

CONPAX



Validación Firma Electrónica

Equipo
Conpax TIC
02/09/2020

Dinko Yaksic

¿Qué es una Firma Electrónica?

Sistema de confianza basado en un algoritmo de criptografía de PKI (infraestructura de llave pública), emitido por una entidad certificadora para proveer:

- Autenticación
 - Identificación
 - Vigencia
- Integridad
 - Coherencia de datos
 - No-manipulación
- No-Repudio
 - Autoría



Ley 19.799: "Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel."

Concepto: Entidad Certificadora

- Empresa encargada de emitir certificados digitales (firmas electrónicas) a público general a partir de un certificado raíz
- Operan como garantes de autenticidad de las firmas emitidas por ellos
- Licitadas por el Ministerio de Economía, con condiciones específicas de rigurosidad (seguridad física, seguridad lógica, patrimonio, asegurada, etc.)
- <https://www.entidadacreditadora.gob.cl>

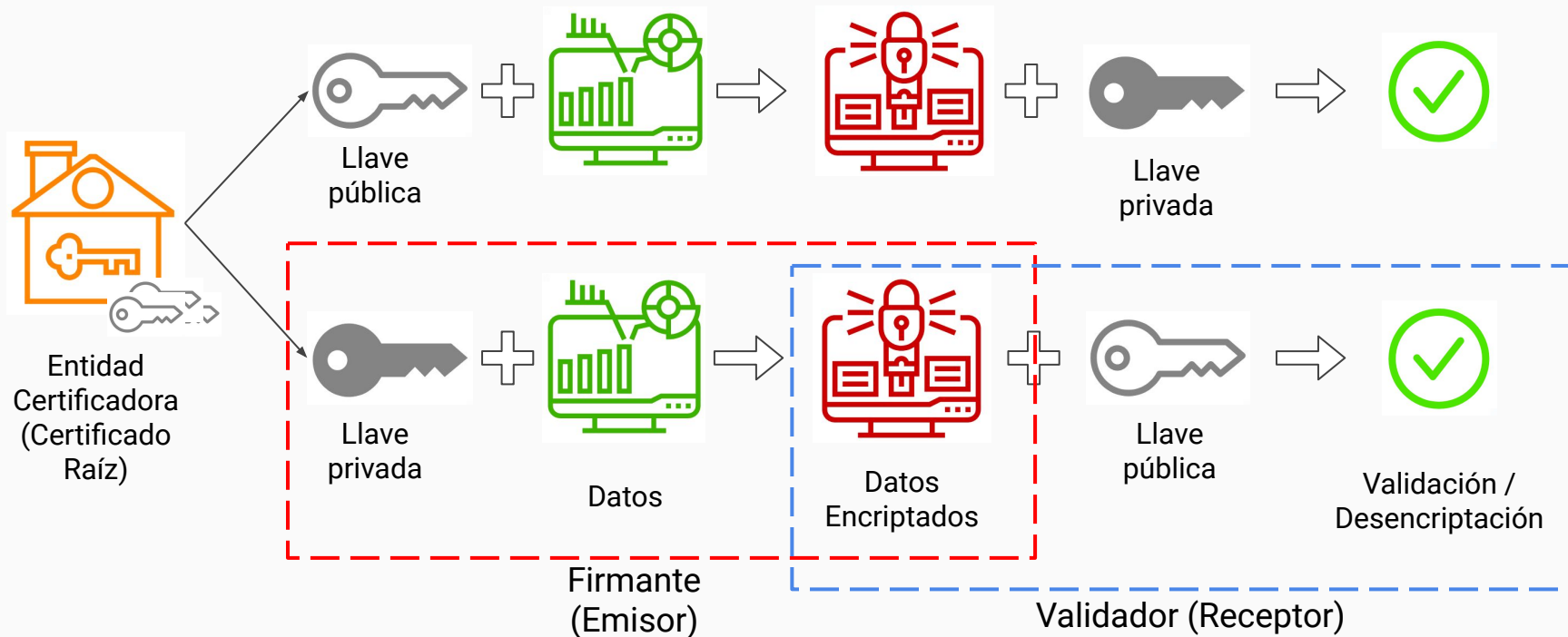
The screenshot shows the homepage of the 'Entidad Certificadora' website. The header includes the logo and navigation links: Home, Acerca de, Entidades Acreditadas, Leyes y Estándares, Noticias, and Ayuda. The main content area features a section titled 'Entidades' with a grid of logos for various accredited entities. On the left sidebar, there are links for 'Entidades Acreditadas', 'Leyes y estándares', 'Preguntas frecuentes', and 'Entradas Recientes'. The main content area displays information for 'E-CERT CHILE', including its accreditation details, representative legal information, and contact details.

The screenshot shows the accreditation page for 'E-SIGN S.A.'. The page includes the company logo and detailed accreditation information. Key details include: Accredited according to R.A.E. N° 330, dated June 1, 2006, by the Subsecretaría de Economía, Fomento y Reconstrucción; Representative Legal: Andrés Cave Valderrama; Domicile: Av. Apoquindo 6550, Oficina 501, Las Condes, Santiago; and the company's website. It also lists the accreditation expiration date (May 6, 2016) and the accreditation number (R.A.E. 3557) for the 'Certificación Biométrica'.

The screenshot shows the accreditation page for '70C'. The page includes the company logo and detailed accreditation information. Key details include: Accredited according to R.A.E. N° 1902, dated June 17, 2016, by the Subsecretaría de Economía y Empresas de Menor Tamaño; Representative Legal: Ricardo Navarro Luft; Domicile: Av. Santa María 2670, Oficina 403, Las Condes, Santiago, Chile; and the company's website. It also lists the accreditation expiration date (October 6, 2016) and the accreditation number (R.A.E. 3917) for the 'Certificación Biométrica'.

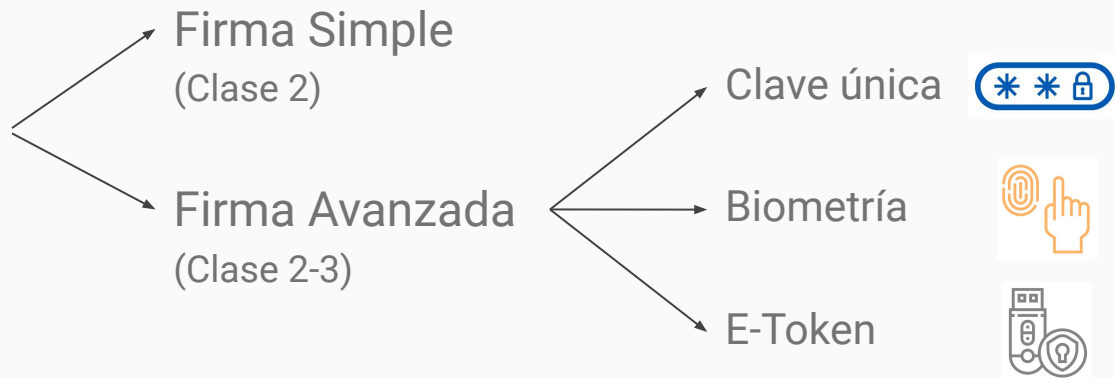
Concepto: Infraestructura PKI

- Sistema criptográfico que permite identificar unívocamente e irrefutablemente la aceptación de un individuo c/r a un documento (o datos, en general)



Tipos de Firma Electrónica

En Chile, se utilizan masivamente 2 tipos de firma electrónica, la simple, para fines tributarios (hasta ahora), y la avanzada, para sustituir la firma manuscrita:



- Masividad: Solo firma simple (en la práctica)
- Repudio: Firma avanzada no-repudiable
- Representación: Validez “notarial” solo firma avanzada

Datos interesantes sobre **Firma Electrónica**

En 1977, Rivest, Shamir y Adler inventan el algoritmo RSA

SIGNiX

Se estima tamaño global de mercado de US\$ 5,5 Bn para 2023

Markets and Markets

Para 2030, se estima tamaño global del mercado de US\$ 30 Bn

Globe News Wire

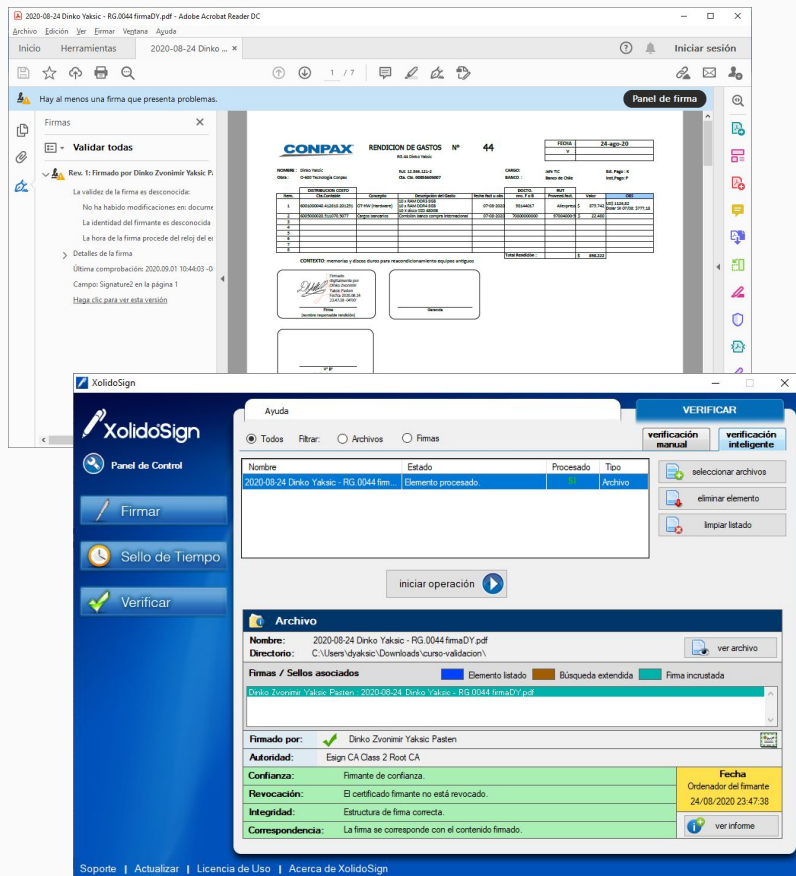
Criptografía básica: Factores primos

1797693134862315907729305190789024733617976978942306572734300
8115773267580550096313270847732240753602112011387987139335765
8789768814416622492847430639474124377767893424865485276302219
60124609411945308295208500576883815068234246288147391313

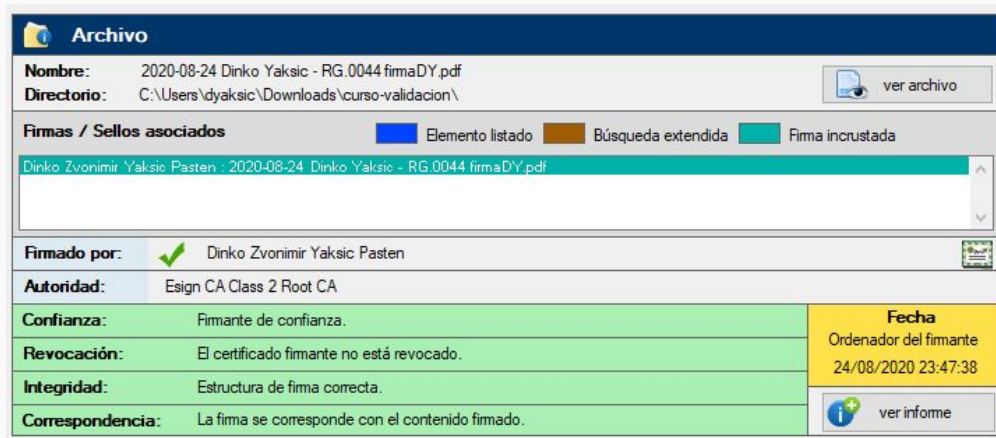
Mayores usuarios (global): BFSI, IT, gobierno, salud, educación

Fortune

Taller 1: Validación de Firmas



- Escenario:
 - Recepción de documento PDF y queremos verificar la validez de una firma
- Utilización de aplicaciones de validación:
 - Adobe Reader
 - Xolido



Taller 2: Validación de Firmas

- Escenario:
 - Recepción de documento PDF y queremos verificar la validez de varias firmas
- Ver estado del documento:
 - Tras segundo firmante
 - Tras primer firmante

Archivo Firmantes: 1 / 2

Nombre: 2020-08-24 Dinko Yaksic - RG.0044 firmaDY firmaFGO.pdf
Directorio: C:\Users\dyaksic\Downloads\curso-validacion\ 

Firmas / Sellos asociados  Elemento listado  Búsqueda extendida  Firma incrustada

FERNANDO GARCIA-OLDINI GAZITUA : 2020-08-24 Dinko Yaksic - RG.0044 firmaDY firmaFGO.pdf
Dinko Zvonimir Yaksic Pasten : 2020-08-24 Dinko Yaksic - RG.0044 firmaDY firmaFGO.pdf

Firmado por:  FERNANDO GARCIA-OLDINI GAZITUA 

Autoridad: E-CERTCHILE CA ROOT 02

Confianza: Firmante de confianza.	Fecha Ordenador del firmante 25/08/2020 11:21:32 
Revocación: El certificado firmante no está revocado.	
Integridad: Estructura de firma correcta.	
Correspondencia: La firma se corresponde con el contenido firmado.	

Archivo Firmantes: 2 / 2

Nombre: 2020-08-24 Dinko Yaksic - RG.0044 firmaDY firmaFGO.pdf
Directorio: C:\Users\dyaksic\Downloads\curso-validacion\ 

Firmas / Sellos asociados  Elemento listado  Búsqueda extendida  Firma incrustada

FERNANDO GARCIA-OLDINI GAZITUA : 2020-08-24 Dinko Yaksic - RG.0044 firmaDY firmaFGO.pdf
Dinko Zvonimir Yaksic Pasten : 2020-08-24 Dinko Yaksic - RG.0044 firmaDY firmaFGO.pdf

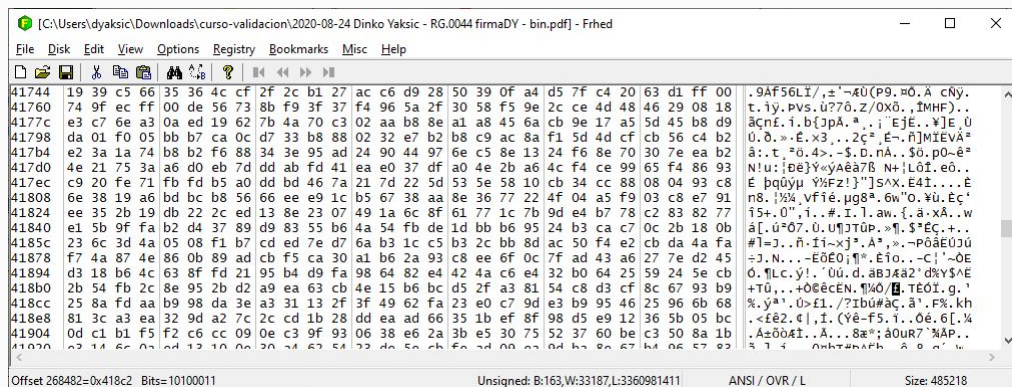
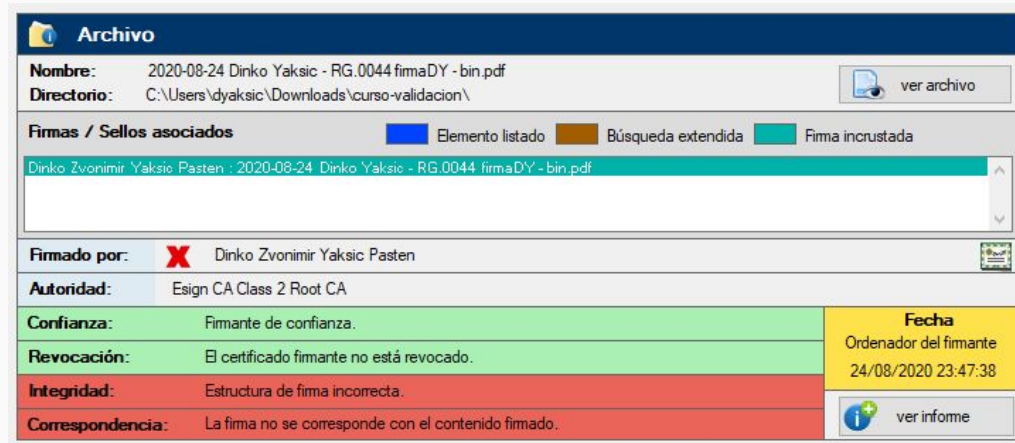
Firmado por:  Dinko Zvonimir Yaksic Pasten 

Autoridad: Esign CA Class 2 Root CA

Confianza: Firmante de confianza.	Fecha Ordenador del firmante 24/08/2020 23:47:38 
Revocación: El certificado firmante no está revocado.	
Integridad: Estructura de firma correcta.	
Correspondencia: La firma cubre solamente una parte del documento.	

Taller 3: Validación de Firmas

- Escenario:
 - Un PDF ya firmado, se alterará binariamente, cambiando contenido interno
- Ver estado del documento:
 - Estado de la firma
 - Integridad y correspondencia



Taller 4: Validación de Firmas

- Escenario:
 - Un PDF ya firmado, se alterará, por ejemplo modificando un monto
- Ver estado del documento:
 - Estado de la firma
 - Partes del documento

Archivo

Nombre: 2020-08-24 Dinko Yaksic - RG.0044 firmaDY - alterado.pdf
Directorio: C:\Users\dyaksic\Downloads\curso-validacion\ [ver archivo](#)

Firmas / Sellos asociados Elemento listado Búsqueda extendida Firma incrustada

Dinko Zvonimir Yaksic Pasten : 2020-08-24 Dinko Yaksic - RG.0044 firmaDY - alterado.pdf

Firmado por: Dinko Zvonimir Yaksic Pasten

Autoridad: Esign CA Class 2 Root CA

Confianza: Firmante de confianza.

Revocación: El certificado firmante no está revocado.

Integridad: Estructura de firma correcta.

Correspondencia: La firma cubre solamente una parte del documento.

Fecha: Ordenador del firmante
24/08/2020 23:47:38

[ver informe](#)

Item.	Cta.Contable	Concepto	Descripción del Gasto	fecha fact u obs	nro. F o B	Proveed.fact.	Valor	OBS
1	6001000040.412610.201251	OT-HW (Hardware)	10 x RAM DDR3 8GB 10 x RAM DDR4 8GB 10 X disco SSD 480GB	07-08-2020	98144017	Allexpress	\$ 875.742	US\$ 1126,82 Dolar SII 07/08: \$777,18
2	6005000020.511070.5077	Cargos bancarios	Comisión banco compra internacional	07-08-2020	70800000000	97004000-5	\$ 22.480	
3								
4								
5								
6								
7								
8								
Total Rendición :							\$ 1.898.222	

CONTEXTO: memorias y discos duros para reacondicionamiento equipos antiguos

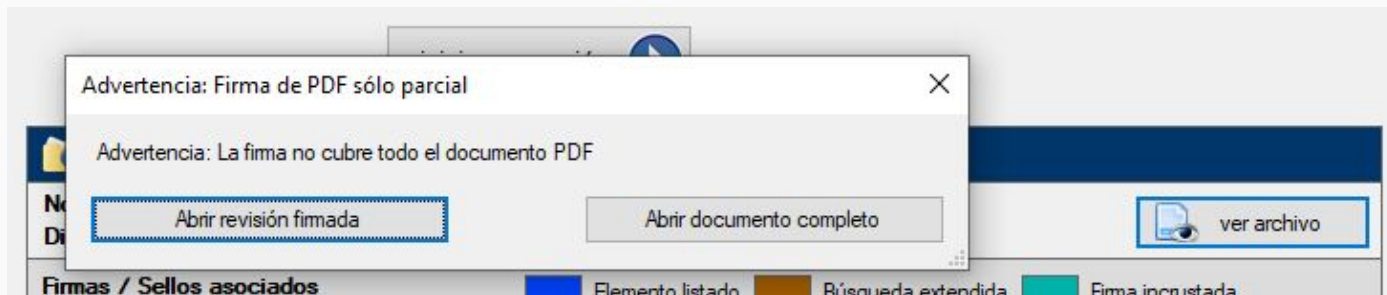
Firmado digitalmente por
Dinko Zvonimir
Yaksic Pasten
Fecha: 2020.08.24
23:47:38 -04'00'

Firma

Gerencia

Resumen de Validación de Firmas

- Recordar herramientas:
 - Tener instalado Certificado Raíz de Entidad Certificadora (Autoridad)
 - Utilizar Xolido para validar
- Recordar análisis en Xolido:
 - Solo permitir en amarillo la fecha de firmado, todo lo demás en verde
 - Si un documento dice “una firma cubre solamente una parte del documento” → Ver Archivo → **Abrir revisión firmada** y revisar!



Fin

¡Muchas gracias!

¿Dudas, comentarios, observaciones?