different types of message transfers that can benefit from eDelivery: Administration to Administration (A2A), Administration to Business… Customer to Customer (C2C).

2.2 Qualified electronic registered delivery service

Qualified eDelivery service means an electronic registered delivery service which:

- is provided by qualified trust service providers, i.e. organisations under national supervision and whose compliance with requirements is regularly checked by an accredited, trusted entity, the so-called conformity assessment body;
- ensures a high level of confidence with regards to the identification of the sender;
- ensures the identification of the addressee before the delivery;
- protects the sending and receiving of data by using an advanced electronic signature or seal of a qualified trust service provider in such a manner as to detect all data alteration;
- protects the date and time of sending and of receiving by using qualified electronic time stamps;
- conforms to other potential standards considered relevant by the Commission.

Figure 1: Qualified eDelivery service example

Registered email is a general-purpose implementation of eDelivery, whereas there are more specific eDelivery services, such as tax declaration delivery or eInvoicing that uses different message types and communication channels.

3. Qualified electronic registered delivery – what key properties does it provide?

3.1 Legal Properties

Data sent and received using a qualified electronic registered delivery service shall enjoy 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 of the date and time of receipt, indicated by the qualified electronic registered delivery service.

Data in this context can equally refer to email, other messages, or structured attachments, depending on the general conditions of the service provider.

Hence, qualified electronic registered delivery provides the sender with a legal proof that he/she has sent a given data at a given time to a given receiver and that this receiver has accepted the message at a given time.

Proof of delivery

The sender receives an unforgeable time stamped proof of when he/she has delivered a given message to a receiver, independently on the receivers' ability to receive it. The currently used receipt for paper based registered mail contains a handwritten address, a date and a signature by a postal officer, which in general is not that difficult to fake.

Proof of reception

Both the sender and the recipient receive an unforgeable time stamped proof of when the receiver received or opened the electronic message.

Proof of integrity

Both the sender and the receiver can be sure that the message has not been changed during transmission.

Protection against the risk of loss, theft, damage or any unauthorised alterations

Qualified and non-qualified electronic registered delivery are services that are legally defined as ensuring the protection of the transmitted data against the risk of loss, theft, damage or any unauthorised alterations.

3.2 Security properties

Sender identification

The receivers know for sure who sends the data to them. Current email and current registered mail has no such proof as anybody can write any sender address on an email or a registered mail.

Secure time stamping

All time indications, i.e. the date and time of sending, receiving and any change of the transmitted data, are protected by a qualified electronic time stamp. Such reliable time sources provide legal presumption of the accuracy of the date and time of the time stamped data as well as the integrity of that data.

Confidentiality

Both the sender and the receiver can be sure that the message cannot be accessed by unauthorised persons during the transmission.

Content (data) integrity

A traditional postal service can never guarantee which message was in the envelope of a registered mail. This opens the door for conflict where the receiver claims to have received a different document than the one the sender claims to have sent. Qualified electronic registered delivery services ensures the integrity of the transmitted data, i.e. of the content of the message.

Control on routing errors

With current email, the sender may accidently type the wrong email address. Qualified electronic registered delivery procedures typically help the user to check different parameters of the receiver before processing to the transmission.

When sending a letter to a non-existent address, the mistake is found out only when the parcel comes back. Qualified electronic registered delivery service provider should inform you about the ability of the receiver to accept the message before you transmit it.

Interoperability

A useful concept of qualified electronic registered delivery services is to indicate to the sender all formats of messages that the intended receiver can process. Sometimes, the service provider can check and accept only messages explicitly accepted by the receiver. Qualified electronic registered delivery service providers can also propose additional services consisting in transforming a message from one format to another, e.g. from Word to PDF, if there is no confidentiality rule avoiding them to get access to the message.

3.3 Functional properties

Sending of large files

Most qualified electronic registered delivery services allow large messages and messages of all kinds of formats to be transmitted. Currently used systems for transmitting large files are not always accepted by the receiver, as they do not have a certified trust level.

Fast processing

Qualified electronic registered delivery services is instantaneous, e. g., much faster than paper based mail.

3.4 Other properties

Reduced risk

During message transmission via insecure current transmission channels, such as email, there is no guarantee on delivery, no assured confirmation of receipt, no proof that the received message is the same as the sent one, and little assurance on the confidentiality of the message. Qualified electronic registered

delivery makes it infeasible to manipulate data, to forge time stamps of sending or receiving, or to provide unauthorised access to the message.

All trust services that are used in qualified electronic registered delivery are provided by trusted service providers, which are regularly checked for having put in place the security measures required to avoid security risks for their customers.

Reduced cost

Qualified electronic registered delivery mainly avoids the logistical costs of delivering printed electronic documents or documents stored on some support such as a CD. Moreover, it reduces the cost of encoding information received on paper or of uploading files from the received support to the ICT system.

Qualified electronic registered delivery also reduces the cost of transmission failure or uncertainty inherent to insecure electronic messaging.

No transmission delays

As electronic transmission is virtually instantaneous, communication partners do not waste time when sharing documents. Similarly, as for parcels, the receiver of large message is informed once a message has been send to him and where he can download or process it.

No double sending

A common business practice today is to send information electronically for fast processing, and to send a signed paper version in addition in parallel for legal purposes. Using a qualified electronic registered delivery service instead of an unsecured messaging system such as email will make the additional sending of a signed paper version obsolete.

Incident handling and liabilities

In case of security incidents on data delivery, a qualified electronic registered delivery service provider must handle it properly and inform his/her supervisory body, who has to assess, whether the qualification status has to be withdrawn or not. Thus, customers will be informed independently and transparently in case of security issue related to the service on which they rely. The qualified trust service provider, nevertheless, remains liable for damage that was made to its customer by his/her negligence or omission.

4. Qualified electronic registered delivery – what cannot be provided?

4.1 Personal repository

(Qualified) electronic registered delivery is not about uploading documents to a central store so that they are available for processing or downloading by other partners wherever they like. It may use a secure repository to temporarily store the message once the sender sends it, until the receiver has accepted it.

4.2 Back-end processing

(Qualified) electronic registered delivery is not about ensuring that back-end processing systems get connected to better share information. It does however, provide a message communication channel to send and receive messages between backend processors. Back-end processors can only process messages of a very specific format, e.g. Excel accepts the formats *.xls, and *.csv, but no scanned image of a table. That is why the format of messages for backend processing has to be specified, but such specification is often out of scope of a pure electronic registered delivery project. Electronic registered delivery technology deals with all kinds of payload, i.e., all kind of message formats, and the communication partners have to agree which message they send over the (qualified) electronic registered delivery infrastructure.

4.3 Archiving

(Qualified) electronic registered delivery is not about archiving the transmitted message, nor the proof of sending or receiving it. However, such additional services can be provided as an additional service either from the (qualified) electronic registered delivery service provider or by a third party.

4.4 Boosting your activity

Your messaging partner will not send more messages just because a new message channel is made available. (Qualified) electronic registered delivery is mainly a less expensive and less risky message transmission technology; but it is not a generator of more messages. Nevertheless, if messaging is less expensive, this may increase the motivation to communicate.

4.5 Faster treatment of messages

A fast messaging transmission system does not guarantee a fast message processing system. The speed at which messages are processed depends on the abilities of the receiver to process the request and on the quality of the integration of (qualified) electronic registered delivery in back-end systems. If the receiver does not have the time to read your message once it is available, you cannot force him, just as the postal service cannot force someone to later pick up a registered letter that could not be delivered because nobody was at home.

5. Qualified electronic registered delivery – what are the potential use cases?

5.1 Overview and context of the given examples

In general, and to put (qualified) electronic registered delivery services into context, they are most often seen coming in addition to other identification and/or trust services as part of a wider solution. Although they allow exchanging data between parties in a legally certain way, communicating parties will have to be authenticated before being allowed to access the service and in some case the messages may be required to electronically signed, sealed and/or notarized (e.g. for longer term preservation).

In this context, and although the properties of qualified electronic registered delivery services have been described in the previous sections, the following properties are key for the use case examples mentioned below:

- Qualified electronic registered delivery services provide the parties involved with a vehicle via which they can obtain "guaranteed delivery" of their data to the other party.
- Optionally such services can amongst others be extended with longer term notarisation services to preserve legal evidence of the transaction having taken place.

These properties allow several "types of use cases" which can be applied in many areas of application as show in the present section. The table below highlights the identified types of use cases. The mapping on areas of applications in no way tries to be exhaustive but only tries to indicate the huge potential of qualified electronic registered delivery services.

	C2C	C2B C2G	B2B	B2G B2A	G2G A2A
Enabling electronic registered mail	●●	●●	●●	●●	
Supporting official submissions		●●		●●	
Accessing sensitive data		●	●●	●●	●●
Exchanging (sensitive) data		●	●●	●●	●●
Notarization of events		●●	●●	●●	

Table 2: QeDelivery application areas

5.2 Enabling electronic registered mail

Electronic registered Mail is, according to ETSI[10], an enhanced form of mail transmitted by electronic

[10] ETSI TS 102 640-1 V2.1.1 - Electronic Signatures and Infrastructures (ESI) - Registered Electronic Mail (REM)

means which provides evidence relating to the handling of an e-mail including proof of submission and delivery. If the service provider for such electronic registered e-mail is a qualified electronic registered delivery service provider, the users can trust the security properties of the offered qualified trust service and use the provided evidences in any legal proceedings. Where today there is a lot of exchanges of (optionally signed) messages, parties at current have no way of knowing with (legal) certainty whether their message has arrived and may not receive any formal proof of delivery. Qualified electronic registered delivery services have the ability to change that.

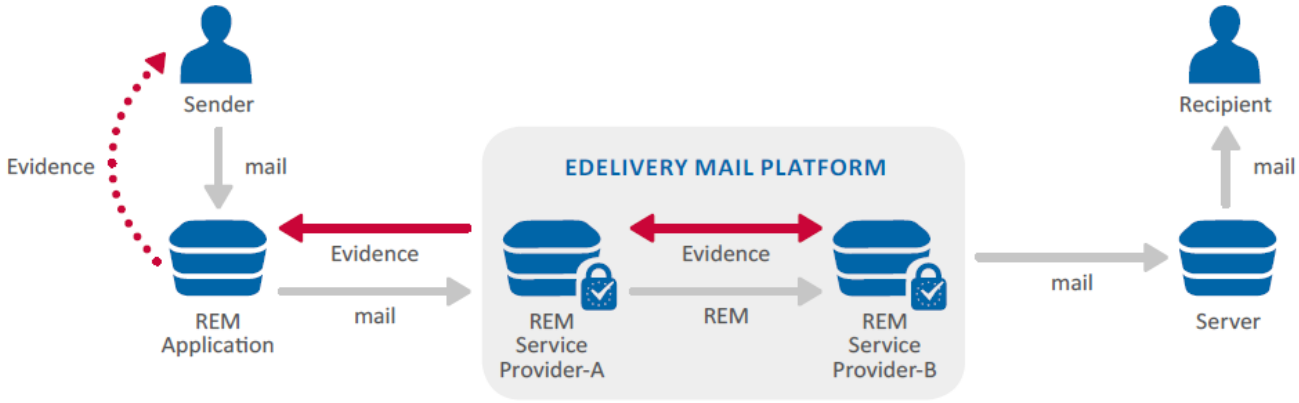

Figure 2: Electronic registered mail delivery service

Examples of concrete application are:

- C2C/B2B: Replacement of registered postal mail by qualified electronic registered delivery services.
- C2G/G2C: Delivery of official notifications (e.g. in context of Court proceedings).

5.3 Supporting official submissions in eGovernment services

Citizens/Companies have multiple possibilities to ask for public subsidies. In most cases, signed documents are used to apply for such help. Upon receipt, the administration encodes the data, sends back a confirmation of receipt, then validates the request and sends back the final decision. In general, citizens fill in the request on their PC, but still print it and send it by ordinary (or registered) post. Public administration can spare encoding time and several processing steps, including generating a confirmation of receipt, should this service be offered by means of a qualified electronic registered delivery service. Faster processing can motivate citizens to use such a qualified trust service rather than sending printed forms. The overall advantages are less paper, no delay on transmission, simplified and automated processing at the administration, and avoidance of manual encoding of electronic forms if predefined message types are used.

http://www.etsi.org/deliver/etsi_ts/102600_102699/10264001/02.01.01_60/ts_10264001v020101p.pdf

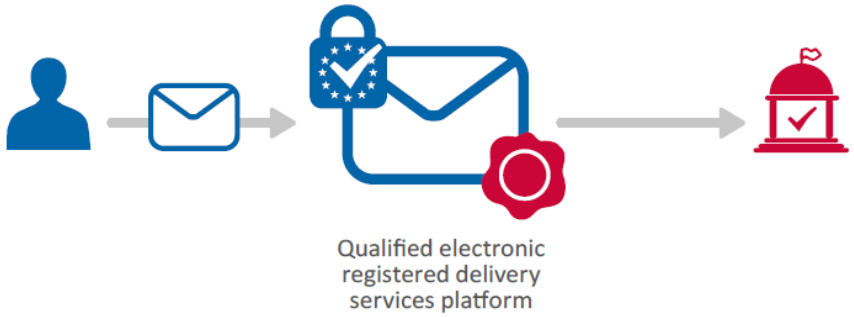

Figure 3: Submission in e-Government services

Examples of concrete application are:

- C2G: Citizens submitting a request for parental leave, for social security benefits, etc.
- B2G: Companies requesting subsidies, filing a periodic report, etc.

5.4 Accessing sensitive data

In many cases certain parties need to get access to sensitive information and be very sure they receive the right information/response to their request. ePrescription is such a case. Today, in most cases, patients bring their prescription to the pharmacist. In case the prescribed medicine is unavailable, they have to contact the doctor to obtain clarifications or authorization of alternative medicine. In all cases, they encode the sold product before establishing a bill addressed both to the patient and to the health insurances. A qualified electronic registered delivery service would allow the doctor to send the prescription in electronic form to the pharmacist chosen by the patient (and at the same time report this prescription to the competent administration). This could also be applied cross border where a person needs to get a prescription and a local pharmacist needs to be able to request the right prescription from the person's doctor.

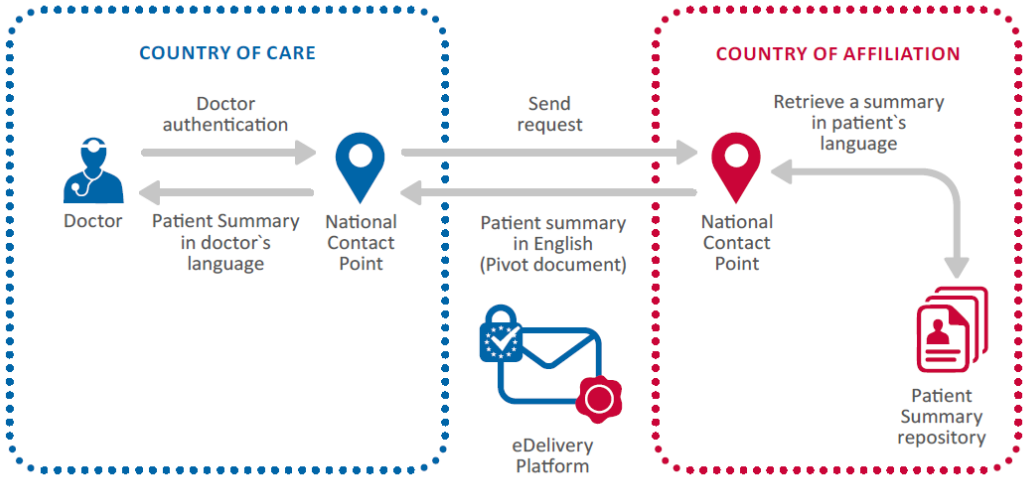

Figure 4: Accessing medical data example

Examples of concrete application are:

- A2C: ePrescription allowing the exchange of and access to the correct prescription by involved parties.
- B2G: Business being able to request formally/officially from government to receive certain attestations/official documents (and to get proof of receipt of the request/handling of their request).
- A2G: Attorneys having to deposit or access court-case files which should for obvious reasons only be exchanged in a secured manner.

5.5 Exchanging (sensitive) data

In many cases information needs to be exchanged in the context of a (longer term running) process. Data may need to be exchanged between social security administrations to handle a pension file or to handle child benefits (cross border). In an electronic procurement process the sequence of events and the exact moment of exchange of data needs to be established. Qualified electronic registered delivery services can not only be used in context of just a single exchange of informative (send/confirm receipt) but can also be used to ensure that a process is fully automated and the right process-controls are being put in place whereby guaranteed/confirmed and legally valid delivery of messages and documents can be very valuable. Examples of use include the use of qualified electronic registered delivery systems in the way enterprise resource planning (ERP) systems operate in large companies. Multiple messages, such as those regarding price negotiations, trading transactions, order management, inventory management, transportation, and capacity management have to be securely transmitted between buyers and vendors.

Examples of concrete applications are:

- G2G: Exchange of social security information (nationally or cross border) such as pension file info, tax information, or child benefit information.
- B2G: Exchange of data in context of import/export and customs handling (including handling of permits) or the handling of eProcurement/eInvoicing.
- B2B: Exchange of information in context of just in time production with contractors and suppliers.
- A2A: Exchange of health files between parties treating the patient and the administration involved in paying the social security covered expenses.

5.6 Notarization of events

Today, in many countries, organisations need to send information to regulators, such as annual reports, activity reports, risk assessment and risk registers, or audit reports. Often, these reports are sent in paper form via registered postal mail, or sometimes are physically delivered to make sure that deadlines are kept. To avoid scanning of such paper-based reports, the regulators often ask for an electronic version on an annexed CD. Faster and more reliable deliveries can be achieved when using qualified electronic registered delivery services whereby the receiving authority can upon receipt notarize the receipt and return a confirmation of that receipt. In addition, there could also be situations whereby a third party acts as go-between to handle the electronic delivery as a neutral third party instead of the receiving party handling the notarization.

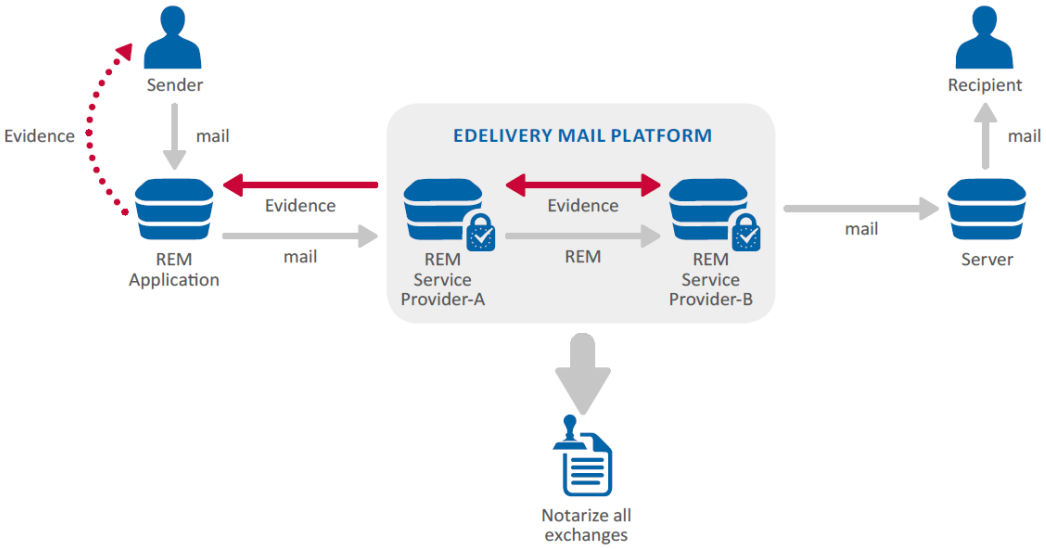

Figure 5: Notarizing events example

Examples of concrete application are:

- B2G: Submission of audit reports and financial statement to financial supervisors or submission of periodic audit reports of qualified trust service providers to the national supervisory bodies.
- B2B: Electronic registered delivery of financial/payment data between involved parties and notarization in a ledger of all transactions.

6. Qualified electronic registered delivery – what are the usage best practices?

6.1 Security guidelines and levels

In this section, we propose recommendations according to three levels which represent the "strength/rigorousness" with which qualified electronic registered delivery services should be applied in a specific context. This "strength/rigorousness" of course depends on the use case or type of application / environment in which qualified electronic registered delivery services are being applied. Dimensions that could have an impact on the "strength/rigorousness" of applying the recommendations, are the criticality of the processes and/or data being involved in the business process which is being supported by the respective qualified trust service. This, every organization has to determine for itself based on a risk assessment. For inspiration possible mapping of basic/recommended/enhanced vs business criticality and/or data protection is being given in Annex B.

In short the three levels of recommendations are in increasing order (whereby the higher level suppose that the lower level is also taken into account):

BASIC	for recommendations to be followed by entities or in processes dealing with normal levels of criticality of data and therefor can live with a lower maturity in implementing trust services (technology).
RECOMMENDED	for recommendations to be followed by entities or in processes dealing with important business data and therefor need to be able to rely on a medium to higher maturity of implementation of trust services (technology).
ENHANCED	for recommendations to be followed by entities or in processes dealing with data of sensitive/high level of criticality and therefor need to be able to rely on a (very) high maturity of implementation of trust services (technology).

6.2 BASIC

Citizens

Be users of a qualified electronic signature or seal, which is often the entry condition to qualified electronic registered delivery services (hereafter QeRDS).

Look for the EU trust mark for qualified trust services when selecting providers.

Make sure to archive your messages in an appropriate way (a single hard disk is far more likely to crash than your letter folder to get lost or burned.

Public administration / Business entity

Understand the opportunities; assess which of your current messaging can benefit from the advantages of QeRDS.

Use QeRDS for key communication partner in a pilot phase before deploying it for all communication partners. Note, however, that it is easier to convince key players than multiple citizens that only rarely exchange messages with the administration.

Use existing or upcoming qualified QeRDS providers that can easily be introduced to your communication partners.

Use, whenever possible, operational or ready to start QeRDS service provider(s) that your communication partner uses for other purposes too, rather than choosing silo solution.

Do not charge for the QeRDS, rather for the service based on the shared message.

Involve the operation staff in changing the delivery procedures.

6.3 RECOMMENDED

Citizens

Privilege qualified QeRDS providers that allow combining several QeRDS (communication with several administrations, with banks, shops) and maybe other services such as archiving, internet service providers).

Organise your QeRDS messages with the same, if not with more care than your paper bills, product guarantees, banking sheets, medical advice, insurance papers, etc.).

Read the applicable terms and conditions, in particular clauses on your responsibility in maintaining the security of your credential or access to the service.

Public administration / Business entity

Correctly define message format and foster integration in the backend systems. There is little benefit for the administration when introducing QeRDS for tax declaration, if the electronically delivered document still needs to be encoded manually in a backend system.

Use open standard and open services whenever the message volume and the cost saving are high enough to finance more than a single service provider to allow fair competition among service provides in the interest of the quality of service offered to your communication partners.

Build your QeRDS introduction project upon an assessment of risks to be avoided, opportunities and cost saving, estimation of implementation and operational costs, and quantified return on investment. Do not underestimate operational costs to operate QeRDS and traditional delivery at the same time, nor setup costs to train staff and change operational procedures

Allow sufficient time to your communication partner to migrate to QeRDS before saving the cost of maintaining traditional messaging systems.

Identify key implementation issues.

Communicate on your project and during your project with the interested parties, in particular the qualified QeRDS providers and the communication partners.

6.4 ENHANCED

Citizens

Make sure that you can continuously, even in case of an ICT issue or loss of your primary credentials, connect and process your QeRDS messages.

Public administration / Business entity

Consult with other public administration to create the critical mass for a QeRDS.

Align your QeRDS introduction strategy with the national strategic for lean administration.

Produce a strategic roadmap for migrating communication, primarily non-electronic communication to QeRDS. Prioritise key applications, but do not ignore quick wins to gain credibility among your stakeholders.

Plan your budget as QeRDS is a substantial investment that does not only change an ICT system, but also your administrative processes and the way you expect your communication partners to behave.

Be prepared that easier communication may trigger more activities for the administration. If a complaint to policy can be made via QeRDS, more people will make complaints than if a victim has to go physically to an office and spend some time waiting for his/her complaint to be accepted. This, however, is a general remark applying to easy access to administration; independently whether it is open via a QeRDS or a dedicated Web portal.

To introduce QeRDS in A2B, negotiate private public partnership to finance the migration towards this new technology.

Use key performance indicators to measure the benefits of QeRDS and the reach of the predicted return on investment.

Consider openness for communication partners using unusual setups, such as eID cards from other EU member states, etc.

Privileged compatibility with commercial products.

Select standards for the message format with great care (e.g. xml format for structured data). Publish your message format in due time to all communication partners, so that they can adapt their backend systems.

7. Qualified electronic registered delivery – example of tools & practical usage aspects

7.1 Implementing qualified electronic registered delivery services (user perspective)

The user experience and tools for using qualified electronic registered delivery services is pretty dependent of the end-user application and interface provided by the related qualified trust service provider.

7.2 Relevant standards regarding qualified electronic registered delivery services (expert perspective)

ETSI Technical Committee Electronic Signatures and Infrastructures (ESI)

ETSI EN 102 640 is multi-part deliverable covering Registered Electronic Mail (REM), as identified below:

- Part 1: "Architecture";
- Part 2: "Data requirements, Formats and Signatures for REM";
- Part 3: "Information Security Policy Requirements for REM Management Domains";
- Part 4: "REM-MD Conformance Profiles";
- Part 5: "REM-MD Interoperability Profiles";
- Part 6: "Interoperability Profiles":
    - Sub-part 1: "REM-MD UPU PReM Interoperability Profile";
    - Sub-part 2: "REM-MD BUSDOX Interoperability Profile";
    - Sub-part 3: "REM-MD SOAP Binding Profile".

The Universal Postal Union (UPU)

The UPU has developed some standards regarding interoperability aspects, the registered electronic mail, in collaboration with CEN[11].

S33 Interoperability framework for postal public key infrastructure:

> "The objective of this standard is to create a common Postal Public Key Infrastructure (PKI) to provide global certification and security services aimed at globally binding the identity of individuals and organisations with their public key. The framework itself and its first four elements (PKI structure, cryptographic algorithms, data formats and data dissemination protocols) are included."

S52 Functional specification for postal registered electronic mail (PReM):

> "This standard defines the functional specification of a secure electronic postal service, referred to as the postal registered electronic mail or PReM service. PReM provides a trusted and certified electronic mail exchange between mailer, designated operators and addressee/mailee. In addition, evidence of corresponding events and operations within the scope of PReM will be generated and archived for future attestation."

[11] http://www.upu.int/uploads/tx_sbdownloader/20160209_Catalogue-of-UPU-standards.pdf

Annex A: Glossary

A.1 eIDAS – What is it?

eIDAS is the acronym used to refer to Regulation (EU) No 910/2014 on electronic identification (eID) and trust services for electronic transactions in the internal market. The eIDAS Regulation is about trust, seamless user experience and convenience in online cross-border transactions.

A.2 Electronic seal

An electronic seal is a piece of data in electronic form, created by a legal person, which is attached to or logically associated with an electronic document (or data) to ensure its origin and integrity.

It is similar in the paper world to the dry seal of a company on a piece of paper to indicate that the document originates from the company and make it authentic and official.

A.3 Message

An information or document sent to a receiver.

A.4 Hash value (of a file)

A hash value is a standardised and unique summary of a message, which is obtained by applying a specific cryptographic tool called a cryptographic hash function.

A hash function is any function that can be used to map digital data of arbitrary size to digital data of fixed size, with slight differences in input data producing very big differences in output data.

A cryptographic hash function is a hash function which has specific security properties:

- It is considered practically impossible to recreate the input message from its hash value;
- It is considered practically impossible to compute from a specific message a second message that has the same hash value (i.e. different messages lead to different has values);
- It is considered practically impossible to find two different messages that would lead to the same hash value (no collisions)

With such properties, when applied to the same message repetitively the hash value is always the same, while if the message is slightly modified (even by one single bit) the hash value will always be different. That allows to verify the integrity of a message compared to the message on which the hash was previously computed; when the hash values are identical, then the messages are identical.

As cryptographic hash values represent large amounts of data as much smaller numeric values, they are often used with digital signatures. Signing a hash value is more efficient than signing the larger value.

A.5 Trusted list

A trusted list is a list including information related to the qualified trust service providers which are established in and supervised by an EU Member State, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014. Those lists have constitutive value and are primary source of information to validate that a qualified status is or has been granted to a QTSP and to the QTS it provides.

Trusted lists are essential elements in building trust among electronic market operators by allowing users to determine the qualified status and the status history of trust service providers and their services.

Member States may include in the trusted lists information on non-qualified trust service providers, together with information related to the non-qualified trust services provided by them. It shall be clearly indicated that they are not qualified according to Regulation (EU) No 910/2014.

Member States may include in the trusted lists information on nationally defined trust services of other types than those defined under Article 3(16) of Regulation (EU) No 910/2014. It shall be clearly indicated that they are not qualified according to Regulation (EU) No 910/2014.

A.6 QTSP/QTS requirements and obligations

The eIDAS Regulation (EU) No 910/2014 foresees a set of requirements and obligations for qualified trust service providers (QTSP) and qualified trust services (QTS) they provide in order to ensure high-level security of the qualified trust services. Those obligations include in a nutshell:

- **Processing of personal data** shall be carried out in accordance with Directive 95/46/EC.
- **Trust** service provider (TSP) is liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation, while the **intention or negligence of a QTSP shall be presumed**, unless proven otherwise by QTS. When TSP informed customer in advance on limitations on the use of their services, and when such limitations are recognisable to third parties, TSP is not liable when limitations have been exceeded.
- **Where** feasible, services must be **accessible for person with disabilities**.
- **Implementing 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. Measures shall be taken to prevent and minimize the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.
- **Very** strict rules regarding the obligation of **notifying security & personal data breaches**.
- **Additional requirements on QTSP operations and practices**:
    - Inform SB of any change in QTS provisioning and of intention to cease;
    - Up-to-date termination plan, agreed with the competent supervisory body (SB), to ensure continuity of service;
    - Requirements on employed staff and subcontractors, when used;
    - Sufficient financial resources and/or liability insurance, in accordance with national law;
    - Consumer information on terms and conditions, incl. on limitations on use;
    - Use of trustworthy systems and products ensuring the technical security and reliability of the supported processes;
    - Use of trustworthy systems to store (personal) data in a verifiable form;
    - Take appropriate measures against forgery and theft of data; and
    - Record and keep accessible activities related data, issued and received, even after cessation of activities.
- **Specific requirements** from the provisions laid down in the eIDAS Regulation with regards to the provision of a specific type of qualified trust service.

All those requirements must be met by the QTSP/QTS before issuing the very first qualified trust service output, i.e. before issuing the very first qualified time stamp in the case of QTSP providing qualified time stamping services.

Once granted a qualified status, the eIDAS Regulation also foresees an active supervision scheme of qualified trust service providers (QTSP) and qualified trust services (QTS) they provide by the national competent supervisory body (SB) to monitor fulfilment of the QTSP/QTS requirements and obligations throughout their lifetime.

A.7 Trust services defined by the eIDAS Regulation

In its Art.3.16, the eIDAS Regulation defines a 'trust service' as 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.

A.8 Qualified trust services defined by the eIDAS Regulation

Only those trust services listed in Art.3.16 of the eIDAS Regulation for which there are applicable requirements in the Regulation can benefit from the qualified status. eIDAS regulates the following nine qualified trust services:

1. **The provision of qualified certificates for electronic signatures**

   Certificates for electronic signature are electronic attestations which link electronic signature validation data to a natural person and confirm at least the name or the pseudonym of that person. Since 1 July 2016, an electronic signature can only be used by a natural person to sign, i.e. mainly to express consent on the signed data/document. This represents a significant difference from the eSignature Directive 1999/93/EC regime where an electronic signature, which could be used by legal persons, was defined as a means of authentication. Under the eIDAS Regulation, the entity who creates an electronic signature (the so called signatory) will be a natural person. Therefore, certificates for electronic signature cannot be issued to legal persons anymore. Instead legal persons can use certificates for electronic seals (see below).
   A qualified electronic certificate for electronic signatures is an essential element for a signatory to create qualified electronic signatures that shall have the equivalent legal effect of a handwritten signature all over the EU.

2. **The provision of qualified certificates for electronic seals**

   As explained above, since 1 July 2016, legal persons cannot create legally valid (qualified) electronic signatures anymore and cannot be issued (qualified) certificates for electronic signatures. Instead legal persons can use certificates for electronic seals, which are electronic attestations that link electronic seal validation data to a legal person and confirm the name of that person. The aim of an electronic seal is not to sign but to serve as an evidence that an electronic data/document was issued by a legal person, ensuring certainty of the data/document's origin and integrity.
   A qualified electronic certificate for electronic seals is an essential element for a legal person to create qualified electronic seals that shall enjoy, all over the EU, the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

3. The provision of qualified certificates for website authentication

Certificates for website authentication are issued to ensure the users (in particular citizens and SMEs) that behind the website there is a legal or natural person identifiable by trustworthy information.
The Regulation sets clear requirements for qualified website authentication certificates to be considered trustworthy together with obligations for qualified trust service providers of such qualified certificates with regard to the security of their operations, their liability and their supervision regime. As a consequence, the Regulation ensures transparency regarding the quality of the service offered to users, accountability of providers with regard to security of their services, trustworthiness of the data associated to qualified authenticated websites and technological neutrality of services and solutions.

4. Qualified preservation service for qualified electronic signatures

Such a qualified trust service aims to ensure the long-term preservation of information, in order to ensure the legal validity and trustworthiness of qualified electronic signatures over extended periods of time and guarantee that they can be validated irrespective of future technological changes.

5. Qualified preservation service for qualified electronic seals

Such a qualified trust service aims to ensure the long-term preservation of information, in order to ensure the legal validity and trustworthiness of qualified electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes.

6. Qualified validation service for qualified electronic signatures

Validation of electronic signature is an ancillary service to electronic signatures whose process aims to confirm the validity of an electronic signature.
Qualified validation services for qualified electronic signatures entail the verification by a qualified trust service provider that the requirements of the eIDAS Regulation are met by a qualified electronic signature in order to confirm its validity.

7. Qualified validation service for qualified electronic seals

Validation of electronic seal is an ancillary service to electronic seals whose process aims to confirm the validity of an electronic seal.
Qualified validation services for qualified electronic seals entail the verification by a qualified trust service provider that the requirements of the eIDAS Regulation are met by a qualified electronic seal in order to confirm its validity.

8. Qualified electronic time stamps services

Electronic time stamps are issued to ensure the correctness of the time linked to data/documents. Qualified electronic time stamp shall enjoy, all over the EU, 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.

9. Qualified electronic registered delivery services

By relying on a qualified electronic registered delivery service, one will benefit, all over the EU, from the presumption of the integrity of the registered 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 that qualified trust service.

The Regulation sets clear requirements for all such qualified trust services to be considered trustworthy together with obligations for their qualified trust service providers with regard to the security of their operations, their liability and their supervision regime.

A.9 Other terms

Browser: short of web browser, is a software application used to locate and display web pages.

Cryptography: the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, and authentication of origin.

Digital certificate: A certificate identifying a public key to its subscriber, corresponding to a private key held by the subscriber. It´s a unique code that typically is used to allow the authenticity and integrity of communication can be verified.

Hyper Text Transport Protocol (HTTP): A communication protocol used to connect to servers on the WWW. It establishes basically a connection with a web server and transmit information (e.g. HTML pages) to the client browser.

Internet: a global computer network that links minor computer networks allowing them to share information via standardized communication protocols.

Public Key Infrastructure (PKI): A PKI is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of digital certificates issued by a certificate authority (CA).

Protocol: a set of instructions required to initiate and maintain communication between sender and receiver devices.

Web server: using the client/server model and the WWW HTTP, web server is a software program that serves web page files to users

World Wide Web (WWW): Also shortened to Web. The World Wide Web is an information space where documents and other web resources are identified by URLs, interlinked by hypertext links, and can be accessed via the Internet.

A.10 Acronyms

ABBREVIATION	DESCRIPTION
CAR	Conformity Assessment Report
GMST	Greenwich Mean Sidereal Time
GMT	Greenwich Mean Time
UTC	Universal Coordinated Time
A2A	Administration to Administration
B2A	Business to Administration

ABBREVIATION	DESCRIPTION
B2B	Business to Business
B2C	Business to Consumer
B2G	Business to Government
C2B	Consumer to Business
C2C	Consumer to Consumer
C2G	Consumer to Government
CAB	Conformity Assessment Body
CEN	Centre Européen de Normalisation
eID	electronic Identification
EN	European standard
ETSI	European Telecommunications Standardisation Institute
EU	European Union
G2G	Government to Government
HTTP	Hyper Text Transport Protocol
HTTPS	HTTP Secure
IETF	Internet Engineering Task Force
MS	Member State
PKI	Public Key Infrastructure
PReM	Postal registered electronic mail
Q&A	Questions and Answers
QeRDS	Qualified electronic registered delivery service
QTS	Qualified Trust Service
QTSP	Qualified Trust Service Provider
QTSP/QTS	Qualified Trust Service Provider and the Qualified Trust Service it provides
QWAC	Qualified Website Authentication Certificate
RFC	Request For Comments
SB	Supervisory Body
SME	Small and Medium-sized Enterprise
TR	Technical Report
TS	Technical Specifications
TSP	Trust Service Provider
WWW	World Wide Web

Annex B: Possible mapping basic/recommended/enhanced vs business criticality and/or data protection

B.1 Understanding an organization's environment and corresponding criticality-levels

When trust services will be used by subscribers and relying parties, there will be many use cases / story-lines / etc. as explained in the use case examples mentioned in this document. However, and depending on the concrete environment the use case is applied in, the "strength/rigorousness" with which the recommendations should be applied might be less or more severe. Dimensions that could have an impact on the "strength/rigorousness" of applying the recommendations, are the criticality of the processes and/or data being involved in the business process which is being supported by the respective qualified trust service. So, without intending to be complete as a risk assessment depends of the concrete environment/context in which the organization is operating, some dimensions which might be considered to determine the risk-profile of the process and/or data being protected (and therefor the minimum "strength/rigorousness" to apply) are:

- **Business critical data & processes**: organizations store or process information that can have a less or more significant impact on their own organization and/or their partners and/or their clients. Examples of potential risks are e.g. loss of integrity of a database, compromise of business-confidential data, incorrect contracting-data, etc.
- **Data & processes with potential financial impact**: organization (especially but not only financial industry related organizations) have several processes which might have direct financial impact for themselves, for their partners and/or their clients ranging from amounts e.g. below a thousand euros to amounts going into millions of euros. Examples of potential risks are e.g.: faulty validation of signatures on mandates or payment instructions, rogue / criminal impersonation of third party providers, hacking of personnel or corporate accounts, false invoices, etc.
- **Personal data (processing)**: Personal data is clearly a very complex and high risk matter. The scope of personal data is very broad, ranging from less delicate personal data, to directly identifiable information to sensitive personal data. The more sensitive the data the stronger and more rigorous one should apply the recommendations. Examples of potential risks are: fines of up to 4% of the global annual revenues of a company, embarrassment due to faulty access personal information, unauthorized access/manipulation to e.g. biometric data, responding to a request-for-info based on an incorrect signed request, health data getting exposed / delivered incorrectly, authenticity/integrity of critical health records being non-verifiable, etc.

Note: We stress that the above are just examples of possible areas to consider to assess the risk-profile of the process and/or data being protected. Depending on the reader's environment other dimensions might apply depending on regulation, corporate policies, contractual obligations, etc.

B.2 Determining applicable criticality-levels and derive resulting minimum applicable recommendations

Following the above, it is proposed that organizations do their own analyses and following map their processes / data-to-be-processed onto the following "criticality-levels":

- "**Standard**" would entail any usage of a trust service under normal circumstance like but not limited to use cases e.g. involving financial exchange of a rather limited amount, personal records

with limited potential impact, or access to data/services of a limited classification level (e.g. internal/restraint).

- "**Advanced**" would entail any usage of a trust service in a context where more precautions / prudence is to be advised like cases which involve financial exchange of a rather important magnitude, personal records with rather important impact if going wrong, or access to data/services of a higher classification level like company-confidential.
- "**Sensitive**" would entail any usage of a trust service in a context where sensitive data is being involved, e.g. involving financial exchanges of a significant amount, personal record access of personal sensitive information, or access to data/services of a high classification level like company-/commercial-secret.

Based on the above "criticality-levels", one can easily see how the levels (Basic, Recommended, Enhanced) can match to these levels:

- **Basic** would entail the recommendations to-be-considered at the moment one is involved in a (trans)action that involves data/services of a "standard" level of criticality.
- **Recommended** would entail the recommendations to-be-considered at the moment one is involved in a (trans)action that involves data/services of an "advanced" level of criticality.
- **Enhanced** would be the recommendations to-be-considered at the moment one is involved in a (trans)action that involves data/services of a "sensitive" level of criticality.

CRITICALITY	RECOMMENDATION	FINANCIAL - CORPORATE - PERSONAL DATA/PROCESSES
normal	Basic	Limited importance
advanced	Recommended	Higher importance
sensitive	Enhanced	Significant importance

Annex C: References and bibliography

C.1 References

REF. ID	DESCRIPTION
[1]	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73–114.
[2]	ETSI TS 102 640: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM).

C.2 Bibliography

ID	DESCRIPTION
(a)	Jos Dumortier & Hannelore Dekeyser: "The Regulatory Framework for Trusted Time Services in Europe", S.Paulus, N. Pohlmann, H. Reimer (Editors): ISSE 2005 Securing Electronic Business Processes, Vieweg (2005), 107-119.
(b)	PEPPOL eDelivery state of play, http://www.peppol.eu/news/peppol-edelivery-state-of-play
(c)	e-CODEX eDelivery convergence, http://www.e-codex.eu/about-the-project/technical-background/e-delivery-convergence.html.
(d)	e-Delivery | e-SENS, http://www.esens.eu/content/e-delivery
(e)	SPOCS Starter kit, http://www.eu-spocs-starterkit.eu/, http://joinup.ec.europa.eu/site/spocs/eDelivery/index.html
(f)	http://www.syncorder.com/en

C.3 Relevant implementing acts

ID	DESCRIPTION
(i)	Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services (Text with EEA relevance). OJ L 128, 23.5.2015, p. 13–15.
(ii)	Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance). OJ L 235, 9.9.2015, p. 26–36.
(iii)	Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on

	electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance). OJ L 235, 9.9.2015, p. 37–41.
(iv)	Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance). OJ L 109, 26.4.2016, p. 40–42

Annex D: Frequently asked questions

D.1 eIDAS Regulation – Questions and answers on rules applicable to trust services as of 1 July 2016

The European Commission complied a Q&A document to help fully understanding the new legal framework in order to implement it or reap the benefits of electronic transactions.

The complied a Q&A document is available from https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas.

The Commission launched the eIDAS Observatory - an online collaborative platform for exchanging views and positions, sharing ideas and good practices. It is a virtual community of stakeholders whose aim is to build a common understanding of the issues relating to the implementation and uptake of the eIDAS Regulation and to facilitate the use of cross-border electronic identification and trust services. You can join the eIDAS Observatory and take part in the discussions.

D.2 How can I find a qualified trust service provider providing qualified electronic registered delivery services?

You can find a qualified trust service provider providing qualified electronic registered delivery services by looking:

- For the use of the EU trust mark for qualified trust services associated to the provision of qualified electronic registered delivery services in the marketing material of envisaged providers;

- For EU MS national trusted list as they are available from the EC list of pointers to the EU MS trusted lists (https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml) or by browsing the EU MS trusted lists from, e.g. http://tlbrowser.tsl.website. Trusted lists are organised per TSP, and then per trust service. Look up for a service type identifying the provision of qualified electronic registered delivery services (http://uri.etsi.org/TrstSvc/Svctype/EDS/Q or http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q) for which the current status is “granted” (http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted).

- For applicable terms and conditions, the policies and practices used by the QTSP to provide its qualified electronic registered delivery services should be available from the “TSP information URI” as part of the TSP information as listed in the relevant EU MS trusted list.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Athens, Greece

TP-06-16-353-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-214-1
DOI: 10.2824/985945