

Título	El papel de la Oficina Permanente en la certificación digital
Documento	Doc. Prel. N.º 9 de septiembre de 2021
Autor	Oficina Permanente
Punto de la agenda	Punto 9.ii.
Mandato(s)	Grupo de Expertos sobre el e-APP y las nuevas tecnologías
Objetivo	Exponer posibles formas de estandarizar la certificación digital en el contexto del e-APP y el papel de la OP en la facilitación de este proceso.
Medida que debe adoptarse	Decisión <input type="checkbox"/> Aprobación <input type="checkbox"/> Para debate <input checked="" type="checkbox"/> Acción / finalización <input type="checkbox"/> Para información <input type="checkbox"/>
Anexos	No constan
Documentos relacionados	No constan

Índice

I.	Introducción.....	1
II.	Los certificados digitales y el e-APP	1
III.	Autoridad de certificación específica	2
IV.	Propuesta para la Comisión Especial.....	3

El papel de la Oficina Permanente en la certificación digital

I. Introducción

- 1 La emisión de una e-Apostilla requiere el uso de un certificado digital para validar la firma, de forma que los certificados digitales constituyen una parte esencial del e-APP. Como en todo lo referente al e-APP, las Partes contratantes gozan de plena discreción para determinar la infraestructura de los certificados digitales que utilicen sus Autoridades Competentes. Sin embargo, la gran variedad de certificados digitales que utilizan las Partes contratantes ha dado lugar a malentendidos en la práctica y, en algunos casos, a que las e-Apostillas sean rechazadas.
- 2 El Grupo de Expertos sobre el e-APP y las nuevas tecnologías, que se reunió en mayo de 2021, debatió las posibilidades de estandarizar la emisión y verificación de e-Apostillas. Entre otras cosas, consideró la posibilidad de establecer normas de certificación digital y de evaluar y acreditar las soluciones del e-APP de proveedores comerciales. Aunque el Grupo llegó a la conclusión de que llevar a cabo una armonización absoluta no es ni necesario ni deseable, reconoció que puede hacer falta seguir debatiendo sobre las normas internacionales, la concesión de licencias y la acreditación de terceros¹.
- 3 El objetivo sería aumentar la aceptación del e-APP apoyando a las Partes contratantes en la implementación del componente de la e-Apostilla. En concreto, ayudaría a las Partes contratantes que no disponen de los recursos o el tiempo para establecer una infraestructura interna. Si más Partes contratantes emiten e-Apostillas, esto también aumentaría su aceptación. Dependiendo del modelo que se elija, también puede haber un elemento de generación de ingresos.
- 4 En este contexto, en el presente documento se estudia la posible estandarización de los certificados digitales en el marco del e-APP y el papel que podría desempeñar la OP para facilitar este proceso.

II. Los certificados digitales y el e-APP

- 5 Los certificados digitales son emitidos por autoridades de certificación, que pueden ser públicas o privadas, utilizando una infraestructura de clave pública. El carácter público o privado de una autoridad de certificación depende de la medida en que otras entidades confíen en sus certificados y no de si la propia autoridad de certificación es pública o privada. Los certificados de autoridades de certificación públicas (por ejemplo, IdenTrust, DigiCert y GlobalSign) gozan de "confianza pública" y pueden utilizarse ampliamente, ya que son reconocidos por los principales navegadores, aplicaciones y dispositivos². En cambio, los certificados de autoridades de certificación privadas están diseñados para ser utilizados dentro de un grupo de usuarios o dispositivos autorizados (por ejemplo, dentro de una empresa u organización) y pueden dar lugar a errores o advertencias si se utilizan fuera de ese grupo. Dada la finalidad del Convenio sobre la Apostilla y los numerosos usos de las (e-)Apostillas, los certificados digitales que gozan de confianza pública son los más apropiados para el e-APP.
- 6 En algunas estructuras de certificación, existe una jerarquía entre las distintas autoridades de certificación. La autoridad de certificación "raíz" o "ancla" está en el nivel más alto, seguida de una autoridad de certificación "subordinada" o "intermedia" para determinar los permisos en otros niveles, y luego la autoridad de certificación "emisora" en el nivel más bajo, responsable de la emisión efectiva del certificado digital. En esta jerarquía, el hecho de que un certificado digital goce

¹ Véase el Doc. Prel. N.º 6 de mayo de 2021, "Informe de la presidencia del Grupo de Expertos sobre el e-APP y las nuevas tecnologías", Anexo I, párr. 12.

² Véanse, p. ej., los miembros actuales de la lista de confianza aprobada por Adobe (*Adobe Approved Trust List (AATL)*), disponible en el sitio: < <https://helpx.adobe.com/acrobat/kb/approved-trust-list1.html> >.

de confianza pública o privada viene determinado por el hecho de que la autoridad de certificación raíz sea pública o privada.

- 7 Cuando una solución comercial de una autoridad de certificación pública no se considere apropiada —por ejemplo, por razones de política o de seguridad— se puede crear una autoridad de certificación raíz diseñada al efecto. Sin embargo, los costos de desarrollo, mantenimiento y seguridad pueden ser considerables, y no hay garantía de que los certificados puedan alcanzar el mismo nivel de confianza pública del que gozan las autoridades de certificación que ya existen. Esto puede generar dificultades para los usuarios y, en el contexto del e-APP, aumentar el riesgo de que las e-Apostillas que se basan en estos certificados digitales sean rechazadas.
- 8 Para superar esta dificultad, algunas autoridades públicas de certificación ofrecen servicios de *hosting* o alojamiento web, que permiten a las organizaciones gestionar sus propios certificados como autoridades de certificación subordinadas (intermedias). Esto permite a las organizaciones ejercer un control total sobre la emisión de certificados digitales sin el costo de establecer su propia autoridad de certificación raíz. De esta manera, los certificados digitales de las organizaciones gozan de la confianza casi universal de las autoridades de certificación públicas.

III. Autoridad de certificación específica

- 9 Establecer una autoridad de certificación específica podría estandarizar la certificación digital en el marco del e-APP. Proporcionar certificados digitales estandarizados a las Autoridades Competentes reforzaría la confianza entre las Partes contratantes y facilitaría la circulación, verificación y aceptación de las e-Apostillas. También ayudaría a las Partes contratantes que aún no han implementado el componente de la e-Apostilla³, ya que el e-APP podría implementarse más rápidamente al no ser necesario para las Partes contratantes establecer una infraestructura de certificación digital interna. Asimismo, podría resultar más económico para las Autoridades Competentes que, de otro modo, habrían recurrido independientemente a soluciones de proveedores comerciales⁴.
- 10 Reconociendo la importancia de la flexibilidad en la implementación, la solución de certificación digital sería opcional y no afectaría a las Partes contratantes que utilicen o desarrollen sus propias soluciones de certificación digital para las e-Apostillas. Además, el hecho de que una e-Apostilla utilice un certificado digital distinto del certificado estandarizado no sería un motivo válido de rechazo.
- 11 Si las Partes contratantes apoyan la creación de una autoridad de certificación específica, es importante que este trabajo se coordine de forma centralizada y con la participación de las Autoridades Competentes. La OP sería la mejor situada para gestionar este proceso, velando por que todas las Partes contratantes actuales y futuras puedan beneficiarse de las infraestructuras que se desarrollen.
- 12 Reconociendo que su papel de secretaría es delicado y que carece de conocimientos técnicos, la OP no desarrollaría ni gestionaría su propia autoridad de certificación interna. En su lugar, teniendo en cuenta las estructuras descritas anteriormente y la necesidad de que los certificados sean aceptados lo más ampliamente posible, el modelo más conveniente y que requiere menos recursos sería que la OP funcione como autoridad de certificación subordinada, alojada en una autoridad

³ Aproximadamente el 20% de las Partes contratantes han implementado el componente de la e-Apostilla del e-APP. Por lo tanto, la mayoría de las Partes contratantes podrían beneficiarse de una infraestructura de certificados digitales fácilmente disponible. Véase el "Cuadro de implementación del e-APP" en la Sección Apostillas del sitio web de la HCCH: < www.hcch.net >.

⁴ Según las tendencias actuales, un número importante de Partes contratantes recurriría a soluciones comerciales. De acuerdo con las respuestas al Cuestionario de 2021 sobre la Apostilla, de las Partes contratantes que actualmente emiten e-Apostillas, aproximadamente el 40% utiliza tecnología de proveedores comerciales. Véase el Doc. Prel. N.º 2 de agosto de 2021, "Resumen de respuestas al Cuestionario de 2021 sobre la Apostilla", párr. 48 y sig.

de certificación raíz pública (como se describe en el párrafo 8). Todas las Partes contratantes interesadas podrían entonces obtener, de la OP, las credenciales necesarias para sus Autoridades Competentes, y emitir e-Apostillas utilizando los certificados digitales de confianza pública diseñados específicamente para su uso en el marco del e-APP.

- 13 A fin de centrar el debate en si la propuesta resulta o no conveniente, por el momento, la OP no ha especificado qué tecnologías deberían utilizarse, ni ha indicado los posibles costos asociados a estos trabajos. Si la propuesta recibe apoyo, la OP estudiaría más a fondo las opciones que se pueden adoptar. Se prevé que la solución que se desarrolle a estos efectos sea adecuada para su utilización en todas las Partes contratantes interesadas, y que incorpore un mecanismo para posiblemente generar ingresos, por ejemplo, para recuperar los costos asociados con el desarrollo y el mantenimiento.

IV. Propuesta para la Comisión Especial

- 14 Se invita a la Comisión Especial a considerar si es conveniente establecer una autoridad de certificación específica para el e-APP y, en caso afirmativo, recomendar que la OP presente una propuesta al CAGP para su consideración.