

Security Policy Cryptography

Information Security

|  |  |
| --- | --- |
|  |  |
| Cryptography |  |
| Number | [Number] |
| Issued on | 04.07.2022 |
| Through | Chief Information Security Officer |
| Entry into force | 04.07.2022 |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH |
| Topic | Compliance |
| Responsible function | Information security |
| Responsible person | Dirk Franken |
| Overriding regulation | Information security policy |
| Replaces | n/a |
| Applicable documents |  |
| Validity | Until further notice |
| Last review | 14.07.2025 |
| Next review | 07.01.2026 |
| Publication | SÜDVERS Intranet |
| Classification | Internal |
| Archive | Document management system |
| Organizational system | [Organizational system] |
| Languages |  |
| Formats |  |
| Remarks |  |

Table of contents

[1 Principles 4](#_Toc188274402)

[2 Objectives 4](#_Toc188274403)

[3 Controls 4](#_Toc188274404)

[3.1 Cryptographic solutions 4](#_Toc188274405)

[3.2 Cryptographic key management 6](#_Toc188274406)

[3.3 Approved cryptographic algorithms 8](#_Toc188274407)

[3.3.1 Symmetric encryption 8](#_Toc188274408)

[3.3.2 Asymmetric encryption 8](#_Toc188274409)

[3.3.3 Cryptographic hash functions 8](#_Toc188274410)

[3.3.4 Authentication of data 8](#_Toc188274411)

[3.3.5 Digital signatures 8](#_Toc188274412)

[3.3.6 Key exchange 9](#_Toc188274413)

[3.4 Approved cryptographic protocols 9](#_Toc188274414)

[3.4.1 Transport Layer Security (TLS) 10](#_Toc188274415)

[3.4.2 Secure shell (SSH) 11](#_Toc188274416)

[3.4.3 IPsec 11](#_Toc188274417)

[3.4.4 WPA2/WPA3 12](#_Toc188274418)

[3.5 Requirements for the certificate 12](#_Toc188274419)

[3.6 Infrastructure for public keys 13](#_Toc188274420)

# Principles

Cryptographic solutions are subject to approval, are documented and are used throughout the SÜDVERS Group.

Cryptographic keys must be managed according to documented standards/procedures and protected against unauthorized access or destruction.

# Objectives

To protect the confidentiality of sensitive information, to maintain the integrity of important information and to confirm the identity of the sender of transactions or messages.

Ensure that cryptographic keys are not compromised (e.g. through loss, damage or disclosure), which could expose critical or sensitive information to attack

# Control en

The approach to the use of cryptographic controls in SÜDVERS must take into account the SÜDVERS classification scheme for information. The controls must apply to data at rest, in use and in transit, including data transported via mobile devices, removable media or over communication lines.

The level of cryptographic protection required must take into account the sensitivity of the information to be protected and the type, strength and quality of the encryption algorithm required. In addition, the impact of encryption on data whose content needs to be checked must be taken into account.

The implementation of encryption must take into account the regulations and national restrictions that may apply to the use of cryptographic techniques in different parts of the world, as well as the issues of cross-border flows of encrypted information.

## Cryptographic solutions

Cryptography must be used in SÜDVERS in order to:

* ensure the protection of the confidentiality of sensitive information or information that is subject to legal and regulatory encryption requirements (e.g. GDPR, DORA, ...)
* determine whether critical information has been changed (e.g. by performing hash functions or digital signing)
* enable proof of the identity of the sender of critical transactions or messages (e.g. by using digital signatures for non-repudiation).

There must be documented guidelines for the use of cryptography in SÜDVERS that include the following:

* Description of the information classification categories for which cryptographic solutions (encryption) must be used (see Information Classification Directive)
* Requirements for systems using cryptographic solutions, including (but not limited to) that
  + only trustworthy keys and certificates are accepted,
  + the protocol used only supports secure versions and configurations

When selecting and implementing a cryptographic solution, the legal aspects of encryption must be taken into account:

* Identification of legal obligations (for relevant jurisdictions)
* Assessment of the risks (including legal risks) associated with the use of cryptographic solutions (including encryption algorithms)
* Selection of a suitable cryptographic solution (e.g. in accordance with legal, regulatory and industry standards).

IT must make provisions for the management of cryptographic solutions, including the following:

* the approval of the use of cryptographic solutions
* Assignment of responsibilities for cryptographic solutions
* Dealing with conflicting laws and regulations (including dealing with licensing issues) relating to the use of cryptographic solutions in different jurisdictions (e.g. by seeking advice from the legal department)
* cryptographic solutions up to date.

The responsible IT managers should have access to this information:

* Expert technical and legal advice on the use of cryptography
* a list of approved cryptographic solutions
* an up-to-date list of cryptographic solutions.

IT must maintain a register of approved cryptographic solutions that:

* specifies the intended use of encryption within SÜDVERS
* Details of the locations (including jurisdictions) where cryptographic solutions are deployed
* contains information on the license requirements for the use of cryptographic solutions

## Cryptographic key management[[1]](#footnote-1)

Secure procedures for the generation, storage, archiving, retrieval, distribution, deactivation and deletion of cryptographic keys must be defined and documented for key management.

A key management system must be based on a set of recognized standards, procedures and secure methods for the aspects listed below:

* for generating keys for various encryption systems and applications;
* for issuing and receiving public key certificates;
* for the distribution of keys to the corresponding entities, including the question of how keys are to be activated upon receipt;
* for storing keys, including how authorized users gain access to keys;
* to change or update keys, including rules on when and how this is done;
* for dealing with compromised keys;
* revocation of keys, including how to revoke or deactivate keys [e.g. if keys have been compromised or if a user leaves an organization (in which case keys should also be archived)]. e.g. if keys have been compromised or if a user leaves an organization (in which case the keys should also be archived)];
* to restore lost or falsified keys;
* for backing up or archiving keys;
* for deleting keys;
* for logging and checking activities relating to key management;
* Definition of activation and deactivation dates for keys so that the keys can only be used for the period of time specified in the organization's key management rules;
* Dealing with court requests for access to cryptographic keys (e.g. it may be necessary to make encrypted data available in unencrypted form as evidence for a court hearing).

All cryptographic keys must be protected against alteration and loss. In addition, secret and private keys must be protected against unauthorized use and disclosure.

Facilities for generating, storing and archiving keys must be physically protected.

Ownership of cryptographic keys must be assigned to persons who:

* are made aware of their responsibility for the use and protection of the keys assigned to them (and, if applicable, the disclosure of the keys)
* must confirm that they understand their responsibility for the use and protection of cryptographic keys.

To reduce the likelihood of compromise, activation and deactivation dates for keys must be set so that the keys can only be used for a limited period of time. This period must depend on the circumstances in which the cryptographic control is used and the perceived risk.

IT must define a method for handling the "mandatory disclosure of cryptographic keys" that includes rules on the following:

* Central and company-wide management of cryptographic keys (e.g. so that a company copy of a user's cryptographic key can be disclosed)
* Establishing a system for storing cryptographic keys (e.g. if copies of the cryptographic keys are kept by an authorized external party such as a legal representative, lawyer or equivalent person)
* Advice for users who cross international borders with their computer equipment that require the transfer of cryptographic keys to authorities (e.g. for international border controls)
* Maintain procedures for responding to e-discovery requests that relate to encrypted information.

## Approved cryptographic algorithms

### Symmetric encryption

The Advanced Encryption Standard (AES) is recommended for symmetric encryption. A key length of 128 bits generally offers a sufficiently high level of security, but key lengths of 192 or 256 bits can also be used.

Operating modes that offer AEAD (Authenticated Encryption with Associated Data) should be preferred, especially Galois Counter Mode (GCM) or Counter-with-CBC-MAC (CCM).

If CTR or CBC mode is used instead, the authenticity of the encrypted text must be ensured by a suitable HMAC (see section "Data authentication").

### Asymmetric encryption

The following are recommended for asymmetric encryption:

* RSA with OAEP padding and a key length of at least 2048 bits,
* Elgamal over a finite body Fp, where p has a length of at least 2048 bits,
* Elgamal via one of the following elliptical curves: M-221, E-222, Curve1174, Cur-ve25519, E-382, M-383, Curve383187, Curve41417, Ed448-Goldilocks, M-511, E521 or one of the Brainpool curves with a bit length of at least 224.

### Cryptographic hash functions

SHA-2 and SHA-3 must be used as cryptographic hash functions.

* The output length should be at least 256 bits.
* MD5 and SHA-1 must not be used as they are considered insecure.

### Authentication of data

HMAC with SHA-2 or SHA-3 is recommended for exclusive data authentication.

Encrypted data should also be authenticated. The best choice here is an operating mode that includes authentication (AEAD operating mode). For other operating modes, an HMAC should be made via the ciphertext (Encrypt-then-MAC). The key for the HMAC should not be the same as for the cipher.

### Digital signatures

RSA, DSA, ECDSA or EdDSA are recommended for digital signatures.

With RSA, the key length should be at least 2048 bits. DSA requires two prime numbers p and q, where p should be at least 2048 bits long and q at least 256 bits long.

One of the following curves should be used for digital signing with elliptical curves ECDSA or EdDSA:

* M-221,
* E-222,
* Curve1174,
* Curve25519,
* E-382,
* M-383,
* Curve383187,
* Curve41417,
* Ed448 Goldilocks,
* M-511,
* E-521 or
* one of the Brainpool curves with a key length of at least 224 characters.

### Key exchange

The Diffie-Hellman protocol via a finite body (DH) or via elliptic curves (ECDH) is recommended for the key exchange. The key exchange must be authenticated. This prevents a man-in-the-middle attack.

For DH, the key length should be at least 2048 bits. If ECDH is used, one of the following curves must be used:

* M-221,
* E-222,
* Curve1174,
* Curve25519,
* E-382,
* M-383,
* Curve383187,
* Curve41417,
* Ed448 Goldilocks,
* M-511, E-521,
* or one of the brainpool curves with a bit length of at least 224.

A new private key (exponent) should be generated for each key exchange (Diffie-Hellman Ephemeral: DHE or ECDHE). This achieves forward secrecy and effectively prevents past traffic from being decrypted after the server's long-term private key has been compromised.

## Approved cryptographic protocols

Cryptographic protocols should always be used in their latest protocol version.

The selection of cryptographic algorithms and procedures in the context of protocols should be based on the recommendations in the previous sections.

Some additional comments and recommendations for a few selected cryptographic protocols are compiled below.

### Transport Layer Security (TLS)

The predecessor protocols of TLS 1.2 (all SSL versions, TLS1.0 and 1.1) have several vulnerabilities and should no longer be used. TLS 1.2 or TLS 1.3 should be used and configured so that the individual cryptographic primitives (encryption, key exchange and authentication) comply with the recommendations in this document.

Recommendations for TLS 1.3:

|  |  |
| --- | --- |
| Cipher Suites: | TLS\_AES\_128\_GCM\_SHA256,  TLS\_AES\_256\_GCM\_SHA384,  TLS\_AES\_128\_CCM\_SHA256,  TLS\_AES\_256\_CCM\_SHA284 |
| Supported groups: | X25519,  X448,  ffdhe2048,  ffdh3072,  ffdhe4096,  ffdhe6144,  ffdhe819 |
| Signature algorithms: | rsa\_pkcs1\_sha256,  rsa\_pkcs1\_sha384,  rsa\_pkcs1\_sha512,  rsa\_pss\_rsae\_sha256,  rsa\_pss\_rsae\_sha384,  rsa\_pss\_rsae\_sha512,  rsa\_pss\_pss\_sha256,  rsa\_pss\_pss\_sha384,  rsa\_pss\_pss\_sha512,  ed25519,  ed448 |

Recommendations for TLS 1.2:

|  |  |
| --- | --- |
| Cipher Suites: | TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256,  TLS\_DHE\_DSS\_WITH\_AES\_128\_GCM\_SHA256,  TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384,  TLS\_DHE\_DSS\_WITH\_AES\_256\_GCM\_SHA384,  TLS\_DHE\_RSA\_WITH\_AES\_128\_CCM\_SHA256,  TLS\_DHE\_DSS\_WITH\_AES\_128\_CCM\_SHA256,  TLS\_DHE\_RSA\_WITH\_AES\_256\_CCM\_SHA384,  TLS\_DHE\_DSS\_WITH\_AES\_256\_GCM\_SHA384. |
| Supported groups: | X25519,  X448,  ffdhe2048,  ffdh3072,  ffdhe4096,  ffdhe6144,  ffdhe819 |

### Secure shell (SSH)

Since SSH-1 has several critical vulnerabilities, it is considered insecure and must not be used.

SSH-2 must be used in one of its latest implementations.

Recommendations:

|  |  |
| --- | --- |
| KexAlgorithms: | diffie-hellman-group14-sha256,  diffie-hellman-group15-sha512,  diffie-hellman-group16-sha512 |
| Box numbers: | aes128-gcm,  aes256-gcm,  aes128-ctr,  aes192-ctr,  aes256-ctr |
| MACs: | hmac-sha2-256,  hmac-sha2-512 |

### IPsec

With an IPsec-based VPN, a high level of security can generally be achieved at the network level. However, a secure configuration is complex and depends heavily on the product in question.

Nevertheless, some basic recommendations can be made:

* IKEv2 should be used for the key exchange. IKEv1 should no longer be used. The use of certificates is recommended for mutual authentication. When using pre-shared keys (PSK), care should be taken to ensure that the PSKs are sufficiently long and complex. In addition to letters and numbers, PSKs should also contain special characters and have a length of at least 20 characters.
* The Encapsulating Security Payload (ESP) mechanism is used to protect confidentiality. However, it should always be used together with authenticity and integrity protection.
* If only authenticity and integrity protection is required, the Authentication Header (AH) mechanism should be used.
* The latest possible implementation of the protocol should be used.

Ideally, tested products with a suitable configuration should be used.

As an alternative to IPsec, a TLS-based VPN solution, e.g. OpenVPN, can also be used. The recommendations for TLS apply.

### WPA2/WPA3

A wired communication channel generally offers better security than a wireless one. However, if communication takes place via WiFi, the WPA2 or WPA3 protocol must be selected. Care should be taken to ensure that the latest implementations are used.

The main risks when using WPA2 are easy-to-guess passwords and the Wi-Fi Protected Setup (WPS) option.

The passwords used for WPA2/WPA3 must contain:

* + Lower case
  + Capital letters
  + Figures
  + Special characters
* The length of the password must be at least 20.
* If possible, WPS should be deactivated at the access points.

To reduce the risks, network traffic should also be encrypted (e.g. with IPsec or TLS).

## Requirements for the certificate

* The maximum expiration date for signing certificates is 1 year.
* The maximum expiry date for SSL/TLS certificates is 2 years.
* All certificates must be at least 2048 bits long.
* All certificates must be managed by the asset management company.

## Infrastructure for public keys[[2]](#footnote-2)

If a public key infrastructure (PKI) is used, one or more certification authorities (CAs) and registration authorities (RAs) must be set up and protected to ensure that the PKI

* works as intended,
* is available if required,
* adequate protection of the associated cryptographic keys and
* can be restored in the event of an emergency

A PKI must be supported by documented standards/procedures that cover the following:

* Methods for protecting important internal CA
* Integration of the public key infrastructure with the business applications and the technical IT infrastructure they will use
* Measures to be taken in the event of loss or compromise of the public key infrastructure.

A PKI must be supported by the establishment of a root certification authority in order to:

* Generate certificates with a public key (digital certificates)
* Revoke public key certificates
* Publication of public key certificates and revocation lists in directories (or similar)
* Archiving of public key certificates and certificate revocation lists in an archive database (or equivalent).

The internal CA must be protected by:

* Restricting access to a limited number of authorized persons (e.g. through strict access control mechanisms and strong authentication)
* Hardening of the operating system(s) they support
* other general security checks

The private keys of internal certification authorities must be protected by :

* Storage on approved hardware (e.g. a hardware storage module (HSM)) that is subject to strict logical and physical controls
* Distribution of the keys to several authorized persons (often referred to as secret splitting or key sharing) to prevent misuse of the CA.

The infrastructure for public keys should:

* be integrated into the SÜDVERS user identity store (e.g. Lightweight Directory Access Protocol (LDAP) directory service, Microsoft Active Directory or equivalent) so that digital certificates are available to all authorized users and applications
* use a consistent, trusted date and time source to ensure that the CA provides accurate timestamps (e.g. via the Network Time Protocol (NTP), which is supported by the Global Positioning System (GPS), atomic clocks or approved time servers on the Internet).

A Registration Authority (RA) should be established to:

* verify the identity of persons who require the use of the PKI
* Issuing authentication hardware (e.g. hardware tokens and smartcards) in connection with the PKI
* monitor the cryptographic key generation
* create and submit applications for the issuance of PKI certificates.

Comprehensive continuity and contingency plans must be developed to deal with the following situations

* Loss of infrastructure for public keys (e.g. as a result of a disaster)
* Compromise or suspected compromise of the public key infrastructure (e.g. invalidation of the root CA and all sub-CAs and revocation of all corresponding digital certificates).

Certification authorities must be configured to restrict the use of cryptographic key pairs generated for users by issuing separate key pairs for these users:

* Encrypting and decrypting information
* Creation and validation of digital signatures.

1. SÜDVERS does not consider this control to be necessary for cryptographic keys used for purposes such as system certificates in connection with AD domain membership, certificates used on web servers to ensure encrypted communication (https), e-mail encryption on a gateway-2-gateway basis, cryptographic keys for VPN connections or similar. [↑](#footnote-ref-1)
2. SÜDVERS assumes that CAs such as those used by Microsoft AD controllers (and similar) are not covered by this topic. [↑](#footnote-ref-2)