

# Evote: il voto telematico per le elezioni degli organi istituzionali delle Università

di Pierluigi Bonetti, Simone Piergallini, Stefano Ravaioli

Il sistema di voto telematico è stato sviluppato nel 1999 con l'obiettivo di gestire a livello nazionale l'elezione dei membri delle Commissioni di valutazione comparativa, organi preposti alla valutazione dei candidati nei concorsi per cattedre universitarie. L'efficacia dimostrata nella gestione di queste complesse votazioni, affiancata alla semplificazione delle operazioni di voto apportate dal sistema (dalla definizione degli elettorati, attivi e passivi, alle operazioni di scrutinio, alla pubblicazione dei risultati), e all'utilizzo dei più elevati sistemi di sicurezza, ha spinto alcuni atenei a chiedere di poterlo utilizzare anche per l'elezione dei propri organi accademici, quindi in ambito locale.

Il sistema, pertanto, è stato progressivamente adattato alle esigenze delle nuove votazioni richieste dai singoli atenei, esigenze che nel tempo sono diventate sempre più complesse per rispondere alle complesse tipologie di elezioni di cui è stata chiesta la gestione al CINECA.

Le prime votazioni gestite con il sistema modificato sulla base delle richieste specifiche di singoli atenei sono state le elezioni dei Rettori delle Università di Pisa e di Firenze, avvenute tra il mese di maggio e il mese di giugno del 2000. Per gestire questo tipo di elezioni è stato chiesto al Consorzio di modificare il sistema in modo che le votazioni potessero essere svolte nel corso di un'unica sessione di voto, eventualmente da ripetersi in più tornate: una struttura di voto semplificata, rispetto a quella realizzata per le valutazioni comparative.

Il voto telematico ha consentito anche in que-



sto caso di velocizzare le operazioni, vale comunque la pena di citare anche altri elementi, seppure secondari rispetto al valore tecnologico del sistema, che contribuiscono a diffonderne l'utilizzo in diversi atenei: vengono eliminate le schede cartacee che nei seggi tradizionali vengono consegnate agli elettori per esprimere le preferenze di voto, l'infrastruttura tecnologica è già presente negli atenei, essendo abitualmente in uso per le votazioni comparative e, infine, gli aventi diritto al voto hanno ormai una familiarità consolidata con il sistema, utilizzandolo da oltre tre anni.

## Modifiche rispetto al sistema originale

A questa prima tipologia di elezioni ne sono seguite altre (elencate nella tabella della pagina seguente) che hanno richiesto diverse modifiche. Ne vediamo due in dettaglio: il voto frazionario e quello con espressione di preferenze multiple.

Ateneo	Votazioni svolte	Date
Università degli Studi Pisa	Elezioni del Rettore	maggio - giugno 2000
Università degli Studi di Firenze	Elezioni del Rettore	giugno 2000
Università Ca' Foscari di Venezia	Elezioni del Rettore	giugno 2000
Università Ca' Foscari di Venezia	Senato Accademico	novembre 2000
Politecnico di Torino	Elezioni del Rettore	giugno 2001
Politecnico di Torino	Suppletive Consiglio di Amministrazione Senato Accademico	luglio 2001
Università degli Studi di Roma "Tor Vergata"	Senato Accademico	ottobre 2001
Politecnico di Torino	Comitato Paritetico della Didattica	ottobre 2001
Università degli Studi di Salerno	Suppletive Consiglio di Amministrazione	maggio 2002
Politecnico di Milano	Elezioni del Rettore	giugno 2002
Università degli Studi di Salerno	Consiglio di Amministrazione EDISU	giugno 2002
Politecnico di Milano	Senato Accademico	settembre - ottobre 2002
Università di Pisa	Senato Accademico Commissioni Scientifiche d'Area Suppletive del Consiglio di Amministrazione Rappresentanza del personale tecnico-amministrativo per le elezioni del Rettore	ottobre 2002
Università degli Studi di Salerno	Consiglio di Amministrazione (corpo non docente) Consulta del personale tecnico-amministrativo	novembre 2002
Università degli Studi di Salerno	Consiglio di Amministrazione (corpo docente) Commissioni Scientifiche di Ateneo	dicembre 2002
Università degli Studi di Pisa	Elezioni del Rettore	dicembre 2002 - gennaio 2003
Istituto Nazionale di Alta Matematica (INdAM)	Rinnovo del Comitato Direttivo	gennaio 2003

### Voto frazionario

Una delle prime estensioni che è stato necessario introdurre nel sistema di voto per gli organi accademici è stata la nozione di voto frazionario. Gli ordinamenti di molti atenei estendono anche al personale tecnico-amministrativo la partecipazione all'elezione del Rettore. Mentre in alcune Università ciò avviene attribuendo il diritto di voto solo ad una loro rappresentanza, solitamente eletta in precedenza, in altri atenei il diritto di voto è esteso all'intero corpo non docente, attribuendo però un valore frazionario ad ogni singola espressione di voto. Tale è, ad esempio, il caso dell'Università Ca' Foscari di Venezia e dell'Università degli Studi di Firenze. Il problema maggiore nell'introdurre tale funzionalità è consistito nell'individuare una soluzione

sufficientemente generale e flessibile in grado di adattarsi ad ogni tipo di arrotondamento e a un numero di cifre decimali arbitrario, compatibile con il più ampio numero di regolamenti che, spesso, definiscono le modalità di calcolo del peso dei voti con regole complesse, di volta in volta diverse, e variabili in funzione del numero effettivo di votanti.

### Voto con espressione di preferenze multiple

Di solito, i regolamenti che disciplinano le elezioni rettorali prevedono, salvo poche eccezioni, l'espressione di un'unica preferenza. Questo cessa di essere vero nel caso dell'elezione di numerosi organi accademici. Questo tipo di funzionalità è stata introdotta per le elezioni del comitato Paritetico della Didattica del 25 Ottobre 2001, predisposte per

conto del Politecnico di Torino. Il regolamento elettorale di questo organismo prevede, infatti, che ogni elettore abbia la possibilità di esprimere fino a tre preferenze.

Realizzando questa funzionalità si è scelto di mantenere la massima uniformità con il software esistente, ed in particolare con il client di voto per le Valutazioni Comparative, al fine di agevolare gli utenti che già avevano acquisito esperienza in queste votazioni (tipicamente il corpo docente). A tal fine, la raccolta delle preferenze avviene in schermate successive, quasi come se si trattasse di votazioni successive, curando semplicemente l'aggiornamento della lista dei candidati in funzione delle preferenze già espresse.

#### **Le elezioni studentesche**

Grazie agli sviluppi ed agli affinamenti che il sistema di voto telematico del Consorzio ha subito nel corso degli ultimi anni, la casistica di tipologie di elezioni con esso gestibili si è via via ampliata.

Attualmente, l'impegno è orientato all'analisi delle problematiche poste dalle elezioni studentesche.

Le principali direzioni di sviluppo sono rappresentate dalla introduzione della gestione del voto di lista e da diverse forme di identificazione degli elettori, oltre che dal fatto di implementare nuovi sistemi per velocizzare le operazioni di scrutinio mantenendo gli standard di sicurezza dell'attuale sistema.

#### **Voto di lista**

La naturale estensione del voto con preferenze multiple già descritto consiste nell'introdurre al suo interno una preferenza relativa ad una lista, ovvero, in termini assolutamente generici, poter esprimere un voto composto scegliendo prima dall'elenco delle liste di candidati e completandolo poi con preferenze espresse fra candidati appartenenti alla lista scelta.

Questa estensione con voto di lista *congiunto* (ovvero che vincola la scelta affettiva dei candidati) è forse l'estensione più immediata del sistema di voto attuale.

In pratica, invece di avere un unico elettorato passivo omogeneo, esso verrebbe ripartito in funzione dell'appartenenza alle liste presenti.

In questo scenario, l'applicazione di voto

dovrebbe semplicemente selezionare quale dei sotto-elettorati debba essere proposto in funzione di una prima espressione di voto con la quale acquisire la preferenza di lista. L'unica accortezza da tenere in conto per l'implementazione di tale estensione, oltre all'ovvia conferma del voto di lista e delle preferenze ad esso collegate, è che l'intera azione avvenga comunque all'interno di un'unica transazione, in modo che non si possano verificare situazioni di parziale espressione di un voto complesso come questo, difficilmente recuperabili in quanto l'inevitabile anonimizzazione delle singole espressioni di voto renderebbe difficoltoso ricondurre l'elettore all'esatto punto in cui una simile interruzione fosse avvenuta. Così come avviene tuttora per l'espressione di semplici preferenze multiple, è molto più semplice e sicuro gestire la registrazione dell'intero *voto composto*, completo di voto di lista e di referenze, all'interno di un'unica operazione atomica.

#### **Identificazione degli elettori**

Lo schema attuale di identificazione degli elettori nei confronti del sistema di voto prevede l'uso di un certificato elettorale cartaceo contenente una *one-time password* per accedere alla propria sessione di voto. Questo schema si è rivelato soddisfacente per le realizzazioni fatte nell'ambito accademico, anche perché la necessità di avere comunque del personale assegnato alla gestione del seggio telematico rende pressoché trascurabile l'aggravio derivante da riconoscimento della persona e consegna del corrispondente certificato cartaceo.

Tuttavia, soprattutto in situazioni di minore criticità, sono ipotizzabili meccanismi di auto-identificazione degli elettori in seggi non presidiati o con un presidio più leggero, ad esempio una semplice sorveglianza sufficiente a garantire la sicurezza e l'integrità degli apparati.

In tali situazioni potrebbe, ad esempio, essere impiegata una smart card personale assegnata all'elettore da utilizzare per accedere al sistema. Chiaramente, i costi connessi all'uso di questo strumento renderebbero applicabile tale schema solo in situazioni in cui si voti con una certa periodicità dal momento che, oltre alle ulteriori smart card, andrebbe prevista una postazione di voto dotata di due lettori, o

*Grazie agli sviluppi ed agli affinamenti che il sistema di voto telematico del CINECA ha subito nel corso degli ultimi anni, la casistica di tipologie di elezioni con esso gestibili si è via via ampliata. Attualmente, l'impegno del Consorzio è orientato all'analisi delle problematiche poste dalle elezioni studentesche*

*Nelle evoluzioni del sistema di voto telematico rispetto alla sua struttura iniziale, sono state mantenute le caratteristiche che avevano decretato il successo del modello originale*

## Ancora un altro successo del voto telematico nelle Università

Vincenzo Tedesco

Responsabile UO7 Organico-reclutamento personale docente,

Responsabile Ufficio Studi, Programmazione e Valutazione dell'Università di Pisa

Si sono concluse in ottobre presso l'Università di Pisa, pioniera di questi eventi, le elezioni per il rinnovo delle cariche accademiche che si sono svolte con il sistema di voto elettronico messo a punto dal CINECA.

L'eccezionalità dell'evento è data dal fatto che l'interfaccia di voto ha gestito in un'unica sessione ben quattro tipologie di votazioni:

- le elezioni dei rappresentanti dei dipartimenti e del personale tecnico amministrativo per il Senato Accademico;
- le elezioni della rappresentanza del personale tecnico-amministrativo avente l'elettorato attivo per le elezioni del Rettore;
- le elezioni dei componenti delle Commissioni Scientifiche di Area;
- le elezioni suppletive per un rappresentante dei professori di II fascia e dei ricercatori nel Consiglio di Amministrazione.

A questo scopo sono stati implementati quattro diversi database, ognuno con i candidati potenziali destinatari delle preferenze di ogni singola votazione: per le elezioni sub2 erano elencati addirittura 211 candidati.

Non ci si trovava dunque di fronte ad un sistema di interazione semplice con l'elettore, nel senso che la coppia di password e chiave di identificazione fornita abilitava a tante elezioni quante ogni singolo utente era tenuto a votare, quindi la corretta definizione degli elettorati ha costituito un momento imprescindibile nell'implementazione del sistema.

A ciò si aggiunga l'altissima percentuale dei votanti, quasi il 72% complessivo pari a 2623 elettori, che la dice lunga sull'altissimo dato dell'affluenza e sulla capacità "ricettiva" di un sistema di voto elettronico implementato con otto postazioni abilitate alla votazione. Si pensi per un attimo che in una normale votazione cartacea la massima capacità di un seggio non supera i 500 elettori. Le persone impegnate nel seggio sono state nove, e meritano un plauso per la dedizione, la professionalità, l'eccezionale disponibilità verso tutti gli elettori. Per concludere, perfetto come sempre si è dimostrato il sistema di assistenza on line dei colleghi del CINECA, fondamentale in alcuni casi per risolvere le situazioni di calo della rete, di congestione fisiologica quando tutti gli apparati tecnici funzionavano a pieno regime.

di un lettore doppio, in modo da conservare l'uso delle smart card di attivazione della postazione (che regola anche il meccanismo mediante il quale vengono resi anonimi tutti i voti depositati nell'urna).

### Ridondanza del voto e parallelizzazione dello scrutinio

Nel sistema di voto telematico del Consorzio viene utilizzata la chiave pubblica della smart card del *Responsabile del Procedimento* (la *carta blu*) per cifrare i voti da depositare nell'urna. Questo schema garantisce che solo chi sia in possesso di tale carta, e dei relativi codici di attivazione, sia in grado di scrutinare l'insieme di voti. La carta blu, dunque, risulta critica per il funzionamento complessivo del

sistema: a ulteriore garanzia della sicurezza del sistema, è previsto che nel caso di un eventuale guasto o smarrimento della carta sia necessario effettuare nuovamente tutte le consultazioni elettorali ad essa connesse. L'operazione di *key recovery*, prevista nella procedura, implica la creazione e spedizione della nuova carta presso il seggio di appartenenza: lo scrutinio, dunque, non potrà essere effettuato fino all'arrivo della nuova carta.

Per eliminare questo *Point of Failure* del sistema senza introdurre ritardi nei tempi di scrutinio in caso di smarrimento della smart card, e senza alterare gli standard di sicurezza, occorre introdurre una carta di backup immediatamente disponibile in loco. Il responsabile del procedimento avrebbe quindi il possesso della smart

card principale, mentre quella di backup andrebbe conservata separatamente nell'ambito dell'organizzazione responsabile della votazione. Il sistema verrebbe modificato in modo che i voti vengano cifrati con la chiave pubblica di entrambe le carte: in questo modo sarebbe possibile scrutinare i voti anche con la carta di backup che, ovviamente, verrebbe abilitata all'operazione solo in caso di smarrimento di quella principale.

L'introduzione di carte multiple è un aspetto interessante delle modifiche nel sistema di voto telematico, poiché consente di velocizzare le operazioni di scrutinio. Attualmente i tempi di scrutinio sono vincolati dal fatto che ogni singolo voto deve essere decifrato dalla carta del responsabile del procedimento. Con le tecnologie attualmente impiegate, questo implica un aggravio di circa 1,1 secondi per ogni singolo voto decrittografato.

Supponendo una dimensione dell'elettorato attivo dell'ordine delle decine di migliaia di persone, tali tempi rischiano di arrivare a picchi di diverse ore, quindi difficilmente proponibili in una situazione come quella di una elezione studentesca, ove, inoltre, il numero stesso degli scrutini da effettuare sarà presumibilmente elevato.

Una soluzione che il CINECA ha già sperimentato per risolvere questo problema è *parallelizzare* lo scrutinio su diverse carte crittografiche. Invece di utilizzare una sola urna associata alla chiave pubblica dell'unica smart card del responsabile del procedimento, si suddividono i voti su un certo numero di urne parziali, di dimensioni inferiori, ciascuna associata alla

chiave pubblica di una diversa smart card e dimensionata per contenere un numero di voti scrutinabile in un tempo ragionevole.

Al termine della votazione, usando più postazioni di scrutinio, il responsabile del procedimento potrà utilizzare contemporaneamente tutte le smart card: ognuna di esse decifrerà i voti contenuti nella corrispondente urna parziale riducendo il tempo necessario allo scrutinio di un fattore pari al numero di carte impiegate. Terminati tutti gli scrutini parziali una delle smart card impiegate sarà in grado di consolidare tutti i risultati in un'unica graduatoria.

Tale schema viene già impiegato per le elezioni di primo grado per il rinnovo del Comitato Direttivo dell'Istituto Nazionale di Alta Matematica (INdAM), ove il fatto che ogni elettore possa esprimere fino a 12 preferenze dà origine a circa 20.000 voti esprimibili da scrutinare.

Anche utilizzando questa tecnica si può comunque utilizzare la tecnica di ridondanza descritta precedentemente, anzi è possibile fare in modo che ogni carta del Responsabile del procedimento sia la carta di backup di una delle altre, per ottenere i vantaggi già descritti senza dover raddoppiare il numero di smart card ma solo al costo di un aumento del tempo di scrutinio di una quantità pari al tempo necessario per scrutinare un'urna parziale (nel caso una delle due smart card vada smarrita).

*Per ulteriori informazioni:*

<http://www.cineca.it/evote>  
[evote@cineca.it](mailto:evote@cineca.it)

Nelle evoluzioni del sistema di voto telematico rispetto alla sua struttura iniziale sono state mantenute le caratteristiche che avevano decretato il successo del modello originale, ovvero:

- impossibilità di risalire al voto espresso dall'elettore;
- inalterabilità dei voti;
- impossibilità di conoscere i risultati parziali a seggi ancora aperti;
- identificazione fisica degli elettori tramite l'intervento di un componente del seggio al momento del voto;
- apertura dell'urna solo al termine delle operazioni di voto e solo da parte del Responsabile del Procedimento;
- impiego di una Public Key Infrastructure e algoritmi di crittografia riconosciuti come standard internazionali.