ALLEGATO 1

Schema di candidatura

UNIVERSITA' DEGLI STUDI DI .....

Al Rettore dell'Università
degli Studi .....

OGGETTO: Presentazione di candidatura elezioni C.U.N.

Il sottoscritto .....nato a .....
il..... C.F.....residente a
.....
(professore prima fascia, seconda fascia o ricercatore anche a tempo determinato)
inquadrato nel settore scientifico disciplinare.....
presso la Facoltà di .....
dell'Università degli Studi di .....
a norma dell'Ordinanza ministeriale in data ..... indetta per il rinnovo del Consiglio Universitario Nazionale, presenta la propria candidatura per l'elezione a componente del predetto Consesso per l'area disciplinare n. .....

(firma autenticata dal Rettore)

data

Allegato 2

CINECA

Technical Data Package

Version 1.0

Executive summary

Gennaio 2010

Autore

Francesca Merighi
- CINECA -
Via Magnanelli 6/3
40033 Casalecchio di Reno (BO)
Tel. 051 6171411 , e-mail: f.merighi@cineca.it

Edizione del 30 Gennaio 2010

Scopo del documento

Scopo del presente documento è fornire una panoramica globale sul sistema di voto elettronico u-Vote. Dettagli approfonditi sono disponibili nei documenti che compongono il Technical Data Package.

Sommario

Introduzione

I sistemi di voto elettronico, intesi come qui sistemi di voto che utilizzano dispositivi elettronici almeno nell'espressione della preferenza, possono apportare notevoli vantaggi ai processi elettorali: aiutano ad incrementare l'affluenza alle urne, permettendo di esprimere il voto da luoghi diversi dai tradizionali seggi, e generano un considerevole risparmio di tempo e denaro.

Per rispondere ad una precisa esigenza del Ministero dell'Università e della Ricerca, nel 1998 Cineca ha realizzato un sistema di voto telematico che, fino ad oggi, è utilizzato per la composizione delle Commissioni di Valutazione e per l'elezione degli Organi Accademici di alcune Università italiane.

Per risolvere il problema di naturale obsolescenza delle macchine e dell'apparato del sistema di voto telematico, Cineca ha avviato un processo di innovazione tecnologica, il cui risultato è il sistema di voto elettronico u-Vote. u-Vote mantiene le caratteristiche di sicurezza, affidabilità e robustezza del sistema di voto telematico del 1998, introducendo al contempo nuove funzionalità utili ad un corretto e razionale svolgimento del processo elettorale.

u-Vote è stato progettato seguendo i principi esposti nelle raccomandazioni sull'e-voting del Comitato dei Ministri del Consiglio Europeo[1]. Il Comitato ha riunito un gruppo interdisciplinare di specialisti, appartenenti a tutti gli stati membri del Consiglio, con l'obiettivo di analizzare i sistemi di voto elettronico. Il risultato dell'analisi è un insieme di principi e standard tecnologici che si propongono come base di un sistema di voto elettronico democratico, e che sono stati d'ispirazione e riferimento per la progettazione di u-Vote.

[1] *LEGAL, OPERATIONAL AND TECHNICAL STANDARDS FOR E-VOTING, Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum*

Confronto tra u-Vote ed il sistema di voto telematico del 1998

Questo paragrafo descrive le principali innovazioni introdotte in u-Vote rispetto al sistema di voto telematico sviluppato da Cineca nel 1998.

Uno dei maggiori benefici apportati dal nuovo sistema è quello di consentire l'espressione delle preferenze, sia da classici seggi elettorali, con stazioni di voto dedicate, che da chioschi. I chioschi sono luoghi pubblici supervisionati in cui sono presenti dei pc general purpose, collegati in rete, che espletano la funzione di stazioni di voto.

L'utilizzo di chioschi ha richiesto un adattamento dell'architettura del sistema rispetto al precedente.

u-Vote mantiene la struttura di sistema distribuito, apportando però cambiamenti all'architettura di rete. Mentre nel sistema del 1998 i server centrali sono raggiungibili solo attraverso una rete privata ISDN, u-Vote offre anche una connettività VPN su rete pubblica.

L'introduzione dei chioschi ha richiesto anche significativi cambiamenti al protocollo di voto: se nel sistema del 1998 la scheda elettorale votata è firmata dalla stazione di voto, nel sistema u-Vote la scheda è firmata da un componente server chiamato Ufficio Elettorale Centrale, attraverso l'applicazione di uno schema crittografico di firma cieca.

Infine la disponibilità di chioschi influisce anche sulla progettazione dei client di voto: nel sistema del 1998 il software per l'espressione delle preferenze è eseguibile solo sulle stazioni di seggio, mentre nel sistema u-Vote il client di voto è eseguibile su qualsiasi macchina dotata di sistema operativo Windows, Linux o Mac OSx.

Alla già usata autenticazione con username e password, distribuiti all'elettore nel seggio elettorale, u-Vote affianca un altro metodo di autenticazione. Nei seggi o chioschi è presente una stazione di controllo, attraverso la quale un ufficiale elettorale abilita a votare l'elettore collegando la sua identità ad una smartcard inserita in una stazione di voto.

Il sistema u-Vote integra anche un servizio di audit, ossia uno strumento che permette ad un osservatore esterno di verificare il corretto svolgimento del processo elettorale.

Le interfacce utente di u-Vote rispondono ai requisiti di usabilità e sono predisposte per soddisfare i requisiti di accessibilità inclusi nelle raccomandazioni del Comitato Europeo dei Ministri.

	Sistema di voto del 1998	**u-Vote**
Canali di voto	Seggi	Seggi o Chioschi
Rete	ISDN in gruppo chiuso	VPN su rete pubblica
Firma scheda	A carico delle stazioni di voto	A carico di CEO (firma cieca)
Client eseguibile su stazioni diverse da quelle di seggio	No	Si (S.O. Windows, Linux o Mac OSx)
Autenticazione dell' elettore	Username e password	Username e password o smartcard di seggio
Applicazioni lato server	ANSI C (moduli di apache)	Java (applicazioni di Tomcat)
Applicazioni lato client	Java 1.1	Java 1.6 o superiore
Sistema di Audit	Non presente	Presente
Rispondenza ai requisiti di usabilità	Parziale	Totale
Rispondenza ai requisiti di accessibilità	Nessuna	Presente la predisposizione (in corso di studio)

I canali di voto

Il sistema u-Vote supporta i seguenti canali di voto, intesi come modalità di espletamento delle operazioni di voto.

Voto in seggio elettorale o Pool Site Voting (PSVC)

L'elettore esprime la preferenza attraverso stazioni di voto pubbliche, per le quali integrità e sicurezza di hardware e software sono controllate dal fornitore del sistema di voto. Le stazioni di voto sono connesse unicamente a reti protette ed accedono ai server centrali attraverso un'infrastruttura di rete sicura ed autenticata, tipicamente una rete privata virtuale o Virtual Private Network (VPN). Le stazioni di voto sono disposte in un ambiente fisico supervisionato chiamato seggio elettorale. Nel seggio elettorale può essere presente anche una stazione di controllo. L'ufficiale elettorale locale sorveglia il seggio assicurando la segretezza del voto e l'integrità della dotazione elettorale, e controlla lo svolgimento dell'evento elettorale attraverso la stazione di controllo. L'ufficiale ha anche il compito di identificare a vista l'elettore ed eventualmente abilitarlo al voto, consegnandogli le credenziali di accesso al sistema. L'elettore può avere o meno un seggio a lui assegnato.

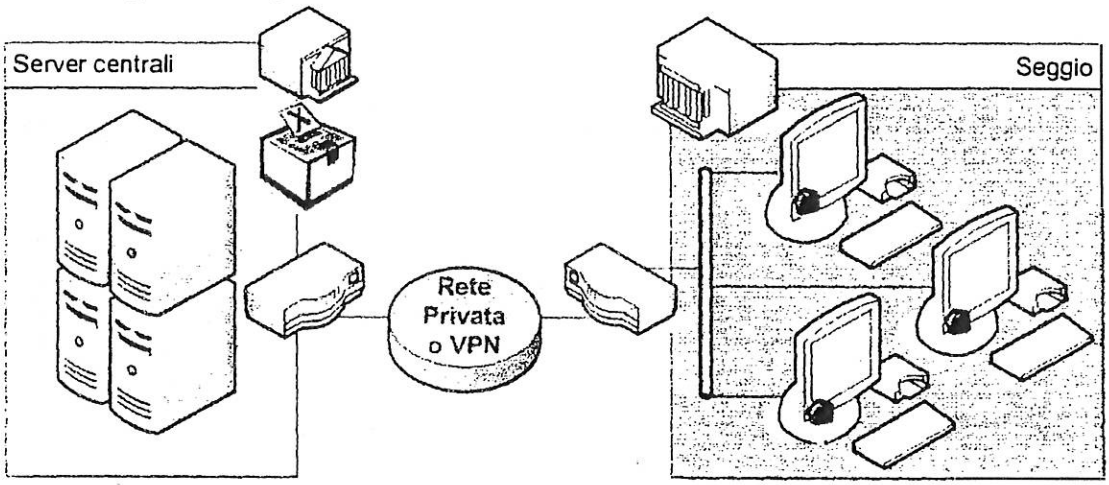


Figura 1: Voto in seggio

Voto remoto in chiosco o Kiosk Voting (KVC)

L'elettore esprime la preferenza attraverso stazioni di voto pubbliche per le quali l'integrità e sicurezza di hardware e software NON sono state controllate dal fornitore del sistema di voto. Le stazioni di voto possono essere collegate a reti pubbliche protette ma anche non protette. L'ambiente fisico in cui sono disposte le stazioni di voto, chiamato chiosco, è supervisionato: è presente un ufficiale elettorale locale che protegge la segretezza del voto e l'integrità della dotazione elettorale, ha il compito di identificare a vista l'elettore ed eventualmente abilitarlo al voto, consegnadogli le credenziali di accesso al sistema. L'elettore può avere o meno un chiosco a lui assegnato.

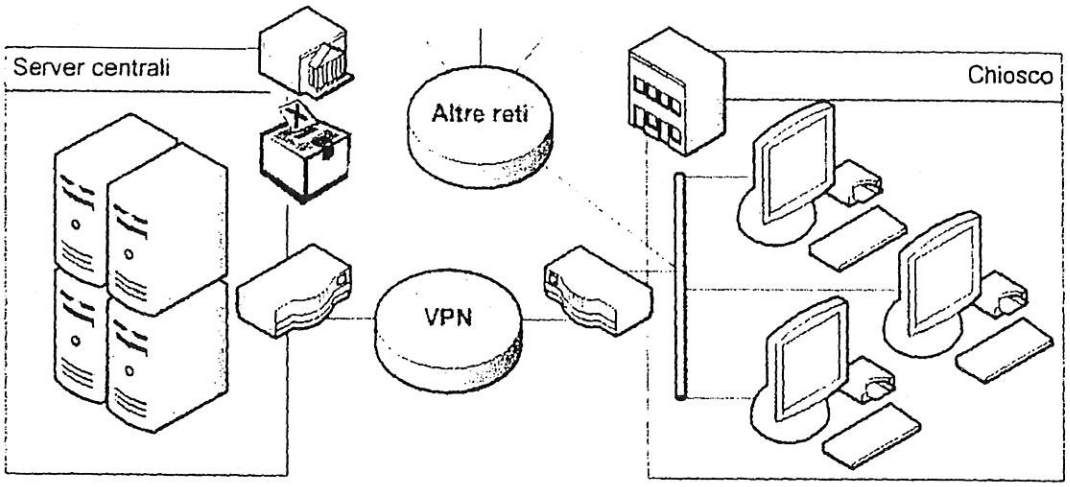


Figura 2: Voto in chiosco

Autenticazione dell'elettore

Per poter procedere all'espressione della preferenza l'elettore deve autenticarsi presso il sistema di voto elettronico, cioè deve dare al sistema delle credenziali che lo identifichino univocamente. Queste credenziali possono essere fornite attraverso diverse modalità di autenticazione:

- **Autenticazione con username e password.** All'elettore viene fornito un nome utente o username univoco ed una password ad esso associata. Username e password possono essere contenuti in un certificato cartaceo distribuito dall'ufficiale elettorale locale dopo l'identificazione a vista dell'elettore, oppure attraverso altri canali prima dell'apertura dell'evento elettorale. Per autenticarsi, l'elettore inserisce username e password nella stazione di voto.
- **Autenticazione con smartcard di seggio.** Ogni seggio è dotato di alcune smartcard di servizio con un certificato digitale per l'autenticazione, almeno una per ogni stazione di voto. L'ufficiale elettorale identifica a vista l'elettore e attraverso la stazione di controllo associa la sua identità al certificato digitale di una delle smartcard di seggio non utilizzate in quel momento. Consegna la smartcard all'elettore che la utilizza per autenticarsi al sistema attraverso la stazione di voto.

Protocolli di voto, scrutinio e verifica

Si consideri una semplificazione del modello del sistema di voto, composta dai seguenti elementi:

- un elettore (***Voter i***), una persona fisica con diritto di voto, identificata da un identificativo univoco ID_i;
- un Ufficio Elettorale Centrale (*Central Election Office*, ***CEO***), un sistema elettronico che distribuisce le schede da votare agli elettori e firma le schede votate e blindate utilizzando una coppia di chiavi asimmetriche (sk_{CEO}, pk_{CEO});
- un' Urna Centrale (*Central Ballot Box*, ***CBB***), un sistema elettronico che raccoglie le schede votate e cifrate e le rende disponibili alle operazioni di scrutinio;
- uno scrutinatore (*Counter*, ***C***), una persona fisica preposta allo scrutinio dei voti, dotata di una coppia di chiavi asimmetriche (sk_C, pk_C) per decifrare i voti presenti nell'urna;
- un Servizio di Audit, un sistema elettronico preposto alla verifica del corretto svolgimento del processo elettorale.

Protocollo di voto

L'elettore si autentica presso CEO. Se non risulta avere diritto di voto, CEO respinge la richiesta dell'elettore, altrimenti gli invia la scheda elettorale da votare.

Sia v_i la scheda elettorale votata dall'elettore. L'elettore applica il cifrario ibrido alla scheda votata v_i ottenendo una chiave simmetrica cifrata q_i e una scheda cifrata x_i e inserisce entrambi in un involucro che chiameremo genericamente scheda cifrata. L'elettore esegue l'operazione di blindatura sulla scheda cifrata ottenendo la scheda cifrata blindata e_i e la invia a CEO affinché venga firmata.

Per introdurre un alias all'identità dell'elettore, viene utilizzato il protocollo di Arto Salomaa, come descritto in seguito.

Se l'elettore ha diritto di voto, CEO sceglie casualmente un numero di validazione vn_i e lo associa all'identità dell'elettore ID_i. Successivamente invia il numero di validazione vn_i a CBB, che memorizza il numero in una lista. CEO firma la scheda blindata ottenendo d_i e la rinvia all'elettore assieme al numero di validazione vn_i.

L'elettore applica l'operazione di sblindatura alla scheda blindata e firmata, ottenendo in questo modo la scheda cifrata e firmata y_i, che invia a CBB insieme al numero di validazione vn_i.

Se CBB trova nella lista il numero di validazione ricevuto, allora registra la scheda cifrata e firmata, elimina il numero di validazione dalla lista, segnala a CEO che l'elettore relativo al numero di validazione vn_i ha votato, e dà conferma all'elettore dell'inserimento della scheda nell'urna.

CEO registra che l'elettore ID_i, corrispondente al numero di validazione vn_i, ha votato.

Il numero di validazione opera come un codice di autorizzazione ad inserire il voto nell'urna, allo stesso tempo protegge la segretezza del voto operando come un alias all'identità del votante: CBB non può collegare il voto all'elettore che lo ha espresso perché non conosce l'associazione fatta da CEO tra il numero di validazione e l'identità dell'elettore.

$\xi_k(m)$: Schema di cifratura simmetrica sul messaggio m con chiave k.

$\xi_i^{-1}(c)$: Schema di decifratura simmetrica sul messaggio cifrato c con chiave k.

$\varepsilon_{pk}(m)$: Schema di cifratura asimmetrica sul messaggio m con chiave pubblica pk.

$\varepsilon_{sk}^{-1}(c)$: Schema di decifratura asimmetrica sul messaggio cifrato c con chiave privata sk.

$\sigma_{sk}(m)$: Schema di firma sul messaggio m con chiave privata sk.

$v_{pk}(s,m)$: Schema di verifica della firma su un messaggio m e sul corrispondente messaggio firmato s, con la chiave pubblica pk.

$\beta_{pk}(m,r)$: Primitiva di blindatura per il messaggio m e il numero casuale r, attraverso la chiave pubblica pk.

$\psi_{pk}(b,r)$: Primitiva di recupero della firma cieca per il messaggio blindato b e il numero casuale r, utilizzando la chiave pubblica pk.

Errore. Non è stato specificato un argomento.

Figura 3: il protocollo di voto

Protocollo di scrutinio

Lo scrutinatore accede a CEO e CBB e controlla che il numero di schede nell'urna corrisponda al numero di elettori che hanno esercitato il diritto di voto.

Lo scrutinatore verifica la firma di CEO sulle schede votate, decifra la chiave simmetrica utilizzando la chiave privata in suo possesso, attraverso la chiave simmetrica decifra la scheda votata e procede al suo conteggio. Infine autorizza la pubblicazione dei risultati.

Errore. Non è stato specificato un argomento.

Figura 4: Il protocollo di scrutinio

Protocollo di verifica

Il Servizio di Audit ha il compito di controllare la correttezza dello svolgimento del processo di voto e scrutinio. In particolare controlla che i voti nell'urna siano autentici verificando la firma di CEO, controlla che nell'urna non ci siano schede duplicate, controlla che il numero delle schede votate corrisponda al numero di elettori che hanno esercitato il diritto di voto. Inoltre il Servizio di Audit è in grado di effettuare una verifica incrociata della correttezza dello scrutinio. Al termine del conteggio dei voti lo scrutinatore mette a disposizione del Servizio di Audit le chiavi simmetriche, decifrate attraverso la sua chiave privata, in modo che esso possa procedere ad un riconteggio dei voti.

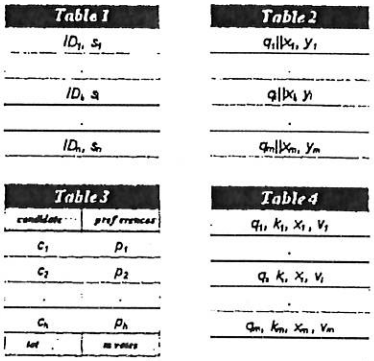
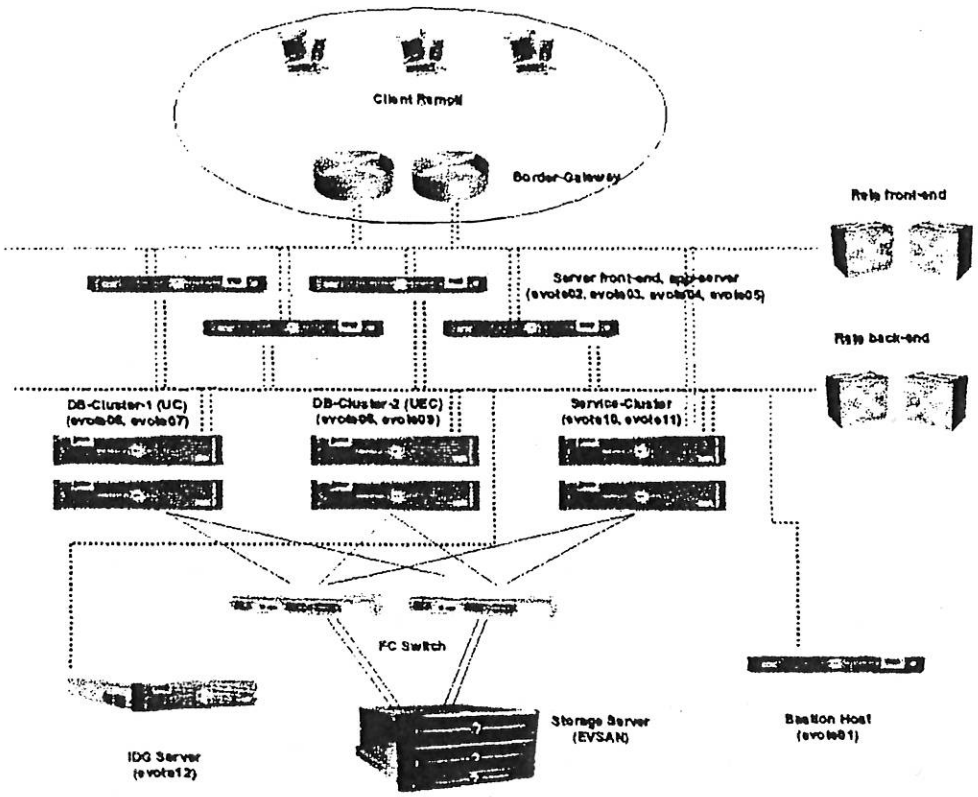


Figura 5: risorse disponibili al Servizio di Audit

Architettura hardware e di rete

Si riporta schematicamente in figura l'infrastruttura generale del sistema u-Vote



I componenti del sistema u-Vote sono:

- 2 cluster HA, composti da 2 host ciascuno, che erogano il DB Oracle (DB-Cluster-x),
- 1 cluster HA composto da 2 host per l'erogazione di servizi di supporto (Service-Cluster),
- 4 host di front end, costituiti da macchine stand alone,
- 1 bastion host, macchina stand alone,
- 1 server di management, macchina standalone (IDG),
- 1 storage server (EVSAN),
- 2 router CISCO con terminazioni ISDN e VPN,
- altri apparati di supporto.

Architettura hardware lato server

L'architettura hardware lato server è progettata per garantire sicurezza e affidabilità.

Entrambi i DB-Cluster (composti da sistemi DELL PE2950-III in configurazione ad alta affidabilità) ospitano un' istanza Oracle release 11g R1, con character set AL32UTF8.

La business continuity dei due database in configurazione single-instance (non Parallel), è gestita dal software di cluster che identifica le eventuali malfunzioni ed effettua la transizione del database da un nodo all'altro mediante **Heartbeat v2**. La configurazione proposta è quella presente su tutte le istanze Oracle in produzione al CINECA ed è in grado di assicurare i massimi livelli di servizio.

Il cluster **Service-Cluster** è costituito anch'esso da due host in HA ed eroga i servizi Radius, DNS, DHCP, NTP.

Gli host di frontend sono sostanzialmente dei web server che ospitano Apache 2.2.13 e Tomcat 6.0.20 esponendo i servizi dell'Ufficio Elettorale e dell'Urna.

Il bastion host è il server di frontiera tra la rete CINECA e quella interna di u-Vote, permette il soddisfacimento dei requisiti di monitoraggio ed assicura l'effettivo isolamento delle macchine.

Il server IDG ospita il software di gestione delle macchine, utilizzato sia per l'installazione che per la configurazione.

I sistemi DB, sono collegati allo storage server dedicato al sistema u-Vote mediante connessioni **FibreChannel utilizzando cammini multipli** verso un sistema dischi in grado di gestire al meglio la fault tolerance.

Architettura hardware lato client

Le stazioni di voto di seggio possono essere costituite o da una macchina fisica completa, dotata di tutte le periferiche di input/output, oppure da una chiave USB, contenente un sistema operativo preconfigurato di sola lettura, che è possibile avviare attraverso un generico pc che carica la chiave USB al boot.

Le stazioni di voto di seggio complete sono costituite da thin client con architettura X86 privi di memoria di massa (hard disk) per limitare le possibilità di danneggiamento in caso di interruzioni di corrente o di altro tipo di incidente.

Le chiavette USB sono invece dotate di memoria flash e di un lettore di smartcard ACR38U in formato SIM. Sulla memoria flash di tali chiavette viene realizzata una partizione protetta in scrittura contenente la stessa immagine del sistema operativo installato sui thin client, mentre nel lettore SIM viene installato il solo chip della stessa smartcard InCard InCrypto34V2 CNS altrimenti utilizzata nel suo formato integrale.

Nei chioschi le stazioni di voto sono costituite da pc general purpose, con sistema operativo Windows, Linux o Mac OSx, messi a disposizione da terze parti. La sicurezza e l'integrità dei pc è totalmente demandata al loro fornitore. Tuttavia Cineca distribuisce delle "best practices" sulla protezione dei pc dalle minacce esterne ed interne, seguendo le quali il fornitore dei pc può essere ragionevolmente sicuro che le macchine rispondano ai requisiti di integrità richiesti.

Le smartcard

Le smartcard attualmente in uso sono InCard InCrypto34V2 CNS. Si tratta di un modello di smartcard crittografica capace di utilizzare chiavi RSA a 1024 bit, su cui è possibile installare certificati di Firma Digitale e autenticazione emessi da Certificatori accreditati CNIPA.

Rete ISDN

Le stazioni di voto accedono ai server centrali attraverso borchie ISDN appartenenti ad un CUG (Close User Group) dedicato ad u-Vote, soluzione che impedisce in tal modo l'accesso al sistema dalla rete telefonica pubblica.

Ogni seggio è dotato di un router ISDN opportunamente configurato e dotato di uno switch a 4 porte ethernet 10/100 per consentire il collegamento delle postazioni di voto.

Rete VPN

In maniera del tutto analoga alla soluzione ISDN, ai concentratori VPN sui router del sistema u-Vote corrisponderanno dei router VPN preconfigurati e distribuiti ad ogni seggio che opti per questo tipo di connettività.

Anche i router VPN sono dotati di switch 4 porte ethernet 10/100 per consentire la realizzazione della LAN su cui attestare le postazioni di voto.

Architettura software

Il sistema u-Vote è formato da vari componenti software lato client e lato server.

I client (di voto e scrutinio) che compongono il sistema u-Vote sono scritti in linguaggio Java. A seconda del loro utilizzo in seggio o nel computer dell'utente, assumono la forma di applicazioni o applet. Un'applicazione Java è un programma residente sulla macchina, lanciato attraverso linea di comando, che può essere eseguito direttamente dalla Java Virtual Machine senza necessità di un container. Diversamente l'applet è un programma che viene eseguito come "ospite" nel contesto di un altro programma, detto appunto container, che tipicamente e nel caso di u-Vote è un browser web. Generalmente l'applet non risiede sulla macchina client ma viene automaticamente scaricata dalla rete all'atto della chiamata. Per merito delle caratteristiche di portabilità del linguaggio Java, i client di voto e scrutinio possono essere eseguiti su qualsiasi sistema operativo che installi una Java Virtual Machine 1.6 o superiore.

La maggior parte dei servizi lato server di u-Vote sono costituiti da Servlet ospitate da Apache Tomcat. Apache Tomcat è un web container open source che fornisce una piattaforma per l'esecuzione di applicazioni Web sviluppate nel linguaggio Java. Una servlet è un programma scritto in Java e residente su un server, in grado di gestire le richieste generate da uno o più client, attraverso uno scambio di messaggi tra il server ed i client stessi che hanno effettuato la richiesta. Nel sistema u-Vote la comunicazione servlet-client avviene attraverso lo scambio di messaggi SOAP su un trasporto http o https, ossia le servlet assolvono alla funzione di Web Service.

I componenti lato server di u-Vote utilizzano basi di dati Oracle, un sistema di gestione dati basato sul modello relazionale.

Usabilità e accessibilità delle interfacce utente

Come esposto nelle raccomandazioni del Comitato dei Ministri del Consiglio Europeo, uno dei principi fondamentali che un sistema elettorale deve rispettare è quello del suffragio universale, cioè tutti coloro che hanno diritto al voto devono essere in condizione di poter votare. Il principio di suffragio universale apre dunque la strada all'introduzione di requisiti funzionali di usabilità e accessibilità per i sistemi di voto elettronico. Le *Voluntary Voting System Guidelines* introducono dei requisiti a cui il processo di voto dovrebbe essere conforme al fine di essere usabile ed accessibile a persone disabili, in particolare a persone con disabilità motorie, uditive e visive.

Il sistema u-Vote è disegnato in modo da soddisfare tutti i requisiti di usabilità funzionali, cognitivi, percettivi e di interazione specificati dalle *Voluntary Voting System Guidelines*.

Per quello che riguarda le disabilità motorie, esse riguardano l'organizzazione fisica del seggio elettorale. Il sistema u-Vote fornisce chiare indicazioni a coloro che allestiscono fisicamente il seggio in modo che i requisiti di accessibilità motoria siano rispettati. Il sistema u-Vote non utilizza segnali acustici per comunicare informazioni necessarie alla fase di voto o scrutinio, di conseguenza è totalmente accessibile ai disabili con problemi uditivi.

Nonostante l'utilizzo del linguaggio Java per l'interfacce utente garantisca buona compatibilità con le tecnologie assistive, alla data odierna l'accessibilità del sistema ai disabili non vedenti e ipo vedenti è ancora in corso di studio approfondito. Fino al rilascio di una versione in linea con i requisiti di accessibilità, i non vedenti possono votare unicamente con l'ausilio di un accompagnatore, come nei sistemi di voto cartacei.

Qualità del prodotto

La qualità di un prodotto, intesa come il livello con il quale una entità risponde ai requisiti stabiliti, può essere misurata attraverso un processo di valutazione che prende a modello opportune caratteristiche di qualità. L'ISO[2], in collaborazione con l'IEC[3], mette a disposizione alcune norme sull'argomento, in particolare la ISO/IEC 9126 e la ISO/IEC 14598.

Il processo di valutazione della Qualità di u-Vote si basa sulla norma ISO/IEC 14598 e utilizza come modello di riferimento le caratteristiche di qualità indicate nella norma ISO 9126, ed in particolare un modello di Qualità Esterna ed un modello di Qualità in Uso.

La Qualità Esterna è la totalità delle caratteristiche del prodotto software da un punto di vista esterno, valutate utilizzando metriche esterne durante la conduzione di prove in ambiente simulato, con dati simulati.

La Qualità in Uso è il punto di vista dell'utente sulla qualità del prodotto software quando questo è utilizzato in un ambiente specifico e in uno specifico contesto d'uso. La valutazione della Qualità in Uso prende a riferimento le Elezioni dei Consigli Scientifici dei Gruppi di Ricerca dell' Istituto Nazionale di Alta Matematica (INdAM) svoltesi nell'Ottobre del 2008 attraverso la versione pre-rilascio del sistema u-Vote.

La valutazione della Qualità del Prodotto evidenzia che il sistema possiede le caratteristiche di Qualità Esterna attese e caratteristiche di Qualità in Uso riporta risultati pienamente soddisfacenti.

[2] International Organization for Standardization, http://www.iso.org.

[3] International Electrotechnical Commission, http://www.iec.ch.

Processo di sviluppo del software

Per definire le responsabilità e le modalità operative inerenti il processo di sviluppo del software che compone il sistema di voto elettronico u-Vote si definisce una procedura operativa che si applica alle seguenti attività:

- pianificazione della progettazione e sviluppo,
- analisi dei requisiti del cliente/prodotto,
- progettazione,
- codifica/sviluppo,
- collaudo del sistema,

svolte nell'ambito del gruppo del "voto elettronico" del dipartimento "Sistemi informativi per il MIUR" del Cineca.

ALLEGATO 3

Schema di candidatura

UNIVERSITA' DEGLI STUDI DI .....

Al Rettore dell'Università
degli Studi .....

OGGETTO: Presentazione di candidatura elezioni C.U.N. – Personale tecnico ed amministrativo

Il sottoscritto .....nato a .....
il.....C.F..... residente a
.....
in servizio presso l'Università degli Studi di .....
qualifica.....a norma dell'Ordinanza ministeriale in data ..... indetta per il rinnovo del Consiglio Universitario Nazionale, presenta la propria candidatura per l'elezione a componente del predetto Consesso in rappresentanza del personale tecnico ed amministrativo.

(firma autenticata dal Rettore o dal Direttore Generale)

data