ENTRUST CERTIFICATE SERVICES

PRODUCT PRIVACY NOTICE

Contents

Entrust Certificate Services Product Privacy Notice

Last updated: April 23, 2024

Entrust Certificate Services Platform

This product privacy notice describes how the Entrust Certificate Services Platform (ECS) and the offerings managed through the platform collect and process personal data pursuant to applicable data privacy laws.

Description

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

Personal Data Collection and Processing

Entrust's ECS platform collects the data in the table below for authorized representatives of our customers who interact with the platform. Some of the offerings managed through ECS also collect additional personal data, as detailed in the offering-specific sections of this notice further below.

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
Password	User authentication
Phone number	Account management, user authentication

Retention Period

Account information is retained for 7 years after account termination unless the account includes ETSI certificates in which case the account information is retained for 15 years after expiration of the last certificate.

Use of Sub-Processors

Different sub-processors are used depending on how the customer implements the ECS platform and the accompanying offerings (e.g., SMS or IDaaS for authentication). Additionally, some public trust certificates require a verification process that may use sub-processors. For the current 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 datacenters in Canada, the EU or the US. The data collected and stored by Entrust as part of public-trust identity verification is hosted in datacenters in Canada. Depending on the type of certificates purchased, may also include the use of services from sub-processors located in various countries (e.g., for identity verification, SMS authentication, provision of one-time passwords (OTPs), or data hosting). To the extent that Customers are in a different country than where the data is hosted or where sub-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 processes 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 the controller for 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, Qualified Website Authentication Certificate (QWAC) eIDAS, QWAC PSD2

Description

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

Verification Process

Entrust collects and processes 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 is 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 are used where required to meet compliance requirements.

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)
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 are kept for 7 years after certificate expiry except for qualified certificates where data is kept for 15 years after certificate expiry.

Verified Mark Certificates (VMC)

Description

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

Verification Process

Entrust collects and processes 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 is determined by applicable industry compliance requirements. Specialized sub-processors are used where required to meet compliance requirements.

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
Gender	Verification

Retention Period

Verification data, certificate data and private key data and logs are kept for 7 years after certificate expiry with the exception that it is kept for 15 years after certificate expiry for qualified certificates.

S/MIME Certificates

Description

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

Verification Process

Entrust collects and processes 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 is determined by the applicable industry compliance requirements.

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 data, certificate data and private key logs are kept for 7 years after certificate expiry.

Code Signing Certificates

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

Description

Entrust 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 collects and processes 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 is 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 are used where required to meet compliance requirements or for fraud prevention.

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)
Photo, Video of face	Verification (fraud prevention-retail purchase only)
Identification document	Verification (fraud prevention-retail purchase only)
Gender	Verification

Retention Period

Verification data and certificate data is kept for 7 years after certificate expiry.

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 further 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. Entrust 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 collects and processes 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 is determined by the certificate type and the applicable industry compliance requirements. Specialized sub-processors are used where required to meet compliance requirements.

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
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 data, certificate data and are kept for 7 years after certificate expiry with the exception of qualified certificates where data is kept for 15 years after certificate expiry.

Remote Signing Service (RSS)

Remote Signing Certificate for Employees (AATL), Remote Signing – eIDAS Employee, Remote Signing – eIDAS Consumer

Description

The Entrust Remote Signing Service is a hosted solution offered in connection with certain certificate types that helps companies and institutions to establish high assurance digital signatures without the need for hardware maintenance or crypto expertise. The Remote Signing service is used to generate employee signing keys and/or sign hashed data. The service is 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 are centrally protected by Entrust within a Hardware Security Module (HSM), and document signatures are approved remotely by users from their device, without the need for a hardware or software token.

Verification Process

Verification is not performed in connection with key storage. Entrust collects and processes 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 is determined by the applicable industry compliance requirements (AATL or eIDAS/Qualified). Specialized sub-processors are used where required to meet compliance requirements.

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)

Retention Period

Verification data, certificate data are kept for 7 years after certificate expiry with the exception of qualified certificates where data is kept for 15 years after certificate expiry. Private keys are not kept beyond the effective date of the certificate with the exception that the qualified certificates are kept for 15 years after certificate expiry.

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,

Description

The Entrust Signing Automation Service is a cloud-based service that enables 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 is used to generate signing keys and/or sign hashed data. The service is accessible through a PKCS11 client or Restful API.

Verification Process

Verification is not performed for key storage. Entrust collects and processes 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 is determined by the applicable industry compliance requirements. Specialized sub-processors are used where required to meet compliance requirements.

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 (AATL, eIDAS/Qualified)
National identification numbers	Verification (AATL, eIDAS/Qualified)
Name	Verification (AATL, eIDAS/Qualified)
Photo	Verification (AATL, eIDAS/Qualified)
Video	Verification (AATL, eIDAS/Qualified)
Mobile Number	Verification (AATL, eIDAS/Qualified)

Retention Period

Verification data, certificate data are kept for 7 years after certificate expiry with the exception of qualified certificates where data is kept for 15 years after certificate expiry.

Private keys are not kept beyond the effective date of the certificate with the exception that qualified certificates are kept for 15 years after certificate expiry.

Private Trust Certificates

Private (Shared) SSL, Mobile Device

Description

Entrust offers a la carte licenses for a limited range of private trust certificates. These certificates are intended for use in private environments. Entrust performs no verification with respect to these private trust certificates. Private trust certificates are also issued as part of a subscription to the PKI as a Service offering (see below).

Personal Data Collection and Processing

No personal data is processed beyond that collected in connection with the ECS platform.

Retention Period

Account information is retained for 7 years after account termination unless the account includes ETSI certificates in which case the account information is retained for 15 years after expiration of the last certificate.

Public Key Infrastructure as a Service (PKIaaS)

Description

Entrust PKIaaS provides cloud-based, highly scalable PKI that is backed by Entrust nShield HSM clusters hosted in Entrust datacenters. PKIaaS provides an agile PKI back-end to applications that require privately trusted certificates, such as mobile device management, user authentication, IoT and DevOps.

Verification Process

PKIaaS can be used by the Customer to generate and issue privately trusted certificates. Entrust does not perform any verification in connection with these certificates.

Personal Data Collection and Processing

No personal data is processed beyond that collected in connection with the ECS platform.

Retention Period

Account information is retained for 7 years after account termination unless the account includes ETSI certificates in which case the account information is retained for 15 years after expiration of the last certificate.