INFRAESTRUCTURA PKI
FIRMA DIGITAL PARA PROFESIONALES

Ing. Fernando Villares – C.I.E. 2019

NORMATIVA VIGENTE

- Ley N° 25.506 de Firma Digital. Reconoce y establece las condiciones para el empleo de la firma electrónica y de la firma digital y su eficacia jurídica, y crea la Infraestructura de Firma Digital de la República Argentina.
- Ley Nº 27.446 LEY DE SIMPLIFICACIÓN Y DESBUROCRATIZACIÓN DE LA ADMINISTRACIÓN PÚBLICA NACIONAL (CAPÍTULO I: Firma digital. Gestión documental electrónica). Actualización de la Ley 25.506.
- Decreto Nº 182/19 **Reglamentación de la Ley N° 25.506 de Firma Digital.** Deroga los Decretos 2628/2002, 283/2003 y 724/2006 y los artículos 8°, 9° y 10 del Decreto N° 561/2016. ANEXO
- Decreto Nº 892/17: **PLATAFORMA DE FIRMA DIGITAL REMOTA.**
- Resolución MM Nº 399-E/16 **Reemplaza la Decisión Administrativa Nº 927/2014 y la Disposición SSTG Nº 7/2015.** Establece los procedimientos y condiciones que se deberán cumplir para emitir certificados digitales en el ámbito de la Infraestructura de Firma Digital de la República Argentina.
- Resolución SGP N° 63/07 - Política de Certificación de la AUTORIDAD CERTIFICANTE RAÍZ de la REPÚBLICA ARGENTINA (ACR-RA).
- Resolución SMA Nº 37-E/16 - Política de Certificación de la AUTORIDAD CERTIFICANTE RAÍZ de la REPÚBLICA ARGENTINA v2.0. Resolución SMA Nº 116-E/17 Exigencia a certificadores licenciados y sus autoridades de registro. Captura de fotografía digital del rostro y la huella dactilar de los solicitantes y suscriptores de certificados de firma digital.
- Resolución SMA Nº 63/18 Homologa los dispositivos de creación de firma digital por hardware y los dispositivos de creación de firma utilizados por la Plataforma de Firma Digital Remota, para la creación de firmas digitales de personas.

Firma Digital

Una **firma digital** es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente identificar a la entidad originadora de dicho mensaje (autenticación de origen y no repudio), y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador (integridad).

Firma electrónica

La **firma electrónica** es un concepto jurídico, equivalente electrónico al de la firma manuscrita, donde una persona acepta el contenido de un mensaje electrónico a través de cualquier medio electrónico válido. Ejemplos:

- Usando una firma biométrica.
- Firma con un lápiz electrónico al usar una tarjeta de crédito o débito en una tienda.
- Marcando una casilla en una computadora, a máquina o aplicada con el ratón o con el dedo en una pantalla táctil.
- Usando una firma digital.
- Usando usuario y contraseña.
- Usando una tarjeta de coordenadas.

Firma digitalizada

La firma digitalizada es un tipo de firma que permite identificar al firmante en un documento electrónico incluyendo el aspecto gráfico de la firma manuscrita.

- Según legislación de firma electrónica y dependiendo de la técnica adoptada, puede ser considerada **firma electrónica simple**, o **firma electrónica avanzada**. En el marco de la firma electrónica simple se incluyen firmas escaneadas o digitalizadas, únicamente en su aspecto gráfico. En el marco de la firma electrónica avanzada se incluye además información grafométrica obtenida en tiempo real de un dispositivo idóneo asociado al sistema de firma vinculándolo con el documento de forma indisoluble, cifrando cierta información para que los datos de generación de firma no estén a disposición del promotor del sistema.

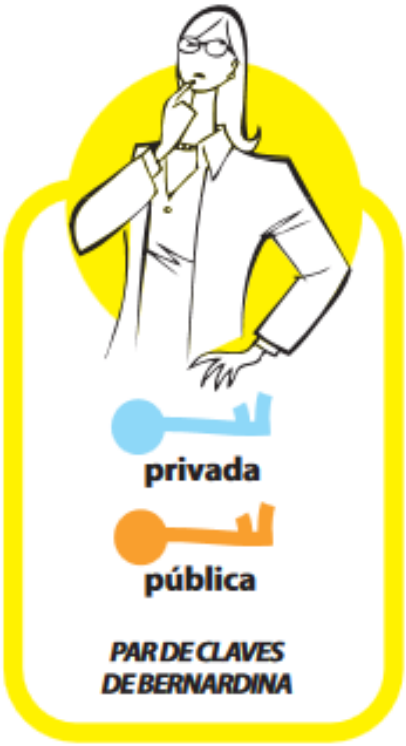
Entonces...Arquitectura PKI

CRIPTOGRAFÍA ASIMÉTRICA

Cifrado asimétrico

El cifrado asimétrico o de llave pública se basa en el concepto de un par de llaves (claves). Cada mitad del par (una llave) puede cifrar información que sólo la otra parte (la otra llave) podrá descifrar. Una parte del par de llaves, la llave privada, sólo es conocida para el propietario designado; la otra parte, la llave pública, se publica abiertamente, pero continúa asociada al propietario.

El cifrado asimétrico garantiza la confidencialidad, autenticidad y el no repudio.

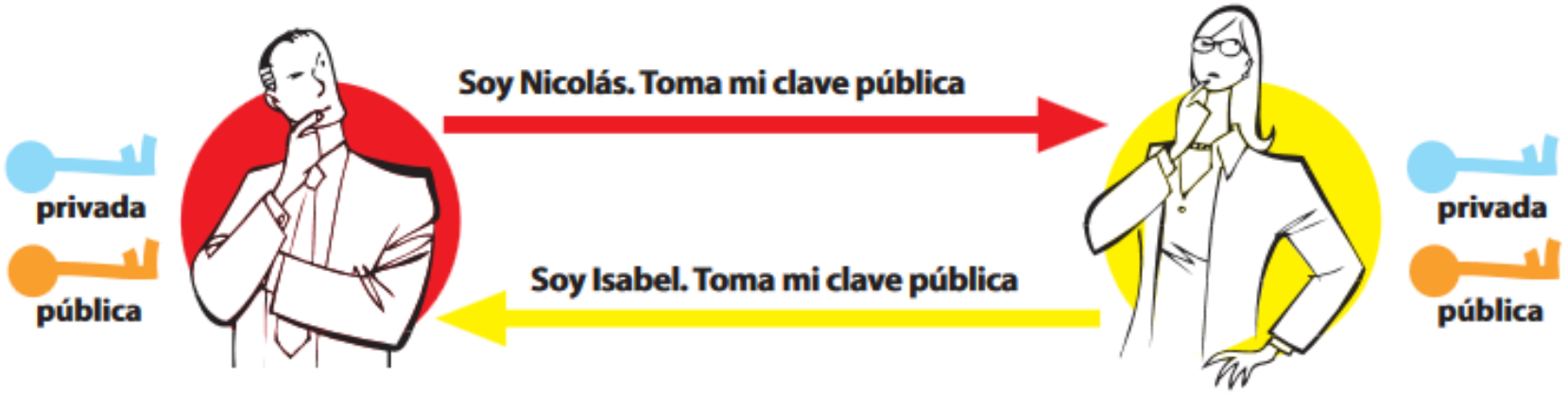


Entonces...Arquitectura PKI

CRIPTOGRAFÍA ASIMÉTRICA

PROCESO DE CIFRADO

Compartir clave públicas



Entonces...Arquitectura PKI

CRIPTOGRAFÍA ASIMÉTRICA

PROCESO DE CIFRADO

Entonces...Arquitectura PKI

CRIPTOGRAFÍA ASIMÉTRICA

PROCESO DE FIRMA ELECTRÓNICA

La firma digital permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación.

Información original en Icaro

Firma

0A 3F 15 12 D4

0A 3F 15 12 D4

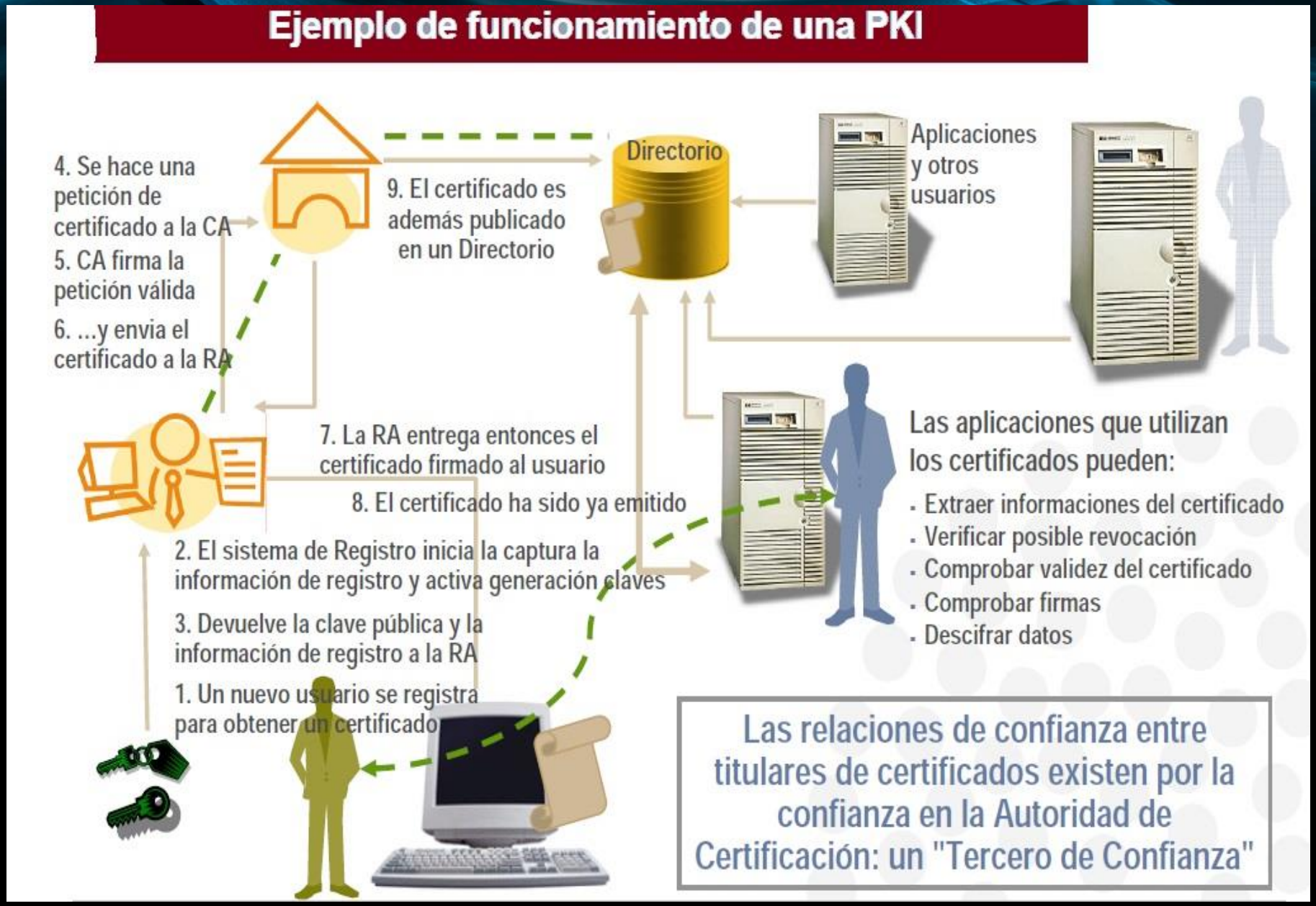
Información original en Icaro

Firma

Idéntico Documento

Distinto Documento

Entonces...Arquitectura PKI



FIRMA DIGITAL OFICIAL EN LA REP. ARGENTINA

Firma Digital

Una solución tecnológica, segura y confiable que permite firmar digitalmente documentos electrónicos.

Validez jurídica

Los documentos electrónicos firmados digitalmente tienen la misma validez jurídica que aquellos firmados de forma hológrafa.

Autenticidad e integridad

Podés identificar al autor fácilmente y verificar si ese documento fue alterado.

Seguridad

Garantizada por la criptografía asimétrica. Contamos con el respaldo de instalaciones seguras y confiables para el almacenamiento de datos biométricos.

Múltiples usos

Podés realizar trámites con entidades públicas y privadas. Podés firmar cualquier tipo de archivo.

JERARQUIA DE ENTIDADES CERTIFICADORAS

AC-RAÍZ
Autoridad Certificante Raíz de la República Argentina

AC-ONTI
Autoridad Certificante de la Oficina Nacional de Tecnologías de Información

AC-MODERNIZACION
Plataforma de Firma Digital Remota (PFDR)

Servicios

Firma Digital por Hardware con Token

Tramitá tu certificado de Firma Digital con token

Firma Digital Remota sin Token

Tramitá tu certificado de Firma Digital Remota sin Token

PDFR, Plataforma digital de firma remota

La **Firma Digital Remota sin Token** posee la misma validez jurídica que la firma hológrafa. Podés gestionar tus certificados y firmar documentos electrónicos desde la Plataforma de Firma Digital Remota y el Firmador para insertarte en la era digital.

- **Validez jurídica:** tener tu firma digital te permite firmar documentos electrónicos digitalmente con la misma validez jurídica que una firma de puño y letra. La firma se encuentra bajo control del firmante en todo momento.
- **Autenticidad e integridad del documento:** podrás identificar al autor fácilmente y verificar si ese documento fue alterado. Por lo cual se asegura la autoría e integridad del mismo.
- **Seguridad:** garantizada por la criptografía asimétrica que asegura la autenticidad de la firma. Contamos con el respaldo de instalaciones seguras y confiables para el almacenamiento de datos biométricos, con roles definidos para cada proceso y persona.
- **Múltiples usos:** podés realizar trámites con entidades públicas y privadas, tales como relaciones impositivas, notificaciones judiciales, operaciones bancarias, contratos a distancia y documentos de comercio exterior. El firmador te permite firmar digitalmente cualquier archivo en formato PDF.

FIRMA DIGITAL CON TOKEN CRIPTOGRAFICO

Se debe poseer un dispositivo criptográfico o Token de estándar FIPS-140-2 nivel 2 o superior, la firma queda protegida en el y bajo nuestra tutela.

- **Validez jurídica:** tener tu firma digital te permite firmar documentos electrónicos digitalmente con la misma validez jurídica que una firma de puño y letra. La firma se encuentra bajo control del firmante en todo momento.
- **Autenticidad e integridad del documento:** podrás identificar al autor fácilmente y verificar si ese documento fue alterado. Por lo cual se asegura la autoría e integridad del mismo.
- **Seguridad:** se basa en la criptografía asimétrica. Instalaciones seguras para el almacenamiento de los datos, los roles definidos para cada proceso y el personal capacitado en todos los sectores, garatizan la seguridad.
- **Múltiples usos:** para hacer trámites con entidades privadas y públicas, tales como declaraciones impositivas y notificaciones judiciales, operaciones bancarias, contratos a distancia y documentos de comercio exterior. Se pueden firmar digitalmente cualquier tipo de archivo.

Como obtenerlas:

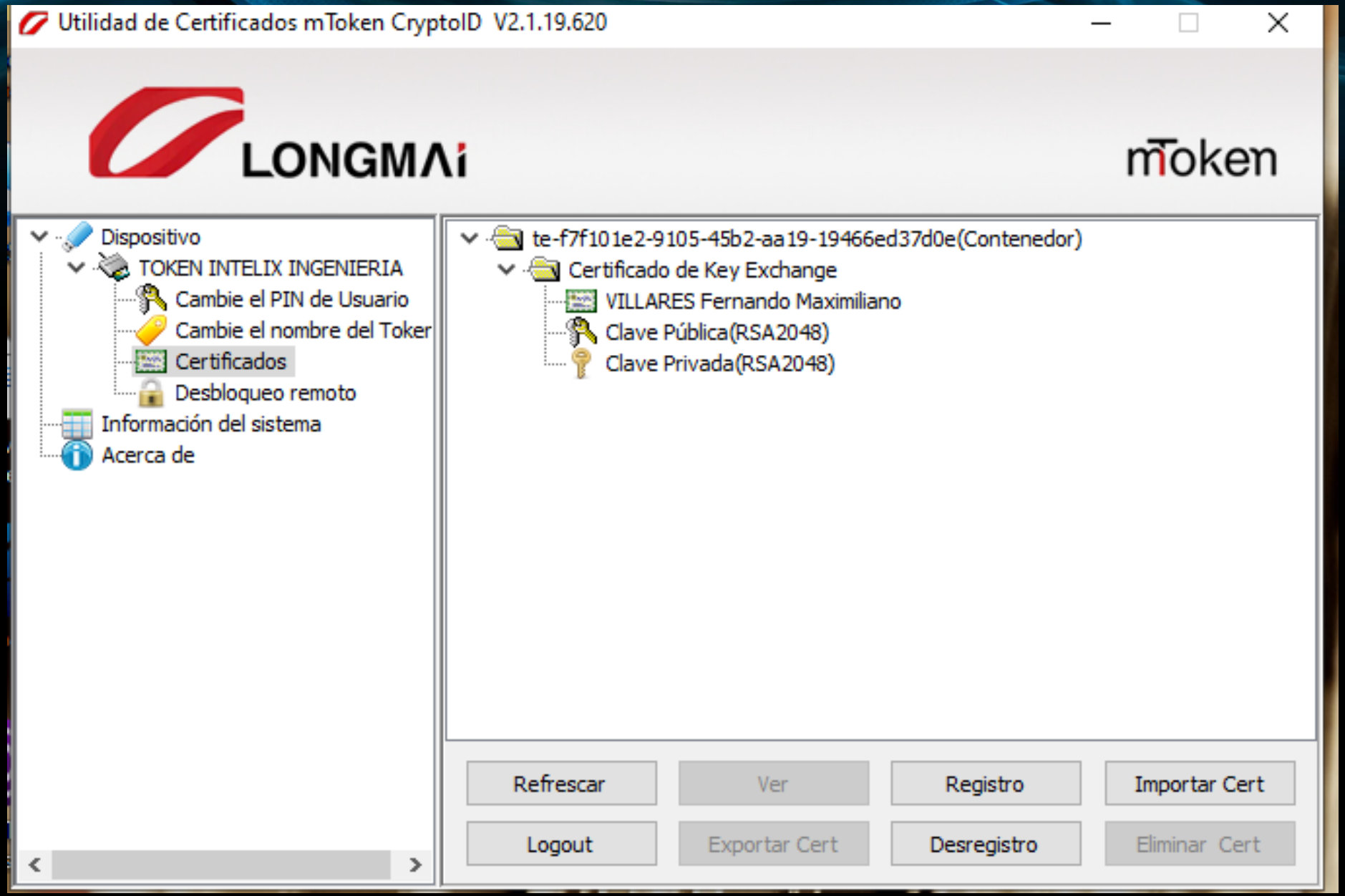
PDFR:

- Sacar turno en registro automotor mas cercano a tu domicilio, ir con DNI.
- Necesita tener instalado el soft Google Authenticator en el celular, si se cambia el celular o se pierde, se debe pedir turno nuevamente para cambiar el OTP dado por el Authenticator
- No tarda mas de 15 minutos.

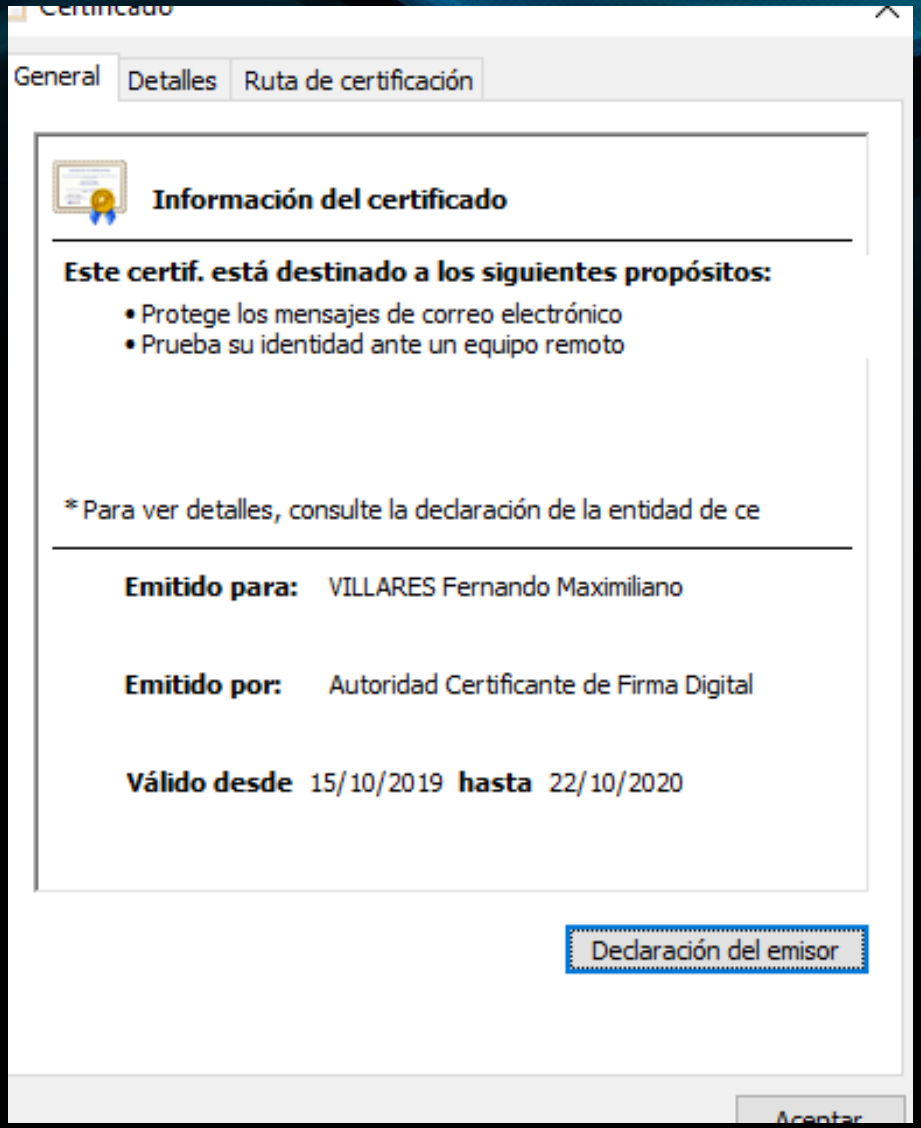
FIRMA DIGITAL CON TOKEN:

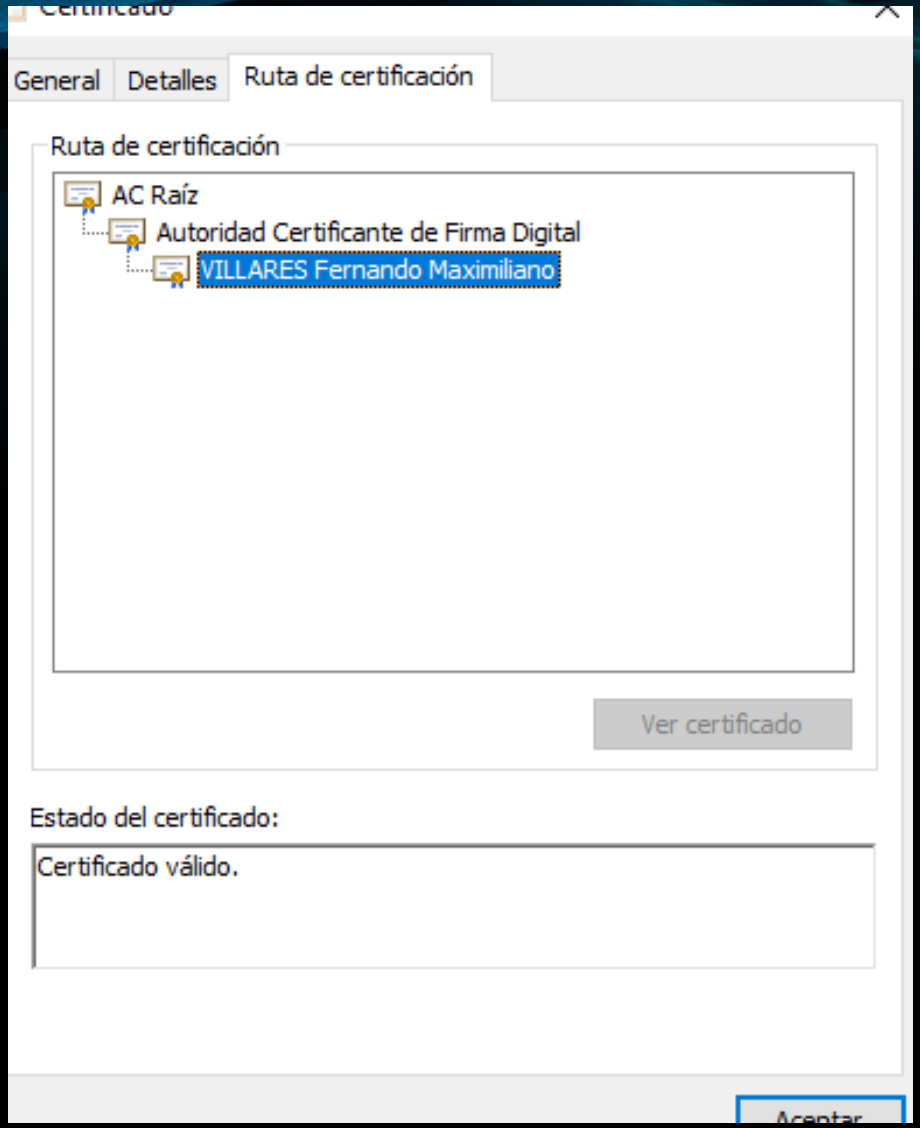
- Adquirir token Certificado FIPS 140-2 Nivel 2 o superior y solicitar su software de gestión y configuración al vendedor.
- Utilizar cuenta del servicio MI argentina y sacar turno, ir con DNI
- Llenar formulario de datos personales y selección de autoridad certificante (Poder Judicial Santa Fe).
- No tarda mas de 15 minutos.

CERTIFICADOS X.509 almacenado en TOKEN



CERTIFICADOS X.509 almacenado en TOKEN





REVOCACION DE CERTIFICADOS

¿Cómo puedo revocar mi certificado de firma digital?

Formas de realizar la REVOCACIÓN:

- Utilizando el Código de Revocación, el cual fue enviado a la cuenta de correo electrónico al momento de la emisión del certificado.
  El servicio de recepción de solicitudes de revocación se encuentra disponible en forma permanente SIETE POR VEINTICUATRO (7x24) horas a través de la Plataforma de Firma Digital Remota. Mirá el instructivo.

- Presentarse en la AR donde generaste tu Certificado.

Listado de Certificados Revocados

Consultar la validez de un certificado:

- Lista de certificados revocados CRL

- Online Certificate Status Protocol http://firmar.gob.ar/ocsp

PROS Y CONTRAS DEL USO DE FIRMA DIGITAL

PROS:

- AHORRO DE COSTES EN PAPEL Y MOVILIDAD, TRAMITES REMOTOS.
- AGILIDAD, EFICIENCIA Y VERSATILIDAD DOCUMENTAL.
- SEGURIDAD, SE DEBEN CONOCER CONTRASEÑAS Y APARTE POSEER EL TOKEN FISICO.
- AUTENTICACION Y AUTORIZACION ROBUSTA Y ECONOMICA DE USUARIOS, EMAILS, DOCUMENTOS, TELEFONOS CELULARES, IP ETC,

CONTRAS:

- POSIBLES USOS INDEBIDOS DE LA FIRMA DIGITAL O TOKEN SI SE PIERDE LA CUSTODIA SOBRE EL TOKEN Y/O CLAVE PRIVADA.
- SE DEBE CONFIAR EN LA CADENA DE AUTENTICACION Y CERTIFICACION
- SE DEBEN REVOCAR LOS CERTIFICADOS INMEDIATAMENTE SI SON EXTRAVIADOS O COMPROMETIDOS.
- PROBLEMAS SI LAS CLAVES PRIVADAS O LA AC RAIZ SON VULNERADAS.

LIVE DEMO:

- PLATAFORMA DIGITAL DE FIRMA REMOTA.
- FIRMA DIGITAL CON TOKEN PARA eMail.
- FIRMA DIGITAL CON TOKEN PARA pdf.
- FIRMA DIGITAL CON TOKEN PARA DOCS

¡GRACIAS POR TODO!

- Ing. Fernando Villares – 11/2019
- https://www.intelix.com.ar
- contacto@intelix.com.ar
-  @fmvillares
- Bajo licencia Creative Commons Atribución-CompartirIgual 2.5 Argentina (CC BY-SA 2.5)

[IN] telix
Ingenieria & Telecomunicaciones