Fraunhofer Institute for Applied and Integrated Security AISEC
Lichtenbergstraße 11
85748 Garching
Germany

Site Security Target Fraunhofer AISEC

Version 1.3

2024-01-31

Common Criteria Information Technology Security Evaluation

Table of contents

1 SST reference

Title:	Site Security Target Fraunhofer AISEC
Version:	1.3
Date:	2024-01-31
Author:	Fraunhofer Institute for Applied and Integrated Security AISEC
EAL covered:	ALC-SARs taken from EAL7

2 SST introduction

The present SST is based on the Eurosmart Site Security Target Template [1] with adaptations such that they fit the site, which provides IC testing services only.

3 Site reference

Site name:	Fraunhofer AISEC
Site address:	Lichtenbergstraße 11, 85748 Garching, Germany
Site owner:	Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V.

Only parts of the site are within the scope of the evaluation.

4 Site description

4.1 Physical scope

Fraunhofer AISEC is in one building solely occupied by Fraunhofer Gesellschaft e.V. The following locations of the site as specified in section 3 above are in the scope of the evaluation:

- Second upper floor (for US readers: third floor):
  - Hardware Security Laboratory (secure area for storage and testing of secure products),
- Ground Floor (for US readers: first floor):
  - Reception desk (CCTV and alarm system operation),
  - Facility management office (access control management).
- Basement:
  - Security systems room (secure area hosting CCTV/access control/alarm systems).

The locations listed above contain secure areas with restricted access under control of AISEC. Only authorized personnel have access to these areas. Within the Hardware Security Laboratory, only trained members of the HWS team are entitled to access sensitive information like physical samples and test result data. To enforce such access restriction, a combination of physical, procedural, personnel and logical measures has been installed.

4.2 Logical scope

The site performs testing of security integrated circuits. The following life-cycle phases as defined in the Protection Profiles (PP) [3] and [4] are subject of this SST:

- Phase 2: IC Development (i.e., testing of engineering samples)
- Phase 3: IC Manufacturing and all phases after that (i.e., testing of final products).

The following services and/or processes provided by Fraunhofer AISEC are in the scope of the site evaluation process:

- Testing of security integrated circuits,
- receiving of test samples from client,
- receiving of test plans from client,
- providing of test procedures and test result data to client,
- storing of test plans and test results data on secure servers,
- storing of test samples before sending back to the client,
- secure reception and preparation for sending of secure tangible items,
- secure reception and provision of data (non-tangible items).

The complete logical flow of the security ICs and smart card related devices (i.e., security products) at the site is covered by this SST. In addition, the management of the security-products-related processes and the site security are also covered by this SST. The product flow of the security products on the site starts with the receipt of the TOE and the corresponding test plan up to providing the test result data. If all testing has been performed, all test samples including defective or rejected products are returned to the client.

The site does not directly contribute to the development of the intended TOE in the sense of Common Criteria. Using the devices provided by the client, the site offers testing services according to the test plan of the client. Within the limits of the client’s test plan, on-site suitable test procedures are created and applied. The applied test procedures and the resulting test result data are then delivered to the client, and so are the test samples. This is regarded as internal shipment and is covered under aspect ALC_DVS.2 (ALC_DEL is not applicable, as delivery to consumers of the secure product is not conducted by the site).

5 Conformance claim

The present SST is conformant to following CC Version 3.1 Revision 5 (April 2017) documents:

- *Common Criteria for Information Technology Security Evaluation,*
  - Part 1: Introduction and general model, CCMB-2017-04-001,
  - Part 2: Security functional components, CCMB-2017-04-002,
  - Part 3: Security assurance components, CCMB-2017-04-003,
- *Common Methodology for Information Technology Security Evaluation, CCMB-2017-04-004.*

The present SST is *CC Part 3 conformant,* as the evaluation of the site comprises the following Security Assurance Components (SARs):

- ALC_CMC.5 Advanced support
- ALC_CMS.5 Development tools CM coverage
- ALC_DVS.2 Sufficiency of security controls

The chosen assurance components of the assurance class 'Life-cycle Support' are taken from assurance level EAL7. For the assessment of the security measures attackers with ***high attack potential*** are assumed. Therefore, the site supports product evaluations up to the highest ALC requirements defined by CC Version 3.1 Revision 5.

Remark: Due to the offered services the Security Assurance Components ALC_DEL, ALC_LCD, ALC_TAT and ALC_FLR are not applicable for the site. That is, a product may claim compliance to aforementioned SARs, and still use this site. The SARs must then be covered by other sites involved in the TOE's life cycle

6 Security problem definition

6.1 Assets

This section describes the assets handled at the site. They can be grouped within the following categories:

- **Physical assets:**
    - Test samples of security integrated circuits from the client
    - Accessories to test samples from the client
- **Document assets:**
    - Test plans from the client
    - Implementation details from the client
    - Test reports created on-site
    - CC documentation for the site (SST, ALC-DVS/CM documentation)
- **Data assets:**
    - Test procedures created on-site
    - Raw test data (e.g., power consumption or EM emanation traces) created on-site

6.2 Threats

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of assets, mainly test samples and corresponding test data. The attacker has sufficient 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 camouflage the intention.

T.Rugged-Theft: An attacker with specialized equipment for burglary, who may be paid to perform the attack, tries to access sensitive areas, and manipulate or steal assets.

T.Computer-Net: A potentially paid hacker with substantial expertise using standard equipment attempts to remotely access sensitive network segments to get access to
(1) development data with the intention to violate confidentiality and potentially also integrity, or
(2) development computers with the intention to modify the development process.

T.Accident-Change: An employee or contractor may exchange products of different production lots or software of different clients during development/production by accident.

T.Unauthorised-Staff: Employees or subcontractors not authorized to get access to assets may violate the confidentiality and potentially also the integrity of products.

T.Staff-Collusion: An attacker tries to get access to assets by getting support from one employee through extortion or bribery.

T.Attack-Transport: An attacker tries to get access to shipped physical security objects when shipped in or out of the site with the intention to compromise confidentiality and/or integrity of the product design data, client and/or consumer data or in classified product documentation.

6.3 Organizational security policies

P.Config-Items: The configuration management system shall be able to uniquely identify configuration items. This includes the unique identification of items that are used for testing.

P.Config-Control: The procedures for setting up the testing process shall be applied by authorized personnel only. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes. The test plan ensures that the client provides sufficient information.

P.Reception-Control: The inspection of incoming items done at the site ensures that the received configuration items comply with the properties stated by the client. Furthermore, it is verified that the items can be identified and assigned to a specific product.

P.Zero-Balance: The site ensures that all sensitive items (security relevant parts of the TOEs of different 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 defective assets. After testing, all assets are sent back to the client. The send back procedures are agreed upon together with the client.

P.Product-Transport: Technical and organizational measures shall ensure the correct labelling of the product or item parts. A controlled internal shipment and/or external delivery shall be applied. The transport supports traceability up to the acceptor. If applicable or required, this policy shall include measures for packing if required to protect the product during transport.

P.Transfer-Data: Any data in electronic form (e.g., test plans, test result data) that is classified as sensitive or higher security level by the client is encrypted to ensure confidentiality of the data. In addition, measures are used to control the integrity of the data after the transfer.

6.4 Assumptions

A.Product-Setup: The site participates in the testing of products. To define the participation of the site in the development/production while maintaining quality, for each product the client will manage the activities to be performed by the site in terms of the test plan provided and the acceptance of the test results by the client. This also covers the setup of secure communication, including key exchange and if required definition of encryption method.

A.Item-Identification: Each configuration item received by the site is appropriately labelled by the sending site to ensure the identification of the configuration item.

A.Internal-Shipment: For incoming items, the client selects the forwarder. For outgoing items, either the client or the site selects the forwarder. If the site selects the forwarder, the client’s approval of the forwarder and its shipping terms and conditions is necessary. Depending on who selects the forwarder, shipping and tracing of the shipment is under control of the client or the site, respectively.

7 Security objectives

O.Physical-Access: The combination of physical partitioning between the different access control levels together with technical and organizational security measures allows a sufficient separation of employees to enforce the “need to know” principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorized people. The access control measures ensure that only registered employees can access restricted areas.

O.Security-Control: Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like motion sensors and similar kinds of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, contractors, and suppliers.

O.Alarm-Response: The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any asset. After the alarm is triggered, the unauthorized person still must overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack.

O.Internal-Monitor: The site performs security management meetings at least every year. 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. Furthermore, an internal audit is performed every year to control the application of the security measures.

O.Maintain-Security: Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorized employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.

O.Logical-Access: The site enforces a logical separation between the internal network and the internet by a firewall. The security measures ensure that only defined services and defined connections are accepted on the internal network. The internal network is appropriately separated to prevent interference between the different environments (office and secure laboratories). Secure network for secure services and configuration is physically separated from any internal network to enforce access control. Access to the secure network and associated systems is restricted to authorized employees working in the related area or involved in the configuration tasks of the production systems. Every user of an IT system has his/her own user account and password. Workstations enforce that every user authenticates using a password and has a unique user ID.

O.Logical-Operation: All logical protection measures are maintained and updated as required. In general, updates are checked before application to ensure authenticity, compatibility, continuity of service and protection against malware. No backup of test plans and test result data is performed for confidentiality reasons.

O.Config-Items: The site has a configuration management system that manages products and parts used. A unique internal identification is assigned to each product to uniquely identify configuration items and allow an assignment to a client. Also, the test procedures and test results are covered by the configuration management.

O.Config-Process: The configuration management is controlled by corresponding tools and procedures for the test plan, test procedures and test results as well as for the documentation that describes the services and/or processes provided by the site.

O.Staff-Engagement: The work contract signed by the employee includes a general confidentiality agreement to protect sensitive information against disclosure. In addition, personnel sign a specific personal NDA. Furthermore, all employees get training on a regular basis that shall ensure the required security awareness and the knowledge of the processes.

O.Zero-Balance: The tracing of functional and defect devices ensures that no security devices are lost during the testing and that all functional and defect devices are sent back to the client after the testing is finished.

O.Reception-Control: The incoming inspection ensures the correct amount and identification of test samples and the verification of the security measure(s) applied to control the integrity during shipment (the process is the starting point of the internal tracing). If an assignment cannot be applied, the product is separated until the identification is clarified.

O.Internal-Shipment: Only trustworthy forwarders are chosen for the transportation of secure products. Prior to transportation, the security products are packed by the client or in the secure area (in agreement with the client) so that no product can get lost accidentally. The four-eyes principle is applied to prevent a single person from uncontrolled access to secure products. Outgoing shipments are performed to recipients/addresses that have been authorized by the client beforehand. If devices are transferred site-internally to the secure area, at minimum two authorized employees are necessary to accompany the devices the whole time from handover by the forwarder until arrival in the secure area.

O.Transfer-Data: The protection of exchanged sensitive data is using encryption as agreed with the client beforehand (e.g., using PGP or GPG). Key management ensures that keys are protected from unauthorized disclosure and that only authorized employees can decrypt sensitive data being transferred.

Remark: As the site does not perform any delivery to consumers of the TOE, there is no security objective about external delivery.

8 Extended assurance components definition

No extended assurance components are defined in this SST.

9 Security assurance requirements

The security assurance requirements selected for the site shall support evaluations up to assurance level EAL7. These security assurance requirements include or exceed the augmentations defined in the PPs [3] and [4]:

ALC_CMC.5 Advanced support

ALC_CMS.5 Development tools CM coverage

ALC_DVS.2 Sufficiency of security controls

The security assurance requirements listed above fulfil the requirements of [9] because hierarchically higher components than the defined minimum site requirements (ALC_CMC.3, ALC_CMS.3, ALC_DVS.1, see section 3.2.3 of [9]) are used in this SST. The description of the site certification process [9] includes specific application notes on the SARs. 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 an SST, the associated processes for the handling of products, or “intended TOEs” are in the scope of and described in this SST. These processes are subject to the evaluation of the site.

Application notes and refinements on ALC_CMC.5

Refer to application notes for site certification in [9], section 5.1 ‘Application Notes for ALC_CMC’.

Due to the Eurosmart PP refinements in [3], [4] for ALC_CMS (see below) not being applicable those for ALC_CMC are also not applicable. At the site, a CM plan is in use to manage the test plans, test procedures and test results that are input or output of the testing services which are in the scope of this certification.

Application notes and refinements on ALC_CMS.5

Refer to application notes for site certification in [9] section 5.2, *Application Notes for ALC_CMS*.

Due to these application notes the refinements from the Eurosmart PPs [3], [4] (see Section 6.2.1.3) are not applicable.

Application notes and refinements on ALC_DVS.2

Refer to application notes for site certification in [9] section 5.4 *Application Notes for ALC_DVS*.

Refer to application note in section 6.2.1.2 *Refinements regarding Development Security (ALC_DVS)* in the Eurosmart PP [3] (application note 26) and [4] (application note 27).

Refer to refinement in section 6.2.1.2 *Refinements regarding Development Security (ALC_DVS)* in the Eurosmart PP [3] and [4].

10 Site summary specification

10.1 Services of the site

The following services and/or processes provided by Fraunhofer AISEC are in the scope of the site evaluation process:

- **Testing of security integrated circuits**,
- receiving of test samples from client,
- receiving of test plans from client,
- providing of test result data to client,
- storing of test plans and test results data on secure servers,
- storing of test samples and scrap before sending back to the client,
- secure reception and preparation for sending of secure tangible items,
- secure reception and provision of data (non-tangible items).

10.2 Preconditions required by the site

This section provides background information on the assumptions defined in section 6.4. The site performs testing of secure IC hardware, and the client needs to support the site security measures with specific information and deliverables. In detail, the client must meet the following preconditions to ensure proper asset protection on site and during transport.

Precondition according to A.Product-Setup: The client must define the test activities to be performed by the site. In addition, the client must define the inputs for the site as well as the acceptance of the results. For secure communication, keys are exchanged securely first, and any data assets are encrypted prior to exchange with the client (e.g., using PGP or GPG). The concrete encryption method must be agreed on with the client beforehand.

Precondition according to A.Item-Identification: The client should properly label all TOE related items to guarantee a unique identification (when not available for incoming test samples, the site will label these with unique identifiers).

Precondition according to A.Internal-Shipment: The client is responsible for the transport to the site. The client or the site is responsible for the transport back to the client. This comprises selection of the forwarder (to be approved by the client if selected by the site). For outgoing transport, beforehand the client must define the shipping address and agree to packaging and corresponding integrity protection measures to be applied by the site.

10.3 Evaluation documentation

The scope of the evaluation according to assurance classes AST and ALC as defined and refined in [9] comprises handling and testing of security ICs and the complete documentation of the site provided for the evaluation:

Assurance class	Assurance component	Evaluation documentation
AST SST evaluation	AST_CCL.1	**Site Security Target Fraunhofer AISEC (this SST)**
	AST_ECD.1	
	AST_INT.1	
	AST_OBJ.1	
	AST_REQ.1	
	AST_SPD.1	
	AST_TSS.1	
ALC Life-cycle definition	ALC_CMC.5	**Configuration Management Fraunhofer AISEC**
	ALC_CMS.5	
	ALC_DVS.2	**Development Security Fraunhofer AISEC**

Table 1: Evaluation documentation

11 Rationales

11.1 Security objectives rationale

Threat or OSP	Security objectives	Rationale
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical, and organizational measures detects unauthorized access and allows for appropriate response to any threat during working hours and during off-time.
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical, and organizational measures detects unauthorized access and allows for appropriate response to any threat during working hours and during off-time.
T.Computer-Net	O.Logical-Access O.Logical-Operation O.Internal-Monitor O.Staff-Engagement O.Maintain-Security	The technical and organizational measures prevent unauthorized access to the internal network.
T.Accident-Change	O.Logical-Access O.Logical-Operation O.Config-Items O.Config-Process O.Staff-Engagement O.Zero-Balance	Configuration control, product tracing and product testing together with training and qualification of employees ensure a controlled testing procedure.
T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Zero-Balance	Physical and logical access control limits the access to products and the testing to authorized persons. Further organizational measures like product tracing and collection of defective devices prevent uncontrolled access to products.
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Zero-Balance O.Transfer-Data	The engagement of trustworthy employees and internal controls prevent theft or modification of products.
T.Attack-Transport	O.Internal-Shipment	The procedure ensures a secure exchange of items.
P.Config-Items	O.Reception-Control O.Config-Items O.Zero-Balance	The incoming control and configuration control ensures the correct assignment of the input for testing.
P.Config-Control	O.Config-Items O.Logical-Access O.Zero-Balance	The Configuration Control and the authentication procedure ensure product specific set-up for the testing.
P.Reception-Control	O.Reception-Control	The incoming control ensures the correct assignment of the input of the production.
P.Zero-Balance	O.Internal-Monitor O.Staff-Engagement O.Zero-Balance	The tracing of all products (functional and defect) ensures the shipment of all products initially received from the client.
P.Product-Transport	O.Config-Process O.Internal-Shipment O.Zero-Balance O.Transfer-Data	The configuration control and internal tracing assure the correct preparation for shipment with the product specific labelling.

Threat or OSP	Security objectives	Rationale
P.Transfer-Data	O.Transfer-Data	The procedure ensures a secure exchange of non-tangible items.

Table 2: Coverage of threats and OSPs by security objectives

Security objective	Threats and OSPs	Rationale
O.Physical-Access: Access to the building is controlled. The access control is enforced by physical measures and associated surveillance by cameras. Within the building, areas are separated if required by the purpose of the area (access levels entrance, employee and secure). During 24/7 a short response time on any alarm or security relevant event is ensured. The structural measures of the access levels provide an increasing resistance against overcoming the protection. While intrusion into the building may be immediate, alarm monitoring starts at the building perimeter, and to enter secure areas inside the building, e.g., those used to store devices during off-time, provide a resistance that should significantly delay an intruder.	T.Smart-Theft T.Rugged-Theft T.Unauthorised-Staff	T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff are addressed by these structural and technical measures. The construction measures limit the access to the secure areas. The access levels require an increasing time from outside to the inside to get over. The objective is supported by O.Security-Control that provides motion and intrusion detection mechanisms so that security guards are alerted, who can prevent a successful attack before the attacker is able to get over the structural and technical measures. In general, the structural and technical measures enforce the access control measures.
O.Security-Control: The surveillance and alarm system comprise CCTV that covers the surroundings of the building and some internal views, intrusion detection at the building perimeter and motion detection inside the building. The access control system can only be configured by the facility management, access to the secure area must be granted by the head of the security environment. Access to the CCTV, alarm and access control systems is also controlled.	T.Smart-Theft T.Rugged-Theft T.Unauthorised-Staff	T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff are addressed by the alarm system. Intrusion detection and video surveillance ensure a timely alert of the security guards. Thereby they can avoid successful attacks with access to sensitive products or items.
O.Alarm-Response: Alarms are signalled at a remote security center. Furthermore, local CCTV and alarm system terminals at the reception desk are present for the local security guard. The security guard on site can immediately respond to the alarm event, the remote security center guarantees to dispatch security guards to respective areas in a time less than the delay a detected intruder is facing before getting hold of any assets (guaranteed response time and expected delay are not stated here for security reasons).	T.Smart-Theft T.Rugged-Theft T.Unauthorised-Staff	T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff are addressed by the alarm response. There is one security guard on site and a remote security center is staffed 24/7, able to take further action if needed according to the action plan.
O.Internal-Monitor: Internal training is performed to ensure the security awareness of the employees. Furthermore, all security incidents that occurred since the last security management meeting are discussed and considered for the actual assessment of the remaining risks.	T.Smart-Theft T.Rugged-Theft T.Computer-Net T.Unauthorised-Staff T.Staff-Collusion P.Zero-Balance	T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion as well as P.Zero-Balance are addressed because issues can be detected, and the application of the security measures is verified. The generated logs of the various systems provide one basis for the analysis, the review of the security measures provide one source for the current risk assessment.

Security objective	Threats and OSPs	Rationale
O.Maintain-Security: The alarm system, the video control system and the physical access control system require regular functional checks to ensure the correct operation. These checks are applied according to the recommendations of the manufacturer. Alerts are traced to allow the distinction between false alarms and attack attempts. The logging of the physical access control system is checked, and abnormal logs are verified to detect irregular behaviour of employees or manipulation attempts. Warnings and error messages of firewall and network are logged and reviewed by the system administrator.	T.Smart-Theft T.Rugged-Theft T.Computer-Net T.Unauthorised-Staff T.Staff-Collusion	T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion are addressed by the maintenance of the security systems because the maintenance measures ensure continuous and effective operation of the security measures.
O.Logical-Access: The IT network is split into different segments for different purposes. The protection of the network segments is applied based on the classification of the operated data. The separation is enforced by network elements like a firewall and/or by physical separation, as applicable. User accounts are managed to limit the access rights to the required level.	T.Computer-Net T.Accident-Change T.Unauthorised-Staff P.Config-Control	T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff as well as P.Config-Control are addressed by the separation of network segments. The network segments are built and configured to prevent misuse. Users have their own account with dedicated password and the account is limited to the access rights required by the job task and their responsibility following a strict need-to-access principle.
O.Logical-Operation: In general, updates are checked before application to ensure authenticity, compatibility, continuity of service and protection against malware. Data assets provided by the client and raw test data are not backed-up for confidentiality reasons. All logical protection measures are maintained and updated as required.	T.Computer-Net T.Accident-Change T.Unauthorised-Staff	T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff are addressed by the maintenance of the network segments and the computer systems. These measures ensure the correct and controlled operation of the network.
O.Config-Items: Each item received is assigned to a unique product part number. For each product, the required part numbers are used to define the product within the configuration management. The configuration management system together with the UID handling ensures the individual tracking of security products.	T.Accident-Change P.Config-Items P.Config-Control	T.Accident-Change, as well as P.Config-Items and P.Config-Control are addressed by the measures used to identify configuration items.
O.Config-Process: The configuration management comprises automated measures during testing. To ensure the correct set up of a process and to ensure reproducible results within the testing appropriate procedures are defined. Further on a team of employees responsible for the product handling and the testing is defined to plan, organise, and control the testing process. This also includes the adaptation of test procedures according to the client’s test plan and related test goals.	T.Accident-Change P.Config-Control P.Accept-Product P.Shipping-Support P.Product-Transport	T.Accident-Change as well as P.Config-Control, P.Accept-Product, P.Shipping-Support and P.Product-Transport are addressed by the requirement to manage the products (also during transportation) and the testing environment.

Security objective	Threats and OSPs	Rationale
O.Staff-Engagement: The work contract signed by the employee includes a general confidentiality agreement to protect sensitive information against disclosure. In addition, personnel sign a specific personal NDA. Furthermore, all employees get training on a regular basis that shall ensure the required security awareness and the knowledge of the processes.	T.Computer-Net T.Accident-Change T.Unauthorised-Staff T.Staff-Collusion P.Zero-Balance	T.Computer-Net, T.Accident-Change, T.Unauthorised-Staff and T.Staff-Collusion as well as P.Zero-Balance are addressed because legal obligations and security awareness supports the prevention and detection of security violations.
O.Zero-Balance: The tracing of functional and defective devices ensures that no security devices are lost during the testing and that all functional and defective devices are sent back to the client after the testing is finished.	T.Accident-Change T.Unauthorised-Staff T.Staff-Collusion P.Config-Items P.Config-Control P.Zero-Balance P.Product-Transport	T.Accident-Change, T.Unauthorised-Staff and T.Staff-Collusion as well as P.Zero-Balance, building on P.Config-Items and P.Config-Control, and P.Product-Transport are addressed because any missing security device can be detected by this process, on-site and during transportation.
O.Reception-Control: The incoming inspection ensures the correct identification of test samples, and the verification of the integrity/authenticity protection measures applied during shipment. The process is the starting point of the internal tracing. If assignment cannot be unambiguously applied, the product is separated until the identification is clarified.	P.Config-Items P.Reception-Control	P.Config-Items and P.Reception-Control are addressed because the unique assignment of the received products and test plans to the configuration management database is required within the received process.
O.Internal-Shipment: During the transfer, the security products are packed so that no product can be lost by accident. Any internal shipment with protected in terms of integrity/authenticity. The four-eyes principle will be applied to prevent a single person from uncontrolled access to secure items. If devices leave the secure area, at minimum two authorized employees are necessary to accompany the devices the whole time until handover to the forwarder.	T.Attack-Transport P.Product-Transport	T.Attack-Transport and P.Product-Transport are addressed because the number of transfers is limited, and the transfers are controlled.
O.Transfer-Data: The protection of exchanged sensitive data is performed using cryptographic algorithms and key management is done as well.	T.Staff-Collusion P.Product-Transport P.Transfer-Data.	This directly addresses P.Product-Transport and P.Transfer-Data.

Table 3: Traceability of security objectives to threats and OSPs

11.2 Security assurance requirements rationale

SAR	Rationale about SAR suitability
ALC_CMC.5 Advanced support (site's CM applies to testing-related configuration items only)	ALC_CMC.5 is 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 development, production, or – relevant here – testing process. The requirement for authorized changes supports the integrity and confidentiality required for the products. Therefore, this assurance component meets the requirements for the configuration management capabilities.
ALC_CMS.5 Development tools CM coverage (site's CM coverage applies to test tools only)	ALC_CMS.5 is suitable to support the reproducible development of secure products due to the requirement to also track security flaws and development tools besides from the configuration items comprising the TOE and its documentation. By placing security flaws information under CM control, this cannot be missed in corresponding follow-up work. By placing development tools under CM control, the acceptance of new versions of development tools is formalized, and any version of the development environment can be recreated at a later stage, e.g., to investigate/reproduce security flaws reported for an older version of the TOE. Therefore, this assurance component meets the requirements for the configuration management scope.
ALC_DVS.2 Sufficiency of security controls	ALC_DVS.2 is required since a high attack potential is assumed for potential attackers. The information used at the site during the testing (and potential prior initialization) of the product can be used by potential attackers developing attacks. Based on the assumed self-protection of the products, the information is needed to apply an attack within considerable time and effort. If keys are used during the initialization process and/or to support the security during the shipment or delivery, secure key handling and a special storage of electronic keys is implemented. Protection Profiles [5] and [6] refine the elements of ADV_DVS.2 in a way that DVS documentation is no longer TOE-specific, but specific for the site and the TOE type which are in the scope of the site evaluation.

Table 4: SAR suitability

SAR	Dependencies	Rationale
ALC_CMC.5	**ALC_CMS.1** **ALC_DVS.2** **ALC_LCD.1***	Dependencies are fulfilled by the SARs for the site, by inclusion of ALC_CMS.5 (hierarchical to ALC_CMS.1), ALC_DVS.2, and ALC_LCD.2 (hierarchical to ALC_LCD.1). Still, as ALC_LCD is not applicable for the site, this dependency must be fulfilled in a product certification by another site (typically the main development site of the client), which is in-line with and further explained in [9].
ALC_CMS.5	**None**	N/A
ALC_DVS.2	**None**	N/A

Table 5: SAR dependency fulfilment

SAR	Security objectives	Rationale
ALC_CMC.5.1C The CM documentation shall show that a process is in place to ensure appropriate and consistent labelling.	O.Config-Items O.Reception-Control	O.Reception-Control comprises the incoming inspection of the product and the associated labelling. The labelling is mapped to the internal identification as defined by O.Config-Item that ensures the unique identification of all security products.
ALC_CMC.5.2C The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Logical-Access O.Config-Items O.Config-Process	O.Config-Items ensure the unique identification of configuration items. O.Logical-Access ensures unique identifiers of responsible users. O.Config-Process provides a controlled configuration management process.
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-Process	O.Config-Process provides a controlled configuration management process allowing an adequate and appropriate review of changes.
ALC_CMC.5.4C The CM system shall uniquely identify all configuration items.	O.Reception-Control O.Config-Items O.Config-Process	O.Reception-Control comprises the incoming labelling and the mapping to internal identifications. O.Config-Items comprise the internal unique identification of all security products. Each product is setup according to O.Config-Process comprising the necessary configuration items.
ALC_CMC.5.5C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config-Process O.Logical-Access O.Zero-Balance	O.Config-Process based on a tracking system with automated generated history which reflects date and person of modifications. O.Logical-Access supports control by limiting access to authorised staff, and by ensuring correct operation. O.Zero-Balance comprises the control of test samples, which are completely sent back to the client after testing.
ALC_CMC.5.6C The CM system shall support the production of the product by automated means.	O.Config-Items	O.Config-Items based on a tracking system with automated generated history which reflects date and person of modifications of the test tools.
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.Config-Process	O.Config-Process ensures correct role separation by user-dependent access control.
ALC_CMC.5.8C The CM system shall clearly identify the configuration items that comprise the TSF.	N/A	The configuration items comprising the TSF are under CM control by the client, who must identify these accordingly.

SAR	Security objectives	Rationale
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 O.Config-Process	O.Config-Items provide a configuration management system that supports the audit of all changes. O.Config-Process provides configuration management by tool-based tracking.
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	O.Config-Items provide a configuration management system.
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.Config-Items	O.Config-Items provide a configuration management system allowing version controlling.
ALC_CMC.5.12C The CM documentation shall include a CM plan.	O.Config-Items O.Config-Process	O.Config-Items and O.Config-Process ensures the identification of persons, hardware, data, and documentation.
ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the TOE.	O.Config-Items O.Config-Process	O.Config-Items represents the management of the test sampled and all testing-related data and documentation at the site. According to O.Config-Process the CM plan describes the services in scope of the site evaluation.
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-Items O.Config-Process O.Reception-Control O.Zero-Balance	O.Config-Items and O.Config-Process ensures the identification of persons, hardware, data, and documentation. The items, which are managed by the configuration management system, are defined in O.Config-Items. O.Reception-Control includes an acceptance procedure for the shipping address to ensure the integrity of the data. O.Zero-Balance ensures that no physical security object is lost. It is sent back to the client.
ALC_CMC.5.15C The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.	O.Config-Items O.Config-Process O.Reception-Control O.Zero-Balance	O.Reception-Control, O.Config-Items, O.Config-Process, and O.Zero-Balance include acknowledgments, reports, logs, and notifications sufficient to provide the required evidence.
ALC_CMC.5.16C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.Config-Items O.Config-Process O.Reception-Control O.Zero-Balance	O.Reception-Control, O.Config-Items, O.Config-Process, O.Zero-Balance and O.Shipping-Support include acknowledgments, reports, logs, and notifications sufficient to provide the required evidence. O.Reception-Control also includes procedures if incoming products cannot be mapped to internal identifiers. O.Zero-Balance ensures that all security products are covered.
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 O.Config-Process	The items, which are managed by the configuration management system, are defined in O.Config-Items. However, O.Config-Process defined the configuration management for the products.

SAR	Security objectives	Rationale
ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.	O.Config-Items O.Config-Process O.Reception-Control O.Internal-Shipment O.Transfer-Data	Items and products are uniquely identified by the associated numbering schemes and version numbers according to O.Config-Items. The labelling for received products and products prepared for the shipment are defined by O.Reception-Control and O.Internal-Shipment. These procedures are supported by automated tools according to O.Config-Process.
ALC_CMS.5.3C For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.	O.Config-Items O.Reception-Control O.Internal-Shipment O.Transfer-Data	According to O.Reception-Control all security ICs are identified and mapped to the client. O.Config-Items leads to a unique identification of the products.
ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	O.Physical-Access O.Security-Control O.Alarm-Response O.Maintain-Security O.Logical-Access O.Staff-Engagement O.Zero-Balance O.Internal-Shipment O.Transfer-Data O.Internal-Monitor	The physical protection is provided by O.Physical-Access, supported by O.Security-Control, O.Alarm-Response, and O.Maintain-Security. Logical protection of data and configuration management is provided by O.Logical-Access. The personnel security measures are provided by O.Staff-Engagement. O.Zero-Balance is achieved by tracking all incoming and outgoing devices. O.Internal-Shipment covers the secure internal shipment of security items. O.Transfer-Data is achieved by encrypted transport of all digital data. O.Internal-Monitor ensures that security measures are maintained, and security incidents are discussed to conclude whether updates are necessary.
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.Internal-Monitor O.Maintain-Security O.Zero-Balance O.Internal-Shipment O.Transfer-Data O.Logical-Operation	ALC_DVS.2.1C's security measures are commonly regarded as effective protection if they are correctly implemented and enforced. Associated control and continuous justification are subject to O.Internal-Monitoring, O.Maintain-Security, O.Zero-Balance, O.Internal-Shipment and O.Transfer-Data. O.Logical-Operation requires maintenance of logical protection measures and therefore supports the correct implementation of ALC_DVS.2.1C's security measures.

Table 6: Traceability of applicable SARs to security objectives

11.3 Assurance measure rationale

Security objective	Rationale about assurance measures (as required by SARs)
O.Physical-Access	**ALC_DVS.2.1C** requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment.
O.Security-Control	**ALC_DVS.2.1C** requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment.
O.Alarm-Response	**ALC_DVS.2.1C** requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment.

Security objective	Rationale about assurance measures (as required by SARs)
O.Internal-Monitor	**ALC_DVS.2.1C** requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment. **ALC_DVS.2.2C** requires that the development-security documentation justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the intended TOE.
O.Maintain-Security	**ALC_DVS.2.1C** requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment. **ALC_DVS.2.2C** requires that the development-security documentation justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the intended TOE.
O.Logical-Access	**ALC_CMC.5.2C** requires that the CM documentation describes the method used to uniquely identify the configuration items. ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items. **ALC_CMC.5.5C** requires that the CM system provides automated measures such that only authorized changes are made to the configuration items. **ALC_DVS.2.1C** requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment.
O.Logical-Operation	**ALC_DVS.2.2C** requires a justification that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. This requires maintenance of the implemented logical security measures.

Security objective	Rationale about assurance measures (as required by SARs)
O.Config-Items	**ALC_CMC.5.1C** and **ALC_CMC.5.2C** require consistent and unique labelling. **ALC_CMC.5.4C** requires that the CM system uniquely identifies all configuration items. **ALC_CMC.5.6C** requires that the CM system supports the production of the product by automated means. **ALC_CMC.5.8C** requires that the CM system clearly identifies the configuration items that comprise the TSF. **ALC_CMC.5.9C** requires that the CM system supports the audit of all changes to the intended TOE by automated means, including the originator, date, and time in the audit trail. **ALC_CMC.5.10C** requires that the CM system provides 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 be able to identify the version of the implementation representation from which the intended TOE is generated. **ALC_CMC.5.12C** requires that the CM documentation includes a CM plan. **ALC_CMC.5.13C** requires that the CM plan describes how the CM system is used for the development of the intended TOE. **ALC_CMC.5.14C** requires that the CM plan describe the procedures used to accept modified or newly created configuration items as part of the intended TOE. **ALC_CMC.5.15C** requires that the evidence demonstrates that all configuration items are being maintained under the CM system. **ALC_CMC.5.16C** requires that the evidence demonstrates that all configuration items have been and are being maintained under the CM system. **ALC_CMS.5.1C** requires that the Configuration List includes the following: the intended TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the intended TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan. **ALC_CMS.5.2C** requires that the Configuration List uniquely identifies the configuration items. **ALC_CMS.5.3C** requires that for each configuration item, the configuration list indicates the developer/subcontractor of the item.

Security objective	Rationale about assurance measures (as required by SARs)
O.Config-Process	**ALC_CMC.5.2C** requires that the CM documentation describes the method used to uniquely identify the configuration items. **ALC_CMC.5.3C** requires that the CM documentation justifies 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 uniquely identifies all configuration items. **ALC_CMC.5.5C** requires that the CM system provides automated measures such that only authorized changes are made to the configuration items. **ALC_CMC.5.7C** requires that the CM system ensures that the person responsible for accepting a configuration item into CM is not the person who developed it. **ALC_CMC.5.9C** requires that the CM system supports the audit of all changes to the intended TOE by automated means, including the originator, date, and time in the audit trail. **ALC_CMC.5.12C** requires that the CM documentation includes a CM plan. **ALC_CMC.5.13C** requires that the CM plan describes how the CM system is used for the development of the intended TOE. **ALC_CMC.5.14C** requires that the CM plan describe the procedures used to accept modified or newly created configuration items as part of the intended TOE. **ALC_CMC.5.15C** requires that the evidence demonstrates that all configuration items are being maintained under the CM system. **ALC_CMC.5.16C** requires that the evidence demonstrates that all configuration items have been and are being maintained under the CM system. **ALC_CMS.5.1C** requires that the Configuration List includes the following: the intended TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the intended TOE; the implementation representation; security flaws; and development tools and related information. **ALC_CMS.5.2C** requires that the Configuration List uniquely identifies the configuration items.
O.Staff-Engagement	**ALC_DVS.2.1C** requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment.
O.Zero-Balance	**ALC_CMC.5.5C** requires that the CM system provides automated measures such that only authorized changes are made to the configuration items. **ALC_CMC.5.6C** requires that the CM system supports the production of the product by automated means. **ALC_CMC.5.14C** requires that the CM plan describe the procedures used to accept modified or newly created configuration items as part of the intended TOE. **ALC_CMC.5.15C** requires that the evidence demonstrates that all configuration items are being maintained under the CM system. **ALC_CMC.5.16C** requires that the evidence demonstrates that all configuration items have been and are being maintained under the CM system. **ALC_DVS.2.1C** requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment. **ALC_DVS.2.2C** requires that the development-security documentation justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the intended TOE.

Security objective	Rationale about assurance measures (as required by SARs)
O.Reception-Control	**ALC_CMC.5.1C** requires a documented process ensuring an appropriate and consistent labelling of the products. **ALC_CMC.5.4C** requires that the CM system uniquely identifies all configuration items. **ALC_CMC.5.14C** requires that the CM plan describe the procedures used to accept modified or newly created configuration items as part of the intended TOE. **ALC_CMC.5.15C** requires that the evidence demonstrates that all configuration items are being maintained under the CM system. **ALC_CMC.5.16C** requires that the evidence demonstrates that all configuration items have been and are being maintained under the CM system. **ALC_CMS.5.2C** requires that the Configuration List uniquely identifies the configuration items. **ALC_CMS.5.3C** requires that for each configuration item, the configuration list indicates the developer/subcontractor of the item.
O.Internal-Shipment	**ALC_CMS.5.2C** requires that the configuration list uniquely identifies the configuration items. **ALC_CMS.5.3C** requires that for each configuration item, the configuration list indicates the developer/subcontractor of the item. **ALC_DVS.2.1C** requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment. **ALC_DVS.2.2C** requires that the development-security documentation justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the intended TOE.
O.Transfer-Data	**ALC_CMS.5.2C** requires that the Configuration List uniquely identifies the configuration items. **ALC_CMS.5.3C** requires that for each configuration item, the configuration list indicates the developer/subcontractor of the item. **ALC_DVS.2.2C** requires that the development-security documentation justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the intended TOE. **ALC_DVS.2.1C** requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment.

Table 7: Assurance measures meeting security objectives

12 References

12.1 Literature

[1] *Site Security Target Template*, Version 1.0, published by Eurosmart, 2009-06-21

[2] *Joint Interpretation Library – Minimum Site Security Requirements*, Version 3.0, February 2020

[3] *Security IC Platform Protection Profile*, Version 1.0, BSI-CC-PP-0035-2007, Eurosmart, 2007

[4] *Security IC Platform Protection Profile with Augmentation Packages*, Version 1.0, BSI-CC-PP-0084-2014

[5] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*, April 2017, Version 3.1 Revision 5, CCMB-2017-04-001

[6] *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*, April 2017, Version 3.1 Revision 5, CCMB-2017-04-002

[7] *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*, April 2017, Version 3.1 Revision 5, CCMB-2017-04-003

[8] *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, April 2017, Version 3.1 Revision 5, CCMB-2017-04-004

[9] *Supporting Document Guidance, Site Certification*, October 2007, Version 1.0, Revision 1, CCDB-2007-11-001

12.2 List of Abbreviations

SST	Site Security Target
PP	Protection Profile
CC	Common Criteria
SAR	Security Assurance Requirement
AISEC	Applied and Integrated Security

13 History of changes

Version	Date	Author(s)	Changes
V1.0	2023-12-19	Security manager	//

V1.1	2024-01-09	Security manager	Clarified phases on page 5;
			Changed to version 3.1 on page 6 and 28;
			Deleted “ALC_TDA3” on page 11,12,14;
			Changed “AST_OBJ2” to “AST_OBJ1” on page 14;
			Added “O.Config-Process” on page 15;
			Added “P.Product-Transport” on page 17 and 18;
			Changed Rationale of “O.Zero-Balance” on page 18;
			Changed Table 4 on page 19;
			Changed Table 5 on page 20;
			Changed Table 7 on page 23f

V1.2	2024-01-22	Security manager	Harmonized “Data/Document assets” on page 7; Added “Document approval” on page 29

V1.3	2024-01-31	Quality manager	Inserted fields “Date” on page 1 and 4;
			Inserted comments at “Versions” on page 1 and 4;
			Changed “13 Document approval” to “History of changes” on page 29;
			Inserted comment at “History of changes” on page 29;
			Removed SARs and added remark on page 6