Requirements specification for PKI in the public sector

Version 2.0
June 2010

Contents

1. Introduction 4
   1.1 Objective and background 4
   1.2 A summary of the scope of the requirements specification 4
   1.3 Use of the requirements specification upon self-declaration 7
   1.4 Use of the requirements specification for procurement 7
2. Scope and conditions 8
   2.1 Certificate classes 8
   2.2 Security levels 8
   2.3 Explanation of classification of requirements 14
   2.4 Explanation of the requirements table 16
3. Definition of terms, abbreviations and references 16
   3.1 Definition of terms 16
   3.2 Abbreviations 19
   3.3 Reference standards 21
   3.4 Reference material 21
4. Requirements for basic certificate services 23
   4.1 Certificates, areas of application and certificate policy 23
      4.1.1 General requirements, all certificate types 23
      4.1.2 Additional requirements for Person-High 26
      4.1.3 Additional requirements for Person-Standard 27
      4.1.4 Additional requirements for Enterprise 27
   4.2 Access to the certificate issuer's public keys 28
   4.3 Information security 29
      4.3.1 General requirements, all certificate types 29
   4.4 Requirements for cryptography and crypto equipment 30
      4.4.1 General requirements, all certificate types 30
      4.4.2 Additional requirements for Person-High 31
      4.4.3 Additional requirements for Person-Standard 32
      4.4.4 Additional requirements for Enterprise 32
   4.5 RA services 35
      4.5.1 RA service for Person-High certificates 35
      4.5.2 RA service for Person-Standard certificates 36
      4.5.3 RA service for Enterprise 38
   4.6 RA service for Person certificates for foreign persons 40

4.7 Software requirements 40
4.7.1 The certificate holder's software 40
4.7.2 The certificate recipient's software 42
4.8 Maintenance and revocation of certificates 43
4.8.1 General requirements, all certificate types 43
4.8.2 Additional requirements for Enterprise 44
4.9 User support 45
5. Requirements for look-up services and directories 46
5.1 Status services and certificate directories 46
5.2 CRL status service 46
5.3 OCSP status service 47
5.4 Access to directory services 48
5.5 Access to look-up services 49
5.6 Joint access to status services 51
5.7 Maintenance of directory and look-up services 51
6. Requirements for authentication services 52
7. Requirements for signing services 53
7.1 General signing requirements 54
7.2 Signing requirements for Person-High 56
7.3 Signing requirements for Person-Standard 57
7.4 Signing requirements for Enterprise 58
7.5 Quality of use 58
7.6 Qualified signatures 60
8. Requirements for message encryption 61
9. Additional services 64
9.1 Time-stamping 64
9.2 Long-term storage beyond 10 years 65

1. INTRODUCTION

1.1 Objective and background

This document is a general, functional requirements specification for the self-declaration and procurement of a PKI based eID to be utilised in connection with electronic communication with and within the public sector in Norway. PKI solutions that are utilised in public enterprises shall comply with the requirements specification. The specification comes under the provisions of § 27 of the eGovernment Regulations [3]. It is further determined in the regulations regarding voluntary self-declaration procedures that the requirements stated in the requirements specification shall be complied with.

The objective of this document is that it should serve to simplify the procurement process and establish common requirements for secure and standardised PKI services in public administration. The individual enterprise must undertake independent security and vulnerability assessments to determine which security services and security level are required, in accordance with their security objectives and strategy, cf. §§ 4 and 13 of the eGovernment Regulations [3]. Equivalent requirements are governed by different regulations, among them the Personal Data Act.

This document forms part of the requirements for several areas of application within and outside of the public sector and, in this respect, has been divided into:

- Requirements for basic certificate services – these are the basic requirements for all PKI solutions that should be self-declared and/or supplied in accordance with this document.
- Requirements for services necessary for the implementation of the following areas of application: authentication, signing and encryption, based on a basic certificate service.
- Requirements for additional services.

Services necessary for the implementation of areas of application such as authentication, signing and encryption should be able to be supplied by both public sector and private certificate issuers.

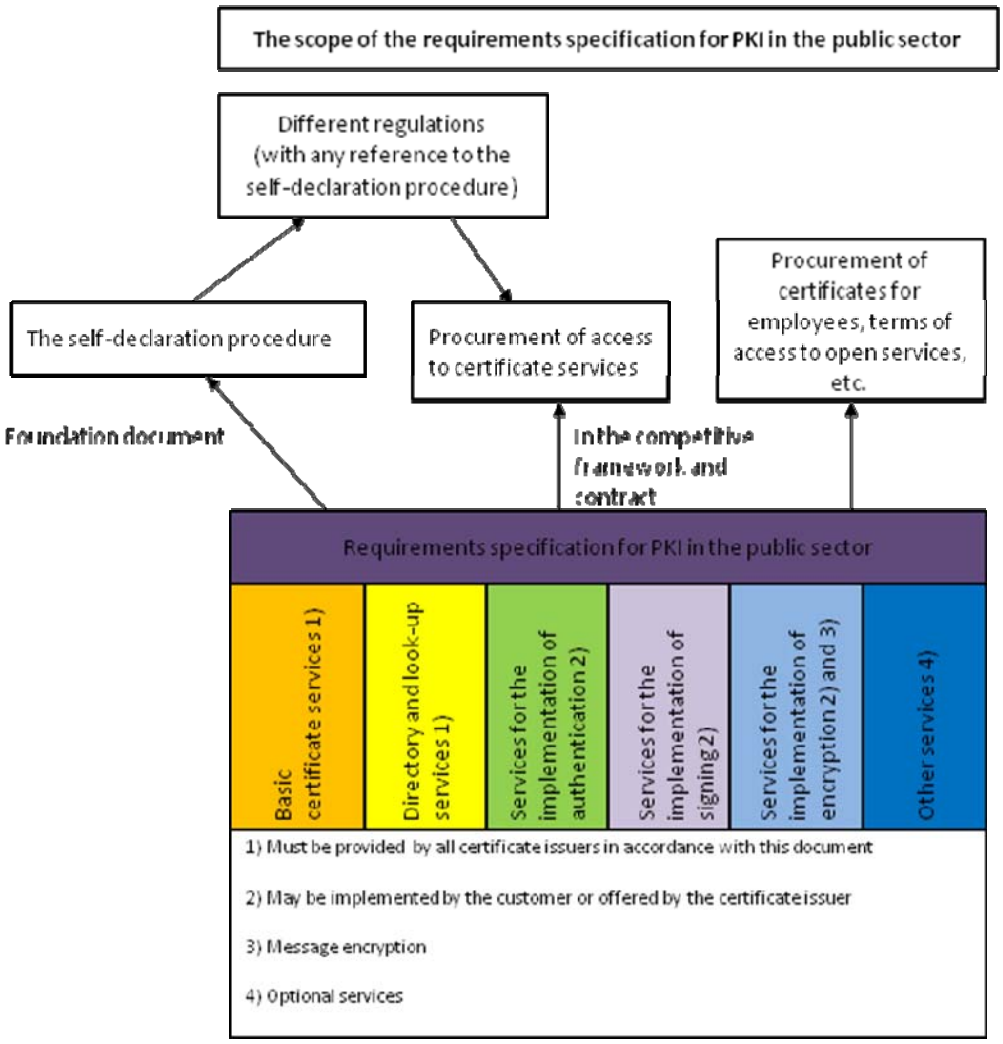
This document has been designed to ensure that the requirements comply with the recommendations of the SEID Project and, as far as possible, with relevant international standards.

1.2 A summary of the scope of the requirements specification

The requirements specification is a general document that determines which common security requirements must form the foundation of basic certificate services and other services that are offered. This document covers the following areas of application: authentication, signing and encryption.

The figure below illustrates the areas of application described in this document. The figure also illustrates that this document supports the self-declaration procedure, see item 1.3 below. Alternative regulations are based on, or refer to, the self-declaration procedure.

Further, this document forms part of the tender documents and the contract when agreements regarding access to certificate services are entered into. Correspondingly, this document will be of relevance to the purchase of certificates for the enterprise or employees, and for the use of open services. See figure below.



This document imposes requirements for three types of certificates divided into the following certificate classes: Person-Standard, Person-High and Enterprise.The certificate classes relate to the two highest security levels in the Framework for Authentication and Non-repudiation [13], see items 2.1 and 2.2.

PKI solutions for mobile phones are becoming widespread and offer a satisfactory level of security. Here, the user's private keys are stored on the mobile phone's SIM card. This document has not been written with PKI for mobile phones in mind, but it should not obstruct the use of a mobile platform if this can be implemented within the requirements of this document.

1.3 Use of the requirements specification upon self-declaration

The self-declaration procedure, and its supervision, should aim to ensure that certificate issuers comply with the requirements of this document, cf. regulations regarding voluntary self-declaration procedures for certificate issuers [12]. The purpose of the self-declaration procedure is to determine which certificates and certificate services comply with public sector requirements within the different services. The procedure contributes to simplifying the procurement process in both the private and public sector.

The Norwegian Post and Telecommunications Authority is appointed as the regulatory authority for the self-declaration procedure and has published a list of issuers, within the various certificate classes, who have declared themselves to the authority. The authority should publish the self-declaration report indicating which areas of use and which associated services the certificate issuer has declared themselves for, with a description of how the requirements are fulfilled. Where there are special grounds, the authority can make exceptions to resolutions in the regulations, cf. regulation § 9 second para.

There are no specific requirements regarding the certificate issuer's services in the regulations on Voluntary Self-Declaration Procedures for Certificate Issuers [12]. According to the regulations, certificate issuers should comply with all absolute requirements (A requirements) that apply to the relevant security products and services relating to the certificate class in which the issuer declared themselves. The *particular security products and services* refer to the products and services that the certificate issuer has chosen to offer within the individual certificate class, and declare themselves for. The specific requirements are outlined in the version of 'Requirements specification for PKI in the public sector', that prevails at any time.

Self-declared certificate issuers should provide *basic certificate services* for the areas of authentication and signing, with associated status services and lookup services. Certificate issuers can choose whether to supply certificates for the area of encryption and which underlying services they will supply. The individual certificate issuer can, as a rule, select which of the services in chapters 6-9 should be self-declared. If a certificate issuer's solution is organised in such a way that it *must* utilise authentication, signing and/or message encryption services from the certificate issuer themselves, these services must also be self-declared. All 'A' requirements for services that the certificate issuer has self-declared themselves for should be fulfilled.

Information regarding which services the individual certificate issuer offers can be obtained from the certificate issuer and from the authority. It would be expedient if this information was available to users through common solutions for the service owners. Certificate issuers may, for example, provide information about which services they offer by completing the table discussed below in item 2.3.

1.4 Use of the requirements specification for procurement

This document has been drafted to cover the requirements applicable to PKI products and services for all types of electronic communication with and within the public sector. This applies both internally within the public sector and between the public sector and individuals, or a private business enterprise. As this document will form the basis of all PKI procurement in the public sector, it will function as an administration standard and will determine common requirements for the solutions.

This document covers the areas of authentication, signing and encryption. However, each respective procurement of PKI solutions is not required to utilise the whole of this document. The individual service owner must assess which areas of application and services they require in order to achieve a given security objective. This document will form part of the tender documents in the invitation to tender in which the part of the document that should be addressed in the bid is specified, and any other additional requirements that may apply. This document is suited to different procurement models.

2. SCOPE AND CONDITIONS

2.1 Certificate classes

This document is divided into three certificate classes. Below is a brief account of the different classes:

***Person-Standard**:*	A person certificate for a specific natural person who is uniquely identified in the certificate.
***Person-High**:*	A person certificate for a specific natural person who is uniquely identified in the certificate. Person-High is based on qualified certificates, cf. § 4 of the Act on Electronic Signatures.
Enterprise:	An enterprise certificate for an entity (enterprise) that is uniquely identified in the certificate.

With the Enterprise certificate class, the enterprise determines how the certificate should be utilised. For example, if it is to be used by a specific natural person authorised by the enterprise or a process under the enterprise's control, e.g. a server. Several enterprise certificates can be issued for the same area of application to one and the same enterprise.

2.2 Security levels

In the draft of version 1.02 of this document, three security levels were identified, two for private persons and one for enterprises. The first version of this document, version 1.02, is based on these three security levels: 'Person-High, 'Person-Standard' and 'Enterprise'.

In April 2008, the Ministry of Government Administration and Reform published its 'Framework for the Authentication and Non-Repudiation of Electronic Communication with and within the Public Sector' [13], in which 4 security levels were used. These 4 security levels are concepts that have been gradually incorporated into the public sector. The security levels in this document relate to the two highest security levels in the framework: levels 3 and 4. ’Person-Standard’ is adapted to the requirements of level 3 and ‘Person-High’ is adapted to the requirements of level 4.

As regards ‘Enterprise’, the requirements set out in version 1.02 of the requirements specification are basically not sufficient to comply with the requirements of level 4, while the requirements are stricter than the minimum requirements for level 3. The requirements for ‘Enterprise’ in version 1.02 of the requirements specification may be fulfilled with ‘soft certificates’ that do not satisfy the requirements given in the level 4 framework for authentication factors not being copyable. Such Enterprise certificates are widespread in the

market today. Even so, the framework uses Enterprise certificates as examples of solutions that *can* satisfy the requirements for level 4. To achieve predictability, it is important that Enterprise certificates can be related to the levels in the framework.

The requirements specification still sets requirements for one certificate class for Enterprise certificate. The minimum requirements for the 'Enterprise' class satisfy the requirements for security level 3 in the framework.

This does not however prevent certificate holders, for example in closed user groups like Norsk Helsenett, from establishing additional requirements and specific solutions for handling such Enterprise certificates, so as to make it reasonable to also use these for level 4. The same applies to Enterprise certificates that fulfil requirement 4.1.4.2 on storing keys in electronic components (B requirement).

For Enterprise certificates that are used by automated *processes under the enterprise's control*, requirement 4.1.4.1 *alone* is not sufficient to comply with the basic assumptions of the framework in order for them to be used at security level 4 (cf. requirement for authentication factors not be copyable). This does not however prevent an enterprise from making use of its own measures to achieve sufficiently good protection against copying and misuse as to make such a certificate usable at security level 4.

Given below are some examples of requirements for such measures that the enterprise itself, and not the certificate issuer, must comply with. The certificate issuer may make such requirements of the certificate holder by means of certificate policy. The requirements shall ensure that the IT system in question has sufficient security against copying and misuse of the certificate and that there is strict control over which processes have access to the Enterprise certificate (see eGovernment Regulations [3] § 21).

Examples of requirements the enterprise itself must comply with
The certificate holder shall only install the Enterprise certificate on systems that are under the certificate holder's control.
The certificate holder shall implement sufficient mechanisms for controlling access to and use of private keys. This shall occur in accordance with the certificate holder's documented security strategy (see eGovernment Regulations § 21, point 1).
The certificate holder shall log all use of private keys, including which process has initiated the use (see eGovernment Regulations § 21, point 1).
The certificate holder shall install and protect private keys so that only authorised personnel may administer certificates and have access to private keys.
Unless private keys are stored in electronic components, storage of private keys shall be encrypted.
Unless private keys are stored in electronic components, encryption shall be used when transferring the Enterprise certificate between the certificate holder's IT systems.
Activating private keys shall involve the use of an activation code. The activation code can be given on start up of IT system, when administrator logs on, when a process is started up or with each individual use. Activation codes may only be stored (cached) linked to IT systems or processes if the activation code is sufficiently protected against copying or misuse.

The table below shows the intended use of the certificate classes Person-High and Person-Standard:

APPLICATIONS FOR CERTIFICATE CLASSES	**Authentication**	**Signing (non-repudiation)**	**Receipt of encrypted information**
Person-High -complies with security level 4 of the Framework for Authentication and Non-Repudiation	Transactions in which there is a need for a high degree of certainty regarding the identity of the originator, for example in connection with access to particularly sensitive information, or where the damage caused by a compromise would be extensive.	Transactions in which there is a need for a high degree of certainty regarding the connection between content and the identity of the originator, or where the damage caused by the compromising of the connection would be extensive.	Documents, etc., containing particularly sensitive information, or where damage caused by a compromise would be extensive.
Person-Standard -complies with security level 3 of the Framework for Authentication and Non-Repudiation	Transactions in which there is a need for a reasonable degree of certainty about the originator's identity, or where a medium level of damage would be caused by a compromise.	Transactions in which there is a need for a reasonable degree of certainty regarding the connection between content and the identity of the originator, or where a medium level of damage would be caused by the connection being compromised.	Documents, etc., that do not contain particularly sensitive information and where the damage caused by a compromise would not be extensive.

The table below shows certificate classes with a selection of properties that the respective classes must comply with:

CERTIFICATE CLASS	**Registration and release procedure**	**Requirements for name structure and content**	**Requirements for protection of private keys**
Person-High	A certificate functioning as an electronic signature shall be a *qualified certificate* and other certificates shall be of the same level of quality. The certificate issuer shall comply with the registration and release procedures resulting from this, including requirements for personal attendance, among other things.	The name structure and certificate content must comply with the requirements in Section 4 of the Act on Electronic Signatures [2] with the clarifications that are governed by 'Recommended certificate profiles for person certificates and enterprise certificates' [10].	Access to private keys requires a minimum of two-factor authentication, in which one of the factors is an item that the user physically possesses. The user shall approve each operation involving private keys by authenticating themselves. Private keys must never appear in plain text in registers that might be compromised, or in other ways provide a basis for unauthorised use.

CERTIFICATE CLASS	Registration and release procedure	Requirements for name structure and content	Requirements for protection of private keys
Person-Standard	The certificate issuer shall comply with the requirements in §§ 10 to 16 of the Act on Electronic Signatures [2], as well as the regulations regarding requirements for issuers of qualified certificates, etc. [4] § 3. A reasonable degree of security must exist to ensure that keys and/or associated access codes/passwords and certificates are issued to the appropriate person. The certificate shall be issued either via regular mail to a registered address or electronically, based on an existing authentication mechanism that provides at least the same degree of certainty of reaching the intended recipient as regular mail to a registered address.	The certificate must comply with the requirements for qualified certificates in § 4, second para. letters b to j, of the Act on Electronic Signatures [2]. The name structure and certificate content must comply with 'Recommended certificate profiles for person certificates and enterprise certificates' [10].	Access to private keys shall require authentication. The user shall have the option to select/decide themselves whether each operation involving private keys shall be authorised. Private keys shall, at the very least, be stored in an encrypted form.

CERTIFICATE CLASS	Registration and release procedure	Requirements for name structure and content	Requirements for protection of private keys
Enterprise	The certificate issuer shall comply with the requirements in §§ 10 to 16 of the Act on Electronic Signatures [2], as well as the regulations regarding requirements for issuers of qualified certificates, etc. [4] §§ 3 and 7. It shall be possible to uniquely identify the enterprise by equipping the certificate with the organisation number of the enterprise from the Central Coordinating Register for Legal Entities, in accordance with the SEID certificate profile [10]. Safeguards must be in place to ensure that keys with associated access codes/passwords and certificates are released to a person authorised to receive them on behalf of the enterprise. (For example, a person with authority from the general manager, owner or equivalent contact person.) Documentation of the relationship should be possible. The enterprise shall be required to log which persons or processes use the certificate	The certificate shall comply with the requirements for qualified certificates in § 4, second para, letters b to j, of the Act on Electronic Signatures [2]. The name structure and certificate content should comply with 'Recommended certificate profiles for person certificates and enterprise certificates' [10]. The certificate should contain the enterprise's organisation number.	It shall be possible to realise access control to private keys. The enterprise shall itself have the possibility to choose/decide whether each operation that involves private keys shall be approved.. For Enterprise certificates used by automated processes, which processes can use private keys shall be specified and controlled. Private keys must as a minimum have encrypted storage.

This document is based on these certificate classes and security levels. Unless otherwise expressly stated, these requirements apply to all certificate classes.

There are stricter security requirements for solutions involving a qualified electronic signature, see item 7.7. According to the Act on Electronic Signatures, a qualified signature is an advanced signature based on a qualified certificate generated by an approved, secure signature creation system. An approved, secure signature creation system must either be approved by a nominated Norwegian agency or an equivalent agency nominated in another EEA country, or it must comply with standards designated by the EU Commission. The Commission has designated the standard CWA 14169 [j] as the requirement to secure the signature creation system.

This document refers to the requirements in the Act on Electronic Signatures and regulations regarding requirements for issuers of qualified certificates, etc., which also apply to Person-Standard, Enterprise-High and Enterprise-Standard. Requirements in the Act on Electronic Signatures – with the exception of requirements in the Act's §§ 6 and 7 – fundamentally apply only to *qualified certificates* (i.e. Person-High) and first and foremost to *issuers* of qualified

certificates. Although this document refers to the requirements of the Act on Electronic Signatures with regulations applicable to Person-Standard and Enterprise, the effects of the requirements are principally contractual. The regulations of the Act on Electronic Signatures regarding compulsory fines in § 20, will come into effect in the case of any false statements regarding self-declaration. The authority can impose compulsory fines under the provisions of the regulations on self-declaration § 13, cf. the Act on Electronic Signatures §§ 16a and 20.

2.3 Explanation of classification of requirements

The classification and grouping of requirements in this document is based on a service-orientated approach. This classification will facilitate the certificate issuers' self-declaration with the services supported by the relevant certificates. Also, public agencies may easily co-ordinate the requirements for the services they need. Upon procurement, the agency may utilise a form indicating the areas of application and services they require. The same form can be completed by the certificate issuers to indicate, in plain language, which services they offer. A simplified table of the certificate classes and associated areas of application and services that are required, as well as a reference to where the requirements to services appear in this document, can be found below. A table for each certificate class must be completed.

Certificate class	**Area of application**	**Services**	**Requirements**
[ ] Person-Standard *or* [ ] Person-High *or* [ ] Enterprise-	[ ] Authentication [ ] Signature [ ] Encryption	**[ ] Basic certificate services** [ ] Maintenance and revocation [ ] User support [ ] RA for Norwegian citizens [ ] RA for foreign citizens [ ] RA for an enterprise certificate **Directory and lookup services** **[ ] Authentication services** [ ] Channel security **[ ] Signing services** [ ] User dialogue - quality of use **[ ] Encryption services** [**] Qualified signature** Long-term storage beyond 10 years [ ] Time-stamping	Chapters 4 and 5 Chapter 4.8 Chapter 4.9 Chapter 4.5.1 and 4.5.2 Chapter 4.6 Chapter 4.5.3 Chapter 5 Chapter 6 Chapter 6 Chapter 7 Chapter 7.6 Chapters 4.4 and 8 Chapter 7.7 Chapter 9.2 Chapter 9.1

Certificate issuers must provide basic certificate services for the areas of authentication and signing. The certificate issuer can choose whether to provide certificates for the area of encryption and the services they will declare themselves for. Encryption and the chosen set of services are referred to as *optional* in item 2.4. If the certificate issuer's solution is organised in such a way that authentication, signing and/or message encryption services from the certificate issuer themselves *must* be used, these services must also be self-declared. It is important to note that a basic eID/certificate service must be present, regardless of whether it is provided by the same certificate issuer as a part-service, or by a different supplier. It is possible, if a supplier so desires, to declare themselves for only one or more of the services in the third column (or the functionality to implement such a service). This is conditional upon these being declared with reference to one or more basic certificates services that the service supports. The 'supplier' will, in this context, be a provider of other services related to electronic signatures covered by the concept of 'certificate issuer', as defined in the Act on Electronic Signatures § 3 no. 10.

The main emphasis of the requirements is provided in chapters 4 and 5, which deals with basic certificate services and constitutes the fundamental service for the provision of eID. Requirements are provided here, covering registration and essential ID verification of the certificate holder, presentation and administration of the certificate and requirement for the establishment of directory and status services. Services for *access* to directory and status services should be provided by the certificate issuer. Additionally, some of the services can be provided by others.

Requirements for services that *enable* authentication, signing and/or encryption are described in separate chapters as dedicated service categories.

The classification of the set of requirements is as follows:

- **Requirements for basic eID/certificate service**
  Requirements covering registration of the certificate holder, presentation and administration of the certificate and requirements for the establishment of directory and status services.
- **Requirements for directory and lookup services**
  Requirements covering how access is gained to certificate information and how much information is accessible.
- **Requirements for authentication**
  Requirements covering authentication functionality and how authentication can contribute to the implementation of information security in the form of channel security.
- **Requirements for signing services**
  Requirements for advanced and qualified signatures, among others.
- **Requirements for encryption**
  Requirements for message encryption
- **Requirements for additional services**

The requirements for basic certificate services will therefore cover all requirements in connection with the presentation of the certificate itself, but also the requirement, among others, that the issuer *has the available* directory and status information for the certificates. Detailed requirements concerning *how* the information is accessed and *what* is accessed will, however, be provided in the chapter on directory and lookup services.

2.4 Explanation of the requirements table

In the following chapters, tables with numbered requirements are used.
These tables include a column for categories (Cat.) in which the following codes are used:

A:	Absolute requirement	- means that the requirement must be satisfied.
C:	Conditional requirement	- means that the requirement should be satisfied
O:	Optional requirement	- used in areas of application and services that the certificate issuer is not required to provide, but in which they can choose to declare themselves.

The code *'Optional requirement'* is used for the area of message encryption and services that certificate issuers themselves have chosen to offer and declare themselves for. These are services that user sites may also offer or they can choose to procure them from other certificate issuers/suppliers. Other suppliers may choose to declare themselves for these services, but this is optional, see item 2.3.

Further, there is a separate column, 'Answer from supplier'. The certificate issuer should enter the following into this column:

Y:	Yes	- This means that the requirement has been fulfilled (and that the solution is included in the offer/contract price).
N:	No	- This means that the requirement has not been fulfilled.
P:	Proviso	Here, a number is provided that refers to a specific description of the proviso. **'NA'** should be entered into this column if the requirement is not applicable to the delivery.

Requirements marked O (Optional) mean:

Y:	Yes	- That the certificate issuer offers the area of application or the service.

3. DEFINITION OF TERMS, ABBREVIATIONS AND REFERENCES

3.1 Definition of terms

Authentication	Authentication is the verification of an alleged identity. Authentication can be based on different authentication factors.
D number	When a migrant person is to be issued with a national identity number, they will often receive a temporary D number first. For foreigners who are legally residing in Norway, this is used in connection with tax issues and public services. The D number comprises eleven digits and consists of a modified date of birth and a five-digit number. The date of birth is modified by adding a '4' to the first digit: Thus, a person born on 1st January 1980 would be assigned 410180, while a person born on 31st January 1980 would be assigned 710180. The five-digit number does not run in series,

	but is allotted sequentially.
eID, electronic ID	A PKI based eID consists of one or more certificates with associated private keys, in which the certificates are issued jointly and identify the same certificate holder. In the case of several certificates/key pairs, these will have different areas of application (authentication, signing or encryption).
National identity number	A national identity number is an eleven-digit registration number allocated to every inhabitant of the country by the Norwegian State. The first six digits indicate the date of birth and the last five digits specify the personal number. A national identity number is a unique identification of an individual person. For access to services, a national identity number should be regarded as a name, not a password. Access to services should never be provided based only on knowledge of a national identity number. Everyone living in Norway and entered in the National Register will have either a national identity number or a D number. According to the Personal Data Act, a national identity number should only be used when there are justifiable grounds and when it is not possible to establish satisfactory identification through other methods, such as name, address, date of birth, membership or customer number.
Integration Module	A software module that can be called up by applications to perform functionality connected with an electronic ID and signature.
Directory service	In a PKI context, the directory service will systematise, store and make available, certificates, CRLs and any other information from the certificate issuer.
Encryption	A process that results in the distortion of a document's contents or other data script so that only appointed recipients may view it and read it. Encryption usually takes places in accordance with fixed algorithms in which the parameters, encryption key and decryption key determine how content is distorted and then restored to plain text. For symmetrical algorithms, the encryption and decryption keys are the same. For public key algorithms, content encrypted with a public key may be decrypted with an equivalent private key[1], and v.v. Encryption keys may be pre-arranged or exchanged through a protocol between the sender and the recipients.
Channel security	Channel protection at the set-up of a secure communication channel provides encryption and content integrity protection between the channel's terminal points. Beyond the terminal points at both ends, the content is unprotected plain text. Confidentiality protection can be implemented by end-users authenticating themselves via an encrypted communication channel, after which subsequent messages are transmitted over the channel.
Message encryption	A method for safeguarding confidentiality in which the messages are encrypted by the sender at the point of origin and can only be decrypted by the intended recipient. Message encryption, as far as the concept is utilised in this document, is realised through the

[1] There are public key algorithms that do not support this type of encryption, but these are not in normal use.

	encryption of a message to the certificate holder, i.e. *the holder of an encryption certificate and associated decryption key*. In locations where this document only uses the term 'encryption', this should be understood as message encryption.
Organisation number	Nine digits that are not information-bearing and that identify a registration entity or sub-unit in the Central Coordinating Registry for Legal Entities.
Person certificate	A certificate in which the certificate holder is a natural person.
PKI	'Public Key Infrastructure' – the infrastructure for public key cryptography is a technology for issuing, managing and utilising electronic IDs and e-signatures based on standardised encryption technology.
Registration authority (RA)	Collects data required for the issuing of a certificate. The registration authority checks and verifies the identity of the upcoming certificate holder and communicates the required data to the certificate issuer.
Registered address	Address registered in the National Register.
Registration entity registered in the Central Coordinating Register for Legal Entities.	Legal person, sole proprietorship or any other entity registered in the Central Coordinating Register for Legal Entities. For a registration entity, the General Manager, owner or equivalent contact person should be registered in the Central Coordinating Register for Legal Entities.
Certificate	A certificate is a connection between a public key, the identification (name) of the certificate holder, and any other information. At the point of signature, the public key is the signature verification data, and the name in the certificate. The certificate is signed by the certificate issuer and, through this, they vouch that the certificate's contents are correct.
Certificate holder	The person who is the rightful user of a certificate, i.e. the person nominated in the certificate as the holder of the public key in the certificate, and who has use of the private key associated with the certificate.
Certificate recipient	A person linked to the certificate's contents in connection with the authentication, encryption and verification of a signature.
Certificate issuer (CA)	A natural or legal person that issues certificates (CA). In this document the certificate issuer is always a legal person.
Certification procedure	Any procedure in which a third party confirms in writing that the certificate issuer's products, procedures or services fulfil specified requirements, and in which the certificate issuer is not entitled to exercise the rights that the certification provides, before the person concerned has received the third party's confirmation.
Standard	A document for joint and repeated use, arrived at by consensus and passed by a recognised body, which provides regulations or guidelines for, or characteristic features of, activities, or the results of them. The intention is to achieve optimum order in any given context.
Particularly sensitive information	Information that is sensitive in accordance with the Personal Data Act and/or is regarded as particularly sensitive in accordance with other regulations/guidelines. Includes information about enterprises

	of a particularly sensitive nature.
Service owner	An enterprise that provides electronic services. This includes web services, enterprises with integration of electronic message exchange in internal systems, or where standard e-mail is used for these exchanges.
Sub-unit	A Company, etc., that is allocated its own organisation number and is registered in the Central Coordinating Register for Legal Entities. A sub-unit does not register a General Manager, owner or equivalent person, but it registers its attachment to a general registration entity in the Central Coordinating Register for Legal Entities.
Validation service	Correct use of eID presupposes that the service owner has assured themselves that the certificate is suited to its particular use and has not been withdrawn. Due to the practical difficulties of compiling the necessary information about the certificate service's suitability for the service owner's purposes, there may be a requirement for a validation service that undertakes the task on behalf of the certificate recipient (service owner).
Enterprise certificate	A certificate that identifies a registration entity or sub-unit in the Central Coordinating Register for Legal Entities. Later in this document, 'enterprise' is used as a common term for registration entities and sub-entities.

3.2 Abbreviations

CA	Certification Authority (Certificate issuer)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CWA	CEN Workshop Agreement
ETSI	European Telecommunications Standards Institute
J2EE	Java 2 Platform, Enterprise Edition (Programming standard)
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
NCP	Normalised Certificate Policy
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
QCP	Qualified Certificate Policy
RA	Registration Authority
RFC	Request For Comment (document series with specifications from IETF. Some RFC documents have the status of 'Internet standard')
RSA	Rivest, Shamir and Adleman (public key crypto-algorithm)
SEID	Collaboration on Electronic ID and signature
S/MIME	Secure/Multi-purpose Internet Mail Extension (Protocol for secure e-mail)
SSL	Secure Socket Layer (protocol for secure communications, used in web services over https, among others)

TLS	Transport Layer Security (protocol for secure communication channel, further development of SSL)
TS	Technical Specification
TSA	Trustworthy external time-stamping service. (In accordance with ETSI TS 102 023, a TSA should be regarded as a certification service provider.)

3.3 Reference standards

The latest updated version of the standards applies to this document.

[a] ETSI TS 101 456 – Policy requirements for certification authorities issuing qualified certificates
[b] ETSI TS 102 042 - Policy requirements for certification authorities issuing public key certificates
[c] ETSI TS 101 733 - Electronic Signature Formats
[d] ETSI TS 101 903 - XML Advanced Electronic Signatures (XAdES)
[e] PKCS #7 –The cryptographic message syntax standard
[f] X.509 - The Directory: Public key and attribute certificate frameworks
[g] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[h] RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
[i] RFC 3629 – UTF-8 – a transformation format of ISO 10646
[j] CWA 14169 – Secure Signature Creation Devices
[k] CWA 14170 – Security Requirements for Signature Creation Systems
[l] CWA 14171 – Procedures for Electronic Signature Verification
[m] PKCS #11 – Cryptographic Token Interface Standard
[n] CMS – Certificate Management Messages (RFC 2797)
[o] AICPA/CICA – WebTrust Programme for Certification Authorities
[p] FIPS PUB 140-2 (2001) – Security Requirements for Cryptographic Modules
[q] ISO/IEC 27001:2005 Information technology – Security techniques – information security management systems – Requirements
[r] RFC 1777 - Lightweight Directory Access Protocol
[s] ETSI TS 102 176-1 – Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash Functions and Asymmetric Algorithms
[t] RFC 5246 -The Transport Layer Security (TLS) Protocol
[u] RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
[v] ETSI TS 102 023 - Policy Requirements for Time-Stamping Authorities (TSAs)

3.4 Reference material

[1] NOU 2001:10 Without Pen and Ink (Uten penn og blekk)
[2] Act of 15th June 2001 no. 81 on electronic signatures
[3] Regulations of 25th June 2004 no. 988 on electronic communication with and within the public administration (eForvaltningsforskriften)
[4] Regulations of 15th June 2001 no. 611 on requirements to issuers of qualified certificates, etc.
[5] Directive of the European Parliament and of the Council 1999/93/EF of 13th December 1999 on a Community framework for electronic signatures
[6] Act of 14th April 2000 no. 31 on the processing of personal data (Personal Data Act).

[7] Regulations of 15th December 2000 no. 1265 on the processing of personal data (personopplysningsforskriften)
[8] Act of 6th March 2009 no. 11 on measures to combat the laundering of proceeds and the financing of terror, etc. (the Money Laundering Act)
[9] Regulations of 13th March 2009 no. 302 on measures to combat the laundering of proceeds and the financing of terror, etc. (hvitvaskingsforskriften)
[10] The SEID project. Recommended certificate profiles for person certificates and enterprise certificates, version 1.01, September 2004.
[11] The SEID Project. Interface for access to Lookup services (approved December 2004).
[12] Regulations of 21st November 2005 no. 1296 on voluntary self-declaration procedures for certificate issuers.
[13] Framework for authentication and non-repudiation of electronic communication with and within the public sector. Guidelines from the Ministry of Government Administration and Reform, April 2008.
[14] Regulations of 9th November 2007 no. 1268 on national registration
[15] Act of 20th June 2008 no. 42 relating to a prohibition against discrimination on the basis of disability (Anti-discrimination and Accessibility Act)
[16] Reference directory for IT standards in the public sector, version 2.0, 25.6.2009.

4. REQUIREMENTS FOR BASIC CERTIFICATE SERVICES

An eID consists of one or more certificates with associated private keys, in which the certificates are issued jointly and identify the same certificate holder. In the case of several certificates/key pairs, these will have different areas of application (authentication, signing or encryption). For the user, an eID should be presented as a unit. This means that the user does not need to actively select which certificate or which key should be used for a given operation. However, for the issuing of eID, there may be separate requirements for certificates that have different purposes. This document therefore contains both general requirements for eID and specific requirements for certificates in different areas of application.

4.1 Certificates, areas of application and certificate policy

An eID consists of one or more certificates and key pairs with different areas of application. Three areas of application are applicable to this document: Authentication, signing and encryption.

The following recommendations have been made:

- It is strongly recommended that all three areas of application are offered, but an eID that only offers authentication and signing may be self-declared. However, several applications for communication with and within the public sector require message encryption and an eID that does not support encryption cannot be used for such purposes.
- It is strongly recommended to hold separate key pairs and certificates for each area of application. In some European countries, it is an absolute requirement for qualified certificates that electronic signatures have their own certificate/key pair. For security reasons, encryption should also have its own certificate/key pair. However, the requirements specification relates to the SEID project's recommended certificate profiles [10] permitting certificates and key pairs that cover several areas of use.

- It is strongly recommended that eIDs should be available over an open, standardised interface for use with third party software and to standard protocols such as TLS/SSL and S/MIME e-mail. It is still possible to self-declare solutions with limited accessibility and areas of application. This may be emphasised in future versions of this document.

4.1.1 General requirements, all certificate types

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.1.1.1	**Authentication certificate** eID shall contain a certificate and key pair for the purpose of authentication (key usage 'digital signature').	A			
4.1.1.2	**Electronic signature certificate** eID shall contain a certificate and key pair for the purpose of an electronic signature (key usage 'content commitment', previous name 'non-repudiation').	A			
4.1.1.3	**Encryption certificate** eID shall contain a certificate and key pair that can be used for message encryption (key usage 'key encipherment', also any possible 'key agreement' and/or 'data encipherment').	C			
4.1.1.4	**Number of certificates and combinations of areas of application** The certificate issuer must state how many certificates and key pairs form part of an eID. It shall be specified when different areas of application are combined in the same certificate/key pair.	A			
4.1.1.5	**Separation of areas of application** Authentication, signature and encryption shall have separate certificates and key pairs.	C			
4.1.1.6	**Use in authentication of TLS/SSL** It shall be possible to use eID for user page authentication of the TLS/SSL protocol [t] (extended key usage 'client authentication').	C			
4.1.1.7	**Use in securing of e-mail** It shall be possible to use eID for the securing of e-mail (extended key usage 'e-mail protection', placed in the relevant certificates and any e-mail addresses included in the relevant certificates).	C			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.1.1.8	**Certificate profile in accordance with SEID [10]** All certificates shall comply with 'Recommended certificate profiles for person certificates and enterprise certificates' [10]. The following deviations from the SEID certificate profile are permitted[2]: • For person certificates for persons not registered in the National Register, there is no requirement to be connected to a national identity number or D number. • For enterprise certificates for enterprises *not registered in Norway*, there is no requirement to be connected to the Central Coordinating Register for Legal Entities. Where these deviations are asserted, name-giving in the 'Subject' field, in these cases, shall be specified, especially in the use of the 'serialNumber' attribute in 'Subject'[3]. Any fields, attributes and extensions included in the certificate, but not specified in [10], shall be specified.	A			
4.1.1.9	**Character set for names in certificates** Names in certificates (issuer name and name of certificate holder) shall be encoded with a UTF-8 character set [i].	A			
4.1.1.10	**Limitations in connection with the certificate holder** Any restrictions (for example, age or entry in the National Register) connected to any person who could be the certificate holder, shall be described.	A			
4.1.1.11	**Limitations to the certificates' area of application** Any restrictions regarding the application of certificates and any special conditions concerning who can be a certificate recipient, shall be described.	A			

4.1.2 Additional requirements for Person-High

The following conditions apply to a Person-High certificate policy:

- A certificate containing an electronic signature *must* be a qualified certificate, and marked as such.
- Certificates not containing this area of application *may* be marked as a qualified certificate, in accordance with the SEID certificate profile [10].

In some European countries, the EU Esignature Directive [5] is interpreted in such a way that it is *only* certificates with a signature that can be qualified, and that these certificates should

[2] The grounds for these deviations are that this document should not *obstruct* certificate issuers from issuing certificates internationally, according to the same policy used for Norwegian person certificates or enterprise certificates. This does *not* include any requirement to offer certificates to any parties other than certificate holders registered in Norway.

[3] It is recommended that REID (Registered Entity ID) is used as an organisation number for enterprises, in this case, as this provides a unique international identifier. See http://www.brreg.no/porvoo13/documents/reid_unique_company_identifier.pdf.

not have other areas of application. This interpretation is acceptable and this document therefore does not impose the requirement that certificates, other than those required for signing purposes, should be qualified.

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.1.2.1	**Registration as an issuer of qualified certificates** Before certificate issuers can declare themselves for Person-High, in accordance with the regulations on voluntary self-declaration procedures for certificate issuers [12], it shall be documented that the issuer is registered as an issuer of qualified certificates, in accordance with the Act on Electronic Signatures [2] § 18, or that a register notification for the issuing of qualified certificates has been sent.	A			
4.1.2.2	**Qualified certificates** It shall be specified which certificates in an eID are marked as a qualified certificate.	A			
4.1.2.3	**Qualified certificate for signing** A certificate containing a signature shall be a qualified certificate, and marked as such.	A			
4.1.2.4	**Certificate policy for certificates marked as qualified** The certificate policy for qualified certificates shall satisfy the requirements of QCP (Qualified Certificate Policy) in ETSI TS 101 456 [a], and also any requirements for QCP+, where a qualified signature is offered.	A			
4.1.2.5	**Certificate policy for certificates not marked as qualified** Requirements in a certificate policy that apply to certificates not marked qualified, shall satisfy the requirements of NCP+ (extended Normalised Certificate Policy) in ETSI TS 102 042 [b].	A			

4.1.3 Additional requirements for Person-Standard

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.1.3.1	**Certificate policy** A certificate policy for Person-Standard shall satisfy the requirements of LCP (Lightweight Certificate Policy) in ETSI TS 101 042 [b].	A			

4.1.4 Additional requirements for Enterprise certificate

The policy requirements for enterprise certificates are outlined below. As explained in point 2.2, the A requirements for Enterprise certificates are defined as being at security level 3 in

the Framework for the Authentication and Non-Repudiation of Electronic Communication with and within the Public Sector [13].

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.1.4.1	**Certificate policy** A certificate policy shall satisfy the requirements of NCP (Normalised Certificate Policy) in ETSI TS 101 042 [b].	A			
4.1.4.2	**Certificate policy, key storage in electronic component** A certificate policy shall satisfy the requirements of NCP+ (extended Normalised Certificate Policy) in ETSI TS 101 042 [b].	B			
4.1.4.3	**Usage of Enterprise certificate** A certificate policy shall require the certificate holder to log which persons (if the certificate is used under personal control) or IT systems and processes use the Enterprise certificate.	A			

4.2 Access to the certificate issuer's public keys

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.2.1	**Access to the certificate issuer's public keys** Issuer certificates (root certificates) necessary for the verification of issued certificates shall be universally (openly) available and distributed in a secure and confidence-inspiring manner. The distribution procedure shall be documented.	A			
4.2.2	**Certification for individual access to issuer certificates** A certificate issuer shall be certified in compliance with the Web Trust for Certification Authorities [o], or shall have a Declaration of Conformity to ETSI TS 101 456 or another procedure that enables the proliferation of issuer certificates in the standard distribution of operating systems, browsers and other software.	C			

4.3 Information security

4.3.1 General requirements, all certificate types

There is no requirement for the certificate issuer to be certified according to a designated standard, but a certification or a completed third party audit will be a way of indicating to the authority that the certificate issuer has fulfilled the requirements for self-declaration.

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.3.1.1	**Management system for information security** The certificate issuer shall have a formalised and documented management system for information security (ISMS) as defined in ISO/IEC 27001, for example. The management system shall, as a minimum, encompass the part of the organisation and procedures that relate to the supply of a basic eID/certificate service, as defined in chapter 4.	A			
4.3.1.2	**Risk assessment and risk handling** The certificate issuer shall regularly undertake a methodical risk assessment in order to evaluate risk, as well as determining security requirements and security measures. Risk assessment shall, as a minimum, be carried out annually and the results, together with associated measures for risk handling, made available to the regulatory authority, upon request.	A			
4.3.1.3	**Choice of security measures** The choice of security measures for information security shall be based upon a completed risk assessment and shall, as a minimum, be in accordance with ISO/IEC 27002:2005.	A			
4.3.1.4	**Certification of a management system for information security** The certificate issuer's management system for information security shall be certified in accordance with ISO/IEC 27001:2005 [q]. A certification shall, as a minimum, encompass the organisation of the operative management of hardware and software for the issuing of certificates. The certificate issuer shall be able to submit a valid ISO/IEC 27001 certificate.	C			
4.3.1.5	**Declaration of Conformity** The certificate issuer shall submit an external audit report in respect of fulfilment of requirements for certificate policies on level QCP/QCP+ [b], as well as possibly NCP/NCP+ or LCP [c]. Documentation relating to completed audits shall not be more than two years old.	C			

4.4 Requirements for cryptography and crypto equipment

4.4.1 General requirements, all certificate types

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.4.1.1	**Key generation – certificate issuer's keys** Key generation of the certificate issuer's own keys shall take place according to a well-documented procedure, and it shall be further documented that this procedure has been adhered to ('key ceremony'). The process shall include certification of the certificate issuer's public keys through self-signed certificates and also any certificates from issuers at a higher level in a given hierarchy.	A			
4.4.1.2	**Certificate holder's keys and certificates** The strength and effective life of certificates and keys shall be in accordance with ETSI TS 102 176 -1 [s]. The certificate issuer shall specify algorithms, key lengths and effective life of keys and certificates for certificate holders. The degree to which keys can be recycled upon the renewal of certificates shall be specified.	A			
4.4.1.3	**Effective life of the certificate issuer's own keys and certificates** The effective life of the certificate issuer's own keys and certificates (for signing of certificates and status information) shall comply with ETSI TS 102 176-1 [s]. The certificate issuer shall specify algorithms, strength and effective life of keys used by the certificate issuer themselves, and for certificates (self-signed and others) for such keys.	A			
4.4.1.4	**Requirements for the cryptographic strength of the certificate issuer** The certificate issuer's hash algorithm and public key algorithm, with associated key length for the signing of certificates and status information (CRL, OCSP), shall comply with the requirements in ETSI 102 176-1 [s].	A			
4.4.1.5	**Security copies of private decryption keys** The certificate issuer shall specify whether security copies of private decryption keys are made and whether this applies to all such keys, or as a voluntary service to certificate holders. Security copies of private decryption keys shall not be made if these keys also have other purposes (authentication and/or signing). If a security copy is made, the manner in which it is stored and secured shall be described. The conditions for access to the security copy shall be described.	A			

4.4.2 Additional requirements for Person-High

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.4.2.1	**Key generation – certificate holder's keys** The certificate issuer shall guarantee that procedures for the generation of certificate holders' keys comply with requirements of the Act on Electronic Signatures [2] § 11, 1st and 3rd para. This shall apply to keys, generated by the certificate issuer, by software or equipment supplied by the certificate issuer (e.g. in a smartcard under the user's control) or by software or equipment supplied by others (e.g. a smartcard from another supplier).	A			
4.4.2.2	**Quality of crypto equipment** The following equipment shall comply with the requirements of FIPS PUB 140-2 [p] level 3 or higher, or equivalent standards (see ETSI TS 101 456 [a] section 7.2.1 and 7.2.2): a) Equipment for the generation and storage/use of the certificate issuer's own private keys. b) Equipment for the generation of keys for certificate holders in the event that private keys must subsequently be written to the memory of certificate holders' private keys (e.g. keys generated in special equipment, and subsequently written to a smart card).	A			
4.4.2.3	**Protection of the certificate holder's private keys** The certificate holder's private keys shall be stored in separate electronic components (e.g. smartcard) in such a way that the keys cannot be read, copied or altered. Access to private keys requires two factors: The physical possession of an electronic component that is not copyable and a static (or dynamic) factor that is also not copyable (e.g. a password that must be remembered by the certificate holder). Users shall authorise each operation involving private keys by authenticating themselves. Electronic components shall, as a minimum, satisfy the requirements in FIPS 140-2 or an equivalent standard, relevant to the product in question. The certificate issuer shall produce documentation indicating how the requirements were fulfilled.	A			

4.4.3 Additional requirements for Person-Standard

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.4.3.1	**Key generation – certificate issuer's keys** The certificate issuer shall guarantee that procedures for key generation of certificate holders' keys comply with the requirements of the Act on Electronic Signatures [2] § 11, 1st and	A			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
	3rd para. This shall apply to keys, generated by the certificate issuer, by software or equipment supplied by the certificate issuer (e.g. in a smartcard under the user's control) or by software or equipment supplied by others (e.g. a smartcard from another supplier).				
4.4.3.2	**Quality of crypto equipment** Equipment for the generation and storage/use of the certificate issuer's own private keys shall fulfil the requirements of FIPS PUB 140-2 [p] level 2 or higher, or equivalent standards (see ETSI TS 102 042 [a] section 7.2.1 and 7.2.2).	A			
4.4.3.3	**Protection of the certificate holder's private keys** Access to private keys requires authentication (fulfilled by logging on to an IT system). The user shall have the option to select/decide whether each operation that involves private keys shall be authorised. Private keys shall, as a minimum, be stored in an encrypted form.	A			

4.4.4 Additional requirements for Enterprise

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.4.4.1	**Key generation – certificate holder's keys** The certificate issuer shall guarantee that procedures for the generation of certificate holders' keys comply with requirements of the Act on Electronic Signatures [2] § 11, 1st and 3rd para. This shall apply to keys, generated by the certificate issuer, by software or equipment supplied by the certificate issuer (e.g. in a smartcard under the user's control) or by software or equipment supplied by others (e.g. a smartcard from another supplier).	A			
4.4.4.2	**Quality of crypto equipment** The following equipment shall comply with the requirements of FIPS PUB 140-2 [p] level 3 or higher, or equivalent standards (see ETSI TS 102 042 [b] section 7.2.1 and 7.2.2): a) Equipment for the generation and storage/use of the certificate issuer's own private keys. b) Equipment for the generation of keys for certificate holders in the event that private keys must subsequently be written to an electronic component for the storage of the certificate holders' private keys (e.g. keys generated in special equipment, and subsequently written to a smart card).	A			

4.5 RA services

The certificate issuer is responsible for ensuring that RA services and issuance procedures for certificates are carried out in accordance with the requirements of the certificate class concerned, also where the certificate issuer uses sub-contractors for RA services.

4.5.1 RA service for Person-High certificates

The certificate issuer is responsible for ensuring that they provide RA services that establish sufficient confidence about a certificate holder's identity, cf. the Act on Electronic Signatures [2] with regulations [4]. It is essential that any and all contact with certificate applicants requiring a physical presence can be performed in adequate geographical proximity to the certificate applicant, so that the procedure involved in acquiring the certificate is not viewed as a barrier to use of the solution.

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.5.1.1	**Documentation of registration and the issuance procedure** For the issuance of certificates, the following shall be described, as a minimum, specifying which tasks shall be carried out by the RA role and which tasks are carried out by the certificate issuer: How and where the certificate holder's key pairs are generated, distributed and installed. How certificate applications are registered, including the way in which personal data is checked and whether consent is obtained for publication of the certificate, in accordance with § 14, 2nd para., letter b of the Act on Electronic Signatures [2]. The routine for the issuance of certificates, including where and how the certificate is delivered to the certificate applicant, cf. § 13 of the Act on Electronic Signatures [2] with the accompanying regulations [4] § 7. The amount of time it takes from when the application has been submitted to when the certificate can be issued, shall be stated. All of these functions shall be adequately covered in the certificate policy and in certificate practice. The description may therefore be provided in the form of references to the relevant parts of these documents.	A			
4.5.1.2	**Organisation of the RA service** The RA service shall be organised in accordance with the requirements in the Act on Electronic Signatures [2] and regulations [4] and ETSI TS 101 456 [a].	A			
4.5.1.3	**RA as sub-contractor** The certificate issuer shall specify which sub-contractors have an agreement with the certificate issuer for the supply of RA services.	A			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
	The certificate issuer shall also specify if other sub-contractors are able to act as RA (e.g. a public enterprise), and which conditions would apply in such cases.				
4.5.1.4	**Technical and organisational solutions for RA** The certificate issuer shall describe which requirements apply to an RA within the following areas, and how it is verified that these requirements have been fulfilled: • Equipment (hardware and software) for RA. • How the RA is authenticated for the certificate issuer. • Training requirements and any other requirements for RA personnel. • Requirements for physical security, IT security and organisational security for RA.	A			
4.5.1.5	**Documentation requirements at issuance of the certificate** When the certificate is issued, an issuer shall require the certificate applicant to submit an identity document in compliance with the requirements in § 5, 1st para. of the money laundering regulations (hvitvaskingsforskriften) [9]. The certificate issuer is responsible for ensuring that the RA service fulfils these requirements.	A			
4.5.1.6	**Registration, storage and deletion of information** The certificate issuer is responsible for registering, storing and deleting information according to the requirements in § 8, 1st and 2nd para. and § 22 of the Money Laundering Act [8] and § 17 of the money laundering regulations (hvitvaskingsforskriften) [9].[4]	A			
4.5.1.7	**Personal attendance, geographical proximity** All relevant certificate applicants residing in Norway shall be able to attend in person within a reasonable geographic proximity. The geographical distribution of RA players shall be described. Any RA services provided for persons residing abroad shall also be described.	A			
4.5.1.8	**Validation against the National Population Register** For persons who are registered in the National Population Register, it must be possible to validate the information against the National Population Register.				

4.5.2 RA service for Person-Standard certificates

The issuance of Person-Standard certificates does not require personal attendance. The issuance can therefore take place based on other mechanisms for ensuring that a certificate has been issued to the appropriate person. This can be based on an already established customer relationship with the recipient, postal dispatch to an address registered in the

[4] For public issuers, there is currently an ongoing legislative work regarding publicly issued electronic identity

National Register, transmission of activation data to a registered mobile phone, and other methods that the certificate issuer regards as being sufficient for the issuance procedure.

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.5.2.1	**Documentation of registration and the issuance procedure** For the issuance of certificates, the following shall be described, as a minimum, specifying which tasks shall be carried out by the RA role and which tasks shall be carried out by the certificate issuer: • How and where key pairs are generated, distributed and installed. • How registration of the certificate application occurs, including how personal information is verified, how consent is obtained for publication of the certificate, and how information is stored. • Procedures for issuing certificates, including where and how certificates are issued to the certificate applicant. The amount of time it takes from when the application has been submitted to when the certificate can be issued, shall be stated. For example, delivery can take place via postal dispatch to an address registered in the National Register, or electronically, based on an existing authentication mechanism that provides at least the same degree of certainty of reaching the intended recipient as regular mail to a registered address. All of these functions shall be adequately covered in the certificate policy and in certificate practice. The description may therefore be provided in the form of references to the relevant parts of these documents.	A			
4.5.2.2	**Organisation of the RA service** The RA service shall be organised in accordance with the LCP requirements in ETSI TS 102 042 [b].	A			
4.5.2.3	**RA as sub-contractor** The certificate issuer shall specify which sub-contractors they have an agreement with for the supply of RA services. The certificate issuer shall also specify if other sub-contractors are able to act as RA (e.g. a public enterprise), and which conditions would apply in such cases.	A			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.5.2.4	**Technical and organisational solutions for RA** The certificate issuer shall describe which requirements apply to an RA within the following areas, and how it is verified that these requirements have been fulfilled: • Equipment (hardware and software) for RA. • How the RA is authenticated for the certificate issuer. • Training requirements and any other requirements for RA personnel. • Requirements for physical, logical and organisational security for RA.	A			
4.5.2.5	**Electronic registration and distribution** It shall be specified whether the supplier is able to offer an RA service based on the re-use of existing authentication solutions, and, if so, how this will be achieved.	A			

4.5.3 RA service for Enterprise certificates

First-time issuance is based on personal attendance by a person in possession of the appropriate authorisation.

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.5.3.1	**Documentation of registration and the issuance procedure** For the issuance of certificates, the following shall be described, as a minimum, specifying which tasks shall be carried out by the RA role and which tasks shall be carried out by the certificate issuer: • How and where key pairs are generated, distributed and installed. • How registration of a certificate application occurs, including how personal information is verified, how verification of the recipient's authorisation to receive the certificate (authority) is undertaken, and how the information is stored. • Procedures for issuing certificates, including where and how certificates are issued to the certificate applicant. The amount of time it takes from when the application has been submitted to when the certificate can be issued, shall be stated. All these functions shall be adequately covered in CP and CPS and the description can therefore be specified accordingly.	A			
4.5.3.2	**Organisation of the RA service** The RA service shall be organised in accordance with the NCP requirements in ETSI TS 102 042 [b].	A			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.5.3.3	**RA as sub-contractor** The certificate issuer shall specify which sub-contractors they have an agreement with for the supply of RA services. The certificate issuer shall also specify if other sub-contractors are able to act as RA (e.g. a public enterprise), and which conditions would apply in such cases.	A			
4.5.3.4	**Technical and organisational solutions for RA** The certificate issuer shall describe which requirements apply to an RA within the following areas, and how it is verified that these requirements have been fulfilled: • Equipment (hardware and software) for RA. • How the RA is authenticated for the certificate issuer. • Training requirements and any other requirements for RA personnel. • Requirements for physical, IT and organisational security for RA.	A			
4.5.3.5	**Personal attendance, geographical proximity** All relevant certificate applicants residing in Norway shall be able to attend in person within a reasonable geographic proximity. The geographical distribution of RA players shall be described. Any RA services provided for persons residing abroad shall also be described.	A			
4.5.3.6	**Unique identification of a registration entity (enterprise)** Unique identification of a registration entity shall be possible. This shall be safeguarded by ensuring that the certificate issuer only releases keys and certificates to authorised representatives of the certificate holder (authorisation from a General Manager, owner or equivalent person in the company) and that the certificate is equipped with the organisation number of the registered entity (enterprise) issued by the Central Coordinating Register for Legal Entities, in accordance with 'Recommended certificate profiles for person certificates and enterprise certificates'[10].	A			
4.5.3.7	**Unique identification of a sub-entity** Unique identification of a sub-entity shall be possible. This shall be safeguarded by ensuring that the certificate issuer only releases keys and certificates to authorised representatives of the certificate holder (authorisation from a General Manager, owner or equivalent person in the company) and that the certificate is equipped with the organisation number of the sub-entity (enterprise) issued by the Central Coordinating Register for Legal Entities, in accordance with 'Recommended certificate profiles for person certificates and enterprise certificates'[10].	A			

4.6 RA service for Person certificates for foreign persons

The certificate issuer should offer an RA service for certificates of the type Person-High and/or Person-Standard to foreign persons who do not possess a D number, to facilitate the registration of relevant information. The requirement facilitates the implementation of the service directive's article 6, item 1a and article 8 item 1, whereby the certificate issuer verifies and registers the foreign certificate applicants so that registered information can be used later as the basis for any electronic requisition and issuance of a D number. On behalf of the certificate issuer, the RA service may also verify information on the certificate applicant and perform quality control on the information that will be entered into the certificates.

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.6	**RA service for Person certificates for foreign persons without a D number** It shall be specified *whether* the certificate issuer is providing this service. In such cases, the requirement below will apply.	O			
4.6.1	**Documentation requirements, registration, storage and deletion of relevant information** Verification and registration of information about foreign persons not in possession of a D number must comply with the same requirements for requisition of a D number in the regulations on national registration [14]. Accumulated information shall be stored and deleted in accordance with the provisions in § 22 of the Money Laundering Act and § 17 of the money laundering regulations (hvitvaskingsforskriften).	A			

4.7 Software requirements

The certificate holder's access to an eID normally requires specially adapted software, e.g. drivers for smartcards and card readers, as well as access to the card's data structures. Software can be permanently installed in the certificate holder's systems or solutions based on Java applets, or equivalent technologies, can be used. The software will usually provide an interface, preferably as defined in open standards, for integration of PKI solutions with applications such as e-mail and browser for an end-user, or professional systems for an enterprise.

4.7.1 The certificate holder's software

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.7.1.1	**Platform independence** The solution shall not restrict the certificate holder to a single platform in respect of the operating system or browser, for example.	A			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
	It shall be specified which hardware the certificate holder may use (PC, MAC, PDA, etc.). Any requirement for interfaces for the equipment (serial port, USB, etc.), shall be specified. Required hardware installation shall be described (e.g. card reader).				
4.7.1.2	**Universal design** The solution shall comply with requirements for universal design in accordance with the Act of 20th June 2008 no. 42, § 11 relating to a prohibition against discrimination on the basis of disability (Anti-discrimination and Accessibility Act) [15], within the stated deadlines under the provisions of the Act.	A			
4.7.1.3	**Support for 'thin clients'** The solution shall be able to support the use of 'thin clients' (Citrix terminal server and similar) for the certificate holder.	C			
4.7.1.4	**Installation of basic software for access to eID** The certificate issuer shall state whether the specific software for access to eID (e.g. for access to a smartcard on a PC) must be permanently installed in the certificate holder's systems. System requirements (operating systems, etc., that are supported) for the software shall be specified.	A			
4.7.1.5	**Use of Java applets and similar** The certificate issuer shall specify whether Java applets or similar technologies are being used to gain access to eID. System requirements (operating systems, etc., that are supported) for the software shall be specified.	A			
4.7.1.6	**Integration with third party software** The certificate issuer shall provide one or more solutions that make the PKI functionality easily accessible for the certificate holder's third party software. The solutions shall support standard interfaces like PKCS#11 [m] and Microsoft CAPI. It shall be specified which interfaces (standard or non-standard) are supported. System requirements (operating systems, etc., that are supported) for the software shall be specified.	C			
4.7.1.7	**Software maintenance** Procedures for maintenance of software and updating of installed software (where relevant) shall be described.	A			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.7.1.8	**Licences** All licences required for software, etc., shall be covered by the certificate issuer's agreement with the certificate holder.	A			
4.7.1.9	**The certificate holder's security and system settings** Where access to eID requires special settings for security on the certificate holder's equipment (e.g. configuration of firewalls), this shall be specified.	A			

4.7.2 The certificate recipient's software

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.7.2.1	**The certificate recipient shall not require an integration module** The certificate recipient shall be able to receive and process certificates without any other type of facilitation than the configuration of their existing systems, e.g. installation of the certificate issuer's root certificate and configuration of access to the OCSP service, as well as any access to CRL and directories.	C			
4.7.2.2	**Integration module specification** Where the certificate issuer (with the possible help of collaborating partners) provides integration modules to certificate recipients, the following requirements will apply: In order to be a certificate recipient, it shall be specified whether the integration module is required (see previous requirement). It shall be specified which integration modules are being provided, e.g. integration modules for service owners and integration modules for the PC environment. For each integration module, it shall be specified which interfaces (e.g. PKCS#11 [m] and Microsoft CAPI) are supported. System requirements for the software shall be specified. This applies to supported operating systems and also any requirements for the programme environment (e.g. J2EE, .Net, etc.).	A			
4.7.2.3	**Software maintenance** Where integration modules are provided, procedures for software maintenance and updating of installed software shall be described.	A			
4.7.2.4	**Documentation for integration modules** Where integration modules are offered, sufficient documentation shall be provided to allow a programmer with general expertise, but no knowledge of the interface, to utilise it.	A			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.7.2.5	**Example code** Where integration modules are offered, a compilable example code shall be available showing the use of all functions in the programming language of the application.	A			
4.7.2.6	**Licences for the service owner** All integration module licences and any other required software licences shall be covered by a user site agreement (an individual agreement or an agreement encompassing several public sector service owners) between the certificate issuer and the certificate recipient.	A			
4.7.2.7	**Licences for end-users** Where integration modules for end-users are offered (to enable the holder of a person certificate to also act as a certificate recipient), licences shall be covered by the certificate issuer's agreement with the certificate holder.	C			

4.8 Maintenance and revocation of certificates

4.8.1 General requirements, all certificate types

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.8.1.1	**Revocation of certificates** The certificate issuer shall provide a service for the revocation of certificates. The service shall permit certificates to be revoked in response to a written, telephonic or electronic communication that contains sufficient authentication. The service shall be available 24 hours a day, seven days a year. Details shall be provided of person(s) authorised to demand the revocation of a certificate and the mechanisms available for protecting against erroneous revocation.	A			
4.8.1.2	**Events requiring revocation** As a minimum, the certificate issuer shall revoke (or suspend, if applicable) certificates on their own initiative in the event of the following: • Where a certificate has been compromised, including notification regarding loss of a private key. • The certificate issuer discovers or has reason to believe that vital information in the certificate is incorrect.	A			
4.8.1.3	**Renewal of certificates** The certificate issuer shall provide a service for the renewal of certificates and keys, e.g. at the expiry of their period of validity,	A			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
	upon revocation of a certificate, or in the case of loss of key carrier/protective mechanism. It shall be specified how this service is offered to the certificate holder. The service shall be capable of offering automatic initiation of renewal. The certificate issuer shall specify the delivery time for certificate renewals.				

4.8.2 Additional requirements for Enterprise

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.8.2.1	**Revocation of enterprise certificates** The certificate issuer shall ensure that any amendments to an enterprise's status in the Central Coordinating Register for Legal Entities that might affect the enterprise's enterprise certificate will result in the revocation of the enterprise certificate no later than 10 working day after being entered in the Register. As a minimum, this applies to: • Changes to the certificate holder's organisation, e.g. as a consequence of closing down. • Changes to the connection to the general registration entity for enterprise certificates that identify sub-entities.	A			

4.9 User support

Unless otherwise specified, this means assistance for users of the PKI service (certificate holders).

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
4.9.1	**Documentation of user support** As a minimum, the following aspects of the user support (help desk) function shall be described: • The service. • Organisation of the service. • Which tasks are solved as 1st line and 2nd line tasks. • Whether enquiries concerning the withdrawal of certificates shall be addressed to user support or as an enquiry to a separate service. • Escalation procedures for support enquiries. • Response time, i.e. the planned reaction time to enquiries. • How certificate holders gain access to the service, whether this is by telephone, electronic mail or web interface. • How user support for certificate holders can be integrated with user support for the applications they utilise.	A			
4.9.2	**Operation of user support** A user support function offering direct assistance in Norwegian to the client shall be offered. As part of the service, user support shall also cover software and hardware supplied to the certificate holder. (This requirement applies to user support for the certificate holder, application developer and operation.)	A			
4.9.3	**Call-out service** In connection with the user support service, the certificate issuer shall also offer call-out services. It shall be specified which areas such services are provided for and the applicable response time. (This requirement applies to user support for the certificate holder, application developer and operation.)	C			
4.9.4	**User support for application developers** A user support scheme shall be offered for application developers using a programme interface to integrate PKI functionality. This service shall be described.	A			

5. REQUIREMENTS FOR LOOK-UP SERVICES AND DIRECTORIES

5.1 Status services and certificate directories

In order to utilise PKI services, status services are required that will respond to whether a certificate has been revoked. These services are available in real time from the certificate issuer. The requirements in this chapter will therefore include performance requirements. The values specified in these requirements are normally regarded as minimum values. Other performance requirements can be used in actual procurements based on this document.

The OCSP service for certificate status is mandatory. A status service in the form of CRL is strongly recommended and may be made mandatory in future versions of this document. There is a requirement that CRL is issued, but no mandatory requirement in respect of publishing.

In addition, there are requirements for a look-up service for national identity numbers linked to person certificates.

A directory service for published certificates would be desirable and is recommended for encryption certificates.

The certificate issuer should describe how the directory services are organised and operated and how these would be delivered, including, as a minimum:

- The relevant directory structure and search parameters that may be applied.
- Whether any form of access control mechanism has been established and, if so, how this functions.

5.2 CRL status service

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
5.2.1	**Revocation lists – regular issuance** The certificate issuer shall issue new CRLs in accordance with X.509 [f] regularly, at least every 24 hours. The frequency of CRL issuance shall appear on the certificate policy. CRLs shall comply with RFC 5280 [g]. CRLs shall only be made available to parties requiring access.	A			
5.2.2	**Revocation lists – issuance at revocation** Revocation of certificates will result in the issuance of an updated CRL, without any unreasonable delay, but no later than 3 hours after the certificate issuer has been made aware of the circumstances.	A			
5.2.3	**Publication of revocation lists** The most recent revocation list shall, as a minimum, be available	C			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
	over http and/or ldap [r]. Any other access interface shall be specified.				
5.2.4	**Restrictions to access** Any access restrictions to CRL shall be specified. Where there are access restrictions, the method of access verification to CRL shall be described.	A			
5.2.5	**Extra distribution points** In certain contexts, it will be inexpedient to obtain CRL from an Internet service. The certificate issuer shall therefore be able to facilitate the distribution of CRL from several distribution points. (Note that there is no requirement to publish URI for such alternative distribution points in the certificates.)	C			
5.2.6	**Availability of CRL status service** A CRL access service shall be available 24 hours a day, every day of the year. The service shall have sufficiently high uptime over the course of the year. The maximum permitted continuous downtime shall be 3 hours. The certificate issuer shall document how uptime is measured and maintained.	C			
5.2.7	**Performance for access to CRL status service** The time used to download a CRL is a function of the size of the CRL and the bandwidth of the connection. The certificate issuer shall describe how CRLs are made available and ascertain that the chosen solution performs satisfactorily.	C			
5.2.8	**Archiving of revocation lists for Person-High and Enterprise** The certificate issuer shall archive issued CRLs for a minimum of 10 years. The Certificate issuer's procedures for CRL archiving shall be described.	A			
5.2.9	**Archiving of revocation lists for Person-Standard** The certificate issuer shall archive issued CRLs for a minimum of 10 years. The Certificate issuer's procedures for CRL archiving shall be described.	C			

5.3 OCSP status service

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
5.3.1	**OCSP service** In the case of revocation of certificates, information shall be made available without any unreasonable delay, but no later than 1 hour after the certificate issuer became aware of the circumstances, with the help of an OCSP service as defined in	A			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
	RFC 2560 [h].				
5.3.2	**Restrictions to access** Any access restrictions to the OCSP service shall be specified. Where there are access restrictions, the method for access verification to the OCSP service shall be described.	A			
5.3.3	**Extra access points** In certain contexts, it will be inexpedient to use an OCSP service on the Internet. The certificate issuer shall therefore be able to facilitate alternative OCSP services. (Note that there is no requirement to publish URI for such alternative services in the certificates.)	C			
5.3.4	**Performance of the OCSP service** Searches in the OCSP service shall generate replies within 1 second (irrespective of workload). The measurement point is the interface with the public network.	A			
5.3.5	**Availability of the OCSP service** The OCSP service shall be available 24 hours a day, every day of the year. On average, over the course of the year, the OCSP service shall have a minimum uptime of 99.5 %. The maximum permitted continuous downtime shall be 3 hours. The certificate issuer shall document how uptime is measured and maintained.	A			
5.3.6	**Archiving of OCSP responses** The certificate issuer shall archive all OCSP responses for a minimum of 10 years. The Certificate issuer's procedures for the archiving of OCSP responses shall be described.	C			

5.4 Access to directory services

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
5.4	**Access to directory services** It shall be specified if directory services are supplied. In such cases the requirements below will apply.	O			
5.4.1	**Certificate directory of issued certificates** The certificate issuer shall offer a directory of issued certificates. The directory shall be available with the help of ldap v3[5] [r]. Specify any other interface to the directory.	C			
5.4.2	**Form and search options** The ldap directory form shall be documented. Directory	A			

[5] Or newer versions when these have become generally used in the market.

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
	information search options shall also be documented.				
5.4.3	**Extra distribution points for the directory** In certain contexts, access to the directory from an Internet service will not be expedient. The certificate issuer shall therefore be able to facilitate access to directories from several distribution points.	C			
5.4.4	**Accessibility consent** Person certificates shall be made publically available only in cases where the certificate holder has given their consent, cf. § 14, 2nd para., letter b, of the Act on Electronic Signatures.	A			
5.4.5	**Access restrictions** Any access restrictions to the directory shall be specified. Where there are access restrictions, the method for access verification to the directory shall be described.	A			
5.4.6	**Connection to an organisation number** In the case of enterprise certificates, details shall be provided of how searches in the directory will show the connection between a certificate and an organisation number.	A			
5.4.7	**Performance of directory searches** The directory service shall provide a response within a maximum of 1 second per search (irrespective of workload). The measurement point is the interface with the public network.	A			
5.4.8	**Directory service availability** The directory service shall be available 24 hours a day, every day of the year. The service shall have sufficiently high uptime over the course of the year. The maximum permitted continuous downtime shall be 3 hours. The certificate issuer shall document how uptime is measured and maintained.	A			

5.5 Access to look-up services

5.5.1	**Look-up service for national identity numbers and D numbers** The certificate issuer shall offer a lookup service permitting authorised parties to connect a certificate to a national identity number/D number. The services shall be in accordance with 'Interface for access to Lookup services' [11] and the release of a national identity number/D number shall be in compliance with § 12 of the Personal Data Act, [6] and § 10-2 of the personal data regulations (personopplysningsforskriften) [7]. The service shall be described.	A			

5.5.2	**Look-up service for the certificate's unique identifier** The certificate issuer shall offer a service permitting authorised parties to connect a certificate to a national identity number/D number, through tracing of the national identity number and return of either the certificate(s) or the unique identifier that is encoded in the attribute 'serialNumber' in the certificate holder's name in the certificate.	C			

5.6 Joint access to status services

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
5.6.1	**Certificate status access** A joint point of access to the certificate status information (OCSP or CRL as described in chapter 5) for the administration shall be facilitated, so that searches can be made by any public sector enterprise whatsoever. Such searches shall not require installation of software specific to the certificate issuer.	A			

5.7 Maintenance of directory and look-up services

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
5.7.1	**Planned downtime** If the certificate issuer has a requirement for updating, revision or maintenance of the service, this shall be agreed with the client within reasonable time before the work commences. Such work shall preferably be undertaken between 01.00 am and 04.00 am on Saturdays, Sundays or Mondays. Agreed downtime is not counted as lack of uptime. Periodic operating procedures such as back-up shall not be counted as agreed downtime. Planned downtime shall not exceed 3 hours per calendar month.	A			
5.7.2	**Operating information** Operating information that is of significance to certificate recipients, such as planned downtime, faults etc., shall be available on a dedicated website. The website shall be available to certificate recipients. The certificate issuer shall also offer a notification service that gives notice of such events.	A			
5.7.3	**Termination of the certificate issuer's service or enterprise** The certificate issuer shall describe whether, and if so, how, it is intended that certificates and status information will be maintained in the event of the termination of the certificate issuer's service or enterprise, see § 3 in the regulations for issuers of qualified certificates, cf. § 14 of the Act on Electronic Signatures.	A			

6. REQUIREMENTS FOR AUTHENTICATION SERVICES

Authentication services should permit certificate holders to gain access to electronic services through the utilisation of PKI based techniques. The service owner should, for their own part, obtain verification of the user's identity, with a specified and understood level of trust (authentication).

PKI based authentication is undertaken with a protocol in which the certificate holder signs a challenge from the opposing party (e.g. a random number sent by a service owner) with a private key, and this signature is verified with the certificate. Even though it is possible for authentication to be followed by communication over an open channel, in practice, a secure communication channel is always preferable where the security requirements demand a PKI based authentication.

In this context, a secure communication channel can be established with the TLS/SSL protocol. TLS/SSL requires authentication of the server side with an SSL server certificate (not covered by this document) and a secure channel can be established, initiated by the server side on its own (unilateral TLS).

Authentication of the user side (bilateral TLS) as well, is optional in the TLS/SSL protocol. It is strongly recommended that eID can be used for bilateral TLS. This provides enhanced security (protection from 'the-man-in-the-middle' (MITM) attack, among others) since both ends are authenticated through integration with the establishment of the secure communication channel. Usage scenarios are:

- Logging on to a service owner where a person certificate (or enterprise certificate) is used for TLS user authentication.
- Set-up of a secure communication channel between IT systems for two enterprises (private-public or public-public) in which 'user authentication' is completed with an enterprise certificate.

An alternative scenario for logging on, covered by this document, is that the service owner sets up a unilateral TLS channel and that the user later authenticates through a dedicated protocol.

A secure communication channel offers confidentiality and integrity protection of content between the terminal points of the channel. Beyond the terminal points at both ends, the content is unprotected plain text. Where the content passes through a chain of channels, it will remain unprotected in all intervening nodes. It is therefore vital to assess when channel security with PKI based authentication of users is sufficient, and when there is a need for additional security mechanisms, i.e. message security (message encryption).

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
6.1	**Authentication services** It should be specified if authentication services are provided. In such cases the requirements below will	O			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
	apply.				
6.1.1	**PKI based authentication** It shall be possible to use eID in a PKI based protocol for authentication. For protocols other than TLS/SSL, the protocol shall be documented and it shall be ascertained that it provides adequate security.	A			
6.1.2	**Channel setting for authentication** Where the PKI based protocol is performed after set-up of a (unilateral) TLS/SSL channel, it shall be described how authentication of the end-users is linked to the secure channel (to prevent a 'man in the middle' attack).	A			
6.1.3	**Requirement for special software, certificate holder** Where the authentication protocol creates a need for the installation of software in the certificate holder's systems, and also any use of Java applets or equivalent technology, this shall be specified. Such software shall be regarded as part of software packages for the utilisation of an eID, and shall be subject to the requirements specified in 4.7.1.	C			
6.1.4	**Requirement for special software, certificate recipient** Where the authentication protocol creates a need for the installation of software in the certificate recipient's systems, and also any use of Java applets or equivalent technology, this shall be specified. Such software shall be regarded as part of software packages for the utilisation of an eID, and shall be subject to the requirements specified in 4.7.2.	C			

7. REQUIREMENTS FOR SIGNING SERVICES

An advanced electronic signature is a cryptographic checksum of a limited amount of data (message, document), in which:

- The checksum is made with the assistance of the certificate holder's private key marked with the term 'signing'.
- The checksum can be verified through use of the certificate holder's corresponding public key, and
- the result is packaged as a signed data object (SDO).

It is strongly recommended that eID should be available over open interfaces for integration with third party software (see requirements in 4.7.1). This chapter will therefore provide

general requirements for signing applications, irrespective of whether the application has been supplied by the certificate issuer or others.

Third party suppliers of signing software *may* self-declare their software in accordance with these requirements.

The results of a signing operation should be SDO in standard format. A recipient of SDO should not be required to install specific software to handle either the SDO format or the validation of certificates for signatures.

7.1 General signing requirements

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
7.1	**Signing services** It shall be specified *whether* the certificate issuer is supplying signing services. In such cases, the relevant requirements in this chapter will apply.	O			
7.1.1	**Support for standard signature formats** Signed data objects shall comply with an established standard format that the recipient could reasonably be expected to handle. Examples are: XML DSIG, PKCS #7 [e], CMS [n], PDF, XAdES (ETSI TS 101 733 [c]), CAdES (ETSI TS 101 903 [d]) and the SEID SDO signing format[6].	A			
7.1.2	**Universal design** The solution shall comply with requirements for universal design in accordance with the Act of 20th June 2008 no. 42, § 11 relating to a prohibition against discrimination on the basis of disability (Anti-discrimination and Accessibility Act) [15], within the stated deadlines under the provisions of the Act.	A			
7.1.3	**Certificates in SDO** SDO shall, as a minimum, contain the certificate of the signing party, as well as any certificates in the certificate path, up to the root certificate.	A			
7.1.4	**Certificate issuer's software, certificate holder** If the *certificate issuer* supplies software or signing services (possibly with a collaborating partner) this shall be regarded as part of software packages for the utilisation of an eID, and shall be subject to the requirements specified in 4.7.1.	C			

[6] Note that the SEID signing format and some of the formats specified in XAdES and CAdES are storage formats more than exchange formats. It is therefore more relevant to use other basic formats for exchange and rather build XAdES, CAdES or SEID SDO on the recipient's side, in connection with archiving.

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
7.1.5	**Open signature validation** An arbitrary recipient in the public sector shall be able to verify a signed document without requiring the installation of the specific eID software used at signing. Verification shall be possible with software chosen by the recipient and shall only require configuration of the recipient's systems (installation of the certificate issuer's root certificate and configuration of access to the OCSP service and/or the CRL service).	A			
7.1.6	**Certificate issuer's software, certificate recipient** If the *certificate issuer* supplies software or a service for the verification of a signed document (possibly with a collaborating partner), this shall be regarded as part of software packages for the utilisation of an eID, and shall be subject to the requirements specified in 4.7.2. Note that requirement 7.1.5 states that such software shall not be necessary.	C			

7.2 Signing requirements for Person-High

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
7.2.1	**Use of private key** Upon signing information, it shall be ensured that the certificate holder authorises every operation involving the use of a private key with a PIN, password or similar.	A			
7.2.2	**Requirements for the signature creation application** Hash algorithms for signing must comply with the requirements for level standards in ETSI TS 102 176-1 [s]. Where there is a need to switch a hash algorithm, the plan for transition to the new algorithm shall be specified. It shall be further documented whether the solution corresponds with the requirements and recommendations in CWA 14170 [k]. Comments shall be provided to each of the points 1-17 in Annex A, A1. In addition, the following points from CWA 14170 [k] shall be documented: If information elements relating to signing (authentication code, keys, documents, attributes, hash value) are transferred over the Internet or between different platforms, this shall be described. Also, the way in which integrity, confidentiality and completeness are safeguarded shall be specified (see Section 7.3). Describe how security requirements for authentication in item 11.8 in CWA 14170 will be satisfied. Describe the safeguards in place to ensure that signature attributes cannot be changed from the attributes chosen by the user or system. Describe the warnings given to the user if signature attributes contain concealed text. If the software contains a dedicated module for presenting the signer's document/data, or provides software for analysing the signer's document/data in order to find concealed codes and data concealed from the signer, the format (Data Content Type) that the	C			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
	software is capable of showing/analysing shall be specified. Describe the warnings that are given if the document contains hidden codes (e.g. macros) or if it is not possible to show all parts of the document.				
7.2.3	**Signature verification** It shall be documented whether solutions for presenting and verifying signed date comply with the requirements of CWA 14171 [l]. State whether the solution is able to: • Present the document as it was shown at the time of signing • Notify the user of any dynamic content in the document • Clearly display the status of signature verification • Ensure that data used to verify the signature complies with the data shown to the verifying party • Ensure that a correct and valid (at the time of signing) certificate is used for the purpose of signature verification • Ensure that any changes relevant to security are discovered.	C			

7.3 Signing requirements for Person-Standard

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
7.3.1	**Use of private key** The user shall have the option of choosing whether each operation that involves the use of a private signing key shall be authorised.	A			

7.4 Signing requirements for Enterprise

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
7.4.1	**Use of private key** With signing of information in which the use of a private key is under the control of a person, it shall be ensured that the certificate holder authorises every operation involving the use of a private key with a PIN, password or similar.	A			

7.5 Quality of use

The following requirements apply if the solution includes user dialogues:

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
7.5.1	**User-friendliness** All user interfaces shall be straightforward and user-friendly. Where de facto standards for user dialogue or user interface have been established, there shall be an option to use them. For example, it shall be possible to publish the relevant standards in the Reference Directory for IT Standards in the Public Sector [16].	A			
7.5.2	**Language** All user dialogues shall be available in Norwegian.	A			
7.5.3	**Help text** Help text shall be available or installable in Norwegian in connection with all user dialogues.	A			
7.5.4	**Instructions for use** Instructions for installation and use shall be available in Norwegian.	A			
7.5.5	**Adaptation of user dialogue** User dialogues in connection with signing shall be adaptable. E.g. this could contain references to signed documents.	C			
7.5.6	**Matching of graphic profile** It shall be possible to adapt the graphic profile of the authentication and signature dialogues to match the application's profile.	C			
7.5.7	**Deliberate actions** The user shall be given a clear warning that they are about to sign the document. The user shall have the option of terminating the signing process.	A			
7.5.8	**'What You See Is What You Sign' (WYSIWYS)** What the user sees shall match what they sign. The way in which this principle is satisfied shall be documented.	A			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
7.5.9	**Response time** Authentication and signing shall take no more than three seconds (not including the time it takes the user to enter a PIN).	A			

7.6 Qualified signatures

7.6	**Qualified signature** It shall be specified *whether* the certificate issuer supplies qualified signatures. In such cases the requirements below will apply.	O			
7.6.1	**Secure signature creation system** The signature creation system shall comply with the requirements of a secure signature creation system, cf. § 9, the Act on Electronic Signatures.	A			
7.6.2	**Use of private key** Upon signing information, it shall be ensured that the certificate holder authorises every operation involving the use of a private key with a PIN, password or similar.	A			
7.6.3	**Requirements for the signature creation application** The hash algorithm for signing must comply with the requirements for level standards in ETSI TS 102 176-1 [s]. Where there is a need to switch a hash algorithm, the plan for transition to the new algorithm shall be specified. It shall be further documented whether the solution corresponds with the requirements and recommendations in CWA 14170 [k]. Comments shall be provided to each of the points 1-17 in Annex A, A1. In addition, the following points from CWA 14170 [k] shall be documented: If information elements relating to signing (authentication code, keys, documents, attributes, hash value) are transferred over the Internet or between different platforms, this shall be described. Also, the way in which integrity, confidentiality and completeness are safeguarded shall be specified (cf. item 7.3 in CWA 14170). Specify how the security requirements for authentication in item 11.8 in CWA 14170 will be satisfied. Describe the safeguards in place to ensure that signature attributes cannot be changed from the attributes chosen by the user or system. Describe the warnings given to the user if signature attributes contain concealed text. If the software contains a dedicated module for presenting the signer's document/data, or provides software for analysing the signer's document/data in order to find concealed codes and data concealed from the signer, the format (Data Content Type) that the software is capable of showing/analysing shall be specified.	A			

	Describe the warnings that are given if the document contains hidden codes (e.g. macros) or if it is not possible to show all parts of the document.				
7.6.4	**Signature verification** If the software in item 7.1.4. is offered, it shall be documented whether solutions for presenting and verifying signed date comply with the requirements of CWA 14171 [l]. State whether the solution is able to: • Present the document as it was shown at the time of signing • Notify the user of any dynamic content in the document • Clearly display the status of signature verification • Ensure that data used to verify the signature complies with the data shown to the verifying party • Ensure that a correct and valid (at the time of signing) certificate is used for the purpose of signature verification • Ensure that any changes relevant to security are discovered.				

8. REQUIREMENTS FOR MESSAGE ENCRYPTION

This document deals with requirements for two methods of PKI based confidentiality protection: Channel security/channel encryption and message encryption.

Both methods can cover several different requirements and also display great differences in the way that the solution is implemented and the technical properties they possess. For a given purpose, the requirement must be identified and the most appropriate solution assessed.

This chapter only deals with requirements for message encryption. (Requirements in connection with channel encryption are provided in the context of authentication functions in chapter 6.)

Message encryption (also known as end-to-end encryption, document encryption or permanent encryption) describes a method for safeguarding confidentiality whereby the sender encrypts a message at the point of origin that can only be decrypted by the intended recipient. Message encryption is implemented by the sender encrypting a message with the aid of a public key from the recipient's certificate (which must be marked that the user is permitted to do so). The message can then be decrypted by the certificate holder through the use of the private decryption key corresponding to the certificate being used. The message is not only encrypted when it is transmitted over the network, but also during storage in intervening systems.

Most public enterprises process personal information and/or confidential information in one or parts of their operation. The processing of such information is covered by the client confidentiality clause in the Public Administration Act, exclusionary provisions of the Open File Act, provisions of the Personal Data Act, and provisions of other Acts. When such information is electronically transmitted there may be a requirement to safeguard its confidentiality using message encryption.

It is optional whether message encryption that complies with this document is supplied. It will not be possible to use eIDs for applications requiring message encryption that are not supported by these requirements.

Third party software for encryption and decryption may be supplied by the certificate issuer (or possible collaborating partners) or by the third party's software supplier.

Requirement no.	**Description of requirement**	**Directory**	**Answer from supplier**		
			Y	**N**	**P**
8.1	**Message encryption** It shall be specified if the certificate issuer provides eID that can be used for message encryption. In such cases the requirements below will apply.	O			
8.1.1	**Encryption of messages with the sender's software** A certificate marked for encryption shall be available for use in software chosen by the sender. A sender in the public sector shall not need to install specific software or have a separate agreement with the certificate issuer in order to carry out encryption to a certificate holder.	A			
8.1.2	**Certificate accessibility** Accessibility of encryption certificates shall be facilitated either • by the certificate holder being able to publish their encryption certificate as part of an approval service (cf. requirement 5.4.6) or • by providing access to the directory of issued certificates specified in 5.4.1, 5.4.3 and 5.5.2. If the requirement complies with directory access, a look-up service shall also be established in which it is possible to trace a national identity number and obtain, in return, an identifier for the certificate (see requirement 5.5.1).	A			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
8.1	**Message encryption** It shall be specified if the certificate issuer provides eID that can be used for message encryption. In such cases the requirements below will apply.	O			
8.1.1	**Encryption of messages with the sender's software** A certificate marked for encryption shall be available for use in software chosen by the sender. A sender in the public sector shall not need to install specific software or have a separate agreement with the certificate issuer in order to carry out encryption to a certificate holder.	A			
8.1.3	**Decryption** Decryption shall be facilitated by either: • The certificate holder obtaining a private decryption key through an open interface for integration with the certificate holder's third party decryption software (Any conditions connected to such integration shall be specified). or • that the certificate issuer provides encryption software, possibly with any collaborating partners. If the software is provided by the certificate issuer (possibly with any collaborating partners), this shall be regarded as part of software packages for the utilisation of an eID, and shall be subject to the requirements specified in 4.7.1.	A			
8.1.4	**Encrypted e-mail** It shall be possible to use eID for encryption (certificate) and decryption (private key) of e-mail in S/MIME v3 format. Any restrictions or conditions for such use shall be specified.	C			
8.1.5	**Requirements for crypto strength of symmetrical crypto** Encryption and decryption software shall use a NIST AES symmetrical crypto-algorithm with a minimum key length of 128 bits. Note that the fulfilment of this requirement in third party software is beyond the certificate issuer's control.	C			

9. ADDITIONAL SERVICES

9.1 Time-stamping

For solutions dependent on 'strong' non-repudiation, time-stamping from a trusted, external time-stamping service (TSA) may be preferable. In accordance with ETSI TS 102 023 [v], a TSA may be regarded as a 'certification service provider', as defined in the e-signature directive [5]. The certificate issuer may provide such a service as an additional service.

It is also possible for parties other than the certificate issuers to provide time-stamping services. In such cases, the recommended solution is that the TSA's certificates are issued by a certificate issuer, preferably with a separate trust anchor (ref. requirement 9.1.4).

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
9.1	**Time-stamping** It shall be specified if a time-stamping service is offered. In such cases the requirements below will apply.	O			
9.1.1	**Interface with the time-stamping service** The interface with the time-stamping service must comply with TSP [u].	A			
9.1.2	**Time-stamping service policy** The time-stamping service policy shall comply with ETSI TS 102 023 [v].	A			
9.1.3	**Security organisation** Requirements given in 4.3.1 of this document apply.	A			
9.1.4	**Separate trust anchor** TSA [v] shall not be subject to the same root certificate as any other certificate issuer.	C			
9.1.5	**Availability of TSA certificates** Relevant root certificates and the TSA's dedicated certificates shall be universally (openly) available and distributed in a secure and confidence-inspiring manner. The distribution procedure shall be documented.	A			
9.1.6	**TSA’s certificate, format** The format of TSA’s certificate shall be specified. The certificate shall support area of use signing. The certificate shall also be marked with extended key usage id-kp-timeStamping.	A			
9.1.7	**TSA's certificate as enterprise certificate** The TSA's certificate for the signing of time-stamps shall be an enterprise certificate in accordance with this document. The certificate shall support the application area of signing. In addition, the certificate	B			

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
	shall be marked with 'extended key usage id-kp-timeStamping'.				
9.1.8	**Restrictions to the use of TSA's certificate** TSA's certificate for the signing of time-stamps shall not be used for other purposes.	A			
9.1.9	**Requirements for cryptography and crypto equipment** Requirements given in section 4.4.1 and 4.4.2 of this document apply. i.e. a TSA shall have crypto-security corresponding to a certificate issuer on the level of Person-High.	A			
9.1.10	**Accuracy of time-stamps** Time-stamps shall have an accuracy of 1 second or more. (Requirements given in ETSI TS 102 023 [v].)	A			
9.1.11	**Accuracy of clocks** Sources for the synchronisation of clocks and the guaranteed accuracy of clocks in the service shall be specified.	A			
9.1.12	**Synchronisation with the Norwegian Metrology Service** The synchronisation of all clocks in the system shall be based on the time given by the Norwegian Metrology Service's atomic clock, or shall offer the equivalent degree of accuracy.	C			
9.1.13	**Validation over a period of time** It shall be ensured that time-stamps can be validated for 10 years after they were issued. This applies irrespective of whether the service continues to be operative at this point in time. Procedures for safeguarding this shall be described.	A			

9.2 Long-term storage beyond 10 years

Requirement no.	Description of requirement	Directory	Answer from supplier		
			Y	N	P
9.2	**Long-term storage** It shall be specified if a long-term storage service is offered. In such cases the requirements below will apply.	O			
9.2.1	**Long-term storage** Revocation lists shall be stored for a minimum of 30 years. Certificates shall be stored for a minimum of 30 years, in addition to the lifetime of the certificate.	A			
9.2.2	**Long-term storage beyond 30 years** The option of concluding an agreement on storage in excess of 30 years shall be offered.	A			