CINECA
Consorzio Interuniversitario

Il sistema di voto telematico per le elezioni del Consiglio Universitario Nazionale

Il documento descrive le funzionalità e le procedure atte a consentire lo svolgimento delle elezioni del Consiglio Universitario Nazionale (CUN) tramite il sistema di voto telematico già in uso in tutti gli atenei italiani per le votazioni dei membri delle Commissioni di valutazione comparativa dei concorsi universitari.

0 Indice

1 Introduzione

Dal giugno 1999 il MIUR fa uso di un sistema di voto telematico per la elezione dei membri delle Commissioni di valutazione per il reclutamento dei docenti e dei ricercatori universitari. Il sistema, usato su base nazionale, è stato validato da una apposita Commissione ministeriale di esperti, che ne ha certificato i requisiti di sicurezza, anonimato e integrità del voto.

Tale sistema, oltre che certificato, risulta essere anche largamente collaudato sul campo, essendo stato usato in occasione di tutte le sessioni nazionali di voto che si sono svolte dal momento della sua entrata in servizio.

In questo documento viene presentata una variante del sistema che, conservando tutti i suddetti requisiti, consente lo svolgimento delle elezioni del Consiglio Universitario Nazionale (nel seguito **CUN**).

1.1 Peculiarità delle votazioni CUN

Rispetto alle elezioni delle Commissioni di valutazioni Comparativa, le elezioni del **CUN** presentano alcune peculiarità che qui evidenziamo:

1. Nelle elezioni del **CUN** sono coinvolti nella votazione sia Docenti e Ricercatori Universitari che personale Tecnico-Amministrativo. Questo implica un afflusso potenziale di circa il doppio di elettori;
2. I docenti votano in collegi partizionati per fascia e area scientifico-disciplinare d'appartenenza; questo rende tali votazioni strutturalmente analoghe a quelle delle commissioni di Valutazione Comparativa;
3. Il personale Tecnico-Amministrativo vota per un unico collegio, la cui urna potrebbe avere un numero di voti estremamente elevato;
4. L'elettorato passivo di ogni collegio è composto dai candidati di cui sono state accettate le candidature;
5. tutte le votazioni vengono scrutinate da un'unica entità centrale.

2 Il sistema di voto telematico CUN

Nel seguito vengono illustrate le caratteristiche principali del sistema di voto telematico progettato dal CINECA per le elezioni del **CUN**, evidenziando le parti nelle quali tale sistema si differenzia da quello impiegato per le elezioni delle Commissioni di valutazione comparativa.

2.1 Caratteristiche generali della soluzione

Il progetto del sistema soddisfa i seguenti requisiti:

a. garantisce che non sia possibile risalire al voto espresso dai singoli elettori, che i voti non siano alterabili, né che sia possibile conoscere i risultati parziali a seggi ancora aperti;

b. consente l'identificazione fisica degli elettori tramite l'intervento della commissione di seggio al momento del voto;

c. l'urna può essere aperta solo al termine delle operazioni di voto e solo dal Presidente della Commissione elettorale centrale;

d. il sistema si appoggia su una Public Key Infrastructure e utilizza algoritmi di crittografia riconosciuti come standard internazionali.

2.2 Aspetti organizzativi: operazioni preliminari

L'espressione del voto avviene presso un seggio, nel quale è richiesta la presenza di una commissione elettorale. Il modello di sicurezza adottato richiede infatti che il seggio elettorale sia ad accesso controllato.

Prima dell'inizio della sessione di voto, ai singoli atenei vengono consegnati dei "certificati elettorali" nominativi, uno per ciascun elettore previsto presso quel seggio. Un certificato elettorale è costituito da una busta sigillata contenente un codice personale ed una chiave di identificazione per l'elettore.

La commissione di seggio detiene delle smartcard, una per ciascuna postazione di voto presente presso il proprio seggio, che vengono impiegate usualmente per attivare le postazioni di voto per le votazioni delle Commissioni di valutazione comparativa. Tali smartcard sono le stesse che dovranno essere usate per le votazioni CUN.

Nelle votazioni CUN, diversamente dalle votazioni delle Commissioni di valutazione comparativa, al Presidente della Commissione centrale viene affidata la smartcard che abilita la postazione di scrutinio, con la quale è in grado di effettuare lo spoglio dei voti a votazione conclusa. Caratteristiche e funzioni di tale postazione informatica verranno descritte nella sezione 5.

2.3 L'identificazione degli elettori

L'accertamento dell'identità degli elettori avviene a cura della commissione di seggio, che si avvale di normali documenti di riconoscimento muniti di foto. All'elettore identificato viene consegnato il certificato elettorale personale sigillato, col quale può accedere alla postazione di voto. Il certificato vale esclusivamente per il turno di voto per il quale viene emesso.

2.4 Svolgimento delle operazioni di voto

Una volta ritirato il proprio certificato elettorale, l'elettore può procedere al voto seguendo una semplice procedura che comprende i passi seguenti.

1. L'elettore accede alla postazione di voto, apre il proprio certificato elettorale e digita il proprio codice personale.
2. Il sistema mostra l'identità associata a tale codice e chiede all'elettore di confermarla. Questa fase permette di evitare che un errore nella digitazione del codice possa condurre ad una erronea identificazione dell'elettore.
3. Una volta che l'elettore abbia confermato la propria identità, il sistema chiede di digitare la chiave segreta di identificazione.
4. Se la chiave segreta di identificazione inserita è corretta, l'elettore viene accreditato presso il sistema. Il sistema presenta a questo punto la lista dei candidati, ovvero degli elettori eleggibili per la votazione in corso che hanno presentato una candidatura formale.
5. A ciascun nominativo è associato un numero progressivo e fra le scelte possibili è prevista anche la "scheda bianca". Nel caso in cui la lista dei candidati sia più lunga della pagina, sono disponibili le seguenti modalità di selezione:
    a. Selezione tramite appositi tasti-cursore che permettono lo scorrimento "in alto" e "in basso" all'interno della lista;
    b. selezione per iniziale del cognome: battendo la prima lettera di un cognome il cursore si posiziona al primo cognome avente tale iniziale;
    c. selezione per codice: battendo un numero il cursore si sposta sull'elettore passivo a cui è stato attribuito tale numero come codice.
6. L'espressione della propria preferenza viene fatta selezionando con uno dei metodi appena indicati uno degli elettori passivi elencati in lista e premendo un apposito tasto di conferma.
7. Prima che la preferenza espressa venga inviata all'Urna Centrale, il sistema richiede una ulteriore esplicita conferma della propria volontà all'elettore, da effettuare con un pulsante di conferma differente da quello usato al punto precedente, onde evitare che una pressione accidentale della tastiera possa provocare espressioni di voto indesiderate.
8. Dopo tale ulteriore e irrevocabile conferma, il voto viene cifrato e inviato all'Urna Centrale, che a sua volta emette una conferma che viene visualizzata a video.
   Con tale invio, la preferenza diviene non più modificabile, né revocabile.

9. Poiché nelle votazioni CUN ogni elettore è chiamato ad esprimere un'unica preferenza per un'unica votazione, l'elettore con l'espressione della propria preferenza termina la procedura di voto. Questo viene pertanto segnalato a video all'elettore ed esso può quindi abbandonare la postazione di voto.
   Parallelamente a questo, la stampante del seggio stampa una riga del verbale contenente data, ora, numero della postazione, cognome e nome dell'elettore e l'indicazione "ha votato", in modo che anche il personale del seggio possa essere notificato dell'avvenuto termine di tale procedura di voto.

Per ragioni di sicurezza, così come accade nelle elezioni tradizionali, non è possibile frazionare l'operazione di voto: un elettore che è entrato in cabina ed ha iniziato la procedura non può uscirne per sospenderla, pretendendo poi di rientrarvi in un momento successivo per completarla.

Solo in caso di problemi tecnici, quale blocco del calcolatore, della rete, ecc., sarà possibile ripetere l'operazione fino a quando il voto non sarà correttamente giunto all'Urna Centrale.

Il funzionamento della postazione di voto è subordinato alla presenza nel lettore della smartcard abilitante, che viene inserita all'apertura dal presidente di seggio.

Ogni inserimento ed estrazione della smartcard viene riportato sul verbale prodotto dalla stampante del seggio, che pertanto riporterà sia le indicazioni di attivazione e disattivazione delle singole postazioni del seggio, sia le indicazioni delle avvenute espressioni di voto dei singoli elettori.

2.5 Svolgimento delle operazioni di scrutinio

Lo scrutinio dei voti delle votazioni **CUN** avviene secondo un protocollo simile a quello predisposto dal CINECA per le elezioni delle Commissioni di valutazione comparativa, operando però una modifica marginale.

Poiché tale protocollo originariamente prevede l'uso di una smartcard per decifrare i voti delle votazioni afferenti al Responsabile del Procedimento, nel caso delle votazioni **CUN**, a causa della mole di voti potenzialmente in gioco, vi sarebbe potuto essere una eccessiva durata dello scrutinio complessivo di tutti i collegi delle votazioni **CUN**.

Infatti una smartcard crittografica del tipo di quelle normalmente impiegate dal CINECA richiede, per decifrare ogni singolo voto, un tempo dell'ordine del minuto secondo, cosicché lo scrutinio di tutti i collegi della votazione **CUN**, nell'ipotesi di una affluenza al voto dell'intero corpo votante, avrebbe potuto avere tempi di scrutinio dell'ordine delle 36 ore.

Per risolvere tale problema il CINECA appronta per il Ministero una apposita Postazione di Scrutinio costituita da un Personal Computer equipaggiato con un dispositivo denominato Token Crittografico ad alte prestazioni.

Tale token crittografico è per i nostri scopi a tutti gli effetti assimilabile ad una smartcard crittografica, con la differenza di avere una velocità di circa due ordini di grandezza superiore.

In particolare esso ha le seguenti proprietà:

- consente l'impiego di chiavi private RSA attraverso una apposita interfaccia applicativa tramite cui esso esegue al suo interno tutte le operazioni crittografiche che ne coinvolgono l'uso
- protegge l'accesso diretto alla parte privata delle coppie di chiavi RSA in esso generate e custodite
- consente al contempo un eventuale recovery sicuro delle chiavi tramite l'uso di apposite smartcard multiple.

Questa modifica architetturale, peraltro marginale viste l'analogia funzionale tra i dispositivi illustrati, è sufficiente a ridurre i tempi di scrutinio per quanto attiene le votazioni del **CUN** entro due ore.

Il Presidente della commissione elettorale centrale mediante la postazione di scrutinio completa del token crittografico è in grado di effettuare lo scrutinio, che comunque può avvenire solo dopo la chiusura delle operazioni di voto.

L'operazione di scrutinio si articola nei seguenti passi:

1. attivazione della postazione di scrutinio;
2. digitazione del PIN (codice di sicurezza) per consentire l'attivazione del token crittografico;
3. l'applicazione di scrutinio, dopo aver verificato telematicamente con l'Ufficio Elettorale Centrale che l'elezione sia chiusa, si fa consegnare dall'Urna Centrale l'elenco degli scrutini eseguibili tramite la postazione e propone l'esecuzione del primo scrutinio al Presidente della commissione elettorale centrale;
4. Su conferma del Presidente della commissione elettorale centrale, la postazione di scrutinio si fa consegnare dai server centrali i voti cifrati dello scrutinio richiesto;
5. il token crittografico decifra i voti e i risultati vengono visualizzati e stampati.

Il predetto procedimento viene iterato per ognuno dei collegi in cui si suddivide la votazione **CUN**, fino al completamento di tutti gli scrutini presenti.

3 Architettura del sistema

I componenti fondamentali del sistema di voto telematico sono:

- La Public Key Certification Authority (ne seguito detta **CA**);
- L'Ufficio Elettorale Centrale (nel seguito detto **UEC**);
- L'Urna Centrale (nel seguito detta **UC**);
- I seggi;
- La rete di comunicazione.

Uno degli elementi caratterizzanti l'architettura è la presenza di due server centrali, l'**UEC** e l'**UC**, fisicamente separati e organizzati in maniera da consentire la separazione dell'identità dell'elettore dai voti da questi espressi. L'uso della cifratura delle preferenze espresse, inoltre, consente di inficiare eventuali tentativi di incrociare i dati.

I server centrali si trovano in un ambiente fisicamente controllato e vigilato 24 ore al giorno, 7 giorni su 7 e offrono garanzie di alta affidabilità, tali da consentire il corretto funzionamento anche in presenza di un singolo guasto su un qualunque apparato.

3.1 La Public Key Certification Authority

L'autorità di certificazione (Certification Authority, CA) costituisce l'infrastruttura di base per identificare due tipi di entità:

1. il Presidente della commissione elettorale centrale (nel seguito denominato **PdEC**);
2. le postazioni di voto (nel seguito dette **PdV**).

A ciascuna entità viene rilasciato un certificato digitale in formato X.509v3, associato ad una coppia di chiavi RSA memorizzate in una smartcard crittografica. La coppia di chiavi che certifica **PdEC** è invece generata e custodita all'interno del token crittografico ad alte prestazioni che costituisce la postazione di scrutinio.

Si noti come nel seguito con il termine **PdEC** non si intenda la persona fisica nominata Presidente della commissione elettorale centrale, ma la singola entità funzionale detentrice del diritto di scrutinio, ovvero nella fattispecie il token crittografico della postazione di scrutinio.

3.2 L'Ufficio Elettorale Centrale

Compito dell'Ufficio Elettorale Centrale (**UEC**) è quello di conservare i dati relativi alla votazione in corso. In particolare l'**UEC** gestisce la lista degli aventi diritto al voto (elettorato attivo), degli eleggibili (elettorato passivo) e dello stato di ciascun elettore attivo per quanto riguarda l'esercizio del proprio diritto di voto. Emette le autorizzazioni al voto e tiene traccia del loro utilizzo dialogando con l'Urna Centrale. Conserva inoltre una copia dei certificati X.509v3 di tutte le entità coinvolte nelle operazioni.

Le uniche informazioni non gestite dall'**UEC** sono quelle che riguardano il contenuto dei voti espressi.

3.3 L'Urna Centrale

L'Urna Centrale (**UC**) è il contenitore dei voti espressi per la votazione in corso. Non dispone di alcuna nozione sull'identità degli elettori, ma è in grado di riconoscere ed accettare i voti validi grazie alle autorizzazioni al voto comunicate dall'**UEC**. Le autorizzazioni al voto non contengono alcun riferimento all'elettore al quale sono state rilasciate. I voti vengono ricevuti e immagazzinati in forma cifrata e l'**UC** non dispone delle chiavi di decodifica. In fase di scrutinio, i voti cifrati vengono estratti e inviati alla postazione di scrutinio, e solo all'interno del suo token crittografico avverrà la decodifica.

L'**UC** si trova su un ambiente operativo separato rispetto all'**UEC** e può essere gestita da una diversa entità amministrativa. Le uniche comunicazioni fra **UC** e **UEC** sono quelle previste dal protocollo applicativo per la comunicazione delle autorizzazioni di voto e delle loro variazioni di stato.

3.4 Il seggio

Il seggio costituisce l'interfaccia verso i servizi centrali. E' presidiato da una Commissione elettorale che ha il compito di identificare fisicamente gli elettori. I client dedicati installati sulle Postazioni di Voto dialogano sia con l'**UEC** per ottenere le autorizzazioni, sia con l'UC per inviare le espressioni di voto. Le **PdV** non conservano localmente nessuna informazione di stato e dipendono quindi totalmente dai server centrali, presso i quali si autenticano grazie alle smartcard.

Sulle **PdV** non viene effettuato alcun tipo di logging, caching o altro che possa consentire di tener traccia delle preferenze espresse. Una stampante produce in tempo reale il verbale delle operazioni del seggio, riportando i nominativi dei votanti, gli eventi significativi (quali attivazione e disattivazione delle **PdV**) e i riepiloghi periodici sulle affluenze.

3.5 La rete di comunicazione

Le postazioni di voto del seggio e la stampante sono connessi fra loro in rete locale sulla quale è presente un router. I protocolli di comunicazione sono quelli della suite TCP/IP, con network private. Presso il seggio sono installati due accessi ISDN BRI (Basic Rate Interface), al fine di garantire la funzionalità del seggio anche nel caso di un guasto su una linea.

La LAN di ogni seggio è connessa via ISDN punto-punto direttamente ai sistemi centrali. Ciascuna linea ISDN è configurata come facente parte di un gruppo chiuso di utenza (CUG), tale da non consentire interazioni con numeri esterni al gruppo definito. La modalità di utilizzo è di tipo dial-on-demand, con apertura dinamica del secondo canale "B" in caso di traffico sostenuto.

L'uso di ISDN al posto della dorsale pubblica di Internet è dovuto a motivi di affidabilità e qualità del servizio, oltre che a ragioni di sicurezza. Tutti gli apparati di rete sono gestiti e controllati centralmente. Allo scopo di garantire un tempestivo supporto tecnico durante le fasi del voto e di diagnosticare rapidamente eventuali anomalie di funzionamento, ciascun seggio è dotato anche di un telefono ISDN che consente comunicazioni esclusivamente con il Supporto Tecnico centrale presso il CINECA, senza neppure la necessità di comporre un numero telefonico.

La postazione di scrutinio può essere attestata su di un collegamento analogo a quello descritto per le postazioni di voto oppure può essere attestata su di una intranet connessa al sistema di voto tramite una connessione VPN.

4 Il protocollo applicativo

Il protocollo applicativo specifica le relazioni fra le entità del sistema di voto telematico ed ha lo scopo di garantire i requisiti di legittimità, integrità, segretezza e anonimato del voto.

Per *legittimità* si intende che deve poter votare solo chi ne ha diritto ed una volta soltanto.

Col termine *integrità* si intende che il voto non deve poter essere modificabile una volta che è stato espresso.

Il termine *segretezza* è relativo al fatto che il contenuto della preferenza non deve poter essere visibile prima dello scrutinio.

Il requisito dell'*anonimato* riguarda l'impossibilità di associare un voto all'identità dell'elettore che lo ha espresso.

Tutte le comunicazioni avvengono in forma cifrata col protocollo SSLv3 (Secure Socket Layer) con chiavi RSA a 1024 bit. Il client e il server si identificano reciprocamente ad ogni operazione tramite certificati X.509v3.

4.1 La fase di voto

I flussi informativi durante la fase di voto sono schematizzati in Figura 1.

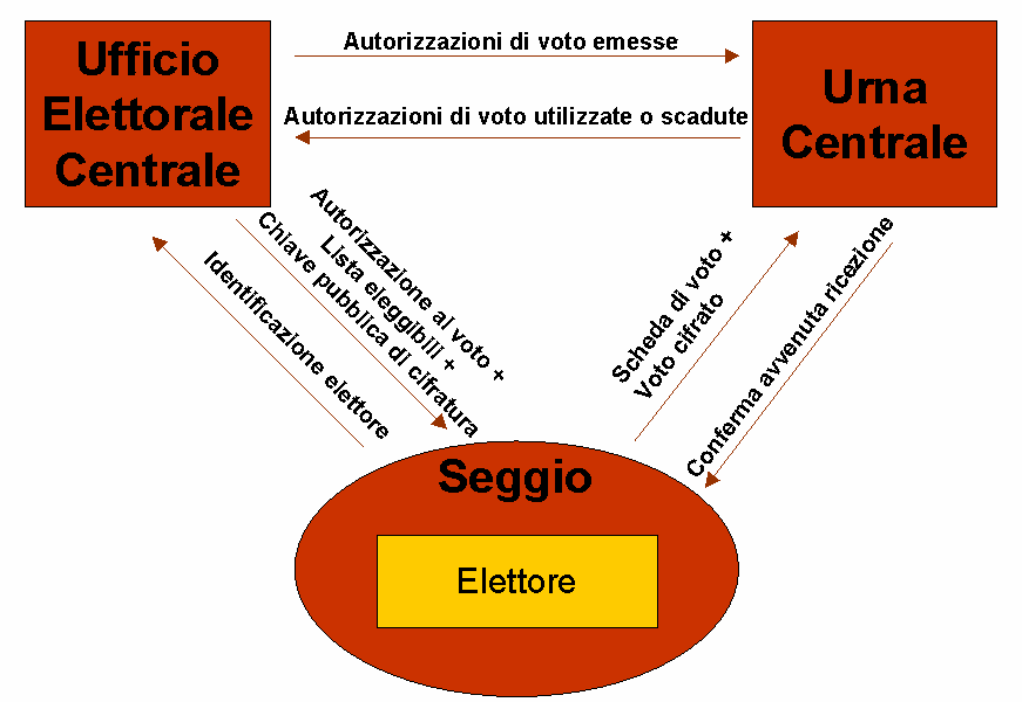

Figura 1: La fase di voto

La legittimità viene garantita dall'**UEC**, che autorizza al voto gli elettori una volta soltanto.

La firma di **PdV** garantisce sull'integrità dei voti.

L'*autorizzazione al voto* viene utilizzata dall'**UC** per decidere se un voto è valido e non viene conservata una volta che ha assolto la propria funzione.

I voti immagazzinati nell'**UC** sono cifrati con la chiave pubblica del **PdEC** e sono firmati con la chiave privata della **PdV** dalla quale provengono. La cifratura risponde ad esigenze di segretezza ed impedisce di conoscere i risultati parziali prima della fine delle operazioni di voto. Inoltre rende inutile, come vedremo nel seguito, anche un eventuale incrocio dei dati fra **UEC** e **UC**, che comunque è impedito dal protocollo.

L'anonimato è ottenuto congiuntamente da cifratura, separazione di **UEC** e **UC**, assenza di dati identificativi dell'elettore nell'autorizzazione al voto e non conservazione di tale autorizzazione da parte di **UC**.

4.2 La fase di scrutinio

Al termine delle operazioni di voto, **UEC** autorizza le operazioni di scrutinio che vengono effettuate a cura di **PdEC**.

Il susseguirsi delle operazioni di scrutinio è schematizzato in Figura 2.

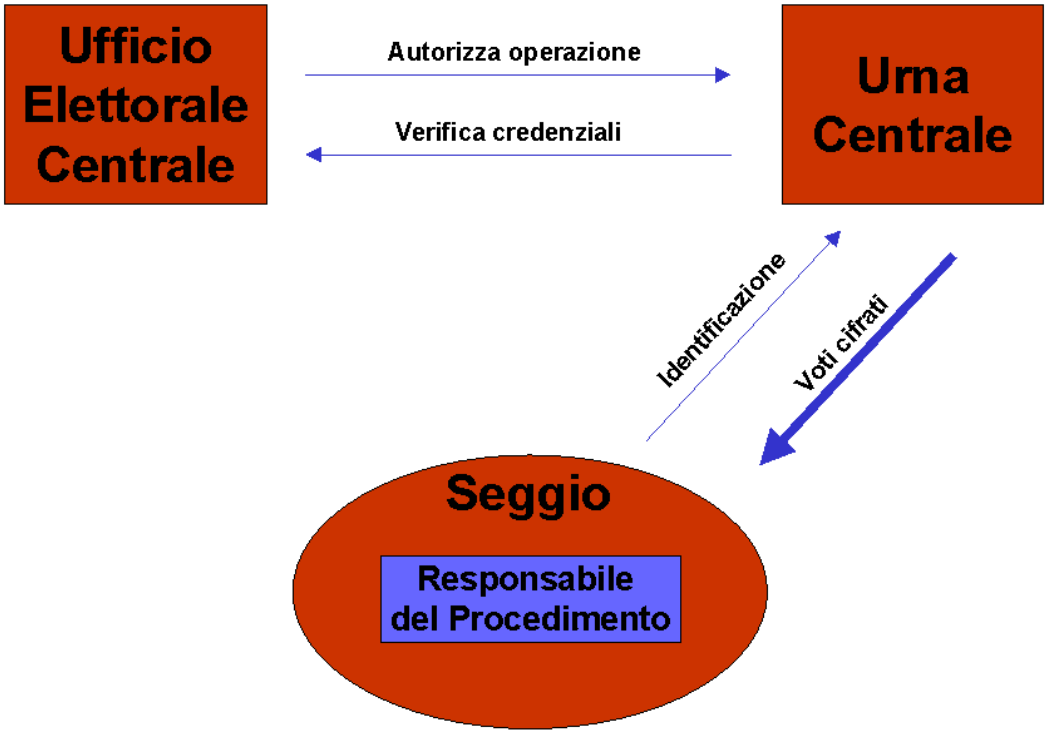

Figura 2: La fase di scrutinio

L'infrastruttura di sicurezza

Compito dell'infrastruttura di sicurezza del sistema è quello di garantire la segretezza, l'anonimato e l'integrità dei voti. La segretezza e l'integrità del voto devono durare fino allo scrutinio, quando il voto viene conteggiato, mentre l'identità dell'elettore che lo ha espresso non deve essere mai ricostruibile neppure a posteriori.

Per garantire questi requisiti si fa largo uso di algoritmi crittografici in tutte le fasi del processo.

Presso l'**UC** non c'è alcuna informazione che consenta di decifrare i voti, né di risalire all'elettore che ha espresso un certo voto, ma solo la firma della postazione dalla quale quel voto proviene. Scopo della firma è quello di consentire la verifica che i voti presenti nell'**UC** sono stati effettivamente generati da una postazione di voto autorizzata.

4.3 La decodifica per lo scrutinio

Al momento dello scrutinio i voti vengono estratti dall'**UC** e inviati alla postazione di scrutinio, secondo le modalità previste dal protocollo applicativo descritto. Le comunicazioni fra **UC** e **PdV** sono protette tramite **SSL**.

Si osservi che il ruolo dell'**UC** è solo quello di conservare temporaneamente i voti cifrati, per poi inviarli in fase di scrutinio alla postazione presso la quale si trova il **PdEC**: lo scrutinio effettivo avviene dunque nella postazione di scrutinio.

4.4 I dispositivi crittografici

L'infrastruttura di sicurezza è basata su dispositivi crittografici con capacità elaborativa che implementano l'algoritmo crittografico a chiave pubblica **RSA**, aventi le proprietà che:

- proteggono l'accesso alla chiave privata,
- necessitano di una chiave di attivazione (ad esempio un codice PIN).

Nella architettura del sistema descritto dispositivi aventi tali proprietà sono le smartcard utilizzate nelle postazioni di voto e il token crittografico ad alte prestazioni costituente la postazione di scrutinio.

4.5 Identificazione delle PdV

I server centrali conoscono la configurazione di ciascun seggio e prima di interagire con le postazioni remote pretendono che:

1. la connessione ISDN provenga dal caller-id atteso (la presenza all'interno del CUG è garantita dalla compagnia telefonica);
2. i router presentino le necessarie credenziali al server di autenticazione;
3. l'hardware delle postazioni sia quello atteso. Solo a queste sarà consentito effettuare il bootstrap;
4. ciascuna **PdV** deve presentare un certificato X.509v3 valido per il seggio nel quale si trova. Il certificato, presente sulla smartcard, consente la client authentication con SSL. Se la smartcard viene estratta o avvengono eventi che interferiscono con il suo regolare colloquio con la **PdV** (quali distacco o spegnimento del lettore) l'applicazione si blocca;
5. il seggio deve risultare in orario di apertura per l'operazione che la **PdV** si accinge a svolgere. La funzione di scrutinio è possibile solo se la fase di voto è già stata completata in tutti i seggi.

5 Certificazione del sistema

L'architettura descritta è funzionalmente del tutto simile a quella che è stata sottoposta al vaglio di una Commissione di esperti nominata dal Ministero dell'Istruzione, dell'Università e della Ricerca, quale garante del corretto svolgimento del processo elettorale nei confronti della comunità accademica italiana. Compito della Commissione è stato quello di esaminare gli aspetti di sicurezza del sistema e determinare se questi sono sufficienti a garantire segretezza, anonimato e integrità dei voti.

La Commissione ha certificato che il sistema rispetta i requisiti di sicurezza richiesti.

Le varianti introdotte a livello di interfaccia di sistema per soddisfare i requisiti richiesti per la elezione del **CUN**, non alterano il protocollo di trasmissione che implementa i meccanismi di sicurezza richiesti.