

INNOPAY

A business of Oliver Wyman



Ministerie van Economische Zaken
en Klimaat



Market impact of the eIDAS revision on trust services

innopay.com

March 2024

Table of contents

1.	Management summary	2
2.	Introduction	3
2.1.	Introduction	3
2.2.	Context	3
2.3.	Goal	3
2.4.	Approach	4
2.5.	Reading guide	4
2.6.	Acknowledgements	5
3.	Conclusions & recommendations	6
3.1.	Overall usage of (qualified) trust services will increase	6
3.2.	Costs for (Q)TSPs will rise due to higher regulatory burden	7
3.3.	Competition among (Q)TSPs will increase in Europe	8
3.4.	A sufficient number of sustainable revenue models will emerge for (Q)TSPs	8
3.5.	Recommendations	8
4.	Context	10
4.1.	eIDAS	10
4.2.	Types of trust services	11
5.	Impact analysis	23
5.1.	Electronic signatures	23
5.2.	Electronic seals	27
5.3.	Electronic time stamps	29
5.4.	Electronic registered delivery services	30
5.5.	Website authentication	31
5.6.	Electronic attestation of attributes	32
5.7.	Electronic archiving services	34
5.8.	Electronic ledgers	35
6.	Cost analysis	37
6.1.	Regulatory costs	37
6.2.	Financial penalties related to eIDAS	41
6.3.	Market adaptation costs	42
7.	Revenue model and competitor analysis	43
7.1.	New revenue models for QES	43
7.2.	Revenue models related to electronic attestation of attributes	43
7.3.	Revenue models for electronic ledgers	46
7.4.	Revenue models for electronic archiving services	46
7.5.	Value of qualified services is limitedly recognised	46
7.6.	Competition increases due to the emergence of a European market	47
8.	Appendix	48
8.1.	Qualified trust services 1-pagers	48
8.2.	Glossary ENG – NL	56
8.3.	List of abbreviations	57

1. Management summary

This report describes the expected change in the use of trust services due to the eIDAS revision, the impact of changing demand on the digital economy, and the investment and regulatory costs involved. The main research question of the report is: What is the economic impact within the Netherlands, both in the short and long term, of the proposed revision of the eIDAS regulation on the various trust services? This report has been conducted by INNOPAY, commissioned by the Ministry of Economic Affairs and Climate Policy, and the findings are based on desk research & interviews.

eIDAS defines trust services as electronic services that contribute to trust in a digital environment. eIDAS formulates five trust services: 1) electronic signatures; 2) electronic seals; 3) electronic time stamps; 4) electronic registered delivery services and 5) website authentication. The eIDAS revision introduces three new trust services: 1) electronic attestation of attributes; 2) electronic ledgers and 3) electronic archiving. Additionally, the management of means for remote electronic signature and electronic seals is introduced as a new sub service for QES and QESeals.

Usage of trust services

Based on the interviews with trust service providers, we assume that the use of qualified electronic signatures and electronic attestations of attributes will increase in the Netherlands due to the introduction of the *European Digital Identity Wallet* (EUDIW). Adoption of the EUDIW in the Netherlands is an important precondition to realise the market potential of electronic signatures and electronic attestations of attributes. Clarity about the role of authentic sources, common standards and (semantic) interoperability are crucial for adoption of (qualified) attestations of attributes.

The use for QESeals and QWACs is expected to increase. Usage of these services depends in part on their alignment with the EUDIW. The foreseen surge in utilisation reflects a larger trend, in which several European legislations (will) require the use of these services for data sharing. The services are also used more often in scalable data sharing initiatives in certain sectors.

There is still uncertainty regarding the adoption of QE-Archiving and QELedger services. The use of qualified electronic time stamps is unlikely to increase in the Netherlands due to the eIDAS revision.

Regulatory pressure & investment costs

The eIDAS revision places several additional requirements on trust service providers, increasing regulatory pressure and, consequently, compliance costs. The increased pressure and costs have a stronger effect on smaller (Q)TSPs and new entrants to the Dutch market. Next to that, in the current situation, growth in demand will not directly lead to additional disproportionate costs or large necessary investments by trust service providers. In most cases the rise in costs is related to increased turnover.

Competition & business models

The eIDAS revision is expected to further open the European market for trust services. It may also lead to market consolidation because larger trust service providers benefit from economies of scale. Harmonised supervision is important for a level playing field. For electronic signatures, new revenue models are created by the eIDAS revision, namely the issuance of (non-professional) signature certificates, free of charge to citizens, in connection with the EUDIW.

Recommendations

The Ministry of Economic Affairs and Climate Policy plays an important role for the internal market of trust services and in taking full advantage of the opportunities that the eIDAS revision offers for the Dutch digital economy. The market's success hinges on policy support and proactive involvement from the Ministry of Economic Affairs and Climate Policy. The following was recommended:

1. Formulate more policy on trust services and provide a clear direction and vision to the market
2. Contribute actively to filling preconditions for success of the EUDIW
3. Invest in better communication about trust services

2. Introduction

2.1. Introduction

This report describes the results of research commissioned by the Ministry of Economic Affairs and Climate on the market impact of the eIDAS revision on trust services, conducted by INNOPAY. The research examines the impact on the market (and use) of the various trust services, the effect on the digital economy, the impact of the legislation on costs for trust service providers and developments around revenue models and competition within the market.

2.2. Context

The current eIDAS regulation (EU 910/240), was adopted on 23 July 2014. A revised text of that regulation, together with an impact analysis, was published by the European Commission on June 3rd 2021¹. The ministries of the *Interior and Kingdom Relations* (BZK) and *Economic Affairs and Climate Policy* (EZK) are responsible for eIDAS within the Netherlands. Ministerial responsibility for trust services is prepared by the Directie Digitale Economie (part of the Ministry of EZK). The Directie follows the Strategie Digitale Economie. This strategy was presented by the Minister of Economic Affairs and Climate Policy to the House of Representatives (Tweede Kamer) on November 18th 2022².

This strategy aims at a resilient, entrepreneurial, innovative and sustainable digital economy, accessible to everyone in the Netherlands. It includes the eIDAS regulation as an element for "creating the right framework and conditions for well-functioning digital markets and services".

Following the publication of the new revision text of the eIDAS regulation, the process of negotiations between member states started. As part of this, the Dutch cabinet Rutte III published a fiche on July 9th 2021 containing its appreciation and views on the regulation³. The government has welcomed the European Commission's initiative and supports the ambition to strengthen the digital single market with this proposal for electronic identities and electronic trust services. On February 29th, the European Parliament adopted the provisional agreement of the eIDAS regulation^{4,5}.

The revision of the regulation introduces three new trust services: the issuance of electronic attestation of attributes to the *European Digital Identity Wallet* (EUDIW), the offering of electronic ledger services and the provision of electronic archiving services. In addition, there are minor changes with regard to the current trust services or their supervision. The introduction of the new trust services in particular is expected to bring major changes to the trust services ecosystem, due to its relationship with the European Digital Identity Wallet.

2.3. Goal

The overarching goal of this study is to provide an analysis regarding the changes resulting from the eIDAS revision in the trust services market. The Ministry of Economic Affairs and Climate Policy will use the analysis and potentially incorporate the insights into national legislation, policy development, and stakeholder communication. As part of the overarching goal, this research seeks to gather knowledge on the economic impact, both short- and long-term, for trust services due to the revision of eIDAS. The economic impact is considered by identifying the cost of additional regulatory burden, investment costs, the impact of competition and possible business models for the trust services market. Finally, this research aims to provide a qualitative description regarding the importance of trust services in the (digital) economy. The main question of this research is formulated as follows:

What is the economic impact within the Netherlands, both short- and long-term, of the proposed amendments to the eIDAS regulation on the various trust services?

¹ [EUR-Lex](#)

² [Rijksoverheid](#)

³ [Published fiche](#)

⁴ [European Parliament](#)

⁵ [eIDAS revision February 2024](#)

In addition to the main research question, the study focuses on seven sub-questions:

- 1** What does the expected use of trust services look like for both citizens (non-professional use) and businesses (professional use)?

- 2** What is the impact of changing demand for trust services on the digital economy?

- 3** What is the impact on the market for trust services? Is the eIDAS revision fuelling demand for trust services? What interest in the new trust services can be expected from market participants?

- 4** What investment costs need to be incurred by trust service providers to realise the potential of increased demand?

- 5** What are the regulatory costs (according to the methodology used by the State) for trust service providers to be compliant?

- 6** What impact on competition in the trust services market can be expected?

- 7** Which business models are permitted for the new trust services based on the revised text of the regulation and offer a sustainable future perspective?

2.4. Approach

The research was done in four iterations. The first iteration focused mainly on desk research and drafting hypotheses for each sub-question. In the second iteration, the hypotheses and drafted analysis were tested. In addition, the first substantive results were elaborated in this iteration. The third iteration involved detailed elaboration of the results and clarification of the results based on validation from the final interviews. The last iteration involved delivering the draft report to the supervisory committee on February 20th, 2024, and after the final feedback, the final report (in Dutch) was delivered on March 19th, 2024, to the client. The Dutch report has been translated to facilitate its distribution throughout Europe.

The analysis consists of three parts: impact analysis (sub-questions 1, 2 and 3), cost analysis (sub-questions 4 and 5) and competitor and business analysis (sub-questions 6 and 7). Information was gathered based on desk research and 19 interviews with various trust service providers and other relevant market players.

The progress and results of this research were validated by a steering committee consisting of representatives from the Ministry of Economic Affairs and Climate Policy, the Ministry of the Interior and Kingdom Relations and the Dutch Authority for Digital Infrastructure.

2.5. Reading guide

The following overview provides a brief explanation for each chapter:

Chapter 3 Conclusions & recommendations

Chapter 3 contains the conclusions and recommendations of this research.

Chapter 4 Context

Chapter 4 outlines the context of this research by explaining the eIDAS regulation. In addition, this chapter provides a description of the various trust services and relevant use cases.

Chapter 5 Impact analysis

Chapter 5 outlines the effects of the eIDAS revision on trust services. In it, the impact of the revision is mapped out for each trust service. Each service is provided with a forecast on market development.

Chapter 6 Cost analysis

Chapter 6 presents the impact of the eIDAS revision on costs for trust service providers. It distinguishes between regulatory compliance costs and market adaptation costs.

Chapter 7 Revenue model and competitor analysis

Chapter 7 focuses on the impact of the eIDAS revision on the revenue models for various trust services and the competitive developments within the various trust service markets.

2.6. Acknowledgements

This report was made possible with the help and expertise of trust service providers, organisations, and the steering committee. We would like to express our gratitude to all involved for their valuable insights and support.

Client and steering committee

Ministry of Economic Affairs and Climate Policy

Ministry of the Interior and Kingdom Relations

Dutch Authority for Digital Infrastructure

Research participants

Aangetekend B.V.

BSI Group

Cleverbase ID B.V. / Vidua

Dienst Uitvoering Onderwijs

Digidentity B.V.

Entrust EU SL

European Blockchain Services Infrastructure

Intesi Group S.p.A.

Kamer van Koophandel

KPN B.V.

Namirial S.p.A.

NotarisID

Open Preservation Foundation / Nationaal Archief

QuoVadis Trustlink BV (DigiCert+QuoVadis)

Signicat AS

SURF

The Bundesdruckerei Group

The Sovrin Foundation

Zivver

3. Conclusions & recommendations

The eIDAS revision has an impact on the trust services market. Our research reveals the following four key conclusions:



Overall usage of (qualified) trust services will increase: The use of most trust services in the Netherlands is expected to increase. The trend is that the Dutch market is moving from non-qualified services to qualified services. This is driven by stricter laws and regulations or requirements of involved parties.



Costs for QTSPs will rise due to higher regulatory burden: The eIDAS revision imposes several additional requirements on QTSPs, increasing the regulatory burden and, as a result, the costs associated with regulatory burden.



Competition among (Q)TSPs will increase in Europe: The eIDAS revision gives further recognition of a stronger legal framework to the trust services market. The eIDAS revision is expected to create a more open European trust services market.



A sufficient number of sustainable revenue models will emerge for (Q)TSPs: In addition to revenue models for new trust services, a new revenue model for qualified electronic signatures emerges. The new and existing revenue models may come under pressure from higher regulatory costs, however.

3.1. Overall usage of (qualified) trust services will increase

The use of most trust services in the Netherlands is expected to increase. The trend is that the Dutch market is moving from non-qualified services to qualified services. This is driven by stricter laws and regulations or requirements from stakeholders. It is important to note that the implementing acts of the eIDAS revision have not been published at the time of writing this report. As the implementing acts affect trust services, the precise impact on all trust services cannot be determined at this time.

3.1.1. Electronic signatures

The market for *Qualified Electronic Signatures* (QES) in the Netherlands is currently small. With the eIDAS revision, every citizen can have a free (non-professional) certificate for qualified signatures in the EUDIW. As a result, there is huge potential growth in qualified electronic signatures (remote) and it is likely to become the norm. Many advanced remote electronic signatures will move to remote QES with the introduction of the EUDIW. The adoption of the EUDIW in the Netherlands is an important prerequisite for fully exploiting the market potential of qualified electronic signatures (remote).

3.1.2. Electronic seals and website authentication certificates

The usage of *Qualified Electronic Seals* (QESeals) and (*Qualified*) *Website Authentication Certificates* ((Q)WACs) in the Netherlands is projected to expand. The use of these services partly depends on the possibility of their deployment in combination with EUDIW, namely through EUDIW data requests and in the sealing of (*Qualified*) *Electronic Attestations of Attributes* ((Q)EAAs). This is part of a larger trend, in which several European legislations (will) make the use of these services obligatory for data sharing, such as the *Payment Services Directive 2/3* (PSD2/PSD3), the *Payment Services Regulation* (PSR) and the framework for *financial data access* (FIDA)⁶, and by the growth of scalable data sharing in certain sectors.

The use of WACs is expected to increase further. This trend is separate from the eIDAS revision and mainly has to do with the expanding usability of these certificates. They are no longer used only for websites, but are also finding their way into other applications, such as IoT devices and e-mails.

3.1.3. Electronic time stamps

The current use of *qualified electronic time stamps* (QTimestamps), as a standalone service is limited in the Netherlands. There are no compelling reasons to foresee a shift in this trend. The eIDAS revision gives little grounds for a rise in demand - the requirements are almost identical to the requirements for this service from the original eIDAS regulation. Usage will only increase when national legislation requires QTimestamps to be mandatory for specific use cases.

⁶ [European Commission](#)

3.1.4. Electronic registered delivery services

The revision of eIDAS is not anticipated to directly affect the utilisation of *qualified electronic registered delivery services* (QERDS) in the Netherlands. An important driver for QERDS is mandatory use in local legislation or inclusion of the service on local 'Comply or Explain list'. Currently, this is not/barely happening in the Netherlands. The use of ERDS is likely to grow. This trend is separate from the eIDAS revision and is mainly driven by the increasing awareness in various industries of the importance and necessity of secure business communication.

3.1.5. Electronic attestations of attributes

Participants in this study predict a sizeable European market for (Q)EAAs because of the introduction of the EUDIW. This forecast relies on the numerous online and offline applications that will be enabled using (Q)EAAs and the EUDIW. The adoption of the EUDIW in the Netherlands is an important prerequisite for fully exploiting the market potential of electronic attestation of attributes. For the utilization of (Q)EAAs, it is essential to have clear understanding of the roles and expectations of authentic sources, along with common standards and (semantic) interoperability.

3.1.6. Electronic archiving services

There is a minor chance that (*qualified*) *electronic archiving services* ((Q)E-Archiving) will be widely used as a standalone service. Some of the interviewees expect that (Q)E-Archiving will be used mainly in combination with other trust services (e.g. together with QES services). Since the added value to organizations is perceived to be minimal, it is expected that this qualified service will see restricted growth.

3.1.7. Electronic ledgers

It is expected that, in the short term, the use of *qualified electronic ledgers* (QELedgers) in the Netherlands will be low and there will be a very small number of providers. The lack of clarity for potential providers, both in terms of technical interpretation and legal frameworks, of this service inhibits the emergence of a new market for this trust service. For providers of QELedgers, obtaining the qualified status may increase trust in the market, which may be desirable in this sector.

3.2. Costs for (Q)TSPs will rise due to higher regulatory burden

The eIDAS revision imposes several additional requirements on QTSPs, increasing the regulatory burden and, as a result, the costs of compliance. This is likely to have more impact for small parties than for large parties. In addition, existing QTSPs can start offering the new services more easily than new entrants. The obligation to make services available and accessible for people with disabilities further increases the regulatory burden. However, QTSPs themselves indicate that they do not expect high additional costs from the Accessibility Act. QTSPs also have to meet requirements of other norms and standards (e.g. NIS2, CA/Browser Forum) for specific trust services. Specifically for remote electronic signatures, mandatory SAM certification results in additional costs for service providers.

There is a risk of delays in the qualification process that will prevent service providers from being certified in time. The concurrent coming into force of the eIDAS revision, the implementing acts, and the accreditation of auditors, coupled with a limited number of auditors and labor market tightness, is partly responsible for this situation. The delays may lead to higher costs as they prolong implementation and operational processes.

The eIDAS revision requires that the identity of the person to whom the qualified trust service (for QEAs, QWACs, QES, and QESeals) is provided and their attributes must be verified with *level of assurance* (LoA) high. QTSPs that do not currently meet this requirement will have to make efforts and costs to comply. Over time, with a sufficient number of users, the EUDIW could enable support for remote identification, potentially reducing the identification costs for QTSPs.

Market adaptation costs are expected to have little negative impact on market players. Under current conditions, an increase in demand will not immediately lead to additional disproportionate costs or large necessary investments. Most services are scalable and will cope well with growing demand. Furthermore, the increase in costs is related to an increase in revenue, which self-evidently decreases its potential negative effect.

3.3. Competition among (Q)TSPs will increase in Europe

The eIDAS revision gives further recognition of a stronger legal framework to the trust services market. The eIDAS revision is expected to create a more open European market for trust services. There will be increasing competition in the market, partly because service providers from Europe will increasingly operate in the Dutch market. This will also give Dutch parties more opportunities in foreign markets.

The trust services market is a (strongly) compliance- and cost-driven market where diversification in product and thus distinctiveness is limited. In addition, the EUDIW limits part of the distinguishing capacity (for example for electronic signatures). Both encourage market concentration. Larger trust service providers have an advantage because they can more easily bear the (high) compliance costs and can also offer a more competitive price due to economies of scale. Labour costs also differ from country to country. These factors have already shaped the current European playing field and resulted in a competitive advantage for some of the larger trust service providers.

Specifically, for qualified electronic signatures, a different market dynamic arises as it is obvious that the government will carry out a procurement process and select one or more trust service providers that provide qualified electronic signatures for the EUDIW.

For a level playing field, however, it is important that supervision is harmonised between different national regulators and supervisory bodies. Interviewees expressed a strong need for as little ambiguity or differences in interpretation as possible. In addition, interviewees indicated that harmonisation is also important within a member state. If eIDAS supervision and NIS2 supervision lie with different supervisory bodies, the costs for QTSPs increase. In the Netherlands, it is therefore desirable that the *Dutch Authority for Digital Infrastructure (RDI)* also takes on the role of supervisor for NIS2 supervision.

3.4. A sufficient number of sustainable revenue models will emerge for (Q)TSPs

Regarding (Q)Timestamps and (Q)ERDS, the eIDAS revision does not significantly affect revenue models. On the other hand, (Q)ESeals and (Q)WACs could see the emergence of new revenue streams through the EUDIW, potentially enhancing the sustainability of existing business models. Nonetheless, these business models might face pressure from increased regulatory costs.

New revenue models are emerging for electronic signatures because of the eIDAS revision. The current revenue model for the advanced signature process (for citizens/non-professional use) will largely disappear. An alternative revenue stream will arise from providing electronic signature certificates for citizens via the EUDIW. A tender process for these certificates for non-professional use will probably be needed from the government. A collateral benefit is that citizens will gain greater familiarity with electronic signatures, which is anticipated to also boost their use in professional contexts.

There are two types of revenue models in the case of electronic attestation of attributes: 1) revenue models for trust service providers and 2) cost/revenue models for authentic sources. The most apparent revenue model for trust service providers involves collecting a monthly or yearly fee from authentic sources for access to the trust services. Alternatively, a revenue model could consist of a partnership where both the trust service provider and the authentic source share the generated revenue. A third option is an agreement between a trust service provider and authentic source on the right to resell the authentic source's data. For authentic sources, there are three cost/earnings models: 1) The holder/citizen pays; 2) The relying party pays and 3) The authentic source pays. The most obvious model varies for each attestation/use case.

3.5. Recommendations

The Ministry of Economic Affairs and Climate Policy plays a vital role in realising the opportunities that the eIDAS revision offers for the Netherlands and its digital economy. Trust services deliver an important contribution to the future of the Dutch digital economy, but success is dependent on policy. An active role of the Ministry of Economic Affairs and Climate is desirable. This is endorsed by Dutch trust service providers.

Formulate more policy on trust services and provide more direction and vision to the market

To maximize the benefits of trust services for the digital economy, there is a need for more comprehensive policies, guidance, and vision from the Dutch government. Such policies could provide solutions and clarify existing uncertainties surrounding the eIDAS revision. Examples include:

- Method used for issuing certificates for qualified signatures for citizens, including advantages & disadvantages
- Providing clarity about 'professional use' for qualified electronic signatures
- Frameworks for issuance and (semantic) interoperability of public and private (Q)EAAs

In addition, the market is looking for clarification on implementing acts, information on the affiliation of regulators in Europe to reduce the risk of different local interpretations and, finally, clarity on the coherence between different legislation, standards, norms and frameworks (e.g. NIS2, eIDAS, Wdo, Wet Diaz, ETSI, ISO, Nen).

Policy, direction, and vision can assist trust service providers and other stakeholders in defining their strategy for offering trust services. Moreover, they require clear rules of the game so that they can act accordingly. This also applies to potential authentic sources for (Q)EAAs and schema providers. Uncertainty can slow down or even hinder usage. An active role and contribution from the Ministry of Economic Affairs and Climate Policy in detailing the implementing acts and communication about them can contribute to clarity for the Dutch market.

Contribute actively to filling preconditions for success of the EUDIW

The EUDIW is closely linked with electronic signatures, seals, and electronic attestations of attributes. Furthermore, QESeals and QWACs might be essential for effective interactions with EUDIWs. This implies that the government's involvement with the EUDIW is inseparable from its role in ensuring the efficient functioning of the trust services market. Furthermore, clear understanding of the EUDIWs functionality for natural persons and legal persons through the *Organisational Digital Identity Wallet* (ODIW), its cost/revenue model, legal liabilities, norms and standards, and the interoperability of (Q)EAAs are critical prerequisites for the success of the EUDIW. A consultation structure in which all relevant parties are involved and jointly contribute to filling the preconditions for the success of EUDIW helps the two-sidedness of this market. The Ministry of Economic Affairs and Climate Policy can play a key role in convening the relevant stakeholders and providing centralised guidance. Moreover, strategic coordination within the government, such as among the different ministries, is essential.

Invest in better communication about trust services

In the short term, improving communication about the usefulness, necessity and possible applications of trust services helps to optimise their use. Both the public and private sectors in the Netherlands have not adequately acknowledged or grasped the importance and necessity of trust services yet. Many stakeholders lack knowledge about the existence of these trust services. Therefore, it is desirable to communicate about the existence and benefits of trust services. The government could utilise initiatives like the Trusted Information Partners (TIP) for this purpose, for instance.

4. Context

4.1. eIDAS

The *electronic IDentification, Authentication and trust Services* (eIDAS) regulation is the European legal regulation on electronic identification and trust services in respect of electronic transactions. The aim of this regulation is to increase digital trust in the internal market and provide a common regulatory framework. The eIDAS regulation entered into force on 1 July 2016 under the official name Regulation (EU) No 910/2014⁷. Now the European Commission is seeking revision of this regulation through the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) no 910/2014 as regards establishing a framework for a European Digital Identity⁸. This research is based on the 10 November 2023 version of that document, which is based on the outcome of the dialogues on the proposal for the revision of the eIDAS regulation.

4.1.1. eIDAS

The original eIDAS regulation contains two parts: *electronic identification* (eID) and the *Trust Services* (TS).

The eID refers to the online identification and authentication of natural and legal persons. Before eIDAS, each member state could already provide one or more eIDs for its citizens and businesses, but since this regulation, there is the possibility to register such eIDs for mutual cross-border recognition of authentication. This means that eIDs from one member state, are also (partially) usable in other member states. In short, eIDAS is the start for cross-border use of eIDs.

The Dutch eID falls under the policy responsibility of the *Ministry of the Interior and Kingdom Relations* (BZK). The Netherlands has opted for a public tool for citizens (DigiD), and the tools for businesses and legal entities provided in public-private partnership: the eHerkenning-stelsel⁹.

eIDAS contains five trust services. The eIDAS legal text defines trust services as electronic services that contribute to trust in a digital environment. Sections 4 to 8 of eIDAS explain the five trust services (see **Figure 1**). Trust services are the policy responsibility of the *Ministry of Economic Affairs and Climate Policy* (EZK). The ministry has appointed the *Dutch Authority for Digital Infrastructure* (RDI) as supervisor of trust services. Trust services in the Netherlands are housed in the telecommunicatiewet¹⁰.

Figure 1: eIDAS has five trust services.



Electronic signatures



Electronic seals



Electronic time stamps



Electronic registered delivery services



Website authentication

⁷ [eIDAS](#)

⁸ [The eIDAS revision](#)

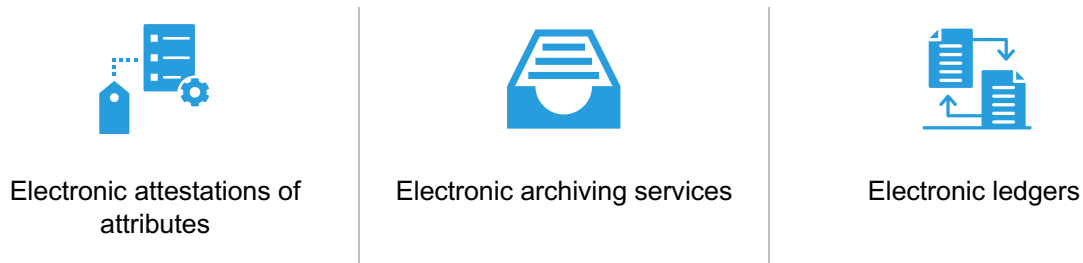
⁹ After the introduction of the Stelsel Toegang, a citizen or company will be able to use other recognised login methods, in addition to DigiD or eHerkenning, if assessed against Digital Government Act (Wdo) requirements to log in to various governmental service providers.

¹⁰ [Overheid](#)

4.1.2. The eIDAS revision

The eIDAS revision introduces three new trust services (see **Figure 2**). Sections 9 to 11 of the eIDAS revision explain the new trust services.

Figure 2: The eIDAS revision introduces three new trust services.



In addition, the eIDAS revision introduces the concept of the *European Digital Identity Wallet* (EUDIW). An EUDIW¹¹ helps EU citizens and businesses identify or authenticate themselves, share certain information and sign electronically. EUDIW falls under the policy responsibility of the Ministry of the Interior and Kingdom Relations. The dividing line between the two Dutch ministries becomes less explicit as certain trust services (e.g. electronic signatures and electronic attestation of attributes) are also used in relation to EUDIWs. In this report, the choice has been made to categorise the services introduced as new in the revision around remote signatures and seals under the Trust Services 'Electronic Signatures' and 'Electronic Seals', respectively.

4.2. Types of trust services

The trust services described in eIDAS can be divided into eight categories, each containing a number of sub services (see **Figure 3**)¹².

Figure 3: The eIDAS revision has 8 trust services with multiple sub services.

Trust services	Sub services
Electronic signatures	<ol style="list-style-type: none"> 1. Creation of electronic signatures and/or issuing of certificates for electronic signatures 2. Validation of electronic signatures and/or certificates for electronic signatures 3. Preservation of electronic signatures and/or certificates for electronic signatures 4. The management of remote electronic signature creation devices¹³
Electronic seals	<ol style="list-style-type: none"> 1. Creation of electronic seals and/or issuing of certificates for electronic seals 2. Validation of electronic seals and/or certificates for electronic seals 3. Preservation of electronic seals and/or certificates for electronic seals 4. The management of remote electronic seal creation devices
Electronic time stamps	<ol style="list-style-type: none"> 1. Creation of electronic time stamps 2. Validation of electronic time stamps
Electronic registered delivery services	<ol style="list-style-type: none"> 1. Provision of electronic registered delivery services 2. Validation of data transmitted through electronic registered delivery services and related evidence
Website authentication	<ol style="list-style-type: none"> 1. Issuing of certificates for website authentication 2. Validation van certificates for website authentication

¹¹ Each country can have one or more EUDIWs for its citizens and one or more EUDIWs for its businesses

¹² The 8 trust services are based on the 8 sections in the eIDAS legal text

¹³ The management of remote electronic signature creation devices is a new service under eIDAS

Electronic attestation of attributes	<ol style="list-style-type: none"> 1. Issuing of electronic attestation of attributes 2. Validation of electronic attestation of attributes
Electronic archiving services	<ol style="list-style-type: none"> 1. Electronic archiving of electronic data and electronic documents
Electronic ledgers	<ol style="list-style-type: none"> 1. Recording of electronic data in an electronic ledger

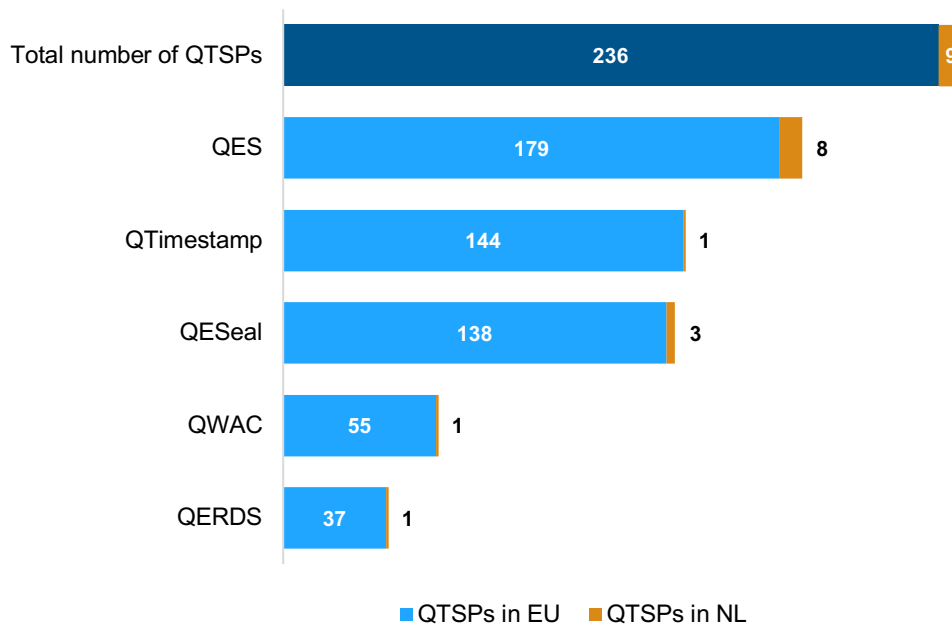
Existing eIDAS trust services
New eIDAS trust services

Each service has a qualified and a non-qualified variant. Qualified trust services meet additional requirements leading to a higher level of reliability and legal certainty. This results in a shift in the burden of proof: with a qualified service, the burden of proof reverses. In the example of a qualified signature, the signatory must prove that he or she did not sign. This is in contrast to non-qualified signatures, where it is the claimant's responsibility to prove that the signature was actually made by the signatory.

Trust services are offered by parties known as *Trust Service Providers* (TSPs). When these parties successfully demonstrate compliance with the requirements of eIDAS through an evaluation by an independent auditor, TSPs can apply to the national supervisory body for *Qualified Trust Service Provider* (QTSP) status.

The European Commission publishes an up-to-date list of registered QTSPs within the European Union for all trust services categorised under eIDAS¹⁴. There are more than 230 trust service providers in Europe (see **Figure 4**)¹⁵. Together, these trust service providers offer more than 700 trust services. Thus, most providers offer several trust services.















Figure 4: Europe has more than 230 trust service providers under eIDAS.




It is important to note that non-qualified TSPs do not have a registration requirement. In several countries, such as the Netherlands, there is also no possibility for registration. In addition, the added value for registration is limited. Some examples of non-registered TSPs include parties such as Zivver, Rpost, Bitdefender, Cloudflare and Google. There are currently nine QTSPs operating in the Netherlands, providing 14 qualified trust services (see **Figure 5**).

¹⁴ [Dashboard European Commission](#)
¹⁵ [eIDAS Dashboard](#) on 01/11/2023

Figure 5: There is at least 1 QTSP for every qualified trust service in the Netherlands.

	QES	QESeal	QTimestamp	QERDS	QWAC
Aangetekend B.V.					
CIBG					
Vidua / Cleverbase ID B.V.					
Digidentity B.V.					
KPN B.V.					
Ministerie van Defensie					
Ministerie van I&W					
NotarisID B.V.					
QuaVadis Trustlink B.V.					

 = offers the qualified trust service

The following sections explain the five existing and three new trust services in more detail and present the main use cases for each service.

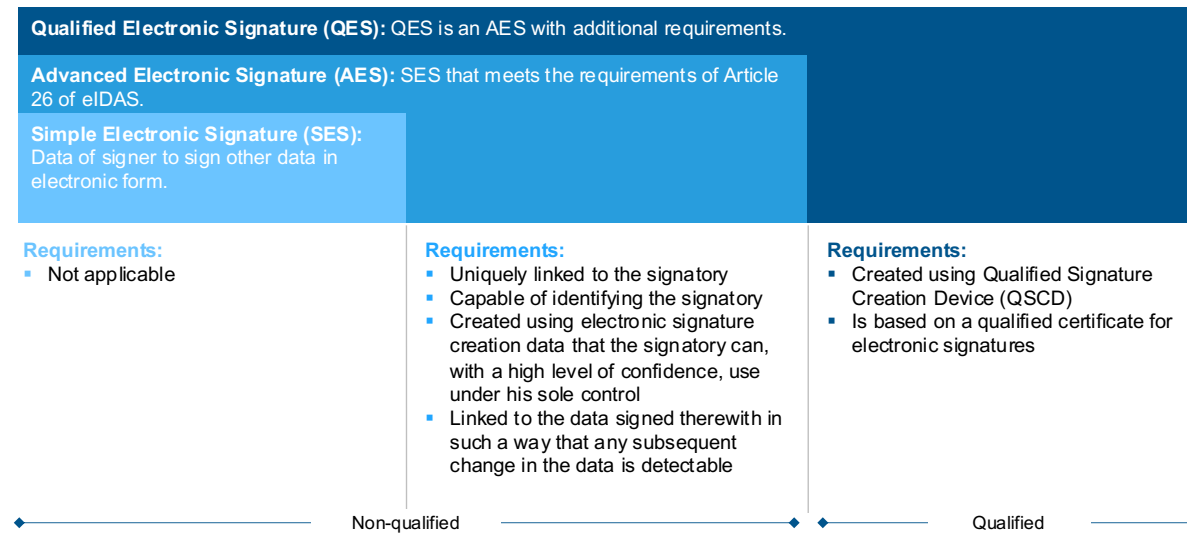
4.2.1. Electronic signatures

An *electronic signature* (eSig) is a digital expression of will by a person agreeing to the content of a document or dataset to which the signature is related¹⁶. It is, on the one hand, the electronic counterpart of the legalised signature and thus a legal binding that obliges the signatory to honour a stipulated agreement of the signed document¹⁷. The eSig can also be used as a means of endorsing the authenticity and integrity of a document. There are three forms of electronic signatures with increasing levels of reliability, namely the *simple electronic signature* (SES), *advanced electronic signature* (AES) and the *qualified electronic signature* (QES). This increasing level of trust is obtained by imposing additional requirements on the signature in each case (see **Figure 6**).

¹⁶See Electronic signatures 1-pager

¹⁷ [European Commission](#)

Figure 6: A QES is an AES with additional requirements where the burden of proof is on the signatory.



QES involves three individual sub-services, namely the creation, validation and preservation of QES. Moreover, a *Qualified Signature Creation Device* (QSCD) needs to be managed that is required for creating QES. The QES refers to the digital signature and the qualified certificate for the QES is the binding agent between this digital signature data and the identity of the signer. The certificate is thus an electronic attestation that links validation data for an electronic signature to a natural person and confirms at least the name or pseudonym of that person. This certificate is labelled qualified when it is issued by a QTSP and meets the eIDAS requirements from ANNEX I¹⁸. **Figure 7** contains an overview of the main use cases for (Q)ES.

Figure 7: Two use cases are common in (Q)ES.

Use case	Description	Example user story	Examples of use
Guaranteeing integrity and originality	The unilateral signing of files by one party/person for the purpose of guaranteeing integrity and originality.	I want to provide sensitive digital information with an integrity and originality guarantee so that the entities I share that information with can act on it.	<ul style="list-style-type: none"> Signing medical documents such as a prescription, referral, or medical statement. Signing (annual) reports or records.
Making (legally binding) agreements	The bilateral signing of files by two parties.	A party and I want to sign a digital contract to record our agreement and legally frame it.	<ul style="list-style-type: none"> Signing notarial deeds and powers of attorney. Signing mortgages or insurance policies. Signing a supply contract, confidentiality agreement or employment contract.

4.2.2. Electronic seals

The *electronic seal* (eSeal) is the digital equivalent of a physical company seal and is set by a legal entity. This digital proof attaches itself to other digital data, for example company contracts or documents, to ensure its originality and integrity¹⁹. In this way, the eSeal serves as proof that such documents have been issued by the relevant legal entity.

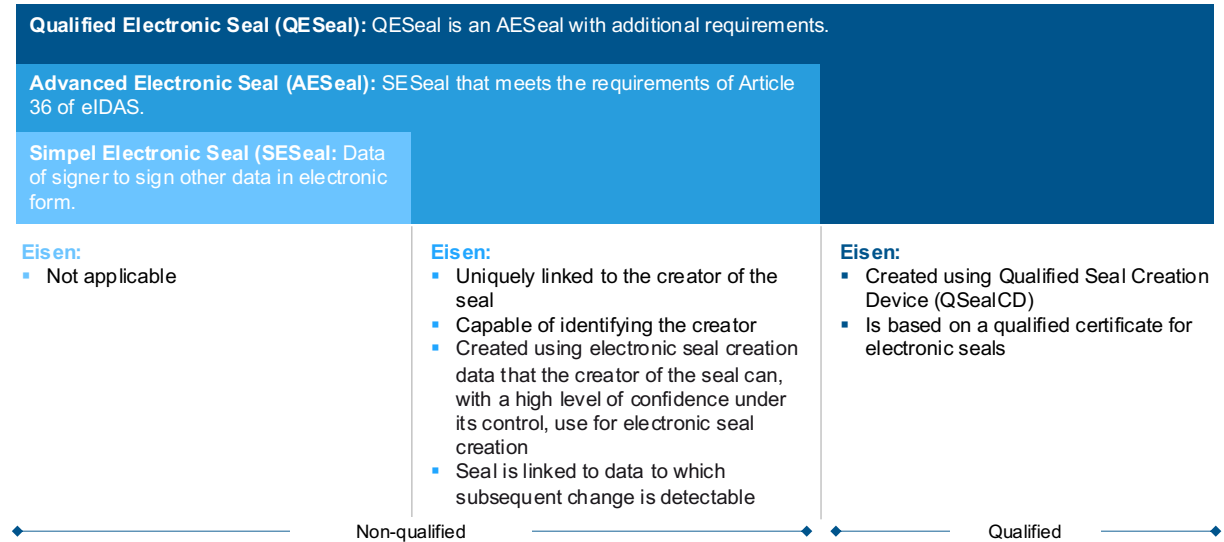
As with the eSig, the eSeal has three forms with increasing levels of trust: the *Simple Electronic Seal* (SESeal), *Advanced Electronic Seal* (AESeal) and *Qualified Electronic Seal* (QESeal) (see **Figure 8**).

¹⁸ [eIDAS ANNEX 1](#)

¹⁹ See (Q)ESeal 1-pager

Generating a QESeal involves four sub-services. These are the services of creation, validation and preservation of both the QESeal and the certificate for the QESeal. Furthermore, a *Qualified Seal Creation Device* (QSealCD) needs to be managed for remote QESeal creation.

Figure 8: An eSeal has three forms with increasing trust levels.



A qualified certificate for QESeals acts as an electronic attestation, linking a legal entity to the validation data of its QESeal and confirming the name of the entity. This certificate is qualified when it is issued by a QTSP and complies with the eIDAS requirements in ANNEX III²⁰.

(Q)Eseals are mostly used for documents, data or transactions with major legal consequences or risks. **Figure 9** contains an overview of the main use cases for (Q)Eseals.

Figure 9: (Q)ESeals are mainly used to ensure the integrity of documents.

Use case	Description	Example user story	Examples of use
Sealing	The sealing of files by legal entities using (Q)Eseal to guarantee their integrity and originality.	I want to digitally seal contracts so that I no longer need a wet seal or signature and can make processes more efficient.	
Requesting / supplying attestations	A relying party uses a QESeal at an EUDIW to prove that the data request was made by the specific relying party.	I want it to be provable later that a relying party requested my data.	
Sealing Machine-2-Machine interaction	Sealing files by two parties.	I want to be able to securely share confidential information.	

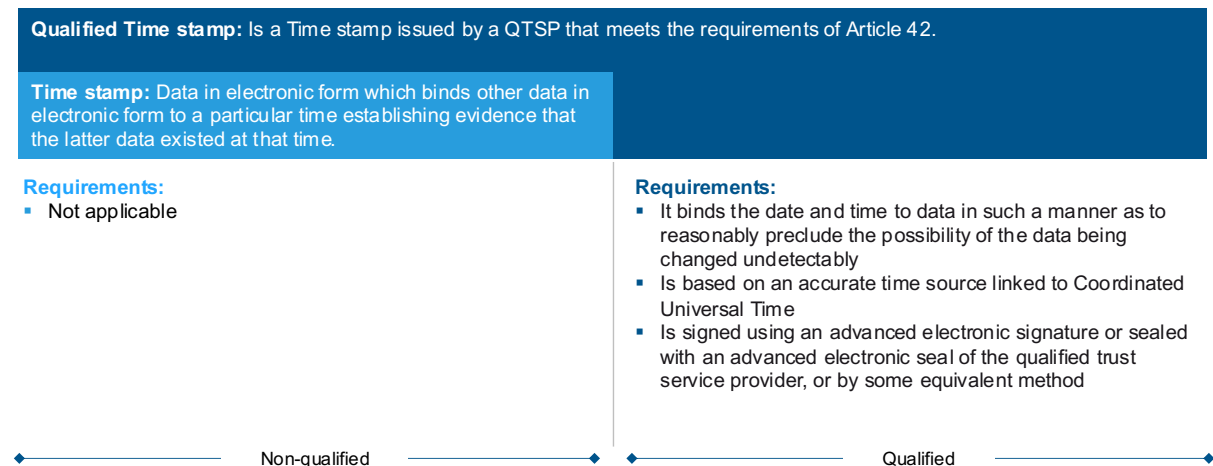
²⁰ [eIDAS ANNEX III](#)

4.2.3. Electronic time stamp

A *qualified electronic Time stamp* (QTimestamp) is a digital proof that links data to a time stamp. It thus demonstrates the existence of data at a specific date and time²¹. This makes it possible to determine when the content was modified or accessed.

The physical equivalent of the time stamp is a stamp that contains information about the time and date when the document was generated. The time stamp involves three sub-services: creation, validation and preservation of the time stamp. Hereby, such services are labelled *qualified electronic time stamp* (QTimestamp) when the time stamp complies with Article 42 of the eIDAS revision²² (see **Figure 10**).

Figure 10: A QTimestamp is a time stamp with additional requirements.



An electronic time stamp can be used in multiple areas²³. **Figure 11** contains an overview of the main use cases for (Q)Timestamps.

Figure 11: (Q)Timestamps are used to conclusively record the correct date and time.

Use case	Description	Example user story	Examples of use
Recording time of an event	Recording the correct time and date an event took place.	I want to be sure that a file was sent at a certain time so that I can check that I am acting in compliance with the requirements.	<ul style="list-style-type: none"> Recording transactions in the financial sector. Logging a patent application, the version of a document, database or software code. Guaranteeing the time when a (Q)ESig has been set.

4.2.4. Electronic registered delivery services

An *Electronic Registered Delivery Service* (ERDS)²⁴ facilitates the digital exchange of data. ERDS ensures secure transfer of data by protecting it from, for example, theft, unauthorised modification or destruction²⁵. (Q)ERDS is similar to registered mail with a postal company's guarantee to deliver mail securely and that unauthorised persons will not know about its contents.

²¹ See (Q)Timestamp 1-pager

²² [eIDAS Article 42](#)

²³ [Datasure about areas of usage for electronic time stamps](#)

²⁴ See (Q)ERDS 1-pager

²⁵ [Doxee about eIDAS](#)

There are two sub-services within this category, namely the provision of ERDS as an end-to-end service and the validation of the data sent via ERDS. The eIDAS revision describes standards and characteristics for this service. QTSPs that offer *Qualified Electronic Registered Delivery Services* (QERDS) receive this label when they meet the requirements from Article 44²⁶ (see [Figure 12](#)).

Figure 12: QERDS is ERDS with additional requirements to ensure secure electronic transfer.

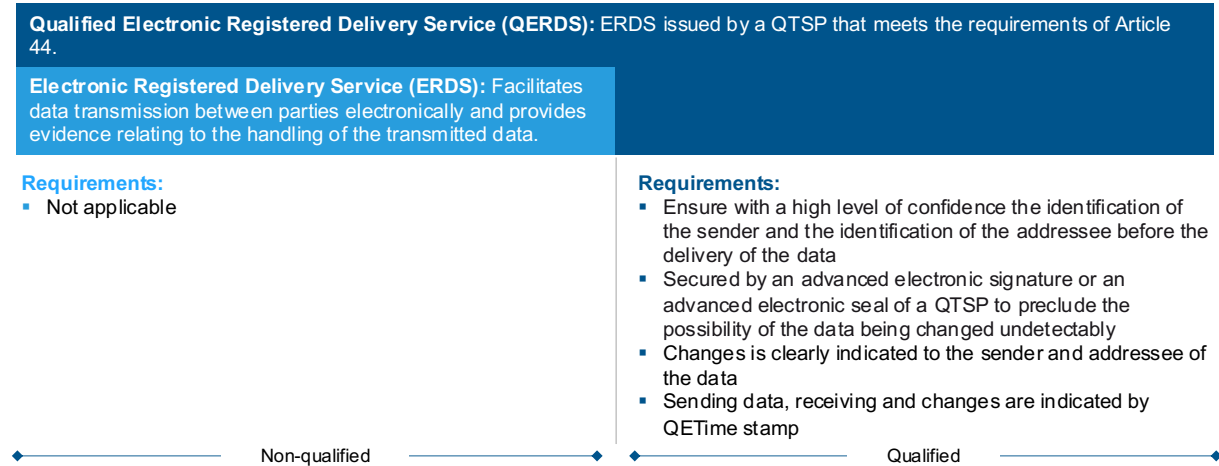


Figure 13 contains an overview of the main use cases for (Q)ERDS.

Figure 13: (Q)ERDS are services that deliver documents via push or pull.

Use case	Description	Example user story	Examples of use
Document or data delivery (push)	Secure and provable electronic delivery of documents or data to the right person via e-mail.	I want to have confidence that my legal documents can be sent securely and correctly and end up with the right person.	<ul style="list-style-type: none"> ▪ Sending data, aimed at a human recipient, contract documents, invoices, diagnoses, intellectual property etc. ▪ Sending data, aimed at automatic processing between machines, such as shipment notes, production data, energy consumption or maintenance data.
Document or data delivery (pull)	The secure and provable electronic delivery of documents or data to the right person in a portal.	I want to have confidence that my legal documents are delivered safely and correctly to a person, so I put them in a portal and send the recipient a notification where they can pick up the documents.	<ul style="list-style-type: none"> ▪ The government sends a citizen a notification that a message is ready in his or her personal inbox.

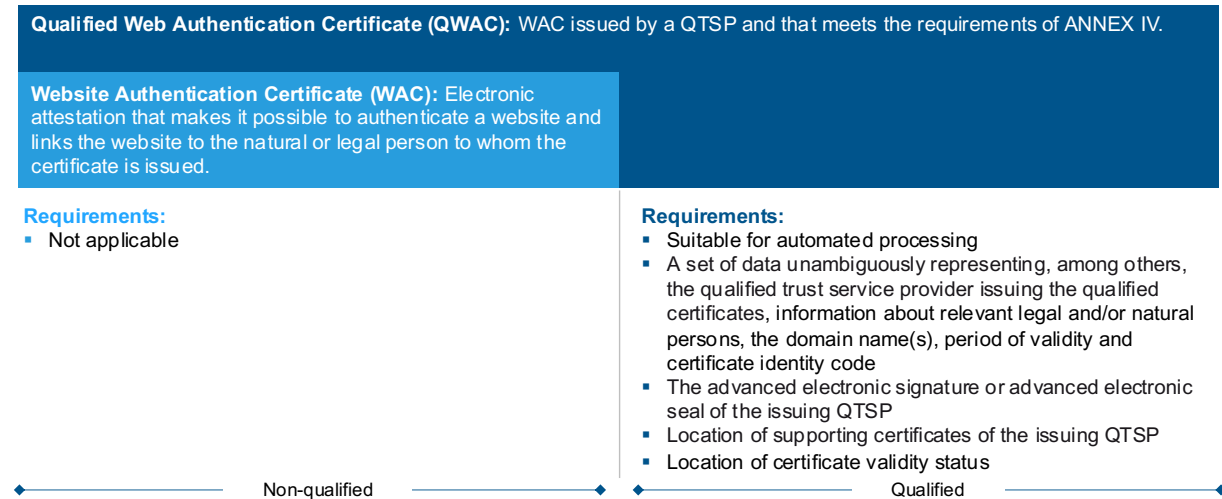
4.2.5. Website authentication

A *Website Authentication Certificate* (WAC) refers to the electronic proof (certificate) for website authentication. These types of certificates ensure the link between a natural or legal person and a

²⁶ [eIDAS revision Article 44](#)

website²⁷. There are two types of sub-services involved in a WAC, namely the creation and validation of the certificate. When a WAC is issued by a QTSP and meets the requirements of ANNEX IV²⁸, it is considered a qualified certificate for website authentication, or a QWAC (see **Figure 14**).

Figure 14: A QWAC is a WAC with additional authentication requirements.



A QWAC is comparable to a quality mark at a grocery store. Consumers know that the quality mark is only issued by authorised bodies that follow meticulous procedures to inspect the grocery store. This allows customers to assume that the store is authentic and can therefore be trusted to provide, for example, only organic or local produce. The existence of a QWAC on a website enables users to trust the identity of the entity operating the website and ensures that communication with it (the service/connection) is secure. A (Q)WAC thereby seeks to establish trust in digital context. It is technically equivalent to other website certificates, such as a Domain Validation (DV) certificate, Organisation Validation (OV) certificate or an Extended Validation (EV) certificate. However, the certificates differ in their issuance process. Each certificate has its own level of authentication, with a DV certificate being the lowest level and an EV certificate or QWAC being the highest level. **Figure 15** provides an overview of the main use cases for (Q)WACs.

Figure 15: A (Q)WAC is used for website authentication and M2M authentication.

Use case	Description	Example user story	Examples of use
Website authentication	Certificates for website authentication allow EU citizens to trust that the website they are visiting is legitimate.	I want to be sure I am on my bank's real website so I can safely transfer money.	<ul style="list-style-type: none"> Internet banking. Shopping online. Filing tax returns. Viewing personal documents.
Mutual Machine-2-Machine authentication	Mutual authentication between service providers to establish a secure connection.	I want to be sure I receive the right data so I make the right decisions based on correct data.	<ul style="list-style-type: none"> Automated (machine-to-machine) processes, such as delivering data from business processes or sensors. Mutual authentication between service providers (as is common in PSD2 between banks and service providers). Authentication of service providers with specific roles in

²⁷ [European Parliament](#)
²⁸ [eIDAS ANNEX IV](#)

non-regulated data sharing schemes.

4.2.6. Electronic attestation of attributes

An electronic attestation of attributes (EAA) refers to a digital proof that provides information about various attributes, such as age, gender or personal qualifications such as memberships, insurance details, a diploma or driving licence²⁹. EAAs can be divided into two different sub-services: issuing and validating EAAs. A digital attestation is a digital equivalent of a physical attestation such as a diploma or driving licence. The issuing authority issues a qualification to the entity to which the document applies and endorses it with a physical signature or company seal. In addition to this, both a natural person and a legal entity can also attribute self-declared attestations, for example your own shoe size or the number of employees in your company.

The EAA consists of two forms with increasing levels of trust: electronic attestation of attributes (EAA) and the qualified electronic attestation of attributes (QEAA). The qualified service is provided by a QTSP in conformity with the requirements established in ANNEX V of the eIDAS revision³⁰ (see **Figure 16**). On top of this, public entities themselves may issue EAAs to the EUDIW (so-called Public EAAs). These public entities must meet the same requirements as QTSPs for QEAA.

Figure 16: A QEAA is an EAA with additional requirements and based on an authentic source.

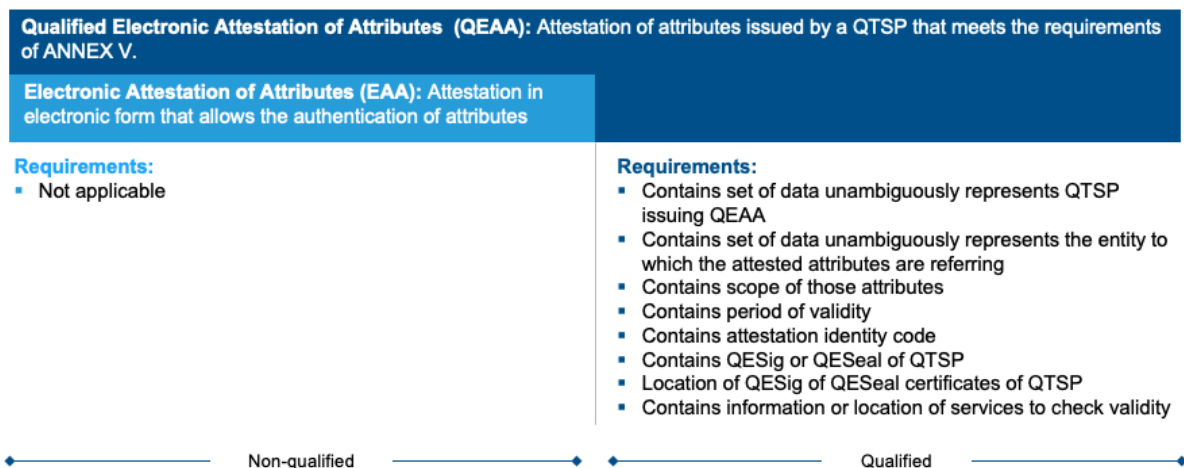


Figure 17 outlines the main use cases for (Q)EAA:

Figure 17: A (Q)EAA has a diverse number of use cases.

Use case	Description	Example user story	Examples of use
Online: Digital registration	Enrolling digitally based on verified attributes.	I want to register quickly and easily with a government agency or commercial service provider.	<ul style="list-style-type: none"> ▪ Registering in a municipality. ▪ Applying for a bank account. ▪ Registering as a customer with a retailer.
Online: Digital data sharing	Sharing digitally validated attributes with external parties.	I want to supply the necessary	<ul style="list-style-type: none"> ▪ Supplying driving licence details for a rental car.

²⁹ See (Q)EAA 1-pager

³⁰ [eIDAS Revision ANNEX V](#)

		information for a service or product.	<ul style="list-style-type: none"> ▪ Supplying a diploma for a job. ▪ Sharing passport details for airline tickets. ▪ Demonstrate membership for discounts at hospitality/shops/websites. ▪ Sharing insurance details for booking a trip.
Offline: physically access a location	Granting access based on verified attributes.	I want access to certain locations and prove it with (Q)EAAs.	<ul style="list-style-type: none"> ▪ Access to hotel rooms ▪ Gaining access to concert or theatre performances. ▪ Gaining access to office spaces.
Hybrid: Sales authorisation	To legitimise the purchase of products or services using verified attributes.	I want to buy something that requires me to meet certain conditions and I prove it with (Q)EAAs.	<ul style="list-style-type: none"> ▪ Buying alcohol (online or in a shop). ▪ The right to personalised offers. ▪ 65+ discount in public transport, museums or other attractions.

4.2.7. Electronic archiving services

The digital counterpart of the physical archive is the *electronic archiving service* (e-Archiving). This service focuses on ensuring the longevity, readability, integrity, and originality of digital data for a, usually, extensive period of time³¹. E-Archiving has one service: archiving electronic data. The eIDAS regulation covers the archiving of electronic documents and data but does not address the process of converting physical documents to true digital copies.

Qualified e-Archiving (QE-Archiving) complies with Article 45i and Article 45j of the eIDAS revision³² (see **Figure 18**).

Figure 18: QE-Archiving is e-Archiving with additional requirements to ensure preservation over long periods of time.

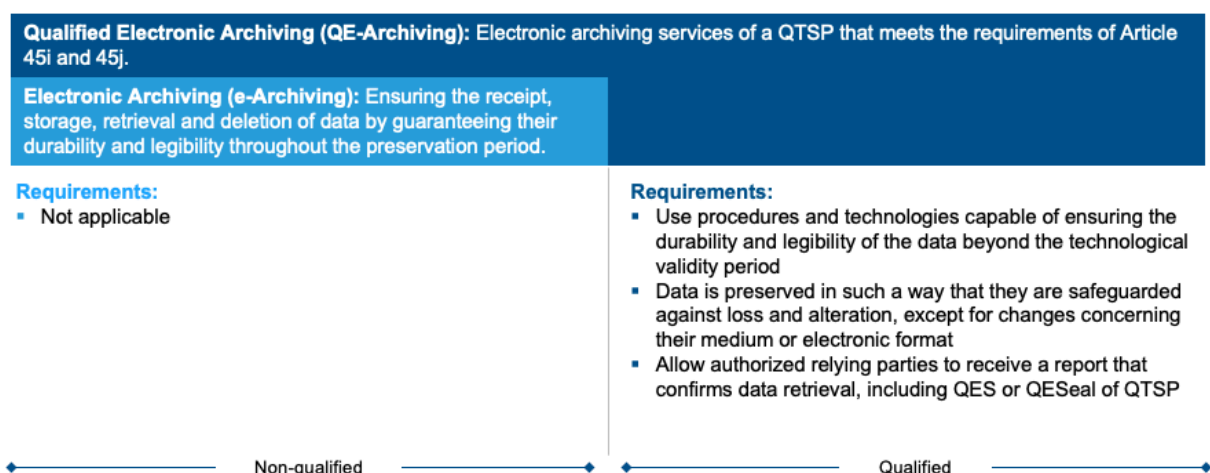


Figure 19 presents an overview of the main use cases for (Q)E-Archiving.

³¹ See (Q)E-Archiving 1-pager

³² [eIDAS revision article 45i and 45j](#)

Figure 19: The main use case of (Q)E-Archiving is to ensure integrity over time.

Use case	Description	Example user story	Examples of use
Ensure integrity of documents	Ensuring the immutability of documents and associated (Q)ESigs and (Q)ESeals over time.	I want assurance that digital files and their seals retain their integrity and legal validity over a long period of time.	<ul style="list-style-type: none"> Recovering the right data in the desired state, e.g. in a corporate or government context. Registering environmental permit, building permit, parking permit, etc. Storing data in accordance with compliance.

4.2.8. Electronic ledgers

Electronic ledgers (eLedgers) are tamper-proof digital records of data in a manner that ensures its authenticity and integrity in terms of date, time and chronological order³³. This category contains no other services apart from the previously stated secure storage of data. ELedgers are the digital equivalent of physical records, such as handwritten corporate financial records. The eLedger definition is intentionally worded in a technology-neutral way, so it includes both *distributed ledger technology* (DLT), mainly blockchain, and the non-distributed variants such as digital double-entry accounting systems used by banks.

By implementing the requirements of the eIDAS revision³⁴, eLedgers obtain the label: qualified or QELedger (see **Figure 20**).

Figure 20: QELedger is an eLedger with additional requirements that increase control over the network.

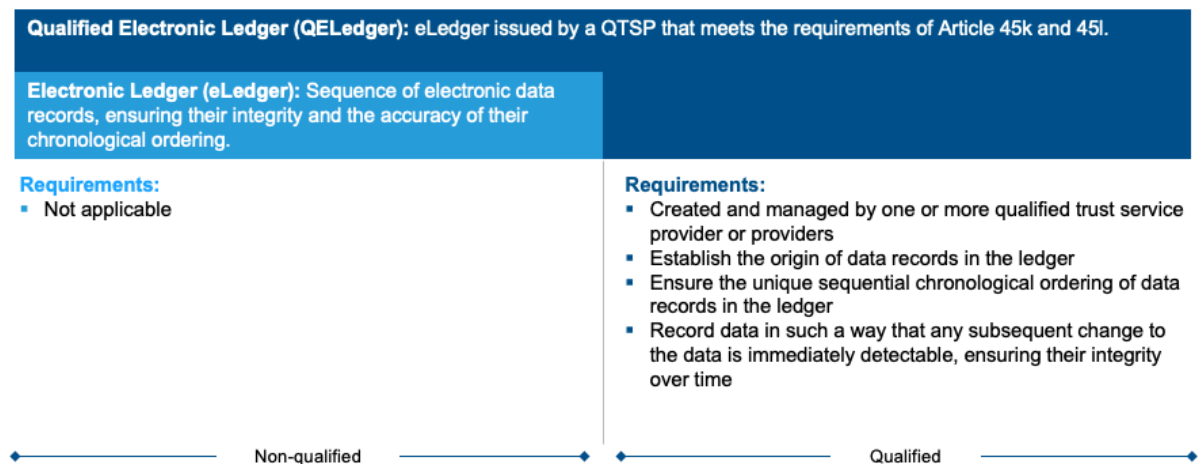


Figure 21 lists the primary use cases for (Q)ELedgers.

³³ [eIDAS Article 3](#)

³⁴ [eIDAS Article 45k and 45l](#)

Figure 21: The use case of (Q)ELedger focuses on the incontrovertible chronological storage of data.

Use case	Description	Example user story	Examples of use
Indisputably store data chronologically	Maintain a database in which transactions are recorded and stored chronologically.	I want to store transactions chronologically, such that this is verifiable and stored in a (de)centralised manner.	<ul style="list-style-type: none"> ▪ Central storage of directors in the chamber of commerce. ▪ Central storage of property ownership at the Land Registry. ▪ Central recording of financial transactions for banks. ▪ Decentralised recording of digital ownership, such as NFTs. ▪ Decentralised storage of lists of trusted parties for digital identity. ▪ Decentralised recording and proof of origin information for raw materials used.

5. Impact analysis

Over the next three to five years³⁵, the trust services market will undergo significant changes. These changes are largely due to the revision of eIDAS, which leads to a redefinition of the requirements and descriptions of trust services. In addition, the development of the EUDIW is helping to build a new infrastructure, which may stimulate demand for trust services. Furthermore, other European legislation is also having a significant impact on the trust services market. **Figure 22** provides an overview of developments in expected demand for (qualified) trust services.

Figure 22: Demand for many qualified trust services is expected to grow (indicative).

Trust services	Demand non-qualified trust services	Demand qualified trust services
Electronic signatures	–	+ +
Electronic seals		+ +
Electronic time stamps		– +
Electronic registered delivery services	+	– +
Website authentication	+	+
Electronic attestation of attributes	+	+ +
Electronic archiving services		+
Electronic ledger		– +

– = Demand service decreases
 + = Demand service increases
 – + = Demand service decreases or increases
 + + = Demand service significantly increases

Besides the impact on individual trust services, we also experience broader effects on the overall trust services market. These impacts are not exclusively linked to one specific service. The following sections will detail these specific and broader impacts.

5.1. Electronic signatures

The market for (Q)ES is undergoing significant changes. Currently, this market is dominated by organisations focusing on the process for non-qualified signatures. In contrast, the market for qualified electronic signatures consists mainly of professional certificates and one-off certificates combined with onboarding processes. Two major developments can be expected from the introduction of the EUDIW and the revision of eIDAS:

- The market for QES is growing as any citizen will be able to get a qualified certificate for electronic signature³⁶.
- The EUDIW is driving growth in the QES market related to private or civil use cases, which makes QES the norm.

The developments follow the assumption (see box below) that EUDIW adoption will be high.

Assumption 1: EUDIW adoption among citizens will be high and similar to DigiD adoption

³⁵ Subject to change in timelines of eIDAS revision and completion of EUDIWs.

³⁶ Until the time comes when EUDIWs can be certified as QSCDs, signatures that will be made through the EUDIW will be the remote signatures (using remote QSCD).

The introduction of the EUDIW creates an attractive alternative with a high level of trust that can be used in both public and private sectors. Each Member State is required to introduce the wallet. Acceptance of the wallet is mandatory for some market players. For citizens, use of the EUDIW is not mandatory. Although acceptance of the EUDIW will also not be mandatory for many market players, we expect the EUDIW to be an attractive tool for many market players for identification and authentication processes. It is expected that the EUDIW will be integrated into existing services and processes.

Business model of one-off (Q)ES providers comes under higher pressure

The current process for creating QES is time-consuming. QTSPs must go through an identification process for each one-off signature. This process involves many steps similar to *Know Your Customer* (KYC) procedures. This introduces costs for the QTSP. With the introduction of the EUDIW, this identification process shifts to the EUDIW. As such, it strains the business model of one-off (Q)ES as it becomes easier and cheaper for parties to offer this as a service. Less impactful changes are expected in the case of professional certificates. For professional use cases, the EUDIW is not necessarily more convenient than a physical smart card used for QES.

EUDIW is driving growth in QES market and normalising its use

The eIDAS revision describes that member states are responsible for making QES certificates available via the EUDIW free of charge to their citizens for non-professional use. In the case of high adoption of the EUDIW, an almost completely new market will emerge. The question arises who will bear the cost of issuance, since it is unlikely that QTSPs will issue these certificates to citizens for free. In addition, it is difficult for the Dutch government to argue that they should become QTSP themselves and issue these certificates, because the QES market is not a new market. The government would then act as a market participant that could distort the market. The government must oblige to the rules of conduct if they choose to act as market participant³⁷. The alternative is to outsource the issuance process to one or more QTSPs.

The introduction of the EUDIW makes using electronic signatures more accessible. It also increases awareness and usage of electronic signatures among citizens. This may lead to higher adoption of electronic signatures in professional contexts. This will lower the threshold for relying parties to request a QES instead of a non-qualified eSig, shifting the market from AES towards QES.

Not all use of QES will shift to remote QES using the EUDIW. Existing physical QES, such as the *Unique Healthcare Provider Identification* (UZI) card, will continue to exist due to practical considerations or switching barriers. A general practitioner might find it more convenient to continue signing prescriptions via the UZI card and a card reader on her computer. Moreover, using the UZI card in an operating room is more convenient than using a phone which is impractical or even prohibited in some cases.

In the professional context, a fee can be charged for the use of QES. It is unclear how this is managed in practice. For example, if the number of signatures that can be made with the QES certificate from the wallet is limited, this could result in lower usage, even in non-professional contexts. In other words, if there is regulation and supervision on the separation between the free non-professional certificates and its paid counterpart, then how this is done will impact the use of signatures, both professional and non-professional.

A good EUDIW customer experience is important. This concerns not only a user-friendly interface, but also integrating its use in existing digital sign environments, such as DocuSign and Adobe Sign. If those environments do not display documents signed with a QES from the wallet or display them unclearly, and users are therefore unable to check their authenticity, the added value of this technology diminishes.






If QES are the norm, then strong growth in the remote signature market is expected

A larger market for the management of remote QSCDs is expected. A QSCD is required for the final 'signing' of the electronic signature. The private keys of the certificates must be stored according to

³⁷ [Rijksoverheid](#)

specific and strict requirements. Within the EU, there is still debate about the location of these private keys, or which type of QSCD should be used in combination with EUDIW. **Figure 23** illustrates some of these options³⁸.

Figure 23: The private keys needed for QES can be stored in several places (not exhaustive).

QSCD options	Description
 Smart cards	Private keys can be stored in the chip of smart cards. This could, for instance, be in the chip of a national ID-card, or a military card. The chip can be issued by a member state itself, keeping control and security in their own hands. The citizen (the holder) needs a phone and uses <i>near field communication</i> (NFC) technology to unlock the wallet using the smart card.
 SIM/eSIM in a phone	Private keys can be stored in a SIM or eSIM embedded in a phone. This can give a better user experience as citizens do not have to use a smart card to unlock the wallet. Telecom providers issue the SIM cards.
 Secure element in phone	Private keys can be stored in the secure element of a phone. This can give a better user experience as citizens do not have to use a smart card to unlock the wallet. In this case, however, the secure element needs to be certified. Phone manufacturers develop the secure element (e.g. Apple, Samsung, Google, Huawei).
 USB token	Private keys can be stored in a USB token (a certified USB stick). Although using a USB token together with a phone may not seem intuitive, it is possible when the EUDIW functions as a web browser plug-in.
 HSM & SAM in combination with EUDIW	Private keys are stored in a <i>Hardware Security Module</i> (HSM) and resides in the cloud. As such, the user does not require physical hardware on its phone. Using an HSM & <i>Signature Activation Module</i> (SAM) still requires strong authentication of EUDIW users.

The details of how to store the private keys will be clarified in the implementing acts. The majority of current mobile phones do not have the right features to store the private keys locally (e.g. in the secure element or on an eSIM). Current phone manufacturers do not benefit from implementing a Secure Element as it only increases the cost price of their products without satisfying a specific customer need. This means that a significant proportion of current and future mobile phones will not be able to store private keys locally. In the long run, if mobile phones can store private keys locally, it is expected that most private keys will be stored in secure elements on the user's phone.

The demand for remote management of QSCDs (HSM & SAM), where private keys (which cannot be stored locally) are stored in the cloud, is likely to increase in the short term. However, the cloud variant does not provide a solution for offline situations. The eIDAS legislation requires EUDIW functions to be available for offline use as well. In practice, this will likely lead to multiple options being used for EUDIWs, depending on the use case.

The market for QES will grow over the next few years

The QES market can be split based on two domains of use, namely non-professional certificates and professional certificates. The first refers to a QES that citizens use as a private person, as opposed to professional certificates where the scope of application is the working environment.

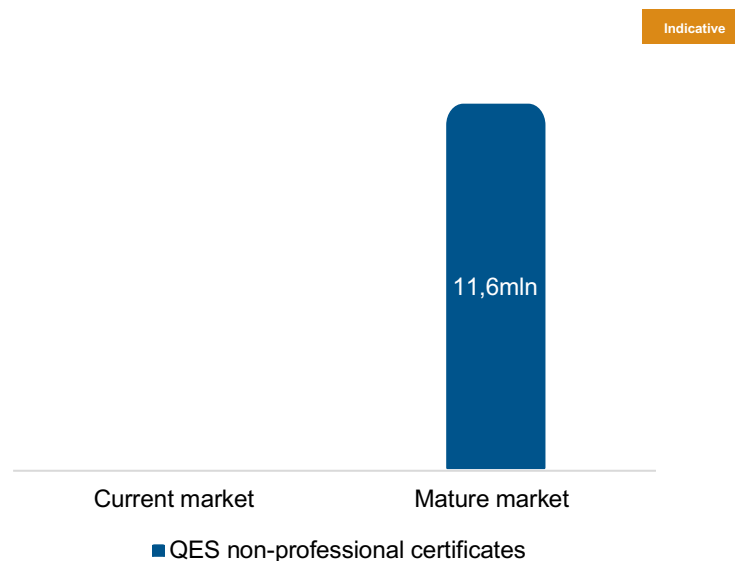
With the introduction of the wallet, the adoption of non-professional QES certificates is expected to follow the same pattern as the adoption of DigiD over the years³⁹. This means that a completely new market will emerge, as the current non-professional QES certificate market is almost non-existent.

³⁸ [Methics, IDEMIA](#)

³⁹ In 2008, when DigiD became mandatory for government agencies, adoption was around 40%. This has now grown to 95% of Dutch citizens aged 14 and above.

About 11.6 million non-professional QES certificates are expected to be in circulation in a mature market (see [Figure 24](#)).

Figure 24: A new market for QES emerges when EUDIW adoption is high⁴⁰.



Assumption 2: Most citizens have one wallet for private matters and additional wallets for work-related matters

In the Netherlands, the ‘NL voorbeeldwallet’⁴¹ is being developed under the supervision of the Ministry of the Interior and Kingdom Relations. The first version will focus on online identification, data sharing and electronic signing in public and private services⁴². It can be expected that, if such a wallet is made available to citizens, free of charge, by the government, the likelihood of multiple wallets being used for private matters is very low. However, it is possible that other wallets will also be certified under the eIDAS revision. Especially for use in work-related matters, there is a chance that citizens will opt for an additional wallet to keep private life separated from their working activities. This is common practice in the physical world too: citizens are free to use different written signatures. The expectation is that every working citizen would then have a private QES certificate and work-related QES certificate. Alternatively, citizens could also use a private wallet that contains mandates for business use.

Within the domain of professional certificates, two types can be distinguished: Occupational certificates and business certificates. Occupational certificates are issued (or withdrawn) by the professional body, as is the case with lawyers, notaries or doctors. This contrasts with business certificates where the employer manages the certificates. Such certificates give employees specific powers, for example signing on behalf of a company, permission to work with equipment or access to locked rooms. An existing example of a business certificate is a certificate for car mechanics so that they can access data from the cars they work on or are authorised to work with hydrogen or electronic vehicles.

There is an existing market for QES in relation to occupational certificates (see [Figure 25](#)). The market to be served is around 120,000 (this does not include military passes). Here, the actual use of QES certificates varies by occupational group. In a mature market, the number of certificates is expected to increase along with the growth of the number of employees in the relevant sectors⁴³. The market for QES business certificates is currently very small. In a mature market, a large proportion of the workforce is expected to start using such certificates.

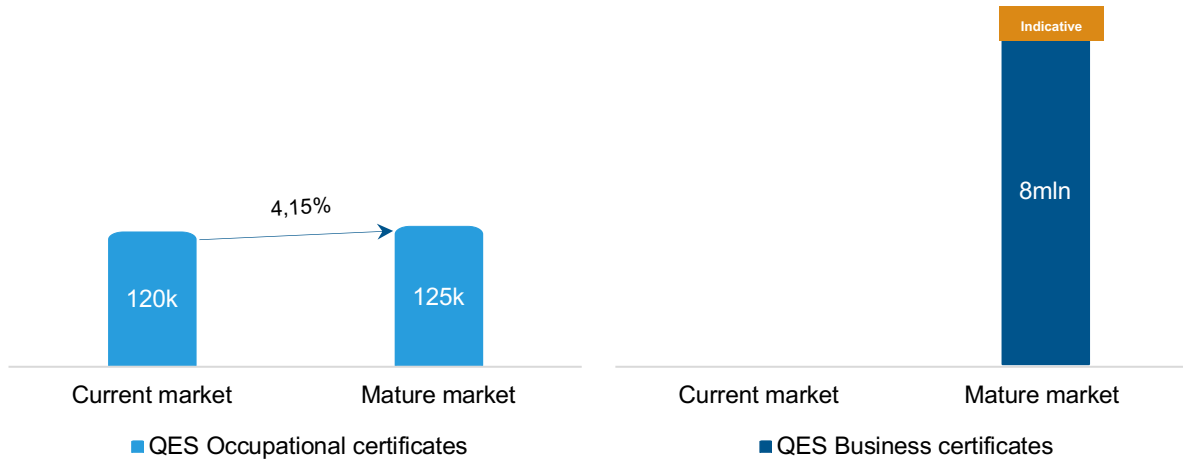
⁴⁰ Defence passes are not included in the professional certificate market.

⁴¹ [EDI Pleio](#)

⁴² [NL wallet on GitHub](#)

⁴³ This growth is linked to the growth of the Dutch population and developments in the labour market.

Figure 25: QES occupational certificates will increase and potentially a new QES Business certificates market emerges.



The growth in the professional certificate market is currently still surrounded by uncertainty, as their function can also be fulfilled by (Q)EAAs. In addition, there is no clarity yet regarding the legal status of a (personal) signature in the form of a personal business certificate in a business context.

5.2. Electronic seals

The eSeals market is changing for market players. *Organisational Digital Identity wallet* (ODIW) adoption is expected to be high. However, the speed of adoption will be slower than the EUDIW due to higher complexity. Nevertheless, strong growth is expected to occur in the Dutch market for QESeals.

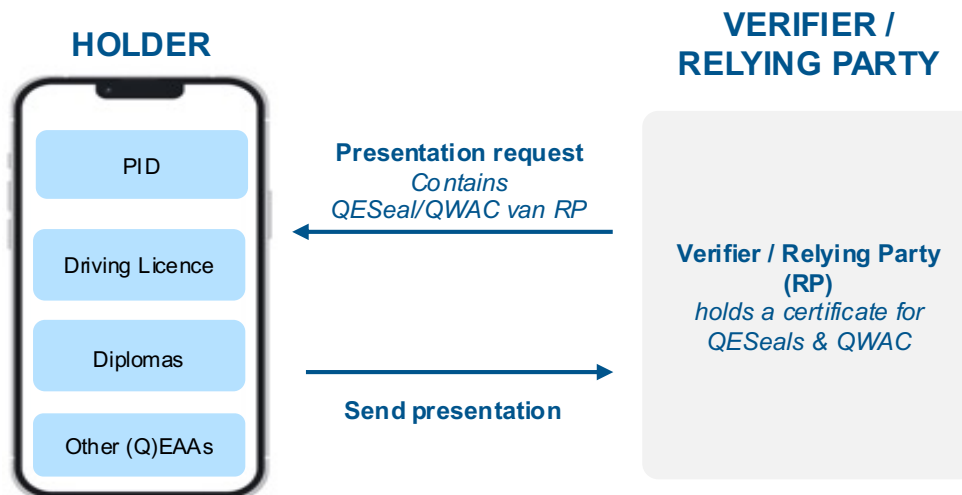
Assumption 3: Adoption of the Organisational Digital Identity Wallet (ODIW) will be high, but the ODIW needs more time than the EUDIW to be adopted.

The Organisational Digital Identity Wallet contains attributes related to the (identification of) organisations. For example, (official) identifiers and attributes at the organisation level. Typical attributes are the Chamber of Commerce number or proof that an IBAN belongs to an organisation. While various wallet solutions are already available in the market for citizens, such wallets are not yet common for organisations. In addition, eHerkenning is mostly used in the Netherlands for authorised access of companies to digital (government) services.

QESeal usage increases as relying parties need to authenticate with a QESeal when conducting wallet data requests

QESeals are expected to play a role between EUDIWs and relying parties. It is expected that data requests towards EUDIWs will only be possible if they are sealed with a QESeal by the *relying party* (RP). **Figure 26** contains a visual representation of this process.

Figure 26: It is expected that relying parties will seal messages to EUDIWs with QESeals and QWACs.



The QESeal acts as an electronic signature that ensures the identity of the sender and prevents unauthorised access to people's wallets. In the Netherlands, RPs must register prior to providing services so that it is known who is allowed to verify attestations. This allows the wallet to see whether an RP is authorised. Because QESeals will be used for this purpose, it is expected that all parties wishing to use the wallet will need a certificate for QESeals.

While the authentication process of RPs has not yet been confirmed, it is very illogical to come up with another new authentication tool for this situation. Especially since trust services and QESeals already exist. This hypothesis is also confirmed by other European legislation around data sharing where QESeals are also required (PSD2).

Other relevant trends regarding data sharing and compliance pressure are fuelling the use of QESeals
There is a clear trend of increasing use of QESeals and the assumption is that it will increase, as various European data sharing legislations mandate their use. This phenomenon occurred with the introduction of the PSD2, which mandates the use of QESeals and QWACs for data sharing between banks and third parties. QESeals are also mandatory for companies wishing to register electrical appliances in the *European Product Registry for Energy Labelling (EPREL)*⁴⁴.

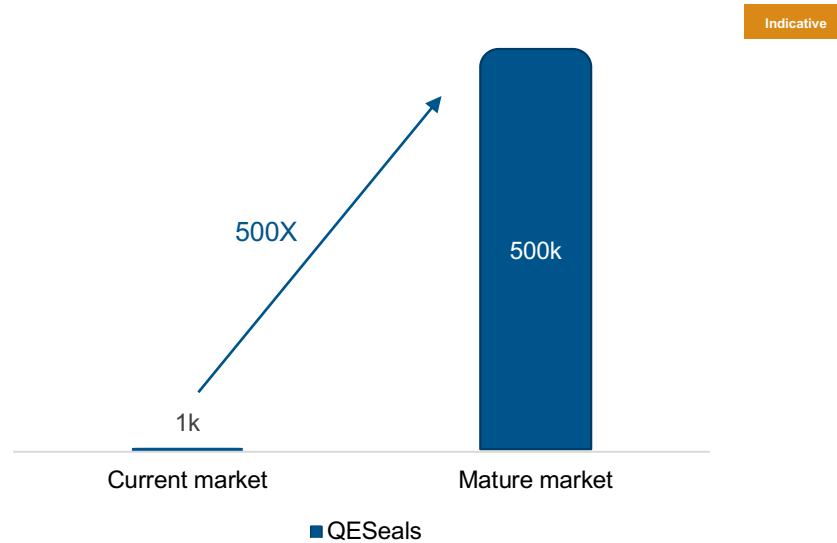
A similar requirement is expected to be included in the *Framework for Financial Data Access (FIDA)*. This means that besides banks, other financial institutions such as pension funds and insurers will also be required to use QESeals and QWACs for data sharing.

QESeals are also desired for scalable data sharing between parties in specific sectors, such as the pension sector, logistics, healthcare and construction industry. It is expected that the need and demand for scalable data sharing between parties will increase, think for instance of the development of data spaces in Europe. This will also increase the use of QESeals for these parties.

A digitally mature business landscape in the Netherlands means large-scale QESeal integration
The totality of these trends means that the market for QESeals is going to change significantly. The current Dutch market is estimated at around 1,000 QESeals. It is expected that in a digitally mature economy, almost the entire SME and large companies will have to get a QESeal in the future. The driver of this development is that eventually the current PKI government certificates will largely be replaced by the combination of QES, QWACs and mainly QESeals. When the Dutch corporate sector develops to the stage of digital maturity where every annual report, invoice and numerous other business documents have a QESeal, it is estimated that there will be around 500,000 QESeal certificates in circulation (see **Figure 27**).

⁴⁴ [Intesi Group](#)

Figure 27: In a digitally mature Dutch economy, almost every company has a QESeal.



5.3. Electronic time stamps

There is expected to be minimal to no change in the Dutch market of QTimestamps as a result of the eIDAS revision. This follows from the current low usage in today's market of QTimestamps in the Netherlands. The limited changes in the eIDAS revision do not seem to change this.

The (Q)Timestamp market is and continues to be limited in the Netherlands

The Dutch market for QTimestamps is currently of limited size. Time stamps are a crucial part of the various trust services, because a time stamp provides extra security and thus creates trust. For example, in the process of a (Q)ES, it is important not only to know who signed and that the signature corresponds to the right person, but also when this person signed. That is why (Q)ES often have a time stamp to seal the signature with proof of a certain time and date.

The lack of a market stems from the fact that, within Dutch practices, the addition of a QTimestamp seldom requires an independent party to insert a QTimestamp. A non-qualified time stamp suffices and is not offered as an independent service. The time stamp is done, in those instances, by the parties involved themselves. The only use cases for an independent time stamp, i.e. (Q)Timestamp, are cases where every microsecond and the sequence of transactions are crucial, for example in trading financial products.

This changes when a legislator, often in a specific context, does require an independent third party to perform time stamping. For example, the Italian government requires companies to provide their tax returns with a time stamp⁴⁵. The Dutch market has no such requirement at present and there are no indications that this obligation will arise in the short term.

The eIDAS revision gives minimal reason to expect increased use QTimestamps

The requirements for (Q)Timestamps in the eIDAS revision are almost identical to those in the original eIDAS. There is no new mandatory requirement for the use of QTimestamps in the new regulation.

In a fully matured digital market where services are entirely digitized, there might be a mandatory requirement to implement QTimestamps in services needing undeniable time verification. A fully digital audit by an accountant or digitally recorded agreements by notaries are examples where there may be an added value of an independent qualified party to conclusively guarantee the date and time for a longer period.

⁴⁵ [EY](#)

5.4. Electronic registered delivery services

It is probable that the market for (qualified) electronic registered delivery ((Q)ERDS) will change minimal because of the eIDAS revision. Current QERDS usage is low and the eIDAS revision contains limited incentives to increase usage.

QERDS use is limited in the Dutch market

The current market for QERDS is small. A key driver for QERDS acceptance is to integrate obligatory use in sectoral legislation or inclusion of the service on the national 'Comply or explain list'. Currently, this is not the case in the large majority of instances in the Netherlands. The qualified trust service includes additional verification procedures that enhance security. In practice, this is unnecessary for most use cases and the additional costs do not outweigh the benefits. There are several sectors, such as the legal sector, that may want to start using QERDS. However, this is currently not yet the case on a large scale.

Unlike QERDS, there is a sizeable existing market for ERDS. ERDS providers operate in various sectors, including healthcare, legal services, financial services, public sector, construction and education.

Use of (Q)ERDS will likely increase due to broader legal validity and interoperability

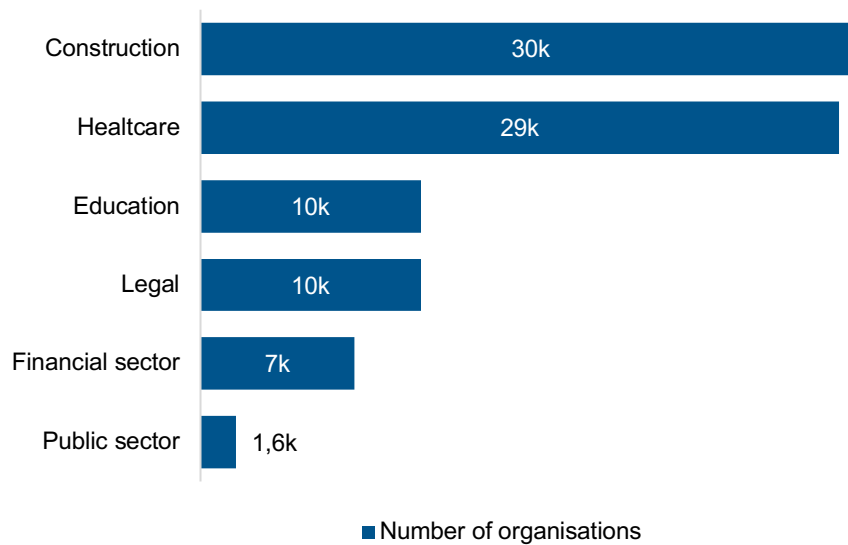
The eIDAS revision contains minimal changes regarding (Q)ERDS. The added mandatory Europe-wide recognition of the various trust services does represent a potential stimulus for increase in the QERDS market.

Article 24a (8)⁴⁶ of the eIDAS revision specifies that a QERDS recognised in one member state has the same status for all other member states. eIDAS allowed Member States the discretion to not recognise QERDS services from QTSPs from other Member States as qualified. This resulted in national restrictions in terms of legal validity and acceptance of the service. Now that it has been stipulated in the eIDAS revision that other member states must recognise the service, this means that there is added value in a QERDS compared to ERDS, as its legal status and acceptance is now conclusively established Europe-wide. It is possible that this will increase the demand for QERDS and make it easier for providers of this service to offer services in other Member States. In practice, however, it appears that limiting factors for this interoperability can arise at times, such as specific requirements in implementing legislation or other bureaucratic factors. For the increase in demand for QERDS, it is therefore important that limiting factors are actively avoided by national regulators.

These developments collectively result in a small current market. The main sectors, healthcare, financial services, public sector, construction and education, collectively contain a potential market of about 95,000 organisations (see [Figure 28](#)). Obligatory use is the main factor that can cause organisations to move from ERDS to QERDS. In addition, the government could potentially fuel growth if it adopts QERDS for correspondence and its internal processes. However, these are not direct consequences of the eIDAS revision.

⁴⁶ [eIDAS Article 24a](#)

Figure 28: The potential market for mandatory use of QERDS involves about 95,000 organisations.



5.5. Website authentication

The use of QWACs is changing in a similar way to the market for QESeals. More organisations will need a QWAC in the future. Like QESeals, the increased demand for QWACs is expected to arise from compliance pressure and the need for higher legal certainty. The increase in demand is unlikely to stem from the use of QWACs for website authentication. In addition, much depends on the implementing acts that might describe what 'acceptance of QWACs' means⁴⁷.

QWACs continue to compete for website authentication

With the eIDAS revision, web browsers must accept QWACs which puts QWACs on a more equal footing when competing with WACs⁴⁸. QWACs have the advantage that they have stronger verification during the issuance process, creating a higher level of legal certainty. This also has a downside: a more complicated and expensive issuance process. For many websites, this is unnecessary so it is expected that most websites will continue to use WACs.

Other relevant trends regarding data sharing and compliance pressure are fuelling the use of QWACs

As for QESeals, the trend is visible that demand for QWACs is increasing, as various European data sharing legislations mandate their use. Section 5.2 already described the obligation of using QWACs under PSD2 and the expectation of the same requirements in the FIDA framework.

QWACs are desired for authentication for scalable data sharing between parties in specific sectors, such as pensions, logistics, healthcare and construction. It is expected that the need and demand for scalable data sharing between parties will increase, think for instance of the development of data spaces in Europe. This will also increase the use of QWACs for these parties.

Use of QWACs increases as relying parties must authenticate with a QWAC on wallet data requests

As well as QESeals, QWACs are going to play an important role between the EUDIWs and relying parties. It is expected that data requests towards EUDIWs will only be possible if they contain a QWAC from the relying party (see **Figure 26**). The QWAC acts as a secure connection between the wallet and the relying party. The secure connection ensures that data sent (information from (Q)EAAs) is not modified between the wallet and the relying party. In addition, the secure connection guarantees that no one else can read the data. This is relevant for the integrity and confidentiality of the data. It is expected that all parties wishing to use the wallet will need a QWAC.

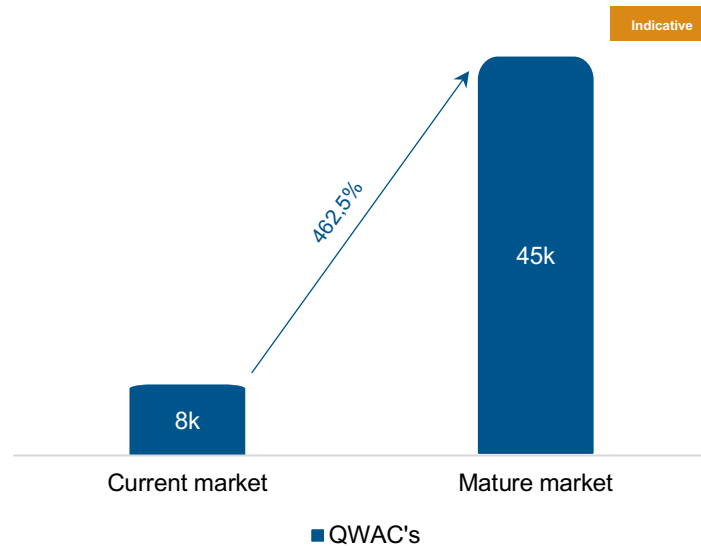
⁴⁷ [Security risk ahead](#)

⁴⁸ [European commission](#)

Although this process has not yet been established, it is illogical to invent another authentication means for this situation. This hypothesis is also confirmed by other European legislation around data sharing where QWAC are also mandated (e.g. PSD2)⁴⁹.

Consequently, the market of QWACs in the Netherlands is projected to more than triple compared to its current state. It is estimated that there are currently around 8,000 QWACs in service. The estimated prediction is that in a mature market, this could potentially rise to 45,000 qualified certificates (see **Figure 29**). Despite the substantial growth, the share of qualified certificates in the total market remains limited.

Figure 29: In a digitally mature business landscape, the growth of QWACs increases sharply.



5.6. Electronic attestation of attributes

A sizeable European market for (qualified) electronic attestation of attributes is expected to emerge in the short term because of the introduction of EUDIW.

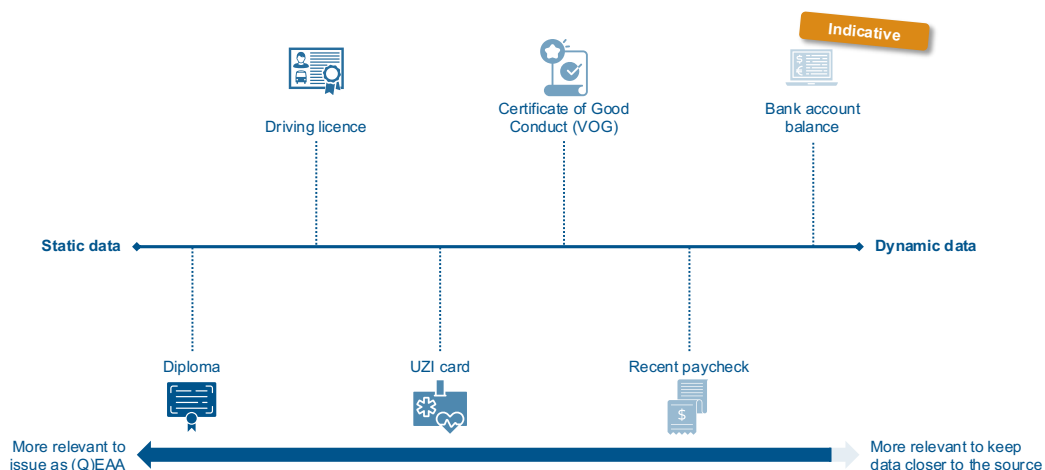
The expected usage is based on the replacement of current physical attestations, such as diplomas and driving licences. New types of attestations are also expected to be used in the future. Some of these attestations are going to be issued by governments/market parties themselves, but it is likely that QTSPs will issue most attestations on behalf of these parties.

(Q)EAAs are mainly issued from static data

The usability of QEAs can be understood by viewing them along the spectrum running from static to dynamic attributes (see **Figure 30**).

⁴⁹ [Infocert](#)

Figure 30: static data are more suited to be issue as (Q)EAA



(Q)EAAs are expected to largely complement or replace existing uses of attributes that are static to a greater or lesser extent. Static attributes are characterised by their immutability and have a validity period of roughly several years to a lifetime. In addition, there is low probability of revocation for these static data points. Examples of more static attributes are university diplomas, or driving licences. A diploma is for life and is rarely revoked in practice⁵⁰.

There are attestations that are somewhere in the middle of the spectrum and the hypothesis is that this category is partially shifting to (Q)EAAs. A VOG or a BRP statement has a validity of a few months, and because of that short duration, it reduces the likelihood of false claims. For such examples, the use is expected to shift to (Q)EAAs. Exceptions are those situations where direct links are already widely used, think of the existing links with the KVK register or the Kadaster.

At the other end of the spectrum are dynamic data points, such as a current bank balance, or location data. For these data points, real-time status is much more important. For highly dynamic attributes, a direct link between issuer and relying party provides the highest level of accuracy. For some dynamic attributes, (Q)EAAs do provide sufficient certainty, but here a risk assessment will be needed to determine this on a case-by-case basis.

Usage of (Q)EAAs will be substantial as it replaces existing use cases

An even more extensive number of digital or physical documents containing attestations about individuals or organisations currently exist, in addition to the examples already mentioned above. Service providers request these documents from citizens to hedge risk or because of legal obligations they have. These documents are often issued in a proprietary manner and checked for accuracy and validity.

EUDIW creates a generic and scalable infrastructure that facilitates parties to share these documents in a user-friendly and cost-efficient way. This new infrastructure is, potentially, a cheaper, more secure and user-friendly alternative compared to the current way of sharing these documents. In some cases, government sources need to open up their data for verification by QTSPs. The use of (Q)EAAs is expected to take off, as it can replace the current way of working in many use cases.

An illustrative example is the application for an extract from the *Basisregistratie Personen* (BRP) to obtain rental accommodation. Citizens must apply for these online, after which they wait 48 hours to receive them by post and send a photocopy to the relevant authority. A (Q)EAA facilitates this entire process within one minute. The rental agency can proceed instantly as human verification of the documents is no longer necessary.

Another possible consequence of the EUDIW is that usage changes from one-off to periodic.

⁵⁰ [Observant online](#)

Stakeholder interviews suggested that periodic use could potentially enrich current data. This would then apply to more dynamic attributes, for example in determining the creditworthiness of an entity where new financial data is considered periodically instead of making judgements based on a single point in time.

Clarity on authentic sources and schema providers is needed

A widespread (Q)EAA market requires clarity on the meaning of the term 'authentic source'. At this moment, it is still unclear which parties will become authentic sources. It is possible that multiple parties become an authentic source for the same data points. In the Netherlands, universities are an authentic source for diplomas, but DUO can also be an authentic source for the same data. It is in the interest of governments to facilitate a (Q)EAA ecosystem and help with resolving uncertainties around authentic sources.

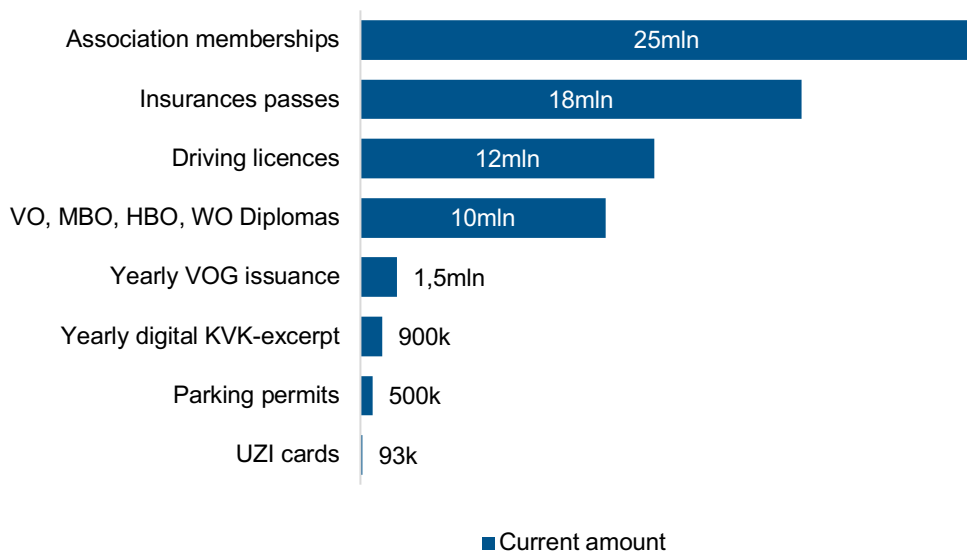
Schema providers play an important role in the development of the (Q)EAA market and for each area of use, this role must be filled. It is at this stage unclear who will fulfil these roles. Schema providers provide common standards, rules and language for specific attestations. This creates a uniform framework within which attributes can be verified and exchanged. In the absence of such a common framework, usage will be severely limited. A potential problem in the current setup is that EUDIW only requires technical interoperability, but there is also a lack of clarity on semantic interoperability.

The market for EAAs increases due to new use cases

The EUDIW also opens new ways for sharing attestations that are not currently shared online. Think, for example, of proof of membership or loyalty campaigns. Here, sharing attestations through the EUDIW is an added value that parties can offer to their customers/members. Sharing this data online is now often not done due to high costs, limited reach or limited customer experience. For this, the EUDIW is a specific solution for smaller local businesses. In addition, new applications may arise through technological innovation that have not yet been foreseen.

All these developments together bring about the expectation that a significant new European landscape for (Q)EAAs will emerge. **Figure 31** provides a quantification of only a limited number of examples. This shows the potential of this market.

Figure 31: The market for QEAA's and EAAs may unfold into a very sizeable new market.



5.7. Electronic archiving services

The use of (qualified) electronic archiving services or (Q)E-Archiving is not expected to surge. Current users of e-Archiving services are not expected to switch to QE-Archiving due to lack of added value. In addition, no obligation to use QE-Archiving is foreseen.

Demand for QE-Archiving will not increase, due to lack of added value compared to e-Archiving

With further digitisation, an increase in e-Archiving services is to be expected. More and more archives will be digitised in the future. With e-Archiving services, an independent party guarantees the validity of the archive. For the public sector and probably much of the private sector, the expectation is that they will initially try to organise e-archiving internally. However, there is an opportunity for this market to grow, specifically for private parties, if it turns out that their internal systems are insufficiently capable of guaranteeing the integrity of their files and the associated certificates.

The added value of QE-Archiving compared to e-Archiving is a higher level of security and legal validity⁵¹. In addition, QE-Archiving service recognised by one member state must also be recognised by all others.

It is expected that these elements alone are insufficient to move the current e-Archiving market to QE-Archiving, as the added value is not significant enough for most use cases. Thus, in many cases, the additional requirements only create a more costly service. interviewed stakeholders expect that most customers will opt for the non-qualified service.

For the above reason, the growth of the QE-Archiving market will likely depend on any national or European obligation to use it. The revised eIDAS regulation does not include any provision of this nature.

5.8. Electronic ledgers

The short-term projection is that the market for QELedger will contain a very small number of providers and that usage is low. This claim is supported by the ambiguity in technical implementation and the obscurity of legal frameworks.

Lack of clarity about the requirements set for QELedger providers and the QELedgers themselves inhibits the emergence of a new market

At this moment, there is a lack of clarity on what concrete requirements are imposed on a QELedger provider and on the service itself. The requirements for certification have not been detailed yet. The eIDAS revision states that these requirements should be available within 12 months. However, it is still unclear whether it will be possible to define requirements that will suffice for audits by a certification body within this timeframe. As a result, there is a risk of delay or possible creation of requirements that are not well aligned with future technological and market developments.

In the interviews, stakeholders expressed that more details are needed regarding the definition of the QTSP as the provider of a QELedger. Depending on the design of the technology, e.g. the consensus mechanism used, different entities or roles can be identified that jointly ensure the functioning of a (Q)ELedger.

Interviewees indicated that they did not yet have a picture of this themselves either. The definition of a QTSP can be narrow or broad. In the case of the narrow definition, the QTSP is only that entity or entities that have developed and monitor the (Q)ELedger. However, in a decentralised world where the (Q)ELedger is developed using open-source software and there are potentially large numbers of (validator) nodes, the task of designating those entities becomes highly complex. To get around this ambiguity, there is the possibility of interpreting the concept of QTSP more broadly, e.g. in the extreme, any entity that provides a service and uses a QELedger for this purpose is a QTSP. This also becomes very complex, because then all participants of the network are QTSPs.

Based on the interviews, it is expected that the narrow definition of QTSP is the most probable. One justification might be that control over the QELedger becomes one of the requirements for certification. If this is going to be the case, it means that the term QELedger will only refer to so-called 'permissioned' blockchains or networks. In these, one or more parties' control and determine who is allowed to participate and who is not. In that case, the eIDAS revision limits the possible number of providers of QELedgers to a small number of parties, namely government-driven initiatives, e.g. EBSI, and private parties capable of building and monitoring their own blockchain infrastructure, such as Microsoft, Amazon or IBM. Decentralised ecosystems, such as cryptocurrencies (e.g. Bitcoin, Ethereum

⁵¹ [eIDAS Article 24 & 45](#)

or Solana) and digital assets using *non-fungible tokens* (NFTs), are then unlikely to be qualified as QELedger.

Legal complexity hinders emergence of a market

Another impeding factor for using the QELedger is legal complexity. Uncertainty about liability within a QELedger ecosystem provides the main legal challenge. Currently, it is unknown what this will look like. Clarity is needed on the liability of the QTSP regarding, for example, illegal activities on the QELedger itself, illegal activities using the QELedger or liability in case of disputes between participants of the QELedger. The complexity increases when there are multiple entities that are jointly providing the QELedger service, as their responsibility to a certain outcome may not be evenly distributed. Without clear specifications, the market for QELedgers is unlikely to take off.

EUDIW is a possible use case for the QELedger

One possible use case for (Q)ELedgers is the EUDIW. This involves storing data related to the issuance and revocation of electronic attribute attestations. This could involve, for example, storing decentralised identifiers, issuer credential definitions, schemas, and revocation updates in a decentralised ledger, as is the case for example with Sovrin⁵².

However, there is no consensus yet on the added value of this application over centralised methods. The specification of the EUDIW, (Q)EAA and (Q)ELedger is described technology-neutral and allows both forms. Several market players indicate that they do not consider this application feasible, partly due to resistance in some countries to using blockchain solutions for the EUDIW. In addition, this use case also requires further specification of a QELedger ecosystem, for example on who is authorised to provide the information of DIDs, issuer credential definitions, schedules, and revocation updates. All this combined makes this option unlikely.

⁵² [Sovrin](#)

6. Cost analysis

The cost analysis includes the relevant costs for trust service providers resulting from the eIDAS revision. This involves the difference between eIDAS and the eIDAS revision. Changes in usage that are not driven by the eIDAS revision, such as market conditions, other laws and regulations (e.g. GDPR, PSD2/PSR), are not considered. Three types of costs can be distinguished:

- 1 Regulatory costs:** Costs incurred by trust service providers to be compliant due to new or changed requirements resulting from the eIDAS revision.
- 2 Financial penalties related to the eIDAS revision:** Fines for non-compliance.
- 3 Market adaptation costs:** Costs incurred by trust service providers due to a changing market because of the eIDAS revision, such as increased demand.

The following paragraphs will further elaborate on these different costs.

6.1. Regulatory costs

According to the 'Handboek Meting Regeldrukkosten' regulatory costs are "those costs incurred by companies (and citizens) to correctly comply with obligations under laws and regulations and to follow all regulations"⁵³. The eIDAS revision increases the regulatory burden for QTSPs. Two components can be identified in this regard:

1. Regulatory burden to become and remain a QTSP
2. Regulatory burden related to specific qualified trust services

6.1.1. Regulatory burden to become and remain a QTSP

The main factors increasing the regulatory burden are not only related to costs, but also to time. QTSPs risk taking longer than desired to become compliant with the eIDAS revision. The sections below explain the main factors that increase the regulatory burden.

Costs rise for organisations to become and stay compliant

The eIDAS revision imposes several additional requirements on QTSPs compared to the original eIDAS. This requires existing and new (Q)TSPs to set up new internal processes to remain compliant. The compliance costs to become a QTSP are higher than the costs for existing QTSPs to become qualified for a new service.

Market participants indicated that they expect significant costs for adapting internal processes to be/remain compliant. **Figure 32** contains some examples of changes with impact, to a greater or lesser extent, on regulatory costs. Regulatory costs that increase are discussed in the text below. Identity assurance for qualified certificates is discussed in section **6.1.2**.

Figure 32: Several changes increase compliance pressure for QTSPs (not exhaustive).

	Changes in eIDAS	Applicable on TSPs	Applicable on QTSPs	Regulatory costs
1	Certain eID services should also be accessible offline where applicable (art. 3)	✓	✓	➔
2	Obligation to make services available and accessible to people with disabilities (art. 15)	✓	✓	➔

⁵³ [Handboek Meting Regeldrukkosten](#)

3	Non-qualified TSPs must take measures to mitigate risks (art. 19a):			
	<ul style="list-style-type: none"> • Registration and onboarding for a particular service • Procedural and administrative controls for offering a trust service • Maintenance and implementation of a trust service 	✓	✗	➔
4	Obligation to report incidents to the supervisory authority within 24 hours (art. 19b, 24)	✓	✓	➔
5	Qualified services and products in one Member State must also be recognised as such in other Member States (Art. 24a)	✗	✓	➔
6	Identity assurance for Qualified Certificates (QWAC, QESig, QESeal) and QEAA at level high (Art. 24)	✗	✓	➔
	✓ = Not applicable			
	✗ = Applicable			
	➔ = no significant changes in regulatory costs			
	➔ = Increase regulatory costs			

A critical demand, stemming from Article 15, is that trust services are required to comply with the Accessibility Act. This means that QTSPs are mandated to make their services accessible to people with disabilities. An example of such an adaptation is the implementation of pre-reading features. The European commission estimates that in 2020, European companies incurred €20 billion in costs related to meeting accessibility requirements⁵⁴.

There are initial and recurring costs related to the accessibility requirement for QTSPs. Initial costs include the additional investment needed to design or set up the products and/or services to comply to the new standards. Recurring costs include costs incurred in providing/delivering the service while supporting people with disabilities. Higher costs are expected for both cases but there is still a high degree of uncertainty.

Trust service providers indicate that some of their services currently already must comply with accessibility requirements (such as the Web Accessibility Directive⁵⁵ and ETSI EN 301 549). They have adapted their services accordingly, or use 'third parties' to meet the requirements (e.g. enabling Apple's VoiceOver to be used for their services). For these reasons, some QTSPs do not expect this requirement to cause major problems.

However, the European Accessibility Act goes a bit beyond the Directive, as an updated ETSI standard is being drafted. This may lead to additional implementation costs.

In addition to the Accessibility Act, QTSPs struggle with a significant regulatory burden, for example, the *Network and information security directive*, or NIS2 directive. This directive adopted by the European Union is intended to improve cybersecurity and resilience of essential services in EU member

⁵⁴ [European Commission 2021](#)

⁵⁵ [European Commission 2016](#)

states. Moreover, QTSPs must comply with *the European Technical Standard Institute*, also known as ETSI standards, developed to ensure interoperability. The trend of ever-increasing compliance is expected to continue. This is a generic trend and QTSPs expect to conform to more standards in the future. This leads to an increase in costs. The higher regulatory burden makes it more challenging for (smaller) QTSPs to bear the costs associated with compliance. In addition, some of the participants expressed a desire for harmonisation of all the different standards they must comply with and centralisation of their supervision with the aim of saving costs by avoiding double audits for similar requirements.

Regulatory costs increase because QTSPs must meet additional requirements of other norms and standards for specific trust services

QTSPs must adhere to many compliance requirements, not limited to eIDAS. One example is the norms and standards for QWACs. When QTSPs want to issue QWACs, they must comply not only with ETSI standards (ETSI EN 319 411), but also to the additional demands imposed by Web browsers. This means that QTSPs are not only certified by the *Rijksinspectie Digitale Infrastructuur* (RDI), but as well by other bodies. An example is the WebTrust for Certification Authorities criteria, issued by the WebTrust for Certification Authorities Task Force. Although these two certifications are theoretically interchangeable, practice shows that QTSPs often obtain both certifications. In addition, a QTSP is expected to constantly track updates via blogs and monitor the community for bugs to implement remedial actions. This requires a constant compliance effort, not a one-time or annual task. Large organisations can bear this burden, but smaller organisations may struggle to make their business model profitable.

Other costs are not showstoppers

The yearly external audits represent a major cost, apart from the costs to keep processes compliant. The external investigation involves a (re)certification audit in one year and a control audit the following year. The (re)certification involves a full audit, while the control audit is more limited. An exception is audits for QWACs, for which Web browsers require a full audit annually. Although external audits incur costs, they are not seen as the biggest financial burden for QTSPs.

An initial audit to obtain qualified status costs between €12,000 and €25,000 (in the best-case scenario) in internal costs, depending on the size of the company, in which country the company conducts the audit, and for which qualified trust service the certification is conducted⁵⁶. This amounts to the costs that trust service providers incur internally for providing the requested evidence (e.g., documentation). In addition to these internal costs, the CAB must also be paid for performing the certification. These costs are estimated at €12,000 to €25,000.

Thus, the estimated initial audit cost for obtaining qualified status for a trust service is approximately €24,000 to €50,000 (see **Figure 33**).

Figure 33: The initial audit cost for QTSPs is between €24,000 and €50,000 (illustrative).

Description	Assumptions	Total
Internal support	20 – 40 person days Average rate: €77 ⁵⁷	€ 12.000 - € 25.000
External audit CAB	10 – 20 person days ⁵⁸ Average rate: €150	€ 12.000 - € 25.000
Total costs initial audit		€ 24.000 - € 50.000

In the case of large enterprises, audit costs will be higher because a more extensive part of the organisation and processes must be evaluated. In addition, each individual trust service requires its own certification.

⁵⁶ [EY 2021](#)

⁵⁷ [Handboek Meting Regeldrukkosten 2023](#)

⁵⁸ [EY 2021](#)

Along initial costs for obtaining qualified status, there are also periodic costs for maintaining the qualified status. eIDAS requires that an audit be done by the CAB at least once every two years to evaluate compliance. In practice, these audits are often done once a year. The costs for this are fully borne by the QTSP. In terms of internal costs, an average of €20,000 to €25,000 (0.2FTE) must be considered. Costs charged by the CAB also apply here: these costs are estimated at €6,000 to €12,000.

Total periodic costs for maintaining qualified status amount to about €26,000 to €37,000 per year, depending on the size of the company and the trust service in question (see [Figure 34](#)).

Figure 34: Periodic audit costs for QTSPs are between €26,000 and €37,000 (illustrative).

Description	Assumption	Total
Internal support	30 – 40 person days (0,2 FTE) Average rate: €77 ⁵⁹	€ 20.000 - € 25.000
External costs audit CAB	5 – 10 person days ⁶⁰ Average rate: €150	€ 6.000 - € 12.000
Total costs periodic audit per year		€ 26.000 - € 37.000

Various QTSPs have indicated that for a large company with complex trust services or processes, these costs can quickly exceed €100,000 per year. Including the initial investment, this brings the total certification cost of providing a qualified trust service over a five-year period to approximately €150,000 to €240,000.

There is a risk of delays preventing QTSPs from being certified on time

The number of auditors qualified to perform the required audits for QTSPs is limited. This can lead to potential delays because auditors are not immediately available to respond to requests. As a result, QTSPs may be forced to wait before they can launch new services. This may also give an advantage to QTSPs that are the first to be certified, allowing them to take a lead in new markets, such as that of (Q)EAAs.

Furthermore, delays may be exacerbated by the simultaneity of the eIDAS revision coming into force, the writing of the implementing acts, the auditing of QTSPs and the auditor's own accreditation process. The eIDAS revision is expected to go into effect in mid-April 2024⁶¹. The implementing acts, which include further technical specifications for certification, are not known at this time. These are necessary for auditors to conduct an adequate audit. During the transition period, the simultaneous occurrence of multiple activities may lead to delays:

1. Dutch auditors themselves must become accredited by the *Raad voor Accreditatie* (RvA)⁶² in the case of the new trust services, while (Q)TSPs want to be certified.
2. Auditors and supervisory bodies need to interpret the implementing acts to conduct a proper audit and assessment. However, the implementing acts are probably not final yet while the eIDAS revision is already in place.

Due to this transition period, QTSPs may experience delays in the certification process.

6.1.2. Regulatory pressure related to specific trust services

For specific trust services, the pressure to comply with regulations continues to increase. This is partly due to the new requirements introduced by the eIDAS revision and partly because these trust services must not only certify themselves under eIDAS but must also comply with requirements from other parties.

⁵⁹ [Handboek Meting Regeldrukkosten 2023](#)

⁶⁰ [EY 2021](#)

⁶¹ Subject to EU timelines

⁶² [Raad voor Accreditatie](#)

The expectation is that only SAM certification results in additional costs in the case of QES

The eIDAS revision introduces new standards for QSCDs managed remotely. QTSPs indicate that compliance pressure is going to increase, as it will be necessary to certify not just the *Hardware Security Module* (HSM) but also the *Signature Activation Module* (SAM). QTSPs estimate that the additional cost of such certification could run into hundreds of thousands of euros. A QTSP may choose to purchase such a module, but this is also very costly.

There are also additional requirements in the eIDAS revision for qualified electronic signatures:

- QES should contain information about the validity of the certificate, or provide a location where this status can be requested
- Additional checks need to be done for 'advanced electronic signatures based on qualified certificates,' such as: 'was the certificate really qualified', 'was the certificate valid at the time of signing', 'does the data match what you are signing'
- For signatures in the wallet, there are specific requirements for the format in which the data is issued (e.g. JOSE (JWT) and COSE)

These requirements are not expected to result in additional costs, as many QTSPs already meet these requirements or can easily adjust their systems.

Cost increases for QTSPs that are not yet at the Level of Assurance (LoA) high for identity assurance at QWACs, QES and QESeal

Article 24 in the eIDAS revision requires that the identity of the person to whom the qualified trust service (for QEAs, QWACs, QES, and QESeals) is provided must be verified with *Level of Assurance* (LoA) high. This means that QTSPs, which currently have a substantial LoA, will have to make additional efforts and costs to raise their level of assurance to high. The advantage of this requirement is that it ensures harmonisation within Europe, creating a more level playing field. LoA high can potentially be achieved by any of the following methods:

- EDI Wallet or an eID scheme
- QESig/QESeal certificate
- Other LoA High means of identification, if approved by the supervisory body
- Physical presence of the person/representative of the legal entity

The adoption of the wallet (as a means of remote identification) represents a significant shift for existing processes that rely heavily on face-to-face verification, offering the potential to lower operational costs. In addition, these EU-wide accepted means ensure that one does not have to set up a new process for each country depending on what is locally available (e.g. iDIN in the Netherlands, Itsme in Belgium). Currently, regulators in different EU member states may have different demands for verification. It is thus expected that this requirement will reduce the regulatory costs for certain operational processes. This is contingent upon the operational costs associated with using the EUDIW. For instance, if the cost of implementing EUDIW authentication becomes too high for a QTSP, it might render the service financially unviable for providers.

6.2. Financial penalties related to eIDAS

A significant change in eIDAS is related to fines for non-compliance. In the eIDAS revision, the Commission sets the lower limit for the maximum penalty amounts⁶³:

- For natural persons: maximum fine minimum of €5,000,000
- For legal entities as trust service providers: maximum fine minimum of €5,000,000 or 1% of worldwide turnover

A minimum maximum means that member states themselves can decide to set a higher maximum penalty amount, but it must be at least as high as indicated by the Commission. In the original eIDAS there were no penalties for non-compliance and national governments were free to determine them themselves. In practice, sanctions are now hardly ever imposed. The comparison with GDPR shows that the fear of high fines has a strong self-regulatory effect. Particularly, large entities involved in high-profile cases are subjected to significant penalties, serving to amplify this effect. Often, by the time it's revealed that legislation has been breached, significant damage to the trust in the service provider has already occurred, leading to substantial impacts on their market position.

⁶³ [eIDAS article 16](#)

Next to the penalties, the eIDAS revision also specifically states that QTSP customers will have the right to recover from QTSPs the tangible and intangible damages they have suffered in the event of non-compliance⁶⁴. Introducing these penalty guidelines could potentially have a major impact on trust service providers.

6.3. Market adaptation costs

Chapter 5 described the effect of the eIDAS revision on trust services, including the effect on demand. If the demand for these services increases or decreases, this is also likely to affect the cost of provisioning for trust service providers. It is expected that, under current conditions, an increase in demand will not immediately result in additional disproportionate costs or large necessary investments. Most of the services are scalable and will cope well with a normal increase in demand. In addition, the increase in costs is proportional to the increase in revenue.

However, a significant increase in demand (certificates for signatures) will require significant investment and redesign (e.g. hardware, knowledge, cloud capacity and automation) of the organisations. At this moment there are a limited number of parties active in the market that are prepared for such an increase in scale. Several smaller parties have limited team capacity or use manual processes and are thus less prepared for a major change in demand. This means they will have to make significant investments to scale, for example in additional hardware or customer service. It is unclear whether this is feasible for these parties.

Next, there is a distinction in market adaptation costs between different existing services.

QTimestamps, QERDS, QEAchiving

For these services, no major change in demand is expected (see **Chapter 5**) and thus most likely no additional costs will need to be incurred. Nonetheless, trust service providers of these services must continue to invest to remain relevant and to be able to deliver changing demand in the future.

QESeals, QWACs

Marginal costs for these services are relatively high, meaning that scalability is low and additional investment/cost is required to realise the potential of the additional demand. This is particularly because identification processes for these services are still largely physically accomplished. As discussed earlier, the eIDAS revision does add that these processes can also be supported by, for example, the EUDIW, with the expectation that this will lead to operational cost savings.

QES

Scalability is anticipated to lead to cost reductions, as larger volumes result in the distribution of costs over a wider base. Operating expenses are expected to increase in proportion to rising revenues. Additionally, trust service providers foresee minimal additional investment being needed to capitalise on the potential offered by growing demand.

New trust services

The rollout of new trust services necessitates additional investments from existing (Q)TSPs. The hesitance of (Q)TSPs to rollout these new services is largely due to the uncertainty surrounding the finalization of implementing acts. Moreover, the viability of (Q)TSPs offering the (Q)EAA-service hinges on the uptake of the EUDIW, which remains highly unpredictable at this stage.

⁶⁴ [eIDAS article 13.1](#)

7. Revenue model and competitor analysis

There are no significant specific effects on revenue models for (Q)Timestamps and (Q)ERDS due to the eIDAS revision. Regarding (Q)ESeals and (Q)WACs, new revenue streams may emerge around the EUDIW, making existing business models more sustainable. However, the business models may come under pressure due to high regulatory costs, see [Chapter 6](#).

New revenue models are emerging for electronic signatures as a result of the eIDAS revision. Out of the new trust services, revenue models for electronic attestations of attributes will have the most impact on the market. A high level of competition is anticipated within this area.

Overall, there is increasing competition in the trust services market, partly due to the creation of a more European market. This trend is already evident and is expected to persist in the years ahead.

Across all trust services, there is limited recognition of the value of qualified vs. non-qualified. Without legal mandates enforcing the use of qualified services, there's a broad allowance for non-qualified alternatives. This scenario significantly strains the revenue models of qualified services.

7.1. New revenue models for QES

The revenue model for electronic signatures is shifting from a process-oriented approach to a means-oriented approach. Herein, the distinction between advanced and qualified signatures is important. The current market for qualified signatures in the Netherlands is limited in terms of professional certificates, as described in the previous chapters. The revenue models for these certificates will change to a small extent.

In the current advanced signature revenue model, companies pay a QTSP for the entire advanced signature process. The introduction of the EUDIW with an electronic signature certificate will eliminate this process and a different revenue model will replace it. The current revenue model will then partially disappear.

This will also create a new revenue model for QTSPs to issue electronic signature certificates to the EUDIW. The requirement for each member state to provide an EUDIW means that the government will likely absorb the cost of this. As this is an existing market, it is difficult for the government to argue that they should become QTSP themselves to issue these certificates. In that case, the government would be acting as a market participant, and to avoid distortion of competition, the government must abide by rules of conduct⁶⁵. There are broadly two options if the government does not act as QTSP:

1. The government conducts a tender procedure and selects one supplier. This creates dependence on one party to provide this service on a very large scale. It is unclear whether this is feasible for all current parties in the market.
2. The government conducts one or more tender procedures and selects multiple suppliers. Here, standardisation and interoperability (both technical and operational) are an important prerequisite.

Hence, winning one or more tenders is probably the main revenue model for trust service providers to issue electronic signature certificates (for citizens). Since there is still barely a market for citizen certificates, it is a new revenue model for trust service providers.

Use of QES by citizens for non-professional use should be free. Revenue models will emerge around the professional use of QES. QTSPs are expected to provide this service at a lower cost, as the costs associated with onboarding are reduced due to the utilisation of the EUDIW wallet for this purpose. A side effect of the introduction of the EUDIW is that citizens will become more familiar with electronic signatures. This is also expected to encourage the use of electronic signatures for professional use.

7.2. Revenue models related to electronic attestation of attributes

There is expected to be a lot of competition in the market for issuing (Q)EAA. It is believed that many authentic sources will outsource this process to QTSPs. Two types of revenue models are emerging in

⁶⁵ [Rijksoverheid](#)

this market for (Q)EAAs: 1) Revenue models for authentic sources issuing (Q)EAAs and 2) revenue models for QTSPs providing (Q)EAA services.

7.2.1. Competition for issuance of electronic attestation of attributes

Trust service providers offering (Q)EAA services will make these services available to authentic sources to issue (Q)EAAs. Authentic sources have three options on (Q)EAAs to issue:



Authentic source as a QTSP: An authentic source decides to become its own QTSP and to issue (Q)EAAs itself.



Authentic source with the help of a QTSP: An authentic source issues (Q)EAAs with the help of a QTSP that is allowed to issue (Q)EAAs. This can be done, for example, through outsourcing or by purchasing the services of a QTSP.



Open market for QTSPs: An authentic source would provide the data and multiple QTSPs could issue (Q)EAAs.

There is an additional option for government agencies. A government agency, if they follow the requirements of eIDAS, can issue its own QEAAs without being a QTSP (so-called Public EAAs).

It is still unclear which option is most desirable for which government agency. Outsourcing presents several benefits, including the delegation of application and audit processes to QTSPs, which relieves the government from bearing very specific regulatory costs. Additionally, the government can opt to centrally issue all (Q)EAAs or allow governmental agencies to make this decision independently.

It is likely that companies that manage an authentic source will outsource the issuance of (Q)EAAs, e.g. a bank as a resource for customer financial data. Generally, the costs associated with acquiring QTSP status for the sole purpose of issuing their own data are unlikely to justify the benefits. However, an exception may arise if an organisation prefers to independently safeguard the security and privacy of its data, thereby retaining full control over it.

It is expected that there will be a lot of competition in the market for QTSPs. The impression, based on the interviews conducted, is that many parties intend to become QTSPs for (Q)EAAs. As a result, QTSPs will compete to provide (Q)EAA services to authentic sources.

The liability associated with issuing (Q)EAAs remains ambiguous, pending further clarity from the implementing acts. Regardless of the acts, a persistent discrepancy exists between the legal framework and its practical application.

7.2.2. Revenue models for QTSPs

The most obvious revenue model for the QTSP is a monthly/annual fee that authentic sources pay for using the service of a QTSP, with possibly a variable component for the number of attestations. A QTSP is likely to offer *Software Development Kits* (SDKs) to authentic sources to ensure that the (Q)EAA service integrates seamlessly with existing applications and products of the authentic source. This will likely require integration (with customisation) between QTSPs and authentic sources. The revenue model is likely to vary per authentic source because accessing the data differs among sources. In certain instances, access to the authentic source is obligatory, while in others, it serves as an optional extra or is driven by compliance requirements.

An alternative revenue model involves a shared revenue structure between QTSPs and authentic sources. An example would be sharing revenue per (Q)EAA issued.

A third revenue model involves an agreement between the QTSP and authentic sources in which the QTSP buys the right to provide access to the authentic source's data to the wallet. Then the QTSP must arrange a revenue stream for the use of this data on behalf of the relying party. To this end, the readability of the attestation must be limited to a set of contracted relying parties. In this model, the

QTSP acts as a reseller of data from the authentic source. This revenue model is especially suitable for high-value data.

7.2.3. Revenue and cost models for authentic sources

The financial framework surrounding an authentic source can either be revenue-generating or cost-incurring, depending on the nature of the source. Unlocking data from an authentic source incurs expenses, primarily in establishing and upkeeping this supplementary channel. For authentic sources, three distinct financial models—either focused on revenue or costs—are conceivable.

Option 1: the holder/citizen pays

One approach for authentic sources involves the holder or citizen bearing the cost of acquiring a (Q)EAA. This concept is not new. Citizens currently already pay for various (government) services such as applying for a *Certificate of Good Conduct* (VOG), a Chamber of Commerce (KVK) excerpt, or a driving licence, see **Figure 35**^{66 67}.

Figure 35: Citizens already pay for various "attestations".



While not a groundbreaking revenue model, this approach could open up new revenue streams for authentic sources down the line. Future attestations might emerge that hold sufficient value to citizens, making them willing to pay for such services. Additionally, there could be instances where these attestations are so crucial to a third party that this entity opts to absorb the costs on behalf of the citizen requesting the (Q)EAA. A common example of this is seen in the case of VOG (Certificate of Conduct) applications processed before individuals join the workforce, where it's often the employer who bears the costs.

Option 2: The relying party pays

An alternative model involves the relying party bearing the cost for accessing attestations originating from authentic sources. This arrangement would necessitate restricting access to these attestations to a predefined group of contracted relying parties. The technical nuances of this approach are still under development. Essentially, a QTSP, either directly or on behalf of an authentic source, would issue credentials that are exclusively usable by contracted relying parties.

In this alternative approach, an authentic source has the option to provide (Q)EAAs to holders/citizens at no cost, while imposing a fee on relying parties interested in accessing these (Q)EAAs from citizens.

Option 3: The authentic source pays

In this option, the authentic source either absorbs the cost internally or integrates it into the pricing of another product. For instance, the expense associated with issuing a diploma (Q)EAA could be incorporated into the overall tuition fees.

⁶⁶ [KVK](#), [Justis](#), [CBR](#)

⁶⁷ Note: Cost of driving licences varies by municipality, on average this is €44.65

7.3. Revenue models for electronic ledgers

The broad definition of eLedgers allows for multiple types of revenue models for that service. These range from decentralised blockchains, such as Bitcoin, Ethereum and Solana, which charge a fee per transaction, to the traditional financial sector uses subscription models, among others. Therefore, no generic revenue model can be identified for eLedgers.

It's highly likely that only permissioned networks will qualify as QELedgers, where periodic revenue models are more straightforwardly applicable. These networks operate as centralised ledgers, making them similar to other Software as a Service (SaaS) offerings. In this setup, customers acquire the service or software from a QTSP, which then oversees its management. This contrasts sharply with decentralised ledgers, where network security and usability are maintained through incentives and game theory embedded at the protocol level. An example of this is the rewards system for mining a Bitcoin block and the effects of halving events on such incentives⁶⁸. In addition to periodic revenue models, a government subsidized QELedger may also be a possibility to cover its costs.

7.4. Revenue models for electronic archiving services

A subscription-based revenue model seems most logical for (Q)E-Archiving. A longer preservation period is involved here, so an annual fee with perhaps a discount for longer-term subscriptions would be desirable.

Another scenario suggests that a distinct revenue model for (Q)E-Archiving might not be developed. Instead, a range of QTSPs could evolve into one-stop shops, offering a suite of trust services. Within this context, (Q)E-Archiving would be integrated as an additional service, aimed at guaranteeing the long-term preservation, accessibility, integrity, and authenticity of information. The large-scale provision of these services by QTSPs could lead to economies of scale, thereby reducing costs. This model would not only streamline the user experience by consolidating services under a single provider but also enhance the value of (Q)E-Archiving by embedding it within a broader suite of trust services.

7.5. Value of qualified services is limitedly recognised

There is still very little recognition of the value that qualified trust services can provide in the Netherlands, both among public and private parties. As a result, current revenue models for qualified services are also still very scarce with minimal demand for these services.

The lack of recognition and awareness leads to confusion in the market, which encourages misuse of the eIDAS trust icon. Despite the icon being protected, QTSPs notice that there are unqualified parties using the icon. Some organisations display the "trust services icon" on their website and state that they are 'eIDAS compliant'. End users cannot distinguish the difference, so qualified services do not reach their full potential.

In other EU member states, qualified services are more recognised, partly because their use is mandatory in some cases according to national legislation. For instance, in Italy, all invoices must be signed with a qualified electronic signature, and in Austria and Germany, all payment terminals must have a qualified electronic seal. This obligation leads to a broader recognition of qualified trust services.

In the Netherlands, Organisations and governmental agencies work together to increase the recognition and awareness through the collaboration platform *Trusted Information Partners* (TIP). TIP enables parties to develop services that allow all citizens, companies, and governments to conduct digital transactions with each other easily and reliably. Within TIP, public and private partners collaborate and make agreements on the use of open standards. The Dutch Tax Authority and the Ministry of the Interior and Kingdom Relations are involved in TIP⁶⁹.

⁶⁸ Approximately every 4 years, the number of bitcoins put into circulation halves until the maximum of 21 million is reached. Half of the bitcoins not yet in circulation are put into circulation every four years.

⁶⁹ [Trusted Information Partners](#)

7.6. Competition increases due to the emergence of a European market

The anticipated revision of the eIDAS regulation is expected to enhance interoperability, paving the way for the development of a unified European market for trust services. This evolution will simplify the process for Dutch trust service providers to extend their offerings across other EU member states. Conversely, it will also lower the barriers for trust service providers from different member states to enter the Dutch market, thereby intensifying competition within the Netherlands. However, the prospect of increased competition is reduced by the likelihood that fewer companies become QTSPs. The stringent compliance demands associated with these services act as a substantial entry barrier, potentially deterring new participants.

Service providers from other EU member states currently enjoy a competitive edge over Dutch providers in the markets for QESeals and QES, primarily because they can offer the same services at significantly lower prices. This price advantage stems from several factors, including economies of scale achieved in their home markets, more intense competition, less burdensome legal requirements, and clearer regulatory guidance. In southern European countries, the use of QESeals and QES is already compulsory in many scenarios, further enhancing the demand and market maturity for these services.

However, this advantage is somewhat mitigated by the introduction of more stringent requirements with the eIDAS revision, particularly the necessity for a high Level of Assurance, a standard that many providers from other member states have yet to meet. Despite this, the competitive edge gained through cost advantage is expected to remain significant. The price disparities are stark, with services in some member states costing up to 15 times less than those in the Netherlands. This situation suggests that the regulatory tightening under the eIDAS revision might not sufficiently level the playing field for Dutch providers, given the substantial cost differences favouring their European counterparts.

In the European market, the risk of 'forum shopping' by QTSPs increases. This means that QTSPs strategically choose in which country to get certified/qualified to reduce costs and efforts, thereby building a stronger competitive position in Europe. Several factors can influence this strategic choice (not exhaustive):

- **Auditor costs:** The cost of auditors, who must also be accredited across Europe, varies by country and accreditation board. The duration and complexity of the accreditation process significantly impact the overall cost for the auditor, which, in turn, influences the audit costs for QTSPs. A longer and more complex accreditation process leads to higher expenses, making some countries more financially attractive for QTSPs seeking certification.
- **Role of supervisory body:** Regulatory frameworks and standards often provide room for interpretation, resulting in varying enforcement by different national regulators. This variation is particularly pronounced in cases where standards, such as those set by ETSI, reference 'Industry Best Practice.' Such references necessitate judgement calls by both the industry and regulators, leading to discrepancies in regulatory insight. These differences can make certification as a QTSP more challenging and costly in certain countries.

These factors underscore the strategic considerations QTSPs must navigate to optimise their certification journey within the European Union, highlighting the complex interplay between regulatory environments and business strategies in the trust service market.

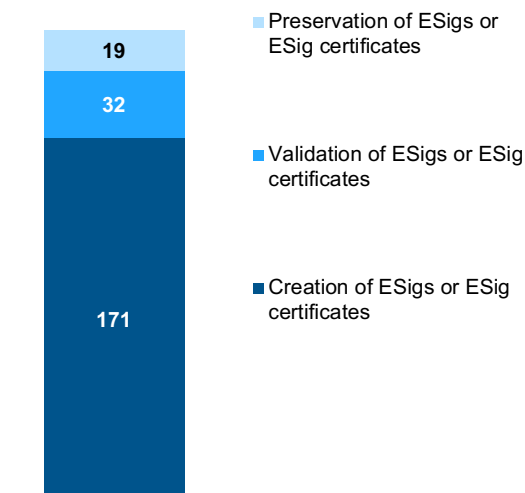
8. Appendix

8.1. Qualified trust services 1-pagers

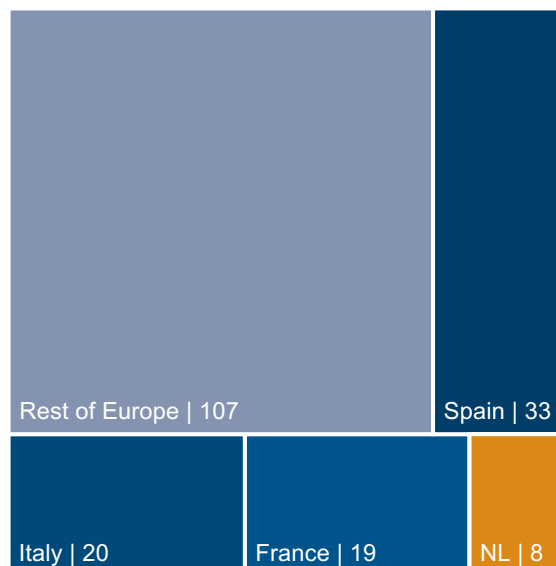
8.1.1. Electronic signatures 1-pager

Name	(qualified) electronic signatures
Abbreviation	(Q)ES
eIDAS articles	3, 25 – 32, 32a, 33, 34, ANNEX I, ANNEX II
Sub services	<ol style="list-style-type: none"> 1. Creation of eSig or eSig certificate 2. Validation of eSig or eSig certificate 3. Preservation of eSig or eSig certificate 4. Management of remote electronic signature creation devices
EIDAS definition	'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'
Goal	The purpose of an eSig is to create trust by enabling the digital signing of a document to endorse the signer's consent or specifically the authenticity and integrity of the document itself.
Dutch QTSPs that offer service	<ol style="list-style-type: none"> 1. CIBG 2. Cleverbase ID B.V. 3. Digidentity B.V. 4. KPN B.V. 5. Ministerie van Defensie 6. Ministerie van Infrastructuur en Waterstaat 7. NotarisID B.V. 8. QuoVadis Trustlink B.V.

QTSPs offering qualified electronic signature services



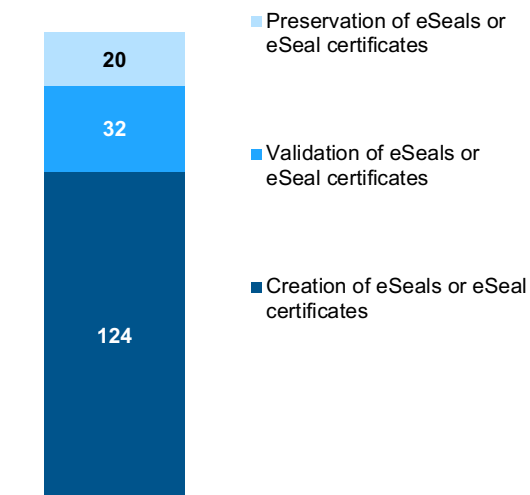
Number of qualified electronic signature QTSPs per country



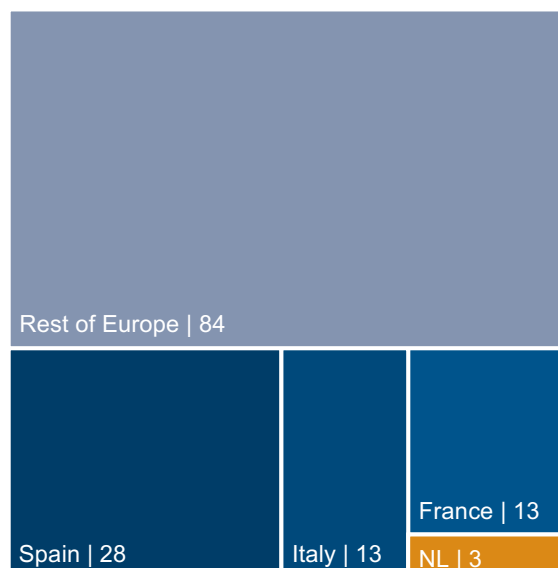
8.1.2. (Q)ESeal 1-pager

Name	(qualified) electronic seals
Abbreviation	(Q)ESeal
eIDAS articles	3, 35 – 39, 39a, 40, ANNEX III
Sub services	<ol style="list-style-type: none"> 1. Creation of eSeal or eSeal certificate 2. Validation of eSeal or eSeal certificate 3. Preservation of eSeal or eSeal certificate 4. Management of remote electronic seal creation devices
EIDAS definition	‘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’
Goal	The purpose of an eSeal is to create trust through the ability to digitally sign a document to endorse the consent of a legal entity or specifically the authenticity and integrity of the document itself.
Dutch QTSPs that offer service	<ol style="list-style-type: none"> 1. Digidentity B.V. 2. KPN B.V. 3. QuoVadis Trustlink B.V.

QTSPs offering qualified electronic seal services

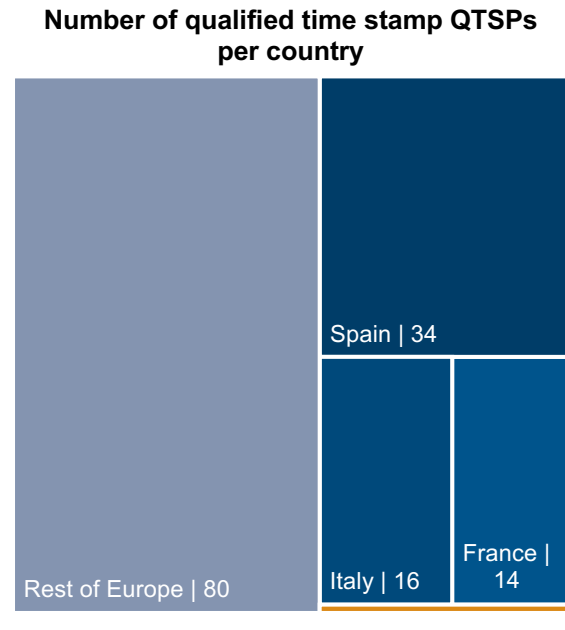
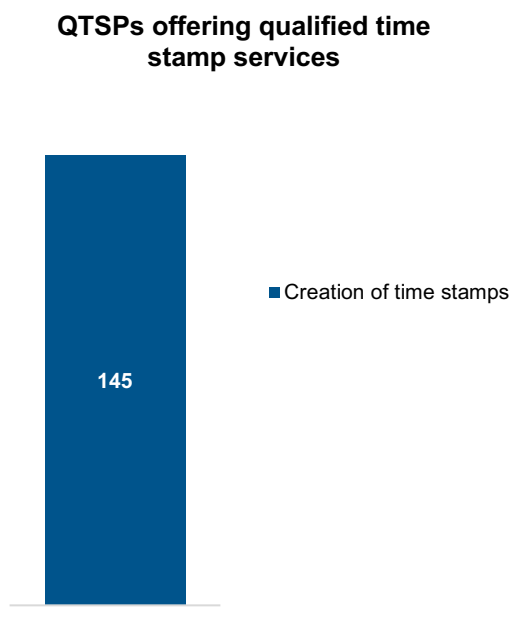


Number of qualified electronic seal QTSPs per country



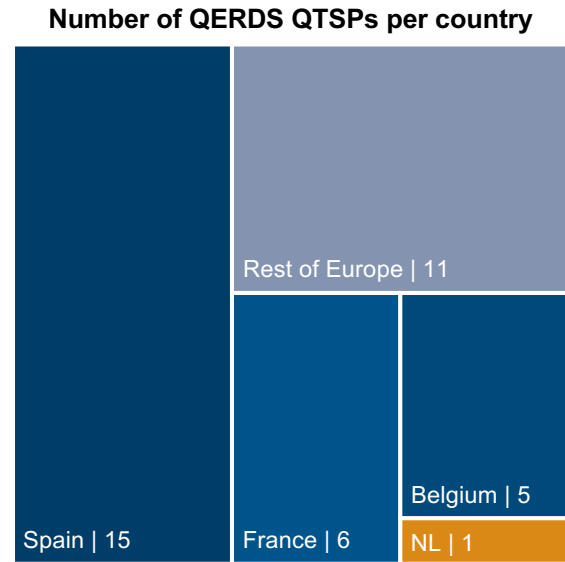
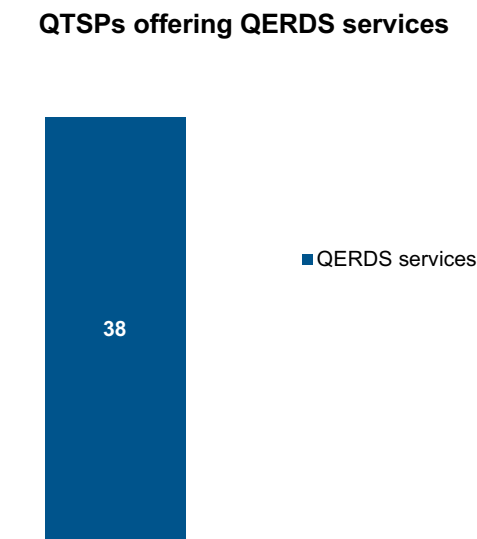
8.1.3. (Q)Timestamp 1-pager

Name	(qualified) electronic time stamp
Abbreviation	(Q)Timestamp
eIDAS articles	Articles: 3, 41, 42
Sub services	1. Creation of time stamps 2. Validation of time stamps
EIDAS definition	‘Electronic time stamp means an electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time’
Goal	The purpose of an electronic timestamp is to create trust by marking electronic data with a time and date that is thereby evidence of their existence or original version.
Dutch QTSPs that offer service	1. QuoVadis Trustlink B.V.



8.1.4. (Q)ERDS 1-pager

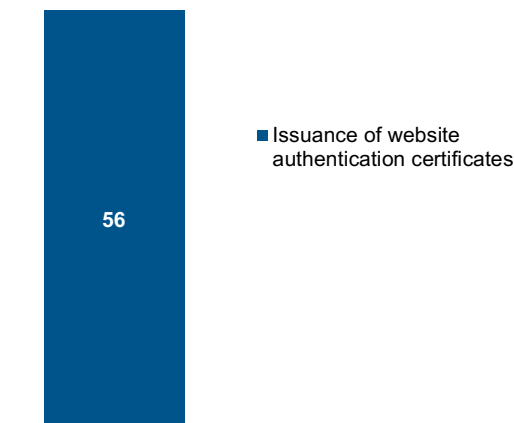
Name	(qualified) electronic delivery service
Abbreviation	(Q)ERDS
eIDAS articles	Articles: 3, 43, 44
Sub services	<ol style="list-style-type: none"> 1. Providing electronic registered delivery services 2. Validation of data sent via electronic registered delivery services
EIDAS definition	‘Electronic registered delivery service means 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’
Goal	The purpose of ERDS is to create trust by ensuring the secure transmission of data between different parties.
Dutch QTSPs that offer service	<ol style="list-style-type: none"> 1. Aangetekend B.V.



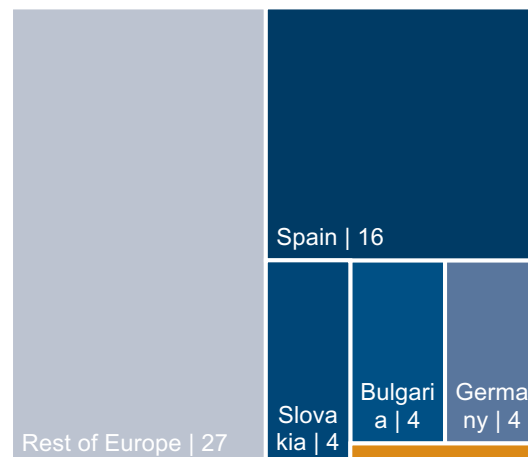
8.1.5. (Q)WAC 1-pager

Name	(qualified) website authentication certificates
Abbreviation	(Q)WAC
eIDAS articles	3, 45, 45a, ANNEX IV
Sub services	1. Issue website authentication certificates 2. Validate website authentication certificates
EIDAS definition	‘Certificate for website authentication means an electronic attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued’
Goal	The purpose of a (Q)WAC is to create trust by ensuring a secure connection between a natural or legal person and a website. In addition, a (Q)WAC creates trust about the identity of the entity behind the website.
Dutch QTSPs that offer service	1. QuoVadis Trustlink B.V.

QTSPs offering qualified website authentication certificate services



Number of qualified website authentication certificate QTSPs per country



8.1.6. (Q)EAA 1-pager

Name	(qualified) electronic attestation of attributes
Abbreviation	(Q)EAA
eIDAS articles	3, 45b, 45c, 45d, 45e, 45f, 45g, 45h ANNEX V, ANNEX VI, ANNEX VII
Sub services	1. Issuing electronic attestation of attributes 2. Validation of electronic attestation of attributes
EIDAS definition	'Electronic attestation of attributes means an attestation in electronic form that allows the authentication of attributes'
Goal	The purpose of a (Q)EAA is to create trust by providing digital evidence about a particular attribute possessed by a natural or legal person.

8.1.7. (Q)E-Archiving 1-pager

Name	(qualified) electronic archiving
Abbreviation	(Q)E-Archiving
eIDAS articles	3, 45i, 45j
Sub services	1. Electronic archiving services
EIDAS definition	“Electronic archiving’ means a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to guarantee their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period’
Goal	The purpose of electronic archiving services is to create trust by ensuring the integrity and originality of digital data for longer periods of time.

8.1.8. (Q)ELedger 1-pager

Name	(qualified) electronic ledger
Abbreviation	(Q)ELedger
eIDAS articles	3, 45k, 45l
Sub services	1. Store data in an electronic ledger
EIDAS definition	'Electronic ledger means a sequence of electronic data records, ensuring their integrity and the accuracy of their chronological ordering'
Goal	The purpose of an electronic ledger is to create trust by facilitating a tamper-proof digital record of data that ensures its authenticity and integrity in terms of date, time and chronological order

8.2. Glossary ENG – NL

English Term	Dutch Term
(Qualified) Certificate for electronic seals	(Gekwalificeerd) Certificaat voor elektronische zegels
(Qualified) Certificate for electronic signature	(Gekwalificeerd) Certificaat voor elektronische handtekening
(Qualified) Certificate services for website authentication	(Gekwalificeerde) Certificaten diensten voor websiteauthenticatie
(Qualified) Electronic archiving	(Gekwalificeerde) Elektronische archivering
(Qualified) Electronic attestation of attributes	(Gekwalificeerde) Elektronische attestering van attributen
(Qualified) Electronic ledgers	(Gekwalificeerde) Elektronische grootboeken
(Qualified) Electronic registered delivery services	(Gekwalificeerde) Diensten voor elektronische aangetekende bezorging
(Qualified) Electronic seals	(Gekwalificeerde) Elektronische zegels
(Qualified) Electronic signatures	(Gekwalificeerde) Elektronische handtekeningen
(Qualified) Electronic time stamps	(Gekwalificeerde) Elektronische tijdstempels
(Qualified) Management of remote electronic signature and seal creation devices	(Gekwalificeerd) Beheer van middelen voor het aanmaken van elektronische handtekeningen en zegels op afstand
(Qualified) Seal creation device	(Gekwalificeerde) Middel voor het aanmaken van elektronische zegels
(Qualified) Signature creation device	(Gekwalificeerde) Middel voor het aanmaken van elektronische handtekeningen
(Qualified) Trust services	(Gekwalificeerde) Vertrouwendiensten
(Qualified) Trust services providers	(Gekwalificeerde) Verlener van vertrouwendiensten
Advanced electronic seals	Geavanceerde elektronische zegels
Advanced electronic signatures	Geavanceerde elektronische handtekeningen
Authentic source	Authentieke bron
Conformity assessment body	Conformiteitbeoordelingsinstantie
Creator of a seal	Aanmaker van een zegel
Credential	Inloggegevens
Cybersecurity scheme	Cyberbeveiligingsschema
Digital Identity Wallet	Wallet voor digitale identiteit
Electronic documents	Elektronische documenten
Electronic identification scheme	Stelsel voor elektronische identificatie
Electronic seal creation data	Gegevens voor het aanmaken van elektronische zegels
Electronic signature creation data	Gegevens voor het aanmaken van elektronische handtekeningen
EU Digital Identity Trust Mark	EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit
Level of assurance	Betrouwbaarheidsniveau
Preservation service for electronic signatures	Bewaringsdienst voor elektronische handtekeningen
Relying party	Vertrouwende partij
Signatory	Ondertekenaar
Strong user authentication	Sterke gebruikersauthenticatie
Zero-knowledge proof	Zero-knowledge proof

8.3. List of abbreviations

Abbreviation	Term
AES	Advanced Electronic Signature
AESeal	Advanced Electronic Seal
BZK	The Ministry of the Interior and Kingdom Relations
DLT	Distributed Ledger Technology
DV	Domain Validation
e-Archiving	Electronic Archiving
EAA	Electronic Attestation of Attributes
eID	Electronic IDentification
eIDAS	Electronic IDentification, Authentication and trust Services
eLedgers	Electronic Ledger
EPREL	European Product Registry for Energy Labelling
ERDS	Electronic Registered Delivery Service
eSeal	Electronic Seal
eSig	Electronic Signature
ETSI	European Technical Standard Institute
EUDIW	European Digital Identity Wallet
EV	Extended Validation
EZK	The Ministry of Economic Affairs and Climate Policy
FIDA	Framework for Financial Data Access
HSM	Hardware Security Module
NFC	Near Field Communication
NIS2	Network and Information Security 2 directive
ODIW	Organisational Digital Identity Wallet
OV	Organisation Validation
PSD2	Payment Services Directive 2
PSD3	Payment Services Directive 3
PSR	Payment Services Regulation
QE-Archiving	Qualified Electronic Archiving
QEAA	Qualified Electronic Attestation of Attributes
QELedgers	Qualified Electronic Ledgers
QERDS	Qualified Electronic Registered Delivery Service
QES	Qualified Electronic Signature
QESeal	Qualified Electronic Seal
QSCD	Qualified Signature Creation Device
QSealCD	Qualified Seal Creation Device
QTimestamp	Qualified Electronic Time stamp
QTSP	Qualified Trust Service Provider
QWAC	Qualified Website Authentication Certificate
RDI	Dutch Authority for Digital Infrastructure
RP	Relying Party
SAM	Signature Activation Module
SES	Simple Electronic Signature
SESeal	Simple Electronic Seal
TIP	Trusted Information Partners
TS	Trust Services
TSP	Trust Service Providers
UZI	Unique Healthcare Provider Identification
VOG	Certificate of Conduct
WAC	Website Authentication Certificate
Wdo	Digital Government Act

Authors

For more information on INNOPAY's specialised expertise in trust services, digital identity or for additional information on this report, please contact:



Vincent Jansen

Vice President

Vincent.jansen@innopay.com



Jorrit Penninga

Manager

Jorrit.penninga@innopay.com



Leon Kluiters

Senior consultant

Leon.kluiters@innopay.com



Jeroen van der Hoeven

Consultant

Jeroen.vanderhoeven@innopay.com



Maurits Mulder

Consultant

Maurits.mulder@innopay.com



Pieter Verhagen

Senior manager

Pieter.verhagen@innopay.com