ENTRUST CERTIFICATE SERVICES

DECLARACIÓN DE PRIVACIDAD

Índice

Entrust Certificate Services

Última actualización: 25 de noviembre de 2021

Entrust Certificate Services (ECS)

Este aviso de privacidad del producto describe cómo Entrust Certificate Services (ECS) recopila y procesa datos personales de conformidad con las leyes aplicables de privacidad de datos.

Descripción

ECS es una plataforma web de gestión del ciclo de vida de certificados que le ayuda a gestionar todos sus certificados digitales, tanto de Entrust como de otras Autoridades de Certificación. Brinda acceso a una gran cantidad de herramientas que generan informes detallados que ayudan a los usuarios a mejorar el tiempo de actividad, evitar fallas de seguridad y preservar la reputación de la marca. ECS proporciona acceso vía web a información técnica, actualizaciones de estado y escaneo de sitios web para la administración del ciclo de vida de un extremo a otro de todos sus certificados digitales.

Recopilación y Tratamiento de Datos Personales

ECS de Entrust recopila los siguientes datos de representantes autorizados de nuestros Clientes:

Tipo de Datos Personales	**Propósito del Tratamiento**
Dirección de la Empresa	Cumplimiento de Confianza Pública/ Gestión de cuenta
Empresa/Organización	Cumplimiento de Confianza Pública / Gestión de cuenta
Dirección de Email	Autenticación de usuario
Dirección IP	Seguridad
Profesión/Cargo	Cumplimiento de Confianza Pública
Nombre	Cumplimiento de Confianza Pública
Contraseña	Autenticación de usuario
Número de Teléfono	Cumplimiento de Confianza Pública

Preguntas y Respuestas de Seguridad	Autenticación de usuario
Nombre de Usuario	Autenticación de usuario

Periodo de Retención

Todos los datos personales recopilados por ECS se conservan de acuerdo con los términos establecidos en los contratos del Cliente..

Uso de Subencargados

Para obtener la lista actual de subencargados, visite https://www.entrust.com/legal-compliance/privacy/sub-processors.

Transferencias Internacionales de Datos

Los productos certificados de Entrust utilizan varios subencargados y centros de datos. En la medida en que los Clientes se encuentren en un país diferente al del subencargado utilizado para la verificación de identificación, autenticación por SMS, provisión de contraseñas de un solo uso (OTP) o alojamiento de datos, puede haber transferencias transfronterizas de datos personales. Cualquier transferencia transfronteriza de datos personales se realiza de acuerdo con los requisitos de la ley de privacidad de datos relevantes (por ejemplo, las Cláusulas Contractuales Estándar para datos personales de la UE transferidos fuera de la UE).

Medidas de Protección de Datos

Para obtener más información sobre cómo Entrust procesa los datos personales recopilados por este producto, consulte el Anexo 2, Apéndice 2 de nuestro acuerdo estándar de tratamiento de datos del cliente (DPA) que se encuentra aquí.

Derechos de Privacidad de Datos

El Cliente es el responsable de todos los datos personales recopilados por ECS. Entrust Corporation, como encargado de los datos, ayudará al Cliente, en la medida de lo posible y razonable, a responder a las solicitudes verificadas de acceso a datos del sujeto que el Cliente reciba con respecto a ECS.

Enmiendas a esta Declaración de Privacidad

Nos reservamos el derecho de modificar esta Declaración de Privacidad del Producto ocasionalmente a medida que evolucionen nuestros negocios, leyes, regulaciones y estándares de la industria. Cualquier cambio entrará en vigor inmediatamente después de la publicación de dichos cambios en https://www.entrust.com/legal-compliance/data-privacy/product-privacy-notices. Le recomendamos que revise esta declaración cada cierto tiempo para mantenerse informado.

Información de Contacto

Para preguntas sobre este aviso de privacidad del producto, por favor, póngase en contacto con privacy@entrust.com. Para obtener el aviso de privacidad general de Entrust Corporation, haga clic aquí.

Productos de Servicios de Certificado

Certificados de Firma de Documentos

Los Certificados de Firma de Documentos de Entrust permiten que las organizaciones confíen en los documentos transmitidos electrónicamente y firmen digitalmente documentos de Adobe y Microsoft Office con confianza. Basadas en la tecnología probada de infraestructura de clave pública (PKI), las firmas digitales son ampliamente reconocidas como una mejor práctica para proporcionar verificación digital de transmisiones electrónicas. Las firmas digitales brindan "no repudio", la capacidad de identificar al autor y verificar que el documento no se haya modificado desde que se firmó digitalmente. La garantía en tiempo real verifica la autenticidad a lo largo de la vida útil del documento. Las organizaciones también pueden utilizar Certificados de firma de documentos para autenticar documentos sensibles que requieran varias firmas.

Datos Personales Obtenidos Adicionalmente:

Algunos Certificados de Firma de Documentos también pueden requerir la fecha de nacimiento y los números de identificación nacional. Además, los Certificados de Firma de Documentos pueden requerir la recolección y almacenamiento de una copia del documento de identificación del suscriptor, una foto de su rostro junto con un video corto de la sesión de verificación de identificación. El propósito del tratamiento de estos datos es la verificación de identidad. Los datos biométricos solo se procesarán en caso de verificación de identidad a través de video.

Certificados de Dispositivo Móvil

Los Certificados de Dispositivo Móvil de Entrust brindan una solución basada en la nube para autenticar dispositivos móviles y brindar acceso seguro a los sistemas corporativos sin implementar una PKI local. Con los certificados de dispositivos móviles de Entrust, los clientes pueden obtener y administrar fácilmente identidades digitales y dispositivos en entornos BYOD, brindando a sus usuarios una experiencia sin fricciones y cumpliendo con los requisitos de seguridad internos.

Datos Personales Obtenidos Adicionalmente:

Los Certificados de Dispositivo Móvil de Entrust requieren que los usuarios finales seleccionen un Nombre de Dispositivo y un Nombre Común. Estos dos nombres no contienen necesariamente datos personales, pero podrían hacerlo, dependiendo de la información con que el usuario final complete el campo personalizado. El Nombre del Dispositivo no se puede ver públicamente, pero el Nombre Común aparece en el certificado.

Firma de Código Público

Los Certificados de Firma de Código Público de Entrust autentican la identidad del editor y verifican que los archivos ejecutables y scripts firmados digitalmente no hayan sido manipulados desde la firma. Esto asegura a los Clientes que el software firmado se descargará de Internet según lo

previsto por el desarrollador. Los certificados firmados ayudan a los editores de software a establecer confianza con sus clientes, evitando que se instale software no verificado en dispositivos corporativos. Los usuarios se sienten seguros al saber que el editor fue verificado por Entrust, una autoridad de certificación (CA) acreditada por WebTrust.

Infraestructura de Clave Pública como Servicio (PKIaaS por sus siglas en inglés)

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

TLS/SSL Públicos

Los Certificados TLS / SSL de Entrust proporcionan identidad validada y cifrado para proteger los sitios web, los usuarios y los datos. El uso de Nombres de Dominio no Totalmente Cualificados (FQDN) en certificados de confianza pública cesó el 1 de noviembre de 2015, y todas las autoridades de certificación públicas revocaron los certificados existentes que contienen no-FQDN antes del 1 de octubre de 2016. Para ayudar a simplificar este cambio, Entrust introdujo Certificados SSL privados que brindan a las organizaciones un método fácil y asequible para el uso continuo de nombres de dominio no registrados..

SMIME Públicos

Los Certificados SMIME de Entrust brindan una manera simple de reducir la posibilidad de pérdida de datos críticos y ataques provenientes del correo electrónico. La autenticación y el cifrado de extremo a extremo de correos electrónicos internos / externos, junto con una implementación totalmente automatizada de certificados S/MIME y la gestión del ciclo de vida a escala, es una de las muchas capacidades que hacen que nuestra solución se destaque de las soluciones tradicionales. Los Certificados SMIME de Entrust cumplen con varias regulaciones de confidencialidad relacionadas con la atención médica, la educación, el gobierno, el ejército, las finanzas y otros sectores de consumo.

Certificados Cualificados

Los Certificados Cualificados de Entrust proporcionan comunicaciones seguras y autenticadas que cumplen con los estándares y regulaciones de seguridad de datos de la Unión Europea (UE), incluida la Directiva Revisada de Servicios de Pago (PSD2).

Los Certificados Cualificados solo pueden ser emitidos por un Proveedor de Servicios de Confianza Calificado (QTSP) reconocido bajo la identificación electrónica y los servicios de confianza (eIDAS). Entrust EU está reconocido en todos los países de la UE y del Espacio Económico Europeo (EEE) como QTSP y se ha sometido a las evaluaciones de conformidad eIDAS correspondientes para

poder proporcionar Certificados Cualificados para la autenticación de sitios web. Véase Entrust EU en la Lista de confianza de la UE.

Datos Personales Obtenidos Adicionalmente:

Los Certificados Calificados también pueden requerir la obtención y almacenamiento de una copia del documento de identificación del suscriptor, una foto de su rostro, junto con un video corto de la sesión de verificación de identificación. El propósito del tratamiento de estos datos es la verificación de identidad. Los datos biométricos solo se procesarán en caso de verificación de identidad a través de video.

Servicio de Firma Remota (RSS por sus siglas en inglés)

El Servicio de Firma Digital de Entrust ayuda a empresas e instituciones a establecer firmas digitales y sellos de empresa de alta seguridad sin necesidad de mantenimiento de hardware o conocimientos de criptografía a través de una interfaz de programación de aplicaciones web (API). El Servicio de Firma Remota de Entrust es una extensión de lo anterior que permite a los empleados utilizar firmas digitales en documentos con sus claves de firma, administradas de forma centralizada en un servicio remoto. Las claves de firma están protegidas de forma centralizada dentro de un Módulo Hardware de Seguridad (HSM), y los usuarios aprueban las firmas de documentos de forma remota desde su dispositivo, sin la necesidad de token de hardware o software. La plataforma proporciona firmas avanzadas y cualificadas según lo definido por eIDAS. Se basa en los Estándares del Instituto Europeo de Telecomunicaciones (ETSI) y del Comité Europeo de Estandarización (CEN), que garantizan un altísimo nivel de confianza y una amplia interoperabilidad con los productos de la industria que requieren firmas digitales. El proceso de incorporación y firma de los usuarios es transparente, no requiere conocimientos específicos y se puede realizar desde cualquier dispositivo..

Datos Personales Obtenidos Adicionalmente:

RSS también puede requerir la obtención y el almacenamiento de una copia del documento de identificación del suscriptor, una foto de su rostro, junto con un video corto de la sesión de verificación de identificación. El propósito del tratamiento de estos datos es la verificación de identidad. Los datos biométricos solo se procesarán en caso de verificación de identidad a través de video.

Servicio de Automatización de Firmas (SAS por sus siglas en inglés)

Con el Servicio de Automatización de Firmas de Entrust, los clientes obtienen todos los beneficios de un sello de la empresa en sus documentos sin la complejidad de la gestión del hardware y los riesgos de la firma manual. La autoría, integridad y no repudio de todos los documentos del cliente se logra mediante la integración de este servicio basado en la nube en las aplicaciones del cliente con el cliente de automatización de firmas Entrust. Los clientes obtienen certificados de firma de documentos reconocidos a nivel mundial, además de sellos de tiempo y servicios de Protocolo en

Línea de Estado de Certificados (OCSP), todos respaldados por HSM basados en la nube de nuestros centros de datos.

Datos Personales Obtenidos Adicionalmente:

El Servicio de Automatización de Firmas también requiere la validación de un representante de la organización, lo que incluye obtener y almacenar una copia del documento de identificación del representante, una foto de su rostro, junto con un video corto de la sesión de verificación de identificación. El propósito del tratamiento de estos datos es la verificación de identidad. Los datos biométricos solo se procesarán en caso de verificación de identidad a través de video.

Certificados de Marca Verificada (VMC por sus siglas en inglés)

Los Certificados de Marca Verificada permiten que las marcas muestren el logotipo de su marca registrada junto con las comunicaciones por correo electrónico.

Entrust, en colaboración con AuthIndicators Working Group, desarrolló un método para estandarizar la apariencia de logotipos verificados junto con los correos electrónicos recibidos. El método incluye el uso de un Certificado de marca verificado, que verifica el logotipo de la marca. Brand Indicators for Message Identification (BIMI) es el organismo de estándares para la tecnología combinada que permite la emisión de VMC.

Datos Personales Obtenidos Adicionalmente:

Los certificados de marca verificada también requieren la obtención y almacenamiento de una copia del documento de identificación del suscriptor, una foto de su rostro, junto con un video corto de la sesión de verificación de identificación. El propósito del tratamiento de estos datos es la verificación de identidad. Los datos biométricos solo se procesarán en caso de verificación de identidad a través de video.