AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

Certification Report for Australian Government Use

Certificate Number: 2001/17

VeriSign Incorporated

VeriSign Processing Center 3.0

Issue 1.0
March 2001

Issued by: -

Defence Signals Directorate - Australasian Certification Authority

CERTIFICATION STATEMENT

VeriSign Processing Center Version 3.0 is a product developed by VeriSign Incorporated implementing a fully integrated Public Key Infrastructure (PKI) managed service that allows an enterprise to issue digital certificates. Using the product, the enterprise can establish a customised PKI and Certificate Authority whilst retaining control over security policy, PKI hierarchy, authentication models and certificate management services.

This report describes the evaluation findings of the VeriSign Processing Center Version 3.0 product to the Common Criteria (CC) Evaluation Assurance Level (EAL) 4, and includes recommendations by the Australasian Certification Authority (ACA) that are specific to the secure use of the product to meet its CC EAL4 level of assurance. It concludes that the product has met the target Assurance Level of CC EAL4.

Originator

Matthew Earley
Certifier
Defence Signals Directorate

Approval

Jane Holzapfel
Assistant Manager, Australasian Information Security Evaluation Program
Defence Signals Directorate

Authorisation

Stewart Skelt
Australasian Certification Authority
Defence Signals Directorate

TABLE OF CONTENTS

Chapter 1 Introduction

Intended Audience

1.1 This certification report states the outcome of the IT security evaluation of the VeriSign Processing Center Version 3.0 (hereafter referred to as Processing Center). It is intended to assist potential users when judging the suitability of the product for their particular requirements, and to advise security administrators on ensuring the product is used in a secure manner. Other users intending to use this product should seek advice from their National Security Advisory Authority to determine its suitability in meeting their particular requirements.

Identification of Target of Evaluation

1.2 The version of Processing Center evaluated was Version 3.0, developed by VeriSign Incorporated.

1.3 The security functionality offered by Processing Center is implemented entirely in software.

1.4 The evaluated components of the Processing Center consist of:

a) Connection Manager;

b) Query Manager ;

c) Bootstrap, UpdateCRL and LoadCA modules;

d) Common Gateway Interface (CGI) modules;

e) Admin Manager Tool;

f) OnSite Control Center;

g) Certificate Lifecycle;

h) Transport processes beamup and beamdown.

1.5 Processing Center consists of one CD-ROM. The CD-ROM contains the Processing Center software, and the administration and user guidance. The version of Processing Center on the CD-

ROM should read **3.0** on its label.

1.6 For further details of the evaluated components of the Processing Center product, including details of how to identify the evaluated version, refer to Appendix C.

Evaluation

1.7 The evaluation was carried out in accordance with the rules of the Australasian Information Security Evaluation Program (AISEP) which is described in Evaluation Memorandum 1 and Evaluation Memorandum 2 (refs [1,2] respectively). In addition, the conditions outlined in the Common Criteria Recognition Arrangement (ref [25]) were also upheld during the evaluation and certification of this product.

1.8 The purpose of the evaluation was to provide assurance about the effectiveness of the Target of Evaluation (TOE), the Processing Center product, in meeting its Security Target (ref [9]). The criteria against which the TOE is judged are expressed in the Common Criteria Part 3 (ref [5]). This describes how the degree of assurance can be expressed in terms of the levels EAL1 to EAL7. The methodology used is described in the Common Evaluation Methodology (CEM) and Evaluation Memoranda 4 and 5 (refs [6,7,8]).

1.9 The evaluation was sponsored by United States based VeriSign Incorporated. The developer of the Processing Center product was also VeriSign Incorporated. A complete listing of the documentation used during the evaluation of this product is included or referenced in Appendix A of this Report.

1.10 The evaluation was performed by CMG Admiral between June 2000 and March 2001, and was monitored by the Certification Group on behalf of the Australasian Certification Authority (ACA). At the end of the evaluation, an Evaluation Technical Report (ETR) (ref [10]) describing the evaluation and its results was presented to the ACA. The Certification Report was then produced, based on the contents of the ETR and the Certification Group's knowledge of the evaluation.

1.11 The Security Target (ref [9]) claimed an assurance level for the product of CC EAL4.

General Points

1.12 Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher evaluation levels) that exploitable vulnerabilities remain undiscovered.

1.13 EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behaviour. Assurance is additionally gained through an informal model of the TOE security policy.

1.14 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

1.15 EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

1.16 Processing Center should only be used within the defined TOE security environment in accordance with the specified assumptions, as explained in section 3.1 of the ST (ref [9]). Also, the security requirements on the IT and non-IT environment must be fully understood in order to determine the suitability of the product in its assumed operational environment, as explained in section 5.3 of (ref [9]). In addition, users should be aware of the certifiers' recommendations as given in Chapter 4 of this report.

1.17 Ultimately, it is the responsibility of the user to ensure that the Processing Center product meets their requirements. For this reason, it is ***strongly*** recommended that a prospective user of the product obtains a copy of the Security Target (ref [9]) from the product vendor, and reads this Certification Report thoroughly prior to deciding whether to purchase the product.

Scope of the Evaluation

1.18 The scope of the evaluation is limited to those claims made in the Security Target (ref [9]). All security related claims in the Security Target were evaluated by CMG Admiral. A summary of the Security Target is provided in Annex B of this Certification Report.

1.19 As there were no cryptographic algorithms or mechanisms claimed in the Security Target (ref [9]), a full cryptographic evaluation was not performed by DSD. However, digital signature verification was identified as a cryptographic operation implemented by the TOE. This cryptographic operation was evaluated by DSD for Australian Government use and found to be appropriate for the protection of material classified RESTRICTED, and non National Security classifications including

IN-CONFIDENCE, PROTECTED and, in consultation with DSD, HIGHLY PROTECTED.

1.20 Other cryptographic operations (including key generation, key storage and the use of Secure Sockets Layer (SSL) to implement a trusted communications path) were not evaluated by DSD. Consequently, the appropriateness of any cryptographic product to be used in conjunction with the Processing Center has not been evaluated by DSD for Australian Government use.

1.21 Potential Commonwealth Government users are encouraged to contact DSD for further advice on the suitability of this product when used in conjunction with other evaluated products to protect national security and non-national security information.

Chapter 2 Security Overview of Processing Center

2.1 Potential users are strongly recommended to read the Security Target (ref [9]). This explains the security functionality of the Processing Center product in greater detail, as well as the intended environment and method of use for the product. A summary of the Security Target can be found in Appendix B. A full copy of the Security Target can be obtained from the sponsor of the evaluation.

Functionality of the TOE

2.2 This section provides a summary of the operational role of the TOE together with the security functions it is designed to perform.

2.3 Processing Center is a fully integrated PKI managed service that allows an enterprise to issue digital certificates. Using the product, the enterprise can establish a customised PKI and Certificate Authority whilst retaining control over security policy, PKI hierarchy, authentication models and certificate management services.

2.4 The TOE provides components for performing Certification Authority (CA) functions (the Enterprise Service Center) and Registration Authority (RA) functions (the OnSite Control Center). It is designed to be installed and operated by "affiliate" organisations of VeriSign. VeriSign operates a major installation at its headquarters in Mountain View, California. Affiliate organisations have established centres using the TOE in a number of countries in order to provide PKI services to customers.

2.5 The TOE supports the concept of "jurisdictions", which are administrative management domains within the TOE. Jurisdictions are identified by their company and department name. A CA may be used by many jurisdictions, but a jurisdiction will only use a single CA to sign certificates.

2.6 The CA component of the TOE is administered by Master Service Administrators (MSAs) and Enterprise Service Administrators (ESAs), while the RA component (equivalent to a jurisdiction) is administered by OnSite Administrators (OSAs). MSAs are responsible for creating other MSAs and ESAs as required. ESAs are responsible for reviewing and approving applications for new OSAs. An OSA administers a particular jurisdiction and is responsible for reviewing and approving requests for certificates from end users. End user certificates can also be issued already configured

for use with specialist devices such as firewalls, email servers and web servers.

2.7 MSAs, ESAs and OSAs identify and authenticate themselves to the TOE using their own certificate. The act of creating an administrator involves the TOE signing a digital certificate that identifies the administrator and the jurisdiction within which the administrator can operate.

2.8 The TOE provides the functionality for managing the operations of the CA and the jurisdictions associated with it and for managing the life cycle of administrator and end user certificates it issues. The evaluated security functions of the TOE counter the following types of threat:

a) unauthorised attempts to create or alter user or CA certificates;

b) unauthorised attempts to use the functionality of the TOE;

c) undetected creation of inappropriate or fraudulent certificates;

d) irreversible creation of inappropriate or fraudulent certificates.

2.9 The evaluated security functions of the TOE do not counter the following types of threat, which must be addressed by environmental and procedural means as specified in the Security Target (ref [9]) and the guidance documentation (refs [11] - [21]):

a) direct physical access to the servers on which the TOE is installed;

b) compromise of the root CA keys used by the TOE;

c) compromise of end users' private keys;

d) malicious operation of the TOE by trusted administrators;

e) fraudulent requests for certificates;

f) compromise of the communications between client web browsers and the TOE's web servers (e.g. by web spoofing or man-in-the-middle attack

2.10 In order to achieve its security objectives, the Processing Center product is dependent on a number of security services provided by the operational environment. While these services do not contribute to the satisfaction of any of the security objectives, certain third party software is used in conjunction with the Processing Center product to facilitate secure and efficient administration of the overall system.

2.11 Processing Center achieves six security objectives for the TOE to create and maintain the confidentiality and integrity of the protected IT assets. Availability concerns are not countered by the TOE. These security objectives for the TOE have been satisfied by nine categories of technical (IT) countermeasures implemented by the TOE (i.e. TOE Security Functions) in software. These are provided individually or in collaboration with one or more of the Processing Center components identified below.

2.12 In addition, Processing Center achieves eleven security objectives for the environment. These security objectives for the environment have been satisfied by a collaboration of technical measures implemented by the IT environment, and by the enforcement of non-IT (eg. procedural) measures.

2.13 There is no hardware or firmware associated with the evaluated configuration of the product. However, the minimum hardware configuration has been stipulated in section 2.4.1 of the Security Target (ref [9]).

2.14 While the intention is to use Processing Center to create and manage a Public Key Infrastructure (PKI), the evaluation of Processing Center has not included some of the mandatory components needed to operate a PKI. Specifically, the evaluation of Processing Center excluded the technology required to implement secure generation and storage of the user (or component) private and public keys. In addition, the technology required to implement a trusted communication path from an external user (eg an OnSite Administrator) to the external-facing web server was also excluded from the evaluation of Processing Center. Therefore, organisations looking for a complete PKI solution are recommended to refer to other products listed in the Evaluated Products List that could be interoperable with Processing Center. Furthermore, Commonwealth Government users should ensure that the product is being used in accordance with Gatekeeper requirements.

2.15 More detailed information on the Processing Center product can be found in the Security Target (ref [9]), and in Appendix B of this report

Architecture of the TOE

2.16 This section provides a summary of the architectural design of the TOE together with the security functions it is designed to perform.

2.17 Processing Center is implemented as a set of distributed processes running on various distributed servers. It is assumed that the servers and their network connections are secured using physical and logical means external to the TOE (refer to assumptions in ST). In practice, this is provided by

installing the servers in highly secure physical locations with firewalls protecting the networks.

2.18 Processing Center comprises the following architectural components:

a. User Interface, comprising:

i) Admin Manager Tool;

ii) OnSite Control Center;

iii) Certificate Lifecycle.

b. Connection Manager

c. Query Manager, comprising:

i) Read/Write Query Manager;

ii) Read Only Query Manager.

d. Signing

e. Transport

f. Database

g. Trusted Path

h. System Operator.

2.19 The OnSite Control Center and Certificate Lifecycle components and a Trusted Path component are hosted on the Front-End Web Server

2.20 The Admin Manager Tool component and a Trusted Path component are hosted on the Internal Facing Web Server.

2.21 The Connection Manager, Query Manager and System Operator components are hosted on the Application Server, while the Signing Server hosts the Signing component, and the Database server hosts the Database component.

2.22 The TSF (the collection of all TOE Security Functions) is composed of the Connection Manager,

Query Manager, Trusted Path and System Operator components. The remaining components do not provide any security functionality of the TOE.

2.23 Users interact with the TOE depending on their role. End users (i.e. customers seeking to obtain user certificates) interact with the TOE using the Certificate Lifecycle web server. This provides facilities for end users to enroll for certificates, pick up their certificate when it has been approved, renew their certificate before it expires and revoke their own certificate if necessary.

2.24 OSAs interact with the TOE via the OnSite Control Center web server, which provides the facilities to review, approve and revoke end user certificates and manage the end user certificate lifecycle. All of these operations are actually performed by the TSF components in the Back-End Network. The OnSite Control Center provides the means for the OSA to request operations and to present their certificate to the TOE for identification and authentication purposes. The Trusted Path component receives the OSA's certificate and requested operation from the OnSite Control Center web server and forwards these in a trusted fashion to the Back-End Network.

2.25 MSAs and ESAs interact with the TOE via the Admin Manager Tool web server. This is similar to the OnSite Control Center, but provides operations for managing administrator certificates and jurisdictions rather than end user certificates. As with the OnSite Control Center, the Admin Manager Tool web server passes the administrator certificate and requested operation to the Trusted Path component, which forwards them to the Back-End Network.

2.26 The System Operator component provides tools for system operators to manage aspects of the TOE that are not available to MSAs or ESAs. This includes loading CA keys for new jurisdictions and creating Certificate Revocation Lists (CRLs).

2.27 The Connection Manager, Query Manager and System Operator components all operate on a dedicated Application Server, while the Transport, Signing and Database components operate on separate servers. The Trusted Path component is separated from the User Interface components by logical means, in that it runs in separate process and address space on the web server machines.

Security Policy

2.28 The following security policies are enforced by the Processing Center:

- Identification and authentication policy, describing the requirements for gaining access to the TOE;

- Access control policy, describing the requirements for controlling access to the various security functions of the TOE;
- Audit policy, describing the requirements for the auditing of security events in the TOE and;
- Trusted path policy, describing the requirements for communication between the users and the TSF.

2.29 The security policy model is summarised in chapter 4.4 of the ETR (ref [10]). Alternatively, the security policy model (ref [22]) may be requested directly from the developer.

2.30 In order for the TOE to comply with the security policy model, the Processing Center product should only be used within the defined TOE security environment in accordance with the secure usage assumptions, as explained in section 3.1 of the ST (ref [9]).

Documentation

2.31 Before using the product, administrators and security managers should ensure that they are aware of and fully understand the relevant operational documentation. In addition, they should ensure that they read Chapter 4 of this document, and the associated administration and user manuals contained on the product CD-ROM (refs [11]-[21]).

Chapter 3 Evaluation Findings

Introduction

3.1. The evaluation of Processing Center followed a course consistent with the generic evaluation work program described in the ITSEM (ref [23]) and the CEM (ref [6]), with work packages structured around the evaluator actions described in the Common Criteria (CC) Part 3 (ref [5]). The results of this work are reported in the ETR (ref [10]) under the CC headings. This report summarises the general results, followed by the findings in relation to the security functionality claimed in the Security Target (ref [9]).

Security Target Evaluation

3.2. The purpose of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

TOE Description (ASE_DES.1)

3.3. The TOE Description adequately described the product type, and the scope and boundaries of the TOE in general terms both in a physical and a logical way.

3.4. The above results have enabled the certifiers to conclude that the ST has met the requirements for the TOE Description, and consider it suitable to be used (in part) as a basis for the evaluation.

Security Environment (ASE_ENV.1)

3.5. The statement of the TOE security environment adequately identified and explained the assumptions about the intended usage of the TOE (and its environment), and the known threats to the protected assets of the TOE (and its environment). There were no identified organisational security policies with which the TOE had to comply with.

3.6. The above results have enabled the certifiers to conclude that the ST has met the requirements for the Security Environment, and consider it suitable to be used (in part) as a basis for the evaluation.

ST introduction (ASE_INT.1)

3.7. The ST introduction identified and adequately described the ST and the TOE. It contained an ST overview in narrative form, and contained a CC conformance claim to meet the predefined assurance level of EAL4.

3.8. The above results have enabled the certifiers to conclude that the ST has met the requirements for the ST introduction, and consider it suitable to be used (in part) as a basis for the evaluation.

Security Objectives (ASE_OBJ.1)

3.9. The statement of the TOE and environmental security objectives were adequately defined, and were clearly traceable back to the identified threats countered by the TOE, and the assumptions on the TOE and its environment. The security objectives rationale demonstrated that the security objectives were suitable to counter the identified threats and cover the identified assumptions.

3.10. The above results have enabled the certifiers to conclude that the ST has met the requirements for the Security Objectives, and consider it suitable to be used (in part) as a basis for the evaluation.

Protection Profile (PP) Claims (ASE_PPC.1)

3.11. The ST did not claim conformance to any PPs.

IT Security Requirements (ASE_REQ.1)

3.12. The statement of the TOE Security Functional Requirements (SFRs) correctly identified the SFRs drawn from CC Part 2 (ref [4]), and the TOE Security Assurance Requirements (SARs) for EAL4 from CC Part 3 (ref [5]). The justification for using the pre-defined EAL4 assurance package was sufficient.

3.13. Security requirements on the IT environment were identified. All operations on the IT security requirements were completed, and the relevant dependencies were satisfied. The security requirements rationale demonstrated that the IT security requirements were suitable to meet the security objectives. It also demonstrated that the set of IT security requirements together forms a mutually supportive and internally consistent whole.

3.14. The above results have enabled the certifiers to conclude that the ST has met the requirements for the IT Security Requirements, and consider it suitable to be used (in part) as a basis for the evaluation.

Explicitly stated IT Security Requirements (ASE_SRE.1)

3.15. The ST did not contain any explicitly stated IT security requirements.

TOE Summary Specification (ASE_TSS.1)

3.16. The TOE summary specification (TSS) adequately described the IT security functions and the assurance measures of the TOE. The TSS traced and clearly mapped all IT security functions to the TOE security functional requirements demonstrating that all TOE security functions contribute to the satisfaction of at least one TOE security functional requirement.

3.17. The IT security functions were informally specified to an appropriate level of detail. Security mechanisms were easily traced back to the relevant TOE security functions.

3.18. The TOE summary specification rationale demonstrated that the IT security functions were suitable to meet the TOE security functional requirements, and that the combination of IT security functions work together to also satisfy the TOE security functional requirements. The rationale also demonstrated, aided by a mapping, that the assurance measures met the assurance requirements for EAL4.

3.19. The TOE summary specification stated that there were no IT security functions that are realised by a probabilistic or permutational mechanism. It is noted that digital signature verification was identified in the specification of the Security Functional Requirements, and that a strength of function claim for cryptographic operations is not required, as DSD determines the appropriateness of cryptographic operations for Australian Government use.

3.20. The above results have enabled the certifiers to conclude that the ST has met the requirements for the TOE Summary Specification, and consider it suitable to be used (in part) as a basis for the evaluation.

ST Evaluation Result

3.21. The certifiers consider that the above results have demonstrated that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the evaluation.

Common Criteria EAL4 Security Assurance Requirements

1.22 EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behaviour. Assurance is additionally gained through an informal model of the TOE security policy.

1.23 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

1.24 EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures. The results of this evaluation are discussed below.

Configuration Management (ACM)

3.25. Configuration management is one method or means for establishing that the functional requirements and specifications are realised in the implementation of the TOE. Configuration management meets these objectives by requiring discipline and control in the processes of refinement and modification of the TOE and the related information. Configuration management systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking any changes, and by ensuring that all changes are authorised.

Configuration Management (CM) Capabilities (ACM_CAP.4)

3.26. The TOE reference was assessed to be unique to each version of the TOE. In addition, the TOE was correctly labelled with its reference.

3.27. The CM documentation included a configuration list, CM plan, and an acceptance plan, and adequately described the method used to uniquely identify the configuration items. The configuration list correctly described the configuration items of the TOE. The CM plan adequately described how the CM system was being used to uniquely identify the configuration items.

3.28. The CM system was demonstrated to operate in accordance with the CM plan, and that all configuration items were being effectively maintained under the CM system. The CM system provided adequate measures to ensure that only authorised changes are made to the configuration items. The CM system appropriately supported the generation of the TOE.

3.29. An acceptance plan was also provided that adequately described the procedures used to accept modified or newly created configuration items as part of the TOE.

3.30. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in November 2000.

3.31. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Configuration Management Capabilities assurance component for EAL4.

Configuration Management Automation (ACM_AUT.1)

3.32. The CM system provided an adequate automated means by which only authorised changes were made to the TOE implementation representation (i.e. the source code), and an automated means to support generation of the TOE.

3.33. The CM plan adequately described the automated tools and how they are used in the CM system.

3.34. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in November 2000.

3.35. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Configuration Management Automation assurance component for EAL4.

Configuration Management Scope (ACM_SCP.2)

3.36. The CM documentation correctly showed that the CM system tracks the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

3.37. The CM documentation adequately described how the configuration items were being tracked by the CM system.

3.38. The above determinations were also supported by the results of a site visit to the development

environment conducted by the evaluators in November 2000.

3.39. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Configuration Management Scope assurance component for EAL4.

Delivery and Operation (ADO)

3.40. This aspect of the evaluation examines the requirements for the measures, procedures, and standards concerned with secure delivery, installation and operational use of the TOE, ensuring that the security protection offered by the TOE is not compromised during transfer, installation, start-up and operation.

Delivery (ADO_DEL.2)

3.41. The delivery documentation adequately described all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

3.42. The procedures and technical measures for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site, were adequately described. The delivery documentation also adequately described how the various procedures allowed for the detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

3.43. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Delivery assurance component for EAL4.

Installation, Generation and Start-Up (ADO_IGS.1)

3.44. The operational documentation adequately described the steps necessary for secure installation, generation, and start-up of the TOE.

3.45. It is noted that a qualified VeriSign engineer performs the installation and generation of the TOE, and that the installation was witnessed by the evaluators to verify the documented procedures.

3.46. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Installation, Generation and Start-Up assurance component for EAL4.

Development (ADV)

3.47. This aspect of the evaluation examines the requirements for the stepwise refinement of the TSF from the TOE summary specification in the ST down to the actual implementation. Each of the resulting TSF representations provide information to help determine whether the functional requirements of the TOE have been satisfied.

Functional Specification (ADV_FSP.2)

3.48. The functional specification informally described the TSF and its external interfaces, including a description on the purpose and method of use of all external TSF interfaces, while also providing complete details of all effects, exceptions and error messages.

3.49. The functional specification was found to be internally consistent and to completely represent the TSF. This was supported by a rationale justifying that the TSF did in fact completely represent the TSF.

3.50. Furthermore, the functional specification was determined to be an accurate and complete instantiation of the TOE security functional requirements.

3.51. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Functional Specification assurance component for EAL4.

High-Level Design (ADV_HLD.2)

3.52. The presentation of the High-Level Design was informal and found to be internally consistent. It adequately described the structure of the TOE in terms of sub-systems, and the security functionality provided by each sub-system of the TSF.

3.53. The TSF does not rely on any protection mechanisms implemented by the underlying hardware, firmware or software of the TOE.

3.54. The High-Level Design identified all interfaces to the sub-systems of the TSF, together with an identification of the interfaces that are externally visible. The purpose and method of use of all these interfaces were adequately described, including details of the effects, exceptions and error messages. Finally, the separation of the TOE into TSP-enforcing and other sub-systems was correctly described.

3.55. Furthermore, the High-Level Design was determined to be an accurate and complete instantiation of the TOE security functional requirements.

3.56. As a result of the above determinations, the certifiers conclude that the TOE fully meets the High-Level Design assurance component for EAL4.

Low-Level Design (ADV_LLD.1)

3.57. The presentation of the Low-Level Design was informal and found to be internally consistent. The Low-Level Design adequately described the TSF in terms of modules, and the purpose of each of these modules. The interrelationships between the modules in terms of provided security functionality and dependencies on other modules were also adequately described.

3.58. The Low-Level Design described how each TSP-enforcing function was provided, and identified all interfaces to the modules of the TSF, including all interfaces that are externally visible. The purpose and method of use of all these interfaces were adequately described, including details of the effects, exceptions and error messages. Finally, the separation of the TOE into TSP-enforcing and other modules was correctly described.

3.59. Furthermore, the Low-Level Design was determined to be an accurate and complete instantiation of the TOE security functional requirements.

3.60. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Low-Level Design assurance component for EAL4.

Implementation (ADV_IMP.1)

3.61. The developer provided the entire source code for the implementation representation. The evaluators chose a subset corresponding to approximately 47% of the TSF.

3.62. The implementation representation was found to unambiguously define the TSF to a level of detail such that the TSF could be generated without any further design decisions. In addition, the implementation representation was confirmed to be internally consistent.

3.63. Furthermore, the implementation representation was determined to be an accurate and complete instantiation of the TOE security functional requirements.

3.64. As a result of the above determinations, the certifiers conclude that the TOE fully meets the

Implementation assurance component for EAL4.

Representation Correspondence (ADV_RCR.1)

3.65. An analysis of the correspondence between all adjacent pairs of the TSF representation was provided. This analysis demonstrated that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation, which was the implementation.

3.66. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Representation Correspondence assurance component for EAL4.

Security Policy Model (ADV_SPM.1)

3.67. The developer provided a TOE Security Policy (TSP) model that was presented informally, and described the rules and characteristics of all the relevant security policies. A rationale was included that appropriately demonstrated that it was complete and consistent with all of the identified security policies.

3.68. The developer also demonstrated that the correspondence between TSP model and the functional specification showed that all of the security functions in the functional specification were consistent and complete with respect to the TSP model

3.69. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Security Policy Model assurance component for EAL4.

Guidance Documents (AGD)

3.70. This aspect of the evaluation examines the requirements directed at the understandability, coverage and completeness of the operational documentation provided by the developer. This documentation, which provides two categories of information, for users and administrators, is an important factor in the secure operation of the TOE.

Administrator Guidance (AGD_ADM.1)

3.71. The administrator guidance clearly described the administrative functions and interfaces, instructions on how to administer the TOE securely, all assumptions regarding user behaviour

that are relevant to the secure operation of the TOE, all security parameters under the control of the administrator, and each type of security-relevant event relative to the administrative functions being performed, including changing the security characteristics of entities under control of the TSF.

3.72. The guidance also contained appropriate warnings about functions and privileges that need to be controlled in a secure environment, and indicated secure values if applicable.

3.73. The administrator guidance described all security requirements for the IT environment that were relevant to an administrator, and was consistent with all other documentation supplied for the evaluation.

3.74. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Administrator Guidance assurance component for EAL4.

User Guidance (AGD_USR.1)

3.75. The user guidance clearly described the functions and interfaces available to the non-administrative users of the TOE, and the use of user-accessible security functions provided by the TOE. Appropriate warnings about user-accessible security functions and privileges that should be controlled in a secure processing environment were also described.

3.76. All user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of the TOE security environment, were clearly presented.

3.77. The user guidance described all security requirements for the IT environment that were relevant to a user, and was consistent with all other documentation supplied for the evaluation.

3.78. As a result of the above determinations, the certifiers conclude that the TOE fully meets the User Guidance assurance component for EAL4.

Life-Cycle Support (ALC)

3.79. This aspect of the evaluation examines the requirements for assurance through the adoption of a well-defined life-cycle model for all the steps of the TOE development, correct use of tools and techniques, and the security measures used to protect the development environment.

Development Security (ALC_DVS.1)

3.80. The development security documentation adequately described all the physical, procedural, personnel, and other security measures that were necessary to protect the confidentiality and the integrity of the TOE design and implementation in its development environment. It also provided evidence that these security measures were being followed during the development and maintenance phases of the TOE.

3.81. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in November 2000.

3.82. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Development Security assurance component for EAL4.

Life-Cycle Definition (ALC_LCD.1)

3.83. The life-cycle definition documentation adequately described the model used to develop and maintain the TOE, and how the model provides the necessary control measures used during these phases.

3.84. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in November 2000.

3.85. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Life-Cycle Definition assurance component for EAL4.

Tools and Techniques (ALC_TAT.1)

3.86. All development tools use during the implementation phase were determined to be well defined. The documentation associated with these tools unambiguously defined the meaning of all statements, including the implementation-dependent options, used in the implementation.

3.87. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in November 2000.

3.88. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Tools and Techniques assurance component for EAL4.

Tests (ATE)

3.89. Testing helps to establish that the TOE security functional requirements are met. Testing provides assurance that the TOE satisfies at least the TOE security functional requirements, although it cannot establish that the TOE does no more than what was specified. Testing at this level of assurance is also directed towards the internal structure of the TSF, such as the testing of subsystems (identified in the High-Level Design) against their specification.

Coverage (ATE_COV.2)

3.90. The test coverage analysis adequately demonstrated the correspondence between the tests identified in the test documentation and the TSF described in the functional specification, and that the coverage was complete.

3.91. The developer's functional testing covered all TSFs specified in the functional specification.

3.92. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Coverage assurance component for EAL4.

Depth (ATE_DPT.1)

3.93. The depth analysis adequately demonstrated that the tests identified in the test documentation were sufficient to demonstrate that the TSF operates in accordance with its high-level design.

3.94. The developer's functional testing covered all sub-systems and sub-system interfaces specified in the high-level design of the TSF.

3.95. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Depth assurance component for EAL4.

Functional Testing (ATE_FUN.1)

3.96. The provided test documentation consisted of test plans, test procedure descriptions, expected test results and actual test results. The documentation identified the security functions that were tested and the goals of each test. The test procedure descriptions described the scenarios for testing each security function. The scenarios did not require that the tests be ordered in any way.

3.97. The expected test results showed the anticipated outputs from the successful execution of these tests, and the test results demonstrated that each security function behaved as specified.

3.98. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Functional Testing assurance component for EAL4.

Independent Testing (ATE_IND.2)

3.99. Independent testing was conducted to confirm that the TOE operates as specified in the documentation supplied for the evaluation. The configuration of the TOE (and its environment) used during testing was consistent with the evaluated configuration, as stipulated in the ST (ref [9]) and the operational guidance (refs [11] - [21]). In addition, an equivalent set of resources was used that were utilised during the developer functional testing of the TSF.

3.100. A 58% sample of the developer tests was selected to verify the developer's test results. All tests executed by the evaluators from the selected sample of developer tests produced the expected results, consistent with the results produced by the developer's own functional testing.

3.101. The evaluators based their own independent testing on the sample identified above, and extended their testing to investigate the behaviour of the certificate request approval process, jurisdiction management, and audit trail functionality. Adhoc testing was also performed where appropriate. All tests were sufficiently documented to enable the tests (and their results) to be reproducible.

3.102. The overall outcome of the evaluator testing effort showed that the TOE security functions have been implemented correctly in the TOE. A summary of the evaluator testing effort for this component can be found in section 5.6 of the ETR (ref [10]).

3.103. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Independent Testing assurance component for EAL4.

Vulnerability Assessment (AVA)

3.104. This aspect of the evaluation examines the requirements directed at the identification of exploitable vulnerabilities. Specifically, it addresses those vulnerabilities introduced in the construction, operation, misuse, or incorrect configuration of the TOE.

Misuse (AVA_MSU.2)

3.105. The guidance documentation appropriately identified all possible modes of operation of the TOE, including operation following failure or operational error, their consequences and implications for maintaining secure operation. The guidance documentation was also determined to be complete, clear, consistent and reasonable.

3.106. The guidance documentation appropriately listed the assumptions about the intended environment, and all the requirements for external security measures. The developer provided analysis of the guidance documentation demonstrated that it was complete. The evaluators confirmed that this analysis showed that relevant guidance is provided for secure operation in all modes of operation of the TOE.

3.107. As the TOE is installed and configured by a qualified VeriSign engineer, the evaluators repeated some of the configuration procedures and witnessed the installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation, and that all insecure states could be detected using this documentation.

3.108. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Misuse assurance component for EAL4.

Strength of Function (AVA_SOF.1)

3.109. The Security Target did not make strength of function claim.

3.110. The single cryptographic operation (i.e. digital signature verification) was evaluated separately by DSD as the National Communications Security Authority. It was determined to be appropriate for Australian Government use.

Vulnerability Analysis (AVA_VLA.2)

3.111. The developer provided a vulnerability analysis searching for ways in which a user can violate the TSP. The documentation showed that none of the identified vulnerabilities were exploitable in the intended environment for the TOE. It also justified that the TOE is resistant to obvious penetration attacks.

3.112. The evaluators performed their own independent vulnerability analysis and conducted penetration testing to ensure that the identified vulnerabilities had been addressed.

3.113. Additional testing did not identify any vulnerabilities that were not considered by the developer. The overall outcome of the evaluator penetration testing effort showed that there are no exploitable vulnerabilities of the TOE in its intended environment.

3.114. Finally, the evaluators determined that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential. A summary of the evaluator testing effort for this component can be found in section 5.7 of the ETR (ref [10]).

3.115. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Vulnerability Analysis assurance component for EAL4.

Specific Functionality

3.116. The TOE Security Functional Requirements and the TOE Security Functions provided by Processing Center are specified in sections 5.1 and 6.1 of the Security Target (ref [9]) and summarised in Appendix B of this report.

3.117. The evaluators found that the product provided the TOE security functionality and satisfied the TOE Security Functional Requirements, as specified in the Security Target (ref [9]).

Discussion of Unresolved Issues

3.118. At the conclusion of the evaluation there were no unresolved issues requiring the consideration of the certifiers.

General Observations

3.119. The certifiers would like to acknowledge the invaluable assistance provided by VeriSign staff during the evaluation. Without the due attention to problems found, and their technical assistance, the process could not have succeeded in the same time frame.

3.120. Further, the certifiers would like to acknowledge the efforts of CMG Admiral in ensuring prompt delivery of the Evaluation Technical Report for certification.

Chapter 4 Conclusions

Certification Result

4.1 After due consideration of the Evaluation Technical Report (ref [10]) produced by the evaluators and the conduct of the evaluation as witnessed by the certifiers, the Australasian Certification Authority has determined that Processing Center has met the requirements of the Common Criteria EAL4 Assurance level.

Scope of the Certificate

4.2 This certificate applies only to version 3.0 of the product. This certificate is only valid when the Processing Center product correctly comprises the designated components. These components are identified in Appendix C and should be verified on receipt of the delivered product.

Recommendations

4.3 The following recommendations involve information highlighted by the evaluators during their analysis of the developer's deliverables, during the conduct of the evaluation, and during the additional activities performed by the Certification Group.

4.4 Processing Center should only be used in accordance with the intended environment described in section 3.1 (Assumptions) of the Security Target (ref [9]). Importantly, **the evaluated configuration of the TOE has only included one ESA jurisdiction.** Multiple ESA jurisdictions for Australian Government environments are only to be implemented upon approval from DSD.

Functionality not part of the Evaluated Configuration

4.5 The Processing Center software package is delivered with several other applications that are used to support the operation of Processing Center. Not all of these applications have been included in this evaluation. The evaluated configuration has been specified in Appendix C of this Report. Functionality and/or components that have not been included in this evaluation of Processing Center are as follows:

1. Universal Service Center
2. Local Hosting
3. Automated Administration
4. Passcode Authentication
5. Go Secure! for Web Applications with the Personal Trust Agent
6. Certificate management tools such as Certificate Parsing Module and Certificate Validation Module
7. Online Certificate Status Protocol (OCSP)
8. OnSite Key Management Service
9. Go Secure! for Microsoft Exchange
10. Go Secure! for Check Point
11. Go Secure! for Lotus Notes
12. Identrus
13. Secure Server OnSite
14. Global Server OnSite
15. OnSite for IPsec
16. Remote ESC Interface
17. Billing system interface.

4.6 Potential users of the TOE are advised that the evaluation of Processing Center has excluded the security functionality required to protect the communications path between the OnSite Administrator and the front-end web server. In practice, this protection is often accomplished by the use of a Secure Sockets Layer (SSL) implementation in an appropriate web browser. While DSD does not endorse the use of SSL as a suitable mechanism for the provision of trusted communications between client and server, under specific circumstances (and in conjunction with a threat and risk assessment) the approval of SSL implementations may be suitable for some Australian Government environments or installations. **Australian Government users are strongly recommended to contact DSD for further advice on the applicability of using SSL implementations in their particular environments.**

4.7 The Certification Group recommends that an appropriate implementation of SSL be evaluated so that it can be used in conjunction with the Processing Center to implement a trusted path for protecting OnSite Administrator communications.

4.8 Potential users are also advised that the evaluation of Processing Center has excluded the security functionality required to generate and store the public and private keys. In practice, the Processing Center product can operate with a variety of tokens compliant to specific interfacing standards (e.g. Public Key Certificate Standard (PKCS) #11). However, no specific tokens were included in the evaluated configuration of the Processing Center. **Potential users are advised to contact DSD for further advice on the use of any cryptographic tokens to be used in conjunction with the Processing Center.**

4.9 The Certification Group recommends that an appropriate token be evaluated so that it can be used in conjunction with the Processing Center to implement secure key generation and secure key storage.

Cryptographic Requirements for Australian Government Use

4.10 The Processing Center evaluation did not contain any cryptographic operation other than the verification of the digital signatures. This operation utilises the RSA algorithm with 512 or 1024 bit key lengths, and is the only cryptographic operation implemented by the Processing Center to be appropriate for Australian Government use.

4.11 Administrators of the TOE should be aware of these restrictions, and ensure the correct versions have been supplied with the evaluated product, and that the configurations of any cryptographic parameters are in line with the above requirement.

4.12 Furthermore, **Commonwealth Government users must ensure that key pairs and certificates are issued by a Gatekeeper compliant product operated by an GPKA-endorsed Certification Authority. Further advice can be obtained by contacting DSD.**

4.13 All cryptographic-relevant material is to be the subject of rigorous levels of physical and technical control as defined in ACSI 57 (ref [24]). Commonwealth Government users are encouraged to contact DSD for further assistance in this area.

Pre-installation considerations for Processing Center components

4.14 Administrators should ensure that, prior to installing any Processing Center server component, the hardware has been appropriately sanitised and contains no software other than the required components specified in Appendix C of this Report. **Furthermore, to avoid the introduction of malicious software and viruses on Processing Center enabled servers, it is recommended that the hard drive of each Processing Center component be re-formatted prior to an installation of the operating system.**

4.15 Potential purchasers of Processing Center need to be aware that the operational documentation is aimed at the administrator level. In addition, **the installation of the product is only to be undertaken by a qualified VeriSign engineer.** It is also recommended that any major upgrade (or serious maintenance) of the operational product be performed under the strict guidance of qualified VeriSign personnel. Organisations considering undertaking Certificate Authority or Registration Authority responsibilities need to have a thorough understanding of the technical issues involved in establishing and maintaining a PKI. **Commonwealth Government agencies wishing to implement a PKI are strongly encouraged to contact DSD for further assistance.**

4.16 Operational documentation is delivered in hard and soft copy with the CD-ROM. Administrators of the Processing Center are advised to ensure that the soft copies of the operational documentation (refs [11] - [21]) are identical to the supplied hard copies. If not, the administrators should report the discrepancy back to VeriSign immediately.

Operational considerations

4.17 The Processing Center has four types of administrators. The Master Service Administrator (MSA) and Enterprise Service Administrator (ESA) administer the back-end administration of the Processing Center (i.e. the Certificate Authority). The OnSite Administrator (OSA) administers the front-end functionality of OnSite (i.e. the Registration Authority). The Enterprise Service Center Administrator (ECSA) administers Processing functionality where satellites have been set up to act as a Certification Authority for their own customers. **The evaluation of Processing Center did not include the functionality offered by ECSAs, and therefore should not be used for Australian Government environments.**

4.18 In addition, another type of administrator is required in order to operate the TOE in its evaluated configuration. This administrator is referred to as the **System Operator** and is primarily responsible for the management of the availability and reliability of the Processing Center components, and the configuration of customer data.

4.19 Personnel undertaking Master Service Administrator and Enterprise Service Administrator duties should be aware that two administrators are required to approve administrative certificates for OnSite Administrators or new jurisdictions. This approval procedure should be clearly stated in the organisation's System Security Plan and/or operational policy governing the management of the PKI.

4.20 Administrators need to ensure that the communications links to and from the Processing Center components (within the protected network) are adequately protected. A failure of a communications link with a front or back-end web server could cause a delay for users or applications in requesting Processing Center services. Please note that the secure usage assumptions outlined in the Security Target (ref [9]) stipulate that appropriate measures must be taken to reduce the likelihood of these types of failure from occurring.

4.21 An exhaustion of disk space may produce unexpected behaviour from the TOE. Importantly, this situation may cause the TOE to cease recording security related information in the audit logs. **Administrators must ensure that there is an adequate amount of available disk space left on system disks, as specified by the evaluated configuration in the Security Target (ref [9]). Administrators should ensure that events in the event log are not automatically overwritten, unless their security policy has deemed it appropriate.**

4.22 Administrators of the TOE need to be aware that the product does not provide protection mechanisms for the audit logs, access control data, and certificate details present on the database server, other than the operating system security offered by Solaris. Rather, the database server is assumed to be protected by the enforcement of the environmental measures, such as access to the major TOE components is restricted to authorised personnel only. Therefore, **administrators must ensure that administrative privilege is restricted to authorised users of all PKI components. Administrators should also ensure that appropriate Solaris password policies are being enforced on Processing Center enabled systems, including the database server.**

Verification of End Users and OnSite Administrators

4.23 Processing Center does not provide a mechanism to validate the credentials supplied to the OnSite Control Center component while processing a new certificate request, an issue common to other PKI implementations. **Staff undertaking PKI administrator duties should ensure that appropriate procedural measures are in place to verify the identity of an end user when the need arises.** Conversely, appropriate procedures should also be in place for end users wishing to verify the identity of their OnSite Administrators, in order to prevent social engineering attacks on end-users of the TOE.

Importance of a Certificate Practice Statement in a Hierarchical PKI

4.24 The Certificate Practice Statement must define the policy and procedures for users of the PKI to regularly confirm the authenticity of the other components in the PKI hierarchy. This is particularly important when a subordinate Certification Authority has been revoked, and end users of the subordinate Certification Authority need to confirm whether their Certification Authority can still be trusted. **It is the responsibility of PKI administrators to ensure that Certificate Revocation Lists (CRLs) are made available in a timely manner, to end users and applications that are using certificates issued by Certificate Authorities in the PKI hierarchy, in accordance with a Certificate Practice Statement.**

Availability considerations for Processing Center

4.25 Administrators should note that the Processing Center product does not counter any external threats to the availability of the front-end web server. Since the functionality of the TOE allows users to inter-operate with a wide variety of applications and technologies, it may be possible for an external party to launch a denial of service attack against the front-end web server. While this type of threat does not invalidate the security objectives of the TOE, **administrators should ensure that adequate measures are in place to protect the front end web server and its network from denial of service or other types of availability attacks coming from outside the protected network.** Furthermore, Australian Government users should contact DSD for assistance on implementing appropriate countermeasures to protect their networks from such attack.

4.26 Further to the recommendation discussed above, the Security Target (ref [9]) recommends that a firewall be correctly positioned to protect the front-end web server from external attack. **Australian Government users are strongly encouraged to protect the TOE from external attack by connecting the public network interface of the front-end web server to the external (untrusted) network via an appropriately assured firewall.**

Verification of Certificate Authority (CA) certificates

4.27 **It is the responsibility of PKI end-users to ensure their certificate is from a trustworthy source, by comparing the fingerprint of the CA that signed their certificate with the fingerprint of that CA's certificate obtained by another means**. Organisations undertaking CA responsibilities should ensure that appropriate mechanisms are in place for users to retrieve the CA fingerprint either by phone, fax, or letter. In the case of hierarchical CAs, these organisations should ensure that users have the option to verify the certificate up to the root CA so that complete trust

can be established in the PKI.

Reflecting the Evaluated Version

4.28 For the TOE to be compliant with its Security Target (ref [9]), the TOE configuration must conform to the following specifications:

a) the hardware and software required for the TOE must be installed and configured as specified in the Processing Center Installation Guide (ref [14]) and the Architecture and Setup Guide (ref [17]). As these documents state, the installation must be done by a qualified VeriSign PSO (Professional Services Organisation) Engineer

b) the TOE operating environment must meet the preferred security requirements specified in the Security and Audit Reference guide (ref [18]).

Appendix A References

[1] Evaluation Memorandum No. 1 - Description of the AISEP
Defence Signals Directorate
EM 1, Issue 1.1, March 1997

[2] Evaluation Memorandum No. 2 - The Licensing of AISEFs
Defence Signals Directorate
EM 2, Issue 1.0, August 1994

[3] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model (CC)
CCIMB-99-031, Version 2.1, August 1999

[4] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements
CCIMB-99-032, Version 2.1, August 1999

[5] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements
CCIMB-99-033, Version 2.1, August 1999

[6] Common Methodology for Information Technology Security Evaluation (CEM)
CEM-99/045, Version 1.0, August 1999

[7] Manual of Computer Security Evaluation Part I - Evaluation Procedures
Defence Signals Directorate
EM 4, Issue 1.0, April 1995
(EVALUATION-IN-CONFIDENCE)

[8] Manual of Computer Security Evaluation Part II - Evaluation Techniques and Tools
Defence Signals Directorate
EM 5, Issue 1.0, April 1995
(EVALUATION-IN-CONFIDENCE)

[9] VeriSign Processing Center Version 3.0 Security Target
VeriSign Inc.
Version 2.0, March 2001
(COMMERCIAL-IN-CONFIDENCE)

[10] VeriSign Processing Center Version 3.0 Evaluation Technical Report

CMG Admiral
Issue 1.0, March 2001.
(EVALUATION-IN-CONFIDENCE, COMMERCIAL-IN-CONFIDENCE)

[11] VeriSign OnSite Introduction
VeriSign Inc.
DOC-GVS-PRD-INT-0001
Issue V2, 2000

[12] VeriSign OnSite Administrators Handbook
VeriSign Inc.
DOC-GVS-ONS-INS-0001
Issue V3, 2001

[13] VeriSign Processing Center Introduction
VeriSign Inc.
DOC-AFF-PRC-INT-0001
Issue V1, 2000

[14] VeriSign Processing Center Installation Guide
VeriSign Inc.
DOC-AFF-PRC-ICG-0001
Issue V2, 2000

[15] VeriSign Processing Center User's Guide
VeriSign Inc.
DOC-AFF-PRC-GID-0002
Issue V4, 2001

[16] VeriSign Processing Center User's Guide Appendix A - Switch Jurisdiction Feature
VeriSign Inc.
DOC-AFF-PRC-GID-0002
Issue V4, 2000
(no longer distributed)

[17] VeriSign Processing Center Architecture and Setup Guide
VeriSign Inc.
DOC-AFF-PRC-ICG-0003
Issue V2, 2001

[18] VeriSign Processing Center Security and Audit Requirements Guide
VeriSign Inc.
DOC-AFF-PRC-GID-0003
Issue V3, 2000

[19] VeriSign Enterprise Service Center Administrator's Guide
VeriSign Inc.
DOC-AFF-SVC-GID-0006
Issue V1, 2000

[20] VeriSign Error Codes and Messages
VeriSign Inc.
DOC-ENT-ONS-ERR-0001
Issue V3, 2000

[21] VeriSign Processing Center Key Ceremony Reference Guide
VeriSign Inc.
DOC-AFF-PRC-GID-0004
Issue V2, 2000

[22] Security Policy Model for VeriSign Processing Center 3.0
VeriSign Inc.
5067/E/5
Issue 2.0, March 2001

[23] Information Technology Security Evaluation Methodology (ITSEM)
Commission of the European Communities
Version 1.0, 10 September 1993

[24] Australian Communications-Electronic Security Instructions (ACSI) 57 (B),
Guidelines for the Use of Cryptographic Systems listed in section VIII of the Defence Signals Directorate Evaluated Products List (EPL)
Bravo Edition, Defence Signals Directorate

[25] Arrangement on the Recognition of Common Criteria Certificates (in the field Information Technology Security)
Available from: http://www.commoncriteria.org/registry/ccra-final.html
May 2000

Appendix B Summary of the Security Target

Security Target

B.1 A brief summary of the Security Target is given below. Potential purchasers should attempt to obtain a copy of the full Security Target to ensure that the TOE security functionality satisfies the requirements of their security policy.

Security Objectives for the TOE

B.2 Processing Center has the following IT security objectives:

a) The TOE must identify and authenticate each user before granting access to TOE security functions.

b) The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes.

c) The TOE must provide a means to generate and issue digital certificates in accordance with accepted PKI standards.

d) The TOE must provide facilities to recover from inappropriate use.

e) The TOE must provide functionality that enables administrators to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

f) The TOE must ensure that only an administrator authorized to manage a particular jurisdiction and with the proper role (Certificate Management) can cause a certificate request for that jurisdiction to be signed by the appropriate CA key.

Security Objectives for the Environment

B.3 Processing Center has the following environmental objectives:

a) Those responsible for the TOE must ensure that the TOE is installed and operated in accordance with the developer's instructions including the implementation of the preferred security requirements as defined in (ref [18]).

b) Those responsible for the TOE must ensure that appropriate guidance is supplied to subscribers as to the preferred method for storing and protecting their private key.

c) Those responsible for the TOE must ensure that users are provided with information as to how to generate a key pair that can be used to create their certificate.

d) Those responsible for the TOE must ensure that the root CA keys cannot altered or observed.

e) Those responsible for the TOE must ensure that acceptable quality root CA keys are always used by the TOE.

f) Those responsible for the TOE must ensure that an acceptable method of destroying root CA keys is available when they are no longer required by the TOE.

g) Those responsible for the TOE must ensure that measures are in place to ensure that CRLs are made available in a timely manner to users and applications that are using certificates issued by the PKI hierarchy. Users are responsible for the correct use of such CRLs in accordance with policies and procedures issued by the operators of the TOE.

h) Those responsible for the TOE must ensure that measures are in place to ensure that the time source used by the TOE for time stamps is accurate.

i) Those responsible for the TOE must ensure that appropriate policies are in place to allow the administrators to identify applicants for certificates and to determining their eligibility. These procedures may be tailored to the needs of each jurisdiction.

j) Those responsible for the TOE must ensure that appropriate policies are in place to ensure that administrators have appropriate procedures for revoking certificates. These procedures would indicate who can order a certificate revoked and how any such order is authenticated. These procedures may be tailored to the needs of each jurisdiction.

k) Those responsible for the TOE must ensure that measures are in place to deliver to the TOE the Administrators commands in a secure manner that enables the TOE to reliably determine who the commands originated from and ensures the integrity of these commands.

Secure Usage Assumptions

B.4 The following assumptions relate to the operation of the TOE:

a) It is assumed that the TOE is operating in an environment that has been secured in accordance with the guidance contained within (refs [18], [14] and [17]).

b) It is assumed that there is an appropriate method, independent of the TOE, available to generate and destroy cryptographic key-pairs for use with the TOE.

c) It is assumed that a user will take appropriate measures to protect his / her private key which may include the storage of the private key on a smartcard or other secure storage device.

d) It is assumed that MSA and ESAs are trusted to perform administration functions for all their subordinate jurisdictions.

e) It is assumed that the private CA root keys are securely stored and cannot be copied, modified or deleted.

f) It is assumed that measures are in place to ensure that CRLs are made available in a timely manner to users and applications that are using certificates issued by the PKI hierarchy. Users are responsible for the correct use of such CRLs in accordance with policies and procedures issued by the operators of the TOE.

g) It is assumed that measures are in place to provide the TOE with a reliable source of current time information suitable for use in a time stamp.

h) It is assumed that administrators have an appropriate policy in place to confirm the identity and eligibility of users before approving their requests for certificates or revoking a certificate in response to its owners request.

i) It is assumed that measures are in place to deliver to the TOE the Administrators commands (eg name value pairs) in a secure manner that enables the TOE to reliably determine who the commands originated from and ensures the integrity of these commands.

Threats addressed by the TOE

B.5 The following threats are addressed by the TOE:

a) An unauthorised person may attempt to alter a users certificate.

b) An unauthorised person may attempt to create or alter the CA's certificate.

c) An unauthorised person may attempt to revoke a certificate or disable a jurisdiction.

d) An administrator may create an inappropriate Jurisdiction.

e) Attempts by unauthorised persons to use the functionality of the TOE may not be detected.

f) An end user may obtain a signed certificate containing information contrary to the policy of their jurisdiction.

g) An end user may obtain a certificate signed within the context for a jurisdiction of which they are not a member.

h) An OnSite Administrator may attempt to sign a certificate within the context of another jurisdiction.

i) Inappropriate issuing of certificates by an administrator may not be detected.

j) Certificates issued inappropriately by an administrator may not be able to be identified and revoked.

Threats addressed by the TOE Environment

B.6 There are no identified threats to be addressed by the TOE Environment.

Organisational Security Policies

B.7 There are no identified organisational security policies relevant to the operation of the TOE.

Summary of TOE Security Functional Requirements

The TOE security functional requirements (SFRs) are tabulated below. Full description and explanation of these SFRs can be found in section 5.1 of the Security Target (ref [9]).

Class FAU: Audit

FAU_GEN.1 Audit data generation

FAU_GEN.2 User identity association

FAU_SAR.1 Audit Review

FAU_SAR.2 Restricted Audit Review

FAU_SAR.3 Selectable Audit Review

Class FCS: Cryptographic Support

FCS_COP.1 Cryptographic operation

Class FDP: User Data Protection

FDP_ACC.1 Subset access control

FDP_ACF.1 Security attribute access control

FDP_ITC.1 Import of user data without security attributes

Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

FIA_UID.1 Timing of identification

FIA_UAU.1 Timing of authentication

Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

FMT_MSA.1 Management of security attributes

FMT_MSA.2 Secure security attributes

FMT_MSA.3 Static attribute initialisation

FMT_MTD.1 Management of TSF data

FMT_SMR.1 Security management roles

Security Requirements for the IT Environment

There are no identified Security Requirements for the IT Environment.

Security Requirements for the Non-IT Environment

There are no identified Security Requirements for the non-IT Environment.

Summary of TOE Security Functionality

B.8 The Processing Center TOE Security Functions (TSFs) are briefly listed below. Full description and explanation of these TSFs can be found in section 6.1 of the Security Target (ref [9]).

B.9 Manage Certificates - OnSite

This TOE Security Function is achieved by the following functions:

MC_ONSITE.1	Process request
MC_ONSITE.2	View request
MC_ONSITE.3	Revoke certificate
MC_ONSITE.4	Generate reports
MC_ONSITE.5	View administrator audit trail
MC_ONSITE.6	View certificate

B.10 Manage Certificates - Processing Center

This TOE Security Function is achieved by the following functions:

MC_PC.1	Process request
MC_PC.2	View request
MC_PC.3	Revoke certificate
MC_PC.4	Generate reports
MC_PC.5	View administrator audit trail
MC_PC.6	View certificate
MC_PC.7	View CA operations audit trail

B.11 Manage OnSite

This TOE Security Function is achieved by the following functions:

M_ONSITE.1	Administrator role wizard
M_ONSITE.2	Download CRL
M_ONSITE.3	End user renewal wizard

B.12 Manage Processing Center

This TOE Security Function is achieved by the following functions:

M_PC.1	Administrator role wizard

B.13 Jurisdiction Management

This TOE Security Function is achieved by the following functions:

JM.1	Process pending jurisdiction requests
JM.2	Create jurisdictions
JM.3	Delete jurisdictions
JM.4	Suspend jurisdictions
JM.5	Reactivate jurisdictions
JM.6	Manage jurisdictions
JM.7	Edit jurisdictions

B.14 End User Functions

This TOE Security Function is achieved by the following functions:

EUF.1	Enrol
EUF.2	Revoke

B.15 Processing Center Initialisation

This TOE Security Function is achieved by the following functions:

PCI.1	Establish first MSA and ESA certificate

B.16 Trusted Path

This TOE Security Function is achieved by the following functions:

TP.1	Establish a trusted path between the boundary of the TOE on the web server and the remainder of the TOE, on the application server.

B.17 System Operations

This TOE Security Function is achieved by the following functions:

SYSO.1	Generate CRL
SYSO.2	Load CA
SYSO.3	System audit

Appendix C Evaluated Configuration

Configuration for Evaluation

C.1 The evaluation was conducted on the VeriSign Processing Center Product, Version 3.0. The evaluated software components of Processing Center have been identified below.

Software

C.2 The software elements of Processing Center are as follows:

a) 1 x CDROM containing the **VeriSign Processing Center Software, Version 3.0**.

b) The evaluated components of the Processing Center are as follows. Note that each of the software components are identified as **version 3.0**:

i) Connection Manager;

ii) Query Manager ;

iii) Bootstrap (HTML & CGI), UpdateCRL (executable) and LoadCA (executable) modules;

iv) Common Gateway Interface (CGI) modules (Perl scripts);

v) Admin Manager Tool (HTML & Javascript files);

vi) OnSite Control Center (HTML & Javascript files);

vii) Certificate Lifecycle (HTML & Javascript files);

viii) Transport processes beamup and beamdown (executables).

Third Party Software

C.3 The third party software used in the evaluation of the Processing Center is as follows. Note that the following software does not contribute to the security functionality implemented by the

Processing Center:

a) Sun Solaris 2.6 (with Patch Cluster 105181-21 or 105181-23)

b) Perl 5.6 (freeware from http://www.perl.com/pub)

c) Oracle 8i Client

d) Oracle Server 8.1.6.0

e) Chrysalis Luna 2/CA/CA3 for Solaris 2.6 (interface software)

f) Netscape Enterprise Server, version 3.5.1 through to iPlanet 4.0

C.4 This evaluation is only valid for the above mentioned version of Processing Center running on the Sun Solaris operating system, with the current recommended patch cluster applied. No other versions, operating systems or third party software are part of the evaluated configuration.

Hardware

C.5 A typical configuration of Processing Center requires the following hardware platforms:

a) Front-End Web Server, which hosts the OnSite Control Center and Certificate Lifecycle components and a CGI module;

b) Application Server, which hosts the Connection Manager, Query Manager and the Bootstrap, UpdateCRL and LoadCA modules;

c) Transport Server, which hosts the transport processes beamup and beamdown;

d) Signing Server, which hosts the signing server process;

e) Database Server, which hosts the database component (not evaluated);

f) Internal-facing Web Server, which hosts the Admin Manager Tool and a CGI module;

g) Three Firewalls, which were not evaluated. These firewalls provide the protection and separation required for the TOE components;

h) Mail/DNS Servers, which were not evaluated. VeriSign recommends the use of two

such servers: one for the de-militarised zone (DMZ) on the front-end, and the other for the back-end. Both should run the latest version of sendmail, BIND 8.x, syslogd, and high-end intrusion detection software. None of this additional software was evaluated.

C.6 Other supporting hardware used in the evaluation of Processing Center includes:

a) Litronics Card Reader;

b) Chrysalis CA^3 Type II PC Card.

C.7 Please note that none of the hardware identified above implements any of the security functionality offered by the Processing Center. The minimum recommended hardware configurations for the above hardware platforms are located in section 2.4.1 of the Security Target (ref [9]).

Procedures for Determining Version of TOE

C.8 In order that an administrator can determine if a delivered product is in fact the evaluated product, the following procedures can be followed in making that determination.

C.9 Once a copy of Processing Center has been received, the administrator should inspect the packaging for any signs of tamper. Any indication of tamper should be reported immediately to VeriSign and the product returned.

C.10 Operational documentation is delivered in hard and soft copy with the CD-ROM. Administrators of the Processing Center are advised to ensure that the soft copies of the operational documentation (refs [11] - [21]) are identical to the supplied hard copies. If not, the administrators should report the discrepancy back to VeriSign immediately.

C.11 It is noted that qualified Professional Services Organisation (PSO) engineers visit each affiliate site to install the TOE and set up the environment. Upon performing this activity, the PSO engineer will verify the authenticity of the delivered CD-ROM with a hash value that was created on the CD-ROM prior to it leaving the VeriSign site.