

Requirements specification for PKI for the public sector

Version 1.02
January 2005

**The Ministry of Modernisation, Norway,
English translation of Publication No. P-0918**

CONTENTS

- 1. Introduction 4
 - 1.1 Purpose and background 4
 - 1.2 Use of the requirements specification 5
- 2. Scope and conditions 7
 - 2.1 Scope 7
 - 2.2 Definitions 8
 - 2.3 Abbreviations 9
 - 2.4 Referenced documents 10
 - 2.5 Referenced standards..... 10
 - 2.6 Explanation of tables 11
 - 2.7 Security levels 12
- 3. General requirements applicable to the products and services supplied 15
- 4. Requirements applicable to keys and certificates..... 16
 - 4.1 General requirements applicable to certificates 16
 - 4.2 Person certificates in certificate class High..... 19
 - 4.3 Person certificates in the Standard certificate class 20
 - 4.4 Enterprise certificates 21
- 5. Requirements applicable to directory and lookup services 22
 - 5.1 Certificate repositories and revocation lists 22
 - 5.2 Linkage to national identity number 24
- 6. requirements applicable to the ra service 25
 - 6.1 Person certificates in certificate class High..... 25
 - 6.2 Person certificates in certificate class Standard 27
 - 6.3 Enterprise certificates 27
- 7. requirements applicable to the signature creation system 28
- 8. requirements applicable to the user environment 30
 - 8.1 Quality of use 30
 - 8.2 Application integration..... 30
 - 8.3 End user systems 31
 - 8.4 User support 32
 - 8.5 Documentation 33
 - 8.6 Response times and availability 34
- 9. requirements applicable to commercial and technical interoperability 35
- 10. Options 37
 - 10.1 Time stamping..... 37
 - 10.2 Notarisation 38
 - 10.3 Long-term storage beyond 10 years 39
 - 10.4 High level of availability..... 39
 - 10.5 Security portal 39
 - 10.6 Qualified signatures 39
 - 10.7 Solution for internal use within public sector agencies 40
 - 10.8 Hardware-based solutions for enterprise certificates 41
- 11. APPENDIX 1 Security levels 42
- 12. APPENDIX 2 Assessment of the requirements applicable to security levels for electronic communications with the public administration..... 50
- 13. APPENDIX 3 The composition of the working group and the reference group 52
- 14. APPENDIX 4 External summary of the SEID workshop on commercial interoperability May 2004 53

15. APPENDIX 5 The SEID Project, publication: task 1 "Recommended certificate profiles for person certificates and enterprise certificates" 53

1. INTRODUCTION

1.1 Purpose and background

This document is a general, functional specification of the requirements applicable to the procurement of PKI (Public Key Infrastructure) for use in connection with electronic communication with and within the public sector.

This requirements specification was drafted in response to a resolution adopted by the Norwegian Government on 17 June 2004, requiring a common specification for electronic ID and signature to be formulated by 15 November 2004. The specification will in turn form the basis for common framework agreements for use by the public sector. The resolution reflects the Government's goal of unlocking the potential that lies in making more public services available in electronic form, allowing the dealings of the citizens, business and industry of Norway with public sector agencies to be simplified and enhancing the efficiency of public administration. The availability of electronic ID and signature is increasingly seen as a prerequisite for efficient electronic interaction with citizens and the private sector.

The specification was drawn up by a working group headed by the Ministry of Modernisation and comprising ten government agencies, three ministries and one greater municipality. The requirements specification has also been reviewed by a reference group chaired by the National Insurance Administration and comprising five government agencies, two ministries and one greater municipality. Three authorities (inspectorates) with responsibilities relating to this area were observers. The compositions of both groups are shown in Appendix 5.

The scope of the requirements specification is intended to cover the need for electronic ID and signature and confidentiality¹ (if not met in other ways) within central government and municipal administration in the following areas:

- electronic services for the general public and business and industry, e.g. applications, notifications etc.;
- electronic reporting to public sector agencies, e.g. the Altinn Internet portal for public reporting;
- electronic document exchange between public sector agencies and between the public sector and private enterprises, at both enterprise and employee level, e.g. via e-mail;
- access to searches in central registers of basic data (via the Internet) for the public, business and industry and for public sector agencies;
- electronic casework within the public sector, e.g. the electronic processing of invoices.

A fundamental objective of the work has been that the requirements specification should simplify the assessment involved in choosing security mechanisms for various applications within the public administration. These assessments include for example weighing up the costs of introducing eID and signature, the user friendliness of a solution and the level of security provided.

¹ Confidentiality requirements that may for example be related to the duty of confidentiality provided for in the Public Administration Act (forvaltningsloven) and the exemptions in the Freedom of Information Act (offentlighetsloven) and the provisions of the Personal Data Act (personopplysningsloven).

It is intended that eID and signature solutions should be supplied by the market, in competition. Moreover, the eID acquired by a user must offer the broadest possible range of uses, i.e. it must permit use in as many electronic services as possible in which eID or e-signatures are required, not only within the public sector, but also in the private sector.

The contents of the document are designed to ensure that the requirements specification:

- as far as possible fulfils the electronic ID, signature and encryption requirements made by Altinn and the Norwegian Health Network,
- is formulated in such a way that it allows a variety of price and procurement models to be used,
- does not exclude the existing products and services of issuers of current certificates, particularly where there is a large number of certificates already in circulation on the market,
- as far as possible follows the recommendations of the SEID Project² and the relevant national standards,
- does not cover the confidentiality requirements that follow from Sikkerhetsloven (the Norwegian Security Act) and Beskyttelsesinstruksen (The Norwegian National Security Authority's standard cryptographic requirements),
- does not specify requirements for time stamping services if they are not related to authentication and signature functions,
- does not encompass types of certificates (e.g. attribute certificates) that are not currently supported by standard solutions available on the market,
- does not address the use of PKI in connection with securing networks, the use of SSL, signing programme codes etc.

1.2 Use of the requirements specification

The requirements specification shall be used in all public sector invitations for tenders for applicable products and services within the field of PKI. It is not the intention that invitations to tender should take in all areas covered in this requirements specification nor that one single Supplier should be capable of supplying solutions that cover all the requirements described herein.

Based on the requirements specification, descriptions of specific products or services will be compiled for the areas in question. One such area might be authentication and signature for use by the general public in web-based public sector services. A second area might be the procurement of certificate solutions for use by an agency's own employees for integration with the applicable IT systems of the agency. A third area might be the procurement of enterprise certificates for secure electronic communication between (public sector) agencies, via e-mail or integrated in message broker systems. In these cases a specific product or service description will detail which parts of this specification are relevant to the procurement, which requirements are not relevant, and will define any additional requirements.

These product and service descriptions will provide the basis for individual procurements or for framework agreements between the public sector, at both central government and local

² See <http://www.pki-forum/seid>

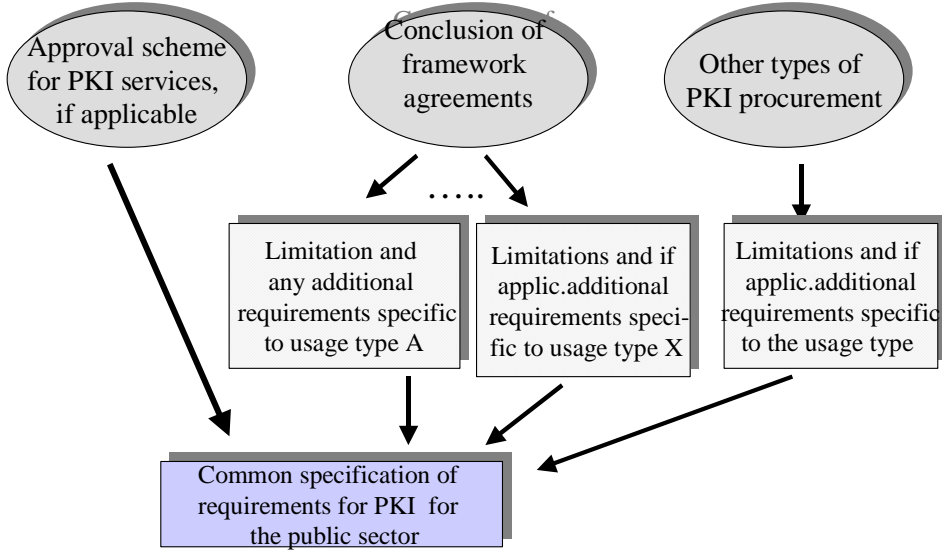
authority levels and one or more suppliers. Moreover, the agreements may also be used by private legal entities with service provision agreements with the public sector.

Public sector agencies wishing to issue independent invitations to tender to the market will be required to base their underlying documentation on this requirements specification.

The requirements specification might also be used as a basis for an approval scheme. The purpose of an approval scheme is to determine which certificates and certificate services meet the requirements of the public sector within the defined certificate classes. An approval scheme could contribute to the establishment of interconnection by establishing fixed evaluation assurance levels and simplifying the procurement process for both the private and the public sector.

The following figure summarises the areas in which it is intended that the requirements specification might be used.

Areas of use of the specification of requirements

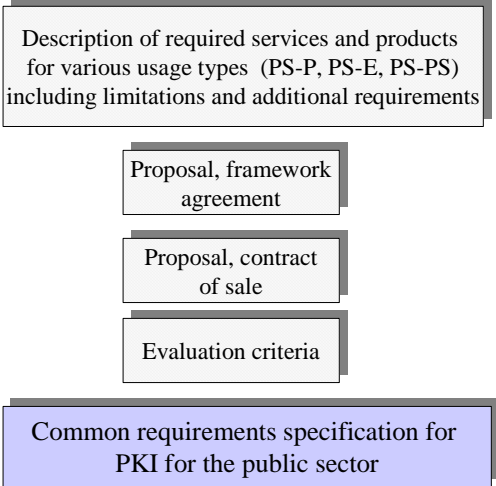


The requirements specification has been drafted to cover the requirements applicable to PKI products and services for all types of electronic communication with and within the public sector. Accordingly the document is not always specific within the individual areas of application and types of use (authentication, signature and encryption). A procurement will accordingly often require a closer definition of the requirements considered relevant to the area of use in question as well as any supplementary requirements that might apply.

The necessary documentation for announcements of invitations to tender will be compiled at central level in the form of draft framework agreements, draft contracts of sale, evaluation documentation etc. These will accompany the requirements specification when an invitation to tender is announced to the market. This documentation will specify the types of services and/or products to which the enquiry relates and which parts of the specification are to be

covered by the offers in question. It is not the intention that all bidders should be capable of supplying products and /or services that meet the entire range of requirements contained in this document.

Competitive basis for announcement of framework agreements



The figure describes the role of this document in the announcement of framework agreements for public sector procurements of PKI products and services.

2. SCOPE AND CONDITIONS

2.1 Scope

A comprehensive PKI solution might encompass:

- A certificate authority (CA) to issue and verify digital certificates
- A registration authority (RA) to verify the information to be included in a certificate before it is issued (or at the time of delivery)
- Directory and lookup services
- Solutions, e.g. software packages, that make the PKI functionality available in a straightforward way and that can be integrated with the end systems of the Client
- Interoperability and interconnection

The areas of use to be covered by the PKI are administrative executive work and communications with and within the public administration. The aim of the specification is to cover the work conducted by and communication between:

- Public sector agencies and Private individuals (PS-P)
- Public sector agencies and (Business) Enterprises³ (PS-E)
- Public sector agencies and Public sector agencies (PS-PS)
- Public sector agencies seeking to acquire person certificates for their employees

³ The enterprise need not be engaged in business. In this context "Enterprises" means all organisations with an organisation number, except public sector agencies.

The requirements specification will also be relevant to other areas of use, for example communications between private individuals and communications where employees of a public sector agency or a private enterprise wish to communicate directly.

The requirements cover PKI solutions for:

- Authentication/Identification
- Signature
- Encryption⁴

The requirements specification does not cover the use of PKI for signing program modules or authentication/key management of processes and computers.

Nor does the document define requirements for employee certificates, since it is assumed that in technical terms person certificates will in many cases cover this requirement. In such cases it will, inter alia, be the issuance procedures and rules on authorisation and use within an enterprise that will determine whether or not a person certificate can be used in a professional context. Much of this document can be used by enterprises seeking employee certificates explicitly linking a person to the enterprise.

The specification describes a PKI solution for integration with one or more applications. The degree of functionality provided by the application and by the PKI solution will vary depending on the solution proposed by the individual supplier. Accordingly, some requirements may be understood as functionality within the application, whereas for other solution concepts these will be requirements relevant to the PKI solution.

Similarly, there may be different solution concepts for the RA function. RA tasks can be performed by the CA, within the user site or within the user's system

2.2 Definitions

Employee certificate	A person certificate certifying that there is a relationship between an identified enterprise and an uniquely identified person within this enterprise. The relationship will typically be between employer and employee, although this is not a requirement.
User	The party using the application with the PKI functionality and the holder of the certificate.
User site	Enterprise offering electronic services on the Web, an enterprise with integration of electronic message exchange in internal systems or where standard e-mail is used for these exchanges.
IT system	An application that conducts its own digital signing and sends presigned data to the public sector. (For example an application in a doctor's office or an application in an accountant's office.)
National identity number	Eleven-digit number in which the six first digits specify date of birth and the five latter digits specify the personal number. Includes D-numbers for foreign citizens.

⁴ More specifically, PKI will be used for key exchanges in connection with encryption.

Integration module	A software module that can be called up by applications to perform actions tasks to electronic ID and signature.
The Client	The party or parties intending to acquire PKI solutions in accordance with this requirements specification.
The Supplier	The organisation or organisations intending to supply PKI solutions to public sector agencies in accordance with all or parts of this requirements specification.
Person certificate	A certificate where the certificate-holder is a natural person.
Registered address	The address registered in the Norwegian "Folkeregister" (National Population Register).
Commercial interoperability	Interoperability between different PKI vendors
Interoperability	In this context interoperability is defined in the same way as in "External summary of the SEID workshop May 2004" [11] (Ref Appendix 3) and with the more detailed definitions provided in Chapter 9.
Certificate issuer	A natural or legal person that issues certificates.
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. Information about enterprises may also be particularly sensitive in nature.
Enterprise certificate	Serves to identify a legal person, i.e. an enterprise registered in the Norwegian Central Coordinating Register for Legal Entities (Enhetsregisteret). A user of the private key associated with the certificate may be a natural person authorised by the enterprise or an automated process under the control of the enterprise, for example a server.

2.3 Abbreviations

AFPKI	The working group on common requirements specification for PKI in the public sector
API	"Application Programming Interface" (program interface)
CMS	Certificate Management Services
CRL	"Certificate Revocation List"
CWA	"CEN Workshop Agreements"
DSP	The Norwegian Central Register of Persons
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	"Normalized Certificate Policy"
NOU	Norges Offentlige Utredninger - Norwegian Official Reports
OCSP	"Online Certificate Status Protocol"
PIN	"Personal Identification Number"
PKI	"Public Key Infrastructure"
PKCS	"Public Key Cryptography Standard"
RA	Registration Authority

RFC	”Request For Comment” (Internet standard)
RSA	”Rivest, Shamir and Adleman” (Asymmetric encryption algorithm)
CA	Certificate Authority, issuer of certificates
SEID	Cooperation on Electronic ID and signatures, project for technical Standardisation of PKI Suppliers in the Norwegian Market.
S/MIME	”Secure/Multipurpose Internet Mail Extension” (Protocol for secure e-mail)
SSL	”Secure Socket Layer” (Protocol for secure WEB traffic)
TS	Technical Specification
URL	”Uniform Resource Locator” (”Address” for WEB information)

2.4 Referenced documents

- [1] Norwegian Official Report 2001:10 Without Pen and Ink (NOU 2001:10 Uten penn og blekk)
- [2] The Act of 15 June 2001 No. 81 on electronic signatures (Lov 15. juni 2001 nr. 81 om elektronisk signatur – e-signaturloven)
- [3] The Regulations of 25 June 2004 No. 988 on electronic communication with and within the Public Administration (the eGovernment Regulations) (Forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen – eForvaltningsforskriften)
- [4] The Regulations of 15 June 2001 No. 611 on requirements applicable to issuers of qualified certificates etc. (Forskrift 15. juni 2001 nr. 611 om krav til utsteder av kvalifiserte sertifikater mv.)
- [5] Directive of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
- [6] The Act of 14 April 2000 No. 31 on the processing of personal data (Lov 14. april 2000 nr. 31 om behandling av personopplysninger - personopplysningsloven)
- [7] The Regulations of 15 December 2000 No. 1265 on the processing of personal data (Forskrift 15. desember 2000 nr. 1265 om behandling av personopplysninger – personopplysningsforskriften)
- [8] The Act of 20 June 2003 No. 41 on measures to combat the laundering of proceeds of crime etc. (Lov 20. juni 2003 nr. 41 om tiltak mot hvitvasking av utbytte fra straffbare handlinger mv. – hvitvaskingsloven)
- [9] The Regulations on measures to combat the laundering of proceeds of crime etc. (Forskrift 10. desember 2003 nr. 1487 om tiltak mot hvitvasking av utbytte fra straffbare handlinger mv. – hvitvaskingsforskriften)
- [10] The SEID Project, Recommended certificate profiles for person certificates and enterprise certificates, Version 1.01, September 2004. See also Appendix 4.
- [11] The SEID Project, External summary of the SEID workshop May 2204, Version 1.0, September 2004. See also Appendix 3.
- [12] The SEID Project, Interfaces for access to lookup services (approved December 2004)

2.5 Referenced standards

The latest version of the following standards shall apply to this requirements specification.

- [a] NO NS-ISO/IEC 17799:2000 – Code of practice for information security management
- [b] ETSI TS 101 456 - Policy requirements for certification authorities issuing qualified certificates

- [c] ETSI TS 102 042 - Policy requirements for certifications authorities issuing public key certificates
- [d] ETSI TS 101 733 - Electronic Signature Formats
- [e] ETSI TS 101 903 - XML Advanced Electronic Signatures (XAdES)
- [f] PKCS #7 –The cryptographic message syntax standard
- [g] PKCS #12 –The personal information exchange syntax standard.
- [h] PC-SC –PC-SmartCard
- [i] X.509 - The Directory: Public-key and attribute certificate frameworks
- [j] RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- [k] RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
- [l] CWA 14169 - Secure Signature-Creation Devices
- [m] CWA 14170 - Security Requirements for Signature Creation Systems
- [n] CWA 14171 - Procedures for Electronic Signature Verification
- [o] PKCS #11 – Cryptographic Token Interface Standard
- [p] PKCS #15 – Cryptographic Token Information Format
- [q] CMS - Certificate Management Messages (RFC 2797)

2.6 Explanation of tables

The following chapters contain tables detailing numbered requirements.

These tables include a column for categories (Cat). The following codes are used in this column:

- | | | |
|-----------|---------------------------|--|
| A: | "Absolute requirement" | means that the requirement shall be satisfied in the offer. |
| C: | "Conditional requirement" | means that the requirement should be satisfied in the offer. |
| O: | "Option" | means that the requirement should be satisfied and that the solution to this requirement shall be supplied as a separate option with a separate price. |

There is also a column headed "Supplier's reply". In this column the Supplier shall enter:

- | | | |
|-----------|---------------|--|
| Y: | "Yes" | means that the requirement is satisfied in the offer and that the solution is included in the price of the offer. |
| N: | "No" | means that the requirement is not satisfied. |
| R: | "Reservation" | Here a number shall be entered referring to a specific description of the reservation.
"NA" shall be entered in this column if the requirement is not relevant to the delivery. |

In the case of requirements market O (Option):

- | | | |
|-----------|-------|---|
| Y: | "Yes" | means that the requirement is satisfied in an option to the |
|-----------|-------|---|

offer. If the option is exercised, this will entail a specified cost in addition to the offered price.

2.7 Security levels

A document describing security levels was drafted in parallel with this requirements specification. Three levels of security were identified, two for private individuals and one for enterprises.

The security levels and a selection of properties are specified in the table:

SECURITY LEVELS	Registration and release procedure	Requirements as to name structure and content	Requirements as to protection of private keys
"Person-High"	The certificate must be a qualified certificate and the certificate issuer must fulfil the registration and release procedures that follow from this, including the requirement as to personal attendance.	The name structure and certificate content must follow the requirements in Section 4 of the Act on Electronic Signatures (e-signaturloven) [2] with the clarifications that follow from "Recommended certificate profiles for person certificates and enterprise certificates" [10].	<ul style="list-style-type: none"> • Access to private keys must as a minimum require two-factor authentication, where one of the factors is something in the physical possession of the user (i.e. cannot be copied electronically). • The user must approve each operation involving private keys by authenticating him/herself • Private keys must never appear in plain text in registers that might be compromised or in other ways provide a basis for unauthorised use.

SECURITY LEVELS	Registration and release procedure	Requirements as to name structure and content	Requirements as to protection of private keys
"Person-Standard"	<p>The certificate issuer must fulfil the requirements in Sections 10 to 16 of the Act on Electronic Signatures (e-signaturloven)[2] and Section 3 of the Regulations on requirements applicable to issuers of qualified certificates etc. (Forskrift om krav til utsteder av kvaliserte sertifikater) [4].</p> <p>Verification must take place upon registration that the person is found in a Norwegian population register and that the name of the person accords with his or her national identity number.</p> <p>A reasonable degree of certainty must exist that keys and/or associated access codes/passwords and certificates are released to the correct person.</p> <p>Release must either be by postal dispatch to the registered address or electronically based on existing authentication mechanisms providing the same degree of security of correct receipt as a postal dispatch to the registered address.</p>	<p>The certificate must fulfil the requirements applicable to qualified certificates in Section 4 second paragraph letters b to j of the Act on Electronic Signatures (e-signaturloven) [2].</p> <p>In other respects the name structure and certificate content must follow "Recommend certificate profiles for person certificates and enterprise certificates" [10].</p>	<ul style="list-style-type: none"> • Access to private keys must require authentication • The user must have scope for choosing/deciding him/herself whether the individual operation involving private keys is to be approved. • Private keys must as a minimum be stored in encrypted form.

SECURITY LEVELS	Registration and release procedure	Requirements as to name structure and content	Requirements as to protection of private keys
<p>"Enterprise"</p>	<p>The certificate issuer must fulfil the requirements in Sections 3 and 7 of the Act on Electronic Signatures [2] (e-signaturloven) and Section 3 of the Regulations on requirements applicable to issuers of qualified certificates etc. (Forskrift om krav til utsteder av kvalifiserte sertifikater) [4].</p> <p>It must be possible to identify the enterprise uniquely 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].</p> <p>Safeguard must be in place to ensure that keys with associated access codes/ passwords and certificates are released to a person with the right to receive them on behalf of the enterprise. (Authorisation from an authorised signatory of the company.) Documentation of the relationship to be possible.</p>	<p>The certificate must fulfil the requirements as to qualified certificates in Section 4 second paragraph letters b to j of the Act on Electronic Signatures (e-signaturloven) [2].</p> <p>The name structure and certificate content must follow "Recommended certificate profiles for person certificates and enterprise certificates" [10]. The certificate must contain the organisation number of the enterprise.</p>	<ul style="list-style-type: none"> • Access control to private keys must be realisable. • The enterprise must have scope for choosing/deciding him/herself whether each operation involving private keys is to be approved. • Private keys must as a minimum be stored in encrypted form.

This requirements specification is based on the above security levels. Unless otherwise explicitly stated all requirements apply to all security levels.

Stricter security requirements may be defined in the future if solutions with qualified electronic signatures become available on the market and the public administration identifies a need for such requirements.

The requirements specification refers to the provisions of the Act on Electronic Signatures and the Regulations on the requirements applicable to issuers of qualified certificates etc. (Forskrift om krav til utsteder av kvalifiserte sertifikater) in the definition of Person-Standard and Enterprise. It must be made clear that these requirements - with the exception of the requirements in Sections 6 and 7 of the Act on Electronic Signatures (e-signaturloven) - generally apply only to qualified certificates (i.e. Person-High) and issuers of such certificates. Although this document refers to the provisions of the Act on Electronic Signatures with Regulations (e-signaturloven med forskrifter) applicable to Person-Standard and Enterprise, the effects of the requirements are contractual only and, as a general rule, in the event of breaches the sanctions provided for in the Act and the Regulations will not apply.

Reference is also made to Appendix 1 "Security levels" and Appendix 2 "Assessment of the requirements applicable to security levels for electronic communications with the public administration".

3. GENERAL REQUIREMENTS APPLICABLE TO THE PRODUCTS AND SERVICES SUPPLIED

The Supplier will be expected to provide solutions that are user-friendly and simple in terms of installation/implementation, integration (in the applications of the enterprise) and other administrative tasks at the user location. The requirement as to user-friendliness and simplicity also applies to the installation and maintenance of keys and certificates by the user (citizen or employee of an enterprise).

The solutions and services offered shall comply with the applicable acts and Regulations and satisfy the following requirements:

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
3.1	Certificate Authority and Registration Authority The Supplier shall provide a service that includes both CA and RA functions in accordance with applicable acts and Regulations. The requirements are described in further detail in Chaps. 4 and 6.	A			
3.2	Directory and lookup services The Supplier shall offer directory and lookup services that enable the distribution of certificates and validation services. The requirements are described in further detail in Chapter 5.	A			
3.3	Integration modules The Supplier shall offer one or more solutions (e.g. integration modules) that in a straightforward way make the PKI functionality available to partners and other software Suppliers/developers, such as electronic patient record systems and communications software, both in the end user environment and in the server environment. The requirements are described in further detail in Chapters 8 and 9.	A			
3.4	User-friendliness All user interfaces shall be straightforward and user-friendly. Where de facto standards for user-dialogue or user-interfaces have been established their use shall be permitted. The requirements are described in further detail in Chapter 8.	A			
3.5	Delivery capacity The Supplier shall have sufficient capacity to handle regular purchases without appreciable waiting times. The Supplier shall describe the ways in which this will be safeguarded, including the delivery time that will apply from the placing of an order until the receipt of a certificate and the delivery time for other services. The Supplier shall also describe the way in which the delivery of certificates, equipment and software will be coordinated upon receipt and installation by the certificate holder or the Client.	A			
3.6	Information security The Supplier's internal system for information security shall be safeguarded in accordance with the applicable acts and Regulations and as a minimum follow the applicable best practice	A			

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
	<p>for information security, e.g. by means of a management system for information security in accordance with NO NS-ISO/IEC 17799:2000 [a].</p> <p>The Supplier shall monitor the security of the solution on a continuous basis and implement measures when necessary. This includes measures in connection with the compromising of keys and the weakening of encryption algorithms and hash algorithms.</p> <p>Documentation shall be provided of the way in which the processing of personal data satisfies the applicable Act (personopplysningsloven) [6] and Regulations [7] and Section 7 of the Act on Electronic Signatures [2] (e-signaturloven). The customer may request documentation of implemented revisions that are no older than two years.</p>				
3.7	<p>Penetration</p> <p>The Supplier shall document the current number of users able to authenticate themselves and sign using the offered solution. Moreover documentation shall be provided of the number and type of applications that have been integrated with the solution. An overview shall also be provided of the forecast number of users and applications in one and three years.</p>	A			

4. REQUIREMENTS APPLICABLE TO KEYS AND CERTIFICATES

4.1 General requirements applicable to certificates

Three types of certificates have been defined on the basis of identified security levels as described in Appendix 1. The table below shows the intended use of the various types of certificates:

USES FOR CERTIFICATE LEVELS	Authentication	Signature (non-repudiation)	Receipt of encrypted information
Person-High	Transactions where there is a need for a high degree of certainty about 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 where there is a need for a high degree of certainty about 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 the damage caused by a compromise would be extensive.
Person-Standard	Transactions where there is a need for a reasonable degree of certainty about the identity of the originator or where the damage caused by a compromise would be medium level.	Transactions where there is a need for a reasonable degree of certainty about the connection between content and the identity of the originator or where the damage caused by the compromising of the connection would be medium level.	Documents etc. that do not contain particularly sensitive information and where the damage caused by a compromise would not be extensive.
Enterprise	Transactions where there is a need for a high degree of certainty that the originator is/represents a specified enterprise or where the damage caused by a compromise would be	Transactions where there is a need for a high degree of certainty about the connection between content and the specified enterprise or where the damage caused by the compromising	Documents etc. containing particularly sensitive information or where the damage caused by a compromise would be

	extensive.	of the connection would be extensive.	extensive.
--	------------	---------------------------------------	------------

See also Appendix 2 for an extended discussion of the security requirements applicable to electronic communications with the public administration.

The following requirements apply to all three types of certificates:

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
4.1.1	<p>Key generation</p> <p>The Supplier shall offer a secure process for key generation in accordance with Section 11 first and third paragraphs of the Act on Electronic Signatures (e-signaturloven) [2] and in compliance with the provisions of Section 3 No.2 letter c of the Act on Electronic Signatures (e-signaturloven) [2]. This applies to private keys generated by the Supplier or by software or equipment supplied by the Supplier.</p>	A			
4.1.2	<p>The revocation of certificates</p> <p>The Supplier shall provide a service for revoking certificates. The service shall permit certificates to be revoked in response to a written, telephonic or electronic communication with sufficient authentication. The service shall be available 24 hours a day, seven days a week. Information on any change of this nature in the status of a certificate shall be available in the revocation service without unaccounted delay, but no later than one hour after the Supplier became aware of the situation. Details shall be provided of the person(s) authorised to require a certificate to be revoked and the mechanisms available for protecting against erroneous revocation.</p>	A			
4.1.3	<p>Events requiring revocation</p> <p>As a minimum the Supplier shall revoke (or if applicable suspend) certificates on his own initiative if:</p> <ul style="list-style-type: none"> • a compromise is suspected, including the loss of a private key, • the Supplier discovers or has reason to believe that information in the certificate is incorrect, • significant changes occur in the customer's organisation as a consequence of closure or bankruptcy (applies to enterprise certificates). 	A			

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
4.1.4	<p>Renewal of certificates</p> <p>The Supplier shall provide a service for renewing certificates and keys, e.g. at the event of their period of validity, upon revocation of certificates or in case of loss of key carrier/protective mechanisms. The Supplier shall also specify how these services will be offered to the certificate holder. The service shall be capable of offering automatic initiation of renewal. The Supplier shall specify the delivery time for certificate renewals.</p>	A			
4.1.5	<p>Requirements as to the certificate issuer's operations</p> <p>The relevant business operations of suppliers offering certificate services for certificate class Person-High shall fulfil the "QCP public" requirements in ETSI TS 101 456 [b]. Any deviations shall be documented point by point. The consequences of deviations shall be stated.</p> <p>Suppliers offering certificate services for certificate class Person-Standard shall in the relevant parts of their business fulfil the LCP requirements in ETSI TS 102 042 [c]. Suppliers offering certificate services for certificate class Enterprise shall in the relevant parts of their business fulfil the NCP requirements in ETSI TS 102 042 [c]. Any deviations shall be documented point by point. The consequences of the deviations shall be stated.</p> <p>The above standards do not cover all types of key usage. Nevertheless, the Supplier shall reply to the requirements pertaining to all types of key usage implemented in the Supplier's service. Backups of encryption keys are exempted from this.</p>	A			
4.1.6	<p>Certificate format</p> <p>The certificate shall follow "Recommended certificate profiles for person certificates and enterprise certificates" [10], unless these are not relevant to the certificate type. If other formats are used any deviations shall be documented. The use of Norwegian characters⁵ in the certificates shall be permitted.</p>	A			
4.1.7	<p>Verification of certificate information</p> <p>The Supplier shall ensure that personal data entered in certificates has been checked against relevant registers, e.g. the DSP (Norwegian Central Register of Persons).</p>	A			
4.1.8	<p>Key requirements</p> <p>The Supplier shall specify the algorithms and key lengths that are used. Moreover, a description shall be provided of the maximum key length in the solution.</p>	A			
4.1.8.1	<p>RSA</p> <p>Asymmetric keys should be based on RSA and should have a length of at least 1024 bits.</p>	C			

⁵ Ref Norwegian Certificate Profile drafted by the SEID Committee.

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
4.1.9	Key usage The Supplier shall describe the guidelines and requirements applicable to the Key Usage field of the certificate. Descriptions shall also be provided of the number of keys and certificates allotted to each user in relation to Key Usage.	A			
4.1.10	Extensions The certificates should support user-specified non-critical extensions of the fields.	C			
4.1.11	Certificate policy The certificate policy applicable to the certificates in question shall be publicly available.	A			
4.1.12	CA certificate The necessary root certificates for verifying issued certificates shall be distributed in a secure and trustworthy way. Procedures shall be documented.	A			

4.2 Person certificates in certificate class High

Certificates in certificate class High are person certificates that are qualified certificates. Issuance is accordingly based on personal attendance⁶. The certificate shall permit linkage to a national identity number and the registration of the person in a Norwegian population register shall be verified.

This level permits various solutions for storing and protecting private keys.

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
4.2.1	Qualified certificates The Supplier shall issue qualified certificates in accordance with the Act on Electronic Signatures (e-signaturloven) [2] and Regulations (Forskrift om krav til utsteder av kvalifiserte sertifikater) [4]. The Supplier shall attach confirmation from the appropriate regulatory authority that the certificate issuer has the authority to issue qualified certificates or attach a copy of the registration notification to the same authority or provide evidence that such registration will take place before the agreement is signed.	A			
4.2.2	Protection of private keys The keys shall be protected in the following way: <ul style="list-style-type: none"> • Access to private keys shall require a minimum of two-factor authentication, where one of the factors is something in the physical possession of the user (i.e. 	A			

⁶ Cf. Section 13 of the Act on Electronic Signatures and Section 7 of the Regulations on requirements applicable to the issuance of qualified certificates etc.

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
	cannot be copied electronically). <ul style="list-style-type: none"> The user shall approve each operation involving private keys by authenticating himself/herself. Private keys shall never appear in plain text in registers that might be compromised or in other ways provide a basis for unauthorised use. 				
4.2.3	Securing the private key The Supplier shall describe how the requirements in 4.2.2 third bullet point are fulfilled. The Supplier shall document the robustness of the solution against known attacks.	A			
4.2.4	The lifetime of certificates The Supplier shall specify and give the reasons for the lifetime of keys and certificates. The minimum lifetime required is 13 months. (Temporary certificates with shorter lifetimes may be permissible.)	A			
4.2.5	Documentation requirements when the certificate is issued When the certificate is issued the Supplier shall require the user to present an identity document in compliance with the requirements in Section 4 first paragraph of the Money Laundering Regulations (hvitvaskingsforskriften) [9].	A			
4.2.6	Registering, storing and deleting information The certificate issuer is responsible for registering, storing and deleting information in accordance with Section 6 first and second paragraphs of the Money Laundering Act (Hvitvaskingsloven) [8] and Section 15 of the Money Laundering Regulations (hvitvaskingsforskriften) [9].	A			

4.3 Person certificates in the Standard certificate class

The Standard certificate class is a person certificate that may be issued without personal attendance. The certificate may be issued either by sending it by post to the registered address or electronically on the basis of an existing authentication mechanism that as a minimum provides the same level of certainty of correct receipt as does a postal dispatch to a registered address.

The certificate shall permit linkage to a national identity number and the registration of the person in the DSP (Norwegian Central Register of Persons) shall be verified.

Requirement number	Description	Cat	Supplier's reply		
			Y	N	R
4.3.1	Requirements as to the identification of certificate applicants In the registration and issuance/dispatch of certificates there shall be reasonable degree of confidence that the certificate is released to the correct person. Including: Verification shall take place at the time of registration that the person is to be found in the DSP (Norwegian Central Register of	A			

Requirement number	Description	Cat	Supplier's reply		
			Y	N	R
	Persons) and that his/her name matches the national identity number. Issuance shall either be by dispatch by post to a registered address or electronically on the basis of an existing authentication mechanism, providing the same level of confidence that the recipient is the correct person as a postal dispatch to the registered address.				
4.3.2	Protection of private keys The following requirements apply to the protection of private keys: <ul style="list-style-type: none"> • Access to private keys shall require authentication. • The user shall have scope for choosing/deciding whether the individual operation involving private keys is to be approved. • Private keys shall as a minimum be stored in encrypted form. 	A			
4.3.3	The lifetime of certificates The Supplier shall specify and give the reasons for the lifetime of keys and certificates. The minimum lifetime required is 13 months. (Temporary certificates with shorter lifetimes may be permissible.)	A			
4.3.4	Mobility / standard storage The solution should ensure that the certificate-holder is able to move the certificate and keys between various systems/work stations in a flexible, straightforward and secure way. The Supplier should describe the way in which this mobility is achieved. Storage of keys as encrypted PKCS #12 [g] objects should be permitted.	B			

4.4 Enterprise certificates

Issuance is based on personal attendance by a person holding an authorisation. The certificate shall contain the organisation number of the enterprise.

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
4.4.1	Unique identification of the enterprise Unique identification of an enterprise shall be permitted. This shall be safeguarded by ensuring that the Supplier releases keys and certificates only to authorised representatives of the Client (authorisation from an authorised signatory of the company) and that the certificate is equipped with the organisation number of the enterprise as issued by the Central Coordinating Register for	A			

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
	Legal Entities (Enhetsregisteret) in accordance with "Recommended certificate profiles for person certificates and enterprise certificates" [10].				
4.4.2	Protection of private keys The following requirements apply to the protection of private keys: <ul style="list-style-type: none"> • Access control to private keys shall be permitted. • The enterprise itself shall have scope for choosing/deciding whether the individual operation involving private keys is to be approved. • Private keys shall as a minimum be stored in encrypted form. 	A			
4.4.3	Linkage to an individual enterprise Use of the private key belonging to this certificate shall be restricted to the correct enterprise. The Supplier shall ensure that access to private keys is subject to very strict controls and that the holder has access to efficient methods of revoking the certificate.	A			
4.4.4	The lifetime of certificates The Supplier shall specify and give the reasons for the lifetime of keys and certificates. The minimum lifetime required is 13 months. (Temporary certificates with shorter lifetimes may be permissible.)	A			
4.4.5	Mobility / standard storage The solution should ensure that the certificate-holder is able to move the certificate and keys between various systems/service in a flexible, straightforward and secure way. The Supplier should describe the way in which this mobility is achieved. Storage of keys as encrypted PKCS #12 [g] objects should be permitted.	C			

5. REQUIREMENTS APPLICABLE TO DIRECTORY AND LOOKUP SERVICES

5.1 Certificate repositories and revocation lists

Use of the PKI services is dependent on a number of information services. Of particular importance are directory services to provide access to certificates and revocation services to revoke certificates that have become invalid as a consequence of the compromise of a private key or for other reasons.

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

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

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
5.1.1	Directory service for certificates The Supplier shall offer a directory service for accessing encryption certificates.	A			
5.1.1.1	Limiting access The directory service shall support access control to allow access to certain types of information to be restricted to authorised users.	A			
5.1.1.2	Directory services via LDAP Directory services shall be offered via LDAP v.3 ⁷ . Specify the software used. If applicable, specify other software interfaces.	A			
5.1.1.3	Directory searches The directory service shall return a reply within maximum 1 second per search (irrespective of loading) (the measurement point is the interface with the public network).	A			
5.1.2	Revocation service When certificates are revoked, the information shall be made available without undue delay via the OCSP service and, if applicable, via CRL in accordance with X.509 [i].	A			
5.1.2.1	Revocation lists Information on revoked certificates shall be made available without unaccounted delay, but no later than one hour after the Supplier became aware of the situation. The CRL Distribution Point attribute of the certificate shall point to the revocation list. CRLs should be in accordance with RFC 3280 [j].	C			
5.1.2.2	OCSP service When certificates are revoked, the information shall be made available without unaccounted delay via an OCSP service as defined in RFC 2560 [k]. The AuthorityInfoAccess field of this certificate shall point to the OCSP service.	A			
5.1.2.3	The performance of the revocation services Searches in the revocation service shall generate replies within 1 second (irrespective of workload) (the measurement point is the interface with the public network).	A			
5.1.3	The availability of the services The Supplier shall ensure that information services, directory services and the receipt of revocations are available 24 hours a day every day of the year. Describe how a short waiting time between the receipt of a revocation notice and publication via the revocation service is achieved.	A			
5.1.3.1	Uptime On average, over the course of the year, the availability of the directory and revocation services shall be 99.95%. The maximum permitted continuous downtime is 1 hour. The Supplier shall document how uptime is measured and maintained.	A			

⁷ Or newer version when these become generally used in the market.

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
5.1.3.2	Planned downtime Planned updates, revisions or maintenance of the service by the Supplier shall be agreed with the Client within reasonable time before the work commences. Such work should preferably be conducted 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 involve agreed downtime. Planned downtime shall not involve 3 hours per calendar month.	A			
5.1.4	Operating information Operating information of significance to the Client, such as planned downtime, faults etc. shall be available on a dedicated website. The website shall be available to the Client. The Supplier shall also offer a notification service that gives notice of such events.	A			
5.1.5	The availability of stored certificate information and the required period of storage The Supplier of Person-High shall store all relevant information pertaining to the certificate in accordance with the requirements in Section 14 of the Act on Electronic Signatures (e-signaturloven) [2] and fulfil the requirements relating to the cessation of business provided for in Section 3 of the Regulations on requirements applicable to issuers of qualified certificates (Forskrift om krav til utsteder av kvalifiserte sertifikater) [4]. The above requirements, including the 10-year storage requirement, shall as far as applicable also apply to the Supplier of Enterprise Certificates, with the exceptions of the requirements in Section 14 second paragraph, letter b of the Act on Electronic Signatures (e-signaturloven) [2] and to the Supplier of Person-Standard. Certificates and revocation lists shall be made publicly available in a practical and expedient way. The Supplier shall describe how these requirements will be fulfilled from time to time, including in the event of the cessation of the business.	A			
5.1.6	Adaptation of directory solutions The solutions shall be adaptable for use by Clients that do not have online access to directory services.	A			
5.1.7	Linkage to organisation numbers In the case of Enterprise Certificates, details shall be provided of how searches in the directory will show the linkage between certificate and organisation number.	A			

5.2 Linkage to national identity number

In many contexts, public sector agencies need secure access to national identity numbers. At the same time, the Personal Data Act (personopplysningsloven) [6] contains specific rules on the use of such numbers.

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
5.2.1	Look-up services for national identity numbers The Supplier shall offer a lookup service permitting authorised parties to link a certificate to a national identity number. The service shall be in accordance with “Interfaces for access to lookup services” [12] and the release of national identity numbers shall be in compliance with Section 12 of the Personal Data Act, [6] and Section 9-2 of the Personal Data Regulations (personopplysningsforskriften) [7]. A description of the service shall be provided.	A			

6. REQUIREMENTS APPLICABLE TO THE RA SERVICE

The design of the RA service and the issuance procedure shall be described from the perspective of certificate classes and user needs.

The Supplier shall offer both a centralised and a delegated (local) RA services and issuance procedures and describe how these can be adapted to the needs of the Client.

6.1 Person certificates in certificate class High

The Supplier shall provide an RA service suitable for the registration of relevant information. On behalf of the certificate issuer, the RA service may also verify information on the party ordering the certificate and secure the quality of the information that will be entered in the certificates. The RA service shall be organised in compliance with the provisions of the Act on Electronic Signatures (e-signaturloven) [2] and the Regulations to the Act (Forskrift om krav til utsteder av kvalifiserte sertifikater) [4]. It is essential that all and any contact with the Client requiring a physical presence can be performed in adequate geographical proximity to the user, so that the process involved in acquiring the certificate is not viewed as a barrier to use of the solution.

Requirement No.	Description	Cat	Supplier's reply.		
			Y	N	R
6.1.1	Documentation of the RA-service The following features of the RA-service shall as a minimum be described: <ul style="list-style-type: none"> • Where and how key pairs are generated, distributed and installed • How certificate applications are registered, including the way in which personal data are checked and how consent is obtained for publication of the certificate in accordance 	A			

Requirement No.	Description	Cat	Supplier's reply.		
			Y	N	R
	<p>with Section 14 second paragraph, letter a of the Act on Electronic Signatures (e-signaturloven) [2]</p> <ul style="list-style-type: none"> • The procedure for issuing certificates, including where and how the certificate is delivered to the certificate applicant, cf. Section 13 of the Act on Electronic Signatures (e-signaturloven) [2] and Section 7 of the Regulations to the Act (Forskrift om krav til utsteder av kvalifiserte sertifikater) [4] • The technical structure of the RA-function • Delivery times • The geographical location of the RA-service and how the necessary contact with the Client/certificate holder is safeguarded 				
6.1.2	<p>Organisation of the RA-service The RA-service shall be organised in accordance with the requirements in the Act on Electronic Signatures (e-signaturloven) [2] and its Regulations (Forskrift om krav til utsteder av kvalifiserte sertifikater) [4] and ETSI TS 101 456 [b].</p>	A			
6.1.3	<p>Geographical proximity Personal attendance shall be possible within adequate geographical proximity of the users, preferably within the municipal boundary.</p>	A			
6.1.4	<p>Local RA and the issuance process The Supplier shall offer an RA and issuance process that enables the Client or a third party nominated by the Client to function as a local RA.</p>	A			
6.1.5	<p>Documentation of local RA The Supplier shall describe the contract structure, liabilities and technical structure involved in implementing local RA offices. This shall include requirements relating to procedures, physical security, personnel etc. Descriptions shall also be provided of:</p> <ul style="list-style-type: none"> • How LRA-services can be established, the resources required, cooperation etc. • Procedures for issuance, cf Section 13 of the Act on Electronic Signatures (e-signaturloven) [2] and Section 7 of the accompanying Regulations (Forskrift om krav til utsteder av kvalifiserte sertifikater) [4] • How communication between LRA and CA will be conducted, standards and security mechanisms. 	A			
6.1.6	<p>Training LRA administrators The Supplier shall offer the necessary training of LRA administrators</p>	A			

6.2 Person certificates in certificate class Standard

Standard person certificates do not require personal attendance and issuance can accordingly be based on other mechanisms in order to ensure that the certificate is issued to the correct person. This could be based on existing customer relationships with recipients, forwarding by the issuer to addresses registered in the DSP (Norwegian Central Register of Persons), sending activation data to cell phones and other methods that the Supplier considers suitable for safeguarding the issuance process.

Requirement No.	Description	Cat	Supplier's reply.		
			J	N	R
6.2.1	Documentation of the RA-service As a minimum, the following aspects of the RA shall be described: <ul style="list-style-type: none"> • How the necessary contact with the Client/certificate holder is safeguarded • How and where key pairs are generated, distributed and installed • Procedures for issuing certificates, including where and how certificates are delivered to certificate applicants • The technical structure of the RA function • Delivery times • Methods of issuance, checking against registers and storing registration information 	A			
6.2.2	Organisation of the RA-service The RA-service shall be organised in accordance with the LCP requirements provided for in ETSI TS 102 042 [c].	A			
6.2.3	Electronic registration and distribution The Supplier shall specify whether the Supplier is able to offer an RA-service based on the re-use of the Client's existing authentication solutions, and if so, how.	A			

6.3 Enterprise certificates

The dissemination process for first-time issuance is based on personal attendance by a person equipped with the appropriate authorisation.

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
6.3.1	Documentation of the RA-service As a minimum, the following aspects of the RA service shall be described: <ul style="list-style-type: none"> • How the necessary contact with certificate applicants / holders is safeguarded (ref 6.1.1 og 6.2.1) • How and where key pairs are generated, distributed and installed • Procedures for issuing certificates, including where and 	A			

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
	<p>how certificates are issued to certificate applicants and how the recipient's authorisation to receive the certificate is checked</p> <ul style="list-style-type: none"> • The technical structure of the RA function • Delivery times 				
6.3.2	<p>Organisation of the RA-service The RA-service shall be organised in accordance with the NCP requirements provided for in ETSI TS 102 042 [c].</p>	A			
6.3.3	<p>Local RA and the issuance process The Supplier should offer an RA and issuance process that enables the Client or a third party nominated by the Client to function as a local RA.</p>	C			
6.3.3.1	<p>Documentation of local RA The Supplier shall describe the contract structure, liabilities and technical structure involved in implementing local RA offices. This shall include requirements relating to procedures, physical security, personnel etc. Descriptions shall also be provided of:</p> <ul style="list-style-type: none"> • How LRA-services can be established, the resources required, cooperation etc. • Procedures for issuance, cf. Section 13 of the Act on Electronic Signatures (e-signaturloven) [2] and Section 7 of the accompanying Regulations (Forskrift om krav til utsteder av kvalifiserte sertifikater) [4] • How communication between LRA and CA will be conducted, standards and security mechanisms 	A			
6.3.3.2	<p>Training LRA administrators The Supplier shall offer the necessary training of LRA administrators</p>	A			

7. REQUIREMENTS APPLICABLE TO THE SIGNATURE CREATION SYSTEM

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
7.1	<p>Requirements as to signature validation systems The Supplier shall document whether the solutions for presenting and verifying signed data comply with the requirements in CWA 14171 [n], including whether the solution is able to:</p> <ul style="list-style-type: none"> • Present the document as it was shown at the time of signing • Notify the user of any dynamic content in the document⁸ 	A			

⁸ Dynamic content means for example macros and active links.

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
	<ul style="list-style-type: none"> Clearly display the status of signature verification Ensure that data used to verify the signature accords 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 				
7.2	<p>Requirements as to the signature creation application</p> <p>If the Supplier supplies a signature service, documentation shall be provided of whether the solution complies with the requirements and recommendations in CWA 14170 [m]. Comments shall be provided to each of points 1-17 in Annex A, A1.</p> <p>In addition, the following points from CWA 14170 [m] shall be documented:</p> <ul style="list-style-type: none"> 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 and the way in which integrity, confidentiality and completeness are safeguarded shall be specified (see. Section 7.3). Describe how the security requirements made of the authentication system in Section 11.8 are 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 Supplier supplies a dedicated module for presenting the signer's document/data, or delivers software for analysing the signer's document/data 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. Describe the warnings that are given if the document contains hidden codes (e.g. macros) or if not all parts of the document can be shown. If the system offers the user the option of choosing how often authentication must take place in relation to the actual process of signature, this shall be described. Specify whether the system features any form of timeout reactions (asks for a password/PIN code) after the user has been inactive for a certain period of time. Describe any logging on necessary in connection with signing. 	A			

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
7.3	<p>Requirements as to signature creation devices</p> <p>The Supplier should specify the ways in which the solution complies with, and, if applicable, deviates from the requirements and recommendations of CWA 14169 [1]. The consequences of these deviations shall be stated.</p> <p>In addition, the Supplier shall document whether signature creation data used to generate signatures have sufficient safeguards.</p>	C			

8. REQUIREMENTS APPLICABLE TO THE USER ENVIRONMENT

8.1 Quality of use

The following requirements apply if the solution includes user dialogues:

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
8.1.1	<p>Language</p> <p>All user dialogues shall be available in the Norwegian language.</p>	A			
8.1.2	<p>Help text</p> <p>Help text shall be available or installable in Norwegian in connection with all user dialogues.</p>	A			
8.1.3	<p>Instructions for use</p> <p>Instructions for installation and use shall be available in Norwegian.</p>	A			
8.1.4	<p>Adaptation of user dialogues</p> <p>User dialogues in connection with signing should be adjustable, for example, to include a reference to the document that is being signed.</p>	C			
8.1.5	<p>Matching of graphic profile</p> <p>It should be possible to adapt the graphic profile of the authentication and signature dialogues to match the profile of the application</p>	C			
8.1.6	<p>Deliberate actions</p> <p>The user shall be given a clear warning that she is about to sign the document. The user shall have the option of terminating the signing process.</p>	A			
8.1.7	<p>"What You See Is What You Sign" (WYSIWYS)</p> <p>What the user sees shall match what she signs. The way in which this principle is satisfied shall be documented.</p>	A			
8.1.8	<p>Signature policy</p> <p>Documentation should be provided on how the solution handles various types of signature policy</p>	C			

8.2 Application integration

If the PKI solution is to be integrated in an application, the following requirements apply:

Requirement No.	Description	Cat	Supplier's Reply		
			Y	N	R
8.2.1	<p>Requirements as to the Integration Module</p> <p>An integration software module for integrating PKI functionality shall be available in the program environment of the application. A description shall be provided of the program environments and interfaces that are supported (e.g.NET, J2EE...).</p> <p>The integration package should support the interfaces and protocols necessitated by other requirements in this document. A specification shall be provided of the standard interfaces, formats and protocols that are supported, e.g.:</p> <ul style="list-style-type: none"> • PC-SC [h] and PKCS#15 [p] for handling smart cards • PKCS#12 [g] for importing and exporting locally stored private keys. Programming interfaces PKCS#11[o], Microsoft Crypto API, (MS CAPI), GSS-API and Java Crypto Extension • "XML Authentication", "XML Encryption" and SAML for securing Web Services and security protocols SSL/TLS. • Message formats such as S/MIME, PKCS#7, CMS, XML DSIG, ETSI TS 101 733, ETSI TS 101 903 and SEID's recommended signature format. 	A			
8.2.2	<p>Documentation</p> <p>Sufficient documentation shall be provided to allow a programmer with general expertise but no knowledge of the interface to utilise it.</p>	A			
8.2.3	<p>Example code</p> <p>Compilable example code shall be available showing the use of all functions in the programming language of the application..</p>	A			
8.2.4	<p>Licences</p> <p>The offer shall include all licences for the software interface and any other program licences required.</p>	A			

8.3 End user systems

End user system means the system used by the end user of the application.

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
8.3.1	<p>Platform independence</p> <p>The solution shall not tie the user to a single platform as regards for example operating system or web browser.</p>	A			
8.3.2	<p>Hardware</p> <ul style="list-style-type: none"> • The offer shall specify the hardware that the user may use. (PC, MAC, PDA...) • Any interfaces required shall be specified (USB v. n...) • Required hardware installation shall be described (card reader...) 	A			

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
8.3.3	Operating system The offer shall specify the operating systems that the end user may use. This shall include versions and support for "thin Clients". (Windows XP, Red Hat Linux, Citrixterminal server etc.) The solution shall as a minimum function on the three most commonly used operating systems for end-user environments (Windows, Linux and MAC).	A			
8.3.4	Web browsers The offer shall specify the web browsers that the end user may use. This shall include versions and support for "thin Clients" (Internet Explorer, Netscape operating under Citrix terminal servers etc.) The solution shall as a minimum function in the most commonly used browser applications for end-user environments.	A			
8.3.5	E-mail programs The offer shall specify the e-mail programs that the end user may use for signing and encrypting e-mail. This shall include version and support for "thin Clients". The offer shall also specify any ties to certificate formats or content.	A			
8.3.6	Other software and components The offer shall specify all and any software that will need to be installed. The offer shall specify requirements as to components that need to be activated in the Client. The need for particular system settings shall be specified.	A			
8.3.7	Adaptation to changes in the end user environment The offer shall describe the Supplier's procedures (including maximum upgrade time) for adapting to new program versions and improvements ("patches" etc) in the user environment.	A			

8.4 User support

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

Requirement No	Description	Cat	Supplier's reply		
			J	N	R
8.4.1	<p>Documentation of user support</p> <p>As a minimum the following aspects of the user support ("help desk") function shall be described:</p> <ul style="list-style-type: none"> • the service • the organisation of the service • the tasks solved as first line and second line tasks • whether enquiries concerning the revocation of certificates should 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 the Client gains 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 use. 	A			
8.4.2	<p>The operation of user support</p> <p>A user support function offering direct assistance in Norwegian to the Client shall be offered. The user support service shall also cover software and hardware supplied to the Client as part of the service. (This requirement applies to user support for certificate holders, application developers and operations.)</p>	A			
8.4.3	<p>Call-out service</p> <p>The Supplier should offer a call-out service in connection with the user support service. A specification should be provided of the areas to which the service applies and the applicable response time. (This requirements applies to user support for certificate holders, application developers and operations.)</p>	C			
8.4.4	<p>User support for application developers</p> <p>A user support scheme shall be offered for application developers using the program interface to integrate PKI functionality. This service shall be described.</p>	A			

8.5 Documentation

The Supplier shall specify and procure all information required in connection with the service. All documents acquired or compiled by the Supplier shall be stored by the Supplier, and shall be available for examination and inspection when requested by the Client.

The minimum requirements applicable to documentation provided by the Supplier are:

- Electronic documentation shall be provided in a format that is compatible with Microsoft Office no more recent than v. 2000 and Open Office.
- Unless otherwise specified, all documentation shall be in the Norwegian language.
- All system documentation and user documentation shall be drafted in accordance with a relevant standard. The Supplier shall specify which standard will be used.

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
8.5.1	Confirmation of qualified certificates The offer shall be accompanied by confirmation from the appropriate regulatory authority that the certificate issuer is able to issue qualified certificates, or by a copy of the registration notification to this same authority, or by evidence that such registration will take place before of the agreement is signed.	A			
8.5.2	Certificate policy for qualified certificates The offer shall be accompanied by the Supplier's certificate policy for qualified certificates	A			
8.5.3	Certificate policy for enterprise certificates The offer shall be accompanied by the Supplier's certificate policy for enterprise certificates/server certificates	A			
8.5.4	Certificate practice The offer shall contain the applicable certificate practices for the certificate policies offered, including certificate practice for the RA-service.	A			
8.5.5	Policy for cooperating with other CAs The Supplier's policy on interoperability agreements at both national and international level shall be stated, as a minimum in the form of the Supplier's policy for cooperating with other certificate issuers.	A			
8.5.6	Documentation of contingency planning The Supplier shall document contingency plans and procedures for emergency situations, including: <ul style="list-style-type: none"> • The maximum time for restoring the service • Back-up procedures 	A			
8.5.7	Documentation of procedurers for disaster situations The Supplier shall document contingency plans and procedures for disaster situations, including: <ul style="list-style-type: none"> • The maximum time for restoring the service • Back-up procedures 	A			
8.5.8	Configuration management and version control The procedures for configuration management and version control of documentation and software shall be described.	A			

8.6 Response times and availability

This chapter specifies the solutions and services relating to the creation of a digital signature. Delays and low availability in the Client's own equipment and the Internet are not encompassed by the requirements.

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
8.6.1	Response time Authentication and signing (including validation) shall take no more than three seconds (not including the time it takes the user to enter a PIN).	A			
8.6.2	The availability of the services The Supplier shall ensure that information services and directory services are available 24 hours a day every day of the year.	A			
8.6.2.1	Uptime Solutions for authentication and signing (incl. validation) shall have an uptime of 99.9 % on average over the course of the year. The Supplier shall document the way in which uptime is measured.	A			
8.6.2.2	Planned downtime Planned updates, revisions or maintenance of the service by the Supplier shall be agreed with the Client within reasonable time before the work commences. Such work should preferably be conducted 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 require agreed downtime.	A			

9. REQUIREMENTS APPLICABLE TO COMMERCIAL AND TECHNICAL INTEROPERABILITY

Interoperability between CAs is to be understood in the following context:

Interoperability entails that a certificate recipient (e.g. a user site) wishing to validate a certificate/signature and needing to use certificates from several different issuers shall be able to do so with the aid of solutions that are as expedient as possible for all parties involved.⁹

Solutions in this context will entail technical interoperability between the systems of various suppliers and with the systems implemented by a user site, both internally and, if applicable, with end users. Moreover, this entails commercial relationships (agreements) between suppliers and user sites, and between suppliers.

Interoperability will be expected between the suppliers of certificate services used by the public sector, in communications with users and internally. Suppliers shall fulfil the requirements provided for in this specification. Applicable suppliers will either conclude a joint framework agreement with the public sector or be approved for communications with the public sector. In the event of renewals of or announcements of new tenders for the applicable framework agreements or new approvals, new players in the market will have to fulfil the

⁹ This definition is taken from the SEID Project document "External summary of the SEID workshop May 2004".

interoperability requirements. Existing suppliers with operational solutions for interoperability will then be expected to make the appropriate arrangements to accommodate this.

The general intentions of the commercial and technical interoperability requirements are:

- The individual certificate holder should have to relate to as few solutions as possible.
- Applications utilising PKI-functionality should have to interact with the minimum number of software modules possible. There should primarily be one single interface: with the PKI supplier with which the user site has an agreement.
- The user site should preferably have a single contract partner only.
- Competition in the market shall be stimulated.

The following comments apply to the term “expedient solutions” (see the definition of interoperability above) for interoperability with the public sector:

- **Simplicity:**
 - The certificate holder shall have to relate to a maximum of one solution per security level.
 - The user site shall have to interact with no more than one integration package.
- **Cost effectiveness:**
 - It shall be more beneficial in financial terms for the user site to have an interoperability solution than to have individual deliveries from two or more suppliers.
 - Cost levels shall be predictable.
- **Justifiable in commercial terms.**
 - The certificate holder should have to relate to no more than one contract partner (per security level)
 - The user site should have to interact with no more than one contract partner.
 - Factors relating to liability, responsibility, rights and obligations on the part of the contract parties in question shall as a minimum be equally well safeguarded with an interoperability solution as with individual agreements.

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
9.1	<p>Willingness to secure interoperability with other contract partners</p> <p>The Supplier shall be prepared to contribute solutions that will secure interoperability with all suppliers delivering solutions based on this requirements specification. This will as a minimum entail that:</p> <ul style="list-style-type: none"> • The application using PKI for authentication and signature needs to use no more than a single Integration Module. • It is possible to search, validate and utilise certificates issued by several CAs by means of this one Integration Module. • It is possible to validate signatures based on certificates from several CAs with the aid of this one Integration Module. • A single agreement can be established to regulate responsibilities and financial factors. 	A			

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
	The Supplier shall describe how this might be resolved.				
9.2	Documentation of the interoperability solution Documentation shall be provided of the way in which the Supplier intends to offer an interoperability solution in which the application uses a single Integration Module and the user site has a single contract counterparty (e.g. in accordance with "External summary of the SEID workshop May 2004" [11], reference model A2 or C1). The documentation shall include a progress plan for implementation.	A			
9.3	Support for technical and commercial interoperability The solution should support interoperability with other suppliers of solutions based on this requirements specification where the application utilises a single Integration Module and the user site has a single contract counterparty (e.g. in accordance with [11], reference model A2 or C1).	C			
9.4	Client interoperability <ul style="list-style-type: none"> • Certificates should be available for running "Microsoft Certificate Store". • Operations with private keys should be available for applications using Microsoft CRYPTOAPI or PKCS#11 [o]. • S/MIME format shall be used for encrypting e-mail. • The solution should support SSL Client certificates. 	C			
9.5	Signature format Generated signatures shall be in accordance with PKCS#7 [f] format, CMS RFC 2797 [q], ETSI TS 101 733 [d] or ETSI TS 101 903 [e].	A			
9.5.1	SEID Task 3 Generated signatures should follow the recommendations of the SEID Committee in "Task 3".	C			
9.6	Directory for certificate validation services Searches in the directory should support OCSP or LDAP v.3 ¹⁰ . Directory searches should be available over the Internet.	A			

10. OPTIONS

10.1 Time stamping

A time stamping service that will certify the exact time of a transaction is a prerequisite for solutions that are dependent upon "strong" non-repudiation.

¹⁰ Or newer versions when these are in general use in the market.

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
10.1.1	Time stamping Time stamping of signature time and certificate validation shall be available for presentation as evidence in the event of a dispute. A description shall be provided of the time stamp stored in or together with the signature and the signed data.	O			
10.1.2	Accuracy All clocks in the system shall be synchronised based on the time given by the Norwegian Metrology Service's (Justervesenet) atomic clock or offer the equivalent degree of accuracy.	O			

10.2 Notarisation

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
10.2.1	Notary service <ul style="list-style-type: none"> • The solution shall function as an independent notary in the event of any future non-repudiation dispute. • Scope shall be offered for signatures to be received and stored and searches of signatures shall be permitted. • Documentation shall be provided of how the correct time is secured. • Documentation shall be provided of how logs are protected against change. • Documentation shall be provided of how signatures are verified against data in signatures. • Documentation shall be provided of how verifiable checks of revocation lists are performed. • Documentation shall be provided of the way in which revocation lists and certificates are stored over the long term. • Documentation shall be provided of the procedures in place to safeguard against data loss. 	O			

10.3 Long-term storage beyond 10 years

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
10.3.1	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.	O			
10.3.2	Long-term storage of results The results of signature verifications and the procedures for signature verification shall be available for 30 years.	O			
10.3.3	Long-term storage beyond 30 years The option of concluding an agreement on storage in excess of 30 years shall be offered.	O			

10.4 High level of availability

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
10.4.1	High level of availability Solutions for authentication and signing (including validation) shall have an uptime of 99.995 % on average over the course of a year.	O			

10.5 Security portal

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
10.5.1	Authentication An Identity Provider in accordance with the Liberty Alliance ¹¹ specifications shall be offered. The solution shall be described. Details shall be provided of the versions and general functions for which support is provided.	O			

10.6 Qualified signatures

The Client will not at the present time require solutions capable of presenting qualified signatures. Nevertheless it is a requirement that the Supplier should be capable at some given point in time of converting the systems to permit the use of qualified signatures.

¹¹ Ref <http://www.projectliberty.org>

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
10.6.1	Secure signature creation system The solution shall be capable of meeting the requirements applicable to secure signature creation, see CWA 14169 [I]. The Supplier shall give a binding date for when use of such a system can commence.	O			
10.6.2	Requirements as to the approved signature creation system A self-declaration or approval from some other signatory of the EEA Agreement shall be furnished.	O			

10.7 Solution for internal use within public sector agencies

The Supplier of a solution for professional use shall offer a solution based on certificates of the type "Person-High". It is intended that the solution should be used internally within enterprises/offices for amongst other purposes logging on to secure e-mail systems and for personal signature/authentication integrated in the internal systems of the agencies. In addition to the general certificate-related requirements, the following requirements also apply:

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
10.7.1	Protection of private key Private keys shall be stored on smart cards that can be used in a reader that supports PC-SC [h].	O			
10.7.2	Local issuance procedure The Supplier should offer an issuance procedure in which the Client handles the registration of user information, card issuance, if applicable design of card surfaces and other aspects of the issuance process in a way that safeguards compliance with the security requirements applicable to the "Person-High" class.	O			
10.7.3	Standby solutions The Supplier should have standby solutions in place for handling situations in which the user has for example left his or her card at home or needs to work without access to his or her own card.	O			
10.7.4	Requirements as to system integration <ul style="list-style-type: none"> • Certificates shall be available for applications that use "Microsoft Certificate Store". • Operations with private keys shall be available to applications using Microsoft CRYPTOAPI or PKCS#11. • The use of the certificate for logging on via MS Windows SmartCard logon shall be supported. 	O			
10.7.5	Requirements as to keys Asymmetric keys shall be based on RSA with a minimum length of 1024 bits.	O			
10.7.6	Certificate types	O			

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
	The Supplier shall offer a minimum of two key pairs with associated certificates. The purpose of the key pairs shall be apparent from the "keyUsage" field.				

10.8 Hardware-based solutions for enterprise certificates

Requirement No.	Description	Cat	Supplier's reply		
			Y	N	R
10.8.1	Protection of private key Private keys shall never appear in plain text in registers that might be compromised or in other ways provide the basis for unauthorised use.	O			

11. APPENDIX 1 SECURITY LEVELS

Security levels for use of PKI in communications with or within the public administration

Introduction

This document has been drawn up by the Working Group for a Common Specification of Requirements for PKI in the Public Sector.

The document will form the basis for a detailed requirements specification, if necessary comprising several parts, describing the requirements applicable to services and products purchased under one or more framework agreements concluded on behalf of the public sector, including local authorities.

At present, there is a high degree of confidence on the part of the general public that public sector agencies prevent information about individual citizens from falling into the hands of unauthorised third parties. This high level of trust shall not be diminished in the transition to electronic services. It is therefore important to establish the levels of security that need to be applied to information of various types in order to ensure that the protection of confidential information is not compromised with the transition to paperless government.

The security levels defined here will form the core of the public sector's use of PKI solutions for electronic ID, electronic signature and for securing the confidentiality of non-classified information. This proposal for coordinating security levels is based on the assumption that users of electronic services provided by the public sector will wish to utilise a wide variety of security solutions, including many different types of PKI, relating to various types of services.

Nevertheless, this does not mean that public sector agencies should refrain from conducting their own independent assessments of the risks and vulnerabilities associated with the use of PKI in their electronic services, as required in the applicable statutes and regulations. However, limiting the range of security levels and the associated requirements will serve to simplify these assessments and the ensuing implementation processes.

The objective

Security levels have been defined in the past in a generic way, including in Norwegian Official Report 2001:10 Without Pen and Ink. The purpose of this document is to define security levels in greater detail to ensure that they safeguard:

- The needs defined by public sector agencies, represented by the Working Group.
- The products and services available.
- Good overall solutions for use in the interplay between the PKI solution and user applications.
- Maximum simplicity. Simpler choices for public sector agencies and less complexity for the user.

The work on security levels has been based on:

- **An assessment of the internal and external communication needs of the public sector; the various types of communication situations that exist; formal requirements in statutes and regulations and other regulatory provisions.**
- **At the same time it is essential to ensure that the requirements specification does not make demands that suppliers will have difficulty in meeting in a cost-effective way.**

One clear objective is that there should be as few security levels as possible in order to minimise the complexity for users of dealing with security solutions. On the other hand, the security levels shall provide public sector agencies with solutions with an adequate trust level.

Each level is defined by a set of criteria encompassing

- Requirements applicable to procedures for registration and for issuing certificates and distributing private keys.
- Certificate profiles / contents, including use of names and linkage to unique identification.
- Requirements applicable to the protection and use of private keys.

Examples of general areas of application for the individual security level are provided by way of guidance.

The use of common security solutions poses a new type of threat

At present, public services utilise a variety of user authentication methods. The choices made by the individual service are based on practical considerations relating to administration and finance and an assessment of risk. A security mechanism that applies not just to one but to many public services is encompassed by a different set of risks. The consequences of abusing a security solution that is adequate for one service will be far greater if the same mechanism is used by several services. The security levels outlined here attempt to provide safeguards in this regard.

Identification of individuals

According to Norwegian Official Report 2001:19 Without Pen and Ink "during the course of their work many public administration agencies need to gain access to the correct name and national identity number of individuals as recorded in the Population Register".¹² A personal certificate concept for use by the public sector should therefore allow a link to a national identity number. As provided for in the SEID Project's certificate profiles it is not advisable for national identity numbers to be recorded directly in the certificate, rather it "should have a unique link to the certificate-holder's 11 digit national identity number/D-number as registered in the Norwegian Central Register of Persons". For a further discussion of the regulations governing the use of national identity numbers in certificates, please see the report entitled "Legal framework for digital signatures and PKI - an outline and discussion of the problems by the PKI forum's legal group" Chapter 3.5.5.¹³

¹² Norwegian Official Report 2001:10 Without pen and ink, Chapter 12.1.3.

¹³ [http://www.handel.no/FileArchive/181/Jussgruppa-rapport-juni-2003\[1\].pdf](http://www.handel.no/FileArchive/181/Jussgruppa-rapport-juni-2003[1].pdf)

Security levels for PKI

Two security levels for person certificates have been defined: "*Person-High*" and "*Person-Standard*". Both of these shall fulfil the requirements applicable to advanced electronic signatures as defined in Section 3 point 2 of the Act on Electronic Signatures (e-signatur-loven) [2].

- "*Person-High*" is a security level for use where the administration needs a high degree of certainty with regard to the identity of the person with whom communications are being conducted.
- "*Person-Standard*" is a security level for use where the administration has a need for a reasonable degree of certainty with regard to the identity of the person with whom communications are being conducted.

Stricter security requirements as to identification may be defined in the future if solutions offering qualified electronic signature become available on the market and the administration determines that a need exists for such stricter security levels.

The confidentiality of information in electronic transfers will be secured by other solutions, not covered by specification, and which may be the same for both security levels. The difference between the security levels lies in the degree of confidence that the transferred information will be received by the correct recipient. In the case of access to stored information there will be differences in the level of certainty that access has been gained by the correct identity.

A security level for enterprises is also suggested, referred to as "*Enterprise*". This is a level of security applicable to enterprises with a need to authenticate, sign and/or encrypt decisions, sign outgoing e-mail or other types of documents and receive encrypted e-mail or documents.

A requirement common to all three levels is that the structure and content of certificates should comply with "Recommended certificate profiles for person certificates and enterprise certificates" as defined by the SEID Project, wherever relevant (see Table A).

Person-High

The "*Person-High*" level is a qualified person certificate. Accordingly, issuance is based on personal attendance. The certificate shall permit linkage with a national identity number and the registration of the person in the DSP (Norwegian Central Register of Persons) shall be verified.

"*Person-High*" permits various solutions for storing and protecting private keys. The requirements as to key storage at this level have been the subject of extensive discussion and the goal throughout has been to formulate requirements that are technologically neutral. The Group has arrived at the following requirements:

1. Access to private keys shall require a minimum of two-factor authentication, where one of the factors is something in the physical possession of the user (i.e. cannot be copied electronically).
2. The user shall approve each operation involving private keys by authenticating himself/herself.

3. Private keys shall never appear in plain text in registers that might be compromised¹⁴ or in other ways provide a basis for unauthorised use.

Person-Standard

The "*Person-Standard*" level is a person certificate which may be issued without the personal attendance of the certificate applicant. Certificates may be distributed by post to the registered address¹⁵ of the recipient. Certificates may also be issued electronically, provided that the user already has some other security solution in place that permits authentication. The prerequisite for this is that the security solution shall offer at least the same degree of certainty that the certificate will reach the correct recipient as does forwarding by post to a registered address. The certificate shall permit linkage to a national identity number and the registration of the person in the DSP (Norwegian Central Register of Persons) shall be verified.

"*Person-Standard*" entails the following requirements as to the protection of private keys:

1. Access to private keys shall require authentication..
2. The person shall have scope for choosing/deciding him/herself whether each operation involving private keys is to be approved.
3. Private keys shall as a minimum be stored in encrypted form.

Enterprise

"*Enterprise*" recommends a standard security level for certificates for enterprises. Issuance is based on personal attendance by a person with authorisation from the authorised signatory of the enterprise as recorded in the Register of Business Enterprises (Foretaksregisteret) or the Central Coordinating Register for Legal Entities (Enhetsregisteret). To enable unique identification of the enterprise the certificate shall contain the organisation number of the enterprise as recorded in the Central Coordinating Register for Legal Entities. Keys and associated access codes/passwords and certificate shall be released only to a person authorised to receive them on behalf of the enterprise (authorisation from an authorised signatory of the company). Documentation to this effect shall be submitted if necessary.

"*Enterprise*" imposes the following requirements as to the protection of private keys:

1. Access control to private keys shall be realisable.
2. The enterprise shall have scope for choosing/deciding whether the individual operation involving private keys is to be approved.
3. Private keys shall as a minimum be stored in encrypted form.

Re point 1: A need may exist for enterprise certificates to be used both by persons and by systems within the enterprise. The mechanism for access control shall accordingly be adapted to the type of use required in the individual case.

¹⁴ I.e. the keys must be satisfactorily secured against known threats, including malware and attacks against the keys during use.

¹⁵ Address registered in the DSP (Norwegian Central Register of Persons)

A) Description of the levels

SECURITY LEVELS	Registration and release procedure	Requirements as to name structure and content	Requirements as to protection of private keys
"Person-High"	<p>The certificate must be a qualified certificate and the certificate issuer must fulfil the registration and release procedures that follow from this, including the requirement as to personal attendance.</p>	<p>The name structure and certificate content must follow the requirements in Section 4 of the Act on Electronic Signatures (e-signaturloven) [2] with the clarifications that follow from "Recommended certificate profiles for person certificates and enterprise certificates" [10].</p>	<ul style="list-style-type: none"> • Access to private keys must as a minimum require two-factor authentication, where one of the factors is something in the physical possession of the user (i.e. cannot be copied electronically). • The user must approve each operation involving private keys by authenticating him/herself • Private keys must never appear in plain text in registers that might be compromised or in other ways provide a basis for unauthorised use.
"Person-Standard"	<p>The certificate issuer must fulfil the requirements in Sections 10 to 16 of the Act on Electronic Signatures (e-signaturloven) [2] and Section 3 of the Regulations on requirements as to issuers of qualified certificates etc. (Forskrift om krav til utsteder av kvalifiserte sertifikater) [4].</p> <p>Verification must take place upon registration that the person is found in a Norwegian population register and that the name of the person accords with his or her national identity number.</p> <p>A reasonable degree of security must exist that keys and/or associated access codes/passwords and certificates are released to the correct person.</p> <p>Release must either be by postal dispatch to the registered address or electronically based on existing authentication mechanisms to provide the same degree of security of correct receipt as post to the registered address.</p>	<p>The certificate must fulfil the requirements as to qualified certificates in Section 4 second paragraph letters b to j of the Act on Electronic Signatures (e-signaturloven) [2].</p> <p>In other respects the name structure and certificate content must follow "Recommend certificate profiles for person certificates and enterprise certificates" [10].</p>	<ul style="list-style-type: none"> • Access to private keys must require authentication • The user must have scope for choosing/deciding him/herself whether the individual operation involving private keys is to be approved. • Private keys must as a minimum be stored in encrypted form.

SECURITY LEVELS	Registration and release procedure	Requirements as to name structure and content	Requirements as to protection of private keys
"Enterprise"	<p>The certificate issuer must fulfil the requirements in Sections 3 and 7 of the Act on Electronic Signatures (e-signaturloven) [2] and Section 3 of the Regulations on requirements as to issuers of qualified certificates etc. (Forskrift om krav til utsteder av kvalifiserte sertifikater) [4].</p> <p>It must be possible to identify the enterprise uniquely 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].</p> <p>Safeguard must be in place to ensure that keys with associated access codes/ passwords and certificates are released to a person with the right to receive them on behalf of the enterprise. (Authorisation from an authorised signatory of the company.) Documentation of the relationship to be possible.</p>	<p>The certificate must fulfil the requirements as to qualified certificates in Section 4 second paragraph letters b to j of the Act on Electronic Signatures (e-signaturloven) [2].</p> <p>The name structure and certificate content must follow "Recommended certificate profiles for person certificates and enterprise certificates" [10]. The certificate must contain the organisation number of the enterprise.</p>	<ul style="list-style-type: none"> • Access control to private keys must be realisable. • The enterprise must have scope for choosing/deciding him/herself whether each operation involving private keys is to be approved. • Private keys must as a minimum be stored in encrypted form.

A2) Requirements contiguous to the security levels

In addition to the security levels, the secure use of certificates will hinge on a number of other factors. The way in which PKI is implemented in user software, the properties of the operating system, protective measures in place in and around the data processing equipment and the behaviour of users – these factors all impact upon security.

Accordingly, it is also necessary to impose requirements on the integration of PKI in software. Moreover, steps must be taken to ensure that the end user agreements - the agreement between the certificate issuer and the certificate holder - contain reasonable requirements as to the care that the user must exercise in connection with certificate usage.

B) Proposed areas of application for the security levels

This part of the document should be regarded as an advisory guideline on how to assess the security levels in relation to various types of threat associated with performing electronic transactions in the public sector. A number of specific examples have been provided where the various levels will meet the need for secure identification, non-repudiation and/or confidentiality. It is important to stress in this context that these examples focus only on how the security levels defined here might be used to cover one or more of the aforementioned security requirements in a given application. This does not rule out the possibility that other types of security measures might also be put in place, which in combination with the security levels provide the necessary security for the specific application in question.

The table below contains a general assessment of the need for both trust and security in electronic transactions and considers the possible consequences of breaches of such trust/security. The table is followed by a number of examples of uses where various aspects of the security requirement might be met by using the security levels proposed here.

USES FOR CERTIFICATE LEVELS	Authentication	Signature (non-repudiation)	Receipt of encrypted information
Person-High	Transactions where there is a need for a high degree of certainty about the identity of the originator, for example in connection with access to particularly sensitive information ¹⁶ or where the damage caused by compromising would be extensive.	Transactions where there is a need for a high degree of certainty about the connection between content and the identity of the originator or where the damage caused by the compromising of the connection is extensive.	Documents etc. containing particularly sensitive information or where the damage caused by a compromise would be extensive.
Person-Standard	Transactions where there is a need for a reasonable degree of certainty about the identity of the originator or where the damage caused by a compromise would be medium level.	Transactions where there is a need for a reasonable degree of certainty about the connection between content and the identity of the originator or where the damage caused by the compromising of the connection would be medium level	Documents etc. that do not contain particularly sensitive information and where the damage caused by a compromise would not be extensive.
Enterprise	Transactions where there is a need for a high degree of certainty that the originator is/represents a specified enterprise or where the damage caused by a compromise would be extensive.	Transactions where there is a need for a high degree of certainty about the connection between content and the specified enterprise or where the damage caused by the compromising of the connection would be extensive.	Documents etc. containing particularly sensitive information or where the damage caused by a compromise would be extensive.

Examples of uses that might be secured by means of certificates in the "Person-High" class include:

- Authentication of unknown users of web-based services providing access to documents and other material containing particularly sensitive information or subject to confidentiality or allowing such information to be altered. One example of this might be access to administrative decisions containing information of this nature. A second example might be gaining access to one's own health records held by a care provider or accessing social security case notes.
- Access to transactions in the Altinn Internet portal for public reporting categorised as level 4 or higher in Altinn's security documents.
- Signing agreements or financial transactions above a certain monetary level, for example State Education Loan Fund promissory notes.
- Applications to the State Education Loan Fund for payment relief or interest relief.
- Authenticating senders of electronic prescriptions, sick notes, medical certificates or applications for medicine refunds.
- Remote access to the internal systems of an enterprise where these systems process particularly sensitive information.

¹⁶ Particularly sensitive information means information that is sensitive in accordance with the Personal Data Act and/or is viewed as particularly sensitive in relation to some other regulations/guidelines. Includes enterprise information of a particularly sensitive nature.

- The encryption of transfers of particularly sensitive information. One example of this would be transfers of the medical records of patients from a hospital to municipal health care services.

Examples of uses that might be secured by means of certificate class "Person-Standard" might include:

- Authenticating unknown users of services such as the filing of tax returns or reports by business and industry not containing particularly sensitive information.
- Applications or other types of approach to public agencies requiring a reasonable level of certainty that the identity of the sender is correct.
- Access to administrative resolutions found on "appropriate information systems", see the e-Government Regulations, and not containing particularly sensitive information.
- Change of residential address (notification of change of address).¹⁷
- Secure e-mail (encrypted and authenticated), not containing particularly sensitive information.
- The filing of certain types of report with the police, for example of bicycle thefts and burglary.
- Access to transactions that may have financial consequences up to a certain level, for example the administration of account information on the payment of benefits (this may depend on the scope and need for assuring the quality of information using other sources).

Examples of uses that might be secured by means of certificate class "Enterprise" might include:

- Authentication in connection with access for searches or updates of common public registers, for example the National Population Register.
- Signing outgoing letters, decisions and other electronic communications in electronic form.
- Secure e-mail (encrypted and authenticated) between public sector agencies or between private enterprises and public sector agencies.
- Securing particularly sensitive information exchanged between public sector agencies and companies.
- Encrypting electronic transfers of particularly sensitive information such as medical records and discharge records. General communications using ebXML envelopes (the ebXML system has been implemented as a standard within the health sector and the Social Security Agency).
- Payments (where the transfer is authorized in advance of payment), orders. Access to services for which the agency is invoiced.

¹⁷ This assumes that the address/notification of change of address is not characterised as particularly sensitive information. This question is currently being reviewed by the Directorate of Taxes.

12. APPENDIX 2 ASSESSMENT OF THE REQUIREMENTS APPLICABLE TO SECURITY LEVELS FOR ELECTRONIC COMMUNICATIONS WITH THE PUBLIC ADMINISTRATION

By Thomas Myhr, The Norwegian Ministry of Trade and Industry

The general rule in Norwegian administrative law is that no formal requirements apply to initiating proceedings before an administrative agency.¹⁸ At the same time, however, particular acts and regulations contain specific formal and documentation requirements, one example being Section 32 of the Public Administration Act, which requires appeals against an administrative decision to be in writing and signed by the appellant or the appellant's representative.¹⁹

In communicating with the administration it is unlikely that a person will effect unauthorised dispositions in respect of an administrative agency on behalf of a third party, e.g. by filing an application for a place in a nursery school under someone else's name. Even were this to take place, the consequences would be limited, normally the administrative agency would spend time on unnecessary procedures and the person stated to be the applicant might receive requests for further information or receive a decision in the matter. In light of this risk level and of the limited consequences, it will be sufficient in this type of administrative practice to require "Person-Standard" for the purposes of identifying the person making contact with the administration. With a certificate of this level of security the administrative agency will be able to identify the sender to a reasonable degree of certainty and this will in most cases be sufficient.

On the other hand, certain aspects of a situation may entail that an administrative agency should or must require use of a higher level electronic signature, including "Person-High". In assessing whether this is the case, it will not be relevant to look to any formal requirements contained in statutes or regulations, at least not in isolation. It is, for example, not the case that the Public Administrations Act's requirements relating to the signature of an appeal against an administrative decision is a formal requirement aimed at the threat level that might be likely in relation to the use of electronic signatures. It is unlikely that anyone other than the appropriate party would complain/appeal against an administrative decision, and were this to happen the consequences would normally be limited. Nevertheless, the administrative agency will need to be able to check that the person appealing against the decision has the right to do so. This requirement will normally be covered by using a "Person-Standard", which would verify the identity of the sender to a reasonable degree of certainty. In considering whether "Person-High" should be required or not, it might be appropriate to look at the considerations underlying the formal and documentary requirements and assess the consequences of incorrectly identifying a person. Here evidentiary considerations in relation to financial values or issues of protection of privacy may form part of such an assessment, as might the question of whether the administrative decision is reversible in relation to the rights of the third party.

¹⁸ As a consequence of this principle Section 3 of the e-Government Regulations provides that unless specific requirements as to form or procedure apply to communications with an administrative agency, the administrative agency's general e-mail address may be used.

¹⁹ Appeals against individual decisions may be filed with the aid of electronic communications if the recipient administrative agency facilitates this, see Section 9 of the e-Government Regulations.

It should be noted however that even where "Person-Standard" is used, the need to encrypt the contents or to use other types of solution to prevent unauthorised access might be just as great as where "Person-High" is used.

The need to use a certain degree of asymmetry in relation to the use of security levels cannot be ruled out. Although it will be sufficient to use "Person-Standard" for filing an application, supplemented, if applicable, by solutions to prevent access by unauthorised third parties, it is by no means impossible that the information held by the administrative agency, even though based on information in an incoming application, may be such that the administrative agency will require use of "Person-High" in order to grant electronic access to this information.

As noted above, "Person-Standard" will provide the administrative agency with a reasonably high degree of certainty about the identity of the person performing the electronic transaction. What is important however is that the signature used (the solution) should secure the integrity of the electronic document. One cannot rule out the fact that a party may subsequently contend that for example an application that was received by the administrative agency does not correspond to the actual application that was filed, that it contains incorrect information or that it is incomplete. Uncertainties surrounding these issues may affect the procedure followed in the case as well as the decision adopted by the administrative agency.

13. APPENDIX 3 THE COMPOSITION OF THE WORKING GROUP AND THE REFERENCE GROUP

The working group

Chair	Ministry of Modernisation	Katarina de Brisis
Editor Security levels	Ministry of Modernisation	Lise Arneberg
Editor Requirements specification	Altinn administrative organisation	Pål Kristoffersen
	Ministry of Trade and Industry	Thomas Myhr
	The Brønnøysund Registers	Hilde Storvig (alternating with)
	The Brønnøysund Registers	Dorthe Kørner
	Directorate of Taxes	Arne Thorstensen (alternating with)
	Directorate of Taxes	Jan-Henrik Stubberud
	Directorate of Taxes	Anders Øksne
	State Education Loan Fund	Hans Petter Nyberg (alternating with)
	State Education Loan Fund	Ingrid Holen
	Norwegian Government Agency for Financial Management	Jan Bjørn Mortensen
	Statistics Norway	Magne Hopland
	Directorate of Health and Social Affairs	Arnstein Vestad (KITH)
	Courts Administration	Ole Martin Hole (alternating with)
	Courts Administration	Geir Trondrud
	Uninett /FEIDE	Jon Strømme
	Trondheim City Council	Anne Hofstad
	National Police Directorate	Eric Gonçalves
	Ministry of Modernisation	Kristian Bergem
	National Insurance Administration	Elisabeth Sunde
	Ministry of Modernisation	Sidsel Tønnessen

Reference group

Chair	National Insurance Administration	Odd Edvardsen
	Aetat Labour Directorate	Wilfred Østgulen
	National Insurance Administration	Svein Burkeland
	Norwegian Public Roads Administration	Annegret Andersen
	Norwegian Association for Local and Regional Authorities	Svein Erik Wilthil
	Oslo City Council	Anne Lise Beckstrøm
	Ministry of Defence, FLO/IKT	Bjørn Kringstad
	National Archives, Noark 5 Project	Ivar Fønnes (deputy: Trond Sirevåg)
	Ministry of Health and Care Services	Jon Georg Lund
	Government Administration Service	Geir Ivar Tunesvik (deputy: Ingar Dahl)
	Ministry of Foreign Affairs	Elisabeth Wemberg
	Directorate of Health and Social Affairs	Inger Elisabeth Kvaase

Observers

Data Inspectorate	Lars Martin Birkeland
Norwegian Post and Telecommunication Authority	Kari Anne Lang-Ree
Norwegian Competition Authority	Espen Sjøvoll

**14. APPENDIX 4 EXTERNAL SUMMARY OF THE SEID WORKSHOP ON
COMMERCIAL INTEROPERABILITY MAY 2004**

Attached as a separate file.

**15. APPENDIX 5 THE SEID PROJECT, PUBLICATION: TASK 1
"RECOMMENDED CERTIFICATE PROFILES FOR PERSON CERTIFICATES AND
ENTERPRISE CERTIFICATES"**

Attached as a separate file. Please refer to <http://www.handel.no/pkiforum/seid> for updated versions of the documents, where applicable.