Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Formazione Superiore e per la Ricerca
Direzione Generale per lo Studente, lo Sviluppo e l'Internazionalizzazione della Formazione Superiore

Al Rettore
Università ed Istituzioni Universitarie
LORO SEDI

del 10/10/2019

Oggetto: ELEZIONI CUN 2020: trasmissione O.M. n. 858/2019

Rettore

Si informa che è in pubblicazione l'O.M. n.858/2019 (con i relativi allegati) alla pagina: https://www.miur.gov.it/web/guest/cun, relativa alle Elezioni CUN 2020 programmate per i giorni 14, 15 e 16 gennaio 2020.

Si prega di darne massima diffusione anche sui propri siti istituzionali.
Grazie per la collaborazione.

IL DIRIGENTE
Dott. Michele Moretta

Il Ministro dell'Istruzione, dell'Università e della Ricerca

VISTO il decreto legislativo 30 luglio 1999, n. 300, e successive modificazioni, recante "*Riforma dell'organizzazione del Governo, a norma dell'articolo 11 della legge 15 marzo 1997, n. 59*" e, in particolare, l'articolo 2, comma 1, n. 11), che, a seguito della modifica apportata dal decreto-legge 16 maggio 2008, n. 85, convertito, con modificazioni, dalla legge 14 luglio 2008, n. 121, ha istituito il Ministero dell'istruzione, dell'università e della ricerca;

VISTO altresì l'articolo 1, comma 5, del predetto decreto-legge n. 85 del 2008, che dispone il trasferimento delle funzioni del Ministero dell'università e della ricerca, con le inerenti risorse finanziarie, strumentali e di personale, al Ministero dell'istruzione, dell'università e della ricerca;

VISTA la legge 16 gennaio 2006, n. 18, recante "*Riordino del Consiglio Universitario Nazionale*", e, in particolare, l'articolo1, comma 7, ai sensi del quale: "*I componenti del CUN che nel corso del mandato perdono o modificano lo status di appartenenza alla fascia o categoria od organismo rappresentato decadono immediatamente e sono sostituiti entro due mesi, con le stesse procedure, per il residuo periodo del mandato originario*";

VISTO l'articolo 1, comma 10, della medesima legge 16 gennaio 2006, n. 18, secondo cui: " *Le elezioni delle componenti di cui al comma 1, lettere a) e c), sono indette con ordinanza del Ministro dell'istruzione, dell'università e della ricerca almeno quattro mesi prima della scadenza di ciascun mandato e si svolgono secondo modalità definite con l'ordinanza medesima. Per l'elezione dei rappresentanti dei professori e dei ricercatori e del personale tecnico e amministrativo, si può utilizzare senza nuovi o maggiori oneri a carico della finanza pubblica una procedura telematica validata, sentiti il CUN e la CRUI, che assicuri contemporaneamente l'accertamento dell'identità dei votanti, della preferenza espressa e della segretezza del voto";*

VISTO il D.M. 8 febbraio 2017, n. 59, con cui sono stati nominati, tra gli altri, consiglieri del CUN: il Prof. Paolo Montesperelli, in rappresentanza dei professori di I fascia dell'area scientifico- disciplinare 14, il Dott. Mauro Cristina Marzo, in rappresentanza dei ricercatori dell'area scientifico – disciplinare 08 e la Dott.ssa Manuela Di Franco, in rappresentanza dei ricercatori dell'area scientifico - disciplinare 06;

VISTA la nota n. 11338 del 1° marzo 2019, con la quale il Rettore dell'Università IUAV di Venezia ha comunicato che il Dott. Mauro Cristina Marzo ha preso servizio in qualità di professore di II fascia nella predetta Università, cessando in pari data dal ruolo di ricercatore presso il medesimo Ateneo;

VISTA la nota del 17 agosto 2019, con la quale il Prof. Paolo Montesperelli ha comunicato le proprie dimissioni dalla carica di consigliere del CUN;

VISTO il decreto del Rettore dell'Università degli Studi di Roma "La Sapienza", n. 2423/2019, con il quale la Prof.ssa Manuela Di Franco è stata nominata professore di ruolo di II fascia per il settore scientifico – disciplinare MED/16 – settore concorsuale 06/D3, presso il Dipartimento di Medicina Interna e Specialità Mediche – Facoltà di Medicina e Odontoiatria;

RITENUTO pertanto necessario, ai sensi del citato articolo 1, comma 7, della legge 16 gennaio 2006, n.18, provvedere alla sostituzione dei predetti consiglieri, dando avvio alla procedura finalizzata all'elezione dei nuovi rappresentanti, rispettivamente, dei professori di I fascia dell'area scientifico-disciplinare 14, dei ricercatori dell'area scientifico – disciplinare 06 e dei ricercatori dell'area scientifico – disciplinare 08;

CONSIDERATO che per le operazioni di voto può essere utilizzata una procedura telematica validata a livello nazionale per assicurare contemporaneamente l'accertamento dell'identità dei votanti, della preferenza espressa e della segretezza del voto;

VISTO che tale procedura predisposta dal CINECA è stata validata nella seduta dell'8 febbraio 2010 da una Commissione di esperti, istituita con decreto del Capo Dipartimento per l'Università, l'AFAM e la Ricerca n. 88 del 21 luglio 2009;

VISTO che anche le precedenti elezioni sono state curate con il supporto telematico del CINECA;

ORDINA

Art. 1
Indizione votazioni

Sono indette, per i giorni **14, 15 e 16 gennaio 2020,** le votazioni per l'elezione delle seguenti componenti del Consiglio Universitario Nazionale:

- n. 1 Professore di I fascia dell'area scientifico - disciplinare 14;
- n. 1 Ricercatore dell'area scientifico - disciplinare 06;
- n. 1 Ricercatore dell'area scientifico - disciplinare 08.

Le votazioni si svolgeranno, nei giorni 14 e 15 gennaio 2020, dalle **ore 9** alle **ore 17,** e il successivo giorno 16, dalle **ore 9** alle **ore 14**.

Ogni Ateneo, nell'ambito dei giorni e degli orari sopra indicati, può fissare, per esigenze organizzative, un proprio calendario e un proprio orario.

Art. 2
Elezioni

Per ciascuna delle sopracitate aree disciplinari saranno costituiti distinti collegi elettorali composti, rispettivamente, dai professori di prima fascia afferenti all'area scientifico-disciplinare 14, dai ricercatori afferenti all'area scientifico - disciplinare 06 e dai ricercatori afferenti all'area scientifico - disciplinare 08, ad ognuno dei quali è attribuito l'elettorato attivo e passivo.

Ogni elettore potrà esprimere il proprio voto per un solo candidato. Sarà eletto il candidato che riporterà il maggior numero di voti.

A parità di voti prevarrà il più anziano nel ruolo e, in caso di ulteriore parità, il candidato più anziano di età.

Art. 3
Formazione degli elenchi dell'elettorato e presentazione delle candidature

Ai fini della determinazione dell'elettorato, il CINECA, tenuto conto dei dati forniti dagli Atenei, predisporrà gli elenchi dei professori di prima fascia dell'area scientifico - disciplinare 14 e gli elenchi dei ricercatori appartenenti alle aree scientifico – disciplinari 06 e 08, in servizio al

1° novembre 2019, e li pubblicherà, in data **14 novembre 2019**, sul sito all'indirizzo **http://elezionicun.miur.it.**

Entro il **22 novembre 2019**, gli interessati potranno proporre opposizione al Rettore che dovrà pronunciarsi in merito entro il **29 novembre 2019**, comunicando al CINECA le eventuali conseguenti modifiche da apportare agli elenchi.

Il CINECA pubblicherà in rete, il **6 dicembre 2019**, gli elenchi definitivi che faranno fede ai fini della determinazione dell'elettorato attivo.

Le candidature saranno formalizzate dagli interessati secondo gli schemi allegati alla presente ordinanza (all. 1), e pubblicate sul sito **http://elezionicun.miur.it.**

Le dichiarazioni di candidatura dei professori di prima fascia afferenti all'area scientifico – disciplinare 14 e dei ricercatori afferenti alle aree scientifico – disciplinari 06 e 08, sottoscritte dagli stessi candidati e autenticate dal Rettore o da un suo delegato, dovranno essere presentate entro il **12 dicembre 2019**, e inviate entro il **17 dicembre 2019**, per il tramite degli Uffici amministrativi di ciascuna Istituzione universitaria, al CINECA che provvederà a pubblicarle il **20 dicembre 2019** e, successivamente, a trasmetterle alla Commissione Elettorale Centrale di cui all'articolo 8.

Il modulo di candidatura pre-compilato potrà essere prodotto automaticamente dagli interessati all'interno del proprio sito personale riservato all'indirizzo **https://loginmiur.cineca.it**, fermo restando l'obbligo di presentare tale dichiarazione sottoscritta e autenticata dal Rettore, o da un suo delegato, al proprio Ateneo di appartenenza.

Art.4
Esercizio del diritto di voto

Ciascun elettore può votare una sola volta presso la sede universitaria di appartenenza. Il voto presso una sede universitaria diversa da quella di appartenenza è ammesso solo previa formale autorizzazione rilasciata dal Direttore del Dipartimento di appartenenza, da consegnare, a cura degli interessati, al Presidente della Commissione di seggio presso cui viene esercitato il diritto di voto.

Non gode di elettorato attivo e passivo il personale sospeso dal servizio a seguito di procedimento penale o disciplinare ovvero che sia stato sospeso cautelarmente in attesa di procedimento penale o disciplinare,

Art. 5
Seggi elettorali

Entro il sesto giorno antecedente a quello fissato per l'inizio delle votazioni, presso le sedi già dotate dell'attrezzatura telematica predisposta per precedenti elezioni, con decreto del Rettore saranno istituiti i seggi elettorali.

La Commissione di seggio sarà composta da un Presidente e da due membri, di cui uno con funzioni di segretario, scelti preferibilmente tra gli elettori del seggio o, in subordine, tra i docenti afferenti anche ad altre aree scientifico-disciplinari e/o tra il personale tecnico - amministrativo delle singole università.

La Commissione di seggio sarà assistita da un funzionario con competenze informatiche. Per la validità delle operazioni della Commissione è necessaria la presenza di almeno due componenti.

In caso di rinuncia, anche nel corso delle operazioni, il Rettore provvederà alla sostituzione.

Art. 6
Operazioni di voto

Il documento che descrive la procedura telematica, atta a consentire lo svolgimento delle elezioni (all. 2), costituisce parte integrante della presente Ordinanza.

Nei giorni e negli orari stabiliti, l'elettore, dopo aver dimostrato la propria identità, aver apposto la propria firma sull'elenco dei votanti a fianco del proprio nominativo e aver ritirato il proprio certificato elettorale, potrà procedere alla votazione.

Il voto è individuale e segreto. Ogni elettore potrà esprimere una sola preferenza.

Le istruzioni sulla procedura di voto saranno disponibili sul sito **http://elezionicun.miur.it.** Una copia delle istruzioni sarà affissa in ciascuna postazione elettorale e sarà, comunque, resa disponibile dal seggio elettorale.

All'ora stabilita per la chiusura delle votazioni ed esaurite le operazioni di voto degli elettori che in quel momento sono presenti nel locale della postazione, il Presidente dichiarerà chiuse le votazioni.

Art. 7
Svolgimento delle operazioni di scrutinio

Il **16 gennaio 2020**, dalle ore **15,** si insedierà la Commissione Elettorale Centrale che procederà alle operazioni di scrutinio, le quali saranno pubbliche.

Al completamento di tutte le operazioni, i risultati saranno pubblicati in rete.

Art. 8
Commissione Elettorale Centrale

Con decreto del Ministro sarà costituita presso il Ministero una Commissione Elettorale Centrale con il compito di effettuare le operazioni di cui all'articolo 7 e al presente articolo.

La Commissione sarà presieduta da un dirigente di ufficio dirigenziale di livello generale del Ministero e sarà composta da un professore di prima fascia, da un professore di seconda fascia e da un ricercatore, designati dal CUN, nonché da tre funzionari del Ministero di livello non inferiore all'area terza, dei quali uno con funzioni di segretario.

La Commissione, al termine delle operazioni di scrutinio, sulla base della graduatoria, proclamerà gli eletti.

Di tutte le operazioni sarà redatto un processo verbale.

IL MINISTRO
On.le Prof. Lorenzo Fioramonti

ALLEGATO 1

Schema di candidatura

UNIVERSITA'DEGLI STUDI DI……..

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

OGGETTO: Presentazione di candidatura elezioni per il rinnovo parziale del C.U.N .

Il/la sottoscritto/a……nato/a a ……..
Il……C.F…….
residente a……..
(professore di prima fascia, ricercatore inquadrato nel settore scientifico disciplinare……..)
presso la Facoltà/Dipartimento……
dell'Università …….
a norma dell'Ordinanza ministeriale del ……indetta per il rinnovo parziale del Consiglio Universitario Nazionale, presenta la propria candidatura per l'elezione a componente del predetto Consesso, in rappresentanza dei professori di I fascia/ ricercatori dell'area scientifico - disciplinare……

……
(firma autenticata dal Rettore, Direttore generale o dai loro delegati)

Data…….

ALL. 2

UNIVERSITÀ DEGLI STUDI DI BOLOGNA

DIPARTIMENTO DI ELETTRONICA INFORMATICA E SISTEMISTICA

Verifica della conformità del sistema u-Vote alle norme europee sui sistemi di voto elettronico

Relazione di sintesi

Roberto Laschi
Università di Bologna
Viale del Risorgimento, 2
40136 Bologna (BO)
roberto.laschi@unibo.it

Marco Prandini
Università di Bologna
Viale del Risorgimento, 2
40136 Bologna (BO)
marco.prandini@unibo.it

Marco Ramilli
Università di Bologna
Via Venezia, 52
47023 Cesena (FC)
marco.ramilli@unibo.it

Revisione 6 - 13 gennaio 2010

Executive summary

Per rispondere alle esigenze di elezione delle Commissioni di Valutazione per il reclutamento dei professori e dei ricercatori, il Ministero dell'Istruzione, dell'Università e della Ricerca ha richiesto nel 1998 al CINECA la realizzazione di un sistema di voto telematico.

u-Vote è l'ultima generazione di tale sistema, risultato del processo di innovazione tecnologica intrapreso dal CINECA al fine di mantenere 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.

Il CINECA ha commissionato al Dipartimento di Elettronica Informatica e Sistemistica (DEIS) dell'Università di Bologna l'esecuzione di un insieme significativo di test di laboratorio atti a verificare la funzionalità e la sicurezza del sistema u-Vote nelle condizioni più realistiche di funzionamento, ivi incluse situazioni di guasto, errore, ed interferenza volontaria da parte di terzi.

Questa relazione riassume le attività svolte dal gruppo di lavoro del DEIS per accertare la conformità di u-Vote alle norme internazionali che riguardano l'intera categoria di sistemi di cui esso fa parte, illustrando:

- gli elementi essenziali di analisi delle raccomandazioni internazionali in materia di definizione delle tipologie di verifiche da condurre;
- le scelte metodologiche ed operative che hanno condotto alla progettazione, realizzazione e documentazione dei test eseguiti.

Questo documento riporta in forma sintetica la struttura dei test eseguiti, i risultati osservati, e le raccomandazioni del gruppo di lavoro per un corretto utilizzo del sistema; i dettagli delle singole procedure di test ed i risultati puntuali della loro esecuzione sono invece riportati in allegati separati (rispettivamente: u-Vote Test Plan ed u-Vote Test Report).

Gli aspetti di maggior rilevanza emersi dall'attività descritta possono essere, in estrema sintesi, così esposti:

- il sistema è reputato adatto all'uso per il quale è stato progettato;
- non risultano presenti vulnerabilità sfruttabili, se sono rispettate le ipotesi di corretto impiego del sistema richieste dal CINECA, e cioè essenzialmente che la sicurezza fisica e l'integrità del sistema operativo delle postazioni di voto siano garantite tramite la predisposizione di seggi secondo le migliori pratiche riportate nel Test Report finale, che individuano dettagliatamente le condizioni ambientali e di configurazione da rispettare per garantire il massimo livello di sicurezza.

Indice

Executive summary 3
Abstract 7
Contesto 7
Metodologia 8
Definizione della normativa di riferimento 8
Passaggio dalla norma di riferimento al piano di test per il sistema u-Vote 9
DTR e ATP 10
Struttura dei DTR 10
Organizzazione generale dei DTR nell'Abstract Test Plan 10
Test Plan 12
Conduzione dei test 14
Ambiente di testing 14
Metodologia 15
Sintesi dei risultati 17
Riferimenti 18

Abstract

Questa relazione riassume le attività svolte dal gruppo di lavoro del Dipartimento di Elettronica Informatica e Sistemistica (DEIS) dell'Università di Bologna, delegato dal CINECA (Consorzio Interuniversitario per il Calcolo Automatico dell'Italia Nord Orientale) all'attività di verifica della conformità del proprio sistema di voto elettronico (u-Vote) alle norme internazionali che riguardano tale categoria di sistemi.

Lo scopo di questo documento è quello di illustrare le scelte metodologiche ed operative che hanno condotto alla progettazione, realizzazione e documentazione dei test eseguiti. Poiché non esiste un vero e proprio quadro normativo di riferimento, si ritiene infatti indispensabile motivare ogni passo logico che ha portato dall'analisi delle raccomandazioni internazionali in materia alla definizione delle tipologie di verifiche da condurre, alla definizione di piani di test dettagliati, ed infine alla loro esecuzione e relativa documentazione dei risultati.

Per mantenere la necessaria leggibilità, questo documento riporta solo in forma sintetica la struttura dei test eseguiti, i risultati osservati, e le raccomandazioni del gruppo di lavoro per un corretto utilizzo del sistema nei casi in cui condizioni al contorno differenti da quelle dell'ambiente di testing possano influire significativamente sul comportamento del sistema medesimo.

I dettagli delle singole procedure di test ed i risultati puntuali della loro esecuzione sono invece riportati in allegati separati (rispettivamente: *u-Vote Test Plan* ed *u-Vote Test Report*), utilizzabili dagli enti interessati all'utilizzo del sistema al fine di determinarne la consistenza ai propri requisiti (ed eventualmente al fine di ripetere autonomamente i test).

Contesto

Per rispondere ad una precisa esigenza del Ministero dell'Università e della Ricerca, nel 1998 il CINECA ha realizzato un sistema di voto telematico che fino ad oggi è stato utilizzato come sistema di voto ufficiale 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 tecnologico del sistema di voto telematico, il CINECA ha avviato un processo di innovazione tecnologica che ha portato al nuovo 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.

Il CINECA ha commissionato al DEIS l'esecuzione di un insieme significativo di test di laboratorio atti a verificare la funzionalità e la sicurezza del sistema u-Vote nelle condizioni più realistiche di funzionamento, ivi incluse situazioni di guasto, errore, ed interferenza volontaria da parte di terzi. Il DEIS ha formato allo scopo un gruppo di lavoro d'ora in avanti chiamato DEIS Working Group (*DWG*).

Metodologia

Definizione della normativa di riferimento

Non esiste in Italia, né a livello di Unione Europea, una precisa norma tecnica che stabilisca gli standard a cui attenersi nella progettazione e realizzazione di un sistema per il voto elettronico. La prima parte dell'attività del DWG quindi è stata la ricognizione della documentazione esistente che potesse essere utilizzata allo scopo di definire una linea normativa accettabile. I risultati di questa attività sono sintetizzati di seguito, e dove meritevoli di approfondimento ripresi nel dettaglio nell'allegato *La regolamentazione delle procedure di voto condotte con sistemi elettronici ed informatici: un confronto tra gli approcci statunitense ed europeo.*

Senza dubbio il documento di riferimento risulta essere la *Recommendation Rec(2004)11* adottata dal Comitato dei Ministri del CoE il 30 settembre 2004 ed intitolata "Legal, operational and technical standards for e-voting" [1]. Anche una lettura superficiale di tale testo, però, evidenzia un problema di implementabilità. Nelle *Recommendation* sono esposti di tutti i principi che devono regolare in termini generali l'adozione di macchine come ausilio alle procedure di voto, ma non in modo "testabile": non vi è alcuna indicazione sufficientemente specifica da poter essere mappata in una procedura di verifica che permetta di attestare la conformità di un sistema candidato a tali principi.

Da questo punto di vista la ricognizione ha invece individuato negli Stati Uniti un esempio di pragmatismo che ha prodotto strumenti avanzati ed efficaci per normare, testare e quindi certificare sistemi di ausilio al voto. La *Election Assistance Commission* si è occupata di redigere tutti i documenti di principio (sebbene questo termine sia da considerare declinato in modo molto meno astratto e generale che non nella *Recommendation*), tra cui spiccano per i nostri fini le *Voluntary Voting System Guidelines* o (*VVSG*) [2]. Il *National Institute for Standards and Technology* coordina la definizione delle precise procedure di testing della conformità dei sistemi alle *VVSG*.

Dal punto di vista operativo, quindi, si è voluto trarre vantaggio dall'importante lavoro svolto dagli organismi USA per realizzare la struttura dei test, naturalmente però finalizzando questi alla verifica della conformità alla *Recommendation* europea. Come meglio spiegato nel citato allegato, l'operazione di mappatura tra principi della *Recommendation* europea e procedure collegate alle *VVSG* è risultata non semplicissima. I problemi fondamentali sono risultati essenzialmente: da un lato, la presenza nella *Recommendation* di norme che esprimono requisiti per la conduzione dell'elezione che poco hanno a che fare con l'utilizzo di sistemi elettronici, e quindi non trovano espressioni omologhe nelle *VVSG;* dall'altro la succitata mancanza di generalità delle *VVSG* che, in alcuni punti, sono dettate più dalla consapevolezza di dover trattare sistemi specifici (perché già largamente diffusi) che dalla più corretta volontà di esprimere principi di ampia validità.

In definitiva però non si sono riscontrate nemmeno difformità concettuali tali da precludere l'adattamento delle *VVSG,* e delle metodologie di testing da esse derivate, in funzione della definizione di un *Test Plan.*

Un intervento più incisivo sulla lettura della *Recommendation* invece è stato fatto alla luce di analisi critiche reperibili in letteratura [3], che evidenziano oggettivi problemi di coerenza interna del documento. Poiché tali analisi, anche in questo caso, non contraddicono sostanzialmente la *Recommendation* ma ne riorganizzano in modo più razionale i contenuti, si è ritenuto opportuno accoglierne il contributo.

Passaggio dalla norma di riferimento al piano di test per il sistema u-Vote

Un sistema come quelli elettronici per il voto oggetto della presente attività è un insieme complesso ed articolato di componenti hardware e software, ognuno dei quali può essere scelto in modo diverso in ogni specifica istanza del sistema medesimo, per realizzare il risultato più soddisfacente in termini di affidabilità, costi, rispondenza alla tipologia di consultazione elettorale, reperibilità sul mercato, ecc..

Il lavoro dell'ente deputato a certificare la conformità di un particolare sistema alla normativa deve essere reso il più possibile indipendente da tali scelte. Si ha quindi la necessità di definire una procedura di derivazione del *Test Plan*, piuttosto che il *Test Plan* stesso, in modo da poterla applicare nel modo più efficiente ed ottenere di volta in volta *Test Plan* rispondenti alle peculiarità che i sistemi da certificare presentano, in funzione del fornitore e del tempo di progettazione e realizzazione.

Sebbene in questo caso specifico il DWG abbia ricevuto dal CINECA l'incarico ultimo di testare un'istanza ben precisa del sistema u-Vote, di comune accordo si è deciso di seguire la strada più generale ed organica, stimando che l'investimento di tempo e risorse necessario possa essere ripagato sul medio e lungo periodo dall'adattabilità delle procedure prodotte alle versioni di u-Vote che certamente seguiranno quella oggetto degli attuali test. I passaggi svolti sono stati quindi:

(a) Mappatura delle *Recommendation* sulle *VVSG* – Come descritto al punto precedente di questa sezione, si è tracciato il parallelo tra le raccomandazioni europee e le norme USA per poter poi utilizzare nei passi successivi quanto già esistente in materia di certificazione per queste ultime; è stata necessaria una riorganizzazione delle raccomandazioni europee, che spesso fanno riferimento in luoghi distinti a proprietà più sensatamente testabili in modo unitario.

(b) Realizzazione dell'*Abstract Test Plan* (*ATP*)– Si è effettuata una riscrittura delle norme dettagliate al passo precedente in forma di istruzioni per il laboratorio di test, senza tuttavia includere alcun dettaglio relativo al sistema da testare: in altre parole, viene esplicitato in termini concettuali cosa si deve testare per verificare la conformità al dettato di ogni articolo normativo, cercando di esplicitare anche, nel massimo grado consentito dal vincolo di non perdere di generalità, in che modo effettuare i test e che risultati considerare rilevanti. Le voci che compongono l'*ATP* sono detti *Derived Test Requirement* (*DTR*), cioè i requisiti di test derivati [dalle corrispondenti norme].

(c) Realizzazione del *Test Plan* – Dato il *Technical Documentation Package* del sistema, i *DTR* possono essere trasformati in istruzioni dettagliate su come eseguire i test sul sistema, introducendo le necessarie specifiche relative alla particolare configurazione hardware, software, e di contesto d'uso previsto.

Vale la pena notare che i risultati intermedi descritti ai punti (a) e (b) possono, se considerati qualitativamente e quantitativamente soddisfacenti, essere fatti propri dagli organismi deputati a livello più alto alla certificazione dei sistemi di voto per stabilire le linee guida generali del processo di validazione dei sistemi, non essendo in alcun modo legati al caso specifico qui trattato.

DTR e ATP

Struttura dei DTR

I requisiti di testing derivati dalle norme specificano che tipo di funzionalità o proprietà del sistema debba essere verificata per poter giudicare la conformità del sistema stesso alla corrispondente norma.

I principi tenuti in considerazione nella scrittura dei *DTR* sono essenzialmente:

1. Ove possibile, specificare il test sotto forma di coppia (stimolo da applicare al sistema, risposta attesa); indicare se appropriato i valori nominali, le fasce di valori accettabili e non per gli stimoli e le risposte;
2. Nei casi in cui non sia adottabile il modello stimolo-risposta per motivi di costo o strutturali, indicare la necessità che il laboratorio di testing possa esaminare il progetto hardware e/o il codice sorgente per verificare non solo la rispondenza logica del sistema al comportamento atteso, ma anche l'adozione di tecniche ingegneristiche allo stato dell'arte (principalmente in termini di affidabilità e robustezza).

Sintatticamente, i *DTR* devono riportare:

1. Il requisito a cui fanno riferimento, cioè la voce normativa il cui rispetto deve essere determinato dal test illustrato; si deve prevedere il caso che un *DTR* possa svolgere il ruolo di verificare in tutto o in parte la rispondenza a più norme, indicando con chiarezza i riferimenti incrociati;
2. L'elenco delle asserzioni da testare per verificare il requisito; spesso queste si ricondurranno direttamente al testo della corrispondente norma, o ne saranno una rielaborazione più facilmente implementabile; possono essere sia positive (verifica di una determinata risposta allo stimolo) che negative (verifica che uno stimolo non produca una determinata risposta);
3. Per ogni asserzione, se necessario, quali richieste il laboratorio deve fare al produttore del sistema per essere poi in grado di trasformare il *DTR* in una voce concreta del *Test Plan*;
4. Ad ogni asserzione sono associate una o più procedure di test, esplicitamente se queste sono specifiche dell'asserzione considerate, o implicitamente se il *DTR* rimanda alle procedure di test di altri *DTR*.

Organizzazione generale dei DTR nell'Abstract Test Plan

Dal lavoro di analisi critica e comparativa della *Recommendation* richiamato in precedenza, discende l'elenco dei *DTR* che va a comporre l'*ATP*, fornito in allegato, e qui sinteticamente illustrato nella sua struttura complessiva; i numeri tra parentesi indicano le norme della *Recommendation* rilevanti per i requisiti descritti, se seguiti da una lettera indicano che la norma è stata frammentata per una più razionale applicazione e solo parte della stessa quindi è tenuta in considerazione.

Sezione 1 - Requisiti funzionali: garanzia dell'universalità, uguaglianza, libertà e segretezza del suffragio;

1.a) Modalità di espressione del voto (5b, 6, 9, 12, 13, 41, 43, 44, 47, 48, 49, 53, 82, 90a, 91, 96)

1.b) Segretezza del voto (11, 16, 18, 19, 34b, 35, 51, 52, 54, 78, 93a, 103a, 106)

1.c) Trattamento e conteggio dei voti espressi e calcolo dei risultati (5a, 7, 8, 92, 94, 95, 98)

1.d) Usabilità ed accessibilità (14, 50, 61a, 63, 64, 65)

Sezione 2 - Requisiti strutturali: garanzia della corretta progettazione ed implementazione delle misure che conducono alla realizzazione dei requisiti funzionali;

2.a) Hardware: integrità, disponibilità e corretto funzionamento dei sistemi (24, 100a)

2.b) Software: migliori pratiche per la progettazione e codifica (26, 66, 93, 111)

2.c) Osservabilità del corretto funzionamento (23, 56, 83)

Sezione 3 - Requisiti di sicurezza: garanzia della resistenza del sistema ad eventi non accidentali

3.a) Analisi del rischio e misure minime a difesa dalle minacce (14, 20, 27, 28, 29, 69, 76, 77)

3.b) Difesa dei dati memorizzati e trasmessi (75c, 81, 86, 89, 97, 99, 109)

3.c) Accesso al sistema e verifica di conformità (32, 33a, 69b, 72a, 74, 75a, 79a, 80)

3.d) Rilevazione di eventi e reportistica di funzionamento (57, 58, 59, 76, 100b, 101, 102, 103, 104, 107, 108)

Test Plan

Il sistema u-Vote rientra nella categoria dei sistemi di voto online. La redazione del *Technical Data Package* (*TDP*) che lo descrive dettagliatamente è naturalmente a carico del produttore, che lo ha fornito al DWG come da allegato. Utilizzando tale documentazione, si possono trasformare i *DTR* in una raccolta di test specifici che vanno a comporre il *Test Plan*, di seguito riportato limitatamente all'elenco dei test, i cui dettagli sono forniti nel corrispondente allegato.

Sezione 1 - Requisiti funzionali: garanzia dell'universalità, uguaglianza, libertà e segretezza del suffragio;

1.a) Modalità di espressione del voto

- ✓ verifica lista candidati
- ✓ verifica lista elettori
- ✓ verifica impossibilita di modificare le liste
- ✓ verifica ordine sparso lista elezione (randomizzazione ordine rappresentati)
- ✓ verifica richiesta conferma prima di accettare ogni variazione di stato
- ✓ verifica voto
- ✓ verifica non ambiguità delle fasi di voto
- ✓ verifica voto multiplo

1.b) Segretezza del voto

- ✓ verifica della privacy del votante

1.c) Trattamento e conteggio dei voti espressi e calcolo dei risultati

- ✓ verificare dell'adeguata archiviazione dei dati ed in particolare della non cancellabilità
- ✓ verifica del timestamp su ogni ballot
- ✓ verifica sistema di conteggio
- ✓ verifica sistema di conteggio multiplo

1.d) Usabilità ed accessibilità

- ✓ verifica corretta interpretazione delle schermate e del layout

Sezione 2 - Requisiti strutturali: garanzia della corretta progettazione ed implementazione delle misure che conducono alla realizzazione dei requisiti funzionali;

2.a) Hardware: integrità, disponibilità e corretto funzionamento dei sistemi

- Integrità
  - ✓ verifica impossibilità di manipolazione hardware
  - ✓ verifica del processo di boot
  - ✓ verifica impossibilità di aggiungere unità esterne
  - ✓ verifica impossibilità di installare wireless technology

- Disponibilità
  - ✓ verifica robustezza alimentazione (power cord)
  - ✓ verifica allarme e gruppo continuità dell'alimentazione
  - ✓ verifica funzionalità di restore in caso di fault
  - ✓ verifica delle performance della macchina
  - ✓ verifica stress di voto (votazione controllata di votanti multipli)
- Correttezza
  - ✓ verifica degli allacciamenti tra componenti del sistema
  - ✓ verifica della calibrazione dei dispositivi
  - ✓ verifica della precisione temporale

2.b) Software: migliori pratiche per la progettazione e codifica

- verifica della logica del sistema
  - ✓ verifica dei modelli del sistema
  - ✓ verifica della congruenza tra documentazione e implementazione
- readteaming su bugs del codice

2.c) Osservabilità del corretto funzionamento

- ✓ verifica degli indicatori di ON/OFF di "online" o "offline", inchiostro, foglio incastrato nella stampante, ecc.
- ✓ verifica della presenza di un unique ID per software di voto

Sezione 3 - Requisiti di sicurezza: garanzia della resistenza del sistema ad eventi non accidentali

3.a) Analisi del rischio e misure minime a difesa dalle minacce

- Controllo dell'accesso
  - ✓ verifica impossibilita di accesso al SO
  - ✓ verifica procedura di autenticazione (robustezza e durata password)
- Integrità del software
  - ✓ verifica vulnerabilità sistema operativo
  - ✓ verifica presenza di antimalware
  - ✓ verifica signature antimalware
  - ✓ verifica processo di aggiornamento delle signature
  - ✓ verifica funzionamento antimalware e verifica del processo di eliminazione file
  - ✓ verifica periodicità di scanning

3.b) Difesa dei dati memorizzati e trasmessi

- Moduli crittografici:
  - ✓ verifica presenza crittografia in trasmissione e ricezione

- ✓ test algoritmo utilizzato
- ✓ test ambiente di cifratura (dove sono inserite le firme, gli hash ecc.)
- ✓ test robustezza del cifrario
- ✓ test sull'efficacia sistema di generazione di numeri casuali
- ✓ verifica di storing dei dati cifrati

• Firma digitale:

- ✓ verifica della presenza
- ✓ verifica della firma apposta ai dati autenticati
- ✓ test sull'utilizzo della firma
- ✓ test sull'ambiente (dove sono inserite le firme gli hashes, ecc.)
- ✓ test sull'efficacia sistema di generazione di numeri casuali

• Comunicazione in rete

- ✓ verifica delle proprietà di difesa del canale da attacchi di "uomo nel mezzo"
- ✓ verifica di limitazione delle comunicazioni al solo dominio del sistema di voto
- ✓ verifica dei processi che hanno accesso alla rete e del loro funzionamento

3.c) Accesso al sistema e verifica di conformità

- ✓ verifica della completezza della documentazione
- ✓ verifica autorizzazioni per la modifica dei file di configurazione
- ✓ verifica del principio di minimo privilegio
- ✓ verifica impossibilita di aggiungere utenti/gruppi, account lockout
- ✓ verifica dell'impossibilità di modifica del codice non autorizzata

3.d) Rilevazione di eventi e reportistica di funzionamento

• Logging

- ✓ verifica corrispondenza dei logs agli eventi
- ✓ verifica identificazione dei log
- ✓ verifica corretta interpretazione dei log
- ✓ verificare unicità del formato di log
- ✓ verificare dell'impossibilità di alterazione del log da parte del software

Conduzione dei test

Ambiente di testing

I test sono stati effettuati presso i Network Security Labs dell'Università degli Studi di Bologna - Seconda facoltà di Ingegneria, con sede a Cesena. Il CINECA ha provveduto personalmente al

trasporto e alla configurazione del sistema di voto all'interno dei laboratori. Tre macchine di proprietà dell'Università sono state connesse al router che collegava la macchina di voto con il server centrale (collocato solo per il test presso il laboratorio). Una macchina chiamata "generatrice" ha svolto il compito di generare il traffico reale al fine di simulare problematiche relative alle problematiche di carico e di concorrenza. Una macchina nominata "Attaccante Diligente" ha svolto il compito di eseguire attacchi mirati al sistema, mentre una macchina denominata "Attaccante Automatico" ha utilizzato software automatici di exploiting e di audit, sia commerciali che open-source.

Metodologia

Considerando la novità sia del sistema, che della procedura di testing sviluppata, la metodologia di testing ha di fatto integrato l'esecuzione dei test veri e propri con la messa a punto di alcuni dettagli del *Test Plan*, che difficilmente avrebbero potuto essere colti in modo appropriato dalla pur rigorosa, ma completamente teorica, analisi fatta tramite i *DTR* ed il *TDP*.

Il flusso di definizione – esecuzione – rapporto dei test, schematizzato in figura 2 il cui contenuto è brevemente chiarito nel seguito, fa riferimento specifico al testing delle caratteristiche di sicurezza, che costituiscono un caso più complesso rispetto alle altre caratteristiche funzionali ed architetturali. È evidente infatti che un *Test Plan* può suggerire le verifiche da compiere per attestare la rispondenza del sistema ai requisiti *minimi* di sicurezza, ma un efficace security testing dipende anche in buona parte dalla capacità di un auditor indipendente di trovare percorsi non ovvi di attacco. Si può considerare questa metodologia un superset più generale di quella comunque adottata per verificare, più semplicemente, la corretta risposta agli stimoli durante i test funzionali.

Define Testing Goals – definire l'obiettivo finale del test; ove per mezzo del *DTR* non sia possibile prevedere tutti gli outcome significativi dei test (come ad esempio nel caso di penetration testing) si provvede a specificare cosa si intende per risultato (nell'esempio, le informazioni raccolte)

Define Objects – definire quale componente è l'oggetto del test, tipicamente questo è chiaro dal *Test Plan*, anche se interazioni e configurazioni non ovvie possono essere l'oggetto di test di sicurezza aggiuntivi.

Posture of the Penetrator – definire quali opportunità di posizionamento e accesso sono disponibili per il tester/attaccante, ad esempio:

- collocazione all'interno o all'esterno del sistema, della rete di comunicazione, ecc.;
- scatola aperta/chiusa: possibilità o meno di modificare il sistema;
- scatola bianca/grigia/nera: grado di visibilità dei dettagli interni del sistema.

Flaw Hypotesis – predisporre un'ipotesi su quali vulnerabilità possono essere presenti.

Find Evidence – definire ed applicare gli Attack Vector (organizzati in Attack Tree) e/o gli stimoli previsti dal *DTR*

Induction Hypotesis – Soprattutto nel caso di security testing, è comune che nuovi obiettivi di test emergano dal comportamento osservato in risposta a stimoli o attacchi, e quindi è opportuno aggiungerli dinamicamente alla lista dei test da effettuare.

Reporting – Documentare dettagliatamente la conduzione del test: corrispondenza tra attività previste dal *Test Plan* ed attività effettivamente condotte, risultati verificati in rapporto a quelli attesi.

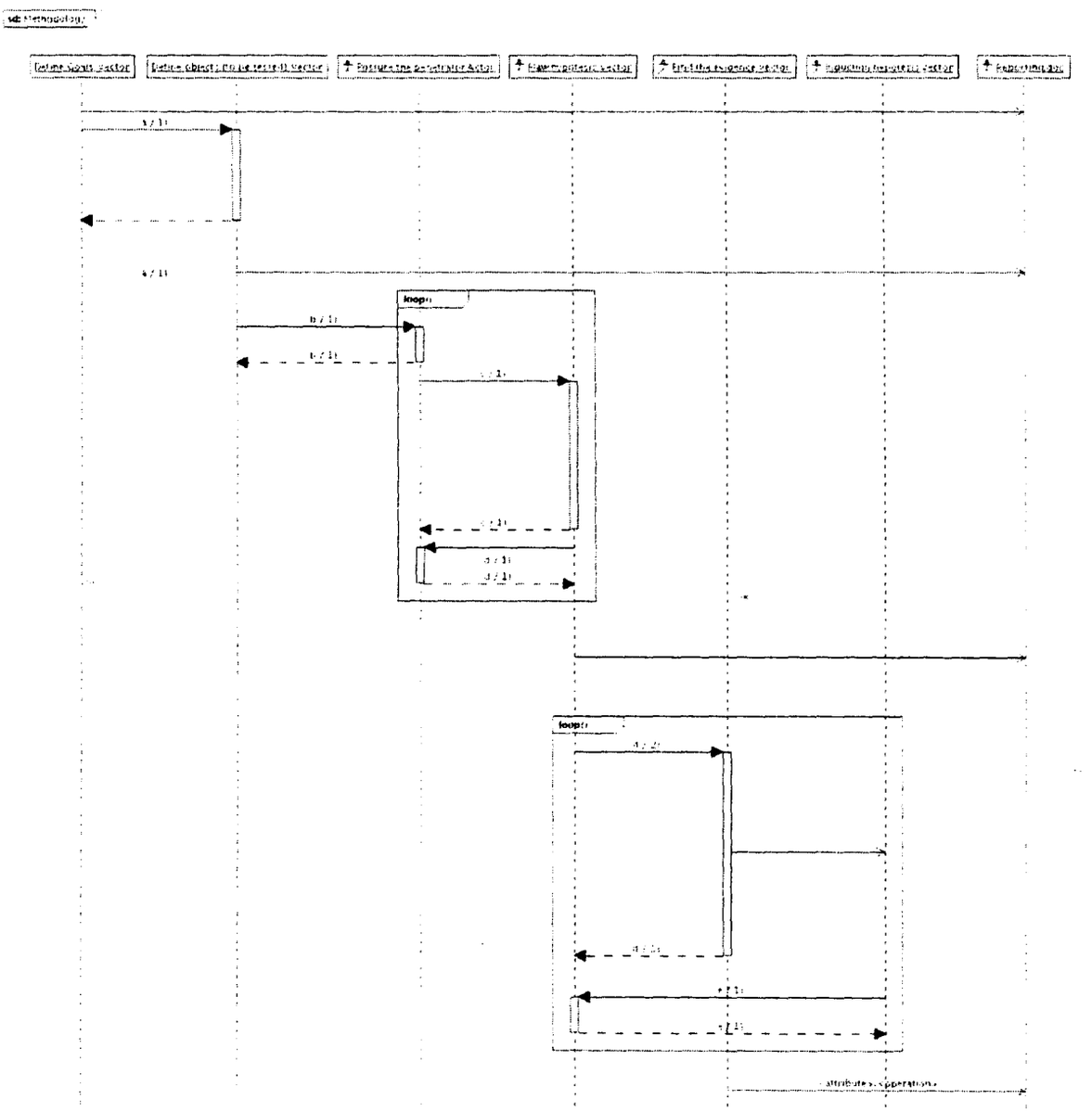


Figura 2 – Metodologia di testing delle caratteristiche di sicurezza

Sintesi dei risultati

I risultati dei test eseguiti secondo i dettami del *Test Plan* sono allegati nel *Test Report*. In questa sede si ritiene opportuno semplicemente richiamare l'attenzione sugli aspetti di particolare sensibilità rilevati, anticipando che:

- tutti i test funzionali sono stati superati,tutti i test strutturali sono stati superati,i test di sicurezza non hanno evidenziato problematiche progettuali e realizzative incongruenti con i prerequisiti specificati dal costruttore.

Il sistema è quindi reputato adatto all'uso per il quale è stato progettato, purché nel rispetto:

- delle ipotesi indicate nella sezione H.4 del TDP, che pongono le precondizioni perché il sistema possa essere considerato sicuro (essenzialmente: la sicurezza fisica e l'integrità del sistema operativo delle postazioni di voto è a carico dell'organizzazione che si avvale del sistema, e non sono quindi previste contromisure addizionali di tipo logico contro potenziali violazioni di tali ipotesi);
- delle raccomandazioni / migliori pratiche riportate nel *Test Report* finale, che individuano dettagliatamente le condizioni ambientali e di configurazione da rispettare per garantire il massimo livello di sicurezza.

Riferimenti

[1] http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/Key_Documents/Rec%282004%2911_Eng_Evoting_and_Expl_Memo_en.pdf

[2] http://www.eac.gov/program-areas/voting-systems/voluntary-voting-guidelines/2005-vvsg

[3] Margaret McGaley, J. Paul Gibson, A Critical Analysis of the Council of Europe Recommendations on e-voting. Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop

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

EXECUTIVE SUMMARY **1**

Introduzione **5**

Confronto tra u-Vote ed il sistema di voto telematico del 1998 ..... **6**

I canali di voto **7**

Voto in seggio elettorale o Pool Site Voting (PSVC) 7

Voto remoto in chiosco o Kiosk Voting (KVC) 7

Autenticazione dell'elettore **8**

Protocolli di voto, scrutinio e verifica **9**

Protocollo di voto 9

Protocollo di scrutinio 10

Protocollo di verifica 10

Architettura hardware e di rete **10**

Architettura hardware lato server 11

Architettura hardware lato client 12

Le smartcard 12

Rete ISDN 12

Rete VPN 12

Architettura software **13**

Usabilità e accessibilità delle interfacce utente **14**

Qualità del prodotto **15**

Processo di sviluppo del software **16**

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.

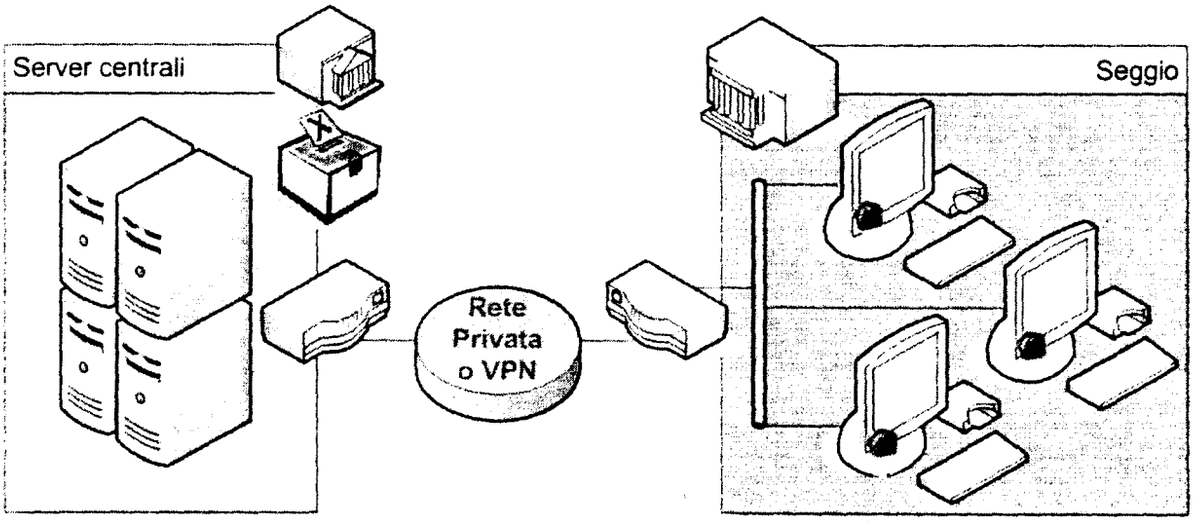


Figura 1: Voto in seggio

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.

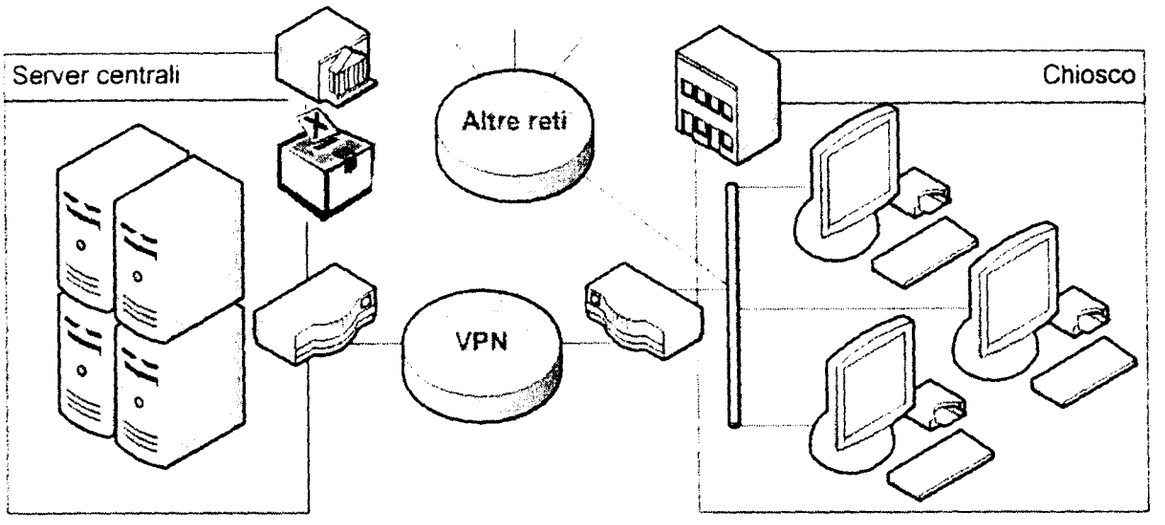


Figura 2: Voto in chiosco

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*.

$\xi_k^{-1}(c)$: 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*.

$\nu_{pk}(s,m)$: 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.

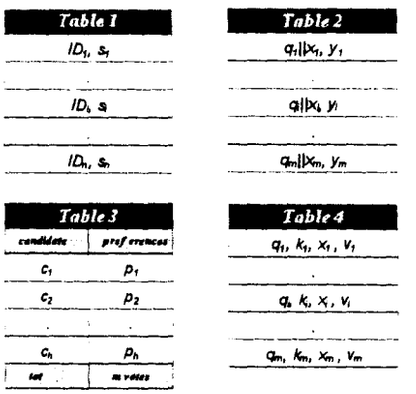
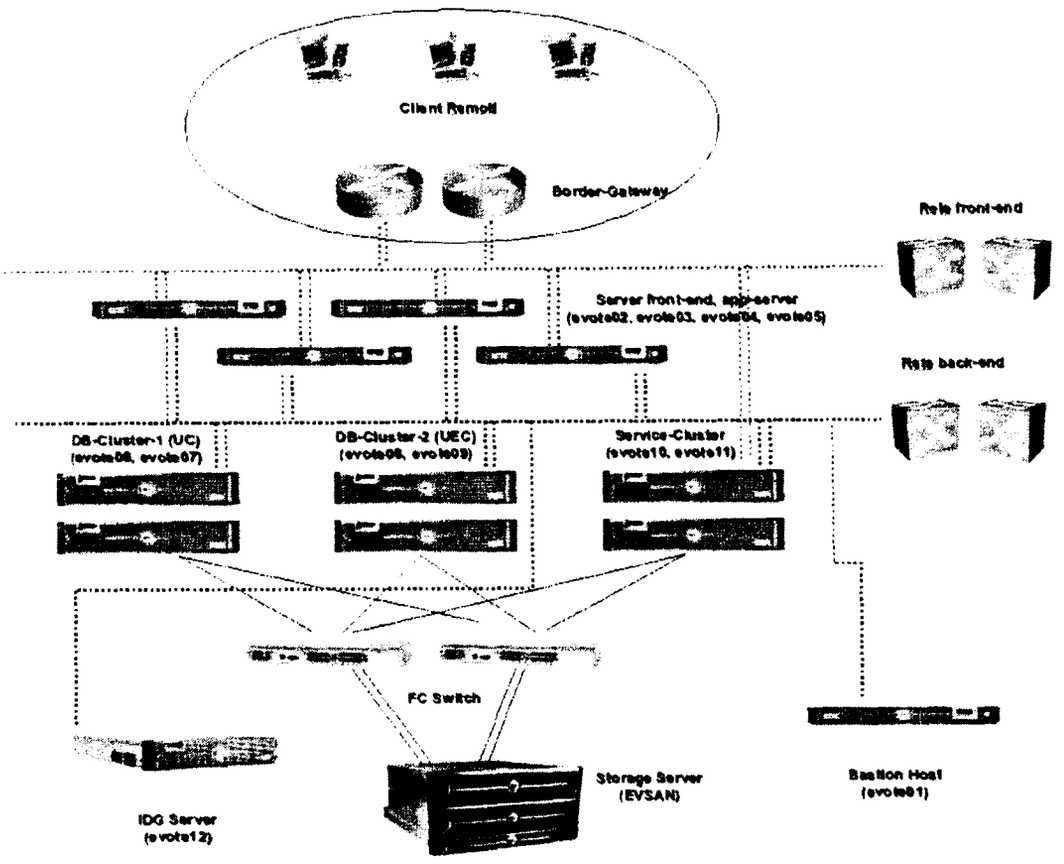


Figura 5: risorse disponibili al Servizio di Audit

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.