PRIMER ENCUENTRO UNIVERSITARIO DE FIRMA DIGITAL

LA CUMBRECITA 2012

UNC
400 AÑOS

Agenda

La finalidad del mismo es construir un ámbito para el intercambio de experiencias y propuestas relacionadas con la aplicación de la firma digital, tanto para procesos de gestión como actividades académicas.

- Motivación
- Aspectos técnicos
- Aspectos legales
- Aplicaciones

MOTIVACIÓN DEL ENCUENTRO

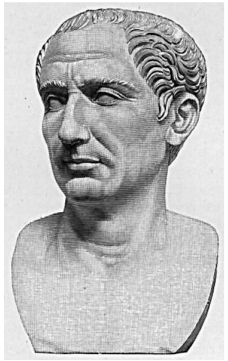
Motivación

La UNC está interesada en construir una Infraestructura de Firma Digital para la enseñanza y aplicación de la Firma Digital en diferentes Unidades Académicas.

- ✓ Cátedras especializadas
- ✓ Recursos humanos formados
- ✓ Tecnología disponible
- ✓ Auditorías específicas
- ✓ Proyectos en SeCyT

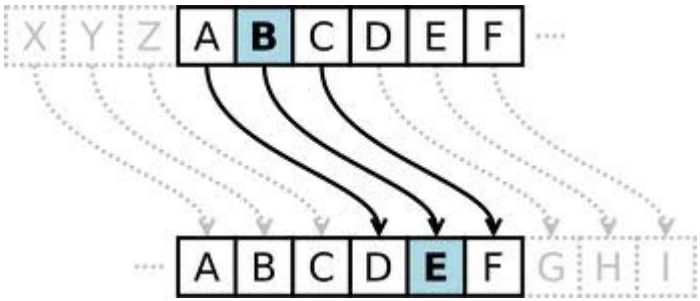
ASPECTOS TECNOLÓGICOS

Aspectos tecnológicos



Desde mucho antes que las TICs irrumpieran en la historia del hombre, la seguridad en el manejo de la información fue una preocupación que se materializó a través de SERVICIOS DE SEGURIDAD.

Confidencialidad

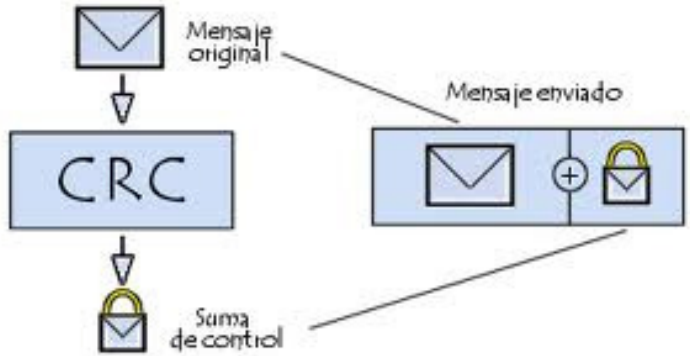


Garantizar que el mensaje es accesible sólo para aquellos autorizados a tener acceso.

Aspectos tecnológicos

Las primeras tecnologías de las comunicaciones dieron origen a nuevos SERVICIOS DE SEGURIDAD.

Integridad



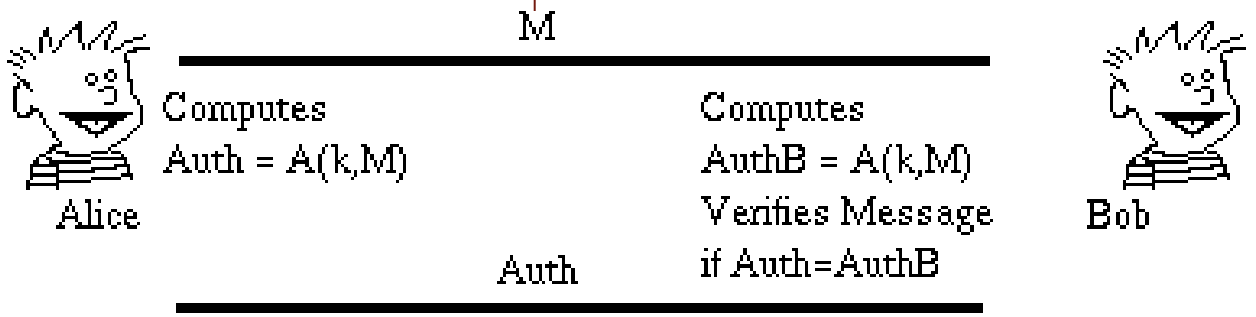
Garantizar que el mensaje no ha sido modificado en la transmisión de un emisor a un receptor.

Aspectos tecnológicos

Las primeras tecnologías de las comunicaciones dieron origen a nuevos SERVICIOS DE SEGURIDAD.

Autenticación

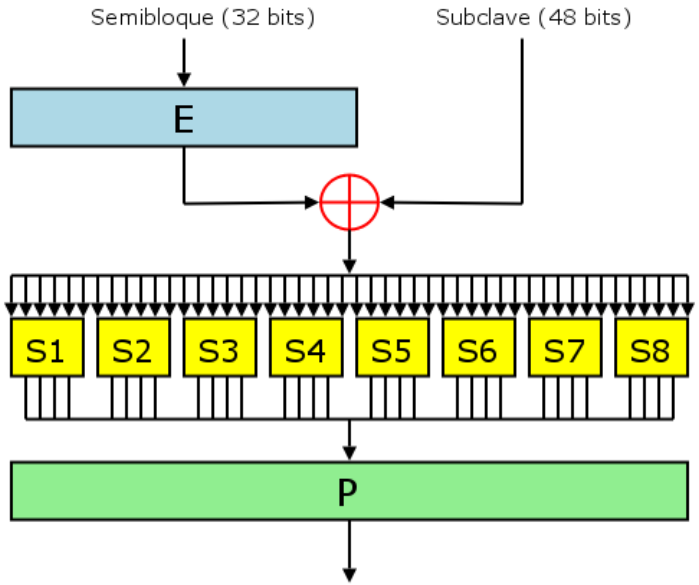
Es el proceso de verificación de la identidad digital del remitente de una comunicación ante una petición de conexión.



Aspectos tecnológicos

La criptografía simétrica hizo posible extender estos servicios al intercambio de información masiva de pares emisor/receptor.

DES



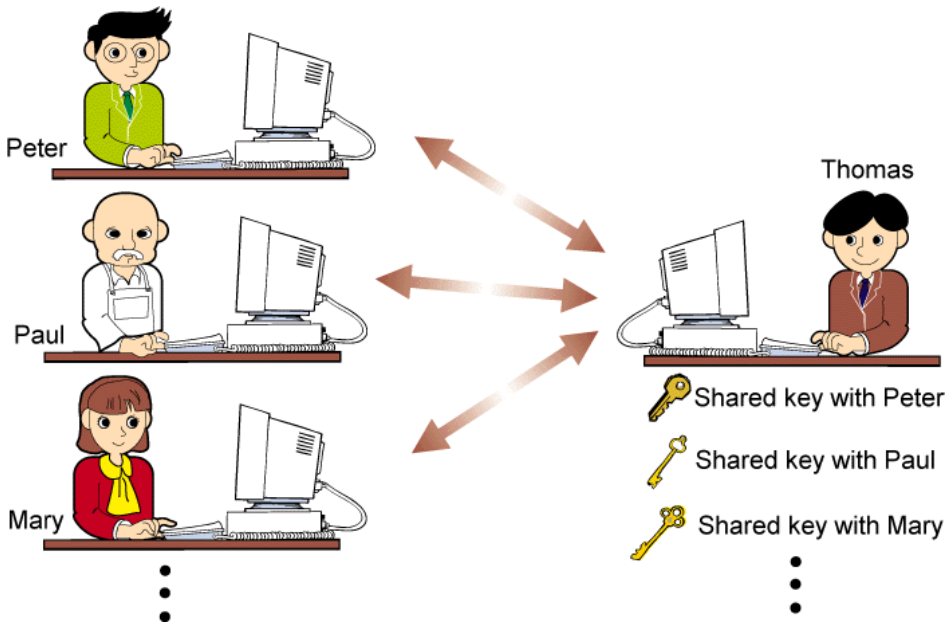
En 1972, se concluyó en la necesidad de un estándar a nivel gubernamental (USA) para cifrar información confidencial.

Aspectos tecnológicos

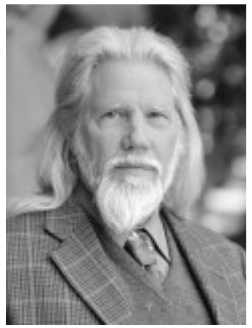
Pero surge una limitación..!!

El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio de claves.

DISTRIBUCIÓN DE CLAVES



Aspectos tecnológicos



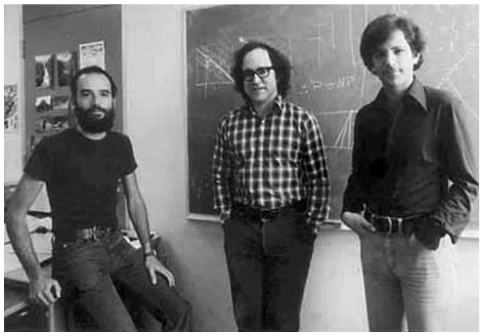
Prácticamente de forma paralela a la aparición de DES, surgen iniciativas para solucionar el problema.

CLAVE PÚBLICA

Whitfield Diffie

En 1976 publica junto a Martin Hellman "*New Directions in Cryptography*", que presentaba un nuevo método de distribución de claves criptográficas para solucionar uno de los problemas fundamentales de la criptografía: la distribución de la clave.

Aspectos tecnológicos

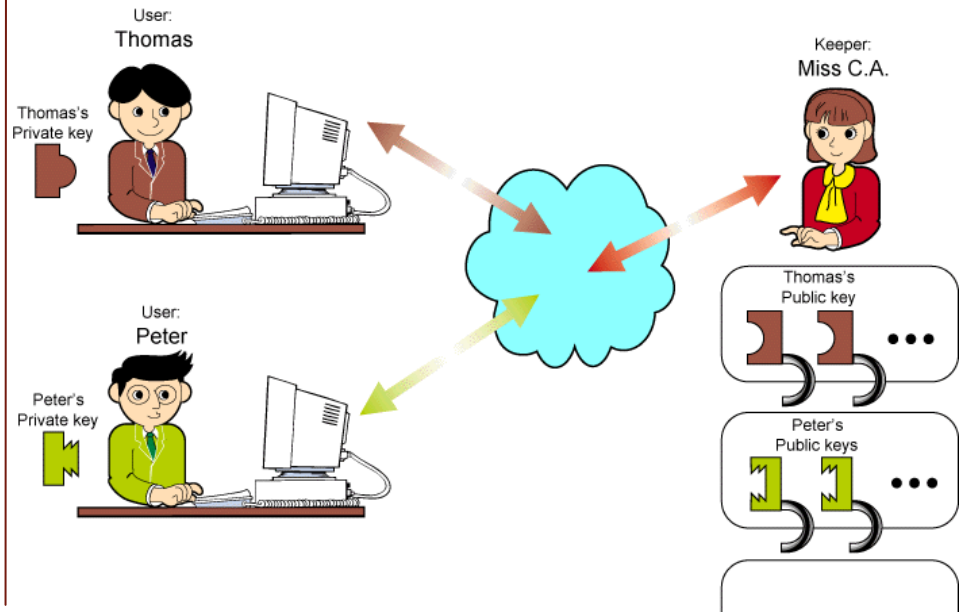


En 1977 se publica RSA (Rivest, Shamir y Adleman).

Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

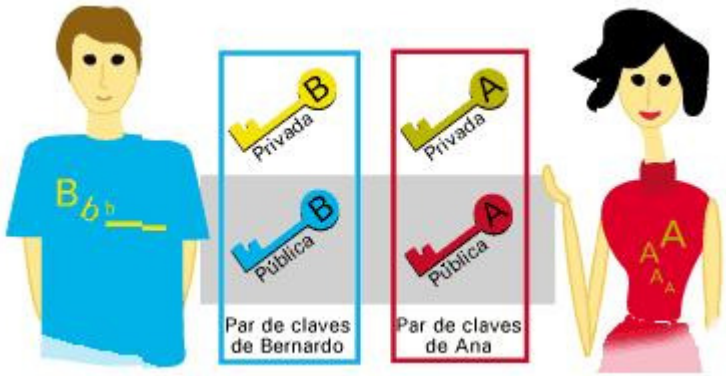
Firmar digitalmente ...???

CLAVE PÚBLICA

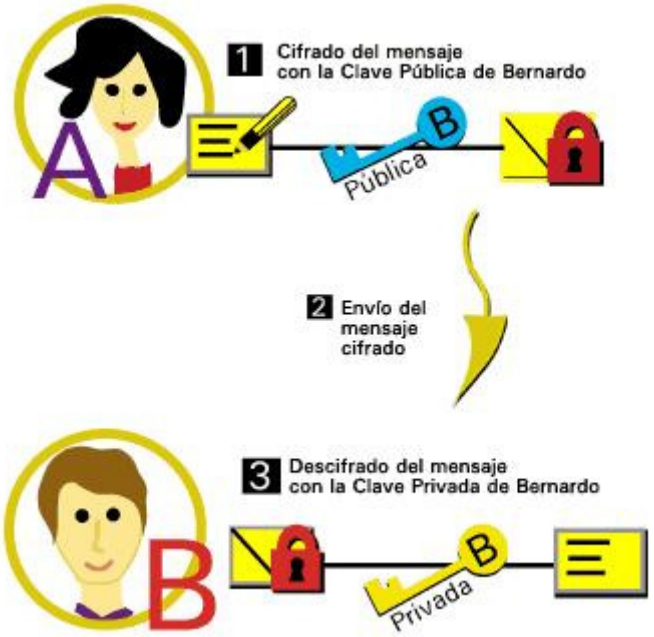


Aspectos tecnológicos

Cambiar la forma en que se implementan SERVICIOS DE SEGURIDAD ya definidos.



CLAVE PÚBLICA
Confidencialidad



Aspectos tecnológicos

Esto retomó la iniciativa sobre más y nuevos SERVICIOS DE SEGURIDAD.

El no repudio es un servicio de seguridad que permite probar la participación de las partes en una comunicación.

No repudio

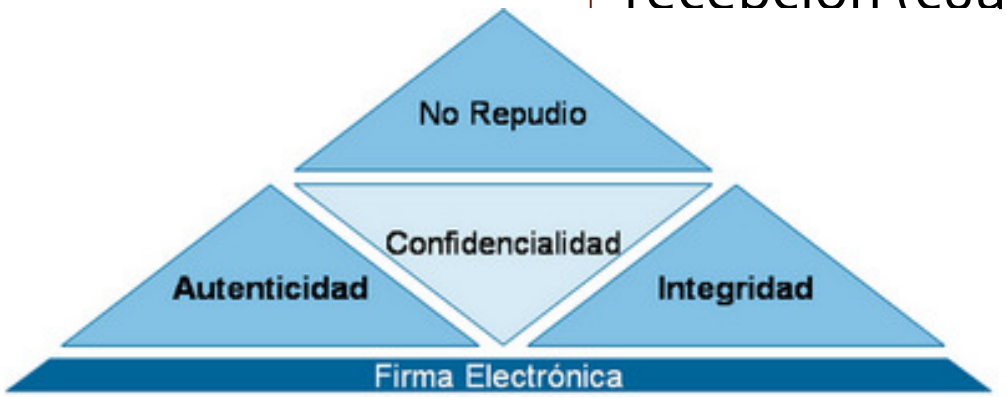
Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Aspectos tecnológicos

Una composición de SERVICIOS DE SEGURIDAD.

Firma Electrónica

Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo



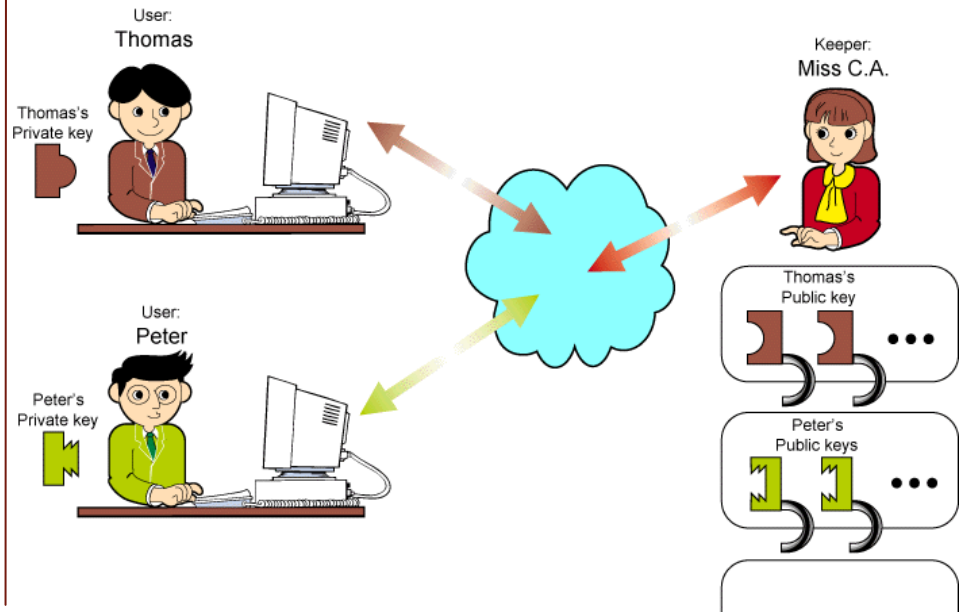
Aspectos tecnológicos

Quedó resuelto definitivamente el problema de Distribución de claves..?

NO..!!

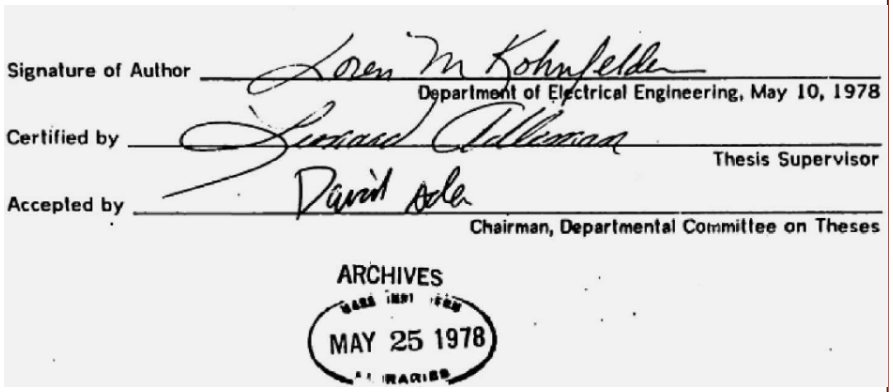
Ahora cuál clave hay que distribuir..??

DISTRIBUCIÓN DE CLAVES



Aspectos tecnológicos

Propuesta presentada por Kohnfelder, L. "*Towards a Practical Public-Key Cryptosystem*", Bachelor´s Thesis, MIT, 1978 [KOHN78].-


Signature of Author Department of Electrical Engineering, May 10, 1978

Certified by Thesis Supervisor

Accepted by Chairman, Departmental Committee on Theses

ARCHIVES

MAY 25 1978

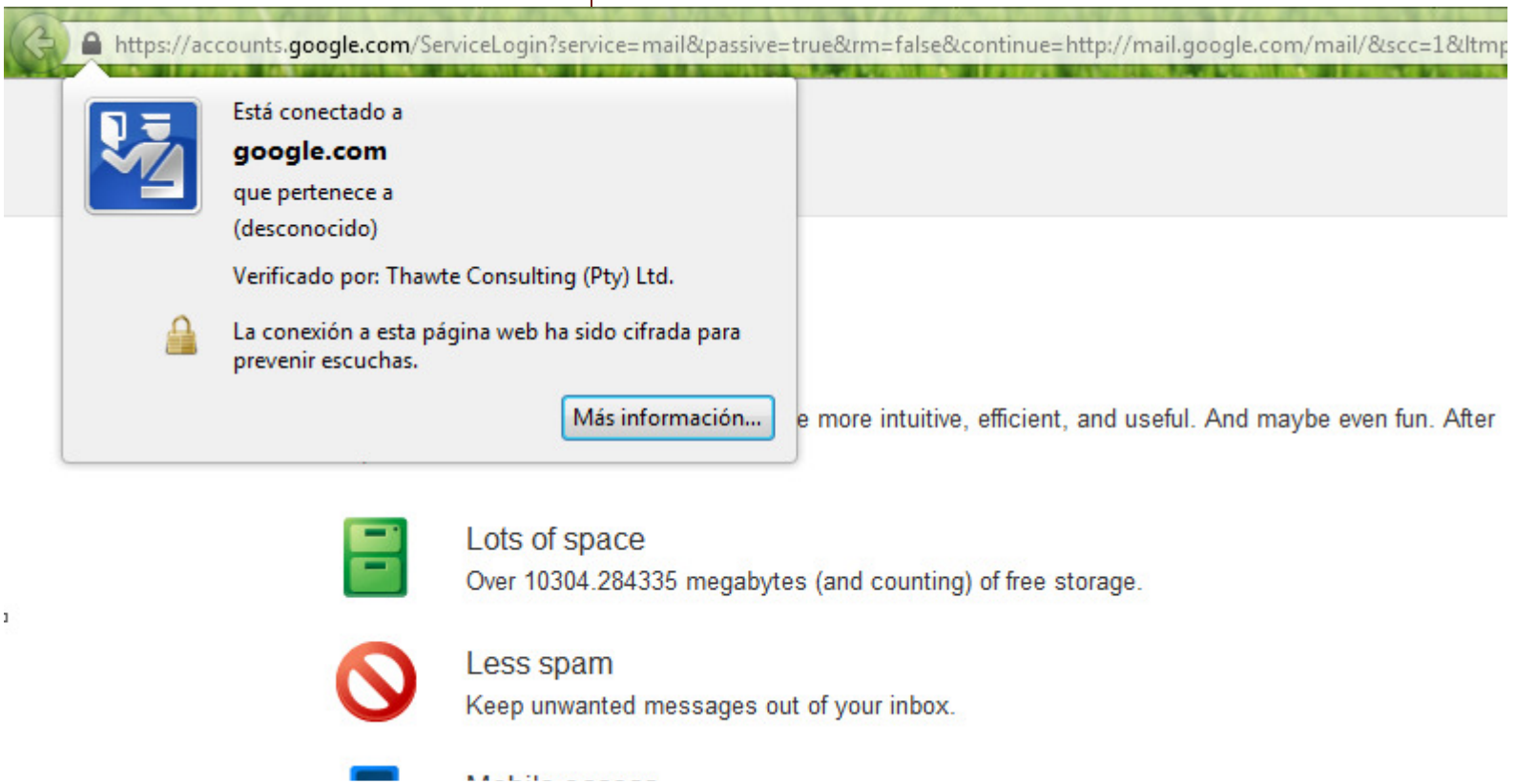
CERTIFICADO DIGITAL

```
Módulo (1024 bits):
d5 14 57 a0 96 40 9f 84 08 c6 66 8d ee ec e3 03
b2 66 85 ac 5d bb 1c ef 15 93 fd 1f 20 a7 10 49
24 5b 39 d2 60 c8 9a dc c0 ce 40 34 e6 59 95 b6
52 50 fe 08 25 45 57 73 5f 3a ed 5f df b6 5c 9d
8a 9c 62 fd 0f 61 be dc f6 87 1d 80 9d 7f 7c 17
13 77 64 3c 47 f3 87 24 1f 60 61 e0 81 11 46 e4
dc 50 5c 39 53 e6 68 3d 86 3c 55 87 c8 be fc 87
13 d9 5a aa 5d cc 3f 07 c1 74 cd c2 5e 27 16 11
```

Aspectos tecnológicos

Todos utilizamos CD de manera transparente, natural, sin darnos cuenta…!!

CERTIFICADO DIGITAL



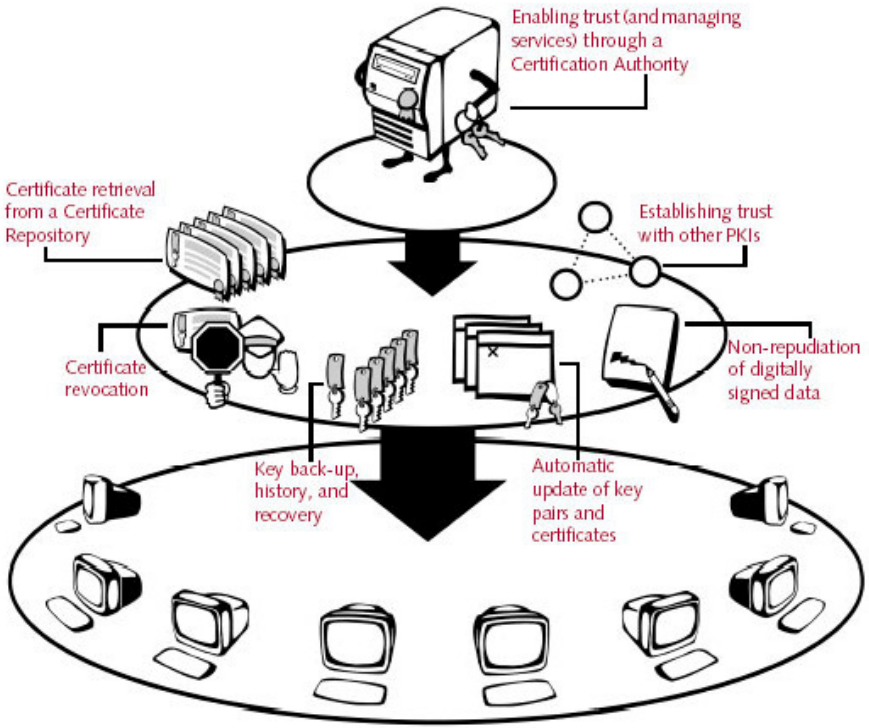
Aspectos tecnológicos

Componentes básicos

- ✓**AC:** Autoridad de Certificación
- ✓**AR:** Autoridad de Registro
- ✓Un repositorio
- ✓Un archivo histórico
- ✓**LCR:** Lista de Certificados Revocados
- ✓Usuarios de **CD**

Infraestructura de Firma Digital

Figure 1: Services implemented by a public-key infrastructure



All the above services are supported by client software, ensuring that users receive a usable, consistent, and transparent PKI.

Aspectos tecnológicos

Disponemos de una tecnología madura para brindar servicios de seguridad compuestos en una arquitectura de comunicaciones distribuida y numerosa.

Conclusión

ASPECTOS LEGALES

Antecedentes

La primera ley en material de Firma Digital en el mundo fue la denominada "Utah Digital Signature Act", publicada en 1995 en el Estado de Utah, en Estados Unidos.

Su objetivo fue facilitar las transacciones comerciales mediante mensajes electrónicos y firma digital.

Antecedentes

El Poder Ejecutivo Nacional de la República Argentina dispuso la creación de la Infraestructura de Firma Digital, aplicable al Sector Público Nacional, a través de la aprobación del Decreto Nº 427 del 16 de Abril de 1998.

La disposición establece la configuración de la siguiente estructura:

- Organismo Licenciante
- Organismo Auditante
- Autoridades Certificantes Licenciadas
- Suscriptores

Antecedentes

Dentro del marco creado por el Decreto Nº 427/98 , las funciones de Autoridad de Aplicación y de Organismo Licenciante son asumidas por la Subsecretaría de la Gestión Pública.

Es la Autoridad Certificante Raíz que emite certificados de clave pública a favor de aquellos organismos o dependencias del Sector Público Nacional que deseen actuar como Autoridades Certificantes Licenciadas, es decir como emisores de certificados de clave pública para sus funcionarios y agentes.

Antecedentes

LEY 25506 DE FIRMA DIGITAL

✓Sancionada el 14.11.2001.

✓Promulgada de hecho el 11.12.2001.

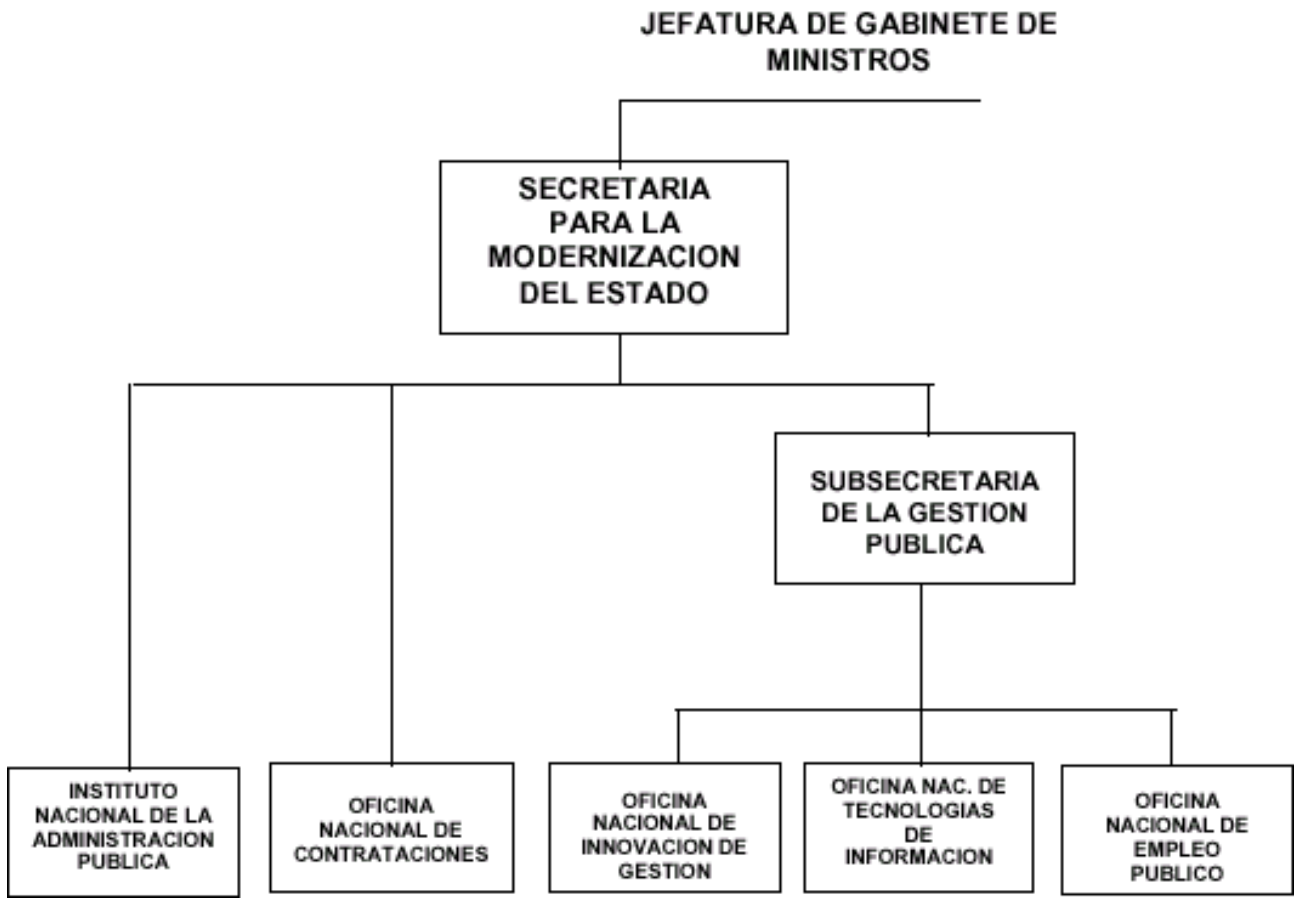
✓Publicada en boletín oficial el 14.12.2001.-

Antecedentes

Decreto 889/2001

2001

ANEXO I



Antecedentes

Decreto 2628/2002

Reglamenta Ley N° 25.506.

- ✓Consideraciones Generales.
- ✓Autoridad de Aplicación. Comisión Asesora para la Infraestructura de Firma Digital.
- ✓Ente Administrador de Firma Digital.
- ✓Sistema de Auditoría.

- ✓ Estándares Tecnológicos.
- ✓ Revocación de Certificados Digitales.
- ✓ Certificadores Licenciados.
- ✓ Autoridades de Registro.
- ✓ Disposiciones para la APN.

Antecedentes

Resolución SGP Nº 64/2007

ARTICULO 1º — Apruébanse los "Procedimientos Operativos para la Instalación y Puesta en Marcha de la Autoridad Certificante Raíz de la República Argentina"

Antecedentes

Resolución SGP N° 87/2008

Habilita a la ANSES para operar como Certificador Licenciado, habiéndose aprobado su Política de Certificación como Autoridad Certificante.

Resolución SGP N° 88/2008

Habilita a la AFIP para operar como Certificador Licenciado, habiéndose aprobado su Política de Certificación como Autoridad Certificante.

Antecedentes

Decreto 901/2009

Aprueba la nueva estructura organizativa de la Jefatura de Gabinete de Ministros y en particular, la de la Secretaría de la Gestión Pública.

En su punto Nº 21 establece la competencia de la Secretaría para actuar como autoridad de aplicación del Régimen Normativo de la Infraestructura de Firma Digital (Ley Nº 25.506)

como así también, en las funciones de ente licenciante de certificadores, supervisando su accionar.

Entre los objetivos de la nueva Subsecretaría de Tecnologías de Gestión, establece su función de Autoridad Certificante de Firma Digital para el SPN.

Antecedentes

Encode

Primer y único certificador licenciado del pais.

APLICACIONES

La FD está presente

- ✓ Home banking
- ✓ Servicios de correo electrónico
- ✓ Firma de documentos
- ✓ Firma de correo electrónico
- ✓ Comercio electrónico
- ✓ Voto Electrónico
- ✓ Sellado de tiempo
- ✓ Firma de SMS
- ✓ …

Conclusiones

Disponemos de una tecnología madura, un marco legal apropiado, iniciativas privadas y públicas, conocimiento y experiencia en las Universidades…

La propuesta es trabajar de manera conjunta para profundizar su aplicación en áreas conocidas y explorar nuevas áreas de aplicación desde las Universidades para el SPN.