Firma Digital

Luis J. Dominguez Perez
luis.dominguez@cimat.mx

Abstract

- La firma electrónica es un instrumento utilizado para validar que la creación de un mensaje o documento es de quien dice serlo, así como garantizar que el documento no ha sido alterado de manera ilegal.
- En esta plática se explicará en qué consiste una firma electrónica, y para qué sirve.
- Así como el uso que se comienza a dar en México, sus retos y oportunidades.

Outline

1 Introducción

Outline

1 Introducción

2 Firma electrónica

- Legislación
- Banco de México
- Casos de éxito

Contenido, sección 1

1 Introducción

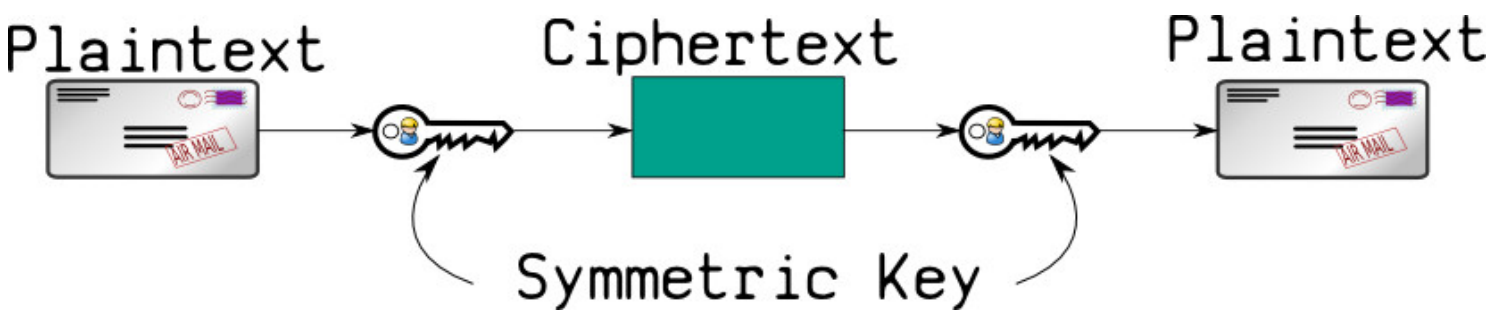
2 Firma electrónica

- Legislación
- Banco de México
- Casos de éxito

Bases de criptografía

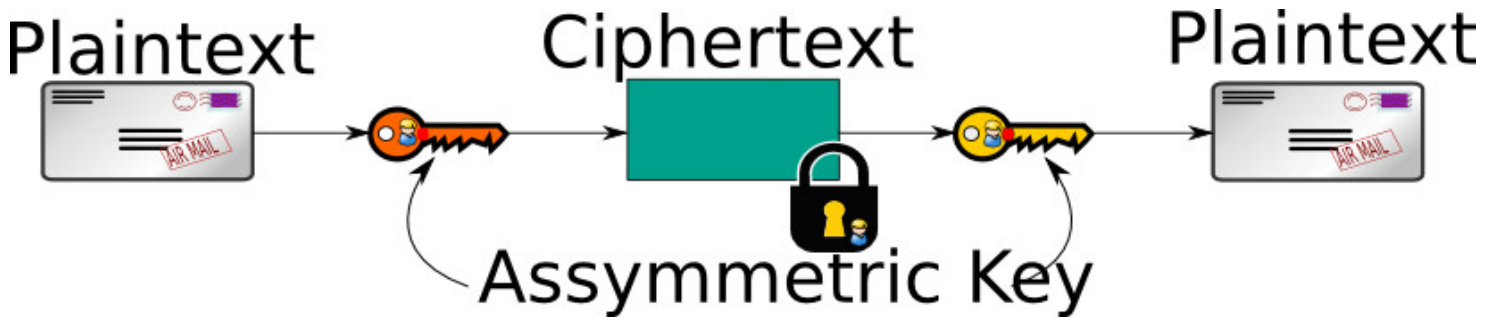
La criptografía soporta el *cifrado simétrico*, y el *asimétrico* para las funciones criptográficas:

- **Cifrado Simétrico.** La misma llave se utiliza tanto para cifrar como descifrar la información. El reto es que la llave tiene que ser intercambiada de manera segura entre las partes.



Bases de criptografía II

- **Cifrado Asimétrico.** Dos llaves diferentes, pero matemáticamente relacionadas se utilizan para cifrar y descifrar la información. Solamente la llamada llave pública es necesaria para las otras partes. Se puede compartir tal cal, y puede no necesitar un protocolo de intercambio de llaves.



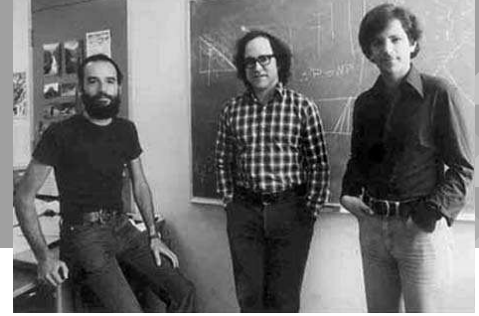
Llave asimétrica


La liberación del criptosistema de llave pública por Diffie, Hellman, (y Teske) en 1976 creó la criptografía moderna, y concentró los esfuerzos de la Teoría Computacional de Números en esa dirección.

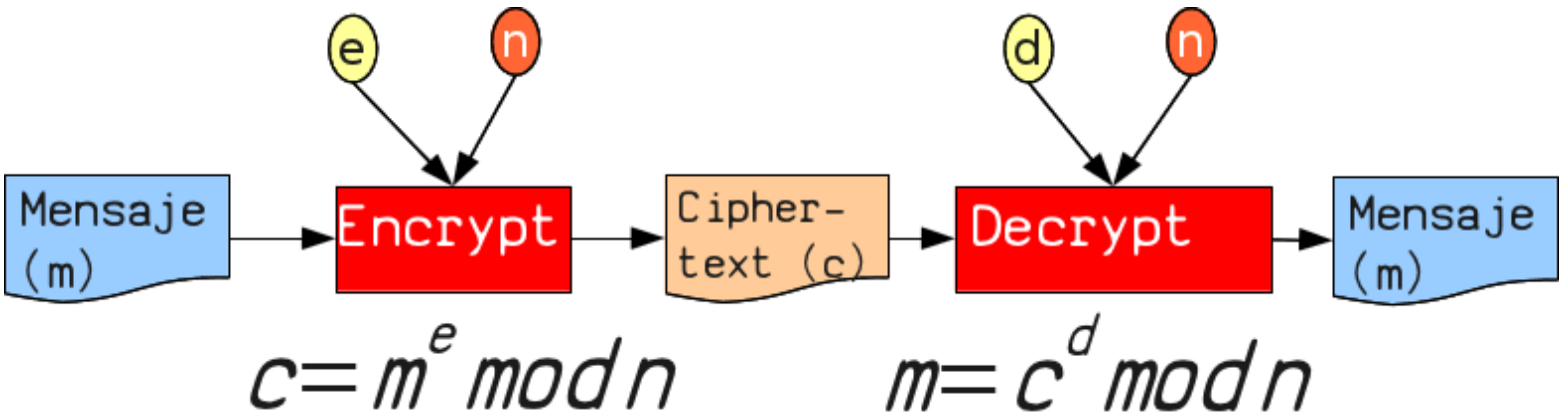
Dados (g, g^x, g^y), ¿cuál es el valor de g^{xy}?

Este problema es inviable para valores suficientemente grandes.

El modelo RSA

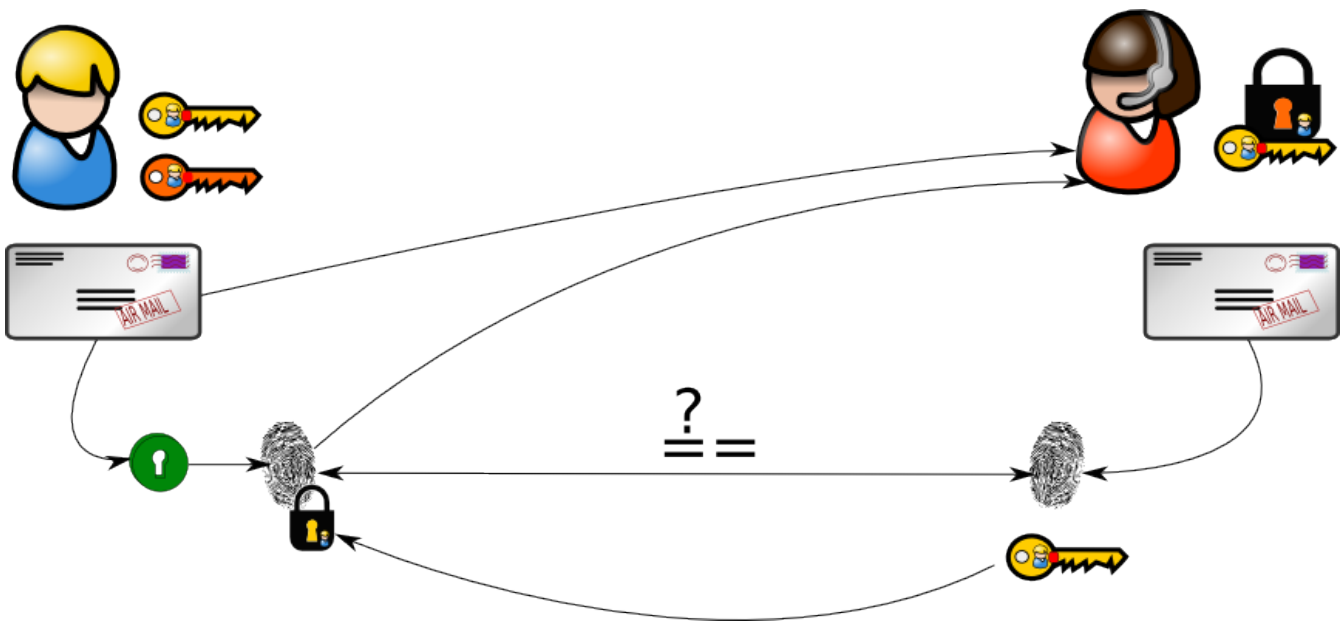


En 1978, el esquema RSA se introdujo como el primer criptosistema utilizable de llave pública. En este caso, estaba basado en el problema de factorización de números enteros muy grandes.

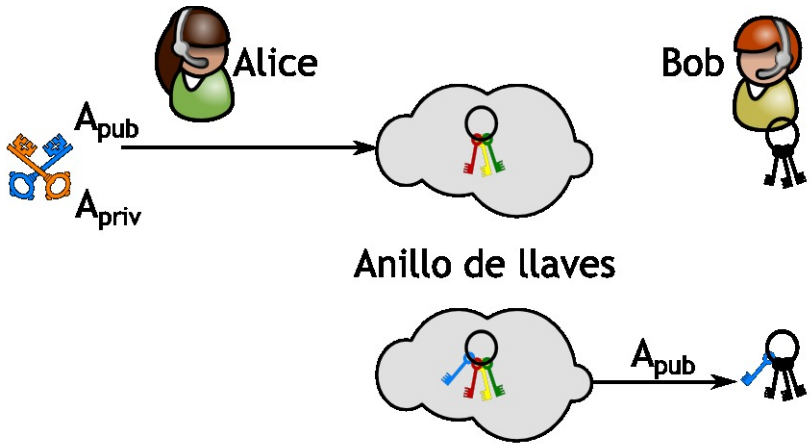


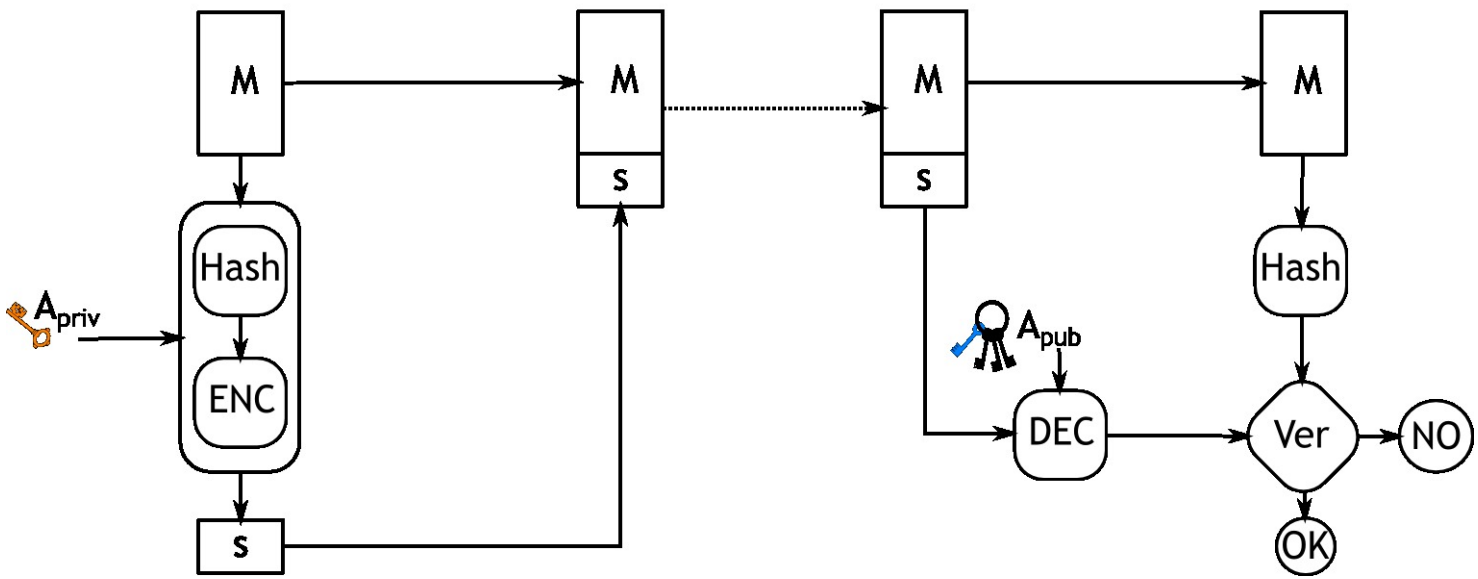
Firma de un mensaje

- Emisor: Obtiene la huella digital del mensaje a enviar
- Emisor: Utiliza su llave privada sobre dicha huella, y la envía como adjunto al mensaje al Destinatario.
- Destinatario: Aplica la llave pública del Emisor sobre la huella digital del mensaje, y compara.



Firma Digital





Certificados digitales

Es un documento que mediante una firma digital de una entidad de confianza, previamente almacenada en el equipo solicitante, asocia una clave pública con una identidad: nombre de la persona, organización, dirección, etc.

El certificado sirve para garantizar que una clave pública en particular pertenece al que dice ser el poseedor de la contraparte privada.

Los certificados son emitidos por una entidad de confianza, una Autoridad Certificadora.

Certificados digitales

Es un documento que mediante una firma digital de una entidad de confianza, previamente almacenada en el equipo solicitante, asocia una clave pública con una identidad: nombre de la persona, organización, dirección, etc.

El certificado sirve para garantizar que una clave pública en particular pertenece al que dice ser el poseedor de la contraparte privada.

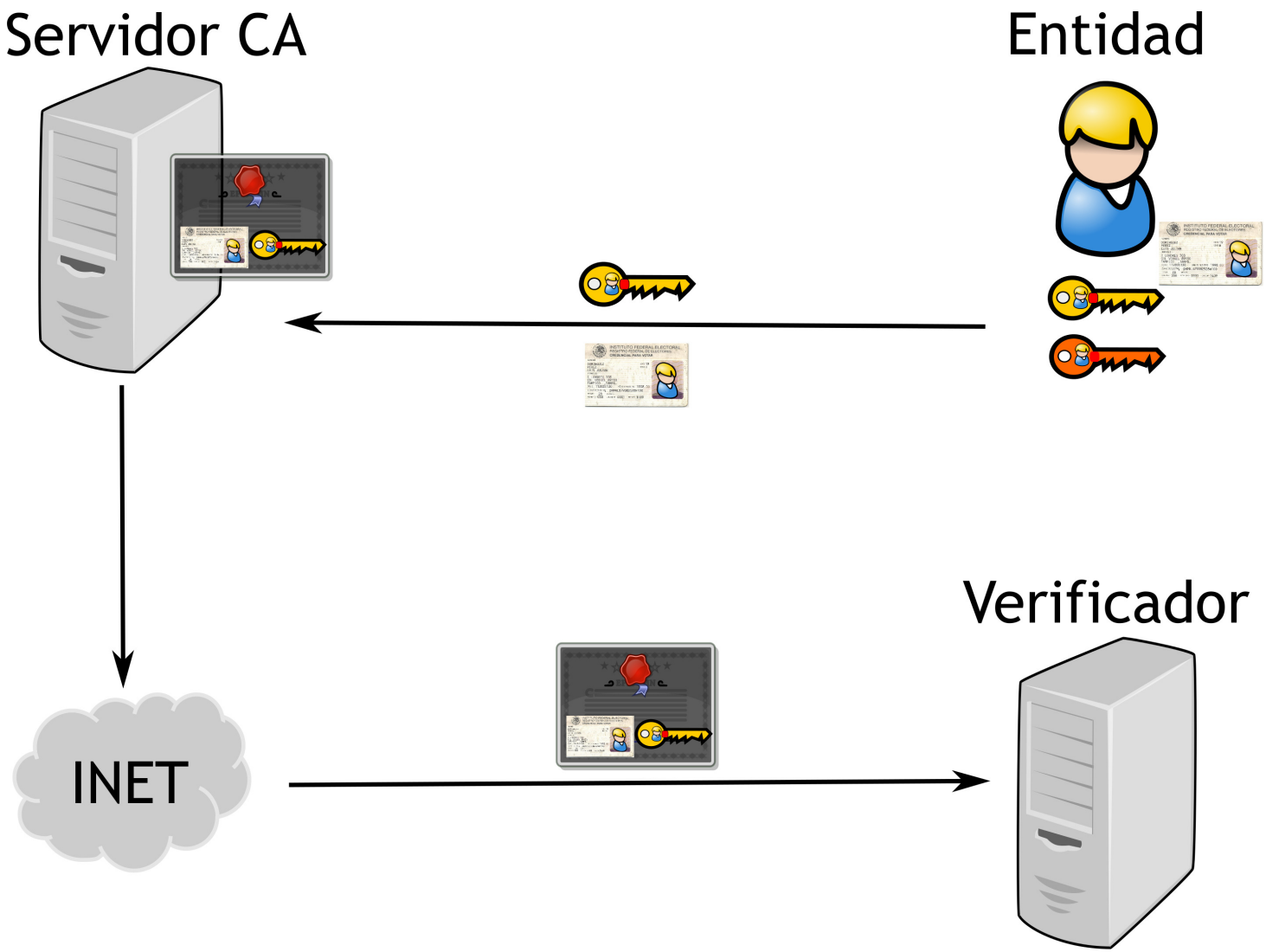
Los certificados son emitidos por una entidad de confianza, una Autoridad Certificadora... aunque en la práctica la relación de confianza se delega a Mozilla, Microsoft, Apple.

Responsabilidades de una CA

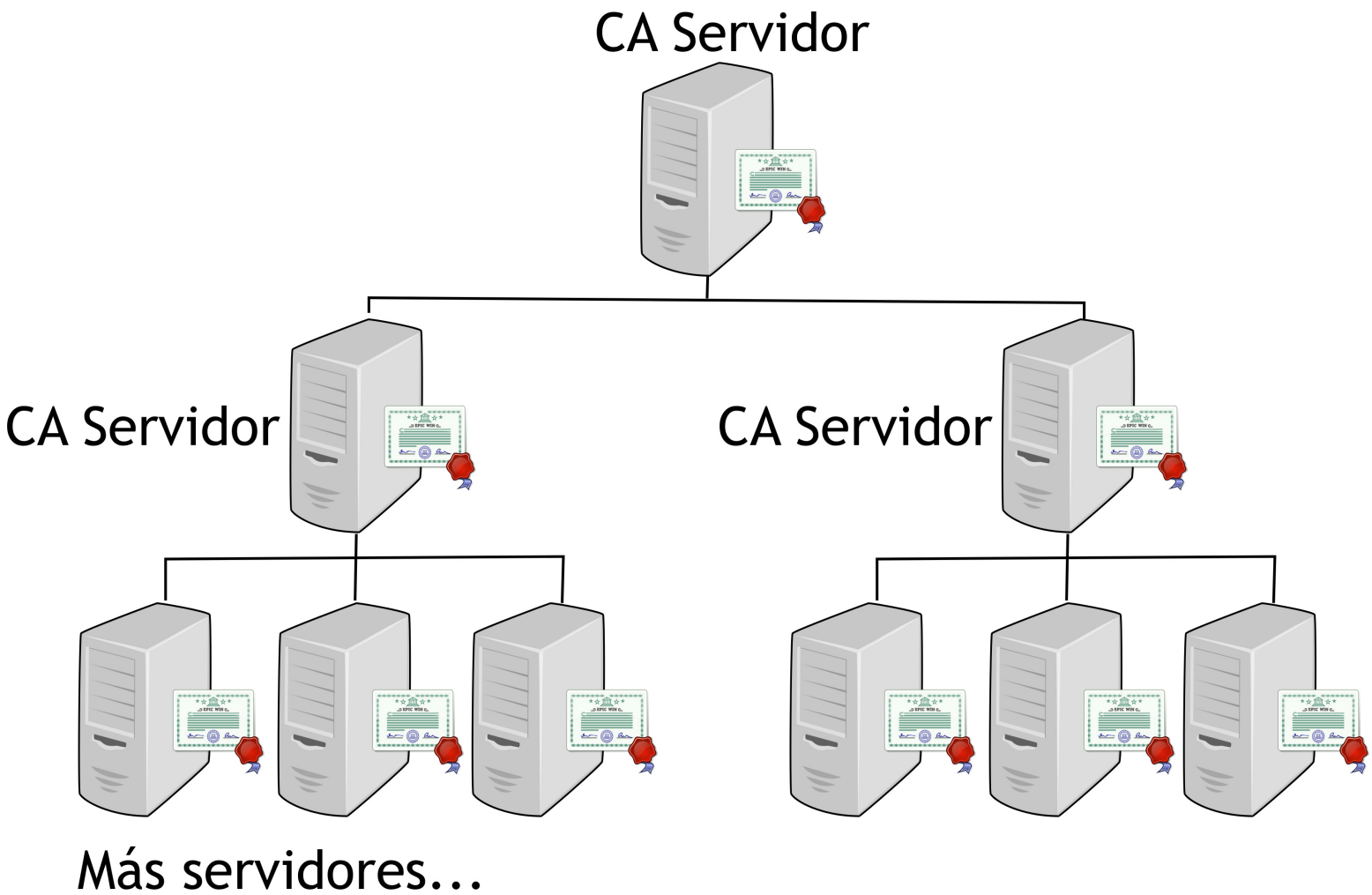
Las responsabilidades básicas son:

- Generación de llaves (Intercambio seguro)
- Emisión de Certificados (¿Qué son?)
- Emisión de CRL's (¿Para qué sirven?)

Certificados



Delegación de Autoridades Certificadoras



Contenido, sección 2

1 Introducción

2 Firma electrónica

- Legislación
- Banco de México
- Casos de éxito

La firma electrónica en México

- Es un paso hacia la transformación de la gestión pública.
- Coadyuva en la erradicación de la corrupción
- Provee una mayor productividad
- Reduce los costos de la ciudadanía al ejercer sus derechos y obligaciones.

Una fórmula para mejorar México

Ley que garantice la equivalencia entre:
firma autógrafa y de tipo digital

+

Esquema que fomente la productividad

=

Economía más competitiva
un México más fuerte
más próspero
con mejor futuro.

Inicios de la firma electrónica

- En un principio, el SAT instruyó el proyecto "Tu firma" (2004)
- Banxico intentó autorizar a terceros para validar las firmas
- SAT crea la CIEC - Clave de Identificación Electrónica Confidencial
- Nace la "FEA" - Firma Electrónica Avanzada (2005)
- Se instrumenta un esquema de PKI

Inicios de la firma electrónica - 2

- Se renombra la FEA por "FIEL" (2007)
- Entran la Secretaría de Economía, la Secretaría de la Función Pública, y el Servicio de Administración Tributaria (2008 – 2012)

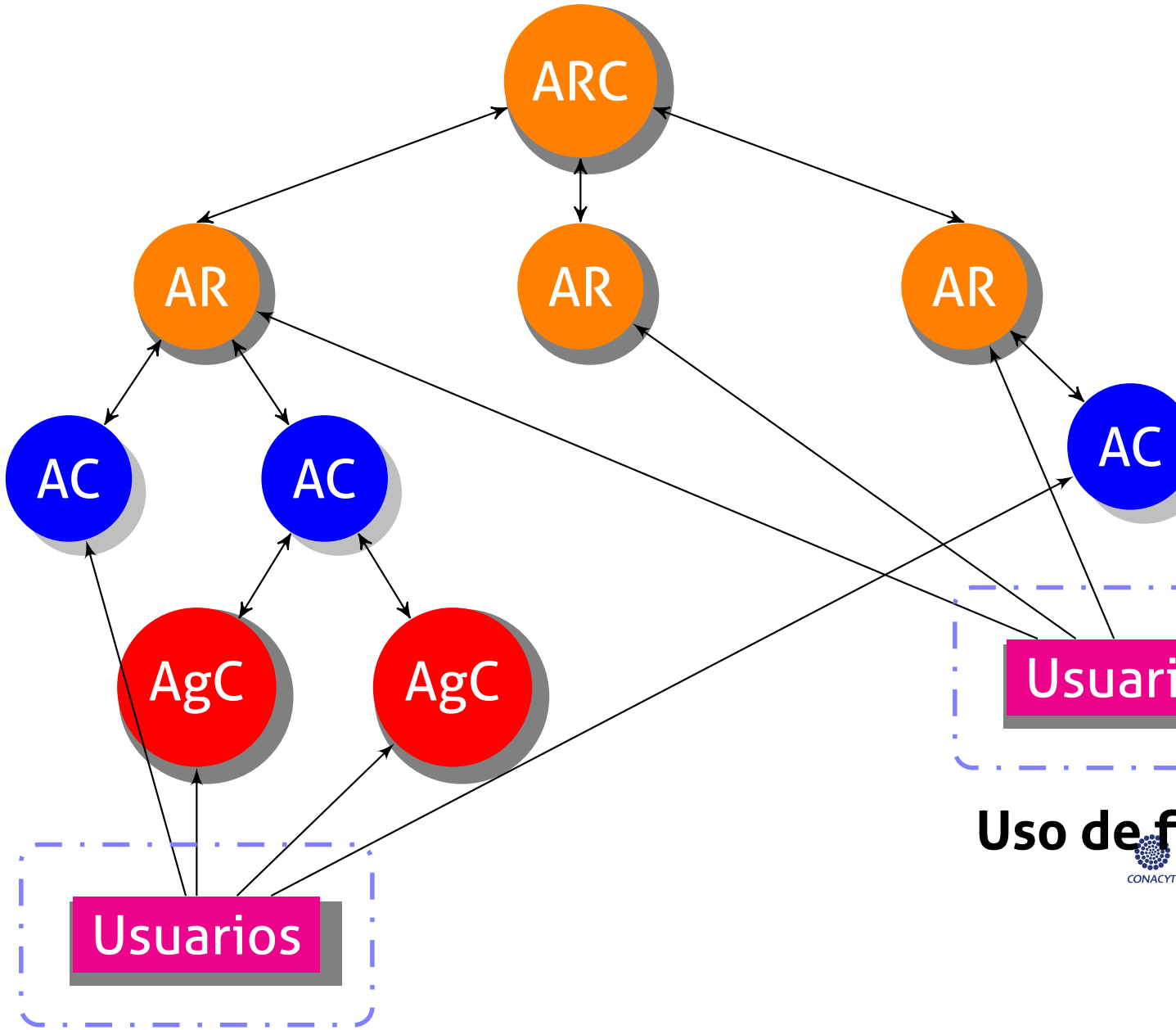
Leyes federales relacionadas

- Ley Federal de Protección de Datos en Posesión de los Particulares - 2010, 2010
- Ley Federal de Transparencia y Acceso a la Información Pública - 2002, 2010
- Código de Comercio - 1889, 2012
- Código Fiscal de la Federación - 1984, 2005
- Ley de Firma Electrónica Avanzada - 2012, 2012
- Decreto de Austeridad 2012 - 2012, 2012

Infraestructura Extendida de Seguridad

- El Banco de México, como Banco Central del país, establece los mecanismos de comunicación para las transacciones financieras
- Define una infraestructura PKI que hace uso extensivo de los certificados digitales
- Delega ciertas actividades a los diferentes actores del mercado financiero

Infraestructura IES



Uso de f

Procesos de Certificación

Casos de éxito

- Caso Colima
  - Mejora de productividad
  - Nuevas leyes
  - Contratación de personal
- Caso UNAM
  - Autenticar y digitalizar
  - Aviso en la Gaceta universitaria
  - Cambio escalonado
- Caso D.F.
  - Corrupción y mejores servicios
  - Nuevas leyes
  - Delegación de trabajo

Casos de éxito - 2

- Caso SAT
  - Productividad y mejor recaudación
  - Nuevas leyes
  - Cambio escalonado
- Caso Banxico
  - Proporcionar una infraestructura
  - Nuevas leyes
  - Concientizar al gobierno

Situación legal de la firma electrónica en México

- Categoria 1. Existe una ley, CA, portal y/o aplicaciones
- Categoria 2. Existe una ley
- Categoria 3. No existe una ley, pero la usan, o planean
- Categoria 4. No hay avance

Cortesia:Miguel Morales

¡Gracias!

- Discusión

luis.dominguez@cimat.mx