Norwegian National Security Authority

Guide

Last updated: 2016-06-06

NSM Cryptographic Requirements

Version 3.1

Cryptographic mechanisms employed within military and governmental systems to protect classified information have been proprietary and unpublished. With the advance of cryptographic products in the commercial market and the adoption of public algorithms for military and governmental use, commercially available cryptographic products can be used to protect classified systems and information. NSM address increase use of commercial crypto products by providing requirements for such implementation.

Norwegian National Security Authority

The Norwegian National Security Authority is a cross-sectoral professional and supervisory authority within the protective security services in Norway and administers Act of 20 March 1998 relating to Protective Security Services. The purpose of protective security is to counter threats to the independence and security of the realm and other vital national security interests, primarily espionage, sabotage or acts of terrorism. Protective security measures shall not be more intrusive than strictly necessary, and shall serve to promote a robust and safe society.

Purpose of guides

NSM's guidance activities are intended to build expertise and increase the security level of organisations through increased motivation, ability and willingness to carry out security measures. NSM regularly issues guides to help implement the requirements of the Security Act. NNSA also publishes guides in other professional areas relating to protective security work.

Postal address
P.O. Box 14
1306 BÆRUM
POSTTERMINAL

Civilian phone/fax
+47 67 86 40 00/+47 67 86 40 09
E-mail address
post@nsm.stat.no

Military phone/fax
515 40 00/515 40 09

URL
www.nsm.stat.no

Content

1 Introduction

The Norwegian National Security Authority (NSM) is the governmental organization authorized to approve cryptographic systems and products for the protection of information classified according to the Security Act.

Traditionally, cryptographic mechanisms employed within military and governmental systems to protect classified information have been proprietary and unpublished. With the advance of cryptographic products in the commercial market, the integration of cryptographic mechanisms in general IT-products and the adoption of public algorithms for military and governmental use, properly implemented in commercially available cryptographic products, could be strong enough to protect classified systems and information.

NSM addresses this increased use of crypto by providing requirements for such implementation.

This document supersedes *NSM Cryptographic Requirements version 3*.

1.1 Background

NSM Cryptographic Requirements is derived from *Lov om forebyggende sikkerhetstjeneste (Sikkerhetsloven)* § 14:

> *Bare kryptosystemer som er godkjent av Nasjonal sikkerhetsmyndighet, tillates brukt for beskyttelse av skjermingsverdig informasjon.*
>
> *Nasjonal sikkerhetsmyndighet er nasjonal forvalter av kryptomateriell og leverandør av kryptosikkerhetstjenester til virksomheter. Nasjonal sikkerhetsmyndighet kan likevel godkjenne andre leverandører av kryptosikkerhetstjenester.*

Further details are provided in Forskrift om informasjonssikkerhet §5-10:

> *Ved overføring, lagring og behandling av sikkerhetsgradert informasjon fastsetter NSM hvilke kryptografiske mekanismer som kreves.*
>
> *Sikring av sikkerhetsgradert informasjon ved bruk av kryptografiske mekanismer kan bare foretas med kryptoutstyr og metode for administrasjon av kryptonøkler og digitale sertifikater godkjent av NSM.*
>
> *Ved overføring av sikkerhetsgradert informasjon utenfor kontrollert område skal det benyttes kryptering og dekryptering.*

In addition, *Forskrift om informasjonssikkerhet* chapter 7 provides requirements on administration of cryptographic equipment and keys.

2 Scope

This document provides requirements and guidance to cryptographic mechanisms used to protect Norwegian classified and unclassified information, and information systems. The document gives technical requirements and guidance on cryptographic mechanisms, but does not detail the evaluation or approval process.

The document defines three levels of strength of cryptographic mechanisms. Presented in this document are requirements for the lowest two levels.

2.1 Levels of Cryptographic Mechanisms

2.1.1 ENHANCED

ENHANCED cryptographic mechanisms are mechanisms providing confidentiality protection of information classified KONFIDENSIELT, HEMMELIG and STRENGT HEMMELIG against any adversary.

The requirements for ENHANCED are classified and only available through NSM on a need-to-know basis.

2.1.2 STANDARD

STANDARD cryptographic mechanisms are mechanisms providing confidentiality protection of information classified BEGRENSET against any adversary.

In addition, STANDARD cryptographic mechanisms are mechanisms providing cryptographic separation between partitions of information systems running in partitioned mode of operation.

NSM recommends using mechanisms at STANDARD level for the protection of highly sensitive, but unclassified information.

2.1.3 MODERATE

MODERATE cryptographic mechanisms are mechanisms providing authentication, integrity protection, and confidentiality protection of data in transit for need-to-know separation within information systems running in system high mode of operation.

In addition, MODERATE cryptographic mechanisms are providing authentication and integrity protection within information systems in dedicated mode of operation.

NSM recommends using mechanisms at MODERATE level for the protection of all other sensitive, but unclassified information.

2.2 Requirements

Requirements for a particular level are the combination of general requirements and STANDARD or MODERATE specific/additional requirements.

3 Eligibility for Approval

In order for a cryptographic mechanism to be considered by NSM according to STANDARD or MODERATE, the following conditions must be met:

1. There must be an identified customer with security need of STANDARD or MODERATE
2. The vendor/developer must be based in Norway or a country approved by NSM
3. The product/module must be evaluated and/or certified
4. The vendor/developer must provide a submission package with relevant information

Relevant information includes, but is not limited to:

- Evaluation and certification status
- Analysis of threats the product is intended to protect against
- Analysis of how the product meets the requirements in this document
- Mitigation of other attacks, such as TEMPEST[1] and side-channel attacks
- Algorithms, modes and key lengths in use and for what purpose(s)
- Key management mechanisms, especially key generation, use and erase
- List of all software modules, libraries, etc. used, with version number and date

4 General Requirements

General requirements follow from *Forskrift om informasjonssikkerhet*, chapters 5 A and 5 B.

- For cryptographic modules, security principles from §5-5 are especially important.
- For integrated cryptographic mechanisms providing security within a system, requirements for security functionality and assurance from §5-9 are especially important.

Protection mechanisms, such as algorithms, standards and protocols, shall be based on open and/or public standards. Proprietary mechanisms shall be avoided.

4.1 Availability of Products

NSM requires that products submitted for approval for STANDARD and MODERATE become generally available. The vendor and/or distributor should make the product and product information generally available before the product is approved.

[1] TEMPEST requirements are applicable for the use of systems outside of Norway.

5 Functional Requirements

Cryptographic mechanisms are in support of a security function. The required security functionality in the information system mandates what cryptographic functionality is needed. Only the necessary cryptographic mechanisms for a particular functionality needs to and should be implemented.

The basis for cryptographic functionality is the cryptographic primitives described in chapter 8 and schemes described in chapter 9.

6 Primitives

6.1 Block Ciphers

Block ciphers are permutation functions that for an *m*-bit message and *n*-bit key produce a *d*-bit ciphertext. The function should be computationally infeasible to invert without knowing the key.

Approved block ciphers are:

ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard (AES) defined in *FIPS PUB 197 Advanced Encryption Standard (AES), November 26, 2001*. AES is a 128-bit block cipher that supports key-lengths of 128, 192 and 256 bits.

Approved key lengths are 128 and 256 bits.

6.2 Hash Functions

Hash-functions are functions that take a message of potentially infinite length as input and produce a finite length cryptographic message digest (a hash) as output. The hash of a message is sometimes called a fingerprint.

Approved hash function is:

SHA-2

Secure Hash Algorithm 2 (SHA-2) defined in *NIST in FIPS PUB 180-4 Secure Hash Standard (SHS), March 2012*.

Approved hash function lengths are 256, 384 and 512 bits.

7 Schemes

7.1 Block Cipher Modes of Operation

A mode of operation specifies how a block cipher operates and describes the details necessary to encrypt data securely. It describes how nonces and keys are combined with cryptographic primitives in order to provide secure encryption. Note that none of the modes in this section provides integrity protection, a feature only achieved if combined with an approved MAC or a dedicated authenticated mode. In general, NSM recommends the use of authenticated encryption.

Approved modes of operation are:

COUNTER MODE (CTR)

CTR turns a block cipher into a stream cipher by encrypting an incremental counter starting at a unique value (nonce) defined by the IV. The mode does not require padding. This is the recommended mode if no integrity protection is required. This mode is highly parallelizable and does not require separate implementation of decryption.

CIPHER BLOCK CHAINING (CBC)

CBC is a widely used mode. This mode requires a separate implementation of decryption. This mode is prone to bit-errors. Bit errors in one ciphertext will corrupt two consecutive plaintexts. This mode requires the use of a secure padding-scheme to avoid padding-oracle attacks.

XEX TWEAKABLE BLOCK CIPHER WITH CIPHERTEXT STEALING (XTS-AES)

XTS-AES is designed for encryption of data at rest. This mode does not provide full integrity protection, but does provide countermeasures against adversaries seeking to manipulate ciphertext.

7.2 Message Authentication Codes

Message authentication codes provide authentication of messages. While hash functions provide cryptographically secure integrity protection, a MAC provides authenticity in addition.

Approved MACs are:

CIPHER-BASED MAC (CMAC)

Cipher-based MAC (CMAC) is specified in *NIST SP 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication* and defines a block cipher based message authentication code algorithm. CMAC is used to ensure the authenticity and integrity of a message.

HASH-BASED MAC (HMAC)

HMAC is specified in *FIPS PUB 198-1 The Keyed-Hash Message Authentication Code (HMAC)* and provides authenticity and integrity protection for messages. HMAC can be used with the approved hash function.

7.3 Authenticated Encryption

Authenticated encryption modes provide both integrity and authenticity. These modes are typically either one-pass or two-pass. Two-pass modes are modes that separate the computation of encryption and authentication tags. Hence, one-pass are usually much faster.

Approved authenticated encryption modes are:

AES GALOIS COUNTER MODE (AES-GCM)

GCM is a one-pass authenticated counter mode. GCM employs universal hashing to protect against adversaries that seek to manipulate data. It is strongly advised against using short authentication tags in GCM.

COUNTER WITH CBC-MAC (CCM)

CCM is a two-pass authenticated mode that combines AES-CTR with CBC-MAC. Being two-pass, this mode is slower than GCM.

7.4 Key Wrap

Key Wrap (KW) is intended to protect the confidentiality and integrity of cryptographic keys. It is characterized by taking as input a secret key (K), a key-encryption key (KEK) to produce a wrapped key W.

Approved key wrap functions are:

AES KEY WRAP (KW)

AES Key Wrap (KW) as defined in *NIST SP 800-38 F Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping* specifies wrapping and ensures the confidentiality and integrity of cryptographic keys.

AES KEY WRAP WITH PADDING (KWP)

AES Key Wrap with Padding (KWP) as defined in *NIST SP 800-38 F Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping* extends KW by specifying a padding scheme. Note that although KW can be used with any padding scheme, KWP is defined to seek interoperability.

7.5 Key Derivation Functions

Key Derivation Functions (KDFs) are used to derive keys from random strings. A KDF takes as input some random secret strings possibly together with additional non-secret data to allow for larger variations.

Approved key derivation functions are:

EXTRACT-THEN-EXPAND

Key derivation as defined in *NIST SP 800-56C Recommendation for Key Derivation through Extraction-then-Expansion*.

7.6 Digital Signatures

Digital signatures can provide integrity protection and authentication.

Note that digital signatures for nonRepudiation or contentCommitment is not supported by this document.

Approved asymmetric signature algorithms are:

ELLIPTICAL CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA)

ECDSA as defined by NIST in *FIPS PUB 186-4 Digital Signature Standard (DSS), Issued July 2013*. ECDSA implements the Digital Signature Algorithm using elliptic curves. A clear benefit of using elliptic curves includes shorter keys and faster generation and verification of signatures.

Approved key lengths for ECDSA are 256 and 384 bits.

Approved message authentication algorithms will be dependent on system and use case.

Note that NSM does no longer see RSA and RSA-DSS as a viable alternative for future long-term security.

7.7 Key Exchange

Key Exchange algorithms use public key cryptography to mainly negotiate and transport secret keys.

Approved key exchange algorithms are:

ELLIPTIC CURVE DIFFIE-HELLMAN (ECDH)

ECDH as defined in *NIST SP 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm* implements Diffie-Hellman (DH) using elliptic curve cryptography.

Approved key lengths are 256 and 384 bits.

It is recommended to implement forward secrecy and authenticated key establishment.

Note that NSM does no longer see RSA and RSA-DH as a viable alternative for future long-term security.

7.8 Elliptic Curves

Elliptic curve cryptography uses elliptic curve transformations to perform cryptographic operations.

Approved elliptic curves are:

BRAINPOOL CURVES

Brainpool Curves as defined in *ECC Brainpool Standard Curves and Curve Generation v. 1.0*.

Approved key lengths are 256, 384 and 512 bits. The names of the approved curves are BrainpoolP256r1, BrainpoolP384r1 and BrainpoolP512r1.

NIST CURVES

NIST curves as defined in *Recommended Elliptic Curves for Federal Government Use July 1999*.

Approved key lengths are 256, 384 and 521 bits. The names of the approved curves are NIST P-256, NIST P-384 and NIST P-521.

7.9 Additional Allowed Mechanisms for STANDARD

In addition, the allowed algorithms and key lengths for STANDARD are as follows.

7.9.1 Integrity Protection and Authentication

RSA algorithm with key length of 2048 bits may be used until 2017-12-31.

Approval of the use of this mechanism will be reviewed and approved on a case-by-case basis.

7.9.2 Key Establishment

RSA and DH algorithms with key length of 2048 bits may be used until 2017-12-31.

Approval of the use of these mechanisms will be reviewed and approved on a case-by-case basis.

7.9.3 Hash Functions

SHA-2 with length of 224 bits will be allowed until 2015-12-31.

Note that the use of SHA-1 is not allowed, including online transactions/key establishment.

7.10 Additional Approved Security Functions for MODERATE

Additionally, the following algorithms and key lengths for MODERATE are allowed, though it is advised to avoid them when implementing new systems.

7.10.1 Integrity Protection and Authentication

RSA algorithm with key length of 2048 bits may be used until 2019-12-31.

7.10.2 Key Establishment

RSA and DH algorithms with key length of 2048 bits may be used until 2019-12-31.

8 Assurance Requirements

As stated under General Requirements, requirements from *Forskrift om informasjonssikkerhet* applies.

All cryptographic mechanisms shall have been validated using test vectors (correctness). The secure operation of cryptographic mechanisms is dependent on the secure implementation of said mechanisms. Evaluations and/or certifications shall include the analysis of secure implementations, in addition to robustness

The relevant evaluations and certifications and levels are specified below.

8.1 Assurance Requirements for STANDARD

Cryptographic modules generating, protecting and using long-term[2] private keys shall be evaluated against Common Criteria, FIPS 140-2 or other equivalent evaluation scheme.

Cryptographic modules generating and using private keys should be approved according to *Security IC Platform Protection Profile (BSI-PP-0035)* or *Security IC Platform Protection Profile with Augmentation Packages Version 1.0 (BSI-CC-PP-0084-2014)*.

- Approved Common Criteria Assurance Evaluation Levels are 4 and above
- The use of other Protection Profiles or Target of Evaluations shall be approved by NSM

Note that Common Criteria certification does not necessarily include cryptographic mechanisms. If not, additional evaluations, such as FIPS 140-2 must be performed.

- Approved FIPS 140-2 Security Levels are 3 and 4
- The use of other evaluations and evaluation schemes shall be approved by NSM

Cryptographic modules generating and using session keys[3] shall be evaluated against Common Criteria, FIPS 140-2, or other equivalent evaluation scheme or vendor specific integration evaluation.

- Approved Common Criteria Evaluation Assurance Levels are 2 and above
- Approved FIPS 140-2 Security Levels are 1 and above

8.2 Assurance Requirements for MODERATE

Cryptographic modules generating, protecting and using keys shall be evaluated against Common Criteria, FIPS 140-2 or other equivalent evaluation scheme.

- Approved Common Criteria Evaluation Assurance Levels are 2 and above
- Approved FIPS 140-2 Security Levels are 1 and above

[2] Long-term private keys are keys used for more than one session.

[3] This includes other keys used only once, such as temporary keys and ephemeral keys, and non-keying material such as nonces and salts.

9 Key Management Requirements

NSM requires the use of asymmetric key management through certificates and Public Key Infrastructure (PKI) for management of long-term keys.

Key management solutions shall be evaluated and/or certified according to a recognized evaluation or certification scheme and profile.

Key management of long-term keys shall be under two-person control, except for personal long-term keys under owner's control. The latter includes keys for devices under sponsor[4] control.

Input and output of critical security parameters shall be through trusted paths.

9.1 Key Generation

Random Number Generators (RNG) must be approved by NSM.

Keys shall be generated by a secure key generation process using seed from an approved RNG. Output from RNG shall be post-processed.

Session keys and other related key material[5] should be generated by the same secure key generation process and be generated within the cryptographic module that protects the long-term private key.

Keys shall be generated such that the compromise of one key shall not compromise other keys.

9.1.1 Specific Requirements for STANDARD

Private keys shall be generated within a hardware cryptographic module.

Secret keys protecting large amount of information and/or being used for long time shall be generated by hardware RNG.

9.1.2 Specific Recommendations for MODERATE

Generation of keys to be used in other cryptographic modules shall be performed in hardware.

9.2 Key Protection and Lifetime

9.2.1 Specific Requirements for STANDARD

Private keys shall be protected by hardware cryptographic module or encrypted. Encryption mechanism and key shall be as strong as the private key is to be used for.

- Elliptical curve keys for users and devices can be valid for up to 39 months.

Secret keys shall when not in use, be encrypted with asymmetric mechanisms of equal strength.

Secret keys may be wrapped with other secret keys before being encrypted with asymmetric mechanisms.

[4] Sponsor is the person (typically equipment administrator) who is responsible for management of keys used in equipment (such as network devices) not operated directly by the sponsor.

[5] This includes other keys used only once, such as temporary keys and ephemeral keys, and non-keying material such as nonces and salts.

9.2.2 Specific Requirements for MODERATE

Private keys shall be protected. Protection mechanism shall be described.

- Private keys in hardware cryptographic modules can be valid for up to 66 months. This does not limit the lifetime of CA certificates.
- Private keys in hardware cryptographic modules for high volume systems shall not be valid for more than 25 months.
- Private keys in software cryptographic modules shall not be valid longer than 13 months.
- Private keys in software cryptographic modules for high volume systems shall not be valid for more than 7 months.

Note that private keys in software cryptographic modules for MODERATE may only provide protection of data in transit. For long-term integrity protection, such as for code, hardware cryptographic modules are required.

Private keys in software cryptographic modules shall be securely deleted when moved from a storage location/device. Private keys in software cryptographic modules shall be excluded from general backup.

The use of private keys in software cryptographic modules shall be monitored to detect misuse.

Private keys corresponding to CA certificates shall be in hardware cryptographic modules.

9.3 Key Accounting

All asymmetric keys shall be accounted. Accounting shall at least include:

- The issued certificate
- The registration officer who approved the certificate issuance
- The certificate holder (user or sponsor)
- The purpose of the certificate (human readable)
- The key generation device (cryptographic module; serial number if applicable)
- The key storage device(s) (if other than key generation device; serial number if applicable)
- Certificate validity period (from, to)
- Private key validity period (from, to)
- Revocation Information (if applicable)

The use of asymmetric keys should be monitored and key use should be counted.

9.4 Key Deletion

Keys shall be deleted as soon as possible after use.

- Keys in RAM shall be securely deleted after use.
- Session[6] keys shall be securely deleted once the session is over.
- Private keys shall be securely deleted at latest when process using the keys is shut down.

The mechanisms used for secure key deletion must be described.

[6] This includes other keys used only once, such as temporary keys and ephemeral keys.

10 Requirements for PKI

10.1 PKI Architecture and Trust

The PKI shall have a hierarchical trust model.

Interoperability with other PKIs shall be at root level.

If separate algorithms are needed for different uses, separate PKIs may be used. If not, one PKI with different policies should be used.

All PKIs used in a classified information system must be approved by NSM. This includes PKIs used by platform and/or devices for initial integrity protection, such as code integrity.

Certificate Pinning should be implemented to prevent digital certificates from trusted PKIs to be used for unauthorised applications or services.

10.2 Requirements for Certificates

Certificates, Certificate Revocation Lists (CRL) and Authority Revocation Lists (ARL) shall comply with Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280).

Certificates shall uniquely identify the holder or sponsor. Certificate subject field should provide human readable information regarding the certificate holder or sponsor.

All certificates shall be unique and (at minimum) public keys and serial numbers shall be unique.

- Certificates can be re-keyed, but not re-certified.
- Serial numbers shall be unique within a CA and should be unique within the PKI.

All certificates shall contain information required to perform certificate status verification, such as:

- Certificate validity period
- Key Usage
- Application policies
- CRL Distribution Points and/or Authority Information Access

All Certification Authorities shall publish Certificate Revocation Lists or Authority Revocation Lists. In addition, other mechanisms to provide certificate status information should be provided, such as Online Certificate Status Protocol (OCSP).

All certificates shall include the keyUsage certificate extension and mark it critical.

- Certificates shall be revoked when the trust is reduced and the revocation reason shall be provided.

As soon as possible after notification of private key compromise or other incident reducing the trust in the certificate, the certificate shall be revoked.

- Whenever several certificates are revoked within a short period of time an out-of-band CRL should be published.

Certificates shall be validated before use. Revoked, invalid or other ways unfit certificates shall be rejected.

10.3 Requirements for Certificate Issuance

Certificate Authorities or Registration Authorities shall verify the quality and uniqueness of each key before issuing a certificate. If weak keys are discovered or same keys have been used before, the CA shall deny the certificate request. The RA and/or CA shall notify the CA operator about the event.

Note that the reissue of a certificate where a name is changed (user certificate) or a domain is added (TLS certificate), will be accepted.

Certificate Authorities shall issue either subordinate CA certificates or end entity certificates. A CA shall not issue both type of certificates.

- Private keys corresponding to certificates with keyCertSign bit set can only be used in combination with crlSign.

10.4 Requirements for Private Key Protection

Some addition requirements are specified for private keys corresponding to certificates with specific key usages.

- Private keys corresponding to certificates with keyCertSign bit set shall be in hardware cryptographic module.
- Private keys corresponding to certificates with digitalSignature keyUsage bit set shall not be archived.

10.4.1 Specific requirements for STANDARD

NSM shall be the policy authority for PKI for STANDARD and operate the root certification authority (Root CA).

The operators of subordinate CAs can be system owners or PKI service provider. Operators must be approved by NSM.

Private keys corresponding to certificates with cRLSign or digitalSignature keyUsage bit set, should be generated within the cryptographic module they will be used.

10.4.2 Specific Requirements for MODERATE

NSM shall be the policy authority for PKI for MODERATE and operate the root certification authority (Root CA) in classified systems.

Note that this does not preclude the use of third party PKIs for system internal security, such as code signing.