DIGITELTS
by MADISON

PDS Certificados Ciudadano

DIGITEL TS Proveedor de servicios de confianza cualificado

Control documental

Líder	Área de servicios de confianza		
Tipo	PDS Certificados Ciudadano		
Distribución	**Público**		
Fecha	2024		
Descripción	Textos de divulgación Certificados Ciudadano		
Aprobado	Comité de Riesgos y Seguridad DIGITEL TS	Fecha	30 Mayo 2024
Estado	Aprobado		

Control de Cambios

Versión	Fecha	Detalle
V1.0	15 abril 2024	Primera versión del documento

1 Textos de divulgación

Este documento contiene la información esencial del servicio de certificación del prestador de servicios de confianza cualificado DIGITEL TS para los certificados de Persona Física.

2 Información de contacto

Autoridad de Certificación de DIGITELTS.

DIGITEL ON TRUSTED SERVICES S.L.U

Dirección. C/ Enrique Cubero, 9, 47014 Valladolid (España)

Teléfono. +34 91 015 05 10

Email. pki@digitelts.es

3 Tipos y finalidades de los certificados

Certificado Cualificado de Persona Física Centralizado.

Este certificado dispone de los siguientes OID: En la jerarquía de certificación de DIGITEL TS: OID 1.3.6.1.4.1.54225.10.3.5 De acuerdo con la política QCP-n-qscd: 0.4.0.194112.1.2

Estos certificados, son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2. Estos certificados funcionan con dispositivo cualificado de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014. Estos certificados son gestionados de forma centralizada, es decir, que la generación y gestión de los datos de creación de firma electrónica es realizada por el prestador, por cuenta del firmante. Estos certificados garantizan la identidad del firmante, y permiten la

generación de la “firma electrónica cualificada”; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendá un efecto jurídico equivalente al de una fima manuscrita. También se pueden utilizar en aplicaciones que no requieran del uso de la firma electrónica cualificada, como las aplicaciones que se indican a continuación: 1) Firma de correo electrónico seguro, 2) Otras aplicaciones de firma digital. Estos certificados no se encuentran autorizados para el cifrado de documentos, de contenidos ni de mensajes de datos. En todo caso, DIGITEL TS no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

Certificado Cualificado de Persona Física.

Este certificado dispone de los siguientes OID: En la jerarquía de certificación de DIGITEL TS: OID 1.3.6.1.4.1.54225.10.3.1. De acuerdo con la política QCP-n: 0.4.0.194112.1.0. Estos certificados, son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2. Estos certificados no funcionan con dispositivo seguro de creación de firma. Estos certificados son gestionados de forma distribuida sin la participación de una herramienta de gestión centralizada. Estos certificados garantizan la identidad del firmante, y permiten la generación de la “firma electrónica avanzada” basada en certificado electrónico cualificado. También se pueden utilizar en aplicaciones que no requieran del uso de la firma electrónica cualificada, como las aplicaciones que se indican a continuación: 1) Firma de correo electrónico seguro. 2) Otras aplicaciones de firma digital. Estos certificados no se encuentran autorizados para el cifrado de documentos, de contenidos ni de mensajes de datos. En todo caso, DIGITEL TS no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

4 Límites de uso de los certificados

4.1 Límites de uso dirigidos a los firmantes

El firmante ha de utilizar el servicio de certificación de los certificados prestado por DIGITEL TS exclusivamente para los usos autorizados en el contrato firmado entre DIGITEL TS y el SUSCRIPTOR, y que se reproducen posteriormente (sección “obligaciones de los firmantes”).

Asimismo, el firmante se obliga a utilizar el servicio de certificación digital de acuerdo con las instrucciones, manuales o procedimientos suministrados por DIGITEL TS.

El firmante ha de cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas que emplee.

El firmante no puede adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital de DIGITEL TS, sin previo permiso expreso.

4.2 Límites de uso dirigidos a los verificadores

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (CRL’s).

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación

o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, visibles en el web de https://www.pki.digitelts.es

El empleo de los certificados digitales en operaciones que contravienen este texto de divulgación, o los contratos con los suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a DIGITEL TS, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

DIGITEL TS no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de DIGITEL TS emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en este texto de divulgación, o en los contratos con los suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

5 Obligaciones de los subscriptores

Generación de claves

El suscriptor autoriza a DIGITEL TS a generar las claves, privada y pública, para la identificación y la firma electrónica de los firmantes, y solicita en su nombre la emisión del certificado.

Solicitud de certificados

El suscriptor se obliga a realizar las solicitudes de los certificados de acuerdo con el procedimiento y, si es necesario, los componentes técnicos suministrados por DIGITEL TS, de conformidad con lo que se establece en la declaración de prácticas de certificación (DPC) y en la documentación de operaciones de DIGITEL TS.

Obligaciones de información

El suscriptor se responsabiliza de que toda la información incluida en su solicitud del certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.

El suscriptor tiene que informar inmediatamente a DIGITEL TS:

- De cualquier inexactitud detectada en el certificado una vez se haya emitido.
- De los cambios que se produzcan en la información aportada y/o registrada para la emisión del certificado.
- De la pérdida, robo, sustracción, o cualquier otro tipo de pérdida de control de la clave privada por el firmante.

Obligaciones de custodia

El suscriptor se obliga a custodiar toda la información que genere en su actividad como entidad de registro.

6 Obligaciones de los firmantes

Obligaciones de custodia

El firmante se obliga a custodiar el código de identificación personal o cualquier soporte técnico entregado por DIGITEL TS, las claves privadas y, si fuese necesario, las

especificaciones propiedad de DIGITEL TS que le sean suministradas. El firmante se obliga a custodiar el código de identificación personal (PIN).

En caso de pérdida o robo de la clave privada del certificado, o en caso de que el firmante sospeche que la clave privada ha perdido fiabilidad por cualquier motivo, dichas circunstancias han de ser notificadas inmediatamente a DIGITEL TS por medio del suscriptor.

Obligaciones de uso correcto

El firmante tiene que utilizar el servicio de certificación de certificados prestado por DIGITEL TS, exclusivamente para los usos autorizados en la DPC y en cualquier otra instrucción, manual o procedimiento suministrado al suscriptor.

El firmante tiene que cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas empleadas.

El firmante no podrá adoptar medidas de inspección, alteración o descompilación de los servicios de certificación digital prestados.

El firmante reconocerá:

- Que cuando utilice cualquier certificado, y mientras el certificado no haya expirado ni haya sido suspendido o haya sido revocado, habrá aceptado dicho certificado y estará operativo.
- Que no actúa como entidad de certificación y, por lo tanto, se obliga a no utilizar las claves privadas correspondientes a las claves públicas contenidas en los certificados con el propósito de firmar certificado alguno.
- Que en caso de quedar comprometida la clave privada, su uso queda inmediata y permanentemente suspendido.

Transacciones prohibidas

El firmante se obliga a no utilizar sus claves privadas, los certificados o cualquier otro soporte técnico entregado por DIGITEL TS en la realización de transacción alguna prohibida por la ley aplicable.

Los servicios de certificación digital prestados por DIGITEL TS no han sido diseñados ni permiten su utilización o reventa como equipos de control de situaciones peligrosas, o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo o sistemas de control de armamento, en las que un error pudiera directamente causar la muerte, daños físicos o daños medioambientales graves.

7 Obligaciones de los verificadores

Decisión informada

DIGITEL TS informa al verificador que tiene acceso a información suficiente para tomar una decisión informada en el momento de verificar un certificado y confiar en la información contenida en dicho certificado.

Adicionalmente, el verificador reconocerá que el uso del Registro y de las Listas de Revocación de Certificados (en lo sucesivo, las CRL's) de DIGITEL TS, se rigen por la DPC de DIGITEL TS y se comprometerá a cumplir los requisitos técnicos, operativos y de seguridad descritos en la mencionada DPC.

Requisitos de verificación de la firma electrónica

La comprobación será ejecutada normalmente de forma automática por el software del verificador y, en todo caso, de acuerdo con la DPC, con los siguientes requisitos:

- Es necesario utilizar el software apropiado para la verificación de una firma digital con los algoritmos y longitudes de claves autorizados en el certificado y/o ejecutar cualquier otra operación criptográfica, y establecer la cadena de certificados en que se basa la firma

electrónica a verificar, ya que la firma electrónica se verifica utilizando esta cadena de certificados.

- Es necesario asegurar que la cadena de certificados identificada es la más adecuada para la firma electrónica que se verifica, ya que una firma electrónica puede basarse en más de una cadena de certificados, y es decisión del verificador asegurarse el uso de la cadena más adecuada para verificarla.
- Es necesario comprobar el estado de revocación de los certificados de la cadena con la información suministrada al Registro de DIGITEL TS (con CRL's, por ejemplo) para determinar la validez de todos los certificados de la cadena de certificados, ya que únicamente puede considerarse correctamente verificada una firma electrónica si todos y cada uno de los certificados de la cadena son correctos y se encuentran vigentes.
- Es necesario asegurar que todos los certificados de la cadena autorizan el uso de la clave privada por el suscriptor del certificado y el firmante, ya que existe la posibilidad de que alguno de los certificados incluya límites de uso que impidan confiar en la firma electrónica que se verifica. Cada certificado de la cadena dispone de un indicador que hace referencia a las condiciones de uso aplicables, para su revisión por los verificadores.
- Es necesario verificar técnicamente la firma de todos los certificados de la cadena antes de confiar en el certificado utilizado por el firmante.

Confianza en un certificado no verificado

Si el verificador confía en un certificado no verificado, asumirá todos los riesgos derivados de esta actuación.

Efecto de la verificación

En virtud de la correcta verificación de los certificados, de conformidad con este texto divulgativo, el verificador puede confiar en la identificación y, en su caso, clave pública del firmante, dentro de las limitaciones de uso correspondientes, para generar mensajes cifrados.

Uso correcto y actividades prohibidas

El verificador se obliga a no utilizar ningún tipo de información de estado de los certificados o de ningún otro tipo que haya sido suministrada por DIGITEL TS, en la realización de transacción alguna prohibida para la ley aplicable a la citada transacción.

El verificador se obliga a no inspeccionar, interferir o realizar ingeniería inversa de la implantación técnica de los servicios públicos de certificación de DIGITEL TS, sin previo consentimiento escrito.

Adicionalmente, el verificador se obliga a no comprometer intencionadamente la seguridad de los servicios públicos de certificación de DIGITEL TS.

Los servicios de certificación digital prestados por DIGITEL TS no han sido diseñados ni permiten la utilización o reventa, como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armamento, donde un error podría causar la muerte, daños físicos o daños medioambientales graves.

Cláusula de indemnidad

El tercero que confía en el certificado se compromete a mantener indemne a DIGITEL TS de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

- Falta de comprobación de la totalidad de medidas de aseguramiento prescritas en la DCP o resto de normas de aplicación.

DIGITEL TS no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

DIGITEL TS no será responsable de los daños y perjuicios ocasionados en los términos indicados en el artículo 11 de Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

8 Obligaciones de DIGITEL TS

En relación con la prestación del servicio de certificación digital DIGITEL TS se obliga a:

- Emitir, entregar, administrar, suspender, revocar y renovar certificados, de acuerdo con las instrucciones suministradas por el suscriptor, en los casos y por los motivos descritos en la DPC de DIGITEL TS.
- Ejecutar los servicios con los medios técnicos y materiales adecuados, y con personal que cumpla las condiciones de cualificación y experiencia establecidas en la DPC.
- Cumplir los niveles de calidad del servicio, en conformidad con lo que se establece en la DPC, en los aspectos técnicos, operativos y de seguridad.
- Notificar al suscriptor, con anterioridad a la fecha de expiración de los certificados, de la posibilidad de renovarlos, así como la suspensión, alzamiento de esta suspensión o revocación de los certificados, cuando se produzcan dichas circunstancias.
- Comunicar a las terceras personas que lo soliciten, el estado de los certificados, de acuerdo con lo que se establece en la DPC para los diferentes servicios de verificación de certificados.

En relación con las comprobaciones del registro

DIGITEL TS se obliga a la emisión de certificados en base a los datos suministrados por el suscriptor, por lo cual podrá realizar las comprobaciones que considere oportunas respecto de la identidad y otras informaciones personales y complementarias de los suscriptores y, cuando resulte procedente, de los firmantes.

Estas comprobaciones podrán incluir la justificación documental aportada por el firmante por medio del suscriptor, si DIGITEL TS lo considera necesario, y cualquier otro documento e información relevantes facilitados por el suscriptor y/o el firmante.

En el caso que DIGITEL TS detecte errores en los datos que se deben incluir en los certificados o que justifican estos datos, podrá realizar los cambios que considere necesarios antes de emitir el certificado o suspender el proceso de emisión y gestionar con el suscriptor la incidencia correspondiente. En caso de que DIGITEL TS corrija los datos sin gestión previa de la incidencia correspondiente con el suscriptor, deberá notificar los datos finalmente certificados al suscriptor.

DIGITEL TS se reserva el derecho a no emitir el certificado, cuando considere que la justificación documental resulte insuficiente para la correcta identificación y autenticación del suscriptor y/o del firmante.

Las anteriores obligaciones quedarán en suspenso en los casos en que el suscriptor actúe como autoridad de registro y disponga de los elementos técnicos correspondientes a la generación de claves, emisión de certificados y grabación de dispositivos de firma corporativos.

Periodos de conservación

DIGITEL TS conserva la información relativa a los servicios prestados de acuerdo con el artículo 24.2.h) del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, durante al menos 15 años desde la extinción del certificado o la finalización del servicio prestado.

DIGITEL TS almacena la información de los logs durante un periodo de entre 1 y 15 años, en función del tipo de información registrada.

9 Garantías limitadas y rechazo de garantías

Garantía de DIGITEL TS por los servicios de certificación digital

DIGITEL TS garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación del mismo.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la DPC.
- Que los servicios de revocación y el empleo del depósito cumplen con todos los requisitos materiales establecidos en la DPC.

DIGITEL TS garantiza al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el depósito, que el certificado ha sido emitido al suscriptor y firmante identificado en el mismo y que el certificado ha sido aceptado.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la DPC.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y depósito.

Adicionalmente, DIGITEL TS garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado reconocido/cualificado, de acuerdo con el anexo I del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona física identificada en el certificado, se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Entidad de Certificación, con los límites que se establezcan. En ningún caso DIGITEL TS responderá por caso fortuito y en caso de fuerza mayor.

Exclusión de la garantía

DIGITEL TS rechaza toda otra garantía diferente a la anterior que no sea legalmente exigible.

Específicamente, DIGITEL TS no garantiza software alguno utilizado por cualquier persona para firmar, verificar firmas, cifrar, descifrar, o utilizar de otra forma certificado digital alguno emitido por DIGITEL TS, excepto en los casos en que exista una declaración escrita en sentido contrario.

10 Política de privacidad

DIGITEL TS dispone de una política de privacidad en la DPC, y regulación específica de la privacidad en relación al proceso de registro, la confidencialidad del registro, la protección del acceso a la información personal, y el consentimiento del usuario.

La información a que se refiere el apartado de períodos de conservación, se conserva por los períodos indicados debidamente registrada y con garantías de seguridad e integridad.

11 Política de reintegro

DIGITEL TS no reintegrará el coste del servicio de certificación en ningún caso.