Protocolo para voto electrónico.

Lázaro A. Escudero Ferrer.

17 de enero de 2002

Protocolo para voto electrónico.

1 Alta del usuario votante.

El usuario debe ir a la base de datos (que denotaremos **BD**), que puede ser la delegación de hacienda, o mejor aún, los ayuntamientos. En esta base de datos, **BD**, el usuario se acredita con su DNI y entrega un formulario, **F**, debidamente cumplimentado con las respuestas y datos pertinentes para la identificación del votante, es decir, se acredita como persona con derecha a votar. En la **BD** se generan las claves de cifrado y descifrado del usuario, es decir, se generan, en ese mismo momento y de forma aleatoria, los números p, q, e y d necesarios para el criptosistema RSA. Hacemos $n = p*q$ y $CuPri = (n, d)$, **Cu**=$CuPub = (n, e)$. Que en mi opinión no deberían de ser inferiores a 1024 bits.

En la **BD** se guarda el formulario, **F**, cifrado con $CuPri$, lo denotamos por **C(F)**. Se le adjunta al usuario el formulario, **F**, rellenado con las claves pública y privada, escritas y ocultas de los ojos de los funcionarios, también se le adjunta un disquete con el formulario **F**, las claves pública y privada y un programa **E** que es como un navegador sencillo, sólo acepta el lenguaje HTML y FTP tanto de subida como de bajada de una dirección de Internet determinada. Con este programa **E** se rellena el voto, se manda el paquete **P**, se recibe el paquete **P"'** y se consulta la lista de votaciones, además se pueden bajar formularios para otras votaciones y para la declaración de la renta, etc.

En este disquete también se adjuntan las claves públicas **C1** de **BD** y **C2** del centro de recuento de votos que denotaremos por **CR**. Estas claves deben de ser como mínimo de 2048 bits.

En la base de datos, **BD**, se borra todo rastro de las claves generadas y de los datos en claro del usuario, solo queda **C(F)**.

2 Primeras Observaciones.

Bien, ya tenemos un usuario que puede votar por Internet. También hemos conseguido que en **BD** estén los datos del usuario y de forma confidencial, nadie puede leer esos datos, pues están cifrados con la clave privada del usuario y la pública todavía no está disponible. Esta situación es más favorable que tener los datos en claro pues cualquier intruso, incluidos los funcionarios, podría leerlos y tendría más fácil la suplantación de personalidad. También hemos conseguido que se utilice software seguro cuyo código fuente debe estar disponible para que todos los usuarios puedan analizar el código de ese programa. No creo que haga falta decir que estos programa deben estar disponibles para todas las plataformas existentes. También debe estar disponible el código fuente del programa que genera las claves de usuario.

3 Como se vota.

Se ejecuta el programa **E**, se conecta a Internet, y se baja la lista de partidos políticos a votar (o la declaración de la renta en su caso) si el usuario lo desea puede desconectarse de Internet y trabajar offline, cuando se está dispuesto a votar, se conecta a Internet y el programa **E** se conecta con **CR** y pone en hora el reloj del sistema del usuario, en la web del **CR** se ofrece la

hora exacta. Esta hora servirá de referencia para una posterior comprobación de la votación.

El programa **E** genera un número de referencia, **nº Ref**, dependiendo de la comunidad autónoma o la provincia en la que esté situado el usuario, no aconsejo que dependa del municipio pues hay municipios muy pequeños y no todos los votantes están dispuestos a votar por Internet. Este número de referencia, **nº Ref**, debe de ser de unas 15 cifras aleatorias aparte de la identificación de la comunidad.

Recordemos que el formulario, **F**, contiene todos los datos personales necesarios para votar.

3.1 Trabajo del usuario.

El programa **E** cifra con **C1** el formulario **F**:

$$\mathbf{D}=C_1(\mathbf{F})$$

Se vota, es decir, se selecciona de una lista el partido político al que se desea votar y además para evitar confusiones se escribe el partido político votado con todas sus letras. **E** cifra este voto y **nº Ref** con la clave **C2**:

$$\mathbf{V}=C_2(\mathbf{n^o\ Ref}+\text{Voto}),\ \text{o en su caso,}\ \mathbf{V}=C_2(\mathbf{n^o\ Ref}+\text{Renta})$$

Se usa el algoritmo H=MD5 como función resumen para firmar digitalmente.

Denotamos por **M** la concatenación de **Cu**, **D** y **V**:

$$\mathbf{M}=\boxed{\begin{array}{c}\mathbf{Cu}\\ \mathbf{D}\\ \mathbf{V}\end{array}}$$

$$\mathbf{R}=F_u(\mathrm{H}(\mathbf{M}))$$

Donde F_u es el cifrado con la clave privada del usuario para garantizar la autenticidad, **R** contiene certificado de integridad y autenticidad.

$$\mathbf{M}+\mathbf{R}=\boxed{\begin{array}{c}\boxed{\begin{array}{c}\mathbf{Cu}\\ \mathbf{D}\\ \mathbf{V}\end{array}}\\ \boxed{R}\end{array}}$$

Se cifra con la clave **C1** el mensaje **M** (unión del **Cu**, $\mathbf{D}=C_1(\mathbf{F})$, $\mathbf{V}=C_2(\mathbf{n^o\ Ref}+\text{Voto})$) y el resumen $\mathbf{R}=F_u(\mathrm{H}(\mathbf{M}))$ y se crea el paquete **P**:

$$\mathbf{P}=C_1(\mathbf{M}+\mathbf{R})$$

Este paquete, **P**, contiene los datos personales del usuario solo legibles por la **BD**, el voto solo legible por **CR** y certificado de integridad y autenticidad.

El programa **E** manda el paquete **P** a **BD**.

3.2 Trabajo de BD.

Recibe **P**.

Descifra **P**, pues él tiene la clave privada de **C1**.

Comprueba que efectivamente **R**=F_u(H(**M**)), ésto se puede hacer pues **Cu** se manda con **M**; si es buena, entonces hay integridad en los datos.(✠[1])

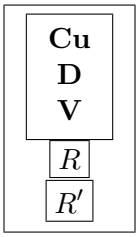
Ahora, descifra **D** y recupera **F**, se va a la base de datos y descifra **C(F)** con **Cu** y comprueba que **F**=$D_u(C_u(\mathbf{F}))$, si es buena y no hay copia de **P**, el usuario tiene derecho a votar.(✠[2])

Hace **R'**=F_1(H(**M**+**R**)), la firma digital de **M**+**R**, cifra **M**+**R**+**R'** con la clave **C2**:

$$\mathbf{P'}=C_2(\mathbf{M}+\mathbf{R}+\mathbf{R'})$$

BD guarda copia de **P** y si hay otro intento de voto es rechazado, en este caso, y si el usuario quiere justificante de por qué se ha rechazado se le manda una copia de **P** que más tarde puede ser analizada.

Manda **P'** a **CR**.

P' = 

3.3 Trabajo de CR.

Recibe y descifra **P'**.

Comprueba que efectivamente **R'**=F_1(H(**M**+**R**)), si es buena, el usuario tiene derecho a votar.(✠[3])

Comprueba que efectivamente **R**=F_u(H(**M**)), si es buena, el voto es el del usuario.(✠[4])

Descifra **V** y lo añade al contador del partido político que se votó.

CR publica en la lista de votaciones.

nºRef + Voto + hora.

Hace **R"**=F_2(H(**M**+**R**+**R'**)), la firma digital de **M**+**R**+**R'**.

Cifra con clave **C1**, **M**+**R**+**R'**+**R"**:

$$\mathbf{P"}=C_1(\mathbf{M}+\mathbf{R}+\mathbf{R'}+\mathbf{R"})$$

Y lo manda a **BD**.

$$\mathbf{P''} = \boxed{\boxed{\begin{array}{c}\mathbf{Cu}\\ \mathbf{D}\\ \mathbf{V}\end{array}}\ \boxed{R}\ \boxed{R'}\ \boxed{R''}}$$

3.4 Trabajo de BD.

Recibe y descifra **P"**.

Comprueba que efectivamente **R"**=F_2(H(**M**+**R**+**R'**)), si es buena, descifra **D** y publica una lista con el DNI del usuario y diciendo que ha votado por Internet y la hora de la votación.(✠[5])

BD guarda copia de **P"** y si hay otro intento de voto es rechazado, en este caso, si el usuario quiere justificante de por qué se ha rechazado se le manda una copia de **P"** que más tarde puede ser analizada.

Hace **R"'**=F_1(H(**M**+**R**+**R'**+**R"**))

Cifra con clave **Cu**, **M**+**R**+**R'**+**R"**+**R"'**:

$$\mathbf{P"'}=C_u(\mathbf{M}+\mathbf{R}+\mathbf{R'}+\mathbf{R"}+\mathbf{R"'})$$

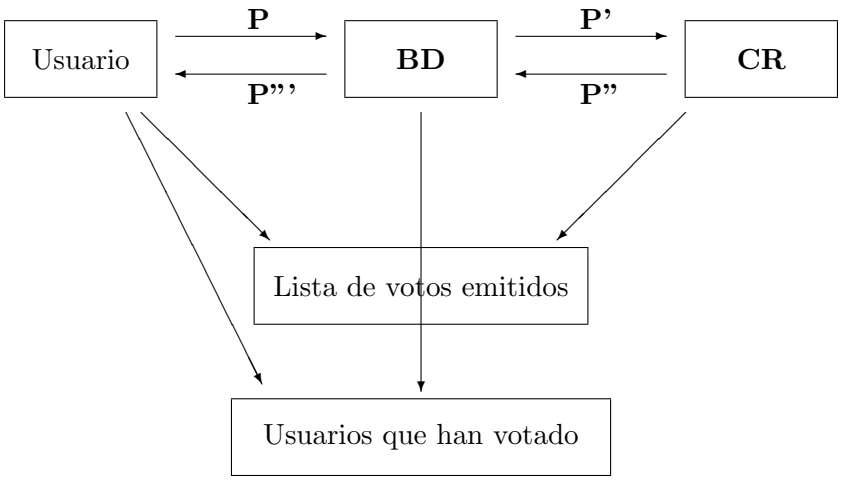
Y lo manda al usuario.

$$\mathbf{P"'} = \boxed{\boxed{\begin{array}{c}\mathbf{Cu}\\ \mathbf{D}\\ \mathbf{V}\end{array}}\ \boxed{R}\ \boxed{R'}\ \boxed{R''}\ \boxed{R'''}}$$

3.5 Trabajo del usuario.

Cuando el usuario recibe **P"'** puede comprobar cada una de las firmas digitales **R***, puede comprobar en la lista publicada por **CR** su número de referencia, **nº Ref**, el voto y la hora de la votación y puede guardar **P** y **P"'** como justificante en caso de error. También puede comprobar la lista publicada por **BD** y cerciorarse que ha votado, aunque sólo sea a título de curiosidad.

4 Esquema de la comunicación.



5 Observaciones:

- Todo este trasiego de mensajes no debe demorarse mucho para que el usuario no esté mucho tiempo conectado a la red.

- **BD** y **CR** deben de ser entidades distintas y separadas para no tener información la una de la otra y no poder hacer corresponder el voto emitido con el usuario.

- Démonos cuenta que la **BD** nunca tiene información sobre el partido político al que votó el usuario y que **CR** nunca tiene información sobre quien es el usuario.

- Si se desea realizar el voto electrónico antes del día de las elecciones, entonces no se debe publicar el partido político al que se votó, pues ésto daría información indeseada antes del día de las elecciones; por ello propongo que en lugar de que **CR** publique **nºRef + Voto + hora**, debe publicar **nºRef + CodigoVoto + hora**, donde **CodigoVoto** es eso, un codigo que el usuario y **CR** pueden identificar como su voto pero que no da información sobre el voto a ojos que no tengan la clave para recuperar ese voto a partir de **CodigoVoto**.

6 Caso especiales.

6.1 (✠[1]):

Si **BD** encuentra algún error a la hora de comprobar que $\mathbf{R}=F_u(\mathrm{H}(\mathbf{M}))$, debe mandar un correo al usuario diciendo que tiene problemas a la hora de comprobar su autenticidad y que el voto no se tendrá en cuenta, que lo intente de nuevo o vote de forma normal.

6.2 (✠[2]):

Si **BD** encuentra algún error a la hora de comprobar que **F**=$D_u(C_u(\mathbf{F}))$, debe mandar una carta al usuario diciendo que tiene problemas a la hora de comprobar su ficha en la base de datos, que lo intente de nuevo o vote de forma normal.

Si **BD** tiene copia de **P**, debe mandar una carta al usuario, adjuntando **P** y diciendo que su votación está en curso, pero que si no está en deacuerdo con esta conclusión que reclame posteriormente mostrando **P**.

6.3 (✠[3]):

(Esto en muy difícil que suceda.)

Si **CR** encuentra algún error a la hora de comprobar que **R'**=F_1(H(**M**+**R**)) debe devolver la carta a la **BD** y si después de varios intentos sigue sin ser correcta la comprobación, se debe mandar una carta al usuario diciendo que su voto no se tendrá encuenta y que debe votar de forma normal.

6.4 (✠[4]):

Análogo a (✠[1]).

6.5 (✠[5]):

(Esto en muy difícil que suceda.)

Si **BD** encuentra algún error a la hora de comprobar que **R"**=F_2H(**M**+**R**+**R'**) debe mandar una carta a **CR** diciendo que vuelva a firma y enviar esta carta. Si el problema persiste, **CR** debe comprobar si la hora sigue siendo válida y si el número de referencia, **nº Ref**, está en las listas como votante que ya ha votado.

Si el usuario ya ha votado seguro que se puede firmar y enviar la carta a **BD** sin ningún problema. Pero si el usuario no ha votado, es decir, si el **nº Ref** no aparece en las listas, entonces se le manda una carta a **BD** diciendo que este usuario no ha votado y la base de datos debe comprobar si tiene copia de **P** y en ese caso volver a enviarla a **CR** y seguir de forma normal, y en caso de que no tenga copia de **P** sin duda ha sido una intrusión, se guarda la información del mensaje para su posterior estudio y por lo demás se ignora este mensaje.

.

****

Autor: Lázaro A. Escudero Ferrer
Correo electrónico: lazaro@tierradelazaro.com
Dirección URL: http://www.tierradelazaro.com

****