Table of Contents

1 Introduction

1.1 Site Security Target Reference

1.1.1 The purpose of this document is to describe the Security Target for the Production of Security IC module at Smartflex Technology Pte Ltd and IC on inlay at Smartflex Innovation Pte Ltd. There is only ONE (1) site located in Singapore for the module production.

Title:	Site Security Target
Revision Number:	05
Date:	29 July 2019
Site:	Smartflex Technology Pte Ltd & Smartflex Innovation Pte Ltd
Site location:	37A Tampines Street 92 #03-01 Singapore 528886
Product Type:	Security IC Modules and IC on inlay
EAL-Level:	EAL 6
Evaluation Body:	SERMA SAFETY & SECURITY- ITSEF
Certification Body:	Agence National de la Securite des Systemes d'Information (ANSSI)

Note that Only Classes AST and ALC are applicable for Site Certification Objectives in this Security Target.

1.2 References

S/N	References
1	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2017-04-001 Version 3.1 Revision 5
2	Common Criteria For information Technology Security Evaluation Part 3: Security Assurance Components CCMB-2017-04-003 Version 3.1 Revision 5
3	Common Criteria Supporting Documents Guidance Smartcard Evaluation February 2010 Version 2.0 CCDB-2010-03-001
4	Common Criteria Supporting Document Guidance Site Certification October 2007 Version 1.0 Revision 1 CCDB-2007-11-001
5	Joint Interpretation Library Minimum Site Security Requirements Version 2.1 December 2017
6	Bundesamt Für Sicherheit in der Informationstechnik Guidance for Site Certification Version 1.0
7	Security IC Platform Protection Profile with augmentation packages Version 1.0 (13.01.2014) Ref: BSI-PP-0084
8	Common Methodology for Information Technology Security Evaluation. Evaluation Methodology CCMB-2017-04-004 Version 3.1 Revision 5

2 SST Introduction

2.1 Identification of the Site

The SST is referring to Smartflex Technology Pte Ltd and Smartflex Innovation Pte Ltd (Smartflex), provides module manufacturing and assembly services for smartcards and identity modules and IC on inlay which is located at the following address:

37A, Tampines Street 92 #01-01
Singapore 528886

The site occupies TWO (2) entire levels of a 8 storey building. These two levels occupied by Smartflex are solely for the use of manufacturing of all secured and non-secured modules. This is the only production site which consists of the production, research and development, engineering, warehousing, business, administration and management activities. The building also houses other tenants whom does not belong to Smartflex' entity and has no access to Smartflex' facility.

Description of the site activity as follow:

2.1.1 Incoming raw Material (Security IC wafers and other raw materials)
Client will send to Smartflex the raw material (their Security IC in wafer format) for production. They will also provide the specification and test program to the site in order to start the process of module manufacturing in the site.

2.1.2 Storage and warehousing of Security IC wafers
Upon physical receipt of the raw material (Security IC), the site will key the incoming material 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 materials which are yet to be processed into the manufacturing process are stored in dedicated warehouse location which entry is accessed only by authorized personnel. Transfers between warehouse and the different production process are also monitored using the electronic production WIP system which tracks the traceability of the wafers.

2.1.3 Module Manufacturing/ Production Process
Before any mass production is perform, the site will have already optimized the production process during the new production introduction stage where the site will study the specifications of the client which is given and defined the Assembly build diagram which is approved by the client before mass production. For every launch of mass production volume, each job is assigned a unique production order number which will be traced from the start to the end of the process. The site also practices Zero Balancing where each wafer lots are traced throughout the process.

Once production is launched, the wafer will undergo the following manufacturing process defined by the process flow below for Smartflex Technology and Smartflex Innovation:

<u>Smartflex Technology Pte Ltd:</u>

Wafer Dicing: Depending on the state of the wafer when received by the client. The wafers could be sawn or unsawn. When wafers are unsawn, the site will need to perform a sawing process to isolate the different ICs in a wafer. Wafers must be sawn in order to start the die attach process. Wafer Map diagrams of the wafers are either provided by the client or downloaded through their secured server, each wafer is uniquely identifiable with their wafer lot numbers.

Die attach: Die attach process will be the bonding of die to substrate. The strong adhesion of the die to the substrate would be the key in this process and the adhesion is made possible using a die attach paste and with the use of thermal oven curing. For wafers which are already sawn, this will be the first production process step.

Wire bonding: After the die attach is completed, the dies would need to be bonded to the substrate, example gold wires and the different pads of the dies are bonded to the bonding pads of the substrate to ensure connectivity.

Encapsulation: Encapsulation process is to ensure that the wire bonded products are properly protected by the glue which is covering the entire area of the package. High Temperature and Ultraviolet adhesive is used in this process.

Testing and Pre-Personalization: In order to check if the connectivity of the modules are good or not, the modules will undergo the testing process via contact probing to ensure that the modules are manufactured correctly and has the correct connectivity. The tests programs which are used to test these modules are derived from the testing specifications which are supplied by the client. The site does not make any amendments to the testing specification and protocols given by the client. As for Pre-Personalization, this is an optional service which is requested by the client. In the event that client require Pre-Personalization data loading onto the modules, they will also sent to the site the specification and data script to be loaded onto the modules. The site does not make any changes to specification and scripts given by the client. The site has a process in place to ensure that the correct scripts are loaded in appropriate modules.

Outgoing buy off and Inspection: Before final packaging of the product, the products are inspected according to the specification as defined by the client. This step is performed by the quality assurance team to ensure that the product send to the client meets the specification and are correct prior sending it to the client.

Packaging: Packaging is the final step whereby the completed modules are packed in reel or sheet format accordingly to the specification as defined by the client.

Smartflex Innovation Pte Ltd:

Wafer Dicing: Depending on the state of the wafer when received by the client. The wafers could be sawn or unsawn. When wafers are unsawn, the site will need to perform a sawing process to isolate the different ICs in a wafer. Wafers must be sawn in order to start the die attach process. Wafer Map diagrams of the wafers are either provided by the client or downloaded through their secured server, each wafer is uniquely identifiable with their wafer lot numbers.

Gold Stud Bumping process: process by which we attach the conductive Au wire to the die. The Au wire formed on the die are called Au stud bumps.

UV Irradiation process: UV tape have strong adhesive strength to ensure the wafer dies do not fly during wafer dicing process. This process lowers the strength/tackiness of adhesive when UV (ultraviolet light) is irradiated. The wafer or chip can be easily removed after UV irradiation.

Flip Chip process: process by which we attach the wafer chips with Au bumps unto the substrate/PET tape via thermosonic bonding. Thermosonic flip-chip bonding is a solderless technology for area-array connections for low cost flip chip packages.

Roll-cut process: process by which we cut the PET tape roll to individual pre-sized sheets.

Testing and Pre-Personalization: In order to check if the connectivity of the IC on inlay are good or not, the IC on inlay will undergo the testing process via contact probing to ensure that the IC on inlay are manufactured correctly and has the correct connectivity. The tests programs which are used to test these IC on inlay are derived from the testing specifications which are supplied by the client. The site does not make any amendments to the testing specification and protocols given by the client. As for Pre-Personalization, this is an optional service which is requested by the client. In the event that client require Pre-Personalization data loading onto the IC on inlay, they will also sent to the site the specification and data script to be loaded onto the IC on inlay. The site does not make any changes to specification and scripts given by the client. The site has a process in place to ensure that the correct scripts are loaded in appropriate IC on inlay.

Outgoing buy off and Inspection: Before final packaging of the product, the products are inspected according to the specification as defined by the client. This step is performed by the quality assurance team to ensure that the product send to the client meets the specification and are correct prior sending it to the client.

Packaging: Packaging is the final step whereby the completed IC on inlay are packed in reel or sheet format accordingly to the specification as defined by the client.

2.1.4 Destruction of secured scrap materials

The good and bad dies in the wafers are all accounted and collected respectively from start of production to the end of the production and are also recorded electronically in the ERP system. For client who has requested that the scrap dies and wafers to be ship back to them, they will arrange the appropriate transportation to be ship back to their facility. For client who has requested that the scrap material to be destroyed, the site will dispose the secured scrap material with the relevant procedure. Even within the module manufacturing process, in case of secured trash, they are disposed in secured trash locations which are defined.

2.1.5 Internal Shipment to clients

Shipments are considered to the internal shipment as they are route back to the client whereby the client will arrange their own transportation to collect the completed modules / IC on inlay. The site will inform the client upon the completion of the production order and completed modules / IC on inlay are ready to be collected by the client- from the site.

The site activities are focused on the life-cycle phase 4: IC Packaging (and Testing) as defined in Security IC Platform Protection Profile with augmentation packages Version 1.0 (13.01.2014) Ref: BSI-PP-0084.

2.2 Site Description

The site consists of production facilities, incoming and outgoing material / finished products, warehousing, production, research and development, product and process engineering, testing, pre-personalisation of modules / IC on inlay, client service (or client service) and information technology (IT).

The entire perimeter of the building premises is surrounded by the fence which is constructed by Smartflex. The main gate entrance to building is secured with car barrier

for vehicle and turnstile for visitor. CCTV cameras are installed along the perimeter and are housed at the Guard house for surveillance.

Physical security- Access controls, restricted access and CCTV surveillances are also located at various locations within Smartflex. CCTV Footages within Smartflex's security perimeters are also housed in the security office for surveillance. Security guard is stationed at point of entry in a Guard house for 24 hours daily.

Logical security- The complete logical flow of the Security IC modules / IC on inlay at the site is covered by the SST. The management of the related processes and site security are also covered by the SST. The product flow of the security modules / IC on inlay on the site begins with the receipt of parts of the TOE (raw materials) up to the packing and handover for the shipment of the finished Security IC modules / IC on inlay.

The scope of TOEs are designed and developed based on the following processes:

- Receiving and storage of security wafers
- Production/ manufacturing of the security IC modules / IC on inlay
- Pre-Personalization of Security modules / IC on inlay which includes the testing and Operating System (OS) loading of completed modules / IC on inlay.
- Handling of Clients' secured pre- personalization data.
- Logistics- Incoming wafers, outgoing finish goods, Storage and warehousing
- Handling of Scrap materials from production process to destruction.

3 Conformance Claim

3.1 Version on Common Criteria

3.1.1 The SST Evaluation is based on Common Criteria Version 3.1, Revision 5.

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

3.1.3 Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2017-04-003 Version 3.1 Revision 5.

3.2 The methodology used for the evaluation

3.2.1 Common Methodology for IT security Evaluation, Evaluation Methodology, CCMB-2017-04-004 Version 3.1 Revision 5

3.3 Evaluation of Sensitive Components

Evaluated Assurance Components are from the assurance level EAL6 Package:

3.3.1	ALC_CMC.5	Advanced Support
3.3.2	ALC_CMS.5	Development tools CM Coverage
3.3.3	ALC_DEL.1	Delivery Procedure (Not Applicable)
3.3.4	ALC_DVS.2	Sufficiency of security measures
3.3.5	ALC_LCD.1	Developer defined life-cycle model
3.3.6	ALC_TAT.3	Compliance with implementation standards – all parts (Not Applicable)

Assurance components evaluated are based on the assurance level EAL6 of the Assurance class "Life- Cycle Support". Assessment of the site security measures demonstrates resistance to penetration of attackers, with a high attack potential. This site supports product evaluations up to EAL6.

The assurance components chosen for the Site Security Target are compliant to the Protection Profile (PP) (Ref: BSI-PP-0084) indicated under Section 1.2 [7]. Therefore the scope of the evaluation is suitable to support product evaluations up to assurance EAL6 conformant to Part 3 of the Common Criteria.

4 Security Problem Definition

The security problems are derived from the potential threats based on the assets owned by the site and the Organizational Security Policies (OSP) are also defined in this section. The security problem definition comprises of mainly: Theft- Theft of information, physical theft of assets and lapse in Physical/ Logical Security- in Production Process, handling of pre-personalization data. These threats are described generally in the SST to cover the aspect of potential attacks which the site has detail procedures, access matrix, blueprints that governs the security of the site.

The configuration management covers the integrity and confidentiality of the TOE and the security management of the site.

5 Assets

This section describes the assets handled at the site. The site has internal documentation and data that is relevant to maintain the confidentiality and integrity of an intended TOE. This comprises site security policies and measures which aims to protect the assets for the maintenance of appropriate controls.

Assets refer to the security elements which are received/ consigned by clients/ owned by the site as follow (but not limited to):

- Client's Secure IC and Wafers.
- Client's Secure Modules / IC on inlay (Finished Products) and other forms of identity module packages.
- Client's Testing Specifications, Test Program and Pre-Personalization Data.
- Secure IC, wafer and modules / IC on inlay which are rejected in the manufacturing process or intended for scrap.
- There are other client specific assets like seals, special transport protection or similar items that support the security of the internal shipment to the client. They are handles the same way as the other assets to prevent misuse, disclosure or lost of these sensitive items or information.

Full list of Assets are managed and controlled in an Asset List.

The integrity of any machinery or tooling used for production is not considered as part of the definition of an asset. However the site has maintained procedures, measures and internal documentation to ensure the importance of this condition.

6 Threats

Threats refer to the potential attacks which could possibly threaten the confidentiality and integrity of the TOE. These threats could possible happen from incoming of materials (secured wafers, IC and dies), in production and testing and in the shipment of secured products. These threats are described generally and are applicable to the site. Following are major threats which describe the potential attacks:

T. Smart-Theft:

In situation where the attacker plans to access the authorized area or restricted boundaries for the purpose of stealing secured items from the site. This attacker could use tools or equipment to break into the physical boundary of the company or building. Potential Physical theft could also happen during incoming of raw material, during in process of manufacturing production till shipment of the finish goods. Concerned assets include Clients Secured IC and wafers, Client's Secured modules / IC on inlay, Clients Testing Specifications, test programs and pre-personalization data, Secure IC wafers or modules / IC on inlay which are rejected in the manufacturing process or intended for scrap, special transport protection like security seals that support the security of the internal shipment to the client.

This attack already includes a variety of targets and aspects with respect to the various assets listed in the section above. It shall cover the range of individuals that try to get used or rejected devices that can be used to further investigate the functionality of the device and search for further exploits. The time spent by an attacker to prepare the attack and the flexibility of such an attack will provide big risk.
Potential attackers could be either existing employee of the company or external attackers whom are not existing employees. It will cause the company financial loss and loss of reputation as the goods are entrusted to the site by the client.

The site has implemented different levels of access control depending on the security restriction of the area. Some additional measures of the different level of access will include additional password entry or escorted by security personnel. Tools like security burglar alarms and CCTV cameras are also installed throughout the entire company to enhance the physical security of the company.

During production of the modules / IC on inlay there are risks of theft from employees. Zero Balancing of security products are observed in the production process- Tracking all pass and fail security parts at incoming, outgoing and during the production process steps and ensuring that all the security wafers are accounted for.

T. Rugged-Theft:

In situation where the attacker is experienced, plans to attack by accessing the permissible area or restricted boundaries for sensitive configuration items. Attacker could be paid for such stealing activities. Concerned assets include Clients Secured IC and wafers, Client's Secured modules / IC on inlay, Client's Testing Specifications, test programs and pre-personalization data, special transport protection like security seals that support the security of the internal shipment to the client.

The risk for this attack could vary dependent on the subject and recognized value of the assets. These attackers could be prepared to take high risks for payment. They are considered to be sufficiently resourced to overcome the security measures. The target of the attack could be devices that can be re-sold or misused in an application context. This can be devices installed at testing or personalization area for cloning or introduction of forged devices. These attackers are considered to have the highest attack potential.

These attackers could not completely be blocked by the physical, technical and procedural security measures. The site has special restricted location and access to highly secured area where such information are the most sensitive. Signed and Secured Keys are also used to transmit confidential or sensitive files with external parties to provide additional protection against such attacks.

T. Computer-Net:

Data theft could happen when the attacker tried to access the network without authorization. The attacker could try to download or intercept confidential documents of the company/ clients' data (such as pre-personalization data) for manipulation. In such cases, data theft through access of the company network or data servers could lead to loss of reputation of the company as well as the leak of confidentiality of clients' knowhow and intellectual property. This could eventually lead to a financial loss, compensation or legal case for the company. Concerned assets include Clients Testing Specifications, test programs and pre-personalization data.

These attackers are considered to have high attack potential because they might have vast technical knowledge to perform such attack whereby the in house system or software may not have sufficient capabilities to withstand such attacks.

Risk of Logical theft is reduced by the implementation of the security firewall to the external network. Limitations are set on websites, web applications and computer applications which are not essential for company use. Computer users also have individual accounts which require password authentication.

The site also houses dedicated servers and procedures in place handling Pre-personalization data which will enhance the security of the data received from the clients. The production network is also separated from the office network which the production network has no access to the internal network and has no access to internet to reduce the risk of any external attacks from hackers.

Sensitive and confidential information exchanges like the pre-personalization data that client send to the site for testing and OS loading are also encrypted when send to the site for decryption. Access of the encryption and decryption key are limited to only users who require access to clients' exchanges.

T. Unauthorized Staff

Unauthorized entry into prohibited area such as store, warehouse, production area and personalization is restricted. Concerned assets include Clients Secured IC and wafers, Client's Secured modules / IC on inlay, Clients Testing Specifications, test programs and pre-personalization data, special transport protection like security seals that support the security of the internal shipment to the client. The site is segregated into different levels of restricted access and the access is only permitted to authorized personnel.

Only authorized personnel are allowed into the different sections of the company and are controlled by the card access matrix which is reviewed and approved by Management.

Subcontractors/ vendors, visitors or non-employee of the site will be subjected to record their particulars and escorted by an employee during the duration of their stay in the site and have restricted access to the site. The site has also internal procedure guiding the access of unauthorized employees entering the site.

T. Staff- Collusion

Threats from external attacker might have collaborated with existing employee to extract data, confidential information or material from the site. Collaboration of such nature could have been motivated by personal interest or extortion. Concerned assets include Clients Secured IC and wafers, Client's Secured modules / IC on inlay, Clients Testing Specifications, test programs and pre-personalization data, Secure IC wafers or modules / IC on inlay which are rejected in the manufacturing process or intended for scrap.

While the site conducts yearly security training and security talks for the employees, they have to also sign the confidentiality agreement during their term of employment with the site.

Procedures such as key ceremony when handling clients' pre-personalization data, limited access and document-controlled access on production data and clients' sensitive data are also available at site. Handling of material or product at site using the 4 eyes principal is also implemented to reduce the tendency of such attacks.

T. Accidental Change

Employee, trainee, freight forwarder could have also make mistakes in executing their tasks and therefore resulting in the wrong mix of the different shipment at collection, mixing the wrong lot or batch of raw materials of products in production or even loading wrong personalization data by mistake. Concerned assets include Clients Secured IC and wafers, Client's Secured modules / IC on inlay, Clients Testing Specifications, test programs and pre-personalization data.

We have measures in place to prevent accidental changes in high risk area prone to accidental change such as incoming shipment identification, outgoing shipment collection identification, in production process during issuing of materials and also loading of personalization data.

T. Attack- Transport

Potential attacker might be planning to get products or confidential data during shipment of the product. Their aim on the attack is to get sensitive information for unauthorized activities, such as replicating sensitive product devices or data, reselling of security devices or getting sensitive information. Concerned assets include Clients Secured IC and wafers, Client's Secured modules / IC on inlay, Secure IC wafers or modules / IC on inlay which are rejected in the manufacturing process or intended for scrap, specific assets like seals, special transport protection or similar items that support the security of the internal shipment to the client. These specific assets are handled the same way as other assets to prevent misuse, disclosure or lost.

Incoming and outgoing shipment of raw material and finished goods/ products to clients are controlled via a restricted channel whereby access is dedicated to only logistics personnel and all transactions of materials are performed between the freight forwarders and logistics personnel are also recorded. Procedure and controls for Freight Forwarders (for incoming and outgoing shipments) are also in place. Collection for the finished goods is also identified with unique numbers whereby it's only made known to the freight forwarder who are collecting the goods.

Internal transportation of TOE is also monitored under the production process security element.

7 Organisational Security Policies (OSPs)

The security policies devised are based on the requirement of the assurance components of ALC for the assurance level EAL 6. The policy in place supports the entire process of the site as described (under section 2.1) and serves as security measures under the Security Assurance requirement (SAR). In addition, scheduled internal security audit and maintenance schedule of security equipment shall ensure the correct and continuous operation of the site's security.

The documentation of the site under evaluation is under configuration management. This comprises all procedures regarding the evaluated test and production flow and the security measures that are in the scope of the evaluation. Guidelines outlining the Security policy of the Site are mapped as follow:

P. Config-Items:

The configuration management system shall be able to uniquely identify configuration items. This includes the unique identification of the items that are created, generated, developed or used at the site.

All products and item codes are guided by the site's configuration system which uses unique item code for different client, Bill of material (BOM) and products. The site also uses a Work in Progress (WIP) and zero balancing system for production and item traceability in the ERP system. Procedure of the client's creation and new product introduction (NPI) are also in place to ensure that the information of the clients, material configuration and process specifications of the product are defined. The documentation (Physical copy) of this clients' assembly build diagram and specifications are controlled documents released only for production. Limited access to these documentations (electronic copy) is also stored in the server, available only to authorized personnel.

Procedures on the creation of the BOM guiding the unique item code for all raw materials (including security products) and clients codes. The entire production system is also guided by the SAP system which control information of the entire process from incoming to production and shipment. The naming and the identification of these configured items are specified during the entire production process.

P. Config-Control:

The procedures governing setting up the production process for new product and the procedure that allows changes of the initial setup for a new product shall only be perform by authorized personnel.

The new product setup includes the following information: identification of the product, properties of the product, itemized level (BOM/ raw material) and properties of the product when internal transfers take place, how the product is tested after assembly, address used for the shipment and other configuration of the processed product. All these setup are also managed via the SAP system and governed by procedure on item master part creation.

Configured items will be tied to the clients' approval documents before releasing it for mass production. Program name will be defined based on the clients name and configuration name. There are internal procedures and work instructions to ensure the traceability of clients' inventory and is further governed by the SAP system.

P. Config-Process:

Services and processes provided by the site are controlled in the configuration management plan. This comprises tools used for assembly and testing of the product like the process control plan will govern how the process is run and what are the tools and assembly equipment used in the production of the modules / IC on inlay This clearly explains in detail the manufacturing processes, quality and testing of the modules / IC on inlay at the site.

The documentation with the process description and the security measures of the site are under version control. Measures are in place to ensure that the evaluated status complies.

P. Reception Control

Procedures on receiving of products, outgoing shipments to clients and internal material flow are followed to ensure that security is not compromise. Inspection of incoming materials is also done on site to ensure that the received configuration items comply with the properties stated by the clients.

Traceability of the materials and products are monitored via SAP system. Information of freight forwarders are also recorded to ensure traceability and accountability. All incoming

shipments have a dedicated incoming reception channel for the transfers of goods (including security material) to ensure security.

P. Accept-Product

The testing and quality control of the site ensures that the released products comply with the specification agreed with the clients. 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

Site ensures that all sensitive items (on the intended TOE from clients) are separated and traced by devices basis. Procedure on zero balancing is practiced to ensure that all scrap materials are accounted for at each different manufacturing process. Security products are traced and recorded to ensure traceability in the ERP system. At the end of the production process where functional or defective assets are consolidated, they are either destroyed or send back to the clients (dependent on the production setup).

The policy on zero balancing covers the handling of products at each production flow of the site. All finished products are returned to the clients that has provided the site with the products. This is considered as internal shipment routing back to the clients.

P. Transport-Prep:

Procedures and measures are ensured for the correct labelling of the product. Products are labelled according to the specification determine by the clients and are verified before shipment to the clients. Products are packed per specification indicated by the clients. Controls are in place when the forwarder indicated by the client before the handover of the security products. Traceability of the outgoing materials and security products are monitored. Information of freight forwarders are also recorded to ensure traceability and accountability. All outgoing and internal shipments have a dedicated outgoing shipment channel for the transfers of goods (including configuration products) to ensure security.

P. Data Transfer

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

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 (according to the production setup).

Assumptions

Each site operating in a production flow must reply on preconditions provided by the previous site. Each site has to reply on the information received by the previous site/client. This is reflected by the assumptions defined below for the interface with Smartflex.

A.Item-Identification

Each Configuration item received by the site is appropriately labelled to ensure the identification of the configuration item

A.Product-Spec

The product developer must provide appropriate specifications and guidance for the assembly and testing of the product. This comprises bond plans for an appropriate assembly process as

well as test requirements and test parameters for the development of the functional tests or a finished test program appropriate for the final testing. The provided information includes the classification of the delivered item and data.

A.Internal shipment

The recipient (Client) of the product is identified by the address of the client site. The address of the client is part of the product setup. The client defined the requirements for packing of the security products in case the standard procedure of Smartflex 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.

The assumptions are outside the sphere of influence of Smartflex. 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.

8 Security Objectives (AST_OBJ)

The site's security objectives and measures shall conform to the EAL 6. These measures defined the physical, data, organizational security measures, and logistical security of the site.

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. Internal transport
O. Data Transfer
O. Control Scrap

O. Physical-Access:

Different Security access supports the different level of access control level of different authorized staff entering the facility. The area of access of the authorized staff is subjected to the basis of each individual's job scope and enforcing the "need to know" principle. The access control supports the limitation for the access to sensitive area including the identification and rejection of unauthorized entry. The site enforces up to three levels (level 0 to level 2) of access control depending on the area of access. The access control measures and mapping ensures that only authorized staff and accompanied visitors can access restricted areas. Any visitors who are accompanied must also be authorized to visit the restricted area by a formal security application, approved by authorized personnel. All Security products are handled in restricted areas only.

O. Security-Control:

The site has defined the responsibilities of each different personnel responsible for the security of the site. Measures, response and controls on the operation of the system for access control and surveillance are also defined. Technical security equipment such as video control, CCTV, sensors will also support the enforcement of the access control. All staff is responsible for registering the visitors, get authorized approval for entry to each area and should ensure to escort the visitors.

O. Alarm Response:

The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any sensitive configuration item (asset). After the alarm is triggered, the unauthorized person still has to overcome further security measures. The reaction time of the employee or security personnel is short enough to prevent a successful attack.

O. Internal- Monitor:

The site performs security management meeting once every year. The security management meetings are used to review security incidences, to verify that the maintenance measures are applied and to reconsider the assessment of risks and security measures. An internal audit is also conducted yearly to control the application and seek further improvement of the security measures defined.

O. Maintain- Security:

Technical security measures are maintained regularly to ensure correct and accurate operations. Access control system to ensure that only authorized employee have access to sensitive area as well as computer/ network system to ensure the protection of the networks and computer systems based on the appropriate configuration.

O. Logical-Access:

The site enforces a logical separation between the internal network and the internet by a firewall. The firewall ensures that only defined services and defined connections are accepted. The internal network is also separated into the production network and the administration network. Additional specific networks for production and configuration are physically separated from any internal network to enforce access control. Access to the production network and internal network is also restricted to authorized employees that are working in the related area or that are involved in the configuration tasks or the production system. Every authorized user of an IT system has its own user account and password managed by the authorized IT administrator. An authentication user account and password is enforced by all computer systems.

O. Logical- Operations:

The network segments and computer systems are kept up to date (software updates, security patches, virus protection, and spyware protection). The backup of sensitive data and security relevant logs is applied accordingly to the classification of the stored data.

O. Config- Items:

The site has a configuration management system that assigns a unique internal identification to each product to uniquely identify configuration items and is assigned to each different client.

O. Config-Control:

The site has 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 has

also integrated a process of change management whereby process to introduce changes to the product or processes is enforced. Only authorized personnel can access the changes in the system. The configuration management system which is automated supports the entire production control.

O. Config- Process:

The site controls its services and processes using a configuration management plan. The configuration management is controlled by tools and procedures for the development of test programs and the assembly of the products, for the management of optimizing the documentation and process flow managed by the site.

O. Acceptance-Test:

The site delivers configuration items that fulfill the specified properties. Specification checks, Machine Parameters, Functional and visual control checks and tests are performed to ensure that the products are compliant to the specifications defined. Tests logs are stored and maintained in the database to support the tracing and identification in case of any systematic failures.

O. Staff engagement:

All employees have to sign a non-disclosure agreement upon their employment with the site. Authorized staffs who are engaged to move, transfer and have contact with the security configuration items have to be trained and qualified based on the security procedures, on handling of the products. Briefing session with employees on basic security procedures of the company is done for every new employee joining the site and yearly sessions are also conducted to facilitate and enforce the importance of security within the site.

O. Zero-Balance:

Tracing of the security product is essential and the site has to ensure that each device of the client are tracked separately and are accounted for each functional and defective device at the production via the ERP system. Devices are tracked until when they are shipped or destructed as determined by clients.

O. Reception-Control:

Upon receipt of products an incoming inspection is performed. The inspection comprises the received amount of products and the identification and assignment of the product to a related internal production process.

O. Internal Transport:

The internal shipment procedure is applied to the configuration item. The recipient of a physical configuration item is identified by the assigned clients address. The internal shipment procedure is applied to the configuration site. The packaging is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of configuration items during the internal shipment.

O. Data Transfer:

Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms (PGP Keys) to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorized employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secured measures and they are sufficiently protected.

O. Control Scrap:

The site has measures to destruct sensitive configuration items. Rejected or defective devices are either destructed by authorized vendors or are returned to the clients.

9 Security Objective Rationale

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

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

10 Mapping of Security Objectives

Threats / OSP	Security Objectives	Justification
T. Smart Theft	O. Physical- Access O. Security-Control O. Alarm Response O. Internal Monitor O. Maintain-Security	Physical Security and protection is an important point for this threat. Therefore we will need to look into the different level of access and security control of the site to monitor the activity and permitted access within the site address in O. Physical-Access, O. Security-Control. In cases whereby security is compromised, alarm response measures will be triggered in response to highlight and/or prevent the attack- O. Alarm response. A robust security system and continuous improvement on Security within the organization and is essential to ensure that security operations are maintained and are reviewed continuously in O. Internal Monitor and O. Maintain-Security. Security Objective O. Physical- Access, O. Security-Control, O. Alarm Response, O. Internal Monitor and O. Maintain-Security directly counter Threat. Smart Theft.
T. Rugged-Theft	O. Physical-Access O. Security-Control O. Alarm Response O. Internal-Monitor O. Maintain-Security	Physical Security and protection is an important point for this threat. Therefore we will need to look into the different level of access and security control of the site to monitor the activity and permitted access within the site address in O. Physical-Access, O. Security-Control. In cases whereby security is compromised, alarm response measures will be triggered in response to highlight and/or prevent the attack- O. Alarm response. A robust security system and continuous improvement on Security within the organization and is essential to ensure that security operations are maintained and are reviewed continuously in O. Internal Monitor and O. Maintain-Security. Security Objective O. Physical- Access, O. Security-Control, O. Alarm Response, O. Internal Monitor and O. Maintain-Security directly counter Threat. Rugged- Theft.
T. Computer-Net	O. Internal-Monitor O. Maintain-Security O. Logical Access O. Logical Operation O. Staff Engagement	Logical Security and protection measure to prevent attack on logical protection of data and configuration management is essential. Supported by O.Internal- Monitor, O.Maintain-Security, O.Logical Access, O. Logical operation. Personnel Security measures are provided by O. Staff Engagement. Site Documentation applicable: Security Objective O. Internal- Monitor, O. Maintain-Security, O. Logical Access, O. Logical Access, O. Logical

		Operation and O. Staff Engagement directly counter Threat. Computer-Net
T. Accidental Change	O. Logical-Access O. Config Control O. Config-Process O. Acceptance-Test O. Staff Engagement O. Zero Balance	Accidental changes could happen if there are no controls in place. Configuration Management data and access are determined to prevent such incidents- Supported by O. Logical-Access. There are certain automated controls in place to support tracing and identification on systematic failures supported in O.Config-Control and O. Config-Process, O. Acceptance-Test and O. Zero balance at the Configuration management process, data management and production process specifications. Personnel Security Measures are provided by O. Staff Engagement. Security Objective O. Logical- Access, O. Config-Control, O. Config-Process, O. Acceptance-Test and O. Staff Engagement and O. Zero Balance directly counter Threat. Accidental-Change.
T. Unauthorized Staff	O. Physical Access O. Security-Control O. Alarm Response O. Internal Monitor O. Maintain-Security O. Logical-Access O. Logical Operation O. Staff Engagement O. Config-Control O. Zero Balance O. Control-Scrap	O. Physical Access, O. Security-Control, O. Alarm Response, O.Internal Monitor and O. Maintain Security ensure that no unauthorized entry is permitted into the site. Logical data access by unauthorized users is defined in O. Logical-Access and O. Logical Operation. Training of staff toward Security under O. Staff Engagement will assist staff in understanding such possible attacks. O. Config-Control ensures configurations can be done by authorized personnel only. Any Scrap that may support an attacker is controlled according to O. Zero Balance and O. Control Scrap. Security Objective O. Physical- Access, O. Security-Control, O. Alarm Response, O. Internal Monitor, O. Maintain-Security, O. Logical Access, O. Logical Operation, O. Staff Engagement, O. Config-Control, O. Zero Balance and O. Control-Scrap directly counter Threat. Unauthorized Staff.
T. Staff Collusion	O. Internal Monitor O. Maintain- Security O. Staff Engagement O. Zero Balance O. Data-Transfer O. Control-Scrap	O. Internal Monitor and O. Maintain Security define the associated control and continuous justification. Training of staff toward Security under O. Staff Engagement will assist staff in understanding such possible attacks. The applied production process and transfer of production material is controlled accordingly to O. Zero Balance, O. Data Transfer and O. Control Scrap. Security Objective O. Internal Monitor, O. Maintain Security, O. Staff Engagement, O. Zero Balance, O. Data-Transfer and O. Control- Scrap directly counter Threat. Staff Collusion.
T. Attack-Transport	O. Internal-Transport O. Data-Transfer	Restricted Channel whereby access is dedicated to only logistics personnel and transactions recorded during material transfers between client and the site are determine by O. Internal- Transport. Attacks on data transfers between clients and site are defined in O. Data-Transfer to prevent any attacks on sensitive test data or materials. Security Objective O. Internal Transport and O. Data Transfer counter Threat. Attack Transport.
P.Config-Items	O. Reception-Control O. Config-Items	Procedure on receiving the materials from client to ensure that correct parts are received and quantities are also correct is defined in O. Reception-Control. To ensure that the correct product is loaded into production system and ship to

		the correct entity, O. Config-Items determines the procedure. Security Objective O. Reception- Control and O. Config-Items directly enforce OSP Config-Items.
P. Config-Control	O. Config-Items O. Config Control O. Logical Access	All raw materials and processes used for identification and manufacturing are covered by O. Config-Items, O. Config Control and O. Logical Access. Security Objective O. Config Items, O. Config-Control and O. Logical Access directly enforce OSP Config-Control.
P. Config process	O. Config Process	Services and Processes provided by the site are controlled in the configuration management plan, O. Config Process. Security Objective O. Config Process directly enforces OSP Config-Process.
P. Reception-Control	O. Reception-Control	Procedures on receiving of products, outgoing shipment and internal material flow are followed accordingly to O. Reception- Control. Security Objective O. Reception Control directly enforce OSP Reception Control.
P. Accept-Product	O. Config-Control O. Config-Process O. Acceptance-Test	Testing and quality control will ensure that products comply with the specifications as defined with the client under O. Config Control, O. Config-Process and O. Acceptance-Test. Security Objective O. Config-Control, O. Config-Process and O. Acceptance Test directly enforce OSP Accept-Product.
P. Zero-Balance	O. Internal Monitor O. Staff-Engagement O. Zero-Balance O. Control Scrap	O. Internal Monitor, O Staff Engagement and O. Zero Balance and O. Control Scrap ensure that the sensitive items (intended TOE from clients) are traced and accounted for from start to scrap. Security Objective O. Internal Monitor, O. Staff Engagement and O. Zero Balance directly enforce OSP P. Zero Balance.
P. Transport-Prep	O. Config-Process O. Internal-Transport O. Data-Transfer	Products should be labelled accordingly to the specification of the clients and labels must be correct in O. Config-Process. Traceability and security of outgoing materials during internal transport are defined in O. Internal Transport and O. Data-Transfer. Security Objective O. Config-Process, O. Internal-Transport and O. Data Transfer directly enforce OSP Transport-Prep.
P. Data-Transfer	O. Data Transfer	O. Data-Transfer is to prevent any attacks on sensitive test data or materials during exchanges between clients and the Site. Security Objective O. Data Transfer directly enforce OSP Data-Transfer.
P. Secure Scrap	O. Security-Control O. Zero Balance O. Control-Scrap	O. Security Control, O. Zero Balance and O. Control Scrap ensure that the sensitive items (intended TOE from clients) are traced and accounted for from incoming material, in production and to scrap. Security Objective O. Security-Control, O. Zero Balance and O. Control Scrap directly enforce OSP Secure Scrap.

11 Extended Assurance Components Definition (AST_ECD)

No extended components are currently defined in this Site Security Target.

12 Security Assurance Requirements (AST_REQ)

Clients using this site Security Target require an evaluation against evaluation assurance level EAL 6. This Security Assurance Requirement (SAR) is often requested in the Security IC Platform Protection Profile.

The Security Assurance Requirements (SAR) is from the class ALC (LIFE-CYCLE SUPPORT) as defined:

- CM Capabilities (ALC_CMC.5)
- CM SCOPE(ALC_CMS.5)
- Development Security (ALC_DVS.2)
- Life-Cycle Definition (ALC_LCD.1)

12.1 Application Notes and Refinements

The description of the site certification process includes specific application notes. The main item is that a product that is considered as intended TOE is not available during the evaluation. Since the terms "TOE" is not applicable in the SST, the associated process for the handling of products (or "intended TOEs") are in the focus and described in this Site Security Target. These processes are subject of the evaluation of the site.

12.1.1 Overview and Refinements regarding CM Capabilities (ALC _CMC)

A production control system is employed to guarantee the traceability and completeness of different production lot. The number of wafers, dice and/ or packaged products (e.g. modules / IC on inlay) is tracked by this system. Appropriate administration procedures are implemented for managing wafers, dice and/ or packaged modules / IC on inlay, which are being removed from the production-process in order to verify and to control pre-defined quality standards and production parameters. It is ensured, the wafers, dice or assembled devices removed from the production stage (i) are returned to the production stage from where they were removed or (ii) are securely stored and destroyed.

According to the processes rather than a TOE are in the focus of the CMC examination. The changed content elements are presented below. The application notes are defined for ALC_CMC.5.

Main elements on the ALC_CMC.5 as compared to the ALC_CMC.4 would be the requirement for the CM system be able to identify the version of the implementation representation from which the TOE is generated helps to ensure that the integrity of this material is preserved by the appropriate technical, Physical and procedural safeguards.

Providing an automated means of ascertaining changes between versions of the TOE and identifying high configuration items are affected by modification items assists in determining the impact of the changes between successive versions of the TOE. This will provide valuable information in determining whether changes to the TOE result in all configuration items being consistent with one another.

The configuration control and a defined change process for the procedures and descriptions of the site under evaluation are mandatory. The control process must include all procedures that have an impact on the evaluated production processes as well as the site security measures.

The life cycle described is a complex production process which sufficient verification steps to ensure the specified and expected results are used during the control of the product. Test procedures, verification procedures and associated expected results must be under configuration management.

The configuration items for the considered product type are listed in section 5. The CM documentation of the site is able to maintain the items listed for the relevant life cycle step and the CM system is able to track the configuration items.

A CM system is employed to guarantee the traceability and completeness of different production lots. Appropriate administration procedures are in place to maintain the integrity and confidentiality of the configuration items.

12.1.2 Overview and refinement regarding CM Scope (ALC_CMS)

The Scope of the configuration management for a site certification process is limited to the documentation relevant for the SAR for the claimed life-cycle SAR and the configuration items handles at the site.

In the particular case of a security IC, the scope of the configuration management can include a number of configuration items. The configuration items already defined in section 5 that are considered as TOE implementation representation" include:

- Security Wafers, ICs/ dies.
- Security Modules / IC on inlay (Finished Products) and other forms of module packages.
- Testing Specifications and Pre-Personalization Data for testing/ OS loading.
- Security Dice and modules / IC on inlay which are rejected in the manufacturing process or intended for scrap.

In addition, process control data, test data and related procedures and programs can be in the scope of the configuration management.

12.1.3 Overview and refinements regarding Delivery Procedures (ALC_DEL)

The CC assurance components of the family ALC_DEL (Delivery) refer to the external delivery of (i) the TOE for parts of it (ii) to the consumer or consumer's site (Composite TOE Manufacturer), The CC assurance components ALC_DEL.1 requires procedures and technical measures to maintain the confidentiality and integrity of the product. The means to detect modifications and prevent any compromise of the initialization Data and/ or Configuration Data may include supplements of the Security IC Embedded Software.

In the particular case of a security IC more "material and information" then the TOE itself (which by definition includes the necessary guidance) is exchanged with clients. Since the TOE can be externally delivered after different life cycle phases, the Site Security Target must consider the data that is exchanged by the sites either as part of the product or separate as input for further production steps.

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

12.1.4 Overview and refinements regarding Development Security (ALC_DVS)

The CC assurance components of family ALC_DVS refer to (i) the development environment", (ii) to the "TOE" or "TOE" design and implementation". The component ALC_DVS.2 "Sufficiency of security measures" requires additional evidence for the suitability of the security measures.

The TOE Manufacturer must ensure that the development and production of the TOE is secure so that no information is unintentionally made available for the operational phase of the TOE. The confidentiality and integrity of design information, test data, configuration data and pre-personalization data must be guaranteed, access to any kind of samples (Clients specific samples) development tools and other material must be restricted to authorized persons only, scrap must be controlled and destroyed.

Based on these requirements the physical security as well as the logical security of the site is in the focus of the evaluation. Beside the pure implementation of the security measures also the control and the maintenance of the security measures must be considered.

12.1.5 Overview and refinements regarding life Cycle Definition (ALC_LCD)

The site does not equal to the entire development environment. Therefore, the ALC_LCD criteria are interpreted in a way that only those life-cycle phases have to be evaluated which are in the scope of the site. The Protection Profile (BSI-PP-0084) provides a life-cycle description there specify life-cycle steps can be assigned to the tasks at site. This may comprise a change of life-cycle state if e.g. testing or initialization is performed at the site or not.

The Protection Profile (BSI-PP-0084) does not include any refinements for ALC_LCD. The site under evaluation does not initiate a life cycle change of the intended TOE. The products are assembled and the functional devices are delivered to the clients. The defective devices are scrapped or also returned to the client.

12.1.6 Overview and Refinements regarding Tool and Techniques (ALC_TAT)

The CC assurance components of family ALC_TAT refer to the tools that are used to develop, analyze and implement the TOE. The component ALC_TAT.3, "Compliance with implementation standards", requires evidence for the suitability of the tools and technique used for the development process of the TOE.

Neither source code of the intended TOE is not handled nor is any task performed at the site that must be considered accordingly to ALC_TAT. Therefore, the component ALC_TAT is not applicable.

.

13 Security Rationale (SAR)

The Security Assurance rationale maps the content elements of the selected assurance components to the security objectives defined in this Site Security Target. 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, the process is based on the assumption that the received configuration items are appropriately labelled and identified.

Table 13A Dependency Table for Class ALC: Life-Cycle Support

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

Note: For Smartflex, The ALC: Life-cycle Support under the assurance level EAL6 Package are:

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

Some of the dependencies are not completely fulfilled which is described below:

ALC_LCD.1 is only partially fulfilled as the site does not represent the entire development process.
ADV_IMP.1 is not fulfilled as there is no specific TOE.

This is in line and further explained in in CCDB-2007-11-001 (Section 5.1 & 5.7 respectively)

Table 13B Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
ALC_CMC.5.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.	O. Config item	All products assembled in the site get an unique client Part ID automatically generated by a database as defined by O. config-item.
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	Incoming inspection accordingly to O. Reception- Control ensures product identification and the associated labelling. This labelling is mapped to the internal identification as defined by O. Config-Item. This ensures the unique identification of security products. O. Config-Control ensures that each client part ID is setup and releases based on a defined process. This comprises also changes related to a client part ID. The configurations can only be done by authorized staff. O. Config-Process provides a configured and controlled production process.
ALC_CMC.5.3C: The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.	O. Config- Process O. Config-Items	O. Config-Process ensures that only authorized staff can apply changes. O. Config-Item. This ensures that unique identification on security product. This comprises changes related to process flows, procedures and items of clients. Departmental Teams are defined to assess and release changes.
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items	O. Reception-Control O. Config-Items O. Config-Control O. Config- Process	O. Reception-Control comprises the incoming labelling and the mapping to internal identifications. O. Config-Item comprises the internal unique identification of all items that belong to a client part ID. Each product is setup according to O. Config-Control comprising all necessary items. O. Config-Process provides a configured and controlled production process.
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. Config- process O. Logical-Access O. Logical – Operation	O. Config-Control assigns the setup including processes and items for the production of each client part ID. O. Config-Process comprises the control of the production processes. O. Logical Access and O. Logical Operation support the control by limiting the access and ensuring that the correction operations for all tasks are performed by

		authorized staff.
ALC_CMC.5.6C: The CM system shall support the production of the product by automated means	O. Config-Control O. Config- Process O. Acceptance-Test O. Zero-balance	O.Config-Control describes the management of the configuration items O.Config-Process comprises the automated management of the production processes. O. Acceptance test provides an automated testing of the functionality and supports the traceability. O. Zero-Balance ensuring tracing of all security products.
ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	O. Reception-Control O. Acceptance-Test O. Config-Process	Different roles are assigned to different departmental teams. Members of the teams are responsible to release different steps of the production and the final product according to O. Reception-Control and O. Acceptance Tests. The management of the production environment and the different teams as described by O.Config-Process.
ALC_CMC.5.8C: The CM system shall clearly identify the configuration items that comprise the TSF.	O. Config-Items	O. Config-Items comprise the internal unique identification of all items that belong to a client part ID.
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the product by automated means, including the originator, date, and time in the audit trail.	O. Config-Control	The automated production control covered by O. Config-Control comprises the logging of all production steps and thereby includes the required audit trail including the originator.
ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O. Config-Control O. Config Process	O.Config-Control describes the management of the configuration items received from the client and delivered to the client. According to O.Config-Process the CM plans covered the general dependencies of the production process.
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	O. Reception- Control comprises the control of the incoming configuration items. O.Config-Items and O.Config-control cover the unique labelling and management of the client configuration items. O.Config-Process ensures that only controlled changes are applied.
ALC_CMC.5.12C: The CM documentation shall include a CM plan	O. Config-Control O. Config-Process	According to O. Config-Control, the setup of each client part ID includes and associated CM plan including the release. O. Config-Process ensures the reliability of the process and tools based on dedicated CM Plans.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for	O. Config-Control O. Config-Process O. Acceptance-Test	O. Config-Control describes the management of the client part IDs at the site.

the development of the product.		According to O. Config process, the CM plans describe the services provided by the site. O. Acceptance test provides an automated testing of the functionality and supports the traceability.
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 O. Acceptance-Test	O. Reception-Control supports the identification of configuration items O. Config-Items ensure the unique identification of each product produces at site by the client part ID. O. Config-Control ensures a release for each new or changed client part ID. O. Config-process ensures the automated control of released products. O. Acceptance test provides an automated testing of the functionality and supports the traceability.
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 O. Internal Transport	The objectives O. Reception-Control, O. Config-Control, O.Config-Process ensure that only released client part IDs are produced. This is supported by O. Zero-Balance ensuring the tracing of all security products. O. Internal-transport includes the packaging requirements, the reports, logs and notifications including the required evidence.
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 O. Acceptance-Test O.Internal-Transport	O. Config-Control comprises a release procedure as evidence. O. Config-Process ensures the compliance of the process. O. Acceptance-Test comprises the control that all finished parts based on the test assigned to this part ID. Since the finished products are returned to the client accordingly to O. Internal-Transport at least the labelling is controlled by the client.

Table 13C. Rationale for ALC_CMS.5

SAR	Security Objective	Rationale
ALC_CMS.5.1C: The AST configuration list includes the following: the TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.	O. Config-Items O. Config-Control O. Config-Process	Since the process is the subject of the evaluation no products are part of the configuration list. O. Config-Item ensures unique part IDs including a list of all items and processes for this part. O. Config-Control describes the release process for each client part ID. O. Config-Process defined the configuration control including part IDs. Procedures and processes.

ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O. Config Items O. Config-Control O. Config-Process O. Reception-Control	Items, products and processes are uniquely identified by the database/ SAP system according to O. config-Item. Within the production process, the unique identification is supported by the automated tools according to O. Config-Control and O. Config-Process. The identification of received products is defined by O. Reception Control.
ALC_CMS.5.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	O. Config items	O. Config Items describes that the site does not engage subcontractors for the assembly of security products.

Table 13D. Rationale for ALC_DVS.2

SAR	Security Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	O. Physical-Access O. Security-Control O. Alarm-Response O. Logical-Access O. Logical-Operation O. Staff-Engagement O. Maintain-Security O. Control-Scrap	The physical protection is provided by O.Physical Access, supported by O. Security- Control, O. Alarm-Response, and O. Maintain-Security. The logical protection of data and the configuration management is provided by O. Logical-Access and O. Logical-Operation. The personnel security measures are provided by O.Staff-Engagement. Any scrap that may support an attacker is controlled accordingly to O. Control Scrap.
ALC_DVS.2.2C: The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.	O. Internal-Monitor O. Logical-Operation O. Maintain-Security O. Zero-Balance O. Acceptance-Test O. Reception-Control O. Internal-Transport O. Data-Transfer	The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. The associated control and continuous justification is subject of the objectives O. Internal Monitoring, O. Logical-Operation and O. Maintain-Security. All devices including functional and non- functional are traced accordingly to O. Zero Balance. O. Acceptance-Test supports the integrity control by functional testing of the finished products. The reception and incoming inspection supports the detection of attacks during the transport of the security products to the site according to O. Reception-Control. The delivery to the client I protected by similar measures according to the requirements of the client based on O. internal-Transport. Sensitive data received and send by the Site is encrypted according to O.Data-Transfer to ensure access by authorized recipients only.
ALC.DVS.2.3C: The evidence shall justify that	O. Reception-Control O. Internal-Transport	The reception and incoming inspection supports the detection of attacks during the

the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	O. Data-Transfer	transport of the security products to the site according to O. Reception-Control. The delivery to the client I protected by similar measures according to the requirements of the client based on O. internal-Transport. Sensitive data received and send by the Site is encrypted according to O.Data-Transfer to ensure access by authorized recipients only.

Table 13E. Rationale for ALC_LCD.1

SAR	Security Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition shall describe the model used to develop and maintain the TOE.	O. Config-Control O. Config-Process	The processes used for identification and manufacturing are covered by O. Config Control and O. Config-Process
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE	O. Acceptance-Test O. Config-Process O. Zero-Balance	The item does not perform development tasks. The applied production process is controlled according to O. Config-Process, the finished client parts are tested according to O.Acceptance-Test and all security products are traced according to O. Zero balance.

Since this SST references the PP, the life-cycle module used in this PP includes also the processes provided by this site. Therefore the life-cycle module described in the PP is considered to be applicable for this site.
The performed production steps do not involve source code, design tools, compilers or other tools used to build the security product (intended TOE). Therefore the site does not use or maintain tools according to the definition of ALC_TAT.3. Therefore, the component ALC_TAT.3 is not applicable.

The site always returns the security products back to the client that provides the security products for the assembly. The site is always involved as the subcontractor. There is no delivery of security products directly to the client regarding the next life cycle step. Therefore the transport of security products is always considered as internal transport.

14 Site Summary Specifications (AST_SSS)

14.1 Preconditions required by the site

Smartflex provides manufacturing and assembly services for smartcards and identity modules / IC on inlay. Sawn wafers are expected as input for the assembly lines. Defect devices on the wafer can be marked by inking or by electronic wafer map files. The packaging and the wafers must be labelled to allow for production product identification.

The devices delivered to the site are tested after the assembly using simple functional tests like the check of the ATR/S as well as open and short measurements based on the test parameters provided by the client. Because the devices are already locked, the configuration data and/or identification data stored on the devices cannot be changed by the functional testing in the test environment.

The production at Smartflex is released after the client accepts the initial samples lot produced. Therefore each client is responsible for the verification of his products based on the samples lot provided by the site.

If specific requirement are needed for the transport of the finished products, the related specifications and other packaging items e.g. security seals are provided by the client.

The client is responsible for delivery and transfer of the products. This comprises the selection of the forwarder and the provision of data for the verification of the transport arrangements.

14.2 Services of the site

Each product setup at the site gets a unique client part ID (Client consigned parts). This part ID is linked with the security device that is assembled in the product.

The processes for assembly, testing and acceptance are setup at the site according to the specifications (E.g. Bonding diagrams, modules / IC on inlay specification, test specification and packaging requirements, if applicable) provided by the client. For the release, a samples lot is produced at the site.

The complete product specific production flow includes a functional test of each device as part of the acceptance process. The functional tests are either developed by Smartflex based on the test specifications and electrical parameters/ limits provided and determined by the client or the test program. The test program are provided by the client are integrated in the test environment of the site. Test program provided by the client must be dedicated for the test tools used at the site.

The site has a standard procedure for packing of finished products and preparation of shipment. If special packaging requirements are provided by the client, they are included in the process setup. The client is alerted if products are ready for transport because the transport will be arranged by the client. Base on the alert, the client provides the pickup information on the forwarder that is used for the verification of the forwarder before the handover of the products.

Defective or rejected products are either returned to the client or they are destructed according to the defined secure destruction process. The client must decide during the product setup whether the rejects and defective devices on the wafer are also returned or if they shall be destructed by Smartflex.

14.3 Objectives Rationale

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

O. Physical- Access
The plant is surrounded by a fence and controlled by CCTV. The access to the site is only possible via access controlled doors. The enabling of the alarm system and the additional external controls are managed according to the running operation at the site. This considers the manpower per shift as well as the operational needs regarding the receipt and delivery of goods. The physical, technical and organizational security measures ensure a separation of the site into four security levels. The access control ensures that only registered and authorized persons can access sensitive areas. This is supported by O. Security- Control that includes the maintenance of the access control and the control of visitors. The physical security measured is supported by O. Alarm-Response providing an alarm system.

Thereby the threats T.Smart-Theft, T. Rugged-Theft can be prevented. The Physical security measures together with the security measure provided by O. Security –Control enforce the recording of all actions. Thereby also T. Unauthorized –Staff is address.

O. Security-Control

During working hours the security officer will monitor the site and surveillance system. During off-hours, the alarm system is used to monitor the site. The CCTV systems support 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 security product during operation as well as during off hours.

This addresses the threats T. Smart-Theft and T.Rugged-Theft. Supported by O. Maintain-Security and O. Physical- Access also an internal attacker triggers the security measures implemented by O. Security-Control. Therefore also the Threat T. Unauthorized-staff and the OSP P. Secure Scrap is addressed.

O. Alarm-Response

During working hours the security officer will monitor the alarm system. The alarm system is connected to a control center that is running 24 hours. O. Physical-Access requires certain time to overcome the different level of access control. The response time of the security officer and security response team (who is on duty) are needed to provide an effective alarm response

This addresses the threats T.Smart-Theft, T-Rugged-Theft and T. Unauthorized-Staff.

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 like firewall, Virus protection and success control. Major changes of security systems and security procedures are reviewed in general management security review meetings (min. 1 per year). 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.Unauthorised-staff, T.staff-Collusion and 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 regularly by the security officer. In case of maintenance, it is done by the suppliers. In addition, the configuration is updated as required by authorized security officer (for the access control system). Log files are also checked for technical problems and specific maintenance requests.

This addresses T. Smart-Theft, T.Rugged-Theft, T. Computer-Net, T.Unauthorised-staff and T.staff-Collusion

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 ID 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 ERP system. Supported by O. Config-Items this addresses the threats T. Accidental-Change and T. Unauthorized –Staff and the OSP P. Config-Control.

O. Logical-Operation
All logical protection measures are maintained and updated as required, at least once a month. 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 and T. Unauthorized-Staff.

O. Config-Item
The configuration management system is in place and assigns a unique internal identification to each product to uniquely identify configuration items and is assigned to each different client. Items, products and processes are uniquely identified by the database/ SAP system

This addresses the OSP P. Config-Items and P. Config-Control.

O. Config-Control
Procedures arrange for a formal release of specifications and test programs based in an engineering run. The information is also stored in the configuration database. Engineering Change Procedures are in place to classify and introduce changes. These procedures also define the separation between minor and major changes and the relevant interactions and releases with clients if required. The ERP requires personalized access controlled by passwords. Each user has access rights limited to the needs of his function. Thereby only authorized changes are possible.

Supported by O. Config-items this addresses the threat T. Unauthorized-Staff, T. Accidental Change and the OSP P. Config-Control, P.Accept-Product

O. Config Process
The release configuration information including production and acceptance specifications is automatically copied to every work order. The test program is automatically loading to the test machine accordingly to the configuration information of the work order.

This addresses the threat T.Accidental-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 client 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 a work order in the ERP system.

This addresses the Threat T.Accidental-Change and the OSP P. Accept-Product.

O. Staff-Engagement
All employees are interviewed before hiring. They must sign and NDA and the staff compliance agreement on Security matters before they start to work in the company. 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. Computer-net, T.Accidental-Change, T. Unauthorized-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. Scrap and rejects are following the good products thru the whole production process. At every process step the registration of good and rejected products is recorded and updated via the ERP system. This security objective is supported by O. Physical-Access, O. Config-Items and O.Staff-Engagement.

This addresses the threats T. Accidental-change, T. Unauthorized-Staff, T.Staff-Collusion, OSP P. Zero-Balance and the P. Secure Scrap.

O. Reception-Control
At reception, each configuration item including security products are identified by the shipping documents, packaging label and information in the ERP system based on shipments alerts from the client and supported by O. Config-Items. If a product cannot be identified, it is put on hold in a secured storage. Inspection at reception is counting the amount of boxes and checking the integrity of security seal 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. Internal-Transport
The recipient of a production lot is linked to the work order in the ERP system and can only be modified by authorized users. Packing procedures are documented in the product configuration. This includes specific requirement of the client. This security objective is supported by O. Staff Engagement and O. Config-Items.

The Threat T.Attack-Transport and the OSP P. Transport-Prep are addressed by the Internal Transport.

O. Data-transfer
Sensitive electronic information is stored and transferred encrypted using PGP procedures.

Supported by O. Logical Access and O. Staff-engagement this addresses the threats T. Staff Collusion and T. Attack-Transport as well as the OSP P. Transport-Prep and P. Data-transfer.

O. Control-Scrap
Scrap is identified and handled in the same way as functional devices. They are stored internally in a secured location. The scrap is either returned to the client using the same packaging requirements as for functional products or its destructed form in a controlled and documented way. Transport and actual destruction of security products is done under supervision of a qualified employee in collaboration with the destructor.

Sensitive information and information storage media are collected internally in a safe location and destructed in s supervised and documented process.

Supported by O. Physical-Access and O. Staff-engagement, this addresses the threats T. Unauthorized-Staff and T-Staff-Collusion, OSP P. Zero balance and the P. Secure Scrap.

14.4 Security Assurance Requirement Rationale

The Security Assurance Rationale is given in section 13. This rationale addresses all content elements and thereby also implicitly all the developer action elements defined in Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components CCMB-2017-04-003 Version 3.1 Revision 5. Therefore the following Security Assurance rationale provides the justification for the selected Security Assurance Requirements. In general the selected Security Assurance Requirements fulfill the needs derived from the Protection Profile. Because they are compliant with the Evaluation Assurance Level EAL6 all derived dependencies are fulfilled.

14.4.1 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 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.

14.4.2 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 considered to be suitable.

14.4.3 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, assembly 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.

14.4.4 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.

14.4.5 ALC_DEL.1

The assurance family “Delivery” is not applicable because the products are returned to the client and this is considered as internal shipment.

14.4.6 ALC_TAT.3

The assurance family “Tools and Techniques” is not applicable because the tools used for the production process do not influence the behavior of the product. Therefore they are not considered under ALC_TAT.

14.5 Assurance Measurement 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 TOE design 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 TOE design and implementation in its development and production 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 TOE design and implementation in its development and production environment. Thereby this objective contributes to meet the Security Assurance Requirement.

O. Internal-Monitor

ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective contributes to meet the security Assurance Requirement.

O. Maintain-Security

ALC_DVS.2.1C: Requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design, implementation and in its development and production environment. Thereby this objective contributes to meet the security Assurance Requirement.

ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

O. Logical-Access

ALC_DVS.2.1C: Requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design, implementation and in its development and production environment. Thereby this objective contributes to meet the security Assurance Requirement.

ALC_CMC.5.5C: Requires that the CM system provides automated measures so that only authorized 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 TOE design, implementation and in its development and production

environment. Thereby this objective contributes to meet the security Assurance Requirement.
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective is suitable to meet the Security Assurance Requirement.
ALC_CMC.5.5C: Requires that the CM system provides automated measures so that only authorized 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. ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. A method used to uniquely identify the configuration items is required by ALC_CMC.5.3C. In addition ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.8C requires that the CM system shall identify the configuration items that comprise the TSF. ALC_CMC.5.11C requires that the version of test programs and the production processes used for production can be identified. 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 TOE. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_CMS.5.3C requires that the developer of each TSF relevant configuration items is indicated in the configuration list. The objective meets 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.5.4C 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.5.6C requires the CM system to support the production of the intended TOE by automated means. ALC_CMC.5.9C requires the support of audit information for all changes to the TOE by automated means including the originator, date and time. ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a chance given to a configuration item. ALC_CMC.5.11C requires that the version of test programs and the production processes used for production can be identified. 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 (production) of the TOE. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are maintained under the CM system. ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC CMC.5.4C. In addition ALC_LCD.1.1C requires that the life cycle definition describes the model used to develop and maintain the products. The objective meets 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 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. The provision of automated measures such that only authorized changes are made to the configuration items as required by ALC_CMC.5.5C. ALC_CMC.5.6C requires that the CM system supports the production by automated means. ALC_CMC.5.7C requires that the person or team accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a chance given to a configuration item. ALC_CMC.5.11C requires that the version of test programs and the production processes used for production can be identified. ALC_CMC.5.12C requires that the CM documentation includes a CM plan. ALC_CMC.5.13C requires that the CM plan describe how the CM system is used for the development of the TOE. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. 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.

O. Acceptance-Test

The testing of the products is considered as automated procedure as required by ALC_CMC.5.6C. ALC_CMC.5.7C requires that the person or team accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.13C requires that the CM plan describe how the CM system is used for the development of the TOE. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE. The operation of the CM system in accordance with the CM plan is required by ALC_CMC.5.16C. In addition ALC_LCD.1.2C requires control over the development and maintenance of the TOE. ALC_DVS.2.2C requires security measures to protect the confidentiality and integrity of the TOE during production. Thereby the objective fulfills this combination of 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 the objective fulfills this combination of Security Assurance Requirements.

O. Zero –Balance

ALC_CMC.5.6C requires that the CM system supports the production of the TOE by automated means. ALC_CMC.5.15C requires evidence that all configuration items are being maintained under the CM system. ALC DVS.2.2C requires security measures that are necessary to protect the confidentiality and integrity of the TOE. ALC_LCD.1.2C requires control over the development and maintenance of the TOE. Thereby this objective is suitable to meet the security Assurance Requirement.

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 person or team accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.11C requires that the version of design data used to generate the test scripts can be identified. ALC_CMC.5.14C requires the the version of test programs and the production processes used for production can be identified. ALC_CMC.5.15C requires evidence that all configuration items are being maintained under the CM system. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_DVS.2.2C requires security measures to protect the confidentiality and integrity of the TOE during internal transport. ALC.DVS.2.3C requires confidentiality and integrity of the product during internal shipment. Thereby this objective is suitable to meet the Security Assurance Requirement.

O. Internal-Transport

ALC_DVS.2.2C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE. ALC.DVS.2.3C requires confidentiality and integrity of the product during internal shipment. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan. Thereby this objective contributes to meet the Security Assurance Requirement.

O. Data-Transfer

ALC_DVS.2.2C: The development Security documentation shall describe all the Physical, Procedural, personnel and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. ALC.DVS.2.3C requires confidentiality and integrity of the product during internal shipment. This objective will meet the Security Assurance Requirement.

O. Control-Scrap

ALC_DVS.2.1C requires physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the TOE design and implementation. Thereby this objective is suitable to meet the Security Assurance Requirement.

14.5.1 Mapping of the Evaluation Documentation

The scope of the evaluation according to the assurance class ALC comprises the processing and handling of security products and the complete documentation of the site provided for the evaluation. The Specifications and descriptions provided by the client are not part of the configuration management at the site.

Table 14.5.1A SAR's to Site documentation mapping for ALC_CMC.5

SAR	Security Objective	Rationale
ALC_CMC.5.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.	O. Config item	All products assembled in the site get an unique client Part ID automatically generated by a database as defined by O. config-item.
ALC_CMC.5.2C: The CM documentation shall	O. Reception –Control O. Config-Item	Incoming inspection accordingly to O. Reception- Control ensures product

describe the method used to uniquely identify the configuration items.	O. Config-Control O. Config- Process	identification and the associated labelling. This labelling is mapped to the internal identification as defined by O. Config-Item. This ensures the unique identification of security products. O. Config-Control ensures that each client part ID is setup and releases based on a defined process. This comprises also changes related to a client part ID. The configurations can only be done by authorized staff. O. Config-Process provides a configured and controlled production process.
ALC_CMC.5.3C: The CM documentation shall justify that the acceptance procedures provides for an adequate and appropriate review of changes to all configuration items.	O. Config- Process O. Config-Item	O. Config-Process ensures that only authorized staff can apply changes. This comprises changes related to process flows, procedures and items of clients. Departmental Teams are defined to assess and release changes. O. Config-Item. This ensures that unique identification on security product.
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items	O. Reception-Control O. Config-Items O. Config-Control O. Config- Process	O.Reception-Control comprises the incoming labelling and the mapping to internal identifications. O. Config-Item comprises the internal unique identification of all items that belong to a client part ID. Each product is setup according to O. Config-Control comprising all necessary items. O.Config-Process provides a configured and controlled production process.
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. Config- Process O. Logical-Access O.Logical - Operation	O. Config-Control assigns the setup including processes and items for the production of each client part ID. O.Config-Process comprises the control of the production processes. O. Logical Access and O. Logical Operation support the control by limiting the access and ensuring that the correction operations for all tasks are performed by authorized staff.
ALC_CMC.5.6C: The CM system shall support the production of the product by automated means	O. Config-Control O. Acceptance-Test O. Config- Process O. Zero Balance	O.Config-Control describes the management of the configuration items O.Config-Process comprises the automated management of the production processes. O. Acceptance test provides an automated testing of the functionality and supports the traceability. O. Zero-Balance ensuring tracing of all security products.
ALC_CMC.5.7C: The CM system shall ensure that the person responsible for	O. Reception-Control O. Acceptance-Test O. Config-Process	Different roles are assigned to different departmental teams. Members of the teams are responsible to release different

accepting a configuration item into CM is not the person who developed it.		steps of the production and the final product according to Reception-Control and O. Acceptance Tests. The management of the production environment and the different teams as described by O.Config-Process.
ALC_CMC.5.8C: The CM system shall clearly identify the configuration items that comprise the TSF.	O. Config- Items	O. Config-Items comprise the internal unique identification of all items that belong to a client part ID
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the product by automated means, including the originator, date, and time in the audit trail.	O. Config-Control	The automated production control covered by O. Config-Control comprises the logging of all production steps and thereby includes the required audit trail including the originator.
ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O. Config-Control O. Config Process	O.Config-Control describes the management of the configuration items received from the client and delivered to the client. According to O.Config-Process the CM plans covered the general dependencies of the production process.
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	O. Reception- Control comprises the control of the incoming configuration items. O.Config-Items and O.Config-control cover the unique labelling and management of the client configuration items. O.Config-Process ensures that only controlled changes are applied.
ALC_CMC.5.12C: The CM documentation shall include a CM plan	O. Config-Control O. Config-Process	According to O. Config-Control, the setup of each client part ID includes and associated CM plan including the release. O. Config-Process ensures the reliability of the process and tools based on dedicated CM Plans.
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 O. Acceptance Test	O.Config-Control describes the management of the client part IDs at the site. According to O. Config process, the CM plans describe the services provided by the site. O.Acceptance test provides an automated testing of the functionality and supports the traceability.
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 O. Acceptance Test	O. Reception-Control supports the identification of configuration items O. Configuration-Items ensure the unique identification of each product produces at site by the client part ID. O. Config-Control ensures a release for each new or changed client part ID.

		O. Config-process ensures the automated control of released products. O.Acceptance test provides an automated testing of the functionality and supports the traceability.
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 O. Internal Transport	The objectives O. Reception-Control, O. Config-Control, O.Config-Process ensure that only released client part IDs are produced. This is supported by O. Zero-Balance ensuring the tracing of all security products. O. Internal-transport includes the packaging requirements, the reports, logs and notifications including the required evidence.
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 O. Acceptance-Test O. Internal-Transport	O. Config-Control comprises a release procedure as evidence. O. Config-Process ensures the compliance of the process. O. Acceptance-Test comprises the control that all finished parts based on the test assigned to this part ID. Since the finished products are returned to the client accordingly to O. Internal-Transport at least the labelling is controlled by the client.

Table 14.5.1B SAR's to Site documentation mapping for ALC_CMS.5

SAR	Security Objective	Rationale
ALC_CMS.5.1C: The AST configuration list includes the following: the TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.	O. Config-Item O. Config-Control O. Config-Process	Since the process is the subject of the evaluation no products are part of the configuration list. O. Config-Item ensures unique part IDs including a list of all items and processes for this part. O. Config-Control describes the release process for each client part ID. O. Config-Process defined the configuration control including part IDs. Procedures and processes.
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O. Config Item O. Config-Control O. Config-Process O. Reception-Control	Items, products and processes are uniquely identified by the database/ SAP system according to O. config-Item. Within the production process, the unique identification is supported by the automated tools according to O. Config-Control and O. Config-Process. The identification of received products is defined by O. Reception Control.
ALC_CMS.5.3C: For each TSF relevant	O. Config item	The site does not engage subcontractors for the assembly of security products.

configuration item, the configuration list shall indicate the developer of the item.		

Table 14.5.1C SAR's to Site documentation mapping for ALC_DVS.2

SAR	Security Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	O. Physical-Access O. Security-Control O. Alarm-Response O. Logical-Access O. Logical-Operation O. Staff-Engagement O. Maintain-Security O. Control-Scrap	The physical protection is provided by O.Physical Access, supported by O. Security- Control, O. Alarm-Response, and O. Maintain-Security. The logical protection of data and the configuration management is provided by O. Logical-Access and O. Logical-Operation. The personnel security measures are provided by O.Staff-Engagement. Any scrap that may support an attacker is controlled accordingly to O. Control Scrap.
ALC_DVS.2.2C: The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.	O. Internal-Monitor O. Logical-Operation O. Maintain-Security O. Zero-Balance O. Acceptance-Test O. Reception-Control O. Internal-Transport O. Data-Transfer	The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. The associated control and continuous justification is subject of the objectives O. Internal Monitoring, O. Logical-Operation and O. Maintain-Security. All devices including functional and non-functional are traced accordingly to O. Zero Balance. O. Acceptance-Test supports the integrity control by functional testing of the finished products. The reception and incoming inspection supports the detection of attacks during the transport of the security products to the site according to O. Reception-Control. The delivery to the client I protected by similar measures according to the requirements of the client based on O. internal-Transport. Sensitive data received and send by the Site is encrypted according to O.Data-Transfer to ensure access by authorized recipients only.
ALC.DVS.2.3C: The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE	O. Reception-Control O. Internal-Transport O. Data-Transfer	The reception and incoming inspection supports the detection of attacks during the transport of the security products to the site according to O. Reception-Control. The delivery to the client is protected by similar measures according to the requirements of the client based on O. internal-Transport. Sensitive data received and send by the Site is

		encrypted according to O.Data-Transfer to ensure access by authorized recipients only.

Table 14.5.1D SAR's to Site documentation mapping for ALC_LCD.1

SAR	Security Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition shall describe the model used to develop and maintain the TOE.	O. Config-Control O. Config-Process	The processes used for identification and manufacturing are covered by O. Config Control and O. Config-Process
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE	O. Acceptance-Test O. Config-Process O. Zero-Balance	The item does not perform development tasks. The applied production process is controlled according to O. Config-Process, the finished client parts are tested according to O.Acceptance-Test and all security products are traced according to O. Zero balance.

15 Definition, List of Abbreviations and List of documents referenced

15.1 Definition

Client: The Site providing the Site Security Target may operate as a subcontractor of the TOE manufacturer. The term "client" is used here to define this business connection. It is used instead of client since the terms "client" and "consumer" are reserved in CC. In this document, the terms words "client" and "consumer" are only used in the sense of CC.

15.2 List of Abbreviations

ABD	Assembly Build Diagram
CC	Common Criteria
EAL	Evaluation Assurance Level
ERP	Enterprise Resource Planning
IC	Integrated Circuit
IT	Information Technology
OS	Operating System
OSP	Organizational Security Policy
NPI	New Product Introduction
NPQ	New Product Qualification
PP	Protection Profile
SAP	Name of Software used for Enterprise Resource Planning
SAR	Security Assurance Requirement
SST	Site Security Target
ST	Security Target
TOE	Target of Evaluation
TSF	Security Function

16 Revision History

Rev.	Date	Justification of Change	Description of Changes
04	30-Aug-18	Update SST Documentation; Incorporate ITSEF comments on CC documentation.	• Update the document references (section 1.2, 3.0 and 8). • Changed ALC_DEL.1 & ALC_TAT.3 to not applicable in section 3.3. • Updated tables and sections 10, 13, 14.3 and 14.5 after mapping the requirements. Added table of dependency for Class ALC: Life-Cycle Support as reference. • Minor updates on some typographical, grammar and re-phrasing of some sentences in each section. • Use the new documentation template format.
05	29-July-19	Update SST Documentation	• Updated revision number and date. • Update contents similar as SF-SP-SEC-07 Rev 12. • Removed reference to ALC_CMS 5.2C from Section 14.5 O. Internal Transport. • Removed all Smartflex document references.

17 Document Approval

	Designation	Name	Signature	Date
Prepared By	Assistant Manager (Security, Safety & Facility)	Fareez Basheer		
Reviewed By	Document Controller	Joseph Lim		
	Senior Operations Manager	Andy Gong		
	General Manager	Pang Sze Yong		
Approved By	Management Representative	Cecilia Chua		
	Chief Executive Officer	Dr. Eric Ng		