Requirements specification for PKI in the public sector

Version 2.0
June 2010

Contents

1. INTRODUCTION

1.1 Objective and background

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

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

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

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

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

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

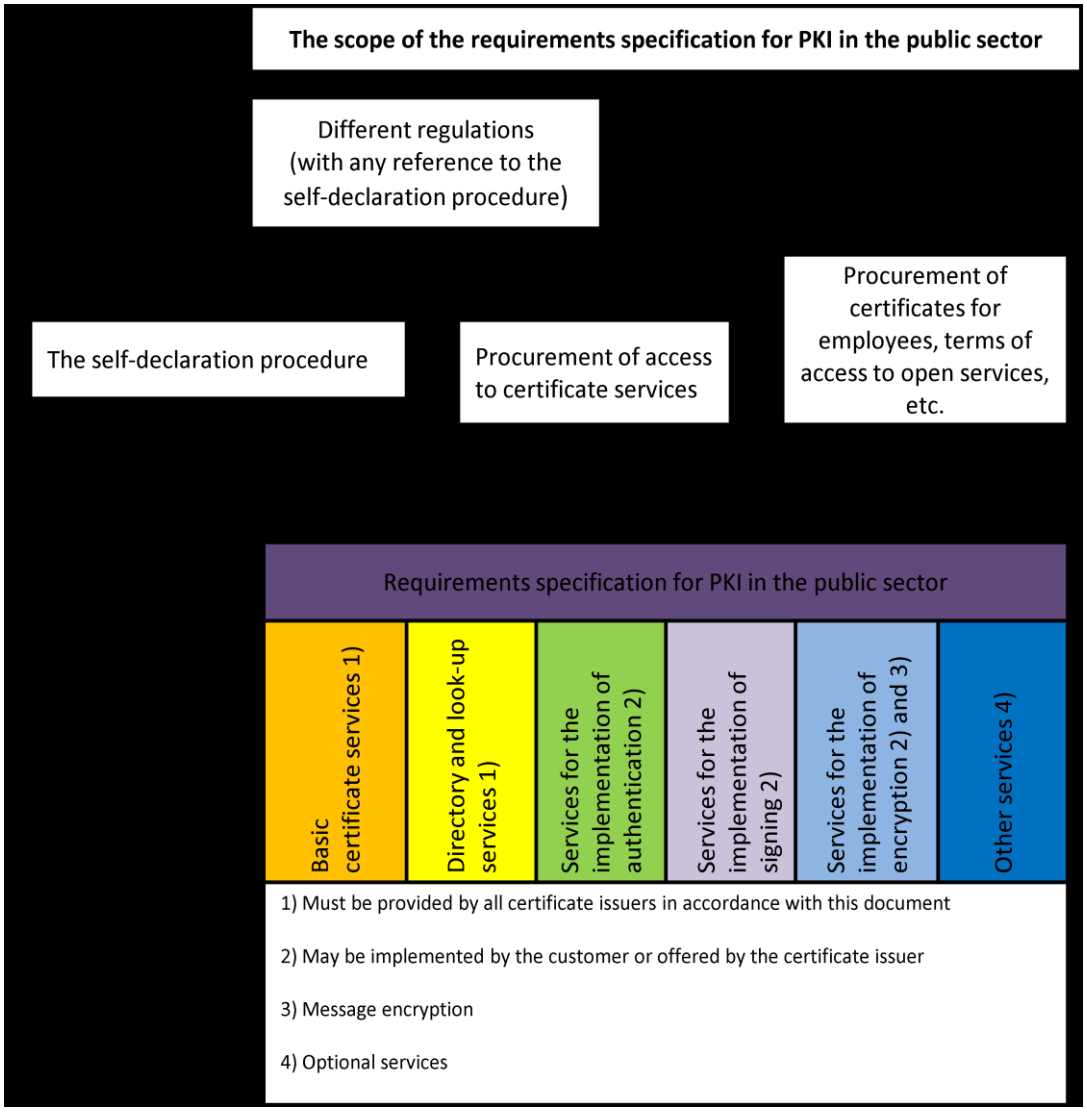
1.2 A summary of the scope of the requirements specification

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

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

Further, this document forms part of the tender documents and the contract when agreements regarding access to certificate services are entered into. Correspondingly, this document will

be of relevance to the purchase of certificates for the enterprise or employees, and for the use of open services. See figure below.



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

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

1.3 Use of the requirements specification upon self-declaration

The self-declaration procedure, and its supervision, should aim to ensure that certificate issuers comply with the requirements of this document, cf. regulations regarding voluntary