



## **Servicios de certificados y firma Términos de uso**

El Acuerdo correspondiente a los servicios de certificados de Entrust, cualesquiera servicios de firma digital o CA



cada cierto tiempo de acuerdo con las condiciones del CPS. Asimismo, se incluye aquí como referencia en el Acuerdo. El CPS aplicable a un Certificado específico depende del tipo de Certificado y puede encontrarse en Internet en <http://www.entrust.net/cps> o contactando con Entrust. Por ejemplo, los



### 1.13. “Servicios de Firma



vencimiento o resolución del Plazo de la Oferta, o por cualquier otra razón identificada para la revocación en el Acuerdo, el CPS o los Estándares del Sector.

3.4.



suscripción a uno o varios de los Servicios Alojados. Por una tarifa adicional, se pueden adquirir otros planes de servicio y niveles de asistencia.

- 7. Conectores.** Puede haber complementos o API que permitan que los Servicios Alojados interoperen con productos o servicios de terceros (cada uno de ellos, un "Conector"). El Cliente reconoce y acepta que dichos Conectores no forman parte de los Servicios Alojados, así como que Entrust no otorga derechos, garantías o asistencia para ningún Conector o para la interoperabilidad de los Servicios Alojados con tales Conectores en virtud del presente Anexo de ECSS. Si el Cliente utiliza cualquier Conector, tiene la responsabilidad exclusiva de asegurarse de que cuenta con todos y cada uno de los derechos necesarios para emplear el Conector,



- 8.5. Acceso no autorizado. El Cliente tomará todas las medidas razonables para evitar el acceso no autorizado a los Servicios Alojados, incluso asegurando, protegiendo y manteniendo la confidencialidad de sus credenciales de acceso. El Cliente es responsable de cualquier acceso y uso de los Servicios Alojados a través de la Cuenta de Administración del Cliente o mediante las credenciales de acceso del Cliente, así como de toda la actividad que tenga lugar en la Cuenta de Administración del Cliente. El Cliente notificará a Entrust de inmediato ante cualquier conocimiento o sospecha de uso no autorizado de los Servicios Alojados o vulneración de su seguridad en relación con los Servicios Alojados y hará todos los esfuerzos











**Anexo A**

Con autorización para solicitar un Certificado de Suscriptor:	
Con autorización para aprobar la solicitud de un Certificado de Suscriptor y autorizar a otros a solicitar Certificados de Suscriptor:	
Con autorización para aceptar el acuerdo de suscriptor en nombre del Suscriptor:	



## Anexo B

### Manifestaciones, garantías y obligaciones de los Suscriptores y Sujetos

#### Parte 1: Suscriptores

Como condición para emitir cualquier Certificado a o para un Suscriptor, cada Suscriptor hace, en su propio nombre y, si corresponde, en nombre de su superior o Agente en virtud de una relación de subcontratista o servicio de alojamiento, los siguientes compromisos, manifestaciones, afirmaciones y garantías en beneficio de los Beneficiarios del Certificado, Entrust y cualesquiera de las Filiales de Entrust que emitirán Certificados a o para el Suscriptor:

#### Para todos los Certificados.

1. Si el Suscriptor solicita la emisión de un Certificado a o para otra Persona, esta ha autorizado al Suscriptor para que actúe en su nombre, incluida la solicitud de Certificados en nombre de dicha Persona, y para que haga los compromisos, manifestaciones, afirmaciones y garantías recogidos en el presente anexo en nombre de dicha Persona, así como en el propio nombre del Suscriptor.
2. Toda la información proporcionada y todas las manifestaciones realizadas, en todo momento, por parte del Suscriptor en relación con cualesquiera Servicios de Certificados, incluso en la solicitud de Certificados y en lo que respecta a la emisión de Certificados, son y serán íntegras, correctas y exactas (y dicha información y manifestaciones se actualizarán de manera oportuna cada cierto tiempo según sea necesario para mantener dicha integridad, corrección y exactitud), y no infringen, se apropian indebidamente, diluyen, compiten injustamente o vulneran de otro modo la propiedad intelectual u otros derechos de cualquier persona, entidad u organización en cualquier jurisdicción. A efectos aclaratorios, al enviar cualquier solicitud de un Certificado utilizando información preseleccionada, se considera que el Suscriptor está volviendo a hacer los compromisos, manifestaciones, afirmaciones y garantías establecidos en este Anexo B. Asimismo, Entrust no tendrá la obligación de emitir ningún Certificado que contenga información preseleccionada si posteriormente se descubre que dicha información ha cambiado o es de algún modo inexacta, incorrecta o errónea.
3. La clave privada correspondiente a la clave pública enviada a Entrust con la solicitud de Certificado se creó mediante sólidas técnicas criptográficas y se han tomado todas las medidas razonables para, en todo momento, garantizar el control (y, en el caso de los Certificados de OV Code Signing y EV Code Signing, el control exclusivo), mantener la confidencialidad y prohibir el uso no autorizado de la clave privada (y cualquier acceso asociado o dato o dispositivo de activación, por ejemplo, contraseña o token), así como protegerla adecuadamente, incluido, en el caso de los Certificados de OV Code Signing y EV Code Signing, de acuerdo con las disposiciones del apartado "Data Security and Private Key Protection" (Seguridad de los datos y protección de las claves privadas) de los BR de Code Signing.
4. Cualquier dispositivo que almacene claves privadas se operará y mantendrá de forma segura.
5. No se instalará ni utilizará ningún Certificado hasta que el Suscriptor (o, en el caso de los Certificados de Code Signing, el Agente del Suscriptor) haya revisado y verificado que el contenido del Certificado es exacto y correcto.
6. En el caso de todos los Certificados SSL, Certificados SSL de EV y Certificados de Private SSL de Entrust, el Certificado se instalará únicamente en los servidores a los que se pueda acceder en el nombre de dominio (subjectAltName(s)) que figure en el Certificado.
7. Los Certificados y la clave privada correspondiente a la clave pública que se incluye en dichos Certificados solo



- 9.3. en el caso de un Certificado de OV Code Signing o EV Code Signing inmediatamente si hay pruebas de que el Certificado se ha utilizado para firmar Código Sospechoso.
10. El Suscriptor dejará de utilizar de inmediato el Certificado y la clave privada correspondiente a la clave pública de dicho Certificado tras su vencimiento o revocación.
11. El Suscriptor responderá al instante a las instrucciones de Entrust con respecto a cualquier Puesta en Riesgo de la Clave o uso indebido o sospecha de uso indebido de un Certificado.
12. El Suscriptor reconoce y acepta que Entrust tiene derecho a revocar un Certificado inmediatamente si:
  - 12.1. El Cliente incumple el presente Acuerdo.
  - 12.2. Entrust descubre que se ha producido una Puesta en Riesgo de la Clave privada del Certificado.
  - 12.3.



- 18.1.1. la o las claves privadas del Sujeto solo se utilizarán para funciones criptográficas dentro del dispositivo criptográfico especificado.
- 18.1.2. si las claves del Sujeto se generan bajo el control del Suscriptor o del Sujeto, las claves del Sujeto se generarán dentro del dispositivo criptográfico especificado.
- 18.2. El Suscriptor da su consentimiento para que Entrust mantenga un seguimiento de la información utilizada en el registro, el suministro del dispositivo del Sujeto, ya sea al Suscriptor o al Sujeto cuando sean distintos, y cualquier revocación posterior, la identidad y cualquier atributo específico incluido en el Certificado, y transmita esta información a terceros en las mismas condiciones que exigen los Estándares del Sector en caso de que Entrust dé por terminados sus servicios.
- 18.3. El Suscriptor exige la publicación del Certificado en la forma y condiciones establecidas en el CPS y obtendrá, en su caso, la autorización del Sujeto para dicha publicación.
- 18.4. La clave privada y la correspondiente clave pública asociadas al Certificado solo se utilizarán de acuerdo con las limitaciones notificadas al Suscriptor, incluso en el CPS.
- 18.5. Si el Suscriptor o el Sujeto genera las claves del Sujeto:
  - 18.5.1. las claves del Sujeto se generarán mediante un algoritmo según lo especificado en los Estándares del Sector para los usos de la clave certificada tal y como se identifica en el CPS.
  - 18.5.2. la longitud y el algoritmo de la clave serán los especificados en los Estándares del Sector para los usos



5. Si el Sujeto genera sus claves, la clave privada del Sujeto se mantendrá el control del Sujeto, y si el Sujeto es un individuo, bajo el control exclusivo del Sujeto.
6. La clave privada del Sujeto se utilizará bajo el control del Sujeto, y si el Sujeto es un individuo, bajo el control exclusivo del Sujeto.
7. El Sujeto notificará a Entrust de inmediato:
  - 7.1. si cualquier información incluida en el Certificado cambia, si es o se vuelve incorrecta o inexacta, o si cualquier cambio en las circunstancias pudiera hacer que la información del Certificado fuera errónea.
  - 7.2. y dejará de utilizar de forma inmediata y permanente la clave correspondiente si hay algún conocimiento o sospecha de pérdida, robo, uso indebido o puesta en riesgo de la clave privada (o los datos de activación de la clave) correspondiente a la clave pública del Certificado, incluso si el valor de la clave privada se ha revelado a una persona no autorizada o esta ha tenido acceso a él, o si se ha perdido el control de la clave privada por otros motivos.
8. Al ser informado de que el Certificado del Sujeto se ha revocado o de que la Issuing CA se ha visto comprometida, el Sujeto dejará de utilizar la clave privada.