Glossario

E-voting Basilea Città / Grigioni / San Gallo / Turgovia

Autori	**Direzione di progetto e-voting (BS)** **Addetto e-voting (GR)** **Direzione Informatica e infrastruttura (SG)** **Specialista e-voting (TG)**
Data	28.04.2023
Versione	1.1
Classificazione	Nessuna

Controllo delle modifiche

Versione	Data	Descrizione	Cognome
1.0	21.12.2022	Versione approvata	Direzione di progetto e-voting (BS) Direzione Informatica e infrastruttura (SG) Specialista e-voting (TG)
1.1	28.04.2023	Integrazione dei Grigioni Completamenti e adeguamenti nel capitolo 2	Direzione di progetto e-voting (BS) Addetto e-voting (GR) Direzione Informatica e infrastruttura (SG) Specialista e-voting (TG)

Organi di verifica/di approvazione

Verificato da	Approvato da	Data
Direzione Diritto e diritti popolari (BS) Direzione Servizio per i diritti politici (SG) Direzione Servizio giuridico (TG)	Direzione Diritto e diritti popolari (BS) Direzione Servizio per i diritti politici (SG) Direzione Servizio giuridico (TG)	12.12.2022
Direzione Sezione servizi (GR)		14.04.2023

Documenti di riferimento

N.	Documento	Versione
[1]	Ordinanza della CaF concernente il voto elettronico (OVE; RS 161.116) del 25 maggio 2022	Stato 1° luglio 2022
[2]	Guida alla valutazione dei rischi della Cancelleria federale svizzera relativa al sistema di voto elettronico della Posta svizzera ("Guida alla valutazione dei rischi") https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Vote--lectronique/Leitfaden%20BK_Risikobeurteilungen%20Vote%20%C3%A9lectronique,%20Oktober%202022.pdf.download.pdf/Leitfaden%20BK_Risikobeurteilungen%20Vote%20%C3%A9lectronique,%20Oktober%202022.pdf	Versione del 04.10.2022

Indice

1 Scopo del documento

Il presente documento descrive i termini utilizzati dai Cantoni nel quadro del voto elettronico. Se nella documentazione della Posta o nell'ordinanza della CaF concernente il voto elettronico (vedi *documento di riferimento [1]*) vengono utilizzati altri termini, sarà inserito un rimando.

Per maggiore chiarezza il glossario è suddiviso in due parti: una parte per i concetti generali riguardanti il voto elettronico e una parte per i concetti tecnici.

1.1 Fonti relative all'origine delle definizioni

Laddove disponibili e opportuno, sono state utilizzate quale base le spiegazioni dei significati tratte dai documenti "Guida alla valutazione dei rischi" (vedi *documento di riferimento [2]*) e "Ordinanza della CaF concernente il voto elettronico" (vedi *documento di riferimento [1]*). Le definizioni originali dei termini elencati sono contrassegnate con caratteri speciali.

Carattere speciale	Fonte della definizione originale
*	"Guida alla valutazione dei rischi" della Cancelleria federale svizzera
**	Ordinanza della CaF concernente il voto elettronico

Tabella 1: Attribuzione dei caratteri speciali secondo la fonte

1.2 Differenze cantonali

In determinati casi le situazioni cantonali sono differenti. Nel presente documento e in tutti gli altri documenti comuni queste differenze sono contrassegnate mediante colori:

Colore	Cantone
viola	Il testo in viola vale solo per il Cantone di Basilea Città
rosso	Il testo in rosso vale solo per il Cantone dei Grigioni
verde	Il testo in verde vale solo per il Cantone di San Gallo
blu	Il testo in blu vale solo per il Cantone di Turgovia

Tabella 2: Colori che indicano le differenze cantonali

2 Glossario – termini generali

La tabella seguente fornisce una panoramica dei concetti generali rilevanti in relazione al voto elettronico.

Termine	Descrizione
Admin board	Persone responsabili per lo svolgimento tecnico della chiamata alle urne.
Programma bug bounty	Un programma bug bounty è un programma che offre una ricompensa a chi scopre e segnala punti deboli. I programmi bug bounty creano incentivi per la verifica pubblica (in particolare da parte di cosiddetti hacker etici) e contribuiscono alla sicurezza del voto elettronico permettendo di individuare ed eliminare tempestivamente i punti deboli. A partire dal 2021 la Posta ha pubblicato il codice sorgente nonché la documentazione relativa al sistema e all'esercizio sulla piattaforma specialistica GitLab. Nel quadro del suo programma bug bounty ricompensa le segnalazioni che contribuiscono a migliorare il sistema con importi che possono raggiungere i CHF 250'000.
Voto per corrispondenza, voto alle urne*	Totalità delle schede elettorali e di voto che sono state consegnate tramite voto per corrispondenza oppure alle urne.
Container	Termine del metodo "OCTAVE Allegro": istanze (fisiche o tecniche) che elaborano, salvano o trasmettono risorse di informazioni.
D0*	Unità temporale all'interno del processo: preparazione della chiamata alle urne.
D1*	Unità temporale all'interno del processo: giorno in cui le urne elettroniche vengono configurate, trasmesse al sistema online della Posta e in cui vengono generate le carte di legittimazione.
D2*	Unità temporale all'interno del processo: giorno in cui vengono definite le chiavi di sicurezza della chiamata alle urne (cfr. termine "chiave di sicurezza"), in cui viene verificata la configurazione della chiamata alle urne e in cui vengono messe a disposizione le urne elettroniche.
D3*	Unità temporale all'interno del processo: giorno in cui vengono decodificati i voti elettronici, determinati i risultati del voto elettronico e i verificatori esaminano la chiamata alle urne.

Termine	Descrizione
D4*	Unità temporale all'interno del processo: post-elaborazione della chiamata alle urne, inclusa la distruzione dei dati.
Electoral board (OVE: verificatori)	Persone che secondo il diritto cantonale sono responsabili per la vigilanza sul regolare svolgimento della chiamata alle urne elettronica e che assumono il ruolo di verificatori previsto dall'OVE. Generano le chiavi di sicurezza della chiamata alle urne (cfr. termine "chiave di sicurezza"). Nel Cantone di Basilea Città è il comitato elettorale (ordinanza sulla fase di prova per il voto elettronico, art. 8a) ad agire quale electoral board. Nel Cantone dei Grigioni è la commissione elettorale e di voto e-voting (ordinanza sui diritti politici nel Cantone dei Grigioni, art. 21g) ad agire quale electoral board. Nel Cantone di San Gallo è una commissione dell'ufficio elettorale cantonale (WAG, art. 11 segg.) ad agire quale electoral board. Nel Cantone di Turgovia è l'ufficio elettorale per gli Svizzeri all'estero (StWV, art. 26) ad agire quale electoral board.
Catalogo elettorale EV*	Registro cantonale degli aventi diritto di voto ammessi al voto elettronico.
Risultati EV*	Risultati dello spoglio delle urne elettroniche.
Oggetto della chiamata alle urne*	Domande che vengono sottoposte agli aventi diritto di voto in caso di votazioni oppure liste con i candidati in caso di elezioni.
Mezzi ausiliari per gli aventi diritto di voto	Documentazione e contenuti messi a disposizione per informare gli aventi diritto di voto (ad. es. materiale di voto, piattaforma informativa, ecc.).
Risorse di informazioni*	Termine del metodo "OCTAVE Allegro": elementi di dati particolarmente importanti, la cui integrità, confidenzialità e/o disponibilità devono essere protette.
Urna di controllo	Urna contenente i voti di controllo dei membri dell'electoral board, al fine di permettere all'electoral board di controllare l'integrità dell'urna.
Carta di legittimazione (CL)*	Un documento che consente agli aventi diritto di voto di esercitare il proprio diritto di voto.

Termine	Descrizione
Urne di prova	Urne che consentono di testare la funzionalità del sistema. Durante il processo vengono impiegate diverse urne di prova, ad esempio il D2 vengono espressi e decodificati voti di prova alla presenza dell'electoral board al fine di garantire che l'intero processo funzioni regolarmente.

Tabella 3: Termini generali

3 Glossario – termini tecnici

La tabella seguente fornisce una panoramica dei concetti tecnici rilevanti in relazione al voto elettronico.

Termine	Descrizione
Back end*	Il back end dell'ambiente e-voting viene gestito dalla Posta e comprende il server di e-voting nonché le componenti di controllo.
Cantonal computer	Normale postazione lavorativa in ufficio di un collaboratore cantonale.
Configuration computer (offline) (OVE: componente di setup) (Posta: setup SDM)	Dispositivo offline necessario per configurare una chiamata alle urne (cfr. termine "Dispositivi offline"). Su questo dispositivo vengono ad esempio generati i codici per le carte di legittimazione. In particolare, su questo dispositivo viene installato il software SDM.
Supporto dati	Chiavette USB o schede SD utilizzate per lo scambio di dati tra dispositivi.
Decryption computer (offline) (OVE: componente di controllo presso il Cantone) (Posta: Tally SDM)	Dispositivo offline necessario per mischiare e decodificare i voti (cfr. termine "Dispositivi offline"). In particolare, su questo dispositivo viene installato il software SDM.
DIS (Data Integration Service)*	Strumento della Posta per generare i file di configurazione di una chiamata alle urne.
Entropia	In crittografia con entropia si intende l'imprevedibilità dei dati. Quanto maggiore è l'entropia, tanto più complessi e imprevedibili sono i dati. In questo modo diventa più difficile decodificarli. Per la sicurezza dell'e-voting è importante che i valori che devono essere casuali lo siano in misura sufficiente e dispongano quindi di un adeguato livello di entropia.
Sistema per la determinazione dei risultati	Sistema cantonale per lo spoglio e il consolidamento dei risultati di tutti i canali di voto.
E-voting landing page	Pagina internet che la Posta mette a disposizione dei Cantoni. La landing page contiene diverse informazioni per gli aventi diritto di voto nonché link che portano alle chiamate alle urne attive nel portale per le elezioni e le votazioni.

Termine	Descrizione
Server di e-voting (OVE: parte di sistema non affidabile) (Posta: voting server)	Componente fondamentale della piattaforma di e-voting sulla quale il Cantone allestisce la chiamata alle urne tramite SDM. Il server di e-voting è parte del back end (cfr. termine "back end"), viene gestito dalla Posta e salva le urne elettroniche.
Valore hash (fingerprint)	Un valore hash (definito anche somma di controllo) è un valore generato tramite una funzione crittografica sulla base di dati. Si tratta di una sorta di impronta digitale dei dati composta da un numero fisso di byte che identifica in modo univoco i dati. I valori hash vengono utilizzati per garantire l'integrità di dati. Ogni modifica ai dati porta a un valore hash completamente diverso. Se il valore hash è identico, si sa che non è stata effettuata alcuna variazione. I valori hash rivestono un ruolo importante ad esempio nella produzione del software necessario per l'e-voting (build). Grazie ai valori hash i Cantoni possono verificare se stanno eseguendo il software corretto e invariato (cfr. termine "Trusted build e trusted deployment").
Codice di inizializzazione sulla carta di legittimazione	Il codice di inizializzazione consiste in una serie di cifre e lettere che si trovano sulla carta di legittimazione. Gli aventi diritto di voto devono inserire il codice di inizializzazione nonché una caratteristica di autenticazione supplementare sulla schermata di avvio del portale per le elezioni e le votazioni per identificarsi e dare avvio al processo di espressione del voto.
KeePass	Password manager impiegato per amministrare in modo sicuro le password.
Componenti di controllo**	Le componenti di controllo sono elementi indipendenti del sistema organizzati in modo diverso, gestiti da persone diverse e assicurati tramite misure particolari. Determinate componenti di controllo sono parte del back end (cfr. termine "back end"), vengono gestite dalla Posta e vengono impiegate in particolare per generare i codici di verifica, per verificare i codici di verifica al momento dell'espressione del voto e per mischiare le urne. Quando le urne vengono mischiate, il decryption computer funge da componente di controllo gestita presso il Cantone.
Log*	Dati mediante i quali è possibile accertare il corretto funzionamento del processo di voto o sulla base dei quali è possibile analizzare un eventuale malfunzionamento.

Termine	Descrizione
Dispositivi offline	Dispositivi isolati necessari per lo svolgimento e la verifica di una chiamata alle urne. I dispositivi offline non hanno accesso a una rete o a internet in nessun momento. I dati vengono trasferiti tramite supporti dati esclusivamente in modo codificato (cfr. termini "configuration computer" e "decryption computer").
Parametri della chiamata alle urne*	Dati di base della chiamata alle urne, ad esempio la data della chiamata alle urne, le date e gli orari nei quali è possibile esprimere il voto, il tipo di votazione e/o di elezione nonché i parametri di sicurezza (ad es. il numero di membri dell'electoral board).
Password della chiamata alle urne	Password che servono a generare la chiave di sicurezza della chiamata alle urne il D2 (le chiavi di sicurezza sono necessarie per codificare e decodificare i voti).
Password dei membri dell'admin board	Password che consentono a un membro dell'admin board di autentificarsi all'SDM (cfr. termine "SDM (secure data manager)").
SDM (Secure Data Manager)*	Software centrale della Posta che permette ai Cantoni di allestire e svolgere una chiamata alle urne. Questo software viene installato sui computer di e-voting dei Cantoni. Ad esempio, grazie a questo software i giorni D1 e D2 vengono generati i codici per gli aventi diritto di voto e le chiavi di sicurezza per la codifica dei voti e il giorno D3 i voti vengono mischiati e decodificati.
Seed	In crittografia il termine seed (termine inglese che significa seme, germe, seminare) definisce il valore iniziale (valore di inizializzazione) per un algoritmo di decodifica. Sulla base dell'inserimento del seed da parte del Cantone vengono calcolati i parametri di decodifica.
Chiave di sicurezza	Elemento crittografico fondamentale per proteggere un asset digitale. Nel contesto del voto elettronico, sulla base dell'inserimento di due password viene generata la chiave di sicurezza per la codifica e la decodifica dei voti.
Software del controllo abitanti	Applicazione software dei comuni / dei Cantoni usata per amministrare e curare i dati degli aventi diritto di voto. L'applicazione viene inoltre utilizzata per generare i file eCH0045 (catalogo elettorale) per la chiamata alle urne (cfr. termine "catalogo elettorale EV").
Software per generare le carte di legittimazione*	Software che viene utilizzato per generare le carte di legittimazione.

Termine	Descrizione
Computer (offline) delle carte di legittimazione (CL)*	Dispositivo offline che viene utilizzato per generare le carte di legittimazione.
Synchronization computer (online) (OVE: parte di sistema non affidabile) (Posta: online SDM)	Dispositivo online necessario per sincronizzare la chiamata alle urne con i server della Posta. In particolare, su questo dispositivo viene installato il software SDM.
Trusted build e trusted deployment	I termini trusted build e trusted deployment (in breve "trusted build e deployment") indicano una produzione (build) e un'installazione (deployment) affidabili del software necessario per l'e-voting. Attraverso il processo di trusted build e trusted deployment viene garantito che il software impiegato dalla Posta e dai Cantoni corrisponda al codice sorgente pubblicato, sottoposto a un controllo pubblico e a una verifica indipendente. Questo processo viene seguito attivamente da uno specialista incaricato dai Cantoni nonché da un rappresentante dei Cantoni. I corrispondenti protocolli vengono pubblicati.
Verification computer (offline)	Dispositivo offline che viene messo a disposizione dell'electoral board per verificare la chiamata alle urne (cfr. termine "dispositivi offline"). In particolare, su questo dispositivo viene installato il software verifier.
Verifier* (OVE: ausilio tecnico dei verificatori)	Software della Posta. Il verifier serve ai verificatori quale ausilio tecnico per verificare la configurazione della chiamata alle urne nonché il mescolamento e la decodifica.
Codici di verifica sulla carta di legittimazione*	I codici stampati sulla carta di legittimazione (codice di conferma e di finalizzazione nonché codici di verifica).
Portale per le elezioni e le votazioni*	Portale web della Posta usato dai votanti per esprimere il voto.

Tabella 4: Termini tecnici

4 Indice delle tabelle