Sistemas de Votación y Autenticación de Votantes. Esquemas y Procesos de Auditorías y Seguridad Electoral

Encuentro Interamericano de Expertos y Representantes de Organismos Electorales sobre:

"Modernización y uso de las tecnologías electorales en el Hemisferio"

Caracas, abril 2008

Dr. Justo Carracedo Gallardo
EUIT de Telecomunicación, Universidad Politécnica de Madrid
director@euitt.upm.es

Ante cualquier innovación …

- Cualquier automatización de tareas que previamente se realizan de forma convencional:
  - Reporta unos beneficios para los usuarios que las llevan a cabo
  - Es vista como una “modernización” (presión social)
  - Presenta (siempre) riesgos
- Ante cualquier innovación: una balanza:
  - Ventajas que **aporta**
  - Riesgos que **comporta**

¿Qué decisión tomar?

Habría que ver qué plato de la balanza

pesa más

- Pero: ¿tenemos libertad para decidir?
- La evolución del entorno social que nos rodea:

¿Nos permite decidir?

¿Aparecen necesidades inducidas?

¿Sustituir el voto mediante boletas de papel?

- a) evaluar las ventajas y los riesgos del sistema que se pretenda implantar
- b) ¿es factible establecer protecciones razonables para **minimizar** los riesgos
- c) el sistema debe adecuarse a los requerimientos de los ciudadanos (de cada país) y no al revés

Para saber a qué nos referimos

- Primer nivel: automatización de algunas tareas
- Segundo nivel: voto electrónico
  - Automatización de todo el proceso
  - Máquinas electrónicas a la vista del votante donde se deposita el voto (que sustituyen a las antiguas urnas para boletas de papel)
- Tercer nivel: voto telemático
  - Uso de **redes** telemáticas y **agentes** telemáticos
  - Los votos se depositan en un agente telemático remoto =>**Urna** remota fuera de la vista del votante
  - La **autorización** para votar y el **voto** “viajan” por la red
  - Dos escenarios para el voto telemático
    - 1) votar desde cualquier sitio (también desde casa)
    - 2) votar desde **puntos específicos de votación**
    - (Así opera el Sistema Votescript)

¿Porqué denominarlo **voto telemático** y no voto a través de **Internet**?

- Internet es una infraestructura de transporte de datos (y muchísimo más)
- Internet significa apertura y multiplicidad de accesos
- Algunas propuestas de **voto telemático** que permiten votar desde cualquier sitio (también **desde casa**) usando los servidores de Internet sí podrían denominarse “voto por Internet”
- El voto telemático desde **puntos específicos de votación** debe estar soportado por **agentes telemáticos propios** y usar una red telemática “propia” **dedicada solamente** al proceso de votación
- (En realidad, esta “red propia” **podrá** ser una red virtual “apoyada” en la infraestructura de transporte de datos de Internet)

Voto telemático desde cualquier sitio

- Votar desde casa a través de Internet es inviable en el medio plazo
  - Porque votar es un acto social, es un acto colectivo
  - Porque votando desde casa la **coacción**, la **suplantación de personalidad** y la **venta de votos** son fáciles de perpetrar
  - Por muchas otras razones

En el sistema VOTESCRIPT

- Es necesario acudir a los lugares de votación, donde hay:
  - Puntos de autenticación
  - Cabinas de votación
  - Cabinas de verificación
- Y además la red virtual de votación está dividida en varias redes virtuales independientes para preservar el anonimato

Tres alternativas en la automatización de los procesos de votación)

- A) El pasado: mantener el sistema clásico de voto mediante boletas de papel automatizando solamente procesos complementarios
- B) El presente: implantar sistemas de voto electrónico con máquinas de votación “in situ”, incluyendo redes telemáticas para transmisión de datos. (Presente **brillante** y prometedor)
- C) El futuro: voto telemático (descartando por ahora pensar en la votación desde casa)

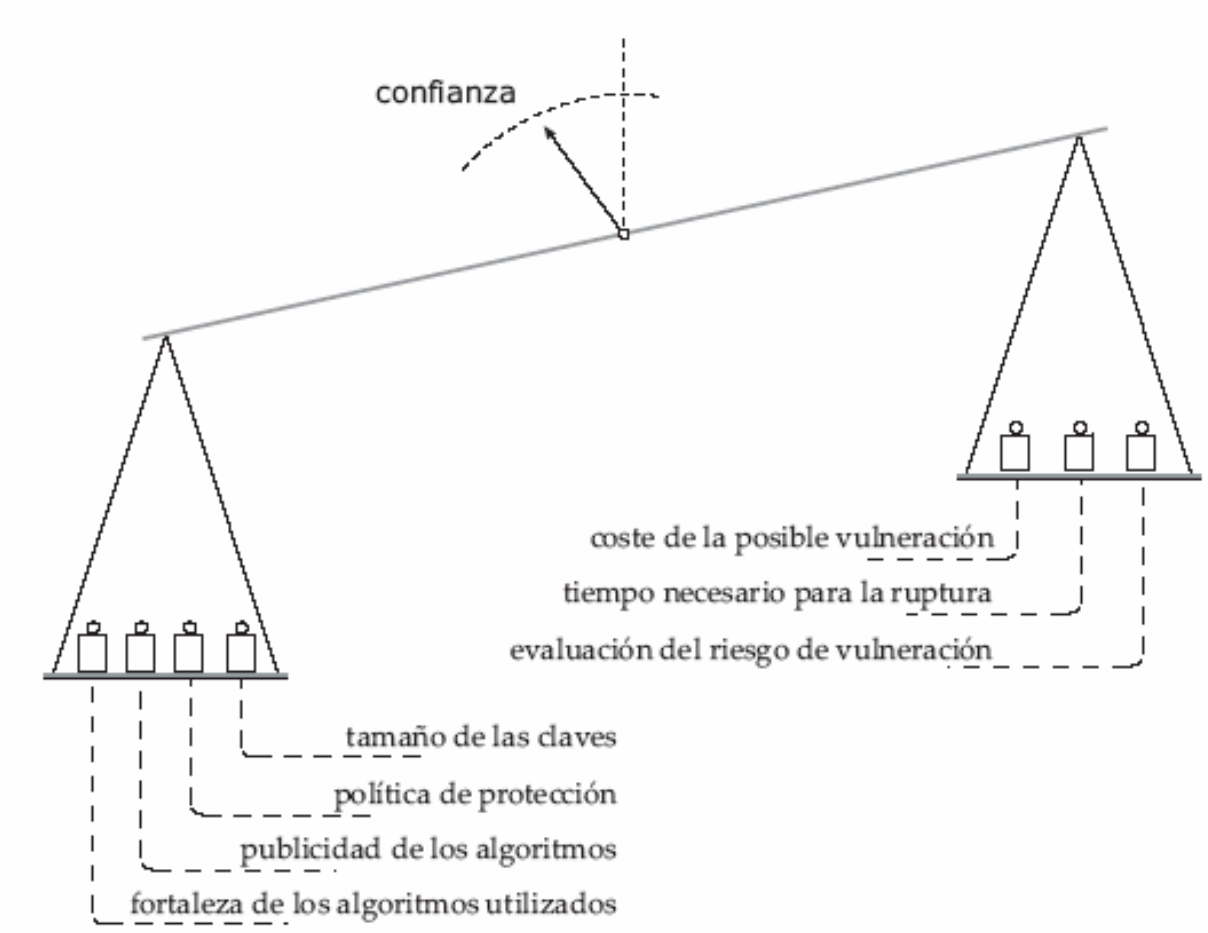
Protección de las redes en el voto telemático

- Las redes presentan un marco idóneo para posibles ataques y operaciones no autorizadas
- Los **servicios de seguridad** protegen las comunicaciones de los usuarios ante determinados ataques externos
  - Autenticación
  - Integridad
  - Confidencialidad
  - Anonimato
  - etc

En el voto telemático, en comparación con el voto electrónico

- Los requerimientos sociopolíticos son bastante más exigentes
- Las exigencias tecnológicas son muchísimo mayores
- Las protecciones de seguridad necesarias están en otro orden de magnitud
  - Protecciones organizacionales
  - Protecciones mediante mecanismos criptográficos robustos
- Los algoritmos pueden (deben) ser públicos: la seguridad reside en las claves criptográficas.
- Hay que proveer sincronizadamente:
  - Autenticación
  - Anonimato

Confianza en los sistemas protegidos con servicios telemáticos de seguridad



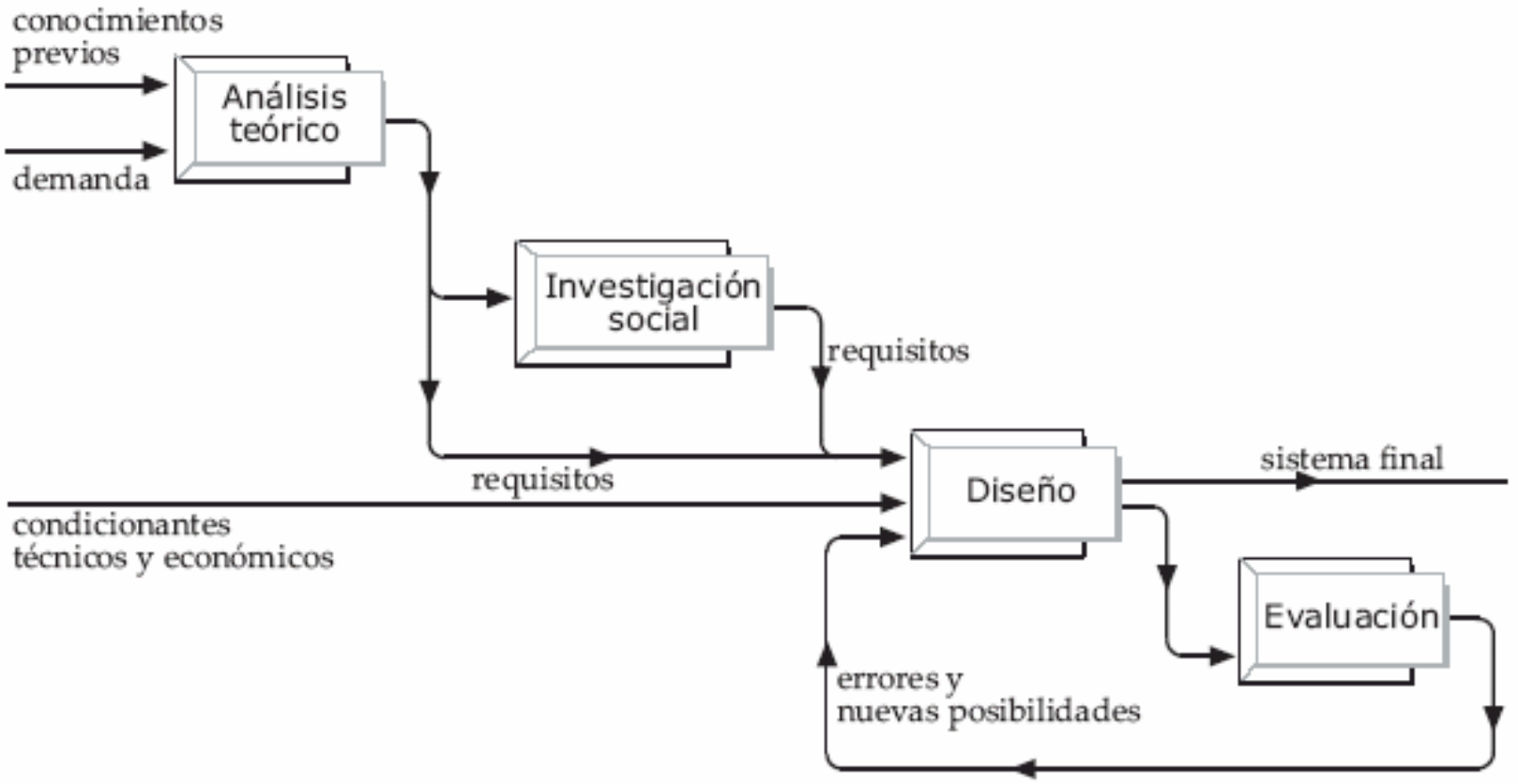
¿Porqué pensar en sistemas de voto telemático? (I)

- Su desarrollo es complejo **inicialmente**
- Pero aportan algunas **ventajas** sustantivas:
  - Voto frecuente (sobre todo en países que demandan procesos electorales reiterados)
  - En un futuro, permite **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
  - Voto 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 distintas discapacidades

¿Porqué pensar en sistemas de voto telemático? (II)

- En la Sociedad de la Información (entre otras cosas) se tiende a **reemplazar** comunicaciones convencionales por comunicaciones mediadas por ordenador (CMC)
- Es un proceso **creciente e imparable**
- Con toda seguridad, **en algún momento**, la votación telemática será "lo natural". (Como montar en auto en lugar de montar en burro)
- Es mejor **estar preparados**, aunque solo sea para contrarrestar a los vendedores de inventos perniciosos para la salud social (necesidades inducidas)
- Inicialmente debería implementarse en **colectivos "acotados"** de complejidad abordable
- Por ejemplo, desde el punto de vista de España, podría sustituir con ventajas:
  - Al voto por correo (que en España es muy vulnerable)
  - Al voto de los emigrantes desde otro país

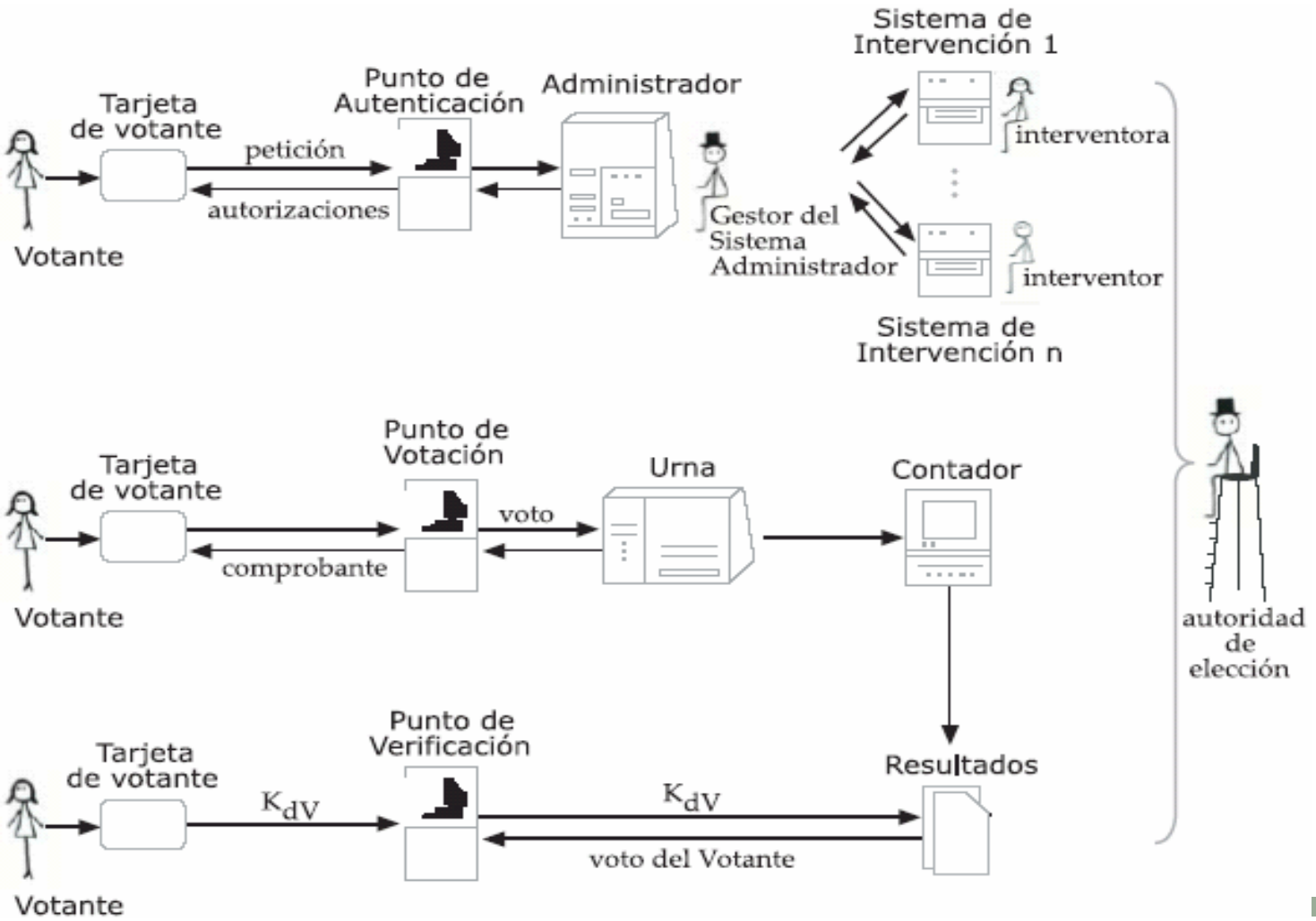
Determinación de requisitos en Votescript



Resumen de requisitos para el sistema VOTESCRIPT

- a) Hay que autenticar al votante y autorizarle a votar una sola vez
- b) El voto debe entregarse de forma anónima y sin coacciones
- c) El recuento debe hacerse de forma fiable y auditable
- d) El Votante debe convencerse de que su voto ha sido tenido en cuenta correctamente
- e) El votante debe recibir una prueba del sentido de su voto (para poder reclamar)
- f) Debe permitirse que ciudadanos autorizados supervisen todo el proceso

Votescript: sistema simplificado de la versión de enero 2004



Una referencia bibliográfica

- Una referencia bibliográfica acerca de Votescript y otros sistemas de votación telemática:

  Seguridad en Redes Telemáticas

  Autor: Justo Carracedo Gallardo

  Editorial: McGraw Hill, 2004

- El capítulo 11 puede verse en: **criptored**

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

Secreto y titularidad de un sistema de voto telemático

- En la votación telemática
  - Todos los que colaboren deben ser gratificados
    - Desarrolladores,
    - empresas de servicio, fabricantes de equipos, instaladores,...
  - Pero: ¡¡¡El sistema **no debe** ser de propiedad privada!!!
  - Debe ser propiedad de la autoridad electoral de cada Estado

- Deben ser conocidos y auditables:

  a) la definición y especificación del sistema y de los protocolos

  b) los códigos fuente de los programas, etc. etc.

- Además, el sistema debe adecuarse a los ciudadanos (de cada país) y no al revés