

# Policy per l'utilizzo e la gestione delle tecniche crittografiche

CCR_SEC_05
Rev. 02 26/10/2025

## 1. Scopo

La presente policy definisce i principi e le regole per l'uso della crittografia all'interno dell'organizzazione al fine di:

- Garantire la riservatezza, l'integrità e l'autenticità delle informazioni trattate;
- Proteggere informazioni e comunicazioni, con particolare riferimento ai dati considerati critici (da qui in poi: *dati riservati*) in relazione all'operatività dell'organizzazione (per esempio: dati personali particolari ai sensi del GDPR, generici dati sensibili in relazione all'eventuale classificazione in vigore);
- Assicurare la conformità alle vigenti normative e linee guida in materia.

## 2. Ambito di applicazione

La presente policy si applica a tutti i sistemi e servizi informatici dell'INFN che trattano *dati riservati* ai fini dell'operatività dell'organizzazione stessa; elenca e distingue obblighi, prescrizioni e buone pratiche per:

- Amministratori di Sistema e utenti privilegiati
- Utenti ordinari - dipendenti, associati, ospiti e visitatori

## 3. Principi generali

L'utilizzo della crittografia deve conformarsi in ogni caso ai seguenti principi di base:

- **Necessità e proporzionalità** – La crittografia deve essere applicata in funzione del livello di rischio e della eventuale classificazione delle informazioni;
- **Utilizzo di algoritmi riconosciuti** – Devono essere utilizzati solo algoritmi e protocolli crittografici riconosciuti da standard internazionali e da questi classificati come sicuri;
- **Sicurezza delle chiavi** – la chiavi crittografiche (certificati X.509 personali e per server/servizi; chiavi SSH; chiavi per la crittografia di dati e documenti) sono da considerarsi elementi critici per la sicurezza dell'organizzazione e vanno generate,

gestite e protette adeguatamente seguendo, se necessario, le prescrizioni elencate nel seguito.

## 4. Disposizioni generali

### Protezione dei dati a riposo

- è raccomandata la cifratura dei dischi di server e workstation ospitanti *dati riservati*; è obbligatoria la cifratura dei dischi di dispositivi mobili contenenti *dati riservati*;
- è obbligatoria la cifratura di *dati riservati* che risiedono su cloud esterne non autorizzate; le chiavi di cifratura non devono risiedere sugli stessi dispositivi che contengono i dati a cui sono riferite;
- le chiavi crittografiche devono, ove richiesto, essere protette da passphrase non banali e vanno conservate su dispositivi sicuri e non in aree condivise via rete a meno che ciò non sia indispensabile per l'operatività dei servizi.

### Protezione dei dati in transito

- è obbligatorio utilizzare esclusivamente protocolli (TLS) o applicativi (ssh, VPN) sicuri per servizi che espongono *dati riservati* (anche tramite API) o richiedono accesso autenticato (portali web, spedizione e lettura posta elettronica, accesso interattivo);
- le chiavi crittografiche non devono essere trasmesse su canali in chiaro;
- eventuali servizi legacy di accesso in chiaro a dispositivi e apparecchiature che per motivi tecnici non supportino protocolli sicuri devono obbligatoriamente essere esposti solo su rete privata e protetti adeguatamente con firewall perimetrali o locali; è vietato esporre su rete geografica servizi che utilizzano protocolli di accesso con autenticazione in chiaro (telnet, ftp, http autenticato);
- è obbligatorio utilizzare la crittografia end-to-end per la trasmissione di *dati riservati* mediante posta elettronica;
- per l'accesso da reti pubbliche non sicure a risorse e servizi dell'INFN è obbligatorio utilizzare i servizi VPN messi a disposizione dai team responsabili delle risorse informatiche delle strutture o utilizzare esclusivamente protocolli di rete criptati.

### Protezione dei backup:

- è raccomandato cifrare i supporti di backup/archiviazione o utilizzare applicazioni di backup che permettano la cifratura dei dati;
- è obbligatorio cifrare i backup prima di trasferirli via rete, o utilizzare protocolli di trasmissione cifrati;
- è obbligatorio cifrare i backup se ospitati su servizi cloud esterni.

## 5. Disposizioni per Amministratori di Sistema e Utenti privilegiati

### 5.1. Implementazione di SSL/TLS

#### Gestione di certificati e chiavi private

- Le chiavi vanno generate su un sistema affidabile e possibilmente isolato e dotato di sufficiente entropia;
- le chiavi RSA devono avere dimensione non inferiore a 2048 bit; per applicazioni particolarmente critiche è opportuno considerare l'utilizzo di chiavi RSA da 3072 bit o, ove le prestazioni siano importanti, chiavi ECDSA da 256 bit o più;
- l'algoritmo di hashing della firma deve essere almeno SHA256;
- per servizi esposti all'utenza è obbligatorio utilizzare solo certificati emessi da CA pubbliche, ed è obbligatorio provvedere al rinnovo tempestivo dei certificati in scadenza;  
per tali servizi non è consentito l'utilizzo di certificati *self-signed*.

#### Protocolli ammessi e configurazioni consigliate

- L'utilizzo di **SSL v2** e **SSL v3** (entrambi insicuri e obsoleti) è **esplicitamente proibito**;
- **TLS v1.0** e **TLS v1.1** sono da considerarsi protocolli legacy, sono stati ufficialmente deprecati nel gennaio del 2020 e **non dovrebbero essere usati**;
- **TLS v1.2** e **TLS v1.3** non presentano problemi di sicurezza noti e **dovrebbero essere i principali o, ancora meglio, gli unici protocolli supportati**.
- Utilizzare solo suite di cifratura sicure (meglio se con selezione da parte del server), Perfect Forward Secrecy (PFS) e protocolli di scambio chiavi forti (Strong Key Exchange): per i dettagli fare riferimento ai documenti della serie "Linee Guida Funzioni Crittografiche" pubblicati da ACN<sup>1</sup>;
- verificare periodicamente le configurazioni dei servizi esposti utilizzando scanner TLS (testssl.sh, SSL Server Test by Qualys)

### 5.2. Configurazione dei server ssh

SSH, la cui versione minima **deve** essere la 2.0, supporta diversi 1) algoritmi di scambio di chiavi, 2) algoritmi di cifratura e 3) codici di autenticazione dei messaggi per garantire autenticità, confidenzialità e integrità delle comunicazioni tra server e client: gli algoritmi obsoleti, poco sicuri o sospettati di compromissione vanno disabilitati anche correndo il rischio di risultare incompatibili con clienti obsoleti. Per valutare la sicurezza della configurazione dei server SSH esposti si raccomanda di utilizzare il tool di audit 'ssh-audit' (<https://github.com/jtesta/ssh-audit>, <https://www.sshaudit.com/>) e di applicare le relative *hardening guide*.

### 5.3. Configurazione dei server di posta elettronica

Per i mail server autenticati e i server per l'accesso alle caselle di posta fare riferimento a quanto già prescritto per la configurazione di SSL/TLS, avendo cura di proibire l'accesso ai

---

<sup>1</sup> <https://www.acn.gov.it/portale/crittografia>

servizi in chiaro; è consigliabile implementare il *TLS opportunistic* anche sugli MTA in modo da garantire – ove possibile - la massima sicurezza delle comunicazioni mantenendo la interoperabilità con gli MTA che non supportano la crittografia.

## **6. Disposizioni per gli utenti**

### **Gestione di certificati e chiavi private**

Le chiavi dei certificati RSA devono avere dimensione non inferiore a 2048 bit ma è consigliabile richiedere già oggi l'emissione di certificati RSA con chiavi di dimensione maggiore (3072 o 4096 bit) o, se supportati dai sistemi nei quali verranno impiegati, di certificati con chiavi ECDSA da 128 o 256 bit.

### **Gestione delle chiavi private SSH**

Le chiavi attualmente utilizzate per l'autenticazione su SSH che offrono il miglior compromesso in termini di sicurezza e prestazioni sono le classiche chiavi RSA e le più recenti chiavi EdDSA basate su curve ellittiche; le prime devono avere dimensione non inferiore a 2048 bit, equivalenti a una sicurezza pari a 112 bit (ma il default sui sistemi Redhat-like di versione uguale o superiore a 9 è 3072 bit, equivalenti a 128 bit), mentre le chiavi basate su curve ellittiche hanno lunghezza fissa.

### **Crittografia end-to-end**

È obbligatorio utilizzare la crittografia end-to-end per la trasmissione di *dati sensibili*; questa prescrizione è particolarmente stringente nel caso della posta elettronica, poiché è in grado di garantire la confidenzialità sul lungo periodo anche delle caselle di posta.

### **Utilizzo di reti wireless pubbliche; VPN**

È sconsigliato l'utilizzo di reti wireless pubbliche in chiaro (cioè non crittografate) per accedere a risorse dell'organizzazione; in caso di necessità è consentito farne uso a patto di utilizzare esclusivamente protocolli criptati per l'accesso a dati e servizi INFN o di attivare la connessione VPN messa a disposizione dalla struttura di riferimento.