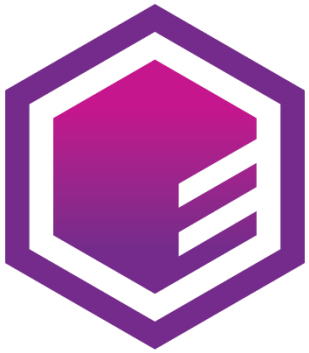

ENTRUST

SERVICIOS DE CERTIFICACIÓN DE ENTRUST

AVISO DE PRIVACIDAD DEL PRODUCTO

Contenido

Aviso de privacidad del producto Servicios de certificación de Entrust

Última actualización: 2 de octubre de 2024

Plataforma de servicios de certificación de Entrust

Este aviso de privacidad del producto describe cómo la plataforma Entrust Certificate Services (ECS) y las ofertas gestionadas a través de la plataforma recopilan y procesan datos personales de conformidad con la legislación aplicable en materia de privacidad de datos.

Descripción

ECS es una plataforma de gestión del ciclo de vida de certificados basada en la Web que lo ayuda a gestionar todos sus certificados digitales de Entrust y otras autoridades de certificación. Brinda acceso a una gran cantidad de herramientas que generan informes detallados para ayudar a los usuarios a mejorar el tiempo de actividad, evitar fallas de seguridad y preservar la reputación de la marca. ECS brinda acceso basado en la Web a conocimientos técnicos, actualizaciones de estado y escaneo de sitios web para la gestión del ciclo de vida de un extremo a otro de todos sus certificados digitales.

Recopilación y tratamiento de datos personales

La plataforma ECS de Entrust recopila los datos de la siguiente tabla para los representantes autorizados de nuestros clientes que interactúan con la plataforma. Algunas de las ofertas gestionadas a través de ECS también recogen datos personales adicionales, como se detalla en las secciones específicas de ofertas de este aviso más adelante. Sólo se tratarán datos biométricos en caso de verificación de identidad mediante vídeo.

Tipo de datos personales	Finalidad del procesamiento
Dirección de correo electrónico	Autenticación del usuario
Dirección IP	Seguridad
Título/puesto	Gestión de cuentas
Nombre y apellido	Gestión de cuentas, Autenticación del usuario
Contraseña	Autenticación del usuario
Número de teléfono	Gestión de cuentas, Autenticación del usuario

Período de conservación

La información de la cuenta se conserva durante 7 años tras la finalización de la cuenta, a menos que la cuenta incluya certificados ETSI, en cuyo caso la información de la cuenta se conserva durante 15 años tras la expiración del último certificado.

Uso de subencargados

Se utilizan diferentes subencargados en función de cómo el cliente implemente la plataforma ECS y las ofertas que la acompañan (por ejemplo, SMS o IDaaS para la autenticación). Además, algunos certificados de confianza pública requieren un proceso de verificación que puede utilizar subencargados. Para consultar la lista actualizada de subencargados, visite https://www.entrust.com/legal-compliance/data-privacy/sub-processors.

Transferencias internacionales de datos

La plataforma ECS y las ofertas que la acompañan, así como los datos recopilados y almacenados por Entrust como parte de la gestión de cuentas (incluida la autenticación) se alojan en centros de datos de Canadá, la UE o EE. UU. Los datos recopilados y almacenados por Entrust para la verificación de identidad de confianza pública se alojan en centros de datos de Canadá. Dependiendo del tipo de certificados adquiridos, los servicios de certificados de confianza pública también pueden incluir el uso de servicios de subencargados (por ejemplo, para verificación de identidad, autenticación por SMS, provisión de contraseñas de un solo uso (OTP) o alojamiento de datos) o terceros responsables del tratamiento o encargados (por ejemplo, para emisión de certificados, verificación y auditoría) ubicados en varios países. En la medida en que los Clientes se encuentren en un país distinto de aquel en el que se alojan los datos o en el que se encuentran los subencargados o terceros responsables del tratamiento o encargados, puede haber transferencias transfronterizas de datos personales. Cualquier transferencia transfronteriza de datos personales se realiza de acuerdo con los requisitos pertinentes de la legislación sobre privacidad de datos (por ejemplo, las Cláusulas contractuales estándar para datos personales del EEE transferidos fuera del EEE).

Medidas de protección de datos

Para obtener más información sobre cómo Entrust procesa los datos personales recopilados por la plataforma ECS y las ofertas relacionadas, consulte el Anexo II del Apéndice 2 de las Cláusulas contractuales estándar de nuestro Anexo sobre el tratamiento de datos de clientes estándar (DPA) que se encuentra aquí.

Derechos de privacidad de datos

El Cliente es un responsable de todos los datos personales procesados por Entrust con el fin de proveer a la ECS. Entrust Corporation, como encargado/proveedor de servicios, ayudará al Cliente, en la medida en que sea razonable y factible, a responder a las solicitudes de acceso a los datos de los interesados que el Cliente reciba con respecto a ECS.

Modificaciones del presente aviso de privacidad

Entrust se reserva el derecho de modificar el presente aviso de privacidad del producto de forma periódica según evolucionen nuestro negocio, la legislación, los reglamentos y las normas del sector. Los cambios entrarán en vigor inmediatamente después de su publicación en https://www.entrust.com/legal-compliance/product-privacy. Lo animamos a revisar este aviso de forma ocasional para mantenerse informado.

Información de contacto

Si tiene alguna pregunta sobre este aviso de privacidad del producto, póngase en contacto con privacy@entrust.com. Para consultar la declaración general de privacidad de Entrust, haga clic aquí.

Certificados TLS/SSL (sitio web) de confianza pública

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

Descripción

Los certificados TLS/SSL proporcionan identidad validada y cifrado para proteger sitios web.

Proceso de verificación

Entrust recopila y procesa datos personales para cumplir los requisitos de verificación exigidos por el sector antes de registrar a una organización o un individuo como suscriptor de un certificado de sitio web de confianza pública. Estos datos de verificación vienen determinados por el tipo de certificado y los requisitos de conformidad del sector aplicables: validación de dominio (DV), validación de organización (OV), validación extendida (EV) o eIDAS/PSD2 (Qualified). Se utilizan subencargados especializados cuando es necesario para cumplir los requisitos de conformidad.

Cuando Entrust realiza o ayuda en la verificación para una Autoridad de Certificación independiente, la información de verificación que recopila podrá estar sujeta a verificación y/o auditoría por parte de dicha Autoridad de Certificación. Dependiendo del contexto, la Autoridad de Certificación podrá actuar como responsable o encargado del tratamiento de esos datos personales.

Recopilación y tratamiento de datos personales

Lo que sigue se añade a los tipos de datos personales y a los fines del tratamiento revelados anteriormente en relación con la plataforma ECS.

Tipo de datos personales	Finalidad del procesamiento
Nombre	Verificación (DV, OV, EV, Qualified)
Título (cargo)	Verificación (OV, EV, Qualified)
Honorífico (Sr./Sra.)	Verificación (Qualified)
Dirección de correo electrónico	Verificación (OV, EV, Qualified)
Número de teléfono	Verificación (OV, EV, Qualified)
Foto, video de cara	Verificación (Qualified)
Grabación de audio de voz	Verificación (EV, Qualified)
Documento de identificación	Verificación (Qualified)

Género	Verificación (Qualified)
Número de teléfono móvil	Verificación (Qualified)

Los datos personales obtenidos mediante identificación por video están bloqueados, con la excepción de que pueden ponerse a disposición si así lo exige la ley.

Período de conservación

Los datos de verificación y de los certificados se conservan durante 7 años tras la expiración del certificado, excepto en el caso de los certificados cualificados, en los que los datos se conservan durante 15 años tras la expiración del certificado.

Certificados de marca verificada (VMC)

Descripción

Los certificados de marca verificada permiten a las empresas mostrar el logotipo de su marca registrada en las comunicaciones por correo electrónico.

Proceso de verificación

Entrust recopila y procesa datos personales para cumplir los requisitos de verificación exigidos por el sector antes de registrar a una organización o un individuo como suscriptor de un certificado de marca verificada. Estos datos de verificación vienen determinados por los requisitos de conformidad del sector aplicables. Se utilizan subencargados especializados cuando es necesario para cumplir los requisitos de conformidad.

Cuando Entrust realiza o ayuda en la verificación para una Autoridad de Certificación independiente, la información de verificación que recopila podrá estar sujeta a verificación y/o auditoría por parte de dicha Autoridad de Certificación. Dependiendo del contexto, la Autoridad de Certificación podrá actuar como responsable o encargado del tratamiento de esos datos personales.

Recopilación y tratamiento de datos personales

Lo que sigue se añade a los tipos de datos personales y a los fines del tratamiento revelados anteriormente en relación con la plataforma ECS.

Tipo de datos personales	**Finalidad del procesamiento**
Nombre	Verificación
Título (cargo)	Verificación
Honorífico (Sr./Sra.)	Verificación
Dirección de correo electrónico	Verificación
Número de teléfono	Verificación
Documento de identificación	Verificación
Foto	Verificación
Video	Verificación
Grabación de audio de voz	Verificación
Género	Verificación

Período de conservación

Los datos de verificación, los datos de certificados y los datos de clave privada, al igual que los registros, se conservan durante 7 años tras la expiración del certificado, excepto en el caso de los certificados cualificados, en los que los datos se conservan durante 15 años tras la expiración del certificado.

Certificados S/MIME

Descripción

Los certificados S/MIME de Entrust se utilizan para firmar, verificar, cifrar y descifrar el correo electrónico.

Proceso de verificación

Entrust recopila y procesa datos personales para cumplir los requisitos de verificación exigidos por el sector antes de registrar a una organización o un individuo como suscriptor o sujeto de un certificado S/MIME. Estos datos de verificación vienen determinados por los requisitos de conformidad del sector aplicables.

Cuando Entrust realiza o ayuda en la verificación para una Autoridad de Certificación independiente, la información de verificación que recopila podrá estar sujeta a verificación y/o auditoría por parte de dicha Autoridad de Certificación. Dependiendo del contexto, la Autoridad de Certificación podrá actuar como responsable o encargado del tratamiento de esos datos personales.

Recopilación y tratamiento de datos personales

Lo que sigue se añade a los tipos de datos personales y a los fines del tratamiento revelados anteriormente en relación con la plataforma ECS.

Tipo de datos personales	Finalidad del procesamiento
Nombre	Verificación, inclusión en el certificado
Dirección de correo electrónico	Verificación, inclusión en el certificado
Número de teléfono	Verificación
Cargo	Verificación

Período de conservación

Los datos de verificación, los datos del certificado y los registros de claves privadas se conservan durante 7 años tras la expiración del certificado.

Certificados de firma de código

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

Descripción

Los certificados de firma de código de Entrust autentican la identidad del editor y verifican que los ejecutables y los scripts con firma digital no hayan sido manipulados desde su firma.

Proceso de verificación

Entrust recopila y procesa datos personales para cumplir los requisitos de verificación exigidos por el sector y para evitar el fraude antes de registrar a una organización o un individuo como suscriptor de un certificado de firma de código. Estos datos de verificación están determinados por el tipo de certificado, el método de compra (compra asistida por un representante de ventas de Entrust o compra minorista en tienda en línea) y los requisitos de conformidad del sector aplicables: validación de organización (OV) o validación extendida (EV). Se utilizan subencargados especializados cuando es necesario para cumplir los requisitos de conformidad o para evitar el fraude.

Cuando Entrust realiza o ayuda en la verificación para una Autoridad de Certificación independiente, la información de verificación que recopila podrá estar sujeta a verificación y/o auditoría por parte de dicha Autoridad de Certificación. Dependiendo del contexto, la Autoridad de Certificación podrá actuar como responsable o encargado del tratamiento de esos datos personales.

Recopilación y tratamiento de datos personales

Lo que sigue se añade a los tipos de datos personales y a los fines del tratamiento revelados anteriormente en relación con la plataforma ECS.

Tipo de datos personales	Finalidad del procesamiento
Nombre	Verificación (OV, EV)
Título (cargo)	Verificación (OV, EV)
Honorífico (Sr./Sra.)	Verificación (prevención del fraude, solo compras minoristas)
Dirección de correo electrónico	Verificación (OV, EV)
Número de teléfono	Verificación (OV, EV)
Grabación de audio de voz	Verificación (OV, EV)
Foto, video de cara	Verificación (prevención del fraude, solo compras minoristas)

Documento de identificación	Verificación (prevención del fraude, solo compras minoristas)
Género	Verificación

Período de conservación

Los datos de verificación y los datos del certificado se conservan durante 7 años tras la expiración del certificado.

Certificados para firmar y sellar documentos

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)

Tenga en cuenta que los Certificados de firma asociados al Servicio de firma remota y los Certificados de sellado asociados al Servicio de automatización de firma se tratan en las secciones correspondientes del Servicio de firma más adelante en este aviso.

Descripción

Gracias a la tecnología de infraestructura de clave pública (PKI), las firmas y los sellos digitales basados en certificados están ampliamente reconocidos como la mejor práctica para la verificación digital de las transacciones electrónicas. Los certificados para firmar y sellar documentos de Entrust proporcionan «no repudio», la capacidad de identificar al autor y verificar que el documento no se ha modificado desde que se firmó/selló digitalmente. La garantía en tiempo real verifica la autenticidad durante toda la vida útil de la firma/sello. Las organizaciones también pueden utilizar certificados para firmar y sellar documentos para autenticar documentos confidenciales que requieran varias firmas.

Proceso de verificación

Entrust recopila y procesa datos personales para cumplir los requisitos de verificación exigidos por el sector antes de registrar a una organización o un individuo como suscriptor o sujeto de un certificado para firmar y sellar documentos. Estos datos de verificación vienen determinados por el tipo de certificado y los requisitos de conformidad del sector aplicables. Se utilizan subencargados especializados cuando es necesario para cumplir los requisitos de conformidad.

Cuando Entrust realiza o ayuda en la verificación para una Autoridad de Certificación independiente, la información de verificación que recopila podrá estar sujeta a verificación y/o auditoría por parte de dicha Autoridad de Certificación. Dependiendo del contexto, la Autoridad de Certificación podrá actuar como responsable o encargado del tratamiento de esos datos personales.

Recopilación y tratamiento de datos personales

Lo que sigue se añade a los tipos de datos personales y a los fines del tratamiento revelados anteriormente en relación con la plataforma ECS.

Tipo de datos personales	Finalidad del procesamiento
Fecha de nacimiento	Verificación
Documento de identificación	Verificación
Título/puesto	Verificación

Números nacionales de identificación	Verificación
Nombre	Verificación
Foto	Verificación
Video	Verificación
Grabación de audio de voz	Verificación (Qualified)
Género	Verificación
Número de teléfono móvil	Verificación

Para la validación cualificada, los datos personales obtenidos mediante identificación por video están bloqueados, con la excepción de que pueden ponerse a disposición si así lo exige la ley.

Período de conservación

Los datos de verificación y de los certificados se conservan durante 7 años tras la expiración del certificado, excepto en el caso de los certificados cualificados, en los que los datos se conservan durante 15 años tras la expiración del certificado.

Servicio de firma remota (RSS)

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

Descripción

El Servicio de firma remota de Entrust es una solución alojada que se ofrece en conexión con ciertos tipos de certificados que ayuda a empresas e instituciones a establecer firmas digitales de alta seguridad sin la necesidad de mantenimiento de hardware o experiencia en criptografía. El servicio de firma remota se utiliza para generar claves de firma de los empleados o firmar datos con hash. El usuario puede acceder al servicio a través del Portal de firma remota, una interfaz de programación de aplicaciones web (API) o un cliente de software de escritorio (tarjeta virtual de escritorio). En particular, con el servicio de firma remota, las claves de firma de los empleados están protegidas de forma centralizada por Entrust dentro de un Módulo de seguridad de hardware (HSM), y las firmas de documentos son aprobadas de forma remota por los usuarios desde su dispositivo, sin necesidad de un token de hardware o software.

Proceso de verificación

Entrust recopila y procesa datos personales para cumplir los requisitos de verificación exigidos por el sector antes de registrar a un individuo como suscriptor o sujeto de un certificado de firma remota. Estos datos de verificación vienen determinados por los requisitos de conformidad del sector aplicables (AATL o eIDAS/Qualified). Se utilizan subencargados especializados cuando es necesario para cumplir los requisitos de conformidad.

Cuando Entrust realiza o ayuda en la verificación para una Autoridad de Certificación independiente, la información de verificación que recopila podrá estar sujeta a verificación y/o auditoría por parte de dicha Autoridad de Certificación. Dependiendo del contexto, la Autoridad de Certificación podrá actuar como responsable o encargado del tratamiento de esos datos personales.

La verificación no se realiza en relación con el almacenamiento de claves.

Recopilación y tratamiento de datos personales

Lo que sigue se añade a los tipos de datos personales y a los fines del tratamiento revelados anteriormente en relación con la plataforma ECS.

Tipo de datos personales	Finalidad del procesamiento
Fecha de nacimiento	Verificación (AATL, eIDAS/Qualified)
Documento de identificación	Verificación, inclusión en certificados de firma (AATL, eIDAS/Qualified)

Correo electrónico	Verificación, inclusión en certificados de firma (solo AATL), gestión de cuentas RSS, autenticación del usuario
Números nacionales de identificación	Verificación (AATL, eIDAS/Qualified)
Nombre	Verificación, inclusión en certificados de firma (AATL, eIDAS/Qualified)
Foto	Verificación (AATL, eIDAS/Qualified)
Video	Verificación (AATL, eIDAS/Qualified)
Número de teléfono móvil	Verificación, gestión de cuentas RSS, autenticación del usuario (AATL, eIDAS/Qualified)

Los datos personales obtenidos mediante identificación por video están bloqueados, con la excepción de que pueden ponerse a disposición si así lo exige la ley.

Período de conservación

Los datos de verificación y de los certificados se conservan durante 7 años tras la expiración del certificado, excepto en el caso de los certificados cualificados, en los que los datos se conservan durante 15 años tras la expiración del certificado. Las claves privadas no se conservan más allá de la fecha de expiración del certificado, con la excepción de que los certificados cualificados se conservan durante 15 años tras la expiración del certificado.

Servicio de automatización de firmas (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)

Descripción

El Servicio de automatización de firmas de Entrust es un servicio basado en la nube que permite a los Clientes aplicar un sello de empresa basado en certificados en sus documentos sin la complejidad de la gestión de hardware y los riesgos de la firma manual. El servicio de automatización de firmas se utiliza para generar claves de firma o firmar datos con hash. Se puede acceder al servicio a través de un cliente PKCS11 o una API Restful.

Proceso de verificación

Entrust recopila y procesa datos personales para cumplir los requisitos de verificación exigidos por el sector antes de registrar a un individuo como suscriptor o sujeto de un certificado de firma remota. Estos datos de verificación vienen determinados por los requisitos de conformidad del sector aplicables. Se utilizan subencargados especializados cuando es necesario para cumplir los requisitos de conformidad.

Cuando Entrust realiza o ayuda en la verificación para una Autoridad de Certificación independiente, la información de verificación que recopila podrá estar sujeta a verificación y/o auditoría por parte de dicha Autoridad de Certificación. Dependiendo del contexto, la Autoridad de Certificación podrá actuar como responsable o encargado del tratamiento de esos datos personales.

La verificación no se realiza en relación con el almacenamiento de claves.

Recopilación y tratamiento de datos personales

Lo que sigue se añade a los tipos de datos personales y a los fines del tratamiento revelados anteriormente en relación con la plataforma ECS.

Tipo de datos personales	Finalidad del procesamiento
Fecha de nacimiento	Verificación (AATL, eIDAS/Qualified)
Documento de identificación	Verificación (AATL, eIDAS/Qualified)
Título/puesto	Verificación (OV, EV, AATL, eIDAS/Qualified)
Números nacionales de identificación	Verificación (AATL, eIDAS/Qualified)
Nombre	Verificación (OV, EV, AATL, eIDAS/Qualified)

Foto	Verificación (AATL, eIDAS/Qualified)
Video	Verificación (AATL, eIDAS/Qualified)
Grabación de audio de voz	Verificación (OV, EV, eIDAS/Qualified)
Número de teléfono móvil	Verificación (OV, EV, AATL, eIDAS/Qualified)

Los datos personales obtenidos mediante identificación por video están bloqueados, con la excepción de que pueden ponerse a disposición si así lo exige la ley.

Período de conservación

Los datos de verificación y de los certificados se conservan durante 7 años tras la expiración del certificado, excepto en el caso de los certificados cualificados, en los que los datos se conservan durante 15 años tras la expiración del certificado.

Las claves privadas no se conservan más allá de la fecha de expiración del certificado, con la excepción de que los certificados cualificados se conservan durante 15 años tras la expiración del certificado.

Certificados de confianza privada

SSL privado (compartido), dispositivo móvil

Descripción

Entrust ofrece licencias a la carta para una gama limitada de certificados de confianza privada. Estos certificados están pensados para su uso en entornos privados. Entrust no realiza ninguna verificación con respecto a estos certificados de confianza privada. Los certificados de confianza privada también se emiten como parte de una suscripción a la oferta de PKI como servicio (véase más abajo).

Recopilación y tratamiento de datos personales

No se procesa ningún dato personal aparte de los que se recopilan en relación con la plataforma ECS.

Período de conservación

La información de la cuenta se conserva durante 7 años tras la finalización de la cuenta, a menos que la cuenta incluya certificados ETSI, en cuyo caso la información de la cuenta se conserva durante 15 años tras la expiración del último certificado.

Public Key Infrastructure as a Service (PKIaaS, Infraestructura de clave pública como servicio)

Descripción

PKIaaS de Entrust proporciona una PKI basada en la nube y altamente escalable que está respaldada por clústeres HSM nShield de Entrust alojados en los centros de datos de Entrust. PKIaaS proporciona un servidor de base de datos PKI ágil a las aplicaciones que requieren certificados de confianza privada, como la gestión de dispositivos móviles, la autenticación de usuarios, IoT y DevOps.

Proceso de verificación

El Cliente puede utilizar PKIaaS para generar y emitir certificados de confianza privada. Entrust no realiza ninguna verificación en relación con estos certificados.

Recopilación y tratamiento de datos personales

No se procesa ningún dato personal aparte de los que se recopilan en relación con la plataforma ECS.

Período de conservación

La información de la cuenta se conserva durante 7 años tras la finalización de la cuenta, a menos que la cuenta incluya certificados ETSI, en cuyo caso la información de la cuenta se conserva durante 15 años tras la expiración del último certificado.