

España, pionera en los Pasaportes COVID con certificado cualificado

La puesta en marcha del Pasaporte COVID ha supuesto un reto para la Administración que ha conseguido ponerlo en marcha en un tiempo récord y con una infraestructura pionera, contando con la colaboración de EADTrust

En este último año y medio se han incluido una enorme cantidad de términos al vocabulario como, por ejemplo: “nueva normalidad”, “aplanar la curva”, “desescalada” o “teletrabajo”. Sin embargo, en los últimos meses hay uno que predomina por encima de los demás: el “Pasaporte COVID”.

En general, todo el mundo tiene una idea de qué es el Pasaporte COVID (o certificado COVID, de acuerdo con su nombre oficial) pero muy pocos saben el desafío tecnológico que ha supuesto para las autoridades sanitarias europeas y, especialmente, para las españolas.

Cuando una persona se descarga su Pasaporte COVID – ya sea porque se ha vacunado, porque ha recibido el alta hospitalaria o porque se ha realizado una prueba diagnóstica – simplemente ve un documento con una serie de datos personales y un código QR. Algo que, aparentemente, parece tan sencillo tiene, sin embargo, grandes implicaciones para la seguridad de la información de los ciudadanos.

Los datos médicos son un tipo de información muy sensible y, por eso, están recogidos en una categoría especial dentro del Reglamento General de Protección de Datos (RGPD) que impiden su tratamiento (artículo 9.1) salvo determinadas excepciones como, por ejemplo, el interés público esencial al que alude el Reglamento (UE) 2021/953 relativo a los certificados COVID-19 en su considerando 48, para justificarlo.

La necesidad de tener un documento que recoja estos datos sanitarios de los ciudadanos en un espacio de tiempo tan rápido, al alcance de todos y garantizando la seguridad de la información ha constituido todo un reto para las Administraciones.

La OMS sienta las bases para su desarrollo

A pesar de la postura de la Organización Mundial de la Salud (OMS) que rechaza exigir certificados de vacunación a los viajeros para entrar o salir de un país, la Unión Europea, ante las iniciativas de los Estados Miembros de expedir certificados de vacunación, puso en marcha el proyecto de un certificado con un enfoque común sobre el contenido, el formato, los principios, las normas técnicas y el nivel de seguridad, de manera que pudieran ser utilizados eficazmente en el contexto transfronterizo.

La propia OMS publicó en marzo un documento de Orientaciones para la elaboración de un Certificado de vacunación inteligente que evite fraudes y falsificaciones y, aunque haya nacido con la COVID-19, que pueda utilizarse en el futuro para demostrar las vacunaciones de otras enfermedades como la

Polio o la Fiebre Amarilla. Estas orientaciones, que incluyen requerimientos técnicos, han constituido la base del actual Pasaporte COVID europeo.

El fundamento de los certificados COVID es que los países puedan confiar en ellos, que no existan dudas de la veracidad de los datos que contiene. El método utilizado para crear ese marco de confianza es el uso de Infraestructuras de Clave Pública (PKI en sus siglas en inglés) para cifrar la información recogida por los Pasaportes COVID mediante certificados de Sello de Entidad.

¿Cómo se asegura la información de los ciudadanos?

Por un lado, gracias a las PKIs, las autoridades que van a leer los códigos QR tienen garantías de la identidad del emisor del Pasaporte, lo que legitima la validez del documento y, por otro, se garantiza que los datos que están recogidos en el Pasaporte COVID no se han modificado. De esta manera, cuando una autoridad lea el Código QR, se comprobará que la información que aparece es igual que la que está en la base de datos de la Comunidad. Por tanto, el documento en PDF no se puede falsificar. No cabe la posibilidad de que una persona intente modificarlo para incorporar pruebas falsas o vacunas que no se ha puesto.

Una estructura del año 2001 para una tecnología de 2021

Las recomendaciones de la OMS referentes al Pasaporte COVID incluyen la creación de una PKI nacional por parte de las autoridades sanitarias, es decir, montar una Autoridad de Certificación (en adelante CA) dentro de cada Estado (puede ser más de una) que emita certificados electrónicos destinados únicamente a firmar certificados COVID. Es decir, recomiendan copiar la infraestructura creada para los pasaportes convencionales.

Actualmente, siguiendo las indicaciones que estableció la ICAO (Organización de Aviación Civil Internacional, en sus siglas en inglés) tras los atentados del 11S, cada Estado tiene una autoridad que expide todos los certificados de los pasaportes y se denomina CSCA (Country Signing Certificate Authority). En España la CSCA es la Dirección General de la Policía quien expide los pasaportes, que incluyen información biométrica cifrada en un chip.

¿Qué ha hecho Europa?

Cuando la UE redactó los requisitos técnicos para el Pasaporte COVID incorporó directamente esta estructura sin tener en cuenta las dificultades que implica crear una Autoridad de Certificación nacional únicamente para emitir certificados electrónicos que firmen los datos de los Pasaportes COVID. Además de la importante inversión, las Autoridades de Certificación se tienen que someter a arduos procesos de control por expertos auditores para garantizar la seguridad de los procesos, por lo que la creación y puesta en marcha de una CA es un proceso que generalmente se alarga años.

Además, otro de los requisitos incorporados por las especificaciones del Pasaporte COVID es la longitud de clave de la firma electrónica, que determina la robustez de la clave y su dificultad para ser descifrada por agentes externos. Se ha establecido que para las firmas electrónicas de los Pasaportes, el sistema utilizado sería la Criptografía de Curva Elíptica (ECC) que permite mayor robustez criptográfica con menores tamaños de clave, por lo que es más ligero, rápido y seguro que las claves RSA que se utilizan comúnmente.

El uso de este sistema criptográfico no está extendido y, de hecho, de los 202 Prestadores Cualificados de Servicios de Confianza Electrónicos de la Unión Europea solamente 20 utilizan ECC y solo 9 emiten certificados de Sello de Entidad. Por tanto, hay muy pocas CAs con la experiencia de implementar la Criptografía de Curva Elíptica en todo el continente.

España, pionera en la implantación del Pasaporte COVID

Ante esta situación, la Administración española (Ministerio de Sanidad, las consejerías de Sanidad de las CCAA y otros organismos públicos) ha sido pionera en el proceso de elaboración de los Pasaportes COVID que han conseguido ponerlo en marcha en un tiempo récord. ¿Por qué? ¿Qué han hecho diferente a otras autoridades sanitarias?

Ante la especificación obsoleta de montar desde cero una CSCA, la mayoría de las Administraciones decidieron contratar el servicio de emisión de certificados electrónicos a un Prestador Cualificado de Servicios de Confianza español: EADTrust, European Agency of Digital Trust.

EADTrust es el único prestador español que emite certificados cualificados de Sello de Entidad con Criptografía de Curva Elíptica y lleva años recomendando su uso debido a su robustez frente a vulnerabilidades como ROCA, que afectó a numerosos prestadores europeos en el año 2017. Emite, además, los certificados con más seguridad del mercado con ECC 384 bits y RSA 8192 bits.

Por ello, las Administraciones han decidido utilizar su Autoridad de Certificación para firmar los datos incluidos en los Pasaportes COVID. Además, otra ventaja respecto a otros países europeos es que los certificados que se están utilizando son Cualificados, es decir, están emitidos de acuerdo con el Reglamento eIDAS que regula los servicios de confianza en la Unión Europea.

Como las especificaciones técnicas se basan en las del pasaporte convencional establecidas por la ICAO, no se incluyó nada relativo al uso de certificados cualificados. Sin embargo, España decidió apostar por utilizar una CA Subordinada publicada en la Lista de Confianza Europea como Root de su PKI.

Al ser el primer país en emitir los certificados, gracias al esfuerzo conjunto de las Administraciones se pudo comprobar que el uso de la tecnología eIDAS de EADTrust es compatible con la PKI diseñada por la ICAO hace dos décadas.

En definitiva, España ha decidido apostar por la experiencia de un Prestador Cualificado que lleva años trabajando con Criptografía de Curva Elíptica para avalar la calidad del servicio y eficiencia en los procesos y conseguir la puesta en marcha del Pasaporte COVID en un tiempo récord. Los ciudadanos que obtengan su certificado cuentan con un nivel de seguridad alto en la protección de sus datos personales, garantizando la autenticidad de los mismos.

Acerca de EAD TRUST

EADTrust es un Prestador Cualificado de Servicios de Confianza que lleva más de diez años

trabajando para ayudar a las empresas a adaptarse a los desafíos de la digitalización, dotándolas de herramientas que garanticen la seguridad, la autenticidad, la integridad y la legalidad de sus procesos.

Sus principales servicios son:

Emisión de certificados cualificados para firma electrónica de persona física y de persona física representante de persona jurídica y de certificados cualificados para sello electrónico de persona jurídica.

Emisión de sellos de tiempo cualificados

Notificación electrónica fehaciente (e-mail certificado)

Comprobación electrónica fehaciente de publicaciones en página web (Publicación fehaciente), especialmente relacionados con juntas de accionistas y otros actos societarios.

Foro Electrónico de Accionistas

Voto Electrónico

Auditoría de digitalización certificada y firma manuscrita digitalizada avanzada

Consultoría

EADTrust, European Agency of Digital Trust, S.L. es una entidad especializada en resolver los retos de la digitalización dando soluciones a las necesidades de las empresas que se plantean cambiar procesos manuales por otros digitales. La combinación de conocimientos legales y técnicos de sus especialistas no dejan cabos sueltos a la hora de responder sobre la legalidad de las soluciones desarrolladas. Desde 2020 presta servicios de confianza digital cualificados según se definen en el Reglamento europeo EIDAS, de aplicación directa en todos los países europeos. Sus certificados basados en Criptografía de Curva Elíptica los emplean varios Ministerios y todas las comunidades autónomas para la emisión de los certificados COVID digitales.

Para más información sobre la empresa, visitar la página www.eadtrust.eu y www.certificados.de

Datos de contacto:

Beatriz de la Villa

917160555

Nota de prensa publicada en: [Madrid](#)

Categorías: [Internacional](#) [Medicina](#) [Sociedad](#) [General](#) [Digital](#) [Seguridad](#)

NotasdePrensa

<https://www.notasdeprensa.es>