Policy on the Use and Management of Cryptographic Techniques

CCR_SEC_05
Rev. 02 26/10/2025

1. Purpose

This policy defines the principles and rules governing the use of cryptography within the organization in order to:

- ensure the confidentiality, integrity, and authenticity of the information processed;
- protect information and communications, with particular regard to data considered critical (hereinafter referred to as *confidential data*) in relation to the organization's operations (e.g. special categories of personal data under the GDPR, or other sensitive data according to any applicable data classification scheme);
- ensure compliance with applicable regulations and guidelines in force.

2. Scope of Application

This policy applies to all INFN information systems and services that process *confidential data* for the purposes of the organization's operations; it identifies and distinguishes obligations, requirements, and best practices applicable to:

- System Administrators and Privileged Users
- Standard Users – employees, associates, guests, and visitors

3. General Principles

The use of cryptography shall in all cases comply with the following fundamental principles:

- **Necessity and proportionality** – Cryptographic measures shall be applied in accordance with the level of risk and any applicable data classification;
- **Use of recognized algorithms** – Only cryptographic algorithms and protocols recognized by international standards and classified therein as secure shall be used;
- **Key security** – Cryptographic keys (personal and service X.509 certificates, SSH keys, keys for data and document encryption) shall be considered critical security assets for the organization and must be generated, managed, and protected appropriately, following, where applicable, the requirements set out below.

4. General Provisions

Protection of Data at Rest:

- Disk encryption is recommended for servers and workstations hosting *confidential data*; disk encryption is mandatory for mobile devices containing *confidential data*;

- Encryption is mandatory for *confidential data* stored on unauthorized external cloud services; encryption keys must not reside on the same devices that store the data to which they relate;
- Cryptographic keys shall, where required, be protected by non-trivial passphrases and stored on secure devices; they shall not be stored on network-shared locations unless strictly necessary for service operation.

Protection of Data in Transit:

- It is mandatory to use exclusively secure protocols (TLS) or secure applications (SSH, VPN) for services that expose *confidential data* (including via APIs) or require authenticated access (web portals, email sending and reading, interactive access);
- Cryptographic keys must not be transmitted over unencrypted channels;
- Any legacy services providing unencrypted access that cannot support secure protocols for technical reasons must be exposed only on private networks and adequately protected by perimeter or local firewalls; exposing services using clear-text authentication protocols (telnet, FTP, authenticated HTTP) on wide-area networks is prohibited;
- The use of end-to-end encryption is mandatory for the transmission of *confidential data* via email;
- When accessing INFN resources and services from public or insecure networks, it is mandatory to use VPN services provided by the relevant IT resources responsible teams or to use exclusively encrypted network protocols.

Backup Protection

- Encryption of backup and archival media, or alternatively the use of backup applications that support data encryption, is **recommended**;
- It is **mandatory** to encrypt backups before transferring them over the network, or to use encrypted transmission protocols.
- It is **mandatory** to encrypt backups stored on external cloud services

5. Provisions for System Administrators and Privileged Users

5.1 SSH/TSL implementation

Management of Certificates and Private Keys

- Keys shall be generated on a trusted, preferably isolated system with sufficient entropy.
- RSA keys must have a minimum length of **2048 bits**; for particularly critical applications, the use of **3072-bit RSA keys** should be considered, or, where performance is a concern, **ECDSA keys of 256 bits or more**.
- The signature hashing algorithm must be at least **SHA-256**.
- For user-facing services, it is **mandatory** to use certificates issued by public Certification Authorities (CAs), and certificates approaching expiration must be renewed in a timely manner.
  The use of self-signed certificates for such services is not permitted.

Permitted Protocols and Recommended Configurations

- The use of **SSL v2** and **SSL v3** (both insecure and obsolete) is explicitly prohibited.
- **TLS v1.0** and **TLS v1.1** are considered legacy protocols, were officially deprecated in January 2020, and should not be used.
- **TLS v1.2** and **TLS v1.3** present no known security issues and should be the primary—and preferably **the only—supported protocols**.
- Only secure cipher suites should be used (preferably with server-side selection), supporting **Perfect Forward Secrecy (PFS)** and strong key exchange mechanisms. For detailed guidance, reference should be made to the *"Cryptographic Functions Guidelines"* published by ACN.
- Exposed services should be periodically reviewed using TLS scanning tools (e.g. *testssl.sh*, *Qualys SSL Server Test*).

5.2. SSH Server Configuration

SSH (minimum supported version: **2.0**) supports multiple key exchange algorithms, encryption algorithms, and message authentication codes to ensure authenticity, confidentiality, and integrity of communications between server and client. Obsolete, weak, or potentially compromised algorithms **must** be disabled, even at the risk of incompatibility with legacy clients.

To assess the security of exposed SSH server configurations, the use of the *ssh-audit* tool (https://github.com/jtesta/ssh-audit, https://www.sshaudit.com/) is recommended, along with the application of the associated hardening guidelines.

5.3. Email Server Configuration

For authenticated mail servers and mail access services, the requirements defined for SSL/TLS configuration apply, with particular care taken to prohibit clear-text access to services. The implementation of **opportunistic TLS** on MTAs is recommended, in order to maximize communication security while maintaining interoperability with MTAs that do not support encryption.

6. Provisions for Users

Management of Certificates and Private Keys

RSA certificate keys must have a minimum length of 2048 bits; however, it is recommended to request certificates with larger key sizes (3072 or 4096 bits) or, where supported by the target systems, certificates using ECDSA keys of 128 or 256 bits.

Management of SSH Private Keys

The SSH keys that currently offer the best balance between security and performance are traditional RSA keys and the more recent EdDSA keys based on elliptic curves. RSA keys must have a minimum length of 2048 bits, corresponding to approximately 112-bit security (on RedHat–like systems version 9 or later, the default is 3072 bits, equivalent to 128-bit security). Elliptic curve–based keys have a fixed length.

End-to-End Encryption

The use of end-to-end encryption is mandatory for the transmission of sensitive data. This requirement is particularly stringent for email, as it ensures long-term confidentiality of mailbox contents.

Use of Public Wireless Networks and VPNs

The use of unencrypted public wireless networks to access organizational resources is discouraged. Where necessary, such networks may be used only if exclusively encrypted protocols are employed to access INFN data and services, or if a VPN connection provided by the relevant organizational unit is activated.