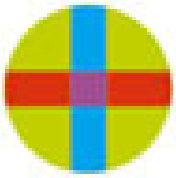

CEU
Universidad
San Pablo

Aquí va el nombre del proyecto

José Carlos Jiménez Gómez

26 de junio de 2014

Agradecimientos

AquÃ hay que ser agradecido, que es de bien nacidos.

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 de voto por internet 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 establecer requisitos que resulten exagerados para la consecución de la elección que implementamos por su simplicidad frente a un proceso a nivel nacional o autonómico.

Abstract

Abstract in English.

Introducción

Este proyecto trata de entrar en la problemática del voto electrónico remoto frente al 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 por internet 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.

Antes de entrar en detalle en el proceso, habrá que definir el tipo de votación que queremos implementar. No se habla en este PFC de voto electrónico como tal, ni siquiera de voto electrónico remoto. Lo que se quiere implementar es una solución de voto por internet, en el que no haga falta la presencia física del votante en el centro de votación, que tenga la oportunidad de ejercer su derecho al voto desde cualquier punto del planeta con conexión a internet. Este detalle, que puede parecer trivial al querer separarlo del concepto de voto electrónico, en realidad es fundamental. En un próximo

capítulo se ahondará en ello, pero podemos avanzar que una de las grandes diferencias a tener en cuenta es que con voto electrónico remoto, podemos utilizar máquinas de votación (que también emitirían el voto por internet), las cuales pueden generar un recibo con el voto emitido por el votante, al estilo de las papeletas que llenan la urna electoral, mientras que con el voto por internet puro, esto no es tan obvio. Con este mecanismo, la auditoría es más simple para el voto electrónico con máquinas en el centro de votación, pues se podrían contar las papeletas generadas. ¿Qué ocurre con el voto por internet, en el que no se generan estos recibos ni hay una urna física donde se depositan? ¿Qué ocurre si el sistema tiene fallas y no se contabilizan (o lo hacen de forma incorrecta) los sufragios, teniendo en cuenta que puede ser imposible un conteo físico de papeletas al no existir estas? Pues como estas, hay muchas cuestiones a las que el voto por internet debe dar solución de forma fiable antes de poder acometer su implantación en procesos electorales de envergadura e importancia.

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

0.1. Antecedentes

El voto electrónico se lleva tratando de desarrollar e implementar desde hace bastante tiempo. Concretamente, podríamos datar el comienzo en el año 1868, cuando el inventor estadounidense Thomas Alva Edison (1847-1931) registró su primera patente, consistente en un instrumento simple para el recuento mecánico de votos. El instrumento se podía colocar en la mesa delante de cada congresista y tenía dos botones, uno para el voto a favor y otro para el voto en contra. Pese a considerarlo un avance, no consiguió ser aceptado en el Congreso de Washington, donde le dieron el siguiente motivo para argumentar el rechazo de los representantes a esta nueva tecnología: XXXXOJO "*If there is any invention on Earth that we don't want down here, that is it.Joven, si hay en la tierra algún invento que no queremos aquí, es exactamente el suyo. Uno de nuestros principales intereses es evitar fraudes en las votaciones, y su aparato no haría otra cosa que favorecerlos*".

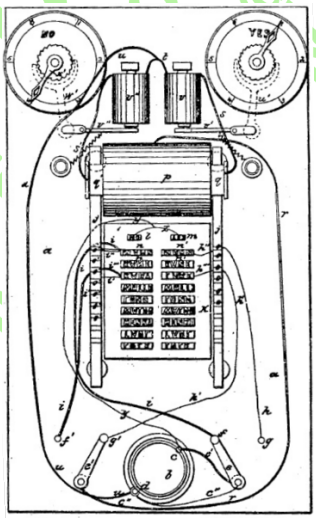

Figura 1: U.S. Patent 0,090,646 – Electrographic Vote-Recorder: Primera patente de Thomas A. Edison. Permitía un voto de tipo 'A favor' o 'En contra' a través de dos interruptores. (1869). Fuente: Wikipedia

A partir de este intento, el voto electrónico ha avanzado tecnológica y socialmente, logrando herramientas más sofisticadas y seguras en conjunción con un entendimiento, comprensión y, en algunos casos, aceptación de su

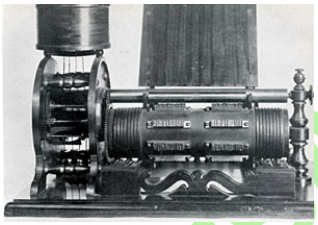

Figura 2: Electrographic Vote-Recorder: Fotografía del invento de Thomas A. Edison. Fuente: Rutgers.edu

uso. Ambos factores han hecho posible que se hayan podido implementar soluciones e integrarlas en procesos electorales reales, ya sea a nivel nacional o de entidades o estamentos.

Experiencias de voto electrónico Vamos a realizar una pequeña muestra de elecciones realizadas con elementos propios del voto electrónico.

España En España

0.2. Estado de la cuestión

En lo referente al voto electrónico...

En cuanto al estado de la cuestión del voto por internet, como hemos destacado, la experiencia más ambiciosa es, sin duda, las elecciones que se llevan a cabo en Estonia, que, desde el año 2005, proveen de un sistema de voto por internet a un cierto sector de la población. Es destacable el desempeño de empresas como la española Scytl, que ha implementado sistemas de voto por internet para voto desde el extranjero para algunos condados de Estados Unidos, ciertos cantones de Suiza y varias provincias de India, la mayor democracia del mundo (en número de votantes).

0.2.1. Voto por internet (i-voting)

Estonia. Estonia es quizá el ejemplo más destacado en cuanto a la utilización del voto por internet en elecciones a nivel estatal. Desde el año 2005 lleva usando una solución de voto electrónico remoto no presencial mezclado con el voto tradicional. El impacto del voto electrónico sobre el electorado

estonio ha ido evolucionando en cada comicio. En el 2005, el primer año en que se comenzó a utilizar, no llegó al 2 % de los votantes los que se decantaron por votar por internet, mientras que en el 2014, este porcentaje superó el 30 % de los sufragistas.

0.2.2. Voto por internet en la EPS

En la Escuela Politécnica Superior de la Universidad San Pablo-CEU ya se realizó una elección por medio de voto electrónico. Sucedió en 2005, cuando en una colaboración entre la Universidad y la multinacional INDRA se celebró la primera elección de delegados de clase a través de voto electrónico con motivo del Día de Internet. En esta experiencia, más de 600 alumnos de los últimos cursos de la Escuela Politécnica eligieron a sus delegados de clase a través de este sistema. En la fecha de la elección, cada alumno emitió su voto a través de un nombre de usuario y una clave personales. Por motivos divulgativos, los organizadores de la elección determinaron que una parte del alumnado censado realizara la votación desde un aula de votación concreta, perteneciente al centro y adecuada para ello; mientras que el resto del alumnado debía elegir sus representantes desde algún equipo personal fuera del dominio de la Universidad. Para que estas elecciones a través de Internet pudiesen llevarse a cabo la Universidad San Pablo-CEU tuvo que adaptar su normativa de régimen interno, pues la que tenía originalmente establecía únicamente la posibilidad de un sistema de voto presencial.

Índice general

0.1. Antecedentes 6
0.2. Estado de la cuestión 7
0.2.1. Voto por internet (i-voting) 7
0.2.2. Voto por internet en la EPS 8

Índice de Figuras **10**

Índice de Tablas **11**

1. Planteamiento **12**
1.1. Objetivos finales del proyecto 12
1.1.1. Descripción del sistema real 12
1.2. Alcance del proyecto 12
1.3. Especificación de requisitos 12

2. Riesgos **13**
2.1. Identificación y gestión de riesgos 13
2.1.1. Identificación de riesgos 13

3. Solución **14**

4. Temp **15**

5. TempEleccionJuntaEscuela **25**

Bibliografía **25**

Índice de figuras

1. U.S. Patent 0,090,646 – Electrographic Vote-Recorder: Primera patente de Thomas A. Edison. Permitía un voto de tipo 'A favor' o 'En contra' a través de dos interruptores. (1869). Fuente: Wikipedia 6
2. Electrographic Vote-Recorder: Fotografía del invento de Thomas A. Edison. Fuente: Rutgers.edu 7

Índice de tablas

Capítulo 1

Planteamiento

1.1. Objetivos finales del proyecto

1.1.1. Descripción del sistema real

1.2. Alcance del proyecto

1.3. Especificación de requisitos

1. Votación por internet
2. Disponibilidad 24/7
3. Todos los requisitos del voto electrónico

temporal ——————————————— La idea es un sistema para la votación de la Junta de Escuela. El sistema debe permitir el voto remoto desde cualquier punto con conexión a internet (incluyendo equipos preparados en la propia Escuela). El voto es secreto.

Capítulo 2

Riesgos

2.1. Identificación y gestión de riesgos

(Uno de los riesgos que hay que tener en cuenta en este tipo de elecciones es la fecha límite. Tiene que funcionar durante un cierto período de tiempo, sin fallo y sin posibilidad de modificación -relativamente-)

2.1.1. Identificación de riesgos

Capítulo 3

Solución

Capítulo 4

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 requirement 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.

Según Fujioka, "Decimos que un esquema de voto secreto es seguro si tenemos lo siguiente:

1. Completitud (Completeness): Todos los votos válidos se cuentan correctamente.
2. Solidez (Soundness): Un votante deshonesto no puede interrumpir la votación.
3. Privacidad (Privacy): Todos los votos deben ser secretos.
4. ???????? (Unreusability): Ningún votante puede votar dos veces.

5. REQUISITOS DE UN SISTEMA ELECTORAL Universal: Implica que deben estar habilitados para votar todos los ciudadanos que cumplan con un conjunto de condiciones (edad, nacionalidad, período de residencia en una determinada jurisdicción, etc.) y solamente ellos. Igual: Todos los ciudadanos que componen el universo de una elección deben poder votar sólo una vez. Todos los votos tienen el mismo valor: un ciudadano, un voto. Secreto: Debe asegurarse que la identidad de los ciudadanos no pueda ser vinculada, de ninguna forma, al voto que emitió. Es más, debe garantizarse que ni

siquiera el mismo elector tiene posibilidades de demostrar que votó de determinada manera. Personal: El voto debe ser emitido en forma personal por el ciudadano. Salvo el caso particular de los ciudadanos con alguna discapacidad especial la tarea de votar es indelegable. Obligatorio: En las elecciones el ciudadano debe votar obligatoriamente. Otros, como la condición de que el elector pueda emitir su voto libre de todo tipo de coerción, es consecuencia de los más elementales principios democráticos. De hecho, el secreto del voto apunta - entre otros objetivos - a garantizar esta situación. Otros requerimientos corresponden a la categoría de esperados o implícitos. Es así que el sistema debe ser, como mínimo, flexible, auditable y conveniente. Asignamos a cada uno de estos requisitos el siguiente significado: Flexible: El sistema debe ser capaz de adaptarse a distintos tipos de elecciones. Dado que la flexibilidad de un sistema basado en computadoras se logra fundamentalmente a través de su software, el mismo debe ser capaz de adaptarse a distintos tipos de elecciones. Existen, en este sentido, un par de alternativas de solución. La primera es construir un sistema totalmente parametrizable, de modo que sin modificar el código, pueda utilizarse para distintas elecciones.

Certificados Digitales X.509

Autoridad Certificadora

Diseño El Sistema Central tiene 2 bases de datos que se cargan en la fase preelectoral: Lista de Candidatos y Lista de Votantes (Censo). Una vez un votante ejerce su derecho al voto, cargamos en el Servidor de Votación una base de datos que reúne al votante, con el voto encriptado y el momento en el que ha votado (Timestamp). Cuando se finaliza la votación y se ordena el recuento, los votos almacenados en el SV, se envían (o se desechan, según el voto) al Servidor de Conteo, el cual llena 2 bases de datos diferentes, en una introduce los votos desencriptados y en la otra los votantes sin el voto. Yo introduciría otro servidor, el de totalización.

El votante entra en la url

Certificados digitales Basados en métodos criptográficos de clave asimétrica Asocian información de una persona o entidad con su clave pública La veracidad de esta asociación la garantiza la Autoridad de Certificación: FNMT Dirección General de Policía (DNIe) Camerfirma, CaCert, etc Regis-

tradores, Notarios, etc

Firma electrónica Permite mirgrar procesos basados en papel (que requerían firmas) a formato electrónico. Garantiza la autenticidad, integridad y no repudio del mensaje firmado. Firma Electrónica Avanzada (ley 59/2003) "firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se rfiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control" Formatos de firma electrónica: PKCS#7 (RSA Laboratories Inc.) XMLDSIG (Propuesta conjunta de estándar IETF/W3C) RFC 3075 XAdES (XML Advanced Electronic Signatures) Adobe PDF

Criptografía de clave asimétrica. Firma digital. Proceso Ana y Bernardo tienen sus pares de claves respectivas Ana escribe un mensaje a Bernardo. Es necesario que Bernardo pueda verificar que realmente es Ana quien ha enviado el mensaje. Por lo tanto Ana debe enviarlo firmado: 1. Resume el mensaje mediante una función hash. 2. Cifra el resultado de la función hash con su clave privada. De esta forma obtiene su firma digital. 3. Envía a Bernardo el mensaje original junto con la firma. Bernardo recibe el mensaje junto a la firma digital. Deberá comprobar la validez de ésta para dar por bueno el mensaje y reconocer al autor del mismo (integridad y autenticación). 4. Descifra el resumen del mensaje mediante la clave pública de Ana. 5. Aplica al mensaje la función hash para obtener el resumen. 6. Compara el resumen recibido con el obtenido a partir de la función hash. Si son iguales, Bernardo puede estar seguro de que quien ha enviado el mensaje es Ana y que éste no ha sido modificado. Con este sistema conseguimos: Autenticidad (la firma digital es equivalente a la firma física de un documento), Integridad (el mensaje no podrá ser modificado), No repudio en origen (el emisor no puede negar haber enviado el mensaje)

Firma electrónica: Aplicaciones Aplicaciones: Factura electrónica Voto electrónico Contratación Electrónica (licitación electrónica y e-subasta) Notificación Electrónica Procedimientos Administrativos electrónicos ...

Requisitos para desarrollar Aplicaciones Web con certificados digitales - Establecimiento de comunicación segura SSL (certificado de servidor) - Vali-

dación de certificados - Revocación de certificados – CRL (Certificate Revocation List) – OCSP (Online Certificate Status protocol) - Implementación de Autenticación y Firma

Implementación (Autenticación) - Instalar certificado raíz en servidor (almacén certificados máquina y habilitar todos los propósitos) - Configurar aplicación Web para requerir certificado digital - Leer el certificado (protocolo https) - Chequear la validez del certificado (revocación CRL - OCSP)

Implementación eFirma - Elección del formato(s) de firma – PKCS#7 – XMLDSIG – XADES - Creación de componente para firmar (activex, applet) o implementación basada en CAPICOM y Crypto - Implementación – CAPICOM (Internet Explorer) – Crypto (Mozilla) – Open Source (OpenSign) – JSR 105 (Java Specification Request #105 - WSDP de Java)

Sacado de "How security problems can compromise remote Internet Voting Systems" (del Dr. Guido Schryec). Riesgos y problemas del voto electrónico basados en estudios del MIT y el Caltech.

1. Primero hablamos de las diferencias entre el voto eléctronico (eVoting) y el comercio electrónico (eCommerce).
2. Security issues del cliente
3. Secutiry issues del servidor
4. Security issues de la conexión

Informe sobre voto electrónico en cuanto a riesgos y seguridad:

1. MIT
2. Caltech
3. SERVE (DoD)
4. Internet Policy Institute
5. i-vote
6. alemanes

Capítulo 5

TempEleccionJuntaEscuela

Empezamoss

Cada categoría de profesores (colaboradores, adjuntos, agregados y catedráticos) elegirá a dos representantes de entre los profesores con contrato a media jornada o jornada completa. Respecto a los alumnos: Cada titulación elegirá a dos representantes de entre todos los delegados de la titulación (dos de Teleco, dos de Informática, dos de Arquitectura y dos de Ingeniería de la Edificación)

Los profes votamos por categorías (los agregados a los suyos, etc.). La diferencia es que en el censo están todos (jornada completa, media jornada y tiempo parcial) pero sólo son elegibles de media jornada para arriba.

- Las categorías de profes son disjuntas; sólo votas en la tuya.

- En cuanto a los alumnos, cada grupo tiene dos delegados (delegado y subdelegado). Recuerda que en Arq. hay varios grupos en cada curso, eso hace un censo más amplio.

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.