Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Diseño e implementación de un sistema de voto electrónico

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Carlos Moreno Moreno

Tutor: Damián López Rodríguez

Curso 2015/2016

Resumen

En este trabajo se lleva a cabo el diseño e implementación de un sistema de voto electrónico, analizando para ello características deseables, distintas aproximaciones realizadas en otros países, así como distintos mecanismos de cifrado, firmas, etc., que permitan asegurar el anonimato del votante y, en definitiva, el buen funcionamiento del sistema. Se ha optado por un protocolo con dos autoridades sin relación, que permite mantener la privacidad del elector siempre que se mantenga la independencia de estas. El sistema cumple propiedades deseables para un sistema de voto electrónico, como la verificalidad, entre otras.

Palabras clave: Voto electrónico, Cifrado de clave pública, Precisión, Privacidad, Verificalidad.

Abstract

In this project we design and implement an electronic voting scheme. We analyse in consequence different approaches carried out in other countries, different mechanisms of encryption, digital signature, etc., in order to allow the privacy of the voter and also the proper functioning of the system. The scheme uses a protocol with two unrelated authorities to make possible the keeping of the privacy of the voter as long as the independence of them remain. The scheme has other desirable properties for an electronic voting system, for instance verifiability.

Keywords: Electronic voting, Public key cryptography, Accuracy, Privacy, Verifiability.

Tabla de contenidos

Índice de ilustraciones

Índice de tablas

1. Introducción

1.1. Motivación

En plena era digital en la que internet está tan presente en nuestras vidas, en la que vivimos con un dispositivo constantemente conectado a la red en el bolsillo, el cual utilizamos para casi todo, sería interesante disponer de un sistema de voto adaptado a esta era, que permita sustituir los sistemas de voto tradicionales como el de las urnas o el voto por correo postal, con el elevado coste en logística que suponen para el estado, así como la incomodidad que puede suponer para el electorado asistir al colegio electoral, tanto para votar como para formar parte de una mesa electoral, además de mejorar aspectos de la única forma de voto no presencial regulada hasta el momento, el voto por correo postal, cuyo funcionamiento se explica brevemente a continuación:

El voto por correo postal [1] [2] requiere de la identificación del elector en Correos a la hora de su solicitud. Una vez solicitado, la Oficina del Censo Electoral remite por correo certificado al elector toda la documentación necesaria, entre ella, todas las papeletas y los sobres para el Congreso y el Senado, además del certificado de inscripción en el censo electoral, que incluye el nombre y DNI del elector. Cuando recibe la documentación, el elector envía a la mesa electoral adjudicada los sobres para el Congreso y Senado (con las papeletas elegidas en su interior) y el certificado de inscripción en el censo, todo en un mismo sobre. Una vez llegado el momento del escrutinio, en la mesa electoral receptora de ese voto se comprueba la pertenencia del elector a esa mesa (revisando el certificado de inscripción) y se introducen los sobres en sus respectivas urnas.

La inseguridad de este tipo de voto reside en que el voto y el identificador del elector viajan juntos, siendo extremadamente fácil violar la privacidad del votante. Además, el votante no tiene forma de verificar que los votos que envía son los que efectivamente se introducen en las urnas. Aparte de esto, al tratarse de un proceso manual, pueden producirse fallos humanos, como que no se envíen todas las papeletas al votante, por lo que este sería incapaz de votar a un partido del que no le llega papeleta.

Debido a todo lo anterior, y teniendo en cuenta referencias de otros países en los que el voto electrónico ya está implantado, se ha decidido diseñar e implementar un sistema de voto electrónico que aúne las características más interesantes de los métodos mencionados anteriormente y que sea viable para su implantación.

El mayor impedimento para la implantación de un sistema de este tipo no es técnico, sino de confianza, pues no resulta fácil convencer al electorado para que adopte un sistema de voto como este. Para conseguir tal confianza, sería deseable que un sistema de voto electrónico cumpliera los requisitos de seguridad propuestos por Neff y Chaum

[3] y Ray y Narasimhamurthi [4] en sus respectivos protocolos, resumidos de forma conjunta a continuación:

- Votos emitidos como se pretende: La papeleta de un votante debe representar exactamente su elección.
- Completitud: El resultado final debe ser un recuento exacto de los votos emitidos.
- Verificalidad: Las dos propiedades anteriores han de ser verificables. Es decir, cada votante debe ser capaz de verificar que el voto que ha emitido representa exactamente su elección. Además, todo el electorado debe ser capaz de verificar que los resultados se corresponden con el recuento exacto de votos.
- Democracia: Sólo los votantes incluidos en el censo pueden votar. Además, cada votante debe poder votar sólo una vez.
- Resistencia coercitiva: Un votante no debe poder ser capaz de probar su elección a un tercero.
- Precisión: Un voto inválido no ha de ser contado. No ha de ser posible añadir o eliminar votos.
- Seguridad: Si un elector decide no votar, nadie debe poder aprovecharse de su voto.
- Privacidad: No ha de poder relacionarse voto y elector.
- Justicia: Nadie puede conocer el resultado de la votación antes de que finalice.

1.2. Objetivos

El objetivo general del proyecto consiste en el diseño y la posterior implementación de un sistema de voto electrónico en línea. El sistema mencionado pretende incluir las características mencionadas anteriormente, especialmente:

- Privacidad: uno de los puntos más importantes. Para que la implantación de este nuevo sistema sea viable, este debe seguir garantizando el anonimato del votante. Sin esta característica no merece la pena siquiera plantearse este método de voto.
- Comunicaciones seguras con el sistema: de nada sirve “garantizar” el anonimato del votante si las comunicaciones de este con el sistema de voto no son seguras, lo que permitiría interceptar el tráfico entre el votante y el sistema, haciendo inútil la característica de la privacidad mencionada anteriormente. El protocolo no se centra en la implementación de esta característica, si bien garantiza su cumplimiento.
- Facilidad de uso: la implantación de este sistema ha de ser un alivio para la población, no un problema. Es por esto que el proceso de voto se ha de simplificar lo máximo posible.

- Verificalidad: los votantes deben poder ser capaces de comprobar que su voto se ha emitido en el sentido elegido. Además, ha de ser posible comprobar que el recuento refleja los resultados reales de la votación.
- Confianza del electorado en el sistema: el método de voto ha de ser lo más transparente posible, evitando cualquier tipo de desconfianza, ya que esto afectaría fatalmente al sistema, pudiendo hacer necesaria la repetición de las elecciones de manera tradicional. Este apartado no depende del protocolo de forma directa, sino más bien del proceso de comunicación de las características al electorado, pero aun así, es un objetivo a cumplir.

2. Situación actual

2.1. Tipos de voto electrónico

Tal y como se menciona en el documento del Instituto Internacional para la Democracia y la Asistencia Electoral (IDEA) "Una introducción al voto electrónico: Consideraciones esenciales" [5] existen distintos esquemas de voto electrónico, entre ellos los más importantes son:

– Registro Electrónico Directo (RED)

Según la definición en [5], en los sistemas RED los votantes emiten su voto directamente desde un aparato electrónico que puede disponer de pantalla táctil, botones físicos, etc. La información sobre la votación se almacena en el disco duro del aparato, lo que elimina la necesidad de la papeleta de papel. Al final de la votación, la información de todos los puntos de votación se envía a un ordenador central, que se encarga de realizar el escrutinio. Se puede observar en la tabla 1 cómo existen sistemas de votos RED con y sin Comprobante de Auditoría de Papel Verificado por el Votante (VVPAT, del inglés *Voter verified paper audit trail*). Como también se puede ver en dicha tabla, las grandes fortalezas de este sistema se encuentran en la mayor rapidez en la obtención de los resultados, la mayor exactitud de los resultados y la prevención del fraude, entre otras. Mientras que las debilidades de este sistema son su costo, su falta de transparencia y falta de comprensión por el electorado en su versión sin VVPAT, así como el riesgo de manipulación, los costos de mantenimiento y la dependencia del proveedor, entre otros. La principal diferencia entre RED con y sin VVPAT es que el primer sistema permite un recuento significativo, es decir, permite realizar dos recuentos paralelos independientes gracias al comprobante de voto emitido, mientras que el segundo no.

Este sistema fue introducido en Venezuela en 2005, con una gran desconfianza en el Organismo Electoral (OE), ya que existía el temor de que el

sistema de voto se usara para manipular los resultados. Estos problemas de confianza, sumados a las debilidades técnicas del sistema, que no eliminaba la posibilidad de relacionar votantes y votos generaron una situación crítica a pocos días de las elecciones de ese año. Para reestablecer la credibilidad se realizaron recuentos masivos con los comprobantes escritos en cerca de la mitad de las mesas de votación, por lo que al final el sistema perdió toda su eficacia en comparación con el sistema tradicional de papeletas.

- Reconocimiento Óptico de Marcas (OMR)

  Los sistemas OMR (del inglés *Optical Mark Recognition*) [5] [6] utilizan una papeleta especial, en la que la opción marcada por el votante es reconocida por lectores ópticos. Estos sistemas pueden funcionar o bien mediante un conteo centralizado (las papeletas pasan por el lector óptico en un centro de escrutinio) o bien mediante un sistema de conteo en las propias mesas electorales, que disponen del lector óptico en el momento en el que el votante introduce su voto. Este último sistema es conocido como PCOS (del inglés *Precinct Count Optical Scan*). En la tabla 1 se puede ver como las mayores fortalezas de este sistema, en su variante PCOS, son la mayor rapidez del recuento, mayor exactitud en los resultados, prevención del fraude en las mesas de votación, así como el recuento significativo, entre otras. Mientras que en sus debilidades se encuentran una presentación de papeletas complicada, incomodidad para los votantes, mayor gasto, menor accesibilidad y menor flexibilidad para realizar cambios, entre otras.

  Este sistema, concretamente en su variante PCOS, fue introducido en Filipinas en 2010. Cerca de una semana antes de las elecciones el sistema estuvo a punto de venirse abajo cuando las casi 75000 máquinas de votación PCOS no estaban configuradas correctamente. Finalmente el problema se resolvió cuando todas las máquinas fueron reconfiguradas en el último momento gracias a una inmensa labor logística. Después de las elecciones (exitosas), quedó la incertidumbre sobre si el OE dependía demasiado del proveedor del sistema.

- Impresoras de papeletas electrónicas (EBP)

  El sistema EBP (del inglés *Electronic Ballot Printer*) [5] consiste en una mezcla de los sistemas RED y OMR. El votante elige a quien quiere votar en una máquina similar a las RED y esta le proporciona una papeleta con marcas que pueden ser leídas por un lector óptico, tal y como ocurre en el sistema OMR. En la tabla 1 se puede apreciar como las principales fortalezas de este sistema son la rapidez de obtención y exactitud de los resultados, la prevención del fraude en las mesas de votación, la flexibilidad para realizar cambios, así como el recuento significativo, entre otras. Entre las debilidades se encuentran, entre otras, el poco ahorro en costos del sistema, el riesgo de manipulación por agentes internos, así como la dependencia del proveedor.

- Sistemas de votación en línea

  En los sistemas de votación en línea [5] los votos son transmitidos a través de la red hacia un servidor central, el cual se encarga del escrutinio. En principio cualquier dispositivo con conexión a internet serviría para este propósito. En la tabla 1 se puede ver como entre sus fortalezas se encuentran la comodidad para los votantes, y un menor costo de introducción y mantenimiento, así como un menor requerimiento de infraestructura. Por otro lado, en las debilidades se encuentran la falta de transparencia, la dificultad para lograr la privacidad y el riesgo de manipulación por parte de agentes internos, entre otras.

  Uno de los países en los que está implantado este sistema de voto es Estonia. El sistema de votación en línea se introdujo en 2005, como complementación del sistema tradicional, obteniendo una gran confianza desde sus inicios. Estonia es un país con una alta confianza en sus instituciones y el voto electrónico por internet se introdujo como parte de un programa de digitalización de las instituciones. Ni siquiera unos ataques por parte de delincuentes informáticos contra la infraestructura digital del gobierno antes de las elecciones de 2007 redujeron la confianza de la población en el sistema de voto. En 2011 aproximadamente el 24 por ciento de los votos se emitieron a través de este sistema de votación en línea.

En la comparación de sistemas de voto electrónico de la tabla 1 se aprecia cómo el voto por internet es el que más ahorro económico supone respecto al resto de sistemas, siendo también el que menos requerimientos de infraestructura requiere. Esto se debe a que, mientras que la infraestructura del resto de sistemas de voto electrónico es distribuida (requieren un alto despliegue logístico, tanto de personal como de equipo tecnológico para cubrir todas las mesas electorales), el voto por internet tiene una infraestructura (casi) centralizada: tan sólo requiere del mantenimiento de los centros de datos y pagar al personal que trabaja en ellos. Si bien los centros de datos están realmente distribuidos para poder dar servicio a todo el electorado, el nivel de distribución de la infraestructura es ínfimo comparado con que el que se requiere para dar servicio a todas las mesas electorales, de ahí que se pueda considerar centralizado.

También se puede ver cómo el sistema de voto electrónico que sale peor parado es el de Reconocimiento Óptico de Marcas en su variante PCOS, pues es el más débil en presentación de las papeletas, comodidad para los votantes, accesibilidad, comunicación en varios idiomas y flexibilidad ante cambios.

Aspectos electorales, en comparación con la papeleta impresa	Voto por Internet	RED sin VVPAT	RED con VVPAT	PCOS	Impresoras de papeletas electrónicas
Mayor rapidez en el conteo y tabulación	Fortaleza	Fortaleza	Fortaleza	Fortaleza	Fortaleza
Mayor exactitud en los resultados	Fortaleza	Fortaleza	Fortaleza	Fortaleza	Fortaleza
Administración de sistemas electorales complicados	Fortaleza	Fortaleza	Fortaleza	Fortaleza	Fortaleza
Mejor presentación de papeletas complicadas	Mixto	Mixto	Mixto	Debilidad	Mixto
Mayor comodidad para los votantes	Fortaleza	Mixto	Mixto	Debilidad	Mixto
Mayor participación y asistencia a las urnas	Fortaleza	Neutro	Neutro	Neutro	Neutro
Abordaje de necesidades en una sociedad con mayor movilidad	Fortaleza	Mixto	Mixto	Neutro	Mixto
Ahorro en costos	Mixto	Debilidad	Debilidad	Debilidad	Debilidad
Prevención del fraude en mesas de votación	Neutro	Fortaleza	Fortaleza	Fortaleza	Fortaleza
Mayor accesibilidad	Mixto	Mixto	Mixto	Debilidad	Mixto
Comunicación en varios idiomas	Fortaleza	Fortaleza	Fortaleza	Debilidad	Fortaleza
Se evita anulación de papeletas impresas	Fortaleza	Fortaleza	Fortaleza	Fortaleza	Fortaleza
Flexibilidad para realizar cambios, manejo de fechas límite	Fortaleza	Fortaleza	Fortaleza	Debilidad	Fortaleza
Impide el voto familiar	Fortaleza	Neutro	Neutro	Neutro	Neutro
Falta de transparencia	Debilidad	Debilidad	Mixto	Mixto	Mixto
Solo expertos entienden plenamente la tecnología de votación	Debilidad	Debilidad	Mixto	Mixto	Mixto
Carácter secreto del voto	Debilidad	Mixto	Mixto	Mixto	Mixto
Riesgo de manipulación por parte de agentes externos	Debilidad	Mixto	Mixto	Mixto	Mixto
Riesgo de manipulación por parte de agentes internos	Debilidad	Debilidad	Debilidad	Debilidad	Debilidad
Costos de introducción y mantenimiento	Fortaleza	Debilidad	Debilidad	Debilidad	Debilidad
Requerimientos de infraestructura/ ambientales	Mixto	Debilidad	Debilidad	Debilidad	Debilidad
Falta de parámetros sobre el e-voto	Debilidad	Debilidad	Debilidad	Debilidad	Debilidad
Recuento significativo	Debilidad	Debilidad	Fortaleza	Fortaleza	Fortaleza
Dependencia del proveedor	Debilidad	Debilidad	Debilidad	Debilidad	Debilidad
Mayores requerimientos de seguridad informática	Debilidad	Debilidad	Debilidad	Debilidad	Debilidad

Tabla 1 - Matriz comparativa de tipos de voto electrónico [5]

El tipo de voto electrónico elegido para el proyecto es el sistema de votación en línea, ya que es el que más objetivos de los propuestos al inicio satisface, debido principalmente a que es el único que no obliga a los votantes a ejercer el voto de manera presencial, con la comodidad para los electores que esto conlleva, además de solucionar los problemas de burocracia y seguridad que tienen los votantes por correo. Aparte de esto, reduce en gran medida la logística necesaria para el proceso electoral, con el consecuente ahorro económico que eso supondría para el Estado. Se asumen los inconvenientes de este tipo de voto y se intenta informar acerca de cuestiones de confianza.

2.2. La confianza en el voto electrónico

La confianza del público en el sistema es un aspecto indispensable en un sistema de voto electrónico. De hecho, la consecución de esta confianza es tan importante o más que la propia implementación del sistema, pues sin esta confianza el sistema no sirve de nada.

Los principales factores que determinan la confianza en el sistema son tanto el contexto sociopolítico en el que se introduce este como los fundamentos técnicos del propio sistema, así como la educación de la ciudadanía para su uso y comprensión. A continuación se exponen brevemente los aspectos que se consideran más relevantes relacionados con cada uno de estos apartados:

2.2.1. Contexto sociopolítico

Tal y como se comenta en [5], un entorno sociopolítico positivo, democrático, en el que la ciudadanía participa en la vida política, contribuye a introducir el voto electrónico e incluso puede mitigar temporalmente algunos problemas que puedan surgir en los detalles más técnicos de su implementación. La confianza en una solución que tenga debilidades técnicas puede, sin embargo, traer problemas posteriores. Las debilidades en los fundamentos operativos, técnicos o jurídicos tarde o temprano saldrán a la luz y podrían desacreditar no sólo el voto electrónico, sino todo el proceso electoral. Esto puede traer como consecuencia la eliminación total del voto electrónico en un país, claro ejemplo es lo ocurrido en los Países Bajos o Irlanda.

En los Países Bajos se suspendió el voto electrónico en 2008 después de haberlo usado durante 20 años, cuando se demostró que en determinadas circunstancias el sistema podría poner en peligro la privacidad del voto. Debido a que el OE no disponía de expertos y dependía demasiado de los proveedores, los votantes tuvieron que volver al voto tradicional presencial en urna. Aun con esto, los votantes todavía confían en el voto electrónico gracias a las experiencias positivas pasadas, por lo que no se descarta volver a implantarlo.

En Irlanda, entre 2005 y 2009 se invirtieron más de 60 millones de euros en un sistema de voto electrónico para llegar después a la conclusión de que el sistema no era confiable y requería de (caras) modificaciones para poder implantarse. Esto, sumado a la falta de confianza en el sistema propició la eliminación del voto electrónico en 2009.

Un entorno sociopolítico negativo plantea problemas, aunque el sistema de voto electrónico sea sólido técnicamente hablando. No es fácil conseguir que estos sistemas sean transparentes y que su funcionamiento sea comprendido por el electorado. Contar con poco apoyo social y político dificultará la implantación de una solución confiable, ya que a los adversarios les resultará más fácil minar la confianza en la tecnología en cuestión aludiendo a alguna de sus debilidades.

España sería un país propicio para la implantación de un sistema de voto electrónico en línea, dado que dispone de un entorno sociopolítico positivo como el mencionado anteriormente. La implantación de un sistema de este tipo ofrecería una alternativa al voto tradicional en urna y por correo como lo ha hecho en otros países. Un sistema de voto electrónico en línea podría permitir a los electores votar de forma más cómoda, así como más segura en el caso de los votantes por correo. Además, permitiría al Estado un gran ahorro tanto logístico como económico.

2.2.2. Fundamentos técnicos y consideraciones de implantación

Si bien el contexto sociopolítico es importante a la hora de inspirar confianza en un sistema de voto electrónico, al final es el propio sistema el que tiene que hablar por sí mismo: un sistema con fallas técnicas podrá conseguir la confianza del público durante un tiempo si recibe el apoyo de entidades suficientes, pero con el tiempo esto no será bastante y se desvelarán sus problemas, provocando la pérdida de confianza no sólo en el propio sistema, sino también en las entidades que lo apoyaron e incluso en el propio sistema político. Es por esto que el sistema que se implante ha de ser robusto y seguro, así como transparente, para que los usuarios de a pie puedan comprobar por ellos mismos la seguridad del sistema. Además de esto, un sistema de voto electrónico que pretenda transmitir confianza ha de ser sometido a auditorías periódicas por distintas entidades externas de confianza.

Como se comenta en [5], la tecnología elegida debe funcionar de manera confiable con la infraestructura disponible, teniendo en cuenta las condiciones predominantes del entorno.

Es altamente aconsejable disponer de un "plan B" en caso de problemas inesperados en la infraestructura, fallas o colapsos del sistema con el fin de garantizar la continuidad del proyecto, especialmente cuando existan limitaciones temporales o cuando se trate de una implementación inicial.

También es importante a la hora de generar confianza en un sistema de voto que la ciudadanía conozca su funcionamiento antes de su uso, pues lo desconocido suele causar rechazo. Esta "educación" podría llevarse a cabo de distintas maneras, complementarias entre ellas: pequeños anuncios televisivos explicando básicamente el funcionamiento del sistema, enviando un manual junto a la tarjeta censal en unas primeras votaciones en las que el uso del voto electrónico se considere opcional, teniendo el sistema preparado en los colegios electorales y animando a los votantes a que lo empleen en lugar del sistema tradicional, guiándolos en caso de dudas para, poco a poco, generar confianza en el sistema.

De este modo, la introducción paulatina de este sistema permitiría a la ciudadanía estar al tanto de su funcionamiento (además de permitir el refinamiento iterativo del sistema, pues un sistema nunca está exento de errores en sus primeras versiones) y se

podría acabar implantando como sistema principal de votación, quedando cada vez más en desuso el sistema tradicional con urnas y papeletas o el voto por correo.

2.3. Código cerrado vs código abierto

Actualmente, tal y como se menciona en [5], todos los sistemas de voto electrónico actualmente disponibles son de código cerrado. Tanto los sistemas privativos como los de código abierto tienen sus ventajas y sus inconvenientes, que se analizan a continuación:

Los defensores del software privativo aluden a la seguridad. Ya que ningún sistema es infalible, sostienen que manteniendo el código en secreto es más difícil para delincuentes informáticos encontrar fallas en el sistema y aprovecharse de ellas para manipularlo. Como contrapartida el software privativo podría permitir con más facilidad la existencia de puertas traseras en según qué contextos, ya que si bien el software ha de ser sometido a auditorías periódicas, tan sólo estos auditores serían capaces de revisar el código, por lo que estos habrían de ser de confianza para garantizar la integridad del sistema.

Los defensores del software libre, en cambio, defienden que si bien es cierto que al hacer público el código los agujeros de seguridad del sistema están más expuestos, no sólo los delincuentes informáticos serían capaces de encontrarlos, sino toda la comunidad informática, que no sólo podría avisar de los errores, sino que además podría incluso ser capaz de encontrar una solución temprana a estos. En cuanto a términos de confianza, el código abierto otorgaría más transparencia al sistema, aunque esto supusiera poner en riesgo la seguridad de este.

El prototipo de sistema de voto electrónico implementado en este proyecto mantiene por el momento su código fuente cerrado, a excepción de la herramienta de generación de voto, pues está escrita en JavaScript y se ejecuta en el navegador, por lo que cualquiera puede inspeccionar el código desde este. Aun así, no se descarta la publicación del código en un futuro.

3. Conceptos previos

En este apartado se introducen una serie de conceptos necesarios para la posterior comprensión del protocolo e implementación llevados a cabo para el sistema de voto electrónico.

3.1. Cifrado Vernam

Tal y como se define en el libro "*Handbook of applied criptography*" [7], el cifrado de Vernam es un cifrado de flujo en el que un texto en claro codificado en binario,

$m_1m_2...m_t$, se combina mediante la operación XOR ($\oplus$) con un flujo de datos aleatorio, $k_1k_2...k_t$, del mismo tamaño y de un sólo uso, que constituye la clave de cifrado, generando un texto cifrado, $c_1c_2...c_t$.

$$c_i = m_i \oplus k_i,\ 1 \leq i \leq t$$

Para volver a obtener el texto original, tan sólo hay combinar mediante una XOR el texto cifrado con la clave.

$$m_i = c_i \oplus k_i,\ 1 \leq i \leq t$$

Algunas de las características del cifrado Vernam son su simplicidad de uso y facilidad de implementación, pero la más importante es, sin duda, su infalibilidad, ya que en las condiciones descritas anteriormente, es imposible tener la certeza de que un criptograma corresponde a un determinado texto en claro.

3.2. *Secure Hashing Algorithm* (SHA)

La familia SHA [7] [8] es un conjunto de funciones resumen (SHA-1, SHA-256, SHA-512…) desarrolladas por la Agencia de Seguridad Nacional de los EEUU (NSA). Una función resumen (o *hash*, picadillo en inglés) es un algoritmo que transforma un conjunto arbitrario de elementos de datos, en un único valor de longitud fija.

Estas funciones permiten "digerir" documentos de cualquier tamaño, obteniendo un resultado de una talla fija (de 160 a 512 bits, dependiendo del algoritmo), lo cual es altamente ventajoso para el uso de firmas digitales, entre otros mecanismos. Pues en lugar de firmar el documento entero –algo que sería computacionalmente alto –se pueden aplicar estas funciones de firma sólo a la función resumen, pues se puede comprobar fácilmente que una función resumen corresponde a un documento concreto.

Las funciones resumen no son inyectivas, por lo que se pueden producir colisiones, esto es, conjuntos de datos distintos pueden obtener la misma función resumen. Es decir, existen conjuntos de datos $x_1 \neq x_2$ tales sus resúmenes $h(x_1) = h(x_2)$. Las posibilidades de colisión disminuyen de manera exponencial con el incremento de la talla del resumen, por lo que la talla a elegir de este dependerá del uso que se le vaya a dar.

3.3. Cifrado de clave pública: cifrado RSA

El cifrado de clave pública (o asimétrico) permite a una persona o entidad B (Bob en la Ilustración 1) disponer de una clave privada sólo conocida por esta y una clave pública asociada, disponible para todo el mundo, A (Alice en la Ilustración 1). Esto permite que los emisores (A) que se quieran comunicar con B, puedan cifrar un mensaje con la clave pública de B, siendo sólo descifrables por B con su clave privada. De esta manera se asegura que tan sólo emisor y receptor pueden leer el mensaje. Este tipo de claves suponen una alternativa a las claves simétricas, que ofrecen muchas menos posibilidades, pues ambos interlocutores son conocedores de la misma clave, lo que

dificulta mecanismos como el de la firma digital. Además del inconveniente que supone el intercambio de la clave, ya que si no se hace por un canal seguro, este tipo de cifrado pierde su efectividad.

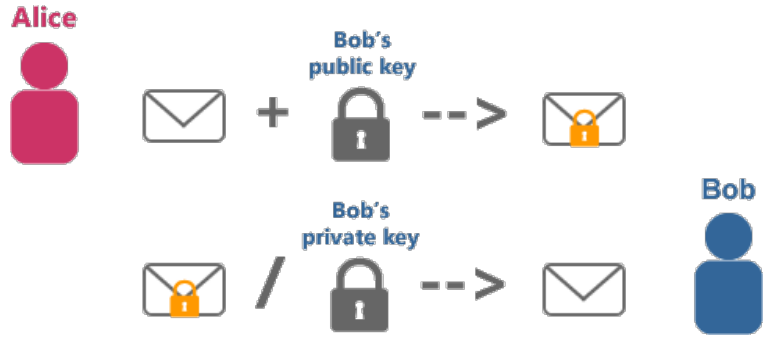

Ilustración 1 - Cifrado de clave pública

Uno de los sistemas de cifrado de clave pública más conocidos es RSA, desarrollado por R. Rivest, A. Shamir y L. Adleman en 1977 . A continuación se muestra su algoritmo tal y como se detalla en [7]:

- Generación de un par de claves RSA por la entidad B:

1. Generar dos números primos aleatorios grandes y distintos, p y q, de aproximadamente el mismo tamaño.
2. Calcular $n = pq$ y $\varphi=(p-1)(q-1)$.
3. Seleccionar un entero aleatorio e, $1<e<\varphi$, tal que el MCD$(e, \varphi) = 1$.
4. Usar el algoritmo de Euclides para calcular el único entero d, $1<d<\varphi$, tal que $ed \equiv 1 \pmod{\varphi}$.
5. La clave pública de B es (n, e); Su clave privada es d.

Los enteros e y d son conocidos como exponente de cifrado y exponente de descifrado, respectivamente, mientras n es conocido como módulo.

- Cifrado con clave pública (de B) por la entidad A.

1. Obtener la clave pública (n,e) de B.
2. Representar el mensaje como un entero m en módulo n.
3. Calcular $c=m^e \bmod n$.
4. Enviar el texto cifrado c a B.

- Descifrado de c para obtener m por parte de B.

1. Usar la clave privada d para recuperar $m = c^d \bmod n$.

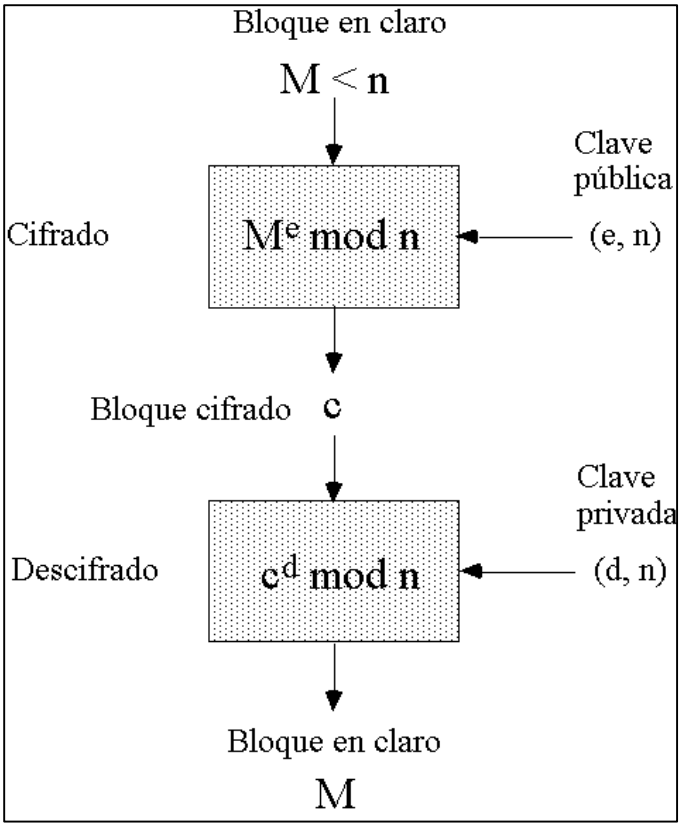

Ilustración 2 - Cifrado RSA

Este sistema permite la creación de canales seguros, que pueden servir para el intercambio de claves simétricas, por ejemplo. De hecho, el protocolo utilizado para las comunicaciones seguras en esta implementación, TLS, del que se habla más adelante, utiliza este sistema para el intercambio de claves simétricas.

A la hora de representar las claves RSA, dos de las codificaciones más utilizadas son DER y PEM [9]:

DER simplemente codifica la clave en formato binario, por lo que al intentar abrir esta en cualquier editor de texto no se ve nada legible, tan sólo símbolos extraños.

La codificación PEM incluye la misma información que la clave en formato DER, sólo que codificada en Base64, con un encabezamiento (*header*, en inglés) y un pie de página (*footer*, en inglés). La codificación PEM es mucho más versátil a la hora de tener que mostrar la clave en una web, enviarla por correo, etc., ya que esta es legible y se puede copiar y pegar con facilidad.

3.4. Firma digital con RSA

La firma digital [7] es un mecanismo de cifrado que permite a un usuario o entidad confirmar su identidad a cualquier otro usuario o entidad. El usuario o entidad que recibe la firma debe ser capaz de probar a un tercero la autenticidad de la firma.

Esta firma ha de poseer las mismas características que la firma tradicional: debe ser fácil de generar por el propietario, no ha de poder ser rechazada por su propietario, sólo el propietario debe ser capaz de generarla, debe ser fácil de verificar por cualquier receptor y debe depender del mensaje, para que esta no sea reutilizable.

Algunos sistemas de cifrado de clave pública se prestan para su uso en sistemas de firma digital: el firmante firma el mensaje cifrándolo con su clave privada, por lo que él es el único capaz de generarla. El receptor del mensaje puede verificar la firma fácilmente usando la clave pública del firmante. Del mismo modo, la firma no puede ser repudiada por el firmante, ya que si puede ser verificada con su clave pública, significa que ha sido firmada con su clave privada, sólo conocida por él.

La firma digital con RSA se implementa aprovechando la coincidencia de dominio y codominio del sistema. Si en el cifrado el emisor (A) cifra el mensaje con la clave pública del receptor (B) y este descifra el mensaje con su clave privada. En la firma, el emisor (A) firma con su clave privada y el receptor (B) verifica la firma con la clave pública de A.

A continuación se describe un protocolo de firma digital con RSA:

- Generación de un par de claves RSA

La generación del par de claves se realiza tal como se muestra en el apartado anterior. Al fin y al cabo, el cifrado y la firma son distintas formas de aprovechar el algoritmo RSA.

- Generación de la firma.

Por temas de ahorro computacional, se suele firmar el resumen h(m) de un mensaje m en lugar del mensaje completo, pues el resumen tiene una talla fija, normalmente menor al mensaje en sí. Se toman *n, d* y *e* de la generación de clave RSA del apartado 3.3.

1. Cálculo de h = hash(m), en módulo n
2. Cálculo de $s = h^d \bmod n$.
3. La firma del mensaje es s, por lo que procede a enviarse [m | s].

- Verificación de la firma.

1. Obtención de la clave pública (n,e).
2. Cálculo de $h = s^e \bmod n$.
3. Cálculo h' = hash(m).
4. Si $h = h$', la verificación ha sido un éxito.

3.5. SSL/TLS

El protocolo SSL/TLS [10] [11] permite proteger las conexiones entre cliente y servidor. Esta protección permite al cliente asegurarse de que ha contactado con el servidor auténtico y enviarle información sensible. Aunque el objetivo inicial era su uso con HTTP, se optó por introducir las mejoras de seguridad a nivel de transporte, para poder aprovecharlas en más aplicaciones.

El protocolo de transporte *Secure Sockets Layer* (SSL) fue desarrollado por Netscape Communications en los años 90, siendo la versión 2.0 la que alcanzó la popularidad. Netscape llegó a publicar una versión 3.0 con muchos cambios respecto a la versión anterior, pero esta apenas caló.

El protocolo *Transport Layer Security* (TLS) fue elaborado por la Internet *Engineering Task Force* (IETF). La versión 1.0 de este protocolo es prácticamente igual a SSL 3.0, por lo que en algunos contextos se considera TLS 1.0 como si fuese SSL 3.1.

Entre las características del protocolo SSL/TLS encontramos principalmente:

- Confidencialidad: El flujo de paquetes intercambiado entre cliente y servidor va cifrado mediante claves simétricas, una para los paquetes enviados del cliente al servidor y otra para los paquetes enviados en sentido contrario. El intercambio de estas claves se lleva a cabo al inicio de la conexión utilizando criptografía de clave pública.
- Autenticación de la entidad: El cliente puede corroborar la identidad del servidor con el que conecta mediante un protocolo basado en firmas digitales. Para la validación de estas firmas, el cliente requiere de la clave pública del servidor, conseguida normalmente a través de certificados digitales. SSL/TLS también permite la autenticación del cliente ante el servidor, aunque esta característica no se usa demasiado debido a que las aplicaciones suelen tener su propio sistema de autenticación.
- Autenticación del mensaje: Cada paquete enviado en una conexión SSL/TLS puede incorporar un Código de Autenticación de Mensaje (MAC, por sus siglas en inglés: *Message Authentication Code*) que demuestre que el paquete no ha sido modificado. Un código MAC es un *hash* del mensaje cifrado con una clave simétrica conocida por emisor y receptor, lo que permite comprobar al receptor que el mensaje recibido no ha sido alterado. Las claves secretas para el cálculo de dichos códigos se acuerdan también de forma segura al inicio de la conexión.
- Eficiencia: Si el cliente pide más de una sesión simultánea o muy cercana en el tiempo, en lugar de repetir la autenticación y el intercambio de claves, existe la opción de reutilizar los parámetros acordados en la primera negociación.
- Extensibilidad: al inicio de cada sesión cliente y servidor negocian los algoritmos que utilizarán para el intercambio de claves, autenticación, cifrado, etc. La extensibilidad del protocolo permite añadir nuevos algoritmos si se descubren otros más eficientes o seguros.

3.6. HTTPS

HTTPS (*Hypertext Transfer Protocol Secure*, en español: Protocolo seguro de transferencia de hipertexto) [12] [13] está basado en HTTP (*Hypertext Transfer Protocol*). HTTPS proporciona mecanismos de comunicación segura entre cliente y servidor con la intención de permitir transacciones comerciales, así como el intercambio de información sensible. Este protocolo hace uso de TCP y se apoya en SSL/TLS para crear un canal cifrado que permita el tráfico de dichos datos sensibles sin que estos puedan ser interceptados por ningún atacante. Por lo general, HTTPS utiliza el puerto 443.

4. Protocolo de voto propuesto

El protocolo de voto electrónico que se propone consta de dos autoridades, Mesa de Identificación (MI) y Mesa de Voto (MV), que se asumen independientes, es decir, no tienen relación entre ellas salvo para la comunicación de sus claves públicas. Además, también se asumen canales de comunicación seguros entre los electores y dichas entidades.

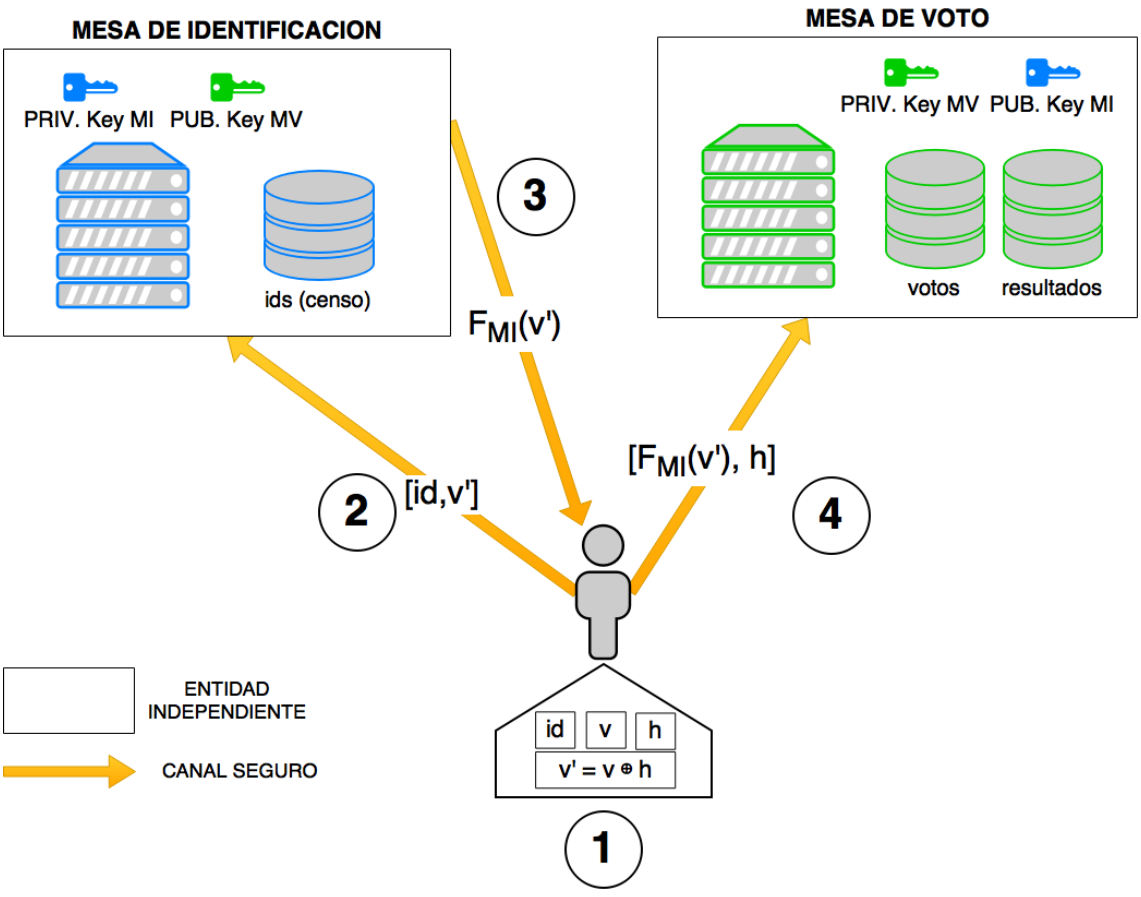

Ilustración 3 - Protocolo de voto electrónico

Tanto la MI como la MV disponen de un par de claves asimétricas, que permiten un sistema de firma digital, siendo conocedores cada una de las entidades de la parte pública de la clave de la entidad contraria.

Sea v el voto del elector. El votante genera un valor aleatorio h, del mismo tamaño que v, que hace de máscara de ocultación tal que $v' = v \oplus h$, siguiendo un proceso similar al cifrado de Vernam, es decir, una operación XOR bit a bit del código de la opción elegida con la máscara generada anteriormente. Teniendo en cuenta las propiedades del cifrado de Vernam, no es posible obtener el sentido del voto sin la máscara de ocultación, siendo el elector el único conocedor de esta máscara.

El elector comunica a la MI el par [id, v'] para identificarse y obtener el voto certificado mediante la firma de este por parte de la MI. A continuación, la MI comprueba que el id del elector pertenece al censo. En caso afirmativo certifica el voto del elector y le devuelve $F_{MI}(v')$. Además, almacena el par [id, v'] con el fin de permitir el mecanismo de "vuelta atrás" del que se habla más adelante. El proceso de identificación y certificación sólo se puede solicitar una vez por votante, salvo que se disponga de un comprobante de máscara repetida expedido por la MV, de lo cual se habla más adelante. Nótese que es imposible para la MI descubrir sentido del voto, ya que este se oculta mediante un proceso de enmascaramiento que comparte características con el cifrado de Vernam, que es infalible siempre que la clave sea de la misma longitud que el mensaje y no sea reutilizada.

Una vez comprobada su pertenencia al censo por la MI, y habiendo recibido $F_{MI}(v')$, el elector comunica a la MV el par $[F_{MI}(v'),h]$. La MV verifica la firma del voto, obteniendo v'. Una vez hecho esto, la entidad obtiene el voto calculando $v = v' \oplus h$. Téngase en cuenta que la MV es incapaz de averiguar la identidad del votante, ya que el id sólo se comunica a la MI y se asume que ambas autoridades son independientes.

Con el fin de permitir al votante la comprobación de la integridad del sistema de voto, la MV almacena junto al voto, la máscara, sólo conocida por el votante (y ahora también la MV, aunque sin poder asociarla a este). De este modo, una vez realizado el escrutinio, el votante puede comprobar que su voto se ha emitido en el sentido correcto utilizando utilizando la máscara.

Pero este método plantea una problemática, pues implica la necesidad de que una misma máscara no se repita para distintos votantes. Es por esto que el protocolo incluye un sistema de "vuelta atrás", con el cual si la MV detecta una máscara repetida, no emite el voto y devuelve al elector un comprobante firmado $F_{MV}(v')$, que le permite volver a identificarse en la MI con un nuevo voto (y por ende, una nueva máscara).

A una hora dada (establecida y anunciada con anterioridad) se cierran las mesas, momento a partir del cual no se pueden emitir más votos. Acto seguido, y antes de realizar el escrutinio, se eliminan todos los registros de la MI, con el fin de aumentar la privacidad del sistema y dificultar cualquier posible vinculación votante-voto. Tras esto, se procede al escrutinio, prácticamente instantáneo, y a la publicación de los resultados.

Este protocolo garantiza las siguientes propiedades, la mayoría presentes en las propiedades deseables mencionadas en la introducción:

- Democracia: Sólo los miembros de un censo dado pueden votar, además de poder hacerlo tan sólo una vez.
- Privacidad: no puede relacionarse votante y voto siempre que las autoridades se mantengan desligadas.
- Seguridad: Bien implementado, nadie debería poder suplantar a otro elector que decida no votar.
- Justicia: No se puede conocer el resultado de la votación antes de que esta termine.
- Verificalidad: Los votantes pueden verificar la integridad de su voto, tanto antes de emitirlo como una vez escrutado.
- Completitud: Bien implementado, el resultado de la votación se adecúa a los votos emitidos. En caso de que el recuento no fuese preciso por problemas de la implementación, siempre se podría volver a realizar el recuento manualmente sobre la lista de votos.
- Precisión: No es posible añadir o eliminar votos. Además, una vez emitido un voto, este no puede ser alterado.

5. Implementación y pruebas

Para la implementación del protocolo mencionado anteriormente se han diseñado distintos portales web que facilitan todo el proceso de voto: generación del voto, Mesa de Identificación, Mesa de Voto, Escrutinio y resultados, así como una pequeña aplicación en Java con la que poder validar localmente el voto firmado por la MI antes de enviarlo a la MV.

5.1. Generación del voto

El portal de generación del voto se encarga, tal y como su nombre indica, de generar el voto que más tarde será firmado por la MI y posteriormente será emitido en la MV. Además, facilita la tarea de ocultamiento del voto, por lo que también genera una máscara descargable.

El generador de voto se ejecuta completamente de forma local en la máquina del votante con el objetivo de evitar cualquier tipo de seguimiento e invasión de la privacidad. Se trata de un portal web programado en HTML y JavaScript, por lo que no necesita comunicarse con el servidor una vez descargados en el navegador los archivos .html y .js (véase la Ilustración 5). De hecho, se anima al votante a desconectarse de internet durante el proceso de generación de voto (véase la Ilustración 4). Es importante el hecho de que la generación del voto y la máscara de ocultación se haga en local, pues es el único momento del proceso en el que se puede vincular al votante con la opción elegida, a través

del id. Una vez generado el voto, la privacidad del usuario no corre peligro, pues la opción elegida ya queda oculta por la máscara.

El voto generado se almacena en un archivo de texto plano, formateado como CSV, con extensión ".voto" y con estructura [id, v⊕h], siendo:

- id: el identificador recibido por el votante por parte del censo. En este prototipo, por falta de recursos, no se ha implementado ninguna medida de seguridad extra para evitar la suplantación de identidad, aunque en una implementación real podría emplearse un sistema de autenticación en dos pasos, enviando un segundo código aleatorio al votante por SMS o similar, como ya se hace en la mayoría de servicios y redes sociales de internet, como Google [14].
- v: el código interno de la opción elegida por el votante en hexadecimal (en esta implementación, el código consiste en el SHA-256 de la opción elegida).
- h: máscara aleatoria con la que ocultar la opción elegida.

En esta implementación, la máscara se calcula como SHA-256 (t1 | palabra | t2), siendo:

- t1: instante de tiempo desde el 1 de enero de 1970, en milisegundos, en el que el votante comienza a generar el voto.
- palabra: palabra introducida por el votante para aportar aleatoriedad
- t2: instante de tiempo desde el 1 de enero de 1970, en milisegundos, en el que se genera el *hash*.

Con el fin de evitar en medida de lo posible las colisiones en las máscaras y el uso del método de "vuelta atrás" explicado en el protocolo se han realizado unas pruebas de colisión de la máscara con los siguientes resultados: se han realizado 100.000 SHA-256 utilizando siempre la misma palabra, cambiando tan sólo los instantes t1 y t2, sin obtener colisión alguna, por lo que se prevé que si la palabra también es distinta en cada SHA la probabilidad de colisión sea todavía menor, siendo suficiente para este prototipo. En una implantación real, en la que el número de votantes fuese mayor se podría optar por la utilización de un SHA-512, así como el uso de más variables aleatorias que reduzcan la posibilidad de colisión.

La máscara que se genera ha de ser descargada, tratándose de un archivo con extensión ".mascara" que contiene la máscara de ocultación, con estructura [h]. Este archivo es necesario a la hora de votar en la mesa de voto, pues sin esta la MV no puede hacer visible el voto. Además, tal y como se comenta en el protocolo, la máscara es un elemento necesario si se pretende comprobar la integridad del voto antes de emitir el voto y una vez realizado el escrutinio.

Resumiendo, una vez finalizada la generación del voto y antes de comenzar el siguiente paso del proceso, el elector ha de tener en su poder dos archivos, el voto en sí (con extensión ".voto") y la máscara de ocultación (con extensión ".mascara").

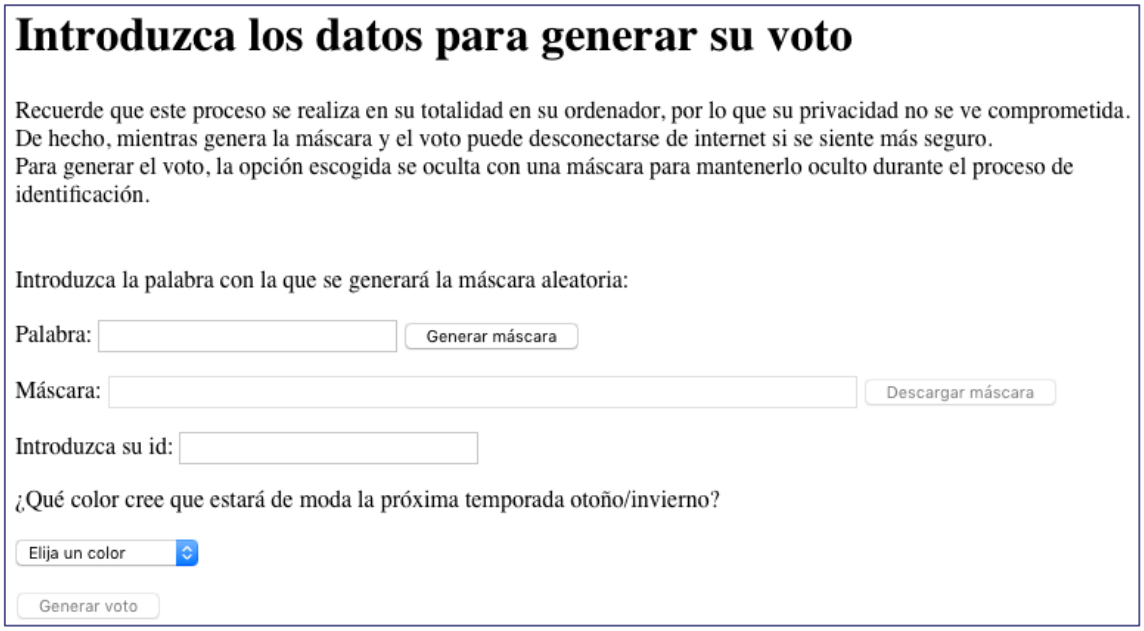

Ilustración 4 - Captura de la generación del voto

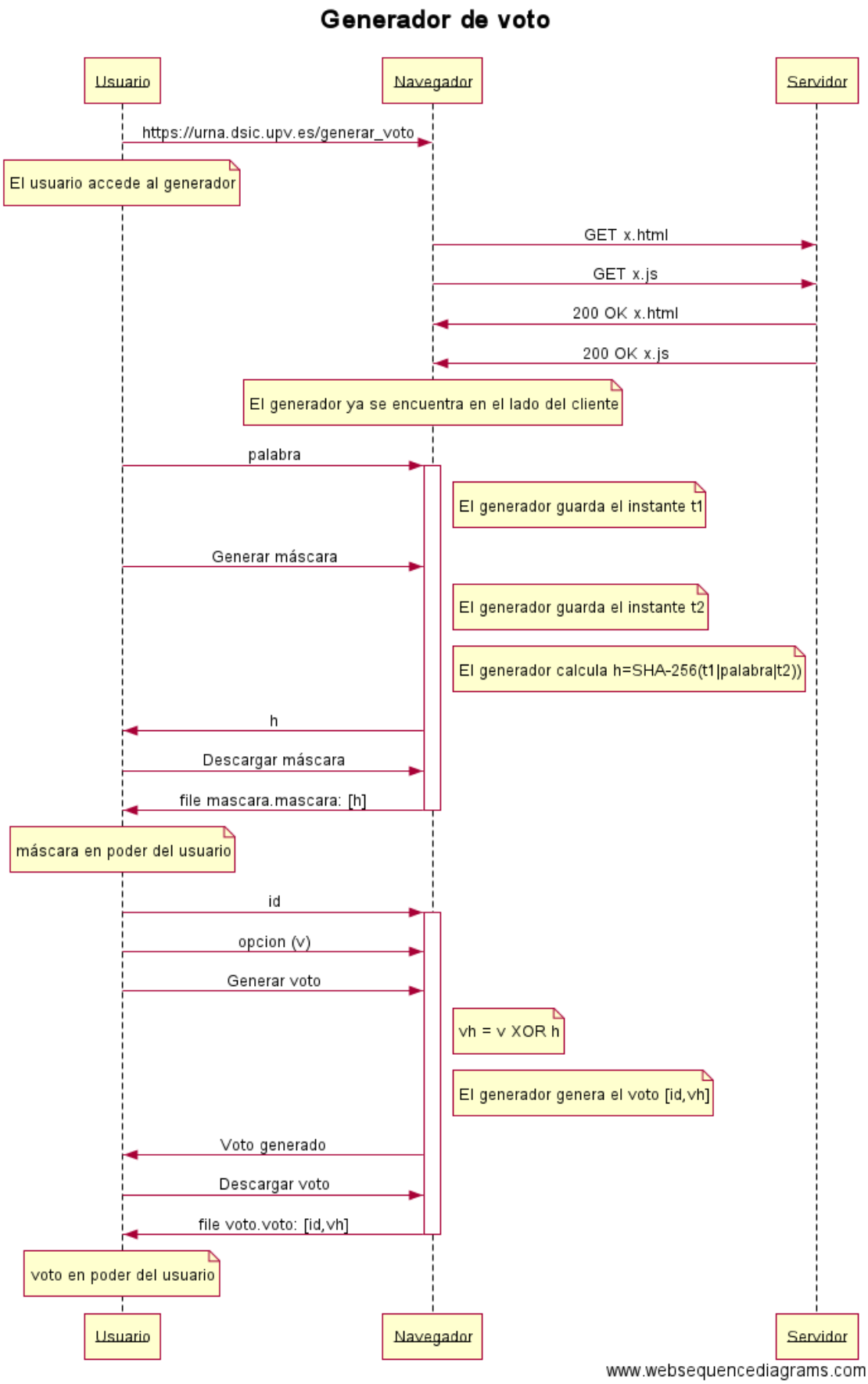

Ilustración 5 - Diagrama de secuencia del generador de voto

5.2. Mesa de Identificación

Una vez generado el voto, el votante ha de identificarse con el fin de comprobar que su id se encuentra en el censo. Este paso se realiza en la MI, otro portal web, esta vez sí con *backend* en el servidor.

En la MI, el usuario aporta su voto (con la opción elegida oculta con la máscara), con el fin de identificarse – la MI comprueba que el id se encuentra en la base de datos del censo – y en caso de efectivamente encontrarse en este, recibir su voto certificado, con el que poder votar en la MV. La estructura del voto certificado por la MI es F_{MI}("2016", v⊕h), siendo "2016" un "número mágico" que permite a la MV verificar la firma. Durante el proceso de identificación, la MI guarda el voto oculto (v⊕h) junto al id del votante en la base de datos con objeto de implementar el mecanismo de "vuelta atrás" mencionado anteriormente.

El proceso de identificación y certificación sólo se puede realizar una vez, salvo que se disponga de el comprobante de máscara repetida de la MV. En ese caso, cuando la MI recibe el nuevo voto generado y el comprobante de la MV, comprueba en la base de datos que el id del nuevo voto tiene asignado el mismo v⊕h incluido en el comprobante, lo que implica que ese votante ha intentado votar con ese v⊕h pero no ha podido hacerlo debido a que la máscara ya existía, por lo que se le permite identificarse de nuevo y certificar el nuevo voto.

Como se ha comentado anteriormente, esta certificación consiste en un proceso de firmado. Se ha optado por esta nomenclatura con el fin de hacer el proceso más comprensible para el público no iniciado en el tema.

Para las firmas digitales (tanto de la MI como de la MV) se ha optado por el sistema criptográfico de clave pública RSA [7], con un tamaño de clave de 1024 bits en formato PEM, si bien es cierto que a la hora de ser manipuladas en el *backend* (Java) son convertidas a formato DER con las librerías Bouncy Castle [15], pues Java no es capaz de manipular el formato PEM de manera nativa.

Además, se ha optado por un protocolo de firma algo distinto al mencionado en la explicación del sistema de firma con RSA, pues no se ha utilizado función resumen para firmar, sino que se ha aplicado la función de firma al voto completo, ya que este es pequeño y el proceso no es muy costoso computacionalmente hablando.

En cuanto a la Base de Datos (BD), el esquema de la MI (véase la Ilustración 6) dispone de tan sólo una tabla, en la que se almacenan los ids de los votantes (el censo) y el voto oculto de estos ('0' en caso de no haber votado aún). Esta tabla es vaciada antes de realizar el escrutinio, como medida extra de seguridad para asegurar la privacidad de los votantes.

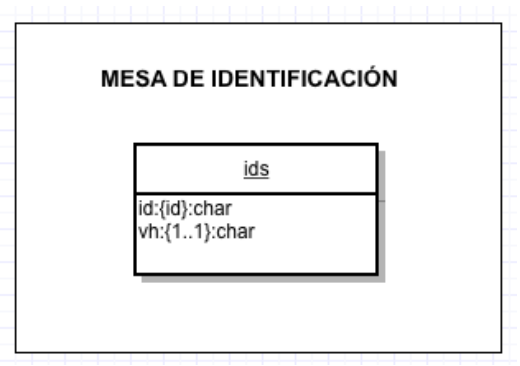

Ilustración 6 - Esquema BD Mesa de Identificación

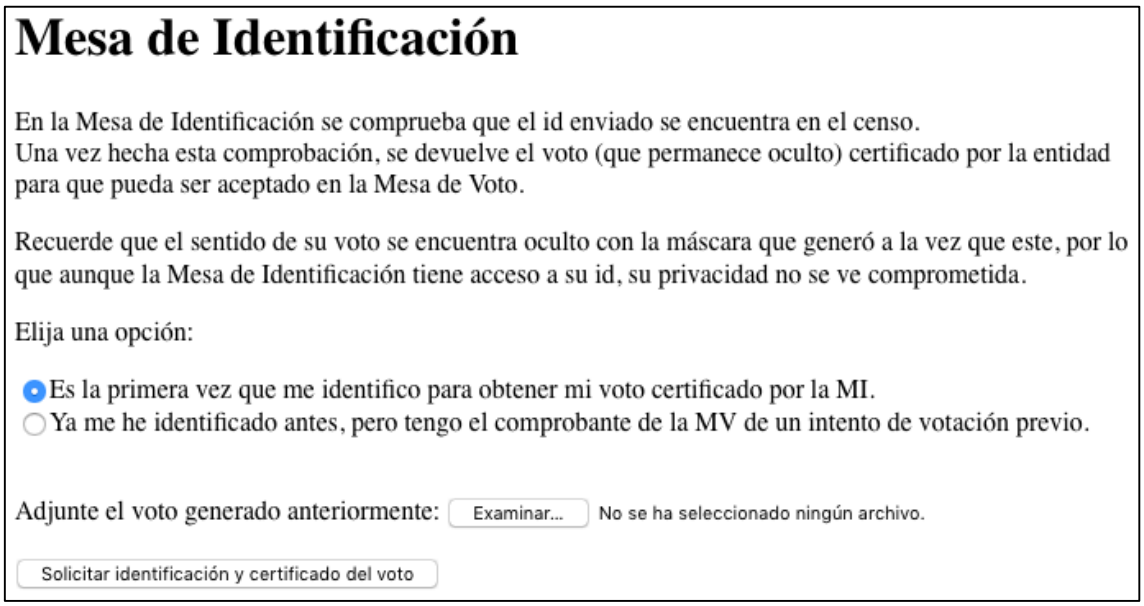

Ilustración 7 - Captura de la MI

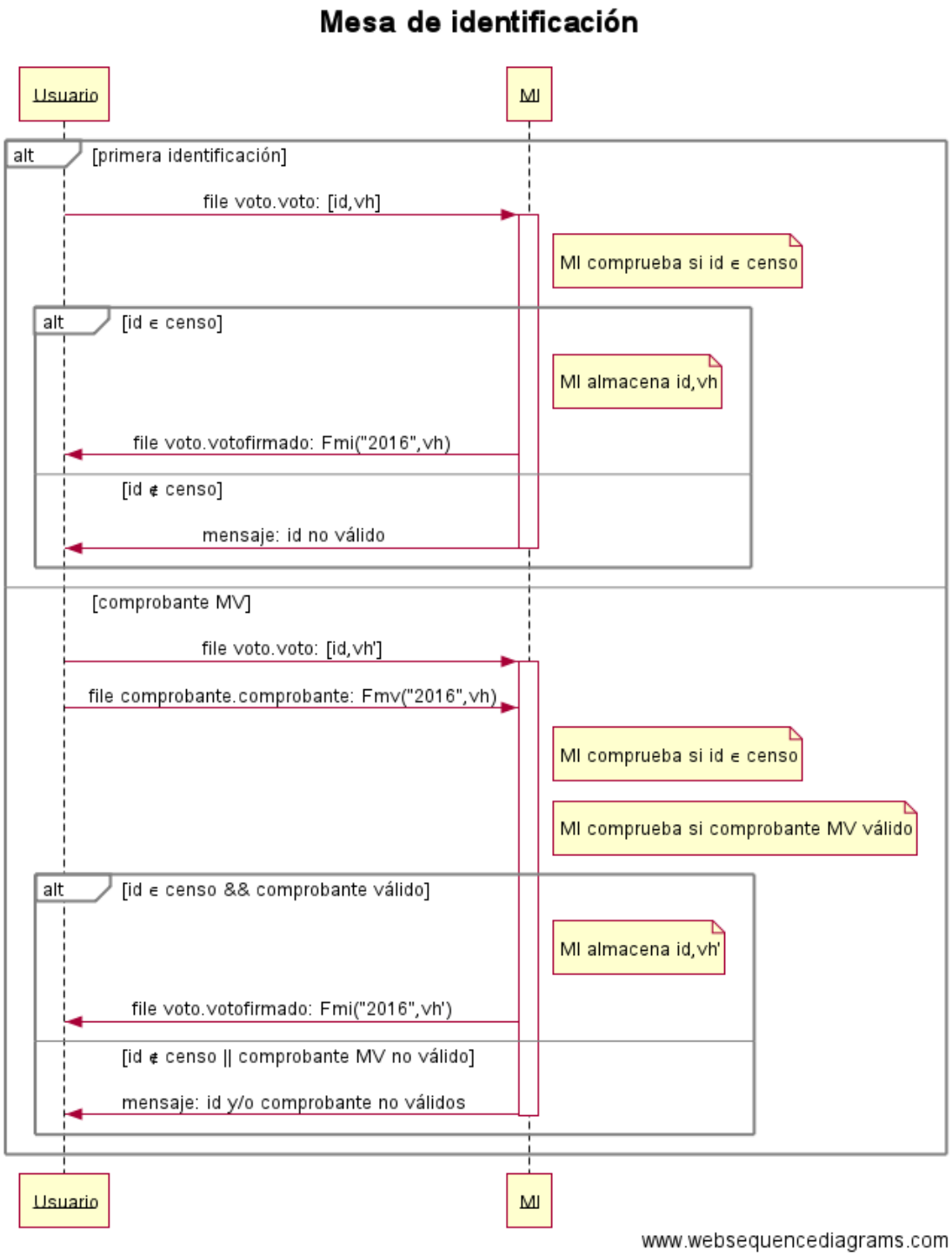

Ilustración 8 - Diagrama de secuencia de la MI

5.3. Mesa de Voto

La Mesa de Voto es el último eslabón en el proceso de votación. Esta entidad es la que se encarga finalmente de almacenar el voto. Consiste de nuevo en un portal web en el que se adjuntan el voto certificado por la MI – F_{MI}("2016", v⊕h) – y la máscara, con la que poder descubrir el voto. Una vez se envían estos elementos, la MV comprueba si la máscara de ocultación se encuentra repetida. Si es así, la entidad genera un comprobante firmado con estructura F_{MV}("2016", v⊕h), con el fin de permitir repetir el proceso de voto, incluyendo la identificación y certificado del nuevo voto en la MI.

En caso de que todo vaya bien y la máscara no se encuentre repetida (lo habitual, según las pruebas realizadas), el voto se emite con normalidad, es decir, la opción elegida se almacena (esta vez sin ocultar) en la base de datos junto a la máscara con la que se había ocultado, que al ser única y secreta, permite al votante comprobar al final del escrutinio que su voto se ha emitido en el sentido correcto.

El esquema en BD de la MV (Ilustración 9) dispone de dos tablas: la tabla "votos", en la que se almacenan las opciones elegidas por los votantes asociadas a la máscara (única y secreta) que sirve para desenmascarar el correspondiente voto; así como la tabla "resultados", en la que una vez finalizada la votación se almacena el recuento de votos, asociando cada opción con el número de votos recibidos.

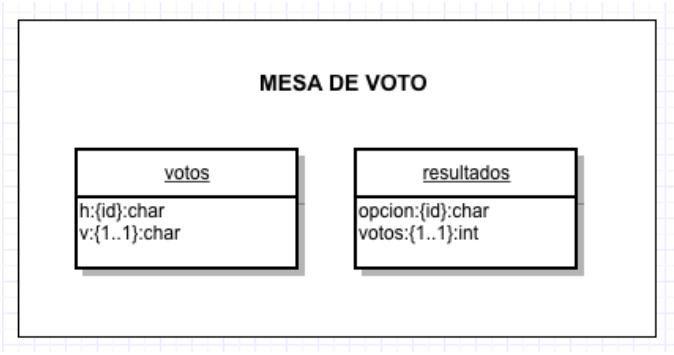

Ilustración 9 - Esquema BD Mesa de Voto

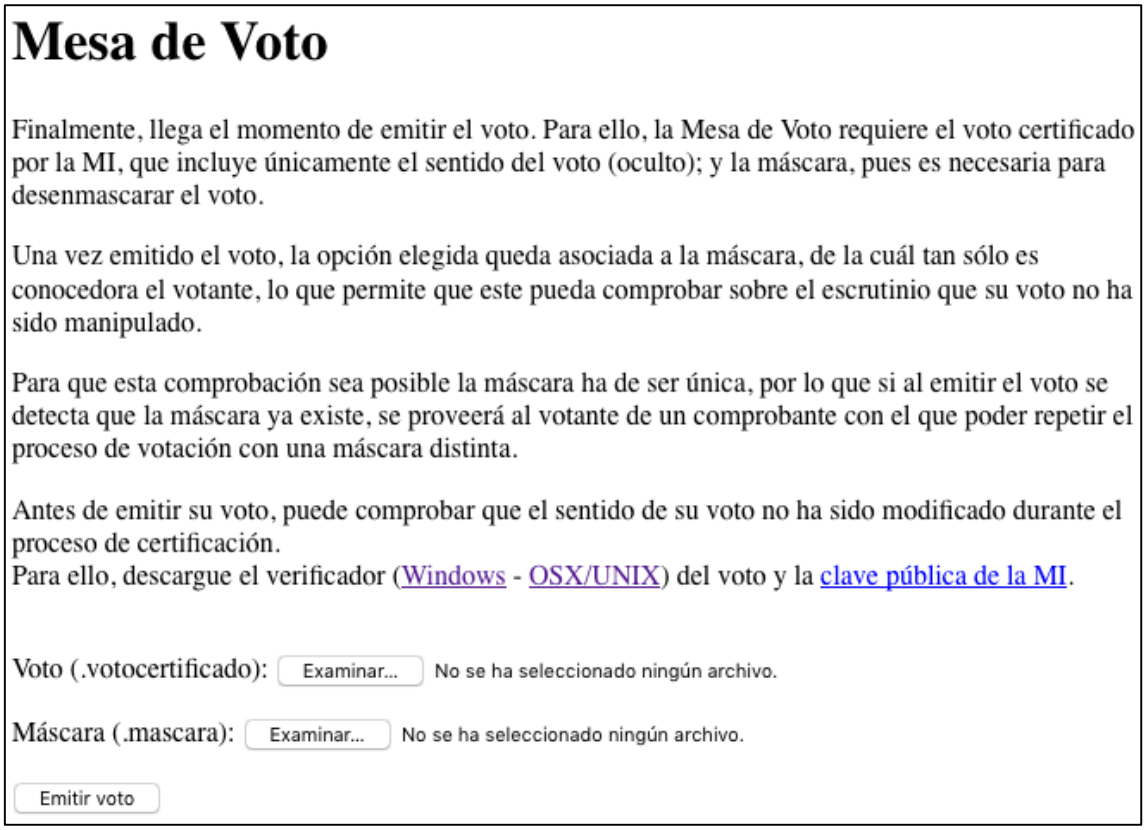

Ilustración 10 - Captura de la MV

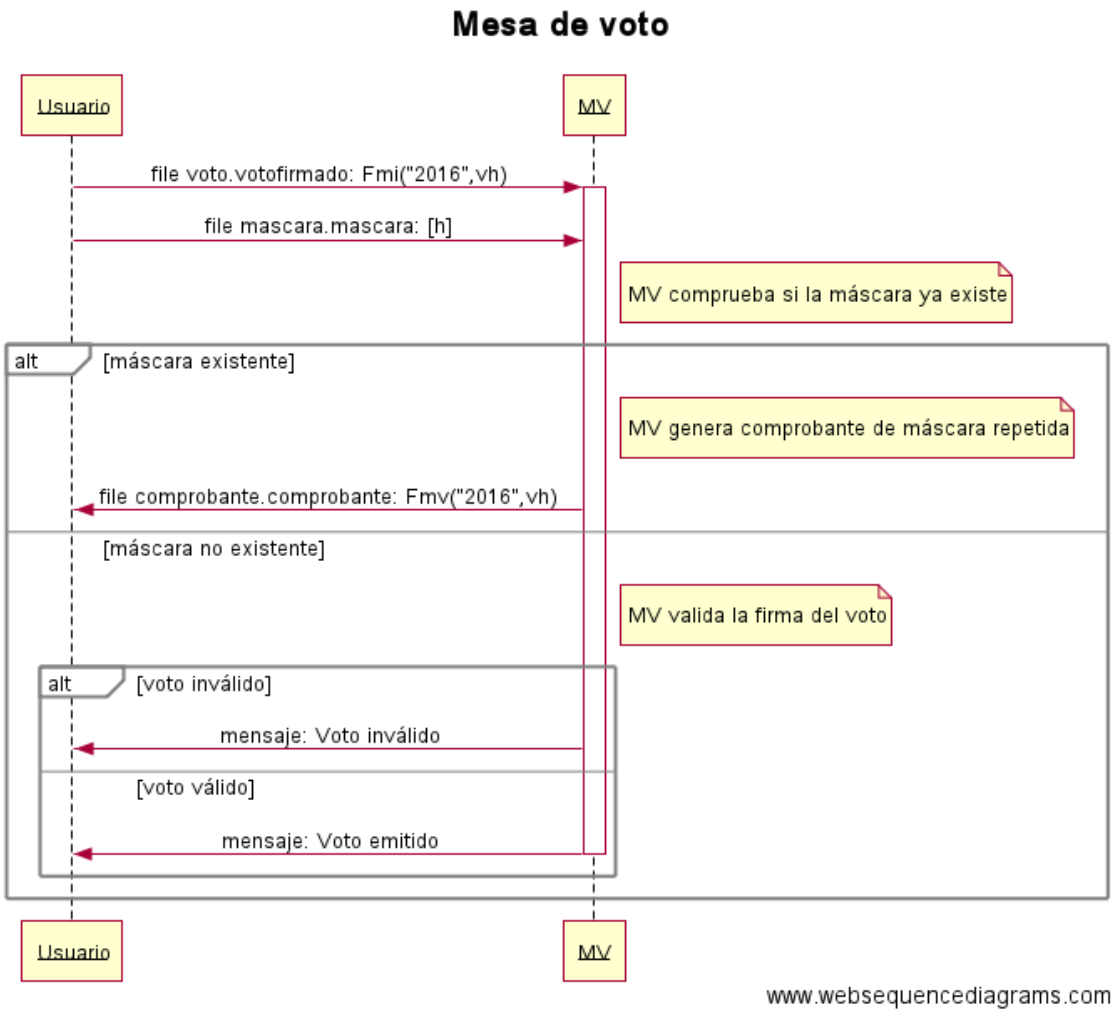

Ilustración 11 - Diagrama de secuencia de la MV

5.4. Escrutinio y resultados de la votación

Después de cerrar las mesas, una vez vaciada la tabla de la MI de la BD y realizado el recuento de los votos se abre un portal web en el que se muestran tanto los resultados de la votación como el escrutinio en su totalidad, con cada voto asociado a su máscara de ocultación, con el fin de que los electores puedan comprobar la integridad de su voto y que no se ha producido ningún tipo de fraude electoral.

Los resultados y el escrutinio se muestran en tablas, ordenadas por número de votos en el caso de los resultados, y por orden alfabético (sobre las máscaras) en el caso del escrutinio. La tabla con el escrutinio cuenta además con un campo que permite filtrar las máscaras, con la finalidad de facilitar al usuario la localización de su máscara y, por tanto, el sentido en el que su voto fue considerado.

Resultados de la votación

Estos son los resultados de la votación.
También está disponible el escrutinio, donde puede comprobar con su máscara que su voto no ha sido manipulado.

Color	Votos
ROJO	2
MORADO	2
ROSA	1
_VOTO_BLANCO_	1
NARANJA	1
NEGRO	1
GRIS	1
AZUL	1
AMARILLO	0
_VOTO_NULO_	0
BLANCO	0
VERDE	0

Ilustración 12 - Resultados

Escrutinio

El escrutinio aparece ordenado alfabéticamente por la máscara.
Utilice el filtro para encontrar su máscara más fácilmente (con los primeros dígitos será suficiente)

Filtrar:

Máscara	Voto
F326A4FF7C533C9943BCD8327D7360F05A1185DBEF8B1F9A39A535B10E6F0107	NARANJA
F31AE1C7B255A5A7A70D5D7E9FA8ED62F014C87F0366AC4B01C792540FDAF299	GRIS
80E5DBCF795FB95917DC3B132575A5770D4632B879349B34CF22AC606AB3215C	ROSA
6A5D6657EDC5808C152578025C53D46B946786336518E8105C33CADB92C4E38B	MORADO
5933023201F63A95B377BA9090ED3C0EF4A5D6EB0B4EA6847F6C866EFD4EB302	NEGRO
57F98C1BEB96D44DE3E29AD34C3DB6E451EC78B3FCBFEEFCCFBC41560F52FFB3	ROJO
4CE5A962D728D9422F29C77AFD1CCD2FE6DBD69AC3D82664F490EB8ADDCC4796	MORADO
4C433FBA2C059179496C88CB14BDA8F08156329D1B162A6E0D408C1942B7FE17	ROJO
2F1775ADD03D5D0A5CA91CCFBC80BD003EFD241C9E5A8AD066D9F3E5A8C3F967	_VOTO_BLANCO_
0BD147C23793612530DBB35BB67E45FC115D7517B8EE2B2BC6E4AA1FB70D8295	AZUL

Ilustración 13 - Escrutinio

5.5. Panel de administración

Además de la parte del sistema visible para el votante, se dispone de un pequeño panel de administración para el administrador de sistema. En principio, para este prototipo, el panel (protegido con usuario y contraseña) tan sólo cuenta con las opciones de abrir y cerrar las mesas y de realizar el escrutinio una vez se han cerrado las mesas.

Se dispone de un esquema en BD para la administración del sistema (Ilustración 14) con una sola tabla, "admin", en la que se almacenan parámetros con distintos valores. P.ej. el parámetro "mesas_abiertas" puede tener valor 0 o 1, dependiendo del estado de las mesas.

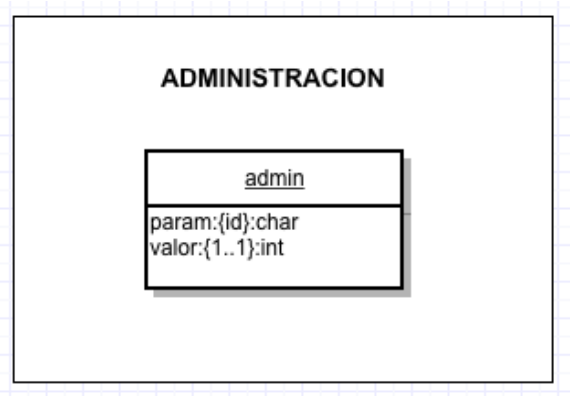

Ilustración 14 - Esquema BD Administración

Ilustración 15 - Panel de administración con mesas abiertas

Ilustración 16 - Panel de administración con mesas cerradas

5.6. Verificador del voto certificado

Con el fin de que el elector pueda verificar su voto certificado y comprobar su contenido antes de emitirlo en la MV, se ha desarrollado una pequeña aplicación en Java. Para ello se han utilizado las librerías de Bouncy Castle, al igual que en el *backend* de las MI y MV, así como las librerías JavaFX para el diseño de la interfaz. Al estar implementada en Java, la aplicación se asume multiplataforma (siempre en términos de escritorio).

Para la verificación del voto, la aplicación requiere del voto certificado por la MI, la máscara generada al principio del proceso y la clave pública de la MI, disponible para descargar en el portal web junto a la aplicación.

Esta se ejecuta completamente en local, por lo que no supone un riesgo para la privacidad del elector, pudiendo si lo considerase necesario desconectarse de internet mientras la utiliza.

Ilustración 17 - Verificador del voto

5.7. Comunicaciones seguras

Un asunto tan delicado como este requiere de unas comunicaciones seguras, pues por mucha privacidad que aporte el protocolo, si las comunicaciones no son seguras, este pierde gran parte de su utilidad, sería como colocar una puerta blindada sin cerradura.

Este trabajo se centra principalmente en la implementación de los detalles del protocolo, por lo que si bien se han implementado unas comunicaciones seguras, estas no son el objetivo principal del proyecto.

Para la implementación de las comunicaciones se ha optado por el uso de HTTPS, ya que garantiza un mínimo nivel de seguridad y resulta fácil de implementar. Debido a la falta de recursos se ha decidido autofirmar el certificado, por lo que al acceder por primera vez al sistema aparece una advertencia de certificado inseguro. Tan sólo hay que indicar que se quiere continuar igualmente y añadirlo a las excepciones para poder acceder sin problema. Para evitar esta advertencia, el certificado debería ir firmado por una Autoridad de Certificación (CA, del inglés *Certification Authority*), lo cual conlleva un coste económico y temporal.

En una implementación real se debería prestar una atención especial a la implementación de unas comunicaciones seguras, así como a la seguridad del sistema en general: seguridad del software utilizado, posibles agujeros de seguridad, seguridad de las infraestructuras, etc. Aun así, los objetivos del proyecto se cubren suficientemente con la elección escogida.

5.8. Consecución de la confianza

Si bien la consecución de la confianza no es un objetivo que se consiga mediante implementación como tal técnicamente hablando, se ha decidido incluirla en este apartado, ya que es uno de los aspectos más problemáticos e importantes del voto electrónico, pues como ya se ha comentado, por muy bueno que sea un sistema de este tipo, si no se consigue que el electorado deposite su confianza en él, no será posible su implantación.

Para tratar de transmitir confianza al elector se han tomado una serie de precauciones:

- Se ha diseñado el sistema lo más simple posible. Tan sólo es necesario pasar por tres webs para realizar el proceso de voto, al igual que únicamente es necesario manejar tres archivos distintos, cuatro en el peor de los casos, con su función bien definida por su extensión: “.voto” para el voto recién generado, “.mascara” para la máscara de ocultación y “.votocertificado” para el voto certificado por la MI. En caso de requerir el comprobante de la MV, “.comprobante” para este.
- Se guía al elector todo lo posible en los portales web, para que no puedan empezar un paso sin terminar el anterior, haciendo (casi) imposible que este se encuentre en una situación en la que no sepa cómo actuar.
- En todos los pasos se explica al elector lo que sucede con su voto, con un lenguaje correcto y lo más comprensible posible para alguien no iniciado en temas de seguridad digital. Además, se hace casi obligatoria la lectura de la explicación, pues se muestra antes de poder realizar ninguna acción.

5.9. Pruebas

Una vez finalizada la implementación del sistema de voto electrónico se ha realizado una fase de pruebas con el objetivo de probar el sistema en un entorno controlado, mediante un *mailing* a 50 usuarios. Al concluir el proceso de voto, han rellenado una encuesta en la que se valora tanto el sistema en general como aspectos más concretos como su usabilidad y confianza transmitida. A continuación se describen los resultados de la encuesta:

En cuanto al nivel de dificultad para cumplimentar la votación (véase la Ilustración 18), se ha obtenido una puntuación mayoritaria de 3 (siendo 1 lo más fácil y 10 lo más difícil), estando además un 70% de las puntuaciones por encima del aprobado.

En cuanto al nivel de explicación del sistema (Ilustración 19), la mayoría de usuarios lo puntúan con un 8, obteniendo un aprobado en el 83% de las valoraciones.

En lo referente al paso peor explicado (Ilustración 20) hay una tendencia clara hacia la valoración negativa del paso de generación del voto, con un 44% de los encuestados, quedando en segundo lugar la identificación y firma del voto en la MI con un 25%.

En cuanto a los navegadores utilizados (Ilustración 21), los dos navegadores más utilizados son Chrome y Firefox (casi empatados al 50%), habiendo utilizado Opera tan sólo un usuario. Además, Safari ha sido el único navegador echado en en falta por un 14% de los encuestados (Ilustración 22).

En las observaciones (Ilustración 23), la mayoría de ellas giran en torno al excesivo número de pasos necesarios para votar, así como a la dificultad en la comprensión del concepto de máscara.

Por último, la puntuación general otorgada al sistema (Ilustración 24) ha sido toda por encima del 5, a excepción de un usuario (un 2,8%). Es decir, un 97,2% de los encuestados aprueban el sistema, con una puntuación predominante de 8.

En definitiva, una vez analizados los resultados, estos son bastante halagüeños, habiendo obtenido un aprobado en todas las secciones. Se marca como pendiente para próximas iteraciones del sistema mejorar tanto la usabilidad del portal de generación del voto como la explicación del concepto de máscara, así como tratar de disminuir el número de pasos necesarios para votar. Además, se valorará hacer el sistema compatible con Safari.

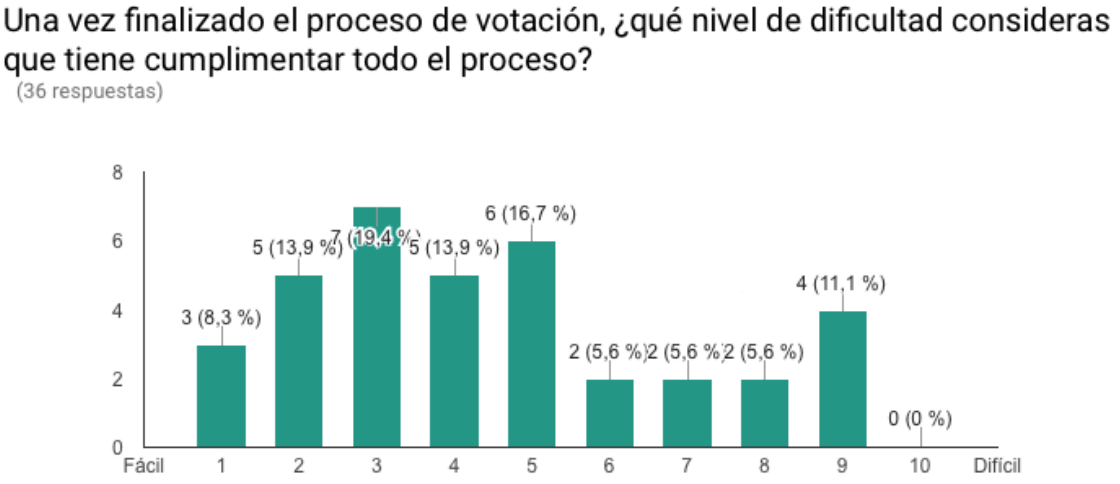

Ilustración 18 - Dificultad del proceso de voto

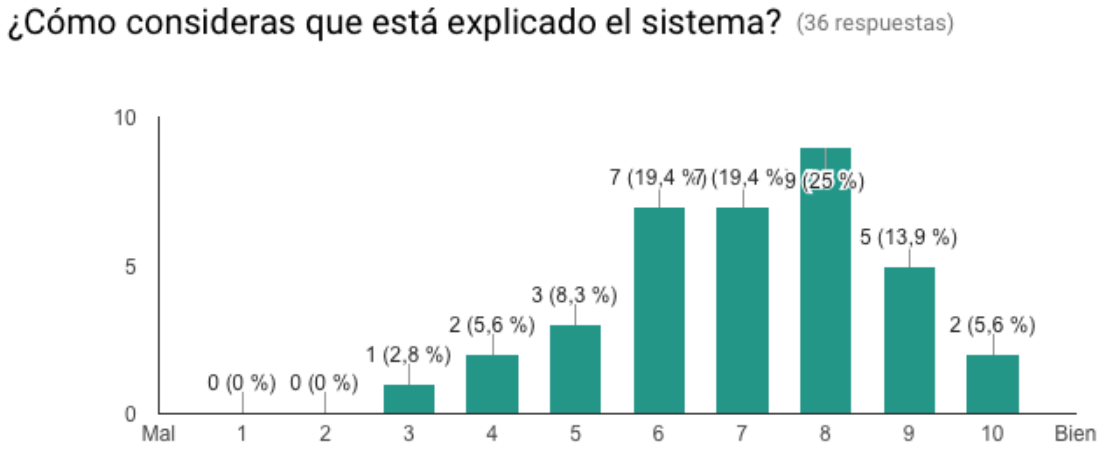

Ilustración 19 - Claridad en la explicación del sistema

Ilustración 20 - Paso peor explicado

¿Qué navegador has utilizado? (36 respuestas)

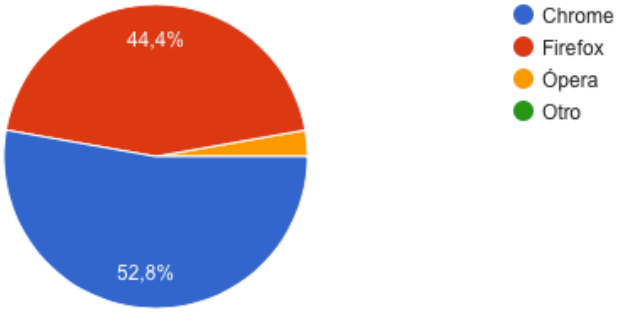

Ilustración 21 - Navegador utilizado

¿Habrías preferido utilizar otro navegador? (18 respuestas)

No
No
No
No
No
No
no
no
no
no
NO
NO
NO
Safari
Safari
Sí. Safari.
Si
Sí, Safari

Ilustración 22 - Sugerencias de adaptación a otros navegadores

Observaciones (14 respuestas)

no
no
El sistema de la máscara no queda claro. Y debería hacerse compatible con otros sistemas operativos (Mac)
La última frase es confusa porque había entendido que tenía que volver a hacerlo y lo he repetido.
Me parece que es un método confidencial y eso es genial pero con tantos pasos creo que no todo el mundo va a saber interpretar el protocolo adecuadamente.
Para mí resulta igual de poco fiable que cualquier otro voto por correo,
Ninguno.
Al principio no he entendido el concepto de la mascara, pero se entiende bien. El sistema es muy claro y sencillo para todo los públicos.
Todo perfecto
Esta muy bien, aunque tenga una cantidad considerable de pasos, se pueden realizar sin problemas gracias a los enlaces que van apareciendo
Faltan colores, y que no identifique al sitio web como un ataque informático.
Creo que este sistema de votación sería idóneo para personas mayores que tienen dificultades para salir de su casa a entregar el voto en colegios electorales, con lo cual, quizá debería de simplificarse algo más, ya que estas generaciones son las que más dificultades tienen a la hora de manejarse con ordenadores. Es bastante sencillo, ya que todo te lo va indicando concretamente y de forma muy específica, pero aún así quizá habría que intentar recortarlo en algún paso menos.
Demasiados pasos, aunque están bien enlazados
El concepto de máscara no queda demasiado claro

Ilustración 23 - Observaciones

¿Qué puntuación general le darías al sistema? (36 respuestas)

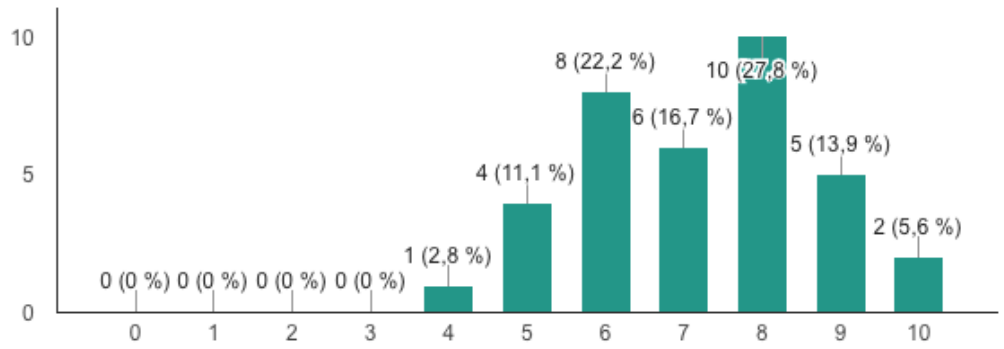

Ilustración 24 - Puntuación general

6. Tecnologías utilizadas

Para la implementación de este proyecto se ha utilizado una combinación de diferentes tecnologías:

6.1. CentOS Linux

CentOS [16] es una distribución Linux derivada de *Red Hat Enterprise Linux*, una distribución ampliamente utilizada en servidores de ámbito profesional, lo que la hace perfecta como anfitriona para un servidor web y de base de datos. Además, durante el grado ha sido una de las distribuciones que más se ha utilizado, sobre todo en redes. Todo esto lo hace el Sistema Operativo (SO) perfecto para albergar el servidor.

6.2. Apache Tomcat

Apache Tomcat es un servidor web que funciona como un contenedor de *servlets*, programas escritos en Java capaces de recibir peticiones web y responder en consecuencia. Tal y como se dice en [17], los *servlets* son componentes web basados en tecnología Java, gestionados por contenedores que generan contenido dinámico. Al igual que otros componentes basados en Java, los *servlets* son clases Java independientes de la plataforma. Estas pueden ser cargadas dinámicamente y funcionar en un servidor web con tecnología Java (como Tomcat). Los *servlets* interactúan con los clientes mediante el paradigma petición/respuesta.

En el caso de la implementación de este sistema de voto electrónico, los *servlets* están presentes en casi todo el proceso de votación: la identificación y la firma del voto en la MI, así como la emisión del voto y la generación del comprobante de máscara repetida en la MV son llevadas a cabo mediante *servlets*.

La decisión de usar de Tomcat como servidor para el sistema de voto se debe principalmente a su funcionamiento con Java, el lenguaje que más se ha utilizado durante el grado, con el que, por tanto, se cuenta con más experiencia.

6.3. JSP

JavaServer Pages (JSP) [18] es una tecnología que permite la creación de páginas web dinámicas de manera similar a como lo hace PHP, pero utilizando lenguaje de programación Java. Una página JSP es un documento basado en texto que describe como procesar una petición para crear una respuesta. Esta descripción intercala datos con

código Java. Para el uso de JSP es necesario un servidor web compatible con contenedores *servlet*, como Tomcat.

Aprovechando la decisión del uso de Tomcat para la utilización de *servlets* Java como *backend* del sistema, se ha optado por utilizar JSP como método para la generación de las webs dinámicas necesarias para el sistema de voto.

6.4. Java

Java [19] es un lenguaje de programación orientado a objetos, concurrente, diseñado para tener las menores dependencias de implementación posibles y poder ser ejecutado en cualquier plataforma sin necesidad de reescribir el código. Para ello hace uso de la Máquina Virtual Java (JVM, *Java Virtual Machine* en inglés), sobre el que se ejecutan los programas. Cualquier sistema operativo capaz de ejecutar la JVM será capaz de, en principio, ejecutar un programa escrito en Java.

Java se ha convertido recientemente en uno de los lenguajes de programación más populares del mundo, gracias principalmente a su carácter multiplataforma.

Java es el principal lenguaje que se ha utilizado en la implementación, ya que además de su uso en *servlets* y JSP, también se ha utilizado para el desarrollo de la aplicación de escritorio que permite verificar el voto certificado antes de emitirlo en la MV. Además, ya que Tomcat funciona con Java, por comodidad se ha aprovechado la librería "keytool" de dicho lenguaje para la generación del certificado X.509 necesario para el uso de HTTPS en el sistema de voto.

6.5. JavaScript

JavaScript (JS) [20] es un lenguaje de programación interpretado, orientado a objetos, basado en prototipos y dinámico. Se utiliza principalmente en el lado del cliente, ejecutado en un intérprete incluido en el navegador web, permitiendo mejoras en la interfaz de usuario y páginas web dinámicas, aunque también se utiliza en muchos entornos sin navegador como node.js [21], entre otros.

JavaScript se utiliza en todo el sistema de voto para otorgar interactividad a los distintos portales web y para validar formularios antes de ser enviados al servidor, entre otras cosas. Pero donde más importancia cobra JS es en el generador del voto, pues el voto se genera completamente en el lado del cliente, utilizando exclusivamente este lenguaje para ello.

6.6. MySQL

MySQL [22] es un Sistema de Gestión de Bases de Datos (SGBD) relacional desarrollado por Oracle Corporation bajo licencia dual GPL/Licencia comercial y está considerada como la base datos *open source* más popular del mundo, y una de las más populares en general junto a Oracle y Microsoft SQL Server.

La gratuidad del software (la versión *Community*), su facilidad de uso y configuración, así como la experiencia previa con este SGBD han sido los causantes de la elección de MySQL como base de datos para el sistema de voto.

6.7. OpenSSL

OpenSSL [23] es un proyecto de software libre consistente en un paquete de herramientas para SSL, así como una librería de criptografía de propósito general.

Estas librerías se han utilizado para generar los pares de claves RSA de las mesas de identificación y de voto, siendo ambos pares de claves de 1024 bits y en formato PEM.

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8qH5/reiHfx6JnUnXSM8Lls83
tswXXlMmyKR2sMt9VeKUdDJ7v5opmsKCDLLg8hvC/0PVhb6GwKJp/4nbA2bBrssu
35PlPTkanY6ifT3t4Hdd1B6BsF3ubIt8EctKgPW/LcZxoAKYhF9sBOjyVs8xzOer
xWU08pESjqoCLvBGFwIDAQAB
-----END PUBLIC KEY-----
```

Tabla 2 - Clave Pública RSA de la MI codificada en PEM

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCwUJrlriG9W7IzXvxAYdgP3Pkq
nEPiCFJjS9KyMsyUI+g5cZ26/+JhxFvztrRXuULxy89An25/nlvYmeLKBnsptD90
9HdSvwDctYQiyJVJECDCb5FyjtL3WzK4Gkct70SrX9+OYZAFE6tctyZYr/puQem9
a6CBIIyHYGT382bYtwIDAQAB
-----END PUBLIC KEY-----
```

Tabla 3 - Clave pública RSA de la MV codificada en PEM

6.8. Librerías adicionales

6.8.1. jsSHA

jsSHA [24] es una librería que permite la generación de distintos *hashes* SHA (SHA-1, SHA-256, SHA-512…) en JavaScript.

Esta librería es utilizada en el generador de voto, ya que el protocolo diseñado requiere generar un SHA-256 en el lado del cliente, para lo que se ha recurrido a JavaScript.

6.8.2. jQuery

jQuery [25] es una de las librerías más populares de JavaScript. Permite simplificar la interacción con HTML, la manipulación de su estructura, así como la gestión de eventos, entre otros aspectos.

Se ha hecho uso de esta librería en la web del escrutinio, con el fin de filtrar las máscaras de la tabla de manera dinámica y en tiempo real.

6.8.3. Bouncy Castle

Bouncy Castle [15] es una colección de librerías utilizadas para criptografía. Están disponibles tanto para Java como para C#.

Estas librerías se han utilizado para los procesos de firmado del voto y verificación del comprobante de máscara repetida de la MV en la MI, así como para la verificación del voto y la firma del comprobante en la MV. También se ha hecho uso de ellas en la aplicación de escritorio que permite verificar el voto antes de emitirlo.

7. Conclusiones y trabajo futuro

7.1. Conclusiones

7.1.1. Resultados del proyecto

Diseñar e implementar un sistema de voto electrónico no es una tarea fácil, ya que cuando se trata de temas de seguridad, privacidad, cifrado, etc., nunca se tiene la certeza de que el sistema sea infalible. Aun así, se ha logrado la consecución de todos los objetivos propuestos al inicio del proyecto. Incluso el apartado en el que menos hincapié se ha previsto desde los objetivos, el de las comunicaciones seguras, se ha implementado garantizado un mínimo nivel de seguridad mediante el protocolo HTTPS. Por lo tanto, teniendo en cuenta que tan sólo se trata de un prototipo que no va a ser implantado de manera profesional hasta ser revisado varias veces, se puede considerar que el proyecto ha sido concluido con éxito.

7.1.2. Aprendizaje

El voto electrónico ha resultado ser increíblemente interesante, especialmente el voto a través de internet. El cual, con una buena implementación, algo que se ha intentado (y conseguido, se espera) puede abrir muchas puertas a nivel técnico para facilitar el desarrollo de unas elecciones, además de permitir un gran ahorro económico y logístico para el Estado y una mayor comodidad para los electores.

La fase de documentación del proyecto ha permitido valorar y ver desde un punto de vista más crítico los sistemas de voto – tanto tradicionales como electrónicos – existentes hasta la fecha: cuáles son sus ventajas y desventajas, las características que ha de tener un buen sistema de voto, etc.

El diseño e implementación han permitido conocer más en profundidad sistemas criptográficos como RSA, SHA, firma digital, etc. No sólo sobre el papel, donde se habían estudiado durante el grado, sino que también ha permitido su utilización durante el proceso de implementación del sistema de voto.

Pero no sólo eso, también ha permitido la adquisición de experiencia con herramientas ya conocidas y utilizadas anteriormente, como Tomcat, del que se han descubierto muchos aspectos de su configuración que se desconocían: uso de HTTPS sobre este, securización del sistema, entre otros.

También ha permitido la interacción de distintos tipos de software en una misma implementación, cosa que rara vez se ha visto en el grado y que es de agradecer, pues los desarrollos profesionales rara vez utilizan una única tecnología para su implementación.

Por último, la que se considera la aportación más importante del proyecto: ha permitido la realización una buena labor de investigación, una buena documentación y la elaboración de una memoria a la altura de la implementación. Pues si bien la memoria no forma parte de la implementación del sistema de voto electrónico en sí, es la parte más importante de este, pues detalla todos sus pormenores, invisibles en la implementación.

7.2. Trabajo futuro

A pesar de la consecución de todos los objetivos marcados al inicio del proyecto, es cierto que algunos de estos se han implementado a nivel de prototipo, sin ahondar demasiado en ellos.

Claro ejemplo es el de la implementación de las comunicaciones seguras mencionado anteriormente, que si bien cumple unos mínimos, por motivos de prioridades no se le ha dedicado toda la atención que este apartado merece.

Por lo tanto, se marca como pendiente la implementación de unas comunicaciones seguras en el sistema de voto electrónico, asunto en el que se ahondará en un futuro, investigando diferentes alternativas a HTTPS, así como en caso de mantenerse este protocolo, obteniendo un certificado firmado por una CA que proporcione garantías al usuario.

La implementación del sistema de voto llevada a cabo en este proyecto puede considerarse el armazón de un sistema de voto electrónico por internet. Una base sólida sobre la que poder seguir trabajando y añadir nuevas funcionalidades. Algunas de estas posibles mejoras serían:

- Mejora de la interfaz: si bien es cierto que los portales web diseñados cumplen su función tal y como están, un HTML plano no es la mejor forma de presentar el sistema de votación al público. Un proyecto futuro podría ser mejorar la capa de presentación del sistema, utilizando para ello HTML5, CSS y JavaScript, con librerías como jQuery.
- Mejora de la seguridad del sistema: aparte de la mejora de la seguridad en las comunicaciones, de la que ya se ha hablado antes, un buen proyecto para el futuro sería la securización del sistema en sí. Buscando y arreglando brechas de seguridad, bastionando el servidor, utilizando medidas contra ataques de denegación de servicio, etc. En definitiva, asegurar el buen funcionamiento e impenetrabilidad del sistema en caso de una implantación real del sistema de voto electrónico.
- Expansión del sistema de voto a distintos sistemas de escritorio y móviles: el sistema implementado en este proyecto está diseñado para funcionar en Firefox, Chrome y Opera sobre sistemas de escritorio (Windows y OSX/UNIX). Un buen proyecto futuro podría ser ampliar los navegadores compatibles, como Microsoft Edge (Internet Explorer ya está de capa caída) o Safari, ambos los exploradores por defecto de Windows y OSX, respectivamente. Así como el desarrollo de aplicaciones móviles que lleven el sistema de voto electrónico a Android e iOS, pues la posibilidad de votar desde el *smartphone* es algo que los electores podrían valorar positivamente.

8. Bibliografía

[1] Ministerio de la Presidencia, *BOE-A-2016-4393,* 2016.

[2] Ministerio de la Presidencia, *BOE-A-1985-11672,* 1985.

[3] C. Karlof, N. Sastry y D. Wagner, «Cryptographic Voting Protocols: A Systems Perspective» USENIX, 2005.

[4] I. Ray, I. Ray y N. Narasimhamurthi, «An Anonymous Electronic Voting Protocol for Voting Over The Internet».

[5] International Institute for Democracy and Electoral Assistance (IDEA) Internacional, «Una introducción al voto electrónico: Consideraciones esenciales» Estocolmo, 2011.

[6] Proyecto ACE, «Sistemas de votación electrónicos - Sistemas de escáner óptico» [En línea]. Disponible: http://aceproject.org/ace-es/topics/et/eth/eth02/eth02b/eth02b2. [Último acceso: Mayo 2016].

[7] A. J. Menezes, S. A. Vanstone y P. C. v. O. Oorschot, Handbook of applied criptography, CRC Press, 1997.

[8] National Institute of Standards and Technology, *Secure Hash Standard (SHS) (FIPS PUB 180-4),* Gaithersburg, 2015.

[9] P. Bakker, «ASN.1 key structures in DER and PEM» ARM Limited, 14 Abril 2014. [En línea]. Disponible: https://tls.mbed.org/kb/cryptography/asn1-key-structures-in-der-and-pem. [Último acceso: Junio 2016].

[10] X. Perramon, «Mecanismos de protección» Fundación para la Universitat Oberta de Catalunya.

[11] T. Dierks y C. Allen, *The TLS Protocol (RFC 2246),* The Internet Society, 1999.

[12] A. Schiffman y E. Rescorla, *The Secure HyperText Transfer Protocol (RFC 2660),* The Internet Society, 1999.

[13] E. Rescorla, *HTTP Over TLS (RFC 2818),* The Internet Society, 2000.

[14] Google Inc., «Verificación en dos pasos» [En línea]. Disponible: https://www.google.es/landing/2step/. [Último acceso: Junio 2016].

[15] Legion of the Bouncy Castle Inc., «Bouncy Castle 1.54 Release Notes» 29 Diciembre 2015. [En línea]. Disponible: https://www.bouncycastle.org/releasenotes.html. [Último acceso: Junio 2016].

[16] The CentOS Project, «CentOS 7 (1511) Release Notes,» 19 Febrero 2016. [En línea]. Disponible: https://wiki.centos.org/Manuals/ReleaseNotes/CentOS7.

[17] C. S. W. y R. Mordani, *Java Servlet Specification 3.1,* Oracle Corporation, 2013.

[18] K.-m. Chung, *JavaServer Pages Specification 2.3,* Oracle Corporation, 2013.

[19] Oracle Corporation, «Java JDK 8u91 Release Notes» 2016. [En línea]. Disponible: http://www.oracle.com/technetwork/java/javase/8u91-relnotes-2949462.html.

[20] Mozilla Developer Network, «JavaScript» Mozilla Foundation, 12 Mayo 2016. [En línea]. Disponible: https://developer.mozilla.org/es/docs/Web/JavaScript. [Último acceso: Junio 2016].

[21] Node.js Foundation, «Node.js» [En línea]. Disponible: https://nodejs.org/. [Último acceso: Junio 2016].

[22] Oracle Corporation, «MySQL 5.7.12 Release Notes» 11 Abril 2016. [En línea]. Disponible: http://dev.mysql.com/doc/relnotes/mysql/5.7/en/news-5-7-12.html. [Último acceso: Junio 2016].

[23] OpenSSL Software Foundation, «OpenSSL 1.0.2 Changelog» 3 Mayo 2016. [En línea]. Disponible: https://www.openssl.org/news/changelog.html. [Último acceso: Junio 2016].

[24] B. Turek, «jsSHA» 13 Mayo 2016. [En línea]. Disponible: https://caligatio.github.io/jsSHA/. [Último acceso: Junio 2016].

[25] The jQuery Foundation, «jQuery 1.12.4 Changelog» 20 Mayo 2016. [En línea]. Disponible: https://blog.jquery.com/2016/05/20/jquery-1-12-4-and-2-2-4-released/. [Último acceso: Junio 2016].

[26] W. Quirós Ramirez y E. J. Salazar Zeledón, «Comprensión de protocolos de red desde una perspectiva de programación».