UNIVERSIDAD SAN PABLO - CEU

ESCUELA POLITÉCNICA SUPERIOR

INGENIERÍA INFORMÁTICA

PROYECTO FINAL DE CARRERA

<TÍTULO DEL PROYECTO FINAL DE CARRERA>

Autor: José Carlos Jiménez Gómez
Director: Raúl García García

5 de julio de 2014

Versión SVN

Rev: **39**
2014-07-05 18:54:03 +0200 (sÃ¡b, 05 jul 2014)
por betisman@gmail.com

URL : https://pfc-carlosjg.googlecode.com/svn/trunk/doc/memoria/pfc.tex

Pagina reservada para la calificación del proyecto

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.

Agradecimientos

Es de bien nacidos ser agradecidos.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

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? 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

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*".

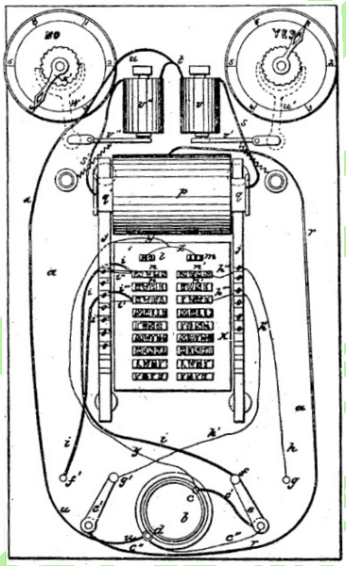

Figura 1.1: *U.S. Patent 0,090,646 – Electrographic Vote-Recorder: Primera patente de Thomas A. Edison. Permitía un voto de tipo 'A favor' o 'En contra' a través de dos interruptores. (1869). Fuente: Wikipedia*

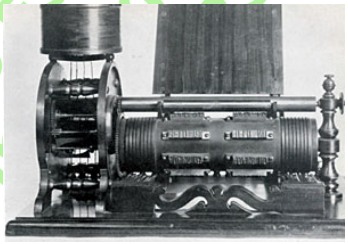

Figura 1.2: *Electrographic Vote-Recorder: Fotografía del invento de Thomas A. Edison. Fuente: Rutgers.edu*

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 uso. Estos 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.

Se considera que el inicio del desarrollo del voto electrónico moderno está datado en 1964, año en el que site condados de EEUU utilizaron un sistema de voto electrónico para las Elecciones Presidenciales.

Podemos estudiar el voto electrónico separándolo en varios niveles, dependiendo de su implantación en el proceso.

- Nivel 0

  Es el sistema de voto tradicional, sin hacer uso de elemenos electrónicos para llevar a cabo ninguna fase del proceso. Es el sistema que se ha venido utilizando desde las primeras votaciones hasta bien entrado el siglo XX y todavía en muchos territorios del planeta.

- Voto electrónico sustitutivo

  En este nivel, se sustituyen algunos procedimientos manuales o elementos utilizados en el voto tradicional por sistemas electrónicos determinados. Lo que se intenta es que el proceso de votación sea lo más parecido al que se ha venido llevando a cabo, pero pudiendo utilizar avances técnicos que mejoren el procedimiento en algunos de los puntos del mismo. Así, dependidendo de la legislación, el nivel democrático y social y la aceptación de la innovación tecnológica, se han adoptado procesos electorales en los que se hace uso de algunos elementos tales como tarjetas magnéticas o documento de identidad electrónico (para identificar al votante o incluso para emitir el voto), urnas de votación electrónica que recuentan los votos de forma automática (RFID, lector código de barras, etc.), pantallas de votación para selección de candidaturas (en EEUU es una de las formas en las que se elige la opción a votar), sistemas de totalización y consolidación de resultados (para evitar el escrutinio manual), e incluso sistemas para guiar el recuento definitivo pasados unos días de la jornada electoral. Así podemos encontrar muchos más ejemplos.
  Como se puede observar, todos los sistemas que se tienen en cuenta en este nivel están orientados a sustituir un elemento del proceso tradicional de votación. Todos están pensados para tener una función en el local electoral, ya sea para la identificación del votante, emisión del voto, escrutinio o (en otro tipo de local electoral) recuento definitivo. Aquí podemos observar, de paso, diferentes fases del proceso electoral, que son fácilmente reconocibles.

- Voto electrónico remoto

  En este nivel, el concepto del voto traspasa el local electoral común. Se trata de que el voto se transmita desde un punto de votación a una ”urna

remota". Dependiendo del punto de origen, podemos dividir este grupo en dos subgrupos, uno en el que los diferentes colegios electorales están interconectados entre si y otro en el que el voto se emite desde cualquier punto con conexión a internet.

- Voto telemático en local de votación

  En esta primera aproximación al voto telemático sigue pensándose en el sistema de voto tradicional en cuanto a que el votante ha de acudir a un local de votación acondicionado para ejercer su derecho al voto. En este local, encontraría una serie de sistemas de identificación (tanto personal frente a los miebros de mesa - como en el sistema tradicional - como telemático frente a una autoridad certificadora remota a través de una identificación digital) para superar el primer paso del proceso. Una vez cerrada la votación, se conectarían los diferentes colegios electorales para comunicar cada uno sus escrutinios y pasar los resultados para la fase de totalización.

- Voto por internet

  La aproximación del voto por internet es la más ambiciosa en términos tecnológicos y de seguridad. En esta, el votante puede ejercer su derecho al voto desde cualquier punto conectado a internet, como puede ser su propia casa o el lugar en el que se encuentre de viaje. La identificación del votante debe ser digital y remota. El voto emitido tiene que ser transmitido a la urna electrónica remota que corresponda. No obstante, desde un punto de vista sociológico, este sistema tiene todavía una serie de retos que debe cumplir, como es el acceso universal al proceso de votación, ya que es complicado asegurar que la totalidad de la población podría hacer uso de un sistema informático de este tipo. Además, encontramos dificultades en cuanto a fraude electoral, ataques al sistema, tolerabilidad al fallo, etc.

Los sistemas de voto electrónico deberían tener como base antes de la implementación la consigna de aportar al proceso al menos las mismas garantías de seguridad que el sistema tradicional al que está sustituyendo / complementando. El voto presencial tradicional permite un recuento de la votación, lo mismo que la mayoría de los sistemas del primer nivel que hace uso de urnas electrónicas, pues generan un recibo o papeleta física. En cuanto al último nivel, esto no está tan claro, pues la mayoría de estos sistemas no generan un resguardo físico de

los votos electrónicos emitidos, por lo que es complicado pensar en un recuento en caso de fallo o de duda de la autoridad electoral o del propio electorado.

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). Otra empresa española, Indra, también tiene soluciones de voto por internet utilizados para elegir las cúpulas directivas de organismos como la Guardia Civil, universidades como la UAH (Universidad de Alcalá de Henares) o la UNED (Universidad Nacional de Educación a Distancia) e incluso de partidos políticos, como es el caso de UPyD (Unión Progreso y Democracia).

Voto por internet (i-voting)

Dentro de las soluciones de voto electrónico telemático, es importante el desarrollo que se ha hecho en cuanto al voto por internet.

Estonia

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.

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 personal. 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.

Análisis del sistema real

Elecciones a la Junta de Escuela de la EPS

Definición de la Junta de Escuela

Según el documento **NORMAS DE ORGANIZACIÓN Y FUNCIONAMIENTO DE LA UNIVERSIDAD SAN PABLO-CEU** [1], 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 *"(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.

Proceso electoral

Capítulo 2

Planteamiento

Objetivos finales del proyecto

Descripción del sistema real

Alcance del proyecto

Especificación de requisitos

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

- Requisitos del voto electrónico

  Dependiendo del autor al que se recurra, se definen unos u otros requisitos diferentes para un proceso de voto electrónico. Vamos a tener en cuenta la opinión de varios autores de cara a los que consideramos en este PFC.

  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.

******** AQUÍ HAY QUE DEFINIR LOS REQUISITOS DEL VOTO ELECTRÓNICO. DEPENDE DEL AUTOR, HAY UNOS U OTROS. HABRÁ QUE DEFINIR CUÁLES SON LOS QUE VAMOS A TENER EN CUENTA PARA ESTE PROYECTO. ESTÁN EN –TEMP– ESPERANDO A QUE DECIDAMOS

- Requisitos funcionales
- Requisitos propios del voto electrónico
- Requisitos del proceso electoral

**** LO QUE HAY QUE DESARROLLAR **** Requisitos de Usuarios: Necesidades que los usuarios expresan verbalmente Requisitos del Sistema: Son los componentes que el sistema debe tener para realizar determinadas tareas Requisitos Funcionales: Servicios que el sistema debe proporcionar Requisitos no funcionales: Restricciones que afectan al sistema

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. Bajo coste.

Fases del proceso electoral

- Fase Preelectoral

Definición de los límites o reglas de la elección : Deben definirse de forma que no parezca ambigua las reglas electorales. Qué se vota, a quién se vota, de qué forma, cómo se cuentan los votos o se asignan los cargos. Quiénes pueden votar, cuándo comienza y finaliza el sufragio.

Elaboración del censo : Las autoridades de la Elección deben realizar un proceso de elaboriación del censo electoral, para identificar qué votantes tienen derecho a ejercer el voto y dónde (con qué opciones de voto).

Registro de votantes : Puede ser necesario que, según los mecanismos de identificación a utilizar, el votante deba registrarse previamente a la elección frente a la Autoridad Electoral, con el fin de, si no existe censo electoral formalizado, introducirse en el censo de la elección o, si existe ese censo previo, obtener la acreditación identificativa necesaria para poder votar de forma remota con las garantías avaladas por la autoridad electoral.

Presentación de candidaturas : A efectos del sistema informático que desarrollamos es el proceso en el que la autoridad electoral define qué candidaturas pueden ser elegidas por cada votante en cada circunscripción (lógica).

- Fase Electoral (Votación)

Identificación : El primer paso del proceso de votación es el de la identificación del votante. Como ya se ha planteado, la identificación del votante es uno de los procesos críticos de una elección, pues, el sistema debe cumplir con varios requisitos básicos del voto electrónico, como puede ser el principio de autenticidad (en el que sólo los votantes autorizados pueden votar) o el democrático (por el cual el votante que tiene derecho a votar lo tiene para hacerlo tan sólo una vez).

Votación : El momento en el que el votante ya identificado, observa las opciones que puede elegir y ejerce su voto a una o varias de ellas (dependiendo del tipo de elección).

- Fase postelectoral

Difusión de resultados

Fase preelectoral

Definición de los límites o reglas de la elección

Para ejercer la democracia de forma correcta las ”reglas del juego” deben estar bien definidas, de forma clara y concisa, estableciendo los límites, los me-

canismos, las fechas y todo lo necesario para una correcta interpretación, sin lugar a ambigüedades. (...)

Estas reglas de la elección son responsabilidad de la Autoridad Electoral encargada de la organización de los comicios, así como del organismo que los convoca. De cara al sistema informático, esta fase preelectoral es la que sienta las bases de la lógica de negocio del sistema. Ya que define las reglas que el sistema deberá cumplir para llevar a cabo correctamente la elección. (...)

Elaboración del censo

Uno de los cometidos de la Autoridad Electoral previamente a la celebración de unos comicios es la elaboración de un censo electoral completo y fiable que les permita tener un control de cuánta gente y quiénes disfrutan del derecho a votar. Además, este censo debe recoger a qué circunscripción pertenece cada votante y la mesa/urna donde debe realizar su voto.

Una circunscripción es una división electoral. Pensando en elecciones legislativas de España, por ejemplo, casi todas las provincias son unicircunscripcionales, excepto Asturias, que se conforma con 3 circunscripciones y la Región de Murcia, compuesta por 5 circunscripciones. Sin embargo, para las Elecciones al Parlamento Europeo, España registra sus votos como una única circunscripción.

Al asignar cargos basándose en circunscripciones, es básico que en el censo esté definido en cuál de ellas vota cada votante. Además, en cada circunscripción, los candidatos varían, por lo que las papeletas entre las que cada votante puede elegir no serán iguales de unas circunscripciones a otras.

Extrapolando a las Elecciones a la Junta de Escuela de la EPS, podemos identificar varias de estas circunscripciones, a saber:

- Alumnos, por titulación: Arquitectura, Ingeniería Informática, Ingeniería de Telecomunicaciones e Ingeniería de la Edificación
- Profesores, por categoría: colaboradores, adjuntos, agregados y catedráticos.

Podemos asumir, entonces que hay 8 circunscripciones. Por las normas de estas elecciones, para cada circunscripción se eligen 2 representantes que serán los que acaben formando la Junta de Escuela, con 16 cargos electos.

La Universidad deberá elaborar un censo con los alumnos y profesores que tienen derecho a votar en las Elecciones, así como definir en qué circunscripción lo harán, para que tengan conocimiento de entre qué candidatos pueden elegir a

sus representantes. De cara al sistema, es importante conocer estas divisiones, tanto para el conteo de los votos, como para la gestión de los candidatos en el momento en el que se presentan al votante.

Por tanto, es necesario tener un sistema que cargue el censo electoral elaborado por la Universidad, así como la definición de las circunscripciones y la relación entre estas y el propio censo de votantes.

Registro de votantes

Pese a que el censo tiene que ser elaborado antes de cada elección, puede ser que la forma que tiene un organismo de conformarlo es a través de un registro de votantes.

Así, en lugar de tener una institución dedicada a definir el censo del país, como en España puede ser el INE, a partir del cual se extrae el censo electoral según el comicio (éste dependerá del tipo de elección y de la circunscipción electoral ******** ¿Ejemplo censo diferente en Buenos Aires para Jefe de Gobierno y para Legislativas?*******); se da el caso de que el Estado no contabiliza automáticamente como votantes a sus ciudadanos al cumplir los 18 años (o la edad mínima para votar, dependiendo del país / territorio), sino que es responsabilidad del propio ciudadano el inscribirse en el registro de votantes. ******* Esto hay que cambiarlo, no vale *********

********** Registro de votantes como mecanismo para la posterior identificación??? Si no podemos usar DNIe, pero se usa una smartcard, habría que realizar el mapeo de la Id del votante con los certificados de la smartcard.... **********

Presentación de las candidaturas

Una vez definido tanto el censo como las divisiones electorales, tienen que presentarse las candidaturas. (...)

Fase electoral

Identificación del votante

El primer paso de un votante a la hora de emitir su voto, en el sistema de voto tradicional es identificarse ante los miembros de la mesa electoral. Para ello, en elecciones como las que organizan el Ministerio de Interior en España o las diferentes Comunidades Autónomas, el votante hace uso de un documento que

verifique su identidad. En España, este documento es el DNI, aunque también se puede hacer uso del Pasaporte. En otros países en los que se carece de un documento oficial de identidad expedido por las autoridades del Estado, se realiza un registro biométrico de los votantes con, por ejemplo, las huellas dactilares de los mismos. En el caso de las Elecciones a la Junta de Escuela de la EPS CEU, la identificación de los votantes...

Una vez identificado al votante, se le tiene que cotejar con el censo de la elección o de la mesa en la que ha sido identificado. En países como España, la elaboración del censo corre a cargo del INE (Instituto Nacional de Estadística) y reparte a los votantes en diferentes mesas repartidas en locales electorales. En otros estados, este censo no existe y se requiere que sea la ciudadanía la que se registre en un Registro de Votantes, con lo que si no se ha acudido a tiempo de realizar este trámite, la persona pierde su derecho al voto.

Para dejar constancia de que un votante ya ha ejercido su derecho al voto, en países como España es tan simple como que los miembros de la mesa electoral lo reflejen en una lista con el censo de su mesa. En otros territorios, sin embargo, la costumbre es marcar de alguna forma a aquellas personas que han votado, como puede ser manchar algún dedo de la mano con tinta indeleble, para que, si volviese a votar a otra mesa, se observara que ya lo había hecho previamente.

En un sistema de voto por internet no hay una interacción directa entre el votante y la autoridad electoral, que es quien debe permitirle votar. Por ello, es muy importante que los mecanismos para identificar al votante sean precisos y confiables. Por ello, hay que valorar qué metodo de identificación es el mejor para cumplir con los requisitos de la elección, incluídos ahí los inherentes al voto electrónico telemático y remoto.

- Usuario / contraseña.

  Para las elecciones de la Junta de Escuela de la EPS, el método de usar un par usuario / contraseña sería una solución sencilla. El censo está bastante acotado y, al ser todos los potenciales votantes miembros de la Universidad, poseen una cuenta de correo electrónico corporativa proporcionada por ésta. El proceso sería tan fácil como, por ejemplo, usar la dirección de correo electrónico de cada alumno / profesor / trabajador de la Escuela como nombre de usuario y enviarles un email a cada uno con una clave aleatoria generada por la autoridad electoral.

  Esta solución, no obstante, sería inviable para elecciones más ambiciosas, como lo son las legislativas estatates o autonómicas, ya que carecemos de elementos como direcciones de correo electrónico de todo el censo.

- DNIe

  Lo ideal para una elección por el sistema de voto por internet es implementar un proceso que resulte sencillo al votante, ya que si resulta ser más complicado que el voto tradicional, el votante no le verá sentido y no hará uso de él. Con este planteamiento, parece que el uso del DNIe es una buena idea. Por un lado, es un documento oficial que llevamos normalmente con nosotros en todo momento. Además es el mismo documento que nos identifica en las elecciones tradicionales, con lo que para el votante no debería suponer ninguna suspicacia ni trauma, al estar completamente insertado en la sociedad su uso para este cometido (asumimos en este supuesto que la implatación del DNIe en España es casi completo, que el votante ya no necesita acudir a una comisaría a solicitarlo y que los certificados no están caducados).

  Ventajas del uso del DNIe como identificador del votante:

  - Documento expedido por las propias Autoridades del Estado, quienes lo avalan.
  - Seguridad.
  - La gente lo lleva consigo constantemente y está acostumbrada a usarlo para identificarse o, incluso, para realizar otro tipo de actividades en internet, como obtener certificados de Organismos Públicos, banca por internet, etc.
  - Es el mismo documento que ya se utiliza para identificarse en las elecciones presenciales tradicionales.

  Inconvenientes del DNIe:

  - Extranjeros con derecho a voto pueden no tener DNIe, pero deberían poder votar con el pasaporte.
  - Certificados caducados. Que los certificados que lleva consigo el DNIe no tengan la misma fecha de caducidad que el propio documento es un punto en contra, ya que los usuarios no lo renuevan al ver que no tienen que hacerlo con el documento físico.
  - Rotura del chip que contiene los certificados.
  - Limitaciones técnicas para las aplicaciones web. En el estado actual de la tecnología, es necesario hacer uso de un applet de Java para

poder firmar con el DNIe. De cara a la identificación, ya hay software Javascript que se salta este paso, aunque no a la hora de firmar, para lo cual, hoy por hoy, no hay alternativa. Este detalle es una limitación importante, quizá no para el oto electrónico, pero sí para el voto universal por internet, ya que requiere de más tecnología que simplemente un dispositivo conectado a internet y un lector. Además, el uso de applets está cada vez peor visto en Internet y se recomienda no implementar alternativas basadas en el estándar W3C. Por desgracia, este organismo todavía no tiene definido de una manera versátil cómo afrontar el problema de la criptografía en los nuevos estándares web.

- Necesidad de HW externo, como son los lectores de Smartcard. Para poder utilizar el DNIe como identificador, el sistema tiene que poder leer los datos que le indica. Si hacemos uso de los certificados que contiene, necesitamos un lector externo, lo cual quizás no sea un problema si usamos un PC que tenemos en casa, pero sí que puede serlo cuando queremos votar desde otro ordenador o incluso desde un dispositivo móvil, donde ya no es tan simple que tengamos este lector y que sea compatible. Cierto es que podríamo hacer uso de la banda MRZ del documento escaneándola pero... (******** no estoy seguro, qué pasa con fotocopias??, yo me fiaría de los certificados).

- MobID

  El Gobierno de Estonia, para sus comicios por internet está desarrollando una tecnología en la que el propio smartphone es la herramietna que sirve para identificarnos. Parece una buena opción, pues hoy por hoy, es bastante común que llevemos el smartphone con nosotros de la misma forma que llevamos el DNI. Además, es un dispositivo muy personal, que no se suele compartir, por lo que podría realizarse una identificación unívoca entre el usuario-votante y su registro en el censo electoral. (******** hay que mirar bien esto, pues no sé si habrá algo desarrollado, de todos modos, en España esto ni se contempla)

- Smartcard

  Otra opción posible es el uso de una smartcard que contenga certificados emitidos por la Autoridad Electoral para cada votante. Los inconvenientes de este método son varios: - Por un lado, requiere un registro previo de los votantes, pues hay que generarles los certificados. - Un problema logístico ya que, una vez generados los certificados e introducidos en las tarjetas,

éstas deben hacerse llegar a los votantes que las van a utilizar. Este paso, en unas elecciones a gran escala puede suponer un esfuerzo injustificado.

En el caso de las Elecciones a la Junta de Escuela de la EPS, podemos pensar en la primera opción. No obstante, como se explica en próximos capítulos, el hecho de necesitar certificados de firma para cifrar y firmar el voto por seguridad, nos hace que tengamos que plantearnos una solución para este problema. Con una simple indentificación de usuario / contraseña no lo vamos a poder resolver, así que se tiene que buscar una alternativa. Sería inteligente tratar de buscar una alternativa que sirva tanto para el paso de votación como para el de identificación, por seguridad, así que podríamos pensar en DNIe. Pero en la Universidad podemos tener miembros del censo que no posean este documento (estropeado, caducado, extranjeros). La forma que tiene la Universidad de acreditar que un alumno forma parte de ella es con un carnet universitario que se entrega tanto a alumnos como a profesionales. Podría ser este documento, el oficial en la Escuela, el que se use como identificador de votante, con lo que estamos hablando de utilizar una smartcard especial, emitida por la propia Autoridad Electoral de forma previa. (********** Lo que pasa es que me temo que estas tarjetas no tienen certificados, con lo que tampoco van a valer para la votación).

Votación

En el sistema tradicional, el momento de la votación es aquel en el que el votante deposita su voto en la urna tras haber escogido la papeleta o marcado la boleta de candidatos y habe sido identificado correctamente por los miembros de la mesa electoral.

Este proceso es al que estamos habituados en los territorios con una cierta historia democrática. En principio, parece bastante transparente, en cuanto a que el votante puede confirmar sin ninguna duda que su voto, efectivamente, se encuentra dentro de la urna sellada, junto con el resto de votos de la mesa.

Aquí encontramos el primer detalle controvertido con respecto al voto por internet. El votante no tiene constancia física de que su voto se ha depositado en la urna correcta, ni siquiera de si está en alguna urna. No ”se ve”.

Es más, sabe que ha introducido en la urna la papeleta que tenía en su mano, que sabe cuál es porque él mismo la ha elegido. Pero en el sistema informático, no sabe si ocurre lo mismo. Puede pensar que aunque haya seleccionado un candidato y el sistema le diga que ha contabilizado su voto por éste, realmente, por detrás esté cambiando el voto y registrando a otro candidato diferente.

Es misión del sistema informático proveer al votante de mecanismos que le permitan verificar todas estas cuestiones. Hay que diseñar el sistema para que haya confianza en él. Quizá esta sea la mayor de las barreras existentes en la actualidad para la implatación del voto por internet, la falta de confianza.

No es por falta de métodos seguros o carencia de medios criptográficos. El problema es que no es fácil que el elector confíe en el proceso, ya que, a priori, parece una gran caja negra.

Fase postelectoral

Capítulo 3

Riesgos

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-)

Identificación de riesgos

Capítulo 4

Solución

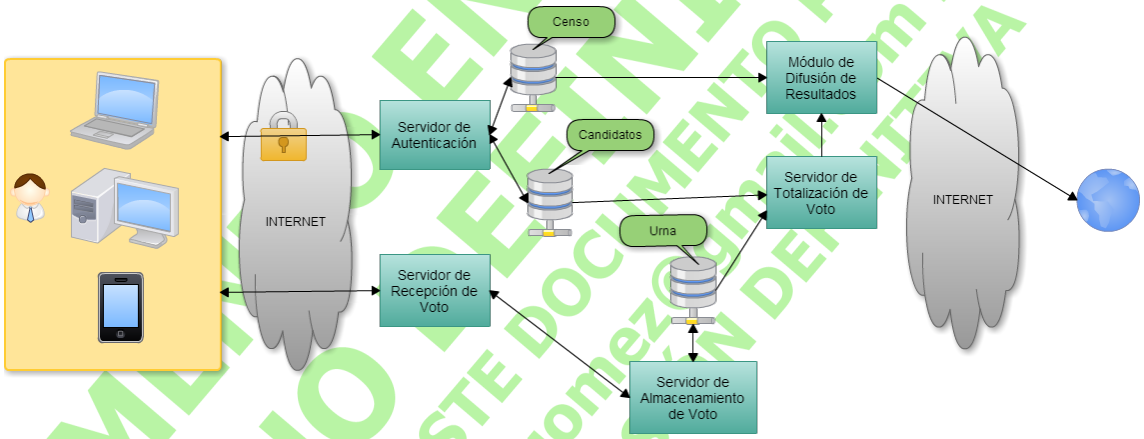

Figura 4.1: *Diagrama de flujo del Sistema*

Capítulo 5

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 Facul-

tad, 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 Registradores, 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) - Validación 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

Requisitos del voto electrónico según la Guía de Implantación de la Junta de Castilla y León:

Autenticidad : Sólo los votantes autorizados pueden votar.

Acotabilidad : El sistema tan sólo autentica la votación dentro de las reglas establecidas.

Anonimato : No se puede relacionar un voto con el votante que lo ha emitido.

Imposibilidad de coacción : Ningún votante debe ser capaz de demostrar ante terceros qué voto ha emitido.

Verificabilidad individual : Cada votante deberá poder asegurarse de que su voto ha sido considerado adecuadamente, de forma que pueda obtener una prueba palpable de este hecho. Podemos distinguir dos tipos de verificabilidad individual: verificabilidad individual del contenido del voto emitido y verificabilidad individual de que el voto ha sido tenido en cuenta adecuadamente. Definida de esta forma, puede parecer que la verificabilidad individual contradice el requisito de imposibilidad de coacción, ya que cuanto más explícita es la verificación individual más riesgos de coacción pueden aparecer. No obstante, se pueden diseñar mecanismos que hagan compatibles ambos requisitos, como la temporalidad de la validez de la verificabilidad individual, de forma que se limita en el tiempo la posibilidad de la verificabilidad individual, y pasado dicho tiempo, se destruyen los ficheros.

Verificabilidad global : Se trata de mecanismos que permitan a ciudadanos autorizados comprobar la validez del recuento final.

Fiabilidad : El sistema debe garantizar que no se produce ninguna alteración de los resultados, ya sea mediante ataques intencionados o fallos en el sistema.

Auditabilidad : Durante el proceso de votación deben registrarse las pruebas de voto y elementos de auditoría que permitieran a las personas autorizadas disponer de garantías para comprobar que todo el proceso de votación es correcto (funcionamiento del sistema, programas, equipos, protocolos, y demás elementos), todo ello sin comprometer la integridad de la elección o la privacidad y anonimato de los votantes.

Neutralidad : No debe ser posible conocer resultados parciales hasta que no finalice el tiempo de la elección.

Movilidad de los votantes : El sistema debe permitir a los participantes que emitan su voto desde cualquier cabina o punto de votación, eliminando la restricción actual de hacerlo en el centro de votación de la zona en la cual está censado.

Facilidad de uso : El votante debería necesitar el mínimo de habilidades y conocimientos especiales para emitir el voto.

Voto nulo o de rechazo : El votante debe poder emitir un voto sin que sea contabilizado como válido para ninguna de las candidaturas propuestas ni ser considerado dentro del bloque de los votos en blanco.

Código abierto : El código fuente de todos los programas informáticos que se utilicen en cualquier etapa del proceso debería ser conocido y verificable por los auditores. La seguridad del sistema no debería estar basada en mantener este código secreto, sino en las claves de cifrado utilizadas en todas las fases del proceso de votación.

Coste mínimo : El coste del sistema de elección debería estar en consonancia con el coste del sistema convencional.

Utilización de una red dedicada : Tanto si se vota a través de Internet como si se vota desde cabina especializada, la red telemática en la que se apoya

el sistema deberá ser, desde un punto de vista lógico, totalmente cerrada, de forma que el acceso a ella esté permitido a los agentes y actores contemplados en el sistema.

Igualdad de oportunidades en la votación : Todo ciudadano debe tener acceso al equipamiento técnico y procedimientos organizativos a la hora de votar.

Flexibilidad física : El equipamiento debe ser accesible y fácilmente utilizable por discapacitados físicos.

Confianza : El votante debería entender el proceso de votación para fortalecer su confianza y aceptación del sistema.

Tabla del mismo documento:

1. Privacidad del voto El voto es secreto, nadie puede saber qué ha votado un elector.
2. Integridad del voto Nadie puede cambiar un voto de un elector.
3. Integridad de la votación Nadie puede cambiar el resultado de la votación.
4. Verificabilidad individual Posibilidad de comprobar que cada voto ha sido contado correctamente.
5. Verificabilidad universal Cualquier votante puede verificar que la elección fue realizada correctamente.
6. Democrático Sólo vota el que tiene derecho a hacerlo y una única vez.
7. Conveniencia de la votación El voto debe ser fácilmente emitido desde cualquier lugar a través de diversos métodos y sin requerir habilidades especiales.

Capítulo 6

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] Normas de organización y funcionamiento de la universidad san pablo-ceu. http://servicios.ceu.es/calidad/Portals/0/Dat/Doc/A.1_NORMAS_DE_ORGANIZACI%C3%93N_Y_FUNCIONAMIENTO.pdf.

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

[3] Voting machines pros and cons. http://votingmachines.procon.org/view.timeline.php?timelineID=000021.

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

[5] Carracedo Verde, José David, Gómez Oliva, Ana, Moreno Blázquez, Jesús, Pérez Belleboni, Emilia, and Carracedo Gallardo, Justo. Votación electrónica basada en criptografía avanzada (proyecto votescript). *Universidad Politécnica de Madrid*. http://vototelematico.diatel.upm.es/articulos/articulo_venezuela_revisado.pdf.

[6] Gordillo, Rafael. Ejemplo de artículo. *REAL BETIS - SEVILLA* (2007).

[7] Incluso HayAutor3, Soy Y., A. . S. . .ªquí va el título de esto que no se ha publicado". Aquí va una nota, 2008.

[8] Morales Rocha, V. M. *Seguridad en los procesos de voto electrónico remoto: registro, votación, consolidación de resultados y auditoría*. PhD thesis, Universitat Politècnica de Catalunya. Departament d'Enginyeria Telemàtica, Marzo 2009. http://www.tdx.cat/bitstream/handle/10803/7043/01VMmr01de01.pdf.

[9] Pérez Belleboni, Emilia, and Carracedo Gallardo, Justo. Uso del dnie para reforzar el anonimato en el voto telemático mediante tarjetas inteligentes. *Departamento de Ingeniería y Arquitecturas Telemáticas. Escuela*

Universitaria de Ingeniería Técnica de Telecomunicación. Universidad Politécnica de Madrid. http://vototelematico.diatel.upm.es/articulos/Uso_DNiIe_anonimato_voto.pdf.

[10] VENTURA BONELL-TEROL, M. A. Propuesta de implantación de votación electrónica en las elecciones a rector de la universidad politécnica de valencia. Master's thesis, Universitat Politècnica de València. Facultat d'Administració i Direcció d'Empreses, Octubre 2011. http://riunet.upv.es/bitstream/handle/10251/14584/PROPUESTA%20DE%20IMPLANTACI%C3%93N%20DE%20VOTACI%C3%93N%20ELECTR%C3%93NICA%20EN%20LAS%20ELECCIONES%20A%20RECTOR%20DE%20LA%20UNIVERSIDAD%20PO.pdf?sequence=1.