Seguridad en Comercio Electrónico

Por: Elisa Mattos Lescano

Facultad de Ciencias Matemáticas

U.N.M.S.M.

Definición del problema

- Internet ha revolucionado la forma de hacer negocios.
- Brindar al usuario información acerca del entorno que gira alrededor del comercio electrónico
- Criterios para decidir el tipo de seguridad que se requiere

Seguridad Lógica

- Controles de Acceso
  - Identificación y Autentificación
  - Roles
  - Transacciones
  - Limitaciones a los Servicios
  - Modalidad de Acceso
  - Ubicación y Horario
  - Acceso Interno
  - Acceso Externo

Seguridad Organizacional/Operacional

- Recuperación de Desastres
- Seguridad Física
- Forénsica
- Educación y Documentación

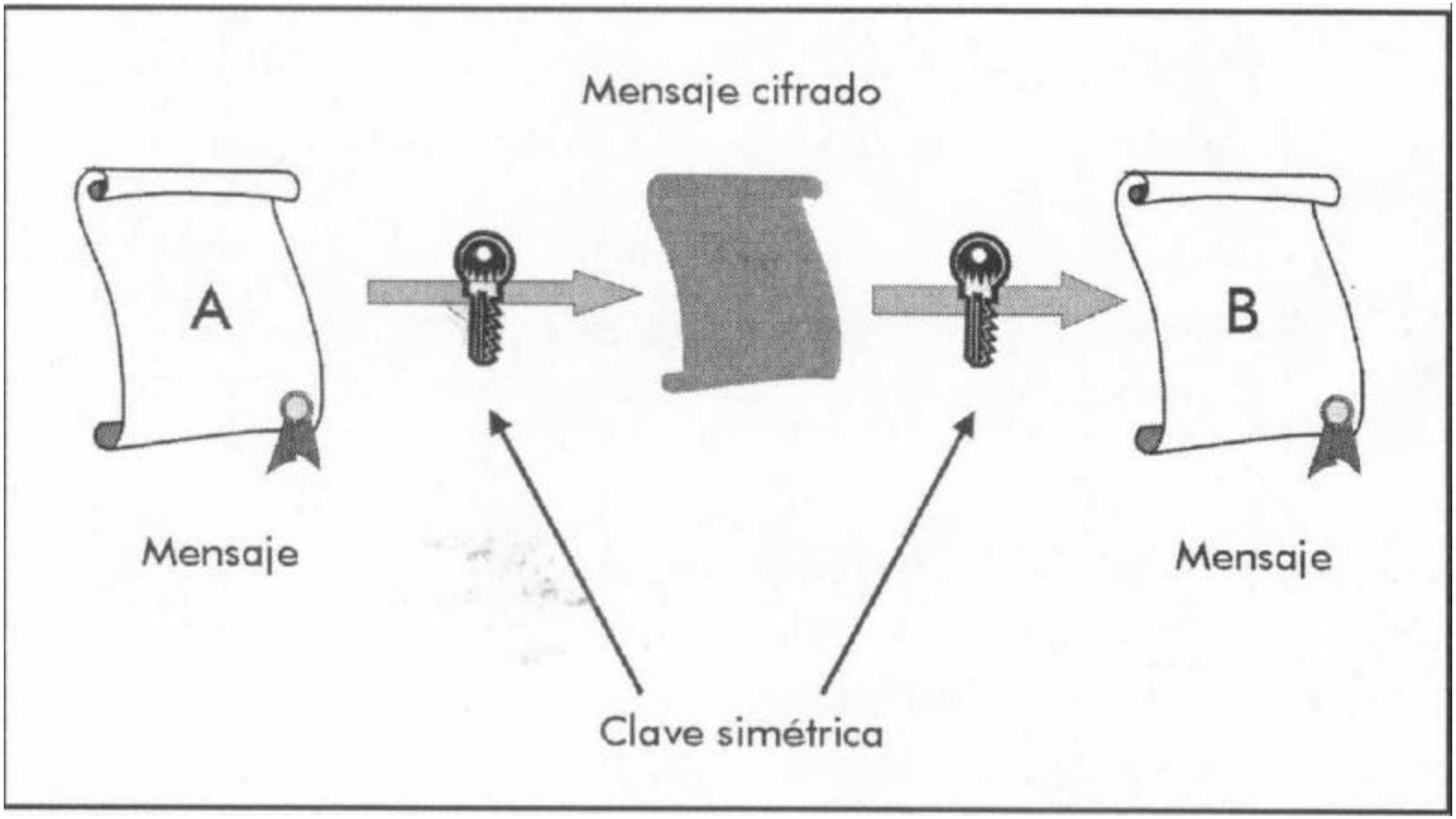
Criptología

- Criptografía
  - Simétrica
  - Asimétrica
  - Resumen
  - Firma Digital
  - Certificados Digitales
- Criptoanálisis

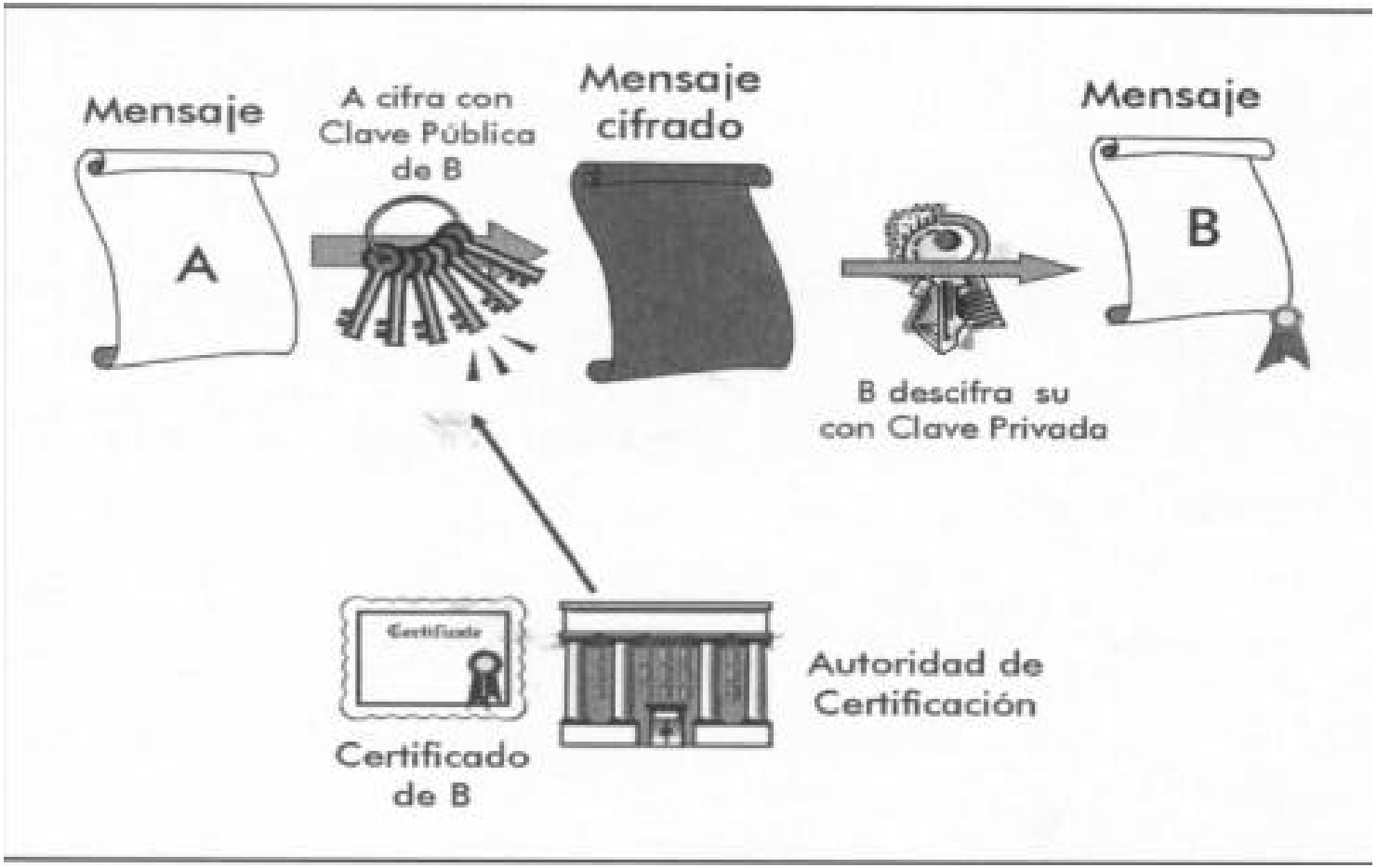
Clasificación de los Criptosistemas

- MÉTODOS DE CIFRA MODERNA
  - CIFRADO EN FLUJO
    - LFSRs A5
      - Telefonía móvil y tiempo real
  - CIFRADO EN BLOQUE
    - CLAVE PÚBLICA
      - EXPONENCIACIÓN
        - RSA , ELGAMAL
          - Intercambio de claves y firma digital
      - SUMA/PRODUCTO
        - CE, MOCHILAS
          - MH (Protección de SW vía HW)
    - CLAVE SECRETA
      - DES; T-DES; CAST; IDEA; RIJNDAEL ...
        - Cifrado propio de la información

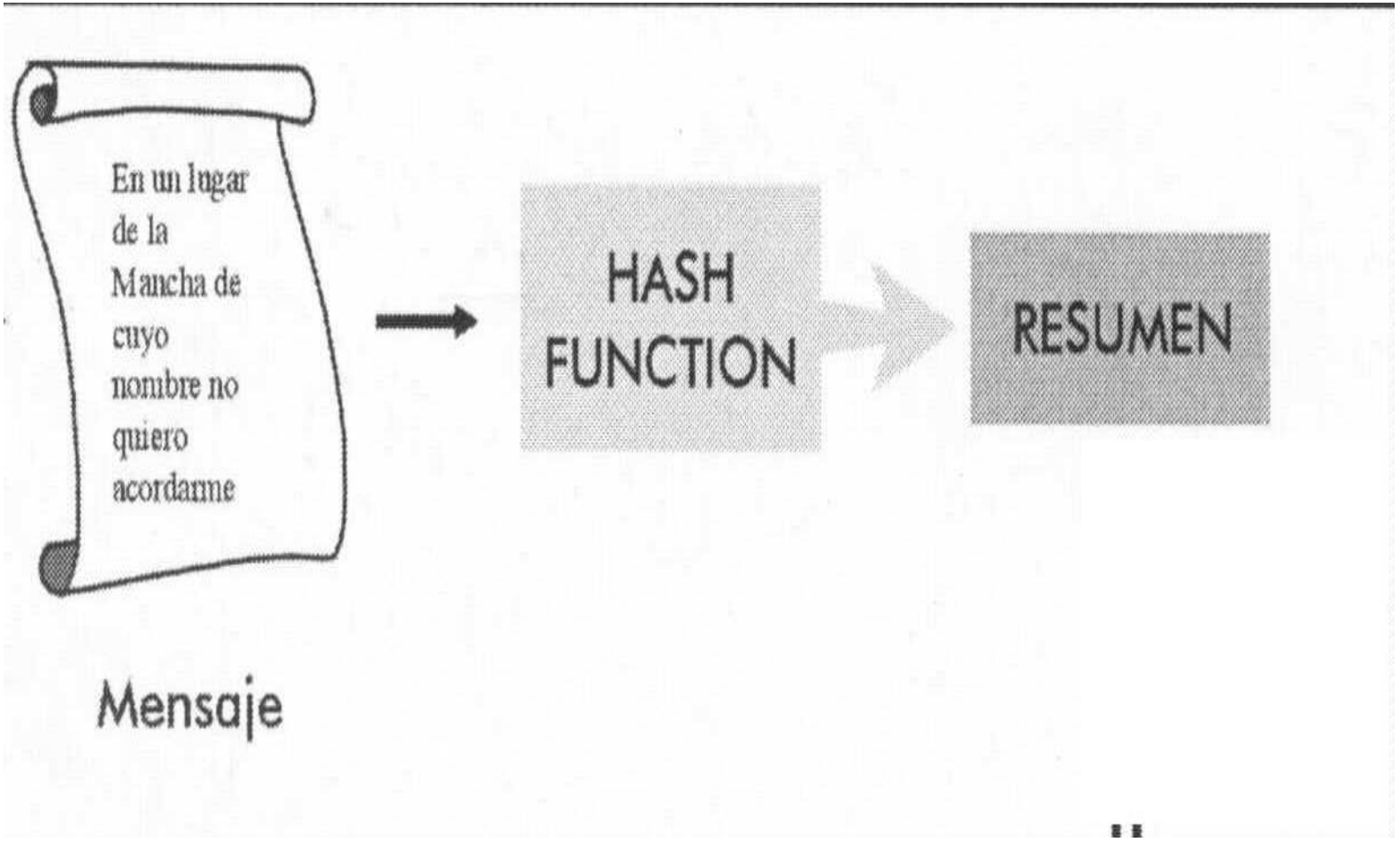
Criptografía Simétrica



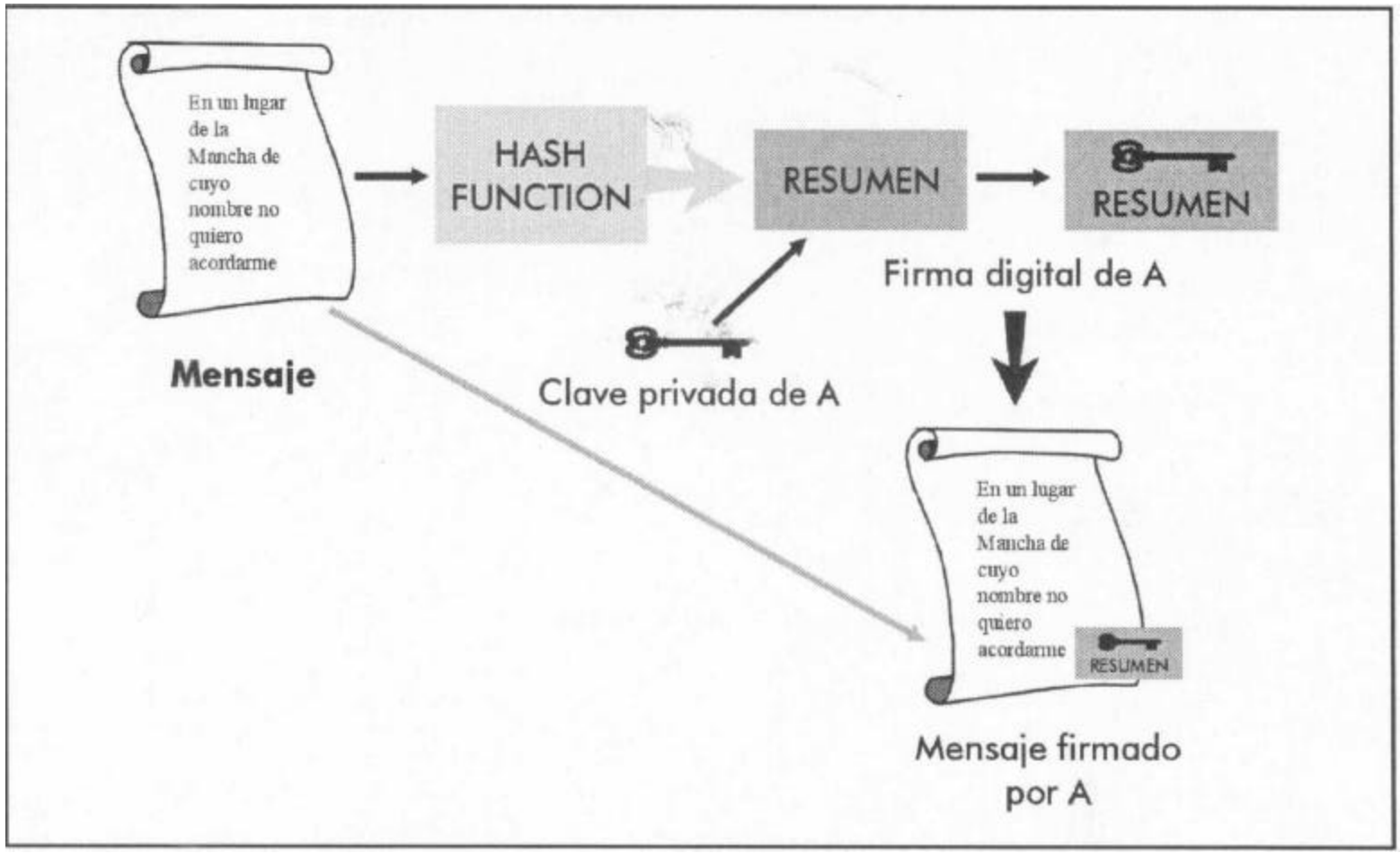
Criptografía Asimétrica



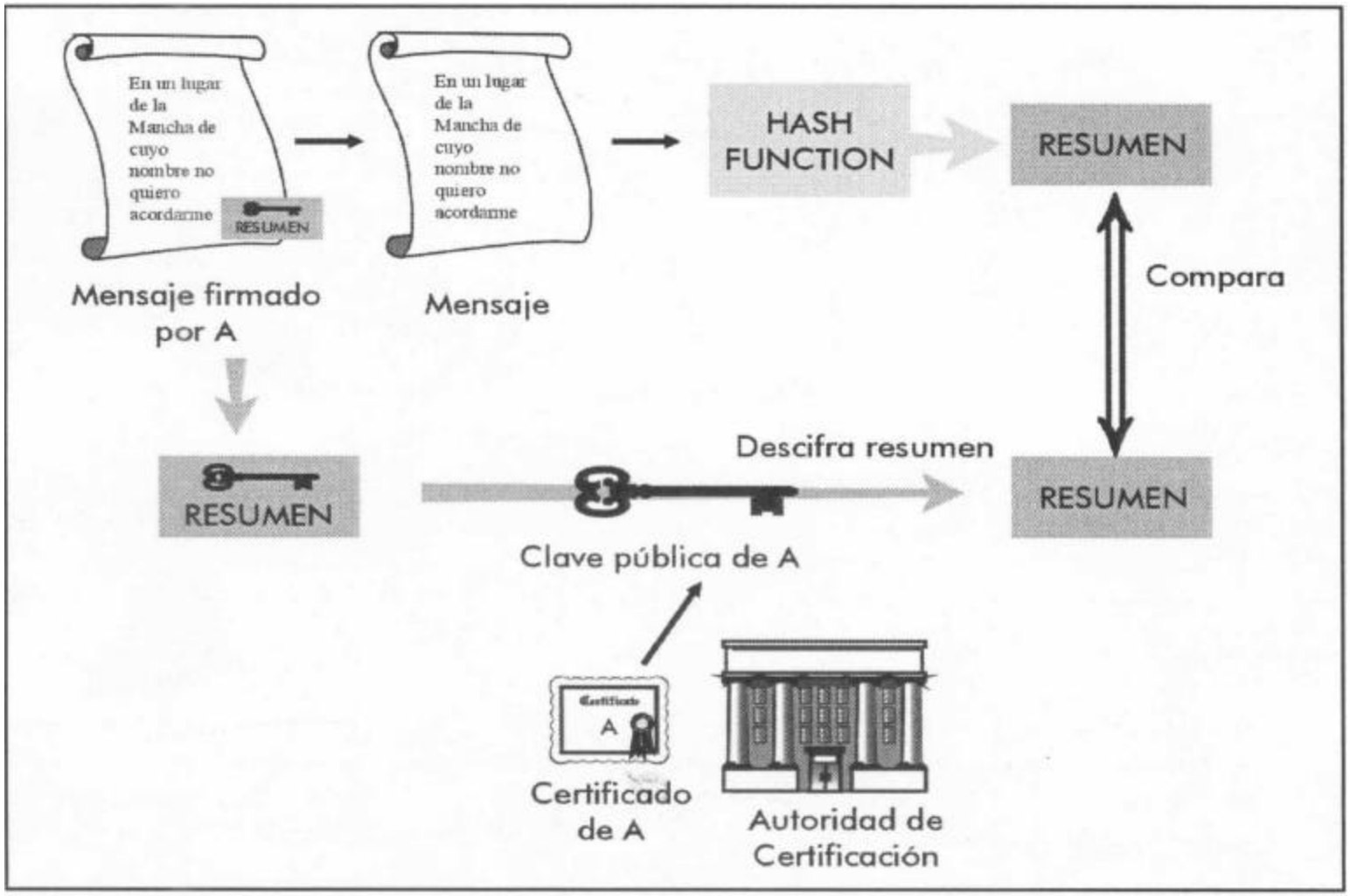
Criptografía de Resumen



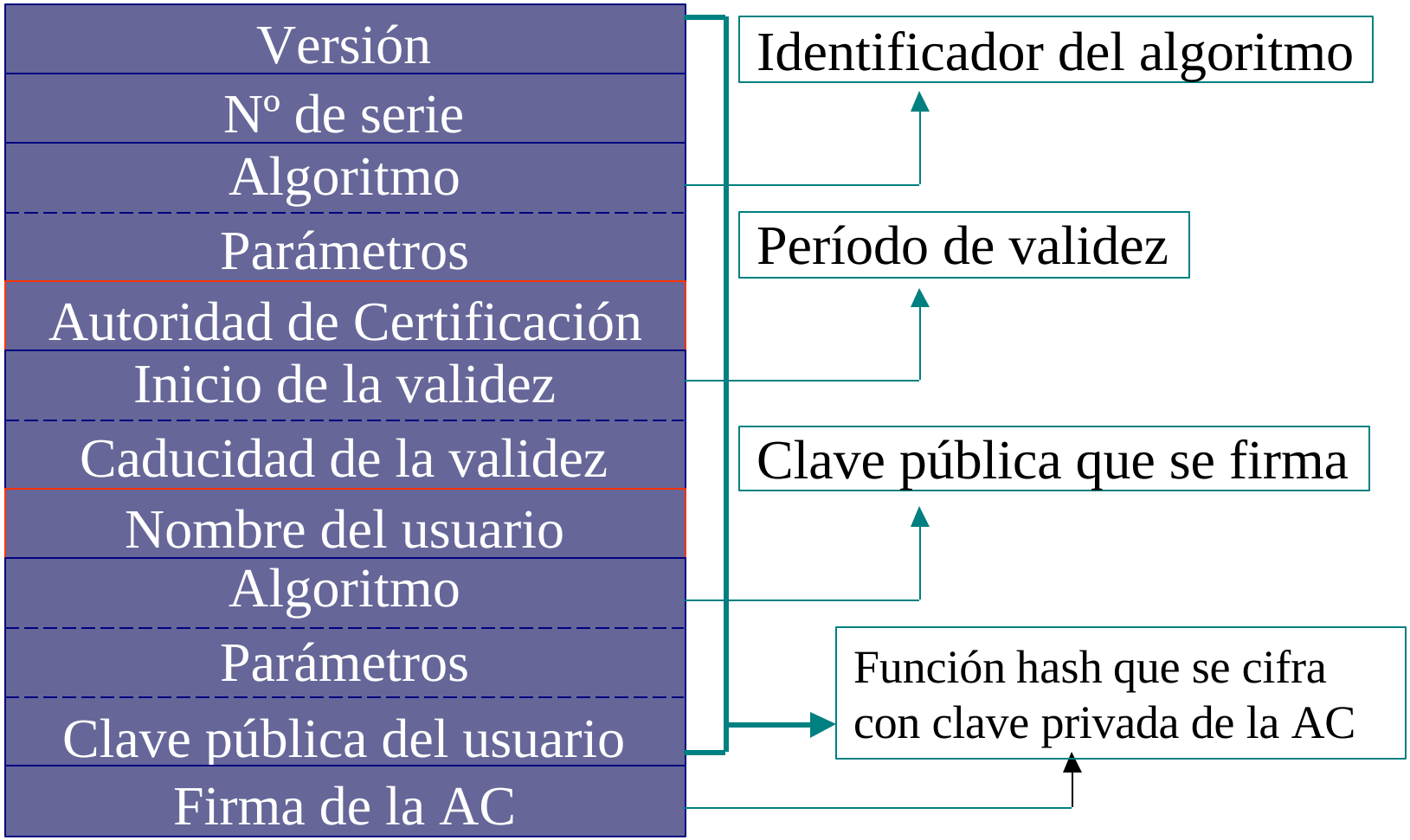
Firma Digital
Generación



Firma Digital
Comprobación



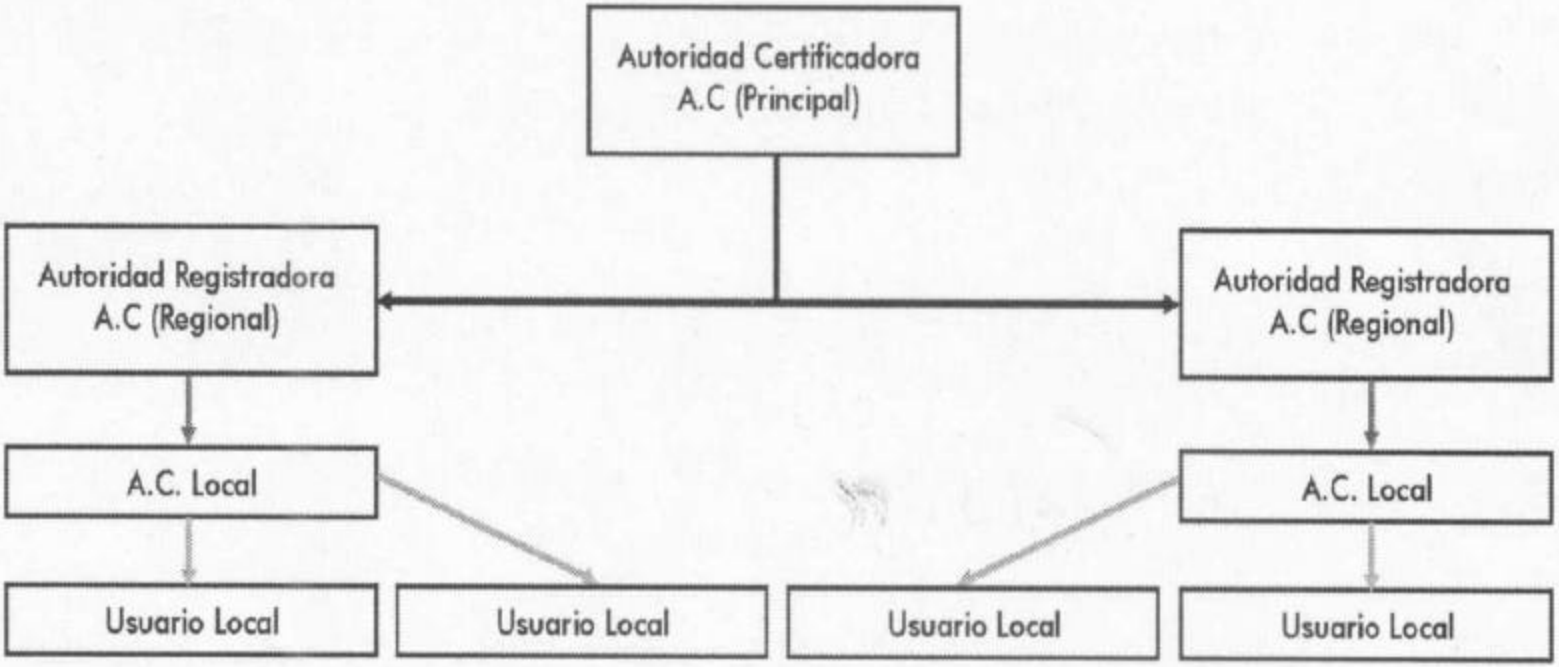
Certificados Digitales
Estándar X.509



Certificados Digitales

Estructura de una AC

Son entidades públicas o privadas cuya función es firmar los certificados digitales y mantener el estatus correcto



Certificados Digitales
PKI

- En una Infraestructura de Clave Pública, tendremos que definir y establecer todos los métodos necesarios para gestionar los certificados digitales de forma óptima. Principalmente, hay que establecer procedimientos para:
  - Emisión de certificados digitales.
  - Revocación de certificados digitales.
  - Consulta de certificados digitales.

Seguridad en Comunicaciones

OSI Vs TCP/IP

Niveles del Modelo OSI		Niveles TCP/IP
Aplicación		Aplicación
Presentación		
Sesión		
Transporte		TCP
Red		IP
Enlace de Datos		Enlace de Datos y Físico
Físico		

Seguridad en Nivel Aplicación

- Servicios
  - Mensajes Electrónicos
  - Pagos en Línea
- Protocolos
  - SET
  - SHTTP
  - S/MIME
  - MPTP

Seguridad en Nivel Transporte

- Servicios
  - Establecer conexión
  - Transferencia de Datos
  - Liberar conexión
- Protocolos
  - TLSP
  - SSL
  - WTLS

Seguridad en Nivel Red

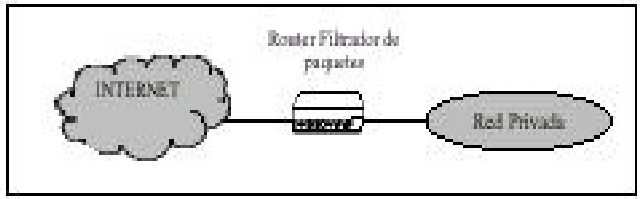
- Servicios
  - Interface de servicios común a subredes de diversa tecnología
  - Establecer ruta
- Protocolos
  - IPSEC

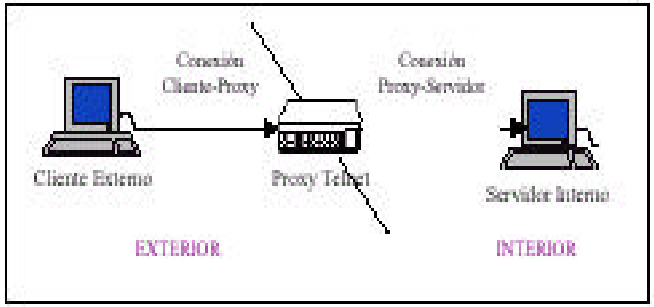
Seguridad en Infraestructura

- Firewalls
- Sistemas de Detección de Intrusos IDS
  - Basado en Host
  - Basado en Red

Tipos de Firewall

- A nivel de red
- A nivel de aplicación

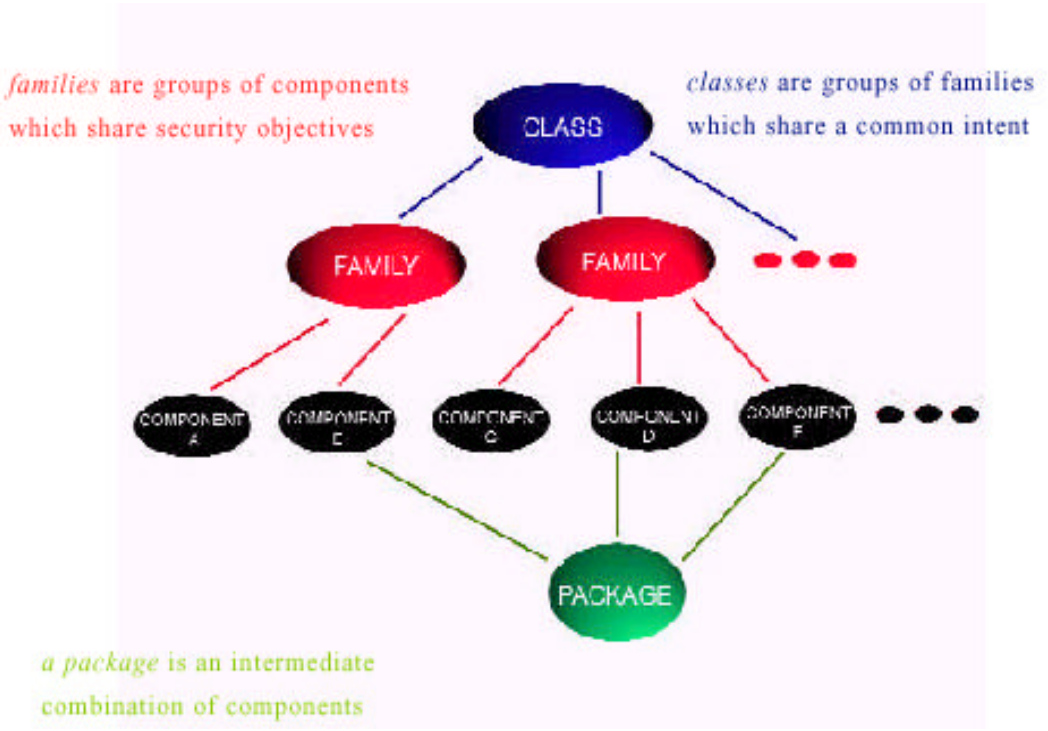




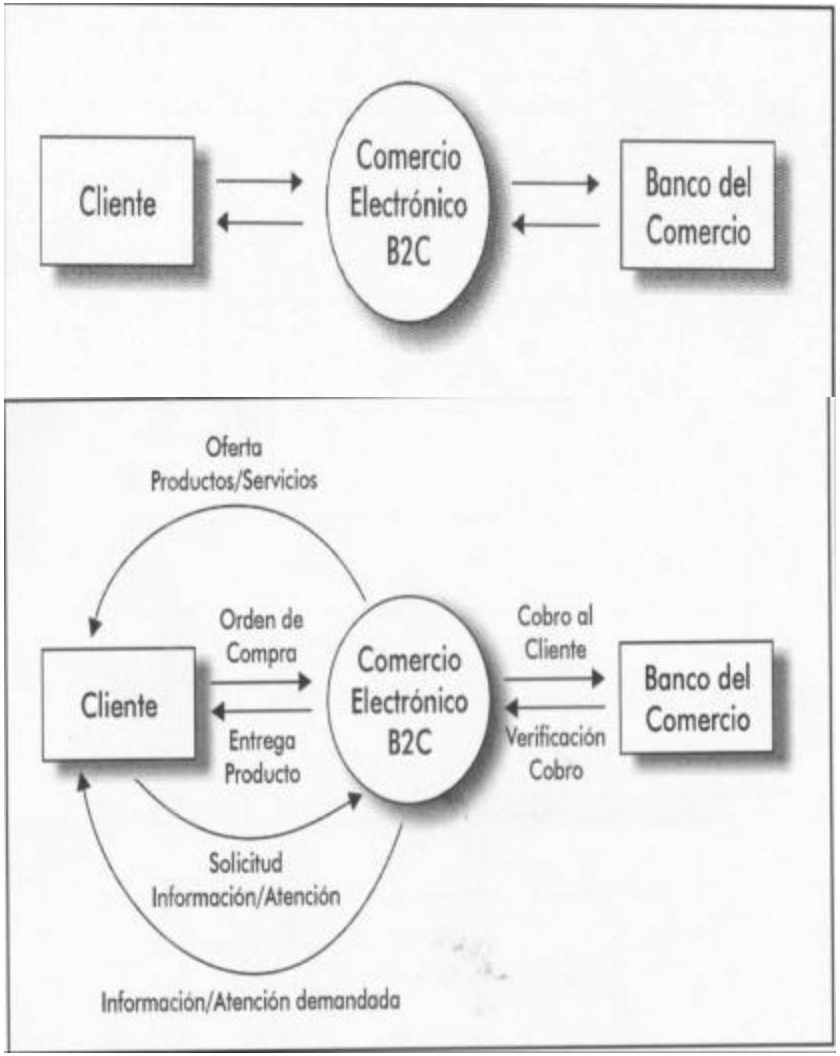
Niveles de Seguridad

- NIST
  - EAL1
  - EAL2
  - EAL3
  - EAL4
  - EAL5
  - EAL6
  - EAL7

Common Criteria



Comercio Electrónico



- Cualquier forma de transacción comercial en la que las partes interactúan electrónicamente en lugar de por intercambio o contacto físico directo.
- Ventajas:
  - Bajo costo de mercadotecnia
  - Alcance a nivel mundial
  - Reducción de costos de manejo y proceso de documentos y transacciones
  - Personalización
  - Mayor competencia y mejora en el servicio, etc.

Marco Legal

- Congreso de la República
  - Ley 27269 de Firmas Digitales
  - Ley 27419 Notificación por correo electrónico. Código Procesal Civil
  - Decreto Supermo 066-2001-PC. Lineamientos para promover masificación de acceso a Internet en el Perú
  - Ley 27291 Permite utilizar medios electrónicos para manifestar voluntad
  - Ley 27309 Incorpora delitos informáticos al Código Penal 15/07/2001

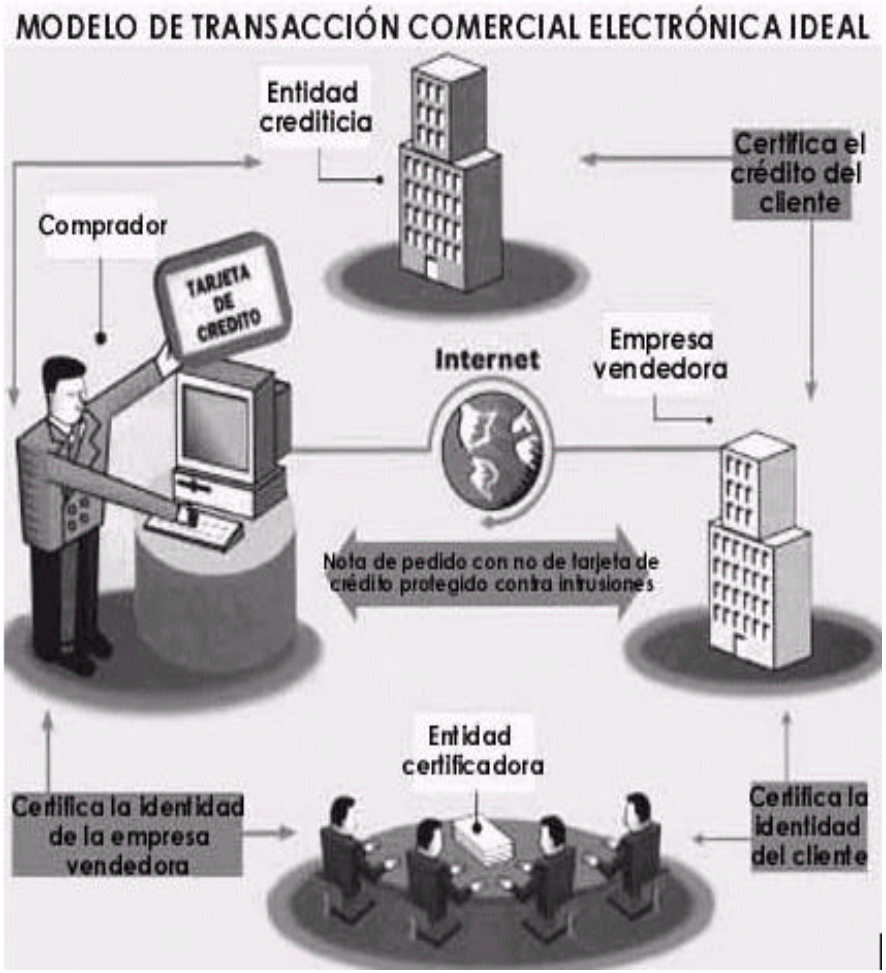
Marco Legal

- Indecopi
  - Código de Barras, especificaciones de simbología, descripción de formato
  - EDI. Mensaje de catálogo de precios/ventas
  - EDI. Mensaje de Información de Inventario
  - Formatos de Elementos de Intercambio de Información de fechas y tiempos

Marco Legal

- IPCE. Funciones
  - Liderazgo en propuestas de adaptación jurídica y normativa
  - Difusor de estrategias de mercadotecnia electrónica
  - Promotor de soluciones en e-commerce
  - Difusor de conocimientos

Contruyendo una Estructura confiable de E-commerce



- La solución incluye dos elementos esenciales, bajo la normatividad correspondiente:
  - Certificados para servidores
  - Sistema de pago seguro en línea

Conclusiones y Recomendaciones

- El impacto del comercio electrónico es arrollador en las empresas y en la sociedad
- Las instituciones bancarias son las que han realizado mayor avance en el comercio electrónico, priorizando el tema de seguridad.
- Es necesario un marco jurídico para las operaciones de comercio electrónico, puesto que la falta de normatividad origina diversos problemas, por ejemplo el pago de impuestos
- Poner en marcha los mecanismos legales aprobados a la fecha.
- Incluir en la normatividad referencia a estándares internacionales no sólo de certificación y de evaluación, también para la definición clara de la PKI nacional