Brought to you by:

ENTRUST
SECURING A WORLD IN MOTION

The eIDAS (2.0) Regulation

for dummies®
A Wiley Brand

Understand eIDAS and eIDAS 2.0

Learn about qualified trust services

Prepare for EU Digital Identity Wallets

By Charlotte Pommier

Entrust
Special Edition

About Entrust

Entrust keeps the world moving safely by enabling strong identities, secure payments, and protected data. We offer an unmatched breadth of solutions that are critical to the future of secure enterprises, governments, the people they serve, and the data and transactions associated with them. With our experts serving customers in more than 150 countries and a network of global partners, it's no wonder the world's most trusted organizations trust us. For more information, visit **www.entrust.com.**

Entrust Digital Security Solutions

Entrust offers an unrivaled portfolio of solutions around identity, applied cryptography, digital certificate management and other advanced technologies to build resilient infrastructures of trust.

Entrust's range of high-assurance products for eIDAS covers Identity and Access Management, digital signing engines, PKI solutions, Hardware Security Modules (HSMs), but also qualified trust services such as electronic signatures, seals and timestamping.

Entrust HSMs

Whether deployed on-premises or as a service, Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations.

Entrust's unique Security World key management architecture provides strong, granular controls over access and usage of keys. For more information, visit entrust.com/HSM.

The eIDAS (2.0) Regulation

Entrust Special Edition

by Charlotte Pommier

for dummies®
A Wiley Brand

The eIDAS (2.0) Regulation For Dummies®, Entrust Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-29344-5 (pbk); ISBN 978-1-394-29345-2 (ebk); ISBN 978-1-394-29346-9 (ePub)

Publisher's Acknowledgments

Development Editor: Jen Bingham
Acquisitions Editor: Traci Martin
Senior Managing Editor: Rev Mengle
Client Account Manager: Jeremith Coward
Production Editor: UmeshKumar Rajasekhar

Table of Contents

Introduction

The very first version of this guide, which was released in 2017, started with, 'Everybody agrees that trading electronically is the future'. Just seven years later, and after a pandemic that dramatically pushed digital transformation forward, electronic trading pretty much feels like our present now.

According to Forbes, 5.35 billion people (around 66 per cent of the world's population today) have access to the Internet, and this number should reach 7.9 billion users by 2029. Digital-first is the new approach, and citizens, governments, and businesses increasingly rely on infrastructures of trust to exchange and transact daily.

Before 2014 many countries, including those in the EU, did their own thing. Each country was influenced by its own legal and data handling policies. Every country had some sort of trust service infrastructure, but many of them didn't recognise each other, particularly when it came to using electronic signatures. For example, a document (such as a contract) electronically signed in one person's home country could not be verified as being legally valid when read electronically in another European country. So, there was no joined-up process across the EU.

REMEMBER

The main point of having the EU is to allow for seamless cross-border activities, so having incompatible electronic trust service infrastructures was an important obstacle to overcome.

Fixing this problem was the objective of a 2014 EU regulation on Electronic Identification and Trust Services (commonly called eIDAS), which began taking full effect in EU member states in 2016. This regulation created consistent standards across the EU for electronic identities (eIDs), authentication, and signatures, ensuring compatibility no matter in which country a citizen resides, and which governments and businesses they are working with.

Almost ten years later (in 2024), the regulation was updated to improve some areas of the initial regulation, specifically around eIDs, and the use of eID wallets. It also introduced some new trust services. This update is commonly referred to as eIDAS 2, but the regulation name didn't change.

This book explains eIDAS (including the changes brought with eIDAS 2) and its consequences in simple, easy-to-understand terms, so even those with no prior knowledge can hopefully make sense of it all.

How This Book Is Organised

As with other *For Dummies* books, this book doesn't just assume that you'll begin on page one and read straight through to the end. Each chapter is written to stand alone, with enough contextual information provided so that you can understand the content.

Chapter 1: What Is eIDAS and What Is a Trust Service?

Chapter 1 explains the history and motivations for the 1999 Signature Directive, which was eIDAS's predecessor, and how it worked in some ways and fell short in others. This sets the stage for explaining how the eIDAS regulation replaced the directive and improved the adoption of trustworthy electronic services for all. You'll learn the basics of the eIDAS regulation, including its goals and the kinds of businesses and government agencies it affected. This chapter also outlines the changes brought by the 2024 amendment to the regulation.

Also in Chapter 1, you'll learn what a trust service is under the eIDAS regulation, the different types of trust services that are currently defined (including the new ones covered in the 2024 amendment), what a trust service provider (TSP) is, and the difference between qualified and nonqualified trust services.

Chapter 2: Electronic IDs and the EU Digital Identity Wallet

Chapter 2 looks at eIDs and trust services for authentication. First, the chapter explains the benefits of electronic identification and describes how eIDAS provides a bridge enabling EU countries to recognise each other's eIDs. You'll learn about the three assurance levels for electronic identification under eIDAS (low, substantial, and high) and the requirements for each.

The chapter also discusses the EU Digital Identity Wallet (EUDIW), a legal and technical framework that was brought by the 2024 update to eIDAS and that will enable governments to deploy standardised digital wallets for citizens to authenticate and transact online.

Chapter 3: Electronic Signatures and Seals: Click on the Dotted Line

Chapter 3 explores the field of electronic signature services, which are one of the many trust services defined by eIDAS, and which have seen good adoption rates across the EU and around the world. You'll find out what electronic signature are good for, and what standards are in place to make sure an electronic signature can be trusted across the EU. You'll learn about the three types of electronic signatures (simple, advanced, and qualified) and when each type is appropriate. You'll also find out about a variant of electronic signatures called a seal. These seals can be applied to documents from companies and other organisations, as opposed to electronic signatures, which are applied by individuals.

This chapter also compares the old-school way of digital signing with smartcards to the newer way (digital signing in the cloud from personal mobile devices), both in how they work and what standards apply to them.

Chapter 4: Building a Trust Service in the eIDAS World

Are you trying to assess whether you should work with a TSP or apply to become a TSP yourself? This chapter will help you understand what it takes to become a TSP, with a focus on infrastructure requirements for e-signatures. The chapter takes a deeper dive into hardware security modules (HSMs) and other related components that are part of a remote e-signature service aligned with eIDAS requirements.

Chapter 5: Five Ways Entrust Can Help You with eIDAS

In Chapter 5, you'll find five ways that Entrust can assist companies like yours, with building or using qualified trust services including qualified e-signatures, qualified website authentication

certificates (QWACs), qualified certificate for electronic seals (QsealCs), and qualified timestamping. The chapter also discusses professional advice and consultancy, commitment to the eIDAS standards, HSM certification compliance, qualified signature creation devices, the signature activation module (SAM), deployment of the EU Digital ID Wallets, and much more.

Appendix: Further Information

Sometimes the devil is in the details. This short appendix contains additional information that you may find helpful to reference, including the current timetable for implementing eIDAS, a framework of standards, and relevant information published online.

Foolish Assumptions

This book assumes that you understand some basics of computing, such as the general idea of secure transactions and the need to know whom you are dealing with when working remotely. However, the book *doesn't* assume you know anything about eIDAS or earlier regulations involving security standards, nor anything about trust services, TSPs, eID Wallets, or HSMs. The book lays all that out in simple terms that anyone can understand.

Icons Used in This Book

Throughout this book, in the margins, you'll notice some handy, helpful icons. Here's what they signify:

REMEMBER

The paragraphs next to this icon spell out the most vital concepts contained in these pages. They identify the key information to file away in your brain, even if you remember nothing else!

TECHNICAL STUFF

This icon points out information that you have no pressing need to know, but may find interesting anyway. If you choose to skip over it, it won't affect the knowledge you gain from this book.

TIP

This icon identifies time- or frustration-saving ideas to help you get your head around eIDAS or improve efficiency.

WARNING

Not to alarm you in any way, but sometimes you need to be wary of certain pitfalls in life. This icon highlights issues to be mindful of relating to eIDAS.

Where to Go from Here

Just start reading! You can use the description of the chapters in this Introduction as a guide. If you already understand the eIDAS regulation and want to skip straight to the solutions that Entrust provides, start with Chapter 5!

Beyond the Book

It's impossible to fit everything you need to know about the eIDAS regulation into a relatively short book. If you're looking for more information, head to `https://www.entrust.com/resources/learn/eidas`.

IN THIS CHAPTER

- Knowing what safeguards existed before eIDAS
- Looking into the basics of eIDAS
- Comparing the roles of trust and identity services
- Understanding what's already been achieved and what's still to come

Chapter 1
What Is eIDAS and What Is a Trust Service?

If you do business online in the EU – or you work with businesses or government agencies that do – you might have already heard about eIDAS (pronounced *ee-idass*).

REMEMBER

Electronic Identification and Trust Services (eIDAS) is a European regulation that was adopted in 2014 and took full effect in 2016. It's designed to create consistent regulations and standards across the EU for electronic identities (eIDs) and trust services that provide security and reliability for digital transactions by issuing, validating, or managing certificates, signatures, seals, timestamps, or other electronic data.

eIDAS ensures that electronic transactions are secure and trusted, no matter where they take place in the EU.

This chapter discusses some basic facts about the eIDAS regulation.

Stepping Back in Time: Before eIDAS

It's been common knowledge for decades now that electronic identification and trust services for authentication and signatures would eventually become ordinary, everyday

technologies in the EU. It has just been a matter of figuring out – as individual nations and as a coalition of EU member states – how to implement those technologies in ways that work for everyone.

eIDAS is actually not the first EU initiative to address trust services. The Electronic Signatures directive (Dir.1999/93/EC) was passed in 1999, which required that electronic signatures be considered the equivalent of written signatures in all member states.

This earlier directive had a narrower scope and allowed each country to take its own approach to implementation, whereas the eIDAS regulation enforces a common approach. Yes, each country had to accept digital signatures on documents, but they couldn't necessarily understand *each other's* signatures because they often had incompatible electronic signing systems.

In fact, according to the European Commission, the haphazard way that the directive was implemented across member states made it de facto impossible to conduct cross-border electronic transactions. Further, the wording of the directive assumed the use of technologies such as smartcards and USB sticks: In 1999 these were state-of-the-art but have largely been replaced today by more modern alternatives, like mobile devices and cloud services (see Chapter 3). Nor did the directive recognise that identification and authentication services other than electronic signatures could benefit from harmonisation across Europe.

As a result, the EU had an ongoing consistency problem with signatures. Things worked fairly well within individual countries, but when citizens or companies wanted to do business somewhere other than their home country, complications often arose. Generally, guidance was needed to ensure that all aspects of the infrastructure for secure electronic transactions could be implemented seamlessly across the EU.

The sidebar 'The complications of inconsistency' gives an imaginary example of the kind of frustrations this situation caused. Thousands of similar situations occurred each day across the EU before eIDAS, where the existing systems worked fine – until a national border was crossed. With more than two dozen countries, each with its own regulations, it was wishful thinking to imagine that each legislature would come up with compatible standards without some guidance. With every passing year, it became clear that an EU-wide regulation was needed.

THE COMPLICATIONS OF INCONSISTENCY

The year is 2013. Consider an EU citizen we'll call Max. Max lives in Austria, but while he was on a holiday in Finland a few years ago, he found a perfect little vacation cottage for sale. Max visited a bank in Finland and filled out the paperwork for a mortgage, and then headed back home to Austria, with the idea that he would finalise the transaction electronically later in the month. The trouble came when Max found out that the Finnish and Austrian government agencies and banking institutions used different methods of electronic identification and document signing. The Finnish bank wasn't able to authenticate Max's online identity or accept his digital signature remotely. As a result, Max and the Finnish bank had to shuffle papers back and forth via overnight mail, with Max having to visit a local banking office in Austria to find notary services to authenticate his signature. So much for the paperless world of the future, eh?

Understanding eIDAS

eIDAS is an EU regulation that establishes consistent standards for eID, authentication, and trust services such as e-signatures. However, the regulation is more than a law. It's a way of building business among 23 million small and medium enterprises (SMEs) throughout 27 EU member states (shown in Figure 1-1), enabling cooperation and growth within a single, secure, digital market.

The full name for eIDAS is: *Regulation (EU) No.910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC.*

In April 2024, the regulation was updated by *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.*

Whew! Is it any wonder we just call it eIDAS?

FIGURE 1-1: The member states of the European Union.

eIDAS sets high standards for providers of identity services and providers of trust services for authentication and signatures, which pushed up the level of security available to businesses and organisations. The amount of step-up needed varied among organisations and also among member states.

REMEMBER

In some member states, the existing regulations were not that different from those articulated in eIDAS, but in other member states there has been a steep upward climb for the security of many businesses and government agencies as they integrated their practices with compliant eID and trust service infrastructures.

Due to the significant harmonisation effort required, eIDAS was designed to be implemented in several stages, with implementing acts being released throughout the years and the expectation that when EU standardisation is fully implemented, all member states will comply with the same high standards.

WHAT'S IN A NAME?

A regulation is similar to a law that applies across all member states. A *directive* prescribes results to be achieved, but each member states must make its own law regarding the implementation.

Since 2014, some implementing acts have been released, but in 2021, the European Commission decided to start working on a full update of the regulation instead, which was adopted in 2024.

The eIDAS vision

So, what does the digital EU look like now that eIDAS is fully implemented? Here are some of the benefits:

- A citizen can use electronic signatures and other trust services across the EU.
- National eIDs are recognised equally in all member states.
- Citizens can use their eIDs and electronic signatures to transact business across Europe.
- Electronic documents are legally recognised in any EU member state, regardless of the member state in which it was written.
- Document seals and timestamps issued in any EU member state are considered valid in any other member state.

TIP

You can see how eIDAS simplified everyday life by watching a short film, 'Back to the efuture: eIDAS' online at `https://www.youtube.com/watch?v=szErHIwoDCU&feature=youtu.be`.

Who and what are impacted by eIDAS?

The eIDAS regulation impacts all providers of services that protect authentication and transaction processes over the public network. The regulation places specific requirements on their operation and their correct implementation, which are verified through the use of audits. eIDAS also requires that all government and public services in the EU recognise standard signature formats and pan-European identities. The trust provided by eIDAS affects just about any organisation that carries out transactions over the

public network, in particular transactions involving commercial or legal matters where it's important to be certain of the participants' digital identities and their activities.

These activities are collectively referred to as digital services supporting a single digital market. Examples include services associated with:

- Travel-related transactions such as car hire
- Tax and financial statements
- Pharmaceutical records
- Legal and insurance contracts
- Banking agreements, including investments and loans
- Business-to-business electronic invoicing
- New third-party payment services, which are opening up traditional banking
- Electronic delivery services, with proof of sending and receiving of data and protection from unauthorized alteration
- Securing access to public websites

The eIDAS regulation also applies to commercial services that require an EU identity, such as the so-called know your customer (KYC) services in banking. For example, any trust service associated with authentication and signatures falls under the eIDAS regulation.

REMEMBER

The individual consumer of these services doesn't have to worry about eIDAS compliance; the burden for compliance falls on the organisations that provide trust services to the public. So, to use the example in the sidebar 'The complications of inconsistency,' nowadays Max doesn't have to worry whether the banks he deals with in Austria or Finland are eIDAS compliant. Because the regulation applies EU-wide, he can assume that they are. The banks, on the other hand, carry the responsibility of ensuring their systems are compliant, so it's important that they work with an eIDAS-compliant trust service provider (TSP). You'll learn more about trust services and TSPs in the 'Putting your trust in trust services' section.

What the eIDAS regulation contains

In a complex regulation that dictates not only the desired effect but also how to achieve it, it can be helpful to break things down into multiple levels.

REMEMBER

The eIDAS requirements are specified in four levels:

- First is the regulation itself, which defines the basic requirements to be adopted across the entire EU. These requirements override any existing national regulations.
- Second comes a set of standards that have been recommended by experts in the industry as a practical way of meeting the regulation's requirements.
- Third, accompanying the standards are implementing acts, which either mandate or recommend the use of the standards. Published acts cover things like eID interoperability and assurance levels, lists of qualified TSPs (QTSPs), signature formats, and signature and seal creation devices. You can find more information about these acts in the Appendix at the end of this book.
- Finally, there are national rules that may extend or adapt nonmandatory standards to meet a nation's perspective. For example, some countries, such as Italy, accept registration via video link as being equivalent to face-to-face.

Shortfalls of eIDAS and the reason for eIDAS 2

In 2021, the European Commission published the result of their evaluation of the eIDAS regulation. In short, the evaluation showed that were was good success in deploying electronic signatures across the EU, but it also highlighted some limitations, especially around eIDs and authentication. They noticed the following issues:

- A lack of legal and technological guidance on how to properly share eID data. That's to say, there was no framework for disclosing only a specific part of an eID (for example: just to disclose a birth date, or last name and not the entire content of an eID)
- A lack of harmonisation of national ID solutions

- Difficulties for the private sector to deploy or leverage eID services
- Strong competition coming from Single (federated) Sign-On solutions from social media platforms such as Google, Apple, Facebook, LinkedIn, and so on

Following this analysis, the European Commission decided to work on an update of the regulation, typically referred to as eIDAS 2. They spent three years designing a more robust framework for generating identity information and sharing it safely.

eIDAS 2 was officially adopted in April 2024. The changes brought to the initial text are giving everyone in the EU a secure, digital version of their identity that's easy to use and accepted everywhere, with the added bonus of protecting their privacy and personal data. It's a big step towards a more integrated and digital-friendly Europe!

Exploring the Role of Identity and Trust Services under eIDAS

The eIDAS regulation has two key aspects: identity services, and trust services. These important services may be defined as follows:

- The first part covers eIDAS services for government-issued eIDs – in other words, proving that a person or company is who they say they are, using an identity issued by the government. The regulation doesn't require a single EU-wide identification scheme; however, it does require mutual recognition between national ID schemes. This is the part that was heavily updated with eIDAS 2, to ensure a better deployment of identity services. Chapter 2 covers eIDs and eID wallets specifically.
- The second part covers eIDAS trust services for authentication and signatures. These are various activities that ensure mutual trust – in other words, confidence not only in all parties' identities, but also that they're accountable for the actions taken. The trust services initially included electronic signatures, timestamping, website authentication, and registered electronic delivery. eIDAS 2 introduced new types of trust services, that are further described in this chapter.

European digital identity services

There are two big parts under eIDAS related to identity: eID services, which aim at verifying someone's identity electronically, and eID wallets, which enable citizens and organisations to store and share their identity data as part of digital transactions.

WARNING

eIDAS 2 is bringing a very important change in the way EU citizens can get and share their eID. The amended regulation says that every member country of the EU must provide their citizens – and businesses! – with a digital wallet to be used on their phone, where they can safely keep proof of their identity, like their driver's license or school diplomas.

These digital wallets, called European Digital Identity Wallets (EUDIWs), will give EU citizens access to all kinds of online services anywhere in Europe. They won't need to use other ways to log in or give away more personal info than necessary. Plus, and this is crucial, they get to pick what info they share and keep the rest private. For example, they can just share their birth year, or their last name, and not the content of their entire eID. Check out Chapter 2 to find out more about the EUDIW.

Putting your trust in trust services

As well as identity services, eIDAS provides guidance for trust services.

In the world of eIDAS, a trust service is a digital service, offered by a vendor called a TSP, that aims to make a digital transaction more secure. Since there are many ways to ensure the security of an online transaction, there are many types of trust services as well.

TRUST SERVICES: A QUICK EXAMPLE

Here's an example of a trust service in operation that most people are familiar with. When a business creates a secure website that people can log into, they typically employ a digital certificate issued by a certificate authority to verify the authenticity of their website. This gives users confidence that their sensitive information, such as credit card

(continued)

(continued)

numbers and account numbers, isn't being snooped on or stolen. Most organisations don't single-handedly set up and maintain their own trust services. Instead, they employ the services of companies called TSPs, which offer third-party services to help ensure the security of online transactions. A TSP is legally liable for any damage caused by its failure to comply with the regulation's security measures, so it's expected that a TSP will employ and demonstrate best practices.

Here is the list of trust services that the amended eIDAS regulation covers:

- **Electronic signatures and electronic seals:** These trust services provide a way to approve electronic documents, as an individual (signature) or an organisation (seal).
- **Timestamps:** This trust service appends the exact date and time on an electronic document, like a rubber stamp on a paper document.
- **Website authentication:** This trust service issues digital certificates for websites, and more specifically, for domain names. The certificates are used to authenticate the owner of the website/domain. If you're familiar with TLS/SSL certificates, they're the same format, they follow the extended validation (EV) guidelines from the CA/Browser Forum and work pretty much the same way.
- **Registered e-delivery:** This trust service provides the digital equivalent of sending a registered letter with tracking and acknowledgement of receipt.
- **Electronic archiving:** This trust service provides a digital archiving vault to keep records in a way that won't damage them over time and that will retain their legal value.
- **Electronic ledgers:** This trust service provides an official (legally recognised) and secure way to record information (typically digital transactions and agreements), just like a notary would.
- **Management of remote electronic signature- and seal-creation devices:** This may be the least obvious trust service, because it's designed for TSPs and not for citizens

and businesses. This trust service enables e-signature vendors to manage digital signing and sealing processes remotely, in a way that is secure, and that ensures the signatories retain full control of the signing process even if they aren't physically performing the signature.

- **Issuance of electronic attestations of attribute (EAA):** This trust service enables the issuance of EAA, which are then stored in a digital identity wallet. An EAA is like a digital stamp of approval that confirms that a piece of information is true. You can learn more about EAA in Chapter 2.

The last four trust services are new additions from the 2024 amendment to the eIDAS regulation.


TIP

Every trust service includes issuance/management of the services, but also their validation (which means, verifying the authenticity of the service provided, for example, an e-signature, an electronic attribute, and so on).

Trust services and qualified trust services

The eIDAS regulation makes a distinction between trust services and *qualified* trust services to establish different levels of security, reliability, and legal recognition for digital transactions within the EU. In other words, every trust service listed in the previous section can have a qualified status or not.

The purpose of having these two types is to give people and businesses options based on their needs:

- For standard, noncritical online transactions, you can use a regular trust service.
- But if you're dealing with transactions that are very important, such as signing or sealing critical documents, you'd want the extra assurance of a qualified trust service.

Qualified trust services must meet strict EU standards and are provided by organisations that have been officially checked and approved by a supervisory body. This means when you use a qualified trust service, you can be confident that your digital transaction is safe and will hold up legally, just like if it was an in-person transaction.

TSP: QUALIFIED OR NOT QUALIFIED?

It's not uncommon for a TSP to provide more than one trust service. Many services including electronic signatures, electronic seals, time-stamping, and website authentication currently rely on the same technology, called public key infrastructure (PKI). So, it makes sense for a TSP to leverage the infrastructure they build for more than one use case. And it's also possible for a TSP to offer both qualified and non-qualified trust services.

And that's where it can become confusing. For example, a QTSP can provide qualified certificates for website authentication, and also non-qualified timestamping services.

So, what matters in the end, is not whether an organisation providing a trust service claims to be a QTSP, but rather if the trust service they provide is qualified or not!

You can check out Chapter 4 to learn more about QTSP requirements.

WARNING

The eIDAS regulation provides a strong legal and technical framework for these trust services, but the objective of this regulation isn't to tell you under which case you should use a qualified, or non-qualified trust service. It's rather up to governments, industries, and associations to recommend or enforce certain types of services.

TIP

The European Commission maintains a list of all the active TSPs in each member state, with the details of their accreditations (for example, which trust services they have been authorised for, and whether they're qualified or not). The list is available at: `https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home`.

IN THIS CHAPTER

- Moving from paper to electronic IDs
- Examining electronic identification levels
- Getting to know the EU Digital Identity Wallet

Chapter 2
Electronic IDs and the EU Digital Identity Wallet

This chapter explores the first major framework covered by the Electronic Identification and Trust Services (eIDAS) regulation: electronic identity (eID) services (the second one, if you don't remember, is trust services).

All EU member countries except Denmark and Ireland currently offer a form of national ID card to their citizens. EU citizens are therefore accustomed to carrying a paper or plastic ID card with them wherever they go. But what if where they go is online? As technology has advanced, more and more activities that used to rely on in-person visits to stores, government offices, and financial institutions can now be handled online, as long as the participating parties can be confident of each other's identities.

This chapter examines the past, present, and future of eIDs, and explains how they fit into the eIDAS regulation. This chapter also discusses the EU Digital Identity Wallet (EUDIW), a new service described in the revised eIDAS regulation (sometimes called eIDAS 2) that was adopted in April 2024.

No Paper, Please! eIDs

For any type of online communication, each party wants to be assured that the unseen person or business on the other end is who they say they are. The level of assurance required depends on the importance of the communication and the consequences involved in being mistaken or deceived.

WARNING

For sensitive matters, such as governmental activities like tax filing and voting ballots, a simple username and password might not be sufficient to prove identity. For these kinds of transactions, different measures have been employed by various EU member states to validate someone's identity online by issuing an identity assertion that positively identifies a legal or natural person. Each member state maintains the identity information for its citizens.

Electronic Identification under eIDAS

Under the eIDAS regulation, a citizen's eID must be recognised equally well in any member state. This cross-recognition requirement applies to all government services, including healthcare and tax registration, as well as to any business services that use official government-issued IDs to validate identities, such as banks, car-hire services, and airlines. Although eIDAS mandates mutual acceptance of eIDs only for public-sector activities, not private-sector ones, businesses that want to confirm a customer's identity (for instance to meet Know Your Customer requirements) can use government-issued electronic eIDs, both for their own convenience and to provide the highest level of customer service.

REMEMBER

eIDAS establishes three assurance levels for electronic identification:

- **Low:** This level of identification gives only a small amount of confidence that a person is who they say they are. This level does, however, require some rules and controls to help reduce the risk of someone misusing or changing the identity information.
- **Substantial:** This level gives a good amount of confidence that a person is who they say they are. This level also requires specific technical rules and controls that greatly reduce the risk of someone misusing or changing the identity information.

» **High:** This level gives a very high level of confidence that a person is who they say they are. It uses strict technical rules and controls to prevent anyone from misusing or changing the identity information.

Depending on the required level of assurance, different methods for identity proofing and verification can be used, with more or less security assurance but also more or less friction. A high level of assurance requires a more stringent verification of the user; for example, signing up for an online newspaper might not need very high security. But for more important matters, like online banking or filing taxes, the organisation providing the service needs to be very sure you are who you say you are.

Having multiple levels helps balance convenience and security, ensuring that both everyday and sensitive transactions can be protected appropriately. The identity proofing methods to obtain the different levels of assurance are covered in the Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015.

Existing eIDs in member states

Most EU member states have adopted a form of eID system based on one or multiple levels of identity assurance as described in the previous section. These ID systems typically consist of a chip-enabled plastic ID card that can be presented in person at a government office or read using some sort of card-reader or chip-reader hardware on a computer. But some members have also deployed a fully digital ID service, such as Italy's Public Digital Identity System (SPID).

Some private organisations have also designed eID schemes that have been recognised by governments, like Itsme in Belgium, which came from a consortium of four Belgian banks. Their mobile app was officially recognised by the Belgian government and is based on a high level of assurance.

Each member state must accept eID schemes from other member states that match the requirements of one of these levels. For example, Belgium and Estonia can mutually recognise each other's identity schemes. As a result, a citizen in Belgium can access an Estonian government service that requires high

assurance identity verification, such as using her smartcard to establish her citizenship ID.

In practice, though, recognition between countries was a little bit complicated because the initial eIDAS regulation that took effect in 2016 didn't provide enough standards and framework for interoperability. This is one of the major reasons why the European Commission decided to work on an amendment of eIDAS in 2021 – see the following section.

eIDAS 2 and the Birth of the EUDIW

The increased usage of eIDs and the continued development of online identities contributed to the emergence of new problems that eIDAS wasn't able to fully cover with the 2014 regulation. In 2021, a pan-European survey around eIDAS organised by the European Commission identified some of the weaknesses of the regulation and the pain points that needed to be addressed in order to encourage the adoption of EU eIDs even further. The European Commission started then working on what is referred to as eIDAS 2, an updated version of the current regulation.

The three main fixes highlighted by the European Commission for eIDAS 2 were to:

- **Open trust services to the private sector:** Most use-cases for the 2014 version of eIDAS were designed for the public sector, making access to private providers too limited and complex. This notably led to the increased use of competing solutions from the private sector, such as Single Sign-On solutions from social media platforms.
- **Reinforce data privacy and security around eIDs**: The 2014 eIDAS technical and legal framework wasn't designed to allow for discretionary/selective disclosure of eID information. That's to say, citizens couldn't limit the sharing of their eID information to what was strictly necessary (for example only their birthdate or only their last name).
- **Provide a stronger framework for national eIDs:** The use of divergent national ID solutions was causing a fragmentation of the EU market, making cross-border recognition of eIDs much harder.

Two key elements of these efforts were:

- The creation of three new trust services (see Chapter 1).
- The creation of a legal and technological framework to design an EUDIW which would facilitate secure exchange of identity information and other electronic attributes, such as medical certificates or professional qualifications within the EU.

What is the EUDIW?

The EUDIW is a digital tool introduced as part of eIDAS 2. It works like a personal wallet in a smartphone that you can use to safely obtain, store, and share important digital documents about yourself, including your eID, passport, or even driver's license. It's also designed to be used to digitally sign or seal documents.

To be more specific, the EUDIW can store two types of data:

- **Identity data,** which creates a citizen's digital ID. Contrary to a scanned passport for example, a digital ID in a wallet stores every piece of information separately: first name, last name, date of birth, address, and so on. This enables selective disclosure of information.
- **Digital documents,** also called credentials, or electronic attestation of attributes (EEA), bound to the citizen. They can be qualified (see Chapter 1), especially if they have an official aspect, such as a diploma, a certification, or a prescription. But they can also be non-qualified when they're less sensitive documents: train tickets, memberships cards, and so on.

The EUDIW is designed to simplify EU citizen's lives. For example, it can be used to provide the documents needed to open a new bank account, to enroll in a university abroad, or to apply for a job. With the EUDIW, it becomes easier for public and private organisations to offer online services across Europe because the wallet means that secure authentication will be available to every individual in the EU. Each member state will offer at least one version of the EUDIW, built to the same common specifications. So, it's a safe, reliable, and private means of digital identification for everyone in Europe.

WHAT'S IN IT FOR EU CITIZENS?

Here are some examples of activities that EU citizens can do remotely, in a secure and privacy-enabled way, using EUDIWs:

- Access online services, both in the public and private space. For example, accessing an eGov platform, opening a bank account, declaring taxes, registering a SIM card, and so on.
- Store important credentials including passports, visas, credit cards, health insurance cards, certifications, prescriptions, diplomas, degrees, and so on.
- Provide proof that they have a valid driver's license, a valid accreditation, that they are 18 or older, and so on, without having to disclose more than what is required.
- Sign documents including agreements, contracts, statements, and so on.
- Authorise transactions, payments, bank transfers, and so on.

You can watch a short introductory video about the EUDIW here: `https://www.youtube.com/watch?v=AynHulTaafk`.

REMEMBER

The introduction of selective disclosure is a real game changer for EU citizens' right to privacy. The way the EUDIW is designed enables users to choose exactly which detail of their eID or document they want to share with the party they're interacting with. For example, when required to prove their age, a citizen can decide to only share the birth year indicated in their passport, instead of having to share all of their passport information. This mechanism helps to limit the risk of losing control of your personal information.

TIP

EUDIW are available for both people and organisations. This means that businesses also get their own place to store identity and documents and share them with other organisations or people, under the same interoperable framework.

Organisations also need to authenticate or prove things, so the EUDIW enables them to store relevant information such as a business registration number, VAT number, headquarters address, and also accreditations or certifications.

How does the EUDIW work?

The technical infrastructure behind the EUDIW is designed to be secure, interoperable, and user-friendly. Here are its key components:

- **Common specifications:** Every EU member state will be required to offer at least one EUDIW to its citizens, residents, and businesses. To make wallets work seamlessly across borders, every member state will rely on a common set of standards and specifications to build their wallets. These common specifications for the EUDIW will be referenced in implementing acts (legislative texts), making them mandatory for all wallets across all EU member states.
- **EUDIW Toolbox:** The Toolbox provides the technical specifications that power the EUDIW. It includes:
  - **The Architecture and Reference Framework (ARF):** The first version of the Toolbox, containing a draft version of the ARF, was published on 10 February 2023. It contains a high-level overview of the standards and practices needed to build the EUDIW. New versions of the Toolbox are being developed continuously through the ongoing work of the eIDAS Expert Group using feedback from the Large-Scale Pilots.
  - **Reference Implementation:** The EUDIW Reference Implementation is a reference implementation that forms the blueprint needed to build the wallet. It consists of code libraries and a reference application that is made publicly available and ready to be used by member states and stakeholders to build their own wallets. The Reference Implementation is built by the Commission and based on the requirements defined in the Architecture and Reference Framework

Who provides what exactly?

Several parties are involved in creating and using EUDIWs:

- **EU member state governments** are required by the eIDAS regulation to provide at least one EUDIW to their citizens. eIDAS regulations mandate EUDIW providers to distribute and support the wallet applications across the country.

- **EUDIW providers** have a contract with EU member state governments to provide EUDIW applications for citizens.
- **Credentials issuers** have the authority to issue verifiable credentials in the EUDIW (also called electronic attestations of attributes), either digital identity data or digital documents. They may be qualified TSPs and therefore able to issue qualified data and documents.
- **Service providers** can be public or private, and provide a service for citizens or customers. They require citizens or customers to provide credentials in order to access the service and can also ask credential issuers to generate verifiable credentials for their specific service.

In the eIDAS regulation, a service provider that wants to leverage EUDIW attributes as part of their service is called a *relying party*. All relying parties need to be registered under their government and declare their intended use of the EUDIW, the type of data they will be requiring from users/businesses through EUDIWs, and the reason why they require this data. At the time of writing (October 2024), the implementing act that clarifies the technical specifications procedures for this declaration system has not been published yet.

AN EXAMPLE

Ana is German and has an EUDIW installed on her smartphone, provided by the German government's selected EUDIW provider. The EUDIW contains her digital ID.

Ana is studying in France, and she goes to a local library (a service provider) for the first time, to borrow a book.

- Because Ana is a new customer, the library invites her to register for a membership using a self-service booth.
- The self-service booth is connected to a credentials issuer that invites Ana to scan a QR code, which triggers her EUDIW.
- The EUDIW on her smartphone prompts her to authorise the disclosure of her first name, her last name, her email address, and her birth day and month to the library (the relying party). She accepts.

- With the collected data, the credentials issuer acting on behalf of the library, generates a new credential that is added to her EUDIW: the library's membership card.
- When Ana goes to the library's reception and asks to borrow a book, the librarian will invite her to scan a QR code to confirm her membership. When Ana scans the QR code, it triggers her EUDIW again, which will prompt her to authorize the disclosure of her membership card number to the library.

And voilà! At no point was Ana required to disclose her country of residence, and the fact she uses a German EUDIW in France didn't change anything to the process or cause any trouble.

When will the EUDIW be available to EU citizens?

The EU was quick to get things started: Four large-scale pilots were launched a full year before the EUDIW was officially voted in! They were launched in April 2023 even though the amending regulation to eIDAS that defined the EUDIW entered into force a year later, in May 2024.

By May 2026 (24 months from the date the amending regulation was voted) all EU citizens shall be given the option to use a form of EUDIW by their EU government.

REMEMBER

Although eIDAS mandates every EU government to provide at least one EUDIW to their citizens, it's important to remember that EUDIWs will remain optional to citizens.

TIP

Although eIDAS 2 was adopted in May 2024, EUDIWs are unlikely to be available before May 2025 at best. There are still a lot of technical details that need to be confirmed via an implementing act, and the deadline for the European Commission to publish the first implementing act is May 2025.

IN THIS CHAPTER

- Finding out more about electronic signatures, seals, and timestamps
- Understanding the different levels of electronic signature
- Checking out the old and new ways of signing
- Discovering what timestamping is and does

Chapter 3
Electronic Signatures and Seals: Click on the Dotted Line

The Electronic Identification and Trust Services (eIDAS) regulation defines a good amount of trust services in addition to eID services. This chapter focuses on the trust services provided by trust service providers (TSPs) that have received the most attention and for which standards have been defined via implementing acts: electronic signatures, electronic seals, and electronic timestamps.

The Electronic Signatures Directive of 1999 is an EU directive that required electronic signatures be considered the equivalent of written signatures in all member states (for more on this, see Chapter 1). Its original authors thought that this directive was going to create a surge in electronic signature usage across the EU, but that didn't happen. One reason was the lack of cross-state compatibility (which eIDAS takes care of), but another was that

the world wasn't ready for it yet. People were still entrenched in the idea that paper signatures were better or more reliable. With the rapid digital transformation that has taken place in recent years across business functions, electronic signatures are now widely seen as a must-have.

Discovering Uses for Digital Signatures

It's easy enough to say what an ink signature on a paper document is good for, right? It signifies the signer's agreement with the document, whether that document is a financial document like a mortgage loan or an estate-planning document like a power of attorney agreement. Signatures don't have to be as formal as all that, though; you might sign a credit card charge receipt at a restaurant, or sign a business letter, without giving it much thought.

A signature is only as good as the confidence you have that the person who signed is the actual person. For low-importance signatures, the signer's identity doesn't matter too much. For example, when a delivery driver comes to your door with a package, he usually doesn't care if you're the package recipient or not when he asks you to sign the delivery document. But for documents that trigger the transfer of financial assets, identity verification is imperative. That's why some important documents require a form of identity verification, to signify that a responsible party checked the signer's ID.

With an electronic signature, you don't, of course, have a trustworthy human comparing the picture on the signer's ID to their physical features, so there has to be another way of verifying the signer's identity. There are many ways to gather proofs of the identity of a signatory, but arguably the most developed technology today that can gather such proofs is digital signing. It's important to know this because the highest level of signature assurance defined by eIDAS (described in the following section) currently relies on digital signing. So, to talk about electronic signatures under eIDAS, you must talk about digital signing.


TIP

For more on digital signing, public key infrastructure (PKI), and cryptographic keys, see the 'A Quick Primer on Digital Certificates, Public Keys, and TSPs' section.

DIGITAL SIGNATURE VERSUS ELECTRONIC SIGNATURE – WHAT'S THE DIFFERENCE?

An *electronic signature* or e-signature can be any kind of electronic record, including an email message or word processing document. An e-signature is a generic term referring to the legal concept of giving consent to something.

A *digital signature* is a specific type of electronic signature that uses a digital certificate (a form of credential representing a natural or legal person) issued by a TSP after they have verified the signatory's identity. However, don't rely on all documentation to adhere to that distinction; the terms are often used interchangeably.

The purpose (and benefit) of a digital signature is to provide assurance that a document hasn't been modified after it's been signed and that it comes from an identified person. This is where digital signatures are actually better (that is, more tamper-evident) than ink-on-paper or basic electronic signatures. That's because a TSP certifies that the digital certificate used to create the signature belongs to the identified individual: The signature created using the cryptographic key associated with the certificate authenticates the signer and ensures that changes to a document are detectable.

Exploring eIDAS Electronic Signature Levels

Just as differing levels of physical signature verification are appropriate in different situations, there are also different digital signature levels. The eIDAS regulation defines three types of electronic signatures:

- Basic electronic signatures
- Advanced electronic signatures
- Qualified electronic signatures

Each level comes with its own set of requirements, as shown in Figure 3-1.

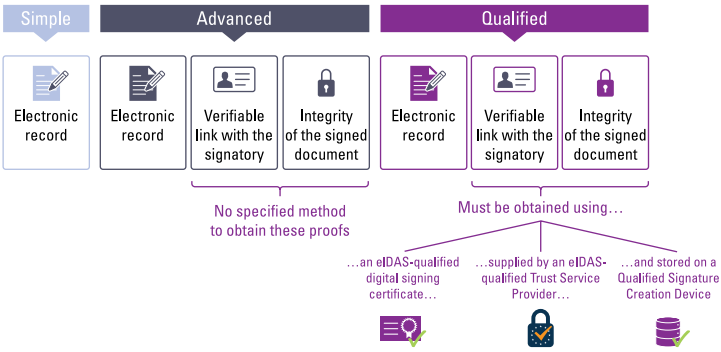

FIGURE 3-1: The three levels of electronic signatures defined by eIDAS.

WARNING

eIDAS doesn't make a distinction between digital and electronic signatures — everything is called an electronic signature (or seal), whether it's based on certificates or not. This is because the authors of the regulation wanted to remain as technology-agnostic as possible.

However, due to the prevalence and interoperability of PKI, a lot of advanced electronic signatures and all qualified electronic signatures are based on digital certificates; so, they're technically digital signatures. An advanced electronic signature is less stringent than a qualified electronic signature. An advanced electronic signature, at the minimum, must be:

- Uniquely linked to the signatory
- Capable of identifying the signatory
- Created in a way that ensures the signatory can maintain sole control
- Linked to the data it relates to in such a manner that any subsequent change to the data is detectable

A qualified electronic signature is a special type of advanced signature (issued by a qualified TSP or QTSP) that must meet all

the requirements for an advanced signature listed above, and in addition must be created by a qualified signature creation device (QSCD), such as a smartcard or a hardware security module (HSM). The QSCD must be certified as compliant with the requirements of the eIDAS regulation, and its dedicated implementation ensures that:

- The private key of the signatory remains under his sole control
- The generated signature creation data are unique, confidential, and protected against forgery
- Management of the signature creation data is a responsibility of a QTSP

QTSPs themselves must be audited by an accredited organisation and comply with the requirements of the eIDAS regulation. The next chapter provides more details about these requirements, notably around how to obtain a QSCD.

An eIDAS qualified electronic signature has the highest level of assurance and recognition, but it requires you to work with a QTSP that can provide qualified certificates in QSCDs. An eIDAS advanced electronic signature doesn't have the same constraint, although it has a specific definition that includes four explicit requirements.

TIP

It's also worth noting that eIDAS recognises even the most basic electronic signatures, as long as there is a form of electronic data recorded.

TECHNICAL STUFF

A qualified electronic signature is assumed to have at least the legal equivalence of a handwritten signature. Out of the three types of signatures defined by eIDAS, it's the only one that lays the burden of proof with the party that disputes the signature. In other words, if someone wants to dispute a qualified electronic signature, it's up to them to prove that something is wrong with it. On the other hand, in case of dispute with an advanced or a simple electronic signature, it is up to the service provider to demonstrate that the signature is valid.

HSM? SMARTCARD? QSCD?

When using PKI technology, secure hardware is an absolute must-have, because the cryptographic keys used with digital certificates are just like passwords: They must be stored in a very secure place that only the right person can access. One example is the nShield Connect HSM (see the accompanying figure).

There are several types of secure hardware that can be used for this purpose:

- Smartcards are physical cards with a chip. They can be inserted into devices to read their content. Smartcards are designed to hold cryptographic keys.
- Some USB tokens can also contain cryptographic keys. They're typically called secure USB tokens.
- HSMs are hardened, tamper-resistant hardware devices that can generate, protect, and manage keys used for encrypting and decrypting data and creating digital signatures and certificates.

eIDAS is technology-agnostic, so it doesn't mention HSMs specifically. Instead, the regulation talks about QSCDs. But the technical references listed in the eIDAS implementing acts refer essentially to HSM standards, especially for remote signing, which you'll learn more about in the 'Remote Signing: The New Way' section.

Gaining the (Electronic) Seal of Approval

Sometimes, it's more appropriate for a company or organisation, rather than an individual, to approve a document. For example, when a nonprofit organisation publishes its by-laws, those

by-laws are a product of the entire board of directors, with no one particular person as the author.

The eIDAS regulation introduces the concept of an *electronic seal* that can be used in situations where individual signatures aren't suitable. An electronic seal is similar to an electronic signature, in that it uses the same technology – you will actually hear about digital seals in most cases. Like electronic signatures, electronic seals can be either advanced or qualified. However, an electronic seal has a different legal meaning, in the following ways:

- The source of an electronic seal is generally assumed to be a legal entity or organisation, whereas an electronic signature comes from an individual.
- Seal creation is under the control of one or more individuals authorised to represent the organisation. (Recall that with individual electronic signatures, being under individual control was a defining hallmark of the technology.)
- Seals don't provide the same legal indication of intent by an individual, but they do provide assurances as to the authenticity of information provided by the business.

Whereas an electronic signature is specifically for legal signatures, an electronic seal is concerned with authenticity and integrity of a document or transaction. Sealing has quickly become important for business-to-business exchanges, such as order processing and invoicing, and business-to-consumer exchanges, such as issuing receipts. Recently, the European banking industry adopted the use of electronic seals, supported by qualified certificates, to secure open-banking transaction for the new third-party payment services that interact with banks on behalf of banking customers (see the 'Payment Services Directives' sidebar).


TIP

Electronic seals have proved to be useful tools. Although electronic seals are a new legal concept in many EU countries, they're becoming increasingly popular for securing business transactions, and even for closing electronic documents once all parties have signed. The properties of digital signing also apply to digital sealing: After sealing, documents become tamper evident, so it's a convenient way to prevent unwanted modifications to an already signed document.

WARNING

Because a digital seal is generated exactly the same way as a digital signature and has the same properties, this also means that the underlying technical requirements for seals and signatures are the same. (Chapter 4 lists out requirements and certifications).

PAYMENT SERVICES DIRECTIVES

This sidebar gives a quick overview of the two Payment Services Directives so that you're familiar with the basics given there is a strong overlap with eIDAS. In 2007, as a reflection of the growing e-commerce industry, the European Commission (EC), the European Banking Authority (EBA), and their advisory bodies recognised a need to offer consumers a wider choice of payment services by encouraging non-bank financial institutions to enter the market for consumers while enabling faster payments and increasing consumer protections and transparency. This led to the publication of the first Payment Services Directive (PSD).

As the payments space continued to evolve with rapidly increasing mobile and Internet payments, the EC reviewed the initial PSD and acknowledged that it required critical improvements and clarifications to keep pace and ensure customer security. As a result, the Payments Services Directive 2 (PSD2) of November 25, 2015 (EU) 2015/2366 came into effect on January 13, 2018. Similar to PSD, PSD2 is a significant step forward in payment industry regulations. Beyond renewed support for the existing goals of PSD – promoting increased competition and cost-effective choices for the consumer by opening up the payment market to new entrants – PSD2 aims to:

- Better protect consumer financial data with stricter security requirements such as stronger authentication
- Require banks to provide open communication interfaces (APIs) that allow access to third-party providers (TPPs)
- Enact specific rules for access to customer accounts
- Make the conditions and information requirements for payment services more transparent
- Redefine user and provider rights and obligations for payment services
- Clarify the criteria and scope of exemptions

To support this open environment, eIDAS Qualified Certificates are used to secure communications between TPPs and banks. TLS/SSL communications can be secured using PSD2 qualified website authentication certificates (QWACs) and data can be sealed using PSD2 qualified certificates for sealing (QsealCs).

Bank-to-customer services, such as establishing identity when opening an account, are regulated by PSD2.

Previously, banking was treated as a closed community, and hence not covered by eIDAS. However, PSD2 opened up payment services to third-party payment service providers.

Digital Signing with Smartcard or USB Tokens: The Old Way

Digital signing existed long before eIDAS was adopted. Prior to this regulation, digital signature systems had mostly been administered using smartcards or secure USB tokens, because the cryptographic key associated with the signatory's digital certificate, which is used for the digital signature, requires secure physical storage. A user would present a smartcard or USB token to a service provider, and the smartcard would provide both proof of identity and signing functionality. For example, a bank employee might present a smartcard to provide proof of identity and use it to generate a signature for a document that the employee presents to a tax collection agency.

Smartcards and USB tokens have their drawbacks, though. Keeping them safe and secure can be difficult – and keeping thousands of them safe and secure can be an administrative nightmare. Issuing hardware tokens to everyone in an organisation who needs to securely sign documents can be expensive and administratively unwieldy, particularly for organisations that may have to support millions of users. People frequently lose or misplace them, so a large organisation may need extra employees to reissue them and reauthenticate users who request replacements. Additionally, they're not really compatible with mobile devices, and may need to be reissued as new security standards emerge. As a result, the adoption rate of these personal hardware devices for electronic signing has been low in the EU.

Remote Signing: The New Way

Rather than letting users figure out how to manage and protect their cryptographic keys in all those personal devices, what if a TSP kept all the signing keys in a single, heavily protected but easy-to-administer location, and then allowed users to connect to it remotely? That's the basic idea behind *remote signing* for advanced and qualified signatures, a new feature introduced by the eIDAS regulation.

REMEMBER

The eIDAS regulation uses the term *remote electronic signatures* when referring to digital signing in the cloud, that's to say when the digital signature is generated using a key pair that is stored remotely from the user. However, the CEN EN 419 241-1 and -2 standards (for more on these, see Chapter 4) refer to *remote signing* or *remote signatures.*

With remote signing, TSPs use HSMs to hold keys on behalf of their users, rather than storing keys on personal smartcards to be managed by the users themselves.

Users work with a remote signing service that employs a certified HSM, such as an Entrust signing service or another service provider using an Entrust *nShield* product. The HSM securely holds the keys, so there's no risk of it being lost or stolen. Users can safely enter their credentials and sign documents using a smartphone, tablet, computer, or other electronic device that has web-browsing capability.

Depending on the member state, HSMs can support remote signing services and secure authentication of signers (users) by:

- Creating and protecting a signing key for each user
- Ensuring that a document can only be signed with an authenticated user's signing key
- Securely authenticating the signer (the user)

REMEMBER

The details of an HSM's cryptography may be complex, but the process from a user's standpoint is pretty simple. A user is about to create an electronic signature through a cloud-based service online. The TSP verifies the user's identity using an appropriate method, such as remote video verification. The TSP then creates a digital signing certificate and a signing key, which are held within

an HSM managed by a TSP, and which can be activated through a mobile device.

How big is signing in the cloud? Huge. Moving forward, the predominant approach for electronic signing will be through remote digital signing in the cloud using mobile devices. Mobile device usage has dramatically increased in recent years and the deployment of EU Digital Identity Wallets (see Chapter 2) is expected to increase the use of remote signing even more.

Figure 3-2 illustrates an approach to remote signing using an HSM.

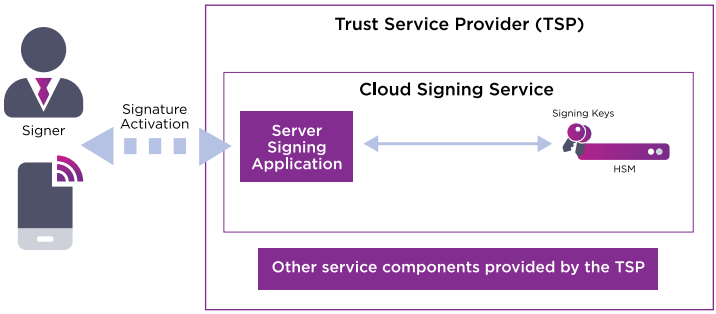

FIGURE 3-2: Remote signing.

Timestamping: Don't Forget It

The eIDAS *timestamping* trust service provides proof of the existence of a document, its signature, or other information at a given time. This is achieved by binding together a digest (or *hash*) of the document or other information with the current date and time using a signature from the TSP, as specified in IETF RFC 3161.

REMEMBER

Timestamping has an important role in ensuring that documents that are stored or archived can be validated many years after they were signed. This type of validation can be used with the document's signature to prove that the signature existed at the time it was timestamped. Thus, even if the circumstances around the creation of the digital signature change (such as the signing key being later compromised or the certificate being revoked), the signature itself remains valid.

Even if the document isn't signed, timestamping can be used when electronically archiving a document to protect its

authenticity, proving its existence at a given time and ensuring that any changes can be detected.

Other methods are widely used to establish evidence of the time of signing, such as email logs, audit logs, and most recently, blockchain time evidence. Nonetheless, timestamping is still considered to be one of the most secure approaches. Timestamping provides proof of a signature's date and time in a similar way to how electronic identification provides proof of the signatory's identity.

REMEMBER

The date and time of an electronic signature can be legally significant in some situations. For example, suppose a client's electronic signature was created using a certificate from a TSP, and then that certificate is discovered to have been revoked. The signature turns out to have been faked and a huge lawsuit hinges on the question, 'Who is responsible?' It all depends on when the signature was created.

Timestamping isn't just for use at the time of signing – it's also for later, when the signed document is archived. Many companies are required by law to keep archives for a very long time, and some documents may be unarchived decades after they were signed, so you never know when a signature is going to become critically relevant. Timestamping helps to ensure that the digital signature will remain valid many years after the digital signature (or seal) was generated.

To support validation over the long term, the revocation information and digital certificate chain that was initially used to validate the signature need to be available indefinitely. Optional features of electronic signature and seal standards provide the capability to store this information along with the signature, as well as adding further timestamps on archived documents using state-of-the-art cryptography. The standards for timestamping under eIDAS were published at the same time as standards for public key certificates.

A Quick Primer on Digital Certificates, Public Keys, and TSPs

One way to verify the identity of someone you're interacting with online is to have a third party vouch for them. You've probably asked a friend to provide a reference for someone who claims they know them, right?

That's the basic idea behind public key certificates: A trusted authority vouches for the identity of someone or an organisation. In order to do this, they rely on technology based on cryptography.

REMEMBER

A *public key* is a code string that uniquely identifies a certain individual or company. However, the word *public* in public key doesn't mean the general public. In *public key cryptography* (also called *asymmetric cryptography*), keys come in pairs: a public key and a private key. The private key must be kept absolutely secure and not shared by its owner, whereas the public key can be shared with anyone.

Here are two scenarios involving Alice and Bob (who are famous in cryptographic circles). Bob wants to send Alice a message, and Alice needs to be sure that the message came from Bob. So, Bob uses his private key to encrypt the message. Alice can then validate that the message came from Bob by decrypting it using Bob's public key, previously exchanged without any need for confidentiality over Bob's public key. In the second scenario, Alice wants to send Bob a message that only he can read, so she encrypts it with Bob's public key. Then the only person who can decrypt it is Bob, using his very well-protected private key.

Certificates provide a way for a user to give her public key to someone, allowing the recipient to verify that the public key is genuine. A trusted third party (such as a TSP) will verify the user's identity, then create a digital certificate (also known as a public key certificate) that will officially bind the public key to this user, who becomes the owner of the certificate. The authenticity of a digital certificate is backed by the reputation of the TSP issuing it.

TIP

A company or individual who wants the trust of customers or constituents online can contract with a TSP to issue a certificate on their behalf. Then when a secure transaction is initiated, the software checks the validity of the certificate, and if everything checks out, the transaction continues. Otherwise, an error appears.

REMEMBER

One of the most important functions as a TSP is to serve as a trusted authority that can vouch for the identity in a digital certificate. To make sure that the entire EU is operating using the same set of standards for certificate trustworthiness, the eIDAS regulation specifies the basic requirements that any public TSP operating within the EU must meet – Chapter 4 provides more details about these standards.

Digital Certificates in Trust Services

Digital certificates have many benefits and applications, one of which is particularly relevant for eIDAS: electronic signatures (and seals). Because digital certificates carry verified identity, they can be used to perform digital signatures in the case of a natural person and seals in the case of organisations/legal persons as defined by the standard.

The role of a TSP was originally limited to the issuance of such certificates in hardware devices (smartcards, USB tokens, HSMs) for citizens and organisations to digitally sign documents and transactions. However, with the emergence of innovative technology and standards, and thanks to the work of the European Committee for Standardization (CEN) and the European Telecommunications Standards Institute (ETSI), TSPs can now build centralized and secure infrastructures for citizens to digitally sign documents without having to carry their digital signing certificate and signing key in hardware: This is remote signing.


TIP

In the world of eIDAS, TSPs are issuers of digital certificates. But in the PKI world, especially in the public trust PKI world, issuers are called certification authorities (CAs). You may see these two expressions used interchangeably, but generally speaking, TSP is used in the context of an EU trust service.

IN THIS CHAPTER

- Overview of TSP standards including signatures, seals, and timestamps
- The essential role of HSMs
- Qualification and auditing

Chapter 4
Building a Trust Service in the eIDAS World

If you're looking for guidance on how to set up your own trust service, how to become a trust service provider (TSP), a qualified TSP (QTSP), or just how to align with Electronic Identification and Trust Services (eIDAS) standards, this chapter is for you. It takes a deeper dive into some of the technical standards used under the eIDAS regulation, so there are a lot of European Telecommunications Standards Institute (ETSI), European Committee for Standardization (CEN), and CC references.

Keeping Everyone Consistent: TSP Standards

REMEMBER

ETSI has established a set of standards for public key certification and timestamping services. Compliance with these standards isn't mandated under eIDAS, but the supervisory bodies of many EU countries generally recommend them, and they are the only recognised best practices for TSPs under eIDAS.

These ETSI standards ensure that the functionality of a trust service is aligned with industry best practices, and that the TSP's information security management system follows the generally

accepted principles defined by ISO 27002. These standards align with – and build upon – internationally recognised profiles and standards for public key infrastructure (PKI) services, such as those adopted by the CA/Browser Forum, the banking industry, and the SAFE BioPharma Association. Taken together, they represent a good basis for auditors examining TSPs with an eye toward best practice for eIDAS compliance.

The following sections provide an overview of these ETSI standards governing TSPs and their operation. As you review them, refer to Figure 4-1 to see how they fit together.

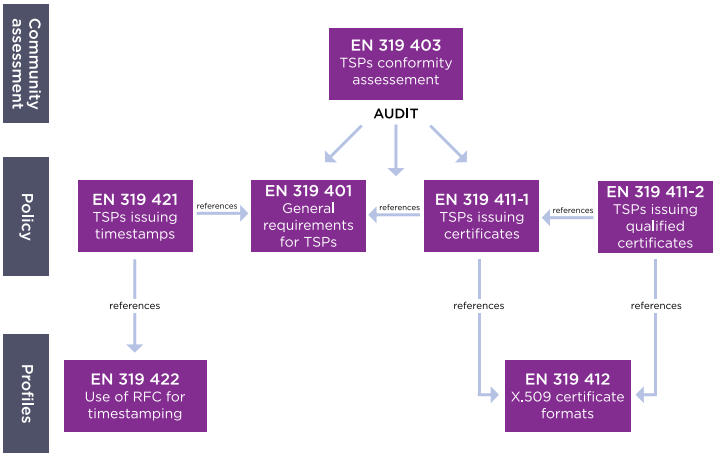

FIGURE 4-1: ETSI standards for public key certification and timestamping services.

THE RELATIONSHIP BETWEEN ETSI AND CEN STANDARDS

The two main European Standards bodies, ETSI and CEN, have worked together to meet the requirements of the eIDAS regulation. CEN provides standards for the security of signing devices and systems required by the regulation such as HSMs and smartcards. ETSI defines standards for the trust services which build upon CEN-compliant secure devices. These cover requirements for the secure operation of trust services, such as their policies and practices, as well as protocol standards which ensure interoperability between users and their TSP, enabling users to easily switch between TSPs.

ETSI general standards

What do all TSPs have in common, regardless of type? There are two general ETSI standards, governing the overall process:

- **EN 319 403-1:** This standard provides detailed requirements for organisations that assess or audit TSPs to ensure legal compliance. Depending on the types of services they provide, TSPs will be audited against one or more of the more specific standards.
- **EN 319 401:** This standard outlines the general policy requirements for managing and operating TSPs. The TSP can be a certificate issuer, timestamp issuer, signature verifier, or an entity that uses electronic signatures or seals.

ETSI standards for specific TSP types

Some standards apply only to certain types of TSPs and services, so they're addressed in specific sets of ETSI policies:

- **EN 319 411-1:** This specification defines the policy and security requirements that are common to TSPs issuing certificates, also known as certificate authorities (CAs). It references EN 319 401 for generic requirements and EN 319 412 for certificate format requirements. The standard replaces TS 102 042 and is aligned with the CA/Browser Forum requirements.
- **EN 319 411-2:** This standard defines the policy and security requirements specifically for QTSPs issuing qualified certificates in the EU, as specified in the eIDAS regulation. For a discussion on QTSPs, see the 'QTSP status' section. EN 319 411-2 references EN 319 411-1 for the majority of the requirements and replaces TS 101 456.
- **EN 319 412:** This standard profiles the use of X.509 certificate formats for individuals, legal entities, website certificates, and qualified certificates.
- **EN 319 421:** This standard covers the policy and security requirements relating to operating and managing TSPs that issue timestamps. Such timestamps can be used in support of electronic signatures or for any application that needs to prove a document existed before a particular time.

- **EN 319 422:** This standard covers the use of RFC 3161 data formats for timestamping.
- **EN 419 241-1 and EN 419 241-2:** These standards define technical requirements for the architecture of a solution supporting remote signing services. It covers both security requirements and the protection profile for qualified signature creation devices.
- **TS 119 431-1:** This standard covers the policy and security requirements for TSPs, including the components of those operating a remote qualified signature creation device/signature creation device (QSCD/SCDev).
- **TS 119 461:** This standard covers the management and operation of an identity-proofing solution, and identity-proofing service requirements.
- **TS 119 495:** This standard covers the requirements for qualified certificates and TSP policies under the Payment Services Directive (EU) 2015/2366 (PSD2). This standard is designed to ensure the secure and reliable issuance of electronic certificates used in payment services.

A series of standards has been published for registered electronic delivery and its specific use in registered electronic mail. The general policies and security for registered electronic delivery are defined in ETSI EN 319 521 with technical protocols and evidence formats defined in a multipart standard, ETSI EN 319 522. ETSI EN 319 531 (policy and security) and ETSI EN 319 532 (technical protocols) specify how EN 319 521 and EN 319 522 are applied to registered electronic mail.

Specifications for the preservation of signatures and signed documents were published in 2019 and 2020. This includes TS 119 511, which specifies policy and security requirements, and TS 199 512, which specifies protocols. These standards may also be applicable to preserving the integrity of any archived documents.


TIP

For more information about standards, see the Appendix at the end of this book.

HSM CERTIFICATION STANDARDS IN EUROPE AND THE U.S.

European governments already have a general scheme for certifying security products in place called *Common Criteria* (CC). CC has become widely accepted, not only by EU member state governments, but also by European industries, international companies that want to sell in the EU, and non-EU governments that tend to follow the EU's direction, such as southern Mediterranean and South American companies. Both EU and non-EU governments are increasingly adopting CC.

HSM certification for eIDAS is based on CC.

The U.S. Government has its own security-related regulations, such as the Federal Information Processing Standards (FIPS). FIPS is the *de facto* standard in the U.S., but isn't accepted by a number of governments, including France and Germany, and some South American countries. Also, delays in delivering updates to the FIPS HSM standard and mistrust in FIPS has encouraged the uptake of CC.

But don't worry: Entrust nShield HSMs have both FIPS and CC certification, so they can meet regulatory requirements the world over.

Understanding Seal and Signature Standards

There are a couple of technical standards to know when building a digital signing or sealing service.

As you'd expect, there are standards for how an advanced and qualified electronic signature (or seal) should be formatted, but most importantly, there are many new standards related to *remote signing*, which is the new way of digital signing introduced with the eIDAS regulation. To learn more about remote signing concepts and how remote signing differs from the traditional local signing, check out Chapter 3.

Signature formats

eIDAS Article 27 (and implementing decision 2015/1506) requires that online government services recognise standard formats for advanced electronic signatures and seals (AdES).

AdES is based on existing ETSI standards, but includes two additional features to ensure an electronic signature or electronic seal can be validated long after a document was signed:

- The signing certificate must be included in the calculation of a digital signature's cryptographic value.
- Optional timestamps can be added to the signature to assist in long-term validation.

AdES covers the use of these standard digital signature formats for electronic signatures or electronic seals:

- **CAdES (EN 319 122): Cryptographic Message Syntax (CMS) Advanced Electronic Signature/Seal:** This standard is based on a binary structure, and is applicable to any data format.
- **XAdES (EN 319 132): XML Advanced Electronic Signature/Seal:** XAdES digital signatures are most appropriate to XML data.
- **PAdES (EN 319 142): Portable Document Format (PDF) Advanced Electronic Signature/Seal:** Only for PDF documents, this standard covers details of how signatures should be presented, displayed, and integrated into a form submission process. The result is that PDF editing and rendering tools inherently support digital signing, whereas the use of CAdES and XAdES will generally require separate tools for editing and signing.
- **ASiC (EN 319 162): Associated Signature Containers:** This standard covers the application of signatures to a package of files, such as a ZIP folder.

In March 2021, ETSI introduced JAdES (TS 119 182-1), another AdES format, to protect JSON formatted signatures. JSON is a data syntax specifically for use with Javascript, so the JAdES format enables electronic signatures and seals to be used in a web

environment. JAdES is based on JSON Web Signatures as defined by RFC 7515, with additional features that may be needed to support the regulation (for example, protection against certificate substitution and long term validity).

In addition to these, ETSI EN 319 172 defines general rules for creating and validating any AdES format. The AdES implementing decision 2015/1506 references earlier versions of the above standards; however, the differences are not significant and shouldn't inhibit interoperability.

WARNING

Businesses may use other formats. However, when government services are involved, or other regulations are in place to mandate the use of advanced electronic signatures, the approved AdES formats are required.

REMEMBER

The eIDAS implementing decisions make no technical distinction in the standards between electronic signatures and seals. The same signing device (such as a hardware security module [HSM] or smartcard) can be used to create either a signature or a seal. With that in mind, here are some specifics for digital signature and seal standards:

- CEN have published advice (in CEN TR 419 210) on how its standards can be used for evaluating devices as QSCDs under the eIDAS regulation.
- Qualified electronic seals that meet the requirements of the regulation can be created using such qualified devices. Qualified electronic seals must be created using digital signatures (for instance, AdES) and must be supported by a qualified certificate issued specifically for qualified electronic seals.

Remote signing standards

A set of CEN standards for devices, and a set of ETSI standards for trust services, have been defined for remote signing and with the intention of meeting the requirements set by eIDAS implementing acts. The CEN standards (EN 419 241-1 and -2) cover the requirements for the signing device:

- EN 419 241-1 defines the general requirements for operating the signing device for remote signing.

- EN 419 241-2 defines the specific technical security requirements of the signing device. These security requirements build on top of CEN standard EN 419 221-5d, which was created with the intention of meeting the eIDAS technical requirements for HSMs.

WARNING

Just to be clear again on the role of eIDAS: The regulation itself doesn't mention which technical standard to use. This is the role of the implementing acts, which are published throughout the lifecycle of a regulation, and which define or amend the technical standards that meet the legal definitions set by eIDAS, such as ETSI or CEN. Meeting this standard is usually achieved via certifications such as CC.

TECHNICAL STUFF

Remote signing means that the cryptographic keys are securely stored by the TSP, but they can only be used under explicit consent of their owner: this is called *sole control.* EN 419 241-1 identifies two levels of sole control assurance:

- Level 1, illustrated in Figure 4-2, relies on the server signing application to ensure that the appropriate signing key is selected. The functionality supporting signature activation and ensuring sole control is implemented as part of the server signing application. This level can use any suitably certified HSM, such as one certified to EN 419 221-5.
- Level 2, illustrated in Figure 4-3, provides greater assurance of sole control by implementing a signature activation module (SAM). This module is certified to be executed within a tamper-resistant environment. The signature activation data passes, in protected form, from the signer's device to the HSM to ensure that the user's signing keys can't be abused, even if the TSP's server signing application were to be compromised.

TIP

Evaluation of the HSM and the SAM can be done separately, and there are different certification methods available. It's expected that the next implementing act will mandate the use of CC for certifications of HSMs and SAMs, and in that case, the technical standards to comply with will be EN 419 221-5 for the HSM and EN 419 241-2 for the SAM.

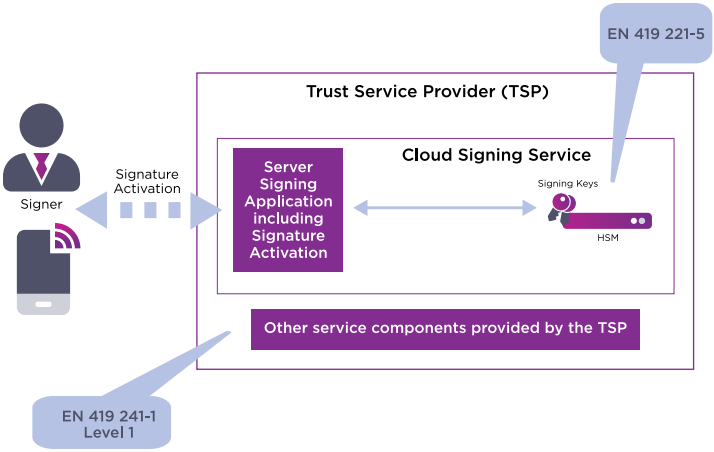

FIGURE 4-2: Remote signing, Level 1.

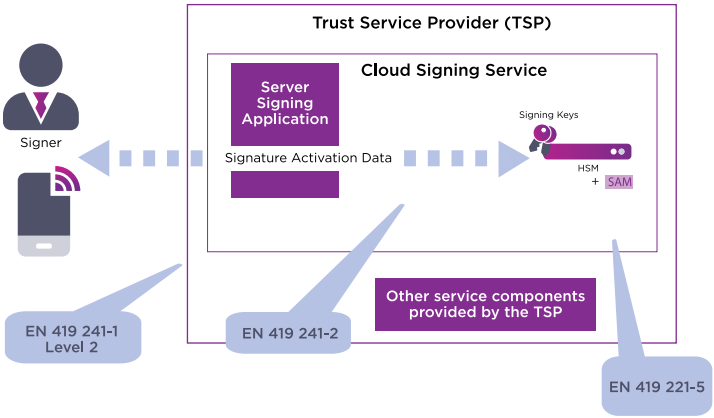

FIGURE 4-3: Remote signing, Level 2.

For Level 2, although not explicitly stated, the CC Protection Profile EN 419 241-2 is expected to become mandatory in the next implementing act. This requires that the code evaluated under EN 419 241-2 operates within a tamper-protected environment (an HSM) conforming to EN 419 221-5.

ETSI was built on the CEN standards, providing a set of standards for trust service security, policy requirements, and protocols for remote signing. ETSI TS 119 431-1 defines the security and policy requirements for operating a CEN EN 419 241-1 conformant device

to ensure that it's secure and meets the requirements of the CEN standard. ETSI TS 119 431-2 defines requirements for TSPs provisioning digital signatures that conform to the eIDAS advanced electronic signatures formats described in the 'Signature formats' section. ETSI TS 119 432 specifies protocols and interfaces applicable when advanced electronic signatures are remotely carried out by a distributed solution that includes two or more services.


WARNING

As with many of the specifics of eIDAS, the legal requirement for remote signing is still somewhat unclear. The eIDAS implementing decision for qualified signature and seal creation devices (EU 2016/650) calls for security comparable with a certified smartcard device until the European Commission recognises specific standards for remote signing. Many countries have been already adapting the Level 2 remote service approach, although interim solutions at Level 2 based on the earlier ETSI standard are still accepted by some countries.


TIP

Yes, there's still some uncertainty at the moment, especially because the EU regulators have been more focused on eIDAS 2 over the last few years, and TSPs are waiting for CEN standards to be officially adopted, but this isn't stopping remote signing from being widely adopted in the EU. Entrust and its partners are already delivering remote signing solutions within the eIDAS framework. By using solutions like Entrust Remote Signing Engines, Entrust PKI, Entrust nShield HSMs, and Entrust Authentication Solutions, you get a clear migration path to standards-based solutions that are recognised throughout the EU. Chapter 5 provides more details about what Entrust can offer.

Knowing Whom to Trust: Qualification and Auditing


WARNING

Would you trust a salesman just because he claims to be trustworthy? Of course not! And neither should customers trust a TSP without some independent verification.

eIDAS introduced the concept of *qualification* for TSPs and cryptographic hardware. Under eIDAS, each member state is responsible for maintaining its own list of QTSPs, and for determining the criteria for being on that list.

The criteria might differ slightly between member states, but there are some basic must-haves. Each member state must also specify criteria for the periodic auditing of TSPs to make sure they continue to comply with all requirements. These lists are made publicly available to other member states and also to potential customers who are shopping for TSP services (see the 'Trust us! National lists of QTSPs' section).

QTSP status

Trust services can be qualified or non-qualified (for more on this see Chapter 1). With a qualified status, the burden of proof is reversed and the QTSP issuing the timestamp or certificate must guarantee good practices and accountability. To be designated as qualified by a member state trust services must meet specific requirements defined by that member state.

Qualified status is also applied to:

- Certificates, which must be issued by a QTSP
- Timestamps, which must be issued by a QTSP
- Cryptographic hardware, which can be used for signature or seal creation: for example, a QSCD
- Ledgers and archiving services, which must be issued by a QTSP
- Electronic attestations of attributes, which must be issued by a QTSP
- Electronic signatures and seals, which require a qualified signing device and a qualified certificate

The ETSI standards for TSPs generally place the same requirements on TSPs irrespective of whether they're qualified or not. Specific requirements are included in the standards where it's necessary to add to generally accepted best practice with requirements specific to EU QTSPs and their qualified certificates. The most important feature of qualified certificates is they're subject to direct regulatory oversight.

QTSPs are identifiable by a trust mark, as shown in Figure 4-4.

FIGURE 4-4: EU trust mark for QTSPs.

TIP

If a signing device or TSP isn't qualified, that doesn't necessarily mean that you should consider it less trustworthy. Other schemes besides the eIDAS regulation aim to ensure trustworthiness. For example, the CA/Browser Forum provides a similar international TSP approval scheme that is accepted by all the major application providers, in spite of being non-qualified in relation to the eIDAS regulation. However, especially for TSPs with customers in EU member states, being qualified is a significant selling point for current and potential customers.

TSP auditing

So, how do TSPs get and keep that coveted spot on the qualified list? They submit their systems for *auditing,* in which an independent third party examines their physical, operational, and technical security. TSPs must be reaudited periodically to keep their status current.

TECHNICAL STUFF

How often must auditing occur? Article 20.1 of the eIDAS regulation requires that QTSPs be audited every two years. Auditing is also a mandatory part of the CA/Browser Forum baseline requirements, which call for an annual audit.

For qualified website authentication certificates (QWACs) the eIDAS qualified level is similar to the CA/Browser Forum's Extended Validation designation. ETSI has therefore established a set of standards for auditing TSPs that meets both the requirements of the eIDAS regulation and those of the CA/Browser Forum. As a result, a TSP needs to be audited only once to be approved under both standards. The TSP auditor will release two statements: one to the CA/Browser Forum pertaining to its extended validation, and one to the eIDAS regulatory authority pertaining to its qualified status.

TECHNICAL STUFF

The CA/Browser Forum agreement has been adopted by the major web software providers, including Apple, Google, Microsoft, Mozilla, Opera, and Qihoo 360 (which serves over a third of the population of China), as well as most of the TSPs inside and outside Europe.

Trust us! National lists of QTSPs

Each EU member state is responsible for publishing a list of TSPs that its national supervisory scheme has recognised as qualified, either under the eIDAS regulation or the earlier directive. A standard structure for this trusted list has been defined (TS 119 612) and is applied to eIDAS by Implementing Act 2015/1505. This standard structure includes an entry for each trust service, together with the TSP's certificate.

TIP

So if each member state has its own list, how does that make for harmonisation across the EU? Easy! The EU publishes one official list that provides links to every member state's list. You can find that list at `https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home`.

To say that these lists are large, complex, and ever-changing is an understatement. As of this writing, there are currently 1,400 entries distributed across 31 national lists, and changes can potentially occur every three days. Because of this, you can imagine the difficulties for application providers in incorporating the trusted lists into their applications. Adobe currently supports trusted lists, as do several providers of custom solutions for government agencies, but it is not yet clear whether other major providers will follow suit.

IN THIS CHAPTER

» Discovering how Entrust can help your business

Chapter 5
Five Ways Entrust Can Help You


TIP

Whether you're looking to use a trust service, or to become a trust service provider (TSP), you'll need a partner to help. Entrust can not only offer signing, sealing, and timestamping services, but they can also provide the necessary hardware, software, and professional services to deploy multiple trust services.

Using a Qualified Service for Electronic Signatures, Seals, Timestamps, and Website Authentication

The Electronic Identification and Trust Services (eIDAS) technical framework is complex, and finding out the right service for your specific use-cases can be tricky. Entrust is a qualified TSP (QTSP) accredited by the Spanish government. They can help you navigate through this landscape thanks to their portfolio, which covers a wide range of scenarios, from a full end-to-end solution that you can plug to your environment to start signing documents in compliance with your eIDAS needs, to a single service to build

or upgrade your own eIDAS-aligned trust service. Entrust offers the following services:

- **Entrust Signhost** is a web service to request and generate advanced and qualified electronic signatures. It's available via a web portal, a REST application programming interface (API), or a mobile application. Learn more at `https://www.signhost.com`.
- **Entrust Remote Signing Service** is a cloud service that generates Adobe Approved Trust List (AATL) or eIDAS qualified certificates for EU employees and consumers to generate eIDAS advanced or qualified signatures. It is based on the Cloud Signature Consortium (CSC) remote signing API. The service is designed to be integrated to signature software and applications, and it has a native integration with Adobe Acrobat Sign and Entrust Signhost. Learn more at `https://www.entrust.com/products/digital-signing/digital-signing-as-a-service/remote-signing-service`.
- **Entrust Signing Automation Service** is a cloud service that generates AATL or eIDAS qualified certificates for organisations to generate eIDAS-advanced seals. It's available via a PKCS #11 API or a REST API. The service is designed to be integrated to workflows and software that automate document sealing processes and it has a native integration with iText and Entrust Signhost. Learn more at `https://www.entrust.com/products/digital-signing/digital-signing-as-a-service/signing-automation-service`.
- **Entrust Timestamping Services** provide both eIDAS qualified and non-qualified RFC3161 timestamps. Entrust's timestamping services are a complimentary offer, which means they're included when you subscribe to Entrust Remote Signing Service or Entrust Signing Automation Service.
- **Entrust Qualified Website Authentication Certificates (QWACs)** are either for standard use under eIDAS or under the Payment Services Directive 2 (PSD2) regulation, to be used as part of a TLS exchange between financial institutions and/or payment service providers. Learn more at `https://www.entrust.com/products/digital-certificates/qualified/qwac-psd2` or `https://www.entrust.com/products/digital-certificates/qualified/qwac-eidas`.

- **Entrust PSD2-compliant qualified certificate for electronic seal (QsealCs)** is to be used as defined by PSD2 to seal data exchanged between financial institutions and/or payment service providers. Learn more at `https://www.entrust.com/products/digital-certificates/qualified/electronic-seal`.

Deploying Your Own eIDAS Trust Service (Qualified or Non-qualified) for Signatures, Seals, Timestamps, or Website Security

Entrust isn't only a TSP, but also a provider of eIDAS-compliant software and hardware that can be used to build a trust service for signatures, seals, timestamps, and QWACS. Entrust products are aligned with the latest European Telecommunications Standards Institute (ETSI) and European Committee for Standardization (CEN) standards to help you ensure you pass the relevant audits and receive your TSP or QTSP accreditation.

If you're looking to provide a trust service (that's to say, build your own service, potentially with the objective to get audited and accredited by an EU government or just to align with eIDAS standards), Entrust can offer:

- **Entrust Remote Signing Engine** is an on-premises platform designed for remote signing, easily accessible through a Web API. Signing keys are centrally protected within a hardware security module (HSM) and document signatures are approved remotely by users from their devices, without the need for a hardware or software token. Learn more a: `https://www.entrust.com/products/digital-signing/digital-signing-engines/remote-signing-engine`.
- **Entrust Signing Automation Engine** is an on-premises platform providing a complete range of web services for integrating digital signatures into applications. It's designed to centrally incorporate digital signature operations in accordance with the standards of ETSI CAdES, XAdES, and PAdES. Learn more at `https://www.entrust.com/`

products/digital-signing/digital-signing-engines/signing-automation-engine.

- **Entrust Hardware Security Modules** are eIDAS-compliant secure storage devices for cryptographic keys, which are at the core of any PKI-based service such as signing, sealing, and timestamping. Learn more at https://www.entrust.com/products/hsm.
- **Entrust Signature Activation Module** is an eIDAS-compliant software component designed to act as a security intermediate between a signing application and the HSMs in a remote signing service deployment. Learn more at https://www.entrust.com/products/digital-signing/signature-activation-module.
- **Entrust Timestamping Authority** is an on-premises timestamping solution used to affix the exact date and time of your digital signatures. Learn more at https://www.entrust.com/products/digital-signing/timestamping-authority.
- **Entrust Public Key Infrastructure Solutions** are a suite of on-premises products used to deploy a robust digital certificate issuance and lifecycle management service – a centerpiece in a trust service. Learn more at https://www.entrust.com/products/pki.
- **Entrust Identity Enterprise** is an on-premises identity and access management (IAM) platform providing user authentication, authorisation, and access control to the right resources. Learn more at https://www.entrust.com/products/iam/identity-enterprise.

Getting Help With Qualified Signature and Seal Creation Devices (HSMs and Signature Activation Modules)

The eIDAS regulation defines three types of electronic signatures: simple, advanced, and qualified (for more on this, see Chapter 3). Qualified is the more stringent standard, and requires a qualified signature creation device (QSCD) certified to meet the eIDAS requirements. Does your HSM qualify?

If you use Entrust nShield HSMs, the answer is yes. Entrust's nShield SoloXC and nShield 5s HSMs are eIDAS compliant, certified against the Common Criteria (CC) Protection Profile, EN 419 221-5. Entrust nShield, Connect+, and Solo+ HSMs are eIDAS compliant. Entrust's eIDAS-approved nShield HSMs can be used alongside their software-based Signature Activation Module (SAM) running in a protected environment. The Entrust SAM is certified against the CC Protection Profile EN 419 241-2, and in combination with their certified HSMs it is part of an eIDAS-approved Remote QSCD, validated under A-Sit. Alternatively, partners can use CodeSafe, the Entrust SDK environment for customised security sensitive code running within the secure HSM hardware boundary. This means that Entrust certified HSMs can be used for:

- Signing certificates and timestamps issued by a TSP under the regulation.
- Signing revocation information for Certificate Revocation Lists and for Online Certificate Status Protocol (OCSP) revocation.
- Signing objects created by other TSPs for such things as electronic delivery or long-term electronic signature preservation.
- Remote signing with an HSM and key management. Entrust works closely with partners to deliver comprehensive signing solutions that use current nShield HSM products. When there are thousands of keys involved, remote signing using smartcards becomes infeasible. However, Entrust HSMs can manage the large numbers of keys needed for practical remote signing solutions.
- Document sealing, for situations where a signing key is under the control of an organisation rather than an individual. A seal is like a signature except it represents an organisation (such as a company or department) rather than an individual (for more on this, see Chapter 3).
- Protecting information exchanged between the new third-party payment service providers and banks under the PSD2.

ENTRUST NSHIELD HSMS TICK ALL THE BOXES

Here's an easy time-saver when shopping for HSMs: Start with Entrust nShield products, because they have everything you're looking for.

Entrust nShield HSMs:

- Have been certified to the latest available standards for eIDAS qualification. If you go with an nShield product, you don't have to worry about whether your system is eIDAS-compliant.
- Provide scalable key management for any size of business and any volume of key services.
- Offer users the flexibility to authenticate with any device type, through any channel.
- Integrate easily with the applications you run.
- Include a secure execution environment called CodeSafe for running sensitive software. It enables HSM functionality to be extended to support applications such as cloud signing.
- Are suitable for operation in dark data centres and in cloud deployments.

You can check this out through the EU's published list of devices recognised as Qualified Signature and Seal creation devices at: `https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD`.

Deploying an EU Digital Identity Wallet (EUDIW) Infrastructure

Digital identity wallets are only the visible part of the iceberg. To ensure these electronic wallets can work and be recognised, a solid and interoperable infrastructure needs to be in place to support the creation and verification of attributes.

Entrust has developed a full infrastructure for the deployment of portable decentralised identities aligned with multiple regulations and requirements. They can provide solutions for:

- ID wallets for individuals and legal entities
- Credentials issuance and verification service
- Credential backup and recovery services
- Digital signing services

These solutions are deployed using Entrust's comprehensive portfolio of products, including Entrust Identity as a Service, Entrust nShield HSMs, and Entrust PKI solutions. They can be deployed to build a platform supporting ID wallets, using the trust framework of your choice among blockchain, databases, PKI, hyperledge, and EBSI.

Getting eIDAS Infrastructure Advice and Consultancy

Given the complexities of the eIDAS regulation and its implementation, it's comforting to have an experienced and trusted partner on your side.

REMEMBER

Entrust is a $1B+ global company, 3,400 colleagues strong, serving customers in more than 150 countries. Entrust is trusted by some of the world's largest governments, financial institutions, and corporations to handle their most sensitive interactions. Entrust HSMs provide data protection for more than 10,000 customers across 100 countries, including:

- 21 NATO member countries
- 15 of the Fortune 30 companies
- 19 of the world's 20 largest banks
- 3,000 financial institutions worldwide
- 4 out of 5 top energy companies
- 4 out of 5 aerospace companies
- 20 leading cloud service providers

TIP

Entrust industry leadership attracts the brightest and best worldwide, and the company employs some of the most respected engineers and analysts in the field of digital data protection and cryptography. That means that when you work with Entrust, you

get advice and thought leadership from the technology experts who are helping to define eIDAS standards.

For large-scale deployments, Entrust Professional Services Group has many years' experience of supporting its customers in meeting EU regulatory requirements, and in meeting regulatory requirements in specific industries, such as banking. The group is ready to assist you to ensure that your solutions are correctly deployed and that your cryptographic applications are configured to conform to industry best practices.

IN THIS APPENDIX

- Knowing what is scheduled to happen (and when)
- Following a standards roadmap
- Heading online to find out more

Appendix
Further Information

You're looking at this book's final few pages now, but maybe you need more specifics? This appendix offers some reference information you might find useful.


TECHNICAL STUFF

Feel free to consider this whole appendix as having a giant Technical Stuff icon stamped over each page! It contains the type of nitty-gritty detail that's useful to have on hand but is most helpfully presented in a fact-focussed end section rather than being scattered throughout the book.

Checking the Timetable?

Implementing eIDAS, and developing all the supporting implementing acts and standards, has been an ongoing process in the EU, which began in 2014.

Here are some of the key dates to be aware of:

- **July 2016:** The latest publication of eIDAS Implementing Acts, start date for the majority of technical requirements for eIDAS, and for existing TSPs to migrate to eIDAS audits. The old 1999 EU Directive became invalidated.
- **July 2017:** A qualified TSP delivering a service that is currently regulated under the Directive must be audited by this date.
- **May 2018:** CEN EN 419 221-5 was published.
- **July 2018:** CEN EN 419 241-1 was published.

- **March 2019:** CEN EN 419 241-2 was published.
- **2020:** The regulation was reviewed. As a result, the European Council asked the Commission to introduce the EU-wide digital ID system by 2021, to secure the identification for the use of public and private online services.
- **May 2021:** Proposal amending Regulation (EU) No 910/2014 as regards to establishing a framework for a European Digital Identity (SEC(2021) 228 final) - (SWD(2021) 124 final) - (SWD(2021) 125 final) published.
- **October 2022:** Commission agreed to publish the Toolbox to implement the European Digital Identity Framework in October 2022, and start pilot phase. `https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_2664`.
- **May 20, 2024:** The European Council adopts the Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

Mapping the Big Picture: A Standards Roadmap

A *standards roadmap* listing all the standards relating to trust services and signatures is described in the ETSI publication TR 119 000. These standards are grouped together by a numbering scheme, as shown in Figure A-1. This diagram may help you see how the many different standards fit together in a coherent whole.

Here are some references to the various standards involved:

- **ETSI standards** can be obtained through the ETSI standards search page at the following URL `www.etsi.org/standards-search`.
- **CEN standards** can be obtained through any European national standards organisation.
- **Specifications for eIDAS electronic identity services** are not issued through the formal standards bodies but are published through a European group comprised of national experts. These specifications may be downloaded at the following URL `https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID`.

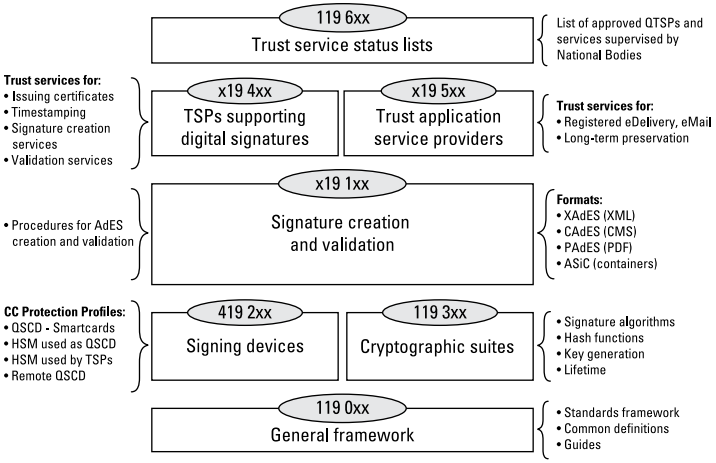

FIGURE A-1: Framework of eIDAS trust service related standards.

Finding Out More Online

Still hungry for more details? Here are some additional references to the related regulatory requirements:

- Trust services and electronic identity in the digital single market: `https://ec.europa.eu/digital-single-market/en/trust-services-and-eid`.
- Regulation (EU) No 910/2014 (eIDAS): `http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN`.
- Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework: `https://eur-lex.europa.eu/eli/reg/2024/1183/oj`.
- Implementing acts supporting eIDAS:
  - Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework:

    `http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1441782373783&uri=OJ:JOL_2015_235_R_0001`.

- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification:

  `http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002`.

- Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists:

  `http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0005`.

- Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies:

  `http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0006`.

- Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices:

  `http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D0650&from=EN`.

- Digital Identity Mapping Exercise Report comparing NIST Digital Identity Guidelines to eIDAS levels of Assurance:

  `https://www.nist.gov/system/files/documents/2023/12/22/EU-US%20TTC%20WG1_Digital_Identity_Mapping_Report_Final%20Draft%20for%20Comment_22122023.pdf`.

» Technical references for the EUDIW:

- Architecture and Reference Framework: `https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework`.
- Reference implementation: `https://github.com/eu-digital-identity-wallet/.github/blob/main/profile/reference-implementation.md`.
- EUDIW large scale projects: `https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+are+the+Large+Scale+Pilot+Projects`.

About the Author

Charlotte Pommier is a senior Product Marketing Manager at Entrust. With over 10 years of experience working in the public trust PKI industry, she has developed a strong technical expertise in digital signing, and is a subject matter expert in certificate-based signature standards and requirements, including eIDAS and AATL. She has been supporting the digital signing portfolio's roadmap and go-to-market strategy at Entrust for the last 5 years.

Everything you need to know about eIDAS, including the eIDAS 2.0 amendment

The European Union's Electronic Identification and Trust Services (eIDAS) Regulation has created a single European market for secure electronic commerce. It means citizens of every EU member state are given means to securely identify themselves and transact online across the EU, from the comfort of their homes or the on-the-go convenience of their mobile devices.

If you are curious to understand what eIDAS entails exactly, if you'd like to know more about the new eID Wallets that are coming up in every EU member country, or if your organisation is looking to use or deploy solutions that are considered trust services under eIDAS such as document signing or sealing, this book can help.

Inside...

- Why eIDAS was created, what it covers, and what changes were brought in the 2024 amendment
- What (qualified) trust services and (qualified) trust service providers are
- What the EU Digital Identity Wallet is and how it will be used
- How electronic signature and seal services work under eIDAS
- Some of the technical standards and requirements to become a trust service provider

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-394-29344-5
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.