TABLE OF CONTENTS

1 SST INTRODUCTION

The purpose of this document is to describe the security target for the qualification and the test production of secure IC products at Presto Engineering HVM SAS Meyreuil.

1.1 SST Reference

Title	PRESTO ENGINEERING MEYREUIL PUBLIC SITE SECURITY TARGET
Reference	KPH7-019
Version	L
Company	Presto Engineering HVM SAS
Site location	Rue de la carrière de Bachasson, Arteparc Bachasson – CS 20029, 13590 MEYREUIL
Product type	Secure Wafers and packaged products
EAL-Level	EAL6

1.2 List of references

[1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model April 2017 Version 3.1 Revision 5 CCMB-2017-04-001
[2]	Common Criteria For information Technology Security Evaluation Part 3: Security Assurance Components April 2017 Version 3.1 revision 5 CCMB-2017-04-003
[3]	Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5, April 2017 - CCMB-2017-04-004
[4]	Supporting Document, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007,
[5]	Joint Interpretation Library Minimum Site Security Requirements Version 3 February 2020
[6]	“Security IC Platform Protection Profile with Augmentation Package ; Version 1 ; Issued 13-01-2014

1.3 Site Description

1.3.1 Physical scope of the site

Presto Engineering HVM SAS is located at rue de la carrière de Bachasson, Arteparc Bachasson – CS 20029, 13590 MEYREUIL.

Presto engineering occupies the ground floor and the first floor of one aisle, in a building constituted by two aisles of three floors. The site consists of a test production facility, a warehouse and a laboratory at the ground level and offices at the 1st floor.

The non-Presto area of this building are out of scope of this Site Security Target.

The site is protected by four main security tools:

- Access Control system
- Video Monitoring System
- Intruder Alarm System
- Telesurveillance and intervention patrol

1.3.2 Site Description

The following services or processes provided by the site are in the scope of the site certification:

- Reception, storage, warehousing and shipment of secure IC wafers, packaged IC and of finish goods
- Test and provisioning program development
- Preparation and management of secure data
- Incoming control, test and/or provisioning, outgoing control of secure IC wafers or packaged IC
- Electrical and functional validation, characterization and qualification of secure IC products
- Reliability of IC products

Provisioning is the insertion into secure products of secure data (pre-personalisation or personalisation data named “secure data” in the rest of this document) in a secure environment.

In this document, “**test program**” refers to program used for testing and/or provisioning secure products.

These services are part of the following phases defined in [6]:

"phase 2 – IC Development "(test program development, IC qualification and reliability), "phase 3 – IC Manufacturing " (wafer sort test, pre-personalisation if necessary) , "Phase 4- IC Packaging" (test, pre-personalisation if necessary, delivery of packaged products) .

Description of the site activity:

a) Incoming material (Secure IC wafers or secure products)
Client will send to Presto the wafers or packaged products for qualification or for production.

b) Receiving and storage
Upon physical receipt of the secure products, the site will key the incoming products into the system. Products have a unique identification code which is electronically setup by the site so that traceability of each product is properly recorded and accounted for. The raw products which are yet to be processed into the manufacturing process are stored in dedicated warehouse location (Die Bank) which entry is accessed only by authorized personnel. Transfers between Die Bank and the production process (Testing House) are also monitored using the electronic MES system which tracks the traceability of the products.

c) Products test and/or provisioning
Once the secure lot is transferred to the Testing House, the operator will scan the bar code of the lot and the MES system will then give the reference of the production flow.

An incoming inspection will check the quality of the received products.

Scanning the bar code of the lot on the test station will also automatically download the right program stored in the production network which is isolated from the general network and from internet.

An outgoing inspection is performed to ensure the quality of the products.

According to specifications agreed with customer, the products are packed in a box on which labels are glued, with the unique identification of the product.

The MES system ensures that the secure products undergo the right process flow before the return to the Die Bank for shipment.

All the test data are recorded in a secure server.

d) Shipments
The products can be shipped internally to another production site or externally to the final customer per the address given by customer and per appropriate shipping procedure.

e) Destruction of secure scrap materials
For client who requested the return of the rejected pieces, the site will arrange the secure shipment to the client.

Otherwise, the wafers or secure products from the site or from other production sites are securely stored in the secure warehouse in a dedicated area. The traceability of each device is ensured and the site will dispose the secured scrap material with the appropriate procedure.

2 CONFORMANCE CLAIMS

- The version of the Common Criteria which this document refers to is:
  - Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model April 2017 Version 3.1 Revision 5 CCMB-2017-04-001
  - Common Criteria For information Technology Security Evaluation Part 3: Security Assurance Components April 2017 Version 3.1 revision 5 CCMB-2017-04-003

- This SST is Common Criteria Part 3 conformant
- For the evaluation, the following methodology will be used:
  - Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5, April 2017,
  - Supporting Document, Site Certification, October 2007, Version 1.0, Revision 1, CCDB-2007-11-001

- There are no extended components required for this SST.
- The Assurance Components which are in the scope of this site are:
  - **ALC_CMC.5,**
  - **ALC_CMS.5,**
  - **ALC_DEL.1,**
  - **ALC_DVS.2,**
  - **ALC_LCD.1,**
  - **ALC_TAT.3**
- The assurance level chosen for the SST is compliant to the Protection Profile (PP) [6] and therefore suitable for Security ICs.
- Assurance components in the scope are based on assurance level EAL6.

3 SECURITY PROBLEM DEFINITION

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site.

3.1 Assets

The table below list all the assets handled by the site:

*Table 1 - **Asset List***

Id	Asset	Asset value
TOE	The products: - Customer's secure wafers and packaged IC - Customer's finished products	Confidentiality Integrity
INFO	All the documentation and information of the products or information related to the processes whatever the format. - Customer's test specifications, product or IP datasheets, technical documents - Customer's data files - Customer's keys & passwords - Secure data - Sub Certificate Authority (Sub-CA)[1] stored in HSM	Confidentiality Integrity
TESTPRO	Test Program	Confidentiality Integrity
INFOSEC	All the documentation of information regarding the systems and security mechanisms configuration (machines and perimeter protection devices configuration, cryptographic keys, password, etc.)	Confidentiality Integrity
DEVSEC	Protection devices or mechanism	Integrity Availability

[1] *Sub-CA: Certificate generated by Presto Engineering and signed by customer*

3.2 Threats

*Table 2 - **Threats***

Identifier	Description	Affected assets
T.Smart-Theft	An attacker tries to access sensitive areas of the site for manipulation or theft of assets. For the attack the use of standard equipment for burglary is considered. Potential attackers could be either existing employees of the company or external attackers whom are not existing employees.	TOE INFO TESTPRO INFOSEC DEVSEC

Identifier	Description	Affected assets
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	TOE INFO TESTPRO INFOSEC DEVSEC
T.Computer-Net	A possibly paid hacker with substantial expertise using standard equipment attempts to remotely access sensitive network segments to get access to the data with the intention to violate confidentiality and possibly integrity	INFO TESTPRO INFOSEC
T.Accident-Change	Employees or subcontractors that are not trained may take products or influence production systems without considering possible impacts or problems. This Threat includes accidental changes e.g. due to working tasks or Maintenance tasks within the development, production or test area. This can apply to any production step and any configuration item of the final product as well as to the final product or its configuration. Further examples may be machine failure or misalignment between operators that are responsible for products of different clients or different products of the same client are mixed during production. This also includes the disposal of sensitive products using the standard flow and not the controlled destruction.	TOE INFO TESTPRO INFOSEC DEVSEC
T.Unauthorised-Staff	Employees or subcontractors not authorised to get access to products or systems used for production get access to products or affect production systems or configuration systems, so that the confidentiality and/or the integrity of the product is violated. This can apply to any production step and any configuration item of the final product as well as to the final product or its configuration.	TOE INFO TESTPRO INFOSEC DEVSEC
T.Staff-Collusion	An attacker tries to get access to material processed at the site. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery.	TOE INFO TESTPRO INFOSEC DEVSEC
T.Attack-Transport	An attacker might try to get data, specifications or products during the internal or external shipment. The target is to compromise confidential information or violate the integrity of the products during the stated internal or external shipment process to allow a modification, cloning or the retrieval of confidential information at later life cycle states. Confidential information comprises design information, test documentation and test data as far as classified as sensitive.	TOE INFO INFOSEC

3.3 Organisational Security Policies

The following policies are introduced by the requirements of the assurance components of ALC for the assurance level EAL6. 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 under evaluation is under configuration management.

This comprises all procedures regarding the evaluated test and assembly flows and the security measures that are in the scope of the evaluation

Table 3 - ***Organisational Security Policies***

Identifier	Description
P.Config-Items	The configuration management system shall be able to uniquely identify configuration items. This includes the unique identification of items that are developed or used at a site as well as the received and transferred and/or provided items. The configuration management relies completely on the naming and identification of the received configuration items. The consistency with the expected identification is verified after receipt and each item is assigned to an internal unique identification. The configuration management system is applicable to documentation of the site, the test software and the products itself. For configuration items that are created, generated or developed at the site the naming and identification must be specified.
P.Config-Control	The procedures for setting up the production process for a new product as well as the procedure that allows changes of the initial setup for a product shall only be applied by authorised personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes. The procedure for the initial set up of a production process ensures that sufficient information is provided by the client. The product setup includes the following information (i) identification of the product, (ii) properties of the product when received at the site (iii) properties of the product when internally or externally shipped, (iv) classification of the items (which are security relevant), (v) who is responsible for destruction of defect devices, (vii) any configuration of the processed item as part of the services provided by the site, (viii) which address is used for the internal or external shipment.
P.Config-Process	The services and/or processes provided by the site are controlled in the configuration management plan. This comprises incoming items and tools used for the testing of the product, the management of flaws and optimizations of the process flow as well as the documentation that describes the services and/or processes provided by the site. The documentation that describes the process descriptions and the security measures of the site is under version control. Measures are in place to ensure that the evaluated status is ensured. In most cases tools are used to support the processes at the site. This comprises e.g. scripts or batch routines developed by the site.
P.Reception-Control	The inspection of incoming items done at the site ensures that the received configuration items comply with the properties stated by the client. Furthermore, it is verified that the product can be identified and a released production process is defined for the product. If applicable this aspect includes the check that all required information and data are available to process the configuration items.
P.Accept-Product	The testing and quality control of the site ensures that the released products comply with the specification agreed with the client. The quality control plan depicts the process, control and measures in place for the acceptance process of the configuration items. Therefore, the properties of the product are ensured when shipped.

P.Zero-Balance	The site ensures that all sensitive items (security relevant parts of the intended TOEs of different clients) are separated and traced on a device basis. At the end of each manufacturing process, the good and scrap products are counted to ensure a zero balancing. For each hand over, either an automated or an organizational “two employees-acknowledgement” (four-eyes principle) is applied for functional and defect assets. Per the released production process the defect assets are either destroyed by the site or sent back to the client.
P.Transport-Prep	Procedures and measures ensure the correct labeling and packing of the product. The site has a list of approved carriers for both internal and external shipments, including carriers selected by the client for its products. The measures to support traceability during the transport are supported by Presto.
P.Data-Transfer	Confidential / sensitive data transfers in electronic form (test programs, test program specifications, technical reports, secure data etc.) are encrypted to ensure security of the data.
P.Secure-Scrap	Storage of the functional or defective Scrap materials are securely maintained with authorized access. Secured scrap products must be destroyed securely with registered vendors or are returned to the clients.

3.4 Assumptions

Presto Engineering is operating in a production flow and therefore must rely on preconditions provided by the previous site and or the client. This is reflected by the following assumptions:

Table 4 - ***Assumptions***

Assumption	Description
A.Item-Identification	Each configuration item received by the site is appropriately labeled to ensure the identification of the configuration item.
A.Product-Specification	The client must provide appropriate specifications and guidance to test the product and to insert secure data. This comprises the requirements for test and provisioning, test fixtures and product set up to ensure the development of the programs (coding and hardware) either for the wafer test or for the final test. The provided information includes the classification of the delivered items, documents and data
A.External-Shipment	The recipient of the product is defined by the client. The client provides the address and shipping information (selected forwarder) to Presto. The client defines the requirements for packing of the security products in case the standard procedure of Presto is not applicable.
A.Product-Integrity	The self-protecting features of the devices are fully operational, and 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.Testdata-Support	The client must provide test data and optional secure data via a secure connection to Presto and according to a data format defined with Presto. The client is responsible for the secure transfer of data up to the Presto security network. The client must provide Sub Certificate Authority to Presto if Presto must generate the secure data.

The assumptions are outside the sphere of influence of Presto. They are needed to provide the basis for an appropriate production process, to assign the product and destruction of all configuration items related to the intended TOE.

4 SECURITY OBJECTIVES

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

*Table 5 - **Security Objectives description***

Objective	Description
O.Physical-Access	The site shall prevent unauthorized physical access and shall ensure an access control based on the “need to know” principle. The access control shall support the limitation for the access to sensitive areas including the identification and rejection of unauthorized people.
O.Security-Control	The site shall assign personnel to operate the systems for access control and surveillance and shall define the responsibilities and measures for responding to alarms.
O.Alarm-Response	Once the alarm is triggered, the site shall ensure that the reaction time is short enough to prevent a successful attack (before the unauthorized person gets access to any sensitive asset).
O.Internal-Monitor	Regular management reviews of the information management system must be performed to ensure continuing suitability, adequacy and effectiveness. The review shall include assessing opportunities for improvement and the need for changes including the information security policy and information security objectives.
O.Maintain-Security	The site shall ensure the correct operation of the relevant security systems to prevent unauthorized physical or logical access to sensitive assets and to ensure the protection of the networks.
O.Logical-Access	The site shall ensure authorized user access and prevent unauthorized user access to information systems or operating systems. The access must be based on the “need to know” principle.
O.Logical-Operation	The integrity of software and information systems shall be ensured. Systems and computers must be kept up-to-date (software updates, security patches, virus protection, spyware protection). A back up of sensitive data must be applied.
O.Config-Items	The site shall define a configuration management system that assigns a unique internal identification to the test program and to each product and shall allow an assignment to each client. The system shall manage configuration.
O.Config-Control	The product configuration and the test programs developed by the site shall be released through a formal release. The site shall ensure the correct control of the changes and shall ensure the correct operation of the planned processes.
O.Config-Process	Development of test programs, test and provisioning of products in production and documentation shall be controlled with tools and procedures.
O.Acceptance-Test	The site shall deliver configuration items that fulfil the specified properties. The tests performed to ensure the compliance shall be logged.
O.Staff-Engagement	The site shall ensure that employees are suitable for their roles and understand their responsibilities.
O.Zero-Balance	The site shall ensure that all secure products are traced and counted on a device basis and tracked until they are either shipped or destructed.
O.Reception-Control	Upon reception of a product, the site shall ensure an incoming inspection. The inspection shall cover the received quantity of products, the identification and the assignment of the product to a related internal production process.
O.-Transport	The site shall define the processes for the shipment of finished or unfinished secure products. This includes internal transfers (within the same or to different premises) and shipment to address defined by the customer.

O.Data-Transfer	Sensitive electronic configuration items (data or documents in electronic form) shall be protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorized employees can extract the sensitive electronic configuration item. The keys must be exchanged based on secure measures.
O.Control-Scrap	The site shall define measures to destruct secure products, sensitive documentation, erase electronic media and destroy sensitive configuration items so that they do not support an attacker.

5 RELATION BETWEEN THE SECURITY OBJECTIVES AND THE SECURITY PROBLEM DEFINITION

This table depicts the Security Objectives Rationale, which includes a tracing which shows how the threat and the OSPs are covered by the Security Objectives and which includes a justification that all threats and OSPs are effectively addressed by the Security Objectives.

*Table 6 - **Mapping of the Security Objectives***

Treat/OSP	Security Objective	Rationale
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Maintain-Security O.Staff-Engagement O.Internal-Monitor	The physical protection and the detection of any unauthorized intrusion are provided by O.Physical-Access, supported by O.Security-Control, O.Alarm-Response. O.Maintain-Security ensure the correct operation of these systems. O.Staff-Engagement ensure the employees are suitable for their roles. O.Internal-Monitor ensure the review of the efficiency of these systems.
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Maintain-Security O.Internal-Monitor	The physical protection and the detection of any unauthorized intrusion are provided by O.Physical-Access, supported by O.Security-Control, O.Alarm-Response, that ensure a quick reaction time. O.Maintain-Security ensures the correct operation of these systems. O.Internal-Monitor ensures the review of the efficiency of these systems.
T.Computer-Net	O.Logical-Access O.Logical-Operation O.Maintain-Security O.Internal-Monitor	The logical protection of data is provided by O.Logical-Access by securing the access of sensitive data. The configuration management and the integrity of the information systems are provided by O.Logical-Access and O.Logical-Operation. O.Maintain-Security ensure the correct operation of these systems. O.Internal-Monitor ensure the review of the efficiency of these systems.

T.Accident-Change	O.Staff-Engagement O.Config-Control O.Config-Process O.Acceptance-Test O.Zero-Balance	O.Staff-Engagement ensure that each employee is trained and understand his responsibilities: employee who are authorized to handle secure products or data are aware of the applicable procedures. O.Config-Process and O.Config-Control ensure that the correct operations are performed and that changes are done by authorized persons only. O.Acceptance-Test provides an automated testing of the functionality and supports the tracing. O.Zero-Balance ensure the tracing of each product and prevent from an accidental mix of products.

Treat/OSP	Security Objective	Rationale
T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Staff-Engagement O.Logical-Access O.Config-Control O.Zero-Balance O.Control-Scrap O.Internal-Monitor	O.Physical-Access ensure the access to sensitive products to authorized employee only and supported by O.Security-Control, ensure that the subcontractors who need the access to restricted area are always accompanied with an authorized employee. O.Staff-Engagement ensure that hired people and subcontractors are trustworthy and that employees and subcontractors are aware of their roles and of the security rules. O.Logical-Access ensure the access to sensitive data to authorized employees only. O.Config-Control ensure that changes are done by authorized persons only. O.Zero-Balance ensure the detection of any stolen product. O.Control-Scrap ensure the prevention of any theft of scrap products. O.Internal-Monitor ensure the review of the efficiency of these systems.
T.Staff-Collusion	O.Staff-Engagement O.Security-Control O.Zero-Balance O.Control-Scrap O.Data-Transfer O.Internal-Monitor	O.Staff-Engagement ensure that hired people are trustworthy. High restricted area are under video surveillance with a record of the images, ensure by O.Security-Control O.Zero-Balance ensure the tracing of each product and of each transaction of products. O.Control-Scrap ensure the prevention of any theft of scrap products. O.Data-Transfer ensure that the sensitive data are stored encrypted with the keys of limited authorized employees. O.Internal-Monitor ensure the review of the efficiency of these systems.
T.Attack-Transport	O.Transport O.Data-Transfer	O.Transport ensure the protection of the product during transport and the detection of any incident. O.Data-Transfer ensure the protection of data during the transfer.
P.Config-Items	O.Reception-Control O.Config-Items	O.Reception-Control ensure an immediate identification of the product upon reception and confirm the received quantity. O.Config-Item ensure that all configuration items for secure products are identified.

P.Config-Control	O.Config-Control O.Config-Items O.Logical-Access	O.Config-Control ensures the right product configuration and the right test program release through a formal defined process. Supported by O.Logical-Access, it also ensures that set up and changes are done by authorized persons only. O.Config-Items ensure an unique identification of the products and processes.
P.Config-Process	O.Config-Process	O.Config-Process defines the configuration control including part IDs, procedures and processes.
P.Reception-Control	O.Reception-Control	The identification of received products and its assignment to an internal production process is defined by O.Reception-Control.
P.Accept-Product	O.Acceptance-Test O.Config-Process O.Config-Control	O.Acceptance-Test ensure that the product is released after the completion of tests defined in a control plan, including the test of the product functionality. O.Config-Process defines the configuration control including part IDs, procedures and processes. O.Config-Control ensures that the testprogram released comply with the customer specifications.
P.Zero-Balance	O.Zero-Balance O.Control-Scrap O.Staff-Engagement O.Internal-Monitor	The tracing and the count of each product all along the manufacturing process and for each product transaction is ensured by O.Zero-Balance. O.Control-Scrap ensure the protection and the secure destruction of the products. O.Staff-Engagement ensure that each employee is trained and understand his responsibilities. O.Internal-Monitor ensure the review of the efficiency of these systems.
P.Transport-Prep	O.Config- Process O. Transport	O.Config-Process ensure the correct labelling of the product. O.Transport ensure the protection of the product during transport and the detection of any incident.
P.Data-Transfer	O.Data-Transfer	O.Data-Transfer ensure the protection of the Sensitive electronic configuration items (data or documents in electronic form).
P.Secure-Scrap	O.Zero-Balance O.Control-Scrap	O.Zero-Balance ensure the tracing and the count of each scrap product all along the scrap process. O.Control-Scrap ensure the protection of the scrap product all along the scrap process and the secure destruction of the products, of the sensitive documentation and of any electronic media containing sensitive documentation or sensitive date.

6 EXTENDED ASSURANCE COMPONENTS DEFINITION

No extended components are currently defined in this SST.

7 SECURITY ASSURANCE REQUIREMENTS

The secure products handled by this site may require an evaluation against assurance level EAL6.

The Security Assurance Requirements (SAR) are chosen from the class ALC (Lifecycle support) as defined in [2]:

- CM capabilities (ALC_CMC.5)
- CM scope (ALC_CMS.5)
- Delivery (ALC_DEL.1)
- Development security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)
- Tools and techniques (ALC_TAT.3)

Because hierarchically higher components are used in this SST, the Security Assurance Requirements listed above fulfil the requirements of:

[4] 'Common Criteria Supporting Document Guidance Site Certification'

[6] 'Security IC Platform Protection Profile - Eurosmart'

7.1 Application Notes and Refinements

The description of the site certification process [4] includes specific application notes. The main item is that a product that is considered as intended TOE (i.e. any TOE type) is not available during the evaluation. Since the term "TOE" is not applicable in the SST, the associated processes for the handling of products are in the focus and described in this SST. These processes are subject of the evaluation of the site.

7.1.1 CM Capabilities (ALC_CMC)

Refer to subsection:

- 'Application Notes for Site Certification' in [4] 5.1 'Application Notes for ALC_CMC'
- 'Refinements of the TOE Assurance Requirements' in [6] 6.2.1.4 'Refinements regarding (ALC_CMC)'

7.1.2 CM Scope (ALC_CMS)

Refer to subsection:

- 'Application Notes for Site Certification' in [4] 5.2 'Application Notes for ALC_CMS'
- 'Refinements of the TOE Assurance Requirements' in [6] 6.2.1.3 'Refinements regarding (ALC_CMS)'.

7.1.3 Delivery Procedure (ALC_DEL)

Refer to subsection:

- 'Application Notes for Site Certification' in [4] 5.3 'Application Notes for ALC_DEL'
- 'Refinements of the TOE Assurance Requirements' in [6] 6.2.1.1 'Refinements regarding (ALC_DEL)'

7.1.4 Development Security (ALC_DVS)

Refer to subsection:

- 'Application Notes for Site Certification' in [4] 5.4 'Application Notes for ALC_DVS'
- 'Refinements of the TOE Assurance Requirements' in [6] 6.2.1.2 'Refinements regarding (ALC_DVS)'

7.1.5 Life-Cycle Definition (ALC_LCD)

Refer to subsection 'Application Notes for Site Certification' in [4] 5.6 'Application Notes for ALC_LCD'

7.1.6 Tools and Techniques (ALC_TAT)

Refer to subsection 'Application Notes for Site Certification' in [4] 5.7 'Application Notes for ALC_TAT'

7.2 Security Assurance Rationale

The Security Assurance Rationale maps the content elements of the selected assurance components of [2] to the Security Objectives defined in this SST. The refinements described above are considered.

The site has a process in place to ensure an appropriate and consistent identification of the products. If the site already receives configuration items, this process is based on the assumption that the received configuration items are appropriately labeled and identified, refer to A.Item-Identification.

Note: The content elements that are changed from the original CC [2] per the application notes in the process description [4] are written in italic. The term TOE can be re-placed by configuration items in most cases. In specific cases, it is replaced by product (in the sense of “intended TOE”).

Table 7 - ***Security Assurance Rationale Mapping***

SAR	Security Objective
ALC_CMC.5.1C The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.	O.Config-Items
ALC_CMC.5.2C The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Reception-Control O.Config-Item O.Config-Control O.Config-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-Control O.Config-Process
ALC_CMC.5.4C The CM system shall uniquely identify all configuration items.	O.Reception-Control O.Config-Items O.Config-Control
ALC_CMC.5.5C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config-Control O.Logical-Access O.Logical-Operation
ALC_CMC.5.6C The CM system shall support the production of the *product* by automated means.	O.Config-Process O.Acceptance-Test
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-Control O.Reception-Control O.Logical-Access
ALC_CMC.5.8C The CM system shall clearly identify the configuration items that comprise the TSF.	O.Config-Items
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-Control
ALC_CMC.5.10C The CM system shall provide an automated means to identify all other	O.Config-Items O.Config-Control

configuration items that are affected by the change of a given configuration item.	
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 O.Config-Items O.Config-Control O.Config-Process
ALC_CMC.5.12C The CM documentation shall include a CM plan**.**	O.Config-Control O.Config-Process
ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the *product.*	O.Config-Control O.Config-Process
ALC_CMC.5.14C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *product*.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process
ALC_CMC.5.15C The evidence shall demonstrate that all configuration items are being maintained under the CM system	O.Reception-Control O.Config-Control O.Config-Process O.Zero-Balance
ALC_CMC.5.16C The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system	O.Config-Control O.Config-Process

SAR	Security Objective
ALC_CMS.5.1C The configuration list shall include the following: the *product* itself; the evaluation evidence required by the SARs; the parts that comprise the *product*; the implementation representation; security flaws; and development tools and related information.	O.Config-Items O.Config-Control O.Config-Process
ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.	O.Reception-Control O.Config-Items O.Config-Control
ALC_CMS.5.3C For each][configuration item, the configuration list shall indicate the develop-er/subcontractor of the item.][is indicated that “TSF rele-vant” has been deleted.	O.Config-Items

SAR	Security Objective
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 *product* design and implementation in its development environment.	O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Maintain-Security O.Control-Scrap O.Transport O.Data-Transfer
ALC_DVS.2.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the *product*.	O.Internal-Monitor O.Maintain-Security O.Data-Transfer
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 *product*.	O.Internal-Monitor O.Maintain-Security O.Data-Transfer

SAR	Security Objective
ALC_LCD.1.1C: The lifecycle definition docu-mentation shall describe the model used to develop and maintain the *product*.	O.Config-Control O.Config-Process
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the *product*.	O.Acceptance-Test O.Config-Process O.Zero-Balance

SAR	Security Objective
ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the *product* to the consumer.	O.Transport

SAR	Security Objective
ALC_TAT.3.1C Each development tool used for implementation shall be well-defined.	O.Config-Control O.Config-Process
ALC_TAT.3.2C The documentation of the development tool shall unambiguously define the meaning of all statements used in the implementation.	O.Config-Control O.Config-Process
ALC_TAT.3.3C The documentation of the development tool shall unambiguously define the meaning of all implementation dependent options.	O.Config-Control O.Config-Process

7.3 Security Requirements Dependencies Rationale

The dependencies for the assurance requirements are as follows:

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

Some of the dependencies are not completely fulfilled:

- ALC_LCD.1 is only partially fulfilled as the site does not represent the entire development environment. This is in-line with and further explained in [4] at §5.1 ‘Application Notes for ALC_CMC’.

- ADV_IMP.1 is not fulfilled as there is no specific TOE. This is in-line with and further explained in [4] at §5.7 ‘Application Notes for ALC_TAT’.

8 SITE SUMMARY SPECIFICATION

The Site Summary Specification describes how the site meets the SARs.

8.1 Preconditions required by the site

This section provides background information on the assumptions defined in section 3.4. These assumptions can be seen as guidance for the client regarding the information and deliverables which are needed to allow the production under the conditions described in this Site Security Target.

To perform the services, the following deliverables are required:

- Wafers or packaged products (with quantities)
- Product identification (product reference, reference of the lot)
- Technical product description for the development of the test program and for the test in production (IC or package layout information, test strategy, design test pattern, test vectors…)
- Test specification
- Address of the recipient, any specific packing and labelling or shipment conditions (approved forwarder)
- Treatment of the rejected or obsolete products: the client must inform Presto if the products can be scrapped by Presto or if they shall be returned to the client.
- Information about the classification of the documents and the product

For the setup of the production process, the relevant specifications and product information are required by Presto. Based on the provided specifications, the test programs are configured. The production is released after a formal review with the customer according to the PRESTO Industrialization process.

The client must ensure secured transfer of the product and the data to the site.

8.2 Services of the Site

Presto Engineering HVM provides Industrialization and Supply chain solutions for Integrated Circuits in a highly-secured environment.

The following services or processes provided by the site are in the scope of the site certification:

- Reception, storage, warehousing and shipment of secure IC wafers, packaged IC and of finish goods
- Test and provisioning program development
- Preparation and management of secure data
- Incoming control, test and/or provisioning, outgoing control of secure IC wafers or packaged IC
- Electrical and functional validation, characterization and qualification of secure IC products
- Reliability of IC products

Provisioning is the insertion into secure products of secure data (pre-personalisation or personalisation data named “secure data” in the rest of this document) in a secure environment.

In this document, “**test program**” refers to program used for testing and/or provisioning secure products.

The site maintains a certified Quality Management System as a basis for all processes including an Information Security Management System, that covers the SAR ALC_DVS.2, the SAR ALC_CMS.5 and contributes also to cover the SAR ALC_CMC.5.

The site proposes a well-defined process for the electrical and functional validation, characterization and qualification of secure IC products of the client, including the reliability tests. Each phase of the process flow includes a formal review with the client for which the site provides relevant reports. This Industrialization process covers the SAR ALC_LCD.1 and contributes to the coverage of the SAR ALC_CMC.5.

The site develops the test programs for the product evaluation and characterization and for the product test or provisioning in production. The test program development process covers the SAR ALC_TAT.3.

The site provides a wafer sort test and packaged test in production that consist of an electrical (parametric) and functional test and a loading of a customer code or a customer application or secure data in the EEPROM or in the Flash of the product. Each product gets a unique part ID that is linked with a production flow and the part list. In addition, the reception and the incoming controls processes have procedures that contribute to the coverage of the SAR ALC_CMC.5.

The site defined specific procedures for the packing and the shipment with secure transport up to the address provided by the client that covers the SAR ALC_DEL.1.

The site can propose a secure destruction process of the reject devices that contributes to the coverage of the SAR ALC_DVS.2 and the SAR ALC_CMC.5.

The site also hosts services that support the processes above from an operational and organizational point of view: Industrialization, Manufacture, Supply Chain, IT & Tools, Facilities & Equipment's, Quality & Security, Suppliers Management Services
The Security Assurance rationale is provided with more details in §7.2.

8.3 Objectives rationale

The objectives rationale is provided in §5. The following rationale gives more justification on how all threats and organizational security policies are effectively addressed by the security objectives.
The table below demonstrates that all threats and OSP are mapped to at least one security objective.

Table 8 - ***Objectives mapping***

	O.Physical-Access	O.Security-Control	O.Alarm-Response	O.Internal-Monitor	O.Maintain-Security	O.Logical-Access	O.Logical-Operation	O.Config-Items	O.Config-Control	O.Config-Process	O.Acceptance-Test	O.Staff-Engagement	O.Zero-Balance	O.Reception-Control	O.-Transport	O.Data-Transfer	O.Control-Scrap
T.Smart-Theft	x	x	x	x	x							x					
T.Rugged-Theft	x	x	x	x	x												
T.Computer-Net				x	x	x	x										
T.Accident-Change									x	x	x	x	x				
T.Unauthorised-Staff	x	x		x		x			x			x	x				x
T.Staff-Collusion		x		x								x	x			x	x
T.Attack-Transport															x	x	
P.Config-Items								x						x			
P.Config-Control						x		x	x								
P.Config-Process										x							
P.Reception-Control														x			
P.Accept-Product									x	x	x						
P.Zero-Balance				x								x	x				x
P.Transport-Prep										x					x		
P.Data-Transfer																x	
P.Secure-Scrap													x				x

O.Physical-Access
The access to the building is only possible via access-controlled doors. The building is controlled by CCTV camera and is protected from intrusion by an electronic detection system. The alarm activation is graduated according to the running operation at the site.
The physical, technical and organizational security measures ensure a separation of the site into three security levels. The access control ensures that only registered persons can access sensitive areas. This is supported by O.Security-Control that includes the access control and the control of visitors.
The physical security measures are supported by O.Alarm-Response providing an alarm system. Thereby the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

O.Security-Control
During working hours, the employees monitor the site and the surveillance system. The alarm system is connected to a central command center that is manned 24 hours. During off- hours, the alarm system is used to monitor the site.
The CCTV system supports these measures because it is always enabled. Further on, the security control is supported by O.Physical-Access requiring different level of access control for the access to secure product during operation as well as during off-hours.
This addresses the threats T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff and T.Staff-Collusion.

O.Alarm-Response
During working hours, the employees monitor the alarm system. The alarm system is connected to a central command center that is manned 24 hours. During off-hours, an intervention patrol supports the alarm system. O.Physical-Access requires certain time to overcome the different level of access control. The response time of the intervention patrol and the physical resistance match to provide an effective alarm response.

This addresses the threats T.Smart-Theft and T.Rugged-Theft.

O.Internal-Monitor

Regular security management meetings are implemented to monitor security incidences as well as changes or updates of security relevant systems and processes. This comprises also logs and security events of security relevant systems. Major changes of security systems and security procedures are reviewed in general management systems review meetings. Upon introduction of a new process, a formal review and release for mass production is made before being generally introduced.
This addresses T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorized-Staff, T.Staff-Collusion and the OSP P.Zero-Balance.

O.Maintain-Security

The security relevant systems enforcing or supporting O.Physical-Access, O.Security- control and O.Logical-Access are checked and maintained regularly by the suppliers. Logging files are checked regularly for technical problems and specific maintenance requests.
This addresses T.Smart-Theft, T.Rugged-Theft and T.Computer-Net.

O.Logical-Access

The internal network is separated from the internet with a firewall. The internal network is further separated into sub-networks by internal firewalls. These firewalls allow only authorized information exchange between the internal sub-networks. Each user is logging into the system with his personalized user name and password. The objective is supported by O.Internal-Monitor based on the checks of the logging regarding security relevant events.
The individual accounts are addressing T.Computer-Net. All configurations are stored in the database of the internal system. This addresses the threats T.Unauthorised-Staff and the OSP P.Config-Control.

O.Logical-Operation

All logical protection measures are maintained and updated as required. Critical items such as virus scanners are updated daily. The backup is sufficiently protected and is only accessible for the administration.
This addresses the threats T.Computer-Net.

O.Config-Items

The site has a configuration management system that assigns a unique internal identification to the test program and to each product. All the product configuration information is stored in databases, covering materials, process, test programs.
This is addressing the OSP P.Config-Items, P.Config- Control.

O.Config-Control

The site has defined a formal release procedure for the test programs, for the product configuration and for the documentation. A change procedure is in place to manage the changes as per a classification (minor or major changes).
This objective is supported by O.Logical-Access to ensure the correct control of the changes and that only authorized changes are possible.
This is addressing the threats T.Unauthorised-Staff, T.Accident-Change and the OSP P.Config-Control, P.Accept-Product.

O.Config-Process

The released configuration information including production and acceptance specifications is automatically copied to every work order. The test program is automatically loaded to the test machine per the configuration information of the work order.
This addresses the threat T.Accident-Change and the OSP P.Config-Process, P.Accept- Product and P.Transport-Prep.

O.Acceptance-Test

Acceptance tests are introduced and released based on the customer approval. The tools, specifications and procedures for these tests are controlled by the means of O.config- Items and O.Config-Control. Acceptance test results are logged and linked to the wafer lot in the system.
This addresses the threat T.Accident-Change and the OSP P.Accept-Product.

O.Staff-Engagement
All employees are interviewed before hiring. They must sign an NDA before they start working in the company. The formal training and qualification includes security relevant subjects and the principles of handling and storage of secure products or secure information. The security objectives O.Physical-Access, O.Logical- Access and O.Config-Items support the engagement of the staff.
This addresses the threats T.Smart-Theft, T.Accident-Change, T.Unauthorised-Staff, T.Staff-Collusion and the OSP P.Zero-Balance.

O.Zero-Balance
Products are uniquely identified throughout the whole process. The amount of functional and non-functional dies on a lot and for a production order is known. At every process step the registration of good and scrapped/rejected products is recorded.
This security objective is supported by O.Physical-Access, O.Config-Control and O.Staff-Engagement.
This addresses the threats T.Accident-Change, T.Unauthorised-Staff, T.Staff-Collusion and the OSP P.Zero-Balance, P.Secure-Scrap.

O.Reception-Control
At reception secure products are identified by the shipping documents, packing labels and information in Presto internal system based on shipment alerts from the customers and supported by O.Config-Items. A product that cannot be identified is put on hold in a secure storage. Inspection at reception is counting the number of boxes and checking the integrity of security seals of these boxes if applicable. Thereby only correctly identified products are released for production.
The OSPs P.Config-Items and P.Reception-Control are addressed by the reception control.

O.Transport
The recipient of a production lot is always linked either to the manufacturing flow defined in OCEAN (for internal shipment between production sites) or to the work order recorded in the ERP system (for shipment to the customer). These recipients can be modified by authorized users only. Packing procedures are documented in the product configuration. This includes specific requirement of the client.
The threat T.Attack-Transport and the OSP P.Transport-Prep are addressed.

O.Data-Transfer
The confidentiality and integrity of the data transfer from/to the site, specifically test program, test procedure data and within the site is ensured by appropriate secure measures. The secure measures include using secure transfer protocol during transfer and or encryption of sensitive information.
This is addressing the threats T.Staff-Collusion and T.Attack-Transport as well as the OSP P.Data-Transfer.

O.Control-Scrap
Scrap is identified and handled in the same way as functional devices. They are stored internally in a secure location. The scrap is either returned to the client using the same packing requirements as for functional products or it is destructed in a controlled and documented way.
The destruction process ensures a transformation to small pieces that cannot be exploited by an attacker.
Sensitive information and information storage media are collected internally in a safe location and destructed in a supervised and documented process.
Supported by O.Physical-Access and O.Staff-engagement this addresses the threats T.Unauthorised-Staff and T.Staff-Collusion as well as the OSP P.Zero-Balance and P.Secure-Scrap.

8.4 Security Assurance Requirements Rationale

The Security Assurance rationale is provided in §7.2. The following rationale gives more justification for the selected Security Assurance Requirements.

- CM capabilities (ALC_CMC.5)
- CM scope (ALC_CMS.5)
- Delivery (ALC_DEL.1)
- Development security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)
- Tools and techniques (ALC_TAT.3)

ALC_CMC.5
The chosen assurance level ALC_CMC.5 of the assurance family “CM capabilities” is suitable to support the production of high volumes 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 and ability to identify the changes and version of the implementation will support the integrity and confidentiality required for the products. Responsibility of different departmental teams is also clearly identified for accepting or authorizing any change on the configuration items. Therefore, these assurance requirements stated will meet the requirements for the configuration management.

ALC_CMS.5
The chosen assurance level ALC_CMS.5 of the assurance family “CM scope” supports the control of the production and test environment. This includes product related documentation and data as well as the documentation for the configuration management and the site security measures. Since the site certification process focuses on the processes based on the absence of a concrete TOE, these security assurance requirements are suitable.

ALC_DEL.1
The security assurance requirement of the assurance class " Delivery" is suitable to define a controlled process for delivery products to the consumer. The confidentiality and integrity of the product during transport is addressed by this assurance class. Since the Protection Profile requires the same assurance level it is considered to be sufficient.

ALC_DVS.2
The chosen assurance level ALC_DVS.2 of the assurance family “Development security” is required since a high attack potential is assumed for potential attackers. The configuration items and information handled at the site during production and testing of the product can be used by potential attackers for the development of attacks. Therefore, the handling and storage of these items must be sufficiently protected. Further on the Protection Profile requires this protection for sites involved in the life-cycle of Security ICs development and production.

ALC_LCD.1
The chosen assurance level ALC_LCD.1 of the assurance family “Life-cycle definition” is suitable to support the controlled development and production process. This includes the documentation of these processes and the procedures for the configuration management. Because the site provides only a limited support of the described life-cycle for the development and production of Security ICs, the focus is limited to this site. However, the assurance requirements are considered to be suitable to support the application of the site evaluation results for the evaluation of an intended TOE.

ALC_TAT.3
The security assurance requirements of the assurance class "Tools and Techniques" shall support the secure development and production of the TOE. The control, capabilities and configuration of the tools contribute to achieve reproducible and consistent development, production and test processes. Therefore, this Security assurance requirement is suitable for this type of product.

8.5 Assurance Measure Rationale

O.Physical-Access
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 *product* and implementation in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

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 *product* design and implementation in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

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 *product* design and implementation in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Internal-Monitor

ALC_DVS.2.2C requires that the development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the product.

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 integrity of the product.

Thereby this objective contributes to meet these Security Assurance Requirements.

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 *product* design and implementation in its development environment.

ALC_DVS.2.2C requires that the development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the product.

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 integrity of the product.

Thereby this objective contributes to meet these Security Assurance Requirements.

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 *product* design and implementation in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorised changes are made to the configuration items. Thereby this objective contributes to meet the Security Assurance Requirement.

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. Thereby this objective contributes to meet the Security Assurance requirement.

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 *product* design and

implementation in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorised changes are made to the configuration items. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Config-Items

ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products. A method used to uniquely identify the configuration items is required by ALC_CMC.5.2C.
ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items.
ALC_CMC.5.8C requires that the CM system clearly identifies the configuration items that comprise the TSF.
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 is able to identify the version of the implementation representation from which the TOE is generated.
ALC_CMC.5.14C requires that the CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the product.
The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information.
ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C.
ALC_CMS.5.3C requires that the developer of each relevant configuration item is indicated in the configuration list.
Thereby this objective contributes to meet the set of Security Assurance Requirements.

O.Config-Control

ALC_CMC.5.2C requires a CM documentation that 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 a unique identification of all configuration items by the CM system.
ALC_CMC.5.5C requires that the CM system provides automated measures so 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. Thereby this objective contributes to meet the Security Assurance requirement.
ALC_CMC.5.9C requires that the CM system supports 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 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 is able to identify the version of the implementation representation from which the TOE is generated.
ALC_CMC.5.12C requires a CM documentation that 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 *product*.
ALC_CMC.5.14C requires that the CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the product.
ALC_CMC.5.15C requests evidence demonstrating that all configuration items are being maintained under the CM system.
ALC_CMC.5.16C requires that the evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.
The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information.
ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. In addition, ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products.
ALC_TAT.3.1C requires each development tool used for implementation shall be well-defined.
ALC_TAT.3.2C requires the documentation of the development tool shall unambiguously define the meaning of all statements used in the implementation.
ALC_TAT.3.3C requires the documentation of the development tool shall unambiguously define the meaning of all implementation-dependent options.
Thereby this objective contributes to meet the set of Security Assurance Requirements.

O.Config-Process
ALC_CMC.5.2C requires a CM documentation that 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.5.6C requires that the CM system supports the production by automated means.
ALC_CMC.5.11C requires that the CM system is able to identify the version of the implementation representation from which the TOE is generated.
ALC_CMC.5.12C requires a CM documentation that 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 *product*.
ALC_CMC.5.14C requires that the CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the product.
ALC_CMC.5.15C requests evidence demonstrating that all configuration items are being maintained under the CM system.
ALC_CMC.5.16C requires that the evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.
The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information.
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. The objective meets the set of Security Assurance Requirements.
ALC_TAT.3.1C requires each development tool used for implementation shall be well-defined. ALC_TAT.3.2C requires the documentation of the development tool shall unambiguously define the meaning of all statements used in the implementation.
ALC_TAT.3.3C re-quires the documentation of the development tool shall unambiguously define the meaning of all implementation-dependent options.
Thereby this objective contributes to meet the set of Security Assurance Requirements.

O.Acceptance-Test
The testing of the products is considered as automated procedure as required by ALC_CMC.5.6C.
In addition ALC_LCD.1.2C requires control over the development and maintenance of the TOE.
Thereby this objective contributes to meet the Security Assurance Requirements.

O.Staff-Engagement
ALC_DVS.2.1C requires the description of personnel security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Zero-Balance
ALC_CMC.5.15C requires evidence demonstrating that all configuration items are being maintained under the CM system.
ALC_LCD.1.2C requires control over the development and maintenance of the TOE. Thereby this objective contributes to meet the set of Security Assurance Requirements.

O.Reception-Control
ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items.
ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system.
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.5.11C requires that the CM system can identify the version of the implementation representation from which the TOE is generated.
ALC_CMC.5.14C requires that the CM plan describes the procedures used to accept modified or newly created configuration items as part of the product.
ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system.
ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C.

Thereby this objective contributes to meet the set of Security Assurance Requirements.

O. Transport
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 *product* design and implementation in its development environment. This includes also the protection during the transport between production sides. Thereby this objective contributes to meet the Security Assurance Requirement.

ALC_DEL.1.1C requires that the delivery documentation describes all procedures that are necessary to maintain security when distributing versions of the product to the consumer.
Thereby this objective meets the Security Assurance Requirement.

O.Data-Transfer
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 product design and implementation in its development environment.
ALC_DVS.2.2C requires that the development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the product.

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 integrity of the product.

This includes also the protection during the transport between production sides.

Thereby this objective contributes to meet the Security Assurance Requirement.

O.Control-Scrap
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 product design and implementation in its development environment.
Thereby this objective contributes to meet the Security Assurance Requirement.

9 HISTORY

Version	Publication Date	Author Date	Approver Date	Comments
A	Jan 09, 2017	Stempfel Security Director	Laban Chief Operating Officer	First release
B	Mar 31, 2017	Stempfel Security Director	Michel Villemain Chief Executive Officer	Updated based on Evaluation Technical Report v0.1
C	Jun 19, 2017	Stempfel Security Director	Michel Villemain Chief Executive Officer	Updated based on PRESTO_NOTE_SST_v5.0 - §7.2 ALC_TAT.2 - §7.3 - §8.2
D	Feb 18, 2019	Stempfel Security Director	Michel Villemain Chief Executive Officer	§1 EAL Level updated from EAL5+ to EAL6 §1.2 List of references updated §1.3.2 Failure analysis activity removed §2 Conformance claim updated for EAL6
E	Jun 19, 2019	Stempfel Security Director	Michel Villemain Chief Executive Officer	Correction based on 18-0571_Presto-2_note_v1.0_Presto
F	Aug 9, 2019	Stempfel Security Director	Michel Villemain Chief Executive Officer	Correction based on 18-0571_Presto-2_note_v2.0_Presto
G	Jan 15, 2020	Stempfel Security Director	Michel Villemain Chief Executive Officer	Provisioning service added
H	Mar 13, 2020	Stempfel Security Director	Michel Villemain Chief Executive Officer	Corrections 7.2 Security Assurance Rationale, ALC_CMC and ALC_CMS updated for the provisioning process
I	Feb 02, 2021	Stempfel Security Director	Michel Villemain Chief Executive Officer	JIL MSSR new version 3.0
J	Feb 12, 2021	Stempfel Security Director	Michel Villemain Chief Executive Officer	Document reference correction
K	May 26, 2021	Stempfel Security Director	Michel Villemain Chief Executive Officer	Document reference correction §1.1
L	Mar 10, 2023	Stempfel Security Director	Cédric Mayor Chief Executive Officer	Document reference update