

Commentary

on selected annexes

of the application for the product certification for the qualified electronic signature or the application for prolonging the certificate validity of the product for the qualified electronic signature (hereinafter referred to as the QES)

Operation directions

This document is a user manual or the manual for installation, setting and maintenance depending on the product determination for the QES. It must describe basic rules of the product usage for the QES.

The document must contain in particular:

- a procedure for installation, setting, configuration, potential error message, a procedure for uninstallation (it may also refer to separate documents: installation, configuration, administration,...),
- in case of architecture – all levels of architecture described,
- system requirements (SW and HW) described unambiguously.

The document can:

- be supplemented with pictures which supplement individual texts illustratively, be supplemented with examples of the usage,
- separately contain a description of input and/or output interface,
- contain a dial of return values, error messages, etc. (if any) for easier orientation.

The document can also contain:

- a description of logging and the structure of audit log (if it does not go beyond the direction framework, otherwise it is required to be included in the document “General product description”),
- security aspects and their fulfillment.

General description of the product

This annex must contain in particular:

- a general product description,
- a basic architecture required for the product operation with detailed description,
- a description of individual activities performed by the product according to the determination, including the function of input and/or output interface,
- legislative requirements in compliance with which the product works (provide a brief reference),
- relevant security properties of the product, fulfillment of security requirements,
- description of logging and the structure of audit logs; in case it was provided in the document Operation directions, it is sufficient to summarize it briefly.

For reasons of explicitness the description may be supplemented with pictures which illustratively supplement and enlarge the text.

Description of basic functionality

In this document it is necessary in particular:

- to describe the basic functionality of the product as a whole and also individually according to functional blocks, the functional model, the information flow,
- to describe the functionality of input/output interface,
- to describe the format and structure of documents being signed, the signature format and structure.

The functionality description must be described in compliance with requirements of the valid legislation for a particular product (pursuant to the Act No. 215/2002 Coll. on Electronic signature and on the amendment and supplementing of certain acts as amended and the NSA Decree No. 134/2009 Coll. on Electronic signature products as amended).

Operation conditions

This document must contain the description of necessary conditions required for the operation and environment where the product for the QES shall be deployed and operated.

The document must contain:

- hardware requirements,
- software requirements,
- environment requirements,
- requirements for products and for support of third parties, licence and other conditions for their fulfillment,
- security requirements,
- conditions for integration of the product for the QES into existing information system of the organization including the description of requirements for the interface and ensuring the required security level, if such system already exists.

The producer of the product for the QES should describe the fulfillment of security requirements where requirements for the operation of the product for the QES from the point of view of assets and risks as well as the methods of their elimination shall be defined.

Supported standards, norms and protocols

In this document it is necessary for example in the form of a list or a table to provide norms, standards, recommendations and protocols which were used at the proposal and implementation of the product for the QES.

The applicant within this document submits the declaration of the manufacturer that the developed product satisfies the requirements of the Act No. 215/2002 Coll. on Electronic signature and on the amendment and supplementing of certain acts as amended and meets the requirements defined in the NSA Decree No. 134/2009 Coll. on Electronic signature

products as amended. Declaration of the manufacturer about the compliance with requirements stipulated by legal rules may also constitute a separate document.

List, parameters and properties of cryptographic functions

In this document the cryptographic functions being used by the product must be provided in the form of a list or a table. It may also contain references to algorithms, e.g. to calculate SHA-256, etc.

Security certificates, compatibility certificates, final report of the audit (if any)

For the certification needs it is necessary to submit security certificates from laboratories or certification centers of the NSA recognized institutions or the affirmation of the third party (by submitting the final report of the security audit – the expert opinion).