Ordinanza della CaF concernente il voto elettronico (OVE)

del 25 maggio 2022 (Stato 1° luglio 2022)

La Cancelleria federale svizzera (CaF),
visti gli articoli 27*e* capoverso 1bis, 27*g* capoverso 2, 27*i* capoverso 3 e 27*l* capoversi 3 e 4 dell'ordinanza del 24 maggio 1978[1] sui diritti politici (ODP),
ordina:

Art. 1 Oggetto

La presente ordinanza disciplina le condizioni per la concessione del nulla osta per prove con il voto elettronico.

Art. 2 Definizioni

[1] Si intende per:

a. *sistema:* l'insieme del software e delle infrastrutture utilizzati per lo svolgimento di scrutini per via elettronica;

b. *sistema online:* la parte del sistema utilizzata per la verifica del diritto di voto, l'espressione del voto crittato e la conservazione del voto crittato;

c. *parte affidabile del sistema:* parte del sistema che comprende uno o più gruppi di componenti di controllo; l'affidabilità di questa parte del sistema è data dal fatto che possono essere scoperti abusi anche se funziona correttamente soltanto una delle componenti di controllo di un gruppo;

d. *componenti di controllo:* le componenti indipendenti del sistema strutturate in modo differente, gestite da diverse persone e garantite da particolari misure;

e. *gestore del sistema:* l'autorità o l'impresa privata che in occasione di uno scrutinio gestisce su istruzioni del Cantone il sistema online e provvede alla sua manutenzione;

f. *esercizio:* tutti gli atti di rilevanza tecnica, amministrativa o giuridica e le relative attività direttive di un Cantone, di un gestore del sistema o di una tipografia che sono necessari per lo svolgimento di scrutini per via elettronica, inclusa la manutenzione;

RU **2022** 336
[1] RS **161.11**

g. *organi preposti all'esercizio:* le organizzazioni o unità organizzative addette all'esercizio, quali una cancelleria di Stato, un gestore del sistema o una tipografia;

h. *verificatori:* le persone che verificano il corretto svolgimento dello scrutinio su mandato del Cantone;

i. *infrastruttura:* l'hardware, il software di componenti terzi secondo l'articolo 11 capoverso 2 lettera a, gli elementi di rete, i locali, i servizi e gli strumenti di ogni genere presso tutti gli organi preposti all'esercizio necessari all'esercizio sicuro del voto elettronico;

j. *software:* l'intera implementazione a partire dal protocollo crittografico, effettuata dallo sviluppatore del software per il voto elettronico, ai fini della verificabilità completa;

k. *protocollo crittografico:* un protocollo con funzioni di sicurezza crittografiche volte ad adempiere i requisiti di cui al numero 2 dell'allegato; situandosi al livello del modello, non contiene istruzioni dirette per l'implementazione ma funzioni di sicurezza astratte;

l. *piattaforma utente:* un apparecchio multifunzionale programmabile collegato a Internet e utilizzato per esprimere il voto, quali un computer standard, uno smartphone o un tablet;

m. *voto registrato:* il voto della cui espressione definitiva la parte affidabile del sistema ha preso atto;

n. *voto parziale:*
   1. nelle votazioni: il voto espresso in merito a un progetto, un controprogetto o una domanda risolutiva,
   2. nelle elezioni: il voto espresso a favore di una lista o di un candidato;

o. *voto espresso conformemente al sistema*: un voto che adempie le seguenti condizioni*:*
   1. il voto è stato espresso conformemente a uno dei modi previsti per compilare una scheda,
   2. un mittente ha espresso il voto in modo definitivo,
   3. i dati di autenticazione client utilizzati e i messaggi di autenticazione che ne risultano corrispondono ai dati di autenticazione server definiti nella fase di preparazione dello scrutinio e attribuiti a un avente diritto di voto, e
   4. il voto è stato espresso utilizzando dati di autenticazione che non sono già stati utilizzati per un altro voto espresso già registrato dalla parte affidabile del sistema online;

p. *dato di autenticazione client:* l'informazione messa a disposizione individualmente agli aventi diritto di voto, come un PIN, di cui questi hanno bisogno – eventualmente assieme ad altri dati di autenticazione client – per poter esprimere un voto;

q. *dato di autenticazione server:* l'informazione necessaria – eventualmente assieme ad altri dati di autenticazione server – per autenticare il mittente di un voto, per mezzo di messaggi di autenticazione, come avente diritto di voto;

r. *messaggi di autenticazione:* le informazioni che una piattaforma utente trasmette al sistema online dopo l'immissione del dato di autenticazione client affinché il mittente di un voto venga autenticato dal sistema online come avente diritto di voto;

s. *certificato:* documento che conferma che un oggetto controllato è conforme a un quadro di riferimento o a uno standard;

t. *certificato elettronico:* serie di dati che conferma determinate caratteristiche di persone o oggetti e la cui autenticità e integrità possono essere esaminate mediante procedimenti crittografici; il certificato elettronico è utilizzato principalmente per identificare e autenticare il proprietario e per crittografare i messaggi;

u. *atti e operazioni critici:* processi in cui si elaborano dati critici;

v. *dati critici:* dati la cui integrità o confidenzialità è determinante per l'adempimento dei requisiti posti al protocollo crittografico.

2 Per il rimanente si applicano le definizioni del numero 1 dell'allegato.

Art. 3 Condizioni di base per la concessione del nulla osta per il voto elettronico per ogni singolo scrutinio

Il nulla osta per il voto elettronico è concesso per ogni singolo scrutinio; devono essere adempiute le seguenti condizioni:

a. la strutturazione e l'esercizio del sistema garantiscono un voto elettronico verificabile, sicuro e affidabile;

b. il sistema è facile da utilizzare per gli aventi diritto di voto; per quanto possibile sono considerate le esigenze di tutti gli aventi diritto di voto;

c. il sistema e i processi operativi sono configurati e muniti di documentazione in modo tale che i processi tecnici e organizzativi possano essere verificati e compresi nei dettagli;

d. il pubblico ha accesso a informazioni adeguate ai destinatari in merito al funzionamento del sistema e ai processi operativi, e sono previsti incentivi per la partecipazione di persone con conoscenze specialistiche.

Art. 4 Analisi dei rischi

1 Il Cantone effettua un'analisi dei rischi con la quale dimostra, specificando le ragioni, che nel suo ambito di responsabilità i rischi di sicurezza sono sufficientemente bassi. A tal fine tiene conto anche del grado di fiducia nel voto elettronico e della sua accettazione da parte del pubblico.

2 Il Cantone valuta se può analizzare da sé i rischi connessi ai compiti dei suoi fornitori di servizi e se sono necessarie analisi dei rischi separate da parte di questi ultimi. Se del caso, chiede loro di eseguire tali analisi dei rischi separate e di inviargliele.

3 Le analisi dei rischi si riferiscono ai seguenti obiettivi di sicurezza:

a. garantire la correttezza del risultato;

b. tutelare il segreto del voto ed escludere risultati parziali anticipati;

c. assicurare la raggiungibilità e la funzionalità del voto elettronico;

d. proteggere le informazioni personali sugli aventi diritto di voto;

e. proteggere da manipolazioni le informazioni destinate agli aventi diritto di voto;

f. escludere l'utilizzo abusivo di riscontri sul comportamento di voto.

4 Ogni rischio viene identificato e descritto chiaramente, mediante la documentazione relativa al sistema e al suo esercizio, per quanto concerne le seguenti caratteristiche:

a. gli obiettivi di sicurezza;

b. eventuali serie di dati connesse agli obiettivi di sicurezza;

c. le minacce;

d. i punti deboli.

Art. 5 Requisiti posti alla verificabilità completa

1 È garantito che ogni manipolazione che causa una falsificazione del risultato possa essere constatata tutelando il segreto del voto (verificabilità completa). Tale garanzia è ritenuta data se i requisiti posti alla verificabilità individuale e alla verificabilità universale sono adempiuti.

2 Sono posti alla verificabilità individuale i seguenti requisiti:

a. ai votanti è data la possibilità di constatare se il loro voto, così come lo hanno immesso nella piattaforma utente, è stato manipolato sulla piattaforma utente o intercettato sulla via di trasmissione; a tal fine i votanti ricevono una nota di conferma secondo cui la parte affidabile del sistema (art. 8) ha registrato il voto, così come essi lo hanno immesso nella piattaforma utente, quale voto espresso conformemente al sistema; tale nota conferma per ogni voto parziale la corretta registrazione;

b. dopo la chiusura del canale di voto elettronico gli aventi diritto di voto che non hanno votato elettronicamente possono richiedere, nei termini legali di ricorso, una nota di conferma secondo cui la parte affidabile del sistema non ha registrato alcun voto che sia stato espresso utilizzando i dati di autenticazione client dell'avente diritto di voto.

3 Sono posti alla verificabilità universale i seguenti requisiti:

a. ai fini della verifica universale i verificatori ricevono una nota di conferma del corretto accertamento del risultato; la nota conferma che il risultato accertato considera i seguenti voti:
   1. tutti i voti espressi conformemente al sistema e registrati dalla parte affidabile del sistema,
   2. soltanto i voti espressi conformemente al sistema,
   3. tutti i voti parziali secondo la nota di conferma generata nell'ambito della verifica individuale;

b. i verificatori valutano la nota di conferma in un processo osservabile; a questo scopo devono avvalersi di ausili tecnici indipendenti e isolati dal resto del sistema.

Art. 6 Validità delle note di conferma

Per la validità delle note di conferma di cui all'articolo 5 è determinante l'affidabilità:

a. della parte affidabile del sistema, per le note di conferma di cui all'articolo 5 capoversi 2 e 3;

b. della procedura di produzione e stampa del materiale di voto, per le note di conferma di cui all'articolo 5 capoverso 2; e

c. dell'ausilio tecnico impiegato dai verificatori per la verifica, per le note di conferma di cui all'articolo 5 capoverso 3.

Art. 7 Tutela del segreto del voto ed esclusione di risultati parziali anticipati

Per la tutela del segreto del voto e l'esclusione di risultati parziali anticipati all'interno dell'infrastruttura sono determinanti:

a. l'affidabilità della parte affidabile del sistema;

b. l'affidabilità della procedura di produzione e stampa del materiale di voto.

Art. 8 Requisiti posti alla parte affidabile del sistema

1 La parte affidabile del sistema comprende uno o più gruppi di componenti di controllo.

2 Le note di conferma sono valide (art. 6) e il segreto del voto è tutelato (art. 7) anche qualora per ogni gruppo solo una delle componenti di controllo funzioni correttamente.

3 L'affidabilità della parte affidabile del sistema è garantita grazie alla diversa configurazione delle componenti di controllo e all'indipendenza del loro esercizio e della loro sorveglianza.

Art. 9 Misure supplementari per ridurre i rischi

Qualora, nonostante le misure prese, i rischi non risultino sufficientemente bassi, occorre adottare misure supplementari per ridurli. Ciò vale in particolare anche quando tutti i requisiti dell'allegato sono già adempiuti.

Art. 10 Requisiti posti alla verifica

1 Enti indipendenti verificano su incarico della Cancelleria federale:

a. il protocollo crittografico (n. 26.1 dell'allegato);

b. il software del sistema (n. 26.2 dell'allegato);

c. la sicurezza dell'infrastruttura e dell'esercizio (n. 26.3 dell'allegato);

d. la protezione da tentativi di introdursi nell'infrastruttura (n. 26.4 dell'allegato).

2 Il Cantone garantisce che il gestore del sistema disponga di un sistema di gestione di sicurezza dell'informazione (ISMS) e che questo venga verificato da enti indipendenti (n. 26.5 dell'allegato). L'ISMS comprende almeno i processi e l'infrastruttura del gestore del sistema rilevanti per raggiungere gli obiettivi di sicurezza.

3 Il Cantone garantisce che la Cancelleria federale e gli enti indipendenti da essa incaricati dello svolgimento delle verifiche di cui al capoverso 1 abbiano accesso al sistema e ai documenti necessari.

4 Le autorità competenti per le verifiche secondo i capoversi 1 e 2 pubblicano gli attestati e i certificati. Se rilevanti per la comprensibilità, vanno pubblicati anche altri documenti. Non devono necessariamente essere pubblicati documenti o parti di documenti se sussistono motivi per una deroga, fondata in particolare sul diritto in materia di trasparenza o di protezione dei dati.

Art. 11 Pubblicazione del codice sorgente e della documentazione relativa al sistema e al suo esercizio

1 Il Cantone provvede affinché i seguenti documenti siano pubblicati:

a. il codice sorgente del software del sistema, inclusi i file contenenti parametri rilevanti;

b. una prova che i programmi leggibili da una macchina siano stati elaborati a partire dal codice sorgente del software pubblicato;

c. la documentazione del software;

d. la documentazione del processo di sviluppo;

e. guide e documentazioni complementari di cui le persone con conoscenze specialistiche necessitano per poter compilare, far funzionare e analizzare il sistema nella propria infrastruttura a partire dal codice sorgente;

f. le specifiche tecniche delle principali componenti del sistema;

g. la documentazione dei processi per l'esercizio, la manutenzione e la sicurezza del sistema;

h. informazioni e descrizioni relative alle lacune conosciute.

2 Non devono necessariamente essere pubblicati:

a. il codice sorgente di componenti terzi quali sistemi operativi, banche dati, server web e server di applicazioni, sistemi di gestione dei diritti, firewall e router, per quanto tali componenti siano ampiamente diffuse e siano costantemente aggiornate;

b. il codice sorgente di portali di autorità vincolati al sistema;

c. documenti o parti di documenti per i quali sussistono motivi per una deroga all'obbligo di pubblicazione, fondata in particolare sul diritto in materia di trasparenza o di protezione dei dati.

Art. 12 Modalità di pubblicazione

1 I documenti da pubblicare secondo l'articolo 11 devono essere preparati e muniti di documentazione in modo tale che possano essere letti e analizzati nella maniera più semplice possibile.

2 Per consentire una verifica da parte del pubblico, tali documenti devono essere:

a. ottenibili via Internet in modo semplice, gratuito e senza registrazione; e

b. disponibili tempestivamente prima dell'impiego previsto del sistema.

3 Chiunque può esaminare, modificare, compilare ed eseguire il codice sorgente a scopi ideali nonché redigere studi in proposito. Può pubblicare studi e conoscenze sulle lacune. Può in particolare consultarsi con altre persone ai fini della ricerca di lacune e in tale contesto citare le informazioni pubblicate.

4 Il proprietario del codice sorgente può:

a. autorizzare l'utilizzo del codice per altri fini;

b. stabilire condizioni specifiche per la trasmissione di segnalazioni volte a migliorare il sistema; in tale contesto può intimare di segnalare immediatamente le lacune e di rispettare un dato termine prima di pubblicare presunte lacune.

5 Se stabilisce condizioni di utilizzo per il codice sorgente e la documentazione oppure condizioni di cui al capoverso 4 lettera b, il proprietario può perseguire le violazioni delle stesse civilmente o penalmente soltanto se qualcuno utilizza il codice sorgente o parti di esso per scopi commerciali o di produzione. Le condizioni di utilizzo e le condizioni di cui al capoverso 4 indicano questo aspetto.

Art. 13 Coinvolgimento del pubblico

1 Il Cantone designa un organo al quale le persone interessate possano trasmettere segnalazioni volte a migliorare il sistema, tra cui:

a. segnalazioni di lacune nei documenti pubblicati secondo l'articolo 11;

b. segnalazioni sulla base di prove d'intrusione nel sistema online effettuate nel quadro di test pubblici.

2 L'organo di cui al capoverso 1 valuta le segnalazioni e informa i segnalatori circa la propria valutazione ed eventuali misure adottate sulla base delle segnalazioni. Queste informazioni sono pubblicate.

3 Il Cantone provvede affinché le segnalazioni che si riferiscono alla sicurezza e contribuiscono a migliorare il sistema siano remunerate adeguatamente.

Art. 14 Responsabilità e competenze per il corretto svolgimento degli scrutini per via elettronica

1 Il Cantone si assume la responsabilità globale per il corretto svolgimento degli scrutini per via elettronica.

2 Deve eseguire da sé compiti importanti. Può delegare a organizzazioni esterne lo sviluppo del software impiegato, compiti legati all'esercizio e la comunicazione per le questioni legate al funzionamento.

3 Designa un organo a livello cantonale che si assume la responsabilità globale e che esegue in particolare i seguenti compiti:

a. definire una direttiva sovraordinata in materia di sicurezza dell'informazione;

b. definire una direttiva in materia di classificazione ed elaborazione delle informazioni per le risorse informative identificate;

c. definire una direttiva in materia di gestione dei rischi;

d. definire e attuare misure per il rispetto delle direttive di cui alle lettere a–c;

e. incaricare un gestore del sistema e definire i requisiti posti alla sua sorveglianza e verifica;

f. definire scadenze per l'esecuzione di atti e operazioni critici;

g. sorvegliare e verificare i lavori del gestore del sistema;

h. accompagnare e istruire i verificatori;

i. valutare e comunicare la correttezza del risultato dello scrutinio sulla base delle note di conferma di cui all'articolo 5 e di altri indicatori.

4 Gli organi preposti all'esercizio si assumono nei confronti del Cantone la responsabilità per l'approntamento e la gestione degli aspetti tecnici legati agli scrutini per via elettronica.

5 I verificatori competenti secondo il diritto cantonale si assumono la responsabilità per l'esercizio dei loro ausili tecnici.

Art. 15 Documenti relativi alle domande

1 Alle domande di cui all'articolo 27*e* ODP vanno allegati informazioni sugli impieghi previsti del voto elettronico e documenti sull'adempimento dei requisiti legali. Tra questi rientrano in particolare:

a. analisi attuali dei rischi secondo l'articolo 4, incluse le indicazioni necessarie per la comprensibilità;

b. certificati e relativi allegati che sono stati realizzati nel quadro delle verifiche di cui all'articolo 10 capoverso 2 e informazioni concernenti la loro pubblicazione secondo l'articolo 10 capoverso 4;

c. informazioni concernenti la pubblicazione di documenti secondo l'articolo 11 e le segnalazioni da parte del pubblico secondo l'articolo 13;

d. verbali relativi a test svolti dal Cantone e segnalazioni di lacune esistenti nel sistema;

e. la motivazione ed eventuali misure per le deroghe secondo l'articolo 16 capoverso 2.

2 Nel caso dei documenti di cui al capoverso 1 che la Cancelleria federale ha già ricevuto e che sono ancora validi, è possibile limitarsi a un rimando.

Art. 16 Ulteriori disposizioni

1 I requisiti dettagliati di natura tecnica e amministrativa posti al voto elettronico sono disciplinati nell'allegato.

2 In casi eccezionali la Cancelleria federale può esonerare un Cantone dall'adempimento di singoli requisiti, sempre che:

a. i requisiti non adempiuti siano indicati nella domanda;

b. l'eccezione sia motivata in modo comprensibile; e

c. il Cantone descriva eventuali misure alternative e, per quanto riguarda l'analisi dei rischi, indichi i motivi per cui valuta tali rischi come sufficientemente bassi.

Art. 17 Abrogazione di un altro atto normativo

L'ordinanza della CaF del 13 dicembre 2013[2] concernente il voto elettronico è abrogata.

Art. 18 Entrata in vigore

La presente ordinanza entra in vigore il 1° luglio 2022.

2 [RU **2013** 5371; **2018** 2279]

Allegato
(art. 2 cpv. 1 lett. k e 2, 9, 10 cpv. 1 e 2 nonché 16 cpv. 1)

Requisiti tecnici e amministrativi posti al voto elettronico

1. Definizioni

Oltre alle definizioni di cui all'articolo 2, si intende per:

1.1. *tutela del segreto del voto:* situazione in cui nessuna persona o componente dispone dei seguenti dati:

1.1.1 voti espressi o dati che permettono di risalire al contenuto dei voti espressi,

1.1.2 dati che permettono di identificare i votanti (dati sugli aventi diritto di voto), e

1.1.3 dati che permettono di associare i dati sugli aventi diritto di voto ai voti espressi;

1.2 *esclusione di risultati parziali anticipati:* situazione in cui nessuna persona o componente dispone in anticipo dei voti espressi o di dati che permettono di risalire ai voti espressi;

1.3 *riferimento di verifica:* un documento, inviato assieme al materiale di voto, che permette agli aventi diritto di voto di verificare, secondo l'articolo 5 capoverso 2 in combinato disposto con il numero 2.5 dell'allegato, se il loro voto è stato espresso correttamente (p. es. un elenco in cui a ogni possibilità di risposta è associato un codice);

1.4 *aggressore esterno:* una persona o un gruppo di persone che non si occupa dello sviluppo e dell'esercizio del sistema, che dispone di risorse e conoscenze specialistiche medie e da cui parte un'aggressione; le sue motivazioni possono comprendere l'attivismo e il profitto finanziario;

1.5 *aggressore interno:* una persona o un gruppo di persone che partecipa allo sviluppo o all'esercizio del sistema e da cui parte un'aggressione; le sue motivazioni possono comprendere l'attivismo, il profitto finanziario e l'intenzione di danneggiare il proprio datore di lavoro;

1.6 *organizzazione nemica:* un gruppo di persone che dispone di ampie risorse e di conoscenze specialistiche al di sopra della media e da cui parte un'aggressione; può anche essere sostenuta da uno Stato; tra le sue motivazioni possono esservi l'ottenimento di dati per la profilazione e l'intenzione di disturbare uno scrutinio o di influenzarne i risultati;

1.7 *aggressore:* una persona, un gruppo di persone o un'organizzazione di cui ai numeri 1.4–1.6;

1.8 *urna elettronica:* un'area dati in cui i voti espressi possono essere memorizzati fino alla decrittazione e allo spoglio;

1.9 *protocollo del sistema:* protocollo realizzato dagli elementi dell'infrastruttura per sorvegliare l'esercizio del sistema e indagare sugli incidenti.

2. Requisiti posti al protocollo crittografico per la verificabilità completa (art. 5)

2.1 Partecipanti al sistema

Il protocollo crittografico disciplina i compiti dei seguenti partecipanti astratti al sistema:

- avente diritto di voto / votante
- piattaforma utente
- componente di setup
- sistema non affidabile (qualsiasi componente diversa dalle componenti elencate in questo numero; sistema NA)
- componente di stampa
- uno o più gruppi di componenti di controllo
- verificatori
- ausilio tecnico dei verificatori

2.2 Canali di comunicazione

Il protocollo crittografico può prevedere i seguenti canali di comunicazione per lo scambio di messaggi tra i partecipanti al sistema:

- avente diritto di voto / votante ↔ piattaforma utente
- piattaforma utente ↔ sistema NA
- componente di setup ↔ sistema NA
- componente di controllo ↔ sistema NA
- sistema NA → componente di stampa
- sistema NA → ausilio tecnico dei verificatori
- componente di stampa → avente diritto di voto / votante
- componente di setup → ausilio tecnico dei verificatori
- verificatori ↔ ausilio tecnico dei verificatori
- canali bidirezionali per la comunicazione tra le componenti di controllo

2.3 Aggressore

2.3.1 Il protocollo crittografico deve proteggere da un aggressore che tenti di influenzare abusivamente i voti e il risultato, di violare il segreto del voto o di rilevare anticipatamente risultati parziali (n. 2.5–2.8).

2.3.2 Occorre presumere che un aggressore disponga delle seguenti capacità:

- è in grado di controllare tutti i partecipanti non affidabili al sistema (cfr. n. 2.4) in modo tale che condividano con esso tutti i dati segreti e agiscano illimitatamente secondo le sue istruzioni;
- è in grado di leggere e sopprimere tutti i messaggi scambiati mediante canali non affidabili e di inserirvi a sua volta messaggi a piacere.

2.4 Partecipanti al sistema e canali di comunicazione affidabili e non affidabili

2.4.1 I partecipanti al sistema e i canali di comunicazione sono considerati «affidabili» o «non affidabili». Le ipotesi di affidabilità ammesse per i singoli partecipanti al sistema sono disciplinate al numero 2.9.

2.4.2 I partecipanti al sistema e i canali di comunicazione affidabili sono considerati protetti contro gli aggressori. Per il protocollo crittografico si possono assumere segnatamente le seguenti ipotesi:

- I partecipanti al sistema affidabili tengono sotto chiave i dati confidenziali e svolgono esclusivamente le operazioni prescritte dal protocollo crittografico.
- I canali di comunicazione affidabili tengono sotto chiave i messaggi trasmessi e li proteggono da manipolazioni.

2.5 Requisiti posti al protocollo crittografico: verificabilità individuale

Gli aventi diritto di voto ricevono note di conferma secondo l'articolo 5 capoverso 2 in combinato disposto con l'articolo 6 lettere a e b che confermano che un aggressore:

- prima della registrazione come voto espresso conformemente al sistema, non ha modificato o sottratto alcun voto parziale dell'avente diritto di voto;
- non ha espresso abusivamente a nome dell'avente diritto alcun voto successivamente registrato e conteggiato quale voto espresso conformemente al sistema.

2.6 Requisiti posti al protocollo crittografico: verificabilità universale

I verificatori ricevono note di conferma secondo l'articolo 5 capoverso 3 lettera a in combinato disposto con l'articolo 6 lettere a e c che confermano che un aggressore:

- dopo che i voti sono stati registrati quali voti espressi conformemente al sistema, non ha modificato o sottratto alcun voto parziale fino al calcolo del risultato;
- non ha inserito alcun voto o voto parziale non espresso conformemente al sistema che sia stato considerato nel calcolare il risultato.

2.7 Requisiti posti al protocollo crittografico: tutela del segreto del voto ed esclusione di risultati parziali anticipati

2.7.1 Deve essere garantito che un aggressore non possa né violare il segreto del voto né rilevare anticipatamente risultati parziali senza porre inoltre sotto il proprio controllo gli aventi diritto di voto o le loro piattaforme utente.

2.7.2 Non vi è alcun obbligo di impedire aggressioni mediante le quali il numero dei voti conteggiati è limitato in modo tale che tutti i voti parziali per un oggetto in votazione, una lista o un candidato siano dello stesso tenore.

2.7.3 Deve essere garantito che un aggressore non possa porre di nascosto sotto il proprio controllo le piattaforme utente manipolando sul server il software per le piattaforme utente. I votanti devono avere la possibilità di verificare se la loro piattaforma utente ha ricevuto dal server il software corretto con i parametri corretti, in particolare con la chiave pubblica per crittare il voto.

2.8 Requisiti posti al protocollo crittografico: autenticazione efficace

Deve essere garantito che un aggressore non possa esprimere un voto conformemente al sistema senza porre sotto il proprio controllo i corrispondenti aventi diritto di voto.

2.9 Elenco dei partecipanti al sistema affidabili e non affidabili

2.9.1 Per la validità delle note di conferma secondo il numero 2.5

2.9.1.1 I seguenti partecipanti al sistema sono considerati non affidabili:

- piattaforma utente
- sistema NA
- tre delle quattro componenti di controllo per ciascun gruppo, fermo restando che le tre componenti non vanno designate
- una quota significativa di aventi diritto di voto
- verificatori
- ausili tecnici dei verificatori

2.9.1.2 I seguenti partecipanti al sistema possono essere considerati affidabili:

- componente di setup
- componente di stampa
- una delle quattro componenti di controllo per ciascun gruppo, fermo restando che la componente non va designata

2.9.2 Per la validità delle note di conferma secondo il numero 2.6

2.9.2.1 I seguenti partecipanti al sistema sono considerati non affidabili:

- piattaforma utente
- sistema NA
- tre delle quattro componenti di controllo per ciascun gruppo, fermo restando che le tre componenti non vanno designate
- una quota significativa di aventi diritto di voto
- componente di setup
- componente di stampa

2.9.2.2 I seguenti partecipanti al sistema possono essere considerati affidabili:

- una delle quattro componenti di controllo per ciascun gruppo, fermo restando che la componente non va designata

- un verificatore di un gruppo, fermo restando che il verificatore non va designato
- un ausilio tecnico di un verificatore affidabile, fermo restando che l'ausilio tecnico non va designato

2.9.3 Per la tutela del segreto del voto e l'esclusione di risultati parziali anticipati secondo il numero 2.7

2.9.3.1 I seguenti partecipanti al sistema sono considerati non affidabili:

- sistema NA
- tre delle quattro componenti di controllo per ciascun gruppo, fermo restando che le tre componenti non vanno designate
- una quota significativa di aventi diritto di voto
- verificatori
- ausili tecnici dei verificatori

2.9.3.2 I seguenti partecipanti al sistema possono essere considerati affidabili:

- componente di setup
- componente di stampa
- piattaforma utente
- una delle quattro componenti di controllo per ciascun gruppo, fermo restando che la componente non va designata

2.9.3.3 Se un gruppo completo di componenti di controllo viene impiegato presso un gestore privato del sistema, nessuna di tali componenti di controllo è considerata affidabile.

2.9.4 Per l'efficacia dell'autenticazione secondo il numero 2.8

2.9.4.1 I seguenti partecipanti al sistema sono considerati non affidabili:

- sistema NA
- tre delle quattro componenti di controllo per ciascun gruppo, fermo restando che le tre componenti non vanno designate
- una quota significativa di aventi diritto di voto
- verificatori
- ausili tecnici dei verificatori
- piattaforma utente

2.9.4.2 I seguenti partecipanti al sistema possono essere considerati affidabili:

- componente di setup
- componente di stampa
- una delle quattro componenti di controllo per ciascun gruppo, fermo restando che la componente non va designata

2.10 Elenco dei canali di comunicazione affidabili e non affidabili

2.10.1 I seguenti canali di comunicazione sono considerati non affidabili:

- piattaforma utente ↔ sistema NA

- componente di setup ↔ sistema NA
- componente di controllo ↔ sistema NA
- sistema NA → componente di stampa
- sistema NA → ausilio tecnico dei verificatori
- canali bidirezionali per la comunicazione tra le componenti di controllo

2.10.2 I seguenti canali di comunicazione possono essere considerati affidabili:

- avente diritto di voto / votante ↔ piattaforma utente
- ausilio tecnico dei verificatori ↔ verificatori
- componente di setup → ausilio tecnico dei verificatori
- componente di stampa → avente diritto di voto / votante

2.11 Requisiti supplementari posti alla validità delle note di conferma

2.11.1 La probabilità che un aggressore possa falsificare una nota di conferma secondo il numero 2.5 quando modifica un voto parziale, sottrae un voto parziale o esprime un voto a nome d'altri può essere al massimo dello 0,1 per cento.

2.11.2 La probabilità che un aggressore possa falsificare una nota di conferma secondo il numero 2.6 quando fa in modo, modificando e sottraendo voti espressi conformemente al sistema e inserendo voti non espressi conformemente al sistema, che il risultato calcolato diverga dello 0,1 per cento dal risultato corretto può essere al massimo dell'1 per cento per ogni oggetto in votazione, elezione di lista o elezione di candidati.

2.11.3 Se la probabilità che un aggressore possa falsificare una nota di conferma secondo il numero 2.6 non è trascurabile in senso crittografico[3], la probabilità di successo deve poter essere ridotta a piacere mediante uno spoglio ripetuto e facendo in modo che i verificatori ricevano per ogni spoglio una nota di conferma secondo il numero 2.6 supplementare e indipendente.

2.12 Requisiti funzionali posti al processo dell'espressione del voto con ripercussioni sul protocollo crittografico

2.12.1 Con le caratteristiche di autenticazione attribuite a un avente diritto di voto può essere espresso un solo voto.

2.12.2 Il votante immette il proprio voto nella piattaforma utente.

2.12.3 Fino al momento in cui dichiara la volontà di esprimere il proprio voto, il votante può modificarlo e verificarlo mediante una panoramica.

2.12.4 Dopo aver avuto la possibilità di verificare il voto mediante la panoramica, il votante dichiara sulla piattaforma utente di voler esprimere il voto nella forma immessa.

[3] Corrisponde più o meno alla probabilità di decrittare, senza conoscerne la chiave, un valore che è stato crittato con un algoritmo ritenuto sicuro e usando i corrispondenti parametri.

2.12.5 Le note di conferma per la corretta espressione del voto secondo il numero 2.5 devono essere strutturate in almeno due note di conferma parziali e sequenziali. Ogni visualizzazione rappresentata quale nota di conferma parziale deve rappresentare un autentico contributo alla validità della nota di conferma secondo il numero 2.5.

2.12.6 La piattaforma utente visualizza al votante la prima nota di conferma parziale dopo che esso ha dichiarato sulla piattaforma utente di voler esprimere il voto.

2.12.7 La piattaforma utente visualizza al votante la successiva nota di conferma parziale soltanto dopo che esso ha confermato, mediante una dichiarazione sulla piattaforma utente, la correttezza della nota di conferma parziale precedente.

2.12.8 Confermando la correttezza della penultima nota di conferma parziale, il votante dichiara la volontà di esprimere il voto definitivamente.

2.12.9 Il gruppo di componenti di controllo registra il voto come espresso conformemente al sistema se ha ricevuto la conferma che il votante vuole esprimere il voto definitivamente.

2.12.10 Se il votante ha verificato l'ultima nota di conferma parziale con esito positivo, l'espressione del voto è conclusa. L'ultima nota di conferma parziale deve poter essere verificata in modo particolarmente facile limitando possibilmente la verifica alla corretta visualizzazione di un unico codice o a un'altra visualizzazione semplice.

2.12.11 A partire dal momento in cui si importano dati sul voto, una componente di setup o una componente di stampa non è più considerata affidabile.

2.13 Requisiti posti alla definizione e alla descrizione del protocollo crittografico

2.13.1 Se possibile si usano elementi crittografici diffusi a livello mondiale e verificati approfonditamente da persone competenti. A titolo di orientamento si può ricorrere a standard, progetti di riferimento e pubblicazioni scientifiche. Le deroghe e i casi dubbi vanno trattati separatamente nel quadro dell'analisi dei rischi di cui all'articolo 4.

2.13.2 Le istruzioni operative devono essere sufficientemente specificate: le singole istruzioni operative devono limitare le possibilità attuative in misura tale che ogni attuazione consentita dall'istruzione sia pure conforme all'adempimento dei requisiti posti al protocollo crittografico.

2.13.3 I canali affidabili possono essere utilizzati per la distribuzione di certificati elettronici tra i partecipanti al sistema. Si applica il numero 3.8.

2.14 Note di conformità sull'adempimento dei requisiti posti al protocollo crittografico

2.14.1 Una nota di conformità simbolica e una nota di conformità crittografica devono attestare che il protocollo crittografico adempie i requisiti di cui ai numeri 2.1–2.12.

2.14.2 Le note di conformità devono riferirsi direttamente alla descrizione del protocollo che serve da base per lo sviluppo del sistema.

2.14.3 Riguardo alle componenti di base crittografiche, le note di conformità possono essere designate quali ipotesi e costruzioni di sicurezza generalmente riconosciute (p. es. «random oracle model», «decisional Diffie-Hellman assumption», «Fiat-Shamir heuristic»).

3. Requisiti posti alle componenti affidabili secondo il numero 2 e al loro esercizio

3.1 L'esercizio della componente di setup e di almeno una componente di controllo del gruppo che comprende una parte della chiave per la decrittazione dei voti rientra nella competenza diretta del Cantone e deve svolgersi nella sua infrastruttura. Lo scorporo a un gestore privato del sistema non è ammesso.

3.2 Per la scelta di valori aleatori segnatamente per le componenti di setup e le componenti di controllo deve essere garantito l'impiego di una sufficiente entropia.

3.3 I verificatori devono verificare almeno una volta le note di conferma secondo il numero 2.6 e utilizzare a tale scopo un ausilio tecnico secondo il numero 2.

3.4 I requisiti d'esercizio posti alle componenti di setup secondo il numero 3 valgono anche per gli ausili tecnici dei verificatori. Nei limiti della loro responsabilità, stabilita dal diritto cantonale, i verificatori possono prevedere deroghe.

3.5 Eccezion fatta per le componenti menzionate ai numeri 3.1 e 3.3, il Cantone può delegare l'esercizio di qualsiasi parte del sistema, comprese le componenti di controllo e la componente di stampa, a fornitori di servizi privati. Un gestore privato della componente di stampa può svolgere esclusivamente compiti d'esercizio che costituiscono una premessa per la preparazione, l'imballaggio e l'invio.

3.6 Le componenti affidabili (componenti di setup, componenti di stampa, ausili tecnici dei verificatori e componenti di controllo) vanno realizzate, aggiornate, configurate e assicurate in un processo osservabile.

3.7 Prima dell'installazione di un software occorre verificare per tutti i programmi, mediante una base ufficiale affidabile, se i file corrispondono alla versione corretta e autentica.

3.8 Nell'installazione di certificati elettronici di altri partecipanti al sistema l'autenticità deve essere garantita. A tal proposito occorre predisporre un processo manuale secondo cui le persone portano i certificati elettronici da una macchina all'altra mediante un supporto di dati fisico secondo il numero 3.13.

3.9 Il momento dell'aggiornamento di tutto il software delle componenti affidabili va scelto in modo tale che i vantaggi attesi dall'aggiornamento prevalgano sui possibili pericoli.

3.10 Le componenti di setup, le componenti di stampa e gli ausili tecnici dei verificatori che, in qualsivoglia forma, partecipano al trattamento di dati critici devono essere sorvegliati fisicamente, secondo il principio del doppio controllo, durante l'intero periodo di calcolo e fino alla cancellazione di eventuali dati critici o alla conservazione sicura. Possono essere collegati tra di loro tutt'al più mediante cavi fisici, affinché, per quanto possibile, sia evidente che nessun altro macchinario possa accedervi fino alla distruzione dei dati confidenziali.

3.11 Per l'installazione o l'aggiornamento del software le componenti affidabili non devono essere collegate a Internet.

3.12 In linea di principio i dati critici devono essere distrutti dopo il loro utilizzo. In alternativa, se vi sono motivi validi, è ammessa una conservazione sicura del supporto di dati.

3.13 I supporti di dati per lo scambio o la conservazione dei dati, ad esempio le chiavette USB, devono essere rimossi dopo il caricamento dei dati nella componente affidabile e possono essere riutilizzati prima della distruzione dei dati soltanto se prima del caricamento dei dati non si trovavano dati critici sulla componente affidabile.

Prima del loro utilizzo, i supporti di dati per lo scambio dei dati devono essere riformattati con l'aiuto di una componente gestita conformemente ai requisiti posti alle componenti affidabili; eventuali dati presenti sul supporto devono essere distrutti.

3.14 Non deve essere possibile alcun accesso logico o fisico a componenti affidabili o a supporti di dati contenenti dati critici senza che un'altra persona se ne accorga; ad esempio, un'altra persona deve partecipare alla concessione dell'accesso (applicazione rigorosa del principio del doppio controllo).

3.15 Un accesso non autorizzato ma andato a buon fine a una componente di controllo non deve possibilmente procurare alcun vantaggio nel tentativo di accedere di nascosto a un'altra componente di controllo. Oltre agli altri requisiti di cui al numero 3, vanno adempiuti a tale scopo i seguenti requisiti:

- una persona che ha un accesso fisico o logico a una componente di controllo non deve avere accesso a un'altra componente di controllo;
- l'hardware, i sistemi operativi e i sistemi di sorveglianza delle componenti di controllo devono per quanto possibile differenziarsi;
- le componenti di controllo devono essere collegate a reti locali differenti;
- una componente di controllo deve essere realizzata mediate un apparecchio fisico. Non è ammessa la virtualizzazione mediante più apparecchi fisici.

3.16 Le componenti di controllo devono essere tali da riconoscere gli accessi non autorizzati e 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.

3.17 Le componenti affidabili possono eseguire esclusivamente le operazioni previste.

3.18 Il software dell'ausilio tecnico dei verificatori deve essere acquistato presso uno sviluppatore di sistema diverso da quello che ha sviluppato la maggior parte del software degli altri elementi del sistema. La pubblicazione del software dell'ausilio tecnico al beneficio di una licenza che adempie i criteri applicabili ai programmi Open Source[4] può motivare un'eccezione. Se i verificatori impiegano più ausili tecnici, la presente disposizione si applica ad almeno uno degli ausili tecnici.

3.19 Per tutti i processi legati all'utilizzazione di componenti affidabili deve essere elaborata una documentazione scritta e facilmente comprensibile per le persone interessate.

3.20 Di ogni accesso e utilizzazione di una componente affidabile o di un supporto di dati contenente dati critici deve essere realizzato un protocollo.

4. Procedura di voto

4.1 I votanti dichiarano di aver preso atto delle regole del voto elettronico e della propria responsabilità.

4.2 Prima di esprimere il voto i votanti sono resi attenti sul fatto che, trasmettendo i loro voti elettronici, partecipano allo scrutinio come se esprimessero il voto per corrispondenza o di persona all'urna. I votanti possono esprimere il proprio voto soltanto dopo aver confermato che hanno preso atto di quanto precede.

4.3 Al momento di esprimere il voto i votanti sono invitati a verificare le note di conferma secondo il numero 2.5 mediante il riferimento di autenticazione e di segnalare al Cantone eventuali dubbi sulla loro correttezza.

4.4 Prima dell'espressione definitiva del voto elettronico gli aventi diritto possono ancora esprimere il proprio voto attraverso un canale di voto convenzionale.

4.5 Il sistema client quale si presenta ai votanti non influenza le loro scelte.

[4] Cfr. in merito la definizione nella «Guida pratica: programmi Open Source nell'Amministrazione federale» (disponibile in tedesco), versione 1.0 del 19.12.2019, cap. 1; ottenibile presso: Cancelleria federale svizzera, CH–3003 Berna; www.bk.admin > Trasformazione digitale e governance delle TIC > Architettura della Confederazione > Open Source Software (OSS).

4.6 Le istruzioni fornite agli utenti non inducono a votare in modo precipitoso o senza riflettere.

4.7 Il sistema non offre ai votanti alcuna funzione che permetta di stampare o memorizzare il proprio voto.

4.8 Dopo l'espressione del voto, ai votanti non è visualizzata alcuna informazione sul voto crittato da loro espresso.

4.9 Nel caso degli aventi diritto di voto che non possono esprimere un voto perché terzi lo esprimono utilizzando abusivamente il loro materiale di voto, i Cantoni possono ancora permettere l'espressione del voto dichiarando nullo il voto espresso abusivamente. La tutela del voto secondo il numero 2.7 va tutelata.

4.10 Si possono prevedere agevolazioni per permettere agli aventi diritto di voto disabili di verificare la nota di conferma. Soltanto in un simile caso è possibile derogare ai requisiti di cui al numero 2.9.1.

4.11 Fintanto che il sistema non ha registrato alcuna conferma dell'espressione definitiva del voto elettronico, gli aventi diritto possono ancora esprimere il proprio voto attraverso un canale di voto convenzionale.

4.12 È permesso utilizzare un mezzo di autenticazione indipendente dal voto elettronico. Nell'ambito dell'analisi dei rischi occorre valutare approfonditamente le ripercussioni sull'integrità della verifica del diritto di voto e la tutela del segreto del voto.

5. Preparazione dello scrutinio

5.1 Se dati riguardanti il catalogo elettorale vengono importati da un sistema terzo che non è sotto il controllo del Cantone, i dati devono essere crittati e firmati. La firma deve essere verificata al momento del ricevimento di tali dati. Per l'invio alla tipografia prevalgono le disposizioni di cui al numero 7.

5.2 I dati necessari per la verifica delle note di conferma secondo il numero 2.6 vengono consegnati ai verificatori.

6. Requisiti posti alle carte di legittimazione di voto

6.1 Le carte di legittimazione di voto devono per quanto possibile essere concepite in modo tale da garantire agli aventi diritto di voto disabili un accesso senza barriere al voto elettronico.

6.2 Gli elementi di sicurezza presenti sulla carta di legittimazione di voto (p. es. campo con patina da grattare) possono essere utilizzati soltanto se è dimostrato che l'informazione coperta è ben protetta contro la lettura non autorizzata.

6.3 Se si rinuncia all'utilizzazione di elementi di sicurezza volti a proteggere le informazioni confidenziali presenti sulla carta di legittimazione di voto, devono essere disponibili processi organizzativi che garantiscano la sicurezza.

7. Requisiti posti alle tipografie

7.1 I dati di stampa per la produzione delle carte di legittimazione di voto sono inviati in forma crittata e con la firma. In alternativa è anche possibile consegnare personalmente un supporto dati contenente i dati di stampa. In tal caso il supporto dati è trasportato e consegnato alla tipografia da due persone che assieme lo sorvegliano (principio del doppio controllo).

7.2 Il crittaggio deve soddisfare i requisiti dello standard eCH-0014[5], capitolo 7.5. In caso di crittografia simmetrica l'elemento segreto necessario per la decrittazione viene inviato ai responsabili della tipografia usando una via parallela sicura.

7.3 I responsabili della tipografia che prendono in consegna il supporto di dati firmano una ricevuta.

7.4 Ai supporti di dati contenenti i dati di stampa, alle componenti su cui vengono decrittati i dati critici e a tutte le componenti che trattano i dati critici si applicano le disposizioni di cui al numero 3 concernenti la componente di stampa.

7.5 I responsabili della tipografia eseguono un controllo delle quantità di materiale.

7.6 Dopo la stampa delle carte di legittimazione di voto la tipografia distrugge i dati ricevuti.

7.7 Se la tipografia si occupa anche dell'imballaggio e dell'invio delle carte di legittimazione di voto, queste ultime vanno imballate assieme al materiale di voto immediatamente dopo la stampa.

7.8 Il canale tra la tipografia e gli aventi diritto di voto può essere considerato affidabile soltanto se gli organi competenti secondo il diritto cantonale inviano per corrispondenza il materiale di voto imballato agli aventi diritto di voto oppure se assicurano la consegna di persona.

8. Informazioni e istruzioni

8.1 L'organo responsabile a livello cantonale elabora un piano per informare i cittadini sul voto elettronico.

8.2 Il piano garantisce che le informazioni siano autorizzate dagli organi competenti.

8.3 Su Internet sono disponibili consigli e istruzioni sull'espressione del voto e informazioni riguardanti la responsabilità degli aventi diritto di voto. Si evita così che essi agiscano in modo precipitoso o senza riflettere.

5 eCH-0014: Normes et architectures pour les applications de cyberadministration en Suisse (SAGA.ch), versione 9.0 del 09.12.2019 (in franc. e ted.); lo standard è ottenibile e scaricabile gratuitamente presso: Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich, www.ech.ch.

8.4 Agli aventi diritto di voto sono illustrate in maniera accessibile la verificabilità, altre misure di sicurezza e il modo di procedere previsto in caso di anomalie.

8.5 Agli aventi diritto di voto vengono illustrati gli aspetti a cui devono prestare attenzione affinché possano esprimere il loro voto in tutta sicurezza.

8.6 Agli aventi diritto di voto viene spiegato in che modo si può cancellare il voto, una volta espresso, da tutte le memorie della piattaforma utente che essi hanno utilizzato per votare.

8.7 In caso di domande sul voto elettronico gli aventi diritto di voto possono chiedere assistenza.

8.8 Gli aventi diritto di voto sono invitati a segnalare all'organo responsabile a livello cantonale le note di conferma secondo il numero 2.5 visualizzate in modo errato, come il codice di verifica, e altre verifiche dall'esito negativo. Questo invito è diffuso anche contestualmente all'invio del materiale di voto.

8.9 Gli aventi diritto di voto sono invitati a tenere sotto chiave il materiale di voto con gli elementi di sicurezza forniti in adempimento del numero 2.5 fino all'espressione definitiva del voto o alla conclusione dello scrutinio.

8.10 Gli aventi diritto di voto ricevono le indicazioni necessarie per controllare l'autenticità del sito Internet utilizzato per esprimere il voto, del server e del software. L'attendibilità di un controllo efficace deve essere supportata dall'impiego di mezzi crittografici in conformità con le migliori prassi.

8.11 Le informazioni essenziali per l'espressione sicura del voto vengono inviate assieme al materiale di voto. Agli aventi diritto di voto viene spiegato che in caso di dubbio devono attenersi alle informazioni contenute nel materiale di voto e non alle informazioni visualizzate sulla piattaforma utente.

8.12 Agli aventi diritto di voto viene spiegato con quali provvedimenti è garantita la tutela del segreto del voto.

8.13 Le lacune note e la relativa necessità di agire vengono comunicate in modo trasparente.

8.14 I verificatori vengono informati e istruiti adeguatamente riguardo ai processi cui sono soggetti la correttezza del risultato, la tutela del segreto del voto e l'esclusione di risultati parziali anticipati (p. es. generazione di chiavi, stampa del materiale di voto, decrittazione e spoglio). Essi sono in grado di capire i punti centrali dei processi e il loro significato.

9. Apertura e chiusura del canale di voto elettronico

Il canale di voto elettronico è a disposizione soltanto nel periodo ammesso.

10. Controllo della conformità e deposito di voti espressi in modo definitivo

Un voto espresso in modo non conforme al sistema non è depositato nell'urna elettronica.

11. Spoglio dei voti depositati nell'urna elettronica

11.1 La decrittazione dei voti e il loro spoglio possono avere inizio al più presto la domenica della votazione o dell'elezione.

11.2 Il Cantone esegue la decrittazione e lo spoglio nella propria infrastruttura.

11.3 Il Cantone provvede alla stesura di un protocollo sulla procedura di decrittazione dei voti e sul loro spoglio. L'organo responsabile a livello cantonale approva il protocollo.

11.4 Dalla decrittazione dei voti fino alla trasmissione del risultato dello scrutinio ogni accesso al sistema o a una delle sue componenti è effettuato da almeno due persone congiuntamente; esso è registrato per scritto e deve poter essere controllato dai verificatori.

11.5 Se i dati riguardanti il risultato vengono trasmessi a un sistema terzo che non è sotto il controllo del Cantone, i dati vengono crittati e firmati.

11.6 Il sistema permette di constatare, per mezzo della carta di legittimazione di voto, se qualcuno ha espresso un voto elettronico.

11.7 La decrittazione e lo spoglio dei voti si svolgono in presenza di verificatori. I Cantoni possono in aggiunta consentire lavori di verifica da remoto.

11.8 Alle componenti utilizzate per lo spoglio dei voti che non sono affidabili secondo il numero 2.4 sono posti gli stessi requisiti validi per le componenti di setup secondo il numero 3.

11.9 Nel verificare le note di conferma secondo il numero 2.6 i verificatori si assumono la loro responsabilità definita dal diritto cantonale.

11.10 L'organo responsabile a livello cantonale sottopone ai verificatori tutti gli indicatori rilevanti per la correttezza del risultato. Oltre alle note di conferma secondo il numero 2.6, vi figurano in particolare il numero e il tipo di anomalie che gli aventi diritto di voto hanno segnalato al Cantone.

11.11 Il Cantone anticipa eventuali anomalie e a tale scopo elabora, d'intesa con gli organi interessati, un piano d'emergenza che stabilisce il modo di procedere nei casi specifici. Garantisce la trasparenza nei confronti del pubblico.

11.12 Se sono disponibili e sempre che la base di dati lo consenta, per accertare la plausibilità del risultato vanno impiegati metodi statistici.

12. Dati confidenziali

12.1 Occorre assicurare che né collaboratori né persone esterne conoscano dati che permettono di stabilire un legame fra l'identità di un votante e il voto che ha espresso.

12.2 Occorre assicurare che prima della decrittazione dei voti né collaboratori né persone esterne conoscano dati che permettono di rilevare anticipatamente risultati parziali.

12.3 Il Cantone non deve inoltrare a imprese private la sua parte della chiave per la decrittazione dei voti di cui dispone, secondo il numero 3.1, sulla componente di controllo da esso gestita.

12.4 Il Cantone tratta in modo confidenziale i risultati dello scrutinio fra il momento della decrittazione dei voti e il momento della loro pubblicazione.

12.5 Il Cantone provvede affinché i dati che permettono di constatare che gli aventi diritto di voto hanno votato per via elettronica siano trattati in modo confidenziale.

12.6 Il Cantone tratta in modo confidenziale i singoli voti dopo lo spoglio.

12.7 Il Cantone provvede affinché i risultati della votazione o dell'elezione di circondari elettorali più piccoli siano trattati in modo confidenziale.

12.8 Dopo l'omologazione vengono distrutti, secondo una procedura prestabilita e documentata, tutti i dati creati nell'ambito dello scrutinio elettronico, relazionati con i singoli voti immessi e classificati come confidenziali.

13. Minacce

13.1 Le minacce elencate ai numeri 13.3–13.40 sono di natura generale e costituiscono una base da integrare. Esse si riferiscono agli obiettivi di sicurezza e vanno considerate nell'ambito dell'identificazione dei rischi. A seconda dei punti deboli accertati nel sistema, nelle analisi dei rischi dei diversi organi l'elenco va concretizzato e integrato in funzione della costellazione concreta e a dipendenza della minaccia specifica.

13.2 Sono considerate possibili minacce:

- le minacce, provocate inavvertitamente o intenzionalmente, che partono da attori interni o esterni che impiegano mezzi elettronici o fisici;
- le minacce riconducibili a una disfunzione del sistema o degli elementi che lo supportano.

	Descrizione	Obiettivo di sicurezza interessato (secondo l'art. 4 cpv. 3)
13.3	Un software nocivo modifica il voto sulla piattaforma utente.	Correttezza del risultato

	Descrizione	Obiettivo di sicurezza interessato (secondo l'art. 4 cpv. 3)
13.4	Un aggressore esterno devia il voto mediante Domain Name Server Spoofing (DNS-Spoofing[6]).	Correttezza del risultato

	Descrizione	Obiettivo di sicurezza interessato (secondo l'art. 4 cpv. 3)
13.5	Un aggressore esterno modifica il voto mediante una tecnica Man In The Middle (tecnica MITM[7]).	Correttezza del risultato
13.6	Un aggressore esterno invia mediante la tecnica MITM dati modificati in mala fede che sono necessari per l'espressione del voto e che provengono dal sistema online (p. es. file JavaScript).	Correttezza del risultato
13.7	Un aggressore interno manipola il software e questo non memorizza i voti.	Correttezza del risultato
13.8	Un aggressore interno modifica, cancella o moltiplica i voti.	Correttezza del risultato
13.9	Un aggressore interno aggiunge voti.	Correttezza del risultato
13.10	Un'organizzazione nemica si introduce nel sistema allo scopo di falsificare il risultato.	Correttezza del risultato
13.11	Un aggressore interno copia il materiale di voto e lo utilizza.	Correttezza del risultato
13.12	Un aggressore esterno utilizza metodi d'ingegneria sociale per deviare l'attenzione del votante dai provvedimenti di sicurezza (verificabilità individuale).	Correttezza del risultato
13.13	Un aggressore esterno si introduce elettronicamente, fisicamente o mediante ingegneria sociale nell'infrastruttura del Cantone e manipola le componenti di setup o sottrae dati rilevanti per la sicurezza.	Correttezza del risultato
13.14	Un aggressore esterno si introduce elettronicamente, fisicamente o mediante ingegneria sociale nell'infrastruttura della tipografia e preleva i codici delle carte di legittimazione di voto.	Correttezza del risultato

6 Noto anche come DNS-Poisoning (avvelenamento della cache DNS). Designa un attacco per mezzo del quale si riesce a falsificare l'associazione fra il nome del nodo ospite (host) e l'indirizzo IP corrispondente.

7 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 logicamente fra due parti in comunicazione fra loro, con il suo sistema esercita un controllo totale sui dati scambiati fra due o più partecipanti della rete e può in tal modo leggere le informazioni e addirittura manipolarle a suo piacimento.

	Descrizione	Obiettivo di sicurezza interessato (secondo l'art. 4 cpv. 3)
13.15	Un aggressore esterno si introduce elettronicamente, fisicamente o mediante ingegneria sociale nell'infrastruttura della Posta e sottrae carte di legittimazione di voto.	Correttezza del risultato
13.16	Nella verificabilità individuale si manifesta un errore.	Correttezza del risultato
13.17	Nella verificabilità universale si manifesta un errore.	Correttezza del risultato
13.18	Un ausilio tecnico dei verificatori presenta un errore.	Correttezza del risultato
13.19	Una backdoor[8] è inserita nel sistema mediante una dipendenza da software e viene sfruttata da un aggressore esterno per accedere al sistema.	Correttezza del risultato, tutela del segreto del voto ed esclusione di risultati parziali anticipati, raggiungibilità e funzionalità del canale di voto, protezione contro le manipolazioni delle informazioni destinate agli aventi diritto di voto, esclusione dell'utilizzo abusivo di riscontri sul comportamento di voto
13.20	Un software nocivo sulla piattaforma utente invia il voto a un'organizzazione nemica.	Tutela del segreto del voto ed esclusione di risultati parziali anticipati
13.21	Il voto è deviato mediante DNS-Spoofing.	Tutela del segreto del voto ed esclusione di risultati parziali anticipati
13.22	Un aggressore esterno legge il voto mediante MITM.	Tutela del segreto del voto ed esclusione di risultati parziali anticipati
13.23	Un aggressore interno utilizza la chiave e decritta voti non anonimi.	Tutela del segreto del voto ed esclusione di risultati parziali anticipati
13.24	Nel verificare la correttezza del trattamento e dello spoglio viene violato il segreto del voto.	Tutela del segreto del voto ed esclusione di risultati parziali anticipati
13.25	Un aggressore interno legge in anticipo i voti senza doverli decrittare.	Tutela del segreto del voto ed esclusione di risultati parziali anticipati
13.26	Un'organizzazione nemica si introduce nel sistema allo scopo di violare il segreto del voto o rilevare anticipatamente risultati parziali.	Tutela del segreto del voto ed esclusione di risultati parziali anticipati
13.27	Un errore verificatosi nel processo di crittaggio ne annulla la funzionalità o ne riduce l'efficacia.	Tutela del segreto del voto ed esclusione di risultati parziali anticipati
13.28	Un aggressore interno manipola il software e quest'ultimo rende pubblici i voti.	Tutela del segreto del voto ed esclusione di risultati parziali anticipati

8 Il termine «backdoor» (porta posteriore) designa una parte del software che consente agli utenti di accedere al computer eludendo le normali protezioni di accesso oppure un'altra funzione altrimenti protetta di un programma per computer.

	Descrizione	Obiettivo di sicurezza interessato (secondo l'art. 4 cpv. 3)
13.29	Un software nocivo presente sulla piattaforma utente rende impossibile l'espressione del voto.	Raggiungibilità e funzionalità del canale di voto
13.30	Un'organizzazione nemica compie un'aggressione in forma di «negazione del servizio»[9] (aggressione DOS).	Raggiungibilità e funzionalità del canale di voto
13.31	Un aggressore interno esegue una configurazione errata; non si arriva allo spoglio.	Raggiungibilità e funzionalità del canale di voto
13.32	Un aggressore interno falsifica le note di conferma crittografiche della verificabilità universale.	Raggiungibilità e funzionalità del canale di voto
13.33	Un errore tecnico del sistema fa sì che il sistema non sia disponibile al momento dello spoglio.	Raggiungibilità e funzionalità del canale di voto
13.34	Un ausilio tecnico dei verificatori non funziona al momento dello spoglio.	Raggiungibilità e funzionalità del canale di voto
13.35	Un'organizzazione nemica si introduce nel sistema allo scopo di perturbarne l'esercizio, manipolare le informazioni destinate agli aventi diritto di voto o sottrarre riscontri sul comportamento di voto dei votanti.	Raggiungibilità e funzionalità del canale di voto, protezione contro le manipolazioni delle informazioni destinate agli aventi diritto di voto, esclusione dell'utilizzo abusivo di riscontri sul comportamento di voto
13.36	Un aggressore interno sottrae dati inerenti agli indirizzi degli aventi diritto di voto.	Protezione delle informazioni personali sugli aventi diritto di voto
13.37	Un software nocivo influenza gli aventi diritto di voto nella formazione delle loro opinioni.	Protezione contro le manipolazioni delle informazioni destinate agli aventi diritto di voto
13.38	Un aggressore interno manipola il sito web d'informazione o il portale delle votazioni, ingannando gli aventi diritto di voto.	Protezione contro le manipolazioni delle informazioni destinate agli aventi diritto di voto
13.39	Un aggressore interno prescrive agli aventi diritto di voto se e come debbano votare o eleggere. Dopo la decrittazione trova nell'infrastruttura riscontri del fatto che gli aventi diritto di voto si sono attenuti alle istruzioni.	Esclusione dell'utilizzo abusivo di riscontri sul comportamento di voto
13.40	Un aggressore esterno prescrive agli aventi diritto di voto se e come debbano votare o eleggere e richiede loro un riscontro del fatto che si sono attenuti alle istruzioni.	Esclusione dell'utilizzo abusivo di riscontri sul comportamento di voto

[9] 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.

14. Constatazione e notifica di eventi e debolezze inerenti alla sicurezza; gestione di eventi e miglioramenti inerenti alla sicurezza

14.1 Un sistema di monitoraggio dell'infrastruttura riconosce gli incidenti che potrebbero mettere in pericolo la sicurezza, inclusa la disponibilità, del sistema e allarma 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.

Errori nella registrazione del voto nelle componenti di controllo e nell'urna devono essere riconosciuti. Ulteriori informazioni relative all'errore devono essere disponibili, in modo da riconoscere ed eliminare la causa. Gli incidenti constatati devono essere notificati all'organo responsabile a livello cantonale.

14.2 Sull'infrastruttura sono redatti protocolli la cui raccolta, trasmissione e memorizzazione sono resistenti alle manipolazioni (protocolli del sistema). I protocolli sono coerenti fra loro e permettono il tracciamento degli eventi pertinenti nell'ambito dell'investigazione di presunte manipolazioni o di errori. Essi servono da attestati per la presa in considerazione completa, non falsificata ed esclusiva di voti espressi conformemente al sistema, nonché per la tutela del segreto del voto e l'esclusione di risultati parziali anticipati.

Il contenuto dei protocolli comprende almeno gli eventi seguenti:

- avvio e conclusione dei processi di audit, di identificazione e di autenticazione
- avvio, riavvio e conclusione della fase di voto o elezione
- avvio dello spoglio con accertamento del risultato
- esecuzione e risultati di eventuali autotest
- disfunzioni constatate negli elementi dell'infrastruttura informatica che compromettono la capacità operativa

Di ogni evento viene documentata la data e l'ora, il tipo di evento, il possibile autore e il risultato, in termini di successo o di insuccesso.

I protocolli del sistema vengono messi a disposizione dell'organo responsabile a livello cantonale in una forma che gli permetta di interpretarne le informazioni.

14.3 Il monitoraggio e la redazione dei protocolli del sistema sottostanno a un continuo processo di miglioramento. Tale processo comprende un dialogo aperto fra gli attori coinvolti nonché una valutazione obiettiva periodica dell'efficacia degli strumenti e dei processi adottati. I risultati di queste valutazioni sono tenuti in considerazione.

14.4 Il monitoraggio e la redazione dei protocolli del sistema non compromettono in alcun modo l'efficacia delle misure adottate per tutelare il segreto del voto.

14.5 È garantito che, in caso di guasto, i voti e i dati a comprova di un funzionamento ineccepibile della procedura di spoglio dei voti vengono memorizzati in modo integro sull'infrastruttura.

14.6 Dopo un guasto al sistema o un'interruzione dei supporti di comunicazione o di memorizzazione, il sistema è posto in una modalità di manutenzione in cui esiste la possibilità di ritornare a uno stato sicuro. Le procedure di voto già avviate vengono interrotte. Il votante può riprendere a votare soltanto quando il sistema è tornato a uno stato sicuro.

14.7 Con l'ausilio di caratteristiche di autenticazione è possibile esprimere voti di controllo non attribuiti ad alcun avente diritto di voto. Il contenuto di questi voti di controllo è iscritto in un protocollo. Il conteggio dei voti di controllo viene confrontato con i protocolli.

È garantito che i voti di controllo sono trattati quanto più possibile alla stregua di voti espressi conformemente al sistema; nel contempo è garantito che non vengono conteggiati.

14.8 La disponibilità dell'infrastruttura viene verificata e iscritta in un protocollo a intervalli di tempo prestabiliti.

14.9 Mediante un processo predefinito e documentato, tutte le parti del sistema vengono regolarmente aggiornate, in modo da eliminare punti deboli di cui si è venuti a conoscenza.

14.10 Le misure di monitoraggio e di protocollo relative all'utilizzo del sistema, alle attività degli amministratori e ai guasti vengono descritte in dettaglio, attuate, sorvegliate e verificate.

15. Utilizzo di misure crittografiche e amministrazione delle chiavi

15.1 I certificati elettronici sono amministrati secondo le migliori prassi.

15.2 Per assicurare l'integrità delle serie di dati su cui si basano la correttezza del risultato nonché la segretezza di dati critici, inclusi i dati di identificazione e di autenticazione delle autorità, sono impiegate misure crittografiche efficaci, conformi allo stato della tecnica.

15.3 Per assicurare la segretezza di dati critici sono impiegate nell'infrastruttura misure crittografiche efficaci, conformi allo stato della tecnica. Questi dati vengono sempre memorizzati sui supporti di dati in modo crittato.

15.4 Le componenti di base crittografiche vengono utilizzate solamente se le lunghezze delle chiavi e gli algoritmi sono conformi agli standard correnti (p. es. NIST, ECRYPT, FiEle). La firma elettronica soddisfa i requisiti posti a una firma elettronica avanzata ai sensi della legge del 18 marzo 2016[10] sulla firma elettronica (FiEle). La verifica della firma avviene mediante un certificato elettronico rilasciato da un prestatore di servizi di certificazione riconosciuto ai sensi della FiEle.

10 RS **943.03**

16. Scambio di informazioni fisico ed elettronico sicuro

16.1 Tutte le componenti dell'infrastruttura sono gestite in una zona di rete separata. La zona viene protetta mediante un adeguato controllo dell'instradamento.

16.2 Il voto elettronico è di principio chiaramente separato da tutte le altre applicazioni.

17. Test del sistema

17.1 Le funzioni rilevanti per la sicurezza del sistema (funzioni di sicurezza) vengono testate. I test vengono documentati con piani di test e con i risultati attesi dai test e i risultati effettivi.

Il piano di test:

- stabilisce quali sono i test da eseguire;
- descrive gli scenari di ciascun test, comprese eventuali dipendenze dai risultati di altri test.

I risultati attesi devono indicare i risultati che ci si attende da una esecuzione riuscita dei test.

I risultati effettivi devono essere coerenti con i risultati attesi.

17.2 Viene eseguita un'analisi della copertura dei test. Essa comprende la prova che:

- i test definiti nella documentazione di test sono coerenti con le specifiche funzionali delle interfacce;
- tutte le interfacce sono state completamente testate.

17.3 Viene eseguita un'analisi della profondità dei test. Essa comprende la prova che:

- i test definiti nella documentazione di test sono coerenti con i sottosistemi relativi alle funzioni di sicurezza e ai moduli che hanno un ruolo nel garantire la sicurezza;
- tutti i sottosistemi relativi alle funzioni di sicurezza identificate nelle specifiche sono stati testati;
- tutti moduli che hanno un ruolo nel garantire la sicurezza sono stati testati.

18. Organizzazione della sicurezza dell'informazione

18.1 Tutti i ruoli e tutte le responsabilità per l'esercizio del sistema sono definiti con precisione, attribuiti e comunicati.

18.2 La configurazione iniziale dell'infrastruttura, per quanto riguarda l'hardware, il software e i diritti d'accesso, e ogni modifica devono essere autorizzate.

18.3 I rischi connessi con terzi (mandatari come fornitori e prestatori di servizi) sono identificati e ridotti nella misura del necessario per il tramite di adeguati accordi contrattuali. Il rispetto degli accordi viene sorvegliato e verificato adeguatamente durante la loro validità.

19. Amministrazione delle risorse immateriali e materiali

19.1 Tutte le risorse immateriali e materiali ai sensi della nozione di asset contenuta nella norma ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements[11], rilevanti per il voto elettronico (organizzazione globale, in particolare i processi organizzativi e le informazioni in quanto tali che vi sono trattate, i supporti di dati, le installazioni per il trattamento delle informazioni dell'infrastruttura e i locali dell'infrastruttura) vengono rilevati in un inventario. È allestito un elenco del personale. L'inventario e l'elenco del personale devono essere tenuti aggiornati. Ad ogni risorsa immateriale e materiale è attribuita una persona che ne assume la responsabilità.

19.2 Viene definito l'uso ammesso di risorse immateriali e materiali.

19.3 Per le informazioni sono emanate e comunicate linee direttrici in materia di classificazione.

19.4 Per la caratterizzazione e l'utilizzazione di informazioni sono approntate delle procedure.

20. Affidabilità del personale

20.1 Per garantire l'affidabilità del personale prima, durante e dopo la sua assunzione o in caso di cambiamenti di ruolo sono approntate e comunicate direttive e procedure adeguate.

20.2 I responsabili del personale si assumono la piena responsabilità delle misure volte a garantire l'affidabilità del personale.

20.3 Il personale dispone di una spiccata sensibilità in materia di sicurezza dell'informazione. A questo scopo è approntato e gestito un programma di formazione e di esercitazione conforme ai compiti da svolgere.

21. Sicurezza fisica e riferita all'ubicazione

21.1 I perimetri di sicurezza dei diversi locali dell'infrastruttura sono definiti in modo chiaro.

21.2 Per l'accesso fisico ai diversi locali dell'infrastruttura le autorizzazioni d'accesso sono definite, introdotte e controllate adeguatamente.

11 La norma può essere consultata o ottenuta dietro pagamento presso la Segreteria centrale dell'Organizzazione internazionale di normazione (ISO), Chemin de Blandonnet 8, CP 401, 1214 Vernier, www.iso.org.

21.3 Per garantire la sicurezza degli apparecchi dentro e fuori i locali dell'infrastruttura sono definite direttive e procedure adeguate, di cui viene sorvegliato e verificato il rispetto.

21.4 Tutti i dati sono trattati, e in particolare conservati, esclusivamente in Svizzera.

22. Gestione della comunicazione e dell'esercizio

22.1 Gli obblighi e gli ambiti di responsabilità sono 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.

22.2 Per proteggersi da software nocivi vengono adottate misure adeguate.

22.3 È allestito e attuato un piano dettagliato per la sicurezza dei dati. Il corretto funzionamento della sicurezza dei dati è verificato periodicamente.

22.4 Sono definite e attuate misure adeguate per la protezione della rete da minacce evidenziate dall'analisi dei rischi secondo l'articolo 4 in combinato disposto con il numero 13 e per la sicurezza dei servizi di rete.

22.5 Le procedure per gestire i supporti amovibili di dati e per smaltire i supporti di dati sono disciplinate in modo dettagliato.

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

23.1 È garantito che durante lo scrutinio ogni modifica successiva dei diritti di accesso e d'intervento avvenga esclusivamente con il consenso dell'organo responsabile a livello cantonale.

23.2 L'accesso all'infrastruttura e al software e ogni intervento sugli stessi sono disciplinati e documentati in dettaglio in base a un'analisi dei rischi. Nei settori ad alto rischio e per tutte le operazioni manuali relative alle urne elettroniche (p. es. apertura del canale di voto, chiusura del canale di voto, avvio dello spoglio) si applica il principio del doppio controllo.

Le operazioni manuali relative alle urne elettroniche (p. es. apertura del canale di voto, chiusura del canale di voto, avvio dello spoglio) sono autenticate in modo esplicito.

23.3 È garantito che non si possano modificare senza autorizzazione informazioni sul sito del voto elettronico né le pagine informative sul voto elettronico.

23.4 Durante lo scrutinio è escluso qualsivoglia intervento sull'infrastruttura che non riguardi il voto elettronico.

23.5 È assicurato che nessuno degli elementi dei dati di autenticazione client possa essere sistematicamente intercettato, modificato o deviato. Per

l'autenticazione sono attuate misure e impiegate tecnologie che riducano sufficientemente al minimo il rischio di abuso sistematico da parte di terzi.

24. Sviluppo e manutenzione di sistemi d'informazione

24.1 Sviluppo

24.1.1 Viene definito un modello di ciclo di vita. Tale modello:
- viene utilizzato per lo sviluppo e la manutenzione del software;
- prevede i controlli necessari nello sviluppo e nella manutenzione del software;
- viene documentato.

24.1.2 Viene allestito un elenco degli strumenti di sviluppo utilizzati e delle opzioni di configurazione selezionate per l'impiego dei singoli strumenti di sviluppo.

24.1.3 La documentazione degli strumenti di sviluppo comprende:
- una definizione di ciascuno strumento di sviluppo;
- una descrizione di tutte le convenzioni e direttive utilizzate nell'implementazione dello strumento di sviluppo;
- una descrizione univoca del significato di tutte le opzioni di configurazione utilizzate per l'applicazione dello strumento di sviluppo.

24.1.4 Si stabilisce quali sono gli standard di implementazione applicati.

24.1.5 Il software è specificato e implementato in modo tale che le funzioni di sicurezza non possano essere aggirate.

24.1.6 Le funzioni di sicurezza sono specificate e implementate in modo tale che siano protette dalle manipolazioni.

24.1.7 L'architettura di sicurezza del software è documentata. La documentazione:
- attesta un grado di dettaglio corrispondente alla descrizione delle funzioni di sicurezza;
- descrive i settori della sicurezza cui si indirizzano le funzioni di sicurezza;
- descrive in che modo i processi di inizializzazione vengono garantiti;
- comprova l'adempimento dei requisiti di cui a numeri 24.1.5 e 24.1.6.

24.1.8 Le specifiche funzionali sono documentate. La documentazione:
- rappresenta l'intero software;
- descrive lo scopo e l'utilizzo di tutte le interfacce;
- identifica e descrive tutti i parametri associati alle interfacce;
- descrive tutte le azioni associate alle interfacce;
- descrive tutti i messaggi di errore diretti che potrebbero risultare dal richiamo delle singole interfacce.

24.1.9 La tracciabilità fra le specifiche funzionali e i requisiti di sicurezza è garantita fino al livello delle interfacce.

24.1.10 Tutte le funzioni di sicurezza sono implementate nel codice sorgente.

24.1.11 La tracciabilità fra l'intero codice sorgente e le specifiche delle funzioni di sicurezza è garantita e la loro corrispondenza è evidente.

24.1.12 Le funzioni di sicurezza sono concepite e implementate in modo che siano ben strutturate. La struttura interna viene descritta e comprende una motivazione che:

- indica le caratteristiche che sono state utilizzate per valutare le nozioni di «ben strutturato» e di «complesso»;
- indica che tutte le funzioni di sicurezza sono ben strutturate e non sono troppo complesse.

24.1.13 Le specifiche comprendono i seguenti elementi:

- una descrizione della struttura del software nella forma di sottosistemi;
- una descrizione delle funzioni di sicurezza nella loro qualità di moduli e, per ogni modulo, il rispettivo obiettivo e una descrizione di come esso sia in relazione con gli altri moduli; la descrizione dei moduli rilevanti per la sicurezza comprende anche le interfacce disponibili, i valori restituiti di queste interfacce e le interfacce degli altri moduli utilizzate per interagire con esse;
- una descrizione di tutti i sottosistemi in relazione alle funzioni di sicurezza, comprese le possibili reciproche interazioni;
- un'illustrazione chiara dei sottosistemi connessi alle funzioni di sicurezza che comprova che tutte le interfacce corrispondono al comportamento descritto nella specifica; l'illustrazione deve presentare un grado di dettaglio che si estende almeno fino ai moduli.

24.1.14 Il software è provvisto di una caratterizzazione univoca.

24.1.15 La documentazione relativa alla gestione della configurazione comprende i seguenti elementi:

- una descrizione del modo in cui gli elementi di configurazione sono identificati;
- un piano di gestione della configurazione che descrive in che modo il sistema di gestione della configurazione è utilizzato nello sviluppo del software e quali sono le procedure applicate per l'accettazione di modifiche o di nuovi elementi;
- la prova che le procedure di accettazione prevedono un'adeguata verifica delle modifiche per tutti gli elementi di configurazione.

24.1.16 Il sistema di gestione della configurazione:

- identifica in modo univoco tutti gli elementi di configurazione;
- appronta misure automatizzate per fare in modo che agli elementi di configurazione vengano apportate soltanto modifiche autorizzate;
- sostiene lo sviluppo del software attraverso procedure automatizzate;
- garantisce che la persona che ha la responsabilità di accettare l'elemento di configurazione non è la stessa che lo ha sviluppato;

– identifica gli elementi di configurazione di cui si compongono le funzioni di sicurezza;
– sostiene con procedure automatizzate la verifica di tutte le modifiche apportate al software, compresi il protocollo dell'autore nonché la data e l'ora della modifica;
– appronta una procedura automatizzata per l'identificazione di tutti gli elementi di configurazione interessati dalla modifica di uno specifico elemento di configurazione;
– è in grado di identificare la versione del codice sorgente sulla base del quale è generato il software.

24.1.17 Tutti gli elementi di configurazione sono inventariati nel sistema di gestione della configurazione.

24.1.18 Il sistema di gestione della configurazione viene utilizzato in conformità con il piano di gestione della configurazione.

24.1.19 È allestito un elenco di configurazione contenente i seguenti elementi:
– il software;
– le prove che i controlli richiesti per il rispetto della sicurezza sono stati eseguiti;
– le parti di cui si compone il software;
– il codice sorgente;
– la commit history[12];
– i rapporti sulle lacune nella sicurezza e sul loro stato di risoluzione.

Per ogni elemento rilevante per le funzioni di sicurezza si menziona lo sviluppatore. Ciascun elemento è identificato in modo univoco.

24.1.20 La documentazione concernente la sicurezza dello sviluppo del software comprende i seguenti aspetti:
– la descrizione delle misure di sicurezza fisiche, procedurali, in materia di personale e altre che sono necessarie per la protezione e l'integrità della configurazione e dell'implementazione del software nel suo ambiente di sviluppo;
– la prova che le misure di sicurezza offrono il livello di protezione necessario a garantire l'integrità del software.

24.2 Esercizio

24.2.1 È allestito un manuale d'esercizio. Per ogni ruolo utente, esso contiene i seguenti aspetti:
– una descrizione delle funzioni accessibili all'utente e delle autorizzazioni che devono essere controllate in un ambiente sicuro, compresi i relativi avvertimenti;

12 La *commit history* consiste in un elenco ordinato di tutte le modifiche apportate a una *repository* con la motivazione di ciascuna modifica.

- una descrizione di come le interfacce disponibili possono essere utilizzate in modo sicuro;
- una descrizione delle funzioni e delle interfacce disponibili, in particolare di tutti i parametri di sicurezza posti sotto il controllo dell'utente, con l'indicazione dei valori rilevanti per la sicurezza;
- una presentazione accurata di tutti i tipi di eventi di sicurezza legati alle funzioni accessibili all'utente che devono essere eseguite, compresi gli adeguamenti delle caratteristiche di sicurezza apportati ad elementi posti sotto il controllo delle funzioni di sicurezza;
- una descrizione delle misure di sicurezza che devono essere attuate per conseguire gli obiettivi di sicurezza d'esercizio.

24.2.2 Il manuale d'esercizio indica tutti i possibili modi d'esercizio del software, comprese la ripresa dell'esercizio dopo la scoperta di errori nonché una descrizione delle conseguenze e delle implicazioni derivanti da tali errori per il mantenimento di un esercizio sicuro.

24.2.3 Il manuale d'esercizio è preciso e adeguato allo scopo.

24.3 Compilazione e deployment affidabili e verificabili

24.3.1 Il processo di preparazione descrive tutti i passi necessari per:

- un'accettazione sicura delle componenti del sistema conformemente alle procedure di fornitura;
- una preparazione sicura dell'ambiente d'esercizio conformemente agli obiettivi di sicurezza d'esercizio;
- un'istallazione sicura del software nell'ambiente d'esercizio.

24.3.2 La fornitura del software o di parti del sistema è documentata e comprende tutti i processi necessari al mantenimento della sicurezza in occasione della fornitura del software.

24.3.3 È eseguita una compilazione affidabile e verificabile con adeguate misure di sicurezza che garantisce che il codice eseguibile sia una rappresentazione verificabile e fedele del codice sorgente che è stato sottoposto a un controllo pubblico e a verifiche indipendenti. La compilazione permette di stabilire una catena di conferme per la verifica del software e comprende in particolare:

- la prova che l'ambiente di compilazione è impostato come quello descritto sulla piattaforma pubblica (insieme degli strumenti con la loro rispettiva versione, sistema d'esercizio ed eventuali configurazioni); eventuali divergenze devono essere documentate e motivate;
- la prova che il software è stato compilato conformemente alle istruzioni disponibili sulla piattaforma pubblica; se al momento della compilazione viene ravvisata una lacuna nelle istruzioni, essa va iscritta in un protocollo e la documentazione deve essere successivamente adeguata;
- la prova che il codice sorgente sottoposto al controllo pubblico e verificato è effettivamente quello che è stato utilizzato per la compilazione;

– la prova che non è stato introdotto alcun elemento diverso da quelli previsti nelle istruzioni;
– la prova che tutte le firme crittografiche delle dipendenze sono state verificate rispetto a un riferimento comprovato, pubblico e affidabile;
– la prova che è stata condotta un'analisi dei punti deboli delle dipendenze e, nel caso in cui esistano punti deboli rilevanti per il software, che esse non rendano il software vulnerabile agli attacchi;
– la prova che gli eventuali parametri introdotti non rendono il sistema vulnerabile agli attacchi.

24.3.4 È eseguito un *deployment* affidabile e verificabile con adeguate misure di sicurezza, in modo da garantire che:

1. il codice utilizzato in produzione sia una rappresentazione verificabile e fedele del codice sorgente che è stato sottoposto a un controllo pubblico e a verifiche indipendenti; e
2. l'ambiente di produzione sia conforme con quello che è stato sottoposto a un controllo pubblico e a verifiche indipendenti.

Il deployment permette di stabilire una catena di conferme per la verifica del software e comprende in particolare:

– la prova che l'ambiente di produzione è conforme con quello che è stato sottoposto a un controllo pubblico e a verifiche indipendenti; eventuali divergenze (versione di firmware, file di configurazione, ecc.) devono essere documentate e motivate;
– la prova che il software utilizzato nell'ambiente di produzione è effettivamente quello che è stato allestito nella procedura di compilazione affidabile e verificabile;
– la prova che gli eventuali parametri introdotti non rendono il sistema più vulnerabile agli attacchi.

24.3.5 La qualità delle prove della compilazione affidabile e verificabile e del deployment affidabile e verificabile è attestata dalla presenza di almeno due testimoni appartenenti a istituzioni diverse o attraverso procedure tecniche volte a stabilire la verità secondo lo stato delle conoscenze scientifiche e l'esperienza.

24.3.6 La catena di conferme della compilazione affidabile e verificabile e del deployment affidabile e verificabile è resa accessibile al pubblico.

24.4 Eliminazione sistematica delle lacune

24.4.1 Vengono definiti processi per l'eliminazione delle lacune. I processi comprendono:

– una documentazione di questi processi, in particolare per quanto riguarda la tracciabilità delle lacune per ciascuna delle versioni del software, nonché dei metodi utilizzati affinché gli utenti del sistema dispongano delle informazioni concernenti le lacune, le correzioni e le possibili misure correttive;

- l'obbligo di descrivere il genere e le conseguenze di tutte le lacune nella sicurezza, le informazioni sullo stato dei lavori volti a trovare una soluzione e le misure correttive decise;
- una descrizione degli strumenti che permettono agli utenti del sistema di comunicare agli sviluppatori del software rapporti e richieste riguardanti presunte lacune nel software;
- una procedura che esiga una reazione in tempi brevi e l'invio automatico di rapporti sulle lacune della sicurezza e i relativi correttivi agli utenti del sistema registrati che potrebbero essere toccati dalla lacuna.

24.4.2 È definito un processo per il trattamento delle lacune segnalate:

- questo processo garantisce che tutte le lacune notificate e confermate sono state eliminate e che le relative procedure sono state comunicate agli utenti del sistema;
- esso prevede delle disposizioni che garantiscono che l'eliminazione di una lacuna nella sicurezza non introduce nuove lacune nella sicurezza.

24.4.3 Vengono definite direttive per la segnalazione e l'eliminazione delle lacune. Esse comprendono:

- una descrizione del modo in cui gli utenti del sistema possono segnalare allo sviluppatore presunte lacune nella sicurezza;
- una descrizione del modo in cui gli utenti del sistema possono registrarsi presso lo sviluppatore, in modo da ricevere rapporti sulle lacune della sicurezza e sui relativi correttivi;
- l'indicazione di specifici servizi di contatto per tutti i rapporti e le richieste di informazioni su questioni di sicurezza riguardanti il software.

24.5 Garanzia della qualità

Periodicamente si verifica in modo obiettivo se i processi eseguiti e i prodotti di lavoro ad essi associati corrispondono alla descrizione dei processi, delle norme e delle procedure che devono essere applicati. Eventuali non conformità sono seguite fino a quando non sono state risolte.

25. Qualità del codice sorgente e della documentazione

Il codice sorgente e la documentazione soddisfano almeno i seguenti criteri di qualità:

25.1 Comprensibilità

25.1.1 Per comprensibilità si intende il rigore logico che va dai requisiti all'implementazione.

25.1.2 Tutti i requisiti posti al protocollo crittografico sono comprensibili per tutti i risultati di lavoro legati al processo di sviluppo del software.

25.1.3 Il legame fra i requisiti legali e il protocollo crittografico, le specifiche e la documentazione dell'architettura è fatto oggetto di una descrizione.

25.2 Completezza

25.2.1 Per completezza si intende l'attuazione completa delle funzioni richieste.

25.2.2 Il software non contiene indicazioni ambigue (input, funzione, output). A ciascun elemento si fa riferimento sempre con lo stesso nome.

25.2.3 Tutti i dati referenziati e tutte le funzioni utilizzate sono definiti nelle specifiche.

25.2.4 Sono utilizzate tutte le funzioni definite nelle specifiche.

25.2.5 Per ogni punto oggetto di decisione (p. es. esecuzione condizionata), le possibili alternative sono definite nelle specifiche.

25.2.6 Tutti i parametri sono definiti nelle specifiche e convalidati (nessuna attribuzione implicita di parametri).

25.2.7 Tutti gli errori gravi che vengono segnalati sono eliminati prima di passare alla tappa successiva del ciclo di sviluppo.

25.2.8 Il protocollo crittografico, la specifica, il design e il codice sorgente sono armonizzati fra loro.

25.3 Coerenza

25.3.1 Per coerenza si intende la proprietà del software di utilizzare procedure e notazioni uniformi nella concezione e nell'implementazione.

25.3.2 Le rappresentazioni nella documentazione seguono una convenzione stabilita dallo sviluppatore del software.

25.3.3 Le funzioni e le variabili seguono una convenzione d'attribuzione dei nomi stabilita dallo sviluppatore del software.

25.3.4 Input e output di funzioni sono trattati in base a una convenzione stabilita dallo sviluppatore del software.

25.3.5 Gli errori sono trattati in base a una convenzione stabilita dallo sviluppatore del software.

25.3.6 I tipi di variabili utilizzati sono coerenti.

25.4 Uniformità della comunicazione

25.4.1 Per uniformità della comunicazione si intende l'utilizzazione di protocolli standardizzati e routine d'interfaccia.

25.4.2 Sono definite regole per la comunicazione con altri sistemi.

25.4.3 La comunicazione si basa su metodi di comunicazione standardizzati.

25.5 Uniformità dei dati

25.5.1 Per uniformità dei dati si intende la proprietà del software di utilizzare una rappresentazione standardizzata dei dati.

25.5.2 La rappresentazione standardizzata dei dati per la comunicazione con altri sistemi viene definita in modo formale.

25.5.3 Per la conversione fra le diverse rappresentazioni vengono definiti degli standard.

25.5.4 Le funzioni di conversione dovrebbero essere centralizzate in un unico modulo.

25.6 Apprendibilità

25.6.1 Per apprendibilità si intende la proprietà del software di permettere agli utenti di familiarizzarsi facilmente con il suo funzionamento.

25.6.2 Le persone che gestiscono e utilizzano il sistema sono formate e ricevono la documentazione necessaria.

25.6.3 La formazione comprende la possibilità di esercitarsi su un sistema previsto appositamente.

25.6.4 Gli strumenti di aiuto sono facilmente accessibili.

25.7 Operabilità

25.7.1 Per operabilità si intende la proprietà del software di agevolare l'interazione con il sistema.

25.7.2 Il software è di facile utilizzo. La navigazione si rifà agli schemi generalmente in uso.

25.7.3 Il sistema client quale si presenta ai votanti è conforme, ad eccezione dei requisiti posti a forme di comunicazione alternative nel capitolo 2.4, alla norma di accessibilità eCH-0059[13]. I Cantoni provvedono affinché questo sia attestato da un servizio specializzato in materia.

25.8 Tolleranza agli errori

25.8.1 La tolleranza agli errori permette la prosecuzione dell'esercizio in condizioni eccezionali.

25.8.2 Gli errori sono rilevati e trattati affinché il programma possa continuare a funzionare senza interruzioni.

25.8.3 Il trattamento degli errori, inclusa la registrazione nel protocollo, avviene al livello più pertinente per la prosecuzione dell'esercizio. Un errore che non può essere trattato a un dato livello è trasferito al livello immediatamente superiore.

25.8.4 Per i parametri di entrata sono definite condizioni di validità.

25.8.5 Tutti i parametri di entrata sono verificati prima che inizi il trattamento.

25.9 Modularità

25.9.1 Per modularità si intende la proprietà del software di fornire una struttura di moduli altamente indipendenti.

13 eCH-0059: Accessibility Standard Version 3.0 del 25.06.2020; la norma è ottenibile e scaricabile gratuitamente presso: Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich, www.ech.ch.

25.9.2 Il compito dei singoli moduli è definito in modo chiaro.

25.9.3 Il compito dei singoli moduli dovrebbe essere ristretto e mirato. Gli obiettivi di due moduli non dovrebbero accavallarsi.

25.9.4 I moduli non condividono dati attraverso una memoria volatile comune (p. es. variabile globale).

25.10 Semplicità

25.10.1 Per semplicità si intende l'implementazione delle funzioni nel modo più comprensibile possibile. In generale, si tratta di evitare le pratiche che aumentano la complessità.

25.10.2 Nella concezione è applicato un approccio top-down (struttura gerarchica).

25.10.3 La concezione non prevede alcuna duplicazione di funzioni fra i moduli.

25.10.4 La concezione non prevede dati globali, ossia dati che possono essere utilizzati da tutti senza essere passati quali parametri.

25.10.5 Nel codice sorgente sono evitate per quanto possibile complicate combinazioni booleane.

25.10.6 Nel codice sorgente nessuna variabile viene riutilizzata per scopi diversi da quelli inizialmente previsti.

25.10.7 Nel codice sorgente il numero di imbricazioni è il più possibile limitato.

25.10.8 La complessità ciclomatica e cognitiva nel codice sorgente è il più possibile limitata.

25.11 Concisione

25.11.1 Per concisione si intende la situazione in cui una funzione può essere implementata nel codice sorgente con un minimo di istruzioni.

25.11.2 Il software non contiene alcun codice morto («dead code») nel codice sorgente.

25.11.3 Il codice sorgente non contiene alcuna variabile inutile.

25.11.4 Il codice sorgente non dovrebbe contenere alcuna ripetizione.

25.12 Intelligibilità

25.12.1 Per intelligibilità si intende la capacità del destinatario di riconoscere gli obiettivi, le ipotesi, le limitazioni, gli input e gli output, le componenti e lo stato del software.

25.12.2 Nel codice sorgente le classi, le funzioni e i passi di elaborazione complessi vengono commentati secondo una convenzione stabilita dallo sviluppatore software.

25.12.3 Le variabili e le funzioni sono designate con nomi significativi.

25.12.4 Un'istruzione dovrebbe comprendere un'unica linea, a meno che la leggibilità sia migliore con la ripartizione su più linee. È da evitare la presenza di più istruzioni su una linea sola.

25.13 Strumentazione

25.13.1 Per strumentazione si intende la proprietà del software di permettere di misurare la sua utilizzazione o di identificare gli errori.

25.13.2 I test unitari[14] coprono tutti i percorsi possibili e i limiti tra valori ammessi e non ammessi dei parametri d'entrata.

25.13.3 I test d'integrazione coprono tutti i moduli.

25.13.4 Gli scenari di test del software coprono tutti i moduli.

25.13.5 Gli errori e le informazioni necessarie sono protocollati nei log.

26. Criteri di verifica dei sistemi e del loro esercizio

26.1 Verifica del protocollo crittografico (art. 10 cpv. 1 lett. a)

26.1.1 Oggetto: si verifica:

- se i requisiti elencati nell'articolo 5 in combinato disposto con gli articoli 6–8 e il numero 2 dell'allegato sono adempiuti; questa valutazione avviene in particolare sulla base di note di conformità crittografiche e simboliche;
- se e fino a che punto il protocollo crittografico si basa su protocolli ed elementi esistenti e comprovati;
- quali approfondimenti e miglioramenti potrebbero contribuire a rafforzare la sicurezza.

26.1.2 Competenze: la verifica viene svolta da esperti in crittografia. La Cancelleria federale commissiona la verifica e controlla che sia svolta conformemente al mandato.

26.1.3 Momento della verifica:

- una verifica completa avviene precedentemente alla prima messa in esercizio;
- la verifica viene di nuovo eseguita dopo 2–3 anni;
- la verifica avviene di nuovo in occasione di ogni modifica del protocollo crittografico e in seguito all'acquisizione di nuove significative conoscenze della ricerca relative alla sicurezza degli elementi crittografici impiegati e alla situazione di minaccia.

26.2 Verifica del software del sistema (art. 10 cpv. 1 lett. b)

26.2.1 Oggetto: si verifica:

14 In un test unitario, lo sviluppatore testa un modulo indipendentemente dal resto del programma per assicurarsi che il modulo soddisfi le specifiche funzionali e funzioni correttamente in tutte le circostanze. Questa verifica è considerata essenziale per le applicazioni critiche.

- se il protocollo crittografico verificato secondo il numero 26.1 è attuato; la corretta attuazione di funzioni di componenti affidabili è verificata in modo particolarmente accurato;
- se il software del sistema adempie i requisiti della presente ordinanza, e sostiene adeguatamente gli obiettivi predefiniti;
- se il sistema client quale si presenta ai votanti è conforme alla norma eCH-0059 secondo il numero 25.7.3; la verifica può basarsi su un certificato valido emesso o un rapporto d'esame allestito da un'istituzione riconosciuta dalla Cancelleria federale che attesta la conformità con la norma.

26.2.2 Competenze: la verifica viene svolta da esperti in crittografia e nello sviluppo di software. La verifica viene commissionata dalla Cancelleria federale.

26.2.3 Momento della verifica:

- una verifica completa avviene precedentemente alla prima messa in esercizio;
- la verifica viene di nuovo eseguita dopo 2–3 anni;
- la verifica avviene di nuovo in occasione di ogni modifica significativa, in particolare:
  - dopo ogni modifica del protocollo crittografico,
  - a ogni modifica, apportata al codice sorgente, delle funzioni la cui affidabilità è determinante per la validità delle note di conferma previste nell'ambito della verificabilità,
  - in caso di acquisizione di nuovi significativi dati della ricerca riguardanti la sicurezza degli elementi crittografici utilizzati e le situazioni di minaccia,
  - in caso di rinuncia o di adeguamenti significativi a meccanismi che servono all'impiego sicuro di componenti affidabili secondo il numero 2.

26.3 Verifica della sicurezza dell'infrastruttura e dell'esercizio (art. 10 cpv. 1 lett. c)

26.3.1 Oggetto: si verifica se:

- il sistema e il suo esercizio presso il Cantone, il gestore del sistema e la tipografia adempiono i requisiti della presente ordinanza e sostengono adeguatamente gli obiettivi predefiniti;
- 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 dimostrano di soddisfare i migliori standard.

26.3.2 Competenze: la verifica viene svolta da esperti in crittografia e nell'esercizio di sistemi altamente sicuri. La verifica viene commissionata dalla Cancelleria federale.

26.3.3 Momento della verifica:

- una verifica completa viene svolta precedentemente alla prima messa in esercizio;

- la verifica viene di nuovo eseguita dopo 2–3 anni;
- la verifica viene eseguita di nuovo in caso di modifiche significative, in particolare:
  - dopo una modifica del protocollo crittografico,
  - in caso di rinuncia o di adeguamenti significativi a meccanismi che servono all'impiego sicuro di componenti affidabili secondo il numero 2,
  - in caso di un adeguamento significativo dei processi o dell'infrastruttura;
- se vengono impiegate nuove versioni di componenti di base (nuovi server, patch riguardanti il sistema operativo o software che servono all'impiego sicuro e indipendente di componenti secondo il numero 2), non deve esser svolto alcun nuovo controllo se è ancora possibile dimostrare che le componenti corrispondono ai migliori standard.

26.4 Verifica della protezione da tentativi di introdursi nell'infrastruttura (art. 10 cpv. 1 lett. d)

26.4.1 Oggetto: si verifica se gli esperti incaricati dalla Cancelleria federale riescono, nell'ambito di un test, a introdursi nell'infrastruttura del sistema on line e ad avere accesso a dati importanti o ad assumere il controllo su funzioni importanti.

I test sono effettuati sulla base delle potenziali vulnerabilità, individuate a seguito di un'analisi metodica della documentazione disponibile al pubblico, in particolare conformemente all'articolo 11.

26.4.2 Competenze: la verifica viene svolta da esperti in sicurezza. Essa viene commissionata dalla Cancelleria federale.

26.4.3 Momento della verifica:

- una verifica completa avviene precedentemente alla prima messa in esercizio;
- la verifica viene di nuovo eseguita dopo 2–3 anni;
- la verifica viene eseguita di nuovo in caso di ogni modifica significativa dell'infrastruttura.
- la verifica ha luogo in caso di acquisizione di nuove significative informazioni riguardanti la sicurezza degli strumenti utilizzati e le situazioni di minaccia.

26.5 Verifica del sistema di gestione di sicurezza dell'informazione (art. 10 cpv. 2)

26.5.1 Oggetto: si verifica se l'ISMS del gestore del sistema è conforme alla norma ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements. Il campo di applicazione dell'ISMS comprende tutte le unità organizzative del gestore del sistema responsabili sotto il profilo giuridico, amministrativo e operativo per il sistema.

26.5.2 Competenze: l'organismo di certificazione è accreditato dal Servizio di accreditamento svizzero per eseguire audit ai sensi della norma ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements. La verifica è commissionata dal Cantone o dal gestore del sistema; il Cantone provvede allo svolgimento della verifica.

26.5.3 Durata di validità di un attestato: gli audit di ripetizione sono svolti negli intervalli stabiliti dalla norma ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements. A ogni impiego è presentato un certificato valido e il relativo «Statement of Applicability». Se viene pubblicata una nuova versione dello standard ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements, al più tardi dopo la scadenza del termine transitorio deve essere presentata la prova di 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.