A Quick Guide to eIDAS, Electronic Signatures, and Digital Certificates

ENTRUST

SECURING A WORLD IN MOTION

Table of Contents

What is eIDAS?

eIDAS stands for Electronic Identification and Trust Services (eIDAS).

It's a European regulation released in 2016 designed to establish consistent standards for electronic identities, authentication, and signatures within the European Union.

What eIDAS does:

- Defines what electronic signatures are, including the different types and what makes them different

- Establishes a set of technical requirements to implement these signatures

- Explains the role of trust services and requirements for trust service providers (TSPs)

What eIDAS does NOT do:

- It does not provide guidance on which type of signature should be used for each use case and document. It's up to governments, industries, and organizations using those signatures to determine that.

What is a Trust Service? A Trust Service Provider (TSP)? A Qualified Trust Service Provider (QTSP)?

Under eIDAS, a **trust service** is an electronic service normally provided for remuneration, which may include:

- The creation, verification, and validation of electronic signatures, electronic seals, electronic timestamps, electronic registered delivery services, and certificates related to those services

- The creation, verification, and validation of certificates for website authentication

- The preservation of electronic signatures, seals, or certificates related to those services

A **trust service provider** is a natural or a legal person who provides one or more trust services either as a qualified or non-qualified trust service provider.

A **qualified trust service provider** is a trust service provider who provides one or more qualified trust services and is granted the qualified status by a supervisory body from an EU country.

Trust services under eIDAS

Certificate Issuing

Timestamping

Website Authentication

Electronic Signature

Electronic Seal

The **EU trust mark** gives the assurance that the providers of electronic trust services and the trust services offered by them are qualified and comply with the rules set out in the eIDAS Regulation. It tells users that they can trust a certain service to carry out their online transactions in a safe, convenient, and secure way.

What is a Signature Creation Device? A Qualified Signature Creation Device?

A **Signature Creation Device (SCD)** is hardware designed to host digital certificates – more specifically their private keys – and generate digital signatures.

Secure USB tokens and hardware security modules (HSMs) are considered signature creation devices.

A **Qualified Signature Creation Device (QSCD)** is an SCD that went through an eIDAS certification process. Only a QSCD combined with a qualified certificate can generate a qualified signature or seal. A signature using only an SCD will generate advanced signatures/seals, even if the certificate itself is qualified.

Secure USB Token

HSM (in PCIe Card Format)

HSM (in Appliance Format)

Signature types under eIDAS

Overview

Electronic Signature
See page 7

- Also called "simple," "standard," or "basic" electronic signature
- No extensive definition
- No technical requirements; simple to implement

Advanced Electronic Signature
See page 8

- Clearer definition compared to electronic signatures, while leaving some flexibility in technical implementation
- Digital signatures are considered advanced electronic signatures

Qualified Electronic Signature
See page 9

- An advanced electronic signature with stronger technical requirements
- Highest level of assurance but the hardest to implement

(Simple) Electronic Signature

Definition

An electronic signature is data in electronic form that is attached to or logically associated with other data in electronic form and is used by the signatory to sign.

- The definition implies that some signature data must be generated, and that there should be a way to tie it to the data signed

- No reference or technical requirements are provided

Requirements

Electronic Record

Examples

The eIDAS definition of an electronic signature is very broad. Some common forms of electronic signatures include:

- A signature drawn with a finger or a mouse

- A box checked or a button clicked on a web form

- A scanned picture of a document with a "wet" signature

Advanced Electronic Signature

Definition

An advanced electronic signature must meet the following requirements:

- Uniquely linked to the signatory

- Capable of identifying the signatory

- Created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control

- Linked to the data signed therewith in such a way that any subsequent change in the data is detectable

Requirements

Electronic Record + Identity Verification & Authentication + (Optional) Digital Certificate
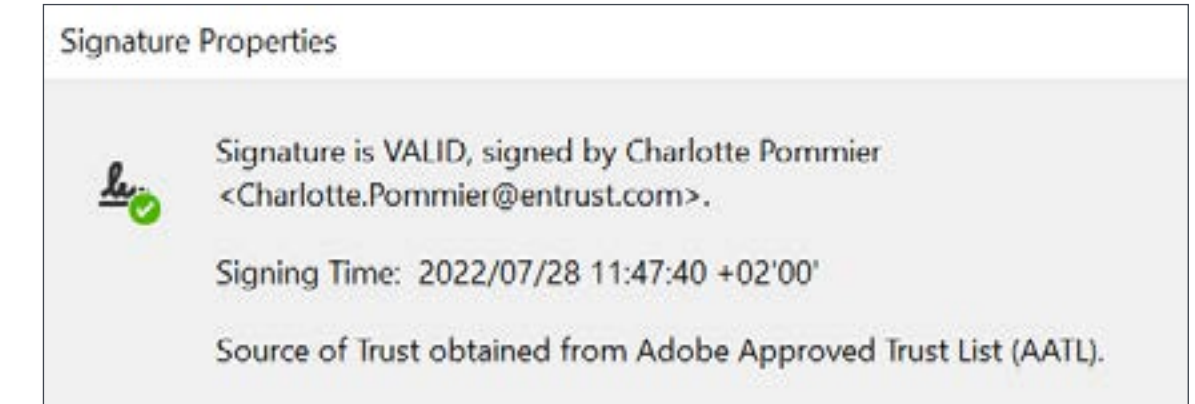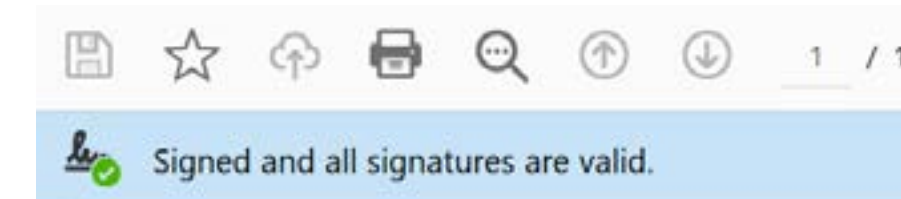
Example

A typical example of an advanced electronic signature is a **digital signature**, which is a signature generated using a digital certificate issued by a trusted certification authority, like Entrust.
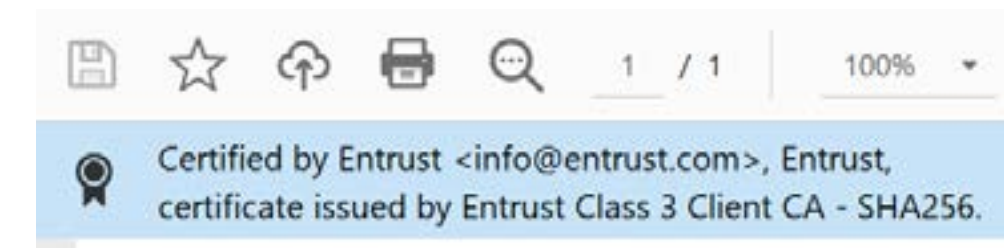
An **advanced signature** can also be obtained if there is sufficient proof of the signatory's identity (for example with an eID). In this case, all the following criteria must be met:

- Their identity has been strongly authenticated

- The signature data is securely recorded

- A digital seal or certification is applied to the signed document to make it tamper-evident
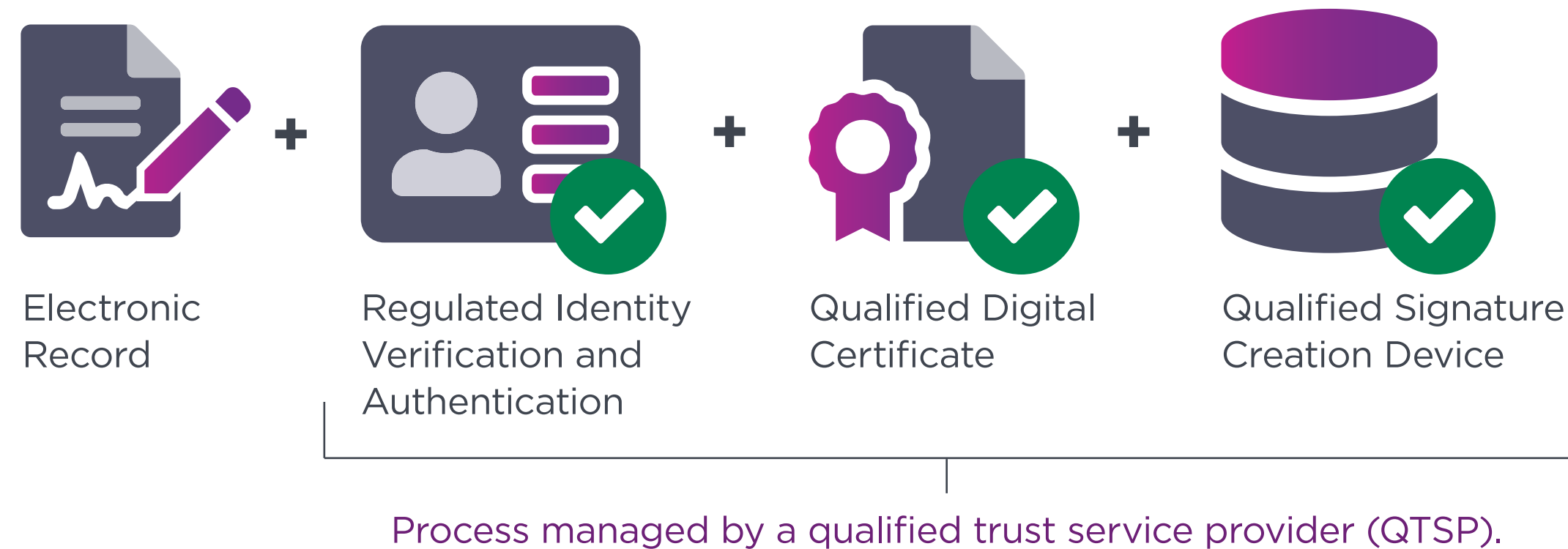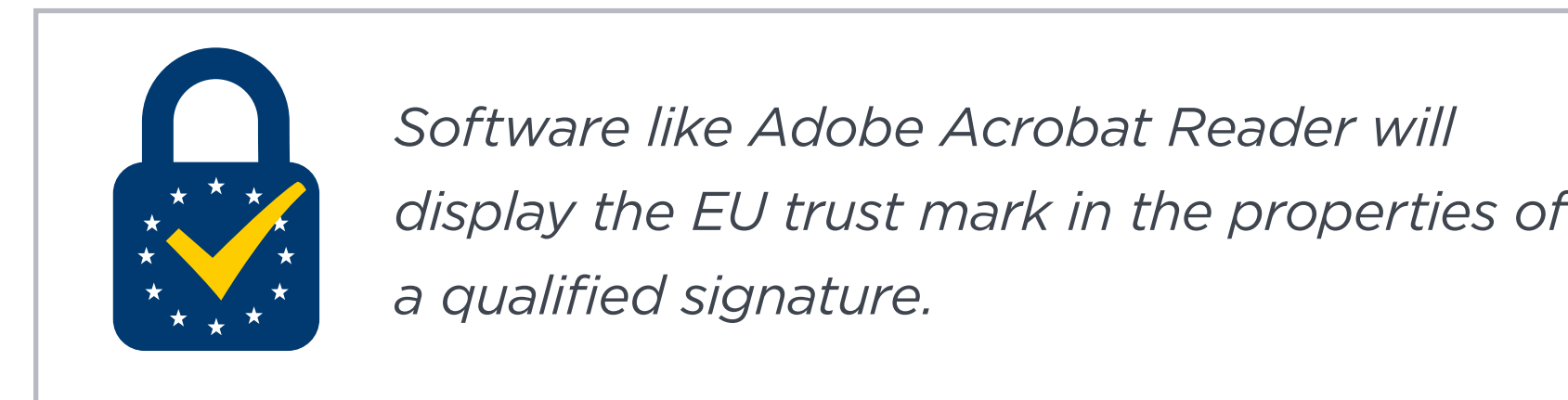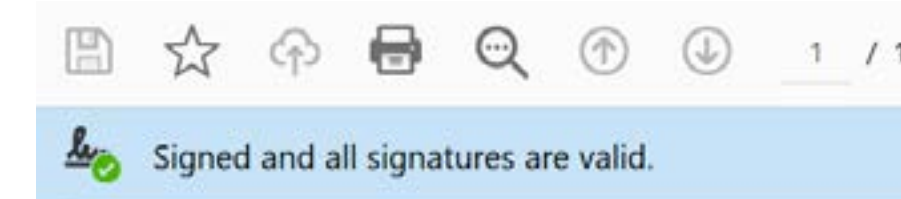
8

Qualified Electronic Signature

Definition

A qualified electronic signature is an advanced electronic signature that's created by a qualified electronic signature creation device, and based on a qualified certificate for electronic signatures.

A qualified electronic signature is, by definition, a digital signature, since it requires a digital certificate.

Requirements

Electronic Record

+

Regulated Identity Verification and Authentication

+

Qualified Digital Certificate

+

Qualified Signature Creation Device

Process managed by a qualified trust service provider (QTSP).

Example

Signed and all signatures are valid.

Signature Properties

Signature is VALID, signed by Charlotte, Laureline, Jennifer POMMIER.

Signing Time: 2023/05/31 15:57:14 +02'00'

Source of Trust obtained from European Union Trusted Lists (EUTL).

This is a Qualified Electronic Signature according to EU Regulation 910/2014

Software like Adobe Acrobat Reader will display the EU trust mark in the properties of a qualified signature.

Digital Certificate types under eIDAS

Overview

	Non-Qualified	**Qualified**
Used for Signatures (Natural Person)	**Certificate for Electronic Signature** Can generate advanced electronic signatures **See page 11**	**Qualified Certificate for Electronic Signature** Can generate advanced and qualified electronic signatures **See page 13**
Used for Seals (Legal Entity)	**Certificate for Electronic Seal** Can generate advanced electronic seals **See page 12**	**Qualified Certificate for Electronic Seal** Can generate advanced and qualified electronic seals **See page 14**

Certificate for Electronic Signature

Definition

A certificate for electronic signature is an electronic attestation that links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person.
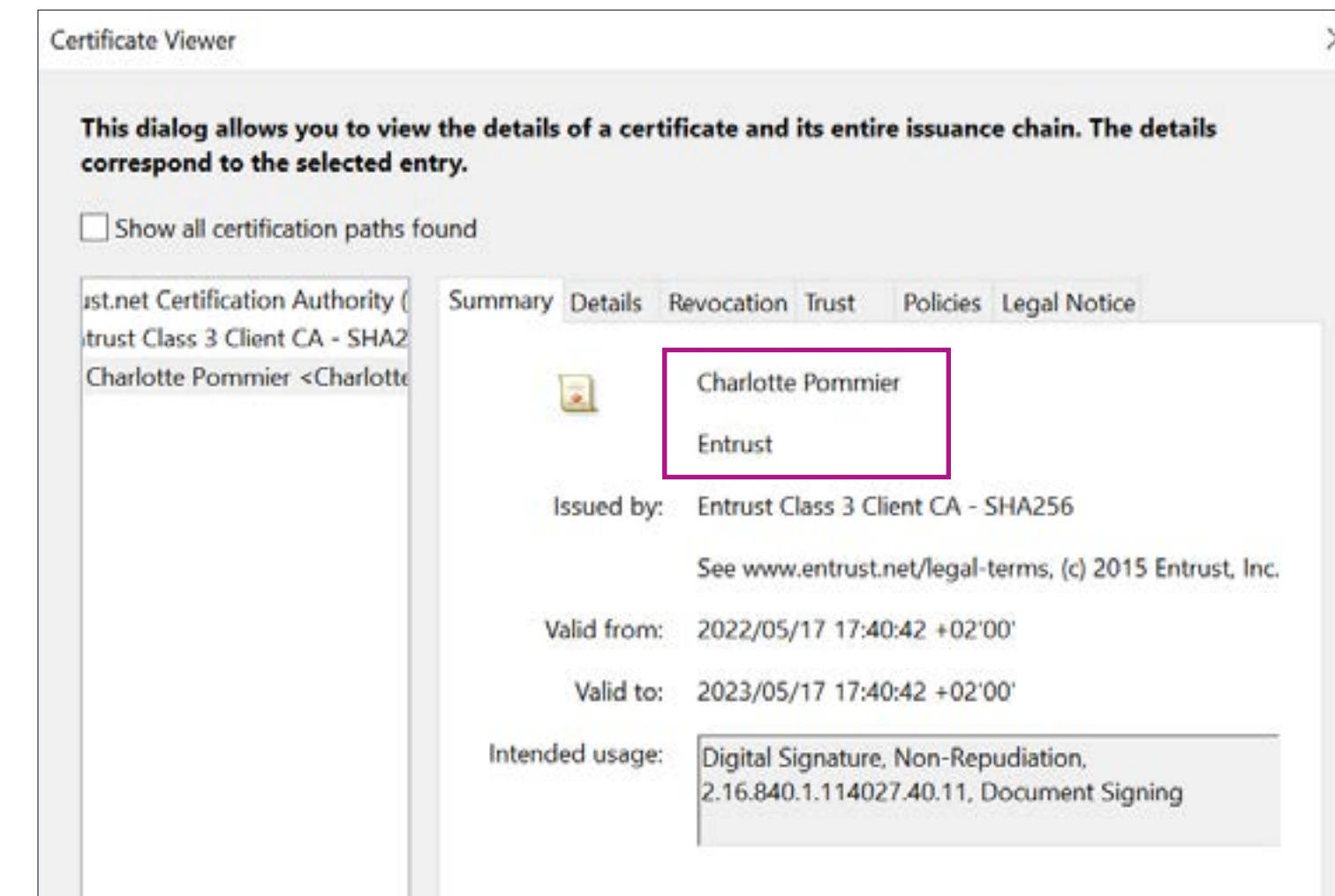
Certificates for electronic signatures are:

- Used for generating advanced electronic signatures
- Also called digital certificates, standard certificates, document signing certificates, or advanced certificates
- Issued by public certification authorities (CA) and trust service providers (TSP)

Requirements

- An identity verification must be performed by the CA or TSP prior to issuance
- eIDAS doesn't provide technical frameworks for this type of certificate; most CAs and TSPs align with WebTrust and AATL (Adobe Approved Trust List) requirements

Example

In Adobe Acrobat Reader's certificate viewer, the certificate contains the details of the person, and if required, the name of the organization they work for.

Can Entrust provide these?
Yes! Learn more about Entrust Certificates for Electronic Signatures

Certificate for Electronic Seal

Definition

A certificate for electronic seal is an electronic attestation that links electronic seal validation data to a legal person (entity) and confirms the name of that person (entity).
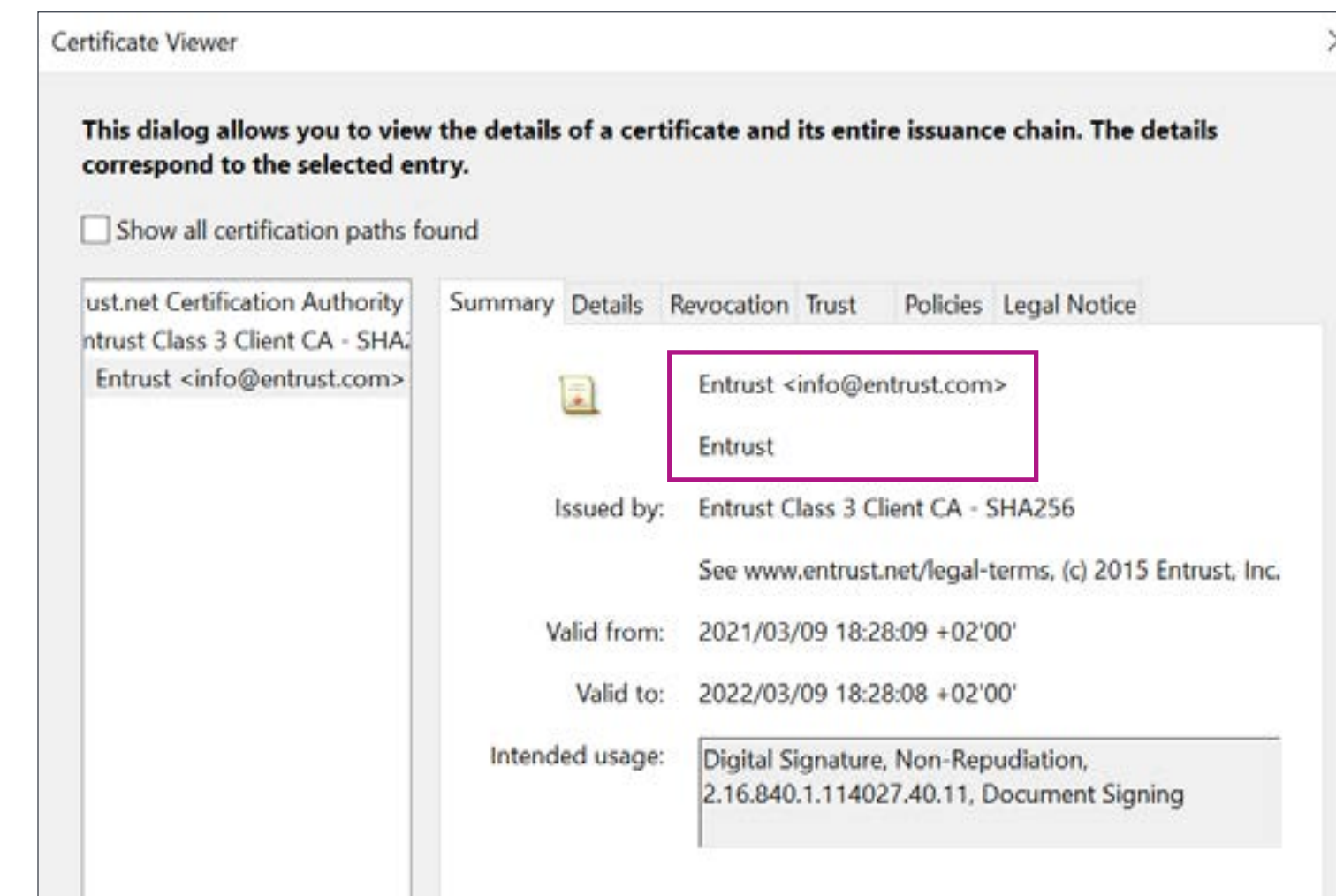
Certificates for electronic signatures are:

- Used for generating advanced electronic seals
- Also called digital seal certificates, sealing certificates, document signing certificate enterprises, or advanced sealing certificates
- Issued by public certification authorities (CA) and trust service providers (TSP)

Requirements

- A verification of the legal entity's existence, good standing, and location must be performed by the CA or TSP prior to issuance
- eIDAS doesn't provide technical frameworks for this type of certificate; most CAs and TSPs align with WebTrust and AATL (Adobe Approved Trust List) requirements

Example

In Adobe Acrobat Reader's certificate viewer, the certificate contains the details of the organization and its email address.

Can Entrust provide these?
Yes! Learn More about Entrust Certificates for Electronic Seals

Qualified Certificate for Electronic Signature

Definition

A qualified certificate for electronic signature is a certificate for an electronic signature that is issued by a qualified trust service provider (QTSP) and meets **these requirements from Annex I of the eIDAS Regulation**.

Qualified certificates for electronic signatures are:

- Used for generating advanced electronic signatures, or qualified electronic signatures when stored in a qualified signature creation device (QSCD)
- Also called qualified signature certificates, QSigCs, or Qsig certificates
- Issued by a QTSP

Requirements

- An identity verification must be performed by the QTSP prior to issuance
- In order to generate a qualified signature, the certificate must be hosted in a QSCD; otherwise it will be only an advanced signature
- eIDAS provides a strong technical framework for the verification of the certificate holder's identity and for the issuance of the certificate
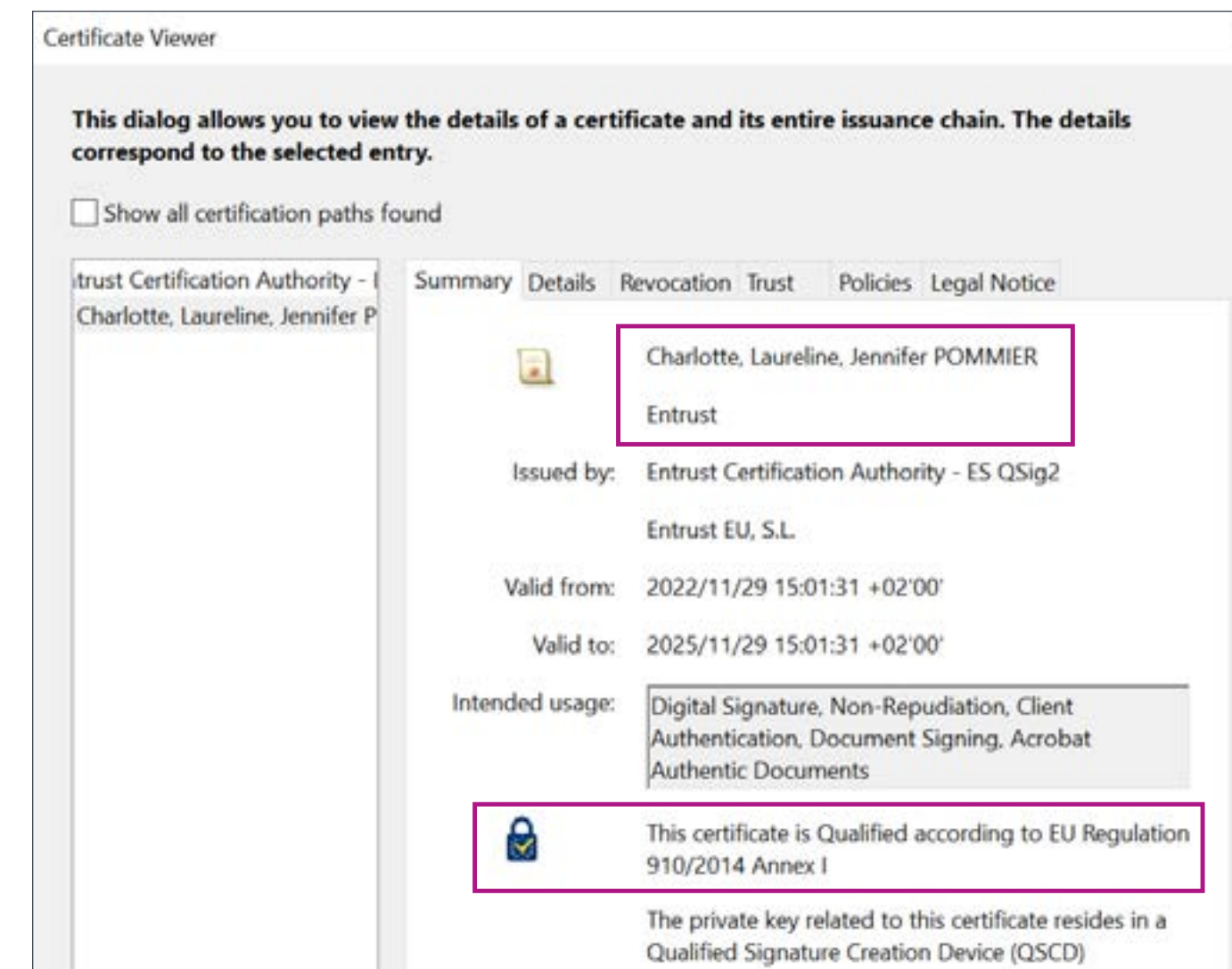
Example

In Adobe Acrobat Reader's certificate viewer, the certificate contains the details of the person, and if required, the name of the organization they work for.

Can Entrust provide these?

Yes, through our Remote Signing Service, we offer qualified certificates for employees' qualified signatures (first name, last name, organization details, organization email address)

Learn more about Entrust Remote Signing Service

Qualified Certificate for Electronic Seal

Definition

A qualified certificate for electronic seal is a certificate for an electronic seal that is issued by a qualified trust service provider (QTSP) and meets **these requirements from Annex III of the eIDAS Regulation.**

Qualified certificates for electronic seals are:

- Used for generating advanced electronic seals, and for generating qualified electronic seals when stored in a qualified signature creation device (QSCD)
- Also called qualified seal certificates, QSealCs, or QSeal certificates
- Issued by a QTSP

Requirements

- A verification of the legal entity's existence, good standing, and location must be performed by the QTSP prior to issuance
- In order to generate qualified seals, the certificate must be hosted in a QSCD; otherwise it will be only an advanced seal
- eIDAS provides a strong technical framework for the verification of the legal entity and for the issuance of the certificate
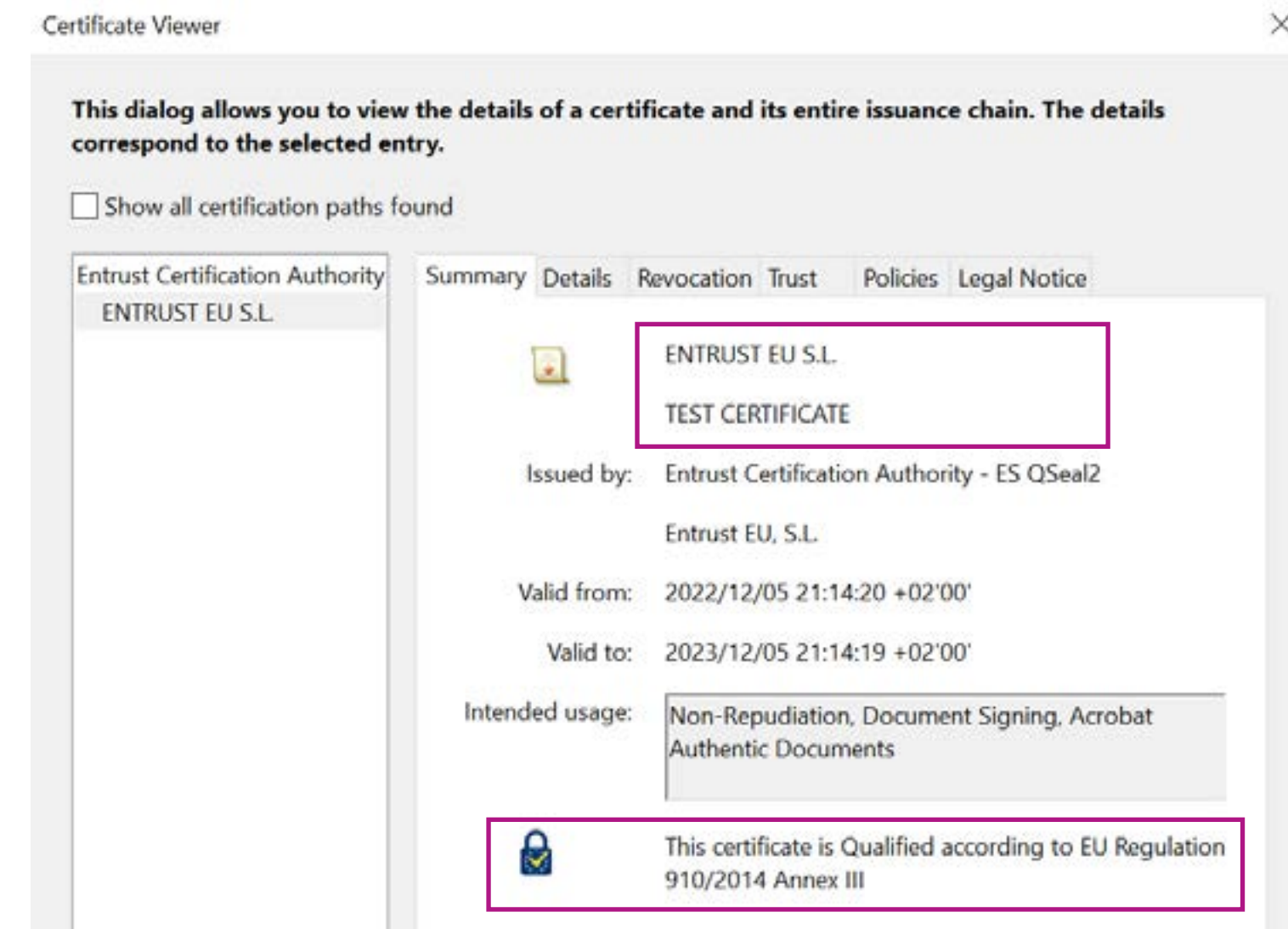
Example

In Adobe Acrobat Reader's certificate viewer, the certificate contains the details of the organization and its email address.
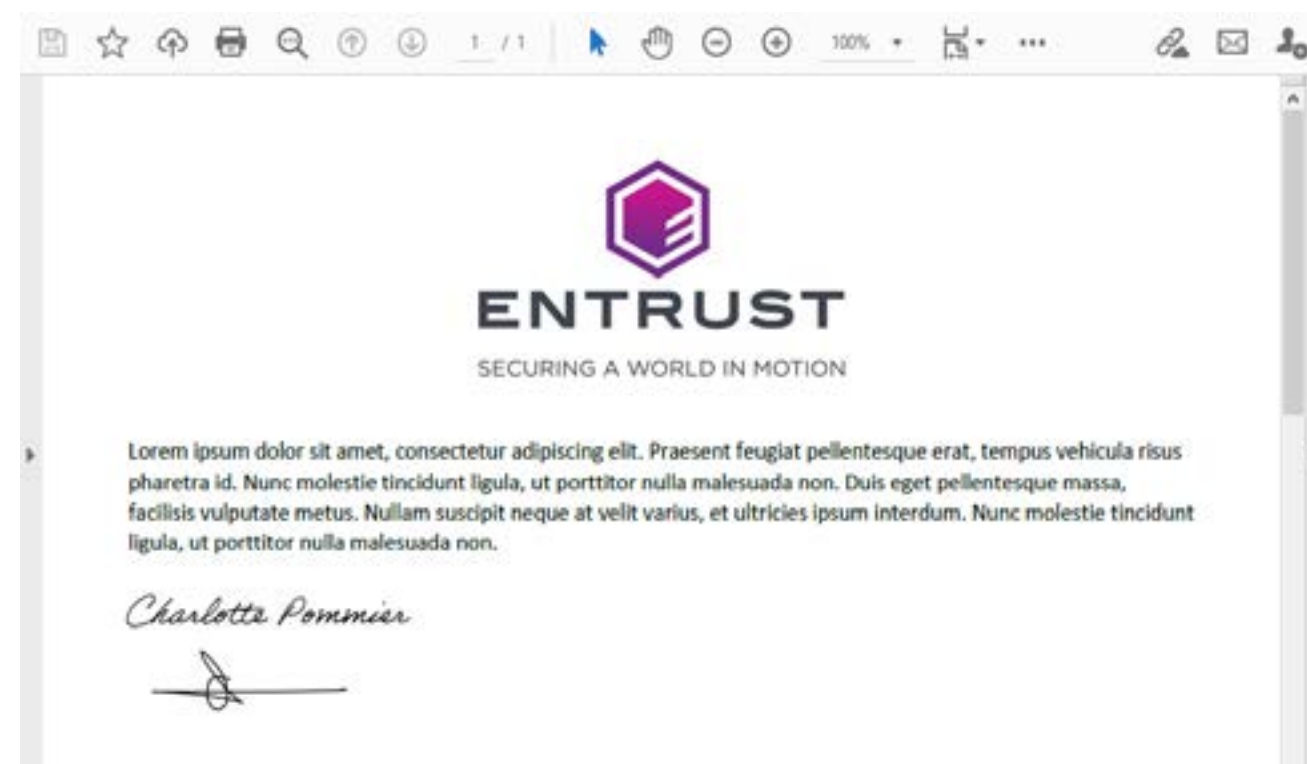
Can Entrust provide these?
Yes, through our Signing Automation Service we provide advanced seals (not hosted in a QSCD).

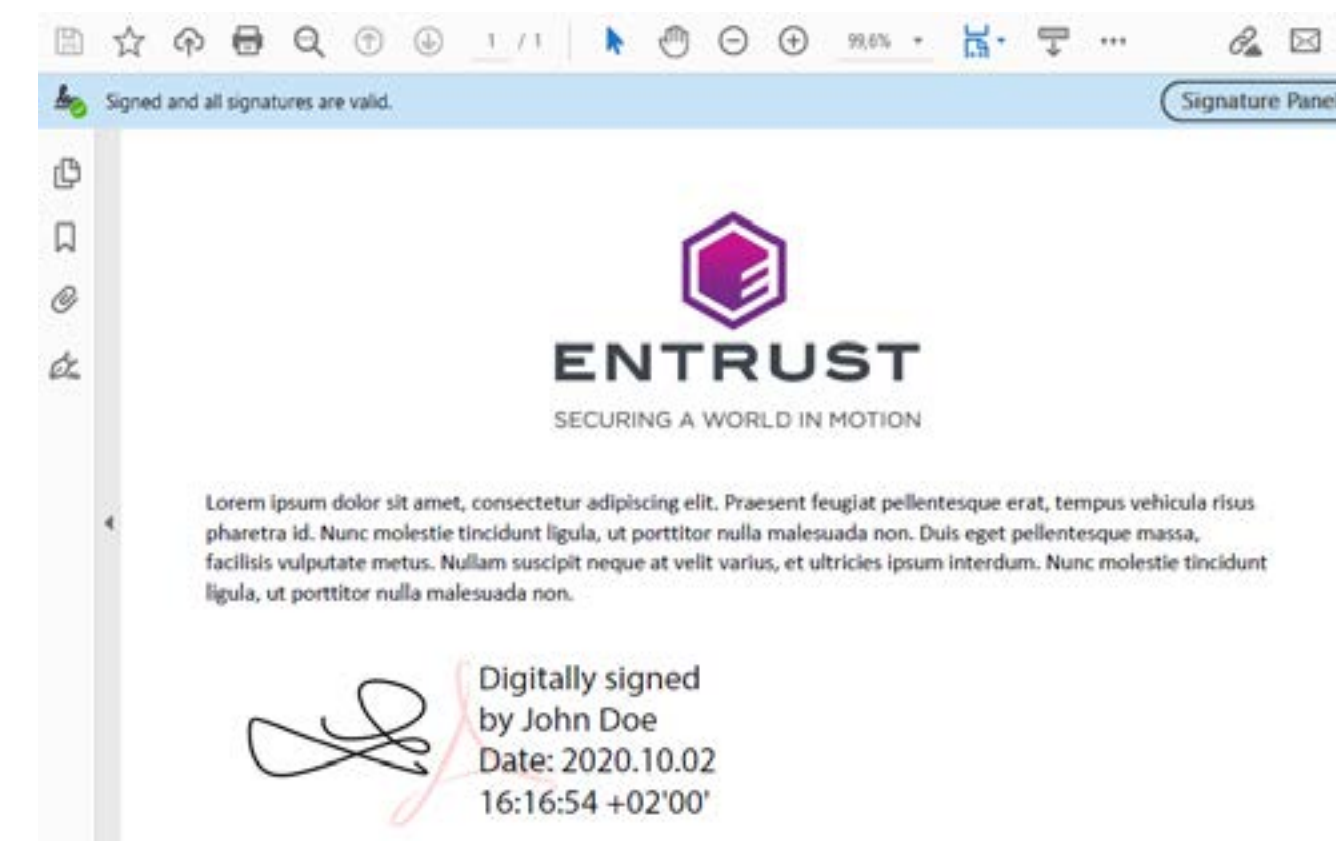**Learn more about Entrust Signing Automation Service**

What's the difference between an electronic signature and a digital signature?

Electronic Signature

An electronic signature is a broad term used to represent a consent or approval in electronic format. It can be a mouse-drawn mark, a finger-drawn mark on a tablet, a box to check, a button to click, a scanned picture of a wet signature, etc.

Digital Signature

A digital signature is a specific type of electronic signature using a digital certificate to generate a cryptographic bond between the document and the signatory. It adds an extra layer of security and identity to provide a higher level of assurance than a simple electronic signature.

Similarly, a seal can be referred to as an **electronic seal** (broad term) or a **digital seal** (when generated using a digital certificate).
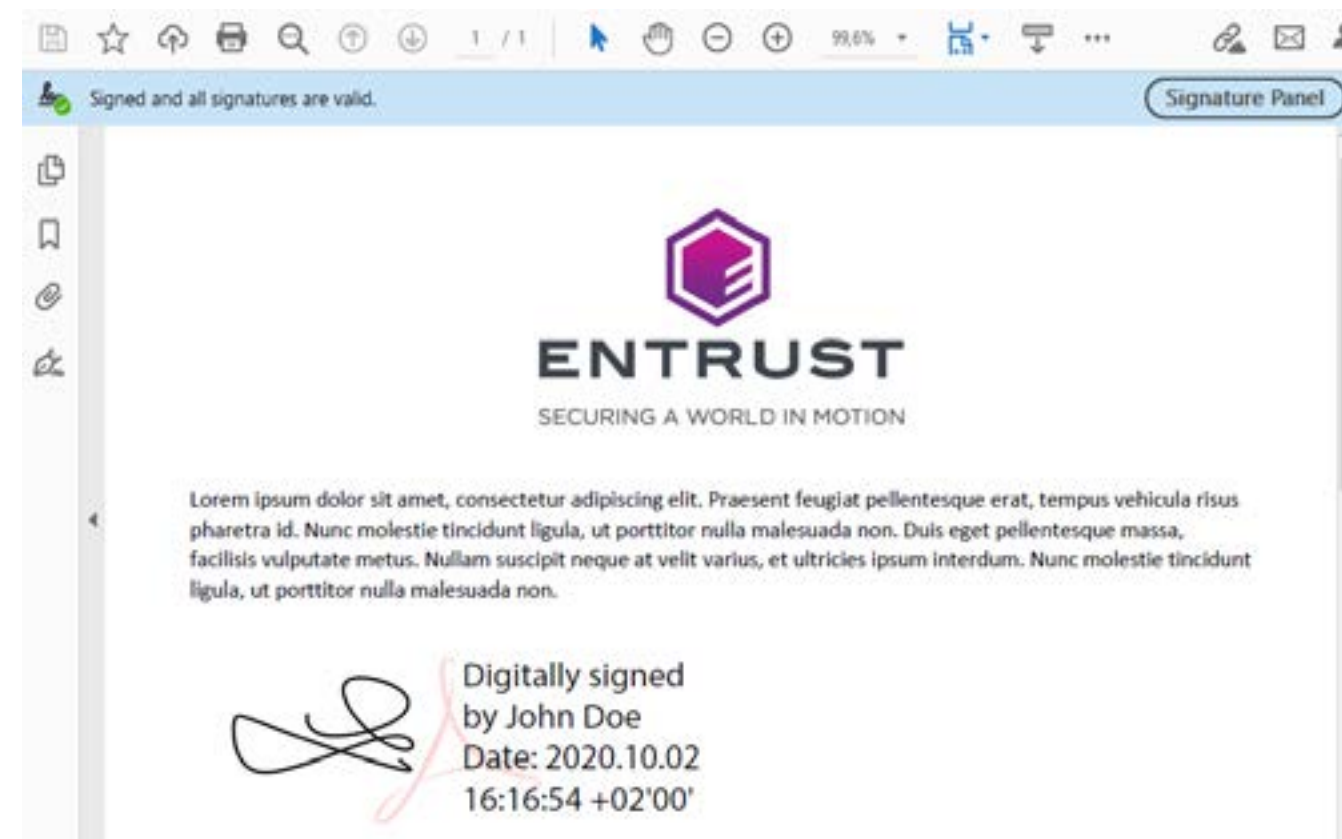
Frequently Asked Questions

What's the difference between a signature and a seal?

Technically speaking, a digital signature and a digital seal are generated exactly the same way. However, these terms have specific meanings under eIDAS and other regulations.

- **An electronic/digital signature represents an individual (natural person)** and usually serves as a proof of approval (e.g., gives consent to the terms included in a document)
- **An electronic/digital seal represents an organization (legal entity)** and usually serves as proof of ownership/authenticity (e.g., certify the content of a document)

Electronic Signature

An electronic signature is "signed" by a person.

Electronic Seal
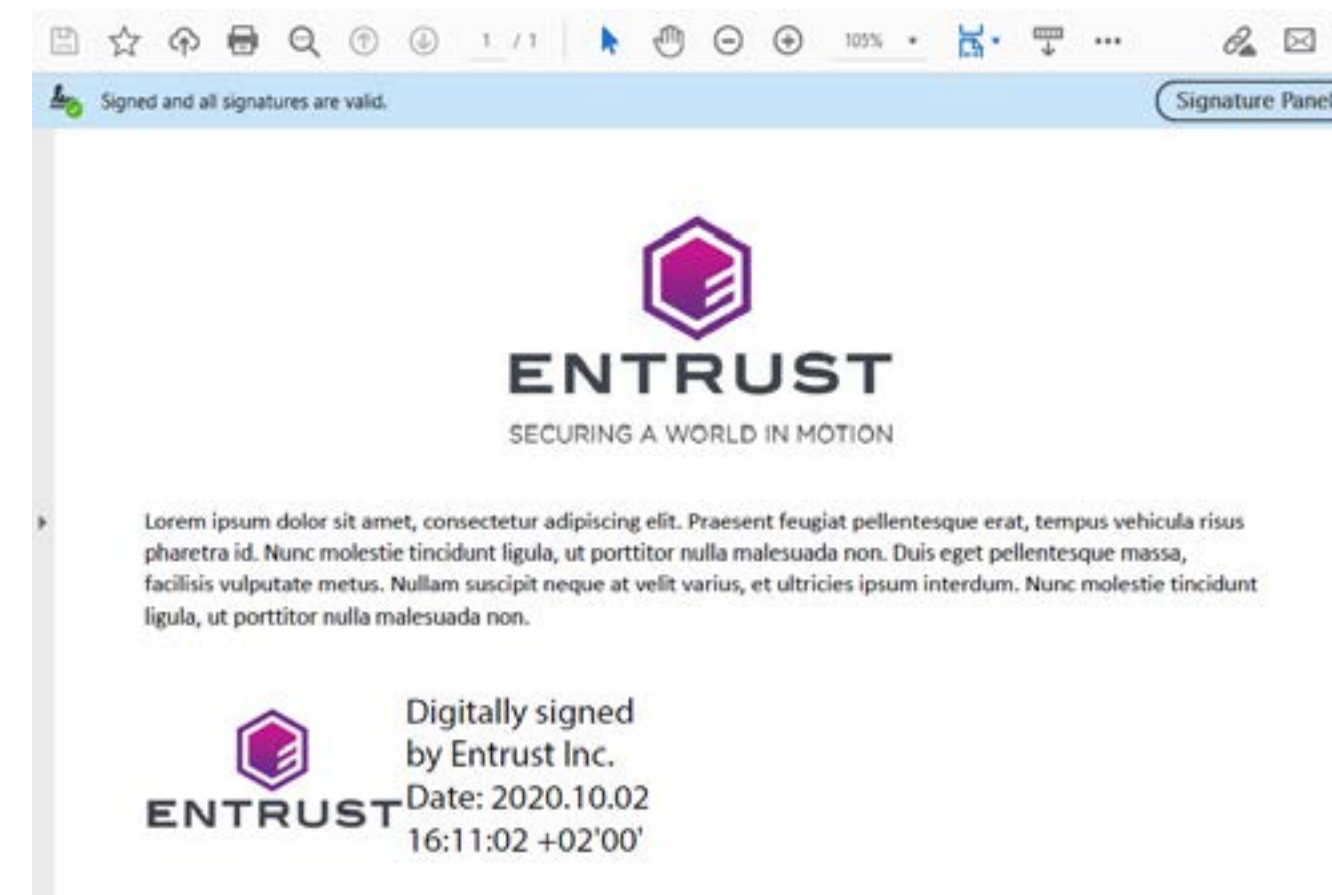
An electronic seal is "signed" by an organization.

Frequently Asked Questions

How do I know which signature type I need?

The suitability, enforceability, or admissibility of electronic signatures will likely depend on many factors, such as:

- The country or state where you operate
- The country or state where the electronic document will be distributed
- The type of electronic document involved

Appropriate legal counsel should be consulted to analyze any potential legal implications and questions related to the use of electronic documents and the use of suitable and/or required solutions to authenticate an electronic signature for their use case.

Requirements can be influenced by:

Country/State Law
e.g., US e-Sign Act

Cross-Border Regulation
e.g., EU eIDAS

Industry Requirement
e.g., KYC, Anti-Money Laundering

Best Practices
e.g., Due Diligence

About Entrust

Our mission

To create and deliver security solutions designed to protect identities, payments, and data for enterprises, citizens, and consumers.

Our digital signing solutions

Entrust is a long-standing expert in PKI infrastructures, a public certification authority, and a qualified trust service provider. Our portfolio includes:
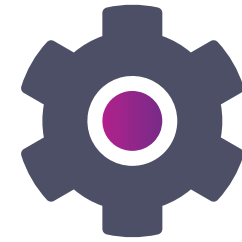
| Document Signing Certificates | Digital Signing as a Service | Cloud-Based Electronic Signing | Signing Infrastructure Deployments | Public Timestamping Service |

We go through stringent audits and accreditations (including WebTrust, and ETSI for eIDAS) to ensure that our digital signing solutions are trusted by software and operating systems across the world.

Digital signatures created using an Entrust-issued digital certificate will be automatically recognized and trusted by major PDF software like Microsoft Office, LibreOffice, Bluebeam software, Adobe Acrobat, and others.

Our signing engines are aligned with eIDAS, and our HSMs are Common Criteria-certified for remote signing deployments.

For more information

+44 (0) 118 953 3000
888.690.2424
+1 952 933 1223
info@entrust.com

entrust.com

ABOUT ENTRUST CORPORATION

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 entrusted to 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.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com   entrust.com/contact