Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Il Consiglio federale

Berna, 29 ottobre 2025

# Proteggere il traffico dati dell'Amministrazione federale

## Rapporto del Consiglio federale in adempimento del postulato 23.3958 della Commissione della politica di sicurezza del Consiglio nazionale del 20 giugno 2023

# Indice

# 1 Il postulato

## 1.1 Postulato «Proteggere il traffico dati dell'Amministrazione federale»

Testo depositato: Il Consiglio federale è incaricato di illustrare quali tecnologie possano essere impiegate per proteggere dai ciberattacchi nei settori critici il traffico dati su Internet tra gli uffici dell'Amministrazione federale, tra l'Amministrazione federale e le imprese parastatali, tra l'Amministrazione federale e i Cantoni nonché tra l'Amministrazione federale e il pubblico. Nel rapporto dovrà in particolare esaminare il potenziale delle diverse infrastrutture di comunicazione che consentono di definire geograficamente il flusso di dati e quindi di meglio proteggerlo da attacchi esterni. Infine illustrerà il rapporto tra costi previsti e benefici attesi di queste tecnologie.

Motivazione: La cibersicurezza nelle reti di comunicazione diventa sempre più importante. A preoccupare molto è il forte aumento di attacchi sempre più aggressivi registrato negli ultimi tempi, soprattutto ai danni delle offerte digitali governative.

Per proteggere il traffico dati dagli attacchi le imprese e l'Amministrazione hanno finora comunicato attraverso linee dedicate o reti chiuse. Le linee dedicate proteggono soltanto il traffico dati da punto a punto, ma non il traffico dati su Internet. Anche se su Internet è criptato, il traffico dati rimane comunque esposto e può essere attaccato da terzi in tutto il mondo allo scopo di decriptare o disturbare la comunicazione.

L'obiettivo del rapporto è illustrare quali sono gli approcci disponibili in quest'ambito. Tra l'altro si dovrà porre l'accento anche sullo standard di comunicazione aperto «Scalability, Control and Isolation On Next-Generation Networks (SCION)», sviluppato dal Politecnico federale di Zurigo. Questo standard consente agli utenti della rete, tra l'altro, di controllare il percorso dei propri pacchetti di dati.

L'Amministrazione ha già realizzato progetti pilota con il protocollo SCION. Inoltre, su iniziativa della Banca nazionale svizzera, la piazza finanziaria elvetica ha deciso di sostituire a medio termine l'attuale infrastruttura di rete (FinanceIPNet) con la «Secure Swiss Finance Network (SSFN)», anch'essa basata sulla tecnologia SCION.

Cronologia: Il postulato è stato presentato il 20 giugno 2023 dalla Commissione della politica di sicurezza del Consiglio nazionale. Il 30 agosto 2023 il Consiglio federale ha proposto di accoglierlo. Il Consiglio nazionale lo ha accolto il 27 settembre 2023.

# 2 Situazione iniziale

Gli autori del postulato desiderano sapere quali tecnologie possono essere impiegate per proteggere il traffico dati su Internet dai ciberattacchi. Hanno espressamente chiesto che il rapporto non si limiti alle tecnologie attualmente impiegate nell'Amministrazione federale, ma comprenda anche quelle non ancora impiegate. Inoltre, deve esaminare le infrastrutture di comunicazione che consentono di proteggere il flusso di dati mediante restrizioni geografiche, mettendo in luce il rapporto tra costi e benefici di tali tecnologie. Secondo la motivazione del postulato, si dovrà porre l'accento in particolare sullo standard di comunicazione aperto «Scalability, Control and Isolation On Next-generation Networks (SCION)», sviluppato dal Politecnico federale di Zurigo.

Gli autori del postulato hanno delimitato l'infrastruttura di comunicazione da esaminare, indicando che va considerato esclusivamente il traffico dati su Internet. Nel contesto del presente rapporto, ciò significa che dovranno essere prese in considerazione principalmente le tecnologie che sostengono il traffico dati tramite Internet. La protezione del traffico dati su linee di comunicazione private non rientra direttamente nella richiesta del postulato, ma viene comunque affrontata nel presente rapporto al fine di trasmettere un quadro completo della comunicazione dati dell'Amministrazione federale civile.

## 2.1 Valutazione delle ciberminacce

Le ciberminacce[1] sono diventate parte integrante del panorama delle minacce tanto in Svizzera quanto a livello internazionale. Tali minacce provengono da attori che sono mossi da motivazioni diverse. Il più delle volte, dietro un ciberattacco si cela un intento criminale. Questo genere di attacchi, spesso associati a estorsione o coazione, è utilizzato dagli autori dei reati per cercare di arricchirsi, nonché come mezzo per conseguire finalità politiche. Gli attivisti vi fanno per esempio ricorso per diffondere la propaganda politica. Per raggiungere questi fini compromettono la funzionalità di siti web o interrompono servizi Internet per destabilizzare la popolazione. I ciberattacchi con il maggiore potenziale di danno sono però quelli a fini di spionaggio o sabotaggio. In questi casi, gli autori penetrano nelle reti informatiche e cercano di agire nell'ombra il più a lungo possibile per rubare informazioni o anche preparare attacchi con ripercussioni fisiche. Le diverse ciberminacce sono descritte con maggiore dettaglio nella Ciberstrategia nazionale[2].

[1] La legge sulla sicurezza delle informazioni (LSIn; RS 128) definisce una ciberminaccia, in generale, come «qualsiasi circostanza o evento che ha il potenziale di provocare un ciberincidente», mentre un ciberincidente è descritto come un evento che «compromette la confidenzialità, la disponibilità o l'integrità delle informazioni o la tracciabilità del loro trattamento» (art. 5 lett. d ed f LSIn).
[2] Il Consiglio federale. Ciberstrategia nazionale (CSN), aprile 2023. https://www.ncsc.admin.ch/ncsc/it/home/strategie/cyberstrategie-ncs.html

I metodi e le tattiche utilizzati per i ciberattacchi sono in continua evoluzione. In determinati scenari di attacco (p. es. phishing) si può già osservare che gli autori ricorrono sempre più all'intelligenza artificiale per contattare in modo mirato le possibili vittime e aumentare così la probabilità di ottenere dati di accesso, oppure per rilevare le attività dell'utente sulla base del traffico di rete intercettato. Nei suoi rapporti di situazione semestrali, l'Ufficio federale della cibersicurezza (UFCS) riferisce correntemente sulle ciberminacce attuali e sui nuovi fenomeni[3].

L'Amministrazione federale, come ogni organizzazione, deve proteggersi in linea di principio da tutte le diverse ciberminacce. Vista la natura delle sue attività è particolarmente esposta agli attacchi a sfondo politico. Negli ultimi due anni, nei confronti dell'Amministrazione federale sono fortemente aumentati in particolare gli attacchi da parte di attivisti politici. Nel giugno 2023, in risposta a un discorso di Volodymyr Zelensky al Parlamento, il gruppo di attivisti pro-Russia «NoName057(16)» ha sferrato attacchi distributed-denial-of-service (DDoS) contro l'Amministrazione federale e altri obiettivi. L'UFCS ha descritto il modo di procedere del gruppo e le ripercussioni di tali attacchi in un rapporto specialistico[4]. Attacchi analoghi si sono verificati nel corso del World Economic Forum 2024 e 2025 nonché durante la conferenza di alto livello sulla pace in Ucraina, tenutasi nell'estate del 2024[5]. Pur non avendo arrecato danni a lungo termine né comportato fughe di dati, gli attacchi DDoS hanno comunque causato sconcerto nella popolazione, disagi al personale dell'Amministrazione federale e un onere considerevole per i team addetti alla sicurezza.

L'Amministrazione federale è anche già stata vittima di attacchi di spionaggio, di cui l'esempio più noto è certamente il ciberattacco nei confronti della RUAG scoperto nel 2016[6]. Gli attacchi di questo genere, complessi e mirati, sono molto più rari di quelli sferrati da criminali o attivisti. Al tempo stesso hanno però anche ripercussioni molto più gravi, in quanto possono compromettere direttamente la protezione delle informazioni sensibili.

In un contesto di crescenti tensioni geopolitiche è dunque prevedibile che la minaccia rappresentata dai ciberattacchi all'Amministrazione federale rimanga elevata e continui tendenzialmente a crescere. Questa sfida è ulteriormente complicata dal fatto che l'Amministrazione federale si avvale dei servizi di numerose ditte terze. Poiché ciò implica un frequente scambio di informazioni o la concessione di accessi temporanei ai sistemi della Confederazione, la sicurezza dell'Amministrazione federale potrà essere garantita solo affrontando anche queste dipendenze e interfacce con adeguate misure di sicurezza di natura fisica e organizzativa. A tale scopo, tra l'altro sulla base della sua decisione del 1° maggio 2025,

[3] https://www.ncsc.admin.ch/ncsc/it/home/dokumentation/berichte/lageberichte.html
[4] Rapporto di analisi dettagliata sugli attacchi DDoS «NoName057(16)».
[5] Conferenza di alto livello sulla pace in Ucraina: primo bilancio dell'UFCS sui lavori della Rete integrata della situazione ciber.
[6] Rapporto tecnico sul software nocivo utilizzato nell'attacco cyber contro la RUAG.

il Consiglio federale ha adottato misure per contrastare i potenziali rischi derivanti dagli accessi da parte di ditte terze[7].

## 2.2 Delimitazione secondo il testo del postulato

Il presente rapporto intende illustrare mediante quali tecnologie è possibile proteggere dai ciberattacchi nei settori critici il traffico dati su Internet tra:

- gli uffici dell'Amministrazione federale,
- l'Amministrazione federale e le imprese parastatali,
- l'Amministrazione federale e i Cantoni nonché
- l'Amministrazione federale e il pubblico.

Con il termine ciberattacco si intende qui il tentativo di cibercriminali, hacker o altri autori di minacce digitali di avere accesso dall'esterno a una rete informatica o un sistema, perlopiù con l'obiettivo di modificare, rubare, distruggere, pubblicare informazioni o comprometterne la disponibilità. Il rapporto si limita inoltre ai ciberattacchi rivolti contro il traffico dati su Internet; vengono quindi esaminate esclusivamente le misure tecnologiche intese a proteggere il trasporto dei dati tramite Internet. Misure organizzative e provvedimenti specifici finalizzati a contrastare vettori di attacchi quali malware, phishing, ransomware o attacchi alle password non costituiscono l'oggetto del presente rapporto e non saranno ulteriormente approfonditi. Sono altresì esclusi dal campo d'esame del rapporto gli attacchi alla tecnologia dell'informazione aziendale e industriale. Secondo il testo del postulato, il rapporto si limita ai settori critici nell'ambito delle quattro relazioni di comunicazione summenzionate. In tale contesto sono considerati settori critici le imprese, i sistemi e le organizzazioni il cui attacco (perturbazione, indisponibilità, divulgazione, intercettazione ecc.) potrebbe turbare la sicurezza pubblica o provocare altre gravi conseguenze.

## 2.3 Delimitazione tecnica

Dall'analisi delle attuali infrastrutture di comunicazione e delle esigenze in materia è emerso che non è necessario concentrarsi esclusivamente sui settori critici e che, anzi, una limitazione a tali settori potrebbe ridurre l'efficacia e la rilevanza delle tecnologie impiegate. È dunque più vantaggioso impiegare una tecnologia globale, universalmente applicabile e adattabile, indipendentemente dal fatto che questa sia destinata a proteggere settori critici o meno critici. Un tale approccio assicura una protezione completa e una migliore anticipazione delle sfide a lungo termine.

[7] Ciberattacco contro Xplain: misure volte a evitare future fughe di dati e controllo di sicurezza dopo la sua acquisizione

Il rapporto intende illustrare in che modo il traffico dati via Internet può essere protetto dagli attacchi esterni. La protezione del traffico dati su linee di comunicazione private non rientra direttamente nella richiesta del postulato, ma viene comunque affrontata nel presente rapporto al fine di trasmettere un quadro completo della comunicazione dati dell'Amministrazione federale civile.

Le catene di approvvigionamento nonché le misure fisiche e organizzative per la protezione del traffico dati non sono esaminate nel presente rapporto.

# 3 Attuali tecnologie di comunicazione dell'Amministrazione federale civile

La trasmissione di dati in seno all'Amministrazione federale civile, in particolare tra i servizi dell'Amministrazione federale, tra l'Amministrazione federale e le imprese parastatali, tra l'Amministrazione federale e i Cantoni nonché tra l'Amministrazione federale e il pubblico, avviene mediante diverse tecnologie di connessione. Per proteggere il traffico dati dalle minacce, la trasmissione ha luogo per lo più attraverso linee private dedicate o all'interno di reti chiuse. Per le connessioni in cui ciò non è possibile o sensato, in particolare tra l'Amministrazione federale e il pubblico, si utilizza Internet. Mentre le linee private dedicate e le reti chiuse consentono un'elevata protezione contro le ciberminacce, la trasmissione dei dati e la raggiungibilità dei sistemi tramite la rete Internet pubblica rimangono esposte ai pericoli delle ciberminacce anche con l'adozione di misure supplementari.

## 3.1 Svizzera

La connessione di ubicazioni in Svizzera con la rete di dati dell'Amministrazione federale avviene per lo più tramite linee private dedicate o all'interno di reti chiuse. Si utilizzano infrastrutture della Confederazione o servizi acquistati sul mercato. La trasmissione attraverso infrastrutture federali consente una definizione esatta del flusso di dati, mentre nel caso di servizi acquistati il flusso di dati è determinato dal provider.

Segue una descrizione delle principali tecnologie di connessione impiegate nell'Amministrazione federale per il collegamento di ubicazioni in Svizzera. Senza misure protettive più estese, attraverso queste connessioni è consentito trasmettere informazioni del livello di classificazione AD USO INTERNO[8] e informazioni con un bisogno di protezione limitato. Le informazioni e i dati con un bisogno di protezione più elevato devono essere protetti all'occorrenza con misure integrative.

[8] Informazioni del livello di classificazione AD USO INTERNO secondo l'art. 18 OSIn

### 3.1.1 Connessioni in fibra ottica

Nella regione di Berna si utilizzano connessioni in fibra ottica della Confederazione (fibra ottica spenta, dark fiber) per collegare le ubicazioni alla rete di dati dell'Amministrazione federale. Le connessioni in fibra ottica sono linee passive, dedicate, fisiche e da punto a punto.

#### Caratteristiche principali

| Vantaggi | Svantaggi |
|---|---|
| **Larghezza di banda e latenza:** massima larghezza di banda realizzabile con una latenza minima. È possibile ottenere velocità superiori mediante componenti ottici migliori, senza sostituire la fibra ottica fisica. | **Disponibilità:** la rete in fibra ottica della Confederazione è per lo più limitata alla regione di Berna. Le connessioni in fibra ottica approntate da terzi devono essere valutate caso per caso. |
| **Indipendenza dai protocolli:** trasporto flessibile di diversi protocolli e formati di dati. Nessun carico aggiuntivo dovuto a protocolli di rete supplementari. | **Costi:** necessità di elevati investimenti una tantum nell'infrastruttura fisica. |
| **Isolamento fisico:** ogni connessione in fibra ottica è isolata fisicamente e indipendente da altre connessioni di comunicazione. | **Flessibilità:** la posa di linee in fibra ottica supplementari può essere dispendiosa in termini di tempo e di costi. Piuttosto inadatte per connessioni temporanee. |
| **Controllo dei percorsi fisici:** controllo completo delle connessioni dati end-to-end e dell'accesso fisico alla rete in fibra ottica. | |

Tabella 1: Caratteristiche principali delle connessioni in fibra ottica

#### Rischi intrinseci

**Danni fisici:** in linea di principio, tutte le connessioni via cavo sono esposte al rischio di danni fisici, per esempio causati da eventi (come terremoti, frane, inondazioni e sabotaggi), lavori di costruzione o manipolazione impropria. In particolare, i cavi di fibra ottica sono fragili, possono rompersi e sono più sensibili dei cavi di rame alle influenze fisiche.

**Rischio di intercettazione:** intercettare i flussi di dati attraverso connessioni in fibra ottica è difficile ma comunque possibile con un certo impegno e con tecniche speciali, a condizione che l'autore dell'attacco abbia accesso fisico alla fibra o ai punti terminali.

### 3.1.2 Servizio Ethernet

Per il collegamento di ubicazioni in tutta la Svizzera alla rete di dati dell'Amministrazione federale si acquistano solitamente servizi Ethernet, vale a dire connessioni monitorate, da punto a punto, di livello 2, approntate da un provider.

#### Caratteristiche principali

| Vantaggi | Svantaggi |
|---|---|
| **Disponibilità:** disponibili in tutta la Svizzera. | **Infrastruttura condivisa:** condivisione dell'infrastruttura del provider con altri utenti. I tempi di latenza possono variare. |
| **Flessibilità:** facilmente estendibili. La larghezza di banda può variare a seconda delle esigenze dell'ubicazione. Adatti anche per connessioni temporanee. | **Controllo dei percorsi fisici:** nessun controllo sui flussi di dati all'interno della rete del provider. |
| **Priorizzazione del traffico dati:** sostiene la priorizzazione delle connessioni sulla base di specifiche interne dell'Amministrazione federale. | |
| **Traffico dati trasparente:** indipendente dai livelli superiori (IP e protocolli di trasporto). | |
| **Isolamento logico:** isolamento logico dei flussi di dati mediante separazione delle VLAN. | |
| **Routing:** il controllo del routing rimane nelle mani dell'Amministrazione federale. | |

Tabella 2: Caratteristiche principali dei servizi Ethernet

#### Rischi intrinseci

**Dipendenza dal provider:** l'acquisto di servizi di rete sul mercato comporta inevitabilmente la dipendenza dal provider selezionato. Se da un lato gli accordi sui livelli di servizio (SLA, Service Level Agreements) consentono di disciplinare contrattualmente, per esempio, la disponibilità, la qualità e altre caratteristiche del servizio, dall'altro la fiducia di fondo nel provider selezionato rimane imprescindibile.

**Rischio di intercettazione:** il provider ha in ogni caso la possibilità di analizzare i metadati della comunicazione. Le comunicazioni non criptate possono essere completamente intercettate dal provider.

### 3.1.3 Rete ottica delle autorità federali

La rete ottica delle autorità federali (ROAF) è un servizio di trasporto ottico da punto a punto gestito e monitorato dal Comando Ciber per l'interconnessione dei centri di ricerca civili o tra due ubicazioni utenti, realizzato su connessioni in fibra ottica della Confederazione.

#### Caratteristiche principali

| Vantaggi | Svantaggi |
|---|---|
| **Larghezza di banda e latenza:** sostegno a tassi di trasmissione elevati con una latenza minima. | **Infrastruttura condivisa:** condivisione dell'infrastruttura con altri utenti (autorità). |
| **Disponibilità:** all'occorrenza disponibile in tutta la Svizzera. Nel caso di nuovi siti può richiedere la realizzazione di nuove linee. | **Costi:** necessità di elevati investimenti nell'infrastruttura fisica. |
| **Isolamento logico:** separazione dei flussi di dati mediante multiplazione ottica. Protezione di altri flussi di dati all'interno della stessa infrastruttura mediante isolamento integrato degli errori a livello di connessione. | **Flessibilità:** la posa di linee in fibra ottica supplementari può essere dispendiosa in termini di tempo e di costi. |
| **Controllo dei percorsi fisici:** controllo completo delle connessioni dati e dell'accesso alla rete ottica. | |
| **Crittografia:** ulteriore protezione dei flussi di dati tramite crittografia del livello di collegamento. | |

Tabella 3: Caratteristiche principali della ROAF

#### Rischi intrinseci

**Dipendenza dalla rete in fibra ottica:** la ROAF dipende dalla rete fisica in fibra ottica sottostante ed è quindi esposta agli stessi rischi intrinseci delle connessioni in fibra ottica. Nella ROAF si attuano però misure di attenuazione dei rischi: a) la rete ottica è realizzata con cavi di fibra ottica ridondanti e tracciati separati e b) i dati sono trasmessi criptati.

## 3.2 Estero

La connessione di ubicazioni all'estero con la rete di dati dell'Amministrazione federale ha luogo mediante servizi acquistati sul mercato. Viene realizzato attraverso un un collegamento a una rete globale di un provider internazionale oppure attraverso una connessione via satellite.

Segue una descrizione delle principali tecnologie di connessione impiegate nell'Amministrazione federale per la connessione con ubicazioni all'estero. I collegamenti a livello internazionale sono protetti con firewall aggiuntivi e i dati sono trasmessi criptati.

### 3.2.1 Servizio MPLS (Multiprotocol Label Switching) internazionale

I servizi internazionali di livello 3 basati su MPLS sono servizi acquistati da un provider e utilizzati per connettere ubicazioni all'estero con la rete di dati dell'Amministrazione federale.

#### Caratteristiche principali

| Vantaggi | Svantaggi |
|---|---|
| **Disponibilità:** la portata globale consente di collegare ubicazioni in tutto il mondo. | **Infrastruttura condivisa:** condivisione dell'infrastruttura con altri utenti. |
| **Isolamento logico:** separazione dei flussi di dati mediante MPLS. | **Flessibilità:** la creazione di nuove connessioni è complessa e comporta un notevole dispendio di tempo. Per apportare modifiche o ampliamenti è necessario il sostegno del provider. |
| **Crittografia:** ulteriore protezione dei flussi di dati tramite crittografia da parte dell'Amministrazione federale. Il materiale criptato ricade sotto la sovranità dell'Amministrazione federale. | **Controllo dei percorsi fisici:** nessun controllo sui flussi di dati all'interno della rete del provider. |
| | **Routing:** il routing non è completamente sotto il controllo dell'Amministrazione federale. |

Tabella 4: Caratteristiche principali dei servizi MPLS

#### Rischi intrinseci

**Dipendenza dal provider:** il ricorso a servizi acquistati sul mercato comporta la dipendenza dal provider selezionato.

**Situazione giuridica all'estero:** i flussi di dati end-to-end possono passare attraverso diversi Paesi, i quali non sono assoggettati al diritto svizzero. La disponibilità delle infrastrutture di comunicazione estere può dipendere dagli eventi politici.

**Rischio di intercettazione:** il provider ha in ogni caso la possibilità di analizzare i metadati della comunicazione; i flussi di dati possono essere monitorati dai governi stranieri. Le comunicazioni non criptate possono essere completamente intercettate dal provider.

### 3.2.2 Connessioni via satellite

Le connessioni via satellite sono servizi acquistati da un provider, utilizzati per connettere ubicazioni all'estero con la rete di dati dell'Amministrazione federale.

#### Caratteristiche principali

| Vantaggi | Svantaggi |
|---|---|
| **Disponibilità:** copertura globale. Disponibile anche in zone remote e difficili da raggiungere. | **Infrastruttura condivisa:** l'infrastruttura di comunicazione e la larghezza di banda sono condivise tra numerosi utenti. I bit rate disponibili dipendono dall'ubicazione e dal grado di sfruttamento della connessione via satellite. |
| **Flessibilità:** indipendente dall'infrastruttura terrestre. Adatto per casi d'emergenza o impieghi temporanei. Le connessioni possono essere stabilite senza una dispendiosa installazione di infrastrutture. | **Latenza:** i ritardi del segnale possono compromettere la comunicazione. Ciò risulta particolarmente problematico per le applicazioni in tempo reale. I tempi di latenza potrebbero essere migliorati con satelliti LEO (Low Earth Orbit) di nuova generazione. |
| **Crittografia:** ulteriore protezione dei flussi di dati tramite crittografia da parte dell'Amministrazione federale. Il materiale criptato ricade sotto la sovranità dell'Amministrazione federale. | **Sensibilità alle condizioni meteorologiche:** possono verificarsi perturbazioni dovute a pioggia, neve o nubi (rain fade). Segnali vicini, interferenze solari e disturbi elettromagnetici possono compromettere una connessione. |
| | **Controllo dei percorsi fisici:** nessun controllo sui flussi di dati all'interno della rete del provider. |

Tabella 5: Caratteristiche principali delle connessioni via satellite

#### Rischi intrinseci

**Rischio di intercettazione:** le connessioni via satellite utilizzano segnali radio per la trasmissione dei dati. Questi segnali sono di per sé intercettabili e possono essere captati con un onere relativamente contenuto.

## 3.3 Internet

Le applicazioni del personale dell'Amministrazione federale per il telelavoro, la comunicazione con il pubblico, i collegamenti tra ubicazioni in Svizzera e all'estero e il collegamento di reti

partner possono avvenire attraverso la rete Internet pubblica. La trasmissione dei dati può avere luogo in modo criptato ed essere ulteriormente protetta, per esempio, con IPSEC VPN.

In particolare, la rete Internet pubblica è utilizzata per la comunicazione tra l'Amministrazione federale e gli utenti in telelavoro nonché tra l'Amministrazione federale e il pubblico. I flussi di dati sono protetti nel miglior modo possibile mediante l'adozione di misure supplementari. L'Amministrazione federale si avvale per esempio di un servizio acquistato sul mercato per la protezione completa della presenza su Internet dagli attacchi DDoS, che può essere attivato in caso di evento. Tra le sue funzioni di sicurezza, il servizio offre una soluzione integrata di geofencing e consente il controllo degli accessi alle risorse online a livello regionale.

### Caratteristiche principali

| Vantaggi | Svantaggi |
|---|---|
| **Disponibilità:** elevata disponibilità. Internet è raggiungibile in ogni parte del mondo mediante numerose tecnologie di connessione. | **Infrastruttura condivisa:** l'infrastruttura di comunicazione e la larghezza di banda sono condivise tra numerosi utenti. Le connessioni sono esposte a DDoS, analisi del flusso di dati, IP spoofing e attacchi man-in-the-middle. Nessun isolamento dei flussi di dati. |
| **Costi:** rispetto alle linee dedicate, i costi di un collegamento a Internet sono bassi. | **Priorizzazione del traffico dati:** le connessioni Internet non hanno una qualità garantita del servizio. Non è possibile dare la priorità a flussi di dati selezionati. La latenza e la variazione del ritardo (jitter) più elevati possono risultare problematici per le applicazioni in tempo reale. |
| **Flessibilità:** i servizi offerti tramite la rete Internet pubblica sono altamente flessibili e generalmente vantaggiosi in termini di prezzo. | **Controllo dei percorsi fisici:** nessun controllo sui flussi di dati. Le connessioni possono passare attraverso le reti di molti provider diversi. |
| | **Routing:** il routing non è sotto il controllo dell'Amministrazione federale. Ciò può causare problemi di sicurezza. |

Tabella 6: Caratteristiche principali delle connessioni Internet

### Rischi intrinseci

**Rete pubblica:** Internet è una rete pubblica e le linee di comunicazione nonché i sistemi coinvolti sono esposti a potenziali ciberminacce. Attacchi adattivi mirati, punti deboli interni o

metodi di attacco alternativi possono eludere i meccanismi di protezione o portarli ai limiti delle loro capacità.

# 4 Tecnologie alternative

Sul mercato sono in linea di principio disponibili tecnologie di comunicazione alternative che mirano ad affrontare le sfide esistenti di Internet.

## 4.1 SCION

SCION (Scalability, Control and Isolation On Next-generation Networks) è un'innovativa architettura Internet sicura, sviluppata dal Politecnico federale di Zurigo. Consente di definire i percorsi di dati, isola i guasti di rete e offre percorsi ridondanti e meccanismi affidabili espliciti per la comunicazione. Attraverso l'introduzione di cosiddetti domini di isolamento (Isolation Domain, ISD), SCION crea un'infrastruttura di routing sicura e scalabile, in grado di ridurre sia i ciberattacchi come il BGP hijacking sia gli attacchi DDoS. All'occorrenza, la crittografia del livello di trasporto può essere integrata con livelli di protezione superiori.

### 4.1.1 Proprietà funzionali di SCION

Dominio di isolamento (ISD): SCION utilizza gli ISD per segmentare la topologia di rete. Gli ISD offrono ambienti isolati e affidabili che rendono più difficili attacchi come l'IP spoofing o le manipolazioni del routing. Vi sono ISD definiti geograficamente, come lo Swiss-ISD, e ISD specifici della clientela, come quello della Secure Swiss Finance Network (SSFN).

Controllo dei percorsi: i gestori di rete hanno il controllo sui percorsi di dati offerti agli utenti. I percorsi di comunicazione a livello AS (Autonomous System) possono essere selezionati dal gestore di rete o dall'utente prima della trasmissione sulla base, per esempio, delle esigenze in materia di sicurezza o di prestazioni. Il mittente può scegliere quali reti di provider utilizzare per la trasmissione dei dati, ma non i percorsi all'interno delle stesse. Il controllo dei percorsi risulta quindi efficace e vantaggioso in particolare per i flussi di dati che attraversano le infrastrutture di più provider.

Resilienza alle perturbazioni di rete: viene sostenuto il routing multiplo, in modo da poter utilizzare diversi percorsi tra l'origine e la destinazione. Rispetto ad altre tecnologie, SCION è più resistente alle perturbazioni di rete.

Routing efficiente e sicuro: SCION utilizza meccanismi di routing propri. Questi consentono di individuare i percorsi in modo rapido e sicuro senza bisogno di un consenso globale o di tabelle di routing centrali. Vengono impiegati metodi crittografici per garantire l'autenticità e l'integrità dei percorsi. La struttura dell'architettura e la verifica basata su firma impediscono che il routing sia soggetto ad attacchi.

Percorsi nascosti (Hidden Paths): i percorsi nascosti consentono di nascondere segmenti di comunicazione specifici in modo da renderli utilizzabili solo per partecipanti autorizzati.

Scalabilità: l'architettura è concepita in modo da funzionare in maniera efficiente anche nelle reti molto grandi. Il ricorso agli ISD e a un processo decisionale locale riduce il carico sui componenti di routing centrali. SCION utilizza una struttura gerarchica per semplificare il routing globale.

### 4.1.2 Normazione

Allo stato attuale SCION non è soggetto alle norme elaborate da organizzazioni internazionali di normazione come l'IETF (Internet Engineering Task Force) o l'ISO (International Organization for Standardization). Una normazione è importante per consolidare la tecnologia presso i fornitori (di hardware) e ridurre il vincolo del fornitore. Sono in corso progressi significativi in tale direzione e l'architettura si basa su protocolli documentati, sostenuti dalla comunità di ricerca, che potrebbero costituire la base per futuri processi di normazione.

### 4.1.3 Vincolo del fornitore

Nella pratica, la realizzazione delle soluzioni di comunicazione basate su SCION comporta una forte dipendenza da Anapaya Systems AG (Anapaya), sebbene l'architettura sia concepita in modo sostanzialmente aperto ed esistano implementazioni open-source del protocollo. L'azienda, una società anonima con sede in Svizzera finanziata da investitori privati[9], è uno spin-off del Politecnico federale di Zurigo. Permangono dipendenze da Anapaya nei seguenti ambiti:

Gestione degli ISD: la gestione e l'assegnazione degli ISD richiedono un coordinamento centrale che allo stato attuale è garantito da Anapaya.

Anapaya come gestore dello Swiss-ISD: Anapaya è il gestore dello Swiss-ISD. Ciò comprende in particolare anche la relativa governance e la gestione delle prestazioni di Public Key Infrastructure (PKI) necessarie per lo Swiss-ISD.

Anapaya come unico offerente di soluzioni SCION commerciali: queste comprendono prodotti come SCION Gate e SCION Edge Router, ma anche i sistemi periferici per il routing, la gestione e l'assistenza. Tali soluzioni sono interessanti per le imprese, in quanto consentono implementazioni semplici e chiavi in mano senza bisogno di conoscenze approfondite di SCION.

Servizio disponibile sul mercato: i servizi offerti sul mercato si basano sulle soluzioni SCION commerciali di Anapaya.

[9] Secondo fonti pubbliche, all'aumento di capitale del 2024 hanno partecipato investitori quali SIX, Mysten Lab, Cape Capital e l'investitore tecnologico Nagy Moustafa (fonte: https://www.zhk.ch/de/wirtschaft-und-politik/news/anapaya-erhaelt-10-millionen-franken-fuer-expansion.html; consultato il 17.9.2025)

### 4.1.4 Maturità

SCION è un protocollo di rete tecnicamente maturo, frutto di anni di ricerca e sviluppo e costantemente perfezionato dalla comunità di ricerca. Esso rappresenta una buona base, ma da solo non basta a risolvere tutte le sfide di una comunicazione dati sicura. I protocolli e i meccanismi sono stati testati a fondo nell'ambito di diversi proof of concept all'interno e all'esterno dell'Amministrazione federale e appaiono tecnicamente stabili. In Svizzera, SCION è per esempio utilizzato presso la SSFN e la Health Info Network (HIN). Nel Cantone di Soletta è stata inoltre realizzata un'applicazione pilota.

In Svizzera SCION può essere acquistato come servizio presso tutti i grandi fornitori di servizi di telecomunicazione. Tuttavia, le offerte commerciali di tali fornitori non riescono a tenere il passo con lo stato attuale della ricerca e dello sviluppo. Esistono inoltre operatori di cloud svizzeri che offrono un'integrazione nativa con SCION. I fornitori cloud su larga scala (hyperscaler) globali non offrono invece alcuna integrazione nativa con SCION, salvo poche eccezioni. Essi ne consentono però l'integrazione se il cliente stesso si occupa della costruzione e dell'esercizio, assumendosi al contempo tutta la responsabilità.

La penetrazione di mercato a livello globale è ancora in una fase iniziale. Di conseguenza, la disponibilità di SCION deve essere verificata individualmente, a seconda della situazione, per ciascuna ubicazione all'estero e il protocollo SCION non gode ancora di ampio supporto da parte dei principali produttori di soluzioni di rete (p. es. Cisco, Juniper).

### 4.1.5 Restrizioni e ostacoli all'adattamento

Sebbene SCION sia interoperabile con le reti esistenti, lo sfruttamento di tutte le sue funzionalità richiede, oltre ai componenti core SCION Core, Edge e Gate, anche diversi servizi di controllo come CA (Certificate Authority), Anapaya Console, Path Server e Beacon Server. La situazione è resa ulteriormente difficile dal fatto che la gestione di un ISD privato attraverso reti pubbliche è possibile solo in collaborazione con i provider interessati. In molti casi, le implementazioni complesse richiedono la partecipazione di Anapaya e l'adesione a un ISD. L'utilizzo di SCION, come accade anche con altri servizi di rete acquistati sul mercato, presuppone inoltre una fiducia di fondo nei provider selezionati.

## 4.2 MPLS (Multiprotocol Label Switching)

Il MPLS è una tecnica di trasmissione dati all'interno di reti di comunicazione, utilizzata frequentemente nelle grandi reti aziendali e di telecomunicazione. È in grado di gestire e priorizzare il traffico dati sulla base di etichette, consentendo una trasmissione rapida ed efficiente. Si tratta di una tecnologia che trova già impiego presso l'Amministrazione federale. In Svizzera è utilizzata direttamente dall'Amministrazione federale per l'approntamento di connessioni dati, mentre all'estero è acquistata come servizio.

#### Caratteristiche principali

**Ingegneria del traffico:** il MPLS consente di gestire e priorizzare il traffico dati in modo preciso.

**Quality of Service (QoS):** garantisce la qualità delle applicazioni in tempo reale, come la trasmissione di audio e video.

**Sicurezza tramite VPN:** il MPLS può essere utilizzato per la creazione di reti private virtuali (VPN) che consentono la comunicazione dati all'interno di un tunnel sicuro.

### Restrizioni

I percorsi MPLS non possono essere configurati direttamente dal cliente finale. Poiché il MPLS è gestito e controllato dal provider a livello centrale, la fiducia in quest'ultimo costituisce un requisito essenziale. La crittografia di trasporto deve essere integrata con livelli di protezione superiori.

## 4.3 SD-WAN (Software-Defined Wide Area Network)

La SD-WAN è un'architettura di rete definita tramite software che consente di gestire e controllare in modo dinamico le reti di comunicazione a lunga distanza. Combina connessioni Internet pubbliche con connessioni private e si avvale di software per ottimizzare il traffico dati e renderlo sicuro. L'ottimizzazione è dinamica e si basa sullo stato di rete di volta in volta attuale. La SD-WAN è gestita a livello centrale dal cliente ed è concepita per le reti di comunicazione a lunga distanza con diverse sedi. L'intero traffico dati tra gli endpoint della SD-WAN è criptato. Questa tecnologia è utilizzata direttamente dall'Amministrazione federale per garantire la comunicazione dati.

### Restrizioni

Come il MPLS, anche la SD-WAN è gestita a livello centrale. Molte soluzioni SD-WAN dipendono dal rispettivo produttore, il che può creare un cosiddetto vincolo del fornitore.

## 4.4 TLS (Transport Layer Security) e DTLS (Datagram Transport Layer Security)

Il TLS è un protocollo crittografico diffuso a livello mondiale che viene utilizzato per il trasporto di dati su connessioni potenzialmente non sicure. Si basa sulla crittografia end-to-end e sull'autenticazione per il trasporto di dati. Con il DTLS si può proteggere anche il trasporto di protocolli non affidabili come lo UDP. Il protocollo è utilizzato in modo pressoché capillare in ogni parte del mondo per proteggere sistemi di comunicazione via e-mail e nel web, al fine di garantire la riservatezza e l'integrità dei dati. Queste tecnologie trovano frequentemente impiego presso l'Amministrazione federale. Esistono anche altri protocolli crittografici che vengono utilizzati per le soluzioni VPN, per esempio nelle applicazioni per il telelavoro.

### Restrizioni

I protocolli TLS e DTLS proteggono la comunicazione, ma non offrono soluzioni per i problemi di fondo legati al trasporto, come la sicurezza del routing o il controllo dei percorsi. Il TLS dipende fortemente dagli organismi di certificazione (CA), il che può sollevare questioni di fiducia e causare problemi nella manipolazione dei certificati.

# 5 Necessità di intervento

L'infrastruttura WAN dell'Amministrazione federale è una soluzione OSI di livello 3 (L3), utilizzata sia dalle diverse unità dell'Amministrazione federale sia dai Cantoni e delle imprese parastatali. Secondo una decisione del Consiglio federale del 31 maggio 2011, i servizi di livello 3 devono essere approntati direttamente dall'Amministrazione federale. L'Ufficio federale dell'informatica e della telecomunicazione (UFIT) è incaricato dello sviluppo e dell'esercizio tecnico di tali servizi.

## 5.1 Interconnessione di ubicazioni della Confederazione

L'interconnessione delle ubicazioni dell'Amministrazione federale in Svizzera si basa di norma sulla fibra ottica spenta (dark fiber), sui servizi Ethernet e sulla ROAF. Queste tecnologie sono descritte nel capitolo 3.

Nella regione e nell'agglomerato di Berna si utilizza per lo più la fibra ottica spenta. Le altre ubicazioni in Svizzera sono collegate prevalentemente con soluzioni di servizi Ethernet acquistate sul mercato o prodotte internamente.

Secondo il messaggio del 21 novembre 2018[10] concernente un credito d'impegno per il sistema nazionale per lo scambio di dati sicuro, determinate ubicazioni federali, i Cantoni e i gestori di infrastrutture critiche devono essere collegati mediante una rete resistente alle crisi. Questa rete RDS+ è attualmente in corso di sviluppo e offrirà tra l'altro una maggiore sicurezza e protezione in caso di interruzioni della corrente. Si basa sulla ROAF di cui al numero 3.1.3.

Nel caso delle reti chiuse come la KOMBV/KTV o della fibra ottica spenta, la sicurezza è garantita in misura sufficiente, come illustrato in un rapporto dell'ADS[11]. In quest'ambito non sussiste pertanto alcuna necessità diretta di intervento dovuta a una scarsa sicurezza della comunicazione dati.

Per le applicazioni per il telelavoro dell'Amministrazione federale e l'interconnessione di ubicazioni di piccole dimensioni è oggi possibile utilizzare una soluzione basata su Internet. La connessione si basa su una soluzione VPN in cui i dati sono trasmessi in forma criptata. Queste connessioni sono in linea di principio esposte ai pericoli intrinseci di una tecnologia basata su Internet, come descritto al numero 3.3.

Per queste ubicazioni interconnesse tramite Internet si potrebbe prendere in considerazione la tecnologia SCION, qualora questa sia disponibile presso l'ubicazione in questione, tale soluzione

[10] FF **2019** 235

[11] Questo studio non è pubblico; per consultarlo si prega di contattare direttamente l'ADS.

appaia economicamente sostenibile e sia richiesta una maggiore flessibilità o una protezione migliore della connessione dati.

## 5.2 Interconnessione delle imprese parastatali

Attualmente le imprese parastatali sono anch'esse in parte collegate con la rete dell'Amministrazione federale tramite le reti chiuse KOMBV/KTV o la fibra ottica spenta. In quest'ambito non sussiste pertanto alcuna necessità immediata di intervento dovuta a una scarsa sicurezza della comunicazione dati.

## 5.3 Interconnessione dei Cantoni

L'interconnessione delle amministrazioni cantonali con l'infrastruttura di rete dell'Amministrazione federale centrale si basa attualmente sulle reti KOMBV/KTV e in futuro sulla rete RDS+. Trattandosi di reti chiuse, come sopra menzionato, in quest'ambito non sussiste pertanto alcuna necessità di intervento dovuta a una scarsa sicurezza della comunicazione dati.

## 5.4 Interconnessione con il pubblico

Oggi l'accesso del pubblico ai servizi della Confederazione avviene tramite Internet ed è pertanto esposto a numerose minacce potenziali. Per la protezione della presenza della Confederazione su Internet è stata introdotta una soluzione di protezione che si è nel frattempo affermata.

Dal punto di vista attuale è possibile ipotizzare che in futuro questi servizi possano essere protetti anche mediante la tecnologia SCION. L'accesso alle reti SCION dall'estero è tuttavia garantito solo in parte. Inoltre, il modello di licenza dei provider non è attualmente chiaro; dai primi accertamenti è emerso che i costi collegati potrebbero essere molto elevati (v. n. 6).

# 6 Economicità

Le ubicazioni dell'Amministrazione federale nella regione di Berna sono interconnesse mediante linee in fibra ottica della Confederazione. Su tale base, la Confederazione realizza i livelli di rete superiori con sistemi propri. Per queste linee in fibra ottica della Confederazione non vi sono praticamente alternative disponibili sul mercato e i costi di esercizio sono relativamente bassi.

Per le linee di comunicazione al di fuori della regione di Berna, per esempio per le ubicazioni esterne o temporanee, esistono solitamente diverse varianti per il collegamento alla rete centrale dell'Amministrazione federale.

Attualmente le ubicazioni esterne che si trovano in Svizzera sono spesso interconnesse tramite servizi Ethernet, il cui vantaggio consiste nella disponibilità di SLA e QoS. In queste ubicazioni si potrebbe prendere in considerazione anche un'interconnessione basata su Internet, che grazie

alla moderna interconnessione offre oggi larghezze di banda elevate a prezzi convenienti. Lo svantaggio di questo genere di connessioni consiste però nella mancanza di SLA e QoS, in quanto i servizi Internet sono generalmente disponibili solo in modalità «Best Effort» e Internet è una rete pubblica utilizzata collettivamente.

In determinate circostanze, gli svantaggi legati alla mancanza di QoS possono essere compensati con una maggiore larghezza di banda, anche se ciò non rappresenta una garanzia di qualità come nei servizi Ethernet. La mancanza di SLA potrebbe invece essere compensata con un collegamento ridondante tramite due provider, eventualmente mediante collegamenti terrestri o basati sulla telefonia mobile.

In questo caso, i punti deboli di un collegamento basato su Internet potrebbero essere ulteriormente compensati da tecnologie innovative come SCION: SCION offre sia il routing multiplo (ridondanza tra più provider o percorsi) sia il routing protetto contro le manipolazioni.

In Svizzera il collegamento di ubicazioni esterne con SCION, come sopra descritto, può costituire una variante meritevole di essere esaminata qualora vi sia la possibilità di rinunciare a QoS e SLA e trarre vantaggio dal routing multiplo e della resistenza agli attacchi DDoS. È emerso che in un caso del genere la soluzione SCION può essere molto interessante anche sotto il profilo economico e non rappresenta necessariamente la variante più costosa.

Dal punto di vista tecnico, il collegamento di ubicazioni all'estero avviene in modo analogo alla Svizzera. Occorre però sottolineare che in questo caso non tutte le ubicazioni possono essere collegate con SCION, in quanto all'estero tale tecnologia è offerta solo da pochi provider; per trarre vantaggio da questa tecnologia è però necessario che il collegamento dell'ubicazione avvenga in maniera continuativa attraverso la rete SCION. Non si sono potuti rilevare dati vincolanti in merito ai costi di un tale collegamento via SCION; la valutazione dovrà avvenire in maniera specifica per ogni progetto.

Dalla prospettiva odierna, un accesso remoto per il personale dell'Amministrazione federale tramite SCION appare economicamente poco allettante, sebbene fattibile e privo di ostacoli a livello tecnico. I modelli di licenza dei provider suggeriscono costi per utente molto elevati, e ciò contando non solo gli utenti effettivi ma anche i loro diversi indirizzi IP, il che riduce ulteriormente l'attrattiva del prezzo.

Non è stato possibile rilevare sul mercato dati relativi ai costi di gestione di uno o più web server nella rete SCION. Non vi è dunque modo di valutare se tale soluzione sia o meno commercialmente sostenibile. Per tale motivo non è neppure oggettivamente possibile un confronto con altre soluzioni.

Un'analisi costi/benefici completa di tutte le tecnologie menzionate nel capitolo 4 non sembra pertinente, in quanto le varie tecnologie mirano a raggiungere obiettivi molto diversi. In particolare, con le tecnologie basate su linee in fibra ottica proprie si perseguono obiettivi quali la sovranità dei dati o la resilienza della rete elettrica. Questi obiettivi possono essere raggiunti solo in modo limitato con una tecnologia basata su Internet come SCION. Un confronto dei costi

e dei benefici appare tuttavia interessante non appena si prendono in considerazione delle connessioni dati basate su Internet. Si tratta oggi, in particolare, delle connessioni di ubicazioni di piccole dimensioni in cui non sono disponibili linee in fibra ottica proprie della Confederazione, di ubicazioni all'estero o di applicazioni per il telelavoro del personale dell'Amministrazione federale.

Negli ultimi casi menzionati, SCION può apportare un valore aggiunto sotto forma di migliore resistenza agli attacchi DDoS o controllo dei percorsi. I costi legati a SCION sono tendenzialmente più elevati, in quanto questa tecnologia rappresenta di norma una prestazione supplementare e non alternativa a una soluzione esistente basata su Internet.

# 7 Conclusione

L'interconnessione dell'Amministrazione federale e delle imprese parastatali è solida e si basa su tecnologie standardizzate consolidate, ampiamente affermate nell'industria. Da un punto di vista fisico si tratta generalmente di reti in fibra ottica proprie o di servizi Ethernet acquistati. Su tale base vengono sviluppate le reti chiuse. Queste reti protette e isolate da Internet soddisfano requisiti in parte molto stringenti in termini di resilienza dalla rete elettrica o presentano un'elevata disponibilità. Per le applicazioni per il telelavoro del personale dell'Amministrazione federale, nonché in casi specifici, si ricorre a Internet per l'interconnessione di ubicazioni della Confederazione, imprese parastatali o Cantoni. Il collegamento tramite Internet avviene in particolare per le ubicazioni esterne di piccole dimensioni, per le ubicazioni all'estero o in altri casi in cui un collegamento tramite fibra ottica spenta o servizi Ethernet non appare efficiente sul piano economico o non è possibile. Il traffico dati con il pubblico passa esclusivamente attraverso la rete Internet pubblica.

I servizi Internet sono fondamentalmente esposti a minacce: il traffico dati via Internet può essere deviato in modo mirato dai potenziali autori di attacchi, oppure può essere disturbato, analizzato o addirittura paralizzato; inoltre, in Internet non ha sostanzialmente luogo alcuna priorizzazione del traffico dati. Per attenuare questi rischi sono state adottate misure che in passato hanno consentito il ripristino dei rispettivi servizi. Anche se le misure tecniche permettono di ridurre numerosi problemi di sicurezza, permangono rischi, come per esempio quelli emersi nel caso Xplain, che devono essere affrontati con misure di natura non solo tecnica ma anche organizzativa.

Per proteggere ulteriormente il traffico dati via Internet, sono da tempo monitorate ed esaminate nell'ambito di test anche tecnologie alternative come SCION, un protocollo sviluppato al Politecnico federale di Zurigo[12]. La tecnologia SCION appare tecnicamente matura

[12] Cfr. tra l'altro «On Building Secure Wide-Area Networks over Public Internet Service Providers», CyCon 2024: Over the Horizon 16th International Conference on Cyber Conflict.

e in alcuni casi potrebbe aumentare la resistenza agli attacchi DDoS e di routing. Le soluzioni SCION disponibili sul mercato non sono tuttavia adatte alla comunicazione in situazioni di crisi a partire dal momento in cui si rendono necessarie soluzioni resilienti in relazione alla rete elettrica. Il protocollo SCION dipende da tutta una serie di sistemi che allo stato attuale non sono resilienti rispetto all'alimentazione elettrica o lo sono solo limitatamente. È tuttavia necessario continuare a monitorare gli sviluppi.

L'impiego di SCION permetterebbe di migliorare un aspetto tecnico della sovranità digitale (la sicurezza del routing); occorre d'altro canto considerare che con l'introduzione della soluzione SCION, allo stato attuale, verrà a crearsi una dipendenza da Anapaya. A livello commerciale non è possibile esprimere una valutazione definitiva su questa nuova tecnologia. Gli attuali modelli di licenza dei provider renderebbero un'introduzione, per esempio per il telelavoro, economicamente molto onerosa. Questi costi aggiuntivi sono attualmente troppo elevati per il telelavoro. Il Consiglio federale si aspetta che i provider rendano più interessanti le loro offerte e accoglie con favore gli sforzi in materia di normazione.

Per il collegamento di ubicazioni a integrazione delle attuali soluzioni VPN, SCION potrebbe risultare interessante dal punto di vista economico.

Finora i provider non sono stati in grado di fornire dati relativi ai costi per mettere i servizi Internet dell'Amministrazione federale a disposizione del pubblico anche tramite SCION; per ogni servizio richiedono tuttavia una negoziazione sul prezzo. Anche in questo caso è necessario monitorare gli sviluppi: sarebbe auspicabile che queste offerte venissero standardizzate sia a livello tecnico che commerciale.

Le incertezze in ambito commerciale non devono mettere in dubbio le prestazioni tecniche di questa soluzione. Tali incertezze suggeriscono piuttosto che SCION costituisca una soluzione tecnica potenzialmente interessante che tuttavia, a differenza delle tecnologie già in uso, attualmente non è ancora offerta come servizio pronto per la commercializzazione con chiari SLA, listini prezzi univoci e modelli di licenza. Per tale motivo, al momento della stesura del rapporto non è possibile effettuare un'analisi solida e conclusiva dei costi e benefici o un raffronto sotto il profilo economico delle tecnologie considerate.

Il rapporto si è limitato a esaminare l'impiego di SCION nell'ottica dell'acquisto; gli strumenti di promozione non sono stati presi in considerazione.

# 8 Prospettive

Nei casi in cui la Confederazione gestisce reti proprie non sussiste alcuna necessità di intervento. Tali reti non sono visibili dall'esterno e sono pertanto sufficientemente protette contro i ciberattacchi provenienti da Internet.

L'impiego di SCION può tuttavia apportare un valore aggiunto nei casi in cui non siano disponibili reti proprie della Confederazione e le connessioni dati avvengano attraverso Internet. In tali casi SCION consente di ottenere una maggiore protezione dagli attacchi DDoS

e di routing. Ne sono un esempio le ubicazioni in Svizzera e all'estero che sono oggi collegate tramite linee VPN. Sono qui compresi anche le applicazioni per il telelavoro del personale dell'Amministrazione federale e l'accesso ai servizi Internet dell'Amministrazione federale.

In tale contesto occorre prestare attenzione alla dipendenza dagli offerenti. Anche se i servizi SCION possono essere acquistati da diversi provider, permane la dipendenza indiretta da Anapaya come gestore dello Swiss-ISD e produttore della tecnologia.

Il Consiglio federale si aspetta che le offerte di mercato dei provider, in particolare quelle rivolte alle imprese, vengano migliorate. Ciò potrebbe rendere più interessante la tecnologia per l'Amministrazione federale.

Il Consiglio federale ha incaricato la Cancelleria federale di continuare a monitorare la tecnologia e i servizi SCION disponibili sul mercato.

A tal fine, nei prossimi due anni verrà chiesto ai fornitori di inoltrare annualmente delle offerte indicative, che saranno valutate dagli organi competenti dell'Amministrazione federale.

# 9 Abbreviazioni e glossario

## Abbreviazioni / glossario

| Termine | Spiegazione |
|---|---|
| ADS | Amministrazione digitale Svizzera |
| BGP | Border Gateway Protocol: protocollo per gestire il routing tra sistemi autonomi in Internet. |
| CA | Certificate Authority: organizzazione fidata che rilascia certificati digitali. |
| DDoS | Distributed Denial of Service: metodo di ciberattacco che sovraccarica reti o servizi con richieste in massa. |
| DTLS | Datagram Transport Layer Security: estensione di sicurezza per i protocolli di comunicazione basati su UDP. |
| Geofencing | Tecnologia che definisce settori geografici per innescare azioni in funzione del luogo. |
| HIN | Health Info Net: rete di comunicazione sicura per il servizio sanitario. |
| IETF | Internet Engineering Task Force: organizzazione che elabora e aggiorna norme per Internet. |
| IP | Internet Protocol: protocollo per indirizzare e inoltrare pacchetti di dati in Internet. |
| IP spoofing | Internet Protocol spoofing: tecnica con cui l'autore di un attacco utilizza un indirizzo IP falso per occultare la propria identità. |
| IPSEC | Internet Protocol Security: protocollo per proteggere la comunicazione IP mediante autenticazione e crittografia. |
| ISD | SCION utilizza Isolation Domain per segmentare la topologia di rete. |
| ISO | International Organization for Standardization: organizzazione internazionale di normazione per le norme in diversi settori. |
| KOMBV/KTV | Rete di collegamento di tutti i Cantoni tra loro e con l'Amministrazione federale |
| Livello 2 | Livello di collegamento dati (modello OSI): il livello di protezione del modello OSI che è competente per l'indirizzamento fisico e l'individuazione di errori. |
| Livello 3 | Livello di rete (modello OSI): il livello di rete del modello OSI che è responsabile del routing e dell'indirizzamento IP. |
| Man-in-the-middle | Attacco man-in-the-middle: attacco in cui un soggetto terzo si inserisce tra due partner di comunicazione e manipola i dati. |
| MPLS | Multiprotocol Label Switching: tecnologia di rete per l'inoltro rapido ed efficiente dei dati. |
| QoS | Quality of Service |
| RDS+ | Rete di dati sicura plus |
| ROAF | Rete ottica delle autorità federali |
| SCION | Scalability, Control and Isolation On Next-generation Networks |
| SD-WAN | Software-Defined Wide Area Network: tecnologia di rete per la gestione flessibile delle reti di comunicazione a lunga distanza. |
| SLA | Accordo sui livelli di servizio |
| SSFN | Secure Swiss Finance Network: rete di comunicazione sicura per istituzioni finanziarie in Svizzera. |

| Termine | Spiegazione |
|---|---|
| TLS | Transport Layer Security: protocollo crittografico per la comunicazione sicura via Internet. |
| UDP | User Datagram Protocol |
| UFCS | Ufficio federale della cibersicurezza |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |

Tabella 7: Abbreviazioni e glossario