LIITE 2 Material needed for product evaluation

1 Introduction

This document describes the material needed for security enforcing product evaluations in Traficom's NCSA functionality. The main document "Liikenne- ja viestintäviraston salaus- ja turvallisuuskriittisten tuotteiden arviointiohje" describes different assurance levels for evaluations. This document is to supplement the main document to list document types and the documentation needed on different assurance levels.

The documentation list is divided into two parts

- The product's generic security evaluation
- Cryptographic security evaluation (this part is classified, TLIV)

The product's generic security evaluation is common for all security enforcing products, including products for data encryption. Cryptographic security evaluation is for security enforcing products for data encryption.

The list is not exhaustive and there may be new components or information identified and requested when knowledge on the dpevice is gained.

The evaluation activities are done at Traficom premises in Kumpula, Helsinki. Evaluation work may be done remotely, for example from home, if the information sensitivity allows that and if this is agreed with the vendor. Customer provided devices may be used to review material where necessary.

2 Generic Product Security Evaluation

Traficom will test the product in practice. The security architecture of the device will be reviewed and the testing will concentrate on the security controls of the device. The testing may include e.g. basic use cases, vulnerabilities, penetration testing and dynamic testing (fuzzing). This chapter describes the needed information.

For cryptographic products the documentation requirements are FIPS 140-3, Appendix A documentation in all assurance levels (described in chapter 3). If that documentation does not include some of the information described in chapter 2.1, also that documentation is needed.

The devices needed for testing are defined in the main document "Liikenne- ja viestintäviraston salaus- ja turvallisuuskriittisten tuotteiden arviointiohje".

2.1 Documentation

Documentation needed to support evaluation

Document	Assurance Level			Comments	
	A	B	C		
High level documentation / Functional description Same topics are covered in cryptographic chapter, but this has some extra point for product security evaluation.					

User guide documents	x	x	x	
Description of the high level architecture, services/interfaces and security controls	x	x	x	For example: • System description in the context of the operating environment • High level design documentation • A high level description of the architecture • Any external (non standard) interfaces • Any other relevant security functionality and parameters • Release notes and possible change logs
Description of the device use cases	x	x	x	An overview of the functionality including the use-cases relevant for the evaluation
Documentation of possible earlier evaluations	x	x	x	
Threat modelling documentation	x	x	x	
SW Bill of Materials	x	x	x	CycloneDX format preferred
Description of Cryptographic characteristics				
High Level Description of the use of cryptography in the products	x	x	x	This is for security enforcing products in general. This can be combined in the security controls description.
Detailed description of cryptographic characteristics				This is for security enforcing products used for data encryption. See details in Cryptographic Security evaluation chapter.
Description of life-cycle-management				
Product lifetime management process	x	x	x	For example software and key management.
Vulnerability management process	x	x	x	
Description of product development processes/environment				

Katakri self evaluation	x	x		
General description of software development process	x	x		For example: • requirements • architecture and design • implementation • testing methodologies • deployment • maintenance
Detailed description of software development process and manufacturing process	x			
Low level documentation				
Detailed description of the architecture and services	x	x		
Detailed description of the security controls	x	x		
HW Bill of Material	x	x		CycloneDX format preferred
Source Code				
Source code of security critical components	x			Cryptographic evaluation will cover the crypto code

For encryption products, there are additional classified document requirements. These are distributed by Traficom.