# SMD_ST_GRENOBLE_SST_25_001

Security target

# Site security target of ST Grenoble

## Document information

This site security target document is based on the Common Criteria (CC) standards, release 1, published in November 2022.

# 1 General information

## 1.1 Introduction

The purpose of this document is to describe the site security target for the development and production of secure semiconductor devices.

This site security target refers to the STMicroelectronics Grenoble (France) site, hereafter referred to as ST Grenoble.

The site can be part of the development and production flow of security IC modules for smart cards, and IT security products.

## 1.2 Terminology

The table below contains the terms used in this security target and their definition.

Table 1. **Glossary**

| Term | Definition |
|---|---|
| Internal client | Only internal clients are identified for the security target (STMicroelectronics). There are no final clients in the scope. |

The table below contains the abbreviations used in this security target and their meaning.

Table 2. **Abbreviations**

| Term | Definition |
|---|---|
| CC | Common Criteria (ISO 15408) |
| EAL | Evaluation assurance level |
| SAR | Security assurance requirements |
| SFR | Security functional requirements |
| SST | Site security target |
| TOE | Target of evaluation |

# 2 Site security target and site reference

## 2.1 Site security target reference

Table 3. Site security target reference

| Element | Description |
|---|---|
| Title | Site security target of ST Grenoble |
| Reference | SMD_ST_GRENOBLE_SST_25_001 |
| Version | 2 |
| Date | 12/09/2025 |
| Company | STMicroelectronics (Grenoble 2) SAS and STMicroelectronics (Alps) SAS |
| Name of the site | ST Grenoble |
| Site location | 12 rue Jules Horowitz, BP 217, 38019 Grenoble Cedex – France |
| Product and development type | Hardware and Firmware development (including test program development) \| Assembly of IC modules (prototyping) |
| EAL level | EAL6+ (augmented with ALC_FLR.2) |
| Evaluation laboratory | SERMA Safety & Security – ITSEF |
| Certification body | Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI) |

# 3 Site description

The ST Grenoble site is located in the area of the “polygone scientifique” in Grenoble (France). The site is in charge of hardware and firmware development, including test and validation activities. Different analysis are performed on products at the reliability and failure analysis laboratory, the validation laboratory and during test operations. For prototyping purposes, the site supports an assembly pilot line. In addition, the development servers are hosted in the ST Grenoble site.

The site relevant areas are listed in Section 3.1: Physical scope. Access to these areas is granted only to personnel with a personal badge.

In the following sections, the physical and logical scopes of the SST are defined.

## 3.1 Physical scope

The Grenoble site is composed of 11 buildings that are fully occupied by STMicroelectronics. The overall site security is under the responsibility of ST Grenoble security manager. The ST Grenoble security manager is supported by the ST Grenoble security team and the Fiducial subcontractor. The areas in the scope of the SST are listed below:

- Connected Security office for hardware and firmware development, validation, product engineering, and IT room
- Connected Security validation laboratory with testers
- Assembly pilot line
- Grenoble reliability & analysis laboratory (GRAL)
- Engineering test room activities
- IT server room hosting firewalls, development servers, and switches
- Computer compiler center (CCC) activities

## 3.2 Logical scope

The ST Grenoble site is in charge of the IC hardware and firmware development including test and validation activities (DEV: Hardware, firmware development, and server).

The site supports the Computer compiler center (CCC) development activity (DEV: Hardware, firmware development, and server).

For prototyping purposes, the site has an assembly pilot line with a reliability laboratory (BE: Back-end manufacturing).

In addition, the ST Grenoble site hosts some of the Connected Security development servers and provides IT infrastructure management for the configuration management development data used remotely from other STMicroelectronics Connected Security sites (ES_DEV: Server).

The activities of the site cover the following phases, defined in [1] and [9]:

- Security IC embedded software development and testing (phase 1)
- IC development and testing (phase 2)
- IC packaging (phase 4)

Supporting services provided by ST Grenoble include physical site security, IT support, facilities management, and more.

# 4 Conformance claims

The evaluation is based on the Common Criteria (CC) standards, release 1, published in November 2022:

- *Common Criteria for Information Technology Security Evaluation, part 1: Introduction and General Model*[2]
- *Common Criteria for Information Technology Security Evaluation, part 3: Security Assurance Requirements*[3]
- *Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the Specification of Evaluation Methods and Activities* [7]
- *Common Criteria for Information Technology Security Evaluation, Part 5: Pre-Defined Packages of Security Requirements* [8].

The evaluation uses the following methodology:

- *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements*[3]
- *Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology*[4]
- *Minimum Site Security Requirements*[5].

There is no extended component required for this SST.

The assurance components from the assurance level EAL6+ (augmented with ALC_FLR.2) are used in the site evaluation. These assurance components include the following:

- ALC_CMC.5: Advanced support
- ALC_CMS.5: Development tools CM coverage
- ALC_DVS.2: Sufficiency of security controls
- ALC_LCD.1: Developer defined life-cycle processes
- ALC_TAT.3: Compliance with implementation standards (all parts)
- ALC_FLR.2: Flaw reporting procedures

The assurance level chosen for the SST is compliant with the protection profile (PP) [1] and therefore suitable for the evaluation of security ICs. This site security target conforms to part 3 of the Common Criteria.

The chosen assurance components are derived from the EAL6 assurance level within the “Life-cycle support” assurance class. For the assessment of the security measures, attackers with high attack potential are assumed. Therefore, this site supports product evaluations up to EAL6+ (augmented with ALC_FLR.2).

The assurance component ALC_DEL.1 is only applicable to external deliveries to the internal client. The assurance component cannot be used for internal shipment. Internal shipment is covered by ALC_DVS. Therefore, the component ALC_DEL.1 is not applicable for internal shipment.

# 5 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.

The site security target is based on the life cycle defined in [1]. The assets (refer to Section 5.1: Assets), the threats (refer to Section 5.2: Threats), and the organizational security policies (OSP) (refer to Section 5.3: Organizational security policies) defined in this SST are derived from the life cycle defined in the protection profile (PP).

The security problem definition comprises two major so called security problems:

- The first set of security problems includes all kinds of attacks regarding theft (for example, samples), or disclosure (for example, design data). These security problems are described in terms of threats.
- The second set of security problems includes the requirements for the configuration management (for example, controlled production flow) and the control of security measures. These security problems are described in terms of organizational security policies (OSP).

## 5.1 Assets

The following section describes the assets handled on the site.

The site has internal documentation and data that are relevant to maintain the confidentiality and integrity of an intended TOE. This comprises site security concepts and the associated security measures as well as key and cryptographic tools for the encrypted exchange of data. These items are not explicitly listed in the site of assets below.

The integrity of any machine or tool used for development, production, testing, and personalization is not considered as an asset. However, appropriate measures are defined for the site to ensure this important condition.

*Note: The equipment storing sensitive data related to testing activities is considered as an asset.*

### 5.1.1 List of assets

- Logical design data (schematics or HDL sources and design documents)
- Physical design data (topographic information about parts of the chip or the whole chip)
- IC dedicated software
- Specific development aids (tools such as ROM translator)
- Test and characterization related data
- Material for software development support
- Products (wafers, modules, chips, or scrap)

There can be further internal client specific assets such as seals, special transport protection or similar items that support the security of the internal shipment to the internal client. They are handled in the same way as other assets to prevent misuse, disclosure, or loss of these sensitive items or information.

## 5.2 Threats

All the threats endanger the integrity and confidentiality of the intended TOE and the representation of parts of the TOE. The intended TOE protects itself in life cycle phase 7. However, during the development, production, test, and assembly, the TOE and its components are vulnerable to such attacks.

The following threats are described in a general way. However, they are applicable to the site. These shall support the mapping to the security objectives of the site.

**T.Smart-Theft**

During a T.Smart-Theft attack, an attacker tries to access sensitive areas of the site for manipulation, theft or 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. In addition, the attacker may be able to use specific working clothes of the site to conceal the intention.

This attack includes already a variety of targets and aspects according to the various assets listed in Section 5.1: Assets. It shall cover the range of individuals that tries to get unregistered or defects devices that can be used to further investigate the functionality of the device and search for possible exploits. This attacker has limited resources and a low financial budget to prepare the attacks. However, the attacker can spend time to prepare the attack, and the flexibility of the attacker provides a notable risk.

It is expected that such an attacker can be defeated by state of the art physical, technical and procedural security measures like access control and surveillance. In general, an access control concept with two or three levels shall be implemented. If two levels are implemented, the more restrictive level of the access control shall prevent the simple access using a lost or stolen access token. Other restrictions may be need for parallel access by two employees. The technical measures shall include automated measures to support the surveillance.

### T.Rugged-Theft

During a T.Rugged-Theft attack, an experienced thief with specialized equipment for burglary, who may be paid to perform the attack tries to access sensitive areas and manipulate or steal sensitive assets.

This attack applies to a site where the risk may differ regarding the assets. Attackers may be prepared to take high risks for payment. They are sufficiently resourced to circumvent security measures and do not consider any damage to the affected company. The target of the attack may be products that can be sold or misused in an application context. This can comprise devices at a specific testing for cloning or introduction of forged devices. This type of attacker is considered to have the highest attack potential.

The attackers may not be completely defeated by the physical, technical, and procedural security measures. Special measures such as storage of items in safes or strong rooms, or the splitting of sensitive data such as the keys provide additional support against such attacks. Additionally, the unique registration of the products can enhance the protection if they can be disabled or blocked.

### T.Computer-Net

During a T.Computer-Net attack, a hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segment,s to get access to development and/or production systems with the intention to modify the development and/or production process, thus violating integrity, and possibly confidentiality.

A logical attack against the network of the site provides the lowest risk for an attacker. The target of such an attack is to access the company network to obtain information to attack or manipulate a product, or to retrieve data allowing them to change the configuration or the personalization. In addition, such action could also allow the access to a third party company processing or producing the product.

These attackers are considered to have a high attack potential. They may have appropriate technical equipment to perform such an attack. Furthermore, the attacker may have the resource to develop or buy software or hardware, which can exploit known vulnerabilities within the tools and the software used by the company.

Therefore, a protective concept with more than one level is expected. This shall include a firewall to the external network, and further limitations of the network users and the network services for internal subnetworks. In addition, computer users shall have individual accounts, which require authentication. For specific tasks or processes, standalone networks may be required. The protection must be supported by appropriate measures, to update and maintain the computer and network system, and analyze logs that may provide indications for attack attempts.

### T.Accident-Change

During a T.Accident-Change attack, an employee, contractor, or student trainee may exchange products of different production lots / different internal clients during production or changes tool configuration that have an impact on the intended TOE by accident.

Untrained employees, contractors, or student trainees may take products or influence the production systems without considering possible impacts or problems. This threat includes accidental changes, for instance due to working tasks of intern engineers, or maintenance tasks, or contractors within the development and production area.

Such accidental changes can include the modification of configurations for tools that may have an impact on the TOE, the wrong assignment of tools for a dedicated process step. Further examples may be machine failure or misalignment between operators that are responsible for products of the same internal client are mixed during production. This also includes the disposal of sensitive products using the standard flow and not the controlled destruction.

### T.Unauthorised-Staff

During a T.Unauthorised-Staff attack, the unauthorized employees or subcontractors obtain access to assets or systems used for development, configuration management and/or production, so that the confidentiality and/or the integrity of the intended TOE is violated. This can apply to any development and/or production step, and to any asset related to the intended TOE, or its configuration.

The maintenance tasks performed by subcontractors may require their access to computer systems storing sensitive data. The implemented security measures may not work since special dedicated access may be used on the network, or specific tools may be used for this dedicated task. This can include the tools, which process the layout data, for instance in the design center, as well as sensitive test and/or configuration data within the test center.

Additionally, other subcontractors (such as cleaning staff or maintenance staff for the building) get limited access that may allow them to start an attack. The disposal of defected equipment and/or sensitive configuration items must be considered.

The attack potential depends on the trustworthiness of the subcontracted company and the access required within the company. Related to these different measures are required.

### T.Staff-Collusion

During a T.Staff-Collusion attack, an attacker tries to get access to assets handled at the site. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery.

Personal accountability shall be traceable as far as possible. Handover procedures with dual control, enforcement of parallel access by two authorized employees and the split of sensitive knowledge can be implemented to prevent such an attack. The measures depend on the assets that must be protected at the site.

### T.Attack-Transport

During a T.Attack-Transport attack, an attacker tries to get hold of any assets during the internal shipment. The objective is to compromise confidential information or violate the integrity of the assets during the shipment process to allow a modification, cloning, or the direct or indirect retrieval of confidential information.

Confidential information includes design, internal clients or consumer data (such as code and data), or classified product documentation.

The protection of the internal shipment depends on the assets that are exchanged. The protection is related to the assets that must be considered during the site evaluation.

During production, testing and/or assembly, sensitive products, and standard products may be handled in parallel. The threats *T.Accident-Change*, *T.Unauthorised-Staff*, and *T.Staff-Collusion* address this aspect. The rationale of the SST must cover the associated measures against these threats.

## 5.3 Organizational security policies

The requirements of the assurance components of ALC for the assurance level EAL6 + (augmented by ALC_FLR.2) introduce the following policies. The chosen policies support the understanding of the production flow and the security measures of the site. In addition, they allow an appropriate mapping to the security assurance requirements (SAR).

The documentation of the site is under configuration management. This comprises all procedures regarding the evaluated production flow and the security measures that are in the scope of the evaluation.

### P.Config-Items

The configuration management system shall identify uniquely all configuration items. This includes the unique identification of items that are created, generated, developed, or used at the site as well as the received and transferred or provided items.

The configuration management may rely completely on the naming and identification of the received configuration items. In this case, at least the consistency with the expected values must be verified and the unique identification must be ensured. This holds also for test programs or other items that are provided to the site for local use. For configuration items that are created, generated, or developed at the site the naming and identification must be specified. For data like configuration or initialization, the identification and handling must be described.

### P.Config-Control

The procedures for setting up the production and development process for a new product as well as the procedure that allows changes of the initial setup for a product is only applied by authorized personnel. Automated systems support the configuration management and ensure access control or interactive acceptance measures for setup and changes. The procedure for the initial setup of a production and development process ensures that sufficient information is provided by the internal client.

The product setup may include the following information, but these shall only be changed by authorized methods in production and development methods:

- Identification of the product
- Properties of the product when received at the site
- Properties of the product when internally shipped
- Classification of the items (which are security relevant)
- Who (either the name of the site or the internal client) is responsible for destruction of defect devices
- How the product is tested after assembly
- Any configuration of the processed item as part of the services provided by the site
- Which address is used for internal shipment.

### P.Config-Process

The services and processes provided by the site are controlled in the configuration management plan. This comprises incoming items, tools used for the development and production of the product, the management of flaws and optimizations of the process flow as well as the documentation that describes the services and processes provided by the site. A released production and development process is defined and under version control.

At least the documentation that includes the process descriptions and the security measures of the site must be under version control. Measures should be in place to ensure that the evaluated status is ensured. In most cases tools are used to support the production of the site. This includes scripts or batch routines developed by the site or a commercial database system. This can also include service levels or quality parameters.

### P.Reception-Control

The inspection of incoming items done at the site ensures that the received assets comply with the properties stated by the internal client. Furthermore, the identification of the intended TOE is checked. A released production process is defined for the intended TOE. If applicable, this aspect includes a verification to ensure that all the required information and data are available to handle the incoming items.

### P.Accept-Product

The testing and quality control of the site ensures that the released intended TOE complies with the specification agreed with the internal client. Automated measures support the acceptance process. Records are generated for the acceptance process of the assets. Thereby, it is ensured that the properties of the intended OTE are ensured when internally shipped.

### P.Zero-Balance

The site ensures that all sensitive items (security relevant parts of the intended TOEs of different internal clients) are separated and traced on a device basis. For each handover, either an automated or an organizational “two employees-acknowledgement” (four-eyes principle) is applied for functional and defect assets. As per the released production process, the defect assets are either collected at the site or sent back to the internal client.

The following policy covers the packing and handover of products at the site after the applied production flow. A destruction process is mandatory. A destrucction process must be agreed between the internal client and the site who is responsible for the destruction of defect devices. If the destruction is performed by the internal client, the zero-balancing must be appropriately extended.

### P.Product-Transport

Technical and organizational measures ensure the correct labeling of the intended TOE. A controlled internal shipment is applied. The transport supports traceability up to the recipient. If applicable or required, this policy includes measures for packing to protect the product during transport.

The following policy supports the electronic transfer of sensitive assets as specified in this section.

**P.Secure-Scrap**

Controls are in place when the forwarder indicated by the internal client before the handover of the security products. Traceability of the outgoing materials and security products are monitored. Information on freight forwarders is also recorded to ensure traceability and accountability. All outgoing and internal shipments have a dedicated outgoing shipment channel for the transfers of goods (including configuration products) to ensure security.

**P.Data-Transfer**

Any data in electronic format (for example, product specification, release information etc.) that is classified as sensitive or higher security level by the internal client is encrypted to ensure confidentiality of the data.

Confidential or sensitive data transfers in electronic format must be sent in a signed, encrypted, and secure manner. All sensitive configuration or information (include product specification, test programs, or test program specification) is also encrypted to ensure security before sending out to internal clients through email.

**P.Flaw-Remediation**

The site is responsible for the remediation of security flaws. The procedures in place within the site must show how flaw remediation is managed giving assurance on the following topics:

- Acceptance and acting upon all reports of security flaw and requests for corrections to those flaws.
- Flaw remediation guidance to address the TOE users.

## 5.4 Assumptions

The site operating in a production flow must rely on preconditions provided by the previous site. This is reflected by the assumptions that must be defined for the interface.

The assumptions are outside the sphere of influence of STMicroelectronics. The assumptions are needed to provide the basis for an appropriate production process, to assign the product to the released production process, and to ensure the proper handling, storage, and destruction of all the assets that are related to the intended TOE.

**A.Prod-Specification**

The internal client must provide appropriate information (for example, specification, definitions, process limits, process parameters, test requirements, test limits, bond plans) to ensure an appropriate development or production process. The information provided includes the classification of the documents and product.

Depending on the site activities, further assumptions may be required. For example: If the site ships the product to the consumer, the related information must be transferred. If the site receives data from the internal client for the configuration, the integrity if the data must be ensured. Furthermore, depending on the status of the assets an assumption on the already operational self-protection of the product may be added to the rationale of the required security measures.

**A.Item-Identification**

Each configuration item received by the site is appropriately labeled to ensure the identification of the configuration item.

**A.Internal-Shipement**

The recipient (internal client) of the product is identified by the address of the internal client site. The address of the internal client is part of the product setup. The internal client provides the address and shipping information via a secure channel to the ST Grenoble site.

**A.Product-Integrity**

The self-protecting features of the devices are fully operational. It is not possible to influence the configuration and behavior of the devices based on insufficient operational conditions, or any command sequence generated by an attacker or by accident.

### A.Destruct-Scrap

Scrap assets are also transferred. They are destructed at the receiving site, so that they are useless for an attacker.

# 6 Security objectives

## 6.1 Security objectives definition

The security objectives are related to physical, technical, and organizational security measures, the configuration management as well as the internal shipment.

### O.Physical-Access

The combination of physical partitioning between the different access control levels together with technical and organizational security measures allows enough separation of the 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 site enforces two or three levels of access control to sensitive areas of the site. The access control measures ensure that only registered employees and registered visitors can access restricted areas. Sensitive products and data 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 or optical fiber.

A special access control measure with a high efficiency is implemented, which is allowed only two access control levels. For development areas, special measures mean to check the PIN, the fingerprint, or similar authentication mechanisms in addition to a badge.

### O.Security-Control

Assigned personnel of the site, or guards, operate the systems for access control and surveillance, and to respond to alarms. Technical security measures such as video control, motion sensors, and similar sensors support the enforcement of the access control. Personnel are also responsible for registering and ensuring that people from STMicroelectronics escort visitors.

### O.Alarm-Response

The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any sensitive configuration item (asset). After the alarm is triggered, the unauthorized person must still overcome further security measures. The reaction time of the employees or guards is short enough to prevent a successful attack. The areas, which are not permanently manned by employees or guards are under permanent alarms.

### O.Internal-Monitor

The site performs weekly security management meetings. The security management meetings are used to review security incidents, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. In addition, quarterly meetings are organized to discuss about security metrics and events. Furthermore, an internal audit is performed every six months to control the application of the security measures. Sensitive processes may be controlled within a shorter time frame to ensure enough protection.

### O.Maintain-Security

Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This includes the access control system ensuring that only authorized employees have access to sensitive areas, and computer/network systems ensuring that they are configured as required to protect 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 the defined services and the defined connections are accepted. Furthermore, the internal network is separated into production, development, office, and administration networks. Specific networks for development, production, and administration are further logically separated from other internal networks to enforce access control. Access to the production, development networks, and related system is restricted to authorized employees involved in the configuration tasks of the production systems. Every user of an IT system owns a user account and a password. An authentication using a unique user account and password is enforced by all computer systems. The implementation is defined on the protection needs of the data related to the provided processes. For the different networks, different coordinated protection levels are available. User accounts and associated user authentication are defined for network segments transferring sensitive data.

### O.Logical-Operation

All network segments and the computer systems are kept up-to-date (software updates, security patches, virus protection, spyware protection, etc.). The backup of sensitive data and security relevant logs is applied according to the classification of the stored data. The backup handles the same or equivalent logical and physical protection as the data used for processing.

### 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 internal 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 production and development process for each new product. In addition, the site has a process to classify and introduce changes for services and processes of released products. Minor changes are handled by the site. Major changes must be acknowledged by the internal client. A designated team is responsible for the release of new products, and for the classification and the release changes. This team includes specialists for all aspects concerning services and processes. The services and processes can only be changed by authorized personnel. Automated systems support configuration management, and production control.

### 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 and production of the product, for the management of flaws and optimizations of the process flow, and for the documentation that describes the services and processes provided by a site.

### O.Acceptance-Test

The site delivers assets that fulfill the specified properties. Parameter checks, functional and visual checks and tests are performed to ensure the compliance with the specification. The test results are logged to support tracing and the identification of systematic failures.

### O.Staff-Engagement

All employees who have access to sensitive assets and who can move parts of the products out of the defined production and development flow are checked regarding security concerns and have to sign a contract confidentiality clause. The security controls operated on employees include among others a criminal background check. Furthermore, all employees are trained and qualified for their job.

### O.Zero-Balance

The site ensures that all sensitive products (intended TOE of different internal clients) are separated and traced on a device basis. Automated control and/or two employees' acknowledgment during hand-over is applied for functional and defective devices. According to the agreed production or development flow the defect devices are either destroyed at the site or sent to the internal client or the consumer.

**O.Reception-Control**

Upon reception of any intended TOE and 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 internal client address. The internal shipment procedure is applied to the configuration item. The address for the shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as agreed with the internal client. The forwarder supports the tracing of assets during internal shipment. For every sensitive configuration item, the protection measures against manipulation are defined.

**O.Transfer-Data**

Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms to ensure the confidentiality and the 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. The keys are sufficiently protected. The O.Transfer-Data is applicable for internal shipment of such data as well.

**O.Control-Scrap**

The site has measures in place to destruct sensitive documentation, erase electronic media and destroy sensitive assets so that they do not support an attacker. The measures in place also include that the site returns the assets to be scrapped to the supplier, according to the secure shipment procedure of the stakeholder. Sensitive assets can be transferred with the functional devices to be destructed on another site. In such case, this is addressed within assumptions for the other site.

**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
- Communications of remediation to users

## 6.2 Security objectives rationale

The site security target includes a security objective 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 includes a justification that shows that all threats and OSPs are effectively addressed by the security objectives.

The assumptions defined in the site security target cannot be used to cover any threat or OSP of the site. They are seen as preconditions fulfilled either by the site providing the sensitive configuration items, or by the site receiving the sensitive configuration items. Therefore, they do not contribute to the security of the site under evaluation.

Table 4. **Mapping of the security objective**

| Threats and OSP | Security objective | Justification |
|---|---|---|
| T.Smart-Theft | O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Internal-Monitor<br>O.Maintain-Security | The justification of structural technical and organizational measures detects unauthorized access and allows for an appropriate response to the threat.<br>O.Physical-Access ensures that the sensitive areas are physically portioned, and that the access is restricted. An unauthorized person cannot just walk-in.<br>O.Security-Control ensures that an attacker is detected when trying to reach the assets through a sensitive area. |

| Threats and OSP | Security objective | Justification |
|---|---|---|
| | | O.Alarm-Response supports O.Physical-Access and O.Security-Control by ensuring that a response is given to the alarm systems and that the response is quick enough to prevent access to the assets.<br>O.Internal-Monitor and O.Maintain-Security ensure that the above security objectives are managed and maintained.<br>Together, these objectives counter T.Smart-Theft. |
| T.Rugged-Theft | O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Internal-Monitor<br>O.Maintain-Security | The combination of structural, technical, and organizational measures detects unauthorized access and allows for an appropriate response to the threat.<br>O.Physical-Access ensures that the sensitive areas are physically partitioned and access restricted, so an unauthorized person cannot just walk-in.<br>O.Security-Control ensures that an attacker is detected when trying to reach the assets through a sensitive area.<br>O.Alarm-Response supports O.Physical-Access and O.Security-Control by ensuring that a response is given to the alarm systems and that the response is quick enough to prevent access to the assets.<br>O.Internal-Monitor and O.Maintain-Security ensure that the above security objectives are managed and maintained.<br>Together, these objectives counter T.Rugged-Theft. |
| T.Computer-Net | O.Internal-Monitor<br>O.Maintain-Security<br>O.Logical-Access<br>O.Logical-Operation<br>O.Staff-Engagement | O.Logical-Access ensures that the networks are protected with firewall to prevent external or internal unauthorized access, and that machines are secured (such as login and password) to restrict access.<br>O.Logical-Operation ensures that all computer systems used to manage the overall network are kept-up-to date (software updates, security patches, virus, spyware protection, etc.).<br>O.Staff-Engagement ensures that all staff is aware of its responsibilities.<br>O.Internal-Monitor and O.Maintain-Security ensure that the above security objectives are managed and maintained.<br>Together, these objectives counter T.Computer-Net. |
| T.Accident-Change | O.Logical-Access<br>O.Logical-Operation<br>O.Config-Items<br>O.Config-Control<br>O.Zero-Balance<br>O.Staff-Engagement<br>O.Acceptance-Test | Automated measures and control procedures allow preventing accidental changes in sensitive items.<br>O.Logical-Access ensures that the networks are protected with a firewall to prevent external or internal unauthorized access and that machines are secured (such as login and password) to restrict access.<br>O.Logical-Operation ensures that all computer systems used to manage the overall network are kept-up-to date (software updates, security patches, virus, spyware protection, etc.).<br>O.Config-Items ensures that all configuration items for secure products are identified.<br>O.Config-Control ensures that the site procedures for development and manufacturing are known and followed for the operations.<br>O.Zero-Balance ensures that all items are traced and accounted for.<br>O.Staff-Engagement ensures that all staff is aware of its responsibilities.<br>O.Acceptance-Test to ensure that the products to be returned to the internal clients are compliant with their specifications.<br>Together, these objectives counter T.Accident-Change. |
| T.Unauthorised-Staff | O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Internal-Monitor<br>O.Maintain-Security<br>O.Logical-Access | Physical and logical access control prohibits access to the assets. The scrap secure destruction limits the number of assets.<br>O.Physical-Access ensures that the sensitive areas are physically partitioned and access restricted, so an unauthorized person cannot just walk-in.<br>O.Security-Control ensures that an attacker is detected when trying to reach the assets through a sensitive area. |

| Threats and OSP | Security objective | Justification |
|---|---|---|
| | O.Logical-Operation<br>O.Staff-Engagement<br>O.Config-Control<br>O.Zero-Balance<br>O.Control-Scrap | O.Alarm-Response supports O.Physical-Access and O.Security-Control by ensuring that a response is given to the alarm systems and that the response is quick enough to prevent access to the assets.<br>O.Logical-Access ensures that the networks are protected with firewall to prevent external or internal unauthorized access, and that machines are secured (such as login and password) to restrict access.<br>O.Logical-Operation ensures that all computer systems used to manage the overall network are kept-up-to date (software updates, security patches, virus, spyware protection, etc.).<br>O.Staff-Engagement ensures that all staff is aware of its responsibilities.<br>O.Zero-Balance ensures that all items are traced and accounted for.<br>O.Control-Scrap ensures that scrap material cannot be accessed by an unauthorized party.<br>O.Config-Control ensures that sites procedures for development and manufacturing are known and followed for the operations.<br>O.Internal-Monitor and O.Maintain-Security ensure that the above security objectives are managed and maintained.<br>Together, these objectives counter T.Unauthorised-Staff. |
| T.Staff-Collusion | O.Internal-Monitor<br>O.Maintain-Security<br>O.Staff-Engagement<br>O.Zero-Balance<br>O.Control-Scrap<br>O.Transfer-Data | The application of internal security measures combined with the hiring policies that restrict to trust-worthy employees limits unauthorized access to assets.<br>O.Staff-Engagement ensures that all staff is aware of its responsibilities.<br>O.Zero-Balance ensures that all items are traced and accounted for.<br>O.Control-Scrap ensures that scrap material cannot be accessed by an unauthorized party.<br>O.Transfer-Data ensures the integrity of the secure shipment of the data.<br>O.Internal-Monitor and O.Maintain-Security ensure that the above security objectives are managed and maintained.<br>Together, these objectives counter T.Staff-Collusion. |
| T.Attack-Transport | O.Internal-Shipment<br>O.Transfer-Data<br>O.Staff-Engagement<br>O.Internal-Monitor | The application of internal shipment policy ensures that the zero-balance principle is correctly applied.<br>O.Internal-Shipment ensures the traceability and security of products during internal transport.<br>O.Transfer-Data ensures the integrity of the secure delivery of data.<br>O.Staff-Engagement ensures that all staff is aware of its responsibilities.<br>O.Internal-Monitor ensures that the above security objectives are managed and maintained.<br>Together, these objectives counter T.Attack-Transport. |
| P.Config-Items | O.Reception-Control<br>O.Config-Items<br>O.Flaw-Remediation | O.Reception-Control ensures an immediate identification of the product.<br>The security objective O.Config-Items directly enforces the OSP.<br>O.Config-Items ensures that all configuration items for secure products are identified.<br>O.Flaw-Remediation ensures that flaw remediation is performed and flaw status is tracked.<br>Together, these objectives cover P.Config-Items. |
| P.Config-Control | O.Config-Items<br>O.Config-Control<br>O.Logical-Access | Network and Logical (O.Logical-Access) protection and the usage of configuration management tools by authorized people ensure the OSP.<br>O.Config-Items ensures that all configuration items for secure products are identified.<br>O.Config-Control ensures that sites procedures for development and manufacturing are known and followed for the development and manufacturing operations. |

| Threats and OSP | Security objective | Justification |
|---|---|---|
| | | Together, these objectives cover P.Config-Control. |
| P.Config-Process | O.Config-Process | The security objective enforces directly this OSP. |
| P.Reception-Control | O.Reception-Control | The security objective enforces directly this OSP. |
| P.Accept-Product | O.Config-Control<br>O.Acceptance-Test<br>O.Config-Process | Application of a configuration management plan and change management monitored by authorized people ensure that the intended TOE is conformant to the accepted one by the internal client.<br>O.Config-Control ensures that sites procedures for development and manufacturing are known and followed for the development and manufacturing operations.<br>O.Acceptance-Test to ensure that the products to be returned to the internal clients are compliant with their specifications.<br>O.Config-Process ensures that configuration management is used and applied for sites services control. |
| P.Zero-Balance | O.Internal-Monitor<br>O.Staff-Engagement<br>O.Zero-Balance<br>O.Control-Scrap | All assets are traced internally until their possible destruction (O.Zero-Balance, O.Control-Scrap) by trained and authorized person (O.Staff-Engagement) to enforce the OSP.<br>O.Staff-Engagement ensures that all staff is aware of its responsibilities.<br>O.Zero-Balance ensures that all items are traced and accounted for.<br>O.Control-Scrap ensures that scrap material cannot be accessed by an unauthorized party.<br>O.Internal-Monitor ensures that the above security objectives are managed and maintained.<br>Together, these objectives counter P.Zero-Balance. |
| P.Product-Transport | O.Config-Process<br>O.Internal-Shipment<br>O.Transfer-Data | Appropriate procedures for internal and external shipment ensure correct labeling and traceability to the recipient.<br>O.Config-Process ensures that configuration management is used and applied for sites services control.<br>O.Internal-Shipment ensures the traceability and security of products during internal transport.<br>O.Transfer-Data ensures the integrity of the secure shipment of the data.<br>Together, these objectives counter P.Product-Transport. |
| P.Secure-Scrap | O.Security-Control<br>O.Zero-Balance<br>O.Control-Scrap | Appropriate procedures for zero balance to ensure that no secure product is lost or theft.<br>O.Security-Control ensures that an attacker is detected when trying to reach the assets through a secure room.<br>O.Control-Scrap ensures that scrap material cannot be accessed by an unauthorized party.<br>O.Zero-Balance ensures that all items are traced and accounted for.<br>Together, these objectives counter P.Secure-Scrap. |
| P.Data-Transfer | O.Transfer-Data | The security objective enforces directly by the OSP. |
| P.Flaw-Remediation | O.Flaw-Remediation | The security objective enforces directly by the OSP. |

# 7 Extended assurance components definition

No extended components are currently defined in this SST.

# 8 Security assurance requirements

Internal clients using this site security target require a TOE evaluation up to evaluation assurance level EAL6+, potentially claiming conformance with the Eurosmart protection profile [1].

The security assurance requirements (SAR) are chosen from the class ALC (life cycle support) as defined in [3]:

- CM capabilities (ALC_CMC.5)
- CM scope (ALC_CMS.5)
- Developer environment security (ALC_DVS.2)
- Flaw remediation (ALC_FLR.2)
- Development life-cycle definition (ALC_LCD.1)
- Tools and techniques (ALC_TAT.3)

The security assurance requirements listed above fulfill the requirements of [6] because hierarchically higher components are used in this site security target.

## 8.1 Application notes and refinements

The description of the site certification process [6] 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 are described in this site security target. These processes are subject of the evaluation of the site:

- CM capabilities:
  - Section 5.1 in [6], “Application notes for ALC_CMC”, for the relevant application notes.
- CM scope:
  - Section 5.2 in [6], “Application notes for ALC_CMS,” for the relevant application notes.
- Development security:
  - Section 5.4 in [6], “Application notes for ALC_DVS”, for the relevant application notes.
- Flaw remediation:
  - Section 5.5 in [6], “Application notes for ALC_FLR”, for the relevant application notes.
- Life-cycle definition:
  - Section 5.6 in [6], “Application notes for ALC_LCD”, for the relevant application notes.
- Tools and techniques:
  - Section 5.7 in [6], “Application notes for ALC_TAT”, for the relevant application notes.

## 8.2 Security assurance rationale

Since this SST references the PP [1], the life-cycle module used in this PP includes also the processes provided by this site. Therefore, the life-cycle module described in the PP [1] is considered to be applicable for this site.

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 [6] are considered.

Table 5. **Mapping and rationale for ALC_CMC**

| SAR | Security objective | Rationale | Reference |
|---|---|---|---|
| ALC_CMC.5.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labeling.* | O.Config-Items<br>O.Config-Control<br>O.Reception-Control<br>O.Config-Process | The TOE is labeled with its unique reference by the configuration management system as defined by O.Config-Items and O.Config-Control.<br>O.Reception-Control ensures the product identification, and the associated labeling.<br>O.Config-Process provides a configured, and controlled production process. | [ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW]<br>[CS_CONF] |

| SAR | Security objective | Rationale | Reference |
|---|---|---|---|
| ALC.CMC.5.2C: *The CM documentation shall describe the method used to uniquely identify the configuration items.* | O.Config-Control<br>O.Config-Items<br>O.Reception-Control<br>O.Config-Process | The method used to uniquely identify the configuration items that are described in the configuration management documentation. Each item is assigned as a unique identifier (O.Config-Items). The configuration items are tracked throughout the life cycle (O.Config-Control).<br>Incoming inspection according to O.Reception-Control ensures product identification, and the associated labeling.<br>O.Config-Process provides a configured and controlled production process. | [ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW]<br>[CS_CONF] |
| ALC_CMC.5.3C: *The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.* | O.Config-Items<br>O.Config-Control<br>O.Reception-Control<br>O.Config-Process | O.Config-Items includes the internal unique identification of all items. Each product is set up according to O.Config-Control including all necessary items.<br>O.Reception-Control includes the incoming labeling, and the mapping to internal identifications.<br>O.Config-Process ensures that only authorized staff can apply changes. This includes changes related to process flows, procedures, and items of internal clients. Teams are defined to assess and release changes. | [ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_FLR_GL]<br>[CS_CONF] |
| ALC_CMC.5.4C: *The CM system shall uniquely identify all configuration items.* | O.Config-Items<br>O.Config-Control<br>O.Reception-Control | O.Config-Items includes the internal unique identification of all items. Each item is setup according to O.Config-Control including all necessary items.<br>O.Reception-Control includes the incoming labeling and the mapping to internal identification. | [CS_CONF]<br>[ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW] |
| ALC_CMC.5.5C: *The CM system shall provide automated controls such that only authorized changes are made to the configuration items.* | O.Config-Control<br>O.Config-Process<br>O.Logical-Access<br>O.Logical-Operation | The configuration management system is used in accordance with the documented processes. The configuration management system provides automated measures. Only authorized changes are made to the configuration items (O.Config-Control). Access is controlled in a way that only authorized users may make changes (O.Logical-Access). An authentication is necessary to get access to the system (O.Logical-Access). The configuration management system manages all relevant assets (O.Config-Items). | [CS_CONF]<br>[ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW] |
| ALC_CMC.5.6C: *The CM system shall support the production of the TOE by automated means.* | O.Config-Process<br>O.Zero-Balance<br>O.Acceptance-Test | O.Config-Process comprises the automated management of the production processes.<br>O.Zero-Balance ensures the control of all security products during production.<br>The site provides automated tools for the development activities and procedures for their uses regarding O.Acceptance-Test. | [CS_CONF]<br>[ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW] |

| SAR | Security objective | Rationale | Reference |
|---|---|---|---|
| ALC_CMC.5.7C: *The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.* | O.Reception-Control<br>O.Logical-Access | O.Reception-Control ensures the reception procedure of the logical assets from the internal client. The person responsible for accepting the logical assets cannot be the developer.<br>O.Logical-Access supports the control by limiting the access and ensuring the correct operation for all tasks to authorized staff. | [CS_CONF]<br>[ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW] |
| ALC_CMC.5.8C: *The CM system shall clearly identify the configuration items that comprise the TSF.* | O.Config-Items<br>O.Config-Control<br>O.Config-Process | The CM system identified the configuration items as part of the TOE. It is labeled with its unique reference by the configuration management system as defined by O.Config-Items and O.Config-Control.<br>According to O.Config-Process the CM plan describes the services provided by the site. | [ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW] |
| ALC_CMC.5.9C: *The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.* | O.Config-Items<br>O.Config-Control<br>O.Config-Process<br>O.Acceptance-Test | The configuration management system is used in accordance with the documented processes. The configuration management system provides automated measures. Changes are properly recorded to the configuration items (O.Config-Items and O.Config-Control).<br>O.Config-Process ensures that only authorized staff can apply changes. This includes changes related to process flows, procedures, and items of internal clients. Teams are defined to assess and release changes.<br>The site provides automated tools for the development activities and procedures for their uses regarding O.Acceptance-Test. | [ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW] |
| ALC_CMC.5.10C: *The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.* | O.Config-Items<br>O.Config-Control<br>O.Config-Process | The configuration management system is used in accordance with the documented processes. The configuration management system provides automated measures. Changes are properly recorded to the configuration items (O.Config-Items and O.Config-Control).<br>O.Config-Process ensures that changes related to process flows, procedures, and items of internal clients are properly recorded through the process. | [ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW] |
| ALC_CMC.5.11C: *The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.* | O.Reception-Control<br>O.Config-Items<br>O.Logical-Access<br>O.Config-Control<br>O.Config-Process | O.Reception-Control includes the incoming labeling and the mapping to internal identification.<br>The configuration management system provides automated measures. Changes are properly recorded to the configuration items (O.Config-Items and O.Config-Control).<br>O.Logical-Access supports the control by limiting the access and ensuring the correct operation for all asks to authorized staff. | [CS_CONF]<br>[ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW] |

| SAR | Security objective | Rationale | Reference |
|---|---|---|---|
| | | O.Config-Process ensures that the versions are properly recorded through the process. | |
| ALC_CMC.5.12C: *The CM documentation shall include a CM plan.* | O.Config-Control<br>O.Config-Process | The configuration management plan is described in the life-cycle documentation (O.Config-Process). The configuration management system is supported by O.Config-Control. | [ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW] |
| ALC_CMC.5.13C: *The CM plan shall describe how the CM system is used for the development of the TOE.* | O.Config-Control<br>O.Config-Process | The configuration management plan is described in the life-cycle documentation (O.Config-Process). The configuration management system is supported by O.Config-Control. | [ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW] |
| ALC_CMC.5.14C: *The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.* | O.Config-Control<br>O.Config-Process<br>O.Reception-Control<br>O.Config-Items | O.Reception-Control supports the identification of configuration items.<br>The configuration management system provides automated measures, such as the identification and the acceptance process (O.Config-Items and O.Config-Control).<br>O.Config-Process ensures the automated controls of released items. | [ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW] |
| ALC_CMC.5.15C: *The evidence shall demonstrate that all configuration items are being maintained under the CM system.* | O.Reception-Control<br>O.Config-Control<br>O.Config-Process<br>O.Zero-Balance<br>O.Internal-Shipment | The objectives O.Reception-Control, O.Config-Control, O.Config-Process ensure that items are maintained under the CM systems.<br>O.Zero-Balance ensures the control of all security products during production.<br>O.Internal-Shipment includes the packing requirements, the reports, and notifications including the required evidences. | [ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW] |
| ALC_CMC.5.16C: *The evidence shall demonstrate that all the configuration items have been and are being maintained under the CM system.* | O.Config-Control<br>O.Config-Process<br>O.Internal-Shipment | O.Config-Control includes a release procedure as evidence.<br>O.Config-Process ensures the compliance of the process.<br>O.Internal-Shipment ensures that the security shipment requirements are covered. | [ALC_CMC_SW1]<br>[ALC_CMC_SW2]<br>[ALC_CMC_HW] |

The security assurance requirements of the assurance requirements of the assurance class “CM capabilities” listed above are suitable to support the development 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.

The scope of the evaluation according to the assurance class ALC_CMS includes the security products, the complete documentation of the site provided for the evaluation, and the configuration as well as the associated tools. The specifications and descriptions provided by the internal client are not part of the configuration management at the ST Grenoble site.

Table 6. **Mapping and rationale for ALC_CMS**

| SAR | Security objective | Rationale | Reference |
|---|---|---|---|
| ALC_CMS.5.1C *The configuration list includes the following: the TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.* | O.Config-Items<br>O.Config-Control<br>O.Config-Processs | The method used to uniquely identify the configuration items is described in the configuration management documentation. Each item is assigned as a unique identifier (O.Config-Items). The configuration items are tracked throughout the life cycle (O.Config-Control).<br>O.Config-Process ensures the compliance of the process. | ST_GNB_Site_Certification_Config_List |
| ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items. | O.Config-Items<br>O.Config-Control<br>O.Config-Process<br>O.Reception-Control<br>O.Internal-Shipment | Items are uniquely identified by the configuration management system according to O.Config-Items. The configuration items are tracked throughout the life cycle (O.Config-Control).<br>O.Config-Process ensures the compliance of the process.<br>The identification of received products is defined by O.Reception-Control. The identification and preparation of items for shipment is defined by O.Internal-Shipment. | ST_GNB_Site_Certification_Config_List |
| ALC_CMS.5.3C: *For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.* | O.Config-Items | ST Grenoble does not involve contractors for the TOE development. According to O.Config-Items all configuration items for secure products are identified. | ST_GNB_Site_Certification_Confi_List<br>[ALC_LCD_GE] |

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 of the configuration management and the security measures. Since the site certification process focuses on the processes based on the absence of a concrete TOE these assurance requirements are suitable.

Table 7. **Mapping and rationale for ALC_DVS**

| SAR | Security objective | Rationale | 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.* | O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Logical-Access<br>O.Logical-Operation<br>O.Staff-Engagement<br>O.Maintain-Security<br>O.Control-Scrap<br>O.Reception-Control<br>O.Internal-Shipment<br>O.Transfer-Data | The physical protection is provided by O.Physical-Access, supported by O.Security-Control, O.Alarm-Response, and O.Maintain-Security.<br>The logical protection of data and the configuration management is provided by O.Logical-Access and O.Logical-Operation.<br>The reception and incoming inspection supports the detection of attacks during the transport of the security products on the ST Grenoble site, according to O.Reception-Control.<br>The shipment to an internal client is protected by similar measures according to the requirements of the internal client based on O.Internal-Shipment.<br>Sensitive data received by the ST Grenoble site is encrypted according to O.Transfer-Data to ensure access by authorized recipients only. | [ALC_DVS_SM]<br>[ALC_DVS_SZ]<br>[ALC_DVS_CI]<br>[ALC_DVS_NA]<br>[ALC_DVS_IT]<br>[ALC_DVS_SRW]<br>[ALC_DVS_AD]<br>[ALC_DEL] |

| SAR | Security objective | Rationale | Reference |
|---|---|---|---|
| ALC_DVS.2.2C: *The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.* | O.Internal-Monitor<br>O.Logical-Operation<br>O.Maintain-Security<br>O.Zero-Balance | The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced.<br>The associated control and continuous justification is the subject of the objectives O.Internal-Monitoring, O.Logical-Operation, and O.Maintain-Security.<br>All devices including functional and nonfunctional are traced according to O.Zero-Balance. | [ALC_DVS_SM]<br>[ALC_DVS_AD]<br>[ALC_DVS_PP] |
| 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<br>O.Internal-Transport<br>O.Data-Transfer | The reception and incoming inspection supports the detection of attacks during the transport of the security products to the sites according to O.Reception-Control.<br>The shipment to the internal client is protected by similar measures according to the requirements of the internal client based on O.Internal-Shipment.<br>Sensitive data received and send by the sites are encrypted according to O.Data-Transfer to ensure access by authorized recipients only. | [ALC_DVS_SM]<br>[ALC_DVS_AD]<br>[ALC_DVS_SRW] |

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, assembly, and testing of the product can be used by potential attacker for the development of attacks. Further on, the protection profile [1] requires this protection for sites involved in the life cycle of development and production of security ICs.

Table 8. **Mapping and rationale for ALC_LCD**

| SAR | Security objective | Rationale | Reference |
|---|---|---|---|
| ALC_LCD.1.1C : *The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.* | O.Config-Control<br>O.Config-Process | The processes used for identification and manufacturing are covered by O.Config-Control and O.Config-Process. | [ALC_LCD_FM]<br>[ALC_LCD_GE] |
| ALC_LCD.1.2C: *The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.* | O.Config-Process<br>O.Zero-Balance | The life-cycle documentation describes the governance that provides for the necessary control over the development and maintenance of the TOE through O.Config-Process and O.Zero-Balance | [ALC_LCD_FM]<br>[ALC_LCD_GE] |

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.

Table 9. **Mapping and rationale for ALC_FLR**

| SAR | Security objective | Rationale | Reference |
|---|---|---|---|
| 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<br>O.Config-Process | The life-cycle documentation describes the procedures used to track security flaws (O.Config-Process and O.Flaw-Remediation). | [ALC_FLR_GL]<br>[ALC_SOP_PSIRT]<br>[ALC_FLR_TER] |

| SAR | Security objective | Rationale | Reference |
|---|---|---|---|
| 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_GL] |
| 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). | [ALC_FLR_GL]<br>[ALC_SOP_CUS] |
| ALC_FLR.2.4C: *The flaw remediation procedures documentation shall describe the methods use dot 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_TER]<br>[ALC_SOP_CUS]<br>[ALC_SOP_FLR] |
| ALC_FLR.2.5C: *The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and inquiries of suspected security flaws in the TOE.* | O.Flaw-Remediation<br>O.Config-Process | 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_TER] |
| 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_GL]<br>[ALC_SOP_CUS] |
| 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_GL] |
| 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). | [ALC_SOP_CUS]<br>[ALC_FLR_TER] |

The security assurance requirements of the assurance class “Flaw remediation“ listed above shall support the flaw remediation management for secure development of the TOE. The flaw remediation process shall be able to collect flaw, to correct flaws and to communicate to the users. Therefore, this security assurance requirement is suitable for this type of product.

Table 10. **Mapping and rationale for ALC_TAT**

| SAR | Security objective | Rationale | Reference |
|---|---|---|---|
| ALC_TAT.3.1C: *Each development tool used for implementation shall be well defined.* | O.Config-Process | The life-cycle documentation (O.Config-Process) describes the development tools used for implementation, ensuring that they are well defined. | [ALC_CMC_HW]<br>[ALC_CMC_SW2] |
| ALC_TAT3.2C: *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 | The life-cycle documentation (O.Config-Process) provides sufficient guidance on statements, conventions, and directives used in the implementation. | [ALC_CMC_HW]<br>[ALC_CMC_SW2] |
| ALC_TAT.3.3C: *The documentation of each development tools shall unambiguously define the meaning of all implementation-dependent options.* | O.Config-Process | The life-cycle documentation (O.Config-Process) provides sufficient guidance on implementation-dependent options. | [ALC_CMC_HW]<br>[ALC_CMC_SW2] |

The security assurance requirements of the assurance class “Tools and techniques“ listed above must 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.

## 8.3 Dependencies

The dependencies of the assurance requirements are as follows:

Table 11. Dependency mapping

| - | ADV_FSP.2 | ADV_FSP.4 | ADV_IMP.1 | ADV_TDS.1 | ADV_TDS.3 | ALC_CMS.1 | ALC_DVS.1 | ALC_LCD.1 | ALC_TAT.1 |
|---|---|---|---|---|---|---|---|---|---|
| ALC_CMC.5 | - | - | - | - | - | x | x | x | - |
| ALC_CMS.5 | - | - | - | - | - | - | - | - | - |
| ALC_DVS.2 | - | - | - | - | - | - | - | - | - |
| ALC_LCD.1 | - | - | - | - | - | - | - | - | - |
| ALC_TAT.3 | - | - | x | - | - | - | - | - | - |
| ALC_FLR.2 | - | - | - | - | - | - | - | - | - |

The assurance life-cycle is the following. Refer to Table 11:

- ALC_CMC.5: ALC_CMS.1, ALC_DVS.2, ALC_LCD.1
- ALC_CMS.5: None
- ALC_DVS.2: None
- ALC_LCD: None
- ALC_TAT.3: ADV_IMP.1
- ALC_FLR.2: None

Some of the dependencies are not completely fulfilled. ALC_CMS.5, ALC_DVS.2, ALC_LCD.1, ALC_TAT.3, and ALC_FLR.2 are only partially fulfilled, as the site does not represent the entire development process.

# 9 Site summary specification

## 9.1 Site preconditions

The site performed development and test services for secure IC hardware design and embedded software. In addition, the site performs assembly activities for prototyping purposes and IT support activities for the STMicroelectronics Connected Security development sites. To perform these services in a secure way, the internal client of the site needs to support the security processes of the site.

Table 12. **Precondition of assumptions**

| Assumption | Precondition |
|---|---|
| A.Prod-Specification | Appropriate information (for example, specification, definitions, process limits, process parameters, test requirements, test limits, etc.) needs to be available to the site for the development to take place. |
| A.Item-Identification | Delivered items are already labeled. |
| A.Internal-Shipment | In case of physical shipment of security relevant items between the internal client and the site, the internal client needs to agree about the shipment details and procedures.<br>To be able to exchange development data and tools securely, it is necessary to establish a secure channel. Therefore, the types of encryption and signature have to be agreed upon and the necessary keys have to be exchanged. |
| A.Product-Integrity | The items need to be protected against alteration or accidentally altered by an unauthorized user. The data shall be complete and trustworthy. |
| A.Destruct-Scrap | The scrap assets are transferred and are managed as the products for internal transport. |

## 9.2 Site services

Table 13. **Detail of the services provided by the site**

| Service | Details |
|---|---|
| IC embedded software development and testing (Phase 1) and IC development and testing (Phase 2) | • Development and validation phases from the typical lifecycle<br>• Secure development of the design documentation, source code, and guidance documentation<br>• CM system administration<br>• Generation and delivery of the intermediate deliverables<br>• Verification and validation processes (simulations and emulation of hardware and software designs in dedicated test environments). Validation comprises verification of the design with real samples. |
| IT infrastructure and administration | • An appropriate environment for sensitive IT equipment employed to remotely connect the external.<br>• Administration of all services with the support of IT global personnel as detailed in this section |
| IC Packaging (Assembly for prototyping) | • Processes for assembly, testing, and acceptance are set up at ST Grenoble according to the specifications provided |
| Supporting services | • Human resources local management<br>• Physical security<br>• Facilities management |

## 9.3 Objectives rationale

The following rationale provides a justification that shows that all threats and OSP are effectively addressed by the security objectives.

### O.Physical-Access

The site implements a “need-to-know” principle by separation measures using a combination of physical partitioning together with technical and organizational security measures. The access control measures support the enforcement of the separation and the “need-to-know” principle. The handling of assets is restricted to separate security areas. By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft, and T.Unauthorised-Staff can be prevented.

### O.Security-Control

The site is using dedicated personnel for guard services. These personnel are responsible for the operation of the access control systems, for the enforcement of the access control, for the surveillance of the technical alarm sensors and the responses to incidents and the hosting of visitors. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff, and it addresses P.Secure-Scrap.

### O.Alarm-Response

In case of an access attempt to an asset by an unauthorized person the site has an alarm system in place. After the alarm is triggered, the unauthorized person still has to overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack. By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft, and T.Unauthorised-Staff can be prevented.

### O.Internal-Monitor

The established security measures of the site are regularly reviewed by security management meetings and internal audits. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion, T.Attack-Transport, and it addresses P.Zero-Balance.

### O.Maintain-Security

Technical security measures are maintained regularly. This ensures that the systems are working correctly and are configured as required to ensure the protection of the networks and computer systems. In addition, all employees are trained regularly. Hence, this helps to prevent the threats: T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion.

### O.Logical-Access

The development network is strictly separated from the other internal networks and the internet by using firewalls. The different projects inside the developer network are separated by logical directory structure. The access to the different project information is protected by personal credentials. By considering the “need-to-know” principle, only an authorized person has access to the project-relating information. Each user has her/his own user account. Based on their classification, assets are in addition only processed in the according logical security area with regard to the implemented access security measures. It prevents the threats T.Computer-Net, T.Unauthorised-Staff, T.Accident-Change, and it addresses P.Config-Control.

### O.Logical-Operations

The workstations used for development purposes are using authentication measures for the users of these systems. Authentication may include multifactor authentication depending on the type of the development workstation. It prevents the threats T.Computer-Net, T.Unauthorised-Staff, and T.Accident-Change.

### O.Config-Items

A configuration management system is in use, which manages all TOE relating hardware, software, and information. Each item gets an internal unique identification. The threats T.Accident-Change is prevented and the security policy P.Config-Items and P.Config-Control are fulfilled.

### O.Config-Control

Procedures arrange for a formal release of configuration documents and specifications for set-up of wafer production. The information is also stored in the configuration database. Engineering change procedures are in place to classify and introduce changes. The system tool requires personalized controlled access. Each user has access-rights limited to the needs of her/his function. Thereby only authorized changes are possible. It addresses the threats T.Unauthorised-Staff and T.Accident-Change. It supports P.Config-Control, P.Accept-Product.

### O.Acceptance-Test

Items quality and acceptance tests are introduced and released based on the related specifications. The tools, specifications, and procedures for these tests are controlled. It supports P.Accept-Product and it covers T.Accident-Change.

### O.Staff-Engagement

The site has established personnel security measures: all employees who have access to assets are checked regarding security concerns. A confidentiality chapter is included in the employee contract. Furthermore, all employees are trained and qualified for their job. This helps to prevent the threats T.Computer-Net, T.Accident-Change, T.Unauthorised-Staff, T.Staff-Collusion, T.Attack-Transport. It addresses P.Zero-Balance.

### O.Config-Process

The configuration items are tracked throughout the life cycle of the TOE. The procedures may be detailed in the CM plan. It prevents the security policies P.Config-Process, P.Accept-Product, P.Product-Transport.

### O.Zero-Balance

The site executes zero balancing to monitor that no secure object gets lost on-site or during transport. Therefore, the amount of incoming and outgoing objects is managed and monitored by the CM system. This helps to prevent the threat of T.Unauthorised-Staff, T.Staff-Collusion, T.Accident-Change. It prevents the security policy P.Zero-Balance and P.Secure-Scrap.

### O.Transfer-Data

For secure data transfer, transport is handled over to the internal client. All secure information is transferred encrypted form. The internal client gets informed if a new release is available. Furthermore, technical measures like cryptography, separation network, split access permission, and secure storage shall be implemented for this kind of data. This helps to prevent threats from T.Staff-Collusion and T.Attack-Transport. It prevents the security policy P.Product-Transport and P.Data-Transfer.

### O.Flaw-Remediation

If any kind of flaw is discovered during the product life cycle, defined procedures to monitor the flaw and inform the internal client are executed. This addresses the OSP P.Flaw-Remediation and P.Config-Items.

### O.Internal-Shipment

All necessary information regarding the transport has to be shared during the project setup with the internal client. All received objects are entered in the configuration management system for traceability. This helps to prevent threat T.Attack-Transport and it addresses the OSP P.Product-Transport.

### O.Reception-Control

At reception each configuration item including security products are identified by the shipping documents, labels and information in the system. Inspection at reception is counting the number of items and checking the shipping list if applicable. Thereby only correctly identified items are accepted. The OSP P.Config-Items and P.Reception-Control are addressed.

### O.Control-Scrap

Scraps are stored internally in a secure location. They are destructed in a controlled and documented way, following corporate procedures. The destruction of items is done under the supervision of qualified employees. It addresses the threats T.Unauthorised-Staff and T.Staff-Collusion. This addresses OSP P.Zero-Balance and P.Secure-Scrap.

## 9.4 Assurance Measure Rationale

**O.Physical-Access:**

- ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development and production environment.

**O.Security-Control:**

- ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development and production environment.

**O.Alarm-Response:**

- ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development and production environment.

**O.Internal-Monitor:**

- 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.Maintain-Security:**

- ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development and production 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.Logical-Access:**

- ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development and production environment.
- ALC_CMC.5.5C requires that the CM system provide automated measures such that only authorized changes are made to the configuration items.
- ALC_CMC.5.7C requires that the CM system support the production of the TOE by automated means. Thereby this objective contributes to meet the Security Assurance Requirement.
- ALC_CMC.5.11C requires that the CM system identifies the versions of the implementation representation from which the TOE is generated.

**O.Logical-Operation:**

- ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development and production 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.
- ALC_CMC.5.5C requires that the CM system provide automated measures such that only authorized changes are made to the configuration items.

**O.Config-Items:**

- ALC_CMC.5.1C requires that the TOE is labelled with its unique reference.
- ALC_CMC.5.2C requires that the CM documentation shall describe the method used to uniquely identify the configuration items.
- ALC_CMC.5.3C requires that the CM documentation justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.
- ALC_CMC.5.4C requires that the CM system provides a uniquely identification to all configuration items.
- ALC_CMC.5.8C requires the CM system to identify the configuration items that comprise the TSF.
- ALC_CMC.5.9C requires the CM system to support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.
- ALC_CMC.5.10C requires the CM system to provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.
- ALC_CMC.5.11C requires that the CM system identifies the versions of the implementation representation from which the TOE is generated.

- ALC_CMC.5.14C requires the CM plan to describe the procedures used to accept modified or newly created configuration items as part of the TOE.
- The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information.
- ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.3C.
- ALC_CMS.5.3C requires that the developer of each TSF relevant configuration item is indicated in the configuration list.

**O.Config-Control:**

- ALC_CMC.5.1C requires that the TOE is labelled with its unique reference.
- ALC_CMC.5.2C requires that the CM documentation shall describe the method used to uniquely identify the configuration items.
- ALC_CMC.5.3C requires that the CM documentation justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.
- ALC_CMC.5.4C requires that the CM system provides a uniquely identification to all configuration items.
- ALC_CMC.5.5C requires the CM system provide automated measures such that only authorized changes are made to the configuration items.
- ALC_CMC.5.8C requires the CM system to identify the configuration items that comprise the TSF.
- ALC_CMC.5.9C requires the CM system to support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.
- ALC_CMC.5.10C requires the CM system to provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.
- ALC_CMC.5.11C requires that the CM system identifies the versions of the implementation representation from which the TOE is generated.
- ALC_CMC.5.12C requires that the CM documentation provide a CM plan.
- ALC_CMC.5.13C requires that the CM plan describe how the CM system is used for the development of the TOE.
- ALC_CMC.5.14C requires the CM plan to describe the procedures used to accept modified or newly created configuration items as part of the TOE.
- ALC_CMC.5.15C requires an evidence, which demonstrate that all configuration items are being maintained under the CM system.
- ALC_CMC.5.16C requires an evidence, which demonstrate that the CM system is being operated in accordance with the CM plan.
- The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information.
- ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.3C.
- In addition, ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products.

**O.Config-Process:**

- ALC_CMC.5.1C requires that the TOE is labelled with its unique reference.
- ALC_CMC.5.2C requires that the CM documentation shall describe the method used to uniquely identify the configuration items.
- ALC_CMC.5.3C requires that the CM documentation justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.
- ALC_CMC.5.5C requires the CM system provide automated measures such that only authorized changes are made to the configuration items.
- ALC_CMC.5.6C requires the CM system to support the production of the TOE by automated means.
- ALC_CMC.5.8C requires the CM system to identify the configuration items that comprise the TSF.
- ALC_CMC.5.9C requires the CM system to support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.
- ALC_CMC.5.10C requires the CM system to provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.
- ALC_CMC.5.11C requires that the CM system identifies the versions of the implementation representation from which the TOE is generated.
- ALC_CMC.5.12C requires that the CM documentation provide a CM plan.

- ALC_CMC.5.13C requires that the CM plan describe how the CM system is used for the development of the TOE.
- ALC_CMC.5.14C requires the CM plan to describe the procedures used to accept modified or newly created configuration items as part of the TOE.
- ALC_CMC.5.15C requires an evidence, which demonstrate that all configuration items are being maintained under the CM system.
- ALC_CMC.5.16C requires an evidence, which demonstrate that the CM system is being operated in accordance with the CM plan.
- The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information.
- ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.3C.
- ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products.
- ALC_LCD.1.2C requires control over the development and maintenance of the TOE.
- ALC_FLR.2.1C requires that the flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
- ALC_FLR.2.5C requires that 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.
- ACL_TAT.3.1C requires that the documentation of each development tool used for implementation is well-defined.
- ALC_TAT.3.2.C requires that the documentation of each development tool unambiguously defines the meaning of all statements as well as all conventions.
- ALC_TAT.3.3C requires that the documentation of each development tool unambiguously defines the meaning of all implementation-dependent options.

**O.Acceptance-Test:**

- ALC_CMC.5.6C requires the CM system to support the production of the TOE by automated means.
- ALC_CMC.5.9C requires the CM system to support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.

**O.Staff-Engagement:**

- ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development and production environment.

**O.Zero-Balance:**

- ALC_CMC.5.6C requires the CM system to support the production of the TOE by automated means.
- ALC_CMC.5.15C requires an evidence, which demonstrate that all configuration items are being maintained under the CM system.
- 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.
- ALC_LCD.1.2C requires control over the development and maintenance of the TOE.

**O.Reception-Control:**

- ALC_CMC.5.1C requires that the TOE is labelled with its unique reference.
- ALC_CMC.5.2C requires that the CM documentation shall describe the method used to uniquely identify the configuration items.
- ALC_CMC.5.3C requires that the CM documentation justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.
- ALC_CMC.5.4C requires that the CM system provides a uniquely identification to all configuration items.
- ALC_CMC.5.7C requires that the CM system support the production of the TOE by automated means. Thereby this objective contributes to meet the Security Assurance Requirement.
- ALC_CMC.5.11C requires that the CM system identifies the versions of the implementation representation from which the TOE is generated.
- ALC_CMC.5.14C requires the CM plan to describe the procedures used to accept modified or newly created configuration items as part of the TOE.
- ALC_CMC.5.15C requires an evidence, which demonstrate that all configuration items are being maintained under the CM system.

- ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.3C.
- ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE. This includes also the protection during the transport between production sides
- ALC_DVS.2.3C: requires that the evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and the integrity of the product.

**O.Internal-Shipment:**

- ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development and production environment.
- ALC_CMC.5.15C requires an evidence, which demonstrate that all configuration items are being maintained under the CM system.
- ALC_CMC.5.16C requires an evidence, which demonstrate that the CM system is being operated in accordance with the CM plan.
- ALC_CMS.5.2C according the unique identification of the packing as configuration item.
- ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE. This includes also the protection during the transport between production sides.
- ALC_DVS.2.3C: requires that the evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and the integrity of the product.

**O.Control-Scrap:**

- ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE. This includes also the protection during the transport between production sides.

**O.Transfer-Data:**

- ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE. This includes also the protection during the transport between production sides.
- ALC_DVS.2.3C: requires that the evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and the integrity of the product.

**O.Flaw-Remediation:**

- ALC_FLR.2.1C requires that the flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
- ALC_FLR.2.2C requires that 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.
- ALC_FLR.2.3C requires that the flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
- ALC_FLR.2.4C requires that the flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
- ALC_FLR.2.5C requires that 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.
- ALC_FLR.2.6C requires that the procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.
- ALC_FLR.2.7C requires that the procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
- ALC_FLR.2.8C requires that the flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

# 10 Documentation references

Table 14. Documentation references

| Reference | Document |
|---|---|
| [1] | *Eurosmart Security IC Platform Protection Profile with Augmentation Packages*, version 1.0, BSI-CC-PP-0084-2014 |
| [2] | *Common Criteria for Information Technology Security Evaluation, part 1: Introduction and General Model*, CC:2022, revision 1, CCMB-2022-11-001, November 2022 |
| [3] | *Common Criteria for Information Technology Security Evaluation, part 3: Security Assurance Requirements*, CC:2022, revision 1, CCMB-2022-11-003, November 2022 |
| [4] | *Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology*, CEM:2022, revision 1, CCMB-2022-11-006, November 2022 |
| [5] | *Minimum Site Security Requirements*, version 3.1, December 2023 |
| [6] | *Supporting Document, Site Certification*, October 2007, version 1.0, Revision 1 |
| [7] | *Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the Specification of Evaluation Methods and Activities*, CC:2022, revision 1, CCMB-2022-11-004, November 2022 |
| [8] | *Common Criteria for Information Technology Security Evaluation, Part 5: Pre-Defined Packages of Security Requirements*, CC:2022, revision 1, CCMB-2022-11-005, November 2022 |
| [9] | *Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile*, version 1.5, BSI-CC-PP-0117 |
| [10] | *Site Security Target Template*, Eurosmart, version 2.0, April 2021 |

# 11 Deliverable references

Table 15. **Deliverable references**

| Reference | Deliverable name | Developer reference |
|---|---|---|
| ST_GNB_Site_Certification_Config_List | ST Grenoble Site Certification Configuration List | ST_GNB_Site_Certification_Config_List |

## Revision history

Table 16. **Document revision history**

| Date | Version | Changes |
|---|---|---|
| 05-Sep-2025 | 1 | Initial release. |
| 12-Sep-2025 | 2 | Updated the following:<br>• Section 2.1: Site security target reference<br>• Section 8.2: Security assurance rationale<br>• Section 8.3: Dependencies |

## Contents

# List of tables

**IMPORTANT NOTICE – READ CAREFULLY**

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice.

In the event of any conflict between the provisions of this document and the provisions of any contractual arrangement in force between the purchasers and ST, the provisions of such contractual arrangement shall prevail.

The purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgment.

The purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of the purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

If the purchasers identify an ST product that meets their functional and performance requirements but that is not designated for the purchasers' market segment, the purchasers shall contact ST for more information.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.