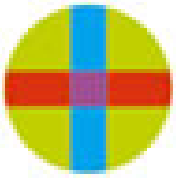

CEU
Universidad
San Pablo

Aquí va el nombre del proyecto

José Carlos Jiménez Gómez

21 de febrero de 2013

Agradecimientos

Resumen

Con el creciente desarrollo de la tecnología y su implantación en la mayoría de los campos de la vida cotidiana, es inevitable pensar en soluciones electrónicas para un elemento tan importante de nuestra sociedad como son los procesos electorales.

Encontramos procesos electorales en multitud de organizaciones, desde estados nacionales a empresas privadas, pasando por juntas de administraciones u organismos públicos.

En cambio, contrario a lo que puede parecer por el intenso uso de las nuevas tecnologías en campos como las transacciones bancarias, telemedicina, comunicaciones o gestiones con la Administración, en el mundo electoral no se está terminando de introducir el voto telemático a gran escala. De hecho, aunque encontramos algunas excepciones como pueden ser Estonia, Venezuela, Brasil y algunos territorios más reducidos, no se utiliza a estos niveles en la totalidad del proceso electoral, quedando reducido a algunas fases del proceso o, simplemente, a ninguna.

En este PFC, vamos a evaluar la implantación del voto telemático a pequeña escala para tratar de escalar los problemas que comportan a nivel nacional. Para ello, vamos a realizar un sistema que soportará de forma íntegra las elecciones a la Junta de Escuela de la Escuela Politécnica Superior de la Universidad San Pablo CEU.

A partir de este desarrollo, trataremos de hacer frente, a pequeña escala, a los problemas que nos encontramos en estas grandes elecciones, aunque para ello tengamos que variar los requisitos ideales para la simple consecución de la elección que implementamos.

Abstract

Introducción

Este proyecto trata de entrar en la problemática del voto electrónico remoto y presencial, de las reticencias sociales y tecnológicas que influyen en su reducida implantación en procesos electorales de gran importancia y alto número de electores. Para ello, vamos a reproducir la situación a escala reducida. Plantearemos una posible solución al proceso necesario para llevar a cabo las Elecciones a la Junta de Escuela de la Escuela Politécnica Superior de la Universidad San Pablo - CEU.

Con este planteamiento es obvio que no vamos a solucionar las trabas técnicas y sociales del voto por internet a nivel de unas elecciones legislativas en, por ejemplo, España. Es un tema que se escapa del objetivo de este PFC, pero sí que vamos a tratar de identificar algunos de los agentes influyentes y buscar una posible solución aplicable a la elección a la Junta de Escuela.

Así, conseguiremos dos objetivos. Por un lado, estudiar la dificultad existente para la implantación del voto electrónico en las elecciones nacionales. Por otro, un soporte electrónico al proceso completo de las Elecciones a la Junta de Escuela, con el cual obtendremos una mejora significativa en el mismo respecto a procesos anteriores.

La forma de llegar a la solución buscada debe comenzar identificando los factores que afectan a un proceso electoral general y, a continuación, personalizar los que se encuentran en el que vamos a estudiar. Una vez identificados estos agentes, definiremos las fases que comportan unas elecciones y estudiaremos cómo podrían ser apoyadas tecnológicamente, evaluando cómo llegar al punto óptimo de integración con el sistema tradicional para mejorar el proceso.

La primera fase se concentrará en desarrollar los sistemas asociados a la

fase preelectoral. En ella, se recoge el censo electoral y se identifican tanto los candidatos como los diferentes cargos que se votan.

La segunda fase, la electoral, la identificamos con los procesos que se requieren durante el periodo que dura la elección (ya sea un día o varios). Esta consistirá en desarrollar los sistemas de identificación y validación de votantes, el sistema de votación, ss

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Planteamiento

1.1. Objetivos finales del proyecto

1.1.1. Descripción del sistema real

Capítulo 2

Temp

Según el documento **NORMAS DE ORGANIZACIÓN Y FUNCIONAMIENTO DE LA UNIVERSIDAD SAN PABLO-CEU**, en su Artículo 9, "Las Facultades, Escuelas y Centros integrados o adscritos son las instancias responsables de la organización de la enseñanza e investigación, de acuerdo con las directrices emanadas de los órganos superiores de la Universidad, y de los procesos académicos, administrativos y de gestión conducentes a la obtención de títulos de carácter oficial y validez en todo el territorio nacional, así como de aquellas otras funciones que determinen las presentes Normas de Organización y Funcionamiento y los restantes reglamentos universitarios."

A partir de esta definición, en el Capítulo II De los órganos académicos, encontramos el Artículo 22 Tipos de órganos, donde se establece que (1c) que las Juntas de Facultad, Escuela o Centro son órganos colegiados. Y encontramos su definición en el Artículo 31 Las Juntas de Centros, donde podemos leer que "La Junta de Facultad, Escuela o Centro es el órgano colegiado de gobierno del mismo, que ejerce sus funciones con vinculación a los acuerdos del Patronato, Consejo de Gobierno y resoluciones del Rector."

También podemos destacar los artículos 32 y 33, donde se establece la composición y funciones de las Juntas de Facultad, Centro o Escuela.

Artículo 32 Composición de las Juntas La Junta de Facultad, Escuela o Centro estará compuesta por miembros natos y electos. Son miembros

natos: El Decano o Director, que presidirá sus reuniones; los Vicedecanos o Subdirectores, el Secretario académico, que levantará acta de sus sesiones y los Directores de los Departamentos integrados en la Facultad o Escuela. Son miembros electos: Quienes resulten elegidos en representación del profesorado y de los alumnos de acuerdo con la normativa que reglamentariamente se establezca.

Artículo 33 Funciones de las Juntas Las competencias de la Junta de Facultad, Escuela o Centro son:

a) Colaborar con el Decano o Director en la gestión de la Facultad, Escuela o Centro.

b) Promover el perfeccionamiento de los planes de estudio y de la metodología docente, así como el establecimiento de nuevos títulos tanto propios como oficiales.

c) Participar en la programación de las actividades de extensión universitaria.

d) Velar por la adecuada dotación de los servicios necesarios para su correcto funcionamiento.

e) Cualquier otra competencia que le pueda ser atribuida en el desarrollo de estas Normas de Organización y Funcionamiento.

Tipos de Voto Electrónico

- Presenciales
  - Urna electrónica (Sistema DRE - Direct-Recording Electronic - sistema de registro electrónico directo): facilita el voto a través de una pantalla táctil, teclado u otro dispositivo. La máquina DRE permite la captura, almacenamiento y escrutinio de los votos.
  - Sistema reconocedor de marca óptica: El votante marca su voto en una papeleta mediante un bolígrafo, por ejemplo, y la inserta en un lector o escáner, a través del cual la máquina automáticamente registra el voto para su posterior contabilización.

- Remotos
  - Sistema de votación telemática a través de Internet: el elector vota mediante una aplicación cliente (normalmente un navegador web) que envía el voto a través de Internet al servidor donde queda almacenado.
  - Sistema de votación telemática a través de dispositivos móviles: el elector vota mediante una aplicación cliente que envía el voto a través de una red móvil e Internet, dependiendo del caso, al servidor donde queda almacenado.

REQUISITOS DESEABLES EN LOS SISTEMAS DE VOTO ELECTRÓNICO

Autenticidad : Sólo los votantes autorizados pueden votar.

Anonimato : El voto es secreto.

Verificabilidad : El votante puede asegurarse de que su voto se ha contado adecuadamente.

Imposibilidad de coacción : El voto emitido no puede ser mostrado.

Posibilidad de emitir un voto nulo .

Fiabilidad : el sistema debe asegurar que no se producen alteraciones de los resultados.

Auditabilidad : se debe poder comprobar que el funcionamiento de los elementos que intervienen en el proceso es correcto.

Usabilidad : cualquier votante debe ser capaz de emitir un voto en un tiempo razonable.

Aplicaciones

Gestión del censo electoral : altas, bajas, informes, solicitud, tramitación del voto por correo...

Gestión de candidatos : solicitud, aprobaciones, difusión del perfil y propaganda...

Gestión del proceso electoral : apertura de urnas, cierre de urnas, descifrado, introducción de votos por correo, escrutinio, recuento, presentación de actas electorales...

Aplicaciones de voto : todas aquellas que mecanizan la ejecución del voto, el almacenamiento y su posterior recuento.

Presentación general de actas y resultados electorales .

A la hora de llevar a cabo una elección con soporte tecnológico, encontramos muchas arquitecturas y una implantación variable del nivel técnico, el cual es más acusado en algunos procesos, llegando hasta el voto digital, mientras en otras se limitan a la fase de identificación del votante, del censo electrónico, del escrutinio o tan sólo de la difusión de resultados.

En base a este concepto y observando algunos procesos electorales anteriores, podemos discernir informalmente varios tipos o fases propias de "elecciones electrónicas":

- e-Counting
- e-Voting
- i-Voting

En elecciones como las legislativas de España de 2011, pudimos ver avances tecnológicos como los denominados, por la empresa Indra - la que llevó a cabo el apoyo tecnológico- MAEs (Mesa Administrada Electrónicamente) que servían como control del censo de la mesa a la que estaban asignadas. Esto es un ejemplo de cómo se puede introducir la tecnología a una parte del proceso electoral. Con estos dispositivos, lo que se conseguía era que los miembros de mesa pudiesen identificar al votante en el censo haciendo uso tan sólo del DNIe del mismo, el cual introducían en el lector incorporado en el equipo y mostraba la información del votante, indicando sus datos personales para cotejo de los miembros de la mesa, así como si había hecho o no uso de su

derecho al voto, con lo que se le podía permitir votar o no. Además, tan sólo informaba de aquellos votantes que debían votar en esa mesa, alertando de que no estaban en el censo en el caso que así fuese. Con este mismo sistema, se podían imprimir, inmediatamente después de cerrar la mesa y contar los votos (a mano) .....

El proceso de votación en la selecciones de Estonia sigue este paradigma:

1. El votante accede al VFS a través de una conexión con protocolo HTTPS y se identifica con su ID-card.

2. El VFS lanza una query usando el Código de Identificación Personal (PIC) a la base de datos de votantes, verifica la ****EINSS****elegibilidad del votante e identifica su ****EINSS****constituency. Si el votante no es ****EINSS****elegible, se envía un mensaje correspondiente.

3. El VFS lanza una query contra el VSS consultando si el votante ya ha votado. Si este es el caso, se informa al votante de ello.

4. El VFS lanza una query usando los datos de ****EINSS****constituency de la base de datos de votante y como resultado recibe la lista de candidatos en esa ****EINSS****constituency. Se muestra la lista al votante.

5. El votante elige un cadidato.

6. La aplicación del votante, teniendo la lista de candiadatos, pide al votante que confirme su elección.

7. La aplicación encripta la elección (choice) y un número aleatorio con la clave pública del VCA. El votante firma el criptograma (a partir de ahora: voto) con su firma digital.

8. La aplicación de votante transmite el sobre firmado digitalmente al VFS, el cual verifica ****EINSS****the formal correctness del material recibido y si la misma persona que se autentificó durante el comienzo de la sesión es la que dió la firma digital.

9. EL VFS redirige el voto recibido al VSS. EL VSS accede al ****EINSS****servidor de confirmación de validez y adquiere un certificado de confirmación de la validez de la firma digital que se ha añadido al voto firmado.

10. En caso de un voto ****EINSS****exitoso, el VSS envía al VFS una confirmación de que el voto ha sido recibido. Un mensaje correspondiente se ****EINSS****deliver también al votante. Una entrada sobre la recepción del voto se graba en el fichero de log (LOG1), usando el formato [PIC, hash(vote)].

11. El votante puede votar varias veces. Todos los votos se transmiten a través del VFS al VSS. En caso de que se reciba un voto reptido, el voto anterior es automáticamente ****EINSS****revoked y se grabará una entrada en el fichero de log correspondiente (LOG2) en la forma [PIC, hash(vote), razón].

12. Al terminar el proceso de voto electrónico, el VFS finaliza todas las comunicaciones.

Si el servidor de confirmación de validez no está disponible en el momento en el que se está produciendo la votación, se almacena la hora en la que el voto se ha recibido. El servicio de confirmación de validez permite verificar la validez del certificado en una etapa posterior. La hora en el servidor del sistema y en el servidor de confirmación de validez deben estar sincronizada. Todas las confirmaciones de validez deben recibirse antes del comienzo de la siguiente fase.

Según Fujioka et al.: Properties of a Secure Secret Voting Scheme Fujioka et al. defines seven requirements of a secure secret election.

1. Completeness: All valid votes are counted correctly.

2. Soundness: The dishonest voter cannot disrupt the voting.

3. Privacy: All votes must be secret.

4. Unreusability: No voter can vote twice.

5. Eligibility: No one who is not allowed to vote can vote.
6. Fairness: Nothing must affect the voting.
7. Verifiability: No one can falsify the result of the voting. Another requierent is:
8. Receipt-freeness: The voter does not need to keep any record of his vote. Also, we can add some requirements defined by Schneier about e-voting.
9. Non-Duplication: No one can duplicate anyone else's vote.
10. Public Participation: Everyone knows who did, and did not, vote.
11. Private Error Correction: A voter can prove his vote was miscounted without revealing how he voted.

Bibliografía

[1] Gordillo, Rafael. .ejemplo de artículo". *REAL BETIS - SEVILLA*, 2007.

[2] Autor1, Nombre / Soy el Autor2, Nombre2 / Incluso HayAutor3, Soy Y. .aquí va el título de esto que no se ha publicado". Aquí va una nota, 2008.

[3] Sitio web de selenium. http://www.selenium.es.

[4] Beck, Kent and Andres, Cynthia. *Extreme Programming Explained: Embrace Change (2nd Edition)*. Addison-Wesley, 2004.