PRESENTACIÓ VOTACIONS ELECTRÒNIQUES
SISTEMA INFORMÀTIC ELECTORAL

DOCUMENT INFORMATIU CU 6/11 2008

Direcció Informàtica

27 de novembre de 2008

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Votacions electròniques

sistema informàtic electoral

Novembre
2008

Origen i desenvolupament (1)

UNIVERSITAT POLITÈCNICA DE CATALUNYA

El Departament de TSC ha treballat internament un model tecnològic de vot electrònic.

Es detecta que manca una regulació normativa i que cal donar garanties al model TIC

La Direcció Informàtica i UPCnet:

- Avaluen la viabilitat TIC del vot telemàtic.
- Defineixen el model tecnològic que ha de donar suport a les votacions electròniques.
- Analitzen diferents eines de vot telemàtic.

Origen i desenvolupament (2)

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Catedràtics experts de la UPC que col·laboren amb el projecte:

Dr. Miquel Soriano

Director del Departament d'Enginyeria Telemàtica.

La seva àrea de recerca se centra en la seguretat en xarxes, comerç electrònic i protecció del copyright.

Dr. Manel Medina

Director del esCERT (Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas).

La seva àrea de recerca se centra en la seguretat informàtica.

La Secretaria General, el Gabinet Jurídic i la Comissió de Reglaments:

- Elaboren el protocol per a la regulació del vot electrònic remot en les eleccions al Claustre Universitari 2008 (prova pilot).
- Elaboren la proposta de modificació de la NORMATIVA D'ELECCIONS AL CLAUSTRE UNIVERSITARI relativa a les votacions electròniques

Prova pilot i difusió

UNIVERSITAT POLITÈCNICA DE CATALUNYA

normativa tecnologia

PROVA PILOT (ETSECCPB)

Secretaris de Departaments (20/5/08)
Secretaris de Centres (21/5/08)
Comissió de Reglaments (6/6/08)
Comissió Permanent del Consell de Govern (16/7/08)
Reunió a l'ETSECCPB (25/9/08)
Prova pilot de vot electrònic a l'ETSECCPB (22/10/08)

VOTACIONS ELECTRÒNIQUES

Presentació a càrrecs de 1r nivell (22/7/08)
Reunió de Secretaris (16/9/08)
Demo tecnológica JEU, CR, MPCU (29/10/08)
Comissió de Reglaments (30/10/08)

Actuacions de futur

UNIVERSITAT POLITÈCNICA DE CATALUNYA

- **Proves pilot en processos electorals a diferents UUBB sense validesa legal:**
  Ens permetrà continuar validant l'aplicatiu i el procediment de votacions electròniques.

- **Propera convocatòria d'eleccions per a la renovació total del Claustre Universitari 2009:**
  Possible aplicació de la Disposició Addicional 4 de la normativa reguladora de les votacions electròniques.

Infraestructura associada (1)

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Nou carnet Universitari UPC.
El nou carnet universitari està dotat d'un xip criptogràfic que permet gravar el certificat digital de signatura reconeguda del CATCert.

Carnet intel·ligent.
- Memòria i processador en el mateix xip
- Identificació per número de sèrie únic i permanent
- Protecció de lectura i escriptura del xip mitjançant un PIN
- Capacitats criptogràfiques
- Informació intercanviada mitjançant protocol APDU (Application Protocol Data Unit). ISO 7816-4

Real Casa de la Moneda
Fábrica Nacional de Moneda y Timbre

gemalto
security to be free
The World Leader in Digital Security

Infraestructura associada (2)

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Certificat Digital

- Certificat Personal d'Identificació i Signatura Reconeguda (CPISR)
- Certificat Personal de Xifrat (CPX)

Un certificat digital és un document electrònic signat per una autoritat de certificació, que identifica a la persona que el posseeix com a membre de la comunitat universitària de la UPC en qualitat de PDI o PAS o estudiant/a, i que conté les dades relacionades amb ella, com ara, les autoritzacions i accessos dels que gaudeix, els serveis als que pot accedir, etc.

Els certificats personals de la UPC continguts en el xip criptogràfic del carnet universitari, generen signatura reconeguda, el nivell més alt de seguretat i equiparable a la signatura manuscrita.

CATCert Agència Catalana de Certificació

Infraestructura associada (3)

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Entitats de registre UPC.

La UPC es constitueix en entitat de registre per tal d'expedir el certificat digital de la UPC a tots els membres de la comunitat Universitària.

La 1ª Entitat de registre de la UPC es formalitza a l'**Univers (Serveis d'activitats socials)** al Campus Nord (edifici C6 planta 0)

- tramiten sol·licituds de certificats
- realitzen la comprovació de la identitat del peticionari personalment
- generen la petició definitiva del certificat
- graven el certificat en el carnet universitari
- enregistren i emeten una justificació acreditativa

Requeriments del programari de votació electrònica

És imprescindible dotar tot el procés de les garanties necessàries per assolir els objectius de seguretat, fiabilitat, transparència i disponibilitat.

Requeriments:

- Autentificació.
- Anonimat.
- Fiabilitat.
- Neutralitat.
- Possibilitat de verificació: individual i general.
- Control del sistema: certificabilitat i auditabilitat.

Requeriments de servei

- Prestació del servei d'urna electrònica per una entitat que no participa en el procés electoral.
- Establir acords de nivells de servei, seguretat i confidencialitat

Requeriments de seguretat tecnològics

- Protocols de transmissió segurs.
- Seguretat d'accés a la infraestructura tecnològica
- Fiabilitat tecnològica. Sistemes a prova de fallides

Requeriments de seguretat de l'urna electrònica

- Seguretat criptogràfica de l'urna i del procés electoral.
- Impossibilitat de relacionar un vot amb un elector/a.
- Eines per identificar si hi ha pèrdua de confidencialitat del procés

Votacions electròniques

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Mesa electoral

- Creació de les claus criptogràfiques
- Custòdia de la clau de desxifratge

Votacions

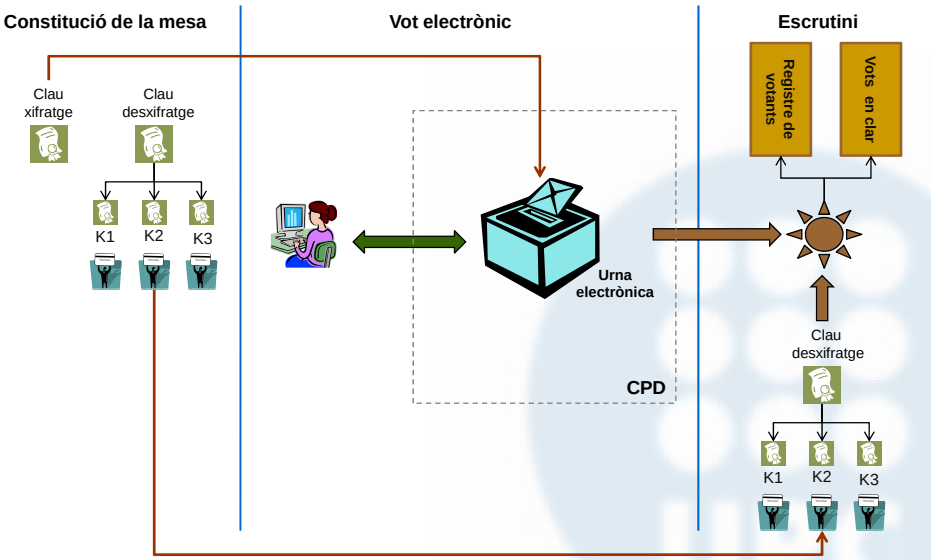
- Vot electrònic a través d'Internet

Escrutini

- Recomposició de la clau desxifratge
- Escrutini de vots

Votacions electròniques

UNIVERSITAT POLITÈCNICA DE CATALUNYA



Votacions electròniques

UNIVERSITAT POLITÈCNICA DE CATALUNYA

La mesa electoral

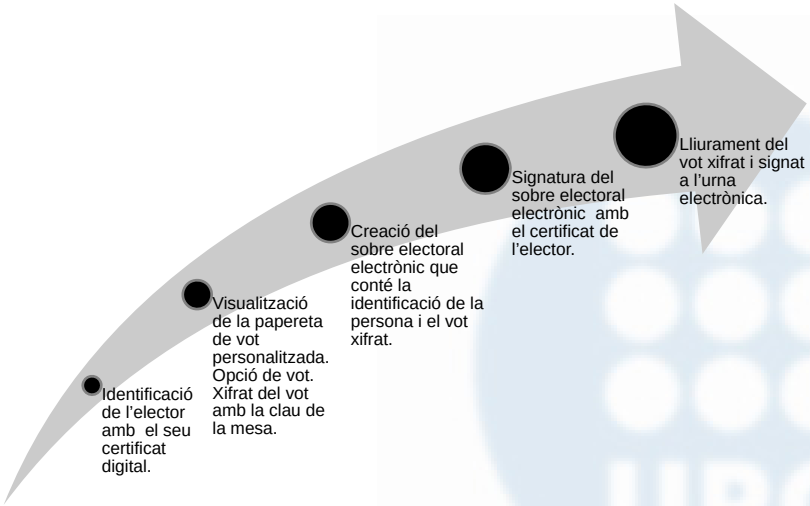
Creació de la clau de xifratge. La clau s'ubica dins de l'urna electrònica i es posa a disposició dels electors per xifrar el vot.

Creació de la clau de desxifratge. La clau només existeix en memòria de forma temporal, es divideix en tantes parts com membres de la Mesa electrònica hi ha, i es reparteix entre aquests dins les targetes criptogràfiques que els hi són lliurades. Serveix per obrir la urna al finalitzar les eleccions

Votacions electròniques

UNIVERSITAT POLITÈCNICA DE CATALUNYA

El vot electrònic



Votacions electròniques

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Escrutini

Recomposició de la clau de desxifratge. La clau es reconstrueix quan es reuneix la Mesa electoral i només existeix en memòria mentre dura l'escrutini.

Mixing. El mixing és la tècnica que mitjançant algorismes criptogràfics trenca la correlació temporal dels vots i la relació entre l'elector/a i el seu vot.

Escrutini. És la darrera acció que es realitza i comptabilitza els vots un cop finalitzades les dues fases anteriors.

Conclusions

UNIVERSITAT POLITÈCNICA DE CATALUNYA

El procés electoral acompleix els requeriments:

- Autentificació dels usuaris mitjançant certificat digital: carnet de la Universitat, DNI, IdCAT i altres certificats validats pel CATCert.
- Anonimat del vot: els vots es mantenen secrets durant tot el procés electoral i en cap moment es pot relacionar la identitat del votant amb el seu vot.
- Fiabilitat: la infraestructura tecnològica és d'alta disponibilitat i garanteix que el seu funcionament 24x7. Hi ha certesa que els vots es dipositen a la urna.
- Neutralitat: La plataforma de vot s'ha d'ubicar de manera que no resulti afectada pel procés electoral.
- Possibilitat de verificació, individual i general: durant tot el procés de votació sempre es pot auditar el nivell de participació, però no es pot accedir al vot.
- Control del sistema: certificabilitat i auditabilitat.