Norwegian National Security Authority

Guide

Last updated: 2007-01-24

Digital Certificates and PKI version 2.0

Technical Infosec Guidance on Digital Certificates and Public Key Infrastructure in System High CIS

This document gives guidance and technical security requirements for the use of digital certificates and public key infrastructure (PKI) within Norwegian classified system high information systems.

Digital certificates are used for authentication, integrity protection, and key management for confidentiality services, and are managed by the PKI.

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. NSM 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
http://www.nsm.stat.no/

Content

1 Introduction

Asymmetric cryptography uses a key pair instead of a single key. The two keys in a key pair are mathematically dependent, and referred to as the private and public key. The private key is to be kept private by the owner, while the public key can be made publicly available.

For confidentiality services, the public key is used for encryption, requiring the private key for decryption. For integrity, authentication and non-repudiation services, the private key is required for signing, using the public key for verification.

These security mechanisms rely on the identification of the key pair holder. To make a secure binding between the key pair and the holder, a digital certificate is used. The digital certificate contains the public key, the identity of the holder and a digital signature to verify the binding.

To manage such bindings between several key pairs and holders, a certificate management system is used. Certification Authorities (CA) issue, maintain and revoke digital certificates, and are bound together to represent a Public Key Infrastructure (PKI).

Typical usage areas for digital certificates are digital signature in documents and email to provide integrity protection; digital signatures for authentication; and encryption for confidentiality protection of files and web services.

1.1 Background

The Security Act, §14, states: “Only cryptosystems that have been approved by the National Security Authority are allowed to be used to protect classified information”. With the publication of “NSM Cryptographic Requirements”, cryptographic requirements such as algorithms, key lengths and key management are provided, but functional requirements for digital certificates and PKI are not provided.

In addition to The Security Act, regulation amendment to the security act, chapter 7 “Administrative Cryptosecurity” gives regulation on the use and handling of keys and cryptosystems.

This guidance supersedes Technical Guidance no. 2 Digital Certificates and Public Key Infrastructure in System High CIS.

1.2 Purpose

The purpose of this directive is to provide functional and technical security requirements for the use of digital certificates and PKI within a Norwegian Classified System High CIS.

With the increased use of PKI and introduction of a classified PKI in Norway, these requirements are provided to establish and maintain a high level of trust to the PKI and System High CIS.

To make the document easier to read, requirements are provided in yellow text-boxes, while prohibitions are provided in red text-boxes.

1.3 References

- Lov om forebyggende sikkerhetstjeneste (The Security Act)
  http://www.lovdata.no/all/hl-19980320-010.html
  http://www.ub.uio.no/ujur/ulovdata/lov-19980320-010-eng.pdf
- Forskrift om informasjonssikkerhet (Regulation amendment to The Security Act)
  http://www.lovdata.no/for/sf/fo/fo-20010701-0744.html
- NSM Cryptographic Requirements version 2.0
  http://www.nsm.stat.no/dokumenter/Veiledninger%20s3/NSM%20Cryptographic%20Requirements%202.0.pdf
- V-FN-01 Veiledning i grunnleggende sikkerhetsarkitektur og -funksjonalitet for FELLESNIVÅ operasjonsmåte (General requirements for SYSTEM HIGH)
  http://www.nsm.stat.no/dokumenter/Veiledninger%20s3/V-FN-01_Fellesnivaa_operasjonsmaate2002-04-17.pdf
- Beskyttelsesinstruksen (The Protection Decree)
  http://www.lovdata.no/for/sf/in/xm-19720317-3352.html

1.4 Definitions

Abbreviation	Definition
ARL	Authority Revocation List
CA	Certification Authority
CAPI	Crypto API in Microsoft Windows
CC	Common Criteria
CIMC	Certificate and Issuing Management Components
CIS	Communication and Information System
CNG	Next-Generation Crypto (Crypto architecture in Microsoft Windows)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
cRLSign	Bit 6 of keyUsage bitstring
digitalSignature	Bit 0 of keyUsage bitstring
DS	Directory Service
EAL	Evaluation Assurance Level
EE	End-entity
Hardware Cryptographic Module	A cryptographic module subject to requirements in FIPS 140-2, chapter 4.5 Physical Security
HSM	Hardware Security Module
Intermediate CA	CA with certificate issued from a superior CA and issuing certificates to subordinate CA(s)
Issuing CA	CA issuing certificates to EE
KA	Key Archive for private keys
keyCertSign	Bit 5 of keyUsage bitstring
keyUsage	The certificate extension defining the allowed key usage(s) for the certificate and corresponding private key. The keyUsage OID is 2.5.29.15.
nonRepudiation	Bit 1 of keyUsage bitstring
NCR	NSM Cryptographic Requirements
OCSP	Online Certificate Status Protocol
PK	Public Key
PKCS	Public-Key Cryptographic Standard
PKI	Public Key Infrastructure
PP	Protection Profile
RA	Registration Authority
Re-certification	Re-issuance of existing certificate and key pair
Re-key	Re-issuance of existing certificate with a new key pair
System High	An operational mode for information systems where: Users are cleared for the highest classification-level of the system. Users are authorized to work with all classifications handled by the system. Users do not have need-to-know for all classified information handled by the system.

2 PKI Architecture and Trust

The PKI is established to provide trust in digital certificates.

The PKI shall have a hierarchical trust model with a common root CA

A hierarchical trust model enables trust between different CA systems subordinate to the root and between different applications. The PKI hierarchy should be shallow for efficiency, yet deep for manageability. A 3-tier hierarchy should be sufficient in most cases.

NSM shall be policy authority for the PKI and operate the root CA

This document shall be used as input to the CP and CPS for a PKI within a Norwegian System High CIS. The requirements here may be refined and extended in the CP and CPS.

By owning the CP and operating the root, NSM maintains control over the PKI while allowing for distributed key and certificate management.

Interoperability with other PKIs shall be at root level

The PKI system should support multiple interconnection methods including cross certification, multiple trust anchors and bridge CA, to enable interoperability with external PKIs.

Use of PKIs not operated by NSM must be approved by NSM

In addition to PKIs operated by NSM, PKIs operated by NATO and NATO NATIONs can be approved for handling classified information within Norwegian CIS. This requires that the PKIs are approved by both NSM and NATO or vendor NATO NATION for handling classified information.

For protection of the enterprise platform, NSM can approve the use of commercial PKIs. Such PKIs may only be used for authentication/integrity protection of code. A complete list of all other PKIs used within the CIS must be presented for approval by NSM.

Certificates and corresponding private keys shall not be used as authorization

Digital certificates used for authentication shall only authenticate the certificate holder towards his CIS user account. For authorization, the CIS shall use its authorization mechanisms towards information, application and services.

3 System Design Requirements

3.1 Systems Integration

The PKI provides digital certificates and key management to a number of users and services, and is considered a security critical component. In addition, it is dependant on other security critical components, such as repositories, for its operations. This requires a tight integration between the PKI and the CIS applications and services.

For general System High requirements, see 0. Contact NSM for systems design and integration requirements.

3.2 System Overview

A PKI system shall consist of a relevant number of the following components depending on the size and use of the PKI. In CIS where certified components providing same or similar functionality already exist, these mechanisms should be used.

The PKI system shall include the following components:

- Certificate Authority (CA)
- Registration Authority (RA)
- Client modules
- Cryptographic modules

In addition, the system should include some of the following components depending on the size of the PKI and what security services it will provide certificates for:

- Centralized key generator
- Validation Authority (VA)
- Key Archive (KA)
- Time Stamp Authority (TA)

3.3 Evaluated and Certified Components

The use of evaluated and certified components is critical to maintain the trust and assurance of the PKI and the CIS it is serving.

PKI products shall be evaluated to an assurance level of CC EAL 4 or higher

Evaluation and certification shall be performed according to CIMC Security Level 3 or higher

To establish the same level of security as the CIS platform and security mechanisms, PKI components must meet the requirements of CIMC. CIMC defines several PKI components in addition to CA and RA services. All components must meet the certification requirement.

Requirements for cryptographic products and modules used in the PKI are stated in NCR. This includes requirements for applications and services using digital certificates for security services, commonly referred to as PK-enabled applications and services.

Cryptographic requirements stated in this document shall be considered as additions to NCR.

If the PK-enabled product is not CC certified against any relevant product specific PPs, the product should be certified against a PP for PK-enabled applications.

3.4 Standards Compliance

The use of standards is important to achieve security and interoperability.

Digital certificates and PKI shall comply with guidance and requirements in relevant standards

Guidance and requirements from standards shall be met. Guidance includes best practices and SHOULD-statements from relevant standards. If requirements from standards are in conflict with requirements stated in this document, the conflicting requirements shall be presented to NSM for consideration.

Relevant standards include, but are not limited to:

Table 1 **Component**	**Standard**
Certificate/Certificate Revocation List	RFC3280 with update (RFC3280bis)
Cryptographic Token Interfaces	PKCS#11, CAPI, CNG
Cryptographic Message Syntax	PKCS#7, PKCS#10
Certificate Policy, Certification Practice Statement	RFC3647
Online Certificate Status Protocol	RFC2560

3.5 Certificate Profile

The certificate profile details the format and contents of the issued digital certificates.

Certificates, CRLs and ARLs shall comply with RFC3280 x.509 v3 profile

All certificates shall include the certificate policies (OID 2.5.29.32) extension and mark it critical.

Certificates shall uniquely identify the certificate holder or sponsor

The certificate holder or sponsor shall be uniquely identified in the certificate and should be linked to a user account in the CIS. This can be done through the Subject field, or other relevant certificate extension. If other relevant certificate extension is used, the Subject field shall contain relevant user information, such as name and organization.

All certificates shall be unique

Even though several certificate fields may contain the same information for each certificate holder or sponsor, at least the certificate serial number and public key shall be unique for each certificate. This does not prevent different CAs from issuing certificates with the same serial number.

Certificates for personal users shall support the use of Norwegian letters.

All certificates shall contain information required for certificate validation

All information required for certificate validation (see chapter 5.1) must be included in the certificates.

All certificates shall include the key usage certificate extension and mark it critical

By including the key usage (OID 2.5.29.15) certificate extension, the certificate and corresponding private key is limited to the key usage(s) specified in the certificate. By marking the extension critical, applications and services using a certificate or private key must ensure that the key usage is allowed before using the certificate or private key. If the key usage is not allowed, the certificate or private key shall be rejected. See chapter 5.1.

EE certificates should include the extended key usage (OID 2.5.29.37) certificate extension and mark it critical. By including the extended key usage certificate extension, the certificate and corresponding private key is limited to the extended key usage(s) specified in the certificate.

3.6 Private Key Protection

Cryptographic requirements for key generation and private key protection are stated in NCR. The following requirements are additions to NCR.

Private keys corresponding to certificates with keyCertSign keyUsage bit set, shall only be used in combination with crlSign

Private keys corresponding to CA certificates shall only be used for signing certificates or CRLs. If the CA needs certificates for other key usages, separate key pair(s) shall be used to prevent misuse of its certificate/CRL signing certificate.

Private keys corresponding to certificates with nonRepudiation keyUsage bit set, shall not be used in combination with other key usages

Non-repudiation certificates shall only be used for digital signatures in support of a non-repudiation service. A separate non-repudiation certificate is designed to prevent misuse, or exploitation of the non-repudiation support.

Private keys corresponding to certificates with digitalSignature, keyCertSign or nonRepudiation keyUsage bit set, shall be in hardware cryptographic module

For infrastructure components, such as computers, firewalls and routers, private keys corresponding to digitalSignature may be in software cryptographic modules.

Private keys corresponding to certificates with digitalSignature or nonRepudiation keyUsage bit set, shall not be archived

Both private keys corresponding to certificates with only digitalSignature or nonRepudiation, and private keys corresponding to certificates with digitalSignature in combination with other key usage(s) shall not be archived.

- Certificates with only digitalSignature or nonRepudiation are used for integrity protection and authentication. The loss of the corresponding private keys will therefore not result in loss of data. In addition, archiving such private keys decreases the trustworthiness of the PKI's integrity protection, authentication or non-repudiation services provided.

- Certificates with digitalSignature in combination with other key usages should only be used for authenticated key establishment of symmetric key for confidentiality protection of data communication. The loss of the corresponding private keys will not result in loss of data.

Private keys corresponding to CA certificates may be archived.

- CA certificates are used for signing certificates and CRLs, and the loss of the corresponding private key may invalidate all certificates subordinate to the CA. For business continuity and disaster recovery, the private key corresponding to the CA certificate may be archived. For availability purposes, the private key may be shared between several HSMs. Such key distribution/sharing shall be performed either with approved mechanisms provided by the HSM vendor, or by manual archive/restore mechanisms under two-person control.
- No single KA operator shall be able to restore the CA private key. CA private key backup shall be under two-person control.

Private keys corresponding to pure confidentiality certificates should be archived.

- Confidentiality certificates are used for data encryption, and the loss of the corresponding private key could lead to loss of data. Confidentiality private keys should be archived by certificate holder and/or archived by KA operators. Key recovery for EE private keys shall be performed by EE alone or KA operators under two-person control.

If confidentiality keys are not archived, other mechanisms must be in place to provide data recovery.

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

This paragraph implies that a fully conformant PKI system supports 4 different certificate types per EE if all services are provided:

- Multipurpose integrity and authentication key pair – in hardware, not backed up
- Multipurpose confidentiality key pair – backed up
- Multipurpose combination (conf & non-conf) key pair – in hardware, not backed up
- Non-repudiation – in hardware, not backed up

For CIS where non-repudiation services are not required and data recovery is provided by other means than key recovery, a single multipurpose confidentiality certificate per EE may be sufficient.

4 Certificate Management

4.1 Certificate Issuance

The RA shall register users and certificate requests

The RA shall register users and request certificates on their behalf. The RA shall securely identify and authenticate the users according to CP, CPS and procedures before sending certificate requests to a CA. The RA shall ensure that the relevant information is provided in the certificate, and verify that names abide by the naming rules defined in policy and procedures. The RA shall reject certificate requests that do not comply with the policy and procedures.

The RA may be geographically distributed to enable local user registration.

Communication between RA and CA must be authenticated and logged. If key archive is performed and private key is communicated between RA and KA/CA, the communication must be confidentiality protected.

CAs shall either issue subordinate CA certificates or EE certificates

Root CA and intermediate CAs shall not issue certificates to EEs. This does not prevent CAs issuing certificates to its operators.

All CA certificates shall be published and generally available within the respective CIS. EE certificates may be published depending usage areas:

- Multipurpose integrity and authentication, and multipurpose combination certificates are usually provided together with the information they protect, thus not required generally available.
- Multipurpose confidentiality certificates may be required generally available to provide data encryption. Such use can be, but is not limited to, email encryption, where sender needs to encrypt the email with the recipients confidentiality certificate.
- Certificates or certificate requests specially marked not for publication shall not be published

Every CA shall archive all certificates, CRLs and ARLs it issues

The PKI must provide a validation service if services requiring long-time signature validation are implemented.

4.2 Certificate Renewal

Certificates are issued with a validity period and may be renewed prior to expiration to enable continued use.

The PKI shall support routine renewal of certificates before certificate expiration

Certificate renewal should be automated.

While re-keying is allowed for EE certificates, re-certification is not.

4.3 Certificate Revocation

Certificate revocation is performed to prevent invalid certificates from being used prior to their expiration date.

Certificates shall be revoked when the certificate trust is reduced.

The revocation reason shall be provided.

Reasons for certificate revocation can be, but are not limited to, private key compromise, changes in certificate holder information, or no longer need for the certificate. Certificates shall not be suspended.

All CAs shall issue CRLs or ARLs

The PKI system shall provide certificate revocation information. In addition to CRLs, other certificate status mechanisms may be provided. Such mechanisms can be, but are not limited to, OCSP and direct CA database query.

To provide updated status information when using an offline certificate status mechanism, CRLs should be published frequently.

All Issuing CAs shall issue a CRL at least every 4 hours. CRL lifetime should be at most 2 CRL publication intervals.

To prevent loss of service because of network propagation delays, CRL lifetime can be up to 2 CRL publication intervals. CRL lifetime should not be significantly longer than the CRL publication interval plus the normal network propagation delay. Other mechanisms to prevent network propagation delays should also be in place. Such mechanisms can be, but are not limited to, publication of CRLs to multiple repositories, and redundant network connections.

For Intermediate CAs, the CRL publication interval may be longer than 4 hours and should be designed in relation to the CA hierarchy. The CRL lifetime shall be significantly less than 2 CRL publication intervals.

Mechanisms may be used to control the size of CRLs, such as delta CRLs, partitioned CRLs and certificate renewal with re-keying. The mechanism(s) must be supported by all components using private keys and certificates before being employed.

4.4 Certificate Termination

When certificates expire and the corresponding private key is no longer needed, the private key shall be deleted.

Expired certificates can be removed from CRLs after one whole CRL publication interval after expiration time to control the size of the CRL. See 4.3 for information on mechanisms to control the size of CRLs.

The PKI must provide a validation service if services requiring long-time signature validation are implemented.

5 Usage Requirements

Specific requirements for PK-enabled applications and services are not within the scope of this document. But some general guidance is provided.

Applications and services using digital certificates for security services should reuse certified mechanisms provided in the platform for certificate validation, signature verification, encryption and decryption.

5.1 Certificate Validation

To maintain trust in the digital certificates and PKI, the applications and services using digital certificates for security services must handle the certificates and private keys correctly.

Before a private or public key is used, the corresponding digital certificate shall be validated

The digital certificate validation shall include, but is not limited to:

- Validity period
- Revocation information
- Certificate chain (full path) to trusted root
- Applicability
- Certificate Policy

If a validation failure occurs, the public or private key usage depends on the application and type of failure, such as:

- For invalid certificates with digitalSignature keyUsage bit set, private keys shall not be used.
- For invalid or revoked confidentiality certificates, only private keys may be used. This allows encrypted content to be decrypted. For re-encryption, a new confidentiality certificate shall be used.
- For certificates with incorrect CP, applicability or keyUsage, neither certificate nor private key shall be used.
- For certificates without available revocation information, the certificate and private key may be used.
- For revoked integrity and authentication certificates, neither certificate nor private key shall be used.
- For certificates chaining to an un-trusted root, neither certificate nor private key shall be used.

6 Publication, updates and contact address

6.1 Publication and updates

This document is published on NSM's web site, http://www.nsm.stat.no/, and can be obtained by contacting NSM. Updates to this document will result in a higher version number. New versions of this document will be published and can be obtained in the same manner.

6.2 Contact address

To comment this document or obtain the latest version, send an email to post@nsm.stat.no with subject "PKI Guidance" or write to:

NSM,
Avdeling for Teknisk Sikkerhet,
PB 14,
NO-1306 BPT,
NORWAY

Annex A Document check

2004-09-29	T-02 Digital Certificates and Public Key Infrastructure in System High CIS approved
2007-01-24	Document approved