



IST-2001-34340

## D8.3 Integration processes analysis

|                                |  |
|--------------------------------|--|
| Distribution List:             | Project Partners   |
| Authors:                       | Christophe ANIER, Lionel VAN AERTRYCK <b>AQL</b>   |
| Distribution List:             | Project Partners   |
| Authorised by:                 |  |
| Date of Issue:                 | April 29th, 2004   |
| Issue:                         | 1.0  |
| File Name:                     | WP8-D8.3-1.00.DOC  |
| Work Package:                  | WP8 Homologation issues and security guidelines  |
| Deliverable Number:            | D8.3   |
| Deliverable Type:              | Public   |
| Deliverable Nature:            |  |
| Total Number of Pages:         | 10   |
| Contact Details for EUROPEPKI: | Project Coordinator GIP-MDS<br>mail:<br>web site: <a href="http://www.europepki.org">www.europepki.org</a> |

## 0 Table Of Contents

|          |   |           |
|----------|---|-----------|
| <b>0</b> | <b>TABLE OF CONTENTS .....</b>                      | <b>2</b>  |
| <b>1</b> | <b>DOCUMENT CONTROL .....</b>                       | <b>3</b>  |
| 1.1      | ABSTRACT .....                                      | 3         |
| 1.2      | KEYWORDS .....                                      | 3         |
| <b>2</b> | <b>MANAGEMENT OVERVIEW .....</b>                    | <b>4</b>  |
| 2.1      | EXECUTIVE SUMMARY .....                             | 4         |
| 2.2      | SCOPE STATEMENT .....                               | 4         |
| <b>3</b> | <b>INTRODUCTION AND GLOSSARY .....</b>              | <b>6</b>  |
| 3.1      | INTRODUCTION .....                                  | 6         |
| 3.2      | GLOSSARY .....                                      | 6         |
| <b>4</b> | <b>CONFIGURATION MANAGEMENT (ACM_CAP.2) .....</b>   | <b>7</b>  |
| <b>5</b> | <b>DELIVERY PROCEDURES (ADO_DEL.1) .....</b>        | <b>8</b>  |
| <b>6</b> | <b>TESTING (ATE_COV.1 AND ATE_FUN.1) .....</b>      | <b>9</b>  |
| 6.1      | TEST COVERAGE MEASURES (ATE_COV.1) .....            | 9         |
| 6.2      | FUNCTIONAL TESTING (ATE_FUN.1) .....                | 9         |
| <b>7</b> | <b>EXPLOITATION DOCUMENTATION (ADO_IGS.1) .....</b> | <b>10</b> |

# 1 Document Control

| <i>Issue</i> | <i>Date of Issue</i>        | <i>Comments</i>                         |
|--------------|-----------------------------|---|
| 0.1          | 21 <sup>st</sup> July 2003  | Creation                                |
| 0.2          | 12 <sup>th</sup> March 2004 | Some additions and corrections          |
| 1.0          | 23rd April 2004             | Final version at the end of the project |

## 1.1 Abstract

The purpose of the deliverables [WP6R6.1] 'Integration Overview ', [WP6R6.2] 'Integration Guidelines and Acceptance Procedures' and [WP6D6.1] is to describe acceptance procedure and integration processes.

The present document present the analysis of there adequacy to Common Criteria requirements satisfaction concerning configuration management (ACM\_CAP.2), delivery procedures (ADO\_DEL.1) and testing (ATE\_COV.1 and ATE\_FUN.1).

## 1.2 Keywords

WP4            Work Package 4  
 GIP-MDS      Groupement d'Intérêt Public Modernisation des Déclarations Sociales  
 CGE&Y        Cap Gemini Ernst & Young  
 AQL            Alliance Qualité Logiciel  
 PP             Protection Profile  
 ST             Security Target

## 2 Management Overview

### 2.1 Executive Summary

This document provides information about configuration management procedures, delivery procedure and test documentation as regard Common Criteria EAL2+ (AVA\_VLA.2) requirements within the scope of the EUROPEPKI project.

A first list of remarks has been provided about the deliverables [WP6R6.1], [WP6R6.2] and [WP6D6.1] and their adequacy with respect to Common Criteria requirements. The present report states if and how these remarks have been taken into account within the latest version of the appropriate EUROPEPKI documents.

**Even if the documentation as been greatly improved concerning these aspects, more information is expected than what is provided for the moment to satisfy CC requirements.** However, it has to be notice that not all the documentation is available at the date of writing the present report, as the development and the testing phase are not finished yet.

### 2.2 Scope Statement

This document refers to the following external documents:

| Reference  | Document  |
|------------|---|
| [WP3D3.6]  | <b>WP3D3.6 Perimeter and requirements of the project</b>  |
| [WP6R6.1]  | <b>WP6 R6.1 Integration process Overview,</b><br>Draft v0.3   |
| [WP6R6.2]  | <b>WP6 R6.2 Integration guidelines and acceptance procedures,</b><br>v1.0   |
| [WP6R6.3]  | <b>WP6 R6.3 Collaborative Environment</b>   |
| [WP6R6.5]  | <b>WP6 R6.5 EuropePKI preliminary installation and usage guide</b>  |
| [WP6D6.1]  | <b>WP6 D6.1 Integration Progress Report One,</b><br>V1.0  |
| [WP5D5.01] | <b>WP5D5 Development overall communication</b><br>V0.1  |
| [CC-01]    | <b>Common Criteria for Information Technology Security Evaluation</b><br>CCIMB-99-031, Part 1: Introduction and general model, Version 2.1,<br>August 1999.   |
| [CC-02]    | <b>Common Criteria for Information Technology Security Evaluation</b><br>CCIMB-99-032, Part 2: Security functional requirements, Version 2.1,<br>August 1999. |

|         |   |
|---------|---|
| [CC-03] | <b>Common Criteria for Information Technology Security Evaluation</b><br>CCIMB-99-033, Part 3: Security assurance requirements, Version 2.1, August 1999. |
|---------|---|

## 3 Introduction and Glossary

### 3.1 Introduction

The initial analysis of the EUROPEPKI documents has been performed on the following versions:

[WP6R6.1]: Draft 0.4

[WP6R6.2]: Draft 0.3

[WP6D6.1]: Draft 0.5

The following documents have been updated:

[WP6R6.2]: v1.0

[WP6D6.1]: v1.0

The following document have been added to perform the analysis:

[WP5D5.01] : v 02a

At the end of the project, the following document have been added to perform the analysis:

[WP6R6.5] : v 04

### 3.2 Glossary

|       |  |
|-------|--|
| CRM   | Customer Relationship Management                     |
| HR    | Human Resources                                      |
| OCSP  | On-line Certificate Status Protocol                  |
| TOE   | Target Of Evaluation                                 |
| SFR   | Security Functional Requirements                     |
| PKI   | Public Key Infrastructure                            |
| CA    | Certification Authority                              |
| RA    | Registration Authority                               |
| CRPKI | Cryptographic Resource for Public Key Infrastructure |

## 4 Configuration Management (ACM\_CAP.2)

The assurance component selected to cover configuration management aspects is ACM\_CAP.2 "Configuration items". This component requires the developer to provide:

- an identified configuration management tool
- a configuration management documentation (including a configuration list)
- versioning rules for the TOE
- a TOE correctly referenced and labelled with its reference.

Concerning the configuration management tool, [WP5D5.01] (section 2.5) makes reference to CVS as the tool to be used for source code control. Source repository structure is partially defined in [WP6R6.2] (section 3.4)

There is still no "official" list of items to be under configuration management, however, the descriptions provided in [WP6R6.2] about each kind of distribution (alpha release, beta release, etc.) include a list of items that have to be part of the distribution. These lists might be a good starting point to define a configuration list.

No information or explicit rules are provided regarding versioning of the TOE and the possible impact of a modification of one of its components on the reference of the TOE (Common Criteria require that the TOE reference shall be unique).

At the end of the project, CVS is used to manage configuration of modules. But there is always no documentation about that. To have a Common Criteria compliance, it's necessary to provide documentation about:

- configuration management rules (user and administration guides),
- versioning rules for the TOE,
- a TOE referenced and labelled with its reference.

## 5 Delivery procedures (ADO\_DEL.1)

The main objective of the component ADO\_DEL.1 is to ensure the integrity of what is delivered to end users (coherent set made of the TOE, the installation procedure and guidance documents for that specific version of the TOE).

The document [WP6R6.2] provides delivery procedures that shall be followed to make either a development delivery (to integrator) or a block delivery (to end-users). These procedures mainly detail what has to be provided within a given delivery, depending on its nature, but not how the integrity of the elements delivered is ensured.

The delivery procedures presented in [WP6R6.2] cover several kinds of release :

- development deliveries (i.e. module deliveries to integration)
  - o skeleton delivery
  - o prototype delivery
  - o complete delivery
  - o final package
- distribution deliveries (i.e. block or set of block deliveries to end-users and testers: CA, RA, Server KGS, Client KGS, etc.)
  - o skeleton distribution
  - o alpha distribution
  - o beta distribution
  - o release distribution
  - o system distribution (coherent set of blocks)

As regard Common Criteria expectations, delivery procedures concern only delivery of the TOE (distribution deliveries) to the end-user's site.

Delivery to end-user will be performed through the connexion of the end user to a public server where each release will be store.

[WP6D6.1], Annexe C, p15: "Coding conventions are required by Common Criteria". In fact, conforming to coding conventions is required by assurance component ALC\_TAT.2 (for a subpart of the TOE implementation only), which component is not part of the chosen EAL but is part of EAL5.

It is still not clear from the documentation if a proof of integrity (like a checksum) will be automatically added to each delivery and the way for the end user to check it.

To have a Common Criteria compliance, it's necessary to explain how the integrity of the elements delivered is ensured during the delivery procedure (i.e. download of the source code).

## 6 Testing (ATE\_COV.1 and ATE\_FUN.1)

Chapter 6 of [WP6R6.2] provides information about acceptance procedures for source code integration. The source code can be produced by WP5 members or by external contributors.

Before going through the quality check procedure, several points relative to conformance control of the source code are checked (function nomenclature, link to specification, etc.).

The quality check procedure requires the developer (WP5 member or external contributor) to provide, among other requested documents, a unit test plan. No detail is provided about what this unit test plan shall contain.

In case the acceptance procedure is validated (an acceptance report is issued), the source code goes through the integration procedure. This step encompasses integration component development and functional testing of the distribution.

The functional tests performed depend on the nature of the distribution. A skeleton distribution will not be tested whereas an alpha (or better) distribution will be.

### 6.1 Test coverage measures (ATE\_COV.1)

The document [WP6R6.2] does not mention any test coverage evidences to be produced by the developer as part of a source code delivery, whereas it is requested by ATE\_COV.1 requirements.

Validation reports that will be issued after any integration phase will contain a global description of the test performed ([WP6R6.2], section 4.10). That description might be sufficient to satisfy CC requirements if it contains, for example, a traceability table showing the links between the tests performed and the security functions implemented. It has to be recalled that complete coverage is not requested at this level, but only evidences of coverage analysis.

Concerning prototype delivery, [WP6R6.2] (section 4.1.2) indicates that source code of the test programs for all the implemented functions must be provided and that the developer has executed all of them. A document, associated to these test programs, that makes explicit this coverage is what is expected to satisfy ATE\_COV.1 requirements.

### 6.2 Functional Testing (ATE\_FUN.1)

Remarks that have been made on the previous version of the documents are still valid regarding ATE\_FUN.1 requirements. Indeed, no test plan and no test procedure are available.

## 7 Exploitation documentation (ADO\_IGS.1)

Installation, generation, and start-up procedures are useful for ensuring that the TOE has been installed, generated, and started up in a secure manner as intended by the developer.

At the end of the project, WP6 provided documentation about first installation of the product [WP6R6.5].

This documentation is not fully complete (it's a draft) but it's a base for a good documentation for an evaluation process because there a part for:

- Installation for a secure state (§5.1 to §5.3),
- Start-up procedure (§5.4),
- First administration (§5.5).