



Retos actuales para la e-administración y el voto electrónico

Fernando A. Acero Martín

Abril 2008

GDFL, las imágenes son propiedad de sus autores.

ÍNDICE



- **Introducción a la firma**
 - Funciones de hash
 - Sistemas de clave pública
 - Concepto de certificado
- **Proceso de firma y verificación**
- **E-dni**
 - Problemas
 - Retos
 - Soluciones posibles
- **Voto electrónico**
 - Tipos de voto
 - Retos actuales
 - Firma homomórfica
 - Soluciones posibles
 - Experiencias

¿QUÉEN VIGILA A LOS VIGILANTES?

“¿Quis Custodiet Ipsos Custodes?”

Juvenal, circa 128 AD

INTRODUCCIÓN A LA FIRMA

ELEMENTOS BÁSICOS

HASH

ENCRIPCIÓN SIMÉTRICA / CLAVE PRIVADA

DES (Data Encryption Standard)

IDEA (International Data Encryption Algorithm)

AES (Advanced Encryption Standard)

SAFER

ENCRIPCIÓN ASIMÉTRICA / CLAVE PÚBLICA

RSA (Rivest, Shamir and Adleman)

PGP (Pretty Good Privacy)

CLAVE
PRIVADA

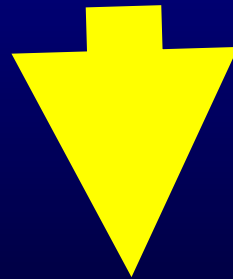
CRIPTOGRAFIA

CLAVE
PÚBLICA

CONCEPTO DE HASH

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus fermentum laoreet augue. Etiam leo. Curabitur eget leo. Duis wisi. In in felis. Phasellus consequat, massa luctus congue suscipit...

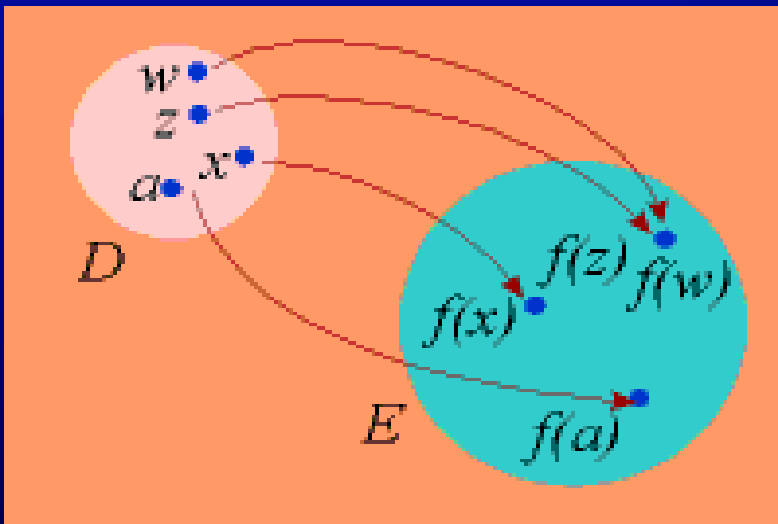
LONGITUD ARBITRARIA



LONGITUD FIJA
hash / fingerprint / digest

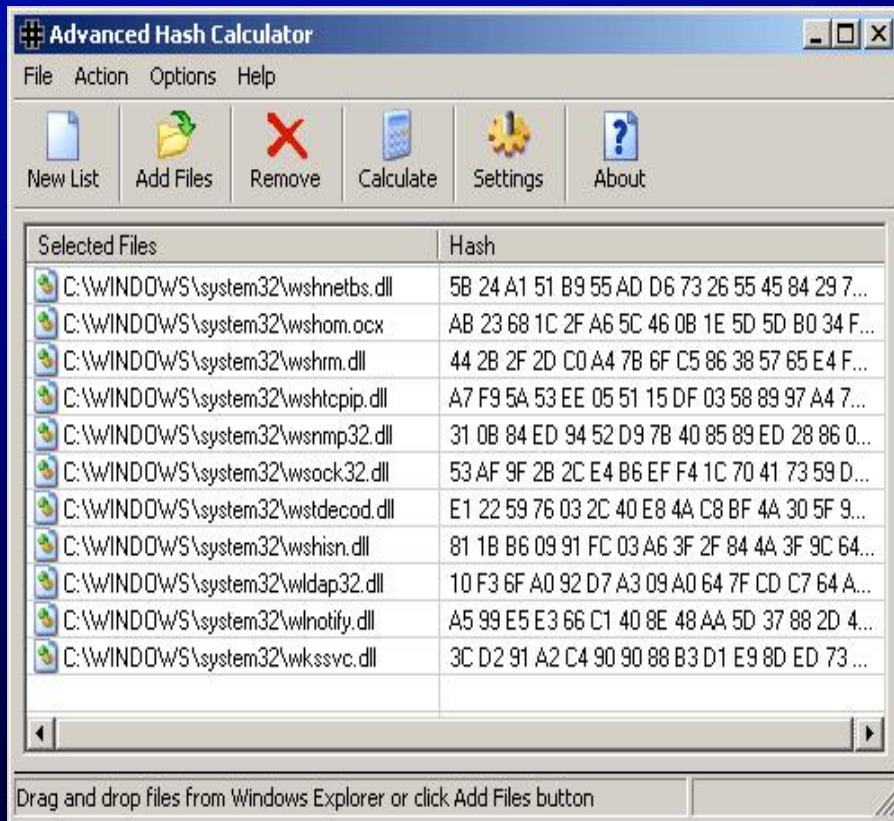
DE70 5273 550F 8BFF DBB6 F674 45CA 8E2A

CARACTERÍSTICAS / CONSECUENCIAS



- Cambio de un bit \Rightarrow cambio de varios bits.
- Habrá necesariamente varios mensajes que compartan en el mismo código de hash. (Colisiones)
- Dificultad para encontrarlos \Rightarrow tamaño del hash \Rightarrow Coste/Eficacia
- Facilidad de cálculo.
- Resistencias:
 - Colisiones.
 - Preimagen.
 - 2ª preimagen.

USOS DEL HASH



- **“NAVAJA SUIZA”** criptográfica.
- **Identificación de mensajes.**
- **Comprobación de modificaciones y errores**
- **Intercambio de claves.**
- **Firma electrónica de mensajes y claves.**
- **Páginas web seguras.**
- **El 99% de los servicios telemáticos las usan.**
- **Nuestra seguridad nacional depende de estas funciones.**

SHA-1

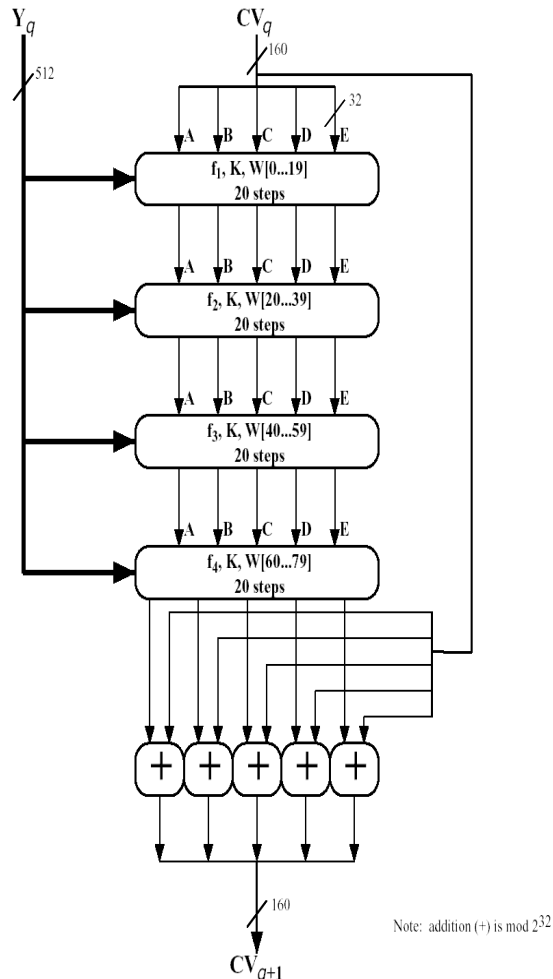
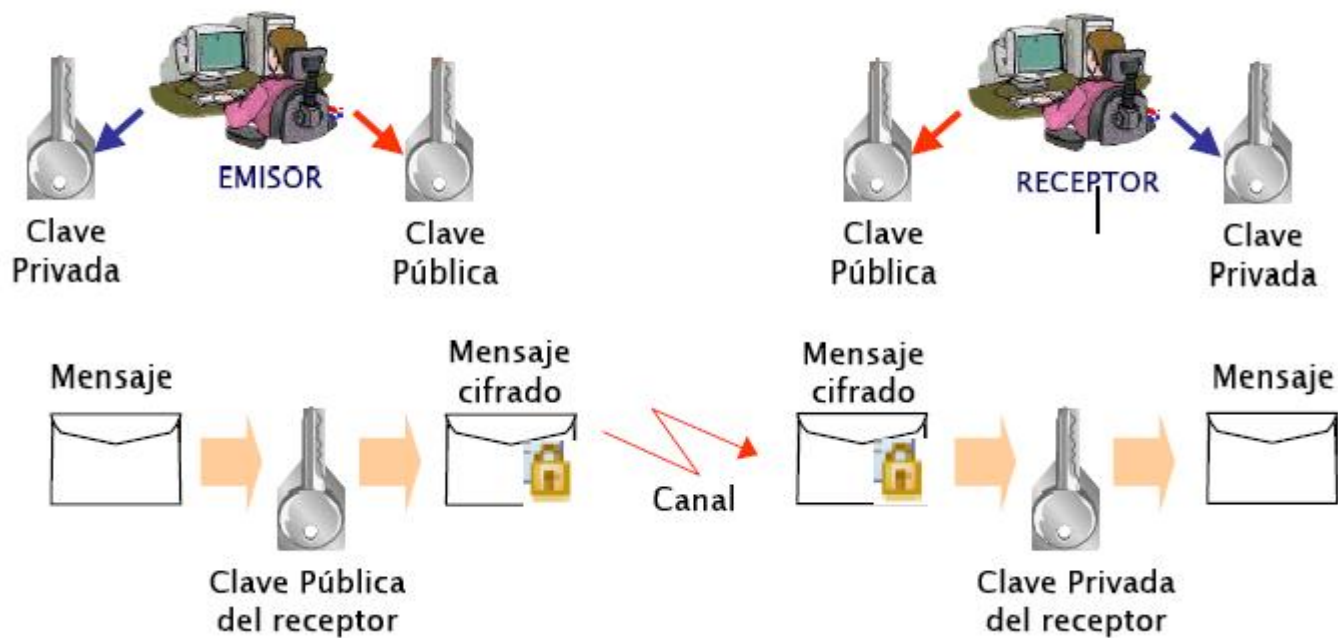


Figure 9.5 SHA-1 Processing of a Single 512-bit Block (SHA-1 Compression Function)

- Diseñado por la NSA, evolución del SHA-0 hace 10 años. SHS (Secure Hash Standard).
- Monocultura SHA-1/MD5/RIPEMD
- 160 bits para mensaje máximo de 2^{64} bits.
- Resistencias:
 - Preimagen $O(2^{160})$. Dado hash no se puede encontrar un mensaje con el mismo hash.
 - Segunda preimagen. Dado un mensaje no se puede encontrar otro con el mismo hash.
 - Colisión $O(2^{80})$. No se pueden encontrar dos mensajes distintos que den el mismo hash.
- SHA-2 (Set-2) 224, 384, 512 bits.

CIFRADO ASIMÉTRICO RSA

Cifrado Asimétrico o de Clave Pública



CIFRADO ASIMÉTRICO RSA

- **Dos claves, una pública y otra privada por usuario. Una invierte el efecto de la otra.**
- **Para cifrar un mensaje se necesita tener su clave pública.**
- **Para descifrar el mensaje se necesita la clave privada.**
- **Para general firmas digitales se necesita la clave privada.**
- **Para verificar firmas digitales se necesita la clave pública.**
- **Sistemas basados funciones de un único sentido:**
 - **Números primos (cuestionados).**
 - **Curvas elípticas (futuro cercano).**

CONCEPTO DE CERTIFICADO



La Clave Pública del Certificado la difunde la AC



Autoridad de Certificación



TERCERO

Un tercero puede comprobar si los datos del certificado han sido alterados respecto a los firmados por la AC

CONFIAR EN LA AUTORIDAD DE CERTIFICACIÓN SUPONE CONFIAR EN LOS DATOS DEL CERTIFICADO

CONCEPTO DE CERTIFICADO

Certificados Digitales:

- Representan identificadores unívocos de una persona en Internet.
- La regulación de la firma conecta directamente con este concepto: la firma debe basarse en certificado.
- Los certificados permiten diversos usos:
 - Permiten la identificación de las personas en Internet.
 - Sirven para evitar la retrocesión y garantizan el “no repudio”.
 - Ofrecen soporte a la firma electrónica con reconocimiento jurídico.
 - Permiten el envío de mensajes cifrados al suscriptor.
 - Permiten ser usados como mecanismo de acceso (como “llave”).

CONCEPTO DE FIRMA

Firma Electrónica:

- **Herramienta de seguridad basada en la criptografía asimétrica o de Clave Pública.**
- **Algoritmo de cifrado RSA y con claves típicamente de 1024 o 2048 bits.**
- **Estándares ampliamente difundidos (X509 v3) PKCS #10 y PKCS #11.**
- **Marco regulatorio sólido en EEUU y la Unión Europea.**
- **Se asocian inequívocamente a una persona.**
- **Si cumple ciertas propiedades es equivalente a la firma manuscrita.**
- **Es considerada la herramienta clave para aportar la seguridad necesaria en la red.**
- **Además de la Firma de mensajes, tiene otras importantes aplicaciones: autenticación, mecanismo de acceso, desarrollo de código seguro, etc.**

PROCESO DE FIRMA Y VERIFICACIÓN

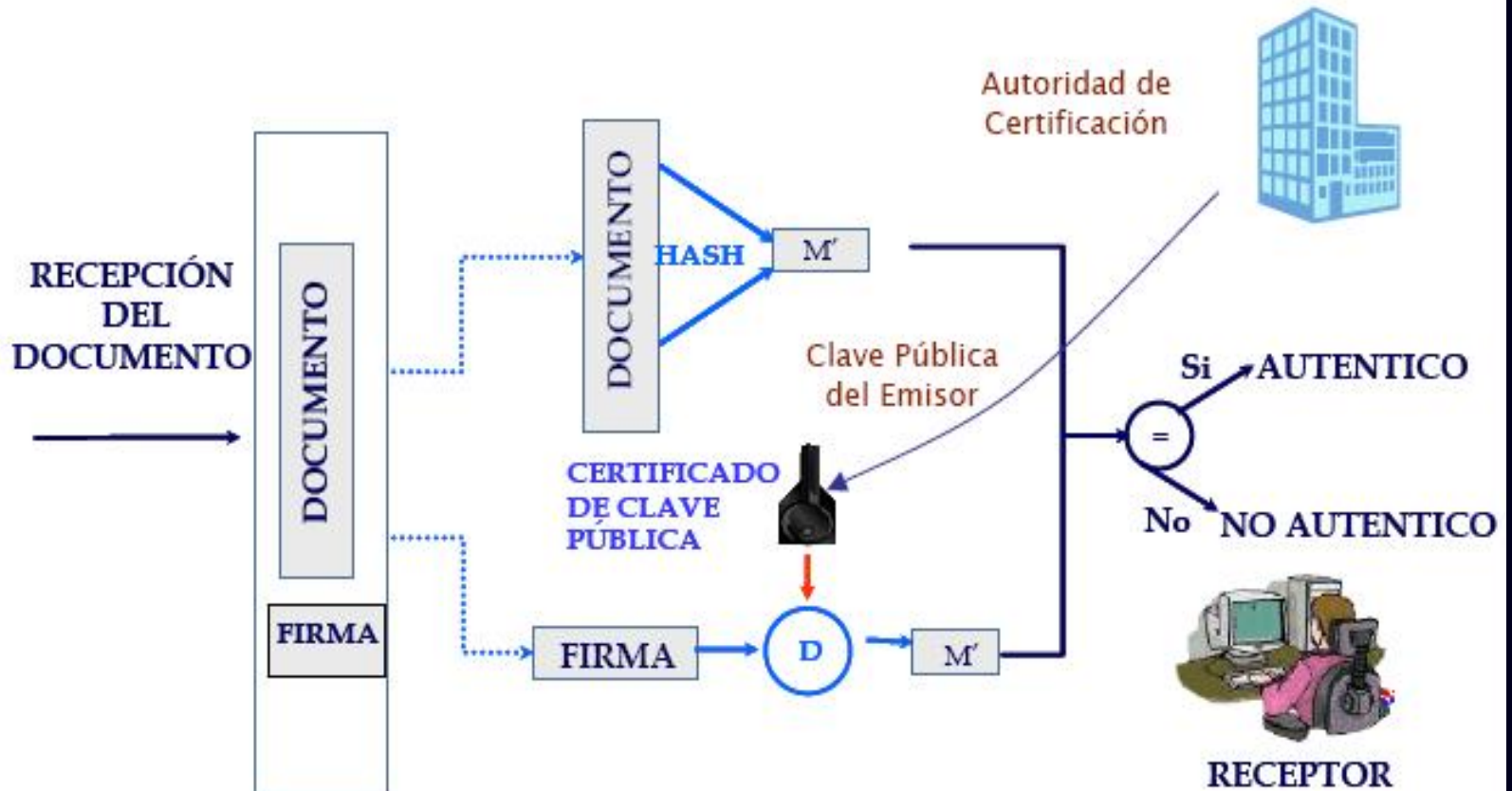
PROCESO DE FIRMA DIGITAL



Generación de una Firma Electrónica:

1. Se toma el documento y se calcula un resumen digital con una función llamada (hash SHA Secure Hash Algorithm).
2. Se emplea la Clave Privada del Certificado para cifrar el resumen.
3. Al resultado, se almacena junto con el Documento original en una estructura de datos.
4. Se envía al destinatario, junto al documento o asociada al mismo, a través de un canal.
5. Cuidado con los metadatos y determinados formatos.

VERIFICACIÓN DE FIRMA




VERIFICACIÓN DE FIRMA

- **Proceso de verificación de la firma:**
- **Se recibe el documento y la firma electrónica.**
- **Se extrae la firma digital.**
- **Se toma el documento y se calcula un nuevo resumen.**
- **Se toma el resumen, se toma la firma digital y la clave pública del firmante y se ejecuta una función matemática, que indica si la firma es correcta.**

E-DNI

CONTENIDO

 **Descripción física del DNI electrónico**

El nuevo Documento Nacional de Identidad dispondrá de un Chip electrónico en el que se registrarán los datos del titular:

- Datos de filiación del titular
- Imagen digitalizada de la fotografía
- Imagen digitalizada de la firma manuscrita
- Plantilla de la impresión dactilar
- Certificado reconocido de autenticación y de firma
- Certificado electrónico de la autoridad emisora
- Par de claves de cada certificado electrónico

El Documento Nacional de Identidad recogerá gráficamente los siguientes datos:

- Apellidos y nombre
- Fecha de nacimiento
- Sexo
- Nacionalidad

Número de serie del soporte

Kinegrama

Posee una fotografía blanco y negro con un holograma en la

Relieves

Firma manuscrita del

Equipo de expedición

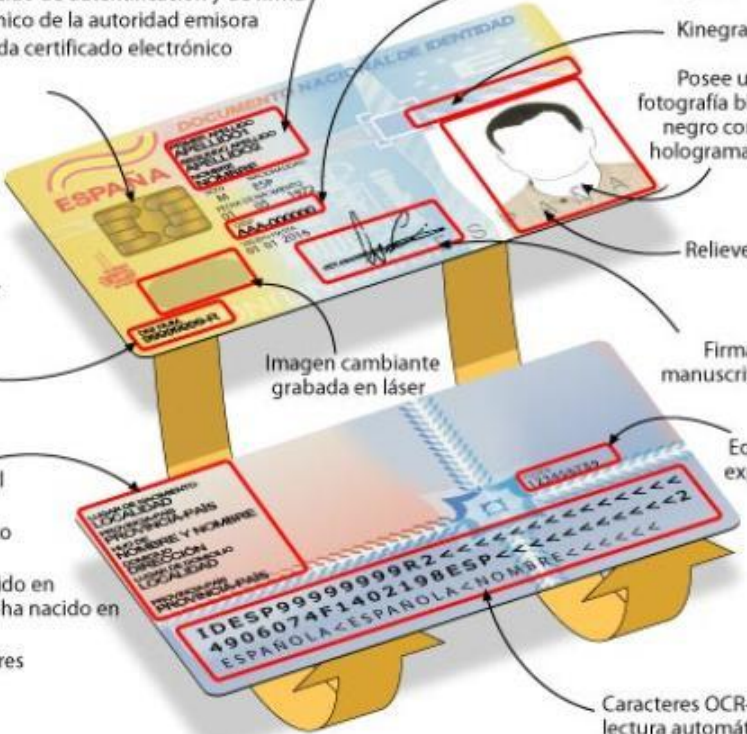
Imagen cambiante grabada en láser

Número personal de Documento Nacional de Identidad y carácter de verificación

Datos de filiación del titular:

- Lugar de nacimiento (localidad)
- Provincia (si ha nacido en España) o Nación (si ha nacido en el extranjero)
- Nombre de los padres
- Domicilio
- Provincia
- Nación

Caracteres OCR-B de lectura automática



El diagrama muestra un DNI electrónico con un chip de identificación. Se detallan los campos de datos personales como 'NOMBRE Y APELLIDOS', 'FECHA DE NACIMIENTO', 'SEXO' y 'NACIONALIDAD'. También se muestra la 'FOTOGRAFÍA' con un holograma, la 'FIRMA MANUSCRITA' y el 'NÚMERO PERSONAL DE DOCUMENTO NACIONAL DE IDENTIDAD'. Se mencionan características físicas como 'RELIEVES' y 'IMAGEN CAMBIANTE GRABADA EN LÁSER'. El chip contiene un 'PAR DE CLAVES' y un 'CERTIFICADO ELECTRÓNICO'. El documento incluye un 'KINEGRAMA' y un 'EQUIPO DE EXPEDICIÓN'.

- **2 CERTIFICADOS RSA 1024 bits (autenticación / cifrado de comunicaciones y firma).**
- **FIRMA SHA-1 / SHA-256**
- **FILIACIÓN**
- **FOTO**
- **HUELLA**
- **FIRMA**
- **CERTIFICADO RAÍZ EMISOR**

PROBLEMAS

- **RSA 1024 basado en factorización de números primos. Avances de Hugo Scolnik y otros, recomiendan el uso de curvas elípticas.**
- **SHA-1 en proceso de búsqueda de colisiones.**
- **No dispone de algoritmos específicos para voto electrónico.**
- **Si el sistema está comprometido, no hay garantías de lo que se firma. (entorno seguro de firma / conocimiento de los usuarios).**
- **Demasiado complicado de cambiar en caso de fallo del sistema criptográfico (lentitud en el despliegue / falta de alternativas en el mercado / coste de implantación).**
- **El problema de la seguridad por oscurantismo - > soporte complicado.**
- **No es trivial su uso e instalación en los sistemas.**
- **Compatibilidad con sistemas operativos (Ley 11/2007 31DIC09).**
- **Contenedor único, certificados públicos encerrados, contraseña única para todo.**

RETOS



- La seguridad y concienciación del usuario.
- Evaluación de riesgos.
- El soporte de versiones y sistemas operativos.
- La certificación de hardware y sus controladores.
- Mantener al día la tecnología.
- Facilitar la instalación y configuración.
- Soporte de aplicaciones.
- Soporte del voto electrónico.
- Legislación no posibilista insuficiente (Custodia Digital).

ALGUNAS SOLUCIONES INMEDIATAS

- **Entorno seguro de firma**
 - Basado en tecnología “live”.
 - Es certificable Common Criteria EAL.
 - Puede contener operativas certificadas (bancos, administración, etc).
 - Puede contener controladores hard certificados.
 - Garantiza la integridad del sistema.
 - Garantiza el acceso a la e-firma con solamente configurar la red.
 - Proporciona una alternativa al problema del soporte de sistemas operativos / controladores.
 - Aplicaciones configuradas para firma de documentos y acceso a servicios.
- **Soporte**
 - Crear un wrapper / librerías que permitan la compilación local bajo cualquier sistema operativo del código propietario.
 - Preinstalación de certificados raíz y controladores.

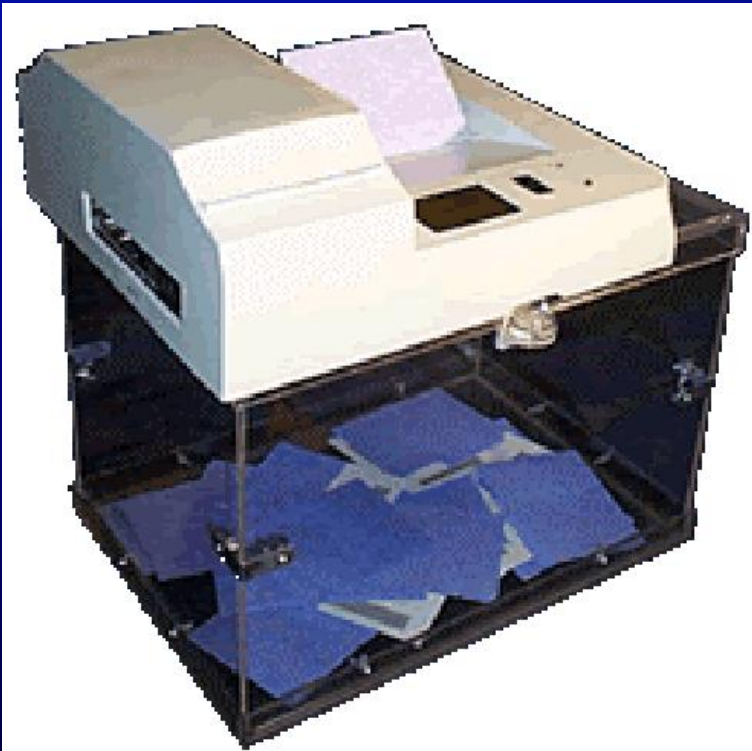
VOTO ELECTRÓNICO

LA TECNOLOGÍA EN NUESTRAS VIDAS

“La tecnología no es buena ni mala, pero tampoco es neutral”.

Melvin Kranzberg

CONCEPTO DISPERSO

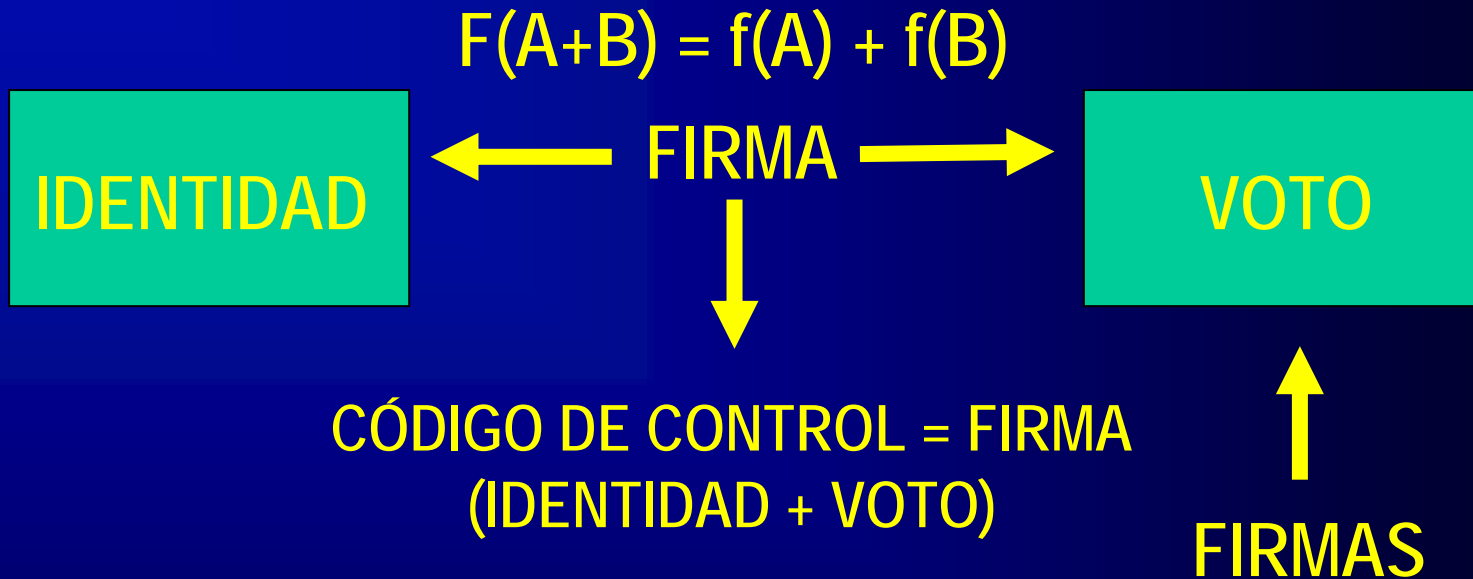


- **Voto directo desde ordenador conectado a Internet.**
- **Urna electrónica en sus distintas variantes.**
- **Asistentes de recuento de voto.**
- **Transmisión telemática de resultados.**

RETOS ACTUALES

- **Voto no presencial electrónico:**
 - Coacciones y amenazas -> voto modificable
 - Desvinculación del voto de la identidad -> Homomórfica $f(A) + f(B) = f(A+B)$.
 - Seguridad del entorno de voto.
- **Voto presencial electrónico.**
 - Desvinculación del voto de la identidad (orden natural).
 - Transparencia.
 - Verificación del proceso -> papeleta de control.
- **Legislación (no solamente posibilista).**
- **La mejor tecnología posible, no la mejor de las disponibles (sin mucha fe en este aspecto).**
- **No renunciar a garantías -> buscar solución.**
- **¿Quién certifica los sistemas?**
- **¿Vale la pena tanto esfuerzo? ¿qué se gana con ello?**
- **La brecha democrática / democracia participativa.**

FIRMA HOMOMÓRFICA



GUARDO MI IDENTIDAD
FIRMADA Y LUEGO PUEDO
COMPROBAR QUE MI VOTO
FIRMADO ESTA EN LA URNA Y
CONTABILIZADO, SIN
COMPROMETER MI IDENTIDAD

ALGUNAS SOLUCIONES

- **Arquitectura y software abiertos (opción de Brasil).**
- **Sistemas de cifrado y firma diseñados específicamente para el voto.**
- **Mantener la cadena de control y verificación.**
- **No sucumbir a la oferta de sistemas sin estudiar a fondo sus pros y contras.**
- **Tener en cuenta el déficit democrático ¿vale la pena? ¿cómo afectará a la democracia?.**
- **Transparencia en todo el proceso, desde la elección de la tecnología a la implantación.**

ALGUNAS EXPERIENCIAS

- **EEUU**
 - Problemas y polémicas (calibración de pantallas táctiles, sistema de auditoría, sistemas propietarios, papeletas complicadas).
- **Brasil**
 - Problemas de auditoria y sistemas propietarios.
- **Estonia**
 - Uno de los países más avanzados, se puede votar desde casa y cambiar el voto, el presencial anula los electrónicos.
- **India**
 - Activo desde 1996, máquinas en colegios, problemas de transparencia.
- **Bélgica**
 - Tarjeta magnética y bolígrafo electrónico -> recibo
 - Últimas elecciones tradicional con ayuda al recuento
- **España**
 - Algunas pruebas no vinculantes con resultados diversos.
 - Solamente País Vasco con legislación habilitante.

PREGUNTAS