Entrust Document Signing Certificates

Generate identity-verified and secure digital signatures on electronic documents with trusted digital signing certificates from Entrust.

Market Challenge

As organizations continue the transition to online processes, they need to:

1. Optimize and increase confidence in their electronic signing processes
2. Ensure the documents they generate and access are authentic and trusted

Solution

Entrust Document Signing Certificates enable organizations to establish the trust of electronically transmitted documents and digitally sign Adobe and Microsoft Office documents with confidence.

Enabled by proven public key infrastructure (PKI) technology, digital signatures are widely recognized as a best practice for providing digital verification of electronic documents and ensuring strong signing processes.

Combined with timestamping, digital signatures can provide “non-repudiation” – the ability to identify the author and the date of signing and verify that the document has not been changed since it was digitally signed.

BENEFITS

Signatures and seals with high assurance

Digital signatures combine strong identity verification, authenticated signing processes, and document integrity mechanisms to provide the highest levels of admissibility.

Alignment with global standards

- Adobe Approved Trust List (AATL)
- Microsoft Root Program
- EU Trusted Lists (EUTL)

Multiple certificate delivery and management options

- USB tokens
- Hardware security modules
- Cloud (as-a-service)

Learn more about our Document Signing Certificates at entrust.com

Entrust Document Signing Certificates

Entrust Document Signing Certificates for organizations

	Document Signing Group	Document Signing Enterprise	Signing Automation Service
	BUY Or contact us for a custom quote	BUY Or contact us for a custom quote	BUY Or contact us for a custom quote
Signing key delivery and management	**Secure USB token** – We ship you a secure USB token that will generate and store your signing key securely.	**Certificate only** (PEM-format file) – You are responsible for generating and securely storing your signing key and generating a CSR. We will deliver your certificate as a file in PEM format. (HSM required; you can use your own or buy one from us).	**Cloud** – The service generates and stores your signing key in Entrust's secure data center. Signatures are requested via a PKCS#11 API.
Available certificate types	**Standard** – AATL (Adobe Approved Trust List)	**Standard** – AATL (Adobe Approved Trust List)	• **Standard** – AATL (Adobe Approved Trust List) • **eIDAS** qualified (European Union Trusted Lists) for eIDAS advanced signatures (seals)
Recommended if	The organization signatures (seals) will be **manually** applied by a person using their computer.	The organization signatures (seals) will be **automated** (unattended signing, backend process, etc.), and you want to manage your signing key and HSM.	The organization signatures (seals) will be **automated** (unattended signing, backend process, etc.), but you do not want to manage your signing key or any HSM.
Compatible with	**Computers** with active USB ports and a local application with digital signing capabilities such as: • Adobe Acrobat Reader • Microsoft Office • LibreOffice • Bluebeam Revu	**Applications and toolkits** with digital signing capabilities and ability to connect to your HSM.	**Applications and toolkits** with digital signing capabilities and compatibility with PKCS #11, such as iText, Java SDK, Open SDK. Requires Signing Automation Client (included in price) and internet access.
Pricing model	Per certificate - unlimited signatures (seals)	**Lite version (10k, 50k or 100k signatures)**: per certificate and number of signatures (seals)/year **Pro version (unlimited signatures):** per certificate	Per service license, certificate, and number of signatures (seals)/year
Is used primarily for	Signing (sealing) electronic documents as an organization (or a department within an organization)		
The signatures will contain	Organization name (Optional: Organization department) Organization email address Organization city and country		
Certificate validity period	1-3 years		
Timestamping service	Included		
Reissues	Unlimited		

Learn more about our Document Signing Certificates at entrust.com

Entrust Document Signing Certificates

Entrust Document Signing Certificates for individuals

	Document Signing Personal	Document Signing Employee	Remote Signing Service
	BUY Or contact us for a custom quote	BUY Or contact us for a custom quote	BUY Or contact us for a custom quote
Signing key delivery and management	**Secure USB token** – We ship you a secure USB token that will generate and store your signing key securely.	**Secure USB token** – We ship you a secure USB token that will generate and store your signing key securely.	**Cloud** – Employees are enrolled by an administrator in the Entrust Certificate Services (ECS) platform. A signing key and certificate is created for each of them and stored in Entrust's secure data center. Employees connect their Remote Signing Service account to compatible applications to request signatures. A Desktop Virtual Card is available for Windows environments. It enables employees to sign using their local application such as Adobe Acrobat Reader.
Available certificate types	**Standard** – AATL (Adobe Approved Trust List)	**Standard** – AATL (Adobe Approved Trust List)	• **Standard** – AATL (Adobe Approved Trust List) • **eIDAS** qualified (European Union Trusted Lists) for eIDAS qualified signatures
Recommended if	The organization signatures (seals) will be **manually** applied by a person using their computer.	The organization signatures (seals) will be **manually** applied by a person using their computer.	You do not want to depend on USB tokens. You want to enable employees to sign from mobile devices.
Compatible with	**Computers** with active USB ports and a local application with digital signing capabilities such as: • Adobe Acrobat Reader • Microsoft Office • LibreOffice • Bluebeam Revu	**Computers** with active USB ports and a local application with digital signing capabilities such as: • Adobe Acrobat Reader • Microsoft Office • LibreOffice • Bluebeam Revu	**Applications** with digital signing capabilities and compatibility with the Cloud Signature Consortium's remote signing protocol. Native integration with Adobe Sign available. Desktop Virtual Card (software) available for Windows environments.
Pricing model	Per certificate - unlimited signatures (seals)	Per certificate - unlimited signatures (seals)	Per user - unlimited signatures
Is used primarily for	Signing electronic documents as an individual (professional or citizen)	Signing electronic documents as the employee of an organization	Signing electronic documents as the employee of an organization
The signatures will contain	Full name Email address City & Country	Employee full name Employee email address Organization name (Optional: organization department) Organization City & Country	Employee full name Employee email address Organization name (Optional: organization department) Organization City & Country
Certificate validity period	1-3 years		
Timestamping service	Included		
Reissues	Unlimited		

Learn more about our Document Signing Certificates at entrust.com

Entrust Document Signing Certificates

Identity verification process

Standard (AATL) document signing certificates for individuals and employees

Entrust verifies the identity of each individual (professional, citizen, or employee) who is enrolled for a document signing certificate. A passport or supported government-issued ID card (for example, a national ID or driver's license) is required.

Entrust will verify the person's identity using one of the following procedures:

1. Automated video identification, where the user's identity is verified online without a live agent
2. Video identification with a live agent in case the automated video identification is unavailable or cannot be completed

eIDAS Qualified Certificates for employees

These certificates can be issued to EU citizens with a valid passport or national ID. Entrust will verify the user's identity using one of the following procedures:

1. Automated video identification with post-approval (an Entrust verification specialist will review the identification process before the issuance of the qualified certificate). This is the default authentication mechanism used by Entrust.
2. Face-to-face notarized identification in case the automated video identification is unavailable or cannot be completed (the signature on the request for the issuance of a qualified certificate is authenticated in the presence of a notary)[1].

System requirements

Download requirements	Signing requirements		Viewing requirements
Applies to certificates in USB tokens	**Applies to certificates in USB tokens**	**Applies to certificates in HSMs or Signing Automation Service**	**Applies to all products, to display and review signatures**
• Microsoft Windows Operating System – 7, 8.1 • Microsoft Windows Server Operating System – 2008 and 2012 • Microsoft Internet Explorer 10 and 11 • FIPS-validated Software - Provided by Entrust upon purchase	• Microsoft Windows Operating System – 7, 8.1, and 10 • Microsoft Windows Server Operating System – 2008 and 2012 • Adobe Reader • Adobe Acrobat • Microsoft Office Word and Excel • OpenOffice • LibreOffice • FIPS-validated Software – Provided by Entrust upon purchase	Compatible toolkits or software with digital signing capabilities • Adobe LiveCycle • iText • Ascertia ADSS Signing Server • Ascertia SigningHub • /n software SecureBlackbox **For Signing Automation Service: The application must support PKCS#11 (such as iText)**	• Adobe Acrobat Reader or other software that supports digitally signed PDF documents • Microsoft Office Word and Excel

[1] Please note that Entrust can help you find a suitable notary; however Entrust will not cover the costs associated with the notarization process.

Learn more about our Document Signing Certificates at entrust.com

Entrust Document Signing Certificates

Compatible systems and applications

Adobe products	Entrust products	Other products
Sign and Certify **Adobe Acrobat** Certificates can be used with Adobe Acrobat for sign or certification. Certification only comes from an Adobe CDS or AATL CA. Certification indicates that the signer was verified to Adobe's requirements and the private key is protected in hardware. • Adobe Acrobat DC • Adobe Acrobat XI Standard • Adobe Acrobat XI Pro • Adobe Acrobat X Standard • Adobe Acrobat X Pro • Adobe Acrobat 9 Standard **Sign only** **Adobe Acrobat Reader** Users can sign with Reader, but signatures cannot be certified.	**Entrust Signing Automation Service** • SwissSign Let's Sign • iText • Oracle/OpenJDK • Entrust Java Toolkit • Signhost (2023) **Entrust Remote Signing Service** • Adobe Acrobat Sign • SwissSign Let's Sign • Signhost (2023)	**Operating Systems** • Microsoft Windows 2012 R2 • Microsoft Windows Server 2008 R2 SP1 • Microsoft Windows Server 2008 SP2 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 • Microsoft Windows Server 2022 • Microsoft Windows 8.1 • Microsoft Windows 10, version 1709 or later • Microsoft Windows 11 **Software** • OpenOffice • LibreOffice • Bluebeam

Please note: For technical questions related to a third party's product, we advise you to contact the third party's support team.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.K. Phone: +44 (0) 118 953 3000
International Phone: +1 952 933 1223
info@entrust.com **entrust.com/contact**