

*Experiencia práctica en voto
electrónico: sistema vasco de voto
electrónico y aplicación en la
UPV/EHU*

Iñaki Goirizelaia

Ingeniería Telemática

Departamento de Electrónica y Telecomunicaciones

Escuela Técnica Superior de Ingeniería de Bilbao

Universidad del País Vasco / Euskal Herriko Unibertsitatea

Inaki.goirizelaia@ehu.es

Índice



- *Introducción*
- *Definiciones previas*
- *Sistemas Electrónicos de Votación (SEV)*
- *Sistemas de Voto por Internet*
- *Propuesta de un Sistema de Voto Electrónico: Demotek*
- *Conclusiones*

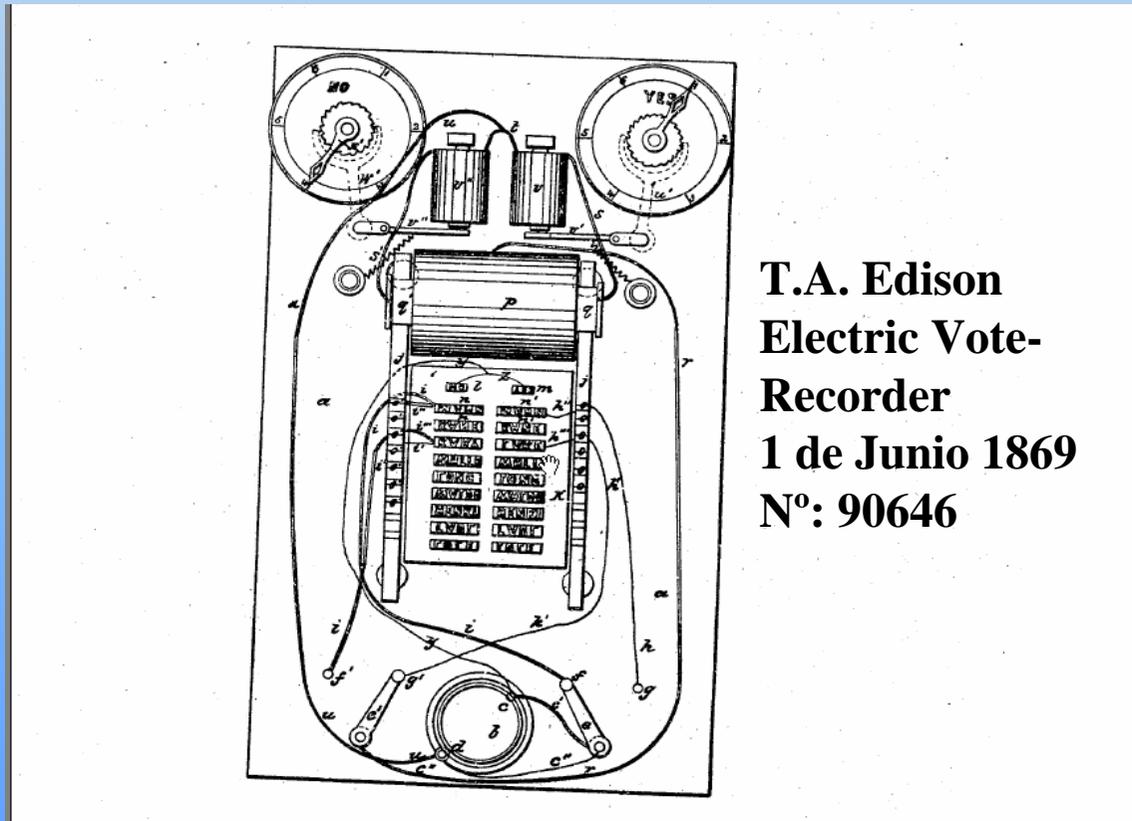
Introducción

- Si podemos utilizar las TICs para comprar nuestros billetes de viaje
- Si podemos utilizar las TICs para hacer la compra
- Si podemos utilizar las TICs para realizar operaciones de banca
- Si podemos utilizar las TICs para operar en bolsa
- Si podemos utilizar las TICs para hacer la declaración de renta
- Si podemos utilizar las TICs para disfrutar de nuestro tiempo libre

¿Por qué no podemos usarla en procesos electorales a gran escala ?

Introducción

- El uso de la tecnología en procesos electorales no es nuevo
- La primera patente otorgada a T.A. Edison fue por su propuesta para una máquina de votar data de 1.869



**NUNCA FUE
UTILIZADA**

Introducción



- En abril de 1.892 se utilizó por primera vez el sistema diseñado por Jacob. H. Myers denominado AVM (Automatic Voting Machine).
- Sistema mecánico.
- Durante la década de los 60 más de la mitad de los norteamericanos utilizaban este sistema de votación.
- En la actualidad gran cantidad de empresas ofrecen soluciones comerciales.

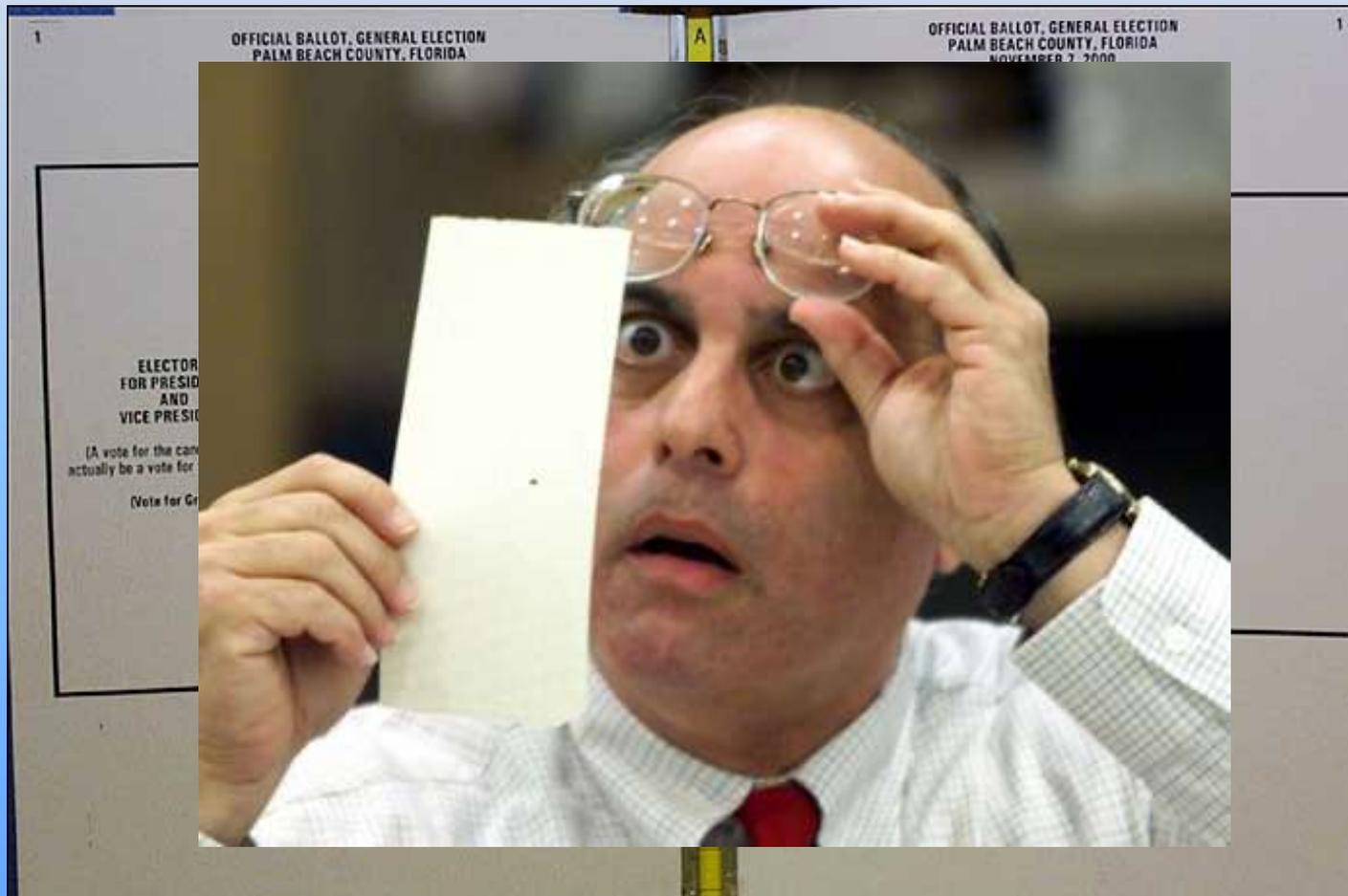
Introducción



- ¿Por qué este interés por la aplicación de la tecnología a procesos electorales?
 - ✓ Desde el punto de vista de la administración, porque los procesos electorales son, ineficientes y muy costosos.
 - ✓ Desde el punto de vista académico, porque es un reto tecnológico e investigador de gran interés.
 - ✓ Desde el punto de vista de elector

Introducción

La famosa papeleta de Florida



Introducción



➤ Además....

- ✓ Estamos creando una sociedad alfabetizada digitalmente
- ✓ La Sociedad de la Información debe ofertar mecanismos para consultar digitalmente a sus miembros, en cualquier momento y en cualquier lugar
- ✓ Incrementar la participación ciudadana

Introducción



- Razones para el uso de las TICs en procesos electorales
 - ✓ Ahorro económico
 - ✓ Mejora de la eficiencia de las tareas electorales
 - ✓ Aumento de la velocidad en la presentación de los resultados
 - ✓ Mejora de la precisión de los resultados
 - ✓ Detección y prevención del fraude electoral
 - ✓ Aumento de la confianza pública en el proceso electoral
 - ✓ Aumento del número de consultas populares
 - ✓ Aumento de la participación electoral
 - ✓ Movilidad del votante
 - ✓ Comodidad del votante

Definiciones previas



➤ TICs aplicadas al proceso de votación

✓ *Sistemas Electrónicos de Votación*

✓ *Sistemas de Votación por Internet*

Sistemas Electrónicos de Votación

Sistema que posibilita la emisión y el recuento automático del voto mediante la utilización de un equipamiento y programa específico.

Generalmente la identificación del votante es un proceso independiente al de la emisión del voto y casi siempre sin automatizar.

➤ **Sistemas Electrónicos de Votación**

- ✓ Toda la información necesaria para permitir el voto está en el propio puesto de votación
- ✓ El votante debe desplazarse al colegio electoral
- ✓ No se permite el uso de equipos no autorizados
- ✓ Es necesario un hardware y software específicamente diseñado para el proceso electoral

Sistemas de Votación por Internet

Sistema que recupera vía Internet la papeleta del servidor electoral y la presenta al votante en la pantalla de su ordenador. El votante marca su opción y la devuelve vía Internet al servidor electoral para su recuento. El sistema realiza el proceso de identificación del elector, emisión y recuento del voto.

- **Sistemas de Votación por Internet**
 - ✓ Elector localizado en cualquier lugar
 - ✓ Único requisito: disponer de un dispositivo con conexión a Internet (PC, tfno. móvil, PDA,...)
 - ✓ No es necesario un hardware específico
 - ✓ En el caso ideal, mediante un procedimiento “seguro” se recibe a través de la red todo lo necesario para identificarse y votar

Características de los Sistemas de Votación

- **Democrático**
- **Preciso**
- **Invulnerable**
- **Privado**
- **Verificable**
- **Conveniente**
- **Flexible**
- **Personas discapacitadas**
- **Fácil de utilizar**
- **Movilidad**
- **Recuento automatizado**
- **Evitar la coacción**
- **Impedir la compra venta de votos**
- **Compatible con la tradición electoral**

Definiciones previas

➤ **Clasificación de los Sistemas de Voto**

✓ *Sistemas Tradicionales*

- Papeleta de voto
- Tarjetas perforadas
- Máquina de palancas

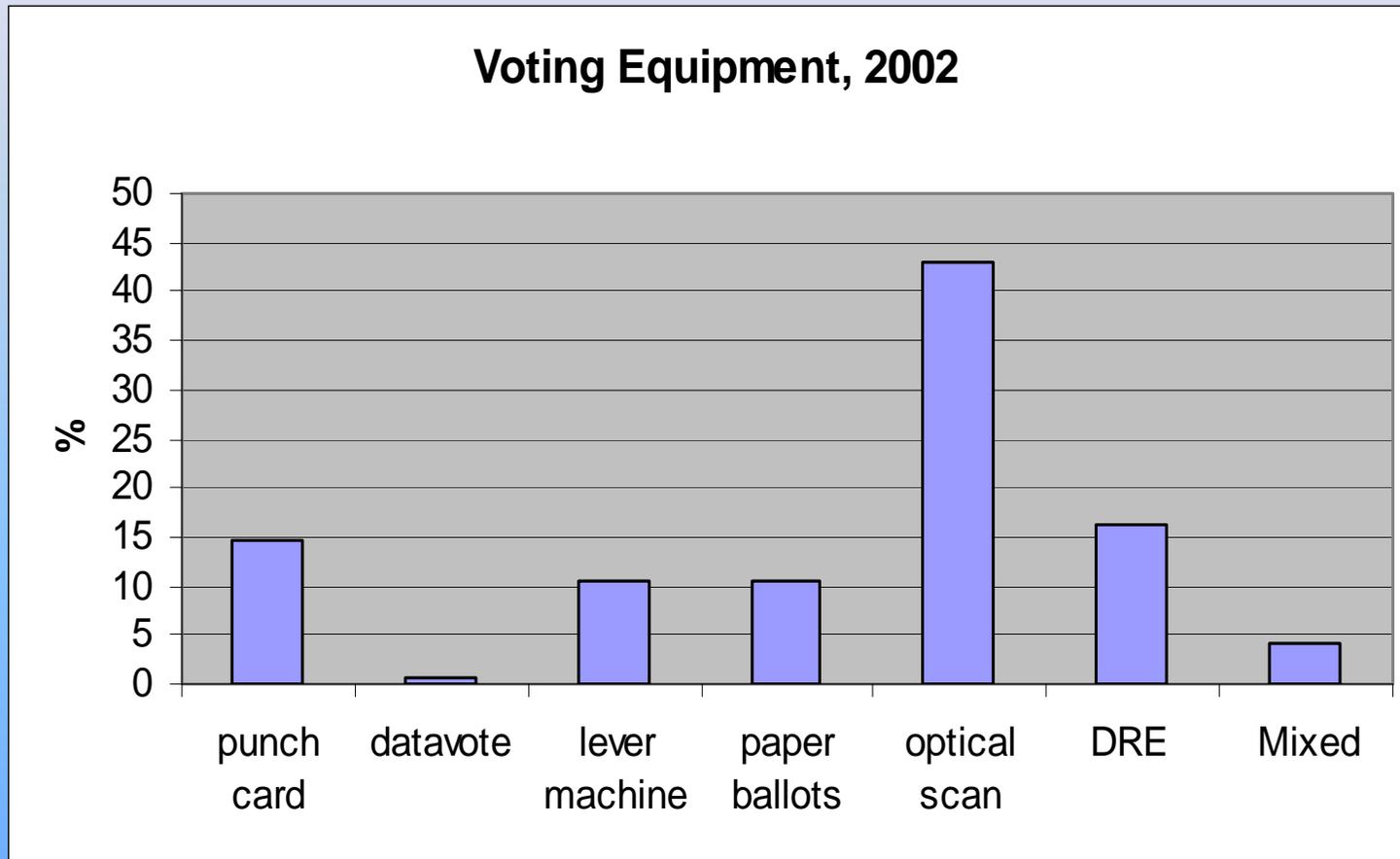
✓ *Sistemas de Voto Electrónico*

- Reconocimiento Óptico de Marcas (OMR)
- Sistemas Electrónicos de Registro Directo (DRE)
- Mixtos

✓ *Sistemas de Voto por Internet*

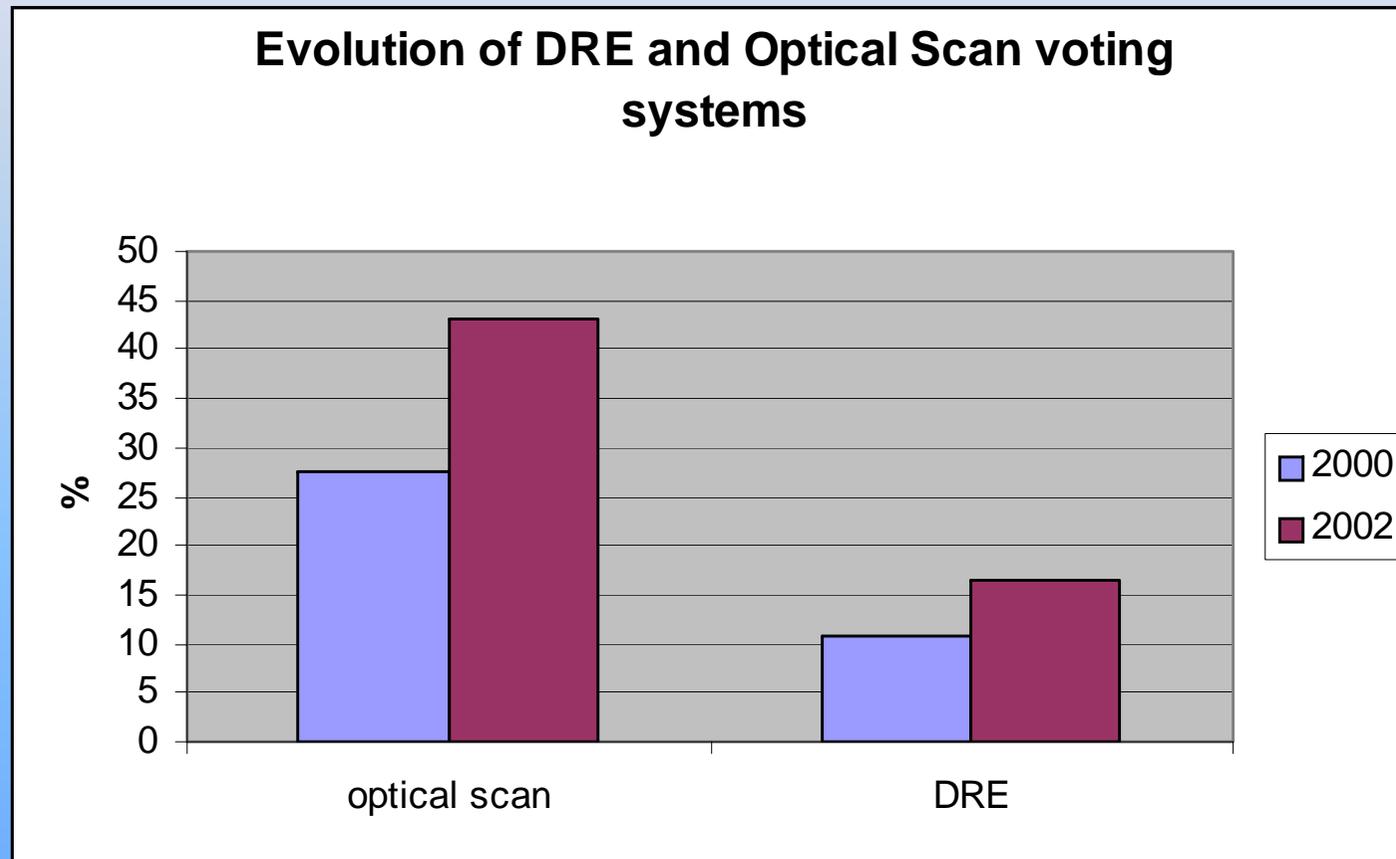
- Voto en quioscos electorales
- Voto en colegio electoral
- Voto remoto

Utilización de Sistemas de Voto



Utilización de diversos Sistemas de Voto en las elecciones generales USA 2002

Evolución de Sistemas de Voto

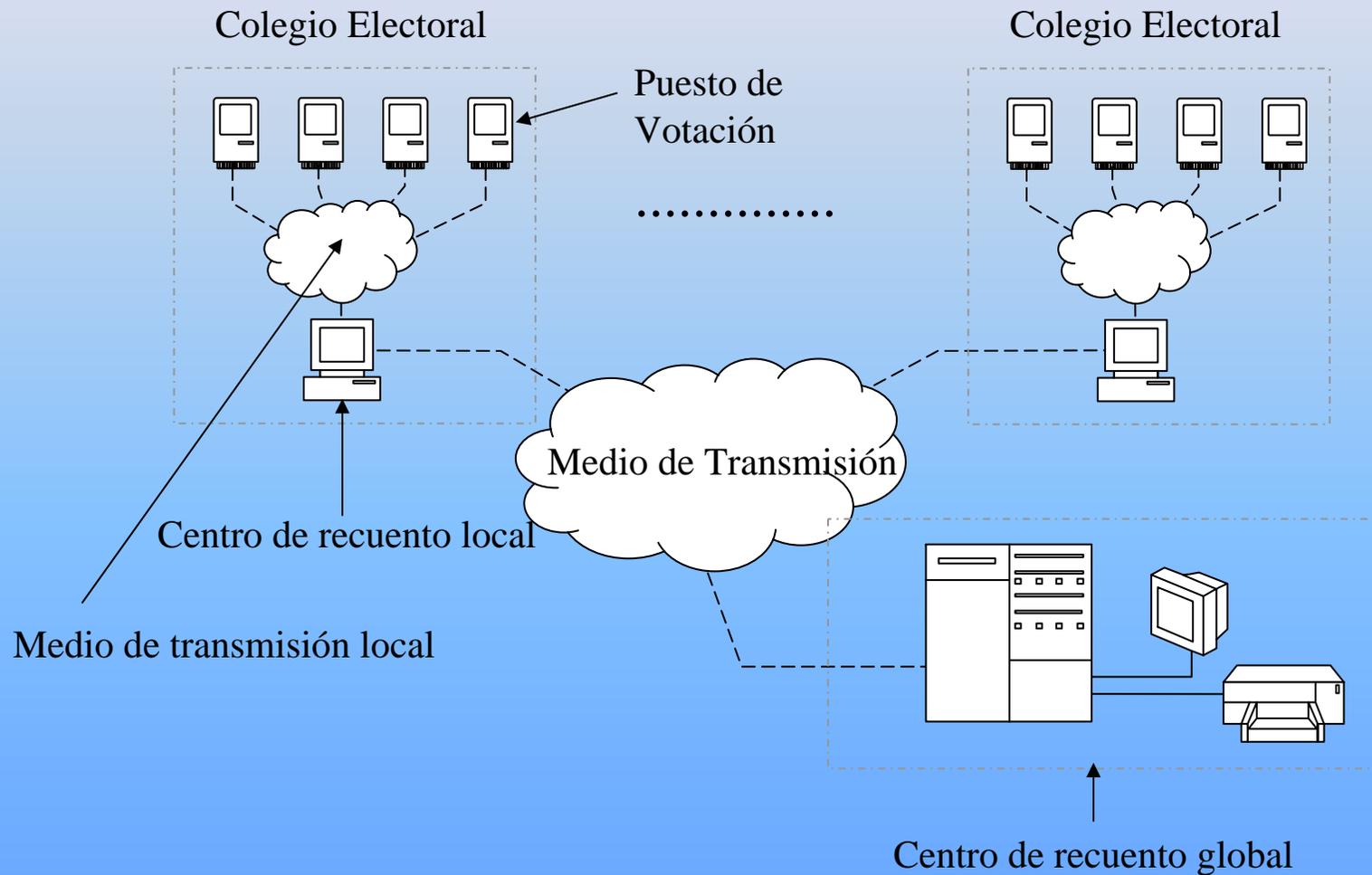


Evolución de Sistemas de Voto mediante reconocimiento óptico y DRE, 2000-2002

➤ **Componentes**

- ✓ Colegio Electoral
 - Puesto de Votación
 - Centro de Recuento Local
 - Medio de Transmisión Local
- ✓ Centro de Recuento Global
- ✓ Medio de transmisión

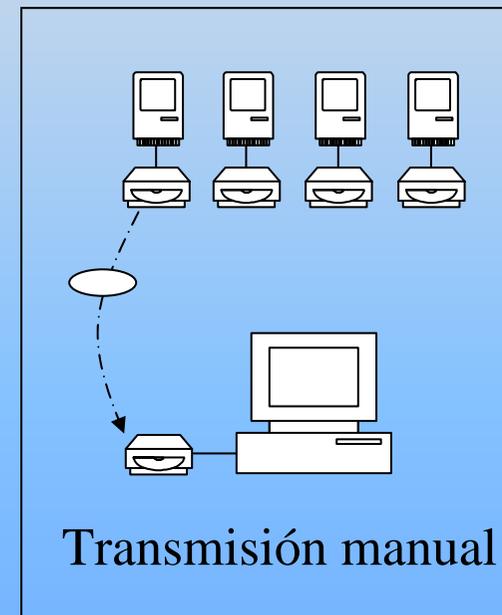
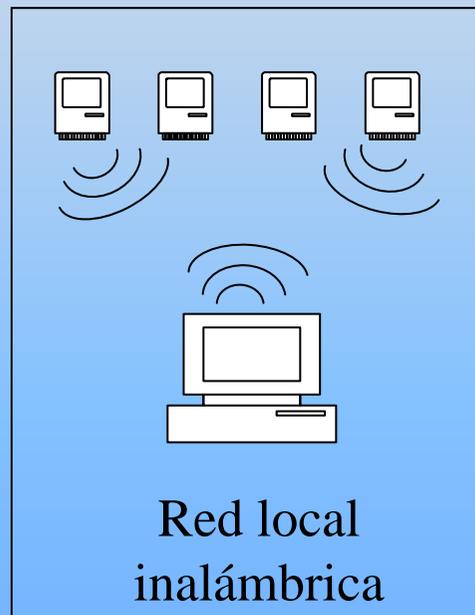
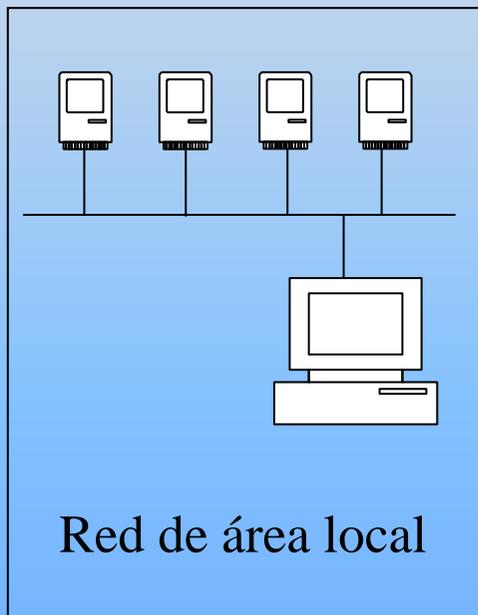
Sistemas Electrónicos de Votación



- **Puesto de Votación**
 - ✓ Normalmente basado en la tecnología DRE o OMR
- **Centro de Recuento Local**
 - ✓ En general ordenadores tipo PC con dispositivo de lectura del voto para leer votos emitidos con anterioridad.
- **Medio de Trasmisión Local**
 - ✓ Diferentes opciones

Sistemas Electrónicos de Votación

Medio de transmisión local

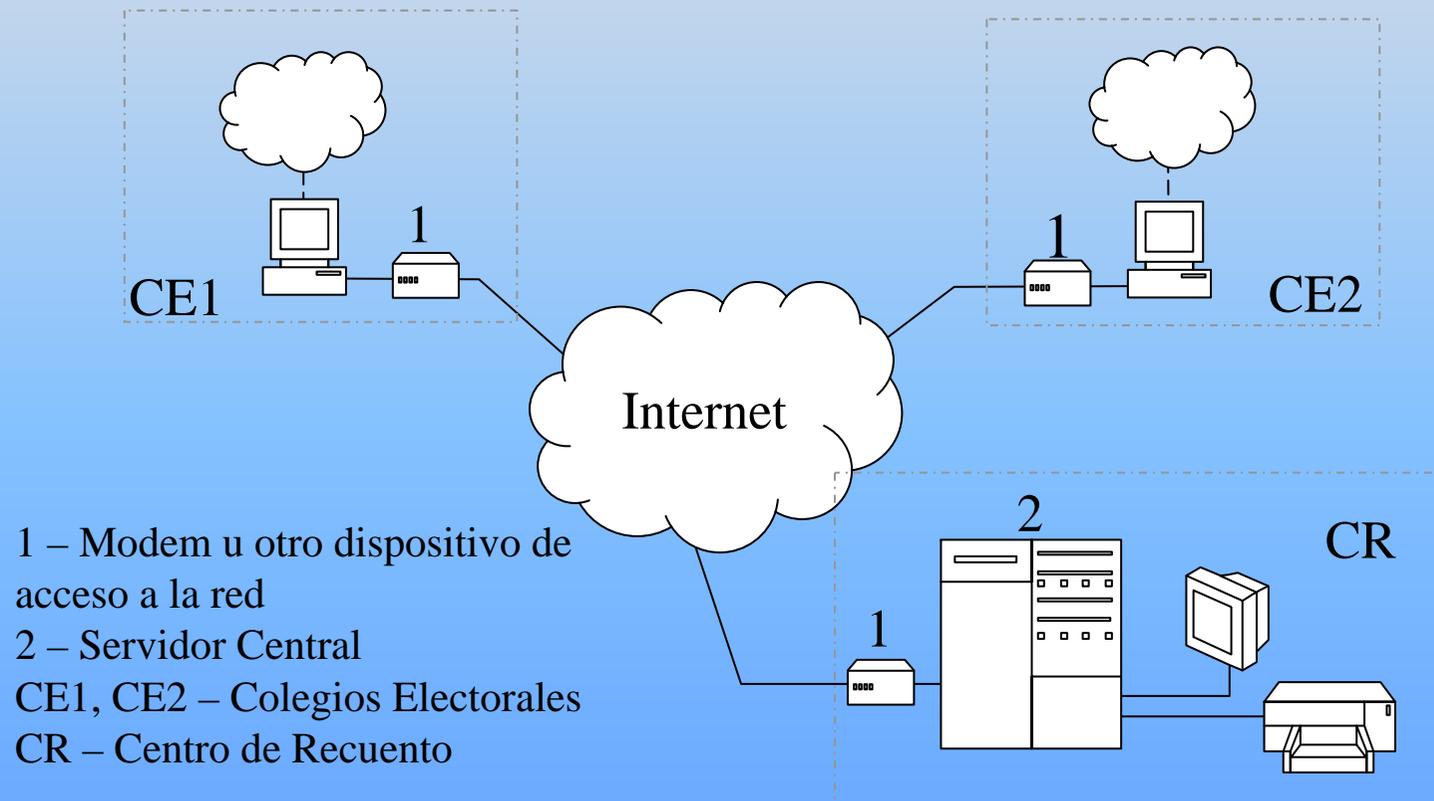


➤ **Medio de Transmisión Global**

- ✓ Internet
- ✓ Manual
- ✓ GSM

Sistemas Electrónicos de Votación

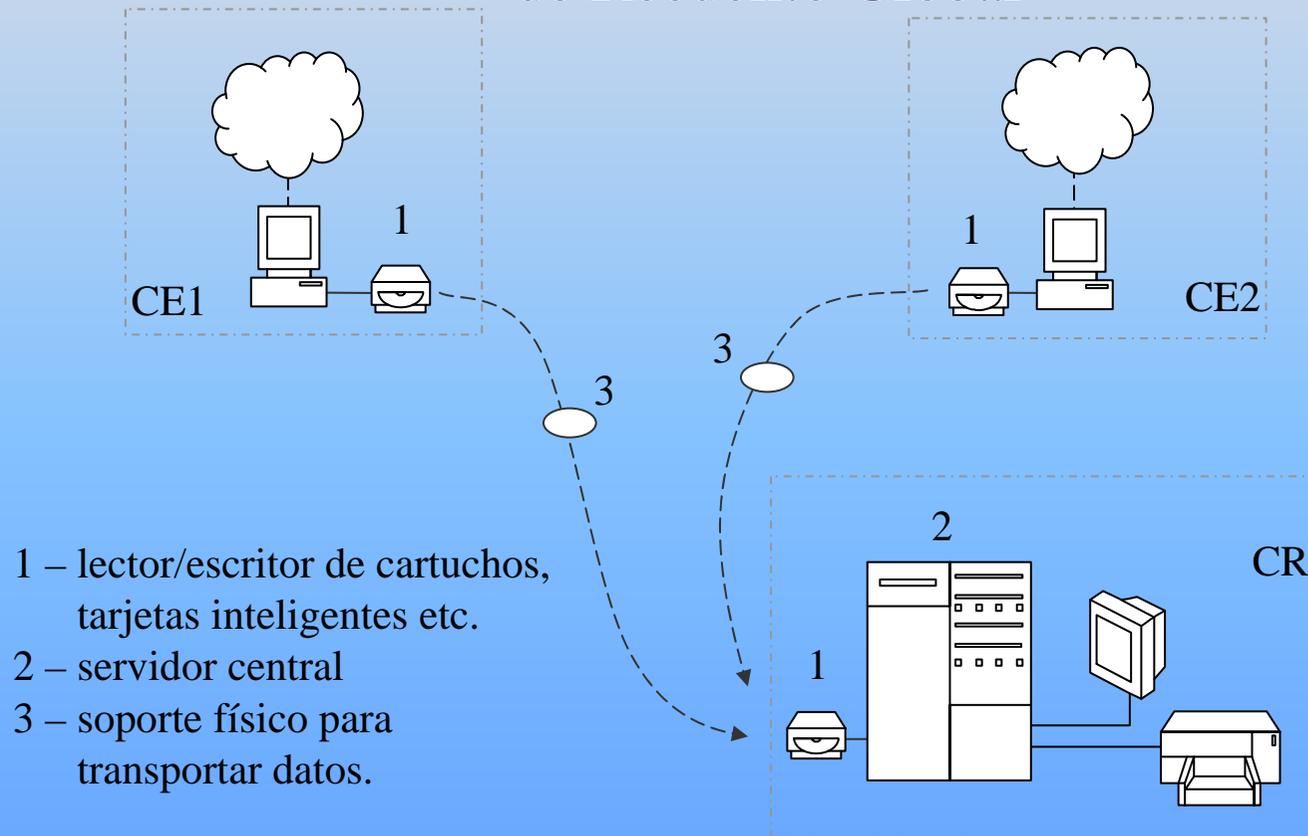
Conexión de los Colegios Electorales al Centro de Recuento Global mediante Internet



1 – Modem u otro dispositivo de acceso a la red
2 – Servidor Central
CE1, CE2 – Colegios Electorales
CR – Centro de Recuento

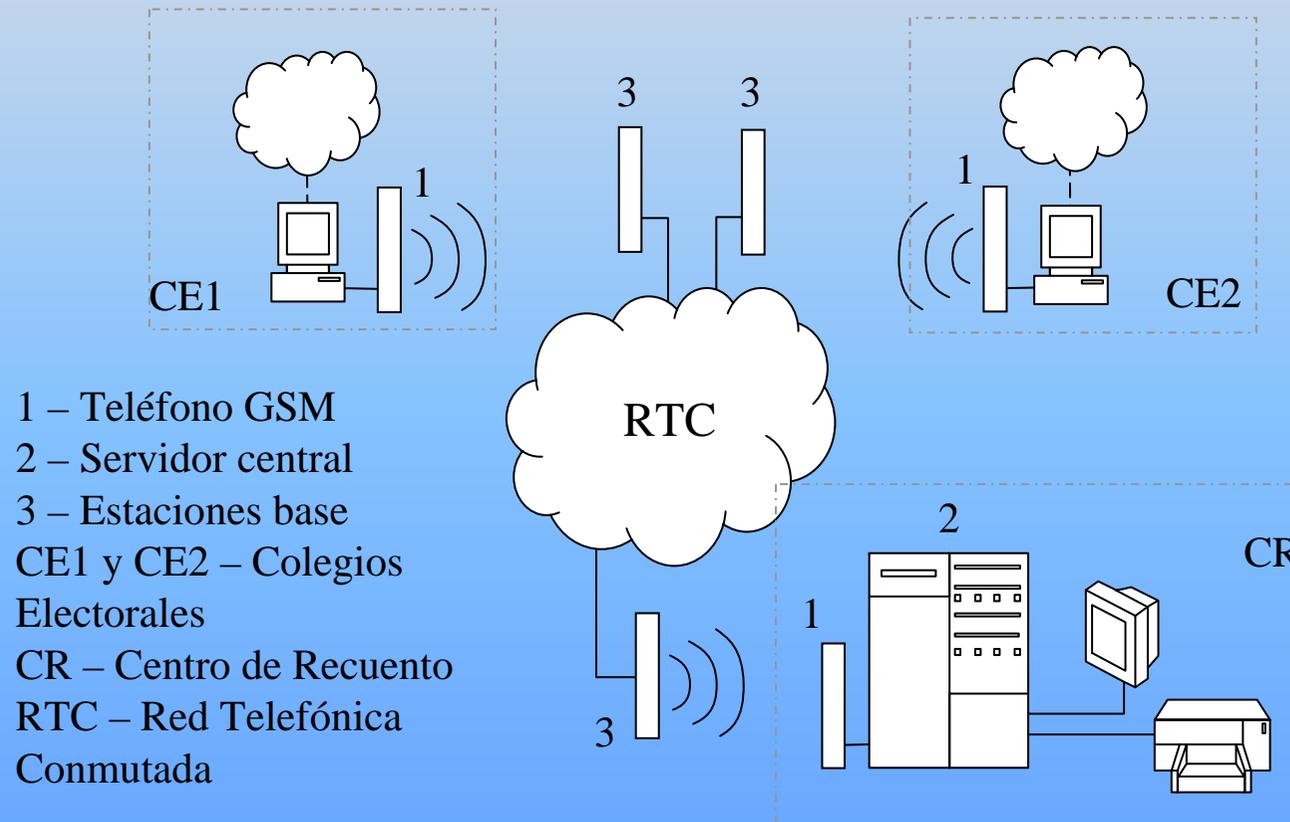
Sistemas Electrónicos de Votación

Conexión manual de los Colegios Electorales con el Centro de Recuento Global

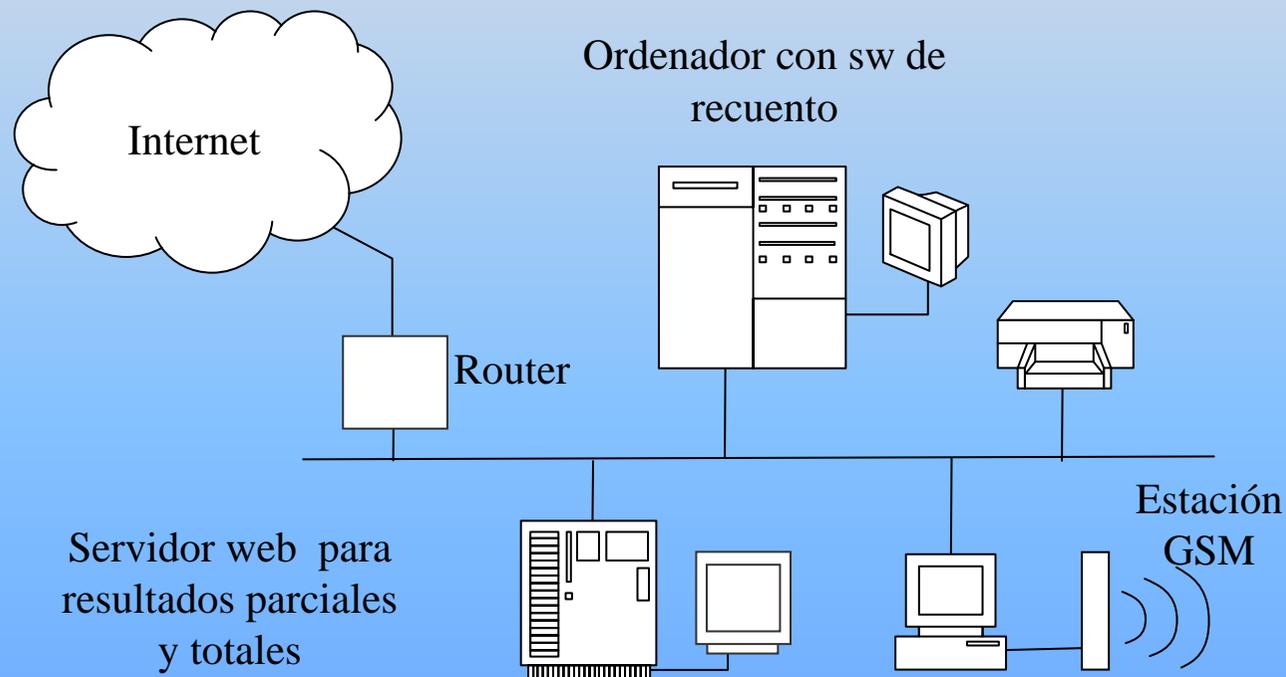


Sistemas Electrónicos de Votación

Conexión de los Colegios Electorales al Centro de Recuento Global mediante red GSM



Centro de Recuento Global I



Centro de Recuento Global II



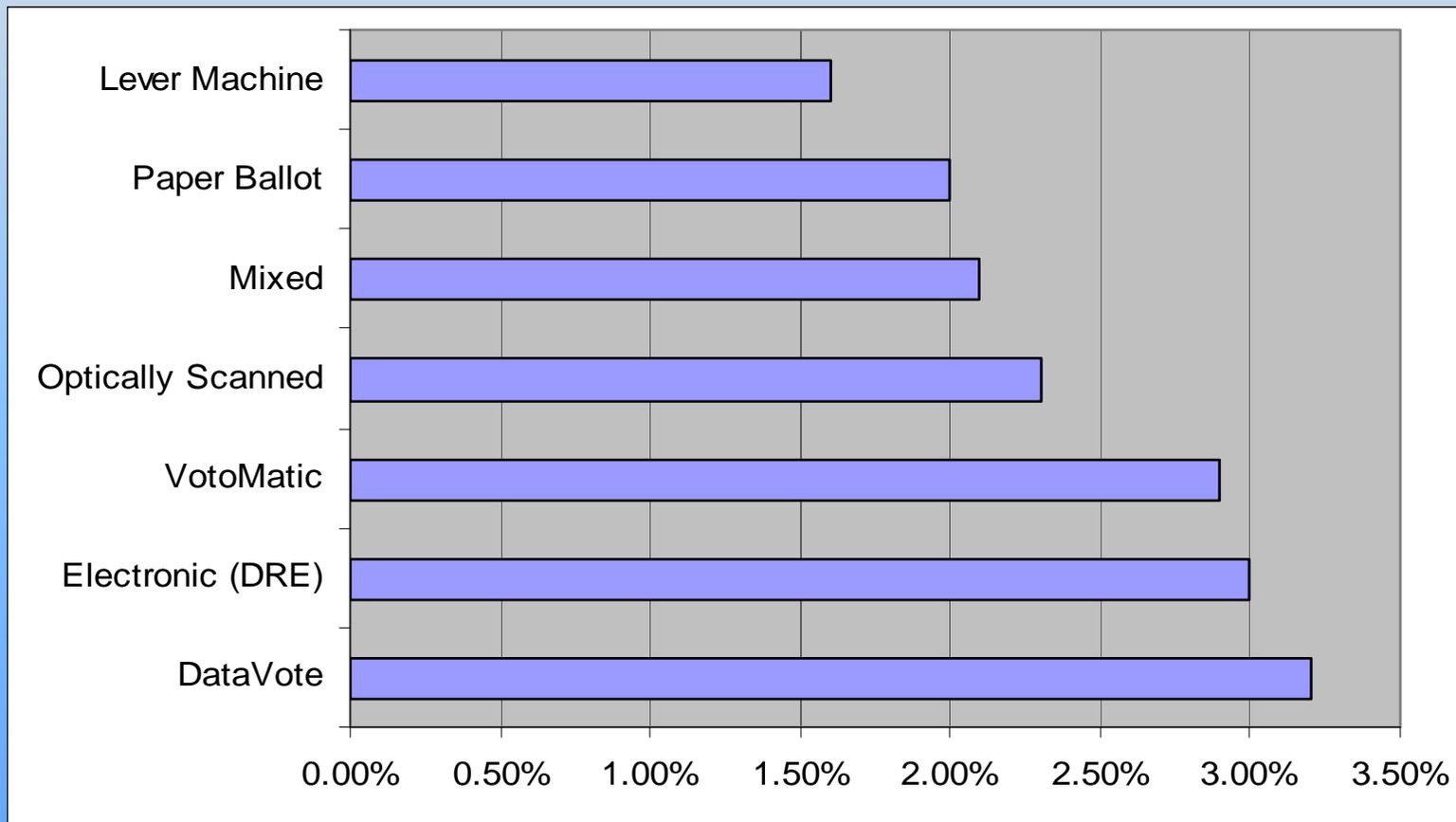
Evaluación de los SEV



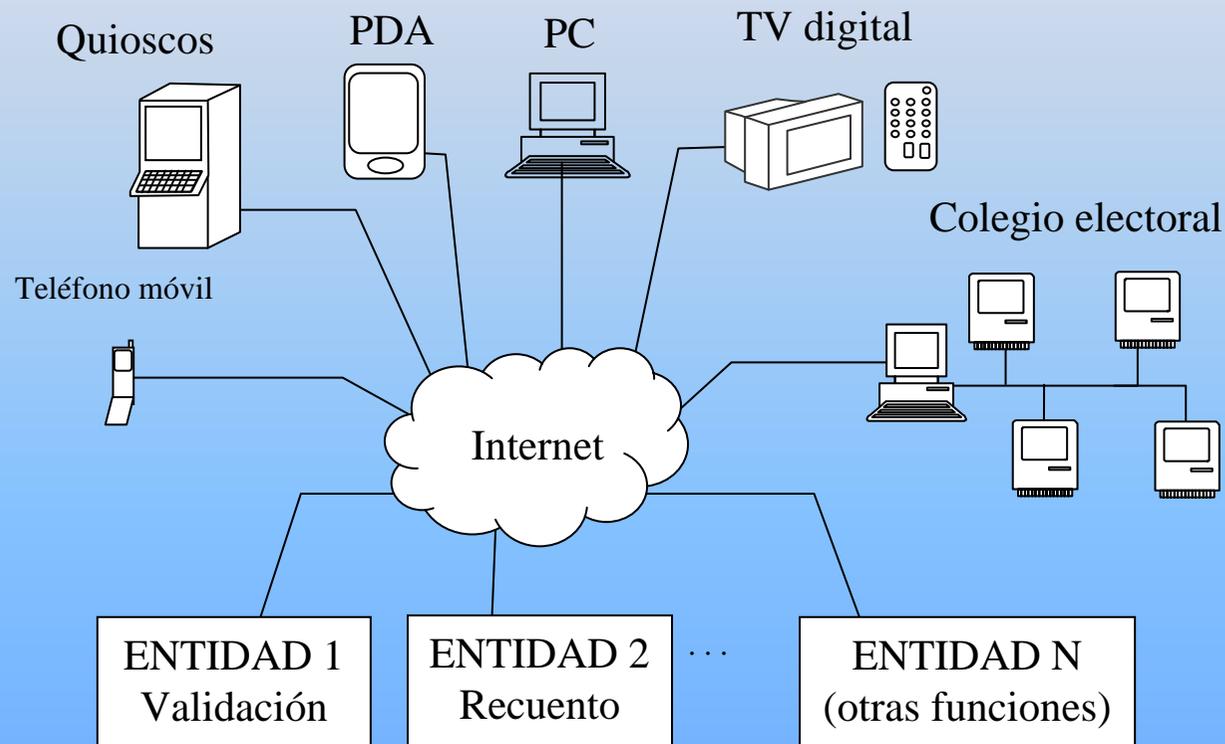
	OMR	DRE
Privacidad	Sí	Sí
Precisión	Posibles problemas	Posibles problemas
Verificabilidad	No en general	No en general
Democrático	Sí	Sí
Conveniente	Si	Si, procedimiento
Flexibilidad	No en general	Muy flexible
Disponibilidad	Fallos de sistema	Fallos de sistema
Discapacitados	No en general	Sí
Facilidad de uso	Sí	Complejo
Automatización	Casi total	Total
Coacción	Como en Sist. Tradici.	Como en Sist. Tradici.
Venta del voto	Muy difícil	Muy difícil
Compatible tradición	No	No

Evaluación de los SEV

Tasa de Error por Tecnología (Ronald L. Rivest, MIT Laboratory for Computer Science)



Sistemas de Voto por Internet



Topología general de un sistema de voto por Internet

Sistemas de Voto por Internet



- Algunos criterios para la evaluación
 - ✓ Autenticación
 - ✓ Partes de confianza
 - ✓ Hardware específico
 - ✓ Protocolo de votación
 - ✓ Verificabilidad
 - ✓ Dispositivos móviles
 - ✓ Protocolos de comunicación

Sistemas de Voto por Internet



	Cybervote	E-poll	i-Vote
Seguridad			
Autenticación	Firma digital	Huella dactilar	Firma Digital en Smart Card
Partes de confianza	PKI, confianza distribuida	PKI	PKI
Hardware específico	Smart Card	Smart Card con detector biométrico	Smart Card
Arquitectura			
Protocolo de votación	Encriptación homomórfica	Protocolo de firma ciega	Protocolo de firma ciega
Verificabilidad	Total	(sin información)	(sin información)
Plataformas			
Dispositivos móviles	Sí	No	No
Protocolos	TCP/IP, SSL	TCP/IP, SSL	TCP/IP, SSL

Movilidad vs. Seguridad Democrática

Coacción

Venta de voto

Petición de voto

Ingeniería social

Registro de electores

Ataques a la plataforma de votación

Necesidad de equipamiento vs. brecha digital

Disponibilidad de infraestructura de comunicaciones

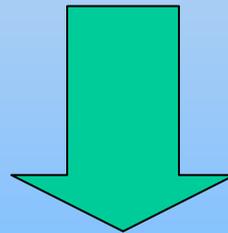
Propuesta para un SEV

- Objetivo a corto (propuesta posibilista):
 - ✓ El sistema debe cumplir los requisitos democráticos exigibles
 - ✓ El sistema debe ser aceptable por la sociedad y los partidos políticos
 - ✓ El sistema debe favorecer las mínimas reformas legales necesarias

Propuesta para un SEV



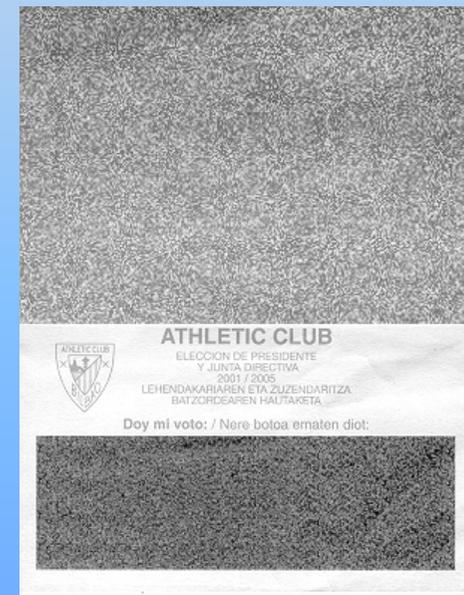
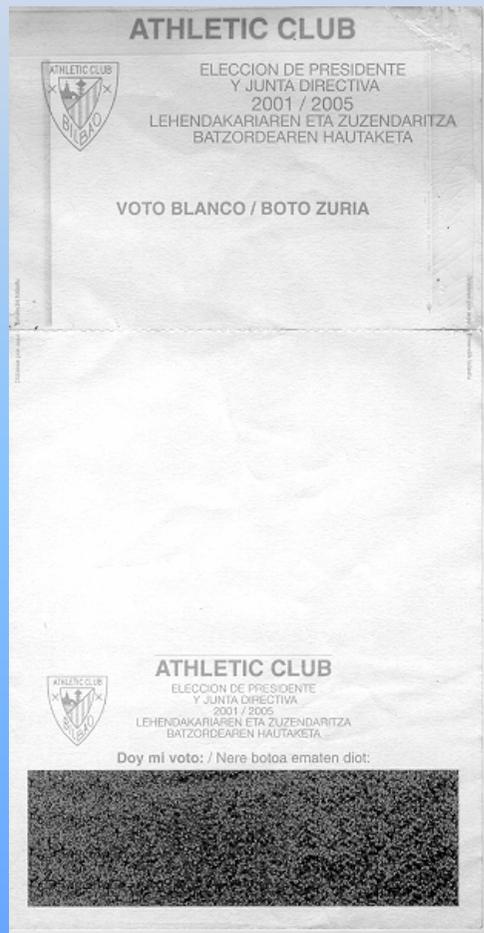
Compatibilidad con la tradición electoral +
mínimas modificaciones legales



En nuestro país a corto plazo implica el uso de
la papeleta de votación tradicional

Propuesta para un SEV

Papeleta Electoral

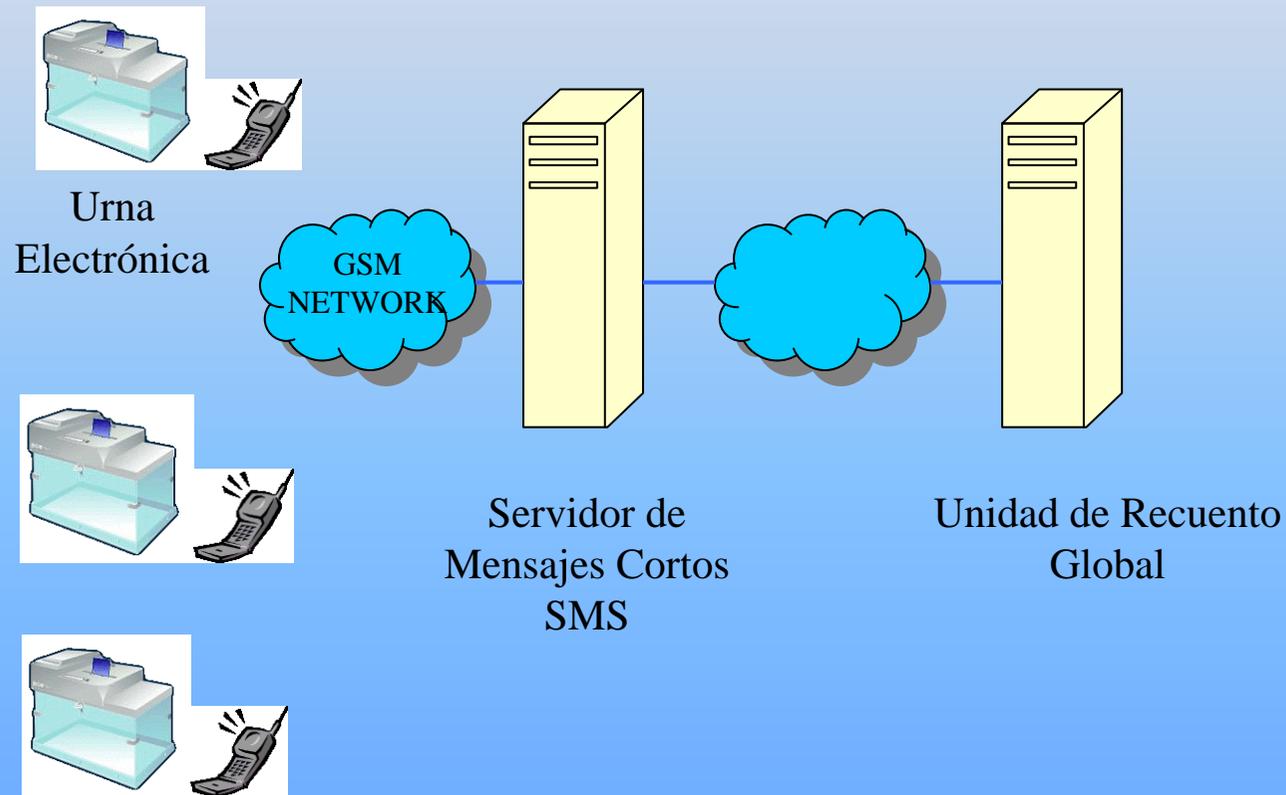


Propuesta para un SEV

Urna



Propuesta para un SEV



Propuesta para un SEV

➤ Tecnología utilizada

- ✓ Reconocimiento Óptico de Caracteres para lectura automática de la papeleta



- ✓ Transmisión de datos SMS. Validez legal únicamente el acta escrita manualmente en cada mesa.

Experiencias sistema Demotek



- Experiencias realizadas
 - ✓ Elección de la comisión permanente de la Junta de la Escuela de Ingeniería de Bilbao, abril 2001
 - ✓ Elecciones a la presidencia del Athletic Club de Bilbao, 1/06/2001
 - ✓ Claustro de Gestión de la UPV/EHU, 17/12/2002
 - ✓ Claustro UPV/EHU para aprobación de estatutos de la universidad, 8/4/2003
 - ✓ Elecciones parlamento de Cataluña, 2004
 - ✓ Elecciones al rector de la UPV/EHU en mayo de 2004

Comparación de los distintos sistemas

	DEMOTEK	OMR	DRE	Internet
Privacidad	Sí	Sí	Sí	Sí, sin ataques
Precisión	Fallo del sistema, mal uso	Fallo del sistema, mal uso	Fallo del sistema, mal uso	Fallo sistema, ataques, mal uso
Verificabilidad	No en general	No en general	No en general	Sí
Democrático	Sí	Sí	Sí	Sí, sin robo de identidad
Conveniente	Sí	Sí	Si, procedimiento	Sí, si procedimiento no muy complicado
Flexibilidad	No	No en general	Muy flexible	Muy flexible
Disponibilidad	Fallos de sistema	Fallos de sistema	Fallos de sistema	Fallos de sistema + ataques
Discapitados	No	No en general	Sí, depende disc.	Si, depende de discapacidad
Facilidad de uso	Muy simple	Simple	Complejo	Complejo
Automatización	Total	Casi total	Total	Total
Coacción	Como en sistema tradicional	Como en Sistema Tradicional	Como en Sistema Tradicional	Mayor problema de este tipo de sistemas
Venta del voto	Muy difícil	Muy difícil	Muy difícil	Sencillo
Movilidad	No	No	No	Sí
Compatible tradición electoral	Sí	No	No	No

Conclusiones



- En nuestro país la única solución posible a corto plazo para procesos electorales a gran escala es un sistema tipo OMR.
- Es necesaria una fase de adaptación y acercamiento hacia el elector.
- La transparencia en los equipos y la disponibilidad del software empleado puede hacer aumentar la confianza del electorado

Conclusiones



- La rápida evolución de la tecnología puede hacer obsoleto el mejor sistema de votación tipo OMR en un corto periodo de tiempo.
- El futuro implica movilidad, consultas más frecuentes en un mundo inalámbrico. Por tanto, el tiempo estimado de vida para los sistemas tipo OMR es muy corto.
- Nuestro trabajo debe ir en la línea de evolución desde sistemas tipo OMR hacia sistemas que posibiliten el voto en su forma más flexible posible.
- Incorporación paulatina de nuevas posibilidades.