TASSI 2014

Posibilidades del voto telemático en la democracia digital

Madrid, marzo 2014

Justo Carracedo Gallardo
Catedrático de EU jubilado de la ETSIS de Telecomunicación
Profesor Ad Honorem de la Universidad Politécnica de Madrid
carracedo@diatel.upm.es

Crecimiento del ciberespacio

- Estamos asistiendo a un proceso en el que tanto
  - las comunicaciones interpersonales como
  - la relación de los ciudadanos con diversos agentes sociales
    - (económicos, gubernamentales, políticos, mediáticos, etc.)
  - que hasta hace poco se llevaban a cabo usando mecanismos de comunicación convencionales
    - (en la mayoría de los casos de forma presencial)
  - están pasando, de forma creciente, a llevarse a cabo utilizando redes de computadores (o redes telemáticas).
  - en lo que podemos considerar como una introducción paulatina en la llamada **Sociedad de la Información.**

Es decir, hay un crecimiento constante del ciberespacio

Sociedad de la Información

- El término “Sociedad de la Información” se usa, quizás, de forma algo ligera, porque de lo que se trata realmente es de la sociedad postindustrial fuertemente influida por las tecnologías de la información y las comunicaciones.
- (No digamos ya de tratar de diferenciarla sociológicamente de lo que algunos denominan “Sociedad del conocimiento”).
- En realidad, la información y el conocimiento es lo que ha marcado y hecho evolucionar al homo sapiens desde siempre.
- En cualquier caso, lo que es evidente es lo que hemos señalado como aparición de un **proceso creciente en el que actividades que antes se hacían por medios convencionales están pasando a llevarse a cabo utilizando redes telemáticas**.
- Lo que también se conoce como CMC (comunicaciones mediadas por computador).

¿Porqué no también una **democracia digital**?

- Si tantas comunicaciones y relaciones convencionales se van trasladando al ciberespacio, ¿porqué no también las actividades inherentes a la gestión de los procesos democráticos?.
- Podemos decir que por democracia digital (o democracia electrónica) puede entenderse: **el uso de las CMC y de las redes telemáticas para mejorar la política y la participación ciudadana en los procesos democráticos de comunicación, de intercambio de ideas y de toma de decisiones**.

Democracia digital, pero segura

- En la traslación al ciberespacio de los procesos de democracia digital (al igual que en todo el abanico de las CMC) es imprescindible que se mantengan, al menos, las mismas garantías de respeto de los derechos ciudadanos y de seguridad que están presentes en las comunicaciones convencionales.
- Para ello es necesario que dichos procesos estén protegidos contra cualquier amenaza de seguridad, bien sea accidental o intencional (*ataque*).
- Los *servicios de seguridad* protegen las comunicaciones de los usuarios frente a los distintos ataques.

Distintos servicios de seguridad

- Autenticación de entidades
- Confidencialidad de datos
- Integridad de datos
- Control de acceso
- No repudio
- Disponibilidad (¿?)
- Anonimato

El servicio de anonimato

- El servicio de anonimato trata de mantener oculta la identidad de la persona que realiza una determinada operación telemática.
- El servicio de anonimato es fundamental en algunos procesos de democracia digital.
- Es uno de los más controvertidos y menos desarrollados debido a las implicaciones sociales que conlleva y a la complejidad de los mecanismos de seguridad que es necesario poner en juego para su provisión.

Voto y democracia

- La existencia de votaciones no garantiza por sí sola la existencia de democracia.
  - Puede que el sistema funcione correctamente pero que en su aplicación no se respeten requisitos fundamentales y se falseen los resultados.
  - Puede que no existan garantías de que se apliquen los veredictos resultantes de las votaciones.
- Eso sí: para un funcionamiento adecuado de la democracia es imprescindible la presencia de sistemas de votación.

Democracia digital y voto

- Los sistemas de votación no pueden quedar aislados del proceso creciente de automatización mediante el uso de las tecnologías de la información y las comunicaciones.
- Por ello, la utilización de sistemas informáticos y telemáticos para automatizar, en todo o en parte, los sistemas de votación es vista como “un avance”
  - puede aparecer una cierta presión social acrítica que tienda a apoyar y aplaudir este tipo de cambios sin pararse a pensar la conveniencia o no de su implantación.
  - a estos movimientos tecnofílicos no son ajenos, obviamente, los fabricantes de tecnología, que ven en estos cambios una oportunidad de negocio.

Riesgos y beneficios

- Lo razonable es que ante cualquier innovación se pongan en un plato de la balanza
  - las **ventajas** que esa innovación **aporta**
  - y en el otro los **riesgos** que **compor**ta.
- Y decidir consecuentemente sobre qué solución adoptar
- La seguridad total (al 100%) no existe;
  - ni en los sistemas automatizados
  - ni en los sistemas convencionales mediante papeletas

Tres niveles en la automatización del proceso electoral

- Primer nivel: automatización de parte del proceso electoral manteniendo el voto mediante papeletas.
- Segundo nivel: voto electrónico.
  - Se dispone de máquinas electrónicas **a la vista del votante** ante las cuales se realiza el acto de depositar el voto. Por ejemplo, Venezuela y Brasil tienen implantados este tipo de sistemas.
- Tercer nivel: voto telemático y voto por Internet
  - la votación se lleva a cabo mediante el uso de redes telemáticas y agentes telemáticos específicos.
  - los votos se depositan en una “urna” remota fuera de la vista del votante.
  - tanto la autorización para votar como el voto “viajan” por la red.

Voto electrónico y voto telemático

- Queda fuera de los objetivos de esta presentación analizar las soluciones que hemos denominado de primer y segundo nivel. No obstante, cabe decir que:
- El voto electrónico (con urna “in situ”) y el voto telemático (con urna remota) son dos alternativas con una **dimensión tecnológica** y unos **requerimientos sociopolíticos** radicalmente distintos.
- No distinguir claramente el voto electrónico y el voto telemático crea confusión en la ciudadanía.

Dos escenarios distintos para el voto telemático (I)

- Escenario a) Para votar es necesario acudir a **puntos de votación** específicos.
  - El sistema está soportado por agentes telemáticos propios independientes funcionalmente:
  - terminal para la autenticación
  - terminal para emitir el voto,
  - urna remota
  - sistemas remotos de gestión y recuento de votos, etc.
  - y usar una **red telemática "propia"** dedicada solamente al proceso de votación. En realidad, lo más razonable es que se trate de una **red virtual** apoyada en la infraestructura de transporte de datos de Internet.

Dos escenarios distintos para el voto telemático (II)

- Escenario b) El votante puede votar desde cualquier sitio, también desde casa.
  - En estos casos lo que se prevé es que el votante use **su propio dispositivo** de conexión para emitir el voto, para autenticarse y para enviar el voto.
  - Existirá también una urna remota y unos sistemas de gestión y recuento de votos también remotos.
  - El votante usa los servicios ordinarios y convencionales de Internet que le brinda el proveedor que tenga contratado.
  - Este caso particular de voto telemático procede denominarlo **voto por Internet**.

Dos escenarios distintos para el voto telemático (y III)

- Así pues, el *voto por Internet* es un caso particular del *voto telemático.*

- Estoy conforme con la definición de voto telemático que da la Wikipedia en español (la toma de una publicación nuestra) pero no en lo de identificar ambas soluciones (dice “voto telemático **o** voto por Internet”)

Dos escenarios distintos para el voto telemático (y IV)

- En inglés se usa *electronic voting* (*eVoting*) tanto para referirse a los sistema de los que aquí hemos *voto electrónico* (con urna “in situ”), como los que hemos denominado *voto telemático* (con urna remota).
- Raramente se encuentra en inglés el término *telematic voting*. Para estos sistemas se utiliza a veces el término *remote electronic voting.*
- En inglés, aunque lo más común es encontrar el término genérico *eVoting*, sí se usa a veces el término *Internet voting.*

Elementos de seguridad utilizados en los sistemas de voto telemático

- Mecanismos criptográficos
  - Mixing networks
  - Firma a ciegas
  - Zero Knowledge
  - Secreto compartido
  - Secreto dividido, ….
- Mecanismos esteganográficos
- Tarjetas inteligentes

Puede consultarse: *Servicios de anonimato para la Sociedad de la Información*, 93 páginas, Cap 11 del libro *Seguridad en Redes Telemáticas,* J. Carracedo, McGraw Hill 2004, en:

http://www.criptored.upm.es/guiateoria/gt_m077c.htm

Mixing networks

- Propuesto inicialmente por Chaum en 1981 como una técnica para implementar correo anónimo, han aparecido multiples variantes.
- Su propósito es ocultar la correspondencia entre las entradas a la red y las salidas.
- Los mecanismos de seguridad suelen apoyarse en criptografía de clave pública.

Firma a ciegas

- La *firma opaca* o *firma a ciegas* (en inglés, *blind signature*) se caracteriza porque
  - la entidad firmante no puede adquirir conocimiento alguno sobre el documento que está firmando.
  - Posteriormente, la firma obtenida podrá ser verificada como válida por el propio firmante o por cualquier entidad que disponga de la información pertinente para ello,
  - pero el firmante no puede establecer ninguna relación con las circunstancias en que realizó la firma

Zero Knowledge

- En determinados escenarios puede ser interesante que una entidad A demuestre con un cierto margen de confianza a un verificador B el conocimiento de una determinada información sin necesidad de revelarla

Secreto dividido

- Consiste en tener una información secreta
  - repartida entre varias entidades comunicantes
  - la recomposición del secreto se realiza solamente si coinciden todas las partes entre las que aquél se había dividido.
- Ejemplo: caja fuerte con tres llaves

Secreto compartido

- Consiste en tener una información secreta
  - repartida entre varias partes, de forma que
  - para reconstruirlo sea imprescindible reunir un número mínimo de ellas,
  - pero no todas las porciones en que ha sido dividido
- Ejemplo: abrir una urna electrónica

Mecanismos esteganográficos

- La *esteganografía* es la ciencia que trata la ocultación de mensajes
- El medio en el que se oculta la información se puede denominar *estegomedio*, *cubierta* (*cover*, en inglés) o *tapadera*
- El *estegoanálisis* es la ciencia y el arte que permite detectar esa información oculta.
  - La ocultación de mensajes usando esteganografía puede tener fines legítimos o ilegítimos

Tarjetas inteligentes

- Una tarjeta inteligente es un dispositivo físico que permite almacenar información de seguridad de forma fiable
  - debido a que tiene un microprocesador incorporado, puede gobernar tareas de entrada/salida y ejecutar algunos algoritmos criptográficos.
  - Ello posibilita, entre otras muchas cosas, que pueda almacenar la clave privada de su titular y cifrar datos con ella.
  - Las más interesantes son las Java Cards.
  - El DNI electrónico es una tarjeta inteligente útil en procesos de votación.

Dificultad tecnológica del voto telemático

- Los requerimientos exigibles son difíciles de cumplir
- Las protecciones de seguridad necesarias abarcan:
  - Protecciones organizacionales
  - Protecciones mediante mecanismos criptográficos robustos
- Una dificultad del voto telemático es que tiene que proveer sincronizadamente dos servicios de seguridad que se presentan como antagónicos:
  - **Autenticación** robusta del votante para averiguar si tiene derecho a votar (o ya lo ha hecho).
  - **Anonimato** a la hora de emitir el voto
- Otra gran dificultad es que tiene que compaginar que el votante adquiera una **prueba** de que su voto ha sido tenido en cuenta y que el votante no pueda demostrar ante terceros qué ha votado.

Publicidad de los procedimientos

- Si el sistema se utiliza en elecciones oficiales, debe ser público, conocido y auditable:
  - La definición y especificación del sistema y de los protocolos telemáticos utilizados.
  - Los algoritmos utilizados. Pueden (deben) ser públicos ya que la seguridad reside en las claves criptográficas y en la robustez del algoritmo.
  - Los códigos fuente de todos y cada uno de los programas que se ejecutan en los distintos equipos informáticos intervinientes.

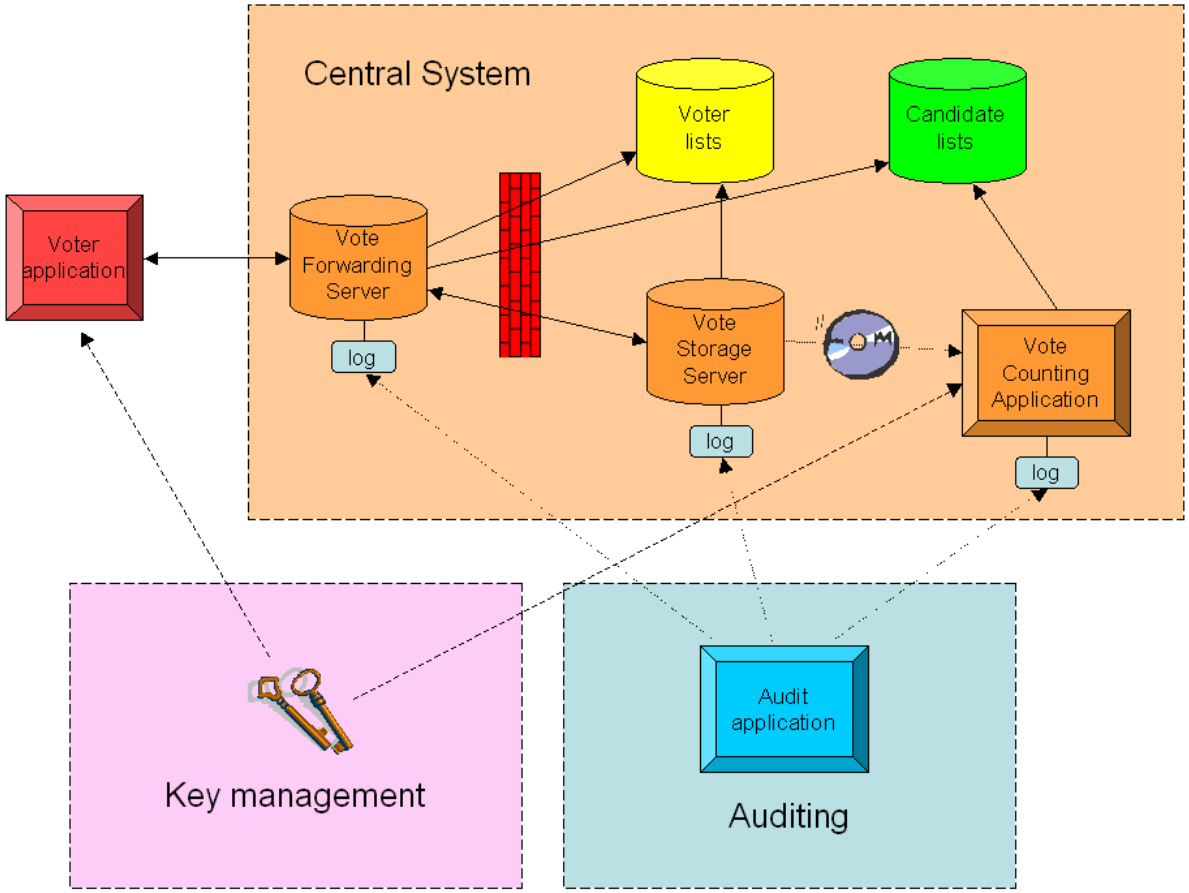
Ventajas que aporta el voto telemático

- El voto telemático aporta algunas **ventajas** sustantivas:
  - Voto frecuente (sobre todo en países que demandan procesos electorales reiterados).
  - En un futuro, permitirá **otra concepción** socio-jurídica del voto (sobre todo en países que tienden hacia democracias avanzadas).
  - El despliegue global puede ser **más barato**, flexible y escalable que el del voto electrónico y el voto con papeletas.
  - Permite votar desde puntos **remotos a la urna** correspondiente (personas desplazadas).
  - Compatibiliza la **ubicuidad** con la pertenencia a un colegio electoral concreto.
  - Puede facilitar la votación a personas con discapacidades.

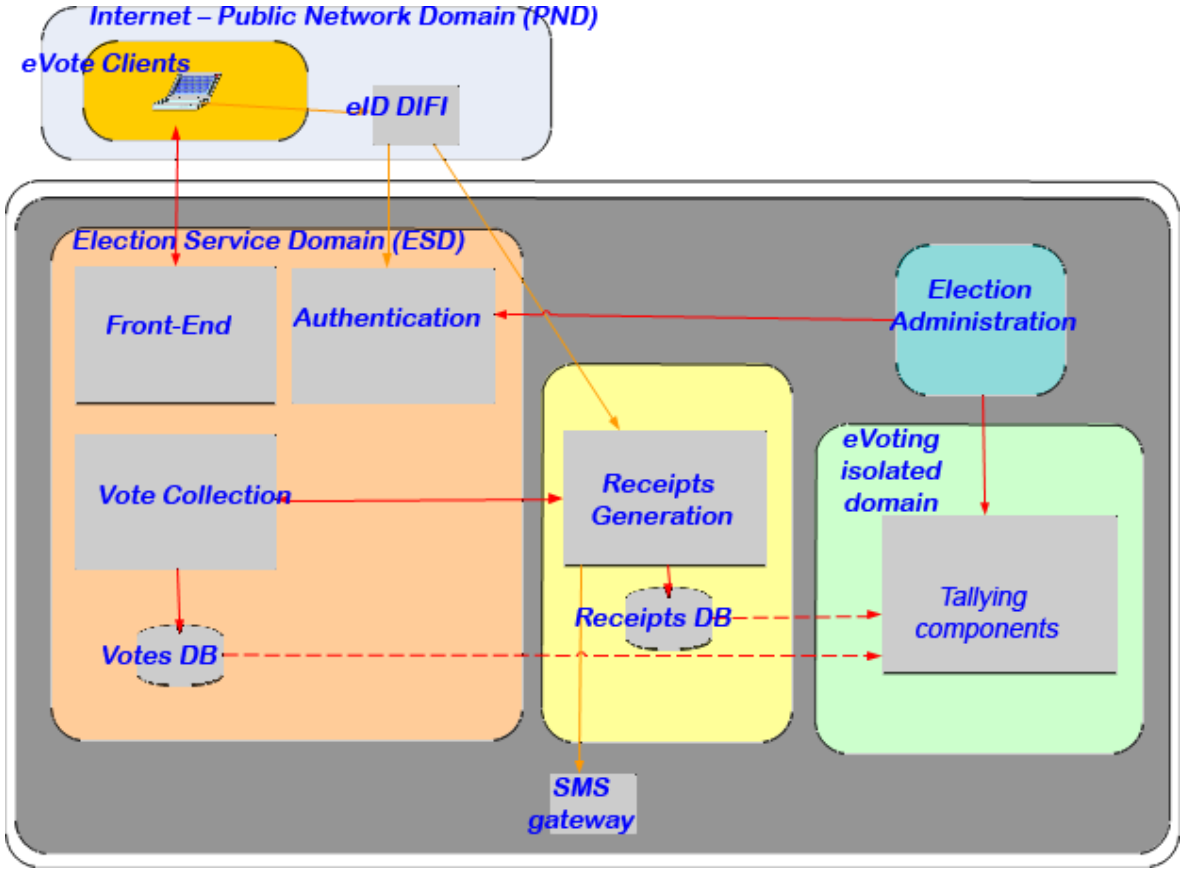
Problemas inherentes al voto por Internet

- Vistas las soluciones propuestas hasta el presente, yo no veo viable la utilización del voto por Internet en elecciones para diputados, concejales, etc.
- Al menos en España y Latinoamérica.
- Porque votando desde casa o desde cualquier lugar, la **coacción**, la **suplantación de personalidad** y la **venta de votos** son difíciles de evitar.
- Cuando los intereses puestos en juego son muy grandes esos ataques son esperables. (Piénsese en Ucrania).
- Pero hay multitud de **otro tipo** de elecciones no oficiales en las que el **voto por Internet** puede **ser muy útil**.

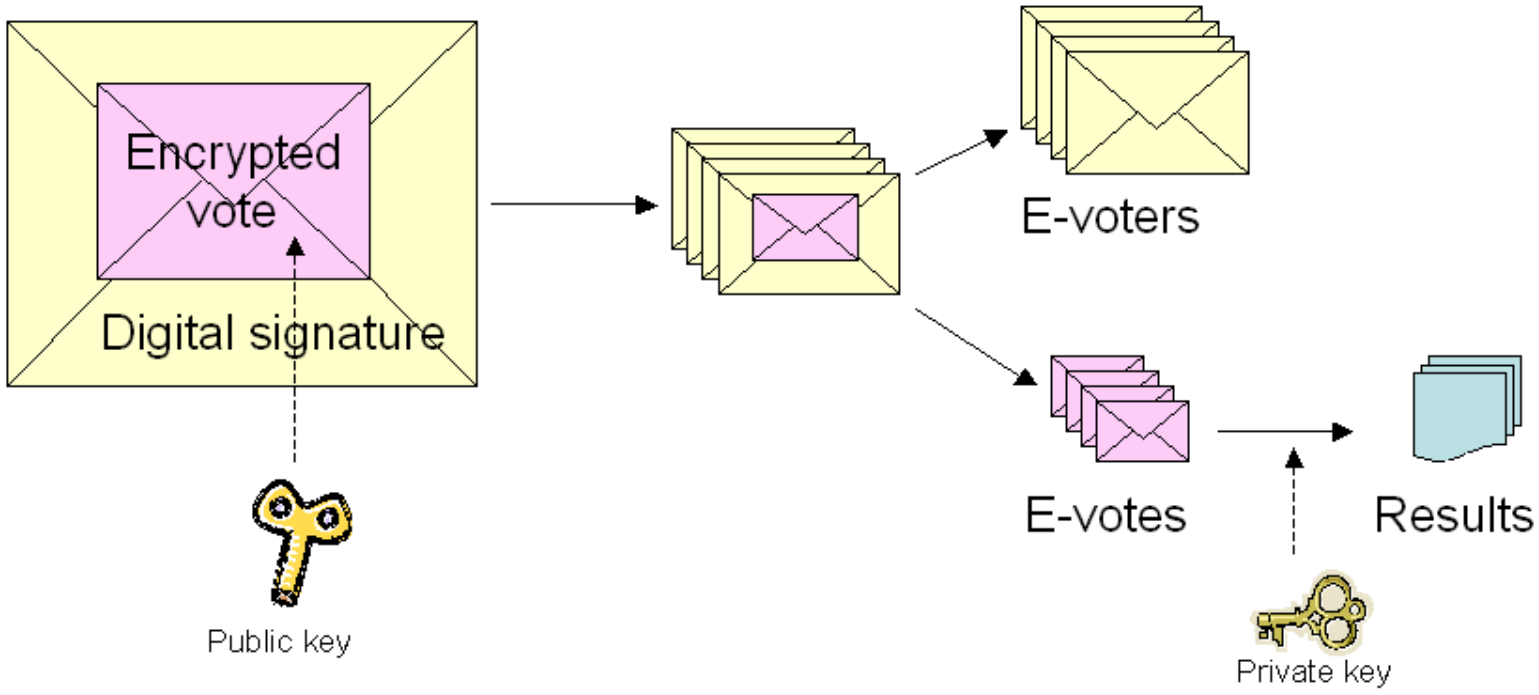
Estonia


Central System
Voter lists
Candidate lists
Voter application
Vote Forwarding Server
log
Vote Storage Server
log
Vote Counting Application
log
Key management
Audit application
Auditing

Noruega


Internet – Public Network Domain (PND)
eVote Clients
eID DIFI
Election Service Domain (ESD)
Front-End
Authentication
Election Administration
Vote Collection
Receipts Generation
eVoting isolated domain
Receipts DB
Tallying components
Votes DB
SMS gateway

Proceso


Encrypted vote
Digital signature
Public key
E-voters
E-votes
Results
Private key

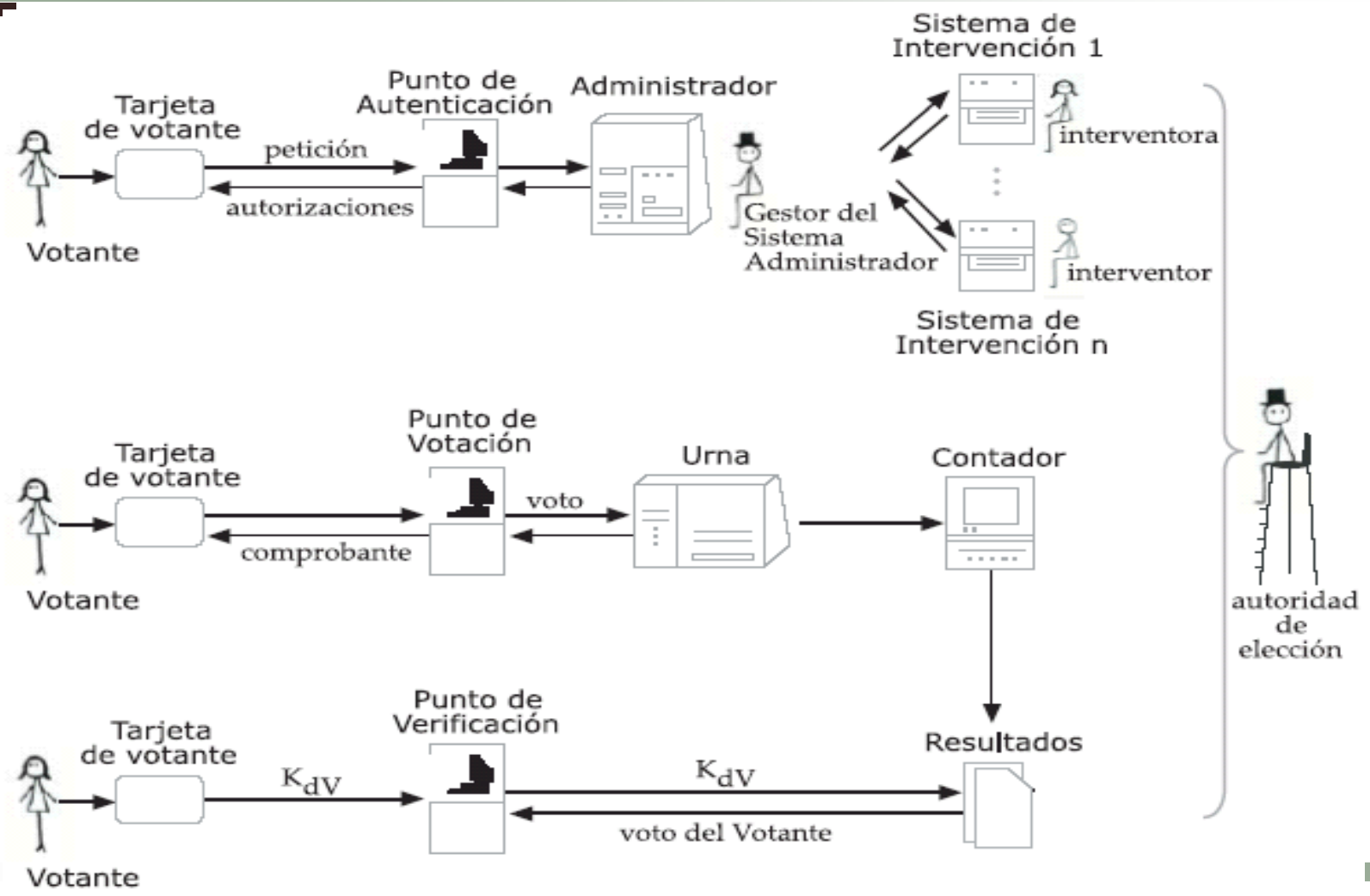
Estonia-Noruega. Resultado de la evaluación conforme al criterio de Seguridad de la Información

	SISTEMA DE VOTACIÓN	
	ESTONIA	NORUEGA
Identificación digital de votantes	●●●	●●
Protección frente a la suplantación de votantes	●●	●●
Usabilidad de la interfaz de votante	●	●
Seguridad criptográfica de la información intercambiada	●●●	●●●
Protección frente a ruptura del secreto del voto por una sola entidad	●●●	●●
Protección frente a ruptura del secreto del voto por colusión entre entidades	●	●
Protección frente a contabilización indebida de votos	●●	●●
Protección frente a denegación arbitraria de derecho a voto	●●●	●●●
● Bajo ●● Medio ●●● Alto		

Estonia-Noruega.
Resultado de la evaluación conforme a los criterios de verificación, auditoría y procedimiento

	SISTEMA DE VOTACIÓN	
	ESTONIA	NORUEGA
Identificación robusta de gestores del sistema	●●●	●●●
Verificación individual de voto	●	●
Verificabilidad de resultados	●	●●
Protección frente a la coacción	●	●
Protección del sistema frente a falsas acusaciones	●●	●●
Capacidad de supervisión de los interventores	●●	●●
Uso de software público	●	●●●
Auditabilidad del sistema	●●	●●
● Bajo ●● Medio ●●● Alto		

Votescript: voto telemático con puntos de votación. (versión de 2004)



Resumen de garantías que ofrece el sistema Votescript

- a) Se autentica al votante y se le autoriza a votar una sola vez.
- b) El voto se entrega de forma anónima y sin coacciones.
- c) El recuento se hace de forma fiable y auditable.
- d) El votante puede convencerse de que su voto ha sido tenido en cuenta correctamente.
- e) El votante recibe una prueba del sentido de su voto (para poder reclamar).
- f) Permitirse que ciudadanos autorizados supervisen todo el proceso.

Conclusiones (I)

- El sistema debe adecuarse a los requerimientos de los ciudadanos (de cada país) y no al revés.

- La implantación del voto telemático será un proceso creciente e imparable. Con toda seguridad, en algún momento la votación telemática será “lo natural” (como lo es actualmente usar el correo electrónico en lugar del correo postal).

Conclusiones (y II)

- Recomendamos ser prudentes y esperar hasta que la ciudadanía esté preparada y los desarrollos tecnológicos hayan adquirido la madurez necesaria.
- Mientras tanto sería muy interesante utilizar voto telemático en elecciones no validadas por el Estado.
- Conviene estar preparados, aunque solo sea para contrarrestar a quienes solo ven el voto una opción de negocio.
- Cambiar al voto telemático merece la pena únicamente si sirve para mejorar la relación de los ciudadanos con las instituciones democráticas y contribuye a reforzar su legitimidad