Acuerdo de Usuario del Servicio de certificados digitales TCS – Trusted Certificate Service

Versión 4.0 rev 04

Definiciones

Servicio de certificados digitales (“Trusted Certificate Service”, ***TCS***, por sus siglas en inglés). Servicio gestionado por GÉANT, la asociación de redes académicas europeas, antes conocida como TERENA, y operado por RedIRIS, que permite ofrecer múltiples tipos de certificados digitales a las instituciones académicas y de investigación afiliadas a la misma, gracias a acuerdos colectivos negociados a escala europea entre GÉANT y operadores de certificación.

CA. Operador de certificación encargado de la prestación del servicio.

Miembro (Member). En este caso RedIRIS, Red académica y de investigación nacional (“National Research and Education Network”, NREN) que ha suscrito un acuerdo con GÉANT para proporcionar a sus Usuarios servicios de emisión de certificados digitales.

Usuarios (Subscribers). Instituciones afiliadas a RedIRIS (organizaciones académicas y de investigación o instituciones sin ánimo de lucro afiliadas a RedIRIS), que solicitan un certificado a través de una cuenta abierta con un operador de certificación. Los Usuarios deberán cumplir, por tanto, los requisitos de afiliación descritos en: http://www.rediris.es/rediris/instituciones/afiliacion.html, y aparecer en el listado de instituciones disponible en http://www.rediris.es/rediris/instituciones/lista.php. Dada la responsabilidad que tiene el Usuario sobre los certificados que éste solicita, como sobre los que piden los Solicitantes (Applicants), el término Usuario se aplica tanto a los Usuarios como a los Solicitantes. Los Usuarios actúan también como Autoridad de Registro.

Solicitantes (Applicants). Individuos pertenecientes a un Usuario, y autorizados por éste, a los que se permite solicitar un certificado en nombre del mismo.

TCS CPS. (Trusted Certificate Service Certification Practice Statement) Declaración de prácticas de certificación del Servicio de certificados digitales disponible en el repositorio de documentación del TCS en https://wiki.geant.org/display/TCSNT/TCS+Repository

La operación y las prácticas de certificación que rigen el servicio de certificados digitales están descritas en la TCS CPS, así como sus documentos accesorios, disponibles en el repositorio de documentación del TCS. En particular, el acuerdo entre GÉANT y la CA en el documento de términos de uso.

El presente documento hace referencia a los términos contractuales entre RedIRIS y los Usuarios del Servicio de certificados digitales, es decir, las instituciones afiliadas a RedIRIS.

Acuerdo de Usuario

D./Dña. <***NOMBRE-PER***>[1], como Persona de Enlace con RedIRIS, y representando a la institución afiliada <***NOMBRE-INSTITUCIÓN-AFILIADA***>[1], que participa como Usuaria y autoridad de registro en el Servicio de certificados digitales de RedIRIS, declara que:

- acepta someterse a los términos contractuales establecidos para el Servicio de certificados digitales, que resultan de aplicación al presente acuerdo, incluida cualquier posible actualización y modificación de los mismos;
- acepta cumplir la TCS CPS, es decir, las Declaraciones de prácticas de certificación, incluidos los documentos auxiliares pertinentes, y las Normas y las Condiciones de uso del Certificado;
- se responsabiliza de que el personal y los representantes involucrados en el Servicio de certificados digitales lean y comprendan las condiciones estipuladas en la TCS CPS y sus normas asociadas, que se hallan publicadas en el repositorio de documentación del TCS en https://wiki.geant.org/display/TCSNT/TCS+Repository. El Usuario manifiesta su conformidad con estas condiciones;
- seguirá las prácticas y los procedimientos descritos en la TCS CPS y actuará de conformidad con las condiciones que la CPS estipula para los Usuarios;
- se responsabiliza de usar los certificados emitidos a través del Servicio de certificados digitales únicamente para fines legales y autorizados con arreglo a los usos y prácticas establecidos por la TCS CPS;
- se responsabiliza de proporcionar información correcta y precisa en sus comunicaciones con RedIRIS. El Usuario asume la responsabilidad de alertar a RedIRIS si en cualquier momento, durante el tiempo de validez del certificado, hubiese cambios en la información presentada originalmente a RedIRIS.
- asume que el servicio es prestado por RedIRIS en términos no comerciales, y que no cabe reclamar responsabilidad a RedIRIS en relación con la prestación de dicho servicio.
- ambas Partes conocen y asumen que han de cumplir con lo establecido en la normativa de protección de datos, compuesta por el Reglamento (UE) 2016/679 (en adelante RGPD) y por la Ley Orgánica 3/2018 (en adelante LOPDGDD), así como cualquier norma que pueda sustituirlas o desarrollarlas en el futuro.
- en todo caso Red.es observará en el tratamiento de los datos personales de las personas y entidades mencionadas anteriormente, lo dispuesto en la anterior normativa para la prestación del servicio, en caso de que Red.es tenga la consideración de Encargado de Tratamiento de conformidad con lo establecido en el art. 28 RGPD, las Partes firmarán el correspondiente Contrato de Encargo de Tratamiento, al que este documento se incluye como Anexo con el número de orden que corresponda.
- el Solicitante conoce y asume que los derechos de acceso y rectificación podrán ejercerse de acuerdo con lo dispuesto en la normativa de protección de datos de carácter personal, mientras que los derechos de supresión, limitación del tratamiento, portabilidad y oposición únicamente podrán ejercerse previa desconexión del proveedor de identidad correspondiente, dado que el tratamiento de datos personales por parte de Red.es es necesario para la prestación del servicio.
- nombra a D./Dña. <***NOMBRE-ADMINISTRADOR***>[1], con correo electrónico personal <***EMAIL-PERSONAL-ADMINISTRADOR***>[1] como administrador principal de la institución <***NOMBRE-INSTITUCIÓN-AFILIADA***>[1], encargado/a de registrar, de forma correcta, todos los datos necesarios de la institución, dar de alta a los Solicitantes y gestionar sus certificados según lo especificado en http://www.rediris.es/tcs/caracteristicas/roles/.

[1] Cumplimente este valor en la tabla de la página 5

El Usuario es consciente de que los certificados que le han sido emitidos pueden ser revocados por RedIRIS o por GÉANT de acuerdo con las condiciones indicadas en la TCS CPS. Además, se compromete a que los certificados no serán utilizados de manera alguna en caso de revocación de los mismos.

En su calidad de Autoridad de registro, el Usuario manifiesta por el presente documento su conformidad con las siguientes condiciones:

1. Aplicabilidad. Las condiciones expuestas se refieren a cada certificado digital emitido para un Usuario en virtud del acuerdo con GÉANT, con independencia de (i) el tipo de certificado digital (correo electrónico, firma de código o TLS/SSL), (ii) cuándo haya solicitado el Usuario el certificado digital, o (iii) cuándo se haya emitido realmente el certificado digital. El Usuario no podrá solicitar un certificado con contenidos que infrinjan los derechos de propiedad intelectual de otra entidad.
2. Generación de clave privada. El Usuario deberá preservar la confidencialidad de todas las claves privadas y aplicar medidas razonables para proteger la clave privada frente a su posible revelación. El Usuario deberá solicitar que se revoque el certificado en el plazo de un día hábil desde que sospeche un uso fraudulento o una situación de riesgo de algún certificado o clave privada. El Usuario deberá generar su par de claves usando uno de los siguientes métodos: (i) en un “token” criptográfico seguro, (ii) usando un programa de criptografía fiable en un sistema informático local del que sea el único usuario y administrador, (iii) en un sistema informático administrado por la institución afiliada o por un tercero si (a) la clave se genera mediante un programa de criptografía fiable, (b) el acceso está limitado a personas designadas, que conocen y respetan las normas de privacidad aplicables y siguen un código de conducta profesional, (c) la clave privada y la contraseña no se envían en texto sin cifrar a través de una red, (d) el archivo con la clave privada encriptada no se envía a través de la red sin proteger, (e) el sistema está situado en un entorno seguro, donde el acceso se controle y esté limitado solo al personal autorizado, y (f) el sistema no conserva las contraseñas o las claves privadas en texto sin cifrar durante más de 24 horas.
3. Almacenamiento de clave privada de la IGTF. Los Usuarios de certificados emitidos como "certificado de Grid" deben almacenar y proteger las claves privadas de acuerdo con las normas para Grid aplicables y en vigor, que se hallan publicadas en el repositorio de documentación de IGTF en https://www.eugridpma.org/guidelines/ y en concreto en el documento “Protection of private key data for end-users in local and remote systems” (https://www.eugridpma.org/guidelines/pkp/)
4. Transparencia de los certificados. Para garantizar que los certificados funcionen correctamente a lo largo de su vida útil, el Usuario deberá permitir a la CA registrar los certificados SSL en una base de datos de certificados pública. Puesto que esto será una condición necesaria para la funcionalidad del certificado, los Usuarios no podrán excluirse de este proceso y manifiestan expresamente su conformidad con el registro de sus certificados. La información del servidor de registros es de acceso público. Una vez aportada esa información, no puede retirarse de un servidor de registros.
5. Restricciones**.** Los Usuarios no podrán (a) compartir su certificado o clave privada con otro Usuario salvo cuando lo permita la CPS, (b) usar un certificado o una clave privada para operar centrales nucleares, sistemas de control de tráfico aéreo, sistemas de navegación aérea, sistemas de control de armamento o cualquier otro sistema que requiera un funcionamiento infalible cuyo fallo pueda derivar en lesiones, muerte o daños ambientales, (c) modificar, subautorizar, descompilar o crear un trabajo derivado de algún certificado (excepto cuando se requiera para un uso aceptado del certificado) o clave privada, (d) usar o presentar declaraciones sobre un certificado en términos distintos a lo estipulado por la CPS, (e) hacerse pasar por otra persona o falsear su filiación con una entidad o usar un certificado de un modo que pueda dar lugar previsiblemente a la presentación de una querella civil o penal contra el Usuario o la CA, (f) usar un certificado para enviar o recibir correspondencia indiscriminada, firmar o distribuir archivos, programas o código que pueda dañar el funcionamiento del ordenador de otros o que se descargue sin el consentimiento de un Usuario, o incumpla la confianza de un tercero, (g) intentar usar un certificado para emitir otros certificados, con

la salvedad de que el Usuario podrá usar el certificado para crear certificados obtenidos por medio de representantes tal como se expone en RFC 3820, o (h) crear intencionadamente una clave privada que sea sustancialmente similar a una clave privada de la CA o de un tercero. Los Usuarios asumen plenamente la responsabilidad de garantizar que los certificados se renueven antes de su expiración.

6. Revocación**.** La CA podrá revocar el certificado de un Usuario sin previo aviso por los motivos expuestos en la CPS, y asimismo si considera que (a) el Usuario o el titular del certificado ha solicitado la revocación del certificado o no ha autorizado su emisión, (b) el Usuario o el titular del certificado ha incumplido las obligaciones previstas en el acuerdo con GÉANT o con una NREN o no ha cumplido lo estipulado en la CPS, (c) una disposición del presente acuerdo que contenga una declaración u obligación relacionada con la emisión, el uso, la gestión o la revocación del certificado se extingue o se declara nula, (d) el Usuario o el titular del certificado es añadido a una lista de personas o entidades vetadas por el Gobierno u opera desde un lugar vetado según las leyes de los Estados Unidos, (e) el certificado contiene información inexacta o engañosa, (f) el certificado no se ha usado para los fines previstos o se ha utilizado para firmar software malicioso, (g) la clave privada asociada a un certificado se ha revelado o se ha puesto en peligro, (h) el acuerdo entre GEANT y la CA termina, (i) el certificado se ha usado o emitido, directa o indirectamente, de forma contraria a la legislación, la CPS o las normas del sector, (j) las normas del sector o la CPS de la CA exigen su revocación, o (k) la revocación es necesaria para proteger los derechos, la información confidencial, las operaciones o la reputación de la CA o de un tercero.

7. Reparación. La única reparación al alcance de un Usuario en caso de defecto en un certificado es el compromiso de la CA de hacer cuanto esté en su mano para corregir el defecto. La CA no estará obligada a corregir un defecto si (i) el Certificado se ha usado indebidamente, se ha dañado o modificado, (ii) el Usuario no ha notificado el defecto a la CA con prontitud, o (iii) el Usuario ha incumplido el acuerdo con GÉANT.

8. Software y equipos. Los Usuarios son responsables en exclusiva de su propia conducta, de su software, del mantenimiento, funcionamiento, desarrollo, seguridad y contenido de su sitio web, así como de todos los ordenadores, los equipos de telecomunicaciones, el software, el acceso a Internet y las redes de comunicaciones (si las hubiese) requeridos para acceder a y utilizar los certificados.

9. Limitación de garantía. LOS CERTIFICADOS Y TODO PROGRAMA, PRODUCTO Y SERVICIO RELACIONADO SE PROPORCIONAN "TAL CUAL" Y "EN FUNCIÓN DE SU DISPONIBILIDAD". EN LA MÁXIMA MEDIDA EN QUE LO PERMITA LA LEGISLACIÓN, LA CA RENUNCIA A TODAS LAS GARANTÍAS EXPRESAS E IMPLÍCITAS, INCLUIDAS LAS GARANTÍAS DE COMERCIABILIDAD, ADECUACIÓN PARA UN FIN CONCRETO Y NO INFRACCIÓN. LA CA NO GARANTIZA QUE LOS SERVICIOS O PRODUCTOS CUMPLAN SUS EXPECTATIVAS O QUE EL ACCESO A LA CUENTA SE PRODUZCA A TIEMPO O ESTÉ LIBRE DE ERRORES. El uso de un certificado SHA-1 podrá ocasionar mensajes de error en los distribuidores de software de aplicación.

10. Limitación de responsabilidad. Este acuerdo no pretende limitar la responsabilidad de las partes por (i) fallecimiento o lesión personal resultante de la negligencia de alguna parte o (ii) fraude o declaraciones fraudulentas efectuadas por una parte. SALVO EN LOS SUPUESTOS EXPUESTOS, EL USUARIO DEBERÁ CONSENTIR EN LIMITAR LA RESPONSABILIDAD MÁXIMA DE LA CA DERIVADA DEL CERTIFICADO A 530.000 $. EL USUARIO DEBERÁ MANIFESTAR SU CONFORMIDAD CON QUE LA CA NO SERÁ RESPONSABLE DE NINGÚN DAÑO INDIRECTO, ESPECIAL O PUNITIVO NI DE NINGUNA PÉRDIDA DE BENEFICIOS, INGRESOS, DATOS U OPORTUNIDADES, INCLUSO SI LA CA FUESE CONSCIENTE DE LA POSIBILIDAD DE TALES DAÑOS. Las limitaciones deberán aplicarse hasta el grado máximo en que lo permita la legislación e independientemente de (i) el motivo o la naturaleza de la responsabilidad, inclusive las reclamaciones de daños y perjuicios, (ii) el número de reclamaciones de responsabilidad, (iii) el grado y la naturaleza de los daños, o (iv) el hecho de si cualquier otra disposición del presente acuerdo se ha infringido o ha demostrado ser ineficaz.

11. Indemnización. En la medida en que lo permita la ley, el Usuario deberá indemnizar, liberar de responsabilidad y defender a la CA frente a cualquier demanda de terceros y cualquier reclamación de responsabilidad, daños y perjuicios y costes, incluidos honorarios razonables de abogados, derivados de la infracción de las presentes condiciones por parte del Usuario.

NOMBRE-INSTITUCIÓN-AFILIADA

NOMBRE-PER

NOMBRE-ADMINISTRADOR

EMAIL-PERSONAL-ADMINISTRADOR

Firma del PER **Firma del Administrador**