Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Cancelleria federale CaF
Sezione Diritti politici

Allegato all'ordinanza della CaF del 13. dicembre 2013 concernente il voto elettronico (OVE, RS 161.116)

Requisiti tecnici e amministrativi relativi al voto elettronico

Versione: 2.0
Entrata in vigore: 1.7.2018

Indice

1. In generale

2.1 Riferimenti

1.1.1 Legge federale del 17 dicembre 1976 sui diritti politici (LDP; RS 161.1)

1.1.2 Ordinanza del 24 maggio 1978 sui diritti politici (ODP; RS 161.11)

1.1.3 Vote électronique: catalogue de critères pour les imprimeries (edito dalla Cancelleria federale, disponibile solo in francese)

1.1.4 Common Criteria: Protection profile for basic set of security requirements for online voting products, versione 1.0 (BSI-CC-PP-0037-2008)

1.1.5 Norme ISO/IEC 27001: Standard 2013

1.1.6 Legge federale del 19 dicembre 2003 sui servizi di certificazione nel campo della firma elettronica (FiEle; RS 943.03)

1.1.7 eCH-0059: Accessibility Standard Version 2.0, 13.04.2011

I documenti summenzionati possono essere ottenuti presso le organizzazioni seguenti:

Testi di legge aventi riferimento alla RS	Ufficio federale delle costruzioni e della logistica (UFCL) Distribuzione di pubblicazioni federali CH-3003 Berna http://www.bundespublikationen.ch
Norme ISO	Segreteria centrale dell'Organizzazione internazionale di normazione (ISO) Rue de Varembé 1 1211 Ginevra http://www.iso.org
Requisiti posti alle tipografie	Cancelleria federale CH-3003 Berna http://www.bk.admin.ch/themen/pore/evoting/07979/index.html?lang=it (in francese)
Common Criteria: Protection profile	Bundesamt für Sicherheit in der Informationstechnik Postfach 200362 D-53133 Bonn, Germania https://www.bsi.bund.de
Standard e-CH	Associazione eCH Mainaustrasse 30, casella postale, 8034 Zurigo http://www.ech.ch

2.2 Abbreviazioni

CaF	Cancelleria federale
LDP	Legge federale sui diritti politici
BSI	Bundesamt für Sicherheit in der Informationstechnik (Germania)
CC	Criteri comuni
DOS	Negazione del servizio (*Denial Of Service*)
DNS	Server di nomi di dominio (*Domain Name Server*)
2. **EAL**	Livello di valutazione della sicurezza (*Evaluation Assurance Level*)
ISO	Organizzazione internazionale di normazione (*International Organization for Standardization*)
MITM	Man In The Middle (Uomo in mezzo)
PIN	Numero di identificazione personale (*Personal Identification Number*)
PP	Profilo di protezione (*Protection Profile*)
SAS	Servizio di accreditamento svizzero
SFR	Requisiti funzionali di sicurezza (*Security Functional Requirements*)
ODP	Ordinanza sui diritti politici

2.1 Definizioni

1.3.1 Autenticazione

1.3.1.1 Dati di autenticazione lato *client*

Tutte le informazioni messe a disposizione di ogni singolo elettore e di cui questi ha bisogno per poter esprimere un voto (può p. es. trattarsi di un PIN, la cui immissione risulta nell'allestimento di una firma elettronica per il voto). Sulla base dei dati di autenticazione *client*, l'ausilio tecnico utilizzato genera un messaggio di autenticazione (p. es. la firma del voto), che viene inviato all'infrastruttura. Per mezzo del messaggio di autenticazione e dei dati di autenticazione lato server (p. es. una chiave pubblica che permette di verificare la firma) l'infrastruttura autentica che il mittente di un voto ha diritto di voto. I dati di autenticazione *client* devono poter essere difficilmente indovinati.

1.3.1.2 Dati di autenticazione lato server

Tutte le informazioni che, per mezzo di un messaggio di autenticazione, permettono di autenticare che il mittente di un voto ha diritto di voto.

1.3.1.3 Messaggio di autenticazione

Tutte le informazioni che una piattaforma utente invia all'infrastruttura dopo l'immissione dei dati di autenticazione *client*, affinché il mittente di un voto venga autenticato come avente diritto di voto. Dev'essere in pratica impossibile generare un messaggio di autenticazione se non si conoscono i dati di autenticazione *client*.

1.3.2 Parti del sistema

1.3.2.1 Sistema

Termine generico che contempla la funzionalità e l'infrastruttura. La parte del sistema composta della piattaforma utente e del software di funzionalità *client* è denominata sistema *client*. La parte del sistema che si compone della piattaforma server e del software di funzionalità server è denominata sistema server.

1.3.2.2 Infrastruttura (I)

L'hardware, il software, gli elementi di rete, i locali, i servizi e gli strumenti di ogni genere necessari all'esercizio tecnico della funzionalità lato server, nel rispetto di tutti i requisiti in materia di sicurezza.

1.3.2.3 Funzionalità (F)

Software lato server, nonché software lato *client* sulla piattaforma utente, sviluppati per garantire tutti i requisiti in materia di sicurezza specificatamente per il voto elettronico.

1.3.2.4 Piattaforma utente

Apparecchio multifunzionale programmabile collegato a Internet e utilizzato per votare. Si tratta generalmente di un computer standard, di uno *smartphone* o di un *tablet*.

1.3.3 Voto

1.3.3.1 Voto nella versione immessa dal votante nella piattaforma utente

Voto che corrisponde alla versione immessa dal votante nella piattaforma utente e che soprattutto da quel momento non è stato manipolato. Corrisponde sempre alla volontà del votante, a meno che questi non abbia commesso un errore al momento dell'immissione.

1.3.3.2 Voto registrato

Un voto è designato come registrato quando l'infrastruttura ha preso atto del suo deposito definitivo.

1.3.3.3 Voto parziale

Nelle votazioni designa un progetto, un controprogetto o una domanda risolutiva, mentre nelle elezioni fa riferimento alla scelta di una lista o alla scelta di un candidato inserito in una lista.

1.3.3.4 Voto espresso conformemente al sistema

Un voto è «espresso conformemente al sistema» se

1. è depositato in modo definitivo dal suo mittente; e
2. i dati di autenticazione *client* utilizzati e il messaggio di autenticazione che ne risulta corrispondono ai dati di autenticazione server definiti nella fase di preparazione dello scrutinio e attribuiti a un elettore; e
3. l'urna elettronica non contiene ancora nessun voto espresso utilizzando gli stessi dati di autenticazione *client*.

1.3.4 Analisi dei rischi

Termine generico che contempla una serie di attività sequenziali volte a *identificare, analizzare* e *valutare i rischi*.

1.3.5 Gestore del sistema

L'organizzazione (autorità o impresa privata) che, in occasione di uno scrutinio, si assume l'intera responsabilità della gestione di tutti gli aspetti tecnici del voto elettronico. A tale scopo mette a disposizione, in misura adeguata, il personale, l'organizzazione e l'infrastruttura. L'insieme delle attività tecniche, amministrative, giuridiche e direttive del gestore di sistema è denominato «esercizio». Il gestore del sistema lavora secondo le istruzioni del responsabile cantonale.

1.3.6 Dati e informazioni classificati

1.3.6.1 Dati e informazioni confidenziali

Dati e informazioni che possono essere resi noti soltanto a determinate persone conosciute.

1.3.6.2 Dati e informazioni segreti

Dati e informazioni confidenziali che non possono essere resi noti ad alcuna singola persona. Ne fanno parte almeno i dati e le informazioni che nella loro totalità consentirebbero di violare la segretezza del voto o di rilevare risultati parziali anticipati. La presente definizione può divergere da altri standard.

2. Requisiti concernenti la configurazione di processi elementari

Qui di seguito sono elencati i requisiti concernenti la configurazione di processi elementari fondamentali. La colonna di destra indica a quale tipo di verifica sottostà un determinato requisito (I: verifica dell'infrastruttura e dell'esercizio; F: verifica della funzionalità).

2.1 Procedura di voto

2.1.1	Il sistema deve essere di facile utilizzo. La navigazione per gli utenti deve seguire schemi generalmente noti.	F
2.1.2	L'accessibilità del sistema *client* deve essere verificata conformemente allo standard eCH-0059 versione 2.0 da un servizio riconosciuto come competente dalla Cancelleria federale.	F
2.1.3	I votanti dichiarano di aver preso atto delle regole del voto elettronico e della loro responsabilità.	F
2.1.4	Prima di votare, gli aventi diritto devono essere resi attenti esplicitamente sul fatto che, trasmettendo i loro voti elettronici, partecipano validamente a una decisione popolare. Prima di esprimere il proprio voto, l'elettore è tenuto a confermare che ha preso atto di questo messaggio.	F
2.1.5	Per votare per via elettronica, l'elettore deve provare all'autorità competente che è autorizzato a farlo utilizzando i dati di autenticazione *client*.	F
2.1.6	I votanti immettono il loro voto nella piattaforma utente e lo depositano nell'urna elettronica avvalendosi dei dati di autenticazione *client*.	F
2.1.7	Il modo in cui il sistema *client* si presenta ai votanti non influenza le loro scelte.	F,I
2.1.8	Fino al momento in cui decidono di depositare il loro voto in maniera definitiva nell'urna, i votanti possono correggerlo. Fino a quel momento il canale di voto convenzionale rimane ancora a loro disposizione.	F
2.1.9	La navigazione per gli utenti non deve indurre questi ultimi a votare in modo precipitoso o senza riflettere.	F
2.1.10	Il sistema permette di votare solo dopo che il votante ha esplicitamente controllato e confermato il proprio voto. Quest'ultimo gli viene mostrato nuovamente prima del suo deposito definitivo.	F

2.1.11	Il sistema offre all'avente diritto di voto la possibilità di interrompere in ogni momento la procedura di voto senza che egli perda la legittimazione a votare.	F,I
2.1.12	Il sistema non offre ai votanti funzioni che permettano la stampa del proprio voto.	F
2.1.13	La persona che ha votato deve poter riconoscere sulla piattaforma utente che il suo voto è stato trasmesso con successo. Essa riceve una conferma che il voto espresso è giunto a destinazione.	F,I
2.1.14	Dopo il deposito del voto, ai votanti non può essere data alcuna informazione sul voto da loro espresso.	F
2.1.15	Non deve essere possibile esprimere un ulteriore voto servendosi degli stessi dati di autenticazione *client*.	F,I

2.2 Preparazione dei dati di autenticazione, delle chiavi crittografiche e di altri parametri di sistema

2.2.1	Il catalogo elettorale è importato nell'infrastruttura.	F,I
2.2.2	Le domande della votazione (p. es. oggetti posti in votazione o liste dei candidati) per ogni livello federale e circondario elettorale interessato sono importate e memorizzate nell'infrastruttura.	F,I
2.2.3	Nell'infrastruttura sono approntati e memorizzati i dati di autenticazione *client* per ciascun avente diritto di voto.	F
2.2.4	Se necessario, per ciascun avente diritto di voto sono approntati e memorizzati temporaneamente i dati di autenticazione *client*. (Ciò è necessario solo nei casi in cui non sia utilizzato alcun mezzo di autenticazione esterno).	F
2.2.5	Le chiavi crittografiche utilizzate sono approntate e memorizzate nell'infrastruttura.	F
2.2.6	Il gestore del sistema definisce i parametri tecnici pertinenti per l'esecuzione di uno scrutinio.	I

2.3 Informazioni e ausilii

2.3.1	Il responsabile cantonale elabora un concetto per l'informazione dei cittadini in materia di voto elettronico.	I
2.3.2	La strategia garantisce che le informazioni siano state autorizzate dagli organismi competenti.	I
2.3.3	Su Internet sono disponibili consigli e regole sul voto e informazioni riguardanti la responsabilità degli aventi diritto di voto. Si vuole così evitare che essi votino in modo precipitoso o senza riflettere.	F,I
2.3.4	Agli aventi diritto di voto sono illustrate in maniera comprensibile le misure di sicurezza; ciò incrementa la loro fiducia nel voto elettronico.	F
2.3.5	Agli aventi diritto di voto vengono illustrati gli aspetti a cui devono prestare attenzione affinché possano votare in tutta sicurezza.	F
2.3.6	Agli aventi diritto di voto viene spiegato in che modo possono cancellare il voto da tutte le memorie della piattaforma utente che essi hanno utilizzato per votare.	F
2.3.7	Gli aventi diritto di voto possono richiedere un supporto tecnico	I
2.3.8	È necessario che i verificatori, per esempio una commissione istituita per la verifica, vengano informati e formati adeguatamente riguardo ai processi che si basano sulla correttezza del risultato, sul rispetto della segretezza del voto e sull'assenza di risultati parziali anticipati (p. es. generazione di chiavi, stampa del materiale di voto, decrittaggio e spoglio). Essi devono essere in grado di capire i processi e il loro significato.	I

2.4 Preparazione alla stampa del materiale di voto

2.4.1	Il materiale di voto deve essere concepito in modo che sia impossibile votare una seconda volta con un canale di voto convenzionale.	F,I
2.4.2	Il file per la stampa del materiale di voto è approntato, includendo eventualmente i dati di autenticazione *client*.	F
2.4.3	Il file per la stampa è trasmesso alla tipografia.	F,I

2.5 Apertura e chiusura del canale di voto elettronico

2.5.1	Il gestore del sistema inizializza il sistema. (L'inizializzazione comprende tutte le regolazioni che bisogna effettuare, secondo la definizione del processo, poco prima dell'apertura del canale di voto elettronico; essa può comprendere ad esempio la messa in servizio di monitor di sistema o la reinizializzazione di contatori e dell'urna elettronica[1]).	I
2.5.2	Il canale di voto elettronico è aperto agli aventi diritto di voto.	F,I
2.5.3	L'apertura o la chiusura anticipata del canale di voto elettronico dev'essere vietata.	I
2.5.4	Il canale di voto elettronico è chiuso agli aventi diritti di voto.	F,I

2.6 Controllo della conformità ed espressione definitiva del voto

2.6.1	Utilizzando il messaggio di autenticazione ricevuto e i dati di autenticazione *client*, il sistema autentica che il mittente del voto ha diritto di voto.	F
2.6.2	Il sistema verifica se per uno stesso elettore è già stato depositato un voto nell'urna elettronica.	F
2.6.3	Quando il voto è espresso in modo conforme al sistema, il sistema deposita il suffragio nell'urna elettronica e informa i votanti della riuscita del voto. Un voto espresso in modo non conforme al sistema non è depositato nell'urna elettronica. Oltre che ad essere stato espresso in modo conforme al sistema, il fatto che un voto sia ben formato[2] può costituire un criterio per la riuscita del voto.	F

2.7 Conteggio dell'urna elettronica

2.7.1	Dopo la chiusura del canale di voto elettronico, al più presto la domenica della votazione, il responsabile cantonale avvia il decrittaggio dei voti contenuti nell'urna elettronica.	F,I
2.7.2	*Abrogato*[3]	
2.7.3	Il responsabile cantonale redige un protocollo sulla procedura di decrittaggio dei voti e sul loro conteggio.	I
2.7.4	Dal decrittaggio dei voti fino alla trasmissione dei risultati della votazione ogni accesso al sistema o a una delle sue componenti deve essere effettuato da almeno due persone; esso deve essere registrato per scritto e poter essere controllato da rappresentanti dell'autorità competente.	F,I

[1] Per «urna elettronica» si intende lo spazio di memoria in cui sono memorizzati i voti espressi fino al loro decrittaggio e spoglio.
[2] Per voto «ben formato» s'intende un determinato modo di compilare una scheda di voto. È possibile definire a priori se e in che modo le schede non compilate correttamente devono essere prese in considerazione per il risultato finale. Per esempio, si può stabilire in anticipo che a una determinata domanda posta in votazione si potrà rispondere soltanto con un «sì», con un «no» oppure lasciando la scheda bianca, e che soltanto queste tre risposte influenzeranno il risultato dello scrutinio. Una risposta come «non voglio votare» avrebbe quale conseguenza che il voto non è «ben formato». È necessario definire in anticipo se i voti che non sono ben formati non potranno essere depositati nell'urna elettronica, se saranno ignorati al momento del conteggio oppure se figureranno nel risultato finale.
[3] Nuovo testo giusta il n. II della modifica del 30 maggio 2018 dell'ordinanza della CaF concernente il voto elettronico (RU *2018* 2279).

2.7.5	I risultati della votazione sono trasmessi a un sistema terzo per l'ulteriore trattamento dei dati, in particolare in vista del loro consolidamento con i voti espressi per mezzo dei canali convenzionali.	F,I
2.7.6	Il sistema mette a disposizione le informazioni necessarie che permettono di constatare, per mezzo di una carta di legittimazione al voto, se un dato avente diritto, che intende votare di persona o per corrispondenza, ha già votato per via elettronica. In caso di prove di voto elettronico con una quota dell'elettorato molto limitata (p. es. solo con Svizzeri all'estero), ai fini della protezione della segretezza del voto bisogna impedire che a servizi esterni all'infrastruttura vengano recapitati elenchi che permettano di identificare gli aventi diritto che hanno espresso il loro voto per via elettronica. Occorrerà invece confermare, su richiesta, se un determinato avente diritto ha espresso il proprio voto. In alternativa, il sistema può generare un elenco contenente codici anonimi che corrispondono alle carte di legittimazione al voto utilizzate.	F,I
2.7.7	Il decrittaggio e il conteggio dei voti si svolgono in presenza di organi o parti indipendenti, in grado di attestare il regolare svolgimento della procedura.	I

2.8 Dati confidenziali e segreti

2.8.1	Si assicura che né collaboratori né persone esterne vengano a conoscenza di dati che permettono di stabilire un legame fra l'identità di un elettore e il voto che ha espresso.	F,I
2.8.2	Si assicura che né collaboratori né persone esterne vengano a conoscenza di dati che permettano di ottenere risultati parziali anticipati prima del decrittaggio dei voti.	F,I
2.8.3	Si assicura che i risultati della votazione saranno trattati in modo confidenziale fra il momento del decrittaggio dei voti e quello della loro pubblicazione.	F,I
2.8.4	Si assicura che i dati che permettono di appurare che gli aventi diritto di voto hanno votato per via elettronica saranno trattati in modo confidenziale.	F,I
2.8.5	Si assicura che i dati personali provenienti dal catalogo elettorale saranno trattati in modo confidenziale.	F,I
2.8.6	Si assicura che i singoli voti saranno trattati in modo confidenziale anche dopo il conteggio.	I
2.8.7	Si assicura che i risultati della votazione saranno trattati in modo confidenziale nel caso in cui solo una minima quota di elettori di un circondario elettorale sia autorizzato a votare per via elettronica.	F,I
2.8.8	Dopo la convalida, il gestore del sistema distrugge – secondo una procedura documentata – tutti i dati creati nell'ambito dello scrutinio elettronico in relazione con i singoli voti immessi e classificati come confidenziali o segreti.	I

2.9 Obblighi del responsabile cantonale

	Il responsabile cantonale è una persona fisica che si assume l'intera responsabilità di uno scrutinio elettronico. In particolare deve: a. definire, emanare e introdurre misure per la sicurezza dell'informazione (direttiva in materia di sicurezza dell'informazione, criteri di base per la gestione dei rischi in materia di sicurezza dell'informazione, campo di applicazione e limiti della gestione dei rischi in materia di sicurezza dell'informazione, organizzazione della gestione dei rischi); b. redigere il contratto concernente l'esecuzione di uno scrutinio e fissare i requisiti di sorveglianza e di verifica; c. affidare l'esecuzione di uno scrutinio a un gestore di sistema; d. fissare le scadenze per l'esecuzione di atti od operazioni critiche; e e. sorvegliare e controllare l'esecuzione di uno scrutinio presso il gestore di sistema incaricato. Il responsabile cantonale può partecipare all'esecuzione di uno scrutinio elettronico.	I

3. Requisiti di sicurezza

Gli obiettivi di sicurezza (cfr. art. 3 cpv. 1) non possono essere raggiunti con assoluta certezza, ma si possono in ogni caso identificare i rischi per la sicurezza. Sulla base di un'analisi dei rischi metodica (art. 3 cpv. 2 e n. 6.4) occorre fornire la prova che eventuali rischi per la sicurezza sono da considerarsi sufficientemente bassi.

3. È possibile identificare un rischio attraverso le minacce e i punti deboli del sistema. Un rischio insorge quando un punto debole di tale sistema può essere sfruttato mediante una minaccia, mettendo potenzialmente in dubbio l'adempimento di un obiettivo di sicurezza. Per ridurre al minimo i rischi si attuano misure di sicurezza che devono adempiere i requisiti di sicurezza a livello di funzionalità, infrastruttura ed esercizio in modo da minimizzare a sufficienza i rischi identificati.

Il numero 3.1 elenca alcune minacce generali e le mette in relazione con gli obiettivi di sicurezza. Questi ultimi vanno considerati quando si identificano i rischi e, a seconda dei punti deboli identificati del sistema e per quanto necessario, concretizzati e integrati.

I requisiti di sicurezza sono riassunti nei numeri 3.2 – 3.15:

da un lato, si riferiscono alle minacce. Per garantire gli obiettivi di sicurezza occorre prevedere, in tutti i punti deboli del sistema esposti a minacce, misure di sicurezza che adempiono i requisiti di sicurezza secondo le migliori prassi;

dall'altro, si riferiscono ai requisiti per la configurazione di processi elementari (cfr. n. 2). Ciò serve da ausilio per capire quali punti deboli occorre considerare nell'attuare un requisito di sicurezza. Ulteriori punti deboli si identificano nel sistema concreto e i requisiti di sicurezza sono messi in relazione con essi per analogia.

Il numero 3.15 comprende requisiti di sicurezza tratti dal profilo di protezione (PP) del Bundesamt für Sicherheit in der Informationstechnik (BSI) [4], pur con alcune differenze. Le differenze e i riferimenti alle minacce e ai requisiti per configurare processi elementari sono indicati nel numero 3.15.

3.1 Minacce

	Descrizione	Obiettivo di sicurezza interessato
3.1.1	Un software nocivo modifica il voto sulla piattaforma utente	Correttezza del risultato
3.1.2	Un aggressore devia il voto mediante DNS-spoofing[4]	Correttezza del risultato
3.1.3	Un aggressore modifica il voto mediante una tecnica Man In The Middle (MITM)[5]	Correttezza del risultato
3.1.4	Un aggressore invia schede di voto corrotte mediante la tecnica MITM	Correttezza del risultato
3.1.5	L'amministratore manipola il software che non memorizza i voti	Correttezza del risultato
3.1.6	L'amministratore modifica i voti	Correttezza del risultato
3.1.7	L'amministratore aggiunge voti	Correttezza del risultato
3.1.8	Un'organizzazione criminale si introduce nel sistema allo scopo di falsificare il risultato	Correttezza del risultato (qui ai sensi di n. 3.1.5/6/7/9)
3.1.9	L'amministratore copia il materiale di voto e lo utilizza	Correttezza del risultato
3.1.10	Un software nocivo sulla piattaforma utente invia il voto all'organizzazione criminale	Protezione della segretezza del voto ed esclusione di risultati parziali anticipati
3.1.11	Il voto è deviato mediante DNS-spoofing	Protezione della segretezza del voto ed esclusione di risultati parziali anticipati
3.1.12	Un aggressore legge il voto mediante MITM	Protezione della segretezza del voto ed esclusione di risultati parziali anticipati
3.1.13	L'amministratore utilizza una chiave e decritta voti non anonimi	Protezione della segretezza del voto ed esclusione di risultati parziali anticipati
3.1.14	Nel verificare la correttezza del trattamento / conteggio viene violata la segretezza del voto	Protezione della segretezza del voto ed esclusione di risultati parziali anticipati
3.1.15	L'amministratore osserva in anticipo voti non crittati	Protezione della segretezza del voto ed esclusione di risultati parziali anticipati
3.1.16	Un'organizzazione criminale si introduce nel sistema allo scopo di violare la segretezza del voto o rilevare risultati parziali anticipati	Protezione della segretezza del voto ed esclusione di risultati parziali anticipati (qui ai sensi di minacce, n. 3.1.13/14/15).
3.1.17	Un software nocivo sul computer dell'avente diritto di voto rende impossibile il diritto di voto	Disponibilità della funzionalità
3.1.18	Un software nocivo influenza gli aventi diritto di voto nella formazione delle loro opinioni	Protezione delle informazioni per gli aventi diritto di voto

[4] Anche DNS-poisoning (avvelenamento della cache DNS): designa un attacco per mezzo del quale si riesce a modificare l'associazione fra il nome del nodo ospite (host) e l'indirizzo IP corrispondente.

[5] Designa l'aggressore che conduce un attacco Man in the middle (MITM). Si tratta di una forma di attacco utilizzata nelle reti di computer. L'aggressore si intromette fisicamente o, come succede più spesso attualmente, per via informatica fra due parti in comunicazione fra loro e con il suo sistema esercita un controllo totale sui dati scambiati fra due o più partecipanti della rete. L'aggressore può in tal modo leggere le informazioni e addirittura manipolarle a suo piacimento.

3.1.19	Un'organizzazione criminale compie un attacco in forma di negazione del servizio (DOS)[6]	Disponibilità della funzionalità
3.1.20	L'amministratore esegue una configurazione errata; non si può arrivare al conteggio	Disponibilità della funzionalità
3.1.21	L'amministratore manipola il sito web d'informazione o il portale delle votazioni, confondendo gli aventi diritto di voto	Protezione delle informazioni per gli aventi diritto di voto
3.1.22	Dopo la decrittazione l'amministratore ricerca un comportamento di voto prestabilito (possibile soltanto per le elezioni)	Esclusione di riscontri sul comportamento di voto nell'infrastruttura
3.1.23	Un'organizzazione criminale si introduce nel sistema allo scopo di perturbarne l'esercizio, manipolare le informazioni indirizzate agli aventi diritti di voto o indagare sul comportamento di voto dei votanti.	Disponibilità della funzionalità, protezione delle informazioni per gli aventi diritto di voto, esclusione di riscontri sul comportamento di voto nell'infrastruttura (qui ai sensi di minacce, n. 3.1.20/21/22)
3.1.24	L'amministratore sottrae dati inerenti agli indirizzi degli aventi diritto di voto	Protezione delle informazioni personali sugli aventi diritto di voto

3.2 Constatazione/Scoperta e notifica di eventi e debolezze inerenti alla sicurezza; gestione di eventi e miglioramenti inerenti alla sicurezza

3.2.1	Un sistema di monitoraggio dell'infrastruttura deve scoprire gli incidenti e allarmare il personale preposto, che li gestisce in conformità con procedure predefinite. Scenari di crisi e piani di salvataggio servono da linea direttrice (ivi compreso un piano che garantisca lo svolgimento delle attività relative agli scrutini) e si applicano in caso di necessità.	F,I - 2.2.1/2/3/4/5/6 - 2.3.3/4/5/ - 2.5.2/3/4 - 2.6.1/2/3 - 2.7.1/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/ 19/20/21/22/23/24
3.2.2	Sull'infrastruttura occorre redigere e, se necessario, rendere disponibili i protocolli dei voti pervenuti. Essi servono da attestati per la presa in considerazione completa, non falsificata ed esclusiva di voti espressi conformemente al sistema. In caso di divergenze devono servire a ricercarne la causa.	F,I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/ 20/22/23
3.2.3	Sull'infrastruttura occorre redigere e, se necessario, rendere disponibili i protocolli degli accessi al sistema, resistenti alle manipolazioni. Essi servono da attestati per la presa in considerazione completa, non falsificata ed esclusiva di voti espressi conformemente al sistema nonché per il rispetto della segretezza del voto e l'assenza di risultati parziali anticipati. In caso di divergenze o di dubbi, devono servire a ricercarne la causa.	F,I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/ 19/20/21/22/23/24
3.2.4	I voti espressi elettronicamente e conteggiati devono essere confrontati con i protocolli dei voti pervenuti sull'infrastruttura per accertare la plausibilità del risultato.	F,I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/ 20/22/23
3.2.5	Occorre garantire che, in caso di guasto, i voti e i dati a comprova di un funzionamento ineccepibile della procedura di conteggio dei voti vengano memorizzati in modo integro sull'infrastruttura.	F,I - 2.1.6/13 - 2.2.1/2/3/4/5/6 – 2.4.2 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/20/23

[6] Dall'inglese Denial Of Service: nel trattamento digitale di dati designa l'impossibilità di accedere a un servizio che in linea di principio dovrebbe essere disponibile.

3.2.6	Con l'ausilio di dati di autenticazione si devono poter esprimere voti di controllo non attribuiti ad alcun avente diritto di voto. Il contenuto di questi voti va iscritto in un protocollo. Il conteggio dei voti di controllo va confrontato con i protocolli riguardanti l'espressione dei voti di controllo. Occorre garantire che i voti di controllo siano trattati quanto più possibile alla stregua di voti espressi conformemente al sistema, garantendo nel contempo che non vengano conteggiati.	F,I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/4 - 2.8.1/2/3/4/5/6/8 - 3.1.1/2/3/4/5/6/7/8/9/13/14/15/16/17/18/21/23
3.2.7	La disponibilità dell'infrastruttura deve essere verificata e iscritta a protocollo a intervalli di tempo scelti.	I - 3.1.19/20/23
3.2.8	I metodi statistici, sempre che la base di dati lo consenta, devono poter essere impiegati per accertare la plausibilità del risultato.	I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/20/22/23
3.2.9	Mediante un processo documentato, le parti del sistema di voto raggiungibili da Internet devono essere regolarmente aggiornate per eliminare punti deboli di cui si è venuti a conoscenza.	I - 3.1.5/6/7/8/9/13/14/15/16/19/21/22/23/24

3.3 Uso di misure crittografiche e amministrazione delle chiavi

3.3.1	I certificati elettronici devono essere amministrati secondo le migliori prassi.	I 2.2.13 - 2.2.5/6 - 2.4.3 - 2.7.5 - 3.1.2/3/4/8/12/16/20/23
3.3.2	Per assicurare l'integrità di serie di dati, su cui si basa la correttezza del risultato, vanno impiegate misure crittografiche efficaci, conformi allo stato della tecnica.	I,F - 2.1.6 – 2.2.1/3/4/5/6 - 2.4.3 - 2.5.1 - 2.6.1/2/3 - 2.7.1/2/5/6 - 3.1.5/6/7/8/9/14/16
3.3.3	Per assicurare la segretezza di serie di dati, su cui si basano la segretezza del voto e l'assenza di risultati parziali anticipati, vanno impiegate misure crittografiche efficaci, conformi allo stato della tecnica.	I,F - 2.1.6 - 2.2.1/3/4/5/6 - 2.4.2/3 - 2.5.1 - 2.6.1/2/3 - 2.7.1/2/5/6 - 2.8.1/2/3/4/6/7/8 3.1.12/13/14/15/16
3.3.4	In nessun momento da quando vengono rilevati a quando vengono conteggiati i voti possono essere depositati o trasmessi in forma non crittata.	I,F 2.1.6/13 - 2.4.2/3 - 2.6.1/2/3 - 2.7.1 - 2.8.1/2 - 3.1.3/4/5/6/7
3.3.5	Nello scambio di dati riguardanti il catalogo elettorale e i risultati devono essere impiegati il crittaggio e la firma. Quest'ultima e l'integrità dei dati vanno verificate al momento del loro ricevimento.	I,F 2.2.1/2 - 2.4.3 - 2.7.5 - 2.8.3/7
3.3.6	Le componenti di base crittografiche possono essere utilizzate solamente se le lunghezze delle chiavi e gli algoritmi sono conformi agli standard correnti (p. es. FIPS 143-3, NIST, ECRYPT, FiEle). La firma elettronica deve soddisfare i requisiti di una firma elettronica avanzata ai sensi della FiEle. La verifica della firma deve avvenire mediante un certificato rilasciato da un prestatore di servizi di certificazione riconosciuto in virtù della FiEle.	I,F
3.3.7	Gli aventi diritto di voto ricevono le indicazioni necessarie per controllare l'autenticità del sito Internet e del server utilizzato per esprimere il voto. L'attendibilità di una verifica efficace deve essere supportata dall'impiego di mezzi crittografici in conformità con le migliori prassi.	I,F 2.1.13 - 2.2.5 - 3.1.2/3/4/11/12

3.4 Scambio di informazioni fisico ed elettronico più sicuro

3.4.1	Tutte le componenti dell'infrastruttura devono essere gestite in una zona di rete separata, che va protetta mediante un adeguato controllo dell'instradamento.	I 2.8.1/2/3/4/5/6/7 - 3.1.6/7/8/9/13/14/15/16/ 20/22/23/24
3.4.2	I sistemi devono essere difesi da attacchi (a prescindere dalla natura od origine degli stessi).	I
3.4.3	Il sistema di conteggio dei voti deve essere gestito all'interno della zona di rete in cui è gestita l'infrastruttura installando una propria sottozona di rete, separata in modo sicuro da tutte le altre sottozone di rete.	I 7.2.1/2/3/4/5/6/7 - 2.8.1/2/3/4/5/6/7 3.1.6/7/8/9/13/14/ 15/16/20/22/23
3.4.4	I trattamenti connessi al voto espresso elettronicamente devono essere chiaramente separati da tutte le altre applicazioni.	I 2.8.1/2/3/4/5/6/7 - 3.1.6/7/8/9/13/14/15/16/ 20/22/23/24

3.5 Test della funzionalità

3.5.1	Sulla base di un concetto di test occorre assicurare una funzionalità conforme alle specifiche. Il concetto deve comprendere copioni di test per ogni tipo di test. Esso disciplina le responsabilità nell'esecuzione, nella redazione dei protocolli e nel rendiconto. Stabilisce a quali condizioni va eseguito un test. Nello sviluppo occorre testare per lo meno ogni funzionalità rilevante per la sicurezza, anche nel caso di adeguamenti di minore importanza.	I,F

3.6 Direttiva in materia di sicurezza dell'informazione

3.6.1	Il responsabile cantonale deve emanare e comunicare una direttiva in materia di sicurezza dell'informazione che definisca un ambito di sicurezza vincolante per l'intero esercizio del sistema. La direttiva deve essere verificata a intervalli di tempo pianificati e se necessario adeguata.	I

3.7 Organizzazione della sicurezza dell'informazione

3.7.1	Tutti i ruoli e tutte le responsabilità per l'esercizio del sistema devono essere definiti con precisione, attribuiti e comunicati.	I - 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23
3.7.2	Per le installazioni destinate al trattamento delle informazioni dell'infrastruttura deve essere avviato un processo di autorizzazione.	I - 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23
3.7.3	I rischi connessi con terzi (mandatari di qualsiasi tipo come fornitori, prestatori di servizi ecc.) vanno identificati e ridotti nella misura del necessario per il tramite di adeguati accordi contrattuali. Il rispetto degli accordi deve essere controllato e verificato adeguatamente durante la loro validità.	I

3.8 Amministrazione delle risorse immateriali e materiali

3.8.1	Tutte le risorse immateriali e materiali ai sensi della nozione di *asset* contenuta nella norma ISO/IEC 27001:2013, rilevanti per il voto elettronico (organizzazione globale, in particolare i suoi processi organizzativi e le informazioni in quanto tali che vi sono trattate; supporti di dati, installazioni per il trattamento delle informazioni dell'infrastruttura; locali dell'infrastruttura) devono essere rilevati in un inventario. Occorre allestire un elenco del personale. L'inventario e l'elenco del personale devono essere tenuti aggiornati. A ogni risorsa immateriale e materiale va attribuita una persona che ne assume la responsabilità.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.8.2	Occorre definire l'uso ammesso di risorse immateriali e materiali.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.8.3	Per le informazioni vanno emanate e comunicate linee direttrici in materia di classificazione.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.8.4	Per la caratterizzazione e l'utilizzazione di informazioni vanno previste procedure.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24

3.9 Affidabilità del personale

3.9.1	Per garantire la affidabilità del personale prima, durante e dopo l'impiego o in caso di cambiamenti di ruolo si devono prevedere e comunicare direttive e procedure adeguate.	I 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23
3.9.2	Per garantire la affidabilità del personale, le istanze decisionali del personale devono assumersi la piena responsabilità.	I 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23
3.9.3	Il personale deve dare prova di una spiccata sensibilità in materia di sicurezza dell'informazione. A questo scopo occorre prevedere e gestire un programma di formazione e di esercitazione conforme ai compiti da svolgere.	I 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23

3.10 Sicurezza fisica e riferita all'ambiente

3.10.1	I perimetri di sicurezza dei locali dell'infrastruttura (locali per i vari gruppi del personale, locali dei server ecc.) vanno definiti chiaramente.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/21/22/23/24
3.10.2	Per l'accesso fisico ai locali dell'infrastruttura si devono definire, introdurre e controllare adeguatamente le autorizzazioni d'accesso.	I 3.1.5/6/7/8/9/13/14/ 15/16/23
3.10.3	Per garantire la sicurezza degli apparecchi dentro e fuori i locali dell'infrastruttura occorre definire direttive e procedure adeguate, nonché controllarne e verificarne il rispetto.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/21/22/23/24

3.11 Gestione della comunicazione e dell'esercizio

3.11.1	Le fasi d'esercizio per le principali attività del sistema vanno descritte in dettaglio.	I 2.2.1/2/3/4/5/6 - 2.3.8 - 2.4.2/3 - 2.5.1/2/3 - 2.7.1/2/3/4/5/6/7 - 3.1.20
3.11.2	I sistemi produttivi possono essere modificati soltanto in conformità con una procedura di gestione delle modifiche documentata.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.11.3	Gli obblighi e gli ambiti di responsabilità devono essere suddivisi in modo tale che i rischi imputabili alle persone correlati con l'esercizio e la comunicazione siano ridotti a rischi residui compatibili con i criteri di accettazione del rischio.	I - 2.2.1/2/3/4/5/6 - 2.3.8 - 2.4.2/3 - 2.5.1/2/3 - 2.7.1/2/3/4/5/6/7 - 3.1.20
3.11.4	Per proteggersi da software nocivi occorre adottare misure adeguate.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.11.5	Occorre allestire e attuare un piano dettagliato per la sicurezza dei dati e verificare regolarmente il corretto funzionamento di quest'ultima.	I 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.4.2 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/20/23
3.11.6	Vanno definite e attuate misure adeguate per la protezione della rete e la sicurezza dei servizi di rete.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.11.7	Si devono disciplinare in modo dettagliato le procedure per gestire i supporti amovibili di dati e per smaltire i supporti di dati.	I - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/9 - 3.1.13/14/15/16 - 3.1.22/23/24
3.11.8	Occorre descrivere in dettaglio, attuare, controllare e verificare le misure di sorveglianza e di protocollo relative all'utilizzo del sistema, alle attività di amministratori e ai guasti.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2/3 - 2.5.1/2/3/4 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23/24

3.12 Assegnazione, amministrazione e revoca dei diritti di accesso e d'intervento

3.12.1	Occorre garantire che durante lo scrutinio ogni modifica successiva avvenga esclusivamente con il consenso del responsabile cantonale.	F,I - 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.4 - 3.1.5/6/7/8/20/23
3.12.2	L'accesso all'infrastruttura e alla funzionalità e ogni intervento sulle stesse devono essere disciplinati e documentati in dettaglio in base a un'analisi dei rischi. Nei settori ad alto rischio occorre applicare il principio del doppio controllo.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.12.3	Occorre garantire che non si possano modificare senza autorizzazione informazioni sul sito del Voto elettronico e/o pagine informative sul voto elettronico.	F,I 2.3.3/3/4/5/6 - 3.1.21/23
3.12.4	Durante lo scrutinio devono poter essere esclusi interventi estranei sull'infrastruttura.	F,I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2/3 - 2.5.1/2/3/4 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23/24

3.12.5	Si deve assicurare che nessuno degli elementi dei dati di autenticazione *client* possa essere sistematicamente intercettato, modificato o deviato. Per l'autenticazione devono essere attuate misure e impiegate tecnologie che minimizzino sufficientemente il rischio di abuso sistematico da parte di terzi.	F,I – 2.1.5/6/15 - 2.2.3/4 - 2.4.1/2/3 - 2.6.1/2 - 2.7.1/2/4/5/6 - 2.8.1/4/5 - 3.1.5/6/7/8/9/13/14/15/16

3.13 Requisiti posti alle tipografie

3.13.1	Nell'adempimento dei loro compiti le tipografie devono soddisfare i requisiti stabiliti nel relativo catalogo destinato alle tipografie.	

3.14 Acquisizione, sviluppo e manutenzione di sistemi d'informazione

3.14.1	Per l'installazione del software su sistemi produttivi vanno descritte in dettaglio e attuate procedure adeguate.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.14.2	Per trattare punti deboli di natura tecnica vanno descritte in dettaglio e attuate procedure adeguate. Occorre prestare particolare attenzione alle parti dell'infrastruttura raggiungibili mediante Internet.	I - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24

3.15 Requisiti derivanti dal profilo di sicurezza del BSI

I requisiti derivanti dal profilo di sicurezza del BSI [4] vanno attuati in via supplementare. Nell'interpretarli, è determinante la terminologia del profilo di sicurezza.

Nel caso di incongruenze materiali tra la versione tedesca e quella inglese del profilo di sicurezza, fanno testo le disposizioni di quest'ultima. In caso di incongruenze rispetto al profilo di sicurezza, l'OVE ha sempre la precedenza.

Le seguenti divergenze dal profilo di sicurezza sono ammesse o vanno rispettate in modo vincolate:

3.15.1	*OE.ElectionPreparation*[7] - il requisito «Preparazione dell'elezione» prevede tra l'altro che gli «elettori» possano verificare le iscrizioni contenute nella «lista del diritto di voto» ed eventualmente chiedere una rettifica. Ciò non deve essere attuato qui in analogia agli aventi diritto di voto.
3.15.2	Non deve avere luogo alcuna registrazione degli aventi diritto di voto. Le iscrizioni nel catalogo elettorale sono determinanti per conferire il diritto di voto.
3.15.3	*OE.ServerRoom* – il requisito *«Locale del server»* prevede che solamente i responsabili della votazione possano accedervi. Tale requisito può essere attenuato prevedendo che soltanto le persone autorizzate dal responsabile cantonale possono accedere, sotto sorveglianza, al locale del server.
3.15.4	*O.Correction* – il requisito «Correzione» prevede che, prima del suo deposito definitivo, i votanti possono correggere il loro voto quante volte lo desiderano. Tale requisito può essere attenuato nel modo seguente: finché decidono di esprimere il loro voto in modo definitivo, i votanti possono correggerlo. (n. 2.1.8 prevale)
3.15.5	In casi ben motivati si possono adottare misure di sicurezza informatica alternative (nel senso della terminologia secondo i CC; *Security Functional Requirements*).

La seguente lista mette in relazione gli obiettivi di sicurezza (nel senso della terminologia secondo i CC; *Security Objectives*) con le minacce e i requisiti concernenti la configurazione dei processi elementari della presente ordinanza.

[7] I requisiti ivi menzionati derivanti dal profilo di sicurezza iniziano con «O», che si riferisce a «security objective» o con «OE», che si riferisce a «security objectives for the operational environment».

O.UnauthorisedVoter	F,I 2.1.5 - 2.2.1/2/3/4 - 2.4.2 - 2.6.1 - 3.1.7/8/9
O.Proof	F,I 2.1.12 - 3.1.22
O.IntegrityMessage	F – 2.1.6/13 – 2.2.5 – 2.4.3 – 3.1.2/3/4
O.SecrecyOfVoting	F – 2.1.6 – 2.2.5 – 2.8.1/2 – 3.1.12/13
O.SecretMessage	F - 2.1.6 - 2.2.5 - 2.8.1/4 - 3.1.9
O.AuthenticityServer	F,I - 2.1.6 - 2.2.5 - 2.4.2 - 3.1.2/3/4/12
O.ArchivingIntegrity	F,I - 2.2.5 - 2.7.2/3/4 - 3.1.6/7/8
O.ArchivingSecrecyOfVoting	F,I - 2.7.2 - 2.8.1/6/8 - 3.1.13/14/16/22
O.Abort	F - 2.1.11
O.EndingElection	F - 2.5.3/4 - 3.1.20
O.EndOfElection	F - 2.5.4 - 3.1.20
O.SecrecyOfVotingElectionOfficers	F - 2.7.2 - 2.8.1/6/7 - 3.1.13/14/16
O.IntegrityElectionOfficers	F - 2.5.1/2/4 - 2.7.4 - 3.1.5/6/7/8
O.IntermediateResult	F - 2.7.1 - 2.8.2/3 - 3.1.15/16
O.OverhasteProtection	F - 2.1.10
O.Correction	F - 2.1.8
O.Acknowledgement	F - 2.1.13 - 3.1.17
O.Failure	F,I - 2.2.6 - 2.5.1 - 3.1.19/20
O.Audit	F,I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9 - 3.1.13/14/15/16/19/20/21/22/23/24
O.OneVoterOneVote	F,I - 2.1.5/8/11/13/15 - 2.2.1/2/3/4 - 2.4.1 - 2.6.1/2/3 - 2.7.6 - 3.1.7/8/17
O.AuthElectionOfficers	F - 2.2.1/2/3/4/5/6 - 2.4.2 - 2.5.1/2/4 - 2.7.1/2/4/5 - 2.8.1/2/3/4/5/6/7
O.StartTallying	F - 2.5.4 - 2.7.1/2 - 3.1.15/16
O.Tallying	F - 2.2.6 - 2.5.1 - 2.7.2 - 3.1.5/7/8 - 3.1.20
OE.ElectionPreparation	F,I - 2.2.1/2/3/4/5/6 - 2.3.1/3 - 2.4.2/3 - 2.5.1 - 2.8.1/2/3/4/5/6/7/8 - 3.1.7/8/20
OE.Observation	F - 2.1.6
OE.ElectionOfficers	I - 2.2.1/2/6 - 2.3.2 - 2.5.1/2/4 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/20/21/22/23/24
OE.AuthData	F,I - 2.2.1/2/3/4 - 2.4.2/3 - 2.8.1/5 - 3.1.8/9
OE.VoteCastingDevice	F,I - 2.1.3 - 2.3.3/4 - 3.1.1 - 3.1.10
OE.ElectionServer	I - 3.1.8 - 3.1.16 - 3.1.23
OE.Availability	I - 3.1.19
OE.ServerRoom	I - 3.1.5/6/7/8/9/13/14/15/16/23
OE.DataStorage	I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.4.2 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/20/23
OE.SystemTime	I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4 - 2.8.1/2/3/4/6/8 - - 3.1.5/6/7/8/9/13/14/15/16/20/22/23
OE.AuditTrailProtection	I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
OE.AuthenticityServer	F - 2.3.3/4/5 - 2.4.2 - 3.1.2/3/4/12
OE.ArchivingIntegrity	F,I - 2.2.5 - 2.7.2/3/4 - 3.1.6/7/8
OE.ArchivingSecrecyOfVoting	F,I - 2.7.2 - 2.8.1/6/8 - 3.1.13/14/16/22
OE.ProtectedCommunication	I - 3.1.5/6/7/8/9/13/14/15/16/22/23/24
OE.Buffer	F - 2.3.6

4. Verificabilità

Gli articoli 4 e 5 stabiliscono le disposizioni concernenti la verificabilità. Il presente numero espone tali disposizioni in maniera più formale al fine di esplicitare i criteri applicabili a entrambe le forme di verificabilità.

A tale scopo, il numero 4.1 definisce un modello astratto ridotto per descrivere lo svolgimento di uno scrutinio. Sulla base di quel modello, il numero 4.2 contiene spiegazioni e ulteriori disposizioni riguardanti l'articolo 4. Il numero 4.3 mostra il modello astratto completo. Il numero 4.4 contiene spiegazioni e ulteriori disposizioni riguardanti l'articolo 5.

4.1 Modello astratto ridotto riguardante l'articolo 4

Nell'astrazione utilizzata, uno scrutinio è definito attraverso un protocollo crittografico[8], consistente nello scambio di messaggi tra le seguenti componenti del sistema:

Aventi diritto di voto / Votanti	Prima dello scrutinio, gli aventi diritto di voto ricevono dal sistema o dalla tipografia i dati di autenticazione *client*. Per inviare un voto comunicano i loro dati di autenticazione *client* e il loro voto alla piattaforma utente.
Piattaforma utente	Genera il messaggio di autenticazione e lo invia assieme al voto crittato al sistema lato server. A tale scopo, utilizza parametri pubblici ottenuti previamente dal sistema. Se necessario, mostra ai votanti messaggi dal sistema lato server.
Ausilio tecnico affidabile degli aventi diritto di voto	In alternativa, i votanti possono comunicare il loro voto e/o i loro dati di autenticazione *client* anche a un ausilio tecnico affidabile che può assumere qualsiasi compito della piattaforma utente.
Sistema (qui sempre lato server)	Genera e invia agli aventi diritto di voto prima di uno scrutinio (eventualmente per il tramite della tipografia) i loro dati di autenticazione *client* e alla piattaforma utente parametri pubblici affinché essa possa generare il messaggio di autenticazione e il voto crittografato. Il sistema giudica se i voti sono stati espressi in modo conforme al sistema, li decritta nel rispetto della segretezza del voto e calcola il risultato dello scrutinio.
Tipografia	Può essere impiegata per stampare i dati di autenticazione *client* e i dati confidenziali mediante i quali i votanti possono fare uso della verificabilità individuale (riferimento di verifica). Riceve i relativi dati dal sistema e li inoltra agli aventi diritto di voto.

Per lo scambio di messaggi, il protocollo può prevedere i seguenti canali di comunicazione:

- votanti ↔ piattaforma utente
- votanti ↔ ausilio tecnico affidabile
- ausilio tecnico affidabile ↔ piattaforma utente
- piattaforma utente ↔ sistema
- sistema ↔ tipografia
- tipografia → aventi diritto di voto

[8]Un protocollo crittografico è un protocollo dotato di funzioni di sicurezza crittografica volto ad adempiere gli obiettivi di sicurezza. I protocolli crittografici figurano nel livello di modello e non presentano funzioni di implementazione dirette ma unicamente funzioni di sicurezza astratte.

Le componenti del sistema e i canali di comunicazione sono affidabili oppure non lo sono. Le componenti affidabili del sistema mettono al sicuro, senza eccezioni, i dati segreti ed eseguono esclusivamente le operazioni prescritte dal protocollo. I canali affidabili assicurano che i messaggi trasmessi rimangano segreti. Inoltre, il destinatario del messaggio può fare affidamento sul fatto che il suo mittente coincide con quella componente del sistema prescritta dalla definizione del canale.

Il modello astratto utilizzato prevede inoltre un aggressore, che può corrompere e sottoporre al proprio controllo tutte le componenti del sistema e tutti i canali di comunicazione non affidabili. Le componenti del sistema corrotte comunicano all'aggressore tutti i dati segreti e operano illimitatamente secondo le sue istruzioni. L'aggressore può altresì leggere o intercettare messaggi scambiati su canali non affidabili e immettere a sua volta messaggi a suo piacimento.

Ipotesi sul grado di fiducia nel modello astratto (verificabilità individuale del protocollo): quanto alla verificabilità individuale si suppone in questo modello che ausilii tecnici affidabili, il sistema e la tipografia siano affidabili. Per contro, la piattaforma utente e una quota significativa degli aventi diritto di voto sono ritenuti non affidabili. Fra i canali di comunicazione si suppongono non affidabili solo i due canali «piattaforma utente ↔ sistema» e «sistema ↔ tipografia».

Obiettivo di sicurezza nel modello astratto (verificabilità individuale del protocollo): considerate le ipotesi di fiducia date, l'aggressore non può raggiungere i seguenti obiettivi senza che un votante abbia la possibilità di riconoscere con grande probabilità un avvenuto attacco:

- modifica del voto prima della registrazione;
- sottrazione del voto prima della registrazione;
- deposito di un voto.

Per raggiungere l'obiettivo di sicurezza, nel protocollo si impiegano esclusivamente elementi crittografici considerati sicuri.

Verificabilità individuale del sistema nell'attuazione: il sistema si avvale di un protocollo crittografico che adempie l'obiettivo di sicurezza per la verificabilità individuale nel modello astratto. Laddove necessario, l'ipotesi di affidabilità delle componenti di sistema e dei canali di comunicazione è giustificata da corrispondenti misure di sicurezza.

Il numero 4.2 mette in relazione le disposizioni dell'articolo 4 con l'obiettivo di sicurezza nel modello astratto e le esegue laddove necessario. Inoltre, esso contiene requisiti di sicurezza riguardanti le componenti di sistema e i canali di comunicazione che nel modello astratto si suppone siano affidabili.

4.2 Disposizioni supplementari inerenti alla verificabilità individuale

4.2.1	(ad art. 4 cpv. 2) La nota di conferma non deve avvenire in un'unica transazione, ma può essere anche ripartita su diversi messaggi che il votante riceve durante il processo di espressione del voto. (In questo caso, l'ultimo di questi messaggi conferma la registrazione del voto quale voto espresso conformemente al sistema). Qualora, prima dell'espressione definitiva del voto (e dunque prima di ricevere l'ultimo messaggio), il votante decida di interrompere il processo, egli deve sempre avere la possibilità di esprimere il proprio voto in modo convenzionale.
4.2.2	(ad art. 4 cpv. 2) Questo requisito va attuato in modo che il rischio dell'acquisto di voti non aumenti in maniera significativa rispetto al voto per corrispondenza.
4.2.3	(ad art. 4 cpv. 3) L'obiettivo consiste nell'impedire che componenti del sistema non affidabili possano esprimere un voto di nascosto. La disposizione va interpretata in tal senso e il protocollo va verificato di conseguenza.

4.2.4	(ad art. 4 cpv. 4) La nota di conferma è valida se permette ai votanti di riconoscere manipolazioni del loro voto conformemente all'obiettivo di sicurezza e considerate le ipotesi date sul grado di fiducia. In questo modo l'aggressore non può ingannare i votanti confezionando mediante le componenti di sistema non affidabili una nota di conferma che li induca a credere che il voto che hanno espresso sulla piattaforma utente è stato registrato come voto espresso conformemente al sistema. La probabilità che l'aggressore riesca ad allestire una simile nota di conferma indovinando correttamente i dati (questo vale per analogia per la nota di conferma che non è stato espresso alcun voto) non deve superare lo 0,1 per cento.
4.2.5	(ad art. 4 cpv. 4) Si possono prevedere facilitazioni per permettere agli aventi diritto di voto disabili di verificare la nota di conferma. Soltanto in questo caso è possibile scostarsi dall'obiettivo di sicurezza: più precisamente, in questo caso la validità delle note di conferma può essere fatta dipendere dall'affidabilità della piattaforma utente. Ciò consente ad esempio la scansione del riferimento di verifica prima di esprimere il voto. Tali facilitazioni devono essere riservate esclusivamente a un piccolo gruppo di aventi diritto di voto che, senza di esse, non sarebbero in grado di interpretare la nota di conferma quanto alla sua validità. Gli aventi diritto di voto per i quali ciò non vale devono essere in linea di massima incentivati a verificare le note di conferma secondo la procedura prevista.
4.2.6	(ad art. 4 cpv. 5) Qualora i votanti utilizzino un ausilio tecnico particolare per procedere alla verifica, esso deve essere stato sviluppato specificatamente per memorizzare in sicurezza elementi segreti ed eseguire operazioni crittografiche, ad esempio apparecchi impiegati per l'*homebanking* sicuro. Inoltre, i votanti devono potersi convincere del corretto funzionamento dell'ausilio esprimendo voti di prova.
4.2.7	(ad art. 4 cpv. 5) Oltre al catalogo «Requisiti posti alle tipografie», vige la seguente disposizione: tutti i macchinari che, in qualsivoglia forma, partecipano al trattamento di dati non crittati o non firmati inerenti al riferimento di verificabilità devono essere sorvegliati fisicamente secondo il principio del doppio controllo durante l'intero periodo di calcolo. Sono ammessi solamente collegamenti di rete i cui elementi sono collegati attraverso cavi fisici in modo tale che, fino alla distruzione dei dati confidenziali, nessun altro macchinario può accedervi in maniera evidente.
4.2.8	(ad art. 4 cpv. 5) Per il sistema lato server non vigono disposizioni supplementari. Nell'attuare i requisiti per la configurazione di processi elementari e i requisiti di sicurezza (cfr. art. 2 e n. 2 e 3) occorre tuttavia considerare che la confidenzialità dei dati connessa con il riferimento di verifica è decisiva per la correttezza del risultato, la segretezza del voto e l'esclusione di risultati parziali anticipati.
4.2.9	(ad art. 4 cpv. 4) L'affidabilità del canale tra tipografia e aventi diritto di voto può essere ritenuta data, se le informazioni sono state recapitate per il tramite della Posta svizzera oppure personalmente dalle persone coinvolte.

4.3 Modello astratto completo riguardante l'articolo 5

Il modello astratto completo concepisce il sistema come non affidabile. Contempla invece verificatori che valutano il corretto accertamento del risultato sulla base di un ausilio affidabile e sulla base di «componenti di controllo» indipendenti.
In questo modo identifica le seguenti componenti supplementari del sistema:

Componente di controllo	Interagisce con il sistema e le rimanenti componenti di controllo cosicché alla fine dello scrutinio possa approntare una nota di conferma valida relativa al corretto accertamento del risultato.
Verificatori	Dopo il conteggio ricevono dal sistema una nota di conferma del corretto accertamento del risultato.
Ausilio tecnico dei verificatori	I verificatori possono utilizzare un ausilio tecnico per valutare la nota di conferma.

Il protocollo crittografico può prevedere i seguenti canali di comunicazione supplementari per lo scambio di messaggi:

- componente di controllo ↔ sistema;
- sistema ↔ ausilio tecnico dei verificatori;
- ausilio tecnico dei verificatori ↔ verificatori;
- canali bidirezionali per la comunicazione tra le componenti di controllo.

Ipotesi sul grado di fiducia nel modello astratto (verificabilità individuale del protocollo): si impiegano varie componenti di controllo che vengono riassunte in uno o pochi gruppi. Come per il sistema, si deve ipotizzare che una singola componente di controllo non sia affidabile. Può tuttavia valere l'ipotesi che almeno una componente di controllo per gruppo sia affidabile, senza tuttavia stabilire di quale si tratti. La quantità di gruppi di componenti di controllo costituisce la parte affidabile del sistema, la cui affidabilità è definita dall'affidabilità di almeno una componente di controllo in ognuno dei gruppi. La validità della nota di conferma che un verificatore riceve in virtù dell'articolo 5 può dipendere solamente dall'affidabilità della parte affidabile del sistema e del suo ausilio tecnico. Si ipotizza poi che almeno un verificatore affidabile verifichi la nota di conferma mediante un ausilio tecnico affidabile. Eventuali ulteriori verificatori e i loro ausilii tecnici sono considerati non affidabili. Tra i canali di comunicazione supplementari si può ipotizzare che sia affidabile unicamente quel verificatore e i suoi ausilii tecnici. Il sistema è da ritenere non affidabile.

Obiettivo di sicurezza nel modello astratto (verificabilità completa del protocollo):

- considerate le ipotesi date sul grado di fiducia riguardanti la verificabilità completa del protocollo, l'aggressore non può raggiungere i seguenti obiettivi senza che un votante o un verificatore affidabile abbia la possibilità di riconoscere con grande probabilità un avvenuto attacco:
  - modifica del voto prima della registrazione nella parte affidabile del sistema;
  - sottrazione del voto prima della registrazione nella parte affidabile del sistema;
  - espressione di un voto;
  - modifica di un voto espresso conformemente al sistema, il cui deposito è stato registrato dalla parte affidabile del sistema;
  - sottrazione di un voto espresso conformemente al sistema, il cui deposito è stato registrato dalla parte affidabile del sistema;
  - inserimento di un voto;
- considerate le ipotesi date sul grado di fiducia riguardanti la completa verificabilità del protocollo, l'aggressore non può né infrangere la segretezza del voto né rilevare risultati parziali anticipati senza corrompere gli aventi diritto di voto o la loro piattaforma utente.

Per raggiungere l'obiettivo di sicurezza si impiegano esclusivamente elementi crittografici considerati sicuri.

Verificabilità completa del sistema nell'attuazione: valgono le medesime disposizioni vigenti per la verificabilità individuale.

Il numero 4.4.4 mette in relazione le disposizioni dell'articolo 5 con l'obiettivo di sicurezza nel modello astratto e le esegue laddove necessario. Inoltre, esso contiene requisiti di sicurezza riguardanti le componenti del sistema e i canali di comunicazione ritenuti affidabili nel modello astratto.

4.4 Disposizioni supplementari inerenti alla verificabilità completa

4.4.1	(ad art. 5 cpv. 1) L'impiego di verificatori contribuisce alla trasparenza. Gli aventi diritto di voto devono poter contare sul fatto che, in caso di dubbio, i verificatori segnalerebbero loro ogni irregolarità. Volutamente non viene precisato da quali cerchie debbano provenire le persone incaricate di svolgere il ruolo di verificatore.
4.4.2	(ad art. 5 cpv. 3) In virtù delle informazioni nella parte affidabile del sistema (tra le quali può trovarsi lo stesso voto crittato), i verificatori possono constatare se un voto è stato considerato nella sua forma invariata quale immissione per l'accertamento del risultato. I votanti devono così poter confidare nel fatto che i dati nella parte affidabile del sistema non vengono eliminati o manipolati. Nella letteratura tecnica si trovano in merito proposte volte a pubblicare i voti crittati su un «albo» elettronico (*public board*). Un albo viene realizzato includendo varie componenti affidabili, cosicché le iscrizioni vengono cancellate o modificate di nascosto soltanto se diverse componenti sono corrotte. Con l'aiuto di una piattaforma utente affidabile i votanti possono in ogni momento constatare che il loro voto si trova nella massa dei voti espressi. Alla fine della votazione, l'albo contiene il risultato e la nota di conferma del corretto accertamento del risultato, confezionata nell'ambito della verificabilità universale. I votanti potrebbero così, nello spirito della massima trasparenza possibile, assumere il ruolo di «verificatori». Varie considerazioni sui rischi, non da ultimo connesse con l'ipotesi, fondata sulla prassi, che le piattaforme utente possano essere considerate non affidabili, possono far propendere per una pubblicazione non illimitata dei dati della parte affidabile del sistema, rilevanti per la verificabilità. È perciò ammissibile mettere a disposizione i dati di una cerchia limitata di verificatori. Nella terminologia della letteratura tecnica, il requisito può perciò essere inteso in questa maniera: *i votanti ricevono dalle componenti competenti per l'albo una nota di conferma che esse hanno ricevuto il loro voto (o dati sufficienti per la verifica universale). La sua validità non può dipendere dall'affidabilità di una piattaforma utente non affidabile o dal sistema. Al più tardi dopo l'accertamento del risultato (ma prima della pubblicazione), i verificatori ottengono l'accesso all'albo e constatano che il risultato considera ogni voto sull'albo in conformità con le norme vigenti.*
4.4.3	(ad art. 5 cpv. 3 lett. b) L'obiettivo consiste nell'impedire che componenti del sistema non affidabili possano esprimere un voto di nascosto. La disposizione va interpretata in questo senso e il protocollo verificato di conseguenza.
4.4.4	(ad art. 5 cpv. 3 lett. c) La confidenzialità dei dati inerenti a un eventuale riferimento di verifica può così dipendere, anche all'interno dell'infrastruttura, solamente dalla parte affidabile del sistema.
4.4.5	(ad art. 5 cpv. 4) L'indipendenza e l'isolamento dell'ausilio tecnico devono garantire che la valutazione della nota di conferma non possa essere influenzata dal sistema. Non si precisa tuttavia volutamente se gli ausilii tecnici e i corrispondenti programmi debbano essere resi disponibili dal sistema o dai verificatori. I verificatori devono tuttavia poter constatare facilmente che l'ausilio funziona correttamente. Tale sarebbe il caso, ad esempio, se i verificatori stessi potessero scrivere i programmi o per lo meno analizzarli preliminarmente. Prima di verificarli, potrebbero realizzare l'ausilio assieme ai responsabili del sistema e compilare e installare i programmi di verifica. Di massima, ai fini della trasparenza, i programmi di verifica dovrebbero essere facili da scrivere.
4.4.6	(ad art. 5 cpv. 4 lett. a, b) Un voto è considerato espresso in modo conforme al sistema soltanto se i dati di autenticazione *client* utilizzati a tale scopo corrispondono a dati di autenticazione lato server definiti nella fase di preparazione dello scrutinio e «attribuiti» a un avente diritto di voto. La nota di conferma deve perciò contenere la conferma che non sono stati generati dati di autenticazione non attribuiti per esprimere i voti. A tale scopo, durante la preparazione dello scrutinio, alle componenti di controllo o ai verificatori devono essere stati consegnati dati pertinenti quale termine di paragone. I verificatori devono constatare che il numero dei dati di autenticazione corrisponde al numero (ufficiale) degli aventi diritto di voto ammessi. In questo caso i dati di autenticazione possono essere considerati come «attribuiti» a un avente diritto di voto. In tal modo non è ancora assicurato che dati di autenticazione *client* di aventi diritto affidabili non siano stati utilizzati abusivamente per esprimere un voto conforme al sistema. In virtù del relativo punto nell'obiettivo di sicurezza del modello astratto o dell'articolo 5 capoverso 3 lettera b, gli aventi diritto di voto possono tuttavia constatarlo.

4.4.7	(ad art. 5 cpv. 5) La nota di conferma è valida se permette ai votanti o ai verificatori di riconoscere manipolazioni dei voti alla luce dell'obiettivo di sicurezza e considerate le ipotesi date sul grado di fiducia. In tal modo l'aggressore non può indurre in errore i verificatori e allestire, avvalendosi delle componenti di sistema non affidabili, una nota di conferma per giustificare un risultato manipolato o influenzarne l'allestimento. Nell'ambito della verificabilità universale vigono le seguenti disposizioni: i verificatori devono in ogni caso potere riconoscere la sottrazione e mancata sostituzione di un voto espresso confomemente al sistema, registrato dalla parte affidabile del sistema; i verificatori devono in ogni caso potere riconoscere l'inserimento di un voto senza che un altro venga sottratto; la probabilità di successo di manipolare lo 0,1 per cento dei voti parziali (p. es. mediante sottrazione e simultaneo inserimento), cosicché non riflettano più il senso della nota di conferma generata nell'ambito della verifica individuale, può essere al massimo dell'1 per cento. Se la probabilità non è trascurabile[9] in termini crittografici, l'incertezza deve poter essere ridotta sufficientemente procedendo a diversi spogli utilizzando nuovi valori aleatori.
4.4.8	(ad art. 5 cpv. 5) Se l'applicazione utilizzata sulla piattaforma utente per crittare il voto è messa a disposizione dal sistema, allora è da attribuire anche al sistema lato server. Si deve impedire che, mediante una manipolazione lato server dell'applicazione, la segretezza del voto di votanti affidabili venga violata senza corrompere la loro piattaforma utente. I votanti devono perciò avere la possibilità di sincerarsi con l'aiuto di una piattaforma affidabile che l'applicazione invia il loro voto crittato con la chiave corretta. Ciò è possibile, ad esempio, impiegando la tecnologia browser che consente di riconoscere il codice fonte dell'applicazione utente. I votanti possono così sincerarsi che la chiave pubblica utilizzata corrisponde a quella dello scrutinio e che l'applicazione esegue esclusivamente le operazioni previste. In alternativa, il codice fonte potrebbe essere firmato mediante un gruppo di componenti di controllo.
4.4.9	(ad art. 5 cpv. 5) Nel senso dell'obiettivo di sicurezza si deve impedire che il sistema lato server possa, in collaborazione con un avente diritto di voto non affidabile, conoscere il contenuto di un voto espresso. A tale scopo occorre assicurare che, neanche dopo un adattamento esteriore, questi possa depositare come se fosse il proprio un voto crittato, espresso con l'obiettivo di conoscere il contenuto del voto mediante la nota di conferma che riceve nell'ambito della verificabilità individuale.
4.4.10	(ad art. 5 cpv. 5) In seguito al requisito riguardante la garanzia della segretezza del voto e l'assenza di risultati parziali anticipati, le chiavi private per decrittare voti non devono essere a disposizione di alcuna componente del sistema, per lo meno durante i periodi di apertura del canale di voto elettronico. È tuttavia ammesso che possano essere calcolate con la partecipazione di tutte le componenti di controllo di un gruppo. È anche ammesso prevedere un gruppo di componenti di controllo sotto forma di un gruppo di persone. Ogni membro di questo gruppo potrebbe conservare su un supporto di memorizzazione portatile una parte della chiave privata. Per garantire la segretezza del voto, dopo la decrittazione la chiave privata può essere resa disponibile solamente se i voti vengono espressi anonimamente e, considerate le ipotesi date sul grado di fiducia, nessuna crittazione di un voto può essere messa in relazione con l'identità di un votante. Non è poi ammesso, come conseguenza del requisito riguardante l'assenza di risultati parziali anticipati che, durante i periodi di apertura del canale di voto elettronico, in un qualsiasi momento vi siano voti in forma decrittata al di fuori della piattaforma utente.
4.4.11	(ad art. 5 cpv. 6) L'identificazione di disfunzioni serie del sistema dipende dall'affidabilità della «parte affidabile del sistema». Tali disfunzioni comprendono segnatamente errori di calcolo che influenzano il risultato, la violazione della segretezza del voto e l'allestimento di risultati parziali anticipati. A questo proposito l'attuazione di proposte note nella letteratura tecnica assicura un'affidabilità particolarmente elevata. Tali proposte sono talmente avanzate che solo nel caso in cui tutte le componenti di controllo di un gruppo non funzionino correttamente – ad esempio a seguito di manipolazioni passate inosservate – non è possibile identificare una disfunzione seria. Ma se una sola componente di controllo funziona correttamente, è possibile riconoscere qualsiasi disfunzione seria del sistema. Nell'astrazione, le componenti di controllo spesso vengono chiamate in inglese *«trustee»*. Nell'astrazione, queste ultime vengono rappresentate quali istanze in grado di eseguire

[9] Corrisponde alla probabilità di decrittare, senza conoscerne la chiave, un valore che è stato crittato con un algoritmo ritenuto sicuro e corrispondenti parametri.

	calcoli complessi e di tenere segreti elementi privati. I calcoli possono contenere la mescolanza e la ricrittazione corrette e comprovabili di voti (quanto alla loro anonimizzazione; ogni *trustee* corrisponde a un nodo misto di una rete di ricrittazione), la tenuta di un albo elettronico affidabile o l'allestimento della PKI («*public key infrastructure*»; infrastruttura a chiave pubblica) e, con l'aiuto della sua chiave privata ripartita, la decrittazione corretta comprovabile di voti. Nell'astrazione, i *trustee* sono spesso rappresentati come persone in grado di calcolare come macchine. Il fatto che tengano sotto chiave gli elementi segreti o non li utilizzino per inviare messaggi che possono essere impiegati abusivamente dipende esclusivamente dalla loro volontà di non voler collaborare con all'aggressore. Pur se in pratica si deve differenziare tra la macchina e la persona che la configura e la sorveglia, la descrizione del protocollo crittografico può tuttavia rappresentare le componenti di controllo quali *trustee* autonomi.
4.4.12	(ad art. 5 cpv. 6) Il software di componenti di controllo deve essere semplice da analizzare e limitarsi per quanto possibile a funzioni crittografiche elementari.
4.4.13	(ad art. 5 cpv. 6) Le componenti di controllo vanno realizzate, aggiornate, configurate e assicurate in un processo osservabile.
4.4.14	(ad art. 5 cpv. 6) Le componenti di controllo devono per quanto possibile differenziarsi tra loro e il loro esercizio deve avvenire indipendentemente dalle altre componenti di controllo. Ciò è funzionale all'obiettivo secondo cui un accesso andato a buon fine ma non autorizzato non procuri per quanto possibile alcun vantaggio nel tentativo di accedere di nascosto a un'ulteriore componente di controllo (implementazione di «trustee»; cfr. n. 4.4.12). Rimane così garantita l'affidabilità di un gruppo di componenti di controllo. A tale scopo occorre prevedere almeno le seguenti misure: • l'esercizio e la sorveglianza delle componenti di controllo devono essere sotto la responsabilità di differenti persone; • l'hardware e i sistemi di sorveglianza delle componenti di controllo devono differenziarsi; • le componenti di controllo devono essere collegate a reti differenti; • le componenti di controllo possono essere accessibili fisicamente e logicamente soltanto per persone responsabili dell'esercizio e della sorveglianza di una componente di controllo specifica. Tentativi di accesso da parte di responsabili di altre componenti di controllo devono essere riconosciuti e notificati ai responsabili delle corrispondenti componenti di controllo.
4.4.15	(ad art. 5 cpv. 6) Le componenti di controllo devono eseguire esclusivamente le operaziomi previste. Devono essere mirate a riconoscere accessi non autorizzati e ad allarmare le persone responsabili. Queste ultime devono prevedere misure di sorveglianza esterne quali la sorveglianza e un protocollo resistente alle manipolazioni del traffico di rete o la sorveglianza fisica con telecamere sottoposte al loro controllo. Le persone responsabili devono essere considerate particolarmente affidabili e degne di fiducia.
4.4.16	(ad art. 5 cpv. 6) Devono essere impiegate almeno quattro componenti di controllo per gruppo con differenti sistemi operativi. Qualora le componenti di controllo siano apparecchi (modulo di sicurezza hardware, HSM) specificamente sviluppati e verificati per l'esecuzione sicura di operazioni crittografiche, un gruppo può essere costituito da due componenti di controllo di fabbricanti differenti. Entrambi gli HSM possono utilizzare il medesimo sistema operativo.
4.4.17	(ad art. 5 cpv. 6) Un HSM deve disporre di un certificato affidabile per confermare che gli elementi segreti sono inaccessibili e che ogni loro utilizzo viene registrato in maniera tale che la persona responsabile possa riconoscere se è abusivo. Il certificato deve per lo meno corrispondere, per analogia, al grado EAL4 dei Common Criteria [CC] o al livello 3 della norma FIPS 140-2. È consentito aggiungere a un HSM un software che operi in un settore protetto. In questo caso il certificato deve riferirsi anche all'affidabilità di quest'ultimo. Occore esaminare il software e la sua corretta installazione.

5. Criteri di verifica dei sistemi e del loro esercizio (ammissione di più del 30 per cento dell'elettorato cantonale)

Ciascuno dei numeri da 5.1 a 5.6 corrisponde a una verifica esterna del sistema. In caso di esito positivo, le organizzazioni competenti rilasciano un attestato all'attenzione del Cantone che ha conferito loro il mandato di verifica. Il Cantone allega l'attestato alla domanda di nulla osta che presenta alla CaF. Gli attestati da presentare sono riassunti nel numero 6.

5.1 Verifica del protocollo crittografico

5.1.1	Criteri di verifica: il protocollo deve adempiere l'obiettivo di sicurezza considerate le ipotesi sul grado di fiducia nel modello astratto di cui al numero 4. A tale scopo devono esserci una dimostrazione crittografica e una simbolica. Riguardo alle componenti di base crittografiche, tali dimostrazioni possono essere condotte con misure di sicurezza generalmente riconosciute (p. es. "random oracle model", "decisional Diffie-Hellman assumption", "Fiat-Shamir heuristic"). Il protocollo deve fondarsi per quanto possibile su protocolli esistenti e sperimentati.
5.1.2	Competenze: le dimostrazioni devono essere fornite o verificate da istituzioni altamente specializzate. La scelta di un'organizzazione va previamente approvata dalla CaF. Procedura concreta: 1. il Cantone notifica alla CaF l'impiego di un nuovo protocollo o la modifica di quello esistente. Esso può proporre un'istituzione o una persona che procede alla verifica; 2. la CaF valuta la proposta; 3. la CaF informa il Cantone della propria decisione. Nel caso di sistemi verificabili individualmente, se le ipotesi sul grado di fiducia sono solide, si possono impiegare protocolli semplici. In questo caso la CaF può prescindere dall'avvalersi di un'organizzazione esterna.
5.1.3	Durata di validità di un attestato: una verifica completa deve avvenire precedentemente alla prima messa in esercizio. Il protocollo deve essere nuovamente verificato in occasione di ogni sua modifica e in seguito a nuove importanti conoscenze della ricerca relative alla sicurezza degli elementi crittografici impiegati.

5.2 Verifica della funzionalità

5.2.1	Criteri di verifica: la funzionalità deve adempiere i requisiti indicati nei numeri 2, 3 e 4 o sostenere adeguatamente gli obiettivi predefiniti. Eventualmente un protocollo va attuato in conformità con l'articolo 4 o l'articolo 5. Occorre assicurare che siano attuati, a titolo di misure di sicurezza, i *Security Functional Requirements* (SFR) indicati nel *Protection Profile* (PP) del Bundesamt für Sicherheit in der Informationstechnik (BSI) oppure mezzi equivalenti. La funzionalità va verificata secondo i criteri principali dell'EAL2 attenendosi al formalismo dei *Common Criteria* (CC).
5.2.2	Competenze: la verifica è svolta da un'istituzione accreditata dal Servizio di accreditamento svizzero (SAS).
5.2.3	Durata di validità di un attestato: la funzionalità va nuovamente verificata in occasione di ogni modifica rilevante, ad esempio dopo una modifica del protocollo crittografico.

5.3 Verifica dell'infrastruttura e dell'esercizio

5.3.1	Criteri di verifica: il sistema e il suo esercizio devono adempiere i requisiti indicati nei numeri 2, 3 e 4 o sostenere adeguatamente gli obiettivi predefiniti. La sicurezza dell'informazione del sistema e del suo esercizio deve essere garantita mediante l'installazione, l'implementazione, l'esercizio, la sorveglianza, la verifica, la cura e il miglioramento di un sistema di gestione di sicurezza dell'informazione (ISMS) ai sensi della norma ISO/IEC 27001:2013 (Information technology – Security techniques – Information security management systems – Requirements). Il campo di applicazione dell'ISMS deve comprendere tutte le unità organizzative del gestore di sistema responsabili sotto il profilo giuridico, amministrativo e operativo per il sistema di Voto elettronico.
5.3.2	Competenze: l'efficacia e l'adeguatezza dell'ISMS devono essere provate presentando il certificato rilasciato da un organismo di certificazione che attesta la certificazione dell'ISMS ai sensi dell'ISO/IEC 27001:2013. L'organismo deve altresì attestare che i requisiti descritti nei numeri 2, 3 e 4 vengono adempiuti se essi non sono già coperti dall'*audit* ai sensi della norma ISO/IEC 27001:2013. L'organismo di certificazione deve essere accreditato dal Servizio di accreditamento svizzero (SAS) per eseguire questo tipo di *audit*.
5.3.3	Durata di validità di un attestato: *audit* di ripetizione devono essere svolti negli intervalli stabiliti dalla norma ISO 27001:2013. A ogni impiego deve essere presentato un certificato valido. Occorre procedere a un *audit* di ripetizione anche se si decide di rinunciare a una misura di sorveglianza volta ad assicurare un impiego sicuro e indipendente di componenti di controllo oppure di adeguare tale misura in modo significativo. Se viene pubblicata una nuova versione dello standard ISO/IEC 27001:2013, al più tardi dopo la scadenza del termine transitorio deve essere provata una certificazione valida dell'ISMS secondo la nuova versione. Il campo di applicazione dell'ISMS non può essere ristretto a favore di questa nuova certificazione.

5.4 Verifica delle componenti di controllo

5.4.1	Criteri di verifica: le componenti di controllo devono adempiere i requisiti sanciti nel numero 4 o sostenere adeguatamente gli obiettivi predefiniti. Le funzioni la cui affidabilità è determinante per la validità delle note di conferma previste nell'ambito della verificabilità vanno verificate accuratamente in base al codice fonte e al protocollo crittografico. Occorre assicurare che siano attuati, a titolo di misure di sicurezza, i *Security Functional Requirements* (SFR) indicati nel *Protection Profile* (PP) del Bundesamt für Sicherheit in der Informationstechnik (BSI) oppure mezzi equivalenti. La funzionalità va verificata secondo i criteri principali dell'EAL4 attenendosi al formalismo dei Common Criteria (CC). Le componenti di base, quali i software volti ad assicurare un impiego sicuro e indipendente di componenti di controllo, i sistemi operativi o i server impiegati devono dimostrare di soddisfare i migliori standard.
5.4.2	Competenze: la verifica è eseguita da un'istituzione accreditata dal Servizio di accreditamento svizzero (SAS).
5.4.3	Durata di validità di un attestato: nei seguenti casi vanno verificate nuovamente le componenti di controllo: – a ogni modifica apportata al codice fonte delle funzioni la cui affidabilità è determinante per la validità delle note di conferma previste nell'ambito della verificabilità; e – in caso di rinuncia o di adeguamenti significativi a meccanismi che servono all'impiego sicuro e indipendente di componenti di controllo; e – nel caso di un HSM (*hardware security module*), l'impiego delle funzioni la cui affidabilità è determinante per la validità delle note di conferma previste nell'ambito della verificabilità deve in ogni caso aver luogo nell'ambito di una verifica. Se vengono impiegate nuove versioni di componenti di base (nuovi server, *patch* riguardanti sistema operativo o software che servono all'impiego sicuro e indipendente di componenti di controllo), non deve avere luogo alcun nuovo controllo se è ancora possibile dimostrare che le componenti corrispondono ai migliori standard.

5.5 Verifica della protezione contro tentativi di introdursi nell'infrastruttura

5.5.1	Criteri di verifica: le persone che conducono un attacco da Internet non devono potersi introdurre nell'infrastruttura per ottenere accesso a dati importanti o assumere il controllo su funzioni importanti. A tale scopo, un'istituzione specializzata tenta di verificare nell'ambito di un test di penetrazione se è in grado di introdursi nell'infrastruttura sulla base della documentazione del sistema, sfruttando i punti deboli conosciuti delle tecnologie impiegate. La documentazione del sistema messa a disposizione dell'istituzione in questione deve contenere almeno i documenti relativi all'architettura, al flusso di dati e alle tecnologie impiegate. L'istituzione verifica per lo meno i punti deboli documentati nell'*Open Web Application Security Project* (OWASP).
5.5.2	Competenze: la verifica è eseguita da un'istituzione accreditata dal Servizio di accreditamento svizzero (SAS).
5.5.3	Durata di validità di un attestato: una nuova verifica deve essere effettuata dopo tre anni.

5.6 Verifica di una tipografia

5.6.1	Criteri di verifica: oltre alle disposizioni figuranti nel catalogo di requisiti posti alle tipografie (cfr. «Vote électronique: catalogue de critères pour les imprimeries») una tipografia deve adempiere il requisito di cui al numero 4.2.5.
5.6.2	Competenze: la verifica è eseguita da un'istituzione accreditata dal Servizio di accreditamento svizzero (SAS).
5.6.3	Durata di validità di un attestato: dopo due anni deve avere luogo una nuova verifica. Anche dopo aver deciso di rinunciare a una misura o di adeguarla in modo significativo occorre procedere a una ripetizione della verifica.

6. Attestati da presentare per il nulla osta

6.1	Il Cantone richiedente presenta gli attestati per le verifiche (cfr. art. 7) ricevuti dalle istituzioni competenti. L'attestato riguardante la verifica di cui al numero 5.3 deve essere un certificato valido ai sensi della norma ISO/IEC 27001:2013.
6.2	Il Cantone può far valere la validità di un attestato per diversi scrutini. In questo caso il Cantone giustifica per quale motivo, riguardo allo scrutinio interessato, non ha ripetuto la verifica. A tale scopo indica tutte le modifiche al sistema pianificate o effettuate fino al momento dello scrutinio, mostrando così che si tratta di adeguamenti di minore importanza che non hanno alcun influsso negativo sull'analisi dei rischi.
6.3	Il Cantone presenta tutti i protocolli dei test risultanti dall'attuazione del concetto di test (n. 3.5). Si impegna a fornire successivamente ulteriori protocolli se un test viene eseguito appena prima dello scrutinio.
6.4	Il Cantone presenta la sua attuale analisi dei rischi (art. 3) e si impegna a segnalare immediatamente le relative modifiche. Tutti i rischi risultanti dall'adempimento degli obiettivi di sicurezza devono essere determinati attraverso un'analisi dei rischi. Devono poi essere valutati anche rischi riguardanti il contesto del voto elettronico nell'amministrazione e a livello pubblico. L'analisi deve avvenire conformemente a una metodologia che prevede le seguenti attività: – identificare i rischi; – analizzare i rischi; – valutare i rischi. I dettagli della metodologia impiegata e i criteri di accettazione dei rischi predefiniti dal Cantone devono essere documentati. Quanto ai rischi risultanti dall'esercizio del sistema, in occasione dell'identificazione dei rischi nel caso in cui oltre il 30 per cento dell'elettorato cantonale sia ammesso al voto elettronico, occorre rispettare integralmente i requisiti metodologici della norma ISO/IEC 27001:2013.