Votazioni Cnr – Descrizione

Configurazione e inizializzazione sistema

Per ogni votazione è necessario l'inserimento dell'elettorato attivo, dei membri della Commissione e dei candidati. Per i primi due è necessario inserire le relative matricole e/o codici fiscali per l'associazione con i propri account Cnr che verranno utilizzati per l'accesso al sistema.

È necessario inserire data e ora di apertura e di chiusura della votazione. Il Sistema gestisce automaticamente la possibilità di votare o meno fornendo opportuna messaggistica agli utenti.

Prima della data e ora di apertura della votazione è indispensabile che almeno due membri della Commissione si riuniscano per la fase di generazione delle chiavi di criptazione.

Generazione chiavi

La generazione delle chiavi (pubblica e privata) viene effettuata da più membri della commissione, presenti contemporaneamente al momento della generazione. In particolare viene effettuato l'accesso al sistema attraverso le credenziali Siper di un membro della commissione, una volta acceduti nell'apposita area destinata ai commissari è possibile per ogni votazione generare le corrispettive chiavi.

I commissari possono decidere il numero di chiavi da generare (numero minimo consentito 2), una volta generate, la piattaforma automaticamente salva le chiavi pubbliche, e avvia il download delle chiavi private che viene effettuato in doppia copia per ogni chiave sulle pendrive fornite dalla commissione.

Effettuato il download, direttamente sulle pendrive e create le copie, le chiavi vengono consegnate ai commissari avendo cura che un solo commissario non sia in possesso di tutte le chiavi. Questo impedisce al singolo commissario di poter effettuare lo spoglio in assenza di altri commissari.

Al fine di garantire la bontà dell'operazione appena descritta (essendo le chiavi private l'unico modo per effettuare lo spoglio), la piattaforma mette a disposizione un test delle chiavi generate che i commissari utilizzeranno per accertarsi che effettivamente le chiavi generate consentiranno lo spoglio.

Procedura di voto

Gli utenti possono accedere alla piattaforma utilizzando le proprie credenziali Siper. Se l'utente appartiene all'elettorato attivo e se l'accesso avverrà durante la fascia di apertura della votazione, l'utente potrà esprimere la propria preferenza. Il sistema richiederà conferma prima di registrare effettivamente l'espressione di voto. Una volta che l'utente avrà confermato la sua scelta il sistema registrerà in maniera completamente disgiunta l'effettuazione del voto, con relativa data e ora e ip, e l'espressione di voto che sarà criptata per renderla segreta e anonima. Ad ogni ulteriore accesso

da parte dell'utente il Sistema non permetterà più di votare notificandogli con opportuna messaggistica di avere già espresso la propria preferenza.

Criptazione del voto

La stringa che rappresenta l'espressione di voto viene appesa in concatenazione ad una stringa generata all'istante di 32 caratteri costituita dall'*md5* di un numero random compreso tra 1 e 2147483647 per rendere diverse le stringhe criptate anche in caso di stessa preferenza.

La stringa così ottenuta viene criptata con algoritmo *AES* con una password generata all'istante di 32 caratteri ottenuta dall'*md5* di un numero random compreso tra 1 e 2147483647. La password utilizzata viene a sua volta criptata con algoritmo *RSA* con la prima chiave pubblica e poi *codificata in base 64* per ottenere una stringa composta esclusivamente di caratteri *ASCI*.

La stringa così ottenuta viene nuovamente criptata con una password generata all'istante nella stessa modalità indicata in precedenza che questa volta viene criptata con la seconda chiave pubblica.

Se durante la fase di generazione delle chiavi la Commissione avrà stabilito di generare più di due chiavi, numero minimo consentito, la procedura appena descritta verrà ripetuta per il numero di chiavi generate.

La stringa così ottenuta viene *codificata in base 64* per ottenerne una composta esclusivamente di caratteri *ASCI*.

Infine viene generata la *codifica json* di un *array* composta da due elementi:

1. la stringa dell'espressione di voto ottenuta dopo tutte le trasformazioni descritte;
2. un *array* delle stringhe delle password utilizzate per la criptazione dell'espressione di voto ottenute dopo le trasformazioni descritte.

La stringa ottenuta dalla *codifica json* contenente quindi l'espressione di voto criptata e le password criptate necessarie per la decriptazione del voto, è quella che verrà salvata sul database.

Procedura di spoglio

La procedura di spoglio viene effettuata dalla commissione, in particolare dai commissari in possesso delle chiavi private. Consiste nella generazione automatica da parte del sistema di un file zip protetto da password contenete report e risultati della votazione. Tale zip viene reso disponibile in download e contemporaneamente inviato dall'indirizzo pec del sistema all'indirizzo pec di un commissario per certificare l'avvenuta trasmissione dei risultati alla commissione. Il file zip viene generato in memoria ram volatile e non viene mai salvato sui server del sistema. Durante lo spoglio le espressioni di voto vengono mescolate, decriptate e automaticamente conteggiate senza essere salvate in alcun modo nel sistema. Ciò impedisce anche ai tecnici a supporto della commissione di conoscere l'esito della votazione. L'unico modo per ricontare i voti è effettuare nuovamente lo spoglio con le chiavi consegnate alla Commissione.

Per effettuare lo spoglio è necessario che un commissario si autentichi con le proprie credenziali Siper e acceda all'area riservata alla Commissione. Successivamente verrà richiesto l'inserimento delle chiavi private, di un indirizzo pec di un commissario, e di una password che verrà utilizzata per criptare il file zip contenete report e risultati della votazione.

Mescolamento

Prima della decriptazione di ogni singolo voto, i voti inseriti nella tabella vengono mescolati al fine di non tenere traccia dell'ordine di inserimento. Questo infatti, incrociato con il registro dei votanti in cui è registrata la data e l'orario, durante l'operazione di spoglio in cui i voti vengono decriptati potrebbe consentire di associare il voto in chiaro all'elettore che lo ha espresso.

I voti vengono estratti dal database in transazione e memorizzati in un *array* che viene a sua volta riordinata in maniera random. Successivamente vengono eliminati tutti i record nel database e vengono reinseriti salvando nuovamente tutti gli elementi presenti nell'*array*.

Prima, durante e dopo la procedura vengono effettuati dei conteggi per verificare che non si perda nessun voto. Qualora una *query* vada in errore o un conteggio dia un risultato inatteso viene effettuato il *rollback* della transazione, altrimenti viene effettuata la *commit* della transazione.

Alla fine del processo la tabella avrà gli stessi voti con un ordinamento diverso.

Decriptazione del voto

Dalla stringa json proveniente dal database vengono estratti i due elementi distinti: l'espressione di voto criptata e l'*array* delle password criptate necessarie per la decriptazione del voto.

A questo punto viene effettuato lo stesso processo della criptazione in senso inverso.

La stringa dell'espressione di voto viene *decodificata in base 64*.

La stringa ottenuta viene decriptata con algoritmo *AES* con la corretta password ottenuta prendendo l'ultimo elemento dell'*array* delle password, decodificandolo in base 64 e decriptandolo con algoritmo *RSA* con l'ultima chiave pubblica inserita.

La stringa ottenuta viene nuovamente decriptata nella stessa modalità appena descritta utilizzando la penultima password opportunamente decriptata con la penultima chiave pubblica.

Se durante la fase di generazione delle chiavi la Commissione avrà stabilito di generare più di due chiavi, numero minimo consentito, la procedura appena descritta verrà ripetuta per il numero di chiavi generate sempre rispettando l'ordine inverso.

Dalla stringa ottenuta vengono scartati i primi 32 caratteri.

La stringa ottenuta rappresenta l'espressione di voto in chiaro.