Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Cancelleria federale CaF

Sezione Diritti politici

31.05.2013

Allegato del Regolamento tecnico Voto elettronico della Cancelleria federale del ... (RS ...)

Entrata in vigore: 1° gennaio 2014

V. 0.9 / maggio 2013

Indice

1. In generale

1.1. Riferimenti

[1] Legge federale del 17 dicembre 1976 sui diritti politici (LDP; RS 161.1)

[2] Ordinanza del 24 maggio 1978 sui diritti politici (ODP; RS 161.11)

[3] Vote électronique: catalogue de critères pour les imprimeries

[4] Common Criteria: Protection profile for basic set of security requirements for online voting products, versione 1.0

[5] Norme ISO/IEC 27001

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

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) Vendita 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
Esigenze per le stamperie	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

1.2. Abbreviazioni

BSI	Bundesamt für Sicherheit in der Informationstechnik (Germania)
CaF	Cancelleria federale
CC	Criteri comuni
DNS	Server di nomi di dominio (*Domain Name Server*)
DOS	Negazione del servizio (*Denial Of Service*)
EAL	Livello di valutazione della sicurezza (*Evaluation Assurance Level*)
ISO	Organizzazione internazionale di normazione (*International Organization for Standardization*)
LDP	Legge federale sui diritti politici
MITM	Man In The Middle (Uomo in mezzo)
ODP	Ordinanza sui diritti politici
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*)
VE	Voto elettronico

1.3. Definizioni

Messaggio di autenticazione: tutte le informazioni che una piattaforma utenti invia all'infrastruttura del VE dopo l'immissione dei dati di autenticazione *client*, affinché chi ha inviato un voto venga autenticato come avente diritto di voto. Deve risultare difficile generare un messaggio di autenticazione se non si conoscono i dati di autenticazione *client*.

Piattaforma utenti: strumento multifunzionale programmabile che è collegato a Internet e che viene utilizzato per votare. Si tratta generalmente di un computer standard, di uno smartphone o di un tablet.

Dati di autenticazione *client*: tutte le informazioni messe a disposizione di ogni singolo elettore e di cui questi ha bisogno per esprimere un voto (può p. es. trattarsi di un PIN, la cui immissione risulta nell'allestimento di una firma del 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 del VE. Per mezzo del messaggio di autenticazione e dei dati di autenticazione server (p. es. una chiave pubblica che permette di verificare la firma) l'infrastruttura del VE autentica che chi ha inviato un voto ha diritto di voto. Deve risultare difficile scoprire i dati di autenticazione *client*.

Negazione del servizio (abbreviato in DOS, dall'inglese *Denial Of Service*): nel trattamento digitale di dati, l'impossibilità di accedere a un servizio che in linea di principio dovrebbe essere disponibile.

DNS-spoofing, o DNS-poisoning (avvelenamento della cache DNS): attacco per mezzo del quale si riesce a modificare l'associazione fra il nome del server e l'indirizzo IP corrispondente.

Urna elettronica: area di memorizzazione nella quale i voti espressi conformemente al sistema vengono registrati in modo crittato. Nell'urna elettronica sono memorizzati unicamente i voti espressi conformemente al sistema.

Man in the middle: designa l'aggressore che conduce un attacco 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 in rete. L'aggressore può in tal modo leggere le informazioni e addirittura modificarle a suo piacimento.

Voto registrato: un voto è designato come registrato quando l'infrastruttura del VE ha preso atto che esso è stato espresso in modo definitivo.

Valutazione dei rischi: termine generico che contempla una serie di attività volte a *identificare, analizzare* e *valutare i rischi* (nota: nella versione 0.73 del Regolamento tecnico è utilizzata erroneamente l'espressione *analisi dei rischi*; l'errore sarà corretto successivamente).

Dati di autenticazione server: tutte le informazioni che, per mezzo di un messaggio di autenticazione, permettono di autenticare che chi ha inviato un voto ha diritto di voto.

Voto così come è stato rilevato: voto che corrisponde al suo rilevamento da parte del votante sulla piattaforma utenti, e che soprattutto da quel momento non è stato manipolato. (Corrisponde sempre alla volontà del votante, a meno che questi non abbia sbagliato al momento dell'immissione).

Voto espresso conformemente al sistema: un voto è «espresso conformemente al sistema» se

1. è espresso in modo definitivo da chi lo ha spedito; e
2. i dati di autenticazione *client* utilizzati e il messaggio di autenticazione che ne risulta corrispondono a un contrassegno di autenticazione lato server definito nella fase di preparazione e attribuito a un elettore prima che si recasse alle urne; e
3. l'urna elettronica non contiene ancora nessun voto espresso utilizzando gli stessi dati di autenticazione *client*.

Voto parziale: nelle votazioni designa un progetto, un controprogetto o una domanda risolutiva; nelle elezioni la scelta di una lista o la scelta di un candidato inserito in una lista.

Esercizio del VE: tutte le attività esercitate dal gestore del sistema di VE. Si utilizza anche solo «esercizio».

Funzionalità del VE: software lato server nonché software client lato client sulla piattaforma utenti, che mette a disposizione la funzionalità necessaria al VE, nel rispetto di tutti i requisiti in materia di sicurezza.

Infrastruttura del VE: l'hardware, il software, gli elementi di rete, i locali, i servizi e gli strumenti di ogni genere necessari all'esercizio tecnico delle funzionalità del VE lato server, nel rispetto di tutti i requisiti in materia di sicurezza. Si utilizza anche solo «infrastruttura».

Responsabile cantonale del VE: il responsabile, presso il Cantone, di una votazione per via elettronica. Definisce ed emana 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), redige il contratto concernente l'esecuzione dei meccanismi che regolano una votazione, compresi i requisiti di sorveglianza e di verifica, e affida l'esecuzione a un gestore di sistema di VE. Se è il caso, partecipa anche all'esercizio del VE. Si utilizza anche solo «responsabile cantonale».

Organizzazione del VE: la struttura organizzativa (compresa l'attribuzione di ruoli e responsabilità), i processi e le procedure organizzative del gestore del sistema di VE, necessarie all'esercizio delle

funzionalità del VE lato server, nel rispetto di tutti i requisiti in materia di sicurezza. Si utilizza anche solo «organizzazione».

Personale del VE: il responsabile dei gestori del sistema di VE, l'incaricato della sicurezza del VE, il responsabile del personale del VE, il responsabile della funzionalità del VE, il capotecnico del VE, gli amministratori del sistema di VE e della rete di VE, i tecnici della costruzione del VE e le parti terze del VE che sono necessari all'esercizio delle funzionalità del VE lato server, nel rispetto di tutti i requisiti in materia di sicurezza. Si utilizza anche solo «personale».

Responsabile del personale del VE: il responsabile del personale del VE presso il gestore del sistema di VE. Si utilizza anche solo «responsabile del personale».

Incaricato della sicurezza del VE: il responsabile del rispetto dei requisiti in materia di sicurezza dell'informazione presso il gestore del sistema di VE. Si utilizza anche solo «incaricato della sicurezza».

Sistema di VE: termine generico che contempla la funzionalità del VE, l'infrastruttura del VE e l'esercizio del VE. Si utilizza anche solo «sistema».

Amministratori del sistema di VE e della rete di VE: i responsabili della sorveglianza e della manutenzione quotidiana degli apparecchi e delle istallazioni dell'infrastruttura del VE presso il gestore del sistema di VE. Si utilizza anche solo «amministratori del sistema e della rete».

Gestore del sistema di VE: l'organizzazione (autorità o impresa privata) che in occasione di una votazione si assume l'intera responsabilità dell'esecuzione dei meccanismi che regolano il voto per via elettronica. Mette a disposizione, in misura adeguata, il personale del VE, l'organizzazione del VE e l'infrastruttura del VE. Taluni compiti concernenti l'esercizio possono tuttavia essere assunti anche dal responsabile cantonale del VE. Si utilizza anche solo «gestore del sistema».

Responsabile dei gestori del sistema di VE: il responsabile generale incaricato della conduzione (inclusa la comunicazione interna ed esterna), del rispetto dei requisiti previsti dalla legge e dal regolamento e degli impegni contrattuali, dell'organizzazione, della tecnica e delle tecnologie presso il gestore del sistema di VE. Si utilizza anche solo «responsabile dei gestori del sistema».

Probabilità trascurabile, in senso crittografico: la probabilità di decrittare, senza conoscerne la chiave, un valore che è stato crittato con un algoritmo ritenuto sicuro e parametrato in modo conseguente.

Voto ben formato: un determinato modo di compilare una scheda di voto. È possibile definire in anticipo 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 potranno essere depositati o meno nell'urna elettronica, se saranno ignorati al momento del conteggio, oppure se saranno presi in considerazione nel risultato finale.

2. Requisiti concernenti la struttura di processi elementari

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

2.1. Procedura di voto

A1.10	Il sistema di VE deve essere di facile utilizzo. Le istruzioni per gli utenti devono rifarsi a schemi già generalmente in uso.	F
A 1.20	Il sistema di VE deve essere senza barriere. Nello sviluppo di tale sistema la Cancelleria federale si avvale di un esperto di provate competenze. Attraverso il suo impegno durante lo sviluppo del sistema di VE lato client e dello sviluppo del materiale di voto per il VE, fa in modo che i bisogni degli aventi diritto di voto con disabilità siano considerati in modo adeguato. L'accessibilità del sistema di VE lato client deve essere verificata da un servizio riconosciuto dall'esperto conformemente allo standard eCH-0059. Nell'ambito della verifica della funzionalità del VE, che costituisce una delle condizioni per il nulla osta, il Cantone presenta un attestato in cui l'esperto valuta in modo positivo l'accessibilità del sistema di VE e del materiale di voto per il VE. Se la valutazione, benché positiva, è soggetta a riserve, dopo essersi consultata con l'esperto , la Cancelleria federale decide se il Cantone può utilizzare il sistema di VE.	F
A 1.30	I votanti dichiarano di aver preso atto delle regole del VE e delle loro responsabilità.	F
A 1.32	Prima di votare, gli aventi diritto devono essere resi attenti esplicitamente del fatto che, trasmettendo loro voti elettronici, partecipano a una decisione popolare. Prima di esprimere il proprio voto, l'elettore è tenuto a confermare che ha preso atto di questo messaggio.	F
A 1.33	Per votare per via elettronica, l'elettore deve provare all'autorità competente che è autorizzato a farlo attraverso i dati di autenticazione *client*.	F
A 1.35	I votanti prendono il loro voto e lo depositano nell'urna elettronica avvalendosi dei dati di autenticazione *client*.	F
A 1.37	Il modo in cui il sistema di VE lato client viene presentato ai votanti non influenza le loro scelte.	F,I
A 1.40	I votanti possono correggere il loro voto fino al momento in cui lo depositeranno in maniera definitiva nell'urna. Fino a quel momento il canale di voto convenzionale rimane a loro disposizione.	F
A 1.42	Le istruzioni per gli utenti non devono indurre a votare in modo precipitoso o senza riflettere.	F
A 1.45	Il sistema di VE permette di votare solo dopo che l'elettore ha esplicitamente controllato e confermato il proprio voto. Quest'ultimo gli viene mostrato nuovamente prima del voto definitivo.	F
A 1.47	Il sistema di VE offre all'elettore la possibilità di interrompere in ogni momento la procedura di voto senza che egli perda il diritto di votare.	F,I
A 1.50	Il sistema di VE tiene conto del fatto che il voto espresso non può essere stampato con i dati cliente utilizzati. (Se la tecnologia lo consente, le funzioni che permettono la stampa devono essere disattivate.)	F
A 1.60	La persona che ha votato deve poter verificare sull'apparecchio di cui si è servita che il suo voto è stato trasmesso. Essa riceve una conferma che il voto espresso è giunto a destinazione.	F,I
A 1.70	Dopo il voto, ai votanti non può essere data alcuna informazione sul voto da loro espresso.	F
A 1.80	Non deve essere possibile votare un'altra volta servendosi degli stessi dati di autenticazione *client*.	F,I

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

A 2.10	Il sistema di VE importa il catalogo elettorale.	F,I
A 2.15	Il sistema di VE importa le domande della votazione (p. es. gli oggetti posti in votazione o le liste dei candidati) per ogni livello federale e circondario elettorale interessato e le memorizza.	F,I
A 2.20	Per ciascun avente diritto di voto, il sistema di VE prepara i dati di autenticazione *client* e lo memorizza.	F
A 2.30	Se necessario, il sistema di VE prepara per ciascun avente diritto di voto i dati di autenticazione *client* e li memorizza. (Ciò è necessario solo nei casi in cui non sia utilizzato alcun mezzo di autenticazione esterno.)	F
A 2.40	Il sistema di VE prepara le chiavi crittografiche utilizzate e le memorizza.	F
A 2.50	Il gestore del sistema di VE definisce i parametri tecnici pertinenti per la realizzazione di una votazione.	I

2.3. Informazioni e sostegni

A 3.10	Il responsabile cantonale del VE elabora per i cittadini una strategia d'informazione sul voto elettronico.	I
A 3.15	La strategia garantisce che le informazioni siano state autorizzate dagli organismi competenti.	I
A 3.20	Su Internet sono disponibili consigli e regole sulla votazione 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
A 3.30	Gli aventi diritto di voto ottengono spiegazioni comprensibili sulle misure di sicurezza; ciò incrementa la loro fiducia nel voto elettronico.	F
A 3.40	Agli aventi diritto di voto vengono illustrati gli aspetti su cui devono prestare attenzione affinché possano votare in tutta sicurezza	F
A 3.45	Agli elettori viene spiegato in che modo possono cancellare il voto dalle memorie dell'apparecchio che hanno utilizzato per votare.	F
A 3.50	Gli elettori possono richiedere un supporto tecnico.	I
A 3.60	È necessario che controllori, per esempio una commissione di verifica, vengano informati e formati adeguatamente riguardo ai processi che sottostanno alla correttezza del risultato, al rispetto della segretezza del voto e all'assenza di risultati parziali anticipati (p. es. generazione di chiavi, stampa del materiale di voto, decrittaggio e spoglio). Essi devono poter capire i processi e il loro significato.	I

2.4. Preparazione alla stampa del materiale di voto

A4.10	Il materiale di voto deve essere concepito in modo che sia impossibile votare una seconda volta con un canale di voto convenzionale.	F,I
A4.20	Il sistema di VE crea il file necessario per la stampa del materiale di voto, includendo eventualmente i dati di autenticazione *client*.	F
A4.30	Il sistema di VE trasmette alla tipografia il file necessario alla stampa	F,I

2.5. Apertura e chiusura del canale di voto elettronico

A5.10	Il gestore del sistema di VE inizializza il sistema di VE. (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.)	I
A5.20	Il gestore del sistema di VE apre il canale di voto elettronico agli aventi diritto di voto.	F,I
A5.30	L'apertura e la chiusura precoci del canale di voto elettronico devono essere vietate.	I
A5.40	Il gestore del sistema di VE chiude il canale di voto elettronico.	F,I

2.6. Controllo della validità e registrazione dei voti espressi in modo definitivo

A6.10	Utilizzando il messaggio di autenticazione ricevuto e i dati di autenticazione *client*, il sistema di VE autentica che chi ha inviato il voto ha diritto di voto.	F
A6.20	Il sistema di VE verifica se per uno stesso elettore è già stato depositato un voto nell'urna elettronica.	F
A6.30	Quando il voto è valido, il sistema di VE informa i votanti della riuscita del voto e registra il suffragio nell'urna elettronica. Un voto non valido non vi viene registrato. (Il fatto che un voto sia ben formato costituisce p. es. un ulteriore criterio che determina la riuscita del voto.)	F

2.7. Conteggio dell'urna elettronica

A 7.10	Immediatamente dopo la chiusura del canale di voto elettronico, e conformemente alla legislazione cantonale, il gestore del sistema di VE avvia il decrittaggio dei voti contenuti nell'urna elettronica.	F,I
A 7.15	Il gestore del sistema di VE avvia il conteggio dei voti decrittati e registra i risultati dello scrutinio per ciascun circondario elettorale. È vietato cercare di ottenere maggiori dettagli.	F,I
A 7.30	Il gestore del sistema di VE redige un verbale sulla procedura di decrittaggio dei voti e sul loro conteggio.	I
A 7.35	Durante l'apertura dell'urna elettronica, ogni accesso al sistema o a una delle sue componenti deve essere effettuato da almeno due persone; esso deve essere protocollato e deve poter essere controllato da una rappresentanza delle autorità competenti.	F,I
A 7.40	Il gestore del sistema di VE trasmette i risultati della votazione 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 tradizionali.	F,I
A 7.50	Il sistema di VE mette a disposizione di un sistema terzo le informazioni necessarie che permettono a quest'ultimo di constatare, per mezzo di una carta di legittimazione, se un dato elettore ha già votato per via elettronica. In caso di tentativi con una percentuale di elettorato molto limitata (p. es. quelle condotte solo con Svizzeri all'estero), ai fini della protezione del segreto di voto bisogna impedire che a servizi esterni all'infrastruttura del VE vengano recapitati elenchi che permettono di identificare gli elettori che hanno espresso il loro voto per via elettronica. In tal caso, occorrerà piuttosto confermare, su richiesta, se un determinato elettore ha ha espresso il proprio voto. In alternativa, il sistema di VE può produrre un elenco contenente i codici anonimi che corrispondono alle carte di legittimazione utilizzate.	F,I
A 7.60	Il decrittaggio e il conteggio dei voti devono poter svolgersi in presenza di organi o parti indipendenti, in grado di attestare il regolare svolgimento della procedura.	I

2.8. Dati confidenziali e dati cui non è possibile accedere

A 8.10	Il sistema di VE assicura che né collaboratori né persone esterne accedano a dati che permettono di stabilire un legame fra l'identità di un elettore e il voto che ha espresso.	F,I
A 8.20	Il sistema di VE assicura che che né collaboratori né persone esterne accedano a dati che permettano di ottenere risultati parziali anticipati prima del momento in cui i voti verranno decrittati.	F,I
A 8.25	Il sistema di VE assicura che i risultati della votazione saranno trattati in modo confidenziale fra il momento in cui i voti verranno decrittati e il momento della loro pubblicazione.	F,I
A 8.30	Il sistema di VE assicura che i dati che permettono di appurare che gli elettori hanno votato per via elettronica saranno trattati in modo confidenziale.	F,I

A 8.40	Il sistema di VE assicura che i dati personali provenienti dal catalogo elettorale saranno trattati in modo confidenziale.	F,I
A 8.50	Il sistema di VE assicura che che i singoli voti saranno trattati in modo confidenziale anche dopo il conteggio.	I
A 8.60	Il sistema di VE assicura che i risultati della votazione saranno trattati in modo confidenziale nel caso in cui solo una minima parte degli elettori di un circondario elettorale abbia il diritto di votare per via elettronica.	F,I
A 8.70	Scaduto il termine di convalida, il gestore del sistema di VE distrugge tutti i dati creati nell'ambito della votazione per via elettronica.	I

3. Requisiti di sicurezza

Non è possibile raggiungere con assoluta certezza gli obiettivi di sicurezza (cfr. art. 2 cpv. 1). In ogni caso si possono identificare rischi per la sicurezza. Sulla base di una valutazione dei rischi metodica (v. cap. 6 n. E 7.40) occorre fornire la prova che eventuali rischi per la sicurezza sono da considerarsi sufficientemente bassi (art. 2 cpv. 1).

È possibile identificare un rischio attraverso le minacce e i punti deboli del sistema di VE: un rischio insorge quando un punto debole di tale sistema viene 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.

La sezione 3.1 elenca alcune minacce generali e le mette in relazione con gli obiettivi di sicurezza. Esse vanno considerate nell'identificare i rischi e, a seconda dei punti deboli identificati del sistema di VE, per quanto necessario rese concrete e integrate.

I requisiti di sicurezza sono riassunti nelle sezioni 3.2 – 3.15.

- da un lato, si riferiscono alle minacce. Per garantire gli obiettivi di sicurezza occorre prevedere, per tutti i punti deboli del sistema di VE esposti a minacce, misure di sicurezza che adempiono i requisiti di sicurezza secondo le pratiche ottimali;
- dall'altro, si riferiscono ai requisiti per strutturare processi elementari (cfr. cap. 2). Ciò serve da ausilio per capire quali punti deboli occorre considerare nell'applicare un requisito di sicurezza. Ulteriori punti deboli si identificano in virtù del sistema di VE concreto e i requisiti di sicurezza sono messi in relazione con essi in maniera analoga.

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

3.1. Minacce

Min3.10	Un software nocivo modifica il voto sulla piattaforma utenti	Obiettivo di sicurezza (OS): correttezza del risultato
Min3.20	Il voto è deviato mediante DNS-spoofing	OS: correttezza del risultato
Min3.30	Man In The Middle (MITM) modifica il voto	OS: correttezza del risultato
Min3.40	MITM invia una scheda corrotta	OS: correttezza del risultato
Min3.50	L'amministratore manipola il software che non memorizza il voto	OS: correttezza del risultato
Min3.60	L'amministratore modifica voti	OS: correttezza del risultato
Min3.70	L'amministratore aggiunge voti	OS: correttezza del risultato
Min3.80	Un'organizzazione criminale si introduce nel sistema e causa danni	OS: correttezza del risultato (qui ai sensi di Min3.50, Min3.60, Min3.70, Min3.90)
Min3.90	L'amministratore copia il materiale di voto e lo utilizza	OS: correttezza del risultato
Min2.10	Un software nocivo sulla piattaforma utenti invia il voto all'organizzazione	OS: protezione del segreto di voto ed esclusione di risultati parziali precoci
Min2.20	Un software nocivo sulla piattaforma utenti invia il voto all'organizzazione	OS: correttezza del risultato, protezione del segreto di voto ed esclusione di risultati parziali precoci
Min2.30	Il voto è deviato mediante DNS-spoofing	OS: correttezza del risultato, protezione del segreto di voto ed esclusione di risultati parziali precoci
Min2.40	L'amministratore utilizza una chiave e decritta voti non anonimi	OS: correttezza del risultato, protezione del segreto di voto ed esclusione di risultati parziali precoci

Min2.50	Nel verificare la correttezza del trattamento / conteggio viene violato il segreto di voto	OS: protezione del segreto di voto ed esclusione di risultati parziali precoci
Min2.60	L'amministratore osserva in anticipo voti decrittati	OS: protezione del segreto di voto ed esclusione di risultati parziali precoci
Min2.70	Un'organizzazione criminale si introduce nel sistema e causa danni	OS: protezione del segreto di voto ed esclusione di risultati parziali precoci (qui ai sensi di Min2.40, Min2.50, Min2.60).
Min1.10	Un software nocivo sul computer dell'avente diritto di voto rende impossibile esercitare tale diritto	OS: disponibilità della funzionalità del VE
Min1.30	Un software nocivo influenza i votanti nella formazione delle loro opinioni	OS: protezione delle informazioni per gli elettori
Min1.40	Un'organizzazione compie un attacco in forma di negazione del servizio	OS: disponibilità della funzionalità del VE
Min1.50	L'amministratore esegue una configurazione errata; non si può arrivare al conteggio	OS: disponibilità della funzionalità del VE
Min1.60	L'amministratore manipola il sito d'informazione ovvero il portale delle votazioni, confondendo gli aventi diritto di voto	OS: protezione delle informazioni per gli elettori
Min1.70	L'amministratore, dopo la decrittazione, ricerca un comportamento di voto prestabilito (possibile soltanto per le elezioni)	OS: esclusione di prove sul comportamento di voto nell'infrastruttura del VE
Min1.80	Un'organizzazione criminale si introduce nel sistema e causa danni	OS: disponibilità della funzionalità del VE, protezione delle informazioni per gli elettori, esclusione di prove sul comportamento di voto nell'infrastruttura del VE (qui ai sensi di Min1.50, Min1.60, Min1.70)
Min1.90	L'amministratore sottrae dati inerenti agli indirizzi dei votanti	OS: protezione delle informazioni personali sugli elettori

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

M1.10	Un sistema di monitoraggio dell'infrastruttura del VE deve scoprire i contrattempi 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 garantisce che si possono portare avanti le attività aventi riferimento con la chiamata alle urne) e si applicano in caso di necessità.	F,I - A2.10,15,20,30,40,50 - A3.20,30,40,45 - A5.20,30,40 - A6.10,20,30 - A7.10, A7.35 - A8.10,20,25,30,40,50,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,50,60,70,80,90
M1.20	Sull'infrastruttura del VE occorre redigere, e se necessario rendere disponibili, verbali dei voti pervenuti. Essi servono da attestati per la presa in considerazione completa, non falsificata ed esclusiva di voti validi. Nel caso di una differenza devono servire a ricercarne le cause.	F,I - A1.35,60 - A5.10,20,40 - A6.10,20,30 - A7.10,35 - 8.10,20,25,30,40,50,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.50,70,80
M1.30	Sull'infrastruttura del VE occorre redigere, e se necessario rendere disponibili, verbali resistenti alle manipolazioni, degli accessi al sistema. Essi servono da attestati per la presa in considerazione completa, non falsificata ed esclusiva di voti validi nonché per il rispetto del segreto di voto e la mancanza di risultati parziali precoci. Nel caso di una differenza, o di dubbi, devono servire a ricercarne le cause.	F,I - A1.35, A1.60 - A2.10,15,20,30,40,50 - A5.10,20,40 - A6.10,20,30 - A7.10,15,35,40,50 - A8,10,20,25,30,40,50,60, 70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,50,60,70,80,90

M1.40	I voti espressi elettronicamente e conteggiati devono essere confrontati con i verbali dei voti pervenuti sull'infrastruttura del VE per rendere plausibile il risultato.	F,I - A1.35,60 - A5.10,20,40 - A6.10,20,30 - A7.10,15,35 - A8.10,20,25,30,40,50,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.50,70,80
M1.50	Occorre garantire che, nel caso di un guasto, i voti e i dati che provano un funzionamento ineccepibile della procedura di conteggio delle legittimazioni vengano memorizzati sull'infrastruttura del VE.	F,I - A1.35,60 - A2.10,15,20,30,40,50 - A4.20 - A5.10,20,40 - A6.10,20,30 - A7.10,15,30,35,40,50 - A8,10,20,25,30,40,50,60, 70 - Min3.80 - Min1.50 - Min1.80
M1.60	Con l'ausilio di dati di autenticazione si devono poter esercitare voti di prova non attribuiti ad alcun avente diritto di voto. Il contenuto di questi voti va verbalizzato sull'infrastruttura del VE. Il conteggio dei voti di prova va confrontato con i verbali riguardanti l'esercizio dei voti di prova. Occorre garantire che i voti di prova siano trattati per quanto possibile alla stregua di voti validi, garantendo nel contempo che non vengano conteggiati come questi ultimi.	F,I - A1.35,60 - A5.10,20,40 - A6.10,20,30 - A7.10,35 - A8.10,20,25,30,40,50,70 - Min3.10,20,30,40,50,60,70,80 - Min2.40,50,60,70 - Min1.10,30,60,80
M1.70	La disponibilità dell'infrastruttura del VE deve essere verificata e verbalizzata a intervalli di tempo scelti.	I - Min 1.40,50,80
M1.80	I metodi statistici, sempreché la base di dati lo consenta, devono poter essere impiegati per rendere plausibile il risultato.	I - A1.35,60 - A5.10,20,40 - A6.10,20,30 - A7.10,15,35 - A8.10,20,25,30,40,50,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.50,70,80
M1.90	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 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,60,70,80,90

3.3. Assegnazione, amministrazione e revoca di diritti di accesso e di intervento

M2.10	Occorre garantire che durante votazione si blocchi ogni modifica fatta successivamente	F,I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20 - A5.10 - A7.35 - Min3.50,60,70,80 - Min1.50,80
M2.20	L'accesso all'infrastruttura del VE e alla funzionalità del VE e l'intervento su di esse devono essere disciplinati e documentati in dettaglio in base a una valutazione dei rischi. Nei settori ad alto rischio occorre applicare il principio del doppio controllo.	I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20 - A5.10 - A7.10,15,35,40,50 - A8.10,20,35,30,40,50,60,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,50, 60,70,80,90
M2.40	Occorre garantire che non si possano modificare senza autorizzazione informazioni sul sito del Voto elettronico e/o pagine informative sul Voto elettronico.	F,I - A3.15,20,30,40,45 - Min1.60,80
M2.55	Durante la votazione nessun intervento estraneo deve poter essere effettuato sull'infrastruttura del VE.	F,I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20,30 - A5.10,20,30,40 - A7.10,15,35,40,50- A8.10,20,35,30,40,50,60,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.50,60,70,80,90

M2.60	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 dell'abuso sistematico da parte di terzi.	F,I - A1.33,35,80 - A2.20,30 - A4.10,20,30 - A6.10,20 - A7.10,15,35,40,50 - A8.10,30,40 - Min3.50,60,70,80,90 - Min2.40,50,60,70

3.4. Uso di misure crittografiche e amministrazione delle chiavi

M3.10	I certificati elettronici devono essere amministrati secondo le pratiche ottimali.	I - A1.60 - A2.40 - A2.50 - A 4.30 - A 7.40 - Min3.20,30,40,80 - Min2.30,70 - Min1.50,80
M3.20	Per assicurare l'integrità di serie di dati, a cui è soggetta la correttezza del risultato,vanno attuate misure crittografiche adeguate.	I,F - A1.35 - A2.10,20,30,40,50 - A4.30 - A5.10 - A6.10,20,30 - A7.10,15,40,50 - Min3.50,60,70,80,90 - Min2.50,70
M3.30	Per assicurare la segretezza di serie di dati, cui sono soggetti il segreto di voto e la mancanza di risultati parziali precoci, vanno attuate misure crittografiche adeguate.	I,F - A1.35 - A2.10,20,30,40,50 - A4.20,30 - A5.10 - A6.10,20,30 - A7.10,15,40,50 - A8.10,20,25,30,50,60,70 - Min2.30,40,50,60,70
M3.40	In nessun momento da quando vengono rilevati a quando vengono conteggiati i voti possono essere archiviati o inoltrati in forma non codificata.	I,F - A1.35,60 - A4.20,30 - A6.10,20,30 - A7.10 - A8.10,20 - Min2.30,40,50,60,70
M3.50	Nello scambio di dati riguardanti il registro elettorale e i risultati devono essere impiegate la codifica e la firma. Quest'ultima e l'integrità dei dati vanno verificate al momento di riceverli.	I,F - A 2.10,15 - A 4.30 - A 7.40 - A 8.25,60
M3.60	I componenti di base crittografici possono essere utilizzati solamente se le lunghezze delle chiavi e gli algoritmi sono conformi agli standard correnti (p. es. FIPS 143-3, NIST, ENCRYPT, ZertES). La firma elettronica deve soddisfare i requisiti di una firma elettronica avanzata ai sensi della legge federale del 19 dicembre 2003 sui servizi di certificazione nel campo della firma elettronica (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
M3.70	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 sostenuta dall'impiego di mezzi crittografici in conformità con le pratiche ottimali.	I,F - A 1.60 - A 2.40 - Min 3.20,30,40 - Min 2.20,30

3.5. Scambio di informazioni fisico ed elettronico più sicuro

M4.10	Il sistema di conteggio dei voti deve essere gestito all'interno della zona di rete dell'infrastruttura del VE installando una sottozona di rete completamente separata da tutte le altre componenti dell'infrastruttura del VE.	I - 7.10,15,30,35,40,50,60 - A8.10,20,25,30,40,50,60 - Min3.60,70,80,90 - Min2.40,50,60,70 - Min1.50,70,80
M4.20	I sistemi sui quali si svolge il Voto elettronico devono essere difesi da eventuali attacchi, a prescindere dalla natura o dall'origine di questi ultimi.	I
M4.30	Tutte le componenti dell'infrastruttura del VE devono essere gestite in una zona di rete separata che va protetta mediante un adeguato controllo dell'instradamento.	I - A8.10,20,25,30,40,50,60 - Min3.60,70,80,90 - Min2.40,50,60,70 - Min1.50,70,80,90

M4.50	I trattamenti connessi al voto espresso elettronicamente devono essere chiaramente separati da tutte le altre applicazioni.	I - A8.10,20,25,30,40,50,60 - Min3.60,70,80,90 - Min2.40,50,60,70 - Min1.50,70,80,90

3.6. Test della funzionalità del VE

M5.10	Un concetto di test deve assicurare il funzionamento conforme alle specifiche della funzionalità del VE. Il concetto deve comprendere copioni di test per ogni tipo di test. Disciplina le responsabilità nell'esecuzione, nella verbalizzazione e nella relazione ai responsabili del VE. Stabilisce a quali condizioni va eseguito un test. Nello sviluppo occorre testare per lo meno ogni funzionalità rilevante sotto il profilo della sicurezza, anche nel caso di adeguamenti di poca importanza. Prima di ogni votazione occorre eseguire un test di carico sul sistema produttivo e testare la disponibilità di ogni funzione.	I,F

3.7. Direttiva in materia di informazione

M6.10	Il responsabile cantonale del VE da parte del Cantone 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 di VE. La direttiva deve essere verificata a intervalli di tempo pianificati e se necessario adeguata.	I

3.8. Organizzazione della sicurezza dell'informazione

M7.10	Tutti i ruoli e tutte le responsabilità per l'esercizio del sistema di VE devono essere definiti con precisione, attribuite e comunicate.	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.50,60,70,80
M7.20	Per le installazioni per il trattamento delle informazioni dell'infrastruttura del VE deve essere aperto un processo di autorizzazione.	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.50,60,70,80
M7.30	I rischi connessi con parti terze vanno identificati e indirizzati per il tramite di pertinenti accordi contrattuali. Il rispetto degli accordi deve essere controllato e verificato adeguatamente durante la loro validità.	I

3.9. Amministrazione dei valori patrimoniali

M8.10	Tutti i valori patrimoniali rilevanti in relazione con il Voto elettronico (organizzazione del VE nel suo insieme, in particolare i suoi processi [organizzativi] e le informazioni, in quanto tali, che vi sono trattate; personale del VE; supporti di dati, installazioni per il trattamento delle informazioni dell'infrastruttura del VE; ambienti dell'infrastruttura del VE) devono essere rilevati e tenuti aggiornati in un inventario. Ogni valore patrimoniale va attribuito a una persona che se ne assume la responsabilità.	I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20 - A5.10 - A7.10,15,35,40,50 - A8.10,20,35,30,40,50,60,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,50, 60,70,80,90
M8.20	Occorre definire l'uso ammesso di valori patrimoniali.	I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20 - A5.10 - A7.10,15,35,40,50 - 8.10,20,35,30,40,50,60,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,50, 60,70,80,90

M8.30	Per informazione si devono emanare e comunicare linee direttrici di classificazione.	I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20 - A5.10 - A7.10,15,35,40,50 - A8.10,20,35,30,40,50,60,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,50, 60,70,80,90
M8.40	Per etichettare e utilizzare le informazioni vanno aperte procedure.	I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20 - A5.10 - A7.10,15,35,40,50 - 8.10,20,35,30,40,50,60,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,50, 60,70,80,90

3.10. Sicurezza del personale

M9.10	Per garantire la sicurezza del personale durante e dopo l'impiego o in caso di cambiamenti di ruolo si devono disporre e comunicare direttive e procedure adeguate.	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.50,60,70,80
M9.20	Per garantire la sicurezza del personale, chi prende le decisioni in seno al personale del VE deve assumere la piena responsabilità.	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.50,60,70,80
M9.30	Per l'intero personale occorre mettere a punto e gestire un programma di consapevolezza, di formazione e di esercitazione della sicurezza dell'informazione conforme ai compiti da svolgere.	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.50,60,70,80

3.11. Sicurezza fisica e inerente all'ambiente

M10.10	I perimetri di sicurezza dei vari ambienti dell'infrastruttura del VE (locali per i vari gruppi di persone del personale del VE, locali dei server ecc.) vanno definiti chiaramente.	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,60,70,80,90
M10.20	Per l'accesso fisico ai vari ambienti dell'infrastruttura del VE si devono definire, disporre e controllare adeguatamente autorizzazioni d'accesso.	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.80
M10.30	Per garantire la sicurezza degli apparecchi dentro e fuori gli ambienti dell'infrastruttura del VE occorre definire direttive e procedure adeguate e controllarne e verificarne il rispetto.	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,60,70,80,90

3.12. Gestione della comunicazione e dell'esercizio

M11.10	Le fasi d'esercizio per le principali attività del sistema vanno descritte in dettaglio.	I - A2.10,15,20,30,40,50 - A3.60 - A4.20,30 - A5.10,20,30 - A7.10,15,30,35,40,50,60 - Min1.50
M11.20	I sistemi produttivi possono essere modificati soltanto in conformità con una procedura di gestione delle modifiche documentata.	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,50,60,70,80,90
M11.30	Gli obblighi e gli ambiti di responsabilità devono essere ripartiti adeguatamente.	I - A2.10,15,20,30,40,50 -- A3.60 - A4.20,30 - A5.10,20,30 - A7.10,15,30,35,40,50,60 - Min1.50

M11.40	Per proteggersi da software nocivi occorre adottare misure adeguate.	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,50,60,70,80,90
M11.50	Si deve allestire e attuare un piano dettagliato per la sicurezza dei dati. Occorre verificare regolarmente la corretta funzione di quest'ultima.	I - A1.35,60 - A2.10,15,20,30,40,50 - A4.20 - A5.10,20,40 - A6.10,20,30 - A7.10,15,30,35,40,50 - A8,10,20,25,30,40,50,60,70 - Min3.80 - Min1.50 - Min1.80
M11.60	Vanno definite e attuate misure adeguate per la protezione della rete e la sicurezza dei servizi di rete.	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,50,60,70,80,90
M11.70	Si devono disciplinare in modo dettagliato le procedure per gestire i supporti rimovibili di dati e per smaltire i supporti di dati.	I - A8.10,20,25,30,40,50,60,70 - Min3.80,90 - Min2.40,50,60,70 - Min1.70,80,90
M11.80	Occorre descrivere in dettaglio, attuare, controllare e verificare le misure di sorveglianza e verbalizzazione dell'utilizzo del sistema, delle attività di amministratori e di verbalizzazione dei guasti.	I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20,30 - A5.10,20,30,40 - A7.10,15,35,40,50 - A8.10,20,35,30,40,50,60,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.50,60,70,80,90

3.13. Requisiti posti alle tipografie

M12.10	Le tipografie devono soddisfare le condizioni stabilite nel catalogo «Esigenze per le stamperie».	

3.14. Acquisizione, sviluppo e manutenzione di sistemi d'informazione

M13.10	Per l'installazione del software su sistemi produttivi vanno descritte in dettaglio e attuate procedure adeguate.	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,50,60,70,80,90
M13.20	Per trattare punti deboli di natura tecnica vanno descritte in dettaglio e attuate procedure adeguate. Occorre prestare particolare attenzione alle parti dell'infrastruttura del VE raggiungibili da Internet.	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,50,60,70,80,90

3.15. Requisiti derivanti dal profilo di sicurezza del BSI

I requisiti derivanti dal profilo di sicurezza del BSI [4] vanno soddisfatti 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, il RT VE ha sempre la precedenza rispetto al profilo di sicurezza.

Le seguenti divergenze dal profilo di sicurezza sono ammesse o obbligatoriamente da rispettare:

M14.10	OR. La preparazione dell'elezione prevede tra l'altro che «elettori» possono esaminare le iscrizioni contenute nella «lista del diritto di voto» ed eventualmente chiedere una rettifica. Ciò non deve essere attuato analogamente per gli aventi diritto di voto nel VE.
M14.20	Non deve avere luogo alcuna registrazione degli aventi diritto di voto. Le iscrizioni nel registro elettorale sono determinanti per conferire il diritto di voto.

M14.30	OR. «Locale del server» prevede che solamente la presidenza del voto può accedervi. Tale requisito può essere attenuato nel senso che soltanto gli aventi diritto designati dal responsabile cantonale possono accedere, sotto sorveglianza, al locale del server.
M14.40	In casi ben motivati si possono adottare misure di sicurezza informatiche alternative (nel senso della terminologia secondo i CC; ingl. *Security Functional Requirements*).

La seguente lista mette in relazione gli obiettivi di sicurezza (nel senso della terminologia secondo i CC; ingl. *Security Objectives*) con le minacce e i requisiti per configurare processi elementari del presente Regolamento.

O.UnauthorisedVoter	F,I - A1.33 - A2.10,15,20,30 - A4.20 - A6.10 - Min3.70,80,90
O.Proof	F,I - A 1.50 - Min1.70
O.IntegrityMessage	F - A1.35,60 - A2.40 - A4.30 - Min3.20,30,40 - Min2.30
O.SecrecyOfVoting	F - A1.35 - A2.40 - A8.10,20 - Min2.30,40,70
O.SecretMessage	F - A1.35 - A2.40 - A8.10,30 - Min3.90
O.AuthenticityServer	F,I - A1.35 - A2.40 - A4.20 - Min3.20,30,40 - Min2.30
O.ArchivingIntegrity	F,I - A2.40 - A7.15,30,35 - Min3.60,70,80
O.ArchivingSecrecyOfVoting	F,I - A7.15 - A8.10,50,70 - Min2.40,50,70 - Min1.70
O.Abort	F - A1.47
O.EndingElection	F - A5.30,40 - Min1.50
O.EndOfElection	F - A5.40 - Min1.50
O.SecrecyOfVotingElectionOfficers	F - A7.15 - A8.10,50,60 - Min2.40,50,70
O.IntegrityElectionOfficers	F - A5.10,20,40 - A7.35 - Min3.50,60,70,80
O.IntermediateResult	F - A7.10 - A8.20,25 - Min2.60,70
O.OverhasteProtection	F - A1.45
O.Correction	F - A1.40
O.AcknowledgeMint	F - A1.60 - Min1.10
O.Failure	F,I - A2.50 - A5.10 - Min1.40,50
O.Audit	F,I - A1.35, A1.60 - A2.10,15,20,30,40,50 - A5.10,20,40 - A6.10,20,30 - A7.10,15,35,40,50 - A8,10,20,25,30,40,50,60,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,50,60,70,80,90
O.OneVoterOneVote	F,I - A1.33,40,47,60,80 - A2.10,15,20,30 - A4.10 - A6.10,20,30 - A7.50 - Min3.70,80 - Min1.10
O.AuthElectionOfficers	F - A2.10,15,20,30,40,50 - A4.20 - A5.10,20,40 -A7.10,15,35,40 - A8.10,20,25,30,40,50,60
O.StartTallying	F - A5.40 - A7.10,15 - Min2.60,70
O.Tallying	F - A2.50 - A5.10 - A7.15 - Min3.50,70,80 - Min1.50
OE.ElectionPreparation	F,I - A2.10,15,20,30,40,50 - A3.10,20 - A4.20,30 - A5.10 - A8.10,20,25,30,40,50,60,70 - Min3.70,80 - Min1.50
OE.Observation	F - A1.35
OE.ElectionOfficers	I - A2.10,15,50 - A3.15 - A5.10,20,40 - A7.10,15,3035,40,60 - A8.10,20,25,30,40,50,60,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.50,60,70,80,90
OE.AuthData	F,I - A2.10,15,20,30 - A4.20,30 - A8.10,40 - Min3.80,90
OE.VoteCastingDevice	F,I - A1.30 - A3.20,30 - Min3.10 - Min2.10
OE.ElectionServer	I - Min3.80 - Min2.70 - Min1.80
OE.Availability	I - Min1.40
OE.ServerRoom	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.80
OE.DataStorage	I - A1.35,60 - A2.10,15,20,30,40,50 - A4.20 - A5.10,20,40 - A6.10,20,30 - A7.10,15,30,35,40,50 - A8,10,20,25,30,40,50,60,70 - Min3.80 - Min1.50 - Min1.80
OE.SystemTime	I - A1.35,60 - A5.10,20,40 - A6.10,20,30 - A7.10,15,35 - A8.10,20,25,30,40,50,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.50,70,80

OE.AuditTrailProtection	I - A1.35, A1.60 - A2.10,15,20,30,40,50 - A5.10,20,40 - A6.10,20,30 - A7.10,15,35,40,50 - A8,10,20,25,30,40,50,60,70 - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.40,50,60,70,80,90
OE.AuthenticityServer	F - A3.20,30,40 - A4.20 - Min 3.20,30,40 - Min 2.30
OE.ArchivingIntegrity	F,I - A2.40 - A7.15,30,35 - Min3.60,70,80
OE.ArchivingSecrecyOfVoting	F,I - A7.15 - A8.10,50,70 - Min2.40,50,70 - Min1.70
OE.ProtectedCommunication	I - Min3.50,60,70,80,90 - Min2.40,50,60,70 - Min1.70,80,90
OE.Buffer	F - A3.45

4. Verificabilità

Gli articoli 3 e 4 stabiliscono le disposizioni concernenti la verificabilità. Il presente allegato riproduce le condizioni in maniera formale, per illustrare i criteri per entrambe le forme della verificabilità.

A tale scopo, alla sezione 4.1 si descrive un modello astratto ridotto per descrivere una chiamata alle urne. Sulla base di quel modello, la sezione 4.2 contiene spiegazioni e ulteriori disposizioni riguardanti l'articolo 3. La sezione 4.3 mostra il modello astratto completo. La sezione 4.4 contiene spiegazioni e ulteriori disposizioni riguardanti l'articolo 4.

4.1. Modello astratto ridotto riguardante l'articolo 3

Nell'astrazione utilizzata, una chiamata alle urne è definita attraverso un verbale crittografico, consistente nello scambio di messaggi tra i seguenti partecipanti al sistema:

Aventi diritto di voto / Votanti	Prima della chiamata alle urne, gli aventi diritto di voto ricevono dal sistema di VE 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 utenti.
Piattaforma utenti	Genera il messaggio di autenticazione e lo invia assieme al voto crittato al sistema di VE lato server. A tale scopo, utilizza parametri pubblici ottenuti prima dal sistema di VE. Se necessario, mostra ai votanti messaggi dal sistema di VE 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 utenti.
Sistema di VE (qui sempre lato server)	Genera e invia agli aventi diritto di voto prima che si rechino alle urne (eventualmente per il tramite della tipografia) i loro dati di autenticazione *client* e alla piattaforma utenti parametri pubblici affinché questa possa generare il messaggio di autenticazione e il voto crittografato. Giudica, secondo le norme note, la validità di voti, li decritta nel rispetto del segreto di voto e calcola il risultato della votazione.
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 verificabilità). Riceve i relativi dati dal sistema di VE e li inoltra agli aventi diritto di voto.

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

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

I partecipanti al sistema e i canali di comunicazione sono affidabili oppure inaffidabili. I partecipanti al sistema affidabili custodiscono sotto chiave, senza eccezioni, i dati segreti ed eseguono esclusivamente le operazioni prescritte dal verbale. I canali affidabili assicurano che i messaggi trasmessi rimangano segreti. Inoltre, chi riceve il messaggio può fare affidamento sul fatto che chi lo invia corrisponde a quel partecipante al sistema prescritto dalla definizione del canale.

L'astrazione utilizzata formalizza inoltre un aggressore, che può corrompere e porre sotto il proprio controllo tutti i partecipanti al sistema e i canali di comunicazione inaffidabili. I partecipanti al sistema corrotti comunicano all'aggressore tutti i dati segreti e operano completamente secondo le sue istruzioni. Esso può altresì leggere o intercettare messaggi scambiati su canali inaffidabili e immettere a sua volta messaggi a suo piacimento.

Ipotesi di affidabilità nel modello astratto (verificabilità individuale del verbale): per la verificabilità individuale in questo modello si suppone che ausili tecnici affidabili, il sistema di VE e la tipografia siano affidabili. La piattaforma utenti e una quota significativa degli aventi diritto di voto si suppone siano inaffidabili. Fra i canali di comunicazione, unicamente piattaforma utenti↔ sistema di VE e sistema di VE ↔ tipografia si suppone siano inaffidabili.

Obiettivo di sicurezza nel modello astratto (verificabilità individuale del verbale): 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
- espressione di un voto

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

Verificabilità individuale del sistema di VE nell'attuazione: Il sistema di VE attua un verbale crittografico che adempie l'obiettivo di sicurezza per la verificabilità individuale nel modello astratto. Laddove necessario, si giustifica mediante pertinenti misure di sicurezza il fatto di ipotizzare l'affidabilità dei partecipanti al sistema e dei canali di comunicazione.

La sezione 4.2 mette in relazione le disposizioni dell'articolo 3 con l'obiettivo di sicurezza nel modello astratto e le esegue laddove necessario. Inoltre, essa contiene requisiti di sicurezza riguardanti i partecipanti al sistema e i canali di comunicazione che nel modello astratto si suppone siano affidabili.

4.2. Disposizioni supplementari inerenti alla verificabilità individuale

D2.05	(ad art. 3 cpv. 1) La prova 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 quale voto espresso conformemente al sistema.) Qualora, prima della espressione del voto definitiva (e dunque prima di ricevere l'ultimo messaggio), il votante decida di interrompere il processo, deve potere continuare a disporre dell'espressione del voto convenzionale.
D2.06	(ad art. 3 cpv. 2) L'obiettivo consiste nell'impedire che partecipanti al sistema inaffidabili possano esprimere un voto di soppiatto. La disposizione va interpretata in tal senso e il verbale esaminato di conseguenza.
D2.07	(ad art. 3 cpv. 4) La prova è valida se serve ai votanti per poter riconoscere manipolazioni del loro voto nel senso dell'obiettivo di sicurezza e considerate le ipotesi di affidabilità date. In questo modo l'aggressore non può ingannare i votanti confezionando una prova, con l'aiuto dei partecipanti al sistema inaffidabili, che lasci credere loro che il loro voto è stato registrato come voto valido nel senso del loro rilevamento. La possibilità di successo dell'aggressore di poter allestire una simile prova indovinando correttamente (analogamente per la prova che conferma che non è stato espresso alcun voto) può essere al massimo dello 0,1%.
D2.08	(ad art. 3 cpv. 4) Per aventi diritto di voto disabili si possono prevedere facilitazioni per verificare le prove. Esclusivamente riguardo a questo caso è possibile scostarsi dall'obiettivo di sicurezza: più precisamente, la validità delle prove in questo caso può dipendere dall'affidabilità della piattaforma utenti. Ciò consente ad esempio lo scanning del riferimento di verifica prima di esprimere il voto. Le facilitazioni devono essere dirette esclusivamente a un piccolo gruppo di aventi diritto di voto che senza di esse non sarebbero in grado di interpretare la prova nella sua piena validità. Gli aventi diritto di voto per i quali ciò non vale vanno, di massima, incitati a verificare le prove in conformità con la procedura prevista.
D2.10	(ad art. 3 cpv. 4) Qualora i votanti utilizzino un ausilio tecnico per verificare, 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.
D2.20	(ad art. 3 cpv. 3 e 4) Oltre al catalogo «Esigenze per le stamperie», vige la seguente disposizione: tutti i macchinari che in qualsivoglia forma partecipano al trattamento di dati del 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 partecipanti sono collegati attraverso cavi fisici in modo tale che, fino alla distruzione dei dati confidenziali, nessun altro macchinario può accedervi in maniera evidente.

D2.30	(ad art. 3 cpv. 3 e 4) Per il sistema di VE lato server non vigono disposizioni supplementari. Nell'attuare i requisiti fondamentali e i requisiti di sicurezza (cfr. art. 5 e 6) occorre tuttavia considerare che la confidenzialità dei dati connessi con il riferimento di verifica è decisiva per la correttezza del risultato, il segreto di voto e l'esclusione di risultati precoci.
D2.40	(ad art. 3 cpv. 3 e 4) L'affidabilità del canale tra tipografia e aventi diritto di voto è giustificata soltanto mediante richiesta, attraverso la notifica fisica, nello specifico per il tramite della Posta svizzera, oppure attraverso la consegna fisica.

4.3. Modello astratto completo riguardante l'articolo 4

Il modello astratto completo concepisce il sistema di VE come inaffidabile. Contempla invece esaminatori che valutano la corretta determinazione dei risultati sulla base di un ausilio affidabile e sulla base di «componenti di controllo» indipendenti.
In questo modo identifica i seguenti partecipanti al sistema supplementari:

Componente di controllo	Interagisce con il sistema di VE e le rimanenti componenti di controllo cosi che esso alla fine della votazione possa approntare una prova valida che confermi la corretta determinazione dei risultati.
Esaminatori	Dopo il conteggio ricevono dal sistema di VE una prova che conferma la corretta determinazione dei risultati.
Ausilio tecnico degli esaminatori	Gli esaminatori possono utilizzare un ausilio tecnico per valutare la prova.

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

- componente di controllo ↔ sistema di VE;
- sistema di VE ↔ ausilio tecnico degli esaminatori;
- ausilio tecnico degli esaminatori ↔ esaminatori;
- canali bidirezionali per la comunicazione tra le componenti di controllo.

Ipotesi di affidabilità nel modello astratto (verificabilità individuale del verbale): si impiegano varie componenti di controllo che vengono riassunte in uno o pochi gruppi. Come per il sistema di VE, si deve ipotizzare che una singola componente di controllo sia inaffidabile. Può tuttavia valere l'ipotesi che almeno una componente di controllo per gruppo è 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 suoi gruppi. La validità della prova che un esaminatore riceve in virtù dell'articolo 4 può dipendere solamente dall'affidabilità della parte affidabile del sistema e del suo ausilio tecnico. Si ipotizza poi che almeno un esaminatore affidabile verifichi la prova con l'aiuto di un ausilio tecnico affidabile. Eventuali ulteriori esaminatori e i loro ausili tecnici sono considerati inaffidabili. Tra i canali di comunicazione supplementari si può ipotizzare che sia affidabile unicamente quello tra gli esaminatori e i loro ausili tecnici. Il sistema di VE è da ritenere inaffidabile.

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

- considerate le ipotesi di affidabilità riguardanti la verificabilità completa del verbale date, l'aggressore non può raggiungere i seguenti obiettivi senza che un votante o un esaminatore affidabile abbia la possibilità di riconoscere con grande probabilità un avvenuto attacco:
  - modifica del voto prima della registrazione mediante la parte affidabile del sistema;
  - sottrazione del voto prima della registrazione mediante la parte affidabile del sistema;
  - espressione di un voto;
  - modifica di un voto espresso conformemente al sistema, la cui espressione è stata registrata mediante la parte affidabile del sistema;
  - sottrazione di un voto espresso conformemente al sistema, la cui espressione è stata registrata mediante la parte affidabile del sistema;
  - inserimento di un voto espresso non conformemente al sistema;
- considerate le ipotesi di affidabilità riguardanti la completa verificabilità del verbale date, l'aggressore non può né infrangere il segreto di voto né rilevare risultati precoci parziali senza corrompere a tale scopo gli aventi diritto di voto o la loro piattaforma utenti.

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

Verificabilità completa del sistema di VE nell'attuazione: vigono le medesime condizioni come per la verificabilità individuale.

La sezione D.4 mette in relazione le disposizioni dell'articolo 4 con l'obiettivo di sicurezza nel modello astratto e le esegue laddove necessario. Inoltre, essa contiene requisiti di sicurezza riguardanti i partecipanti al sistema e i canali di comunicazione che nel modello astratto si ipotizza siano affidabili.

4.4. Disposizioni supplementari inerenti alla verificabilità completa

D4.10	(ad art. 4 cpv. 1) L'impiego di esaminatori serve alla trasparenza. Gli aventi diritto di voto devono potere partire dal presupposto che, in caso di dubbio, gli esaminatori li renderebbero attenti a irregolarità. Si lascia tuttavia consapevolmente aperto da quali cerchie vanno incaricate persone di svolgere il ruolo di esaminatori.
D4.20	(ad art. 4 cpv. 2a) In virtù delle informazioni nella parte affidabile del sistema (tra le quali può trovarsi lo stesso voto crittografato), esaminatori possono accertare se un voto è stato considerato in forma immutata quale immissione per il rilevamento dei risultati. 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 di pubblicare i voti crittati su un «albo» elettronico (ingl. *public board*). Un albo viene realizzato includendo varie componenti affidabili, così che le immissioni vengono cancellate o modificate di soppiatto soltanto se varie di queste componenti sono corrotte. Con l'aiuto di una piattaforma utenti 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 prova della corretta determinazione dei risultati, confezionata nell'ambito della verificabilità universale. I votanti potrebbero così, nello spirito della massima trasparenza possibile, assumere il ruolo degli «esaminatori». Varie considerazioni sui rischi, non da ultime connesse con l'ipotesi, orientata alla prassi, che le piattaforme utenti debbano essere considerate inaffidabili, possono far propendere per una pubblicazione non illimitata dei dati rilevanti per la verificabilità dalla parte affidabile del sistema. È perciò ammesso mettere a disposizione i dati a una cerchia limitata di esaminatori. Nella terminologia della letteratura tecnica, il requisito può perciò essere inteso in questa maniera: *i votanti ricevono dalle componenti competenti per l'albo una prova 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 utenti inaffidabile o dal sistema di VE. Al più tardi dopo la determinazione dei risultati (ma prima della pubblicazione), gli esaminatori ottengono l'accesso all'albo e constatano che il risultato considera ogni voto sull'albo in conformità con le norme vigenti.*
D4.30	(ad art. 4 cpv. 2b) L'obiettivo consiste nell'impedire che partecipanti al sistema inaffidabili possano esprimere un voto di soppiatto. La disposizione va interpretata in questo senso e il verbale esaminato di conseguenza.
D4.40	(ad art. 4 cpv. 2c) La confidenzialità dei dati inerenti a un eventuale riferimento di verifica può così dipendere, anche in seno all'infrastruttura del VE, solamente dalla parte affidabile del sistema.
D4.50	(ad art. 4 cpv. 3a) L'indipendenza e l'isolamento dell'ausilio tecnico garantiscono che la valutazione della prova non può essere influenzata dal sistema di VE. Si lascia tuttavia consapevolmente aperto se gli ausili tecnici e i corrispondenti programmi debbano essere messi a disposizione dal sistema di VE o dagli esaminatori. Gli esaminatori devono tuttavia poter constatare facilmente che l'ausilio funziona correttamente. Ciò si può ad esempio conseguire se gli esaminatori possono scrivere i programmi o per lo meno analizzarli in anticipo. 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 per verificare devono essere facili da scrivere.
D4.60	(ad art. 4 cpv. 3b) Un voto è valido soltanto se i dati di autenticazione *client* utilizzati a tale scopo corrispondono a dati di autenticazione server definiti nella fase di preparazione e «attribuiti» a un avente diritto di voto prima che si recasse alle urne. La prova deve perciò contenere la conferma che non sono stati generati dati per esprimere voti non validi. A tale scopo, durante la preparazione della votazione, alle componenti di controllo o agli esaminatori devono essere stati consegnati dati pertinenti quale termine di paragone. Gli esaminatori 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 valido. In virtù del relativo punto nell'obiettivo di sicurezza del modello astratto o dell'articolo 4 capoverso 2b, gli aventi diritto di voto possono tuttavia constatarlo.
D4.70	(ad art. 4 cpv. 4) La prova è valida se serve ai votanti o agli esaminatori per potere riconoscere le manipolazioni dei voti nel senso dell'obiettivo di sicurezza e considerate le ipotesi di affidabilità date. In tal modo l'aggressore non può ingannare i partecipanti al sistema che verificano, allestendo con l'aiuto dei partecipanti al sistema inaffidabili una prova per giustificare un risultato manipolato, ovvero influenzandone l'allestimento. Nell'ambito della verificabilità universale vigono le seguenti disposizioni: – gli esaminatori devono in ogni caso potere riconoscere la sottrazione senza sostituzione di un voto valido la cui espressione è stata registrata mediante la parte affidabile del sistema; – gli esaminatori devono in ogni caso potere riconoscere l'inserimento di un voto non valido 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 contemporaneo inserimento), così che non riflettano più il senso della prova generata nell'ambito della verifica individuale, può essere al massimo dell'1 per cento. Se la probabilità è trascurabile, non in senso crittografico, l'incertezza deve poter essere ridotta a sufficienza conteggiando più volte utilizzando nuovi valori casuali.
D4.80	(ad art. 4 cpv. 4) Se l'applicazione utilizzata sulla piattaforma utenti per crittare il voto è messa a disposizione dal sistema di VE, allora è da attribuire anche al sistema di VE lato server. Si vuole impedire che, mediante una manipolazione lato server dell'applicazione, il segreto di voto di votanti affidabili venga violato senza corrompere la loro piattaforma utenti. 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 può ad esempio essere conseguito impiegando la tecnologia che utilizza browser e che consente di riconoscere il codice fonte dell'applicazione utenti. I votanti possono così sincerarsi che la chiave pubblica utilizzata corrisponde a quella della votazione e che l'applicazione esegue esclusivamente le operazioni previste. In alternativa, il codice fonte potrebbe essere firmato mediante un gruppo di componenti di controllo.
D4.90	(ad art. 4 cpv. 4) Nel senso dell'obiettivo di sicurezza si deve impedire che il sistema di VE lato server possa, in collaborazione con un avente diritto di voto inaffidabile, conoscere il contenuto di un voto espresso. A tale scopo occorre assicurare che neanche dopo un adeguamento questi possa esprimere come proprio un voto crittato espresso con l'obiettivo di conoscere il contenuto del voto mediante la prova che riceve nell'ambito della verificabilità individuale.
D4.A0	(ad art. 4 cpv. 4) In conseguenza del requisito riguardante la garanzia del segreto di voto e la mancanza di risultati parziali precoci, le chiavi private per decrittare voti non devono essere a disposizione di alcun partecipante al sistema, per lo meno durante gli orari di apertura del canale di voto elettronico. È tuttavia ammesso che in caso di partecipazione di tutti i componenti di controllo di un gruppo possa essere presa in considerazione. È anche ammesso prevedere un gruppo di componenti di controllo in modo che venga attuato 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 il segreto di voto, dopo la decrittazione la chiave privata può esserci solamente se i voti vengono espressi anonimamente e, considerate le ipotesi di affidabilità date, nessuna crittazione di un voto può essere messa in relazione con l'identità di un votante. Non è poi ammesso, in conseguenza del requisito riguardante la mancanza di risultati parziali precoci che, durante gli orari di apertura del canale di votazione elettronico, in un qualsiasi momento vi siano voti in forma decrittata al di fuori della piattaforma utenti.
D4.B0	(ad art. 4 cpv. 5) L'affidabilità di un gruppo di componenti di controllo è decisiva. Il principio per cui, ipotizzando almeno una componente di controllo affidabile, un gruppo non può conteggiare erroneamente di soppiatto, ovvero non può rivelare elementi segreti atti a infrangere il segreto di voto o a rilevare i risultati parziali precoci, corrisponde alle proposte note dalla letteratura tecnica. Nell'astrazione, le componenti di controllo in inglese spesso vengono chiamate «trustee». Nell'astrazione, queste ultime vengono rappresentate quali istanze in grado di eseguire calcoli complessi e di tenere segreti elementi privati. I calcoli possono contenere la mescolanza e la ricrittazione corrette 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 macchinari. Se tengono sotto chiave gli elementi segreti, ovvero se non li utilizzano per inviare messaggi che possono essere impiegati abusivamente viene fatto dipendere

	esclusivamente dalla loro volontà di non voler collaborare con all'aggressore. Pur se in pratica si deve differenziare tra il macchinario e la persona che lo configura e sorveglia, la descrizione del verbale crittografico può tuttavia rappresentare le componenti di controllo quali trustee autonomi.
D4.C0	(ad art. 4 cpv. 5) Il software di componenti di controllo deve essere semplice da analizzare e limitarsi per quanto possibile a funzioni crittografiche elementari.
D4.D0	(ad art. 4 cpv. 5) Le componenti di controllo vanno realizzate, aggiornate, configurate e assicurate in un processo osservabile.
D4.E0	(ad art. 4 cpv. 5) 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 che un accesso non autorizzato andato a buon fine per quanto possibile non procuri alcun vantaggio nel tentativo di accedere di soppiatto a un'ulteriore componente di controllo (implementazione di «trustee»; v. n. D4.B0). 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; – devono 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.
D4.F0	(ad art. 4 cpv. 5) Le componenti di controllo devono eseguire esclusivamente le operaziomi previste. Devono essere focalizzate a riconoscere accessi non autorizzati e ad allarmare le persone responsabili. Queste ultime devono prevedere misure di sorveglianza esterne quali la sorveglianza e la verbalizzazione resistente alle manipolazioni del traffico di rete o la sorveglianza fisica con telecamere che si trovano sotto il loro controllo. Le persone responsabili devono essere considerate particolarmente affidabili.
D4.I0	(ad art. 4 cpv. 5) Devono essere impiegate almeno quattro componenti di controllo per gruppo con differenti sistemi operativi. Qualora le componenti di controllo siano apparecchi (hardware modulo di sicurezza, HMS), un gruppo può essere costituito da due componenti di controllo di fabbricanti differenti. Entrambi gli HMS possono utilizzare il medesimo sistema operativo.
D4.J0	(ad art. 4 cpv. 5) Un HMS 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 può riconoscere se è abusivo. Il certificato deve per lo meno corrispondere a un livello 3 in analogia con una profondità d'esame di EAL4 secondo Common Criteria o FIPS 140-2. È ammesso aggiungere a un HMS un software che si svolge 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 d'esame (per sistemi di Voto elettronico verificabili individualmente e completamente)

Ognuna delle sezioni da 5.1 a 5.6 corrisponde a un esame esterno del sistema di VE. Qualora l'esame dia esito positivo, le organizzazioni competenti rilasciano un documento all'attenzione del Cantone che conferisce il mandato d'esame. Il Cantone allega il documento alla sua domanda di accesso da parte della CaF. I documenti da presentare sono riassunti al capitolo 6.

5.1. Esame del verbale crittografico

E1.10	Criteri di prova: il verbale deve adempiere l'obiettivo di sicurezza considerate le ipotesi di affidabilità nel modello astratto di cui al numero 4. A tale scopo devono esserci una prova crittografica e una simbolica. Riguardo alle componenti di base crittografiche, le prove possono essere condotte con misure di sicurezza generalmente riconosciute (p. es. random oracle model, decisional Diffie-Hellman assumption, Fiat-Shamir heuristic). Il verbale deve fondarsi per quanto possibile su verbali esistenti e sperimentati.
E1.20	Competenze: le prove devono essere fornite o esaminate da istituzioni altamente specializzate. La scelta di un'organizzazione va previamente approvata dalla CaF. Procedura concreta: 1. il Cantone notifica alla CaF una modifica apportata al verbale. Esso può fare proposte sull'istituzione, se del caso sulla persona, che dovrebbe procedere all'esame; 2. la CaF valuta la proposta; 3. la CaF informa il Cantone sulla propria decisione. Nel caso del sistema di VE verificabile individualmente, a causa delle forti ipotesi di affidabilità si possono impiegare semplici verbali. In questo caso la CaF può prescindere dall'avvalersi di un'organizzazione esterna.
E1.30	Durata di validità di un documento: una verifica completa deve avvenire precedentemente alla prima messa in servizio. Il verbale deve essere nuovamente verificato in occasione di ogni modifica del verbale e in caso di nuove importanti nozioni acquisite dalla ricerca quanto alla sicurezza di elementi crittografici impiegati.

5.2. Esame della funzionalità del VE

E2.10	Criteri di prova: la funzionalità del VE deve adempiere i requisiti indicati nei capitoli 2, 3 e 4 o sostenere adeguatamente gli obiettivi predefiniti. Eventualmente un verbale va attuato in conformità con l'articolo 3 o l'articolo 4. Occorre assicurare che siano attuati quali misure di sicurezza i Security Functional Requirements (SFR) indicati nel Protection Profile (PP) del Bundesamt für Sicherheit in der Informationstechnik (BSI) o mezzi equivalenti. La funzionalità del VE va esaminata secondo i criteri principali dell'EAL2 attenendosi al formalismo dei Common Criteria (CC).
E2.20	Competenze: l'esame è svolto da un'istituzione accreditata dal Servizio di accreditamento svizzero (SAS).
E2.30	Durata di validità di un documento: la funzionalità del VE va nuovamente verificata in occasione di ogni modifica rilevante, ad esempio dopo una modifica apportata al verbale crittografico.

5.3. Esame dell'infrastruttura del VE e dell'esercizio

E3.10	Criteri di prova: il sistema di VE e il suo esercizio devono adempiere i requisiti indicati nei capitoli 2, 3 e 4 o sostenere adeguatamente gli obiettivi predefiniti. La sicurezza dell'informazione del sistema di VE e del suo esercizio deve essere garantita mediante installazione, implementazione, esercizio, sorveglianza, verifica, cura e miglioramento di un sistema di gestione di sicurezza dell'informazione (ISMS) ai sensi dell'ISO/IEC 27001:2005 (Information technology – Security techniques – Information security management systems – Requirements). Il campo di applicazione dell'ISMS deve comprendere tutte quelle unità organizzative dell'esercente responsabili sotto il profilo giuridico, amministrativo e operativo per il sistema di Voto elettronico.

E3.20	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 27001:2005. L'organismo deve altresì attestare che i requisiti descritti nei capitoli 2, 3 e 4 vengono adempiuti se essi non sono già coperti dall'audit ai sensi dell'ISO/IEC 27001:2005. L'organismo di certificazione deve essere accreditato dal Servizio di accreditamento svizzero (SAS) per eseguire questo tipo di audit.
E3.30	Durata di validità di un documento: audit di ripetizione devono essere svolti negli intervalli stabiliti dall'ISO 27001. A ogni impiego deve esserci un certificato valido. Occorre procedere a un audit di ripetizione anche se si decide di rinunciare a una misura di sorveglianza che serve a un impiego sicuro e indipendente di componenti di controllo oppure di adeguarla in modo significativo. Se viene pubblicata una nuova versione dello standard ISO/IEC 27001:2005, al più tardi dopo la scadenza del termine transitorio deve essere provata una certificazione valida dell'ISMS secondo la nuova versione, senza ridurre il campo di applicazione di quest'ultimo.

5.4. Esame delle componenti di controllo

E4.10	Criteri di prova: le componenti di controllo devono adempiere i requisiti sanciti nel capitolo 4 o sostenere adeguatamente gli obiettivi predefiniti. Le funzioni la cui affidabilità è determinante per la validità delle prove previste nell'ambito della verificabilità vanno esaminate accuratamente in base al codice fonte e al verbale crittografico. Occorre assicurare che siano attuati quali misure di sicurezza i Security Functional Requirements (SFR) indicati nel Protection Profile (PP) del Bundesamt für Sicherheit in der Informationstechnik (BSI) o mezzi equivalenti. La funzionalità del VE va esaminata secondo i criteri principali dell'EAL4 attenendosi al formalismo dei Common Criteria (CC). Per le componenti di base, quali i software, che servono all'impiego sicuro e indipendente di componenti di controllo, i sistemi operativi o i server impiegati deve essere dimostrato che corrispondono ai migliori standard.
E4.20	Competenze: l'esame è eseguito da un'istituzione accreditata dal Servizio di accreditamento svizzero (SAS).
E4.30	Durata di validità di un documento: nei seguenti casi vanno riesaminate le componenti di controllo: – a ogni modifica apportata al codice fonte delle funzioni la cui affidabilità è determinante per la validità delle prove 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 prove previste nell'ambito della verificabilità deve in ogni caso avere luogo nell'ambito di un esame. 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 continua a essere dimostrato che le componenti corrispondono ai migliori standard.

5.5. Esame della protezione contro tentativi di introdursi nell'infrastruttura del VE

E5.10	Criteri di prova: aggressori competenti da Internet non devono potersi introdurre nell'infrastruttura del VE 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 del VE sulla base della documentazione del sistema, tra cui essa deve avere almeno documenti inerenti all'architettura, al flusso di dati e alle tecnologie impiegate. L'istituzione esamina per lo meno i punti deboli documentati nell'Open Web Application Security Project (OWASP).
E5.20	Competenze: l'esame è eseguito da un'istituzione accreditata dal Servizio di accreditamento svizzero (SAS).
E5.30	Durata di validità di un documento: dopo tre anni deve avere luogo un nuovo esame.

5.6. Esame di una tipografia

E6.10	Criteri di prova: oltre alle disposizioni figuranti nel catalogo «Esigenze per le stamperie», una tipografia deve adempiere il requisito D.2.20 nell'allegato D.
E6.20	Competenze: l'esame è eseguito da un'istituzione accreditata dal Servizio di accreditamento svizzero (SAS).
E6.30	Durata di validità di un documento: dopo due anni deve avere luogo un nuovo esame. Anche a seguito di una decisione di rinunciare a una misura oppure di adeguarla in modo significativo occorre procedere a una ripetizione dell'esame.

6. Attestati da presentare per il nulla osta

E7.10	Il Cantone che fa domanda presenta gli attestati per le verifiche (cfr. art. 1 cpv. 2 e 3) ricevuti dalle istituzioni competenti. L'attestato riguardante l'esame in conformità con la sezione 5.3 deve essere un certificato valido ai sensi dell'ISO/IEC 27001:2005.
E7.20	Il Cantone può far valere per svariate votazioni la validità di un attestato. In questo caso il Cantone giustifica per quale motivo, riguardo alla votazione attuale, non ha proceduto a una ripetizione del corrispondente esame. A tale scopo indica tutte le modifiche al sistema di VE pianificate o effettuate fino al momento della votazione, mostrando così che si tratta di adeguamenti di poca importanza che non hanno alcun influsso negativo sulla valutazione dei rischi.
E7.30	Il Cantone presenta tutti i verbali dei test risultanti dall'attuazione del concetto di test (n. B5.10). Si impegna a presentare ulteriori verbali se un test viene eseguito appena prima della votazione.
E7.40	Il Cantone presenta la sua attuale valutazione dei rischi e si impegna a segnalare immediatamente le modifiche nella valutazione dei rischi. Tutti i rischi risultanti dall'adempimento degli obiettivi di sicurezza devono essere determinati attraverso una valutazione dei rischi. Devono poi essere valutati anche rischi riguardanti il contesto del Voto elettronico nell'amministrazione e a livello pubblico. La valutazione deve avvenire conformemente a una metodologia che prevede l'osservanza delle 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. Per i rischi risultanti dall'esercizio del sistema di VE, nell'identificazione dei rischi nel caso di sistemi verificabili individualmente e completamente devono essere rispettati integralmente i requisiti metodologici dell' ISO/IEC 27001:2005.