DECISIÓN DE EJECUCIÓN (UE) 2021/1073 DE LA COMISIÓN

de 28 de junio de 2021

por la que se establecen especificaciones técnicas y normas relativas a la aplicación del marco de confianza para el certificado COVID digital de la UE establecido por el Reglamento (UE) 2021/953 del Parlamento Europeo y del Consejo

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2021/953 del Parlamento Europeo y del Consejo, de 14 de junio de 2021, relativo a un marco para la expedición, verificación y aceptación de certificados COVID-19 interoperables de vacunación, de prueba diagnóstica y de recuperación (certificado COVID digital de la UE) a fin de facilitar la libre circulación durante la pandemia de COVID-19 ([1]), y en particular su artículo 9, apartados 1 y 3,

Considerando lo siguiente:

(1) El Reglamento (UE) 2021/953 contempla el certificado COVID digital de la UE, que sirve para demostrar que una persona ha recibido una vacuna contra la COVID-19, se ha sometido a una prueba con resultado negativo o se ha recuperado de una infección.

(2) Para que el certificado COVID digital de la UE funcione en toda la Unión, es preciso establecer especificaciones técnicas y normas que permitan cumplimentar, expedir y verificar de forma segura los certificados COVID digitales, garantizar la protección de los datos personales, establecer la estructura común del identificador único del certificado y expedir un código de barras válido, seguro e interoperable. Este marco de confianza también sienta las premisas de cara a garantizar la interoperabilidad con las normas y sistemas tecnológicos internacionales y, como tal, podría servir como modelo para la cooperación en el ámbito mundial.

(3) La capacidad de leer e interpretar el certificado COVID digital de la UE requiere una estructura de datos común y un consenso sobre la importancia de cada campo de datos de la carga útil y sus valores posibles. Para facilitar dicha interoperabilidad, es preciso definir una estructura de datos común y coordinada para el marco del certificado COVID digital de la UE. Las orientaciones para este marco han sido elaboradas por la red de sanidad electrónica creada sobre la base de la Directiva 2011/24/UE del Parlamento Europeo y del Consejo ([2]). Dichas orientaciones deben tenerse en cuenta a la hora de establecer las especificaciones técnicas que determinan el formato y la gestión de la confianza del certificado COVID digital de la UE. Debe detallarse una especificación sobre la estructura de datos y establecerse mecanismos de codificación, así como un mecanismo de codificación de transporte en un formato óptico legible por máquina («QR») que pueda mostrarse en la pantalla de un dispositivo móvil o imprimirse en una hoja de papel.

(4) Además de las especificaciones técnicas sobre el formato y la gestión de confianza del certificado COVID digital de la UE, deben establecerse normas generales en cuanto a la cumplimentación de los certificados que se apliquen a los valores codificados en el contenido de dicho certificado. La Comisión debe actualizar y publicar periódicamente los conjuntos de valores que aplican esas normas basándose en los trabajos de la red de sanidad electrónica en esta materia.

(5) Con arreglo al Reglamento (UE) n.º 2021/953, los certificados auténticos que conforman el certificado COVID digital de la UE deben ser identificables individualmente mediante un identificador único de certificado, teniendo en cuenta que los ciudadanos pueden haber recibido más de un certificado durante el período de vigencia del Reglamento (UE) n.º 2021/953. Para que pueda identificarse al titular, el identificador único de certificado debe estar formado por una secuencia alfanumérica, y los Estados miembros deben garantizar que no contenga ningún dato que lo vincule a otros documentos o identificadores tales como números de pasaporte o de documento de identidad. Para garantizar que el identificador del certificado sea único, deben establecerse especificaciones técnicas y normas sobre su estructura común.

([1]) DO L 211 de 15.6.2021, p. 1.

([2]) Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88 de 4.4.2011, p. 45).

(6) La seguridad, autenticidad, validez e integridad de los certificados que conforman el certificado COVID digital de la UE y su conformidad con la legislación de la Unión en materia de protección de datos son fundamentales para su aceptación en todos los Estados miembros. Estos objetivos se alcanzan gracias al marco de confianza, que establece las normas y la infraestructura para la expedición y verificación fiables y seguras de los certificados COVID digitales de la UE. El marco de confianza debe basarse, entre otras cosas, en una infraestructura de clave pública con una cadena de confianza que comprenda desde las autoridades sanitarias de los Estados miembros u otras autoridades de confianza hasta cada entidad que expida certificados COVID digitales de la UE. Por consiguiente, y con vistas a garantizar un sistema de interoperabilidad válido en toda la UE, la Comisión ha creado un sistema central —la pasarela del Certificado COVID digital de la UE (en lo sucesivo, «pasarela»)— que almacena las claves públicas utilizadas a efectos de verificación. Al escanearse el certificado de código QR, la firma digital se verifica a través de la correspondiente clave pública, almacenada con anterioridad en dicha pasarela central. Para garantizar la integridad y autenticidad de los datos, pueden utilizarse firmas digitales. Las infraestructuras de clave pública garantizan la confianza al vincular las claves públicas a los emisores de certificados. A fin de garantizar la autenticidad, en la pasarela se utilizan varios certificados de clave pública. Para garantizar un intercambio seguro entre los Estados miembros de los datos correspondientes a las claves públicas y hacer posible una interoperabilidad generalizada, es preciso establecer los certificados de clave pública que pueden utilizarse y determinar cómo deben generarse.

(7) La presente Decisión permite aplicar los requisitos del Reglamento (UE) 2021/953 de manera que limite el tratamiento de datos personales al mínimo necesario para que el certificado COVID digital de la UE sea operativo y contribuya a que su puesta en práctica por los responsables del tratamiento finales respete la protección de datos desde el diseño.

(8) Con arreglo al Reglamento (UE) 2021/953, las autoridades u otros organismos designados que sean responsables de la expedición de los certificados se consideran responsables del tratamiento a efectos del artículo 4, apartado 7, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([3]) en el ejercicio de su función de tratamiento de datos personales durante el proceso de expedición. Dependiendo de cómo organicen los Estados miembros el proceso de expedición, puede haber una o más autoridades u organismos designados; por ejemplo, los servicios regionales de salud. Conforme al principio de subsidiariedad, su elección corresponde a los Estados miembros. De ahí que, cuando existan múltiples autoridades u otros organismos designados, sean los Estados miembros quienes mejor situados están para garantizar que se delimiten claramente sus respectivas responsabilidades, ya sean responsables del tratamiento a título independiente o conjunto (incluidos los servicios regionales de salud que creen un portal común de pacientes para la expedición de certificados). Del mismo modo, y en lo que respecta a la verificación de los certificados por las autoridades competentes del Estado miembro de destino o de tránsito o por los operadores de servicios de transporte transfronterizo de viajeros que, conforme a la legislación nacional, deban aplicar determinadas medidas de sanidad pública durante la pandemia de COVID-19, tales verificadores deben cumplir sus obligaciones con arreglo a las normas de protección de datos.

(9) No hay tratamiento de datos personales a través de la pasarela del Certificado COVID digital de la UE, ya que el portal tan solo alberga las claves públicas de las autoridades de firma. Estas claves se refieren a las autoridades de firma y no permiten la reidentificación directa o indirecta de una persona física a la que se haya expedido un certificado. Por tanto, en su función de gestión de la pasarela, la Comisión no debe ser ni responsable ni encargada del tratamiento de datos personales.

(10) El Supervisor Europeo de Protección de Datos, a quien se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([4]), emitió su dictamen el 22 de junio de 2021.

(11) Dado que, para la aplicación del Reglamento (UE) 2021/953 a partir del 1 de julio de 2021, son necesarias especificaciones técnicas y normas, está justificada la aplicación inmediata de la presente Decisión.

(12) Por consiguiente, y habida cuenta de la necesidad de una rápida implementación del certificado COVID digital de la UE, la presente Decisión debe entrar en vigor el día de su publicación.

([3]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva n.º 95/46/CE, Reglamento general de protección de datos (DO L 119 de 4.5.2016, p. 1).

([4]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

En el anexo I figuran las especificaciones técnicas del certificado COVID digital de la UE, que establecen la estructura de datos genérica, los mecanismos de codificación y el mecanismo de codificación de transporte en un formato óptico legible por máquina.

Artículo 2

En el anexo II de la presente Decisión figuran las normas relativas a la cumplimentación de los certificados a que se refiere el artículo 3, apartado 1, del Reglamento (UE) 2021/953.

Artículo 3

En el anexo III figuran los requisitos que establecen la estructura común del identificador único de certificado.

Artículo 4

En el anexo IV figuran las normas de gobernanza aplicables a los certificados de clave pública en lo que respecta a la pasarela del Certificado COVID digital de la UE y que regulan los aspectos de interoperabilidad del marco de confianza.

La presente Decisión entrará en vigor el día de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Bruselas, el 28 de junio de 2021.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO I

GESTIÓN DEL FORMATO Y DE LA CONFIANZA

Estructura de datos genérica, mecanismos de codificación y mecanismo de codificación de transporte en un formato óptico legible por máquina (en lo sucesivo denominado «QR»)

1. Introducción

Las especificaciones técnicas establecidas en este anexo contienen una estructura de datos genérica y mecanismos de codificación para el certificado COVID digital de la UE («CCD»). También detallan un mecanismo de codificación de transporte en un formato óptico legible por máquina («QR»), que puede mostrarse en la pantalla de un dispositivo móvil o imprimirse. Los formatos de contenedor de certificados sanitarios electrónicos de estas especificaciones son genéricos, pero en este contexto se utilizan para contener el CCD.

2. Terminología

A efectos del presente anexo, se entenderá por «emisores» las organizaciones que utilicen estas especificaciones para expedir certificados sanitarios y por «verificadores» las organizaciones que acepten los certificados sanitarios como prueba del estado de salud. Por «participantes» se entiende los emisores y los verificadores. Algunos de los aspectos establecidos en el presente anexo deben coordinarse entre los participantes, como la gestión de un espacio de nombres y la distribución de claves criptográficas. Se parte de la premisa de que una parte, en adelante denominada «Secretaría», lleva a cabo estas tareas.

3. Formato de contenedor de certificados sanitarios electrónicos

El formato de contenedor de certificados sanitarios electrónicos («HCERT») está diseñado para proporcionar una solución uniforme y estandarizada para los certificados sanitarios de diferentes emisores («emisores»). El objetivo de estas especificaciones es armonizar la forma en que se representan, codifican y firman estos certificados sanitarios con el fin de facilitar la interoperabilidad.

La capacidad de leer e interpretar un CCD expedido por cualquier emisor requiere una estructura de datos común y un consenso sobre la importancia de cada campo de datos de la carga útil. Para facilitar esta interoperabilidad, se define una estructura de datos coordinada común mediante el uso de un esquema «JSON» que constituye el marco del CCD.

3.1. *Estructura de la carga útil*

La carga útil está estructurada y codificada como CBOR con una firma digital COSE. Esto se conoce comúnmente como «CBOR Web Token» (CWT), y se define en RFC 8392 ([1]). La carga útil, tal y como se define en las siguientes secciones, se transporta en una notificación hcert.

El verificador debe comprobar la integridad y autenticidad del origen de los datos de la carga útil. Para proporcionar este mecanismo, el emisor debe firmar el CWT utilizando un esquema de firma electrónica asimétrica, tal como se define en la especificación COSE (RFC 8152 ([2])).

3.2. *Notificaciones CWT*

3.2.1. Descripción de la estructura del CWT

Encabezado protegido

— Algoritmo de firma (alg, etiqueta 1)

— Identificador de clave (kid, etiqueta 4)

Carga útil

— Emisor (iss, clave de notificación 1, opcional, ISO 3166-1 alfa-2 del emisor)

— Emitido a las (iat, clave de notificación 6

— Hora de expiración (exp, clave de notificación 4)

— Certificado sanitario (hcert, clave de notificación -260)

— Certificado COVID digital de la UE v1 (eu_DCC_v1, clave de notificación 1)

Firma

([1]) rfc8392 (ietf.org)
([2]) rfc8152 (ietf.org)

3.2.2. Algoritmo de firma

El parámetro Algoritmo de Firma(alg) indica qué algoritmo se utiliza para la creación de la firma. Debe cumplir o superar las directrices actuales de SOG-IS que se resumen a continuación.

Se define un algoritmo primario y otro secundario. El algoritmo secundario solo debe utilizarse si el algoritmo primario no es aceptable dentro de las normas y reglamentos impuestos al emisor.

Para garantizar la seguridad del sistema, todas las implementaciones deben incorporar el algoritmo secundario. Por esta razón, deben implementarse tanto el algoritmo primario como el secundario.

Los niveles del conjunto SOG-IS para los algoritmos primario y secundario son:

— Algoritmo principal: El algoritmo principal es el algoritmo de firma digital de curva elíptica (ECDSA) definido en la sección 2.3 de la norma (ISO/IEC 14888-3:2006), que utiliza los parámetros P-256 definidos en el apéndice D (D.1.2.3) de la norma (FIPS PUB 186-4) en combinación con el algoritmo de hash SHA-256 definido en la función 4 de la norma (ISO/IEC 10118-3:2004).

Esto corresponde al parámetro ES256 del algoritmo COSE.

— Algoritmo secundario: El algoritmo secundario es el RSASSA-PSS definido en (RFC 8230 ([3])) con un módulo de 2048 bits en combinación con el algoritmo de hash SHA-256 definido en la función 4 (ISO/IEC 10118-3:2004).

Esto corresponde al parámetro del algoritmo COSE: PS256.

3.2.3. Identificador de clave

La notificación de identificador de clave (kid) indica el certificado de firmante de documentos (DSC) que contiene la clave pública que debe utilizar el verificador para comprobar la exactitud de la firma digital. La gobernanza de los certificados de clave pública, incluidos los requisitos aplicables a los DSC, se describe en el anexo IV.

Los verificadores utilizan la notificación de identificador de clave(kid) para seleccionar la clave pública correcta de una lista de claves pertenecientes al emisor indicado en la notificación de emisor (iss). Un emisor puede utilizar varias claves en paralelo por razones administrativas y al realizar sustituciones de claves. El identificador de clave no es un campo crítico para la seguridad. Por esta razón, también puede colocarse en un encabezado no protegido si es necesario. Los verificadores deben aceptar ambas opciones. Si se dan ambas opciones, se debe utilizar el identificador de clave del encabezado protegido.

Debido al acortamiento del identificador (por razones de limitación del espacio), existe una posibilidad pequeña, pero no nula, de que la lista general de DSC aceptada por un verificador contenga DSC con kid duplicados. Por esta razón, un verificador debe comprobar todos los DSC con ese kid.

3.2.4. Emisor

La notificación de emisor (iss) es un valor de cadena que, a título facultativo, puede contener el código de país ISO 3166-1 alfa-2 de la entidad que emite el certificado sanitario. Un verificador puede usar esta notificación para identificar qué conjunto de DSC debe utilizarse para la validación. La clave de notificación 1 se utiliza para identificar esta notificación.

3.2.5. Hora de expiración

La notificación de hora de expiración (exp) deberá contener un sello de tiempo en el formato NumericDate (como se especifica en la sección 2 de RFC 8392 ([4])) que indique durante cuánto tiempo se considerará válida esta firma particular sobre la carga útil, después de lo cual un verificador deberá rechazar la carga útil como expirada. La finalidad del parámetro de expiración es forzar un límite del período de validez del certificado sanitario. La clave de notificación 4 se utiliza para identificar esta notificación.

La hora de expiración no debe exceder el período de validez del DSC.

([3]) rfc8230 (ietf.org).
([4]) rfc8392 (ietf.org)

3.2.6. Emitido a las

La notificación «emitido a las» (iat) deberá contener un sello de tiempo en el formato NumericDate (como se especifica en la sección 2 de RFC 8392 ([5])), que indique la hora de creación del certificado sanitario.

El valor del campo Emitido a las no debe ser anterior al período de validez del DSC.

Los verificadores pueden aplicar políticas adicionales con el fin de restringir la validez del certificado sanitario en función de la hora de su emisión. La clave de notificación 6 se utiliza para identificar esta notificación.

3.2.7. Notificación de certificado sanitario

La notificación de certificado sanitario (hcert) es un objeto JSON (RFC 7159 ([6])) que contiene la información sobre el estado de salud. Pueden existir varios tipos diferentes de certificados sanitarios bajo la misma notificación, uno de los cuales es el CCD.

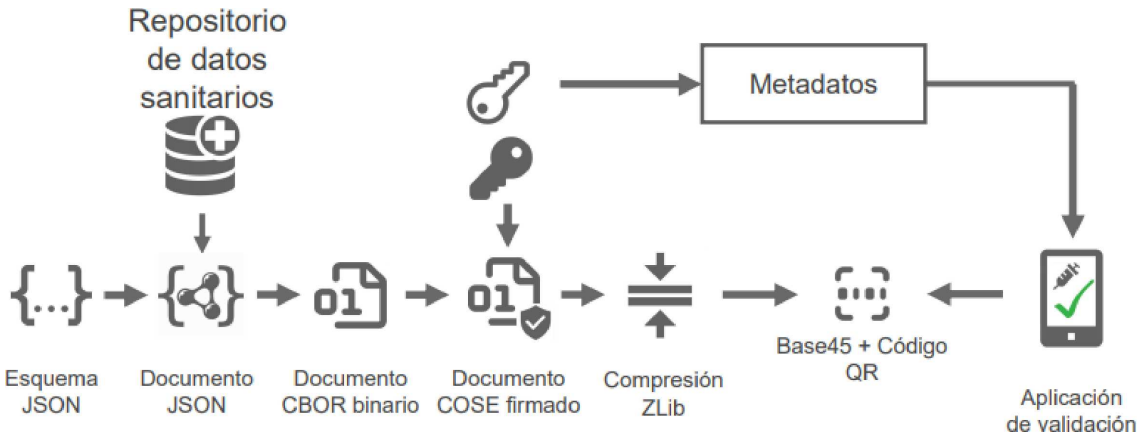
El JSON sirve meramente para fines de esquema. El formato de representación es CBOR, como se define en (RFC 7049 ([7])). Es posible que los desarrolladores de aplicaciones no decodifiquen nunca, ni codifiquen desde y hacia el formato JSON, sino que utilicen la estructura en memoria.

La clave de notificación que se utiliza para identificar esta notificación es -260.

Las cadenas del objeto JSON deben normalizarse de acuerdo con la composición canónica de formato de normalización (NFC) definida en la norma Unicode. Sin embargo, las aplicaciones de decodificación deben ser permisivas y robustas en estos aspectos, y se recomienda encarecidamente la aceptación de cualquier conversión de un tipo razonable. Si se encuentran datos no normalizados durante la decodificación, o en funciones de comparación posteriores, las implementaciones deben comportarse como si la entrada estuviera normalizada con respecto a NFC.

4. **Serialización y creación de la carga útil del CCD**

Como patrón de serialización, se utiliza el siguiente esquema:



El proceso comienza con la extracción de datos, por ejemplo, de un repositorio de datos sanitarios (o de alguna fuente de datos externa), y los datos extraídos se estructuran según los esquemas de CCD definidos. En este proceso, la conversión al formato de datos definido y la transformación para la legibilidad humana pueden tener lugar antes de que comience la serialización a CBOR. Las siglas de las notificaciones se asignarán en todos los casos a los nombres de visualización antes de la serialización y después de la deserialización.

No se permite contenido opcional de datos nacionales en los certificados emitidos conforme al Reglamento (UE) 2021/953 ([8]). El contenido de los datos se limita a los elementos de datos definidos en el conjunto mínimo de datos especificado en el anexo de dicho Reglamento (UE) 2021/953.

([5]) rfc8392 (ietf.org)
([6]) rfc7159 (ietf.org).
([7]) rfc7049 (ietf.org).
([8]) Reglamento (UE) 2021/953 del Parlamento Europeo y del Consejo, de 14 de junio de 2021, relativo a un marco para la expedición, verificación y aceptación de certificados COVID-19 interoperables de vacunación, de prueba diagnóstica y de recuperación (certificado COVID digital de la UE) a fin de facilitar la libre circulación durante la pandemia de COVID-19, DO L 211 de 15.6.2021, p. 1.

5. **Codificaciones de transporte**

5.1. *Sin procesar*

Para interfaces de datos arbitrarias, el contenedor HCERT y sus cargas útiles pueden transferirse «tal cual», utilizando cualquier transporte de datos subyacente, seguro y fiable de 8 bits. Estas interfaces pueden incluir comunicación de campo próximo (NFC), Bluetooth o la transferencia a través de un protocolo de capa de aplicación, por ejemplo, la transferencia de un HCERT del emisor al dispositivo móvil del titular.

Si la transferencia del HCERT del emisor al titular se basa en una interfaz de solo presentación (por ejemplo, SMS, correo electrónico), la codificación de transporte sin procesar obviamente no es aplicable.

5.2. *Código de barras*

5.2.1. Compresión de la carga útil (CWT)

Para reducir el tamaño y mejorar la velocidad y la fiabilidad en el proceso de lectura del HCERT, el CWT deberá comprimirse utilizando ZLIB ((RFC 1950 ([9])) y el mecanismo de compresión Deflate en el formato definido en (RFC 1951 ([10])).

5.2.2. Código de barras QR 2D

Para poder manejar mejor los equipos heredados diseñados para operar con cargas útiles ASCII, el CWT comprimido se codifica como ASCII utilizando Base45 antes de ser codificado en un código de barras 2D.

Se utilizará el formato QR definido en (ISO/IEC 18004:2015) para la generación de códigos de barras 2D. Se recomienda una tasa de corrección de errores «Q» (alrededor del 25 %). Dado que se utiliza Base45, el código QR debe utilizar codificación alfanumérica (modo 2, indicado por los símbolos 0010).

Para que los verificadores puedan detectar el tipo de datos codificados y seleccionar el esquema de decodificación y procesamiento adecuado, los datos codificados en Base45 (según esta especificación) deberán llevar como prefijo la cadena de identificador de contexto «HC1:». Las futuras versiones de esta especificación que afecten a la retrocompatibilidad deberán definir un nuevo identificador de contexto, mientras que el carácter que sigue a «HC» deberá tomarse del conjunto de caracteres [1-9A-Z]. El orden de los incrementos se define en ese orden, es decir, primero [1-9] y luego [A-Z].

Se recomienda que el código óptico se represente en el soporte de presentación con una diagonal de entre 35 mm y 60 mm para adaptarse a los lectores con óptica fija en los que se requiere que el soporte de presentación se coloque en la superficie del lector.

Si el código óptico se imprime en papel con impresoras de baja resolución (< 300 ppp), debe prestarse atención a que cada símbolo (punto) del código QR se represente con cuadrados exactos. Una escala no proporcional llevará a que algunas filas o columnas del QR tengan símbolos rectangulares, lo que en muchos casos dificultará la legibilidad.

6. **Formato de listas de confianza (lista de DSC y CSCA)**

Cada Estado miembro tiene la obligación de proporcionar una lista de una o más autoridades nacionales de firma de certificados (CSCA) y una lista de todos los certificados de firmante de documentos (DSC) válidos, y de mantener estas listas actualizadas.

6.1. *CSCA/DSC simplificados*

A partir de esta versión de las especificaciones, los Estados miembros no partirán del principio de que se utiliza información alguna de la lista de revocación de certificados (CRL), ni que el período de uso de la clave privada es verificado por los implementadores.

En cambio, el principal mecanismo de validez es la presencia del certificado en la versión más reciente de esa lista de certificados.

([9]) rfc1950 (ietf.org).
([10]) rfc1951 (ietf.org).

6.2. *Infraestructura de clave pública (PKI) de e-DVLM de la OACI y centros de confianza*

Los Estados miembros pueden utilizar una CSCA diferente, pero también pueden presentar sus certificados CSCA de e-DVLM y/o DSC existentes, e incluso pueden optar por obtenerlos en estos centros de confianza (comerciales) y presentarlos. Ahora bien, todo DSC debe estar siempre firmado por la CSCA presentada por ese Estado miembro.

7. **Consideraciones de seguridad**

Cuando diseñen un sistema utilizando esta especificación, los Estados miembros deberán identificar, analizar y supervisar determinados aspectos de seguridad.

Como mínimo, deben tenerse en cuenta los siguientes aspectos:

7.1. *Tiempo de validez de la firma HCERT*

El emisor de HCERT debe limitar el período de validez de la firma especificando una hora de expiración de la misma. Esto obliga al titular de un certificado sanitario a renovarlo a intervalos periódicos.

El período de validez aceptable puede estar determinado por limitaciones prácticas. Por ejemplo, un viajero puede no tener la posibilidad de renovar el certificado sanitario durante un viaje al extranjero. Sin embargo, también puede darse el caso de que un emisor esté considerando la posibilidad de que se produzca algún tipo de ataque a la seguridad que exija que el emisor retire un DSC (invalidando todos los certificados sanitarios emitidos con esa clave que aún estén dentro de su período de validez). Las consecuencias de un incidente de este tipo pueden limitarse alternando periódicamente las claves del emisor y exigiendo la renovación de todos los certificados sanitarios, con un intervalo razonable.

7.2. *Gestión de claves*

Esta especificación se basa en gran medida en fuertes mecanismos criptográficos para asegurar la integridad de los datos y la autenticación de su origen. Por lo tanto, es necesario mantener la confidencialidad de las claves privadas.

La confidencialidad de las claves criptográficas puede verse comprometida de diferentes maneras, por ejemplo:

— El proceso de generación de claves puede ser defectuoso, dando lugar a claves débiles.

— Las claves pueden quedar expuestas por un error humano.

— Las claves pueden ser robadas por agentes externos o internos.

— Las claves pueden calcularse mediante criptoanálisis.

Para mitigar el riesgo de que el algoritmo de firma sea débil, lo cual permitiría que las claves privadas se vieran comprometidas por medio del criptoanálisis, esta especificación recomienda a todos los participantes que implementen un algoritmo de firma secundario de reserva basado en parámetros diferentes o en un problema matemático distinto del primario.

En cuanto a los riesgos mencionados relacionados con los entornos operativos de los emisores, se aplicarán medidas de mitigación para garantizar un control eficaz, como la generación, el almacenamiento y la utilización de las claves privadas en módulos de seguridad de hardware (HSM). Se recomienda encarecidamente el uso de HSM para la firma de certificados sanitarios.

Independientemente de que un emisor decida utilizar HSM o no, debe establecerse un calendario de sustitución de claves en el que la frecuencia de sustitución sea proporcional a la exposición de las claves a redes externas, otros sistemas y otro personal. Un calendario de sustitución bien elegido también limita los riesgos asociados a los certificados sanitarios emitidos de manera errónea y permite a un emisor revocar dichos certificados sanitarios por lotes, retirando una clave, si es necesario.

7.3. *Validación de datos de entrada*

Estas especificaciones pueden utilizarse de forma que impliquen la recepción de datos de fuentes no fiables en sistemas que pueden ser de naturaleza crítica. Para minimizar los riesgos asociados a este vector de ataque, todos los campos de entrada deben ser validados adecuadamente por tipos de datos, longitudes y contenidos. La firma del emisor también se deberá verificar antes de que tenga lugar cualquier procesamiento del contenido del HCERT. Sin embargo, la validación de la firma del emisor implica en primer lugar el análisis sintáctico del encabezado del emisor protegido, en el que un posible atacante puede intentar inyectar información cuidadosamente diseñada para comprometer la seguridad del sistema.

8. **Gestión de la confianza**

La firma del HCERT requiere una clave pública para su verificación. Los Estados miembros harán públicas estas claves. En última instancia, cada verificador necesita tener una lista de todas las claves públicas en las que está dispuesto a confiar (ya que la clave pública no forma parte del HCERT).

El sistema consta de (solo) dos capas; para cada Estado miembro, uno o varios certificados a nivel de país que firman uno o varios certificados de firmante de documentos que se utilizan en las operaciones cotidianas.

Los certificados de los Estados miembros se denominan certificados de las autoridades nacionales de firma de certificados y son (por lo general) certificados autofirmados. Los Estados miembros pueden tener más de uno (por ejemplo, en caso de descentralización regional). Estos certificados CSCA firman periódicamente los certificados de firmante de documentos (DSC) utilizados para firmar los HCERT.

La «Secretaría» desempeña un papel funcional. Agregará y publicará periódicamente los DSC de los Estados miembros, después de haberlos cotejado con la lista de certificados CSCA (que se han transmitido y verificado por otros medios).

La lista resultante de DSC proporcionará entonces el conjunto agregado de claves públicas aceptables (y los correspondientes identificadores de clave) que los verificadores pueden utilizar para validar las firmas sobre los HCERT. Los verificadores deben obtener y actualizar esta lista periódicamente.

Estas listas específicas de los Estados miembros pueden adaptarse en el formato para su propio entorno nacional. Por consiguiente, el formato de archivo de esta lista de confianza puede variar, por ejemplo, puede ser un JWKS firmado (formato del conjunto JWK según la sección 5 de RFC 7517 ([11])) o cualquier otro formato específico de la tecnología utilizada en ese Estado miembro.

Para garantizar la simplicidad, los Estados miembros pueden presentar sus certificados CSCA existentes desde sus sistemas e-DVLM de la OACI o, como recomienda la OMS, crear uno específico para este ámbito sanitario.

8.1. *Identificador de clave (kids)*

El identificador de clave (kid) se calcula al construir la lista de claves públicas de confianza a partir de los DSC y consiste en una huella dactilar SHA-256 truncada (primeros 8 bytes) del DSC codificada en formato DER (sin procesar).

Los verificadores no necesitan calcular el KID basándose en el certificado DSC y pueden cotejar directamente el identificador de clave en el certificado sanitario emitido con el KID de la lista de confianza.

8.2. *Diferencias con el modelo de confianza PKI del e-DVLM de la OACI*

Aunque se basa en las mejores prácticas del modelo de confianza PKI del e-DVLM de la OACI, se harán una serie de simplificaciones en aras de la rapidez:

— Un Estado miembro puede presentar varios certificados CSCA.

— Se puede establecer para el período de validez del DSC (uso de la clave) cualquier duración que no exceda la del certificado CSCA, y dicho período puede no indicarse.

— El DSC puede contener identificadores de políticas (uso de claves extendido) que son específicos de la red de sanidad electrónica.

— Los Estados miembros pueden optar por no verificar nunca las revocaciones publicadas, sino, en lugar de ello, basarse exclusivamente en las listas de DSC que reciben diariamente de la Secretaría o que elaboran ellos mismos.

([11]) rfc7517 (ietf.org).

ANEXO II

NORMAS PARA CUMPLIMENTAR EL CERTIFICADO COVID DIGITAL DE LA UE

Las normas generales relativas a los conjuntos de valores establecidos en el presente anexo tienen por objeto garantizar la interoperabilidad en el plano semántico y permitirán implementaciones técnicas uniformes para el CCD. Los elementos contenidos en este anexo pueden utilizarse en los tres diferentes escenarios (vacunación/pruebas/recuperación), tal como se establece en el Reglamento (UE) 2021/953. En este anexo solo se enumeran los elementos que requieren una normalización semántica mediante conjuntos de valores codificados.

La traducción de los elementos codificados a la lengua nacional es responsabilidad de los Estados miembros.

Para todos los campos de datos no mencionados en las siguientes descripciones de conjuntos de valores, se recomienda la codificación en UTF-8 (nombre, centro de realización de pruebas, emisor del certificado). Se recomienda que los campos de datos que contengan fechas de calendario (fecha de nacimiento, fecha de vacunación, fecha de recogida de la muestra de la prueba, fecha del primer resultado positivo de la prueba, fechas de validez del certificado) se codifiquen siguiendo la norma ISO 8601.

Si por alguna razón no se pueden utilizar los sistemas de codificación preferidos que se enumeran a continuación, se pueden utilizar otros sistemas de codificación internacionales y se debe asesorar sobre cómo asignar los códigos del otro sistema de codificación al sistema de codificación preferido. El texto (nombres de visualización) puede utilizarse en casos excepcionales como mecanismo de reserva cuando no se dispone de un código adecuado en los conjuntos de valores definidos.

Los Estados miembros que utilicen otro tipo de codificación en sus sistemas deberán asignar dichos códigos a los conjuntos de valores descritos. Los Estados miembros son responsables de estas asignaciones.

Los conjuntos de valores serán actualizados periódicamente por la Comisión con el apoyo de la red de sanidad electrónica y el Comité de Seguridad Sanitaria. Los conjuntos de valores actualizados se publicarán en el sitio web correspondiente de la Comisión, así como en la página web de la red de sanidad electrónica. Se debe proporcionar un historial de cambios.

1. **Enfermedad o agente al que se dirige/Enfermedad o agente del que se ha recuperado el titular: COVID-19 (SARS-CoV-2 o una de sus variantes)**

   Sistema de codificación preferido: SNOMED CT.

   Utilícese en los certificados 1, 2 y 3.

   Los códigos seleccionados harán referencia a la COVID-19 o, si se necesita información más detallada sobre la variante genética del SARS-CoV-2, a estas variantes si dicha información detallada es necesaria por razones epidemiológicas.

   Un ejemplo de código que debe utilizarse es el código SNOMED CT 840539006 (COVID-19).

2. **Vacuna o profilaxis de la COVID-19**

   Sistema de codificación preferido: Clasificación SNOMED CT o ATC

   Utilícese en el certificado 1.

   Algunos de los códigos que deben utilizarse de los sistemas de codificación preferidos son, por ejemplo, el código SNOMED CT 1119305005 (vacuna de antígeno del SARS-CoV-2), 1119349007 (vacuna de ARNm del SARS-CoV-2) o J07BX03 (vacunas de la COVID-19). El conjunto de valores debe ampliarse cuando se desarrollen y pongan en uso nuevos tipos de vacunas.

3. **Vacuna contra la COVID-19**

   Sistemas de codificación preferidos (por orden de preferencia):

   — Registro de la Unión de medicamentos para vacunas con autorización para toda la UE (números de autorización).

   — Un registro mundial de vacunas, como el que podría establecer la Organización Mundial de la Salud.

   — Nombre de la vacuna en otros casos. Si el nombre incluye espacios en blanco, estos deben sustituirse por un guion (-).

Nombre del conjunto de valores: Vacuna.

Utilícese en el certificado 1.

Un ejemplo de código de los sistemas de codificación preferidos que debe utilizarse es EU/1/20/1528 (Comirnaty). Ejemplo de nombre de la vacuna que se utilizará como código: Sputnik-V (siglas de Sputnik V).

4. **Titular de la autorización de comercialización o fabricante de la vacuna contra la COVID-19**

Sistema de codificación preferido:

— Código de organización de la EMA (sistema SPOR para ISO IDMP).

— Un registro mundial de titulares de autorizaciones de comercialización o de fabricantes de vacunas, como el que podría establecer la Organización Mundial de la Salud.

— Nombre de la organización en otros casos. Si el nombre incluye espacios en blanco, estos deben sustituirse por un guion (-).

Utilícese en el certificado 1.

Un ejemplo de código que debe utilizarse del sistema de codificación preferido es ORG-100001699 (AstraZeneca AB). Un ejemplo de nombre de organización que se utilizará como código: Sinovac-Biotech (siglas de Sinovac Biotech).

5. **Número en una serie de dosis, así como número total de dosis en la serie**

Utilícese en el certificado 1.

Dos campos:

1) Número de dosis administradas en un ciclo.

2) Número de dosis previstas para un ciclo completo (específico para una persona en el momento de la administración).

Por ejemplo, 1/1, 2/2 se presentarán como completados; incluyendo la opción 1/1 para las vacunas que constan de dos dosis, pero para las que el protocolo aplicado por el Estado miembro es administrar una dosis a los ciudadanos a quienes se diagnosticó COVID-19 antes de la vacunación. El número total de dosis en la serie debe indicarse según la información disponible en el momento de la administración de la dosis. Por ejemplo, si una vacuna específica requiere una tercera inyección (refuerzo) en el momento de la última inyección administrada, el segundo número del campo deberá reflejarlo (por ejemplo 2/3, 3/3, etc.).

6. **Estado miembro o tercer país en el que se administró la vacuna/se realizó la prueba**

Sistema de codificación preferido: Códigos de país ISO 3166:

Utilícese en los certificados 1, 2 y 3.

Contenido del conjunto de valores: la lista completa de códigos de 2 letra s), disponible como conjunto de valores definidos en FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2)

7. **Tipo de prueba**

Sistema de codificación preferido: LOINC.

Se utilizará en el certificado 2, y en el certificado 3 si se introduce, mediante un acto delegado, el apoyo a la expedición de certificados de recuperación basados en tipos de prueba distintos de la NAAT.

Los códigos de este conjunto de valores se referirán al método de la prueba y se seleccionarán al menos para separar las pruebas NAAT de las pruebas RAT, tal como se expresa en el Reglamento (UE) 2021/953.

Un ejemplo de código que debe utilizarse del sistema de codificación preferido es LP217198-3 (Inmunoanálisis rápido).

8. **Fabricante y nombre comercial de la prueba utilizada (opcional para la prueba NAAT)**

Sistema de codificación preferido: lista del Comité de Seguridad Sanitaria de pruebas rápidas de antígenos mantenida por el JRC (base de datos de dispositivos de diagnóstico *in vitro* y métodos de prueba de la COVID-19).

Utilícese en el certificado 2.

El contenido del conjunto de valores incluirá la selección de pruebas rápidas de antígenos que figuran en la lista común y actualizada de pruebas rápidas de antígenos de la COVID-19, establecida sobre la base de la Recomendación 2021/C 24/01 del Consejo y acordada por el Comité de Seguridad Sanitaria. El JRC mantiene la lista en la base de datos de dispositivos de diagnóstico *in vitro* y métodos de prueba de la COVID-19 en: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat

Para este sistema de codificación, se utilizarán los campos pertinentes, como el identificador del dispositivo de la prueba, el nombre de la prueba y el fabricante, siguiendo el formato estructurado del JRC disponible en https://covid-19-diagnostics.jrc.ec.europa.eu/devices

9. **Resultado de la prueba**

Sistema de codificación preferido: SNOMED CT.

Utilícese en el certificado 2.

Los códigos seleccionados deberán permitir distinguir entre resultados positivos y negativos de las pruebas (detectado o no detectado). Se pueden añadir valores adicionales (como indeterminado) si los casos de uso lo requieren.

Algunos códigos que deben utilizarse del sistema de codificación preferido son, por ejemplo, 260415000 (No detectado) y 260373001 (Detectado).

ANEXO III

ESTRUCTURA COMÚN DEL IDENTIFICADOR ÚNICO DE CERTIFICADO

1. **Introducción**

Todo certificado COVID digital de la UE (CCD) incluirá un identificador único de certificado (UCI) que contribuya a la interoperabilidad de dichos certificados. El UCI puede utilizarse para verificar el certificado. Los Estados miembros serán responsables de la implementación del UCI. El UCI es un medio para verificar la veracidad del certificado y, en su caso, para enlazar con un sistema de registro (por ejemplo, un sistema de información sobre vacunación). Estos identificadores también permitirán a los Estados miembros afirmar (en papel y digitalmente) que las personas han recibido la vacuna o se han sometido a pruebas.

2. **Composición del identificador único de certificado**

El UCI seguirá una estructura y un formato comunes que faciliten la interpretación humana o mecánica de la información y podrá referirse a elementos como el Estado miembro de vacunación, la propia vacuna y un identificador específico del Estado miembro. Garantiza la flexibilidad de los Estados miembros para formatearlo, respetando plenamente la legislación sobre protección de datos. El orden de los distintos elementos sigue una jerarquía definida que puede permitir futuras modificaciones de los bloques y mantiene su integridad estructural.

Las posibles soluciones para la composición del UCI forman un espectro en el que la modularidad y la interpretabilidad humana son los dos principales parámetros diversificadores y una característica fundamental:

— Modularidad: el grado en que el código está compuesto por bloques componentes distintos que contienen información semánticamente diferente.

— Interpretabilidad humana: el grado en que el código tiene sentido o puede ser interpretado por el lector humano.

— Único a nivel mundial; el identificador de país o autoridad está bien gestionado; y se espera que cada país (autoridad) gestione bien su segmento del espacio de nombres y no recicle ni vuelva a emitir nunca identificadores. La combinación de todo ello garantiza que cada identificador sea único a nivel mundial.

3. **Requisitos generales**

Deben cumplirse los siguientes requisitos generales en relación con el UCI:

1) Juego de caracteres: solo se admiten caracteres alfanuméricos US-ASCII en mayúsculas (de la «A» a la «Z» y del «0» al «9»). con caracteres especiales adicionales para separarse de RFC3986 ([1]) ([2]), a saber {'/','#',':'}.

2) Longitud máxima: los diseñadores deben intentar que la longitud sea de veintisiete a treinta caracteres ([3]).

3) Prefijo de la versión: se refiere a la versión del esquema del UCI. El prefijo de la versión es «01» para esta versión del documento; el prefijo de la versión se compone de dos dígitos.

4) Prefijo del país: el código de país se especifica en la norma ISO 3166-1. Los códigos más largos (de tres caracteres en adelante, por ejemplo, «ACNUR») se reservan para su uso futuro.

5) Sufijo del código/suma de comprobación:

5.1. Los Estados miembros deben utilizar una suma de comprobación cuando sea probable que se produzcan transmisiones, transcripciones (humanas) u otras corrupciones (es decir, cuando se utilice en formato impreso).

5.2. La suma de comprobación no debe utilizarse para validar el certificado y no forma parte técnicamente del identificador, sino que se utiliza para verificar la integridad del código. Esta suma de comprobación debe ser el resumen ISO-7812-1 (LUHN-10) ([4]) de todo el UCI en formato de transporte digital/por cable. La suma de comprobación se separa del resto del UCI con el carácter «#».

([1]) rfc3986 (ietf.org).

([2]) Es posible que los campos como el sexo, el número de lote, el centro administrador, la identificación del profesional sanitario y la fecha de la próxima vacunación no sean necesarios para fines distintos del uso médico.

([3]) Para la aplicación con códigos QR, los Estados miembros podrían considerar la posibilidad de un conjunto adicional de caracteres hasta una longitud total de setenta y dos caracteres (incluidos los veintisiete-treinta del propio identificador) que pueden utilizarse para transmitir otra información. La especificación de esta información corresponde a los Estados miembros.

([4]) El algoritmo Luhn mod N es una extensión del algoritmo Luhn (también conocido como algoritmo mod 10) que funciona para códigos numéricos y se utiliza, por ejemplo, para calcular la suma de comprobación de las tarjetas de crédito. La extensión permite que el algoritmo trabaje con secuencias de valores en cualquier base (en nuestro caso, caracteres alfabéticos).

Debe garantizarse la retrocompatibilidad: los Estados miembros que con el tiempo cambien la estructura de sus identificadores (dentro de la versión principal, actualmente v1) deberán garantizar que dos identificadores idénticos representen el mismo certificado o afirmación de vacunación. O, en otras palabras, los Estados miembros no pueden reciclar los identificadores.

4. **Opciones de identificadores únicos para los certificados de vacunación**

Las directrices de la red de sanidad electrónica para los certificados de vacunación verificables y los elementos básicos de interoperabilidad ([5]) prevén diferentes opciones disponibles para los Estados miembros y otras partes que pueden coexistir entre diferentes Estados miembros. Los Estados miembros pueden utilizar estas diferentes opciones en diferentes versiones del esquema UCI.

([5]) https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf.

ANEXO IV

GOBERNANZA DEL CERTIFICADO DE CLAVE PÚBLICA

1. Introducción

El intercambio seguro y fiable de claves de firma para los certificados COVID digitales (CCD) de la UE entre los Estados miembros se realiza a través de la Pasarela del Certificado COVID Digital de la UE (DCCG), que actúa como repositorio central de las claves públicas. Con la DCCG, los Estados miembros están facultados para publicar las claves públicas correspondientes a las claves privadas que utilizan para firmar los certificados COVID digitales. Los Estados miembros que dependen de ella pueden utilizar la DCCG para obtener material de claves públicas actualizado en el momento oportuno. Más adelante, la DCCG puede ampliarse para intercambiar información complementaria de confianza que proporcionen los Estados miembros, como las normas de validación de los CCD. El modelo de confianza del marco de CCD es una infraestructura de clave pública (PKI). Cada Estado miembro mantiene una o varias autoridades nacionales de firma de certificados (CSCA), cuyos certificados tienen una vida relativamente larga. De acuerdo con la decisión del Estado miembro, la CSCA puede ser la misma o diferente de la utilizada para los documentos de viaje de lectura mecánica. La CSCA emite certificados de clave pública para los firmantes de documentos nacionales, de corta duración (es decir, los firmantes de los CCD), que se denominan certificados de firmante de documentos (DSC). La CSCA actúa como anclaje de confianza, de modo que los Estados miembros que confían en ella pueden utilizar el certificado de la CSCA para validar la autenticidad e integridad de los DSC que cambian periódicamente. Una vez validados, los Estados miembros pueden proporcionar estos certificados (o solo las claves públicas que contienen) a sus aplicaciones de validación del CCD. Además de las CSCA y los DSC, la DCCG también utiliza la PKI para autenticar las transacciones y firmar los datos, como base de la autenticación y como medio para garantizar la integridad de los canales de comunicación entre los Estados miembros y la DCCG.

Las firmas digitales pueden utilizarse para lograr la integridad y la autenticidad de los datos. Las infraestructuras de clave pública establecen la confianza vinculando las claves públicas a identidades verificadas (o emisores). Esto es necesario para que otros participantes puedan verificar el origen de los datos y la identidad del interlocutor de la comunicación y decidir sobre la confianza. En la DCCG, se utilizan varios certificados de clave pública en aras de la autenticidad. Este anexo define qué certificados de clave pública se utilizan y cómo deben diseñarse para permitir una amplia interoperabilidad entre los Estados miembros. Proporciona más detalles sobre los certificados de clave pública necesarios y ofrece orientaciones sobre las plantillas de los certificados y los períodos de validez para los Estados miembros que quieran operar su propia CSCA. Dado que los CCD deben ser verificables durante un período de tiempo definido (a partir de la emisión, expiran después de un tiempo determinado), es necesario definir un modelo de verificación para todas las firmas aplicadas en los certificados de clave pública y los CCD.

2. Terminología

La siguiente tabla contiene las abreviaturas y la terminología utilizadas en este anexo.

Término	Definición
Certificado	O certificado de clave pública. Un certificado X.509 v3 que contiene la clave pública de una entidad
CSCA	Autoridad nacional de firma de certificados
CCD	Certificado COVID digital de la UE. Un documento digital firmado que contiene información sobre la vacunación, las pruebas o la recuperación
DCCG	Pasarela del Certificado COVID Digital de la UE. Este sistema se utiliza para intercambiar DSC entre los Estados miembros
$DCCG_{TA}$	El certificado de anclaje de veracidad de la DCCG. La clave privada correspondiente se utiliza para firmar la lista de todos los certificados CSCA fuera de línea
$DCCG_{TLS}$	El certificado de servidor TLS de la DCCG
DSC	Certificado de firmante de documentos. El certificado de clave pública de la autoridad de firma de documentos de un Estado miembro (por ejemplo, un sistema que está autorizado a firmar CCD). Este certificado lo expide la CSCA del Estado miembro
EC-DSA	Algoritmo de firma digital de curva elíptica. Un algoritmo de firma criptográfica basado en curvas elípticas
Estado miembro	Estado miembro de la Unión Europea

Término	Definición
mTLS	TLS mutua. El protocolo de seguridad de la capa de transporte con autenticación mutua
Nota:	El *backend* nacional de un Estado miembro
NB_{CSCA}	El certificado CSCA de un Estado miembro (puede ser más de uno)
NB_{TLS}	El certificado de autenticación de cliente TLS de un *backend* nacional
NB_{UP}	El certificado que un *backend* nacional utiliza para firmar los paquetes de datos que se cargan en la DCCG
PKI	Infraestructura de clave pública. Modelo de confianza basado en certificados de clave pública y autoridades de certificación
RSA	Algoritmo criptográfico asimétrico basado en la factorización de enteros utilizado para la firma digital o el cifrado asimétrico

3. **Flujos de comunicación y servicios de seguridad de la DCCG**

Esta sección ofrece una visión general de los flujos de comunicación y los servicios de seguridad en el sistema DCCG. También define qué claves y certificados se utilizan para proteger la comunicación, la información cargada, los CCD y una lista de confianza firmada que contiene todos los certificados CSCA incorporados. La DCCG funciona como un centro de datos que permite el intercambio de paquetes de datos firmados para los Estados miembros.

Los paquetes de datos cargados son proporcionados por la DCCG «tal cual», lo que significa que la DCCG no añade ni elimina DSC de los paquetes que recibe. El *backend* nacional (NB) de los Estados miembros estará habilitado para verificar la integridad y autenticidad de extremo a extremo de los datos cargados. Además, los *backend* nacionales y la DCCG utilizarán la autenticación mutua TLS para establecer una conexión segura. Esto se suma a las firmas en los datos intercambiados.

3.1. *Autenticación y establecimiento de la conexión*

La DCCG utiliza la seguridad de la capa de transporte (TLS) con autenticación mutua para establecer un canal cifrado autenticado entre el *backend* nacional (NB) del Estado miembro y el entorno de la Pasarela. Por lo tanto, la DCCG posee un certificado de servidor TLS ($DCCG_{TLS}$) y los *backends* nacionales poseen un certificado de cliente TLS (NB_{TLS}). Las plantillas de los certificados se proporcionan en la *sección 5*. Cada *backend* nacional puede proporcionar su propio certificado TLS. Este certificado se incluirá explícitamente en la lista blanca y, por lo tanto, puede ser emitido por una autoridad certificadora de confianza pública (por ejemplo, una autoridad certificadora que siga los requisitos básicos del CA/Browser Forum), por una autoridad certificadora nacional o puede ser autofirmado. Cada Estado miembro es responsable de sus datos nacionales y de la protección de la clave privada utilizada para establecer la conexión con la DCCG. El enfoque de «traiga su propio certificado» requiere un proceso de registro e identificación bien definido, así como procedimientos de revocación y renovación, como se describe en las *secciones 4.1, 4.2*y *4.3*. La DCCG utiliza una lista blanca en la que se añaden los certificados TLS de los *Nota:* tras haberse registrado satisfactoriamente. Solo los *Nota:* que se autentiquen con una clave privada que corresponda a un certificado de la lista blanca pueden establecer una conexión segura con la DCCG. La DCCG también utilizará un certificado TLS que permite a los *Nota:* verificar que realmente están estableciendo una conexión con la DCCG «real» y no con alguna entidad malintencionada que se hace pasar por ella. El certificado de la DCCG se entregará a los *Nota:* una vez se haya registrado correctamente. El certificado $DCCG_{TLS}$ será emitido por una autoridad de certificación de confianza pública (incluida en todos los principales navegadores). Es responsabilidad de los Estados miembros verificar que su conexión a la DCCG es segura (por ejemplo, cotejando la huella dactilar del certificado $DCCG_{TLS}$ del servidor al que se conecta con la proporcionada tras el registro).

3.2. *Autoridades nacionales de firma de certificados y modelo de validación*

Los Estados miembros que participan en el marco de la DCCG deben utilizar una CSCA para emitir los DSC. Los Estados miembros pueden tener más de una CSCA, por ejemplo, en caso de descentralización regional. Cada Estado miembro puede utilizar las autoridades de certificación existentes o crear una autoridad de certificación específica (posiblemente autofirmada) para el sistema del CCD.

Los Estados miembros deben presentar su(s) certificado(s) CSCA al operador de la DCCG durante el procedimiento oficial de incorporación. Tras el registro satisfactorio del Estado miembro (*véase la sección 4.1 para más detalles*), el operador de la DCCG actualizará una lista de confianza firmada que contiene todos los certificados CSCA que están activos en el marco del CCD. El operador de la DCCG utilizará un par de claves asimétricas específico para firmar la lista de confianza y los certificados en un entorno sin conexión. La clave privada no se almacenará en el sistema DCCG en línea, de manera que, si el sistema en línea se ve comprometido, un atacante no pueda comprometer la lista de confianza. El correspondiente certificado de anclaje de veracidad $DCCG_{TA}$ se proporcionará a los *backends* nacionales durante el proceso de incorporación.

Los Estados miembros pueden obtener la lista de confianza de la DCCG para sus procedimientos de verificación. La CSCA se define como la autoridad de certificación que emite los DSC, por lo que los Estados miembros que utilizan una jerarquía de autoridades de certificación (AC) de varios niveles (por ejemplo, AC raíz -> CSCA -> DSC) deben proporcionar la autoridad de certificación subordinada que emite los DSC. En este caso, si un Estado miembro utiliza una autoridad de certificación existente, el sistema de CCD ignorará todo lo que esté por encima de la CSCA y pondrá en la lista blanca solo la CSCA como anclaje de veracidad (aunque sea una autoridad de certificación subordinada). Esto se debe a que el modelo de la OACI solo permite exactamente dos niveles: una CSCA «raíz» y un DSC «hoja» firmado solo por esa CSCA.

En caso de que un Estado miembro opere su propia CSCA, el Estado miembro es responsable del funcionamiento seguro y de la gestión de claves de esta autoridad de certificación. La CSCA actúa como anclaje de veracidad para los DSC, por lo que la protección de la clave privada de la CSCA es esencial para la integridad del entorno de los CCD. El modelo de verificación en la PKI del CCD es el modelo «shell», que establece que todos los certificados en la validación de la ruta de certificados deben ser válidos en un momento determinado (es decir, en el momento de validación de la firma). Por lo tanto, se aplican las siguientes restricciones:

— La CSCA no emitirá certificados cuya validez sea mayor que la del propio certificado de la autoridad de certificación.

— El firmante del documento no firmará documentos cuya validez sea mayor que la del propio DSC.

— Los Estados miembros que gestionan su propia CSCA deben definir los períodos de validez de su CSCA y de todos los certificados emitidos y deben ocuparse de la renovación de los certificados.

La *sección 4.2* contiene recomendaciones sobre los períodos de validez.

3.3. *Integridad y autenticidad de los datos cargados*

Los *backends* nacionales pueden utilizar la DCCG para cargar y descargar paquetes de datos firmados digitalmente tras una autenticación mutua satisfactoria. En un principio, estos paquetes de datos contienen los DSC de los Estados miembros. El par de claves que utiliza el *backend* nacional para la firma digital de los paquetes de datos cargados en el sistema de la DCCG se denomina «par de claves de firma de carga del *backend* nacional» y el certificado de clave pública correspondiente se abrevia como «certificado NB_{UP}». Cada Estado miembro aporta su propio certificado NB_{UP}, que puede ser autofirmado o emitido por una autoridad de certificación existente, como una autoridad de certificación pública (es decir, una autoridad que emite certificados de acuerdo con los requisitos básicos del CAB-Forum). El certificado NB_{UP} será diferente de cualquier otro certificado utilizado por el Estado miembro (es decir, CSCA, cliente TLS o DSC).

Los Estados miembros deben proporcionar el certificado de carga al operador de la DCCG durante el procedimiento de registro inicial (*véase la sección 4.1 para más detalles*). Cada Estado miembro es responsable de sus datos nacionales y debe proteger la clave privada que se utiliza para firmar las cargas.

Otros Estados miembros pueden verificar los paquetes de datos firmados utilizando los certificados de carga que proporciona la DCCG. La DCCG verifica la autenticidad e integridad de los datos cargados con el certificado de carga de *Nota:* antes de que se faciliten a otros Estados miembros.

3.4. *Requisitos de la arquitectura técnica de la DCCG*

Los requisitos de la arquitectura técnica de la DCCG son los siguientes:

— La DCCG utiliza la autenticación mutua TLS para establecer una conexión cifrada autenticada con los *Nota:* Por lo tanto, la DCCG mantiene una lista blanca de certificados de cliente NB_{TLS} registrados.

— La DCCG utiliza dos certificados digitales ($DCCG_{TLS}$ y $DCCG_{TA}$) con dos pares de claves distintas. La clave privada del par de claves $DCCG_{TA}$ se mantiene fuera de línea (no en los componentes en línea de la DCCG).

— La DCCG mantiene una lista de confianza de los certificados NB_{CSCA} que está firmada con la clave privada $DCCG_{TA}$.

— Los cifrados utilizados deben cumplir los requisitos de la *sección 5.1*.

4. Gestión del ciclo de vida de los certificados

4.1. *Registro de backends nacionales*

Los Estados miembros deben registrarse en el operador de la DCCG para participar en su sistema. Esta sección describe el procedimiento técnico y operativo que debe seguirse para registrar un *backend* nacional.

El operador de la DCCG y el Estado miembro deben intercambiar información sobre las personas de contacto técnico para el proceso de incorporación. Se supone que las personas de contacto técnico están legitimadas por sus Estados miembros y la identificación/autenticación se realiza por otros canales. Por ejemplo, la autenticación puede lograrse cuando el contacto técnico de un Estado miembro proporciona los certificados como archivos cifrados con contraseña por correo electrónico y comparte la contraseña correspondiente con el operador de la DCCG por teléfono. También pueden utilizarse otros canales seguros definidos por el operador de la DCCG.

El Estado miembro debe proporcionar tres certificados digitales durante el proceso de registro e identificación:

— El certificado TLS NB_{TLS} del Estado miembro.

— El certificado de carga NB_{UP} del Estado miembro.

— El certificado o los certificados NB_{CSCA} de la CSCA del Estado miembro.

Todos los certificados proporcionados deben cumplir los requisitos definidos en la *sección 5*. El operador de la DCCG verificará que el certificado proporcionado se adhiere a los requisitos de la *sección 5*. Tras la identificación y el registro, el operador de la DCCG:

— añade el certificado o los certificados NB_{CSCA} a la lista de confianza firmados con la clave privada que corresponde a la clave pública $DCCG_{TA}$;

— añade el certificado NB_{TLS} a la lista blanca del punto final TLS de la DCCG;

— añade el certificado NB_{UP} al sistema DCCG;

— proporciona el certificado de clave pública $DCCG_{TA}$ y $DCCG_{TLS}$ al Estado miembro.

4.2. *Autoridades de certificación, períodos de validez y renovación*

En caso de que un Estado miembro quiera operar su propia CSCA, los certificados de la CSCA pueden ser certificados autofirmados. Actúan como anclaje de veracidad del Estado miembro y, por lo tanto, este debe proteger firmemente la clave privada correspondiente a la clave pública del certificado CSCA. Se recomienda que los Estados miembros utilicen un sistema fuera de línea para su CSCA, es decir, un sistema informático que no esté conectado a ninguna red. Se utilizará un control multipersonal para acceder al sistema (por ejemplo, siguiendo el principio de la presencia de dos personas). Tras la firma de los DSC, se aplicarán controles operativos y el sistema que contiene la clave privada de la CSCA se almacenará de forma segura con estrictos controles de acceso. Se pueden utilizar módulos de seguridad de *hardware* o tarjetas inteligentes para proteger aún más la clave privada de la CSCA. Los certificados digitales contienen un período de validez que obliga a la renovación del certificado. La renovación es necesaria para utilizar claves criptográficas nuevas y para adaptar el tamaño de las claves cuando nuevas mejoras en el cálculo o nuevos ataques amenacen la seguridad del algoritmo criptográfico que se utiliza. Se aplica el modelo «shell» (véase *la sección 3.2*).

Se recomiendan los siguientes períodos de validez, dado que la validez de los certificados COVID digitales es de un año:

— CSCA: 4 años

— DSC: 2 años

— Carga: 1-2 años

— Autenticación de clientes TLS: 1-2 años

Para una renovación oportuna, se recomiendan los siguientes períodos de uso de las claves privadas:

— CSCA: 1 año

— DSC: 6 meses

Los Estados miembros deben crear nuevos certificados de carga y certificados TLS a tiempo, por ejemplo, un mes antes de la expiración, para permitir un funcionamiento sin problemas. Los certificados CSCA y los DSC deben renovarse al menos un mes antes de que finalice el uso de la clave privada (teniendo en cuenta los procedimientos operativos necesarios). Los Estados miembros deben proporcionar los certificados CSCA y los certificados de carga y TLS actualizados al operador de la DCCG. Los certificados caducados se eliminarán de la lista blanca y de la lista de confianza.

Los Estados miembros y el operador de la DCCG deben llevar un control de la validez de sus propios certificados. No existe una entidad central que mantenga un registro de la validez del certificado e informe a los participantes.

4.3. *Revocación de certificados*

En general, los certificados digitales pueden ser revocados por su autoridad de certificación emisora mediante listas de revocación de certificados o el respondedor del protocolo de comprobación del estado de un certificado (respondedor OCSP). Las CSCA para el sistema de CCD deben proporcionar listas de revocación de certificados (CRL). Aunque otros Estados miembros no utilicen actualmente estas CRL, deberían integrarse para futuras aplicaciones. En caso de que una CSCA decida no proporcionar CRL, los DSC de esta CSCA deberán renovarse cuando las CRL sean obligatorias. Los verificadores no deben utilizar OCSP para la validación de los DSC y deben utilizar CRL. Se recomienda que el *backend* nacional realice la validación necesaria de los DSC descargados del Portal de CCD y solo remita un conjunto de DSC de confianza y validados a los validadores de CCD nacionales. Los validadores de CCD no deben realizar ninguna comprobación de revocación de DSC en su proceso de validación. Una de las razones para ello es proteger la privacidad de los titulares de CCD y evitar cualquier posibilidad de que el uso de cualquier DSC particular pueda ser monitorizado por su respondedor OCSP asociado.

Los Estados miembros pueden retirar sus DSC de la DCCG por su cuenta utilizando certificados válidos de carga y TLS. La eliminación de un DSC significa que todos los CCD emitidos con este DSC dejarán de ser válidos cuando los Estados miembros obtengan las listas de DSC actualizadas. La protección del material de clave privada correspondiente a las DSC es crucial. Los Estados miembros deben informar al operador de la DCCG cuando deban revocar los certificados de carga o TLS, por ejemplo, debido a que se haya comprometido el *backend* nacional. El operador de la DCCG puede entonces eliminar la confianza del certificado afectado, por ejemplo, eliminándolo de la lista blanca de TLS. El operador de la DCCG puede eliminar los certificados de carga de la base de datos de la DCCG. Los paquetes firmados con la clave privada correspondiente a este certificado de carga dejarán de ser válidos cuando los *backends* nacionales eliminen la confianza del certificado de carga revocado. En caso de que deba revocarse un certificado CSCA, los Estados miembros informarán al operador de la DCCG, así como a otros Estados miembros con los que tengan relaciones de confianza. El operador de la DCCG emitirá una nueva lista de confianza en la que ya no figure el certificado afectado. Todos los DSC emitidos por esta CSCA dejarán de ser válidos cuando los Estados miembros actualicen su almacén nacional de confianza. En caso de que deban revocarse el certificado $DCCG_{TLS}$ o el certificado $DCCG_{TA}$, el operador de la DCCG y los Estados miembros deberán colaborar para establecer una nueva conexión TLS de confianza y una lista de confianza.

5. **Plantillas de certificados**

Esta sección establece los requisitos criptográficos y orientaciones, así como los requisitos sobre las plantillas de los certificados. Para los certificados de la DCCG, esta sección define las plantillas de los certificados.

5.1. *Requisitos criptográficos*

Los algoritmos criptográficos y los conjuntos de cifrado TLS se elegirán sobre la base de la recomendación actual del Servicio federal alemán de Seguridad de la Información (BSI) o SOG-IS. Estas recomendaciones y las de otras instituciones y organizaciones de normalización son similares. Las recomendaciones pueden encontrarse en las directrices técnicas TR 02102-1 y TR 02102-2 ([1]) o en los mecanismos criptográficos acordados por SOG-IS ([2]).

5.1.1. Requisitos del DSC

Se aplicarán los requisitos previstos en el *anexo I* de la *sección 3.2.2*. Por lo tanto, se recomienda encarecidamente que los firmantes de documentos utilicen el algoritmo de firma digital de curva elíptica (ECDSA) con NIST-p-256 (como se define en el apéndice D de FIPS PUB 186-4). No se admiten otras curvas elípticas. Debido a las restricciones de espacio del CCD, los Estados miembros no deben utilizar el RSA-PSS, aunque se permita como algoritmo de

([1]) BSI - Directrices técnicas TR-02102 (bund.de).
([2]) SOG-IS - Documentos de apoyo (sogis.eu).

reserva. En caso de que los Estados miembros utilicen el RSA-PSS, deberán utilizar un tamaño de módulo de 2048 o, como máximo, de 3072 bits. Se utilizará SHA-2 con una longitud de salida de ≥ 256 bits como función resumen (hash) criptográfica (véase ISO/IEC 10118-3:2004) para la firma DSC.

5.1.2. Requisitos sobre certificados TLS, de carga y CSCA

Para los certificados digitales y las firmas criptográficas en el contexto de la DCCG, los principales requisitos sobre los algoritmos criptográficos y la longitud de las claves se resumen en la siguiente tabla (a partir de 2021):

Algoritmo de firma	Tamaño de la clave	Función resumen (hash)
EC-DSA	Mínimo 250 bits	SHA-2 con una longitud de salida ≥ 256 bits
RSA-PSS (relleno recomendado) RSA-PKCS#1 v1.5 (relleno heredado)	Mínimo 3000 bits de módulo RSA (N) con un exponente público e > 2^16	SHA-2 con una longitud de salida ≥ 256 bits
DSA	Mín. 3000 bits primo p, 250 bits clave q	SHA-2 con una longitud de salida ≥ 256 bits

La curva elíptica recomendada para EC-DSA es NIST-p-256 debido a su aplicación generalizada.

5.2. *Certificado CSCA (NB_{CSCA})*

El siguiente cuadro ofrece orientación sobre el modelo de certificado NB_{CSCA} si un Estado miembro decide operar su propio CSCA para el sistema de CCD.

Las entradas **en negrita** son obligatorias (deben incluirse en el certificado), las entradas *en cursiva* son recomendables (deberían incluirse). Para los campos ausentes, no se definen recomendaciones.

Campo	Valor
Subject	**cn=<nombre común único y no vacío>,***o=<Proveedor>*,**c=<Estado miembro que opera la CSCA>**
Key usage	**firma de certificados,***firma de CRL* (como mínimo)
Restricciones básicas	**CA = true, path length constraints = 0**

El nombre del asunto no debe estar vacío y debe ser único dentro del Estado miembro especificado. El código de país (c) debe coincidir con el Estado miembro que utilizará este certificado CSCA. El certificado debe contener un identificador de clave del firmante único (SKI) según RFC 5280 ([3]).

5.3. *Certificado de firmante de documentos (DSC)*

El siguiente cuadro proporciona orientación sobre el DSC. Las entradas **en negrita** son obligatorias (deben incluirse en el certificado), las entradas *en cursiva* son recomendables (deben incluirse). Para los campos ausentes, no se definen recomendaciones.

Campo	Valor
Serial Number	**número de serie único**
Subject	**cn=<nombre común único y no vacío>**, *o=<Proveedor>*, **c=<Estado miembro que utiliza este DSC>**
Key Usage	**digital signature** (como mínimo)

([3]) rfc5280 (ietf.org).

El DSC debe estar firmado con la clave privada correspondiente a un certificado CSCA que utilice el Estado miembro.

Se deben utilizar las siguientes extensiones:

— El certificado debe contener un identificador de clave de autoridad (AKI) que coincida con el identificador de clave del firmante (SKI) del certificado CSCA emisor.

— El certificado debe contener un identificador de clave de firmante único (de acuerdo con RFC 5280 ([4])).

Además, el certificado debe contener la extensión de punto de distribución CRL que apunta a la lista de revocación de certificados (CRL) que proporciona la CSCA que emitió el DSC.

El DSC puede contener una extensión de uso de claves extendido con cero o más identificadores de políticas de uso de la clave que restringen los tipos de HCERT que este certificado puede verificar. Si hay uno o más, los verificadores comprobarán el uso de la clave con el HCERT almacenado. Para ello se definen los siguientes valores de «extendedKeyUsage»:

Campo	Valor
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 para emisores de pruebas
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 para emisores de vacunas
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 para emisores de recuperación

En ausencia de cualquier extensión de uso de claves (es decir, sin extensiones o con cero extensiones), este certificado puede utilizarse para validar cualquier tipo de HCERT. Otros documentos pueden definir los correspondientes identificadores de políticas de uso de claves extendido que se utilizan con la validación de los HCERT.

5.4. *Carga de certificados (NBUP)*

El siguiente cuadro proporciona una guía para el certificado de carga del *backend* nacional. Las entradas **en negrita** son obligatorias (deben incluirse en el certificado), las entradas *en cursiva* son recomendables (deben incluirse). Para los campos ausentes, no se definen recomendaciones.

Campo	Valor
Subject	**cn=<nombre común no vacío y único>**, *o=<Proveedor>*, **c=<Estado miembro que utiliza este certificado de carga>**
Key Usage	**digital signature** (como mínimo)

5.5. *Autenticación de clientes TLS del backend nacional (NB_{TLS})*

El siguiente cuadro proporciona orientación para el certificado de autenticación de cliente TLS de *backend* nacional. Las entradas **en negrita** son obligatorias (deben incluirse en el certificado), las entradas *en cursiva* son recomendables (deben incluirse). Para los campos ausentes, no se definen recomendaciones.

Campo	Valor
Subject	**cn=<nombre común no vacío y único>**, *o=<Proveedor>*, **c=<Estado miembro en el *backend* nacional>**
Key Usage	**digital signature** (como mínimo)
Extended key usage	client authentication (1.3.6.1.5.5.7.3.2)

([4]) rfc5280 (ietf.org).

El certificado también puede contener el *server authentication (1.3.6.1.5.5.7.3.1)* del uso de claves extendido, pero no es obligatorio.

5.6. *Certificado de firma de lista de confianza ($DCCG_{TA}$)*

El siguiente cuadro define el certificado de anclaje de veracidad de la DCCG.

Campo	Valor
Subject	**cn = Digital Green Certificate Gateway** ([5]), **o=<Proveedor>, c=<país>**
Key Usage	**digital signature** (como mínimo)

5.7. *Certificados de servidor de TLS de la DCCG ($DCCG_{TLS}$)*

El siguiente cuadro define el certificado TLS de la DCCG.

Campo	Valor
Subject	cn=<FQDN o dirección IP de la DCCG>, o=<Proveedor>, c=<país>
SubjectAltName	dnsName: <nombre DNS de la DCCG> o su iPAddress: <Dirección IP de la DCCG>
Key Usage	**digital signature** (como mínimo)
Extended Key usage	server authentication (1.3.6.1.5.5.7.3.1)

El certificado también puede contener el *client authentication (1.3.6.1.5.5.7.3.2)* del uso de claves extendido, pero no es obligatorio.

El certificado TLS de la DCCG deberá ser emitido por una autoridad de certificación de confianza pública (incluida en todos los principales navegadores y sistemas operativos, siguiendo los requisitos básicos del CAB Forum).

([5]) En este contexto se ha mantenido el término «certificado verde digital» en lugar de «certificado COVID digital de la UE» porque es el término que se codificó y utilizó en el certificado antes de que los colegisladores eligieran un nuevo término.