



IST-2001-34340

D8.1 Security reference document list

Distribution List:	Project Partners
Author:	Christophe ANIER, AQL
Distribution List:	Project Partners
Authorised by:	Yann Fraval, GIP-MDS
Date of Issue:	September 27th, 2002
Issue:	1.0
File Name:	EUPKI-WP8-D8.1-1.0.DOC
Work Package:	WP8 Homologation issues and security guidelines
Deliverable Number:	D 8.1
Deliverable Type:	Public
Deliverable Nature:	
Total Number of Pages:	15
Contact Details for EUPKI:	Project Coordinator Yann Fraval GIP-MDS mail: yann.fraval@gip-mds.fr web site: www.eupki.org

0 Table Of Contents

0	TABLE OF CONTENTS	2
1	DOCUMENT CONTROL	4
1.1	ABSTRACT	4
1.2	KEYWORDS	4
2	MANAGEMENT OVERVIEW	5
2.1	EXECUTIVE SUMMARY	5
2.2	SCOPE STATEMENT	5
3	INTRODUCTION AND GLOSSARY.....	6
3.1	GLOSSARY	6
4	SECURITY TARGET DOCUMENT	7
4.1	STATE OF WORK.....	7
4.2	SECURITY TARGET DOCUMENT	7
5	ASSURANCE LEVEL PROPOSAL.....	8
6	ASSURANCE MEASURES.....	9
6.1	ADV_FSP.1: INFORMAL FUNCTIONAL SPECIFICATION	9
6.1.1	<i>Presentation</i>	9
6.1.2	<i>Expected deliverables for the evaluation</i>	9
6.2	ADV_HLD.1: DESCRIPTIVE HIGH-LEVEL DESIGN	10
6.2.1	<i>Presentation</i>	10
6.2.2	<i>Expected deliverables for the evaluation</i>	10
6.3	ADV_RCR.1: INFORMAL CORRESPONDENCE DEMONSTRATION.....	10
6.3.1	<i>Presentation</i>	10
6.3.2	<i>Expected deliverables for the evaluation</i>	11
6.4	ACM_CAP.2: CONFIGURATION ITEMS.....	11
6.4.1	<i>Presentation</i>	11
6.4.2	<i>Expected deliverables for the evaluation</i>	11
6.5	ADO_DEL.1: DELIVERY PROCEDURES	11
6.5.1	<i>Presentation</i>	11
6.5.2	<i>Expected deliverables for the evaluation</i>	11
6.6	ADO_IGS.1: INSTALLATION, GENERATION, AND START-UP PROCEDURES	12
6.6.1	<i>Presentation</i>	12
6.6.2	<i>Expected deliverables for the evaluation</i>	12
6.7	AGD_ADM.1: ADMINISTRATOR GUIDANCE	12
6.7.1	<i>Presentation</i>	12
6.7.2	<i>Expected deliverables for the evaluation</i>	12
6.8	AGD_USR.1: USER GUIDANCE.....	12
6.8.1	<i>Presentation</i>	12
6.8.2	<i>Expected deliverables for the evaluation</i>	13
6.9	ATE_COV.1: EVIDENCE OF COVERAGE.....	13
6.9.1	<i>Presentation</i>	13
6.9.2	<i>Expected deliverables for the evaluation</i>	13
6.10	ATE_FUN.1: FUNCTIONAL TESTING.....	13
6.10.1	<i>Presentation.....</i>	13
6.10.2	<i>Expected deliverables for the evaluation.....</i>	13
6.11	ATE_IND.2: INDEPENDENT TESTING - SAMPLE.....	14
6.11.1	<i>Presentation.....</i>	14
6.11.2	<i>Expected deliverables for the evaluation.....</i>	14
6.12	AVA_SOF.1: STRENGTH OF TOE SECURITY FUNCTION EVALUATION	14
6.12.1	<i>Presentation.....</i>	14
6.12.2	<i>Expected deliverables for the evaluation.....</i>	14
6.13	AVA_VLA.2: INDEPENDENT VULNERABILITY ANALYSIS	14

6.13.1 *Presentation*..... 14
6.13.2 *Expected deliverables for the evaluation*..... 15

1 Document Control

<i>Issue</i>	<i>Date of Issue</i>	<i>Comments</i>
0.1	26 th June 2002	Creation
0.2	9 th July 2002	Draft for review
0.3	26 th July 2002	Version to be validate by the partners
1.0	26 th September 2002	Amendments determined in the 2 nd steering meeting

1.1 Abstract

The purpose of the deliverable D8.1 'The security document list' is to establish the list of necessary proof elements for the evaluation of EUPKI product.

This document provides information about assurance requirements and associated expected deliverables.

1.2 Keywords

EUPKI	EUPKI, the libre software Public Key Infrastructure (project name)
WP8	Work Package 8
GIP-MDS	Groupement d'Intérêt Public Modernisation des Déclarations Sociales
CGE&Y	Cap Gemini Ernst & Young
AQL	Alliance Qualité Logiciel

2 Management Overview

2.1 Executive Summary

This document provides information about assurance requirements and associated expected deliverables.

2.2 Scope Statement

The scope of this document is to present the necessary contents of proof elements for evaluation.

This document refers to the following external documents:

Reference	Document
D3.6	Perimeter and requirements of the project

3 Introduction and Glossary

3.1 Context

The context of the present project is special because the source code developed within the project will be distributed under Open Source licence at the end of the project.

As regard evaluation requirements, the distribution of the source code does not have any impact. Indeed, each step of the evaluation process will be performed the same way, independently of this fact.

Nevertheless, the situation will not be the same after a certificate issuance of the product EUPKI. Indeed, any contributor will then be allowed to add new functionalities through integration of new modules or by modifying existing parts of the EUPKI. These developments might be not conformant to the evaluation process requirements (update documentation, user guidance, etc..), thus it should be difficult to perform a renewal evaluation process in order to maintain the certificate.

Consequently, the initial version of the EUPKI project can be candidate for an evaluation process and a certificate issuance. Concerning the following versions, certificate maintenance will be possible only if the contributors conform closely to Common Criteria expectations.

3.2 Glossary

OCSP On-line Certificate Status Protocol

4 Security Target Document

4.1 State of work

During the Work Package 3, participants have proposed

- Functions requirements
- Assets which have to be protected by the TOE. (See chap 8.1 in D3.6).

Functions requirement expressed in WP3 are not Security Functions as expected by the Common Criteria but are functionalities covered by the projects. The definition of the Security Functions depends on the scope of the TOE and on its possible decomposition into several components.

Questions that need to be addressed in order for this document to be more accurate are the following:

- What will be evaluated ? One global TOE including all the aspects of the EUPKI project or a composition of components independently evaluated (RA, CA, etc...) ?
- What are the wish of the partners concerning certification scope ?

4.2 Security Target Document

Once the scope of the TOE will be defined, we will be able to write a Security Target (one for the TOE, or one for each component of the TOE) document.

This document will first includes:

- Environment of use stated as Assumptions, Threats to be countered by the product and Security policies with which the TOE must comply.
- Security Objectives: The statement of security objectives shall define the security objectives for the TOE and its environment. The security objectives shall address all of the security environment aspects identified. They shall reflect the stated intent and shall be suitable to counter all identified threats and cover all identified organisational security policies and assumptions.
- A choice of Security Functional Requirements extract from CC part 2.

Then, and after validation of the content, the reminder chapters will be completed in order to get an (even *close-to-be*) Security Target conformant to Common Criteria requirements from which we will be able to define what deliverables will be needed to conduct an evaluation process.

5 Assurance Level proposal

The technical board propose Evaluation Assurance Level 2 (EAL2) augmented with a stronger vulnerability analysis (assurance component AVA_VLA.2-Independent vulnerability analysis instead of AVA-VLA.1) to insure a minimum assurance level. This minimum is defined by the WP8 because it's more easy to reach and it's not sure that an higher assurance level is really necessary.

Evaluation Assurance Level 2 augmented is composed of the following components:

- ADV_FSP.1: Informal functional specification
- ADV_HLD.1: Descriptive high-level design
- ADV_RCR.1: Informal correspondence demonstration
- ACM_CAP.2: Configuration items
- ADO_DEL.1: Delivery procedures
- ADO_IGS.1: Installation, generation, and start-up procedures
- AGD_ADM.1: Administrator guidance
- AGD_USR.1: User guidance
- ATE_COV.1: Evidence of coverage
- ATE_FUN.1: Functional testing
- ATE_IND.2: Independent testing - sample
- AVA_SOF.1: Strength of TOE security function evaluation

Augmentation:

- AVA_VLA.2: Independent vulnerability analysis

6 Assurance Measures

The simplest measures to reach the assurance requirements are to have one or more documents for each assurance component.

So in this chapter, the contents of each document is described with a set of requirements

6.1 ADV_FSP.1: Informal functional specification

6.1.1 Presentation

To perform the evaluation task associated to the assurance component ADV_FSP.1, the evaluator analyses the functional specification, the administrator guidance, the user guidance and the chapter TOE Summary Specification in the Security Target.

The functional specification shall be a clear description of the security functions described in the Security Target. This description is of the same level of abstraction than in the Security Target but has to provide details about externally visible parts of the security functions. Externally means input and output of each security function, including error messages.

For example, the description of the security function F4 (repudiate key) is described in the TSS with one sentence whereas the description in the functional specification must states that this function takes as input a key, an identified operators, etc. and then, as a result, add the key to the revocation list. Moreover, actions that will be performed in case of invalid key, not enough identified operator or any other incorrect input shall be described (informing a given authority for example).

Functions that are not directly available to a user (that can be either an administrator or an end-user) but that contribute indirectly to the overall security shall also be described.

It has to be noted that as soon as an interface is provided by the product it has to be described. Nevertheless, the description can be short if the interface does not have relation to security functions.

All Security functions must be described in terms of:

- input
- output
- informal behaviour description explaining what is the relation between the input and the output.
- action or behaviour in case of error

6.1.2 Expected deliverables for the evaluation

- Functional specification of the TOE

It has to be noted that this document can contains more information than what is requested by the Common Criteria (allowing the use of a document not dedicated to the evaluation), but in that case a clear distinction shall be made between security enforcing functions and not security enforcing functions.

6.2 ADV_HLD.1: Descriptive high-level design

6.2.1 Presentation

The second level of specification is the description of the security functionalities provided by the TOE in terms of major structural units. This document is the main entry point for the evaluator to understand how the TOE implements the Security Functions. The evaluator will check that this description is a correct realisation of the functional specification.

The high level design shall provide for each interface, if it is external (visible from outside of the TOE) or internal (used only between subsystems). Relation between subsystems shall also be described.

Concerning the EUPKI project, the descriptive high level design may be fulfilled by the document D4.1 titled "Global Architecture".

6.2.2 Expected deliverables for the evaluation

- "Global architecture" document

It has to be noted that this document can contains more information than what is requested by the Common Criteria (allowing the use of a document not dedicated to the evaluation), but in that case a clear distinction shall be made between security enforcing functions and not security enforcing functions.

6.3 ADV_RCR.1: Informal correspondence demonstration

6.3.1 Presentation

The informal correspondence demonstrations make explicit the link between the different levels of specification of the security functions (Security Functions in the Security Target, functional specification and high level design).

The objective for this evaluation task is to be sure that every aspects of the security functions described in the security target are also present in the less abstract TOE representation (i.e. high level design in the project).

Each step towards a more detailed specification is checked in order to identify a forgotten security aspect as earlier as possible.

It has to be noted that this document is, of course, not only for the evaluator but primarily a way for the developer to be sure that nothing has been mess during the specification stages.

6.3.2 *Expected deliverables for the evaluation*

- Correspondence representation between ST (chapter TSS) and FSP
- Correspondence representation between FSP and HLD

6.4 ACM_CAP.2: Configuration items

6.4.1 *Presentation*

Configuration management is of prior importance in security. When a user interacts with a product he shall be able to uniquely identify its version in order to be sure that he is interacting with the certified version of the product. Consequently, the configuration management of the product has to be evaluated.

No particular document has to be produced except the list of items that compose the TOE and whose versions are managed with a configuration management system (that do not have to be automated with respect to ACM_CAP.2).

The TOE must be labelled with its actual version number (like for example title of dialog box) and the configuration list must be update accordingly to modifications applied to the identified components of the TOE.

6.4.2 *Expected deliverables for the evaluation*

- Configuration management documentation
- Configuration list (for example: source code, guidance, development documentation, etc..)

6.5 ADO_DEL.1: Delivery procedures

6.5.1 *Presentation*

The objective of the ADO_DEL.1 activity is to determine whether the delivery documentation describes all procedures used to maintain integrity when distributing the TOE to the user's site. This does not covered the delivery of keys managed by the TOE but the delivery of the TOE itself.

Concerning the EUPKI project, this assurance requirement will require the developer to describe the delivery procedures used for example when the client side is downloaded by a user because the client part of the application is a part of the TOE.

6.5.2 *Expected deliverables for the evaluation*

- Delivery procedures

6.6 ADO_IGS.1: Installation, generation, and start-up procedures

6.6.1 Presentation

The objective of the ADO_IGS.1 activity is to determine whether the procedures and steps for the secure installation, generation, and start-up of the TOE have been documented and result in a secure configuration.

All parts of the TOE that need to be initialised shall be covered by a documentation describing initialisation and start-up procedures. The term "generation" covers the compilation of the TOE if it is planned to be delivered as source code, so the generation documentation has for example to identify all the compiler parameters required to obtain a secure generation of the TOE.

6.6.2 Expected deliverables for the evaluation

6.7 AGD_ADM.1: Administrator guidance

6.7.1 Presentation

The administrator guidance shall describe the use of all the administrative functions of the TOE in order for the TOE to stay in a secure state whatever happens. The administrators shall have all the information needed to react accordingly to security related events.

The term *administrator* is used in the Common Criteria to indicate a human user who is trusted to perform security critical operations within the TOE, such as setting TOE configuration parameters. The operations may affect the enforcement of the TSP, and the administrator therefore possesses specific privileges necessary to perform those operations. The role of the administrator(s) has to be clearly distinguished from the role of non-administrative users of the TOE.

In the context of the EUPKI project, the administrators are:

- *to be completed*

6.7.2 Expected deliverables for the evaluation

- Administrator manuals

6.8 AGD_USR.1: User guidance

6.8.1 Presentation

The objectives of the evaluation of the user guidance are to determine whether it describes the security functions and interfaces provided by the TOE security functions and whether this guidance provides instructions and guidelines for the secure use of the TOE.

The term *user* is used in the Common Criteria to indicate any human interacting with the TOE who is not a TOE administrator.

In the context of the EUPKI project, the user are:

- *to be completed*

6.8.2 *Expected deliverables for the evaluation*

- End-user manuals

6.9 ATE_COV.1: Evidence of coverage

6.9.1 *Presentation*

The objective of this sub-activity is to determine whether the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the functional specification.

6.9.2 *Expected deliverables for the evaluation*

- Evidences showing that the test have been related to the security function and that all the security functions have been covered by at least one tested. These evidences can be provided as part of the test documentation.

6.10 ATE_FUN.1: Functional testing

6.10.1 *Presentation*

The objective of this sub-activity is to determine whether the developer's functional test documentation is sufficient to demonstrate that security functions perform as specified. This activity is strongly related to the independent testing of the TOE by the evaluator.

Consequently the evaluator will look for evidences that the security functions have been tested accordingly. Thus when designing test, the developer has to link them to security functions.

The test scripts shall be sufficiently detailed (initial configuration, parameter values, assumption about environment, etc...) in order for the evaluator to be able to repeat them in the same conditions.

6.10.2 *Expected deliverables for the evaluation*

- Test scripts (including expecting test result and actual test results)

6.11 ATE_IND.2: Independent testing - sample

6.11.1 Presentation

The purpose of this activity is to determine, by independently testing a subset of the TOE security functions, whether the TOE behaves as specified, and to gain confidence in the developer's test results by performing a sample of the developer's tests.

6.11.2 Expected deliverables for the evaluation

- Test scripts (including expecting test result and actual test results)

6.12 AVA_SOF.1: Strength of TOE security function evaluation

6.12.1 Presentation

For each security mechanism implemented by a probabilistic or permutational and for which the developer has claimed a strength of function, the evaluator has to check that the implementation actually insure such a strength of function. This check is made on the basis of an analysis provided by the developer.

Cryptographic mechanism are out of scope of this evaluation activity.

As the strength of function is claimed for function and not for mechanism used to achieve this strength, the developer has to analyse each mechanism implied in the implementation of a security function independently before analysing the overall security obtained through their mutual cooperation.

Strength of Function (SOF) are expressed either as rating (level like SOF_Low, SOF-Medium and SOF-High) or as metrics (i.e. numerical computation analysis showing that the mechanism is resistant to brut force attack for example).

6.12.2 Expected deliverables for the evaluation

- Strength of Function claim in the security target
- Strength of function analysis for each probabilistic or permutational mechanism.

6.13 AVA_VLA.2: Independent vulnerability analysis

6.13.1 Presentation

The objective of this sub-activity is to assess that the TOE is resistant to an attack conducted by an attacker with a low attack potential. Roughly speaking, such an attacker will use publicly available software to exploit public vulnerabilities that do not need a detailed information about the TOE. More information about attack potential computation can be found in CEM, annex B.4. Several parameters are taken into account to establish the quotation of a vulnerability like expertise level needed, access time to the TOE, time needed to identify the vulnerability, amount and type of information about the TOE needed to identify and exploit a vulnerability (like IP address of a web server).

In order to reach this objective, both the developer and the evaluator have to perform an independent vulnerability analysis with associated penetration testing to validate the analysis.

These vulnerability analysis must take into account all the deliverables available and public domain attacks. The idea is to identify existing and potential ways to prevent the TOE to satisfy the security objectives defined in the Security Target.

Conclusion of the analysis shall be that none of the public domain attacks can be exploited to the TOE by an attacker with a low attack potential because counter-measures (either technical or organisational) exist that prevent such attacks.

6.13.2 Expected deliverables for the evaluation

- Vulnerability analysis showing that:
 - all the deliverables have been taken into account in the search for vulnerability
 - covers all the public domain attacks applying to the TOE
 - explains why none of these attacks can be exploited by an attacker with a low attack potential.