

# Firma Electrónica Avanzada Vs. Firma Electrónica Simple

---

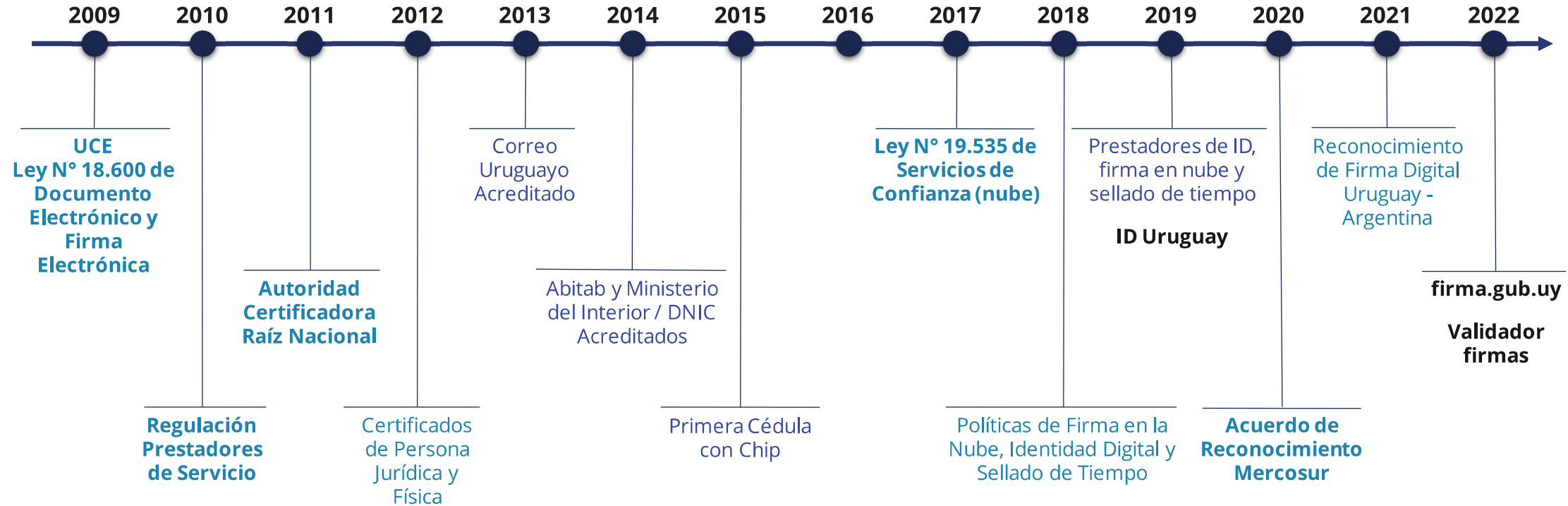
ALADI, Noviembre 2023



Uruguay  
Presidencia

⟷ agestic

# Evolución

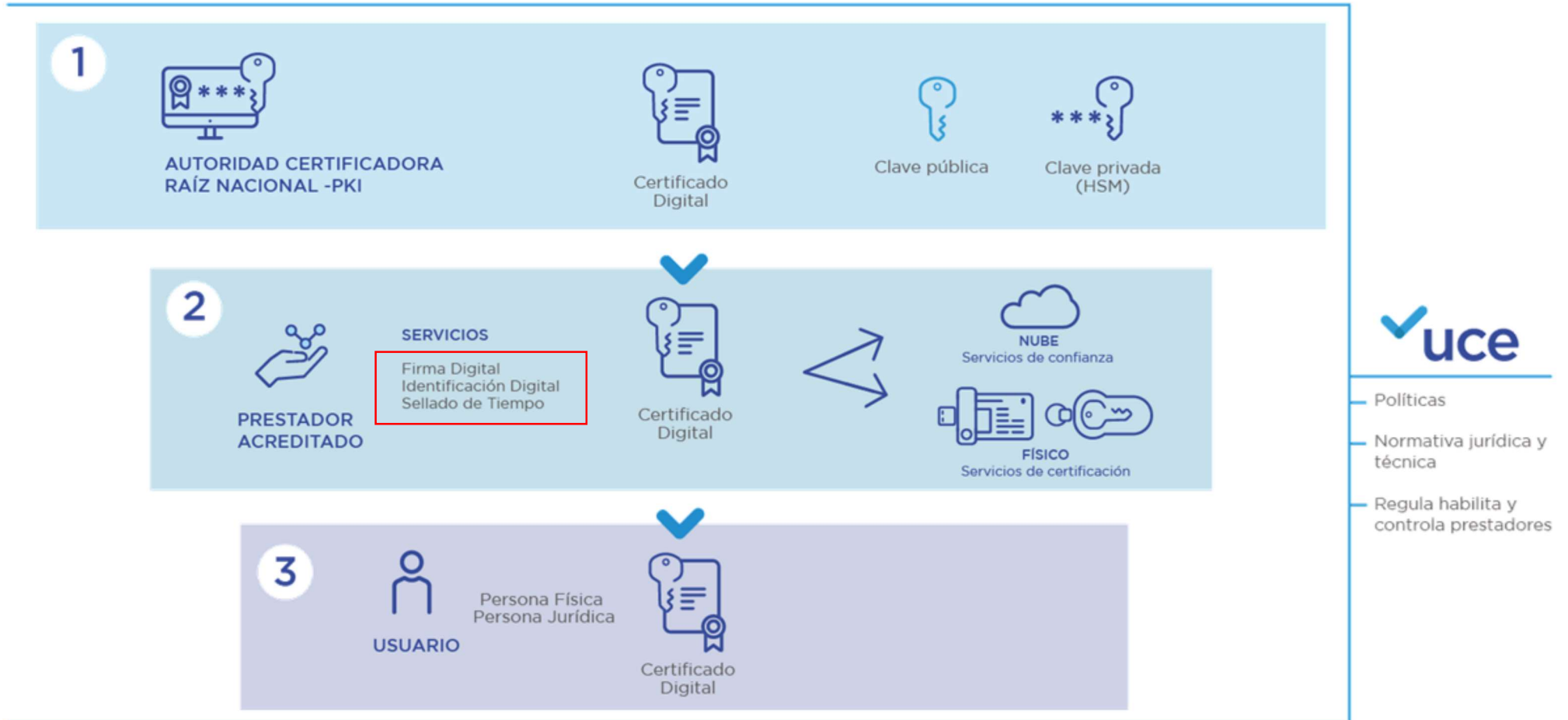


Marco Normativo e Infraestructura base

Ecosistema y Prestadores Acreditados

Soluciones para facilitar y promover el uso

# Infraestructura de Claves Públicas (PKI) = Cadena de Confianza



Raíz PKI  
AGESIC

Autoridad  
Certificadora  
Raíz Nacional  
(Root)

Tipos de  
Servicios de  
Confianza

Prestadores  
Servicios de  
Certificación

Prestadores  
Servicios de  
Confianza

Prestadores  
Sellado de  
Tiempo

Servicios /  
Prestadores  
Acreditados

Firma Persona  
Jurídica

Firma Persona  
Física

Firma PF con  
Actividad  
Empresarial

Identidad Digital

Firma Persona  
Física

Sellado de  
Tiempo



Usuarios

Personas Físicas (Naturales) – Empresas (Persona Jurídica) - Unipersonales

# Firma Digital

## Firma Electrónica Vs. Firma Electrónica Avanzada (Digital)



### Firma Electrónica

Un conjunto de datos, adjuntos a un documento electrónico acordados como válidos entre las partes.



### Firma Electrónica Avanzada (Digital)

- > **Identificación unívoca del firmante (no repudio).**
- > **Integridad**
- > Control exclusivo del dispositivo de creación de firma.
- > Verificable por terceros.
- > **Certificado Digital reconocido** emitido por un prestador acreditado.
- > Equivalente a firma hológrafa

# Documento digital

*"Representación digital de hechos o actos"*

- > Es una nueva forma de documento de carácter inmaterial.
- > Es generado o emitido electrónicamente y solo puede hacerse público mediante tecnología informática.
- > Interactividad entre los documentos.

# Infraestructura de Claves Públicas (PKI)

- > Jerarquía de Autoridades Certificadores (CA), con una raíz
- > Método seguro, confiable y escalable para la distribución de claves públicas de forma segura, correcta y verificable.
- > Establece globalmente **una relación directa entre una clave pública y su “propietario” en un certificado digital x.509**
- > Regulado a través de la autoridad nacional competente

Es un ecosistema complejo de **tecnologías, procedimientos y políticas** para crear, administrar, almacenar, distribuir y revocar certificados digitales



# Infraestructura de Claves Públicas (PKI)



## 1. Autoridad Certificadora Raíz Nacional (AGESIC)

Clave privada en HSM (integridad y confidencialidad), clave pública en certificado digital



## 2. Prestadores de Servicios de Confianza

Clave privada en HSM (integridad y confidencialidad), clave pública en certificado digital

- 1. Ministerio del Interior / DNIC
- 2. Abitab
- 3. El Correo
- 4. Antel

Autoridad Certificadora (CA)

## 3. Personas y Empresas



- 1. Identificación de la entidad
- 2. Clave pública
- 3. Período de validez
- 4. Para qué se va a utilizar (firma, autenticación, etc)
- 5. Temas técnicos: algoritmos de cifrado utilizados, url de la lista de revocación

Clave privada en tarjeta inteligente, token o nube del prestador, clave pública en certificado digital x.509



# Validar una Firma Electrónica Avanzada Uruguay



## 1. Validar el certificado x.509:

- ✓ Formato
- ✓ Validez del certificado Vs. Fecha de la Firma

## 2. Validar la firma: $\text{hash}(\text{documento}) = ?$ descifrado de firma utilizando la clave pública del certificado

- ✓ Integridad
- ✓ Identificación unívoca del firmante

## 3. Revocación

- ✓ Utilizando la URL del certificado, consultar la revocación en el Prestador Acreditado (CRL o OCSP)

## 4. Cadena de Confianza (PKI)

- ✓ Repetir pasos 1, 2 y 3 para el certificado del Prestador Acreditado que firmó el certificado del usuario

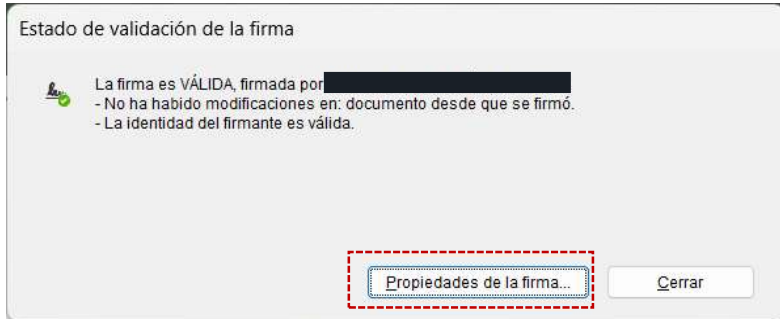
## 5. Cadena de Confianza (PKI)

- ✓ Repetir pasos 1, 2 y 3 para el certificado de la Raíz

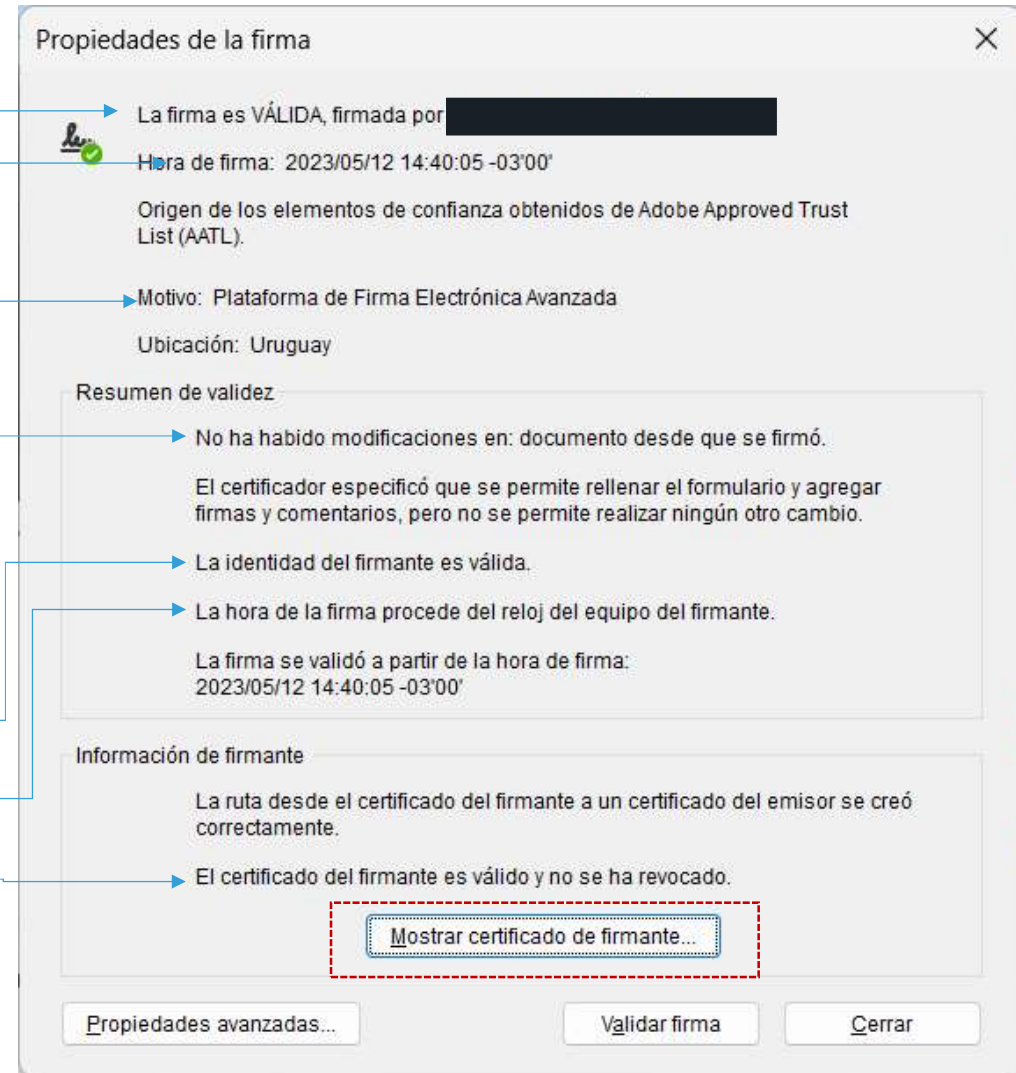
## 6. Firma Electrónica Avanzada reconocida

- ✓ Chequear si el certificado de la raíz está reconocido como de confianza (lista de confianza)

# Analizando una firma electrónica avanzada

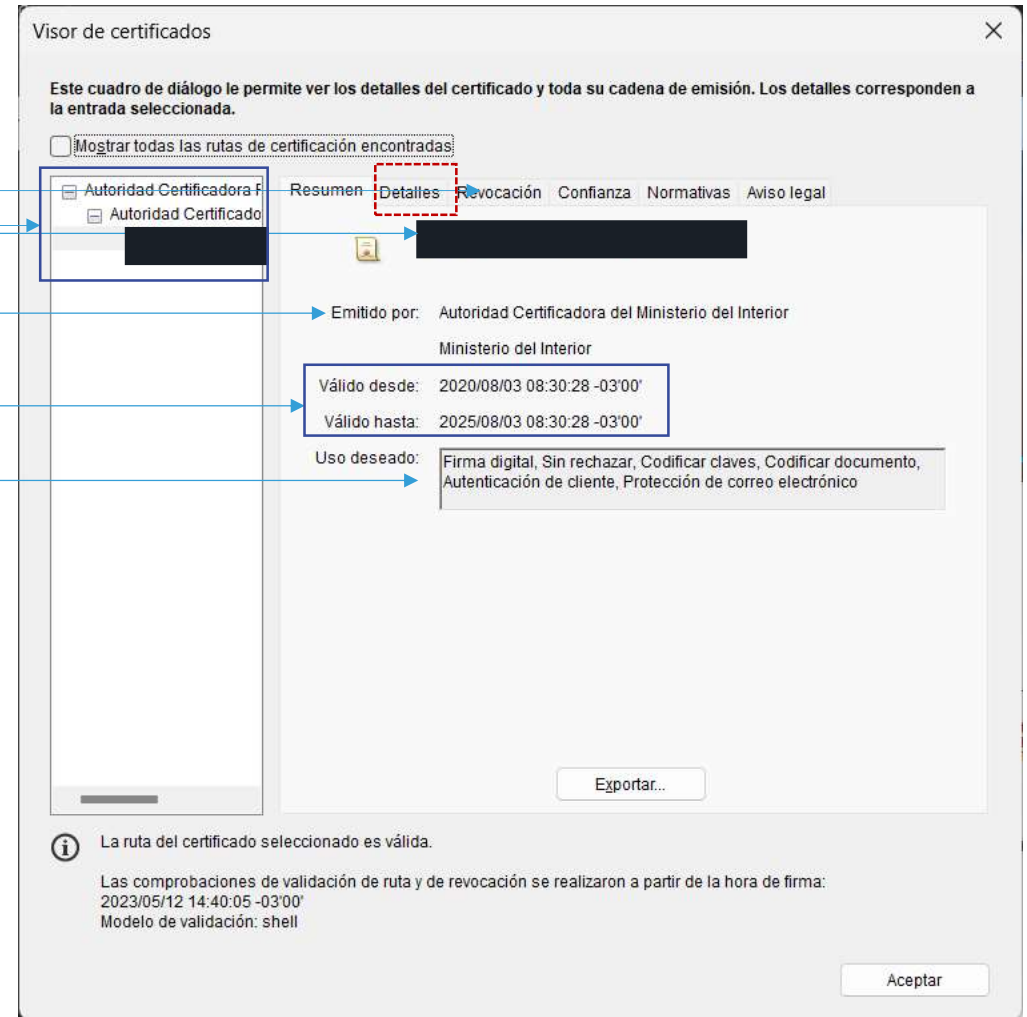


- > Nombre del firmante
- > Fecha, hora y huso horario del momento de la firma
- > Sistema que se utilizó para firmar
- > Confirmación de la integridad del documento
- > Verificación de la identidad del firmante
- > Indica si se utilizó el reloj del equipo donde se hizo la firma o un proveedor de sellado de tiempo
- > Verificación de la revocación del certificado del firmante



# Analizando una firma electrónica avanzada

- > Información sobre la lista de revocación
- > Certificados de la cadena de confianza - PKI
- > Nombre del firmante
- > Quién emitió y firmó el certificado del firmante
- > Período de validez del certificado
- > Para que se debe utilizar este certificado



Visor de certificados

Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.

Mostrar todas las rutas de certificación encontradas

Autoridad Certificadora F  
Autoridad Certificado

Resumen Detalles Revocación Confianza Normativas Aviso legal

Emitido por: Autoridad Certificadora del Ministerio del Interior  
Ministerio del Interior

Válido desde: 2020/08/03 08:30:28 -03'00'  
Válido hasta: 2025/08/03 08:30:28 -03'00'

Uso deseado: Firma digital, Sin rechazar, Codificar claves, Codificar documento, Autenticación de cliente, Protección de correo electrónico

Exportar...

**i** La ruta del certificado seleccionado es válida.

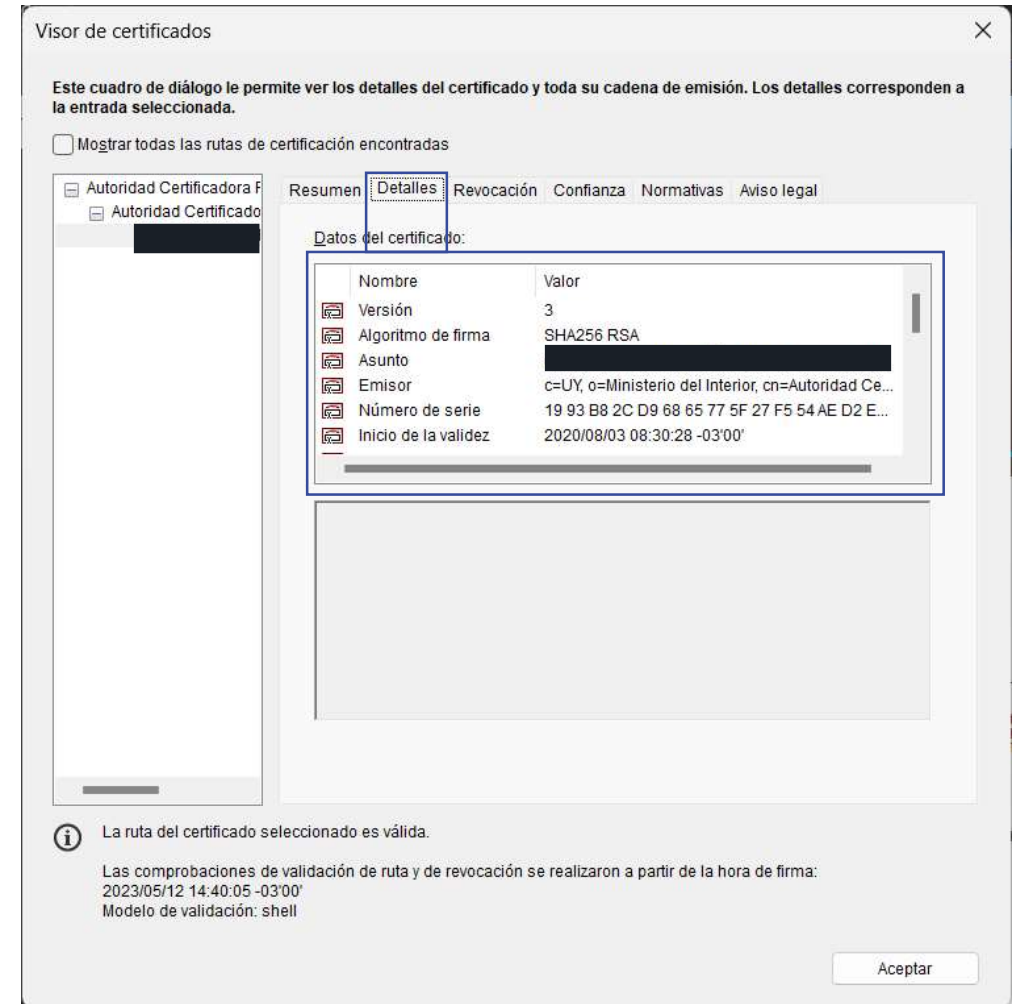
Las comprobaciones de validación de ruta y de revocación se realizaron a partir de la hora de firma:  
2023/05/12 14:40:05 -03'00'  
Modelo de validación: shell

Aceptar

# Analizando una firma electrónica avanzada

Los campos más relevantes son:

- > Algoritmo de firma: Algoritmos de hash y cifrado que se utilizaron para firmar
- > Asunto: identificación del firmante (nombre completo, código país y nro de documento)
- > Emisor: Autoridad Certificadora que emitió el Certificado del firmante
- > Número de serie del certificado
- > Inicio y fin de la validez del certificado
- > Puntos de distribución CRL: URL donde se publica la CRL de la Autoridad Certificadora, de esta forma un validador puede determinar si el certificado está revocado
- > Normativas del certificado: política que define la normativa asociada al certificado
- > Identificador de clave de autoridad: OID que identifica a la Autoridad Certificadora
- > Acceso a la información de autoridad: URL donde se encuentra el certificado de la Autoridad Certificadora en formato .cer
- > Uso de clave ampliado: este campo establece si además el certificado se puede utilizar para autenticación (según la normativa uruguaya). Ejemplo: los emitidos por El Correo no tienen este campo, dado que El Correo solo es prestador de firma
- > Uso de clave: para que se puede utilizar el certificado
- > Clave Pública: La clave pública del certificado según el tamaño y algoritmo utilizado
- > Compendio sha1 de clave pública: hash (sha1) de la clave pública
- > Datos X.509: el certificado en base 64



**Visor de certificados**

Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.

Mostrar todas las rutas de certificación encontradas

Autoridad Certificadora F  
 Autoridad Certificada

Resumen **Detalles** Revocación Confianza Normativas Aviso legal

Datos del certificado:

Nombre	Valor
Versión	3
Algoritmo de firma	SHA256 RSA
Asunto	[REDACTED]
Emisor	c=UY, o=Ministerio del Interior, cn=Autoridad Ce...
Número de serie	19 93 B8 2C D9 68 65 77 5F 27 F5 54 AE D2 E...
Inicio de la validez	2020/08/03 08:30:28 -03'00'

**i** La ruta del certificado seleccionado es válida.

Las comprobaciones de validación de ruta y de revocación se realizaron a partir de la hora de firma:  
2023/05/12 14:40:05 -03'00'  
Modelo de validación: shell

Aceptar

# Analizando una firma electrónica avanzada

Todos estos datos se pueden ver para cada uno de los certificados de la cadena de confianza:

1. Raíz: Autoridad Certificadora Raíz Nacional
2. Autoridad Certificadora (prestador acreditado)
3. Persona física – persona jurídica – persona física con actividad empresarial

Un validador tiene toda la información para determinar si una firma fue válida o no:

- ✓ Fecha de la firma Vs. Período de validez del certificado
- ✓ Titular del certificado
- ✓ Revocación del certificado

- ✓ Cadena de confianza: si el certificado pertenece a una PKI reconocida como de confianza o no. Este caso pueden haber dos grandes escenarios:
  - > Cada firma trate adjunta toda la cadena y sus certificados (caso uruguayo)
  - > Cada firma solo trae el certificado del firmante y de su CA
  - > Cada firma solo trae el certificado del firmante



Lista de confianza

Visor de certificados

Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.

Mostrar todas las rutas de certificación encontradas

Autoridad Certificadora F  
Autoridad Certificado

Resumen Detalles Revocación Confianza Normativas Aviso legal

Datos del certificado:

Nombre	Valor
Versión	3
Algoritmo de firma	SHA256 RSA
Asunto	[Redacted]
Emisor	c=UY, o=Ministerio del Interior, cn=Autoridad Ce...
Número de serie	19 93 B8 2C D9 68 65 77 5F 27 F5 54 AE D2 E...
Inicio de la validez	2020/08/03 08:30:28 -03'00'

La ruta del certificado seleccionado es válida.

Las comprobaciones de validación de ruta y de revocación se realizaron a partir de la hora de firma:  
2023/05/12 14:40:05 -03'00'  
Modelo de validación: shell

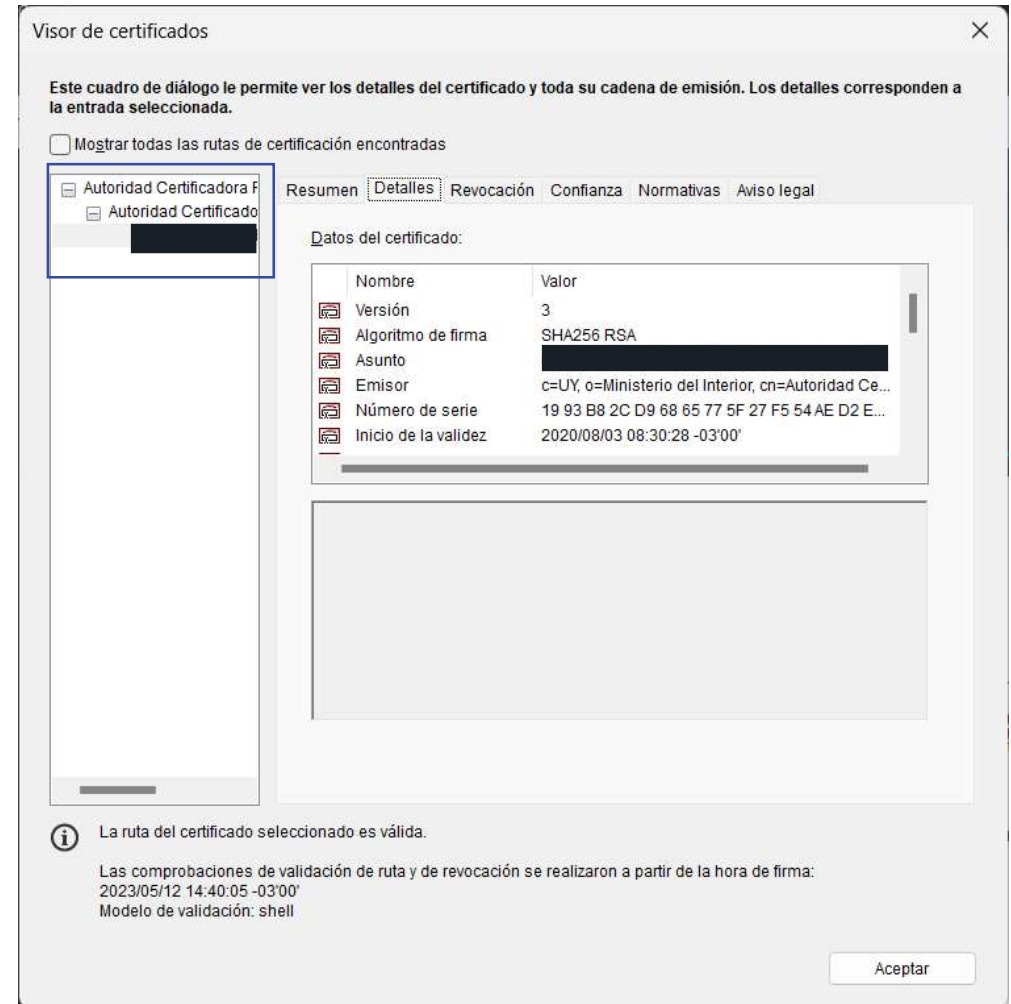
Aceptar

# Analizando una firma electrónica avanzada

Lista de Confianza: Es una lista de todas las organizaciones de confianza según la normativa que aplique. En este caso, todos los prestadores acreditados frente a la UCE.

Se puede implementar de diferentes formas:

1. En el caso uruguayo, todas las firmas se emiten incluyendo la cadena de confianza, con conocer el certificado de la Raíz es suficiente.
2. Si las firmas incluyen el certificado del firmante y de su CA, entonces es necesario incluir todos los certificados de las Cas n la lista de confianza. El campo "Acceso a la información de autoridad", también sirve para "encontrar a su padre"
3. Si las firmas solamente incluyen el certificado del firmante se hace más complejo. No es posible mantener una lista de confianza con los certificados de todas las personas físicas o jurídicas. Técnicamente se podría utilizar el campo "Acceso a la información de autoridad" para ubicar a su padre, pero no es un caso que se implemente.



Visor de certificados

Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.

Mostrar todas las rutas de certificación encontradas

Autoridad Certificadora F  
 Autoridad Certificado

Resumen Detalles Revocación Confianza Normativas Aviso legal

Datos del certificado:

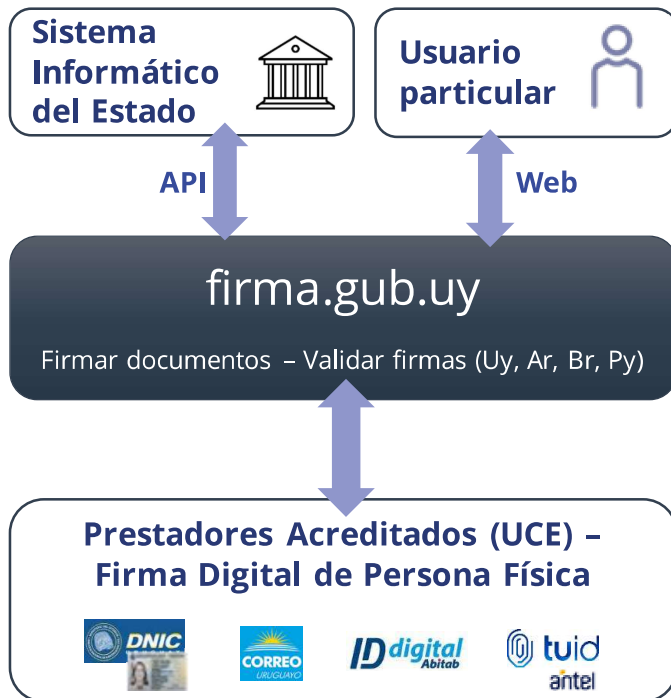
Nombre	Valor
Versión	3
Algoritmo de firma	SHA256 RSA
Asunto	[REDACTED]
Emisor	c=UY, o=Ministerio del Interior, cn=Autoridad Ce...
Número de serie	19 93 B8 2C D9 68 65 77 5F 27 F5 54 AE D2 E...
Inicio de la validez	2020/08/03 08:30:28 -03'00'

**i** La ruta del certificado seleccionado es válida.

Las comprobaciones de validación de ruta y de revocación se realizaron a partir de la hora de firma:  
2023/05/12 14:40:05 -03'00'  
Modelo de validación: shell

Aceptar

El objetivo de **firma.gub.uy** es facilitar el uso de la firma digital y la validación de firmas digitales en documentos.



## Beneficios:

- > Habilita todas las firmas electrónicas avanzadas reguladas por la UCE
- > Usuario particular: lo utiliza a través de un explorador web
- > Organismo: integrándose mediante API resuelve la firma en forma embebida dentro de su sistema informático
- > Aplicación multiplataforma (Win, Linux, iOS) para la firma en dispositivos físicos
- > Firma en Lote (firma de múltiples documentos en un solo proceso)
- > Permite ubicar gráficamente la firma
- > Valida firmas electrónicas avanzadas de Uruguay, Argentina y Brasil



¿Preguntas?

¡Gracias!



Uruguay  
Presidencia

⟷ agestic