



ENTRUST



Remote Signing Service

Generate high assurance digital signatures with signing keys securely hosted in the cloud

HIGHLIGHTS

A cloud-based document hash signing service to connect to signing applications

Entrust Remote Signing Service integrates into web and desktop applications to securely generate publicly recognized digital signatures on documents – without the burden of managing digital certificates and signing keys locally.

High assurance signatures for digital agreements

Digital signatures are a special type of electronic signature based on widely recognized PKI technology, which uses digital certificates and signing keys.

Digital signing combines strong identity verification, authenticated signature processes, and document integrity mechanisms to provide the highest levels of assurance for your signatures.*

Trusted by Adobe and eIDAS

Entrust is part of the Adobe Approved Trust List (AATL) and European Union Trusted Lists (EUTL) for the issuance of qualified certificates. All our digital certificates for document signing are natively trusted by Adobe Acrobat solutions.

*The definition and criteria for acceptance of electronic signatures vary by country. Check local regulations for your signing use case.

KEY FEATURES & BENEFITS

- **Workflow-Agnostic:** Use the service with Entrust Signhost or any other compatible signing application
- **Proven Technology and Standards:** Based on globally recognized PKI technology and Cloud Signature Consortium (CSC) remote signing protocols
- **Secure Signing Process:** Only a hash value (fingerprint) of the documents to sign is sent to the Remote Signing Service; the documents to sign never leave the signing application
- **Tamper-Evident Documents:** Digital signatures create read-only documents; any modification will break the digital signature
- **Identity Verification:** Entrust performs a remote identity verification of the signatory prior to issuing a digital certificate; the signatory's verified identity is embedded into the digital signature
- **Timestamping:** Guarantees the exact date and time of signing

[Learn more about our verified signing solutions at entrust.com.](https://www.entrust.com)



Remote Signing Service

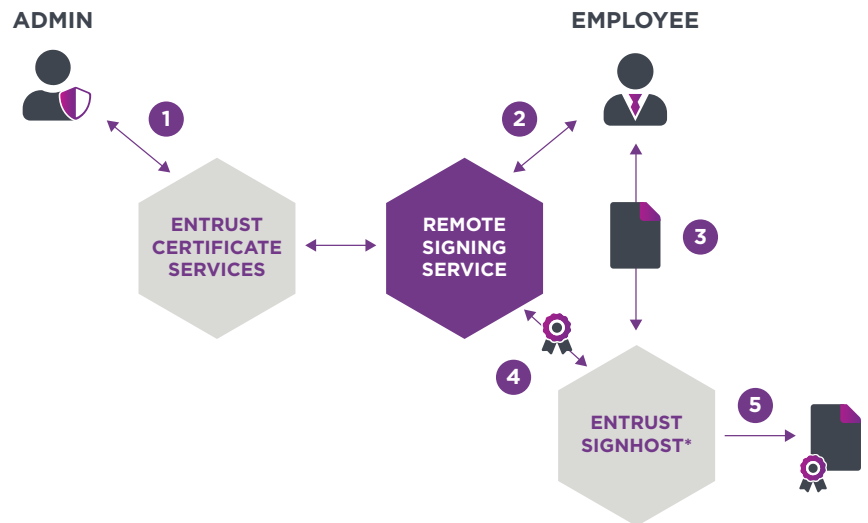
USE CASES

Remote digital signing for the workforce (Adobe-trusted or eIDAS-qualified signature)

Employees are considered frequent signers, often signing documents multiple times a year. Our workforce solution generates long-lived (valid 1-3 years) certificates that employees can activate remotely during each signing process.

Setup process

1. Administrators enroll the employee via the Entrust Certificate Services (ECS) web portal.
2. The enrolled employee goes through a self-service remote video identity verification provided by Entrust. Once the verification is approved, they receive credentials to access the Entrust Remote Signing user portal to generate and manage their certificate.



Signing process

3. Enrolled employees receive or submit a document to sign using a signing application.*
4. Entrust Remote Signing Service is called and prompts the employee to enter their credentials and authorize the use of their certificate for the signature.
5. Once authorized, Entrust Remote Signing Service will generate the raw digital signature and send it to the signing application to be embedded in the final document.

* Entrust Signhost is the signing application we recommend. However any third-party signing application that supports the remote signing API from the Cloud Signature Consortium (CSC) can be used for this use case, including Adobe Acrobat Sign.

WHAT'S INCLUDED

- Entrust Certificate Services account for certificate license management
- Adobe-trusted document signing certificates or eIDAS-qualified certificates for qualified signatures, valid for 1-3 years
- Remote video identity verification for each certificate issued
- User portal for certificate management and signing logs
- Optional desktop virtual card for Microsoft Windows operating systems
- Entrust timestamping services (RFC 3161-compliant or eIDAS-qualified)
- Entrust OCSP services
- Maintenance and support services

Learn more about our verified signing solutions at [entrust.com](https://www.entrust.com).



Remote Signing Service

USE CASES

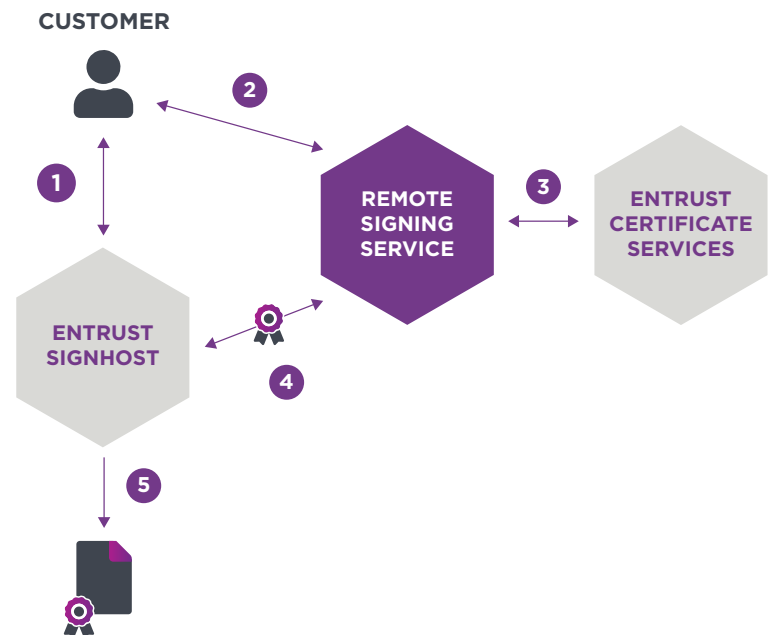
Remote digital signing for customers (eIDAS-qualified signature)

Customers or consumers are considered occasional signers. They likely sign documents only a few times in a year.

Entrust Remote Signing Service provides a self-service remote identity verification that leads to qualified electronic signatures (QES) in a single workflow – without the need for an app download or credentials management. Once the identity verification is approved, the customer is issued a short-lived certificate to complete the transaction and sign document(s).

Signing process

1. The customer receives an invitation from Entrust Signhost to sign a document indicating that identity verification is required.
2. Signhost connects to Entrust Remote Signing Service to trigger an automated remote video identification of the customer.
3. An Entrust-certified agent reviews the collected identity information, per the EU eIDAS regulation. Signhost notifies the customer when the verification is approved.
4. The customer signs the document. Entrust Remote Signing Service creates a short-lived digital certificate that includes the customer's verified information and generates a raw signature that is sent back to Entrust Signhost.
5. Entrust Signhost embeds the eIDAS-qualified digital signature into the final document and adds a timestamp.



Note: Our remote digital signing for customers is based on eIDAS-qualified certificates and therefore available to EU citizens or residents only. It's used specifically with Entrust Signhost (no third-party signing applications).

WHAT'S INCLUDED

- Entrust Certificate Services account for certificate license management
- eIDAS-qualified certificates for qualified signatures, valid for 24 hours
- Remote video identity verification for each certificate issued
- eIDAS-qualified timestamping services
- Maintenance and support services

Learn more about our verified signing solutions at [entrust.com](https://www.entrust.com).



Remote Signing Service

THE ENTRUST ADVANTAGE

Our certifications

Entrust goes through stringent audits and accreditation processes to ensure that our signing solutions are trusted. We are a **publicly trusted certification authority** (CA), a member of the **Adobe Approved Trust List** (AATL), an EU qualified trust service provider in the **EU Trusted Lists** (EUTL) and a member of the **Cloud Signature Consortium** (CSC).

ABOUT ENTRUST

Entrust is an innovative leader in identity-centric security solutions, providing an integrated platform of scalable, AI-enabled security offerings. We enable organizations to safeguard their operations, evolve without compromise, and protect their interactions in an interconnected world – so they can transform their businesses with confidence. Entrust supports customers in 150+ countries and works with a global partner network. We are trusted by the world most trusted organizations.

Learn more at
[entrust.com](https://www.entrust.com)



Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
UK Phone: +44 (0) 118 953 3000

Entrust and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer. ©2024 Entrust Corporation. All rights reserved. SL25Q2-verified-signing-solutions-sb