DOC_ID: 4525_014

Site Security Target

Nordic Oulu - Finland

Headquarters | Otto Nielsens veg 12, 7052 Trondheim, Norway | P.B. 2336, 7004 Trondheim | +47 72 89 89 00
Document classification: Public

Table of Contents

Table of Figures

1. Document Information

1 This document is based upon the Eurosmart Site Security Target Template [1] with adaptions such that it fits the site (i.e. development site).

1.1 Reference

Title: Site Security Target Nordic Oulu - Finland

Version: 2.11

Date: 10 June 2024

Company: Nordic Semiconductor ASA

Name of site: Nordic Oulu - Finland

Site type: Development

1.2 Version History

Version	Date	Comment/Editor/Changes
0.1	05 May 2021	Initial version
0.2	21 July 2021	Draft version sent to Certification Lab
0.3	09 August 2021	Document reviewed and updated based on Certification Lab's comments
0.4	13 August 2021	Formatting update with Nordic logo and font.
1.0	13 August 2021	Official 1st version release to Certification Lab
1.1	28 September 2021	Official 1st version, 1st revision release to Certification Lab
1.2	04 October 2021	Document updated based on Certification Lab's comments
1.3	25 October 2021	Document updated based on Certification Lab's comments
1.4	07 December 2021	Correction of the Site Name and Reference
2.0	17 October 2023	Formatting updates, version sent to Certification Lab
2.1	2 November 2023	Document updated based on Certification Lab's comments
2.2	9 November 2023	Updated DOC ID
2.3	16 November 2023	Updated ALC_FLR.3 for Flaw Remediation.
2.4	09 January 2024	Document reviewed and updated based on Certification Lab's comments. Updated version sent to Certification Lab.
2.5	16 January 2024	Document reviewed and updated based on Certification Lab's comments. Updated version sent to Certification Lab.
2.6	22 February 2024	Document reviewed and updated based on Certification Lab's comments. Updated version sent to Certification Lab.
2.7	15 March 2024	Document reviewed and updated based on Certification Lab's comments. Updated version sent to Certification Lab.
2.8	10 April 2024	Document reviewed and updated based on Certification Lab's comments. Updated version sent to Certification Lab.
2.9	30 April 2024	Document reviewed and updated based on Certification Lab's comment. Updated version sent to Certification Lab.
2.10	4 June 2024	Public version of the document. Version sent to Certification Lab.
2.11	10 June 2024	Updated DOC ID. Version sent to Certification Lab.

2. SST Introduction

2.1 Site Reference

The site is identified and referenced as follows:

Company	Nordic Semiconductor ASA
Name of the site	Nordic Oulu - Finland
Location	Technopolis Peltola Campus Yrttipellontie 1, 90230 Oulu, Finland

2.2 Site Description

2.2.1 Physical Scope

The following areas of the site specified in Section 2.1 are in the scope of the SST:

- Secure development room
- IT Network rooms
- Files Server room

2.2.2 Logical Scope

The following high-level description of the services and/or processes provided by Nordic Semiconductor ASA are in the scope of the site evaluation process. More details can be found in chapter 8.2.

The site areas in scope here are dedicated to development projects.

The activities of the site cover the IC Embedded Software Development and Testing (Phase 1) and/or IC Development and Testing (Phase 2) as defined in 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084). IC Development includes IC hardware design and IC dedicated software design (e.g. firmware).

Supporting services are provided within the same location, such as physical site security, local IT management, HR related services, and facilities management.

3. Conformance Claim

This SST is conformant with Common Criteria version 3.1:

- Common Criteria for Information Technology Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017 [2]

- Common Criteria for Information Technology Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017 [3]

For the evaluation, the following methodology will be used:

- Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5, April 2017 [4]

- Supporting Document, Site Certification, CCDB-2007-11-001 [5]

- JIL – Minimum Site Security Requirements v3.1of December 2023

The evaluation of the site comprises the following assurance components:

- ALC_CMC.4
- ALC_CMS.5
- ALC_DVS.2
- ALC_LCD.1
- ALC_TAT.2
- ALC_FLR.3

The assurance level chosen for the SST is compliant to the Security IC Platform Protection Profile [6] and therefore suitable for the evaluation of (software for) Security ICs.

The chosen assurance components are derived from the assurance level EAL5 of the assurance class „Life-cycle Support “. For the assessment of the security measures attackers with high attack potential are assumed. Therefore, this site supports product evaluations up to EAL5 augmented with ALC_DVS.2 and ALC_FLR.3.

4. Security Problem Definition

The Security Problem Definition comprises 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 the TOE and the security management of the site.

Note: Where necessary the items in this section have been re-worked to fit the site.

4.1 Assets

The following section describes the assets handled at the site.

Asset	Description
Development data	The site has access to (and optionally copies) electronic development data related to developed TOEs. Both the integrity and the confidentiality of these electronic documents must be protected.
Development systems	To perform its development activities, the site uses tools and the libraries that come with these tools. The integrity of these tools must be protected.
IT infrastructure	To perform its development activities, the site has a local dedicated server; data are backed-up to another secure site. The combination of hardware and software used to allow the development systems access the assets is evaluated at Nordic Global IT. The integrity of this infrastructure must be protected.
Physical security objects	The site has physical security objects (printed documents, media used to store development data, samples, etc.) related to developed TOEs. Both the integrity and the confidentiality of these must be protected.

4.2 Threats

Threat	Description
T.Smart-Theft	An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive assets. The attacker has enough time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered.
T.Rugged-Theft	An experienced thief with specialized equipment for burglary, who may be paid to perform a targeted attack tries to access sensitive areas and manipulate or steal sensitive assets.
T.Computer-Net	A possibly paid hacker with substantial expertise using standard equipment attempts to remotely access sensitive network segments to get access to (1) development data with the intention to violate confidentiality and possibly integrity or (2) development computers with the intention to modify the development process at the site.

T.Accident-Change	An employee may change tool configuration that have an impact on the intended TOE by accident.
T.Unauthorised-Staff	Employees or subcontractors not authorized to get access to assets violating the confidentiality and possibly the integrity of products.
T.Staff-Collusion	An attacker tries to get access to assets by getting support from one employee through extortion or bribery.
T.Attack-Transport	An attacker might try to get development data and finished products during the internal shipment and/or the external delivery. The target is to compromise confidential information or violate the integrity of the products during the stated internal shipment and/or the external delivery process to allow a modification or the retrieval of confidential information.

4.3 Organizational Security Policies

Policy	Description
P.Config-Items	The configuration management system shall be able to uniquely identify all configuration items. This includes the unique identification of items that are created, generated, developed or used at a site as well as the received and transferred and/or provided items.
P.Config-Control	The procedures for setting up the development process for a new product as well as the procedure that allows changes of the initial setup for a current product shall only be applied by authorized personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes
P.Config-Process	The services and/or processes provided by the site are controlled in the configuration management plan. This comprises incoming items, tools used for the development of the product, the management of flaws and optimizations of the process flow as well as the documentation that describes the services and/or processes provided by the site. A released development process is defined and under version control.
P.Organise-Product	The development, configuration, pre-personalisation, initialization process is applied as specified by the client. If the data includes sensitive items like keys relevant for the life-cycle or configuration data that affect the security of the intended TOE, appropriate measures are in place. This includes the requirement that the knowledge of sensitive keys is split to at least two different persons. Furthermore, technical measures like crypto-boxes, separation of network, split access permission and secure storage is implemented for this kind of data.
P.Programming-Rules	The site ensures that the development tools documentation defines the meaning of all statements as well as all implementation-dependent options.
P.Transfer-Data	Any sensitive configuration items (e.g. development data, finished products, etc.) are encrypted to ensure confidentiality and integrity of the data.
P.Lifecyle-Doc	The site follows the life cycle documentation that describes: (1) Description of configuration management systems and their usage; (2) A configuration items list; (3) Site security; (4) The development process; (5) The development tools; (6) Flaw remediation process; (7) Delivery procedure.

P.Reception-Control	The inspection of incoming items done at the site ensures that the received configuration items comply with the properties stated by the client. Furthermore, it is verified that the product can be identified and a released production process is defined for the product. If applicable this aspect includes the check that all required information and data is available to process the items.
P.Config_IT-env	In addition to the used software on development workstations and servers, the site uses configuration management systems for file versioning and problem tracking. For file versioning the team members are assigned to project specific, centralized repositories to support proper management of multiple products and the site internal procedures. The team members are requested to use only project related IT equipment with provided tools.
P.Flaw-Remediation	The site is in charge of security flaw remediation. The procedures in place within the site must show how flaw remediation is managed giving assurance on the following topics: (1) acceptance and acting upon all reports of security flaws and requests for corrections to those flaws. (2) flaw remediation guidance to address to TOE users.

4.4 Assumptions

Each site must rely on the information received by the previous site/client. This is reflected by the assumptions that must be defined for the interface.

Assumption	Description
A.Inherit-secure-IT	The local IT equipment (for example workstations) is connected to a secure remote IT-infrastructure through a secure (encrypted) network connection. The local workstations, the remote secure IT-infrastructure and the secure connection to it satisfy all relevant ALC requirements and are provided and managed by Nordic.
A.Remote.Services	The facilities required to safeguard the remote IT-infrastructure and to establish a secure link to the development site have all the necessary security measures to provide a secure environment. The IT infrastructure is remotely managed.
A.Prod-Specification	The client must provide appropriate information (e.g. specifications, definitions, process limits, process parameters, test requirements, test limits, bond plans) to ensure an appropriate development or production process. The provided information includes the classification of the documents and product
A.Item-Identification	Each configuration item received by the site is appropriately labelled to ensure the identification of the configuration item.

5. Security Objectives

The Security Objectives are related to physical, technical and organizational security measures, the configuration management as well as the internal shipment and/or the external delivery

The SST includes a Security Objectives Rationale with two parts. The first part includes a tracing which shows how the threats and OSPs are covered by the Security Objectives. The second part include a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives.

Note that the assumptions of the SST cannot be used to cover any threat or OSP of the site. They are pre-conditions fulfilled either by the site providing the sensitive assets or by the site receiving the sensitive assets. Therefore, they do not contribute to the security of the site under evaluation.

Objective	Description
O.Physical-Access	The combination of physical partitioning between the different access control levels together with technical and organizational security measures allows a sufficient separation of employees to enforce the „need to know" principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorized people. The access control measures ensure that only registered employees can access restricted areas. Sensitive assets are handled in restricted areas only. Network cabling is protected according to classification of the transferred data by avoiding routes through public areas or by usage of appropriate cryptographic measures
O.Security-Control	Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, contractors and suppliers
O.Alarm-Response	The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any asset. After the alarm is triggered, the unauthorized person still has to overcome further security measures. The reaction time of the employees or guards is short enough to prevent a successful attack
O.Internal-Monitor	The site performs security management meetings. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures.
O.Maintain-Security	Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorized employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.

O.Logical-Access	The site implements a firewall system to enforce a logical separation between the internal network and the internet. The firewall system ensures that only defined services and defined connections are accepted. Furthermore, the internal network is separated into a development network and an office network. Access to the development network and related systems is restricted to authorized employees that work in the related area or that are involved in the configuration tasks or the development systems. Every user of an IT system has individual credentials.
O.Logical-Operation	Development computers enforce that every user authenticates using individual credentials, and all development systems and IT infrastructure are kept up to date. The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.
O.LifeCycle-Doc	The site uses life cycle documentation that describes: (1) Description of configuration management systems and their usage; (2) A configuration items list; (3) Site security; (4) The development process; (5) The development tools; (6) Flaw remediation process.
O.Config-Items	The site has a configuration management system that assigns a unique internal identification to each product to uniquely identify configuration items and allow an assignment to the client. Also, the internal procedures and guidance are covered by the configuration management.
O.Config-Control	The site applies a release procedure for the setup of the development process for each new product. In addition, the site has a process to classify and introduce changes for services and/or processes of released products. Minor changes are handled by the site, major changes must be acknowledged by the client. A designated team is responsible for the release of new products and for the classification and release of changes. This team comprises specialists for all aspects of the services and/or processes. The services and/or processes can be changed by authorized personnel only. Automated systems support configuration management.
O.Config-Process	The site controls its services and/or processes using a configuration management plan. The configuration management is controlled by tools and procedures for the development of the product, for the management of flaws and optimizations of the process flow as well as for the documentation that describes the services and/or processes provided by a site.
O.Staff-Engagement	All employees who have access to sensitive assets are checked regarding security concerns and have to sign a nondisclosure agreement. Furthermore, all employees are trained and qualified for their job
O.Transfer-Data	Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorized employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secure measures and they are sufficiently protected

O.Control-Scrap	The site has measures in place to destruct sensitive documentation (e.g. paper shredder), erase electronic media and destroy sensitive assets so that they do not support an attacker
O.Programming-Rules	The site maintains well-defined development tools and their corresponding development tools documentation
O.Organise-Product	For the configuration, pre-personalization, initialization or process it is ensured that the specified process is applied. The data integrity is controlled. The operation is applied in crypto-boxes or similar devices. After the release process changes are only applied based on the request of the client. The update is done according to a controlled process.
O.Reception-Control	Upon reception of any intended TOE an immediate incoming inspection is performed. The inspection comprises the received amount, their identification and the assignment of the items to a related internal process.
O.Internal-Shipment	The recipient of a physical configuration item is identified by the assigned client address. The internal shipment procedure is applied to the configuration item. The address for shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of assets during internal shipment. For every sensitive configuration item, the protection measures against manipulation are defined.
O.Config_IT-env	In addition to the software used on development workstations and servers, the site uses configuration management systems for the file versioning and problem tracking. For the file versioning unique repositories are used to support proper management of multiple products and the site internal procedures. Only project related tools and IT equipment is used.
O.Flaw-Remediation-Monitor	All security flaws discovered by development teams or raised by the TOE user must be monitored and managed.
O.Flaw-Remediation-External	Corrections and guidance on corrective actions for Security Flaw with consequences for TOE users are provided to TOE users.

5.1 Mapping of Security Objectives

The Security Objectives Rationale provides a justification that shows that all threats and OSP are effectively addressed by the Security Objectives.

Security Objectives / Threats/OSPs	O.Physical-Access	O.Security-Control	O.Alarm-Response	O.Internal-Monitor	O.Maintain-Security	O.Logical-Access	O.Logical-Operation	O.Config-Items	O.Config-Control	O.Config-Process	O.Organise-Product	O.Staff-Engagement	O.Reception-Control	O.Internal-Shipment	O.-Transfer-Data	O.Control-Scrap	O.Programming-Rules	O.Lifecycle-Doc	O. Config.IT-env	O.Flaw-Rem-Monitor	O.Flaw-Rem-External
T.Smart-Theft	X	X	X	X	X																
T.Rugged-Theft	X	X	X	X	X																
T.Computer-Net				X	X	X	X					X									
T.Accident-Change						X	X	X		X		X					X				
T.Unauthorised-Staff	X	X	X	X	X	X	X					X				X					
T.Staff-Collusion				X	X							X			X	X					
T.Attack-Transport														X	X			X			
P.Config-Items								X													
P.Config-Control									X												
P.Config-Process										X											
P.Reception-Control													X								
P.Lifecycle-Doc																		X			
P.Transfer-Data															X						
P.Organise-Product											X										
P.Programming-Rules																	X				
P.Config_IT-env																			X		
P.Flaw-Remediation																				X	X

5.2 Security Objectives Rationale

2 The following rationales provides a justification that shows that all threats and OSP are effectively addressed by the Security Objectives.

Threats and OSP	Security Objective(s)	Rationale
T.Smart-Theft T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat. Physical and logical access control prohibits access to assets.
T.Computer-Net	O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat. Physical and logical access control prohibits access to assets.
	O.Logical-Access O.Logical-Operation	The development network is not connected to anything that an attacker could use to set up a remote connection. Logical access and operation ensure that users have individual credentials and the account is limited to the access rights required by the job task and their responsibility following a strict “need to know principle”.
	O.Staff-Engagement	Hiring policies restrict hiring to trustworthy employees limits unauthorized access to assets. All employees get training that shall ensure the knowledge of the processes.
T.Accident-Change	O.Logical-Access O.Logical-Operation	The development network is not connected to anything that an attacker could use to set up a remote connection. Logical access and operation ensure that users have individual credentials and the account is limited to the access rights required by the job task and their responsibility following a strict “need to know principle”.
	O.Config-Items O.Config-Process	The use of backup and appropriate storage of the backup are applied to prevent the loss of data. Organizational measures ensure that confidentiality is preserved, and that integrity changes of delivered configuration items are detected and appropriately responded upon.
	O.Staff-Engagement O.Programming-Rules	All employees get training that shall ensure the knowledge of the processes.
T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat. Physical and logical access control prohibits access to assets.
	O.Logical-Access O.Logical-Operation	The development network is not connected to anything that an attacker could use to set up a remote connection. Logical access and operation ensure that users have individual credentials and the account is limited to the

		access rights required by the job task and their responsibility following a strict "need to know principle".
	O.Staff-Engagement	Hiring policies restrict hiring to trustworthy employees limits unauthorized access to assets. All employees get training that shall ensure the knowledge of the processes.
	O.Control-Scrap	Secure destruction of scrap limits the amount of assets
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat. Physical and logical access control prohibits access to assets. Systems are properly maintained.
	O.Staff-Engagement	Hiring policies restrict hiring to trustworthy employees limits unauthorized access to assets. All employees get training that shall ensure the knowledge of the processes.
	O.Control-Scrap	Secure destruction of scrap limits the amount of assets
	O.Transfer-Data	The data transfer method ensure that confidentiality is preserved, and that integrity changes of delivered configuration items are detected and appropriately responded upon.
T.Attack-Transport	O.Transfer-Data O.Internal-Shipment	The data transfer method ensure that confidentiality is preserved, and that integrity changes of delivered configuration items are detected and appropriately responded upon. Internal shipment take place only through secure corporate network.
	O.LifeCycle-Doc	Organizational measures ensure that confidentiality is preserved, and that integrity changes of delivered configuration items are detected and appropriately responded upon.
P.Lifecycle-Doc	O.LifeCycle-Doc	The use of backup and appropriate storage of the backup are applied to prevent the loss of data. Organizational measures ensure that confidentiality is preserved, and that integrity changes of received configuration items are detected and appropriately responded upon.
P.Programming-Rules	O.Programming-Rules	All employees get training that shall ensure the knowledge of the processes.
P.Reception-Control	O.Reception-Control	Organizational measures ensure that confidentiality is preserved, and that integrity changes of delivered configuration items are detected and appropriately responded upon.
P.Transfer-Data	O.Transfer-Data	The data transfer method ensure that confidentiality is preserved, and that integrity changes of delivered configuration items are detected and appropriately responded upon. Internal shipment take place only through secure corporate network.
P.Config-Items	O.Config-Items	The security objective directly enforces the OSP.

P.Config-Control	O.Config-Control	
P.Config-Process	O.Config-Process	
P.Organise-Product	O.Organise-Product	
P.Config_IT-env	O.Config.IT-env	The Security Objective directly enforces the OSP.
P.Flaw-Remediation	O.Flaw-Remediation-Monitor O.Flaw-Remediation-External	The Security Objective directly enforces the OSP.

6. Extended Assurance Components Definition

No extended components are defined in this Site Security Target.

7. Security Assurance Requirements

3 Clients using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL5 augmented with ALC_DVS.2 and ALC_FLR.3, potentially claiming conformance with the Eurosmart Protection Profile [6].

4 The Security Assurance Requirements (SAR) are chosen from the class ALC (Life-cycle support) as defined in [3]:

- CM capabilities (ALC_CMC.4)
- CM scope (ALC_CMS.5)
- Development Security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)
- Tools and techniques (ALC_TAT.2)
- Flaw Remediation (ALC_FLR.3)

5 The Security Assurance Requirements listed above fulfil the requirements of [5] because hierarchically higher components are used in this SST. In addition, the minimum set of SARs is extended by SAR of the assurance components for "Life-cycle definition“ (ALC_LCD.1), “Tools and techniques” (ALC_TAT.2) and “Flaw Remediation” (ALC_FLR.3).

7.1 Application Notes and Refinements

6 The description of the site certification process [5] includes specific application notes. The main item is that a product that is considered as „intended TOE” is not available during the evaluation. Since the term „TOE” is not applicable in the SST the associated processes for the handling of products or „intended TOEs” are in the focus and described in this SST. These processes are subject of the evaluation of the site.

7.1.1 CM Capabilities (ALC_CMC.4)

7 Refer to subsection ‘Application Notes for Site Certification’ in [5] 5.1 ‘Application Notes for ALC_CMC’.

7.1.2 CM Scope (ALC_CMS.5)

8 Refer to subsection ‘Application Notes for Site Certification’ in [5] 5.2 ‘Application Notes for ALC_CMS’.

7.1.3 Development Security (ALC_DVS.2)

9 Refer to subsection ‘Application Notes for Site Certification’ in [5] 5.4 ‘Application Notes for ALC_DVS’.

7.1.4 Life-cycle Definition (ALC_LCD.1)

10 Refer to subsection ‘Application Notes for Site Certification’ in [5] 5.6 ‘Application Notes for ALC_LCD’.

7.1.5 Tools and Techniques (ALC_TAT.2)

11 Refer to subsection ‘Application Notes for Site Certification’ in [5] 5.7 ‘Application Notes for ALC_TAT’.

7.1.6 Flaw remediation (ALC_FLR.3)

12 Refer to subsection ‘Application Notes for Site Certification’ in [5] 5.7 ‘Application Notes for ALC_FLR’.

7.2 Security Assurance Rationale

13 The Security Assurance Rationale maps the content elements of the selected assurance components of [3] to the Security Objectives defined in this SST. The refinements referred above are considered.

14 The site has a process in place to ensure an appropriate and consistent identification of the products. The site receives assets, for this process refer to A.Item-Identification.

15 Note: The content elements that are changed from the original CEM [4] according to the application notes in the process description [5] are written in italic. The term TOE can be replaced by configuration item or asset in most cases. In specific cases it is replaced by product or „intended TOE”.

16 The SAR Rationale does not explicitly address the developer action elements defined in [2] because they are implicitly included in the content elements. This comprises the provision of the documentation to support the evaluation and the preparation for the site visit. This includes the requirement that the procedures are applied as written and explained in the documentation.

Security Requirements Rationale - Dependencies

	ADV_FSP.2	ADV_FSP.4	ADV_IMP.1	ADV_TDS.1	ADV_TDS.3	ALC_CMS.1	ALC_DVS.1	ALC_DVS.2	ALC_LCD.1	ALC_TAT.1
ALC_CMC.4						X	X		X	
ALC_CMS.5										
ALC_DEL.1										
ALC_DVS.2										
ALC_FLR.3										
ALC_LCD.1										
ALC_TAT.2			X							

Table 1: Dependency Table for Class ALC: Life-Cycle Support

Note, for Nordic Oulu site, the ALC: Life-cycle Support under the assurance level EAL5+ are:

- ALC_CMC.4: ALC_CMS.1, ALC_DVS.2, ALC_LCD.1
- ALC_CMS.5: None
- ALC_DEL.1: None
- ALC_DVS.2 (at AVA_VAN.5 level): None
- ALC_LCD.1: None
- ALC_FLR.3: None
- ALC_TAT.2: ADV_IMP.1

Some dependencies are not completely fulfilled which is described below:

ALC_DEL.1 is not applicable to the site.

SAR	Security Objective	Rationale	Aspects	Reference
ALC_CMC.4.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.	O.Config-Items O.LifeCycle-Doc O.Reception-Control O.Config_IT-env	Appropriate and consistent labelling is ensured through the application of the Document Control Procedure	Each product is already labelled when it is received at the site. The received products are checked and mapped to an internal product identification.	- Doc. Control Procedure - Configuration Management Procedures - SW Baseline Document
			Registration of each client and each product/file in a data base ensures unique labels and assignments.	Technology Database
ALC_CMC.4.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Config-Items O.LifeCycle-Doc	The method used to uniquely identify the configuration items is described in the CM documentation.	All items can be uniquely identified using version control tools and labeling as described above.	- Doc. Control Procedure - Configuration Management Procedures - SW Baseline Document
ALC_CMC.4.3C: The CM system shall uniquely identify all configuration items.	O.Config-Items O.Config-Process O.LifeCycle-Doc	All configuration items are uniquely identified by the configuration management system.	All items can be uniquely identified using version control tools and labeling as described above.	- Doc. Control Procedure - Configuration Management Procedures - SW Baseline Document
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-Process O.Logical-Access O.LifeCycle-Doc	The configuration system provided the automated measures such that only authorized change is made to the configuration items.	Restricted access to the different tools and repositories allows only authorized persons to do changes. Review and approval of changes is required.	Configuration Management Procedure - SW Baseline Document - Project Checklists
ALC_CMC.4.5C: The CM system shall support the production of the *product* by automated means.	O.Config-Process O.Config-Control O.LifeCycle-Doc O.Config_IT-env	The building of the software and the testing are supported by the automated means of the configuration management system.	The development tools support the production of the product by automated means.	- R&D Tools register

SAR	Security Objective	Rationale	Aspects	Reference
ALC_CMC.4.6C: The CM documentation shall include a CM plan.	O.Config-Control O.Config-Process O.LifeCycle-Doc	The configuration management plan is described through the CM documentation.		- Processes Wizards (PM and SW Release)
ALC_CMC.4.7C: The CM plan shall describe how the CM system is used for the development of the *product*.	O.Config-Control O.Config-Process O.LifeCycle-Doc	The CM system usage is described in the CM documentation.		- Processes Wizards (PM and SW Release)
ALC_CMC.4.8C: The CM plan shall describe the procedures used to accept modified or newly created configuration items (as part of the *product*).	O.LifeCycle-Doc	The acceptance procedure for modified and newly created configuration items are described in the CM documentation.		- Processes Wizards (PM and SW Release)
ALC_CMC.4.9C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.Config-Control O.Reception-Control O.LifeCycle-Doc	The configuration items are listed in the CM documentation. All electronic items are maintained under the configuration management system.	Documents are stored in Nordic Project Database and/or Development tools. Evidence can be provided during a site visit.	- Doc. Control Procedure
ALC_CMC.4.10C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.Config-Process O.LifeCycle-Doc	The configuration list is generated from the configuration management system. This is also described in developer documentation. The configuration items are tracked throughout the life-cycle of the TOE. Each item gets an internal	Documents are stored in Nordic Project Database and/or Development tools. Evidence can be provided during a site visit or project deliverables.	- Doc. Control Procedure - Internal audits Process

SAR	Security Objective	Rationale	Aspects	Reference
		unique identificatory for identification.		

Table 1: Rationales, Aspects and References for ALC_CMC.4

17 The security assurance requirements of the assurance class „CM capabilities“ listed above are suitable to support the production of complex products due to the formalized acceptance process and the automated support. The identification of all configuration items supports an automated and industrialized production process. The requirement for authorized changes supports the integrity and confidentiality required for the products. Therefore, this assurance level meets the requirements for the configuration management.

18 The scope of the evaluation according to the assurance class ALC_CMS comprises the security products, the complete documentation of the site provided for the evaluation and the configuration and initialization data as well as associated tools. The specifications and descriptions provided by the client are not part of the configuration management at Nordic Oulu - Finland.

SAR	Security Objective	Rationale	Aspects	Reference
ALC_CMS.5.1C: The configuration list shall include the following: *clear instructions how to consider these items in the list*; the evaluation evidence required by the SARs *of the life-cycle*; *development and production tools* and security flaw reports and resolution status.	O.Config-Control O.Config-Process O.LifeCycle-Doc	All configuration list and configuration items are maintained by the configuration management system.		- Secure Development Policy. - Project Management Wizards.
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.Config-Items O.Config-Control O.Config-Process O.LifeCycle-Doc	All configuration items are uniquely identified by the configuration management system.	All configuration items are maintained in the CM systems. Every document can be uniquely identified as stated above for ALC_CMC.4.1C.	Refer to ALC_CMC.4.1C

SAR	Security Objective	Rationale	Aspects	Reference
ALC_CMS.5.3C: *For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.*	O.Reception-Control O.Config-items O.Config-Process O.LifeCycle-Doc	The configuration management system identifies the developers/sub-contractors.		- Technology Database

Table 2: Rationales, Aspects and References for ALC_CMS.5

19 The security assurance requirements of the assurance class „CM scope“ listed above support the control of the production and test environment. This includes product related documentation and data as well as the documentation for the configuration management and the site security measures. Since the site certification process focuses on the processes based on the absence of a concrete TOE these assurance requirements are suitable.

20

SAR	Security Objective	Rationale	Aspects	Reference
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.LifeCycle-Doc O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Control-Scrap O.Staff-Engagement O.Transfer-Data O.Internal-Shipment	The development security documentation (O.LifeCycle-Doc) describes the physical (O.Physical-Access, O.Security-Control, 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) security measures that are necessary to	Access control to the building, surveillance, alarm system, receptionist and guard to prevent access to the building for unauthorized persons	- ISMS Manual
			Internal storage of products in a strong room	
			Organizational measure to enforce security and alarm tracing	
			Access control inside the building to enforce the production and control by authorized persons only	
			Tracing and control of visitors	

SAR	Security Objective	Rationale	Aspects	Reference
		protect the confidentiality and integrity of the intended TOE design and implementation in its development environment.	Tracing and control of external companies	
			Training of employees regarding security measures	
			Trustworthiness and tracing of employees	
			Personal accountability for products	
			Policies and procedures for the internal handling of confidential information	
			Network security measures to ensure logical protection	
			Authentication to computer systems using username and password	
			Maintenance of security measures	
			Protection of the internal shipment	
			Destruction of sensitive documents, data, products and other items	
			Emergency handling	

SAR	Security Objective	Rationale	Aspects	Reference
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 the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the intended TOE.	The justification is provided in this security target because it shows that all threats are addressed by the measures. In addition, the measures are monitored to control the effectiveness.	SST
ALC_DVS.2.3C: The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	O.Reception-Control O.Internal-Shipment O.Transfer-Data	The reception and incoming inspection support the detection of attacks during the transport of the security products to the site according to O.Reception-Control. The delivery to the client is protected by similar measures according to the requirements of the client based on O.Internal-Shipment. Sensitive data received and send by the Site is encrypted according to O.Data-Transfer to ensure access by authorized recipients only.	The justification is provided in this security target because it shows that all threats are addressed by the measures. In addition, the measures are monitored to control the effectiveness.	SST

Table 4: Rationales, Aspects and References for ALC_DVS.2

21 The security assurance requirements of the assurance class „Development security“ listed above are required since a high attack potential is assumed for potential attackers. The assets and information handled at the site during development, production, testing, assembly and pre-personalization or personalization of the product can be used by potential attackers for the development of attacks. Any keys loaded into the intended TOE also support the security during the internal shipment. Therefore, the handling and storage of

electronic keys must also be protected. Further on the Protection Profile [6] requires this protection for sites involved in the life-cycle of Security ICs development and production.

SAR	Security Objective	Rationale	Aspects	Reference
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.	O.LifeCycle-Doc O-Organize-Product	Nordic has a development process to develop and maintain the TOE.	The TOE is developed and maintained as per Nordic development process.	- Process Maps - Processes Wizards
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	Nordic development process includes control checkpoints.	The TOE is developed and maintained as per Nordic development process. It includes Reviews and checklists signed-off at specific Project Milestones. Internal audits are performed as well.	- Process Maps - Processes Wizards - Project Checklists

Table 5: Rationales, Aspects and References for ALC_LCD.1

22 The security assurance requirements of the assurance class „Life-cycle definition“ listed above are suitable to support the controlled development and production process. This includes the documentation of these processes and the procedures for the configuration management. One site provides only a limited support of the described life-cycle for the development and production of Security ICs. However, the assurance requirements are suitable to support the application of the site evaluation results for the evaluation of an intended TOE.

SAR	Security Objective	Rationale	Aspects	Reference
ALC_TAT.2.1C: Each development tool used for implementation shall be well-defined.	O.Config-Process O.Programming-Rules	Nordic uses well-known and publicly available development tools.	Each tool is described into the R&D Tools Register including tutorials how-to use/configurate.	- R&D Tools Register -Processes Wizards
ALC_TAT.2.2C: 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.Config-Process O.Programming-Rules	Nordic also maintain the corresponding tools documentation, that defines statements and implementation dependent options.	Each tool is described into the R&D Tools Register including tutorials how-to use/configurate.	Refer to ALC_TAT.2.1C
ALC_TAT.2.3C: The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.	O.Config-Process O.Programming-Rules	Nordic also maintain the corresponding tools documentation, that defines statements and implementation dependent options.	Each tool is described into the R&D Tools Register including tutorials how-to use/configurate.	Refer to ALC_TAT.2.1C

Table 6: Rationales, Aspects and References for ALC_TAT.2

23 The security assurance requirements of the assurance class „Tools and Techniques“ listed above shall support the secure development and production of the TOE. The control, capabilities and configuration of the tools contribute to achieve reproducible and consistent development, production and test processes. Therefore, this Security assurance requirement is suitable for this type of product.

SAR	Security Objective	Rationale	Aspects	Reference
ALC_FLR.3.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.	O.LifeCycle-Doc O.Config-Control O.Config-process O.Flaw-Remediation-Monitor	The life cycle documentation (O.LifeCycle-Doc) together with the documentation of the development tools unambiguously defines flaw remediation procedures.	Flaw remediation process is described in development tools for internal procedures and for external it is available on Nordic’s website and, send to customer under request.	-PSIRT Process and Procedures

ALC_FLR.3.2C 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.Config-Process O.Flaw-Remediation-Monitor	O.Config-Process ensures that all security flaws are tracked, the impacts are analyzed and the status is documented.		Refer to ALC_FLR.3.1C
ALC_FLR.3.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.	O.Config-Items O.Config-Process O.Flaw-Remediation-Monitor O.Flaw-Remediation-External	O.Config-Items ensures that corrective actions are identified. O.Config-Process ensures that corrective actions will need to be provided before marking security flaw report as resolved. The monitoring of flaws (O.Flaw-Remediation-Monitor) lead to a monitoring and management of each discovered flaw that ensures that status of the flaw is updated once the security flaw report is resolved. If this flaw was relevant for the TOE user, corrections and guidance of corrective actions are provided to the TOE user (O.Flaw-Remediation-External).		Refer to ALC_FLR.3.1C
ALC_FLR.3.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections	O.Flaw-Remediation-Monitor O.Flaw-Remediation-External	The monitoring of flaws (O.Flaw-Remediation-Monitor) lead to a monitoring and management of each discovered flaw. If this		Refer to ALC_FLR.3.1C

and guidance on corrective actions to TOE users.		flaw was relevant for the TOE user, corrections and guidance of corrective actions are provided to the TOE user (O.Flaw-Remediation-External).		
ALC_FLR.3.5C 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-External	For all TOE user relevant flaws, guidance and corrections are provided to the TOE user (O.Flaw-Remediation-External).		Refer to ALC_FLR.3.1C
ALC_FLR.3.6C The flaw remediation procedures shall include a procedure requiring timely response and the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.	O.Flaw-Remediation-Monitor	All security flaws are distributed automatically by using a management system (O.Flaw-Remediation-Monitor).		Refer to ALC_FLR.3.1C
ALC_FLR.3.7C 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-Monitor O.Flaw-Remediation-External	The monitoring of flaws (O.Flaw-Remediation-Monitor) lead to a monitoring and management of each discovered flaw. If this flaw was relevant for the TOE user, corrections and guidance of corrective actions are provided to the TOE user (O.Flaw-Remediation-External).		Refer to ALC_FLR.3.1C

ALC_FLR.3.8C 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-External	Each corrective action is documented and evaluated by the developer for functionality and side effects (O.Flaw-Remediation-External).		Refer to ALC_FLR.3.1C
ALC_FLR.3.9C 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-External	For all TOE user relevant flaws, guidance and corrections are provided to the TOE user (O.Flaw-Remediation-External).		Refer to ALC_FLR.3.1C
ALC_FLR.3.10C The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.	O.Flaw-Remediation-External	All relating TOE users get informed about security flaws and corrective actions by the developer (O.Flaw-Remediation-External).		Refer to ALC_FLR.3.1C
ALC_FLR.3.11C The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.	O.Flaw-Remediation-Monitor O.Flaw-Remediation-External	The monitoring of flaws (O.Flaw-Remediation-Monitor) lead to a monitoring and management of each discovered flaw. If this flaw was relevant for the TOE user, corrections and guidance of corrective actions are provided to the TOE user (O.Flaw-Remediation-External).		Refer to ALC_FLR.3.1C

Table 7: Rationales, Aspects and References for ALC_FLR.3

24 The security assurance requirements of the assurance class „Flaw remediation“ listed above shall describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users. It includes

documentation that used to track all reported security flaws in each release of the TOE and guidance on corrective actions to TOE users. Therefore, this Security assurance requirement is suitable for this type of product.

8. Site Summary Specification

8.1 Preconditions required by the Site

Assumption	Precondition
A.Inherit-secure-IT	IT personnel outside Nordic Oulu provide the necessary systems engineering support to the site in order to design, implement and maintain the necessary IT infrastructure required by the development team in order to perform TOE development and testing.
A.Remote.Services	The external party provides equivalent certified facilities to provide the required environmental site security to the IT infrastructure. IT administration is handled remotely. Final access to development data is by no means granted to such groups.
A.Prod-Specification	Appropriate information (e.g. specifications, definitions, process limits, process parameters, test requirements, test limits) need to be available to the site for the development to take place.
A.Item-Identification	Delivered items are already labelled.

Table 3: Precondition of assumptions

8.2 Services of the Site

Service	Details
IC Embedded Software Development and Testing (Phase 1) and/or IC Development and Testing (Phase 2)	• Development and Validation phases from the typical lifecycle. • Secure development of the design documentation, source code and guidance documentation. • CM System administration. • Generation and delivery of the intermediate deliverables. • Verification and Validation processes (simulations and emulation of hardware and software designs on dedicated test environments. Validation comprise verification of the design with real samples.
Local IT infrastructure and administration	• An appropriate environment for sensitive IT equipment employed • Administration of all services with the support of IT global personel as detailed in 8.1 Preconditions required by the site.
Supporting services	• HR management • Physical security • Facilities management

Table 4: Details of the services provided by the site

8.3 Mapping between SARs and Aspects

Refer to chapter 7.2 for aspects and references.

9. References

9.1 Literature

[1] „Site Security Target Template, Version 2.0, published by Eurosmart,“ Eurosmart, 15.04.2021.

[2] Common Criteria, „Common Criteria for Information Technology Security Evaluations, Part 1: Introduction and General Model; Version 3.1, Revision 5,“ April 2017.

[3] Common Criteria, „Common Criteria for Information Technology Security Evaluation, Part3: Security Assurance Requirements; Version 3.1, Revision 5,“ April 2017.

[4] Common Criteria, „Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5,“ April 2017.

[5] Common Criteria, „Supporting Document, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001,“ October 2007.

[6] „Security IC Platform Protection Profile with Augmentation Packages,Version 1.0, BSI-CC-PP-0084-2014,“ 13.01.2014.

[7] JIL – Minimum Site Security Requirements v3.1of December 2023

9.2 Definitions

Client	The site providing the Site Security Target may operates as a subcontractor of the TOE manufacturer. The term „client” is used here to define this business connection. It is used instead of customer since the terms „customer” and „consumer” are reserved in CC. In this document the terms words „customer” and „consumer” are only used here in the sense of CC.
Intended TOE	In the view of this site certification, there is no real product certified as the site certification is - per definition – product independent. Therefore, also no TOE does exist, and this SST is referring to the “intended TOE” only.
Product	A “product” would be the result of the development and production process.

9.3 List of Abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
IC	Integrated Circuit
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SST	Site Security Target
ST	Security Target
TOE	Target of Evaluation