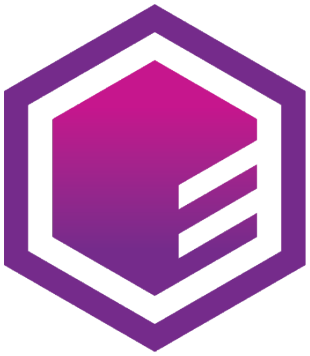

ENTRUST

PUBLIC TRUST CERTIFICATE & SIGNING SERVICES

(NOW DISCONTINUED)

PRODUCT PRIVACY NOTICE

Table of Contents

Public Trust Certificate Services Product Privacy Notice

Last updated: January 14, 2026

Discontinuation Notice & Description

Entrust has sold its public certificate business to Sectigo Limited and as of September 9, 2025, it discontinued Public Trust CA services in the Entrust Certificate Services (ECS) platform. This product privacy notice describes how the Entrust Certificate Services Platform (ECS) and the offerings managed through the platform previously collected and processed personal data pursuant to applicable data privacy laws. Although these services are now discontinued, personal data previously collected will be stored in accordance with this notice for the applicable retention periods.

ECS was a web-based certificate lifecycle management platform that helped manage digital certificates, from both Entrust and other Certification Authorities. It provided access to a host of tools generating detailed reports that helped users to improve uptime, avoid security lapses and preserve brand reputation. ECS provided web-based access to technical insights, status updates, and website scanning for end-to-end lifecycle management of digital certificates.

Personal Data Collection and Processing

Entrust's ECS platform collected the data in the table below for authorized representatives of our customers who interacted with the platform. Some of the offerings managed through ECS also collected additional personal data, as detailed in the offering-specific sections of this notice further below. Biometric data was only processed in case of identity verification via video.

Personal Data Type	Purpose for Processing
Email Address	User authentication
IP Address	Security
Job Title/Position	Account management
First and Last Name	Account management, User authentication
Phone number	Account management, user authentication

Retention Period

Account information will be retained until September 2040.

Use of Sub-Processors

Different sub-processors were used depending on how the customer implemented the ECS platform and the accompanying offerings (e.g., SMS or IDaaS for authentication). Additionally, some public trust certificates required a verification process that may have used sub-processors. For the most recent list of sub-processors, visit https://www.entrust.com/legal-compliance/data-privacy/sub-processors.

International Data Transfers

The ECS platform and the accompanying offerings, and the data collected and stored by Entrust as part of account management (including authentication) are hosted from data centers in Canada or the US. The data collected and stored by Entrust for public-trust identity verification is hosted in data centers in Canada or the US. Depending on the type of certificates purchased, public-trust certificate services may also have included the use of services from sub-processors (e.g., for identity verification, SMS authentication, provision of one-time passwords (OTPs), or data hosting) or third-party controllers or processors (e.g., for certificate issuance, verification and auditing) located in various countries. If a customer is located in a different country than where the data is hosted or where sub-processors or third-party controllers or processors are located, there may be cross-border transfers of personal data. Any cross-border transfers of personal data are made in accordance with relevant data privacy law requirements (e.g., the Standard Contractual Clauses for EEA personal data transferred out of the EEA).

Data Protection Measures

For more information on how Entrust processed personal data collected by the ECS platform and related offerings, please refer to Schedule 2 Annex II to the Standard Contractual Clauses of our standard customer data processing addendum (DPA) found here.

Data Privacy Rights

The customer is a controller of all personal data processed by Entrust for the purpose of providing ECS. Entrust Corporation, as the processor/service provider, will assist the customer, to the extent reasonable and practicable, in responding to data subject requests the customer receives with respect to ECS.

Amendments to this Privacy Notice

Entrust reserves the right to amend this product privacy notice from time to time as our business, laws, regulations and industry standards evolve. Any changes are effective immediately following the posting of such changes to https://www.entrust.com/legal-compliance/product-privacy. We encourage you to review this notice from time to time to stay informed.

Contact Information

For questions about this product privacy notice, please contact privacy@entrust.com. For Entrust's general privacy statement, please click here.

Public Trust TLS/SSL (Website) Certificates

DV SSL, Standard OV SSL, Standard Plus OV SSL, Advantage OV SSL, Multi-domain OV SSL, Wildcard OV SSL, Multi-Domain EV SSL, eIDAS Qualified Website Authentication Certificate (QWAC), PSD2 QWAC

Description

TLS/SSL Certificates provide validated identity and encryption to secure websites.

Verification Process

Entrust collected and processed personal data to comply with industry-mandated verification requirements prior to registering an organization or individual as a subscriber for a public trust website certificate. This verification data was determined by the certificate type and the applicable industry compliance requirements: domain validation (DV), organization validation (OV), extended validation (EV) or eIDAS/PSD2 (Qualified). Specialized sub-processors were used where required to meet compliance requirements.

Where Entrust performed or assisted with verification for an independent Certification Authority, the verification information it collected may be subject to re-verification and/or audit by that Certification Authority. The Certification Authority may act as a processor or controller of that personal data based on the context.

Personal Data Collection and Processing

The following is in addition to the personal data types and purposes for processing disclosed above in connection with the ECS platform.

Personal Data Type	Purpose for Processing
Name	Verification (DV, OV, EV, Qualified)
Title (job title)	Verification (OV, EV, Qualified)
Honorific (Mr./Ms. Mrs.)	Verification (Qualified)
Email address	Verification (OV, EV, Qualified)
Phone number	Verification (OV, EV, Qualified)
Photo, Video of face	Verification (Qualified)
Audio recording of voice	Verification (EV, Qualified)
Identification Document	Verification (Qualified)
Gender	Verification (Qualified)

Mobile Number	Verification (Qualified)

Personal data obtained by means of video identification is blocked with the exception that it can be made available if legally required.

Retention Period

Verification and certificate data will be retained until September 2040.

Verified Mark Certificates (VMC)

Description

Verified Mark Certificates allow companies to show their registered brand logo alongside email communications.

Verification Process

Entrust collected and processed personal data to comply with industry-mandated verification requirements prior to registering an organization or individual as a subscriber for a verified mark certificate. This verification data was determined by applicable industry compliance requirements. Specialized sub-processors were used where required to meet compliance requirements.

Where Entrust performed or assisted with verification for an independent Certification Authority, the verification information it collected may be subject to re-verification and/or audit by that Certification Authority. The Certification Authority may act as a processor or controller of that personal data based on the context.

Personal Data Collection and Processing

The following is in addition to the personal data types and purposes for processing disclosed above in connection with the ECS platform.

Personal Data Type	Purpose for Processing
Name	Verification
Title (job title)	Verification
Honorific (Mr./Ms. Mrs.)	Verification
Email address	Verification
Phone number	Verification
Identification Document	Verification
Photo	Verification
Video	Verification
Audio recording of voice	Verification
Gender	Verification

Retention Period

Verification and certificate data will be retained until September 2040.

S/MIME Certificates

Description

S/MIME Certificates are used to sign, verify, encrypt, and decrypt email.

Verification Process

Entrust collected and processed personal data to comply with industry-mandated verification requirements prior to registering an organization or individual as a subscriber or subject for an S/MIME certificate. This verification data was determined by the applicable industry compliance requirements.

Where Entrust performed or assisted with verification for an independent Certification Authority, the verification information it collected may be subject to re-verification and/or audit by that Certification Authority. The Certification Authority may act as a processor or controller of that personal data based on the context.

Personal Data Collection and Processing

The following is in addition to the personal data types and purposes for processing disclosed above in connection with the ECS platform.

Personal Data Type	Purpose for Processing
Name	Verification, inclusion on certificate
Email address	Verification, inclusion on certificate
Phone Number	Verification
Job Title	Verification

Retention Period

Verification and certificate data will be retained until September 2040.

Code Signing Certificates

OV Code Signing (includes Signing Automation – OV Code Signing Certificate), EV Code Signing (includes Signing Automation – EV Code Signing Certificate)

Description

Code Signing Certificates authenticate the publisher's identity and verify that the digitally signed executables and scripts have not been tampered with since signing.

Verification Process

Entrust collected and processed personal data to comply with industry-mandated verification requirements and for fraud prevention prior to registering an organization or individual as a subscriber for a code signing certificate. This verification data was determined by the certificate type, purchase method (Entrust sales rep-assisted or online store retail purchase), and applicable industry compliance requirements: organization validation (OV) or extended validation (EV). Specialized sub-processors were used where required to meet compliance requirements or for fraud prevention.

Where Entrust performed or assisted with verification for an independent Certification Authority, the verification information it collected may be subject to re-verification and/or audit by that Certification Authority. The Certification Authority may act as a processor or controller of that personal data based on the context.

Personal Data Collection and Processing

The following is in addition to the personal data types and purposes for processing disclosed above in connection with the ECS platform.

Personal Data Type	Purpose for Processing
Name	Verification (OV, EV)
Title (job title)	Verification (OV, EV)
Honorific (Mr./Ms. Mrs.)	Verification (fraud prevention-retail purchase only)
Email address	Verification (OV, EV)
Phone number	Verification (OV, EV)
Audio recording of voice	Verification (OV, EV)
Photo, Video of face	Verification (fraud prevention-retail purchase only)
Identification document	Verification (fraud prevention-retail purchase only)
Gender	Verification

Retention Period

Verification and certificate data will be retained until September 2040.

Document Signing and Sealing Certificates

Document Signing – Personal, Document Signing – Employee (AATL), Document Signing – Group (AATL), Document Signing Enterprise LITE (AATL), Document Signing Enterprise Pro (AATL), PSD2 Qualified Certificate for Electronic Seal (QSealC)

Note that Signing Certificates associated with the Remote Signing Service and Sealing Certificates associated with the Signing Automation Service are covered in the applicable Signing Service sections below in this notice.

Description

Enabled by proven public key infrastructure (PKI) technology, certificate-based digital signatures and seals are widely recognized as a best practice for providing digital verification of electronic transactions. Document Signing and Sealing Certificates provide "non-repudiation," the ability to identify the author and verify that the document has not been changed since it was digitally signed/sealed. Real-time assurance verifies authenticity throughout the lifetime of the signature/seal. Organizations can also use Document Signing and Sealing Certificates to authenticate sensitive documents requiring multiple signatures.

Verification Process

Entrust collected and processed personal data to comply with industry-mandated verification requirements prior to registering an organization or individual as a subscriber or subject for a document signing or sealing certificate. This verification data was determined by the certificate type and the applicable industry compliance requirements. Specialized sub-processors were used where required to meet compliance requirements.

Where Entrust performed or assisted with verification for an independent Certification Authority, the verification information it collected may be subject to re-verification and/or audit by that Certification Authority. The Certification Authority may act as a processor or controller of that personal data based on the context.

Personal Data Collection and Processing

The following is in addition to the personal data types and purposes for processing disclosed above in connection with the ECS platform.

Personal Data Type	Purpose for Processing
Date of birth	Verification
Identification document	Verification
Job Title/Position	Verification

National identification numbers	Verification
Name	Verification
Photo	Verification
Video	Verification
Audio recording of voice	Verification (Qualified)
Gender	Verification
Mobile Number	Verification

For qualified validation, personal data obtained by means of video identification is blocked with the exception that it can be made available if legally required.

Retention Period

Verification and certificate data will be retained until September 2040.

Remote Signing Service (RSS)

Remote Signing Certificate for Employees (AATL), Remote Signing – eIDAS Employee, Remote Signing – eIDAS Consumer, eIDAS Qualified Certificate for Electronic Signature (QSigC)

Description

The Entrust Remote Signing Service was a hosted solution offered in connection with certain certificate types that helped companies and institutions to establish high assurance digital signatures without the need for hardware maintenance or crypto expertise. The Remote Signing service was used to generate employee signing keys and/or sign hashed data. The service was accessible by a user either via the Remote Signing Portal, a web application programming interface (API), or a desktop software client (desktop virtual card). In particular, with the Remote Signing Service, employee signing keys were centrally protected by Entrust within a Hardware Security Module (HSM), and document signatures were approved remotely by users from their device, without the need for a hardware or software token.

Verification Process

Entrust collected and processed personal data to comply with industry-mandated verification requirements prior to registering an individual as a subscriber or subject for a remote signing certificate. This verification data was determined by the applicable industry compliance requirements (AATL or eIDAS/Qualified). Specialized sub-processors were used where required to meet compliance requirements.

Where Entrust performed or assisted with verification for an independent Certification Authority, the verification information it collected may be subject to re-verification and/or audit by that Certification Authority. The Certification Authority may act as a processor or controller of that personal data based on the context.

Verification is not performed in connection with key storage.

Personal Data Collection and Processing

The following is in addition to the personal data types and purposes for processing disclosed above in connection with the ECS platform.

Personal Data Type	Purpose for Processing
Date of birth	Verification (AATL, eIDAS/Qualified)
Identification document	Verification, Inclusion on signature certificates (AATL, eIDAS/Qualified)

Email	Verification, Inclusion on signature certificates (AATL only), RSS account management, user authentication
National identification numbers	Verification (AATL, eIDAS/Qualified)
Name	Verification, Inclusion on signature certificates (AATL, eIDAS/Qualified)
Photo	Verification (AATL, eIDAS/Qualified)
Video	Verification (AATL, eIDAS/Qualified)
Mobile Number	Verification, RSS account management, user authentication (AATL, eIDAS/Qualified)

Personal data obtained by means of video identification is blocked with the exception that it can be made available if legally required.

Retention Period

Verification and certificate data will be retained until September 2040.

Signing Automation Service (SAS)

Signing Automation Document Signing, Signing Automation eIDAS Document Signing, Signing Automation – OV Code Signing Certificate, Signing Automation – EV Code Signing Certificate, eIDAS Qualified Certificate for Electronic Seal (QSealC)

Description

The Entrust Signing Automation Service was a cloud-based service that enabled customers to apply a certificate-based company seal on their documents without the complexity of hardware management and the risks of manual signing. The Signing Automation Service was used to generate signing keys and/or sign hashed data. The service was accessible through a PKCS11 client or Restful API.

Verification Process

Entrust collected and processed personal data to comply with industry-mandated verification requirements prior to registering an individual as a subscriber or subject for a remote signing certificate. This verification data was determined by the applicable industry compliance requirements. Specialized sub-processors are used where required to meet compliance requirements.

Where Entrust performed or assisted with verification for an independent Certification Authority, the verification information it collected may be subject to re-verification and/or audit by that Certification Authority. The Certification Authority may act as a processor or controller of that personal data based on the context.

Verification was not performed in connection with key storage.

Personal Data Collection and Processing

The following is in addition to the personal data types and purposes for processing disclosed above in connection with the ECS platform.

Personal Data Type	Purpose for Processing
Date of birth	Verification (AATL, eIDAS/Qualified)
Identification document	Verification (AATL, eIDAS/Qualified)
Job Title/Position	Verification (OV, EV, AATL, eIDAS/Qualified)
National identification numbers	Verification (AATL, eIDAS/Qualified)
Name	Verification (OV, EV, AATL, eIDAS/Qualified)
Photo	Verification (AATL, eIDAS/Qualified)
Video	Verification (AATL, eIDAS/Qualified)

Audio recording of voice	Verification (OV, EV, eIDAS/Qualified)
Mobile Number	Verification (OV, EV, AATL, eIDAS/Qualified)

Personal data obtained by means of video identification is blocked with the exception that it can be made available if legally required.

Retention Period

Verification and certificate data will be retained until September 2040.

Private Trust Certificates

Private (Shared) SSL, Mobile Device

Not Discontinued

Entrust continues to offer private trust certificates as part of its portfolio of PKI offerings. Please see the applicable Product Privacy Notice for a description of how Entrust collects and processes personal data pursuant to applicable data privacy laws with respect to these private trust offerings.

Public Key Infrastructure as a Service (PKIaaS)

Not Discontinued

Entrust continues to offer Public Key Infrastructure as a Service as part of its portfolio of PKI offerings. Please see the applicable Product Privacy Notice for a description of how Entrust collects and processes personal data pursuant to applicable data privacy laws with respect to this private trust offering.