THALES

Building a future we can all trust

Thales Ottawa Colonnade Site Security Target

Document Information

Document Part Number	002-000537-001
Release Date	18 July 2024

Revision History

Revision	Date	Reason
E	18 July 2024	References updated
D	7 March 2024	References updated
C	11 January 2024	Addressed lab comments
B	11 December 2023	Typo correction
A	17 November 2023	Initial release

Trademarks, Copyrights, and Third-Party Software

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

> The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

> This document shall not be posted on any network computer or broadcast in any media other than on the appropriate certification lists and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

ACRONYMS AND ABBREVIATIONS

Term	Definition
CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
CM	Configuration Management
CPL	Cloud Protection and Licensing
DIS	Digital Identity and Security
EAL	Evaluation Assurance Level
HR	Human Resources
HSM	Hardware Security Module
ISMS	Information System Management System
IT	Information Technology
JIL	Joint Interpretation Library
MSSR	Minimum Site Security Requirements
OSP	Organizational Security Policy
SAR	Security Assurance Requirement
SST	Site Security Target
TOE	Target of Evaluation

REFERENCES

CC References

[CC Part 1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, April 2017, Version 3.1, Revision 5

[CC Part 2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, April 2017, Version 3.1, Revision 5

[CC Part 3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, April 2017, Version 3.1, Revision 5

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, April 2017, Version 3.1, Revision 5

[MSSR] Joint Interpretation Library Minimum Site Security Requirements, February 2020, Version 3.0.

[Site Certification] Supporting Document Guidance Site Certification, October 2007, Version 1.0, Revision 1.

Thales References

[ALC] Thales Ottawa Colonnade Assurance Life Cycle, 18 July 2024, Rev D

[MSSR_Checklist] Thales Ottawa Colonnade MSSR Checklist, 18 July 2024, Rev D

[HDLC] HSM Development Lifecycle, EC.ENG.2.0014, June 2022, Version 11.0

1 Site Security Target Introduction

This section of the Site Security Target (SST) introduction provides the SST reference and the site reference.

1.1 SST Reference

SST Title	Thales Ottawa Colonnade Site Security Target
Version	Rev. E
Date	18 July 2024
Reference	002-000537-001

1.2 Site Reference

Company	Thales Digital Identity and Security (DIS) Cloud Protection and Licensing (CPL)
Site Name	Thales Ottawa DIS CPL
Site Address	20 Colonnade Road, Ottawa, Ontario, Canada

1.3 Site Description

1.3.1 Physical Scope

The physical scope of the site is the development facilities located at the address specified in Section 1.2. This includes the following functional areas:

- Reception
- First floor network and IT support
- Second floor secure development and IT support

1.3.2 Logical Scope

The Thales DIS CPL location at 20 Colonnade Road in Ottawa is dedicated to product development and testing, and the associated supporting services, such as IT management, Human Resources (HR) services and Site Management.

The site supports the following development activities with respect to Hardware Security Module (HSM) products:

- hardware
  - design from identification of requirements to development of prototypes
  - design testing
- firmware/software
  - development from identification of requirements to releasable code
  - testing
  - flaw remediation

The site does not support manufacture of devices, or shipping to customers.

2 Conformance Claim

This SST is conformant with Common Criteria (CC) 3.1 Rev. 5, specifically [CC Part 1] and [CC Part 3] and the evaluation methodology described in [CEM].

The SST is CC Part 3 conformant.

The evaluation of the site includes the following Security Assurance Components (SARs):

- ALC_CMC.4
- ALC_CMS.4
- ALC_DVS.2
- ALC_FLR.2
- ALC_LCD.1
- ALC_TAT.1

The selected assurance components are derived from the assurance level EAL4 augmented with ALC_DVS.2 and ALC_FLR.2 from the Life-cycle Support assurance class. The site is intended to implement security measures effective against an attacker with high attack potential as defined in [CEM], consistent with product claims of AVA_VAN.5.

3 Security Problem Definition

The Security Problem Definition is comprised of the security problems derived from threats against the assets handled by the site and security problems derived from the configuration management requirements. The configuration management covers the integrity of TOE products and the security management of the site.

3.1 Assets

The assets in Table 3-1 are handled at the site.

Table 3-1: Assets Handled at the Site

Asset	Description
Development Data	The site supports the maintenance of electronic information relating to the development such as requirements, specifications, source code, guidance documentation and configuration management information. The integrity and confidentiality of this data must be protected.
Development systems and tools	In support of development activities, the site maintains the IT infrastructure that makes up the development environment and the various tools supported by the environment. The integrity of these systems and tools must be maintained.
Cryptographic Keying Materials	Keying material used in the development of products is produced and maintained at the site. The integrity and confidentiality of this material must be protected.

3.2 Threats

The threats in Table 3-2 are countered by the security features of the site.

Table 3-2: Threats to the Security of the Site

Threat	Description
T.Smart-Theft	An attacker attempts to access sensitive areas of the site for manipulation or theft of assets. The attacker has sufficient time to investigate the site from outside of the controlled boundary. The use of standard equipment for burglary is assumed for this attack.
T.Rugged-Theft	An experienced thief with specialized equipment for burglary, who may be paid to perform a targeted attack, attempts to access sensitive areas and manipulate or steal sensitive assets.
T.Computer-Net	A hacker with substantial expertise and standard equipment, who may be paid, attempts to remotely access sensitive network segments to get access to: • development data with the intention to violate confidentiality and possibly integrity; and/or • development systems and tools with the intention to compromise the development process.

Threat	Description
T.Unauthorised-Staff	Employees or subcontractors are able to access sensitive assets for which they are not authorized access and violate the confidentiality and/or the integrity of these assets.
T.Staff-Collusion	By obtaining support from an employee through extortion or bribery, an attacker attempts to access assets and to violate the confidentiality and/or the integrity of these assets.
T.Attack-Transport	An attacker attempts to access assets during a delivery, and to violate the confidentiality and/or the integrity of these assets.

3.3 Organizational Security Policies (OSPs)

The organizational security policies in Table 3-3 are countered by the security features of the site.

Table 3-3: Organizational Security Policies Addressed by the Site

OSP	Description
P.Config-Mgmt	The configuration management system shall be able to uniquely identify configuration items including parts and assemblies, design documentation and guidance. The configuration management plan includes processes for change control that ensure that only authorized changes are made, processes that ensure tracking and maintenance of development tools, and processes that ensure that flaw remediation is performed, and flaw status is tracked.
P.Flaw-Remediation	The site is responsible for the remediation of security flaws. The procedures include: • Acceptance, triage and prioritization of reports; • Corrections or mitigations; and • Communications of remediation to users.
P.LifeCycle-Doc	The site follows the procedures outlined in the life cycle documentation which includes: • A description of the configuration management system and its usage; • A configuration items list; • Site security procedures; • A description of the development process; • A description of the development tools; and • A flaw remediation process.

3.4 Assumptions

The assumptions in Table 3-4 are made for the operational environment associated with the site.

Table 3-4: Assumptions for the Site

Assumption	Description
A.Secure-Local-IT	Local IT equipment, such as workstations, is connected to the secure IT infrastructure at the Ottawa CPL Colonnade site. The entire system including the network, servers and workstations is managed according to Thales DIS CPL IT policies.
A.Remote.Services	The facilities required to establish a secure link from a remote location to the development site and safeguard the remote IT-infrastructure implement all the necessary security measures to provide a secure environment. Remote access to the IT infrastructure is managed according to Thales DIS CPL IT policies.
A.Project-Security	Thales CPL Information System Management System (ISMS) personnel manage access to project workspaces and the relevant configuration management resources as required for a given project.
A.Trusted-Personnel	Staff assigned to the Thales Ottawa Colonnade site projects are deemed to be trustworthy. This includes local employees, remote employees, employees from other Thales sites, and contracted staff.

4 Security Objectives

This section describes the security objectives of the site. The security objectives address configuration management, flaw remediation, tool usage, and physical, technical and organizational security measures throughout the product lifecycle. This section includes a Security Objectives Rationale. This rationale provides a tracing between the security objectives and the threats and OSPs described in Section 3. It also includes a justification describing how the threats and OSPs are effectively addressed by the security objectives.

4.1 Security Objectives of the Site

The Security Objectives of the Site are described in Table 4-1.

Table 4-1: Security Objectives of the Site

Objective	Description
O.Alarm-Response	The technical and organizational security measures ensure that an alarm is generated before an unauthorized person is able to access sensitive configuration items. After the alarm is triggered, the unauthorized individual must overcome further security measures to access assets. The reaction time of the employees or guards is sufficiently short to prevent a successful attack.
O.Config-Control	The site applies a release procedure for the setup of the development process for new configuration items, including new product releases. In addition, the site has a process to manage and control changes to configuration items, such that changes can be made by authorized personnel only. Automated systems support configuration management.
O.Config- Env	The site tracks and maintains development tools and procedures for their use. These tools are supported by development workstations/systems and servers.
O.Config-Items	The site maintains a configuration management system that assigns a unique identifier to each configuration item. The configuration management system is supported by procedures and guidance.
O.Control-Scrap	The site has measures in place to securely dispose of sensitive documentation, erase electronic media, and destroy sensitive configuration items such that they cannot be used to support an attacker.
O.Flaw-Remediation	The site follows procedures for the remediation of security flaws. The procedures include • Acceptance, triage, and prioritization of reports; • Corrections or mitigations; • Testing of corrections; and • Communications of remediation to users.

Objective	Description
O.Internal-Monitor	The Thales Security and Certifications team meets regularly with development teams. Meetings with development teams are typically held quarterly. These meetings are used to review security incidences, to verify that maintenance measures are applied, and to continually assess risks and security measures. Facilities personnel assess and report on operational, physical, and logical security measures monthly. An internal audit is performed annually to verify the application of the security measures.
O.LifeCycle-Doc	The site follows the procedures outlined in the life cycle documentation which includes: • A description of the configuration management system and its usage; • A configuration items list; • Site security procedures; • A description of the development process; • A description of the governance and life-cycle processes; • A description of the development tools; and • A flaw remediation process.
O.Logical-Access	The site implements a firewall to enforce a logical separation between the internal network and the internet. The firewall ensures that only approved services and approved connections are accepted. The internal network is separated by classification levels. Dedicated networks are physically separated to enforce access control. Access to the development network and related systems is restricted to authorized employees who require access to perform assigned tasks. All users of the IT systems and applications have their own user accounts and passwords. Authentication is enforced by all computer systems.
O.Logical-Operation	All users must authenticate using their unique usernames and passwords. Access to more sensitive information and applications require multi-factor authentication. The IT infrastructure, including the development systems, is properly maintained through the application of software updates, security patches, and malware protections. Backup data is protected in accordance with its classification.
O.Maintain-Security	Technical security measures are established and maintained to ensure site security. The logs related to the access of sensitive systems and data are regularly reviewed. Review of the physical access control system ensures that only authorized employees have access to sensitive areas, and review of the computer/network systems ensure that they are configured as required to ensure the protection of sensitive data and applications.
O.Physical-Access	Access to all areas of the site is controlled through the use of electronic badges and PINs. The access control measures ensure that only authorized employees can access restricted areas. Assets are handled in restricted areas only. The building perimeter is reinforced to prevent and detect unauthorized entry.
O.Staff-Engagement	All employees who have access to sensitive configuration items are subject to vetting regarding security concerns and are required to sign a non-disclosure agreement. All employees are appropriately trained and qualified for their assigned roles.
O.Transfer-Data	Sensitive electronic configuration items (data or documents in electronic form) are cryptographically protected to ensure confidentiality and integrity.

4.2 Security Objectives Rationale

The Security Objectives Rationale traces the Security Objectives to the threats and OSPs that they address, and provides a rationale that demonstrates that all threats and OSPs are effectively addressed by the Security Objectives.

Note that the assumptions do not contribute to the security of the site under evaluation, but describe pre-requisites for the site which are outside of the evaluation.

Table 4-2: Mapping of Threats and OSPs to Security Objectives

Threats and OSPs	Objectives	Rationale
Threats		
T.Attack-Transport	O.Transfer-Data	O.Transfer-Data ensures that the sensitive configuration items are protected when transferred electronically.
T.Computer-Net	O.Internal-Monitor O.Logical-Access O.Logical-Operation O.Maintain-Security O.Staff-Engagement	O.Logical-Access, O.Logical-Operation and O.Staff-Engagement prevent unauthorized access from the internal and external networks, and O.Internal-Monitor and O.Maintain-Security ensure application of these security measures. The threat is effectively mitigated by these objectives.
T.Rugged-Theft	O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Physical-Access	O.Physical-Access and O.Alarm-Response detect unauthorized access; O.Internal-Monitor and O.Maintain-Security ensure application of these security measures. The threat is effectively mitigated by these objectives.
T.Smart-Theft	O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Physical-Access	O.Physical-Access and O.Alarm-Response detect unauthorized access; and O.Internal-Monitor and O.Maintain-Security ensure application of these security measures. The threat is effectively mitigated by these objectives.
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement	O.Staff-Engagement ensures that staff are aware of their responsibilities. O.Internal-Monitor and O.Maintain-Security ensure implementation of the required security measures. The threat is effectively mitigated by these objectives.

Threats and OSPs	Objectives	Rationale
T.Unauthorized-Staff	O.Alarm-Response O.Control-Scrap O.Internal-Monitor O.Logical-Access O.Logical-Operation O.Maintain-Security O.Physical-Access O.Staff-Engagement	O.Physical-Access, O.Alarm-Response, O.Logical-Access, O.Logical-Operation, O.Staff-Engagement and O.Control-Scrap prevent unauthorized access to assets, and O.Internal-Monitor and O.Maintain-Security ensure application of these security measures. The threat is effectively mitigated by these objectives.
OSPs		
P.Config-Mgmt	O.Config-Control O.Config-Env O.Config-Items O.Flaw-Remediation	O.Config-Items ensures that the configuration management system uniquely identifies configuration items. O.Config-Control ensures the proper change control of configuration items. O.Config-Env ensures the tracking and maintenance of development tools. O.Flaw-Remediation ensures that flaw remediation is performed and flaw status is tracked.
P.Flaw-Remediation	O.Flaw-Remediation	O.Flaw-Remediation directly enforces P.Flaw-Remediation.
P.LifeCycle-Doc	O.LifeCycle-Doc	O.LifeCycle-Doc directly enforces P.LifeCycle-Doc.

5 Extended Components Definition

No extended assurance components are defined for this SST.

6 Security Assurance Requirements

Product evaluations referencing this Site Security Target will be at Evaluation Assurance Level (EAL) 4+.

The Security Assurance Requirements (SARs) claimed in this SST are:

- CM Capabilities (ALC_CMC.4)
- CM Scope (ALC_CMS.4)
- Development Security (ALC_DVS.2)
- Flaw Remediation (ALC_FLR.2)
- Life-cycle Definition (ALC_LCD.1)
- Tools and Techniques (ALC_TAT.1)

These SARs fulfil the requirements of [Site Certification] as follows:

- ALC_CMC.4 is hierarchically higher than ALC_CMC.1 and therefore fulfills the minimum requirement for ALC_CMC.
- ALC_CMS.4 is hierarchically higher than ALC_CMS.3 and therefore fulfills the minimum requirement for ALC_CMS.
- ALC_DVS.2 is hierarchically higher than ALC_DVS.1 and therefore fulfills the minimum requirement for ALC_DVS.
- The additional SARs (ALC_FLR.2, ALC_LCD.1 and ALC_TAT.1) are from the ALC class.

6.1 Application Notes and Refinements

[Site Certification] describes the procedures for evaluating a site in the absence of a Target of Evaluation (TOE) product. The subject of the evaluation is the process for the handling of intended TOE products, rather than the TOE itself. The evaluation procedures are further refined by the following application notes as follows:

- CM Capabilities
    - See [Site Certification], Section 5.1, ‘Application Notes for ALC_CMC’, for the relevant application notes.
- CM Scope
    - See [Site Certification], Section 5.2, ‘Application Notes for ALC_CMS’, for the relevant application notes.
- Development Security
    - See [Site Certification], Section 5.4, ‘Application Notes for ALC_DVS’, for the relevant application notes.
- Flaw Remediation
    - See [Site Certification], Section 5.5, ‘Application Notes for ALC_FLR’, for the relevant application notes.

- Life-cycle Definition
    - See [Site Certification], Section 5.6, ‘Application Notes for ALC_LCD’, for the relevant application notes.
- Tools and Techniques
    - See [Site Certification], Section 5.7, ‘Application Notes for ALC_TAT’, for the relevant application notes.

6.2 Security Assurance Rationale

The Security Assurance Rationale maps the content elements of the selected assurance components to the Security Objectives defined in this SST. The refinements described in [Site Certification] have been considered.

Table 6-1: ALC_CMC.4 Rationale

SAR	Objective	Rationale
ALC_CMC.4.1C (Refined): The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.	O.Config-Control O.Config-Items	The TOE is labelled with its unique reference by the configuration management system (O.Config-Items, O.Config-Control). Appropriate and consistent labelling is ensured through the use of the configuration management system (O.LifeCycle-Doc).
ALC_CMC.4.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Config-Control O.Config-Items O.LifeCycle-Doc	The method used to uniquely identify the configuration items is described in the configuration management documentation (O.LifeCycle-Doc). Each item is assigned a unique identifier (O.Config-Items). The configuration items are tracked throughout the life-cycle (O.Config-Control).
ALC_CMC.4.3C: The CM system shall uniquely identify all configuration items.	O.Config-Items	All configuration items are uniquely identified by the configuration management system (O.Config-Items).
ALC_CMC.4.4C: The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config-Control O.Config-Items O.LifeCycle-Doc O.Logical-Access O.Logical-Operation	The configuration management system is used in accordance with the documented processes (O.LifeCycle-Doc). The configuration management system provides automated measures such that only authorized change are made to the configuration items(O.Config-Control). Access is controlled such that only authorized users may make changes (O.Logical-Access). An authentication is necessary to get access to the system (O.Logical-Operation). The configuration management system manages all relevant assets (O.Config-Items).

SAR	Objective	Rationale
ALC_CMC.4.5C: The CM system shall support the production of the TOE by automated means.	O.Config-Env O.LifeCycle-Doc	The site provides automated tools for development work (O.Config-Env), and procedures for their use (O.LifeCycle-Doc).
ALC_CMC.4.6C: The CM documentation shall include a CM plan.	O.Config-Items O.LifeCycle-Doc	The configuration management plan is described in the Life-cycle documentation (O.LifeCycle-Doc). The configuration management system is supported by documentation (O.Config-Items).
ALC_CMC.4.7C: The CM plan shall describe how the CM system is used for the development of the TOE.	O.Config-Items O.LifeCycle-Doc	The configuration management plan is described in the Life-cycle documentation (O.LifeCycle-Doc). The configuration management system is supported by documentation (O.Config-Items).
ALC_CMC.4.8C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.	O.Config-Control O.LifeCycle-Doc	The acceptance procedures for modified and newly created configuration items are described in the Life-cycle documentation (O.Config-Control, O.LifeCycle-Doc).
ALC_CMC.4.9C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.Config-Items O.LifeCycle-Doc	The configuration items are listed in the Life-cycle documentation (O.LifeCycle-Doc). The site maintains an automated configuration management system (O.Config-Items).
ALC_CMC.4.10C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.Config-Control O.Config-Env O.Config-Items O.LifeCycle-Doc	The configuration list (O.LifeCycle-Doc) is generated from the configuration management system (O.Config-Control, O.Config-Env, O.Config-Items).

Table 6-2: ALC_CMS.4 Rationale

SAR	Objective	Rationale
ALC_CMS.4.1C: The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.	O.Flaw-Remediation O.LifeCycle-Doc	The configuration list (O.LifeCycle-Doc) includes the required items. The flaw remediation system provides reports and status information (O.Flaw-Remediation).
ALC_CMS.4.2C: The configuration list shall uniquely identify the configuration items.	O.Config-Items	The configuration management system assigns a unique identifier to each configuration item (O.Config-Items).

SAR	Objective	Rationale
ALC_CMS.4.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	O.Config-Control O.Config-Env O.Config-Items	The configuration management system (O.Config-Control, O.Config-Env, O.Config-Items) indicates the developer of each configuration item.

Table 6-3: ALC_DVS.2 Rationale

SAR	Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	O.Alarm-Response O.Control-Scrap O.Internal-Monitor O.Maintain-Security O.LifeCycle-Doc O.Logical-Access O.Logical-Operation O.Physical-Access O.Staff-Engagement O.Transfer-Data	The development security documentation (O.LifeCycle-Doc) describes all the physical (O.Physical-Access, O.Alarm-Response), procedural (O.Internal-Monitor, O.Maintain-Security, O.Control-Scrap), personnel (O.Staff-Engagement), and other (O.Logical-Access, O.Logical-Operation, O.Transfer-Data) security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	O.LifeCycle-Doc	The development security documentation (O.LifeCycle-Doc) justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

Table 6-4: ALC_FLR.2 Rationale

SAR	Objective	Rationale
ALC_FLR.2.1C: The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.	O.Flaw-Remediation O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) together with the flaw remediation documentation (O.Flaw-Remediation) describe the procedures used to track security flaws.
ALC_FLR.2.2C: The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.	O.Flaw-Remediation	The flaw remediation procedures ensure that the flaw is described and its correction status is available (O.Flaw-Remediation).
ALC_FLR.2.3C: The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.	O.Flaw-Remediation	The flaw remediation procedures ensure that corrective actions are identified for security flaws (O.Flaw-Remediation).

SAR	Objective	Rationale
ALC_FLR.2.4C: The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.	O.Flaw-Remediation	The flaw remediation procedures ensure that remediation actions are provided to TOE users (O.Flaw-Remediation).
ALC_FLR.2.5C: The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.	O.Flaw-Remediation	The flaw remediation procedures ensure that TOE users are able to provide reports of suspected TOE security flaws (O.Flaw-Remediation), and that these procedures are documented.
ALC_FLR.2.6C: The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.	O.Flaw-Remediation	The flaw remediation procedures ensure that remediation actions are taken, and that remediation procedures are provided to TOE users (O.Flaw-Remediation).
ALC_FLR.2.7C: The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.	O.Flaw-Remediation	The flaw remediation procedures ensure that remediation actions do not introduce new flaws (O.Flaw-Remediation).
ALC_FLR.2.8C: The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.	O.Flaw-Remediation	The flaw remediation procedures ensure that TOE users have a means of reporting suspected security flaws (O.Flaw-Remediation).

Table 6-5: ALC_LCD.1 Rationale

SAR	Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.	O.LifeCycle-Doc	The Life-cycle documentation (O.LifeCycle-Doc) describes the model used to develop and maintain the TOE.
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	O.LifeCycle-Doc	The Life-cycle documentation (O.LifeCycle-Doc) describes the governance that provides for the necessary control over the development and maintenance of the TOE.

Table 6-6: ALC_TAT.1 Rationale

SAR	Objective	Rationale
ALC_TAT.1.1C: Each development tool used for implementation shall be well-defined.	O.LifeCycle-Doc	The Life-cycle documentation (O.LifeCycle-Doc) describes the development tools used for implementation, ensuring that they are well defined.
ALC_TAT.1.2.C: The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.	O.LifeCycle-Doc	The Life-cycle documentation (O.LifeCycle_Doc) provides sufficient guidance on statements, conventions and directives used in the implementation.
ALC_TAT.1.3C: The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.	O.LifeCycle-Doc	The Life-cycle documentation (O.LifeCycle-Doc) provides sufficient guidance on implementation-dependent options.

7 Site Summary Specification

7.1 Preconditions Required by the Site

The following table summarizes the preconditions that must be met to ensure that the security measures of the site protect its assets.

Table 7-1: Site Preconditions

Precondition	Assumption
Local and remote IT personnel provide the necessary systems engineering support to the site in order to design, implement and maintain the IT infrastructure required by the development team in order to perform TOE development and testing.	A.Secure-Local-IT
Remote workstations are purchased, configured, controlled, and maintained by Thales CPL and are connected using an encrypted link.	A.Remote.Services
Account setup, access permissions, access to tools and direction for their use is fully under Thales control and performed in accordance with applicable policies.	A.Project-Security
Personnel have been trained and acknowledged responsibilities for maintaining security.	A.Trusted-Personnel

7.2 Services of the Site

Development and testing activities are performed at the Thales Ottawa Colonnade site. These services include HSM hardware design and testing, firmware software development, testing and flaw remediation activities. Site support services include IT support, HR and general site management.

7.3 Site Summary Specification

The Site Summary Specification identifies the evidence that demonstrates that the site meets the SARs, and describes aspects of how the site meets the SARs. The full title, date and version of the references are found on Page 6 of this document.

Table 7-2: ALC_CMC.4 Summary

SAR	Met By	Evidence
ALC_CMC.4.1C (Refined): The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.	The configuration management system ensures unique identification of every configuration item.	[ALC] Section 2.1
ALC_CMC.4.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	The configuration management documentation describes the method used to identify the configuration items.	[ALC] Section 2.1

SAR	Met By	Evidence
ALC_CMC.4.3C: The CM system shall uniquely identify all configuration items.	All configuration items are uniquely identified by the configuration management system in which they are maintained.	[ALC] Section 2.1
ALC_CMC.4.4C: The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	Access is restricted to the configuration management system based on role. Users must be identified and authenticated prior to gaining access. Procedures ensure that changes are reviewed and approved prior to acceptance.	[ALC] Section 2.2
ALC_CMC.4.5C: The CM system shall support the production of the TOE by automated means.	The site provides automated tools for development work.	[ALC] Section 2.1
ALC_CMC.4.6C: The CM documentation shall include a CM plan.	The configuration management plan is described in the Life-cycle documentation.	[ALC] Sections 2, 3
ALC_CMC.4.7C: The CM plan shall describe how the CM system is used for the development of the TOE.	The configuration management plan is described in the Life-cycle documentation.	[ALC] Section 2
ALC_CMC.4.8C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.	The acceptance procedures for modified and newly created configuration items are described in the Life-cycle documentation.	[ALC] Section 2.2.3
ALC_CMC.4.9C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	The configuration items are listed in the Life-cycle documentation. The site maintains an automated configuration management system that can provide a Bill of Materials for each TOE.	[ALC] Sections 2, 3, 8
ALC_CMC.4.10C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	Evidence will be provided during the site audit.	To be provided during the Site Visit

Table 7-3: ALC_CMS.4 Summary

SAR	Met By	Evidence
ALC_CMS.4.1C: The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.	The configuration list includes the required items.	[ALC] Section 8

SAR	Met By	Evidence
ALC_CMS.4.2C: The configuration list shall uniquely identify the configuration items.	Each configuration item is assigned a unique identifier.	[ALC] Section 8
ALC_CMS.4.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	The configuration list indicates the developer of each configuration item.	[ALC] Section 8

Table 7-4: ALC_DVS.2 Summary

SAR	Met By	Evidence
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	The development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	[ALC] Section 4 [MSSR_Checklist]
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	The development security documentation justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Procedures are consistent with mitigating the risk of an attacker with a high attack potential.	[ALC] Section 4 [MSSR_Checklist]

Table 7-5: ALC_FLR.2 Summary

SAR	Met By	Evidence
ALC_FLR.2.1C: The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.	The life cycle documentation describes the procedures used to track security flaws.	[ALC] Section 5.2
ALC_FLR.2.2C: The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.	The flaw remediation procedures ensure that the flaw is described, and its correction status is available.	[ALC] Section 5.2
ALC_FLR.2.3C: The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.	The flaw remediation procedures ensure that corrective actions are identified for security flaws.	[ALC] Section 5.2

SAR	Met By	Evidence
ALC_FLR.2.4C: The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.	The flaw remediation procedures ensure that remediation actions are provided to TOE users.	[ALC] Section 5.2
ALC_FLR.2.5C: The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.	The flaw remediation procedures ensure that TOE users are able to provide reports of suspected TOE security flaws, and that these procedures are documented.	[ALC] Section 5.2
ALC_FLR.2.6C: The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.	The flaw remediation procedures ensure that remediation actions are taken, and that remediation procedures are provided to TOE users.	[ALC] Section 5.2
ALC_FLR.2.7C: The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.	The flaw remediation procedures ensure that remediation actions do not introduce new flaws.	[ALC] Section 5.2
ALC_FLR.2.8C: The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.	The flaw remediation procedures ensure that TOE users have a means of reporting suspected security flaws.	[ALC] Section 5 How to Report a Security Vulnerability | Thales (thalesgroup.com)

Table 7-6: ALC_LCD.1 Summary

SAR	Met By	Evidence
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.	The Life-cycle documentation describes the model used to develop and maintain the TOE.	[HDLC]
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	The Life-cycle documentation describes the governance that provides for the necessary control over the development and maintenance of the TOE.	[HDLC] Section 3.3

Table 7-7: ALC_TAT.1 Summary

SAR	Met By	Evidence
ALC_TAT.1.1C: Each development tool used for implementation shall be well-defined.	The Life-cycle documentation describes the development tools used in the design and testing of Hardware Security Module (HSM) products, ensuring that they are well defined.	[ALC] Section 7
ALC_TAT.1.2.C: The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.	The Life-cycle documentation provides references to the guidance on statements, conventions and directives used in the implementation.	[ALC] Section 7
ALC_TAT.1.3C: The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.	The Life-cycle documentation provides references to the guidance on implementation-dependent options.	[ALC] Section 7