
 Code of conduct for information security www.normen.no	Published with the support of: 
<h2>Requirements when using PKI for external communication</h2>	Supporting document Fact sheet no 49 Version: 1.1 Date: 15 Dec 2010

Target group This fact sheet is particularly relevant for:	<input checked="" type="checkbox"/> Supplier <input checked="" type="checkbox"/> ICT manager <input type="checkbox"/> Researcher <input type="checkbox"/> Project manager	<input checked="" type="checkbox"/> Head of security/Security coordinator <input checked="" type="checkbox"/> Organization manager/management <input type="checkbox"/> Person or body responsible for research	<input type="checkbox"/> Staff/employee <input checked="" type="checkbox"/> Data processor <input type="checkbox"/> Privacy protection ombudsman
Responsibility	The data controller is responsible for creating solutions and procedures for the use of PKI.		
Execution	Prior to, during, and when using PKI solutions for signing, authentication, and encryption for external communication.		
Purpose	Provide an overview of the requirements for the use of PKI in connection with the organization's external communication.		
Scope	Provide an overview of the requirements for the use of the certificate classes enterprise certificate and personal certificate (Person-High) for external communication.		
Authority	<ul style="list-style-type: none"> The Personal Data Regulations sections 2-11, 2-12, and 2-13. Section 4 of the Act relating to electronic signatures. 		
References	<ul style="list-style-type: none"> Code of conduct for information security (the Code), Chapter 5.2.1, 5.2.4, and 5.5.2 (www.normen.no) Specification of requirements for PKI in public administration (www.difi.no/artikkel/2010/04/kravspesifikasjon-for-pki) Framework for authentication and non-repudiation in electronic communication in and with the public sector (www.regjeringen.no/fad) KITH Report R16/06 Framework for electronic message exchange in the healthcare sector (www.kith.no) Fact sheet 16 - Creating a message communication solution Fact sheet 29 – Home office Fact sheet 20 – Security and partnership architecture Fact sheet 32 – Electronic patient and user communication 		

Introduction

PKI has a range of applications in the sector. The requirements concerning the use of PKI are described in a number of places, depending on the field of application. There are nevertheless some basic and general requirements that apply to all uses of PKI for external communication (including remote access, use of a home office, and wireless communication). This fact sheet provides an overview of these requirements. For specific uses of PKI please refer to the various fact sheets and documents referenced above.

No	Action
1.	Basic PKI requirements <ol style="list-style-type: none"> a) Prior to the acquisition of PKI solutions for the signing, encryption, or authentication for external communication the organization shall conduct a risk assessment of the solution in question. The risk assessment shall be conducted by the organization or by the organization's supplier b) According to the Code and the 'Framework for authentication and non-repudiation in electronic communication in and with the public sector' PKI solutions shall be implemented at security level 4 c) When performing risk assessment of PKI solutions the level of acceptable risk shall be equivalent to risk level 4 in the 'Framework for authentication and non-repudiation in

No	Action
	<p>electronic communication in and with the public sector'</p> <p>d) If the organization develops requirement specifications for implementing PKI, the deliverable must adhere to the 'Requirements specification for PKI in the public sector'</p>
2.	<p>Certificates – general information</p> <p>a) PKI entails that a neutral and trusted third party (TTP) issues a certificate. Issuers of qualified certificates to the sector must be registered with the Norwegian Post and Telecommunications Authority. For a list of certificate issuers registered in accordance with the self-declaration procedure, see http://www.npt.no</p> <p>b) 'Qualified certificate' means a certificate issued by an issuer registered with the Norwegian Post and Telecommunications Authority in accordance with a certificate policy that accords with Electronic Signature Act</p> <p>c) A qualified certificate is personal and serves as proof of identity confirming that a communication party is who he represents himself to be</p> <p>d) Prior to acquiring certificates and a technical solution for PKI the organization should clarify with its communication party which supplier is being used and if it is able make lookups in the supplier in question's catalogue (e.g. if PKI is to be used between organizations connected to the health net it is necessary to confirm with Norwegian Healthnet SF which certificate suppliers are supported)</p>
3.	<p>Certificate class: Person-High</p> <p>a) Is a personal certificate for a specific physical person who is uniquely identified by the certificate. Person-High is based on qualified certificates</p> <p>b) A sector PKI solution may include a smart card with additional personal information, e.g. a PIN or a fingerprint. The contents of the smart card combined with e.g. the owner's PIN or fingerprint constitute the individual's personal signature and proof of identity, and should be treated accordingly. A valid proof of identity is required in order to receive a smart card and/or PIN.</p>
4.	<p>Certificate class: Enterprise</p> <p>a) An enterprise certificate is issued to an organization registered in the Central Coordinating Register of Legal Entities (see www.brreg.no) and which is uniquely identified by the certificate by reference to the organization number in the Central Coordinating Register of Legal Entities</p> <p>b) The organization decides on the use of the enterprise certificate, e.g. if it will be used by a physical person authorized by the organization or by an automated process controlled by the organization, such as a server</p> <p>c) If necessary an organization may be issued with several enterprise certificates (e.g. solution for sending case summaries, access from home offices, etc.)</p>
5.	<p>Implementing procedures</p> <p>a) The organization must develop a procedure for updating its communication partners' and its own certificate when these expire</p> <p>b) The organization should develop a directive for employees issued with smart cards. The directive should include the following:</p> <ul style="list-style-type: none"> - The smart card should be considered a personal proof of identity and should be stored in a secure manner - Never let anyone borrow your smart card - Protect your personal PIN and never disclose it to others - Never write down your PIN in a manner that others may read - If the card is lost or stolen this should immediately be reported to the PKI supplier's revocation request service

Examples of the use of certificate classes

Personal certificate:

- Healthcare personnel sign sick notes, prescriptions, treatment requirements, etc., which are wrapped in an ebXML envelope
- An employee's personal authentication when logging in from a home office solution
- A service employee's personal authentication when logging in through a remote access solution
- A patient's personal authentication when logging in to the organization's solution for electronic patient communication

Enterprise certificate:

- Sign an ebXML envelope containing one or more other messages that may have been signed using a personal certificate
- Authentication in connection with a supplier connecting its support solution to the organization's network
- Encryption/decryption of messages