Equip
d'Estudis
Electorals

ELECCIONS A RECTOR
UNIVERSITAT AUTÒNOMA DE BARCELONA
7 MARÇ 2002

AVALUACIÓ DE LA PROVA PILOT DE VOTACIÓ ELECTRÒNICA

Equip d'Estudis Electorals

ÍNDEX

Equip d'Estudis Electorals

PRESENTACIÓ

L'informe que teniu a les mans pretén avaluar l'experiència que va tenir lloc a la Universitat Autònoma de Barcelona el 7 de març de 2002. Amb motiu de les Eleccions a Rector d'aquesta universitat, es va convidar als Professors/es Funcionaris Doctors de la Facultat de Ciències Polítiques i Sociologia a participar en una prova pilot de votació electrònica remota. Aquesta va ser conduïda per l'empresa Scytl, especialista en processos electorals realitzats amb mitjans electrònics, en col·laboració amb l'Equip d'Estudis Electorals, que treballa, entre altres, en qüestions relacionades amb les implicacions socials i polítiques del vot electrònic, i la Secretaria General de la UAB.

Tot seguit presentem els resultats d'aquesta avaluació. En primer lloc, exposarem breument el què significa i implica el vot electrònic a l'actualitat. Aquest apartat ajudarà a aquells lectors que abordin el tema per primera vegada.

A continuació presentarem una descripció del desenvolupament de l'experiència. Tractarem de mostrar com funciona tècnicament l'adaptació del sistema ideat per Scytl per a la prova pilot de la UAB (tenint en compte les limitacions de temps i recursos imposades). A partir d'aquí, avaluarem la prova pilot des de dues grans vessants: els aspectes tècnics i les qüestions directament relacionades amb els electors (com per exemple, la participació electoral).

Per a la realització d'aquesta avaluació hem comptat amb les opinions d'alguns dels professors/es que formaven part del cens electoral per a la prova pilot. Concretament, hem disposat de dues fonts. Per una banda, i com veurem en l'explicació sobre el procediment de la votació *on-line*, al final d'aquesta se li demanava al votant que contestés a una enquesta. Un total de 5 professors van accedir-hi i hem pogut comptar amb les seves respostes.

Malgrat això, donat el caràcter limitat d'aquestes dades, dies després de l'elecció vam mantenir una sèrie d'entrevistes amb alguns dels professors/es per tal de conèixer les seves opinions d'una forma més completa. A més a més, amb la intenció d'obtenir una representació de tots els possibles punts de vista, vam conversar amb electors que van participar a la prova pilot, però també amb altres que van admetre no haver-ho fet.

Pretenem doncs mostrar aquest ventall d'opinions al voltant del desenvolupament de la prova pilot: en el cas dels professors que van participar, van poder-ho fer sense dificultats? Quins defectes i/o avantatges hi van trobar? I pel què fa als professors que no van participar: quin en va ser el motiu? Estava directament relacionat amb el funcionament de la pròpia prova? El segon gran apartat ("Avaluació de l'Experiència") tractarà de donar resposta a aquestes i altres preguntes.

Finalment, la nostra conclusió exposarà algunes reflexions i recomanacions en relació a la implementació de mecanismes de vot electrònic a partir de l'avaluació d'aquesta experiència.

Equip d'Estudis Electorals

PREÀMBUL: QUÈ ÉS I QUÈ IMPLICA EL "VOT ELECTRÒNIC"?

Des d'una aproximació global, l'expressió "vot electrònic" comprèn tots aquells mecanismes que utilitzen alguna forma de tecnologia per a dur a terme l'acció de votar. Es tracta per tant d'un ampli ventall de mecanismes que poden prendre formes diverses en funció d'aquests dos elements:

➔ La utilització d'aparells electrònics pot afectar els diferents moments que conformen l'acció de votar:

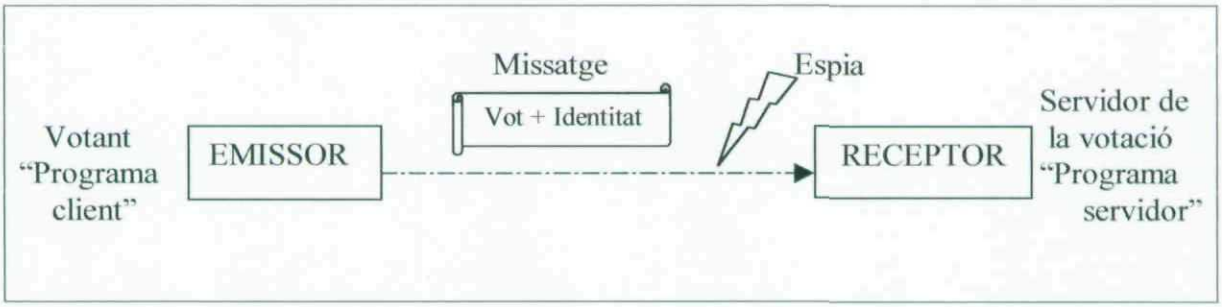
- *Identificació, autenticació i validació del votant.*
- *Establiment de les preferències del votant respecte de les opcions que se li plantegen.*
- *Emissió del vot.*
- *Recompte de vots.*
- *Verificació (si s'escau).*

➔ Existeixen diverses formes de tecnologia aplicables a aquests estadis de les votacions:

- *Sistema de tarja perforada*: aquest sistema incorpora una tarja, un aparell per perforar les targes i un aparell tabulador que identifica les marques de les targes i compta el nombre de vots destinats a cada opció. Els votants només han d'introduir la tarja al primer aparell i perforar l'espai reservat per al candidat o per la opció que volen triar. Llavors l'introdueixen a l'aparell tabulador que anirà fent un recompte. En alguns casos, en lloc d'un aparell tabulador hi ha una urna tradicional que serà traslladada a una oficina central de recompte.
- *Sistemes de votació amb aparell lector (escàner òptic)*: el primer en desenvolupar-se va ser l'anomenat "*Optical Mark Reading*" (OMR). Aquest dispositiu reconeix les marques ja no perforades, sinó escrites a una papereta: per exemple una creu a una casella. Desenvolupaments posteriors permeten reconèixer, ja no només creus, sinó fins i tot números o lletres (sistema OCR: "*Optical Character Recognition*" o el més recent ICR: "*Intelligent Character Recognition*").

- *Sistema d'Enregistrament Directe (DRE)*: els votants marquen les seves opcions directament a un aparell electrònic, per exemple, amb una pantalla tàctil o una pantalla i un teclat. Les dades de la votació queden enregistrades a un disc dur, disquet, "smartcard",... i poden ser transmeses a un ordinador central a través d'aquests o d'una xarxa (interna o externa en el cas d'Internet).

Precisament, el darrer graó en el desenvolupament tecnològic de mecanismes de votació electrònica és el que no suposa un desplaçament del votant fins al col·legi electoral. Aquest emet el seu vot des de qualsevol ordinador connectat a la xarxa (Internet), enviant-lo a un servidor. La transmissió del vot ha de realitzar-se de forma segura per evitar possibles atacs (d'un possible "espia"). Actualment, la criptografia estudia els mètodes que es poden utilitzar en la transmissió de dades via Internet mitjançant el xifratge (amb els anomenats protocols i esquemes de votació). El següent croquis mostra la base dels esquemes de votació electrònica remota:



En el disseny de qualsevol esquema d'aquest tipus són indispensables una sèrie de requeriments per tal de permetre'n una implementació amb totes les garanties. I és que una votació és una transmissió de dades que requereix una cura especial en les qüestions relacionades amb la seguretat. A més a més, s'ha de tenir en compte un disseny de l'esquema pensant en la seva utilització per part de votants sense aptituds específiques en aquest camp. Precisament, són molts els autors que han definit els requeriments que qualsevol esquema hauria de ser capaç de garantir.

Normalment, tot i que pot variar-ne la ordenació o la denominació, existeix força consens en les diferents propostes[1]:

Discriminació	Només podran votar les persones prèviament autoritzades i només podran emetre un sol vot.
Privacitat	Secret de vot i anonimat del votant: no s'ha de poder relacionar el contingut del vot amb la identitat del votant.
Precisió/exactitud	S'han d'incloure en el recompte única i absolutament tots els vots autoritzats i vàlidament emesos sense que pateixin cap tipus d'alteració.
Imparcialitat	Ningú no ha de poder conèixer resultats parcials de la votació abans del final d'aquesta.
Possibilitat de verificació	Verificació universal: verificació del conjunt de resultats. Verificació individual: el votant ha de poder verificar que el seu vot en concret ha estat tingut en compte a l'hora de fer el recompte[2].
Comoditat/agilitat	Ha de resultar còmode per al votant seguir les passes per emetre el seu vot. S'ha de poder realitzar l'emissió del vot en una sola sessió i en un temps no excessiu.
Flexibilitat	S'ha de preveure la possibilitat d'incloure una gran varietat d'opcions a triar pel votant. S'ha de preveure la possibilitat de celebrar eleccions simultànies.
Mobilitat	El votant hauria de poder triar lliurement el punt de la xarxa des del qual vol emetre el seu vot.

[1] D'entre les diverses propostes existents hem triat les següents obres per extreure'n un únic llistat:
- BORRELL, Estudi i Desenvolupament d'un Esquema Criptogràfic per Realitzar Votacions Segures sobre una Xarxa Local, tesi doctoral, UAB, 1996.
- CRANOR i CYTRON, "SENSUS: a Security-Conscious Electronic Polling System for the Internet", Informe presentat a la International Conference on System Sciences, 1997, Estats Units, disponible a www.lorrie.cranor.org..
- RIERA, Design and Implementable Solutions for a Large Scale Electronic Voting Schemes, tesi doctoral, UAB, 1999.

[2] Aquesta possibilitat, que no es dóna en les votacions convencionals, és sovint contestada donat que es contradiu amb requeriments com el de privacitat i pot portar a pràctiques com la compra-venda de vots o la coerció.

De forma general, els requeriments relacionats amb aspectes de seguretat han de solucionar-se per mitjà de mecanismes tècnics. També per aquesta via es poden resoldre aspectes relacionats amb la conveniència del sistema de cara al votant: requeriments de *Comoditat/Agilitat*, *Flexibilitat* i *Mobilitat*.

No obstant, existeixen certs reptes propis de qualsevol sistema de vot electrònic on esdevenen clau els factors social i polític. Com ja hem mencionat, els votants no tenen perquè reunir unes aptituds específiques.

Precisament, tot i que les noves tecnologies s'han desenvolupat a un ritme molt ràpid, la possibilitat de gaudir d'alguns dels seus components, com és el cas d'Internet, requereix a banda de recursos econòmics, un grau de coneixements bàsic. L'accés a la tecnologia és per tant desigual, és a dir que alguns segments de la població en poden quedar exclosos en funció de característiques com els nivells de renda o d'educació, o l'edat: "Socially disadvantaged groups (with less economical resources and a lower level of education) as well as older people are the slowest to take up new technologies if at all"[3].

De fet, s'argumenta sovint que l'arribada d'aquestes tecnologies a tots els ciutadans és lenta però progressiva. Sigui com sigui, en el moment present es pot parlar d'una veritable divisió entre aquells que hi tenen accés i aquells que no: és l'anomenada divisió digital.

En relació amb les votacions electròniques, aquesta realitat implica que alguns ciutadans tindrien més facilitat que d'altres a l'hora d'utilitzar qualsevol mecanisme electrònic per emetre el seu vot. Les conseqüències més directes en aquest sentit podrien passar per un augment de l'abstenció entre els segments més afectats.

De forma general, i acceptant de forma consensuada les recomanacions d'un informe presentat per la California Internet Voting Task Force, els experts coincideixen en què els sistemes de votació electrònica han d'implementar-se gradualment, partint des de les seves formes més bàsiques per tal d'assolir la confiança necessària i garantir-ne la utilització per part dels electors[4].

---

[3] SÁNCHEZ, J. i TORRAS, L., "Internet Voting: Socio-Political Considerations", paper nº19, disponible a www.democraciaweb.org.

[4] CALIFORNIA INTERNET VOTING TASK FORCE, "A Report on the Feasibility of Internet Voting", 2000, disponible a www.ss.ca.gov/executive/ivote.html.

No obstant, si realment existeixen tantes dificultats i tants riscos, la pregunta que se'ns planteja inevitablement és: quin és l'objectiu principal de qualsevol sistema de votació electrònica?

La resposta ens porta sense dubte a alguna forma de facilitació de l'acció de votar, encara que es redueixi a realitzar un recompte més ràpid i menys costós. Però en qualsevol dels casos, no s'ha de facilitar un aspecte en detriment de qualsevol altre: per exemple, no per evitar el desplaçament del votant vulnerarem el seu anonimat. I per suposat, no s'ha de beneficiar a uns electors en detriment d'uns altres, com podria ser la conseqüència de la divisió digital.

El vot electrònic, i més especialment el vot per Internet, s'ha presentat sovint com el gran remei a alguns dels mals de l'acte de votació i de les eleccions per generalització. No obstant, cal saber realitzar un balanç raonable dels seus beneficis i inconvenients.

LA PROVA PILOT REALITZADA A LA UAB:

Elecció:	Eleccions al Rector/a de la Universitat Autònoma de Barcelona.
Data:	Dijous, 7 març 2002. Entre 9h00 i 18h00.
Lloc:	Facultat de Ciències Polítiques i Socials.
Cens:	Professors/es Funcionaris Doctors. Total: 48 electors.
Organització:	Scytl, Equip d'Estudis Electorals (EEE), UAB.
Implementació tècnica:	Scytl.
Avaluació:	EEE, Fundació Jaume Bofill.

EL PROCEDIMENT DE LA VOTACIÓ.

Un cop obert el procés electoral, el votant havia de seguir les següents passes per emetre el seu vot[5]:

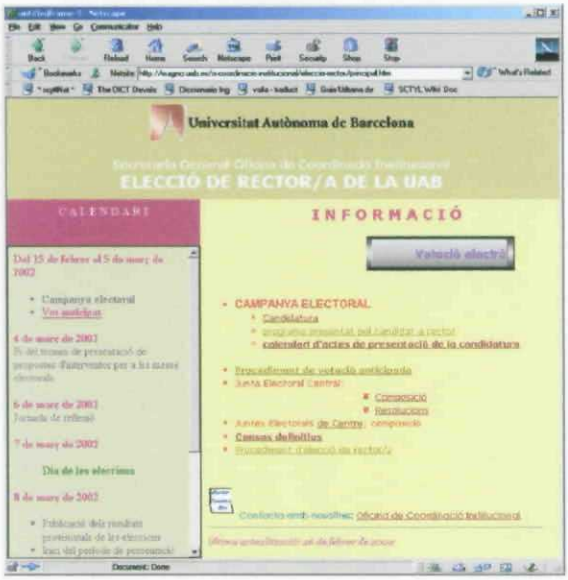
① El votant havia d'instal·lar amb un mínim d'antelació el seu Certificat Digital seguint les instruccions que se li havien lliurat[6]. (Una còpia de les instruccions amb l'explicació detallada per a la instal·lació es troba a l'annex I).

② Es connectava a la pàgina web oficial de les Eleccions al Rector:

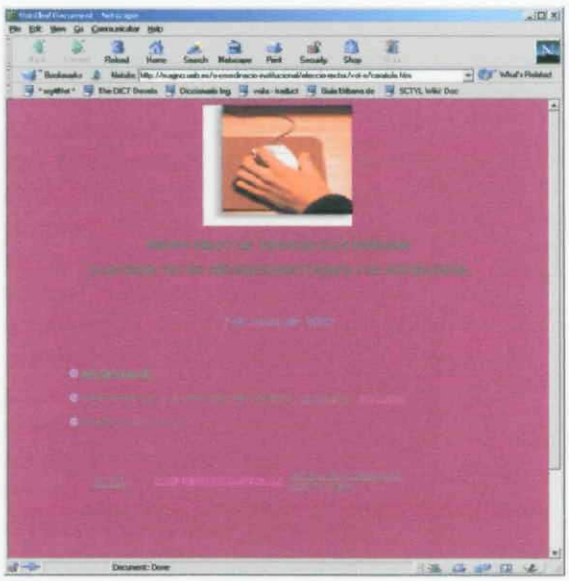
https://www.uab.es/eleccio-rector/

[5] Cada Professor Funcionari Doctor havia rebut una guia amb informació detallada sobre aquestes passes a seguir.
[6] Veure explicació sobre el funcionament dels Certificats Digitals al següent apartat, pp. 16-18.

Accedia a la pàgina web de la votació a través de l'enllaç que es trobava a l'icona "Votació Electrònica".

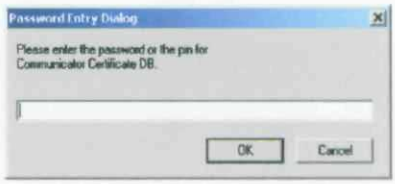


③ Un cop a la pàgina de la votació, tenia la possibilitat de consultar informacions diverses sobre les votacions electròniques. Per passar a la votació havia de seleccionar l'opció "Plataforma de votació".



④ Automàticament, apareixia una finestra que iniciava el procés d'autenticació del votant a través del Certificats Digital prèviament instal·lat.

El votant havia de seguir unes instruccions que se li havien lliurat en el moment de la instal·lació del Certificat. També les podia trobar a la pàgina de les votacions (pas anterior).

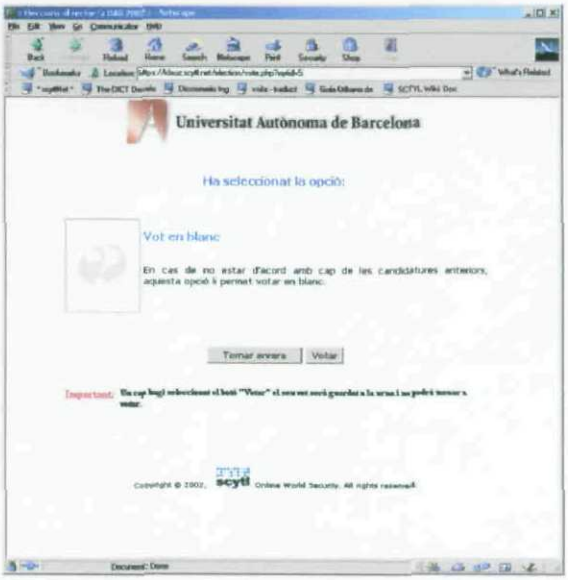


⑤ Un cop realitzada l'autenticació, apareixia la pantalla amb les opcions de la votació: una foto del candidat amb el seu nom, algunes dades personals i un enllaç amb el seu programa electoral. També es va preveure una opció de vot en blanc.

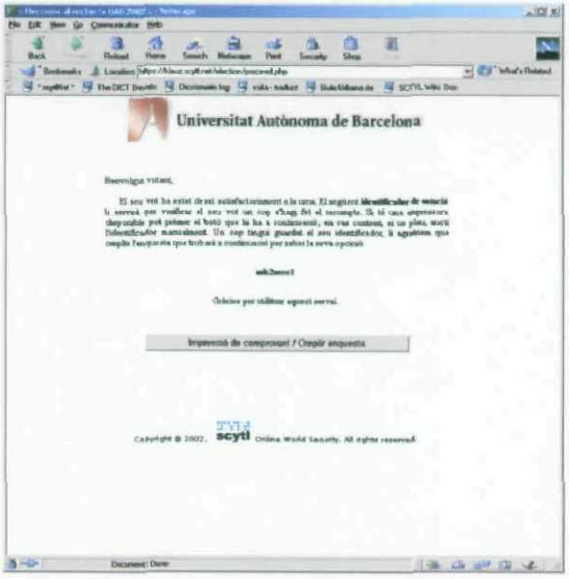
El votant seleccionava la seva opció.

⑥ Apareixia una pantalla de confirmació amb la opció triada. El votant podia tornar

enrere i triar de nou o bé confirmar, equivalent a l'emissió del seu vot.

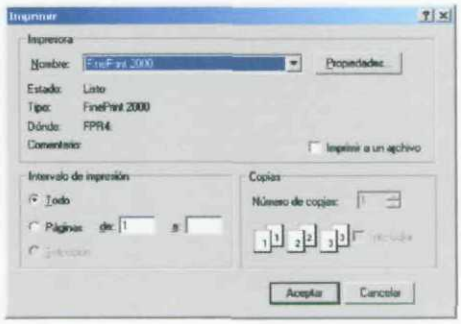


⑦ La següent pantalla confirmava que el vot havia estat emès. També es mostrava un codi identificador del vot que es podia utilitzar per a la verificació posterior.

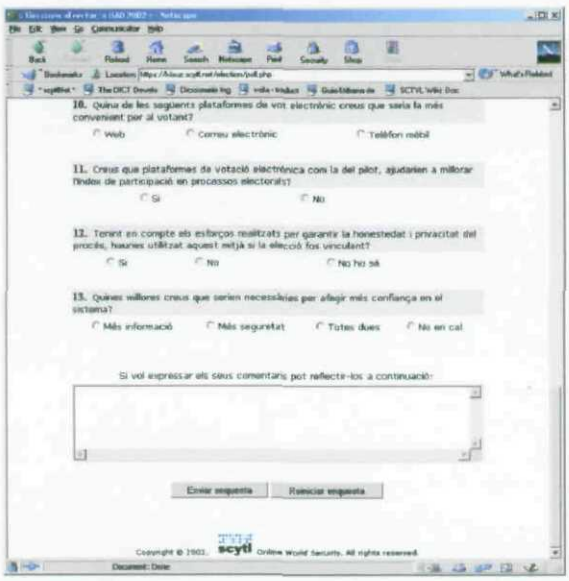


⑧ El votant seleccionava "Impressió de comprovant / Omplir enquesta".

Apareixia una pantalla per imprimir el comprovant. Hi havia la possibilitat de cancel·lar aquesta operació.



⑨ Per últim, es convidava al votant a contestar una enquesta de forma anònima. En acabar, havia de triar la opció "Enviar enquesta".



El votant podia deixar l'enquesta sense omplir i continuar.

⑩ Apareixia una última pantalla d'agraïment. El procediment de votació havia finalitzat. El votant podia tornar a la pàgina d'origen amb l'opció "Sortir".

EL QUÈ EL VOTANT NO VEU: DESCRIPCIÓ TÈCNICA DEL SISTEMA.

Actualment, existeixen tres grans tipus d'esquemes de votació electrònica remota, que han estat desenvolupats (o es troben en fase de desenvolupament) per part de diferents empreses del sector:

- Esquema de seguretat limitada al protocol SSL (Secure Socket Layer)[7]: desenvolupat per l'empresa Election.com. Es tracta d'un esquema que resulta molt còmode pel votant, però amb mínimes garanties pel què fa als requeriments de seguretat.
- Esquema que utilitza funcions homomòrfiques[8]: desenvolupat per l'empresa Votehere. És un dels esquemes més segurs, però resulta excessivament complex en la seva utilització per part del votant.
- Esquema que utilitza Canals Anònims: desenvolupat per diverses empreses, entre elles Scytl, del qual va posar en pràctica una adaptació a la prova pilot de la UAB. A continuació en detallem el funcionament.

Esquema que utilitza Canals Anònims. Variant desenvolupada per Scytl:

L'objectiu d'aquest esquema consisteix en ocultar l'origen dels missatges que arriben al servidor. En altres paraules, es tracta d'ocultar la identitat del votant de manera que es rebi el seu vot sense saber qui l'ha enviat. Per això, els votants envien els seus missatges (vots) al servidor a través d'un **Canal Anònim**. El resultat serà una llista dels vots, la qual es pot consultar sense conèixer quin missatge ha estat generat per cada participant. D'aquesta manera, es realitza el recompte sense vulnerar l'anonimat dels votants i el secret del seu vot (requeriment de privacitat).

---

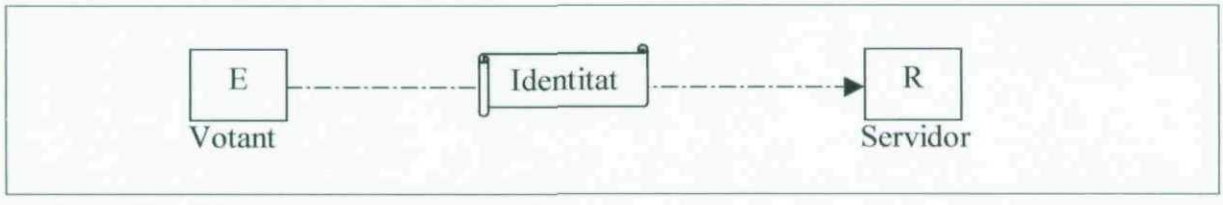
[7] Es tracta d'un protocol creat per l'empresa Netscape que permet la transmissió segura de dades a través de la xarxa gràcies a un sistema de xifratge.

[8] Les funcions homomòrfiques permeten realitzar el recompte dels vots sense haver de desxifrar-los. D'aquesta manera es pot comprovar la identitat del votant (requeriment de discriminació) i incloure el seu vot en el recompte sense vulnerar el requeriment de privacitat (anonimat del votant i secret de vot).

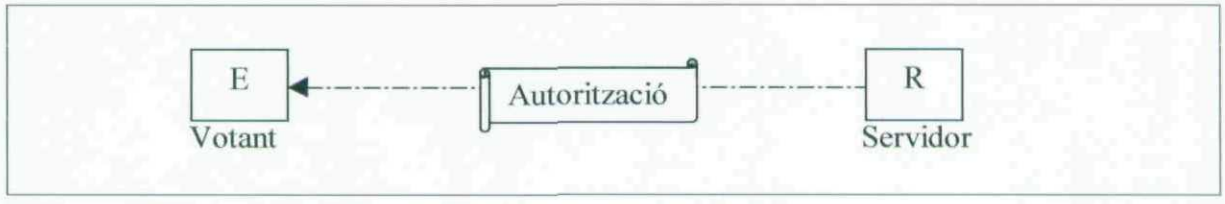
No obstant, en funció d'aquesta primera descripció, l'esquema resultaria del tot inviable ja que no es respectaria un requeriment bàsic com és el de la discriminació: s'ha de controlar la identitat del votant en algun moment donat per evitar el vot de persones no autoritzades o el vot múltiple.

Per resoldre aquest inconvenient existeixen diverses propostes teòriques. Totes elles parteixen de la mateixa base:

1 → El Votant envia la seva Identitat al Servidor:

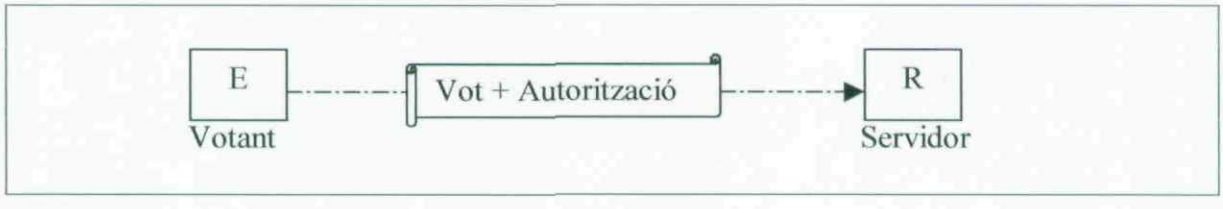


2 → El Servidor comprova el seu caràcter d'elector i li envia una Autorització deslligada de la seva identitat:



3 → El votant utilitza l'Autorització per emetre el seu Vot.

Alguns autors han proposat que el servidor que emeti les autoritzacions i el que rebi els vots siguin diferents i no tinguin cap relació que permeti conèixer a quin votant correspon cada autorització ("Model de les Dues Agències")[9]:



[9] Per una explicació més detallada d'aquesta i altres propostes, veure: CRANOR, L.F., "Computerized polls may save money, protect privacy", article disponible a www.acm.org.crossroads.index.html".

En el cas de la prova pilot de la UAB, donades les restriccions imposades per la manca de temps i de recursos, es va optar per una solució simplificada: els electors havien d'instal·lar als seus ordinadors un **Certificat Digital**, lliurat personalment al Deganat de la Facultat en un disquet. D'aquesta manera s'evitava que cada participant hagués de realitzar més d'una sessió en el moment de la votació (com mostra el croquis).

Per a la instal·lació d'aquests Certificats Digitals, juntament amb el disquet, es lliurava als professors unes instruccions detallades amb les passes a seguir al seu ordinador. Existien dues versions: una per instal·lar el Certificat a un navegador Netscape Communicator (amb el requisit que fos de versió 4.7 o superior) i una altra per instal·lar-lo a un navegador Internet Explorer (versió 5 o superior)[10].

També es va posar a disposició dels professors l'assistència del Servei Informàtic de la UAB per resoldre qualsevol problema amb la instal·lació. Concretament, en el moment en què els professors acudien a recollir el disquet amb el Certificat se'ls preguntava si desitjaven rebre aquesta assistència. En cas afirmatiu, un tècnic del Servei Informàtic es posava en contacte amb aquest/a per concertar una cita i instal·lar-li el Certificat Digital a l'ordinador del seu despatx.

En realitat, dies després de comunicar als professors aquest procediment, i un cop comprovat que van ser molt pocs els qui van acudir al Deganat de la Facultat a recollir el seu disquet, es va optar per què el Servei Informàtic realitzés aquesta instal·lació als ordinadors de tots els professors (amb alguna excepció quan va ser impossible concertar una cita al seu despatx).

Pel què fa al funcionament en termes tècnics dels Certificats Digitals, a continuació n'oferim una descripció. Recordem que es tracta d'un mecanisme que ha de permetre la identificació del participant. En aquest cas, exposem la seva utilitat per a una votació. No obstant, actualment, aquest mecanisme comença a ser implementat per a altres usos, com per exemple en el cas d'Espanya, per realitzar la declaració de l'IRPF a través d'Internet.

[10] Veure còpia de les instruccions a l'Annex I.

☛ Els Certificats Digitals:

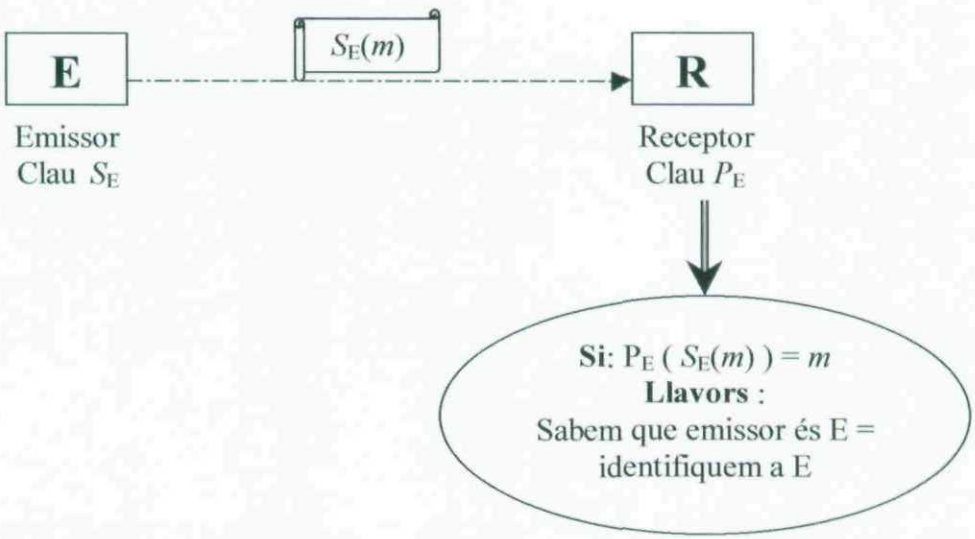
Els certificats digitals són una forma protegida de *signatures digitals*.

Les Signatures Digitals (o criptografia de clau pública):

Es tracta d'un sistema de xifratge que utilitza dues claus relacionades entre elles. La primera d'aquestes és una clau secreta que només la pot tenir l'emissor i serveix per xifrar el missatge. La segona clau, que servirà per desxifrar-lo, és una clau pública a l'abast de tothom.

De fet, la criptografia de clau pública no és utilitzada per mantenir protegit un missatge secret mitjançant el xifratge. Qualsevol persona pot tenir accés a la clau pública i desxifrar el missatge. Però donat que només una única persona és la posseïdora de la clau secreta, amb la clau pública corresponent podem comprovar la procedència del missatge: si amb una clau pública podem desxifrar el missatge, voldrà dir que aquest missatge ha estat xifrat amb la clau privada corresponent. I si coneixem a qui pertany aquesta clau privada, sabrem qui és l'emissor del missatge. El següent esquema mostra el procediment:

➔ L'emissor xifra el missatge m amb la seva clau secreta S: $S_E(m)$, que té la seva corresponent clau pública P_E, a l'abast del receptor:



➲ **SIGNEM** el missatge amb la clau secreta: $S_E(m)$ => **Signatura digital.**

➲ Quan apliquem la clau pública: **verifiquem la signatura**: $P_E\ (S_E(m)) = m$.

El problema d'aquest procediment és que qualsevol pot tenir accés a la clau pública. Llavors, si aquesta (acompanyada de la identitat del propietari de la clau privada corresponent) es troba a un directori públic a la mateixa xarxa i no està protegida, qualsevol persona amb els recursos necessaris pot manipular el directori per falsejar la veritable identitat del propietari. **La solució passa per l'existència d'algun tipus d'autoritat que realitzi signatures digitals sobre les claus públiques dels participants**.

Obtenim així els **CERTIFICATS DIGITALS**:

1➔Cada participant ha de realitzar un registre oficial de la seva identitat i de la seva clau pública[11]: (Participant A, P_A), (Participant B, P_B), etc.

2➔L' autoritat signa la parella: S_{Aut} (A, P_A), S_{Aut} (B, P_B), etc.:

S_{Aut} (A, P_A) = certificat de la clau pública de A o **Certificat de A**.
S_{Aut} (B, P_B) = certificat de la clau pública de B o **Certificat de B**.

3➔A més a més, és necessari que l'autoritat signi la seva pròpia clau pública:

S_{Aut} (Autoritat, P_{Aut}) = Certificat de l'autoritat.

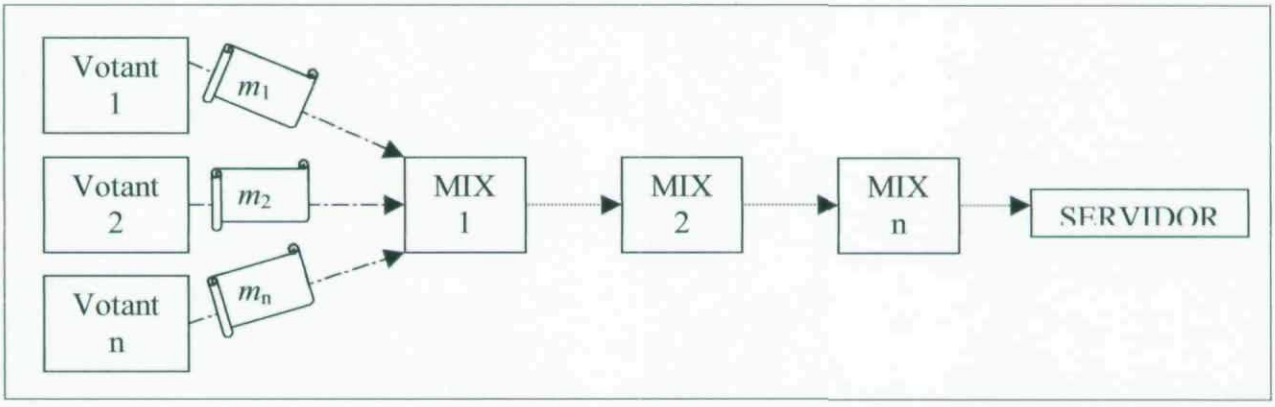
En el cas dels Certificats, també tenim un directori públic. Però ara està protegit per les signatures de l'autoritat. La base d'aquest sistema resideix en el fet que confiem en aquesta autoritat.

[11] Paradoxalment, això pot implicar un moviment físic del participant. No obstant, els Certificats poden ser utilitzats en més d'una ocasió, per exemple en diverses votacions, evitant els posteriors moviments dels participants en cadascuna d'aquestes. De fet, sovint s'equiparen els Certificats Digitals al Document Nacional d'Identitat, que s'ha de renovar cada cert nombre d'anys davant l'autoritat corresponent. Llavors, durant el període de vigència, es pot fer servir per a identificar-se cada cop que sigui necessari.

En definitiva, els Certificats Digitals permeten realitzar la identificació del votant amb totes les garanties. Això comporta la possibilitat que les autoritats electorals discriminin entre electors i persones no autoritzades, evitant també l'emissió de vots múltiples. Llavors, retornant a la descripció dels esquemes que utilitzen Canals Anònims, recordem que aquests pretenen ocultar l'origen dels vots generant-ne un llistat que no permeti conèixer quin missatge ha estat transmès per cada participant. Combinant un Canal Anònim amb la utilització dels Certificats Digitals, l'adaptació de Scytl per a la prova pilot a la UAB pretén garantir que es compleixin alhora requeriments com el de la discriminació i el de la privacitat.

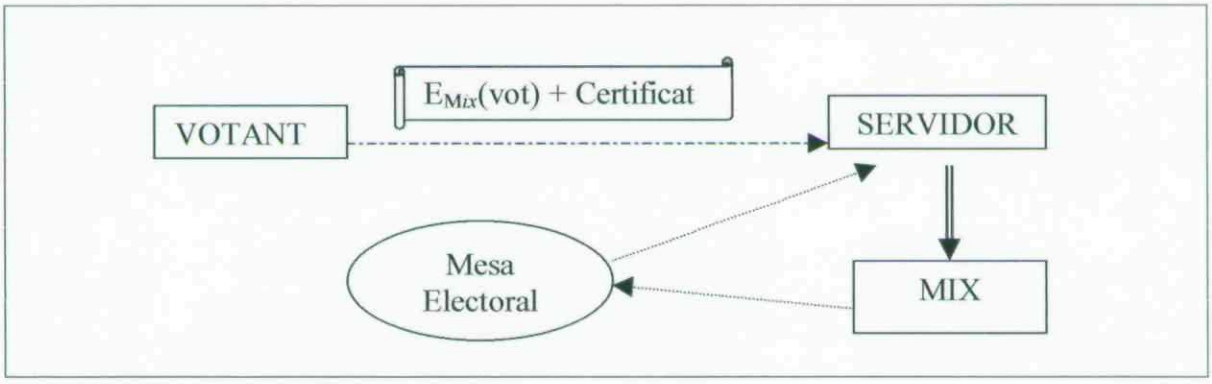
Pel què fa a la descripció tècnica dels esquemes que utilitzen Canals Anònims, la principal proposta teòrica en aquest sentit és la que incorpora el concepte de "*mix-net*" (o xarxa formada per *mixs*) desenvolupat inicialment per David Chaum.

Un *mix* és un element que actua realitzant transformacions criptogràfiques sobre els missatges que circulen en el canal. Tal i com mostra el croquis, cada votant ha d'enviar el seu missatge, que inclou vot i autorització, xifrat amb les claus públiques dels *mixs* (normalment, per una major seguretat, s'utilitzen diversos *mixs* en escala: tots els missatges passen per tots els *mixs*). Els *mixs* reben els missatges, els desxifren, els barregen i els envien al servidor de manera protegida. A més a més, cada *mix* és capaç de suprimir els missatges repetits que hi hagi a la seva entrada (evitant així possibles casos de vot múltiple).



El problema d'aquest esquema resideix en la complexitat i el risc en termes de seguretat del fet que els *mixs* es trobin al propi canal. La proposta de Scytl implementada a la prova pilot de la UAB consisteix en utilitzar un sol *mix* després de la recepció dels vots al servidor, és a dir fora del mateix canal.

El següent quadre mostra el funcionament d'aquesta variant:



El votant fa arribar el seu vot xifrat amb la clau del *Mix* (E_{Mix}(vot)) al primer Servidor. Aquest realitza la identificació a partit del Certificat Digital[12] i emmagatzema els vots xifrats exercint la funció d'una urna.

A la prova pilot, aquest aparell es va situar al Centre de Càlcul del Servei Informàtic de la UAB, i estava controlat constantment per tècnics de Scytl que podien actuar en cas que es detectés qualsevol complicació.

Un cop finalitzada la votació, el *Mix* actua barrejant els vots, desxifrant-los i realitzant-ne el recompte. El *Mix* ja no pot conèixer la identitat dels votants que ha quedat deslligada dels vots. (A la UAB, aquest aparell es va situar a la Sala de Graus de la Facultat de Ciències Polítiques i Sociologia).

L'avantatge d'aquest esquema resideix en la separació de responsabilitats entre el primer Servidor i el *Mix*. Cadascun dels aparells realitza tasques diferenciades en moments

[12] De forma més precisa, es realitza un protocol que implica una sèrie d'intercanvis de claus entre votant i servidor receptor que permeten autenticar-se mútuament i xifrar el vot. L'avantatge és que aquests intercanvis no afecten al votant, que envia el seu vot sense complexitats i còmodament en una sola sessió.

separats, com la identificació i el desxifratge. De fet, aquest esquema no funcionaria si hi hagués el risc d'una "col·laboració" entre els dos aparells. Evitar aquesta possibilitat és la funció de la Mesa electoral[13].

Aquesta és l'encarregada de donar inici a les votacions activant el Servidor receptor (els seus membres han d'introduir al Servidor el seu Certificat Digital). Al final de la votació, la Mesa desactiva el Servidor i trasllada físicament les dades de la urna fins al *Mix* (per exemple, en format CD-ROM). En el cas de la prova pilot a la UAB, i per simplificar, es va optar per enviar la urna fins al *Mix* a través de la xarxa amb una connexió segura.

Llavors, el Mix inicia la seva tasca (barreja, desxifratge i recompte) i s'obtenen els resultats de la votació.

Per últim, el votant té la possibilitat de verificar que el seu vot ha estat tingut en compte en el recompte: un cop ha emès el seu vot, se li lliura un codi identificador. Al final de la votació, juntament amb els resultats, es publica un llistat amb els codis dels vots que han estat inclosos al recompte.

Llavors, el votant no podrà comprovar el contingut concret del seu vot[14]. De fet, l'esquema de votació no permet la possibilitat que aquest s'hagi manipulat (el Servidor no pot obrir els missatges que arriben a la seva entrada perquè estan xifrats amb la clau del *Mix*!). En tot cas, la única actuació deshonesta que podria efectuar el Servidor consistiria en eliminar vots de la urna: si fos així, el codi del vot no apareixeria al llistat final generat pel *Mix* i el votant podria reclamar.

[13] Es tracta d'una mesa electoral similar a les que es constitueixen en les votacions convencionals, pero amb tasques diferenciades. En aquest cas, estava composada per un President (el Degà de la Facultat, Dr. Fausto Miguélez) i dos vocals escollits entre el cens (Dr. Joaquim Brugué i Dr. Josep Mª Masjuan).

[14] I per tant, no pot demostrar el seu vot davant d'un possible comprador.

AVALUACIÓ DE L'EXPERIÈNCIA:

A l'hora d'analitzar i avaluar el desenvolupament de qualsevol experiència de votació electrònica, cal tenir en compte dos elements:

- ⇨ El funcionament dels aspectes tècnics.
- ⇨ El desenvolupament del procés en relació als electors.

Si bé es tracta de qüestions molt relacionades, tractarem d'analitzar l'experiència del 7 de març a la UAB a partir d'aquesta distinció.

AVALUACIÓ TÈCNICA:

Els diversos esquemes de votació electrònica remota desenvolupats fins al moment presenten defectes que provenen, en la majoria dels casos, de les contradiccions que sorgeixen al tractar de garantir els diversos requeriments[15] al mateix temps.

Així, per exemple, quan es pretén augmentar la seguretat, acostuma a fer-se en detriment de la comoditat pel votant, que haurà d'aplicar xifratges gairebé impossibles o bé dedicar-hi més d'una sessió (com és el cas dels esquemes que utilitzen funcions homomòrfiques o Canals Anònims).

En sentit contrari, si es busca reduir al mínim l'esforç la complexitat pel votant, la solució passarà per evitar que hagi de realitzar aquest tipus de xifratges. Llavors, s'eliminen elements de seguretat i no es pot garantir el que passa amb el seu vot (i la seva identitat!) un cop l'ha enviat a través de la xarxa (esquemes de seguretat limitada al protocol SSL).

Combinar seguretat i conveniència resulta doncs el principal repte de qualsevol esquema de votació electrònica remota.

L'esquema dissenyat per Scytl per portar a terme la prova pilot de la UAB tracta, amb força èxit, de trobar l'equilibri en aquesta difícil combinació. No obstant, també es constaten algunes mancances. A continuació presentem una avaluació de l'esquema realitzada a partir del llistat de requeriments exposat al preàmbul.

---

[15] Cf. llistat de requeriments a la p.6.

Discriminació	✓	El Servidor realitza l'autenticació dels votants a través dels Certificats Digitals. Com hem vist, els Certificats Digitals són una forma segura d'identificació del votant, donat que confiem en l'autoritat que els emet. Com a mesura afegida de seguretat, el *Mix* és capaç de detectar els missatges que li arriben repetits.
Privacitat	✓	Queden garantits el secret de vot i l'anonimat del votant: el Servidor, encarregat de comprovar la identitat del votant, no pot obrir els missatges/vots xifrats. Quan aquests arriben al *Mix*, ja estan deslligats de la identitat del votant. A més, el Mix els barreja per evitar qualsevol possibilitat de conèixer l'emissor del missatge per l'ordre o moment de recepció. En conjunt, el contingut del vot i la identitat del votant queden totalment deslligats.
Precisió/ exactitud	✓	El Servidor no pot manipular els vots de la urna ja que estan xifrats amb la clau del *Mix*. En cas que els eliminés, el sistema de verificació ho detectaria.
Imparcialitat	✓	El recompte no s'inicia fins que les dades de la urna es troben al *Mix*, que és l'únic que pot desxifrar els vots. No hi ha possibilitat de recomptes parcials: la Mesa electoral és l'única capacitada per donar l'ordre de traslladar les dades. Aquest ordre es dóna al final de la votació.
Possibilitat de verificació	✗	El votant pot comprovar que el seu vot ha estat tingut en compte al recompte verificant que el codi identificador del seu vot apareix al llistat. Malgrat això, no podrà comprovar el contingut concret del vot.

Comoditat/ agilitat	✗	La votació no va resultar excessivament difícil i es podia realitzar en pocs minuts. L'únic inconvenient es pot trobar en la instal·lació del Certificat Digital i en la seva utilització durant les votacions. En realitat, tècnicament parlant, l'emissió del vot com a tal no comportava grans complexitats. En aquest sentit, l'esquema sí respecta aquest requeriment. No obstant, i com veurem en el següent apartat, per parlar de comoditat i agilitat hem de tenir en compte una visió global de totes les passes que el votant va haver de realitzar per votar.
Flexibilitat	✓	L'esquema permetia triar entre la opció del candidat i el vot en blanc. Potser s'hagués hagut d'incloure una opció de vot nul.
Mobilitat	✓	El votant podia instal·lar el Certificat Digital i emetre el seu vot des de qualsevol ordinador connectat a la xarxa, sempre i quan complís els requisits mínims per a Netscape Communicator o Internet Explorer. (En la majoria de casos, aquesta tasca va ser realitzada pel Servei Informàtic). L'únic possible inconvenient resideix en el fet que calia decidir amb antelació des de quin ordinador es votaria el dia de l'elecció. Això implicava també que en cas d'acceptar l'assistència per part dels tècnics del Servei Informàtic, aquests només podien desplaçar-se fins al despatx del professor, limitant així la opció de triar un altre emplaçament.

Clau: ✓ = el requeriment queda garantit
✗ = el requeriment no queda totalment garantit.

Com es pot veure, l'esquema desenvolupat per Scytl per la prova pilot es presenta com un dels més segurs del mercat. Només en el cas de la *Possibilitat de Verificació* no es compleixen totes les garanties: no es dóna exactament una verificació universal ja que, tot i

que es poden recomptar els vots emmagatzemats a l'urna tantes vegades com es vulgui, no es pot tenir la certesa de que coincideixen exactament amb els vots emesos pels votants (ja que no es pot verificar el contingut d'aquests). Com a aspecte positiu, això evita la possibilitat de la compra-venda de vots o la coerció.

D'altra banda, sí es pot comprovar que hi ha la mateixa quantitat de vots emesos que vots inclosos al recompte. Però per això és necessari que tots els votants realitzin la verificació. Per tant, per garantir aquest requeriment, el votant ha de realitzar una nova sessió al final de l'elecció!

Hem de recordar que la possibilitat de verificació és un element que ve incorporat per la pròpia utilització de tecnologia i la manca de confiança que aquesta pot comportar. Així, en una votació convencional, aquesta etapa no es percep com a necessària donat que existeixen elements de confiança externs.

Pel què fa als requeriments relacionats amb la conveniència de l'esquema, és precisament el de la *Comoditat/Agilitat* el que possiblement es garanteix en menor mesura. Certament, els Certificats Digitals poden ser utilitzats en més d'una ocasió. Per tant, a mig termini, la incomoditat de la seva instal·lació es recupera evitant posteriors desplaçaments. A més a més, es tracta d'una forma segura de garantir requeriments tan importants com són la discriminació i la privacitat. Però, en qualsevol cas, des del punt de vista estrictament del votant, la instal·lació suposava una etapa afegida al procediment.

A més, per aquells electors que van optar per fer-ho ells mateixos, la instal·lació podia resultar una mica complexa[16]. En realitat, el votant només havia de seguir les passes clarament exposades a les instruccions que se li havien lliurat. Però també és cert que l'elector realitzava la instal·lació sense entendre ben bé el què estava fent. Cal tenir present que aquest no només no té perquè reunir unes aptituds especials, sinó que, a més a més, és molt probable que no estigui acostumat al vocabulari especialitzat informàtic. Així, alguns termes com el de "Certificat Digital" mateix podien portar a confusions.

[16] També és cert que en la majoria dels casos, la instal·lació la van realitzar tècnics del servei d'Informàtica de la UAB.

Malgrat tot, i com veurem en el següent apartat, explicar als votants en què consisteixen aquests conceptes suposaria una complicació afegida, i fins i tot en alguns casos, una molèstia sense interès!

En tot cas, la instal·lació equivalia, en certa manera, a realitzar una sessió prèvia. Per tant, el votant que va seguir tot el procés, va realitzar un total de tres sessions: instal·lació del Certificat[17], votació i verificació!

Cal afegir que des d'un punt de vista estrictament tècnic, es pot considerar que l'emissió del vot no presentava grans dificultats ni resulta excessivament incòmode: el votant només havia d'accedir a la pàgina de la votació i seguir les indicacions que apareixien a les successives pantalles[18]. Això també és cert si es té en compte una concepció de la utilització dels Certificats Digitals com l'esmentada més amunt: si aquests equivalen a una mena de D.N.I. que, en teoria, ja posseïm amb anterioritat, podem considerar que la identificació es realitza en la mateixa sessió de l'emissió del vot: quan apareix la pantalla d'autenticació al accedir a la "Plataforma de votació". (El que sí que constitueix una nova sessió per al votant és la Verificació).

Precisament, un dels grans atractius dels sistemes de votació electrònica resideix en la possibilitat d'unir aspectes aparentment tan diferents com són la tecnologia informàtica i la política, en una manifestació bàsica d'aquesta com són les eleccions i més concretament, els procediments de votació. També hem vist al preàmbul d'aquest informe que aquesta tecnologia és aplicable a diversos estadis. I hem comprovat que aquest ha estat el cas de la prova pilot a la UAB: des de la identificació del votant (mitjançant la utilització de Certificats Digitals) fins a la verificació (que presenta alguns dubtes).

Llavors, creiem que el concepte de *Comoditat/Agilitat* ha de ser entès en relació al conjunt d'aquestes etapes. L'esfera tècnica no pot separar-se del component polític. Com tampoc no pot oblidar la veritable intenció dels dissenys que planteja: facilitar l'acció de votar (preferiblement, des del punt de vista de l'elector).

Per tant, si el votant no s'ha d'enfrontar únicament a una de les etapes (emissió del vot) sinó a totes elles, la *Comoditat/Agilitat* ha de ser la característica general d'aquest conjunt. I

[17] Inicialment, el votant havia de recollir el seu Certificat al Deganat de la Facultat. Donada la seva localització, aquest fet no suposava un esforç excessiu. Però es pot considerar una molèstia més.

en el cas de la prova pilot a la UAB, el conjunt equivalia a realitzar tres sessions força complexes, o com a mínim, feixugues.

En definitiva, la prova pilot realitzada a la UAB reprodueix, tot i que en menor mesura, algunes de les mancances pròpies de qualsevol sistema de votació electrònica remota. En aquest cas, la comoditat és la més afectada. I per tant, el votant es qui es veu perjudicat... si finalment decideix emetre el seu vot electrònicament.

ELS ELECTORS DAVANT LA PROVA PILOT:

Com hem vist a l'apartat anterior, quan parlem de vot electrònic, hem de tenir en compte que l'elector participarà en alguna cosa més que la mera emissió del seu vot. En realitat, es pot veure implicat diverses fases de la votació: l'abans, el durant i el després.
Així, per exemple, a més d'haver de resoldre qüestions tècniques com la instal·lació del seu Certificat Digital, el votant serà objecte d'una campanya informativa.
En el cas de l'experiència a la UAB, des de mitjans de febrer, els professors/electors van rebre diverses comunicacions. Es tractava de cartes i missatges de correu electrònic enviats des del Deganat de la Facultat on se'ls informava de la realització de la prova pilot. Les explicacions, que a cada nova comunicació eren més específiques, tenien dos components: per una banda, tractaven de presentar breument algunes característiques de la prova, amb especial rellevància en el tema de la seguretat. Per l'altra, animaven als professors a participar, exposant el caràcter innovador i experimental de l'experiència. En tots dos casos, l'objectiu principal era assolir la seva confiança i la seva participació sense dificultats.

[18] Cf. Procediment de la Votació, pp.9-13.

Es va assolir la confiança dels electors?

El resultat de l'enquesta realitzada al final de la votació electrònica[19] mostra clarament que no hi va haver cap problema de manca de confiança: quan es pregunta sobre possibles millores per afegir més confiança en el sistema, la majoria dels enquestats va contestar que no en calien.

Aquesta impressió queda refermada en les posteriors opinions expressades pels professors quan els vam consultar. Fins i tot en alguns casos en què un elector no va poder o no va voler votar, la manca de confiança no és la causa exposada per explicar la seva abstenció.

En realitat, l'elevat grau de confiança assolit resulta sorprenent. És evident que aquesta qüestió va molt lligada al disseny tècnic del sistema de votació. Si es compleixen els requeriments de seguretat esmentats anteriorment i els electors en tenen coneixement, aquests podran emetre el seu vot amb tota confiança.

Malgrat això, i com avançàvem més amunt, és evident que en una elecció pública d'aquest tipus els electors no tenen perquè reunir unes aptituds tècniques específiques. Ni tampoc se'ls pot exigir que tractin d'entendre com funciona l'esquema de votació a utilitzar. Encara més, si es posés en marxa una campanya amb objectius d'aquest tipus, el més probable seria que els electors entenguessin l'elecció com una preocupació i una molèstia excessiva: els esforços per generar confiança no només no servirien sinó que tindrien efectes contraris als desitjats!

A la prova del 7 de març es va optar per no aportar als electors dades específiques sobre les qüestions tècniques. La informació que se'ls feia arribar no entrava en detall sobre la forma en què quedaven garantits els seus drets (secret de vot, anonimat, el propi dret de vot (integritat del vot),...). Simplement s'indicava que el sistema era del tot segur: "(...) ens hem assegurat que es tracti d'un mecanisme extremadament segur: només els individus autoritzats a fer-ho podran votar i el contingut del seu vot serà totalment anònim"[20].

Precisament, en la generació de confiança va resultar molt positiu el fet que les cartes i missatges fossin comunicacions del Degà de la Facultat, conegut personalment per tots els

[19] Recordem que només 5 dels 12 electors que van emetre el seu vot electrònicament van contestar a l'enquesta que se'ls proposava.

electors (i un més entre ells). A més a més, els mateixos organitzadors de la prova, especialment i sobretot els membres de l'Equip d'Estudis Electorals, són companys dels electors (i, en alguns casos, electors també). Aquest fet mateix, així com la informació a través de converses informals entre membres de l'EEE i alguns professors, van afavorir la generació de confiança.

Per tant, més enllà de si el sistema era efectivament segur o no, va ser la identitat corporativa i el vincle amb la UAB i/o els membres d'aquesta el què va donar la confiança necessària als electors que van emetre el seu vot (o que ho haguessin fet en el cas de no donar-se unes circumstàncies concretes). Això ens porta a pensar que en el cas de generalitzar aquest tipus d'experiències a d'altres col·lectius de la mateixa universitat, caldria verificar si aquestes pautes podrien reproduir-se.

D'altra banda, també cal tenir en compte que es tractava d'una elecció pública però menor, i amb una sola candidatura. És probable que en un context diferent i més conflictiu el grau de confiança no hagués estat tan elevat.

En tot cas, si realment no es va donar cap problema de manca de confiança, com s'explica que no participessin més professors?

La participació electoral a la prova pilot:

El següent quadre mostra els resultats per cadascuna de les convocatòries a la Facultat de Ciències Polítiques i Sociologia per al Sector A (Professors/es Doctors Funcionaris)[21]:

[20] Fragment de la primera carta enviada pel Degà als electors, 11 de febrer 2002. Veure Annex II.

[21] Font: Oficina de Coordinació Institucional, UAB. Total Cens Sector A Facultat Ciències Polítiques i Sociologia: 48 electors.

Votació convencional (vinculant)	Vots emesos	33
	Vots vàlids a candidatura	22
	Vots en blanc	6
	Vots nuls	5
Votació electrònica (prova pilot, no vinculant)	Vots emesos	12
	Vots vàlids a candidatura	9
	Vots en blanc	3

Com es pot veure, sobre un total de 48 electors, 12 van emetre el seu vot a la prova pilot, el què suposa un 25% del cens. Pel què fa a les votacions convencionals, es van comptabilitzar un total de 33 vots emesos. Admetent que tots els professors que van participar a la prova pilot ho van fer prèvia o posteriorment a la votació convencional, llavors podem considerar que van emetre el seu vot electrònicament un 36,4% dels votants[22].

Pel què fa als resultats, a la prova pilot, un 75% dels vots van anar destinats a la candidatura, enfront d'un 66,7% en la votació convencional. En el cas dels vots en blanc, els resultats són de 24 i 18,2% respectivament. Per tant, tot i que les dades no coincideixen exactament, sí que es respecten les proporcions per a cadascuna de les categories. A més a més, cal tenir en compte que a la prova pilot no es podia emetre un vot nul, cosa que sí era possible a la votació convencional, on va ser utilitzat per un 15,1% dels votants.

Aquesta dada ens indica que potser seria recomanable incloure aquesta opció a les votacions electròniques. Sobretot si tenim en compte que part dels vots nuls emesos a les votacions convencionals podien ser fruit d'algun tipus de protesta[23].

[22] Pels comentaris recollits, resulta lògic pensar que cap elector es va abstenir a les votacions convencionals i va participar a la prova pilot.

[23] Alguns professors/es podrien haver volgut mostrar la seva protesta contra la recentment aprovada Llei Orgànica d'Universitats (LOU), en base a la qual es realitzaven les eleccions a Rector.

En qualsevol cas, existeixen tres tipus d'electors:

- Electors que van votar de forma convencional però no van emetre el seu vot a la prova pilot.
- Electors que van votar de forma convencional i posteriorment van emetre el seu vot a la prova pilot.
- Electors que no van participar de forma convencional, bé perquè no van poder, bé perquè no van voler. Podem considerar que tampoc van participar a la prova pilot.

Una de les explicacions a l'abstenció a la prova pilot la podem trobar en el primer grup de professors. De forma general, es tracta d'electors que van considerar més fàcil exercir el vot de forma convencional i deixar de banda la convocatòria electrònica. En realitat, l'enquesta i les opinions exposades per alguns dels professors que sí van participar mostren que la votació electrònica no presentava grans dificultats[24]. No obstant, aquesta no tenia perquè ser la impressió inicial.

Paradoxalment, va ser la campanya informativa la que va generar aquest desconcert en alguns professors. Efectivament, el volum de cartes i missatges que va rebre cada elector va resultar excessiu, obtenint així un efecte pervers en relació als objectius inicials: per una banda, els electors confiaven en el sistema i "s'atrevien" a emetre el seu vot sense patir per qüestions de seguretat com l'anonimat o el secret de vot. Però per l'altra, hi havia una sensació de que tot plegat era massa complex.
En alguns casos, els professors van optar per deixar de llegir les cartes que els hi arribaven! Llavors, si en comptes de tractar-se d'una prova sense validesa, els electors haguessin hagut de triar entre un o altre mecanisme per emetre un vot vinculant, els hauria semblat més còmode votar de forma convencional desplaçant-se fins a la facultat (fet que en molts casos no era degut exclusivament a la celebració d'eleccions, sinó per altres motius).

[24] Al llarg de la jornada electoral alguns votants van constatar petits problemes en el moment de realitzar l'emissió del vot (per exemple, problemes amb la connexió). Malgrat això, la presència de tècnics de Scytl al Centre de Càlcul del Servei Informàtic va permetre solucionar aquestes qüestions amb relativa rapidesa.

Cal tenir en compte que no estem parlant d'un grup de persones especialment afectat per una manca d'accés a les noves tecnologies, és a dir, per la divisió digital. És cert que la majoria d'electors del cens tenen coneixements molt bàsics a nivell d'informàtica. Però per altra banda, constitueixen un tipus de segment que coincideix amb aquell que sol tenir més avantatges en relació a l'accés a la tecnologia[25]:

- es tracta d'un grup format majoritàriament per homes: aproximadament un 71% del cens són homes, enfront d'un 29% de dones;
- són Doctors, i per tant, persones amb una alta formació, molt per sobre de qualsevol mitjana poblacional;
- es tracta de persones que treballen a un espai com és la Universitat, on no falten ordinadors connectats a la xarxa amb els quals entren en contacte habitualment;
- etc...

Per tant, no podem trobar les causes de l'abstenció a la prova pilot en un desconeixement total de qüestions relacionades amb tecnologies informàtiques. Més encara si constatem nivells de confiança com en aquest cas (encara que provinguin d'altres causes). Malgrat això, les campanyes informatives han de realitzar-se tenint en compte que accés a tecnologia no suposa necessàriament domini d'aquesta, com tampoc implica gust o interès en el seu ús. Les inquietuds informàtiques de molts usuaris no van més enllà de la simple utilitat.

Finalment, pel què fa al tercer tipus d'electors, és a dir, aquells que no van participar en cap de les votacions, existeixen dues possibilitats.

Per una banda, alguns professors no van participar perquè no van voler fer-ho. Entre aquests, una de les raons exposades per justificar aquesta abstenció voluntària va ser la situació ja esmentada de protesta contra la LOU. Per tant, les votacions electròniques no eren el motiu de l'abstenció per sí mateixes. Al contrari, en unes altres circumstàncies, és probable que aquests electors haguessin accedit a participar a la prova pilot.

[25] Font: Equip d'Estudis Electorals, "Adaptació a Catalunya d'experiències de votacions electròniques", 2002, pendent de publicació.

Per altra banda, hi ha aquells electors que per raons diverses no van poder emetre el seu vot el 7 de març. Per exemple, per no trobar-se a la UAB aquell dia. De fet, en aquests casos, el vot electrònic remot hagués suposat un avantatge en cas d'haver estat una alternativa vinculant al vot convencional. A més a més, per aquells que ja havien instal·lat el seu Certificat Digital es podria haver previst la possibilitat de realitzar votacions abans del dia fixat per la jornada electoral, com s'ha donat en algunes experiències de vot remot en altres països[26]. A més a més, les votacions remotes haurien de tancar-se abans de les votacions convencionals, de manera que si algun elector tingués problemes per emetre el seu vot electrònicament, tingués temps de fer-ho de forma alternativa per no perdre un dret tan important com el mateix dret de vot.

Sigui com sigui, resulta raonable que, en no poder emetre el seu vot de forma vinculant, la opció del vot a la prova pilot resultés absurda per aquests professors.

Per tant, i en conjunt, la participació a la prova pilot no es va veure afectada per qüestions relacionades amb la pròpia experiència (aspectes tècnics, confiança,...). Més aviat, es van donar una sèrie de circumstàncies que van allunyar alguns electors de l'urna "virtual".

De totes maneres, no es poden obviar alguns errors estratègics comesos, com en la realització de la campanya informativa.

ALTRES OBJECTIUS DE LA PROVA PILOT:

Com hem vist al llarg d'aquesta avaluació, qualsevol experiència de votació electrònica parteix d'una sèrie d'objectius que cal assolir per garantir-ne l'èxit. Es tracta d'aspectes tècnics (seguretat, conveniència,...) i polítics (confiança, participació,...).

Ara bé, en el cas de la prova pilot del 7 de març, també es perseguia un altre tipus de finalitat. Concretament, la Universitat Autònoma de Barcelona pretenia donar a conèixer la realització d'aquesta experiència de cara a l'exterior. De fet, la col·laboració de l'empresa

[26] És el cas de les eleccions primàries internes del Partit Demòcrata d'Arizona celebrades en aquest Estat dels Estats Units al març de 2000. Es tracta de l'únic cas de votació electrònica remota vinculant (amb mecanismes convencionals alternatius). Les votacions remotes es van iniciar 4 dies abans de la jornada electoral.

Scytl en la organització, però sobretot en la implementació tècnica de la prova, es realitzava a canvi de la promoció que es podia realitzar des del Gabinet de Premsa de la Universitat. L'objectiu era que es portés a terme una campanya informativa entre els principals mitjans de comunicació per tal de donar a conèixer l'existència i desenvolupament (amb èxit) de la prova. Per a Scytl, això implicava una bona plataforma per presentar públicament la seva tasca en el disseny i desenvolupament d'esquemes de votació electrònica. Per a la UAB, es tractava de posar en evidència el seu caràcter capdavanter en l'àmbit de l'aplicació de tecnologia.

Finalment però, aquesta promoció no es va realitzar en els termes acordats inicialment. L'abast de la noticia no va anar més enllà de les publicacions internes de la pròpia Universitat[27]. L'única via per la qual se'n podia tenir coneixement a l'exterior va ser a través de la reproducció d'aquests breus articles a la secció de notícies de la pàgina web de la UAB[28]. Aquest error, que es produeix principalment en detriment de Scytl, s'ha d'atribuir per tant a la Universitat. I malgrat que no va afectar al desenvolupament com a tal de la prova pilot, aquesta errada ha de ser inclòs al conjunt d'elements que conformen la part negativa de l'experiència.

D'altra banda, cal afegir que independentment dels avantatges que tant Scytl com la UAB podien extreure en cas d'haver-se realitzat una promoció més extensa de la prova pilot, és evident que aquest tipus d'experiències han de servir per localitzar possibles defectes. Uns dels principals objectius és tenir la possibilitat d'anticipar-se als errors i millorar-los en posteriors experimentacions. Llavors, aquesta tasca d'avaluació – que en part pretenem realitzar aquí – ha de tenir en compte, per una banda, les especificitats del cas concret que hem posat en marxa, però per l'altra, els aspectes més generals que s'han pogut comprovar en altres proves i experiències d'aquest tipus.

---

[27] Veure: *L'Autònoma*, (publicació interna de la UAB) febrer 2002, Edició extraordinària, p.2
i *L'Autònoma*, març-abril 2002, núm. 152, p.2.

[28] Veure: "Prova pilot de votació electrònica per a l'elecció del rector", 13 febrer 2002, disponible a www.uab.es/actualitat/notcampus/votelectronic0202.htm.
i "La prova pilot de votació electrònica a la UAB un èxit de seguretat i accessibilitat", 8 març 2002, disponible a www.uab.es/actualitat/notcampus/resultatsvotelectronic0302.htm.

Es pot entendre per tant que la promoció de l'experiència ha de servir, científicament parlant, per donar a conèixer les millores que es proposen per alguns dels problemes localitzats en altres experiències. Per exemple, hem vist que sovint resulta difícil combinar seguretat i comoditat. Si realment Scytl ha estat capaç d'aportar millores en aquests aspectes més problemàtics, és necessària una promoció per donar a conèixer les peopostes de solució. La prova pilot de la UAB hauria d'haver tingut més en compte aquest fet.
En un mateix sentit, dels errors que se n'hagin extret no només n'aprendran Scytl i la UAB, sinó també tots aquells organismes que decideixin tirar endavant una experiència d'aquest tipus.

Per tant, no podem obviar que la promoció que va tenir la prova pilot de la UAB va resultar totalment insuficient tenint en compte alguns dels objectius que s'havien marcat des d'un principi. Malgrat que el desenvolupament de les votacions no es va veure afectat per aquest esdeveniment, en cas d'haver-se dut a terme una major promoció de l'experiència, els beneficis haguessin estat molt majors.

CONCLUSIONS

Globalment, la prova pilot realitzada el 7 de març a la UAB presenta un balanç força positiu. És cert que existeixen alguns dubtes sobre una implementació vinculant d'un sistema d'aquest tipus, sobretot si tenim en comte algunes de les limitacions tècniques exposades en aquest informe. En aquest sentit, haurem de confiar en el què els avenços en les noves tecnologies (i més concretament, en els especialistes que hi ha darrera d'aquests avenços) ens puguin oferir.

Pel què fa a la reacció dels votants davant d'aquesta experiència, l'alt grau de confiança expressat resulta esperançador. Precisament, aquesta és una de les qüestions que més preocupen a l'hora de posar en marxa mecanismes d'aquest tipus. No obstant, no hem d'oblidar les característiques específiques que envoltaven la prova pilot: especialment, les característiques i magnitud del cens. A la UAB, hem pogut veure que van ser els propis organitzadors els qui van generar aquesta confiança. En cas de generalització a altres àmbits, caldria tractar de reproduir el fenomen que es dóna en les votacions convencionals, que consisteix en atorgar la confiança a una autoritat. Malgrat això, és previsible que una generalització d'una experiència com aquesta, per exemple al conjunt de la comunitat universitària, aporti nous reptes que la prova pilot no ha mostrat. En realitat, aquesta ha de ser la funció de les proves experimentals com aquesta.

D'altra banda, tot i que els experts anuncien un ràpid desenvolupament de l'ús de tècniques informàtiques com en el cas dels Certificats Digitals, no hem d'oblidar que per als votants, aquests són encara incomparables a altres suports físics com els que utilitzem habitualment (per exemple, el Document Nacional d'Identitat), potser per desconeixement. Per tant, mentre no es produeixi aquesta interiorització a les costums quotidianes, el volum de comunicacions que s'han de realitzar com a campanya informativa generen una sensació que no afavoreix a la prova ni al propi votant. Podem avaluar i millorar qüestions tècniques, fins i tot relacionades amb la comoditat del sistema. Però mentre l'elector percebi aquesta pràctica com una molèstia – més que complicada, feixuga – serà impossible tractar de mostrar-ne els avantatges. Ens trobem davant d'una paradoxa encara sense solució.

De forma general, hem de tenir en compte el què ens plantejàvem a l'inici d'aquestes pàgines: qualsevol innovació d'aquest tipus ha de tenir com a objectiu alguna forma de facilitació de l'acció de votar. El vot remot presenta molts avantatges, però també molts inconvenients encara. Precisament, aquest tipus d'avaluacions han de servir per enriquir el debat al voltant de la idoneïtat d'implementar mecanismes de votació electrònica. I si és possible, per reduir o eliminar els inconvenients.

No obstant, mentre es continuïn identificant defectes, el vot electrònic ha de tractar-se amb precaució. Sense oblidar que el status quo és una alternativa com qualsevol altra.
En tot cas, el més recomanat és avançar gradualment mentre experimentem i millorem propostes més agosarades. Fins i tot, es pot optar per mecanismes que no afectin l'acció de votar, però facilitin altres aspectes com pot ser el recompte. Qualsevol opció ha de ser estudiada si realment aporta noves possibilitats sense comportar cap inconvenient.

ANNEXOS

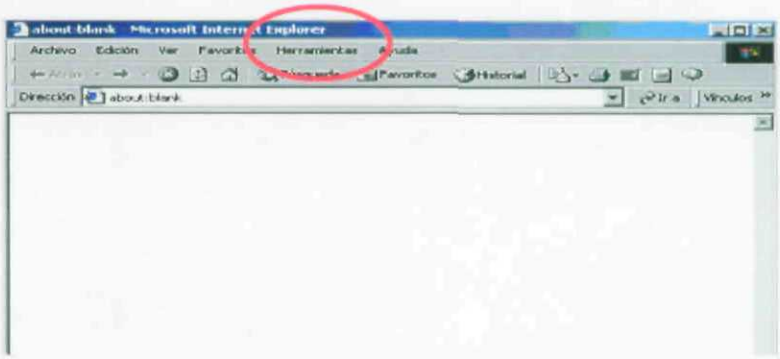
I - Instruccions que van rebre els elector per a la instal·lació del seu Certificat Digital.

II - Còpia de la primera carta que van rebre els electors informant sobre la realització de la prova pilot.

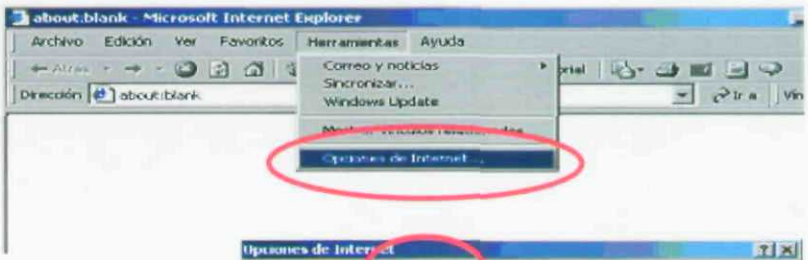
INSTAL·LACIÓ DEL CERTIFICAT PER A INTERNET EXPLORER

Per instal·lar els certificats del pilot a un navegador de Internet Explorer cal que aquest sigui de la versió 5 o superior. En cas afirmatiu el passos a seguir serien els següents:

1. Obrir el navegador i seleccionar el menú "Herramientas"

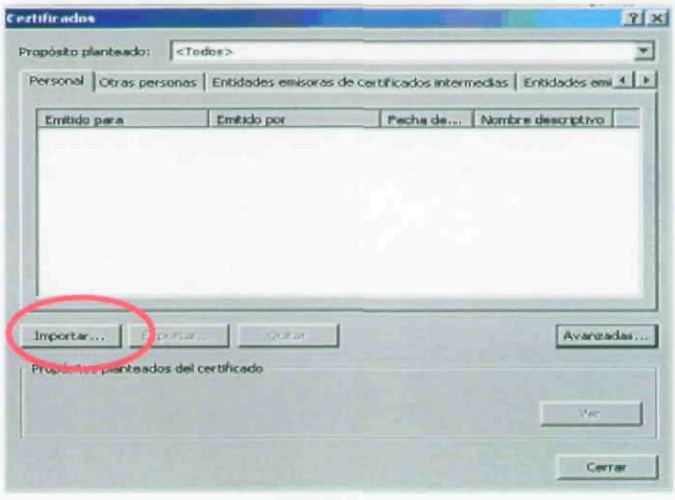


2. Seleccionar la opció "Opciones de Internet" del menú desplegat

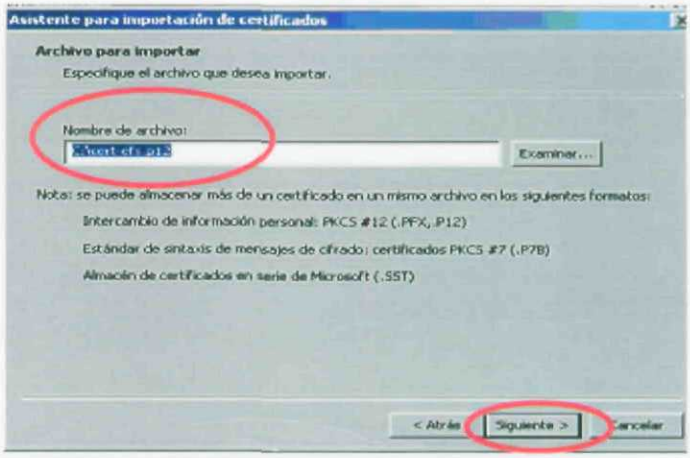


3. Anar a la pestanya "Contenido" i seleccionar el botó "Certificados"

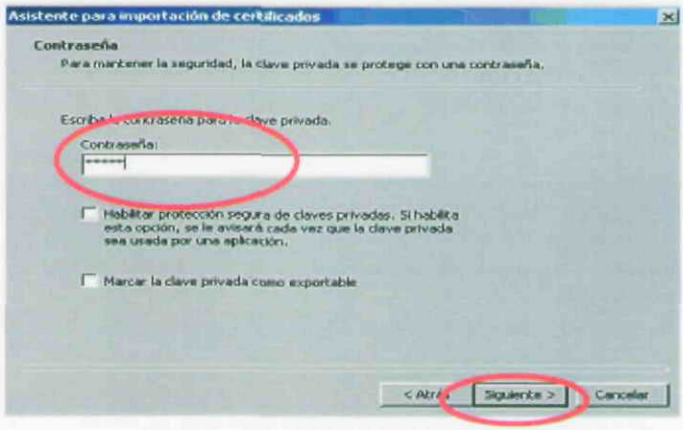
4. Prémer el botó "Importar..."



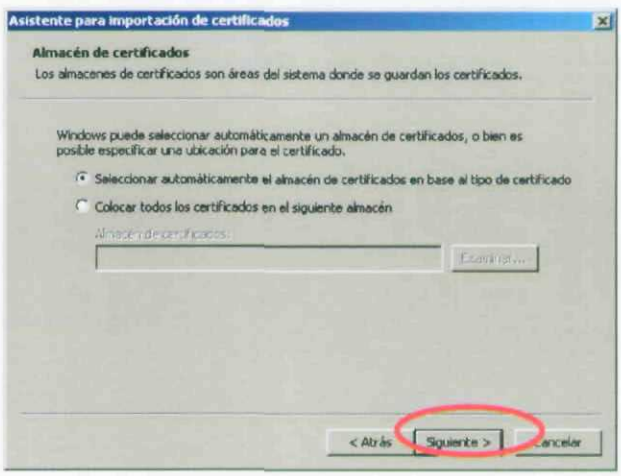
5. Introduïu el disquet a la disquetera i especifiqueu la ruta a Nombre de archivo la ruta: "A:\cert.p12". Prémer "Siguiente"



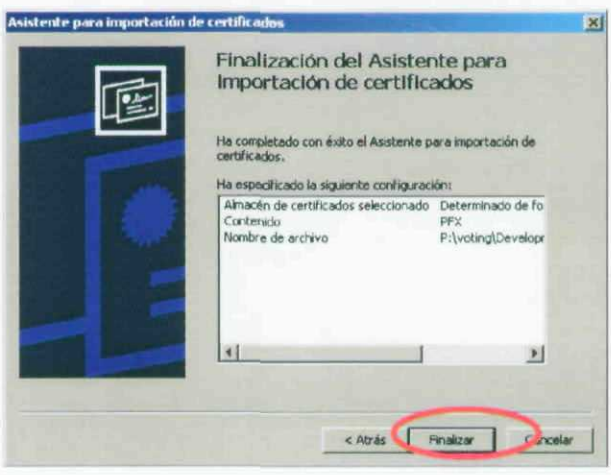
6. Introduir el **password del certificat** (lliurat amb el document que acompanya al disquet) i prémer el botó "Siguiente"



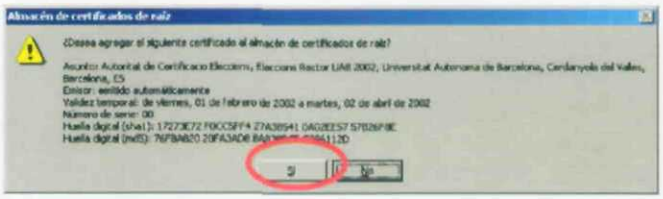
7. Seleccionar "Siguiente" en la següent pantalla



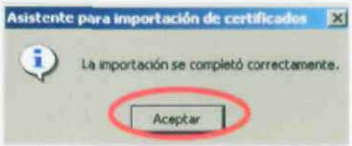
8. Seleccionar "Finalizar" en la següent pantalla



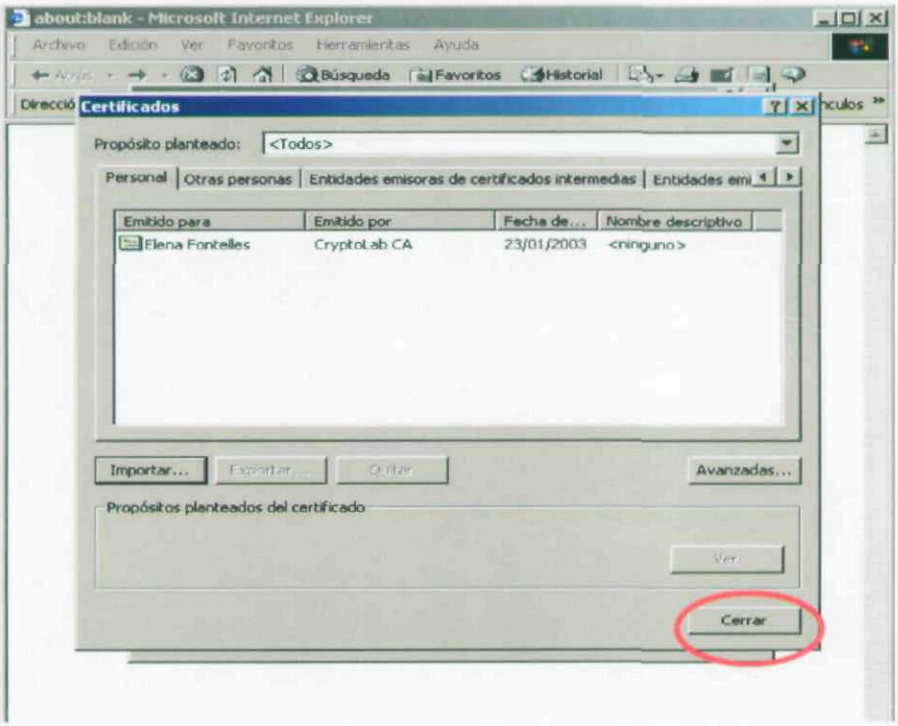
9. A continuació es demana confirmació per guardar el certificat al navegador. Seleccionar "Si"



10. El certificat s'he instal·lat correctament. Seleccionar "Aceptar"



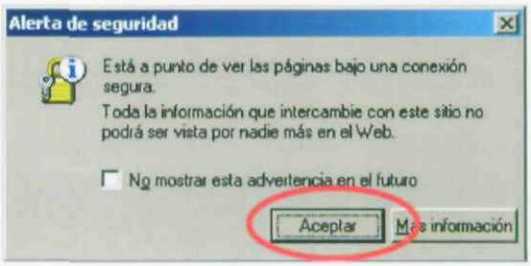
11. Ja pot utilitzar els certificats en el navegador. Prémer "Cerrar" per continuar.



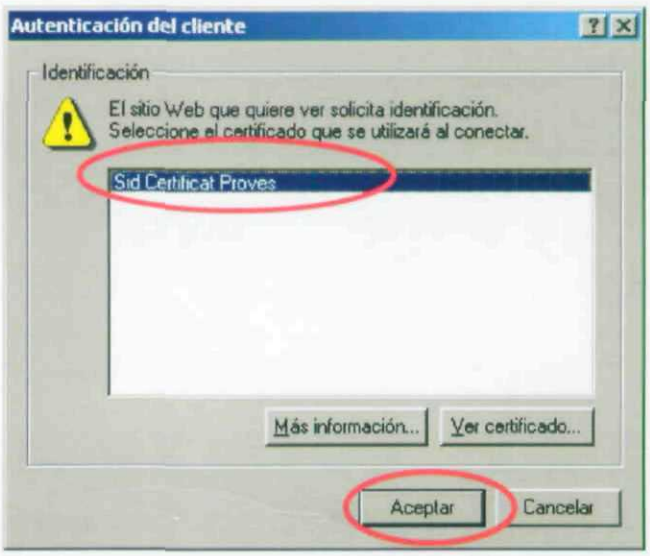
FUNCIONAMENT DELS CERTIFICATS DURANT LES VOTACIONS. VERSIÓ INTERNET EXPLORER

Un cop instal·lats els certificats al navegador de "Internet Explorer" ja es poden utilitzar per a la identificació en les votacions. La seqüència de finestres que apareixen quan es demana el certificat de votant és la següent:

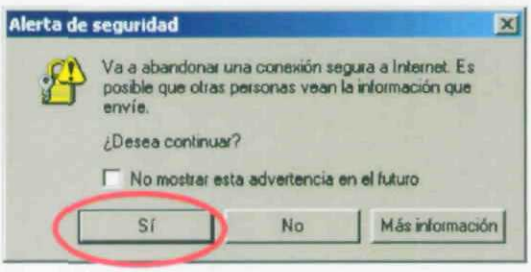
1. Quan es sol·licita l'accés al servidor de les votacions pot aparèixer la següent finestra el primer cop que ens connectem. Només indica que estem iniciant una connexió segura. En aquest cas prémer "Continuar"



2. A continuació es demanarà el certificat de votant. Seleccioneu el vostre certificat, apareix identificat amb el vostre nom, i seleccioneu "Aceptar"



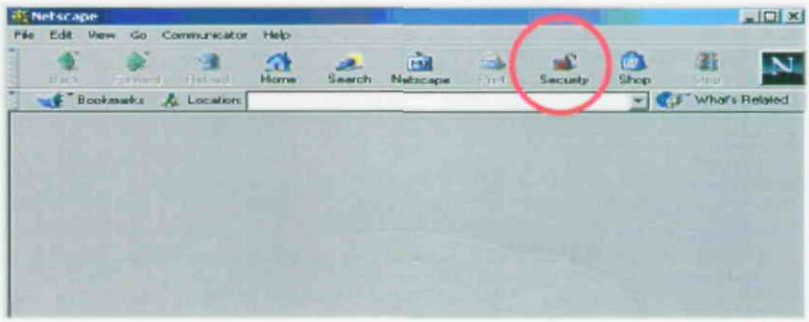
3. Un cop finalitzada la votació, al abandonar el web pot aparèixer la següent finestra. Només ens informa que estem abandonant la connexió segura. Prémer "Si" per continuar



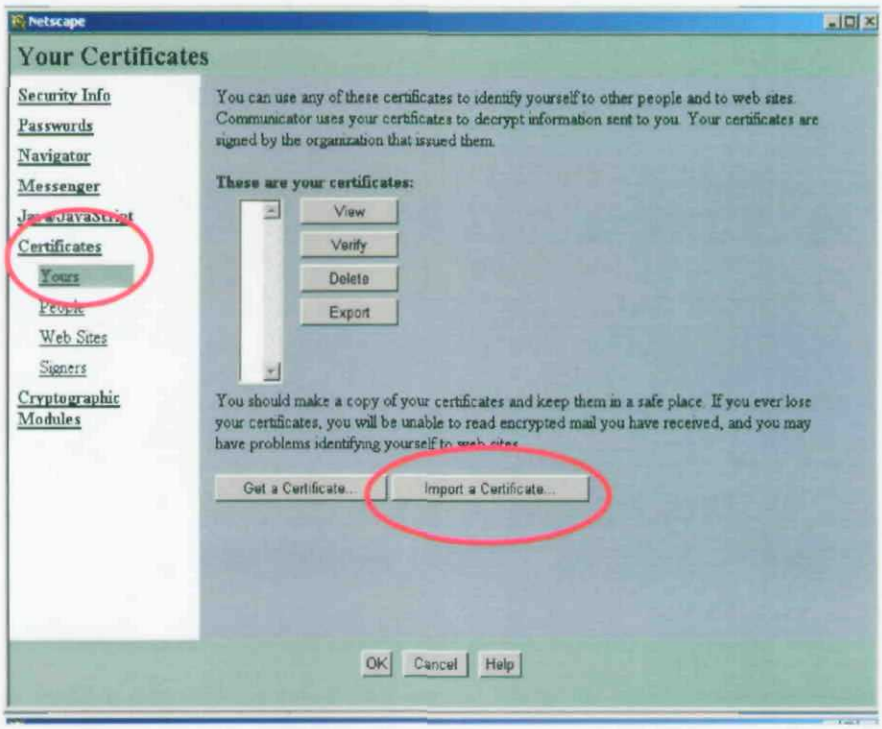
INSTAL·LACIÓ DEL CERTIFICAT PER A NETSCAPE COMMUNICATOR

Per instal·lar els certificats del pilot a un navegador Netscape Communicator cal que aquest sigui de la versió 4.7 o superior. En cas afirmatiu el passos a seguir serien els següents:

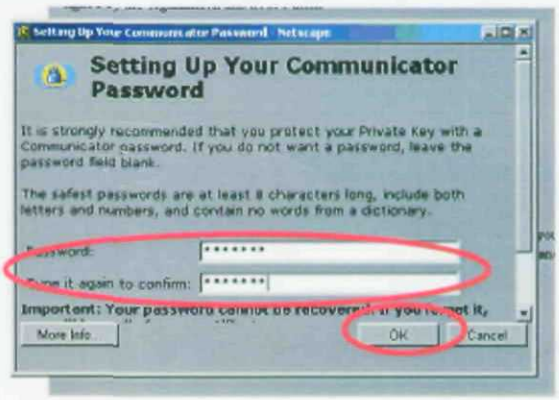
1. Obrir el navegador i prémer al botó "Seguridad"



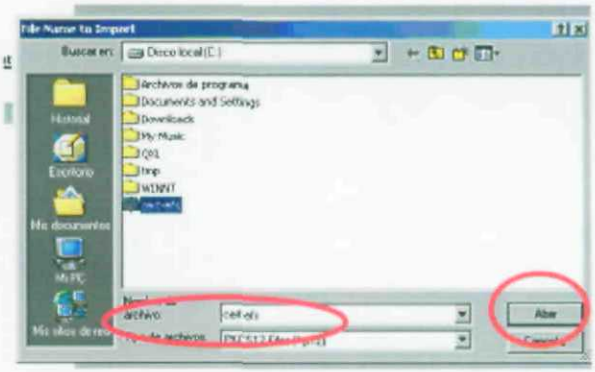
2. Anar a l'opció "Certificados -> Personales". Un cop allí prémer el botó "Importar Certificado"



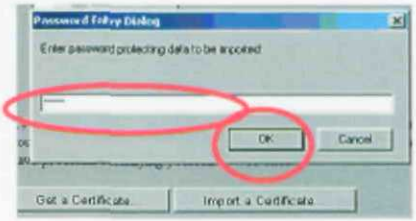
3. A continuació es demanarà una paraula clau. Aquesta és el **password del navegador** i no té res a veure amb el **password del certificat** que acompanya el disquet. Si encara no l'havia configurat, li demanarà que introdueixi una de nova per duplicat. Un cop introduït **el nou password del navegador guardi'l, doncs el tornarà a necessitar en el moment de votar**. Aquesta paraula clau és la que utilitza el propi navegador per protegir el certificat. Per continuar premi "Aceptar".



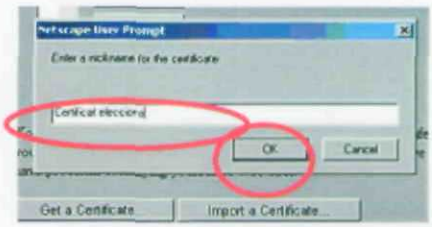
4. La següent finestra demanarà la ruta del vostre certificat. Introduir el disquet que conté el certificat a la disquetera, a "Nombre de archivo" especifiqueu A:\cert.p12 i a continuació seleccioneu el botó "Abrir"



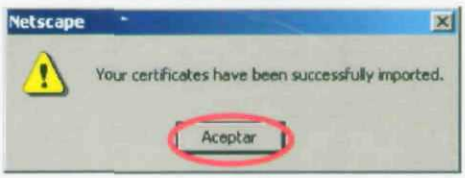
5. Introduir el **password del certificat** (lliurat amb el document que acompanya al disquet) i prémer "Acceptar".



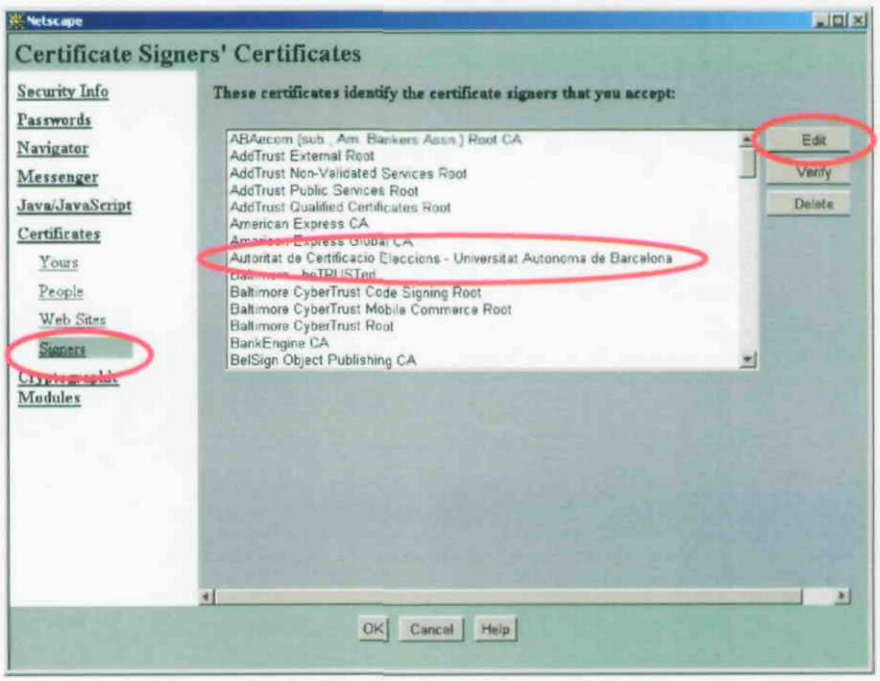
6. Donar un nom identificatiu en el certificat. Aquest és el nom intern que utilitzarà el navegador per identificar-lo. Es recomana posar "Votacio UAB 2002". Després prémer "Aceptar".



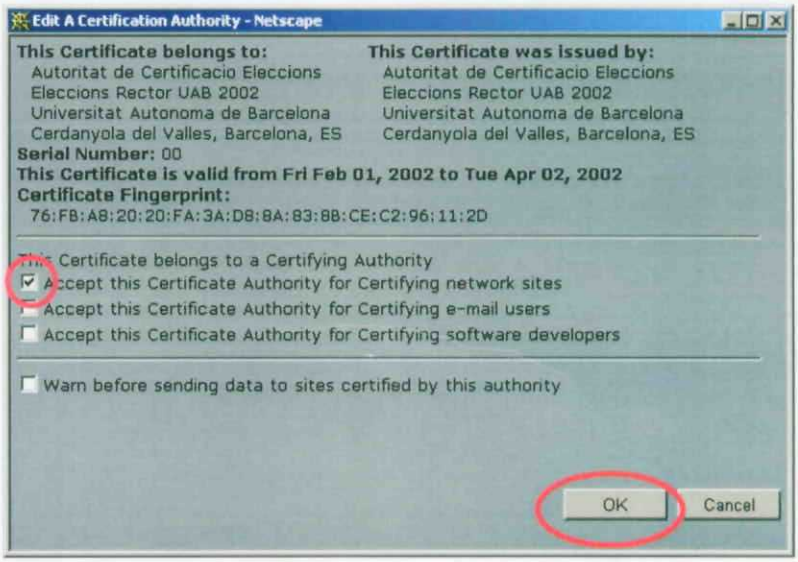
7. El certificat ha estat importat correctament i ja pot ser utilitzat pel navegador. Prémer "Aceptar".



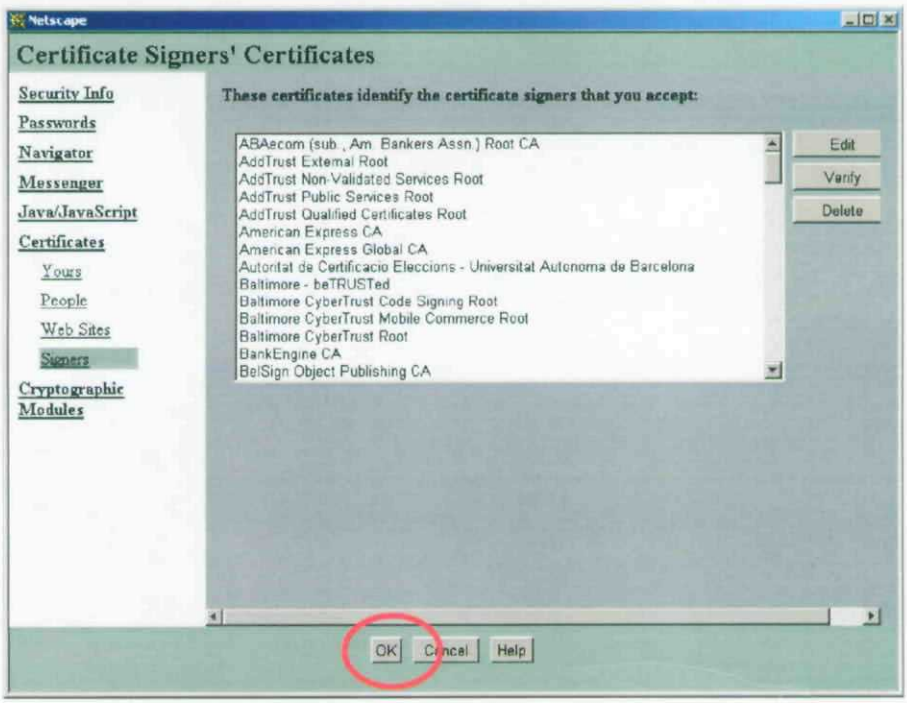
8. Anar a l'opció "Certificados -> Signers". Un cop allí seleccioneu de la llista la opció "Autoritat de Certificacio Eleccions – Universitat Autonoma de Barcelona " i després prémer el botó "Editar"



9. Seleccioneu la opció "Aceptar esta Autoridad de Certificación para certificar sitios de red". Un cop seleccionada prèmer el botó "Aceptar".



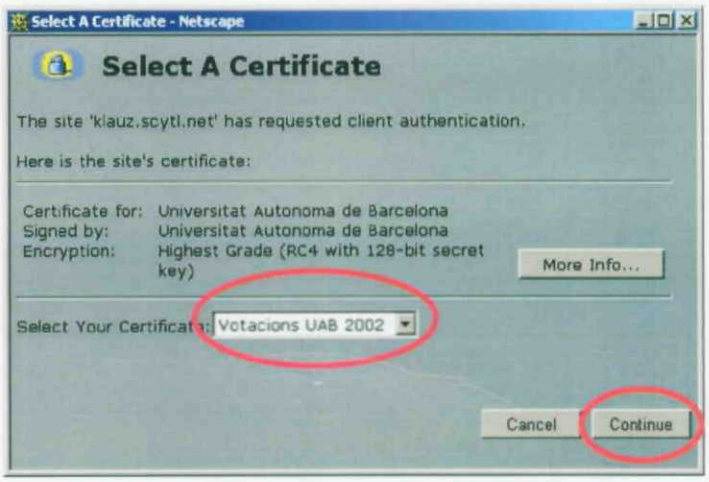
10. Prémer "Aceptar" per tancar la finestra de gestió de certificats.



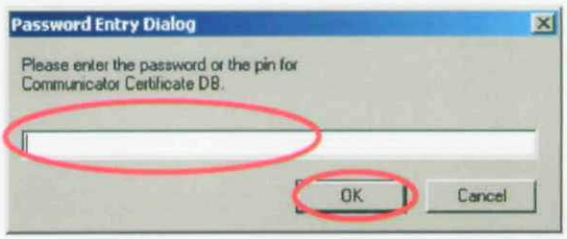
FUNCIONAMENT DELS CERTIFICATS DURANT LES VOTACIONS. VERSIÓ NETSCAPE COMMUNICATOR

Un cop instal·lats els certificats al navegador de Netscape ja es poden utilitzar per a la identificació en les votacions. La seqüència de finestres que apareixen quan es demana el certificat de votant és la següent:

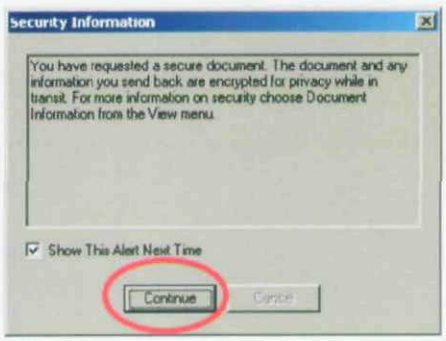
1. Quan es sol·licita l'accés al servidor de les votacions es demanarà el certificat de votant. En la finestra que apareix a continuació seleccionar el certificat (és el nom especificat en el punt 6 de la guia d'instal·lació). Un cop seleccionat prémer "Continuar".



2. A continuació es demanarà el **password del navegador**. Aquest password és el que es va introduir en el **pas 3 de la guia d'instal·lació del certificat per a Netscape**. Un cop introduït el **password del navegador** prémer "Aceptar"

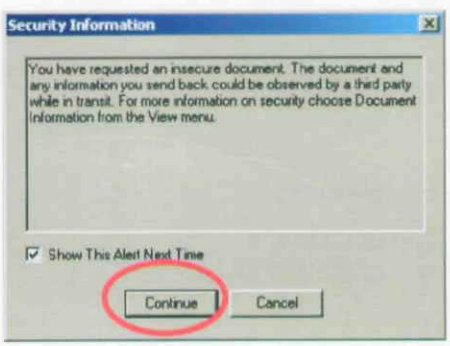


3. La finestra que surt a continuació pot apareixer el primer cop que ens connectem a un lloc segur. En aquest cas prémer "Continuar"



4. El pas 1 es repetirà cada cop que sigui necessària la autentificació de la connexió (depèn de la versió del navegador).

5. Quan abandonem el web de votacions pot aparèixer la següent finestra per avisar-nos. En aquest cas prémer "Continuar"



Benvolguda professora/Benvolgut professor,

Com ja saps, el proper dia 7 de març, dijous, es celebraran les eleccions de rector de la Universitat Autònoma de Barcelona.

Els experts en qüestions electorals ens avisen que d'aquí a poc temps algunes eleccions podrien començar-se a celebrar en suport electrònic i no amb paperetes com fins ara. Les oportunitats que ens ofereixen les xarxes informàtiques als centres universitaris converteixen l'elecció de rector/a en una ocasió ideal per a incorporar aquesta tecnologia. Per tot això, la Secretaria General de la UAB i el Deganat de la Facultat hem decidit realitzar una prova experimental de votació electrònica, coincidint amb l'elecció del 7 de març, entre els professors funcionaris doctors (Sector A) de la nostra Facultat.

Per a dur a terme la prova pilot, els professors funcionaris doctors, a més de votar -com la resta del cos electoral de la UAB- en urnes convencionals, tindreu l'oportunitat de votar una segona vegada en una plana web preparada per a aquest efecte.

És important destacar alguns aspectes relacionats amb aquesta prova pilot. El primer és precisament que és experimental i, per tant, no vinculant. Només els vots emesos a l'urna convencional entraran en el recompte oficial. Els vots emesos a la plana web tindran el valor de posar a prova un important instrument per al futur. El segon és que ens hem assegurat que es tracti d'un mecanisme extremadament segur: només els individus autoritzats a fer-ho podran votar i el contingut del seu vot serà totalment anònim. Un grup d'experts de sòlid prestigi internacional està treballant per a garantir aquestes condicions d'extrema seguretat.

Properament el Deganat de la Facultat es posarà en contacte per a explicar-vos el sistema de votació, particularment els mecanismes que en garanteixen la seguretat.

El degà de la Facultat i el secretari general de la Universitat us animem que participeu en aquest projecte, utilitzant el mecanisme de votació electrònica que l'equip d'experts ha preparat. Us preguem que participeu en aquesta experiència i que ens feu saber la vostra opinió sobre el seu funcionament. Que quan arribi el futur estiguem preparats depèn, en part, del fet que el mecanisme s'hagi posat a prova experimentalment i ens haguem pogut anticipar als errors. La vostra participació serà, doncs, fonamental.

Rebeu una salutació ben cordial.

Fausto Miguélez
Degà de la Facultat de C. Polítiques i de Sociologia

Enric Marín
Secretari general de la UAB

Bellaterra (Cerdanyola del Vallès), 11 de febrer de 2002