Document title:

PRESTO ENGINEERING UTAC PUBLIC SITE SECURITY TARGET

Document Type:	Security Target
Reference	KPH7-022-B
Release Date:	Oct 3, 2017
Security Level:	General Business Use

Author	**Controller**	**Approver**
Olivier STEMPFEL Quality & Security Manager	Kiattiyot Ungkusonmongkon Presto resident Manager	Michel Villemain Chief Executive Officier
Date: Oct 3, 2017	Date: Oct 3, 2017	Date: Oct 3, 2017

TABLE OF CONTENTS

1 SST INTRODUCTION

The purpose of this document is to describe the security target for the test production of secure IC products at Presto Engineering, Inc. area located in Thailand.

1.1 SST REFERENCE

Title	PRESTO ENGINEERING UTAC SITE SECURITY TARGET
Reference	KPH7-007
Version	B
Company	Presto Engineering, Inc. Representative Office in Thailand
Site location	UTAC Thai Limited (UTL3) / Location: C1 (Building C, 1st floor) 73 Moo 5,Wellgrow Industrial Estate Bangsamak, Bangpakong, Chachoengsao, 24180, Thailand
Product type	Secure Wafers and dies
EAL-Level	EAL5+

1.2 LIST OF REFERENCES

[1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model September 2012 Version 3.1 Revision 4 CCMB-2012-09-001
[2]	Common Criteria For information Technology Security Evaluation Part 3: Security Assurance Components September 2012 Version 3.1 revision 4 CCMB-2012-09-003
[3]	Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 4, September 2012
[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 1.1 (For trial Use) July 2013
[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

The Presto Engineering, Inc. area is hosted by UTAC at the following address:

UTAC Thai Limited (UTL3) / Location: C1 (Building C, 1st floor)
73 Moo 5,Wellgrow Industrial Estate
Bangsamak, Bangpakong,
Chachoengsao, 24180, Thailand

The UTAC UTL3 site hosting Presto's area is EAL6 certified (ANSSI-CC-SITE-2016/10).

Presto occupies a part (300 square meters) of the 1st floor of the building C1 at UTAC UTL3. The Presto area is delimited by a physical cage protected by an access control managed by Presto and by a video monitoring system inside the cage.

An access controls at the entrance of the building C1 limits the access. The physical security systems of UTL3 site are listed below:

- Access Control system
- Video Monitoring System
- Intruder Alarm System
- Site Security Guards

1.3.2 Site Description

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

- **Incoming control, electrical test and outgoing control of secure IC wafers**
- **Back grinding, sawing and outgoing control of secure IC wafers**

Description of the site activity:

a) Incoming material (Secure IC wafers or secure products)

Client will send to Presto the wafers for production.

b) Receiving and storage

Upon physical receipt of the secure wafers, the site will key the incoming wafers into the system. These wafers have a unique identification code which is electronically setup by the site so that traceability of each wafer is properly recorded and accounted for. The raw wafers 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 wafers.

c) Wafer test

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 wafers.
Scanning the bar code of the lot on the prober 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 wafers.
The MES system ensures that the secure wafers undergo the right process flow before the return to the Die Bank for shipment. All the test data are recorded in a secure server

c) Wafer grinding and sawing

The wafers are grinded and sawn before a full automatic visual inspection.
The MES system ensures that the secure wafers undergo the right process flow before the return to the Die Bank for shipment. All the test data are recorded in a secure server
According to specifications agreed with customer, the wafers are packed in a cassette on which labels are glued, with the unique identification of the product.

d) Shipments

Wafers are shipped internally to another production site or to Presto Hubs per appropriate shipping procedure.

e) Destruction of secure scrap materials

The scrap materials are all shipped to Presto Engineering Meyreuil.

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 September 2012 Version 3.1 Revision 4 CCMB-2012-09-001
  - Common Criteria For information Technology Security Evaluation Part 3: Security Assurance Components September 2012 Version 3.1 revision 4 CCMB-2012-09-003
- This SST is Common Criteria Part 3 conformant.
- There are no extended components required for this SST.
- The Assurance Components which are in the scope of this site are:

  ALC_CMC.4, ALC_CMS.5, ALC_DVS.2
- 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 **EAL5+**.

The activities of Presto Engineering, Inc. area are not related to the delivery of secure products. The site does not provide any contribution to ALC_DEL.1.

The site is a test site so it only intervenes in the test phase in the life cycle of products then the site does not provide any contribution to ALC_LCD.

The site does not develop any product neither test program then the site does not provide any contribution to ALC_TAT.

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 IC - Customer's finished products	Confidentiality Integrity
INFO	Customer test data	Confidentiality Integrity
TESTPRO	Test Program for wafer sort	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

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 con-figuration.	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 shipment. The target is to compromise confidential information or violate the integrity of the products during the stated internal 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 EAL5. 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 for the wafers 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 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 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 of the product. The products are packed as required by the client. The site has a list of approved carriers for internal shipments. 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 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. The scrap materials are all shipped to Presto Engineering Meyreuil.

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	Presto Meyreuil must provide appropriate hardware, test programs and test set up to ensure the wafer test and the wafer grinding and sawing.
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.

The assumptions are outside the sphere of influence of Presto site located at UTAC. 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 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 site shall have a procedure for the setup of the production process for each new product, from the release of a new configuration of the product to the production of the product. The site shall ensure the correct control of the changes and shall ensure the correct operation of the planned processes.
O.Config-Process	Test of wafer 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 security products are traced and counted on a device basis and tracked until they are either shipped.
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 internal shipment of finished or unfinished secure products. This includes internal transfers within the same or to different premises.

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 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 test program 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 and the secure destruction 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 EAL5+.
The Security Assurance Requirements (SAR) are chosen from the class ALC (Lifecycle support) as defined in [2]:

- CM capabilities (ALC_CMC.4)
- CM scope (ALC_CMS.5)
- Development security (ALC_DVS.2)

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 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)'

7.2 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.4.1C The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.	O.Config-Items
ALC_CMC.4.2C 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.4.3C The CM system shall uniquely identify all configuration items.	O.Reception-Control O.Config-Items O.Config-Control
ALC_CMC.4.4C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config-Control O.Logical-Access O.Logical-Operation
ALC_CMC.4.5C The CM system shall support the production of the *product* by automated means.	O.Config-Process O.Acceptance-Test
ALC_CMC.4.6C The CM documentation shall include a CM plan**.**	O.Config-Control O.Config-Process
ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the *product.*	O.Config-Control O.Config-Process
ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *product*.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process
ALC_CMC.4.9C The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.	O.Reception-Control O.Config-Control O.Config-Process O.Zero-Balance

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan	O.Config-Control O.Config-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

7.3 Security Requirements Dependencies Rationale

The dependencies for the assurance requirements are as follows:

- ALC_CMC.4: ALC_CMS.1, ALC_DVS.1, ALC_LCD.1
- ALC_CMS.5: None
- ALC_DVS.2: None

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’.

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.

In order to perform the services, the following deliverables are required:

- Wafers (with quantities)
- Product identification (product reference, reference of the lot)
- Any specific packing and labelling
- Treatment of the rejected or obsolete products
- 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.

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:

- **Incoming control, electrical test and outgoing control of secure IC wafers**
- **Back grinding and sawing of secure IC wafers**

The site maintains a Security Management System that covers the SAR ALC_DVS.2, the SAR ALC_CMS.5 and contributes also to cover the SAR ALC_CMC.4.

The site provides a wafer sort test in production that consist of an electrical (parametric) and functional test and a loading of a customer code or a customer application 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.4.

The site ensures a secure transport up to the Presto hubs or to another production site.

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.

	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 Presto site is surrounded by a cage and controlled by CCTV. The access to the Presto site is only possible via access controlled doors managed by Presto.
The Presto site is hosted by UTAC on its UTL3 site, EAL6 certified. The access control of the UTAC site and of the building hosting the Presto site is managed by UTAC.
The access control ensures that only registered persons can access to the UTAC site. 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 UTAC site and surveillance system. During off- hours the guard and the alarm system are used to monitor the UTAC site.
The CCTV system supports these measures. 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 UTAC security officer monitors the alarm system. The alarm system is connected to a central command center that is manned 24 hours. O.Physical-Access requires certain time to overcome the different level of access control. The response time of the security officier 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 are 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 who have access to the Presto area have to sign the Presto access policy and have to sign a non-disclosure agreement upon their employment with UTAC. The formal training and qualification includes security relevant subjects and the principles of handling and storage of security products.
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 wafer 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 to the manufacturing flow defined in PIMS. 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 returned to the Presto Meyreuil site.
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 §1. The following rationale gives more justification for the selected Security Assurance Requirements.

- CM capabilities (ALC_CMC.4)
- CM scope (ALC_CMS.5)
- Development security (ALC_DVS.2)

ALC_CMC.4

The chosen assurance level ALC_CMC.4 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 cleared 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_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.

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.4.4C 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.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.4.4C 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.4.1C 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.4.2C.
ALC_CMC.4.3.C requires that the CM system uniquely identifies all configuration items.
ALC_CMC.4.8C 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.4.3C.
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.4.2C requires a CM documentation that describes the method used to uniquely identify the configuration items.
ALC_CMC.4.3C requires a unique identification of all configuration items by the CM system.
ALC_CMC.4.4C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items.
ALC_CMC.4.6C requires a CM documentation that includes a CM plan.
ALC_CMC.4.7C requires that the CM plan describes how the CM system is used for the development of the *product*.
ALC_CMC.4.8C 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.4.9C requests evidence demonstrating that all configuration items are being maintained under the CM system.
ALC_CMC.4.10C 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.4.3C.
Thereby this objective contributes to meet the set of Security Assurance Requirements.

O.Config-Process

ALC_CMC.4.2C requires a CM documentation that describes the method used to uniquely identify the configuration items.
ALC_CMC.4.5C requires that the CM system supports the production by automated means.
ALC_CMC.4.6C requires a CM documentation that includes a CM plan.
ALC_CMC.4.7C requires that the CM plan describes how the CM system is used for the development of the *product*.
ALC_CMC.4.8C 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.4.9C requests evidence demonstrating that all configuration items are being maintained under the CM system.
ALC_CMC.4.10C 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.

O.Acceptance-Test

The testing of the products is considered as automated procedure as required by ALC_CMC.4.5C.
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.4.9C requires evidence demonstrating that all configuration items are being maintained under the CM system.

O.Reception-Control
ALC_CMC.4.2C requires a CM documentation that describes the method used to uniquely identify the configuration items.
ALC_CMC.4.3C requires a unique identification of all configuration items by the CM system.
ALC_CMC.4.8C 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.4.9C 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.4.3C.
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 sites. Thereby this objective contributes to meet 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. This includes also the protection during the transport between production sides.

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.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	Author Date	Controller Date	Approver Date	Comments
B	O Stempfel Oct 3, 2017	K Ungkusonmongkon Oct 3, 2017	M Villemain Oct 3, 2017	Updated according to Serma “PRESTO_NOTE_SST_UTAC_v1.0”