



Preguntas frecuentes sobre firmas digitales



Alvaro Cuno

Gerencia de Registros de Certificación Digital

Sub Gerencia de Certificación e Identidad Digital

**REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL
RENIEC**

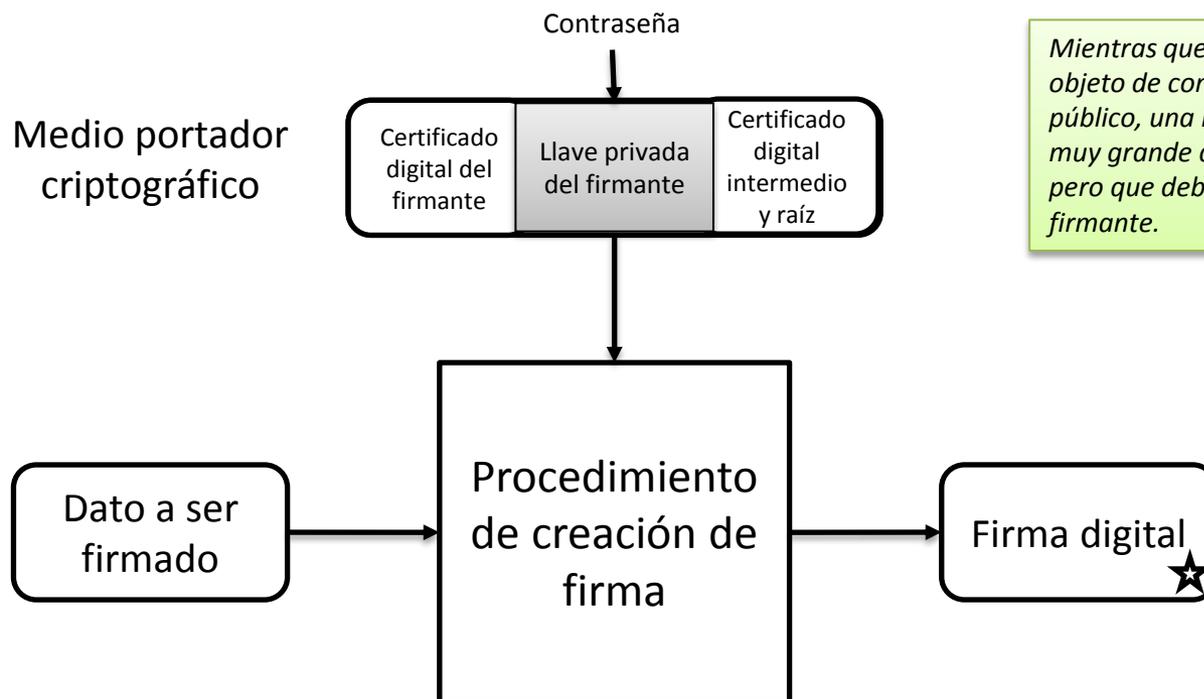
1. ¿El RENIEC entrega firmas digitales?

1. ¿El RENIEC entrega firmas digitales?



1. ¿El RENIEC entrega firmas digitales?

No. El RENIEC entrega certificados digitales a nombre del firmante.

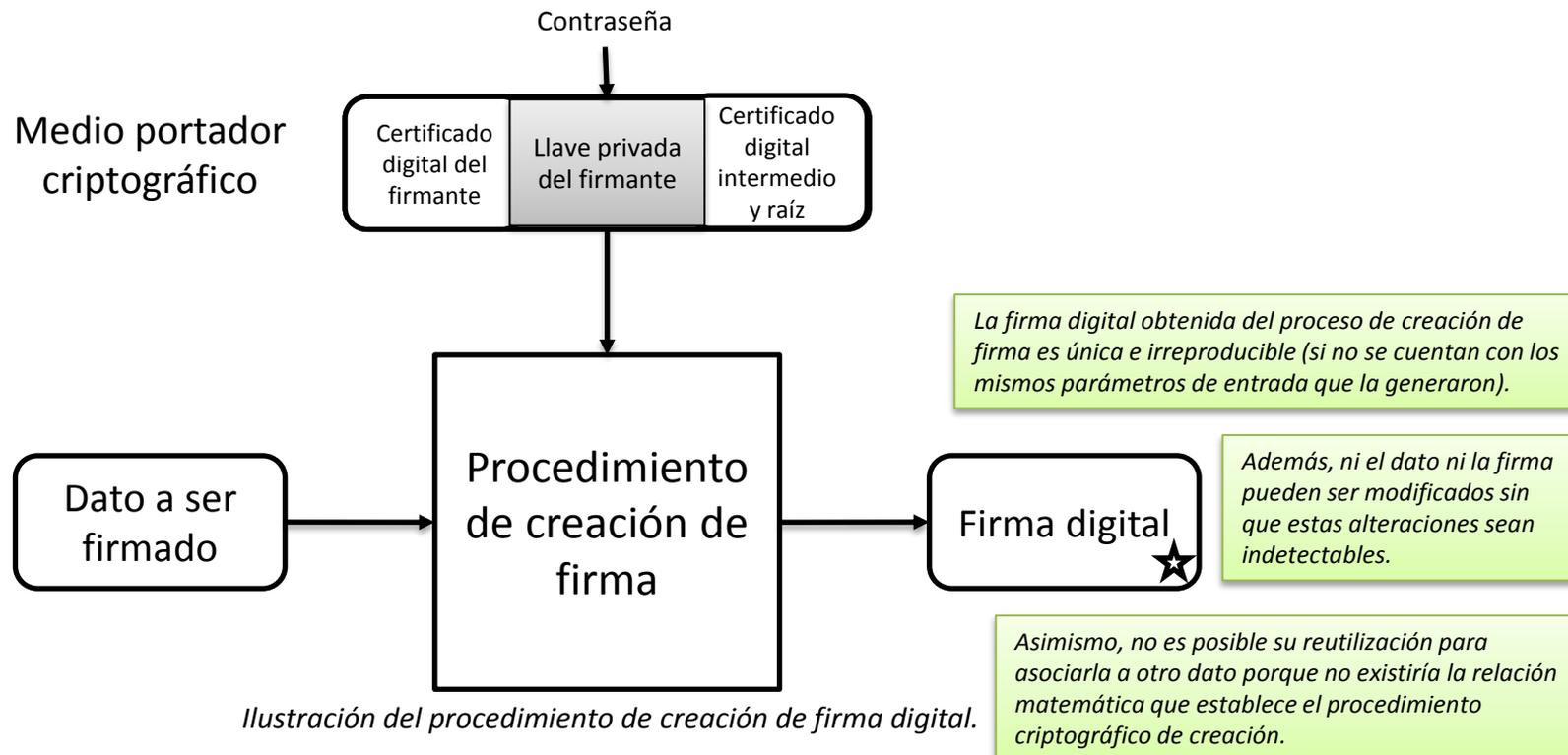


Mientras que el certificado digital es un objeto de conocimiento, posesión y uso público, una llave privada es un número muy grande que es desconocido por todos pero que debe estar en control exclusivo del firmante.

Ilustración del procedimiento de creación de firma digital.

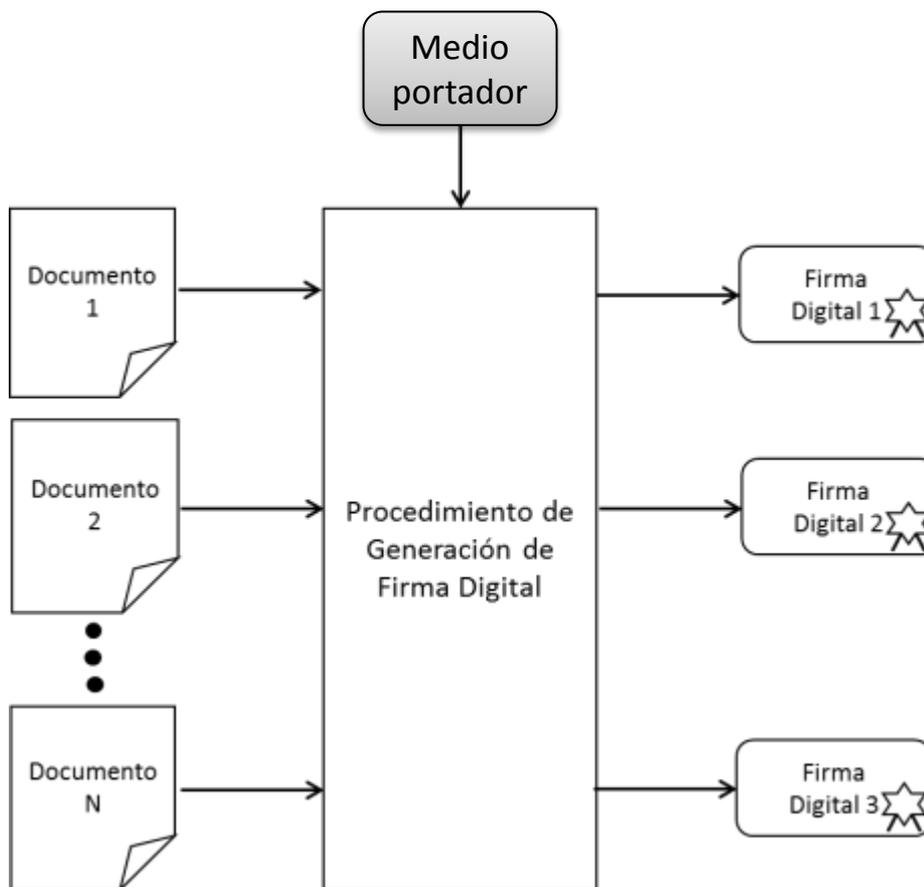
1. ¿El RENIEC entrega firmas digitales?

No. El RENIEC entrega **certificados digitales** a nombre del firmante.



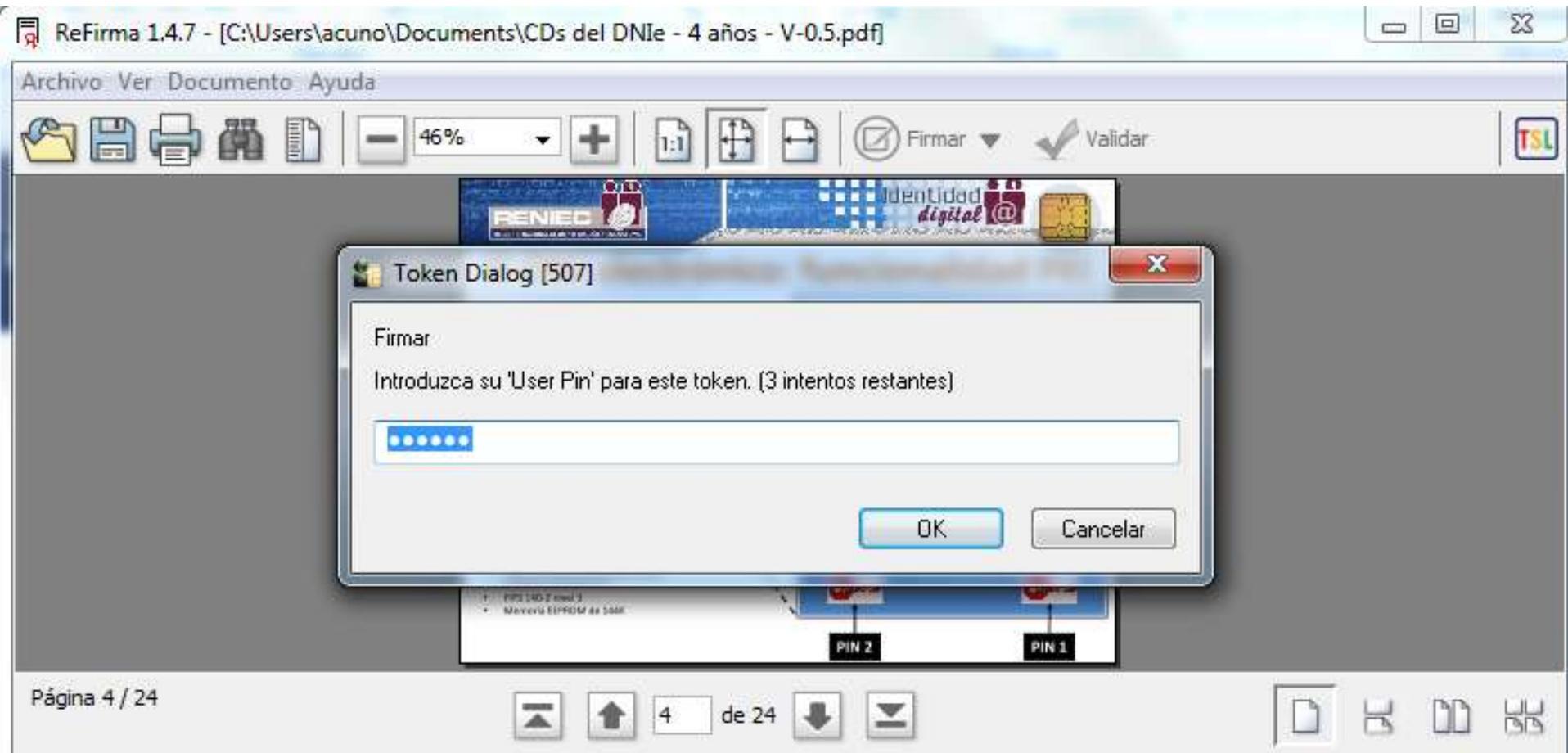
1. ¿El RENIEC entrega firmas digitales?

Ilustración de las múltiples y diferentes firmas digitales que puede crear un mismo firmante usando un único dispositivo seguro.



A diferencia de una firma manuscrita que suele ser un patrón único, posible de ser generado solamente por el firmante (independiente del dato firmado y del instante de la firma), una firma digital siempre será diferente para cada momento y para cada dato firmado.

2. ¿La “clave” que se solicita al momento de firmar es la “clave privada”?



2. ¿La “clave” que se solicita al momento de firmar es la “clave privada”?



2. ¿La “clave” que se solicita al momento de firmar es la “clave privada”?

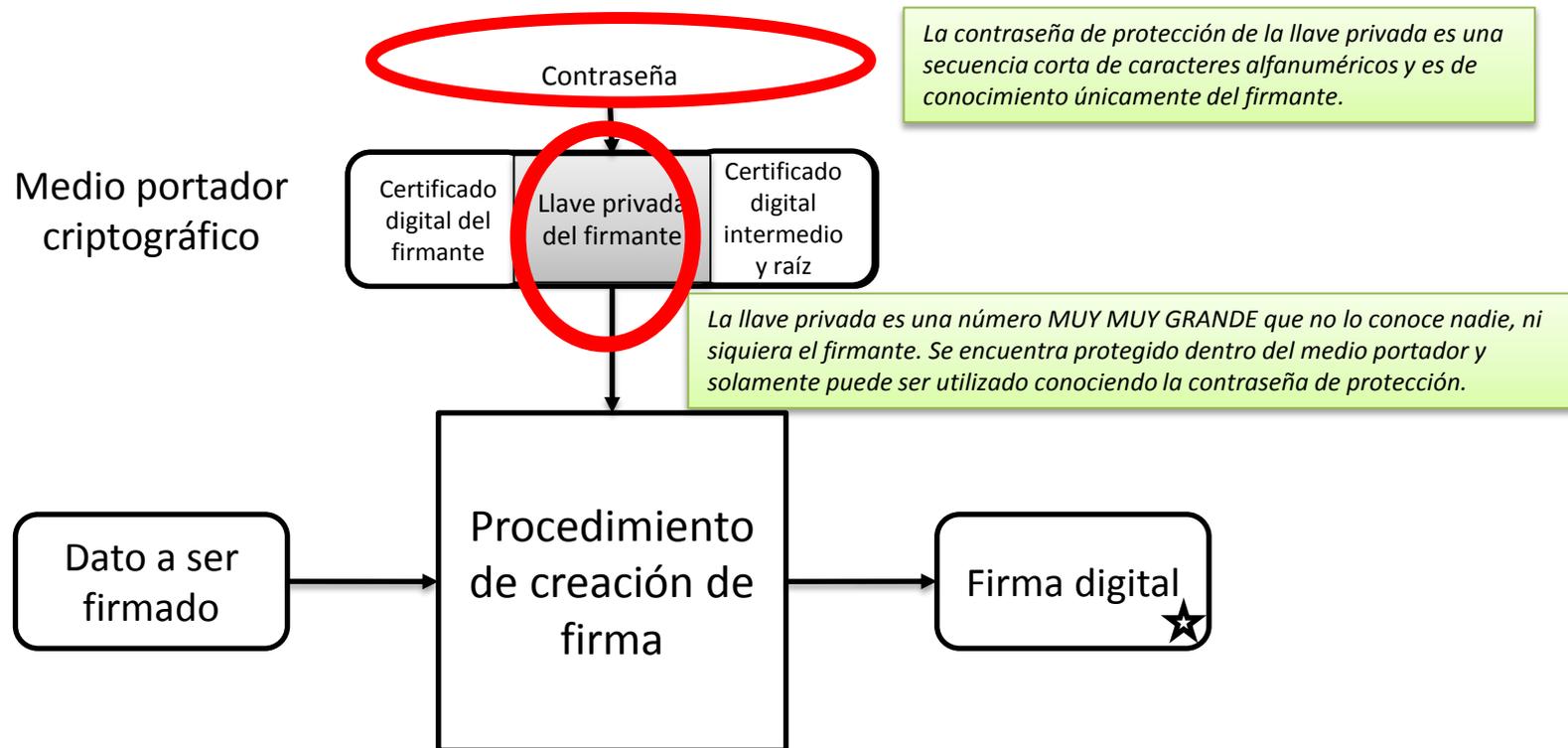


Ilustración del procedimiento de creación de firma digital.

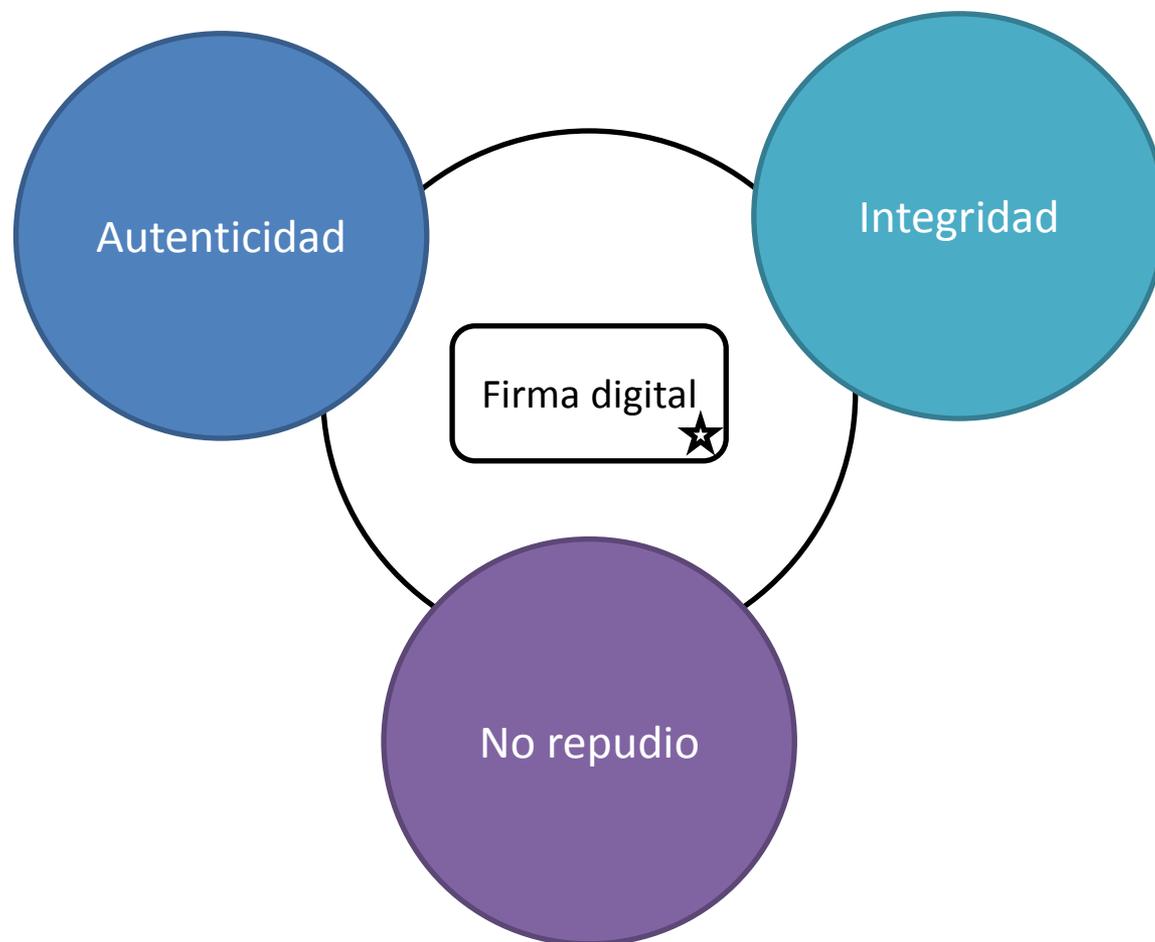
3. ¿Una firma digital garantiza la
confidencialidad?

3. ¿Una firma digital garantiza la confidencialidad?

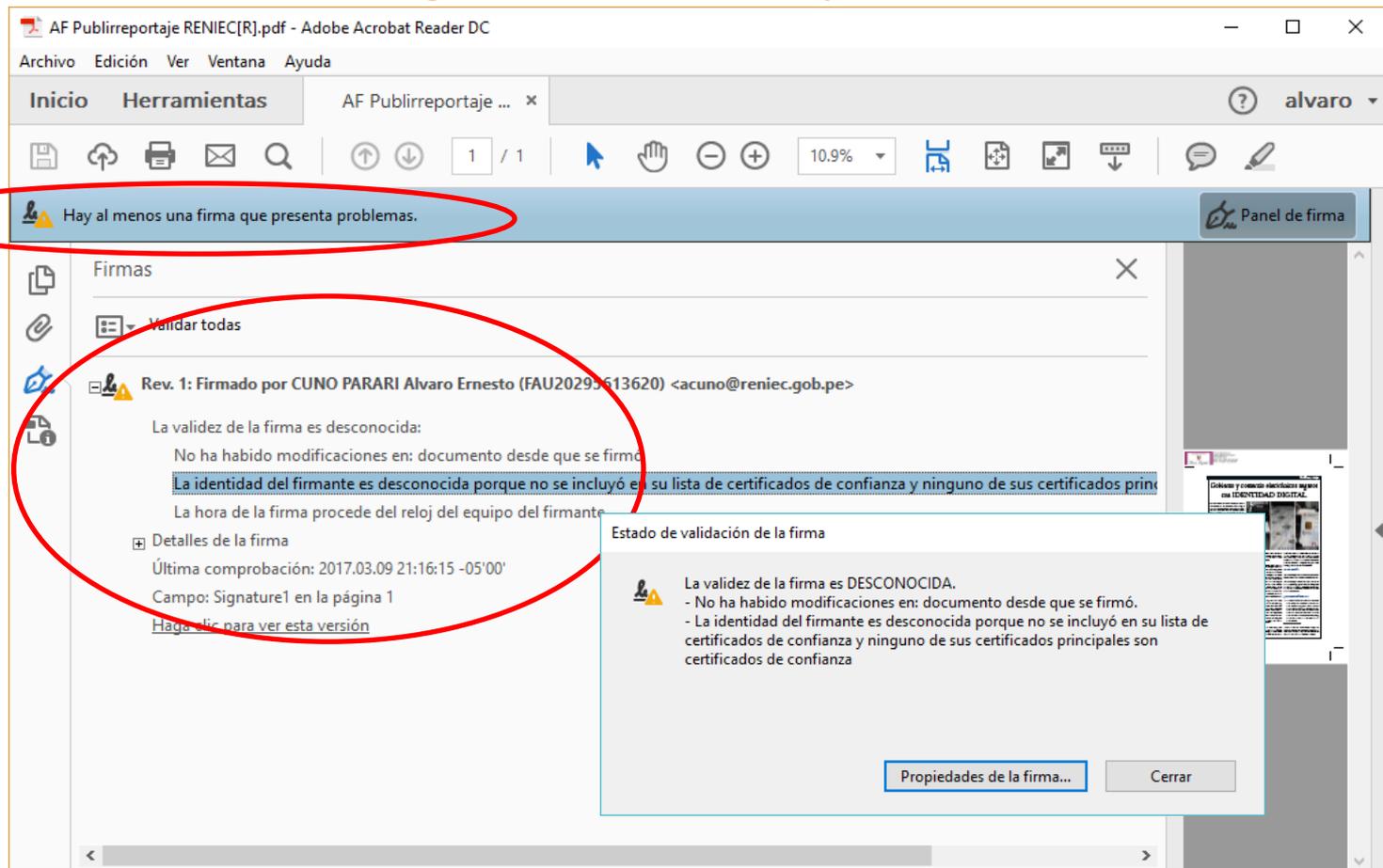


3. ¿Una firma digital garantiza la confidencialidad?

No. Una firma digital garantiza: autenticidad, integridad y no repudio



4. ¿Porqué el software acrobat reader no reconoce como válida la firma digital generada con un certificado digital emitido por el RENIEC?



4. ¿Porqué el software acrobat reader no reconoce como válida la firma digital generada con un certificado digital emitido por el RENIEC?

Es porque el software acrobat reader no es un producto que forma parte de la IOFE. La lista de sw acreditados puede verse aquí:

<https://www.indecopi.gob.pe/web/firmas-digitales/lista-de-servicios-de-confianza-trusted-services-list-tsl->

4. ¿Porqué el software acrobat reader no reconoce como válida la firma digital generada con un certificado digital emitido por el RENIEC?

Es porque el software acrobat reader no es un producto que forma parte de la IOFE. La lista de sw acreditados puede verse aquí:

<https://www.indecopi.gob.pe/web/firmas-digitales/lista-de-servicios-de-confianza-trusted-services-list-tsl->



Adobe
Approved
Trusted List
(AATL)

European
Union
Trusted Lists
(EUTL)

4. ¿Porqué el software acrobat reader no reconoce como válida la firma digital generada con un certificado digital emitido por el RENIEC?

Es porque el software acrobat reader no es un producto que forma parte de la IOFE. La lista de sw acreditados puede verse aquí:

<https://www.indecopi.gob.pe/web/firmas-digitales/lista-de-servicios-de-confianza-trusted-services-list-tsl->



Adobe Approved Trusted List (AATL)
European Union Trusted Lists (EUTL)

Microsoft Trusted Root Certificate

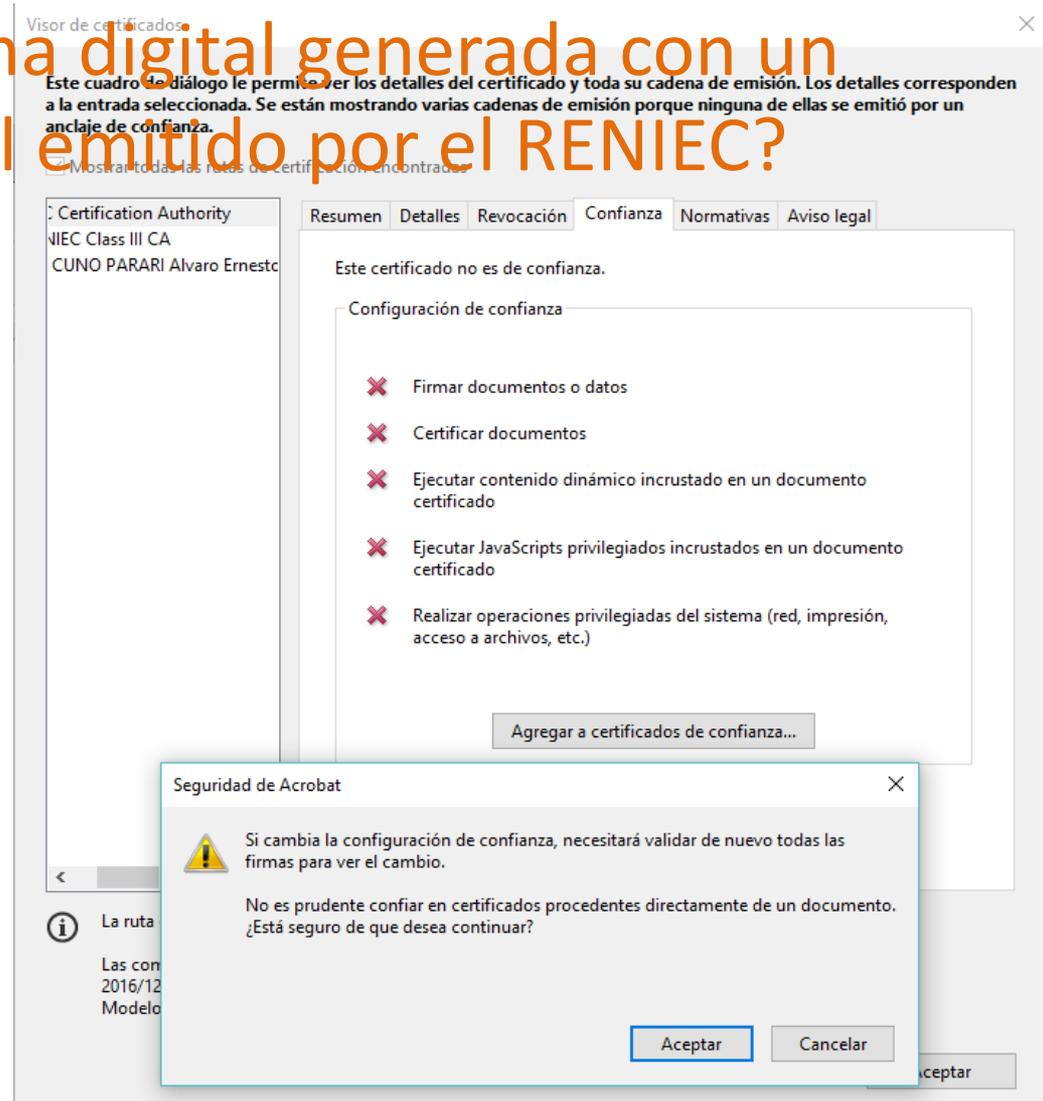
Apple Root Certificate program

Mozilla CA Certificate Policy

Oracle Java Root Certificate program

4. ¿Porqué el software acrobat reader no reconoce como válida la firma digital generada con un certificado digital emitido por el RENIEC?

Los usuarios de acrobat reader puede agregar manualmente el certificado digital raíz de RENIEC en el repositorio local de confianza del aplicativo.



4. ¿Porqué el software acrobat reader no reconoce como válida la firma digital generada con un certificado digital emitido por el RENIEC?

The screenshot shows the Adobe Acrobat Reader interface. At the top, the title bar reads "AF Publiirreportaje RENIEC[R].pdf - Adobe Acrobat Reader DC". The menu bar includes "Archivo", "Edición", "Ver", "Ventana", and "Ayuda". The toolbar shows various icons for file operations and navigation. A status bar at the top indicates "Firmado y todas las firmas son válidas." (Signed and all signatures are valid), which is circled in red. Below this, a "Firmas" (Signatures) panel is open, displaying a signature entry: "Rev. 1: Firmado por CUNO PARARI Alvaro Ernesto (FAU20295613620) <acuno@reniec.gob.pe>". This entry is also circled in red. The details for this signature are as follows:

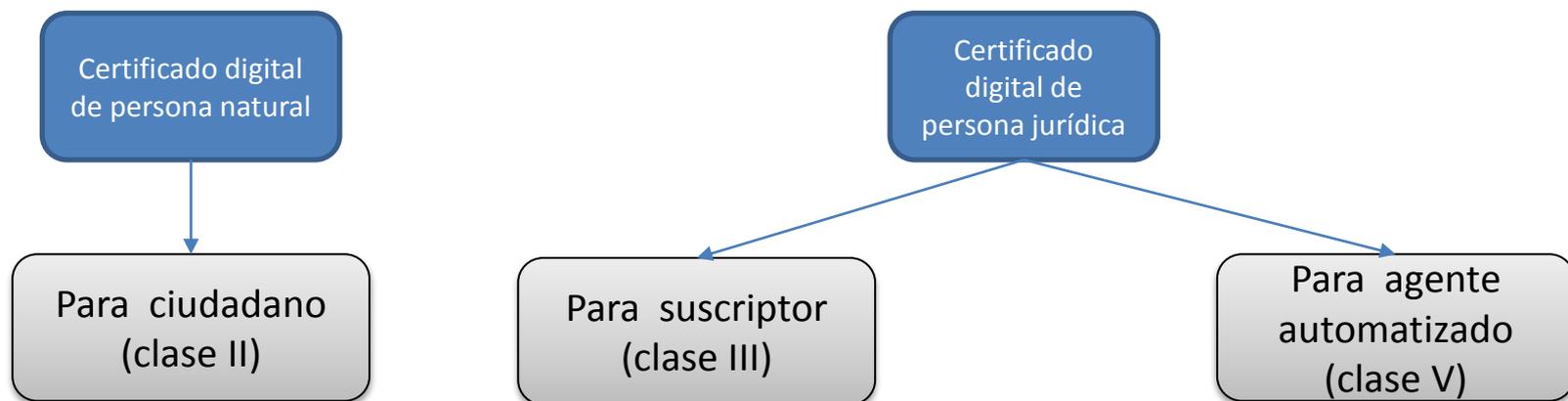
- La firma es válida:
- No ha habido modificaciones en: documento desde que se firmó
- La identidad del firmante es válida
- La hora de la firma procede del reloj del equipo del firmante.
- La firma no está activada para LTV y caducará después de 2017/11/28 14:42:31 -05'00'

Additional details shown include "Última comprobación: 2017.03.09 21:55:17 -05'00'", "Campo: Signature1 en la página 1", and "Haaa clic para ver esta versión". The background shows a document page with the heading "Gobierno y comercio electrónicos seguros con IDENTIDAD DIGITAL".

5. ¿Qué tipos de certificados digitales emite el RENIEC?

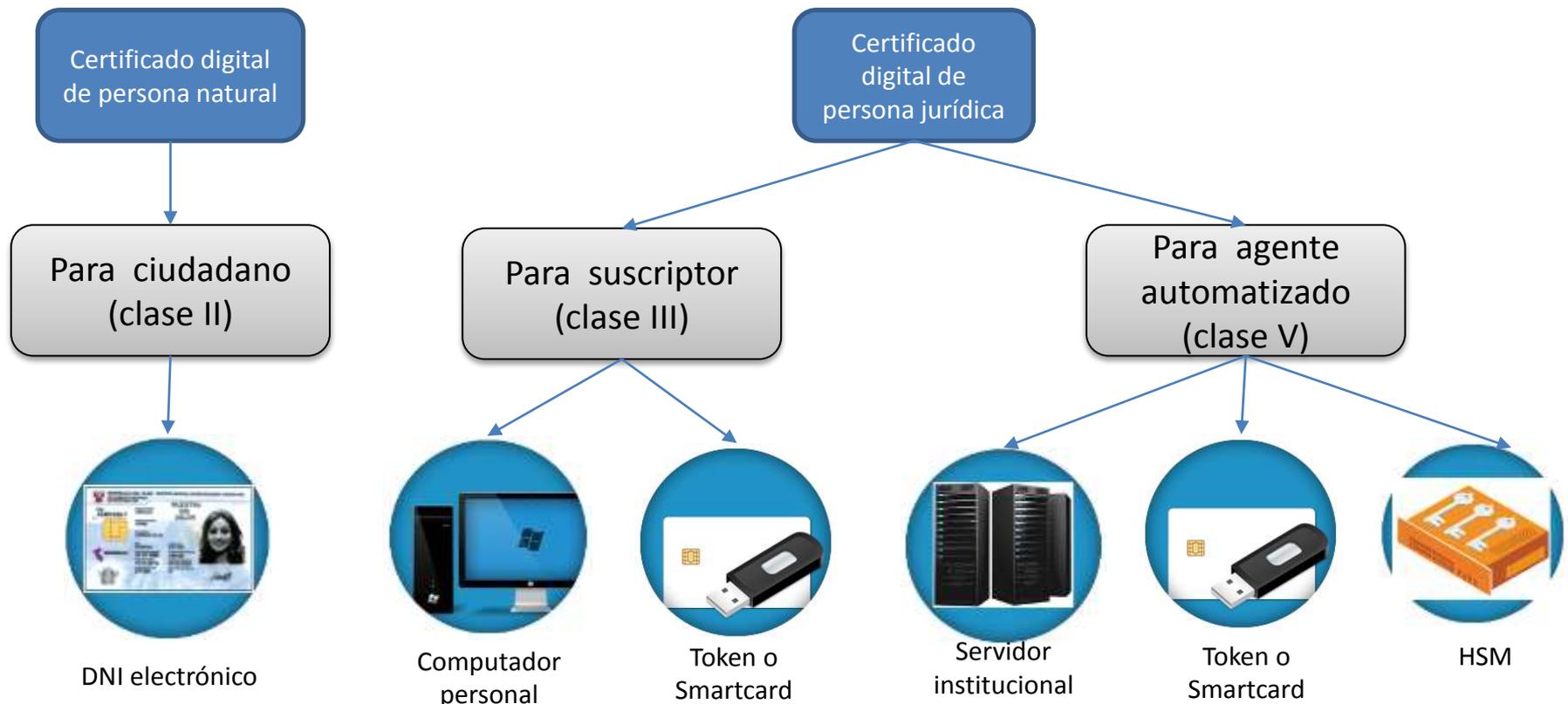
5. ¿Qué tipos de certificados digitales emite el RENIEC?

Actualmente, el RENIEC emite certificados digitales para: ciudadano, para suscriptor y para agente automatizado



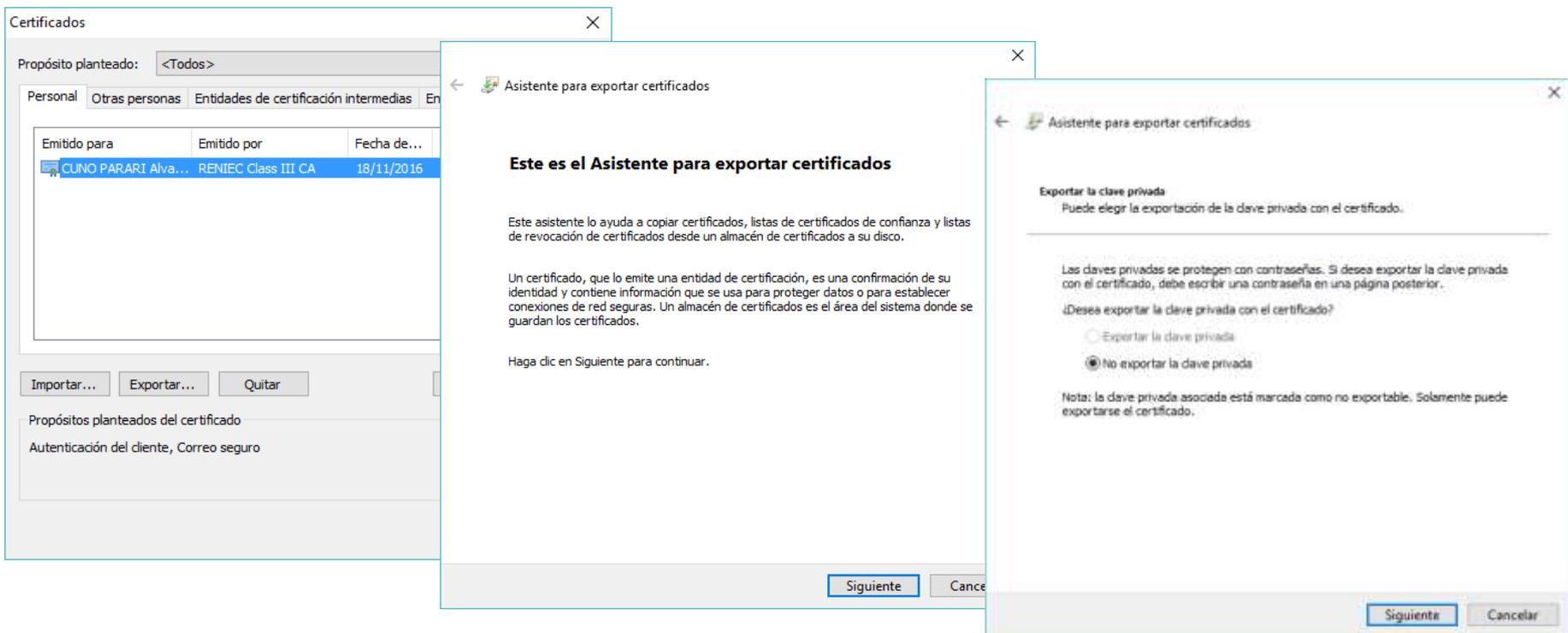
5. ¿Qué tipos de certificados digitales emite el RENIEC?

Actualmente, el RENIEC emite certificados digitales para: ciudadano, para suscriptor y para agente automatizado



6. Mi certificado digital emitido por el RENIEC fue instalado en el repositorio del SO de mi PC, ¿por qué no puedo exportarlo?

Por tratarse de un objeto público, un certificado digital instalado en el repositorio del SO puede ser exportado sin ningún problema hacia un archivo .CER utilizando el asistente de MS Windows.



The image shows a sequence of three overlapping windows from the Windows operating system:

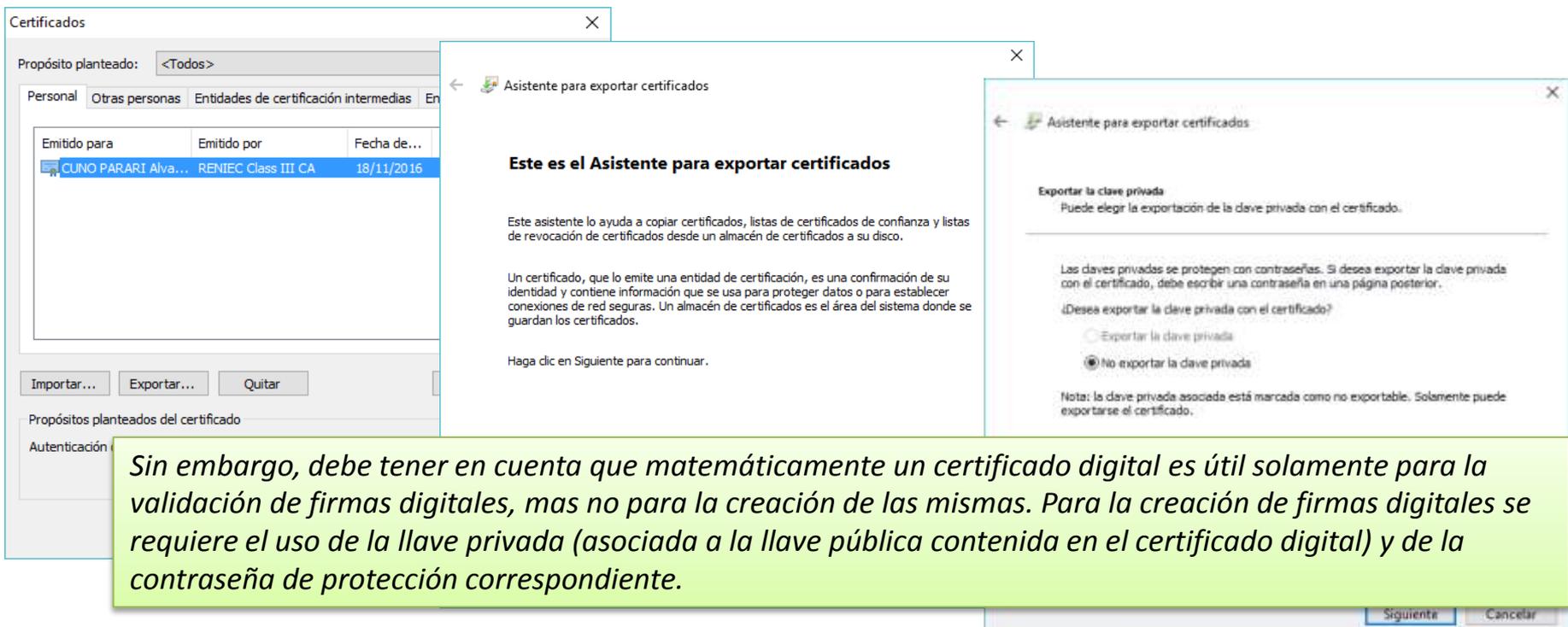
- Left Window (Certificados):** A window titled 'Certificados' showing a list of certificates. The selected certificate is:

Emitido para	Emitido por	Fecha de...
CUNO PARARI Alva...	RENIEC Class III CA	18/11/2016

 Below the list are buttons for 'Importar...', 'Exportar...', and 'Quitar'.
- Middle Window (Asistente para exportar certificados):** The first step of the wizard, titled 'Este es el Asistente para exportar certificados'. It explains that the assistant helps copy certificates and lists of certificates of trust and revocation. It also states that a certificate is a confirmation of identity and contains information used for secure connections. A 'Siguiente' button is visible at the bottom.
- Right Window (Asistente para exportar certificados):** The second step of the wizard, titled 'Exportar la clave privada'. It asks '¿Desea exportar la clave privada con el certificado?' and provides two radio button options:
 - Exportar la clave privada
 - No exportar la clave privada
 A note at the bottom states: 'Nota: la clave privada asociada está marcada como no exportable. Solamente puede exportarse el certificado.' 'Siguiente' and 'Cancelar' buttons are at the bottom.

6. Mi certificado digital emitido por el RENIEC fue instalado en el repositorio del SO de mi PC, ¿por qué no puedo exportarlo?

Por tratarse de un objeto público, un certificado digital instalado en el repositorio del SO puede ser exportado sin ningún problema hacia un archivo .CER utilizando el asistente de MS Windows.



The image shows two overlapping windows from the Windows operating system. The background window is the 'Certificados' (Certificates) control panel window, showing a list of certificates. The foreground window is the 'Asistente para exportar certificados' (Export Certificates Assistant) dialog box.

Certificados window:

- Propósito planteado: <Todos>
- Personal | Otras personas | Entidades de certificación intermedias | En...
- Table with columns: Emitido para, Emitido por, Fecha de...
- Row 1: CUNO PARARI Alva..., RENIEC Class III CA, 18/11/2016
- Buttons: Importar..., Exportar..., Quitar
- Propósitos planteados del certificado
- Autenticación

Asistente para exportar certificados window:

Este es el Asistente para exportar certificados

Este asistente lo ayuda a copiar certificados, listas de certificados de confianza y listas de revocación de certificados desde un almacén de certificados a su disco.

Un certificado, que lo emite una entidad de certificación, es una confirmación de su identidad y contiene información que se usa para proteger datos o para establecer conexiones de red seguras. Un almacén de certificados es el área del sistema donde se guardan los certificados.

Haga clic en Siguiente para continuar.

Exportar la clave privada
Puede elegir la exportación de la clave privada con el certificado.

Las claves privadas se protegen con contraseñas. Si desea exportar la clave privada con el certificado, debe escribir una contraseña en una página posterior.

¿Desea exportar la clave privada con el certificado?

Exportar la clave privada

No exportar la clave privada

Nota: la clave privada asociada está marcada como no exportable. Solamente puede exportarse el certificado.

Buttons: Siguiente, Cancelar

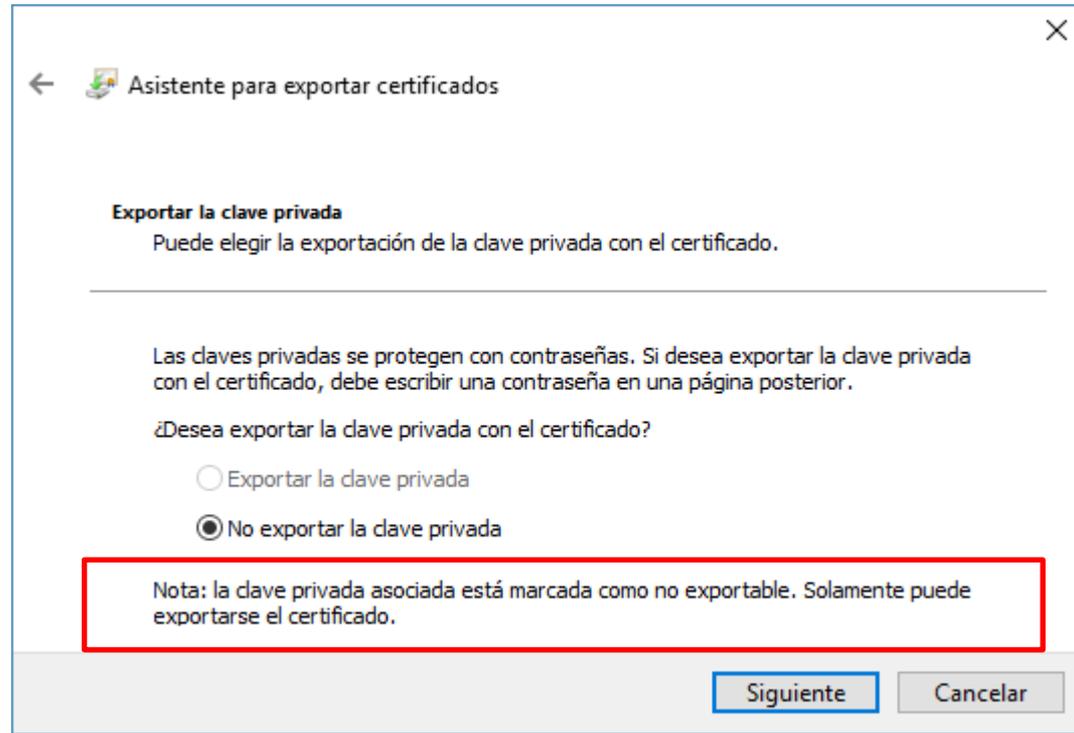
Sin embargo, debe tener en cuenta que matemáticamente un certificado digital es útil solamente para la validación de firmas digitales, mas no para la creación de las mismas. Para la creación de firmas digitales se requiere el uso de la llave privada (asociada a la llave pública contenida en el certificado digital) y de la contraseña de protección correspondiente.

7. Mi certificado digital fue instalado en el SO de mi PC, ¿por qué no puedo exportarlo a un fichero .PFX?

Un fichero .PFX es un contenedor de objetos criptográficos, protegido por una contraseña, que contiene usualmente un certificado digital y su llave privada asociada

Tal como fue mencionado en la pregunta anterior, no existe ningún impedimento técnico que impida exportar un certificado digital. Sin embargo, no sucede lo mismo cuando se trata de su llave privada asociada.

Si el certificado digital fue emitido por el RENIEC, entonces no es posible exportar su llave privada asociada, puesto que ésta ha sido generada de tal forma que no es posible su exportación por motivos de seguridad (**suplantación**).



← Asistente para exportar certificados

Exportar la clave privada
Puede elegir la exportación de la clave privada con el certificado.

Las claves privadas se protegen con contraseñas. Si desea exportar la clave privada con el certificado, debe escribir una contraseña en una página posterior.

¿Desea exportar la clave privada con el certificado?

Exportar la clave privada

No exportar la clave privada

Nota: la clave privada asociada está marcada como no exportable. Solamente puede exportarse el certificado.

Siguiete Cancelar

8. Debido a la naturaleza de mis labores requiero crear firmas digitales desde diferentes PCs ubicadas en diferentes lugares, ¿cómo puedo proceder?

Para los casos donde el usuario requiera crear firmas digitales desde diferentes computadores, se recomienda solicitar que su certificado digital sea instalado en un token o smartcard de su propiedad donde se generarán las respectivas llaves pública y privada. De esta manera podrá llevarlo consigo y utilizarlo para firmar digitalmente desde cualquier lugar.



8. Debido a la naturaleza de mis labores requiero crear firmas digitales desde diferentes PCs ubicadas en diferentes lugares, ¿cómo puedo proceder?

Para los casos donde el usuario requiera crear firmas digitales desde diferentes computadores, se recomienda solicitar que su certificado digital sea instalado en un token o smartcard de su propiedad donde se generarán las respectivas llaves pública y privada. De esta manera podrá llevarlo consigo y utilizarlo para firmar digitalmente desde cualquier lugar.



También es posible solicitar varios certificados para un mismo suscriptor. En este caso cada certificado sería instalado en un computador diferente.



8. Debido a la naturaleza de mis labores requiero crear firmas digitales desde diferentes PCs ubicadas en diferentes lugares, ¿cómo puedo proceder?

Para los casos donde el usuario requiera crear firmas digitales desde diferentes computadores, se recomienda solicitar que su certificado digital sea instalado en un token o smartcard de su propiedad donde se generarán las respectivas llaves pública y privada. De esta manera podrá llevarlo consigo y utilizarlo para firmar digitalmente desde cualquier lugar.



También es posible solicitar varios certificados para un mismo suscriptor. En este caso cada certificado sería instalado en un computador diferente.

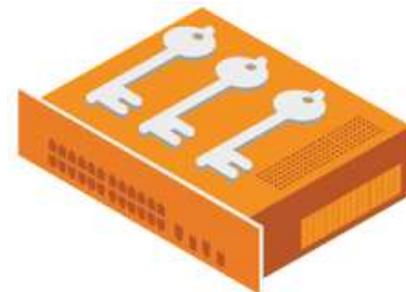
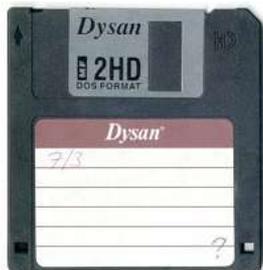


También es posible optar por usar su DNI electrónico.



9. Una persona nos ha sugerido almacenar los certificados digitales de los suscriptores de mi organización en un servidor HSM para que desde allí puedan firmar digitalmente, ¿es posible hacer eso?

Tal como fue mencionado anteriormente, al tratarse de objetos públicos, no existe ningún impedimento técnico para almacenar certificados digitales en cualquier repositorio, inclusive en un Diskette o CD-ROM o HSM.



Asimismo, tal como fue mencionado anteriormente, los certificados digitales almacenados en el Diskette o CD-ROM o HSM no son de utilidad para crear firmas digitales, sino únicamente para su validación.

10. ¿Es posible almacenar los certificados digitales (junto con sus llaves privadas asociadas) de los suscriptores de mi organización en un servidor HSM para que desde allí puedan firmar digitalmente?

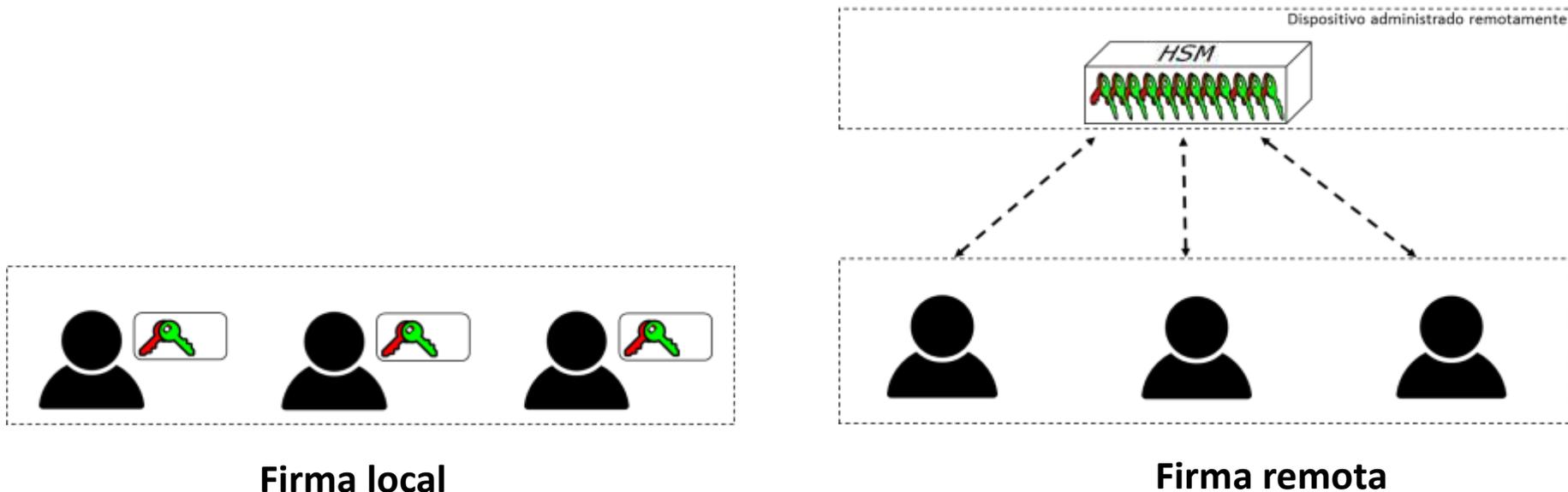
Técnicamente, y bajo algunas condiciones, podría ser posible almacenar certificados digitales y sus llaves privadas asociadas en un servidor HSM y utilizarlos para crear firmas digitales.

Sin embargo, debido a que la Ley de Firmas y Certificados Digitales, su Reglamento y sus Guías de Acreditación no contemplan esta modalidad de firma, estas firmas digitales no estarían siendo generadas bajo el marco de la IOFE por lo que carecerían de la equivalencia funcional y jurídica con las firmas manuscritas, y del valor probatorio que la normatividad les confiere.

11. ¿Qué es la firma digital remota?

11. ¿Qué es la firma digital remota?

Es un modelo de creación de firmas que contempla que las llaves privadas de los firmantes se encuentren almacenadas centralizadamente en un dispositivo criptográfico HSM que es gestionado remotamente (on-cloud or on-premise).



¡Gracias por la atención!



Preguntas frecuentes sobre firmas digitales

Alvaro Cuno

Gerencia de Registros de Certificación Digital

Sub Gerencia de Certificación e Identidad Digital

**REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL
RENIEC**