



White paper sulla sovranità digitale

Sfruttare l'innovazione e
mantenere il controllo



Indice

Sovranità digitale: una questione chiave del nostro tempo	3
La sovranità digitale al vaglio dell'esperto: intervista al Prof. Dr. Matthias Stürmer	6
Leve importanti per la sovranità digitale: salvataggio e cifratura dei dati	8
La sovranità digitale al vaglio dell'esperto: intervista a David Rosenthal	11
Conclusione: la sovranità risiede nel mantenere la capacità di agire	12

Sovranità digitale: una questione chiave del nostro tempo

Le tecnologie digitali caratterizzano quasi tutti gli ambiti della vita e dell'economia. Le attività dello Stato, la creazione di valore economico e la quotidianità sociale si basano sulle infrastrutture digitali. Al tempo stesso, il mercato tecnologico globale è dominato da pochi grandi fornitori, i quali promuovono le innovazioni, ma creano anche dipendenze. Per questo la sovranità digitale è sempre più al centro dell'attenzione.

Una cosa è chiara: le possibilità digitali sono ormai indispensabili per le aziende e la società. Anche la rinuncia completa a soluzioni estere non è realistica né efficace nel mercato globalizzato.

Il presente white paper pone quindi la questione dell'equilibrio: in che modo autorità, aziende e organizzazioni possono trarre vantaggio dall'innovazione mantenendo al contempo il controllo dei propri dati, sistemi e risorse digitali? In altre parole, come si fa a raggiungere la sovranità digitale in un mondo globalizzato e interconnesso?

Swiss Post Digital – Per una Svizzera digitale forte

Per la Posta sovranità digitale significa sfruttare l'innovazione mantenendo al contempo il controllo su dati, sicurezza e processi critici. È fondamentale che le organizzazioni comprendano i propri rischi, gestiscano consapevolmente le dipendenze e mantengano sempre la capacità di agire. La Posta offre varie soluzioni per una comunicazione digitale sicura, soluzioni software collegabili e servizi di cibersicurezza. Architetture di soluzione aperte, protezione dei dati e metodi di cifratura all'avanguardia garantiscono la sovranità digitale delle soluzioni della Posta.

Inoltre, la Posta si impegna nella rete «SDS – Svizzera digitale sovrana», sia nel comitato consultivo sia all'interno della rete, per promuovere lo scambio e contribuire a plasmare la sovranità digitale in Svizzera.



Dalla parola chiave a una definizione orientata alla pratica

Non esiste ancora una definizione unitaria di sovranità digitale. A seconda della prospettiva, essa comprende aspettative diverse in termini di tecnologia, dati e infrastruttura. Tutti concordano sul fatto che la sovranità digitale descrive la capacità di utilizzare le tecnologie digitali in modo autonomo e di mantenere il controllo su dati, sistemi e processi digitali.

Il Consiglio federale definisce la sovranità digitale come segue: «La sovranità digitale significa disporre, come Stato, della capacità di controllo e di agire necessaria nello spazio digitale per garantire l'adempimento dei compiti statali»¹

Scoprite nel white paper altre soluzioni concrete per una digitalizzazione efficiente e sicura.

IncaMail

IncaMail è il servizio di codifica delle e-mail sicuro della Posta. Con IncaMail aziende, autorità privati possono inviare per e-mail informazioni e documenti confidenziali in modo codificato, tracciabile e conforme alla protezione dei dati (conforme alla LPD e al RGPD).



- L'infrastruttura utilizzata per tutte le attività di ricezione e inoltro di IncaMail ai destinatari è gestita in Svizzera.
- Il portale clienti, tramite il quale è possibile consultare IncaMail anche online, è ospitato nel cloud. Tuttavia, i dati non vengono gestiti nel cloud. Ogni richiesta avviene tramite l'infrastruttura locale cifrata.



¹ Consiglio federale (2025): sovranità digitale della Svizzera. Rapporto del Consiglio federale in adempimento del postulato Z'graggen 22.4411 «Sovranità digitale della Svizzera», Berna, 26 novembre 2025, capitolo 5.1 Definizione.

Quattro principi a sostegno della sovranità digitale

Con architetture di soluzione aperte, le organizzazioni possono evitare dipendenze per mantenere sempre la capacità di agire. Le istruzioni operative sono costituite da quattro principi:

1 Identificare i dati critici

I dati dovrebbero essere classificati in base alla necessità di protezione e ai requisiti normativi. Non tutte le informazioni necessitano delle stesse misure di protezione. Soprattutto per l'utilizzo di servizi cloud è fondamentale un'analisi differenziata.

2 Proteggere efficacemente i dati

Una codifica forte, una gestione delle chiavi propria, architetture zero trust e piani di accesso e autorizzazione chiari costituiscono la base per la protezione dei dati.

3 Creare alternative

Chi pianifica scenari di uscita, riduce le dipendenze da singoli fornitori e punta su interfacce aperte e standard, mantiene la capacità di agire.

4 Rafforzare le competenze all'interno dell'azienda

La sovranità digitale non nasce solo dalla tecnologia. È fondamentale avvalersi di membri del personale e di dirigenti che comprendono le opportunità, i rischi e le dipendenze e sono in grado di prendere decisioni fondate.

La Lettera digitale



La Posta mette a disposizione un'infrastruttura per l'invio e la ricezione di lettere in formato digitale, portando così il segreto epistolare nell'era digitale. Dal 2026 la Lettera digitale fa parte del mandato di servizio universale della Posta.

- La Lettera digitale viene elaborata in Svizzera. La moderna infrastruttura cloud garantisce l'elaborazione sicura di grandi volumi di invii e un'elevata protezione contro i rischi informatici. Grazie a una gestione delle chiavi separata, il fornitore cloud non ha accesso ai contenuti delle lettere.
- Una volta recapitata, la lettera può essere letta solo dalla destinataria o dal destinatario. Né la Posta né terzi hanno la possibilità di accedere al contenuto della lettera.
- La piattaforma soddisfa le disposizioni dell'Ordinanza sulle poste, è stata sottoposta a una valutazione d'impatto sulla protezione dei dati da parte dell'IFPDT e verificata dalla PostCom.

La sovranità digitale al vaglio dell'esperto:

intervista al Prof. Dr. Matthias Stürmer

Due esperti, due prospettive: il Prof. Dr. Matthias Stürmer e David Rosenthal inquadrano e condividono il loro punto di vista su opportunità, rischi e opzioni d'intervento. Leggete l'intervista a Matthias Stürmer qui sotto, quella con David Rosenthal a pagina 11.

Signor Stürmer, chi critica dice che la sovranità assomiglia a un isolamento. Dove finisce la sovranità e dove inizia l'autarchia?

Viviamo in una società interconnessa e non sarebbe né sensato né realistico voler produrre o gestire tutto autonomamente. Sovranità digitale non significa isolamento, ma indipendenza e libertà di decisione. In concreto, è importante la flessibilità dei fornitori, perché in ultima analisi porta a maggiori competitività e innovazione. In Svizzera e in generale nel settore informatico dobbiamo recuperare molto terreno. Un cambiamento è possibile solo se lo affrontiamo concretamente.

Quali domande dovrebbero porsi oggi le autorità e le organizzazioni?

Una domanda centrale è: come possiamo ridurre la dipendenza dalle aziende IT, il cosiddetto «vendor lock-in»? Iniziando dalle informazioni sul mercato svizzero dei fornitori di servizi IT. Un pregiudizio comune è che solo i noti fornitori IT americani offrano i servizi cloud richiesti. Tuttavia, se ci guardiamo intorno, possiamo constatare che anche in Svizzera abbiamo molte aziende IT competenti e innovative.

Molto spesso ci si chiede se gli hyperscaler sono meglio di altri quando si parla di ciber-sicurezza. Cosa ne pensa?

Senza dubbio i grandi fornitori hanno a disposizione più risorse. Al contempo, però, rappresentano anche un obiettivo di attacco più allettante.

«Sovranità digitale non significa isolamento, ma libertà di decisione»

Se un attacco va a buon fine, è probabile che siano coinvolti molti dati. La cibersicurezza non è un argomento a favore o contro un fornitore: è un compito permanente per tutti. In fin dei conti, autorità, aziende e piccoli fornitori lavorano allo stesso obiettivo.

Quando si tratta di sovranità digitale, gli altri Paesi sono più avanti della Svizzera?

Sì. Da anni la Germania investe in modo mirato in soluzioni cloud indipendenti e software open source, e con ZenDiS ha creato un proprio centro per la sovranità digitale che offre openDesk come alternativa a M365. Anche la Francia persegue con «La Suite» un approccio statale coraggioso per mettere in atto concretamente la sovranità digitale. In Svizzera si continua spesso a sostenere che solo i grandi gruppi big tech siano in grado di fornire servizi IT di qualità.

Cosa deve fare concretamente la Svizzera nei prossimi tre anni per aumentare la propria sovranità digitale?

Abbiamo bisogno di un centro nazionale per la sovranità digitale, un organismo che riunisca le conoscenze specialistiche, fornisca consulenza alle autorità e assicuri il trasferimento del

know-how. Con la fondazione del centro SDS – Svizzera digitale sovrana abbiamo compiuto un primo passo presso la BFH. Il fabbisogno è enorme: ogni giorno ricevo richieste da amministrazione, politica e organizzazioni. La pressione politica sta crescendo sensibilmente, da sinistra a destra. Ora sono necessari investimenti nelle basi e un'attuazione coordinata.



Il nostro esperto:

il Prof. Dr. Matthias Stürmer è direttore dell'istituto Public Sector Transformation della Scuola universitaria professionale di Berna (BFH) e docente presso l'Istituto di informatica dell'Università di Berna. È considerato uno dei più noti esperti svizzeri in materia di sovranità digitale, open source e digitalizzazione dello Stato e della società.

Tresorit SecureCloud

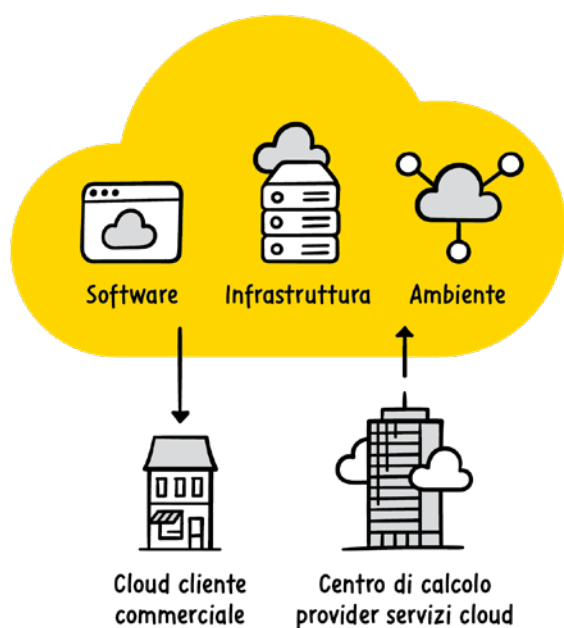


Come elemento costitutivo della sovranità digitale, la sovranità dei dati si manifesta soprattutto laddove i dati vengono condivisi ed elaborati congiuntamente. Che si tratti della collaborazione con team, clienti e partner o dello scambio sicuro di documenti sensibili, con soluzioni come Tresorit SecureCloud, le aziende possono gestire la collaborazione digitale in modo sicuro ed efficiente, mantenendo al contempo la sovranità sui propri dati, diritti di accesso e luoghi di archiviazione.

- La crittografia end-to-end garantisce che solo le persone autorizzate possano accedere ai contenuti. L'architettura zero knowledge assicura che le aziende mantengano il controllo sulle proprie chiavi crittografiche.
- Affinché le aziende possano adempiere ai propri requisiti regolatori e organizzativi individuali, sono disponibili opzioni flessibili per la residenza dei dati nell'UE, in Svizzera e in altre regioni.

Leve importanti per la sovranità digitale: salvataggio e cifratura dei dati

Piattaforme digitali, analisi dei dati e intelligenza artificiale: lo sviluppo e la gestione di soluzioni digitali richiedono infrastrutture efficienti. Tramite i servizi cloud le organizzazioni possono acquistare in modo flessibile potenza di calcolo, spazio di memoria e software come servizi. In questo modo hanno accesso alle tecnologie più moderne, possono implementare le innovazioni più velocemente e adattarne l'utilizzo in base alle esigenze.



Civetica Cloud



Civetica è la piattaforma eGovernment della Posta che riunisce i processi amministrativi comunali in un ambiente unitario, sicuro e controllato. Sostituisce soluzioni individuali isolate con una soluzione globale integrata. Circa il 20% dei Comuni svizzeri si affida alla soluzione ERP Civetica.

- Civetica Cloud salva i dati esclusivamente in centri di calcolo in Svizzera.
- La soluzione garantisce una localizzazione controllata dei dati e un approccio in linea con i requisiti di sovranità delle organizzazioni svizzere.

I cloud non sono tutti uguali

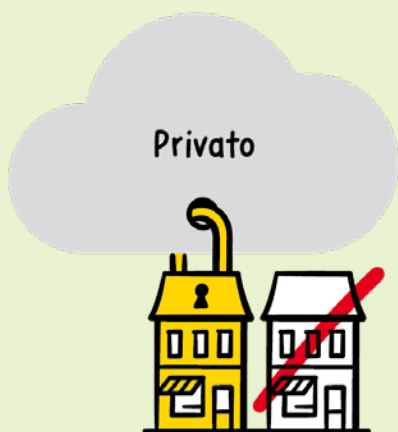
In relazione ai servizi cloud e alla sovranità digitale è fondamentale chiedersi: chi può accedere all'infrastruttura cloud e in che modo sono protetti i dati in essa contenuti?

A seconda dei requisiti e delle condizioni quadro normative, si consigliano ambienti cloud diversi. Anche la cifratura dei dati e la gestione delle chiavi sono fondamentali.

Quali servizi cloud esistono?

Privato

Un ambiente cloud dedicato che viene utilizzato da una sola organizzazione. Può essere gestito presso un centro di calcolo di proprietà oppure da un offerente terzo esterno e offre un livello di controllo e di sicurezza elevato.



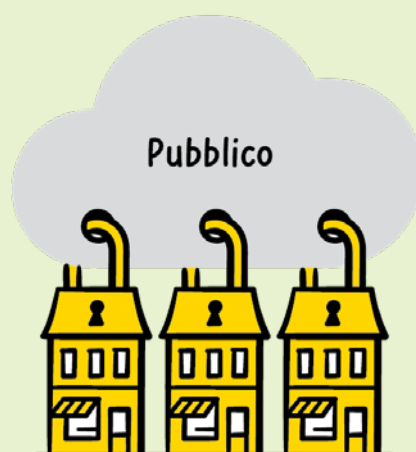
Forma mista

Combinazione di cloud pubblico e privato, in cui dati e applicazioni possono essere migrati tra entrambi gli ambienti a seconda delle esigenze.



Pubblico

Le risorse IT vengono messe a disposizione da un offerente terzo esterno tramite l'internet pubblico e utilizzate congiuntamente da più clienti.



Sicurezza per i vostri dati

Il fornitore può visualizzare i dati salvati nel cloud? Se i dati sensibili vengono elaborati in un ambiente cloud, le misure organizzative e tecniche dovrebbero garantire che solo gli organismi autorizzati possano accedere ai dati. Il fornitore cloud può essere esplicitamente escluso dall'accesso mediante una gestione delle chiavi separata.

Le seguenti misure proteggono i dati e i servizi nel cloud:

- **Gestione delle chiavi interna:** l'organizzazione gestisce autonomamente le chiavi di codifica e mantiene quindi il controllo sull'accesso ai dati.
- **Cifratura dei dati:** i dati rimangono protetti durante il salvataggio e la trasmissione e non sono leggibili da terzi.
- **Concetti di accesso e autorizzazione:** solo le persone autorizzate possono accedere a sistemi e informazioni.
- **Valutazioni del rischio e verifiche di sicurezza continue:** assessment periodici garantiscono il rispetto dei requisiti di sicurezza, protezione dei dati e compliance.

Sovranità con un fornitore di servizi cloud globale?

Le grandi aziende globali svolgono un ruolo centrale nel mercato del cloud. Gestiscono infrastrutture distribuite in tutto il mondo e fanno ogni anno ingenti investimenti in sicurezza, sviluppo e innovazione tecnologica. In questo modo assicurano un accesso rapido a tecnologie moderne, un'elevata disponibilità e un utilizzo efficiente ed economico delle risorse IT.

Se le organizzazioni intendono sfruttare questi vantaggi garantendo comunque l'indipendenza dei propri servizi e la protezione dei loro dati, dovrebbero scegliere l'ambiente cloud in modo consapevole:

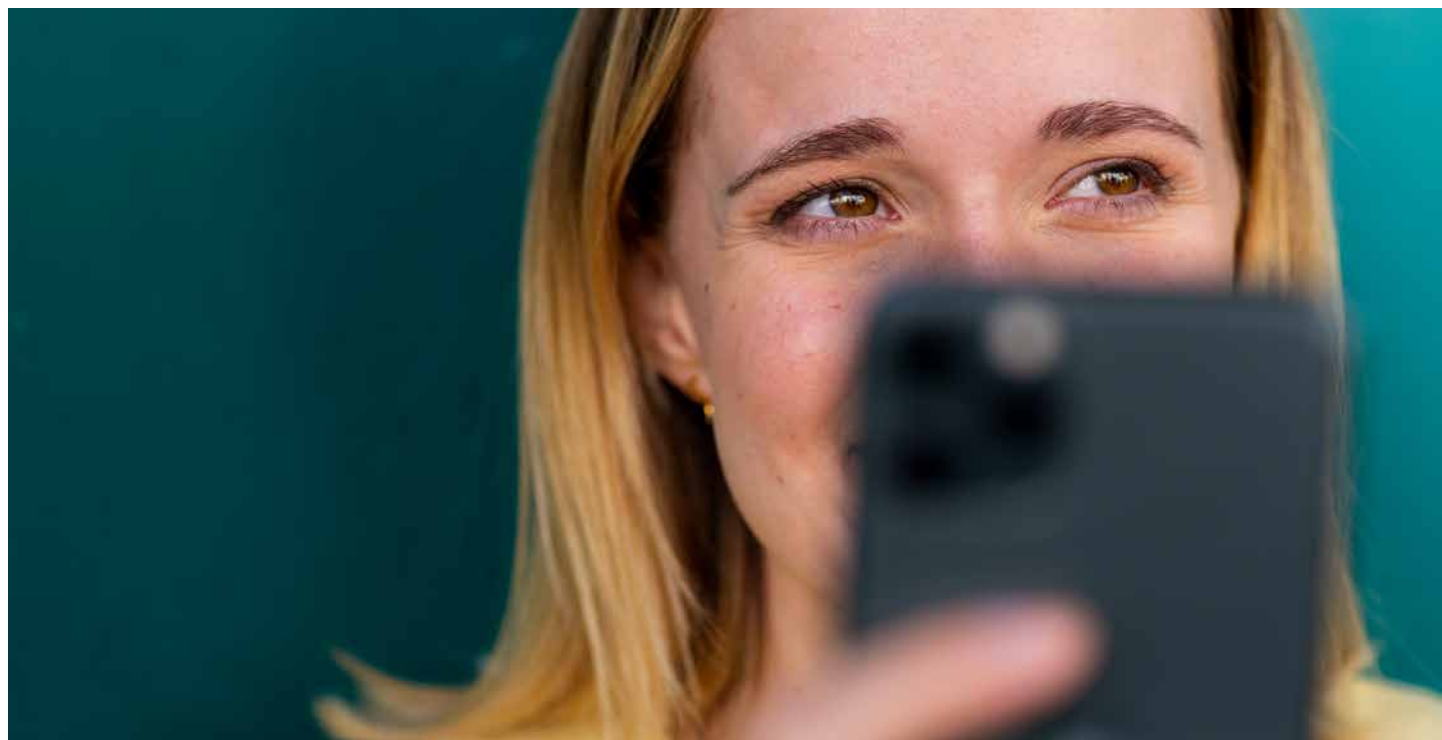
- Scegliere l'ambiente cloud: cloud privato, cloud pubblico, forma mista
- Definire un concetto di accesso e codifica e garantire una verifica di sicurezza e una valutazione del rischio continue

Certificati TLS



I certificati TLS (Transport Layer Security) confermano l'identità e l'autenticità di siti web (domini) e organizzazioni e assicurano la trasmissione cifrata di dati tra utenti e servizi online. In quanto parte integrante fondamentale di un'infrastruttura sicura, costituiscono la base per la fiducia in internet e nella comunicazione digitale. Il Trust Service Provider SwissSign, unico fornitore svizzero di certificati TLS, contribuisce a mantenere un ecosistema digitale affidabile.

- L'infrastruttura fiduciaria è gestita in Svizzera da SwissSign ed è controllata dal provider stesso in centri di calcolo geograficamente ridondanti.
- Con questo prodotto le organizzazioni possono utilizzare certificati TLS riconosciuti a livello internazionale, mentre governance, controllo e competenza giuridica restano in Svizzera.



La sovranità digitale al vaglio dell'esperto:

intervista a David Rosenthal

Signor Rosenthal, molti mettono in guardia dalle dipendenze da fornitori cloud statunitensi. Secondo lei, questo rischio viene sopravvalutato o sottovalutato?

Viene interpretato in modo errato. La maggior parte delle persone teme la dipendenza perché i fornitori risiedono negli Stati Uniti. Secondo me il problema principale è rappresentato dalla posizione dominante sul mercato e dai rischi di accumulazione. Nell'IT le dipendenze sono sempre esistite e non sono mai state positive, ma sono state anche inevitabili. Non esistono formule magiche.

Lo US CLOUD ACT è spesso al centro del dibattito: quanto è reale nella pratica il rischio di un accesso ai dati svizzeri?

Questo è un pericolo che viene sopravvalutato. In primo luogo, il CLOUD Act non è niente di particolare, lo abbiamo praticamente anche in Svizzera. In secondo luogo esistono contromisure anche senza codifica end-to-end; purtroppo alcuni ammonitori ignorano sistematicamente questo aspetto. Infine, anche senza CLOUD Act le autorità statunitensi ricevono dati dalla Svizzera, e in modo del tutto legale tramite l'assistenza giudiziaria. L'abitudine di concentrarsi eccessivamente sul CLOUD Act distoglie l'attenzione da rischi molto più grandi, come ad esempio il pericolo rappresentato dagli hacker: in molti casi vi è una grande reticenza nei confronti delle soluzioni cloud e quindi i nostri dati rimangono sui nostri server, dove spesso la protezione lascia molto a desiderare.

Da cosa si riconosce che la sovranità di un'organizzazione è adeguata e dove iniziano le criticità della dipendenza?

Dispone di un piano B o addirittura di un piano C, nel caso in cui un fornitore dovesse fallire o si dovesse rinunciare ai suoi servizi? Esistono

«L'abitudine di concentrarsi eccessivamente sul CLOUD Act distoglie l'attenzione da rischi notevolmente maggiori»

soluzioni di ripiego? E in caso affermativo, dove? Ha distribuito consapevolmente i componenti della sua soluzione IT tra fornitori diversi, non puntando quindi tutto sullo stesso cavallo? Dispone di un know-how interno sufficiente a comprendere e attuare le sue opzioni? Preferisco quindi parlare di resilienza digitale piuttosto che di sovranità digitale.

Quali fraintendimenti le capita di incontrare più spesso nel dibattito pubblico?

Che gli Stati Uniti hanno libero accesso ai nostri dati quando si utilizzano provider cloud statunitensi.



Il nostro esperto:

David Rosenthal è uno dei principali esperti svizzeri di diritto dei dati e della tecnologia. È partner di VISCHER e fornisce consulenza ad aziende e autorità in materia di protezione dei dati, IT e diritto IA.

Conclusione: la sovranità risiede nel mantenere la capacità di agire

Sovranità digitale significa strutturare in modo consapevole l'impiego delle tecnologie digitali, gestire i rischi e mantenere la capacità di agire anche in un mondo interconnesso. Chi conosce i propri dati, comprende le dipendenze e ha alternative tecnologiche può sfruttare l'innovazione senza perdere il controllo:

- 1** Le organizzazioni di successo combinano diverse tecnologie e modelli operativi in base ai propri requisiti e alle disposizioni di legge.
- 2** In casi particolari o se la gestione dei dati è sancita dalla legge, possono essere utili infrastrutture locali o modelli operativi speciali per i dati degni di particolare protezione.
- 3** Per le applicazioni standardizzate le piattaforme cloud offrono spesso vantaggi decisivi in termini di innovazione ed efficienza.
- 4** I componenti open source possono inoltre contribuire ad aumentare la trasparenza e a ridurre le dipendenze.

La sovranità digitale è garantita laddove le organizzazioni comprendono le proprie dipendenze tecnologiche, gestiscono attivamente i rischi e mantengono sempre la propria capacità di agire. Proprio questa gestione consapevole e differenziata della tecnologia costituisce la base della sovranità digitale.

Voto elettronico



Il sistema di voto elettronico della Posta consente di votare per via elettronica in modo sicuro. Speciali misure tecniche di sicurezza e crittografiche garantiscono la segretezza del voto e, al contempo, consentono di verificare la presenza di manipolazioni durante l'intero scrutinio. Dal 2023 il voto elettronico è utilizzato con successo in diversi Cantoni.

- Il software per il voto elettronico, i server e i dati sono gestiti in Svizzera.
- La Posta mette a disposizione di tutti i principali componenti e documenti del sistema e invita specialisti a verificarlo. Con un cosiddetto programma bug bounty, la Posta offre anche incentivifinanziari per la verifica pubblica e la segnalazione di punti deboli.
- La Posta mette a disposizione parti importanti del codice con una licenza open source libera. In questo modo è possibile utilizzare e sviluppare liberamente le relative parti del codice sorgente.

