Declaración de Divulgación de PKI

1 Introducción

Este documento es la Declaración de divulgación de PKI ("PDS" en sus siglas en inglés), según lo exigen los estándares europeos ETSI EN 319 411-1, ETSI EN 411 319-2 y ETSI EN 319 421 relacionados con los servicios de Certificado Cualificado de Autenticación de Sitio Web ("QWAC"), Certificado Cualificado de Sello Electrónico ("QSealC"), Certificado Cualificado de Firma Electrónica ("QSigC") y Sellos Cualificados de Tiempo ofrecidos por el prestador cualificado de servicios de confianza **Entrust EU S.L.**, empresa española con número de IVA ESB81188047 (“Entrust EU”).

Entrust EU emite certificados QWAC, QsealC, QsigC y Sellos Cualificados de Tiempo de conformidad con el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.° 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital ("Reglamento eIDAS") y la Directiva 2015/2366 / UE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior ("PSD2").

Este documento no sustituye ni reemplaza los Términos y Condiciones del servicio de certificados QWAC, QSealC, QSigC y Sello Cualificado de Tiempo ni la Declaración de Prácticas de Certificación de Entrust EU ("CPS" en sus siglas en inglés) ni la Declaración de Prácticas de Sellado de Tiempo (“TPS” en sus siglas en inglés) publicadas en el sitio web de Entrust EU (ver a continuación los denominados "requisitos"). Simplemente proporciona una descripción general de los Requisitos clave en un formato simplificado.

2 Información de contacto de la CA

Se puede contactar con la CA en las direcciones siguientes:

Oficinas corporativas
Entrust EU, S.L.U.
Pe La Finca. Paseo Club Deportivo, 1 Bloque 3 BJ
28223 Pozuelo De Alarcón (Madrid)
España
At: Servicio de Certificados

Asistencia o cuestiones relativas a los Certificados
Tel: +1-866-267-9297 o +1-613-270-2680

Email: ecs.support@entrust.com

Para preguntas relacionadas con esta Declaración de divulgación de PKI u otros documentos de los servicios de certificado QWAC, QsealC, QsigC o Sello Cualificado de Tiempo de Entrust EU, por favor, envíe un correo

electrónico a ecs.support@entrust.com.

Para solicitar la revocación de un certificado, siga el procedimiento en línea descrito en la CPS (que requiere las credenciales del Suscriptor que se proporcionan en el momento de la emisión del certificado) utilizando la página web https://www.entrust.com/support/certificate-solutions/report-a-problem o bien la dirección de correo electrónico problemreport@entrust.com. Para obtener más información, consulte la CPS publicada en el sitio web de Entrust EU.

3 Tipos de certificado, procedimientos de validación y uso

Entrust EU emite QWAC, QSealC y QSigC (en conjunto, "Certificados" proporcionados por los servicios de certificados) de acuerdo con la norma europea ETSI EN 319 411-2, el Reglamento eIDAS 2024/1183 y otras normas relacionadas. Los certificados se ofrecen al público en general (empresas privadas, entidades públicas y otras personas jurídicas, pero no a personas físicas), de acuerdo con los términos y condiciones publicados en la CPS y el Acuerdo de Suscripción de Entrust EU, que están disponibles en el sitio web. Cualquier restricción en el uso del certificado se indica en las Secciones 1.4.1, 1.4.2, 4.5 y 6.1.7 de la CPS.

Todos los certificados están firmados con la función de hash SHA-256. Para obtener más información sobre las políticas de certificados admitidas (por ejemplo, sus respectivos OID y otras funciones), consulte la documentación publicada en el sitio web de Entrust EU en https://www.entrust.com/legal-compliance/entrust-certificate-services-repository y la CPS.

La información sobre los Certificados Raíz relevantes de Entrust EU y las CA emisoras se publica en el sitio web de Entrust EU. Para confirmar el estado de Entrust EU como Prestador cualificado de servicios de confianza en la Lista de confianza del Gobierno de España, consulte https://webgate.ec.europa.eu/tl-browser/#/tl/ES.

Entrust EU proporciona tanto las Listas de Revocación de Certificados (CRL en sus siglas en inglés) como un servicio de verificación de estado en línea basado en el estándar OCSP para permitir la validación de los certificados. Las URL de ambos se incluyen en todos los Certificados, respectivamente en las extensiones CRLDistributionPoint ("CDP") y AuthorityInformationAccess ("AIA").

4 Tipos de sellos de tiempo y uso

Entrust EU ofrece servicios calificados de sellado de tiempo de acuerdo con el Reglamento (UE) 2024/1183 ("Reglamento eIDAS") y emite Sellos Cualificados de Tiempo de conformidad con ETSI EN 319 421.

Todas los Sellos de Tiempo están firmados con la función hash SHA-256. Los hash de Solicitud de Sello de Tiempo aceptables incluyen SHA-256, SHA-384 y SHA-512.

Los Sellos de Tiempo se ofrecen al público en general (empresas privadas, entidades públicas y otras personas jurídicas, pero no a personas físicas), de acuerdo con los términos y condiciones publicados en la TPS y el Acuerdo de Suscriptor de Entrust EU, que están disponibles en el sitio web.

Entrust EU puede limitar la tarifa y cobrar tarifas por sus Servicios Cualificados de Sellado de Tiempo.

5 Límites de confianza

Los Certificados se emiten para fines de QWAC, QSealC y QSigC.

Las limitaciones en el uso de Certificados pueden especificarse dentro de los Certificados mismos en el atributo UserNotice de la extensión CertificatePolicies.

Las limitaciones sobre el valor de las transacciones en las que se puede usar el certificado pueden especificarse en los certificados, dentro de la extensión de certificado qcStatements, por medio del elemento QCEuLimitValue.

Los Sellos de Tiempo Cualificados garantizan una precisión de al menos un segundo.

Entrust EU conserva todos los registros relacionados con el ciclo de vida de los certificados y los registros relativos a la emisión de Sellos de Tiempo, así como todos los registros de auditoría de servicio de CA/TSA, durante quince años.

6 Obligaciones de los subscriptores

Los suscriptores de certificados están sujetos a las siguientes obligaciones:

- Toda la información proporcionada y todas las representaciones realizadas por el Suscriptor en relación con cualquier Certificado son y serán completas, precisas y veraces (y el Suscriptor actualizará de inmediato dicha información y representaciones según sea necesario para mantener dicha integridad y exactitud);
- El suministro de información de verificación razonablemente solicitada por Entrust EU o su delegado no se retrasará injustificadamente;
- La Clave Privada correspondiente a la Clave Pública enviada a Entrust EU en relación con una Solicitud de Certificado se creó mediante técnicas criptográficas razonables, si no fue generada por una CA;
- Se han tomado todas las medidas necesarias para mantener el control exclusivo y la confidencialidad de la clave privada (y cualquier información o dispositivo de acceso asociado, por ejemplo, contraseña o token) y protegerlos adecuadamente en todo momento;
- Cualquier información proporcionada a Entrust EU o a cualquier RA de un tercero independiente en relación con una Solicitud de Certificado no infringe, se apropia indebidamente, diluye, compite injustamente o viola la propiedad intelectual u otros derechos de cualquier persona, entidad u organización en cualquier jurisdicción;
- El / los Certificado(s) no se instalarán ni utilizarán hasta que el Suscriptor haya revisado y verificado la exactitud de los datos en cada Certificado;

- El suscriptor responderá de inmediato a las instrucciones de Entrust EU con respecto a (1) el compromiso de la Clave Privada asociada con cualquier certificado y (2) uso indebido o supuesto uso indebido de un certificado;
- Todo uso del Certificado y su Clave Privada asociada cesará de inmediato, y el Suscriptor notificará de inmediato a Entrust EU y solicitará la revocación del Certificado, si (1) cualquier información incluida en el Certificado cambia, es o se vuelve incorrecta o inexacta, o si cualquier cambio en cualquier circunstancia pudiera hacer que la información en la Solicitud de Certificado o Certificado sea incorrecta, engañosa o inexacta; o (2) hay algún uso indebido o compromiso real o presunto de la Clave Privada (o datos de activación de clave) asociados con la Clave Pública en el Certificado;
- Todo uso del (1) Certificado y (2) Clave Privada asociada con la Clave Pública en dicho Certificado cesará al vencimiento o revocación de dicho Certificado y dicho Certificado se eliminará de los dispositivos y / o software en los que se haya instalado;
- Los Certificados no se utilizarán para actividades peligrosas o ilegales (incluidas las que causen daños y perjuicios); y se usarán solo para el propósito en que se emitieron;
- El sujeto nombrado en el Certificado corresponde al Suscriptor, que legalmente existe como una entidad válida en la jurisdicción mercantil especificada en los Certificados;
- Para QWAC, el Certificado se instalará solo en el servidor accesible con el nombre de dominio que figura en el Certificado, y solo se utilizará de conformidad con todas las leyes aplicables, únicamente para los negocios autorizados de la compañía, y únicamente de conformidad con el Acuerdo de Suscripción y la CPS;
- Para QWAC, el Suscriptor tiene el derecho exclusivo de usar el nombre de dominio que figura en el Certificado;
- El sujeto nombrado en el Certificado corresponde al Suscriptor, que legalmente existe como una entidad válida en la jurisdicción mercantil o Registro especificados en los Certificados.

Para obtener más información, consulte la CPS, incluida la Sección 9.6.3.

Los suscriptores de sellado de tiempo deben:

- Verificar que el token de sello de tiempo se haya firmado correctamente;
- Verificar los servicios de validación de Entrust EU (es decir, CRL u OCSP) para confirmar que la Clave Privada utilizada para firmar el token de Sello de Tiempo no se ha visto comprometida;
- Utilizar funciones criptográficas seguras para solicitudes de Sellado de Tiempo o software para crear Sellos de Tiempo;
- Informar a sus usuarios finales (incluidas las Partes que confían pertinentes) sobre la documentación de las políticas y prácticas de Entrust EU.

7 Obligaciones de las partes que confían acerca de la verificación del estado del certificado

Todos aquellos que confían en la información contenida en los Certificados ("Partes que confían") primero

deben verificar que los Certificados no estén suspendidos o revocados. Dicha verificación se puede realizar consultando la lista de Certificados revocados (CRL) publicada por Entrust EU o consultando el servicio OCSP proporcionado por Entrust EU en las direcciones (URL) contenidas en los mismos Certificados.

Antes de confiar en un Sello de Tiempo, las Partes que confían deben verificar que el Sello de Tiempo se haya firmado correctamente y que el Certificado asociado no haya sido revocado como se describe anteriormente.

8 Garantía limitada y exención de responsabilidad / limitación de responsabilidad

Para conocer las limitaciones de garantía y responsabilidad, consulte las disposiciones del Acuerdo de Suscripción y la CPS (en particular, consulte las Secciones 7 - 9 del Acuerdo de Suscripción y las Secciones 9.7 - 9.9 de la CPS).

9 Acuerdos aplicables, Declaraciones de Prácticas y Políticas

Los acuerdos y condiciones que se aplican a los servicios de certificados se encuentran en los siguientes documentos, publicados en el sitio web de Entrust EU:

- Declaración de Prácticas de Certificación (CPS) de Entrust EU
- Declaración de Prácticas de Sellado de Tiempo (TPS) de Entrust EU
- Acuerdo de Suscripción

Las Políticas de Certificado (CP) admitidas se describen en la CPS; ver también la sección 3 arriba.

10 Política de privacidad

Entrust EU cumple con el Reglamento general de protección de datos (UE) 2016/679 ("RGPD") y la Política de Privacidad de Entrust Corporation en https://www.entrust.com/legal-compliance/data-privacy/privacy-statement y la Política de Protección de Entrust Data en https://www.entrust.com/legal-compliance/policies/data-protection-policy.

Entrust EU conserva todos los registros relacionados con los Certificados y Sellos Cualificados de Tiempo emitidos por Entrust EU (por ejemplo, evidencia de la identidad de los suscriptores; solicitudes de emisión de certificados, incluida la aceptación de los Términos y Condiciones; solicitudes de revocación de certificados; etc.).

11 Política de reembolso

Para ver la política de reembolso de Entrust EU, consulte la CPS Sec. 9.1.5.

12 Leyes aplicables, quejas y resolución de conflictos

Los servicios de certificados proporcionados por Entrust EU están sujetos a la ley de Ottawa, Canadá. La aplicabilidad, ejecución, interpretación y validez de la CPS/TPS se rigen por la ley de Ottawa, Canadá, independientemente del contrato u otra elección de disposiciones legales. Para obtener información adicional, consulte la CPS Sec. 9.13 y 9.14.

Para todas los conflictos legales relacionados con los servicios de certificados de Entrust EU, consulte las disposiciones alternativas de resolución de conflictos en la CPS Sec. 9.13. Para cualquier asunto que no se resuelva mediante resolución alternativa de conflictos, los tribunales de Ottawa, Canadá, tendrán jurisdicción exclusiva, salvo que se disponga lo contrario en el Acuerdo de Suscriptor y la CPS/TPS. Ver en particular la CPS Sec. 9.13 y 9.14.

13 Lista de confianza de QTSP y auditoría

Entrust EU figura en la lista de confianza del Gobierno de España como prestador cualificado de servicios de confianza (QTSP en sus siglas en inglés) y está autorizado a emitir QWAC, QsealC, QSigC y Sellos Cualificados de Tiempo de conformidad con el Reglamento eIDAS.

Los servicios de certificados de Entrust EU están sujetos a una evaluación de conformidad anual, de acuerdo con las normas europeas ETSI EN 319 411-1 y ETSI EN 319 411-2, ETSI TS 119 495, ETSI EN 319 421 y normas relacionadas por un auditor independiente, cualificado y acreditado, según lo requerido por el Reglamento eIDAS.

***