SITE SECURITY TARGET LITE
Olivia Prime

Sii Sp. z o. o. / Branch in Gdańsk
Grunwaldzka 472E
80 – 309 Gdańsk

The certification ID:

Date approved:

.....

Managing Director

Gdańsk 2018

Table of Contents

Document Information

1.1 Reference

Title: Site Security Target Lite Olivia Prime for Sii Sp. z o. o.

Version: Version 1.3

Date: 14.02.2019

Company: Sii Sp. z o.o.

Name of the site: Olivia Prime Sii Sp. z o.o.

Product type: **Security IC**

EAL-Level: The site allows the development of TOEs with an EAL level up to EAL 6

1.2 Version history

VERSION	DATE	COMMENT/EDITOR/CHANGES
1.0	30.06.2017	Initial version
1.1	10.07.2017	Added LITE to title on first page.
1.2	24.10.2017	Update for Oliva Star building
1.3	14.02.2019	Update for Oliva Prime building

2 SST Introduction (AST_INT)

This chapter is divided into the sections "Identification of the Site" and "Site description".

This Site Security Target refers to the site Building Sii Sp. z o.o./Branch in Gdańsk (Olivia Prime, 10th floor).

The site can be a part of the production flow of the Product Type and is a subject of evaluation.

Identification of the SiteThe site Building Sii Sp. z o. o./Branch in Gdańsk is located at:

One location: Olivia Prime, 10th floor

Street: Grunwaldzka 472E

City: 80-309 Gdańsk

Country: Poland

Software development and validation will take place in dedicated rooms **10.01.17, 10.01.18, 10.01.19, 10.01.20, 10.01.21, 10.01.22, 10.01.23** and dedicated server room **10.01.24** (properly prepared regarding security measures). These rooms are located on the 10th floor of the Olivia Prime (office building).

Appendix: Structural outline – Olivia Prime, 10th floor (restricted document – available on site during evaluation process)

2.1 Site Description

Sii Sp. z o.o./Branch in Gdańsk is located in Olivia Business Centre – an office buildings complex in Gdańsk, Poland. Sii's rooms, labs and offices are situated on the 10th floor of Olivia Prime. The whole storey on the 10th floor of Olivia Prime forms a consistent working area and is occupied exclusively by Sii.

The following areas of the site specified in Chapter 0 are in the scope of the SST:

- **Olivia Prime:** location of Development and Testing Centre,

The building Olivia Prime, 10th floor is exclusively used by Sii but the area where the relevant activities (Development and Testing Centre) take place is limited to the 10th floor in building **Olivia Prime**.

All the physical security services (i.e. Access Control System, Alarm System and CCTV system) and procedures concerning physical security are provided by SII.

However, main parts of the IT security depend on NXP equipment (tools, CM system, switches, routers) and procedures. Therefore the scope of the certification is limited to the use of the site for NXP Semiconductors projects.

NOTE: Each time the term "client" or "customer" is used is this document it point on NXP Semiconductors.

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

Development of IC dedicated software (Software products) and embedded Software for smart card products including module tests, integration tests and system tests. Furthermore validation of functionality on silicon is part of the activities.

LIFE CYCLE:

The typical Life Cycle model for Smart Cards usually comprises the following phases:

- Preparation,
- Development,
- Production,
- Delivery,
- Operation,

whereas the site under evaluation supports only the life cycle phase

- **Development.**

The development life cycle phase consists of two main parts:

- Software development (phase 1)
- Software Validation/verification (phase 1)

Software Development

The goal of the Software Development is to generate all source files (containing source code) for the product.

The entry documents for Implementation are:

- Software Detailed Design (SDD),
- Software Unit Test Specification (SUTS).

The products of Implementation are:

- source code for Modules/Units,
- Draft User Documentation.

The main activities which are undertaken during Implementation are:

1. The source code is generated based on the design.
2. Code is crosschecked.

Verification and Validation

The goal of the **Verification and Validation** is to verify the integrated software against software designs and customer requirements specifications.

The entry documents for Verification and Validation are:

- crosschecked Module/Unit source code,
- Software Test Specification (STS) and Software Integration Test Specification (SITS),
- Customer Requirements Specifications (CRS) or Software Requirement Specifications (SRS).

The products of Verification and Validation are:

- Software product (e.g. hex, bin file) with all validated Modules/Units,
- Code for Test Cases,
- Updated User Documentation.

The main activities which are undertaken during Verification and Validation are:

Verification activities:

1. The test code is generated based on the test specification.
2. The software tests validate the individual Module/Unit according to STS.
3. All Modules/Units are integrated. The integrated code is tested according to SITS in the simulated environment.
4. All bugs discovered during the module and integrated software testing are addressed and solved within the team.
5. Software User Documentation is verified vis-à-vis the software code and accordingly updated.

Validation activities:

1. Customer Acceptance Tests (CAT) are performed for products which have acceptance tests done by or provided by the Customer. For other SW products, the integration tests are executed once again on the integrated SW on IC.
2. Any bugs discovered during SW validation will be first recorded and analyzed, then solved or escalated by the project team. Consultation with PM and/or Customer is recommended if the problems have heavy impact on the project goals.
3. Integration tests will be repeated until no more bugs are identified. In situations where the team has to release software that has known bugs, the bug details need to be mentioned in the release notes.

4. Software User Documentation is validated vis-à-vis the SRS or CRS. Any non-conformances are removed from the software User Documentation and the deliverable code.

Security

The Development and Testing Centre is a security area with a restricted access. Only authorised persons are allowed to enter this area.

The infrastructure is separated between the rooms with physical boundaries in a form of walls. All windows in project rooms are protected with sensors generating an alarm in case of any irregularities. Corridors and lifts are monitored by cameras. Smoke and fire detection alarm system is provided and connected to Gdańsk Firefighting monitoring centre. The facility has separate and independent power supplies UPS and power Generator.

The security area is secured by mantraps which can only be entered after successful authentication by card (company badge, visitor badge). A company badge or visitor badge has to be presented for access to the campus which hosts the Olivia Prime. Only authorised persons are allowed to enter.

For visitors getting access to the 14th floor of Olivia Prime a guest badge has to be requested to the ground floor Welcome Desk (the visitor ID is checked and put into Entry/Exit book). Any visitor must sign confidentiality agreement and get escort of Sii employee.

Every employee of Development and Testing Centre must enter through Olivia Prime. Next step is a turnstile at Welcome Desk (accessible by badge) and elevator in which badge is requested to get access to the 10th floor. There is no possibility of getting to other floors. To enter every project room a badge is requested again. Video control of all project rooms enables recording and checking events happening during day and night. Recordings are kept on server in a secured Data Archive Room administered by an authorised Sii employee. All recordings are stored for 90 days in an electronic form.

The security of the building is controlled by a Guard Services operated 24 hours and 7 days a week. Security guards are hired by Building Administrator and they have no access to Sii, if they have to raise an alert, the emergency Sii contact is called.

The cleaning company is operating during standard working hours, they access only under supervision.

3 Conformance Claims (AST_CCL)

The evaluation is based on Common Criteria Version 3.1, Revision 5.

1. Common Criteria for Information Technology Security Evaluation, Part 1: **Introduction and General Model**; Version 3.1, Revision 5
2. Common Criteria for Information Technology Security Evaluation, Part 3: **Security Assurance Requirements**; Version 3.1, Revision 5

For the evaluation the following methodology will be used:

1. Common Methodology for Information Technology Security Evaluation: **Evaluation Methodology**; Version 3.1, Revision 5
2. JIL Minimum Site Security Requirements
3. Supporting Document Guidance Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007
4. Guidance for Site Certification version 1.1, BSI

The assurance components chosen for the Site Security Target are taken from the definition of the EAL 6, as this is the level usually applied in Security IC (for Smart Card Code) development. Both the Sii Gdańsk site and the SST are conformant to the Common Criteria Part 3.

The chosen assurance components are derived from the assurance level **EAL6** of the assurance class **"Life-cycle Support"**. For the assessment of the security measures attackers with high attack potential are assumed.

The evaluation of the site comprises the following assurance components:

1. **ALC_CMC.5**
2. **ALC_CMS.5**
3. **ALC_DVS.2**
4. **ALC_LCD.1**
5. **ALC_TAT.3**

4 Security Problem Definition (AST_SPD)

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site and security problems derived from the configuration management requirements. The configuration management covers the integrity the security management of the site.

The Security Problem Definition comprises two major so called security problems. The first set of security problems comprises **all kind of attacks regarding theft** (e.g. samples) **or disclosure** (e.g. design data) or manipulation of assets. These security problems are described in terms of threats.

The second set of security problems comprises the requirements for the configuration management (e.g. controlled modification) and the control of security measures. These security problems are described in terms of Organisational Security Policies (OSP).

4.1 Assets

The following 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 concepts and the associated security measures as well as key and cryptographic tools for the encrypted exchange of data. These items are not explicitly listed in the list of assets below.

The integrity of any machine or tool used for software development, and for software testing is not considered an asset. Appropriate measures are defined for the site to ensure this important condition. These items consist of commercial available software which are programmed and customized by client.

Security Embedded Software Development / IC dedicated software development:

- Software specifications, (Software Detailed Design (SDD) and Software Unit Test Specification (SUTS)),
- Source code/Object code in any form,
- Pre-personalization data,
- Test profiles and test results,
- FPGAs containing netlists, (SmartCard Emulator),
- Un-fused secure element samples, (chips, cards),
- Physical prototype samples, (chips, cards),
- Development boards,
- Documentation related to the design of the logical objects, (Reviewed Software Detailed Design (SDD) document and Software Unit Test Specification (SUTS)),

- Documentation related to the testing of the security products. (Software Unit Test Specification (SUTS)) Software Integration Test Specification (SITS/STS), Customer Requirement Specifications (CRS) or Software Requirement Specifications (SRS)).

Described assets due to their specification are divided into groups:

1. Development data: The site has access to (and optionally copies thereof) electronic development data (specifications, guidance documentation, source code, etc.) in relation to developed TOEs. Both the integrity and the confidentiality of these electronic documents must be protected.
2. Development tools: To perform its development activities the site uses tools (e.g. compiler) to transform source code (and potentially the libraries that come with these tools) into binaries. The integrity of these tools (running on local or remote development computers) must be protected.
3. Physical security objects: The site has physical security objects (samples, emulators, printed documents, etc.) in relation to developed TOEs. Both the integrity and the confidentiality of these must be protected.

4.2 Threats

The threats identified for the site imply the necessity of defining assets which are endangered by those threats, those assets are described in 4.1 Assets.

The following threats are considered:

T. Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of all endangered assets 1 Development data to violate confidentiality and integrity, 2 Development tools in this case lab machines and 3 Physical security object such as samples and hardware emulators. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered. In addition the attacker may be able to use specific working clothes like cleaning service or technical maintenance service to camouflage the intention.

T. Rugged-Theft: An experienced thief with specialised equipment for burglary, who may by paid to perform the attack tries to access sensitive areas and manipulate or steal sensitive assets 1 Development data to violate confidentiality and integrity, 2 Development tools in this case lab machines and 3 Physical security object such as samples and hardware emulators .

T. Computer-Net: A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get 1 development data such as source code and documentation, or modify the 2 development tools such as IT infrastructure to violate the production process at the site.

T. Unauthorized-Staff: Employees or subcontractors not authorized to get access to products or systems used for production get access to 3 physical security objects especially samples and emulators or affect 2 development tools such as production systems or configuration systems or 1 development data so that the confidentiality and/or the integrity of the product is violated. This can apply to any production step and any asset of the final product as well as to the final product or its configuration.

T. Staff-Collusion: An attacker tries to get access to material processed at the time in order to get access to 1 development data so that the confidentiality and/or the integrity of the product will be violated or to get access to 3 physical security objects so that the confidentiality of the product will be violated. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery.

T. Attack-Transport: An attacker might try to get 3 physical security objects like specifications printouts or products during the internal shipment and/or the external delivery. The target is to retrieve from 3 physical security objects a 1 development data to compromise confidential information or violate the integrity of the products during the stated internal shipment and/or the external delivery process to allow a modification, cloning or the retrieval of confidential information after further production steps. Confidential information comprises design data, customer and/or consumer data like code and data (including personalization data and/or keys) stored in the ROM and/or EEPROM or classified product documentation.

The threats identified for the site imply the necessity of defining objectives which are intended to minimise the following risks:

1. physical loss
2. intellectual loss
3. loss of reputation

Any physical or intellectual loss may lead to project realisation disturbance or may even cause a project to be discontinued.

Loss of reputation may cause the site to stop being considered trustworthy by the current and potential clients.

4.3 Organisational Security Policies

The following policies are introduced by the requirements of the assurance components of ALC for the assurance **level EAL 6**. The chosen policies shall support the understanding of the production flow and the security measures of the site. In addition, they shall allow an appropriate **mapping to the Security Assurance Requirements (SAR)**.

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

The following policies are applicable:

P.Config-Items: The configuration management system (provided by the client) shall be able to uniquely identify configuration items. This includes the unique identification of items that are created, generated, developed or used at a site as well as the received and transferred and/or provided items.

P. Config-Control: The procedures for setting up the development process for a new product as well as the procedure that allows changes of the initial setup for a product shall only be applied by authorised personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes. The procedure for the initial set up of a production process ensures that sufficient information is delivered by the client.

P.Config-Process: The services and/or processes provided by a site are controlled in the configuration management plan. This comprises tools used for the production of the software, the management of flaws and optimisations of the process flow as well as the documentation that describes the services and/or processes provided by the site.

P.Reception-Control: The inspection of incoming items done at the site ensures that the received configuration items comply with the properties stated by the client. Furthermore, it is verified that the software can be identified and a released development process is defined for the software. If applicable this aspect includes the check that all required information and data is available to process the items.

P. Organise-Product: The development process is applied as specified by the client. If the data includes sensitive items like keys relevant for the life-cycle or configuration data that affect the security appropriate measures must be in place. This includes the requirement that the knowledge of sensitive keys shall be split to at least two different persons. Furthermore, technical measures like crypto-boxes, separation of network, split access permission and secure storage shall be implemented for this kind of data.

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

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

4.4 Assumptions

Each site operating in a production flow must rely on preconditions provided by the previous site. Each site has to rely on the information received by the previous site/client. This is reflected by the assumptions that are defined for the interface. The following assumptions are applicable:

A. Prod-Specification: The client must provide appropriate requirements specifications, definitions, assembly guidance, test requirements, test limits in order to ensure an appropriate development or production process. The provided information includes the classification of the documents and product.

A. Services-Ensurance: The client provides CM system used for product (software) development, as well as configures, and monitors internetwork devices (Routers, switches, firewalls and other VPN components) and establishes encrypted, secure connectivity (HW VPN) between Sii and client's premises. The client also provides, configures, and monitors laptops for secure software development.

A. Init-Data: The scripts for the configuration and initialisation / pre-personalisation process are provided by the client. The client verifies the configuration and/or initialisation / pre-personalisation process during the product introduction and the release process of the site.

A. Process-Specification: The development process is defined by the client who is the process owner. The Developers team working on the evaluated site is responsible for realization of a part of this process only.

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

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.

5 Security Objectives (AST_OBJ)

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

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

O. Security-Control: Assigned personnel of the site operate the systems for access control and surveillance and respond to alarm. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. This personnel are also responsible for registering and ensuring escort of visitors, unauthorized Sii employees, contractors and suppliers.

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

O. Internal-Monitor: The site performs security management meetings at least every six months. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audits is performed every year to control the application of the security measures.

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

O. Logical-Access: The site enforces a logical separation between the internal network and the internet by a firewall. The firewall ensures that only defined services and defined connections are accepted. Furthermore, internal network is separated into a production network and an office 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 related system is restricted to authorised employee that work in the production systems. Every user of on IT system has its own user account and password. An authentication using user account and password is enforced by all computer systems.

O. Logical-Operation: All network segments and the computer systems are kept up-to-date (software, updates, security patches, virus protection, spyware protection). The back-up of sensitive data and security relevant logs is applied according to the classification of the stored data.

O. Config-Items: The site uses a configuration management system (provided by the client) that assigns a unique internal identification to each product to uniquely identify configuration items and allow an assignment to the client. Also the internal procedures and guidance are covered by the configuration management.

O. Config-Control: The site applies a release procedure for the setup of the production process for each new product. In addition, the site has a process to classify and introduce changes for services and /or processes of released products. Minor changes are handled by the site, major changes must be acknowledged by the client. A designated team is

responsible for the release of new products and for the classification and release of changes. This team comprises specialists for all aspects of the services and/or processes. The services and/or processes can be changed by authorised personnel only. Automated systems support configuration management and production control.

O. Organise-Product: For the development process it is ensured that the specified process is applied. The data integrity is controlled. Keys and other sensitive data can only be constructed by at least two employees. The operation is applied in crypto-boxes or similar devices. After the release process changes are only applied based on the request of the client. The update is done according to a controlled process.

O. Staff-Engagement: All employees who have access to sensitive configuration items and who can move parts of the product out of the defined production flow are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.

O. Internal-Shipment: The recipient of a physical configuration item is identified by the assigned client address. The internal shipment procedure is applied to the configuration item. The address for shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of configuration items during internal shipment. For every sensitive configuration item, the protection measures against manipulation are defined.

O. Transfer-Data: Sensitive electronic configuration items (data or documents in electronic form) are protected witch cryptographic 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 secure measures and they are sufficiently protected.

5.1 Security Objectives Rationale

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

5.1.1 Mapping of Security Objectives

Threat and Organisational Security Policy	Security Objectives	Rationale

T. Smart-Theft	O. Physical-Access O. Security-Control O. Alarm-Response O. Internal-Monitor O. Maintain-Security	The combination of structural, technical and organisational measures detects unauthorized access and allow for appropriate response on any threat. O. Physical-Access ensures that the Secure Rooms are physically partitioned off, so cannot be entered without access control check. O. Security-Control ensures that an attacker will be detected when trying to reach the assets through the Secure Rooms. O. Alarm-Response supports O. Physical_Access and O. Security_Control by ensuring that a response will be given to the alarm systems and that this response is quick enough to prevent access to the assets. O. Internal-Monitor and O. Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T. Smart_Theft.
T. Rugged-Theft	O. Physical-Access O. Security-Control O. Alarm-Response	The combination of structural, technical and organisational measures detects unauthorized access

	O. Internal-Monitor O. Maintain-Security	and allow for appropriate response on any threat. O. Physical-Access ensures that the Secure Rooms are physically partitioned off, so cannot be entered without access control check. O.Security-Control ensures that an attacker will be detected when trying to reach the assets through the Secure Rooms. O.Alarm-Response supports O.Physical_Access and O.Security_Control by ensuring that a response will be given to the alarm systems and that this response is quick enough to prevent access to the assets. O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T. Rugged_Theft.
T. Computer-Net	O. Internal-Monitor O. Maintain-Security O. Logical-Access O. Logical-Operation O. Staff-Engagement	The technical and organisational measures prevent Unauthorized access to the internal network. Requirements and rules regarding this threat are defined in both Site's and client's documentation.

		O.logical-Access ensures that the development network is not connected to anything that an attacker could use to set up a remote connection. O.Logical-Operation ensures that all computer systems used to manage the Business Unit network are kept up to date (software updates, security patches, virus and spyware protection). O.Staff-Engagement gives employees trainings, security checks to prevent access to assets or configurations items. O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T.Computer-Net.
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	Physical and logical access control limits the access to sensitive data to authorised persons. Any other person may enter the project rooms only under the supervision of an authorised person (typically PM). Requirements and rules regarding this threat are defined in both Site's and client's

		documentation. O. Physical-Access ensures that the Secure Rooms are physically partitioned off, so cannot be entered without access control check. O.Security-Control ensures that an attacker will be detected when trying to reach the assets through the Secure Rooms. O.Alarm-Response supports O.Physical_Access and O.Security_Control by ensuring that a response will be given to the alarm systems and that this response is quick enough to prevent access to the assets. O.Logical-Access and O.Logical-Operation ensures that unauthorized people can't have access to assets or configurations items. O.Staff-Engagement gives employees trainings, security checks to prevent access to assets or configurations items. O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T.

		Unauthorised-Staff.
T. Staff-Collusion	O. Internal-Monitor O. Maintain-Security O. Staff-Engagement O. Transfer-Data	The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees prevent Unauthorized access to sensitive data or items. O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. O. Transfer-Data ensures that sensitive electronic configuration items (data or documents in electronic form) are protected. Together, these objectives will therefore counter T.Staff-Collusion.
T. Attack-Transport	O. Transfer-Data O. Internal-Shipment O. Staff-Engagement	The applied security measures on sensitive data during internal shipment prevent modification or disclosure of any sensitive data during transport. The applied security measures on physical items during internal shipment allow detection of attempted attacks (e.g. suspicious

		and/or damaged parcel). O. Transfer-Data ensures that sensitive electronic configuration items (data or documents in electronic form) are protected. O. Internal-Shipment ensures that for every sensitive configuration item, the protection measures against manipulation are defined. O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). Together, these objectives will therefore counter T. Attack-Transport.
P. Config-Items	O. Config-Items	All configuration items are assigned a unique identifier by the CM System provided by the client. O. Config-Items ensures that all configuration items are assigned a unique identifier by the CM System provided by the client This objective will therefore fulfil P. Config-Items.
P. Config-Control	O. Config-Items O. Config-Control O. Logical-Access	The services provided by the site and processes defined by the client are described in the internal procedures and guidance. The procedures

		and guidance are covered by the configuration management. O. Config-Items ensures that all configuration items including procedures are assigned a unique identifier by the CM System provided by the client O. Config-Control ensures that site applies a release procedure for the setup of the production process for each new product. O. Logical-Access ensures access control and interactive acceptance measures for set up and changes. This objective will therefore fulfil P. Config-Control.
P. Config-Process	O. Config-Items O. Config-Control	The services provided by the site and processes defined by the client are described in the internal procedures and guidance. The procedures and guidance are covered by the configuration management. O. Config-Items ensures that all configuration items including documentation are assigned a unique identifier by the CM System provided by the client

		O. Config-Control ensures that site applies a release procedure for the setup of the production process for each new product. Together, these objectives will therefore fulfil P. Config-Process.
P. Reception-Control	O. Transfer-Data O. Internal-Shipment O. Staff-Engagement	The controlled shipment and delivery procedures ensure correct shipment and delivery of items. The applied security measures on incoming items done at the site ensures that the received configuration items comply with the properties stated by the client. O. Transfer-Data ensures that sensitive electronic configuration items (data or documents in electronic form) are protected. O. Internal-Shipment ensures that for every sensitive configuration item, the protection measures against manipulation are defined. O. Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). Together, these objectives will therefore fulfil P. Reception-Control.

P. Organise-Product	O. Logical-Access O. Logical-Operation O. Organise-Product	The development process (being part of client's production process) is applied as specified by the client. All process activities requiring justified change necessitates client's permission. The client's procedures define the exact rules in that matter. O.Logical-Access and O.Logical-Operation ensures that unauthorized people can't have access to assets or configurations items. O. Organise-Product ensures that for development the specific process and security measures are applied. Together, these objectives will therefore fulfil P. Organise-Product.
P. Product-Transport	O. Config-Items O. Internal-Shipment O. Transfer-Data	The controlled shipment and delivery procedures ensure correct shipment and delivery of items. O. Config-Items ensures that all configuration items are assigned a unique identifier by the CM System provided by the client O. Internal-Shipment ensures that for every sensitive configuration item, the protection measures against

		manipulation are defined. O. Transfer-Data ensures the secure traceability of package. Together, these objectives will therefore fulfil P. Product-Transport.
P. Transfer-Data	O. Logical-Access O. Logical-Operation O. Transfer-Data	Any classified or higher security level data in electronic form is encrypted to ensure confidentiality of the data and sent to client over encrypted VPN connection. In addition measures are used to control the integrity of the data after the transfer. The client's procedures define the exact rules in that matter. O.Logical-Access and O.Logical-Operation ensures that unauthorized people can't have access to assets or configurations items. O. Transfer-Data ensures the protection of sensitive electronic configuration items. Together, these objectives will therefore fulfil P. Transfer-Data.

6 Extended Components Definition (AST_ECD)

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

7 Security Assurance Requirements (AST_REQ)

The security assurance requirements for this Site Security Target shall support an evaluation according to the assurance level EAL6.

7.1 Application Notes and Refinements

The description of the site certification process [4] includes specific application notes. The site shall allow product evaluation according to the assurance component AVA_VAN.5. The main item is that a product that is considered as intended TOE is not available during the evaluation. Since the term “TOE” is not applicable in the SST the associated processes for the handling of products are in the focus and described in this SST. These processes are subject of the evaluation of the site.

The Security Assurance Requirements (SARs) are:

Class ALC: Life-cycle support

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

7.1.1 Overview and refinements regarding CM (Configuration Management) capabilities (ALC_CMC)

Configuration Management, as being the practice of handling all project changes systematically to maintain project integrity over time, is defined at the project starting phase.

According to [4]the processes rather than a TOE are in the focus of the CMC examination. The changed content elements are presented below. Since the application notes in [4]are defined for ALC_CMC.5.

Sii implements certain procedures, rules and uses tools that are required to manage and evaluate proposed changes, track the status of changes, and to maintain project documentation.

Changes occurring within the project operation could be divided into groups:

1. **Changing project requirements** – change control management
2. **Software revision control changes** – practice that tracks and provides control over changes to source code
3. **Validation set-up configuration changes** – based on BKC (Best Known Configuration) provided by a Client.

Within development and validation projects different tools and frameworks are created according to defined revision control system. Supporting Client's projects Sii makes use of many different source control version tools, e.g. following steps described below:

1. **Revision control changes process - step 1:**

   Create local working copy from repository, perform code changes and develop new code on local copy (each programmer on his station), test code and update local copy, commit to repository, after each change committed application build occurs and Continuous Integration process is started (automated source code and functionality validation), push to project common remote repository.

2. **Revision control changes process – step 2:**

   Create local workspace, create global change list (consist of all changed files), modified files are shelved remotely, Continuous Integration process is started (source code build, automated tests), code review process is triggered, code merge with latest versions from remote repository, once again CI process is carried out, code changes are submitted to project common remote repository.

Changes to development and validation platform configurations are based on BKC (Best Known Configuration) provided by Client on weekly/biweekly basis. Package is installed on test platforms and all configuration issues are reported in defined by Client tracking tool as artefacts or items. After resolving new BKC issues manual and automated test execution process starts.

CAUTION: In case of Sii all the documentation concerning ALC_CMC is mainly based on the one provided by the client.

7.1.2 Overview and refinements 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 handled at the site.

As this site is not directly involved with producing, storing or delivering the TOE, the only relevant configuration items under CM scope are:

- This Site Security Target for this site,
- The Development Security documentation for this site (site security procedures),
- Life Cycle Support documentation
- The client's documentation described in 4.1,
- All documentation related to the inspection of the development process (client's audits confirmed with reports, internal audits confirmed with reports)
- Test results.

In order to manage the client's documentation (described in 4.1 as well as related to the inspection of the development process) an appropriate revision control system is provided by client. In order to manage the site security procedures documentation an internal web application (based on share point repository) is used.

7.1.3 Overview and refinements regarding Delivery procedure (ALC_DEL)

Due to the specific nature of projects realised in the evaluated site (our engineers are part of larger teams situated in various locations in Europe) and due to client's requirements, the site does not define any internal procedure concerning external delivery. In fact, the development process does not contain any external delivery.

As a result, the ALC_DEL procedure is not applicable to this site.

7.1.4 Overview and refinements regarding Development Security (ALC_DVS)

The combination of physical partitioning between the different access control levels together with technical and organisational security measures allows a sufficient separation of employees to enforce the "need to know" principle. The access control shall support the limitation for the access to these areas including the identification and rejection of Unauthorized people.

Assigned personnel of the site operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, sensors support the enforcement of the access control. This personnel are also responsible for registering and ensuring escort of visitors, Unauthorized Sii employees, contractors and suppliers.

The technical and organisational security measures ensure that an alarm is generated before an Unauthorized person gets access to any asset. After the alarm is triggered the Unauthorized person still has to overcome further security measures. The reaction time of the employees or guards is short enough to prevent a successful attack.

The site performs security management meetings at least every six months. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed to control the application of the security measures.

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

The computer systems are connected to the encryption equipment are kept up-to-date (software updates, security patches, virus protection, spyware protection).

The Site has measures in place to destruct sensitive documentation, erase electronic media and destroy sensitive configuration items so that they do not support an attacker.

All employees who have access to assets are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.

7.1.5 Overview and refinements regarding Life-cycle definition (ALC_LCD)

The Site is not equal to the entire development environment. Therefore the ALC_LCD criteria are interpreted in a way that only this life-cycle phase has to be evaluated which is in the scope of the site. For this site the ‘Development’ life-cycle phase is relevant.

7.1.6 Overview and refinements regarding Tools and Techniques definition (ALC_TAT)

The CC assurance components of family ALC_TAT refer to the tools that are used to during development process. The client's defines which tools and techniques have to be used by the site. The client provides the complete environment with all necessary tools preinstalled. The proper usage of the provided tools and defined techniques is verified be the client during audits.

7.2 Security Assurance Rationale

7.2.1 Security Assurance Rationale – Dependencies

The dependencies for the assurance requirements are as follows (see (Common Criteria, July 2009), appendix C):

SAR	Dependency
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:

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

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

7.2.2 Security Assurance Rationale – ALC-CMC

SAR	Security Objectives	Rationale
ALC_CMC.5.1C The TOE shall be labelled with its unique reference.	O. Config-Items O. Config-Control	The particular modules are stored in Version Control System which manages version numbering of particular source code and binary files. That Product, which has been integrated

		from few modules, has a unique version, label in the team work platform, stored package and Release Notes. For details refer to [9] Life-cycle Support document. O. Config-Items ensures that all configuration items are assigned a unique identifier by the CM System provided by the client. O. Config-Control ensures that site applies a release procedure for the setup of the production process for each new product. Together, these objectives will therefore fulfil ALC_CMC.5.1C.
ALC_CMC.5.2C The CM documentation shall describe the method used to uniquely identify the configuration items.	O. Config-Items O. Config-Control	The site uses naming conventions defined and provided by the client. The naming conventions (e.g. project naming, on-chip naming, file version numbering) allows unique identification of the configuration items. O. Config-Items ensures that all configuration items are assigned a unique identifier by the CM System provided by the client. O. Config-Control ensures that site applies a release

		procedure for the setup of the production process for each new product. Together, these objectives will therefore fulfil ALC_CMC.5.2C.
ALC_CMC.5.3C The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.	O. Config-Control	Adequate and appropriate review of changes to configuration items is covered by the Change Control procedures managed by the project leader. These procedures are defined by the client in the Project Management Plan (per project). O. Config-Control ensures that site applies a process to classify and introduce changes for services and /or processes of released products. Together, these objectives will therefore counter ALC_CMC.5.3C.
ALC_CMC.5.4C The CM system shall uniquely identify all configuration items.	O. Config-Items O. Config-Control	The site uses naming conventions defined and provided by the client. The naming conventions (e.g. project naming, on-chip naming, file version numbering) allows unique identification of the configuration items. O. Config-Items ensures that

		all configuration items are assigned a unique identifier by the CM System provided by the client O. Config-Control ensures that site applies a release procedure for the setup of the production process for each new product. Together, these objectives will therefore fulfil ALC_CMC.5.4C.
ALC_CMC.5.5C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	O. Config-Control O. Logical-Access	All configuration items are kept under configuration control by O. Config-Control. The O. Config-Control objective is supported by O. Logical-Access that requires the authentication of each user before any change can be applied to a configuration item. O. Config-Control ensures that site applies a process to classify and introduce changes for services and /or processes of released products. O. Logical-Access ensures access control and interactive acceptance measures for set up and changes. Together, these objectives will therefore fulfil

		ALC_CMC.5.5C.
ALC_CMC.5.6C The CM system shall support the production of the TOE by automated means.	O. Config-Control O. Organise-Product	The CM plan describes in detail a system integration process i.e. automated means to produce the TOE. It uses continuous integration tool do define compilation process and built system with compiler. For details refer to [9] Life-cycle Support document. O. Config-Control ensures that site applies a release procedure for the setup of the production process for each new product. O. Organise-Product ensures that for development the specific process and security measures are applied. Together, these objectives will therefore fulfil ALC_CMC.5.6C.
ALC_CMC.5.7C The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	O. Config-Control O. Organise-Product	The modified source code undergoes the code review performed by a SE other that the one who developed it. For the module an Architect of this module decides if all new/modified functionalities should be released and send to System Integrator. For the product release the System Integrator decides if the modified module will be included in the Product

		version being released. O. Config-Control ensures that site applies a process to classify and introduce changes for services and /or processes of released products. O. Organise-Product ensures that for development the specific process and security measures are applied. Together, these objectives will therefore fulfil ALC_CMC.5.7C.
ALC_CMC.5.8C The CM system shall identify the configuration items that comprise the TSF.	O. Config-Control O. Organise-Product	The CM documentation defines Security Objects and the CM plan defines the storage method and access. Access levels (managed by Configuration Managers) are being set for users to modules in the team work platform. For details refer to [9] Life-cycle Support document. O. Config-Control ensures that site applies a release procedure for the setup of the production process for each new product. O. Organise-Product ensures that for development the specific process and security measures are applied.

		Together, these objectives will therefore fulfil ALC_CMC.5.8C.
ALC_CMC.5.9C The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.	O. Config-Control O. Organise-Product	The VCS within team work platform enables review of an author, date and time of particular changes to the module source code files. The team work platform offers a GUI which enables review of audit trail. For details refer to [9] Life-cycle Support document. O. Config-Control ensures that site applies a process to classify and introduce changes for services and /or processes of released products. O. Organise-Product ensures that for development the specific process and security measures are applied. Together, these objectives will therefore fulfil ALC_CMC.5.9C.
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. Organise-Product	All change requests are created in the tracker. Based on it a list of change requests is being reviewed and concerned by a body called Change Control Board. Accepted change requests are directed to the Product architect, who makes

		changes to the Product documentation and creates tasks for the SEs in the tracker. For details refer to [9] Life-cycle Support document. O. Config-Control ensures that site applies a process to classify and introduce changes for services and /or processes of released products. O. Organise-Product ensures that for development the specific process and security measures are applied. Together, these objectives will therefore fulfil ALC_CMC.5.10C.
ALC_CMC.5.11C The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.	O. Config-Items O. Config-Control	The implementation representations (source codes) are managed in a revision control system which automatically assigns a unique number to each revision (version). Reference to revision numbers are used in Change Requests, Problem Reports, Release Notes etc. O. Config-Items ensures that all configuration items are assigned a unique identifier by the CM System provided by the client. O. Config-Control ensures

		that site applies a release procedure for the setup of the production process for each new product. Together, these objectives will therefore fulfil ALC_CMC.5.11C.
ALC_CMC.5.12C The CM documentation shall include a CM plan.	O. Config-Control	The CM documentation includes the CM plan document maintained for the Project by a Configuration Manager. The CM plan is a single document. The CM plan is being versioned during maintenance. O. Config-Control ensures that site applies a release procedure for the setup of the production process for each new product. That objective will therefore fulfil ALC_CMC.5.12C.
ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the TOE.	O. Config-Control O. Organise-Product	The CM plan describes how the CM system is used in aspects of change control, system integration tools, Responsibilities in CM process, activities of Change Control Board, VCS and TOE labelling, Data-backups. For details refer to [9] Life-cycle Support document. O. Config-Control ensures that site applies a release

		procedure for the setup of the production process for each new product. O. Organise-Product ensures that for development the specific process and security measures are applied. Together, these objectives will therefore fulfil ALC_CMC.5.13C.
ALC_CMC.5.14C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.	O. Config-Control O. Organise-Product	The CM plan describes the System Integration Process. For the source code the acceptance procedure includes code review, commit, built verification and validation, subsequently integration into module and further integration into system. For the documentation the acceptance procedure includes commit and review. For details refer to [9] Life-cycle Support document. O. Config-Control ensures that site applies a process to classify and introduce changes for services and /or processes of released products. O. Organise-Product ensures that for development the specific process and security measures are applied.

		Together, these objectives will therefore fulfil ALC_CMC.5.14C.
ALC_CMC.5.15C The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O. Config-Items O. Config-Control	All configuration items are kept under configuration control according to O. Config-Items and O. Config-Control. For details refer to [9] Life-cycle Support document. O. Config-Items ensures that all configuration items are assigned a unique identifier by the CM System provided by the client O. Config-Control ensures that site applies a release procedure for the setup of the production process for each new product. Together, these objectives will therefore fulfil ALC_CMC.5.15C.
ALC_CMC.5.16C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O. Config-Items O. Config-Control	As the evidence of usage of the CM system in accordance with the CM plan there are among the others: System integration reports, V&V reports, Tracker artifacts (ie. tickets with their history entries),Revisions of files in the VCS, Logs for a file in the VCS, Code review reports, CR history in the RMS.

		O. Config-Items ensures that all configuration items are assigned a unique identifier by the CM System provided by the client. O. Config-Control ensures that site applies a release procedure for the setup of the production process for each new product. Together, these objectives will therefore fulfil ALC_CMC.5.15C.

7.2.3 Security Assurance Rationale – ALC-CMS

SAR	Security Objectives	Rationale
ALC_CMS.5.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.	O. Config-Items O. Config-Control	Configuration list for each release in case of projects executed in the Site is included in the Release Notes for that release. For details refer to [9] Life-cycle Support document. O. Config-Items ensures that all configuration items are assigned a unique identifier by the CM System provided by the client. O. Config-Control ensures that site applies a release procedure for the setup of the production process for each new product. Together, these objectives

		will therefore fulfil ALC_CMS.5.1C.
ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.	O. Config-Items	All configuration items in the release notes are listed by a name and a version number or a tag in the VCS. O. Config-Items ensures that all configuration items are assigned a unique identifier by the CM System provided by the client. That objective will therefore fulfil ALC_CMS.5.2C.
ALC_CMS.5.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	O. Config-Items	For all configuration items (including TSF relevant configuration items) the release notes include information who and how changed it, the reference to the team work platform project and requirements management system project related to the change. O. Config-Items ensures that all configuration items are assigned a unique identifier by the CM System provided by the client. That objective will therefore fulfil ALC_CMS.5.3C.

7.2.4 Security Assurance Rationale – ALC-DEL

SAR	Security Objectives	Rationale

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.	Not applicable for that site.	Not applicable for that site.

7.2.5 Security Assurance Rationale – ALC-DVS

SAR	Security Objectives	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. Maintain-Security O. Logical-Access O. Logical-Operation O. Staff-Engagement O. Internal-Shipment O. Transfer-Data O. Internal-Monitor	For details refer to [9] Life-cycle Support document. O. Physical-Access, O. Security-Control and O. Alarm-Response ensures the physical security measures. O.Logical-Access and O.Logical-Operation ensures that unauthorized people can’t have access to assets or configurations items. O.Staff-Engagement gives employees trainings, security checks to prevent access to assets or configurations items. O. Internal-Shipment ensures that for every sensitive configuration item, the protection measures against manipulation are defined. O. Transfer-Data ensures that sensitive electronic

		configuration items (data or documents in electronic form) are protected. O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore fulfil ALC_DVS.2.1C.
ALC_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	O. Internal-Monitor O. Internal-Shipment O. Transfer-Data O. Maintain-Security	For details refer [9] Life-cycle Support document. O. Internal-Monitor and O. Maintain-Security ensures the sufficiency of applied security measures. O. Internal-Shipment ensures that for every sensitive configuration item, the protection measures against manipulation are defined. O. Transfer-Data ensures that sensitive electronic configuration items (data or documents in electronic form) are protected. Together, these objectives will therefore fulfil ALC_DVS.2.2C.
ALC_DVS.2.3C The evidence shall justify that the security measures provide the necessary level of protection to maintain the	O. Internal-Monitor O. Internal-Shipment O. Transfer-Data O. Maintain-Security	The justification of security measures to provide the necessary level to maintain the confidentiality and integrity of products is

confidentiality and integrity of the TOE.		commonly covered by the alignment of security measures with state of the art Minimum Site Security Requirements. Together, all of these objectives (O. Physical-Access, O. Security-Control, O. Alarm-Response, O. Maintain-Security, O. Logical-Access, O. Logical-Operation, O. Staff-Engagement, O. Internal-Shipment, O. Transfer-Data O. Internal-Monitor) are related to the implemented security measures in place and will therefore fulfil ALC_DVS.2.3C.

7.2.6 Security Assurance Rationale – ALC-LCD

SAR	Security Objectives	Rationale
ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.	O. Config-Control O. Organise-Product	For details refer to [9] Life-cycle Support document. O. Config-Control ensures that site applies a release procedure for the setup of the production process for each new product. O. Organise-Product ensures that for development the specific process and security measures are applied. Together, these objectives

		will therefore fulfil ALC_LCD.1.1C.
ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	O. Config-Control O. Organise-Product	For details refer to [9] Life-cycle Support document. O. Config-Control ensures that site applies a release procedure for the setup of the production process for each new product. O. Organise-Product ensures that for development the specific process and security measures are applied. Together, these objectives will therefore fulfil ALC_LCD.1.2C.

7.2.7 Security Assurance Rationale – ALC-TAT

SAR	Security Objectives	Rationale
ALC_TAT.3.1C Each development tool used for implementation shall be well-defined.	O. Organise-Product	The [9] Life-cycle Support document shows that the development tools used for implementation are well-defined. O. Organise-Product ensures that for development the specific process and security measures are applied. That objective will therefore fulfil ALC_TAT.3.1C.
ALC_TAT.3.2C The documentation of each development tool shall	O. Organise-Product	The [9] Life-cycle Support document shows that the development tools used for implementation are well-

unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.		defined. O. Organise-Product ensures that for development the specific process and security measures are applied. That objective will therefore fulfil ALC_TAT.3.2C.
ALC_TAT.3.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.	O. Organise-Product	The [9] Life-cycle Support document shows that the development tools used for implementation are well-defined. O. Organise-Product ensures that for development the specific process and security measures are applied. That objective will therefore fulfil ALC_TAT.3.2C.

8 Site Summary Specification (AST_SSS)

8.1 Preconditions Required by the Site

This section provides background information on the assumptions defined in chap. 4.4.

Assumption	Fulfilment of assumption
A. Prod-Specification: The client must provide appropriate requirements specifications, definitions, assembly guidance, test requirements, test limits in order to ensure an appropriate development or production process. The provided information includes the classification of the documents and	The client provides appropriate documentation concerning the software development for smart cards. All documents provided by the client are classified as **'company confidential', 'strictly confidential'** or similar classification if they require protection against disclosure. All documents with no classification as confidential document are regarded as 'public' or ‘internal use’.

product.	
A. Services-Ensurance: The client provides CM system used for product (software) development, as well as configures, and monitors internetwork devices (Routers, switches, firewalls and other VPN components) and establishes encrypted, secure connectivity (HW VPN) between Sii and client's premises. The client also provides, configures, and monitors laptops for secure software development.	The Site is connected with the Client environment by the hardware VPN, which is configured and managed by the Client. The Client provides properly configured work stations. Security measures for data transfer, network and software development environment which are also settled and managed by the Client.
A. Init-Data: The scripts for the configuration and initialisation / pre-personalisation process are provided by the client. The client verifies the configuration and/or initialisation / pre-personalisation process during the product introduction and the release process of the site.	The client provides laptops for project development with pre-configured environment, installed software, predefined security rules and Sofos HDD encryption. Each time an additional software is changed or modification needed a special application "Run Advertised Programs" is used. (according to How to Installing Programs via "Run Advertised Programs" client's internal document)
A. Process-Specification: The development process is defined by the client who is the process owner.	The Sii team working on the evaluated site is responsible for realization of a part of this process only. The client is responsible for acceptance (based on acceptance tests) of the result of the development process. The result of the development process performed on the site is not the final product of the whole process.
A. Item-Identification: Each configuration item received by the site is appropriately labelled to ensure the identification of the configuration item.	The site uses naming conventions defined and provided by the client. The naming conventions (e.g. project naming, on-chip naming, file version numbering) allows unique identification of the configuration items.
A. Internal-Shipment: The recipient	For every internal shipment expected from the

(client) of the product is identified by the address of the client site. The address of the client is part of the product setup.	Site, the client has to provide the Site appropriate address data. This shall be address data for physical items and equivalent address data (e.g. email address) for the delivery or shipment of electronic items.

8.2 Services of the Site

Services provided by Sii for Client connected with software development for smart cards are the following:

- Elaboration of architecture documentation and software design documentation,
- Development of source code,
- Design and development of test software and test environments,
- Design and development of test frameworks,
- Development of test cases and documentation,
- Providing validation services,

All services mention above are performed in the development environment managed by the client.

The services mentioned above constitute the Development phase of the Smart Card life-cycle.

8.3 Objectives Rationale

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

O. Physical-Access:

The development site is operated by Sii only and is not shared with other companies.
The site is separated into different security levels. The development site is monitored by security staff Sii and security guards on duty and surveillance cameras at all times. Only authorized users are allowed within the development site. They have to authenticate themselves by staff badge or visitor badge.

These measures prevent access to sensitive areas for any unauthorized person and therefore prevent the threats T. Smart-Theft, T. Rugged-Theft, T. Unauthorized-Staff.

O. Security-Control:

The security guards are monitoring the site and the surveillance system 24 hours a day. According the security level the areas are patrolled by the guards frequently. The alarm system and the CCTV system support the security control. Further on the security control is supported by O. Physical-Access requiring different level of access control for the access to the related assets 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 is addressed.

O. Alarm-Response:

The alarm system is connected to the guard house that is manned 24 hours a day. Additional patrolling and the CCTV system support the alarm respond. Additionally, the employees are responding the alarm system during working hours. O. Physical-Access requires certain time to overcome the different level of access control. The response time of the guard and the physical resistance match 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 physical security access control, alarm system, Firewall, and Virus protection. Major changes of security systems and security procedures are reviewed and approved by the responsible security managers.

In addition, internal audits are performed on a regular basis to ensure the application of the security measures.

The monitoring and protection of the IT systems (CCTV, access control, alarm system and network) are handled by the IT departments under supervision of the IT security manager of the company's security staff.

This addresses the threats T. Smart-Theft, T. Rugged-Theft, T. Computer-Net, T. Unauthorized-Staff, T. Staff-Collusion.

O. Maintain-Security:

All security related alarm and detection systems are checked on a regular basis. Logs for building access or site access as well as access to especially secured areas are stored and checked on a regular basis by security guards. Network security is monitored permanently by the IT department.

This addresses the threats T. Smart-Theft, T. Rugged-Theft, T. Computer-Net, T. Unauthorized-Staff, T. Staff-Collusion.

O. Logical-Access:

The IT network is logically separated from the outside world by a firewall system consisting of several firewalls which ensures that only authorized connections from and to the IT network are possible. At least two firewalls (i.e. outer firewall and inner firewall) are present between the outside world and any internal network.

Each user has an individual account. To access data on the company's network every user has to authenticate himself either by login name and password or token and password. Multiple successive failed authentication attempts lead to a blocked the account. The number of retries depend on the authentication method.

Access rights to all network resources are set according to a need-to-know or need-to have

basis, respectively. Access rights of users who do not need access to a network share any longer (e.g. change of jobs) are revoked. In particular, all accounts of employees who leave the company are deactivated.

This addresses the threats T. Computer-Net and T. Unauthorized-Staff and support the OSPs P. Config-Control, P. Organize-Product and P. Transfer-Data.

O. Logical-Operation:

Virus protection and patch management for operating systems and applications ensure the correct operation of the systems and prevent the systems from malfunction. They ensure that protective measures of the IT workplaces are up-to-date (virus definitions, security patches of operating system, security patches of programs, etc.). In addition, regular backups are applied to all network shares related to the configuration management system to prevent loss of data. Backup tapes are securely stored.

This addresses the threats T. Computer-Net and T. Unauthorized-Staff and support the OSP P. Organize-Product and P. Transfer-Data.

O. Config-Items:

All configuration items are identified by a unique version number by the configuration management system. The configuration management system allows unique labelling of any set of configuration items in the configuration management system.

By this the OSPs P. Config-Items, P. Config-Control, P. Config-Process and P. Product-Transport are addressed.

O. Config-Control:

The services provided by the site and processes defined by the client are described in the internal procedures and guidance. The procedures and guidance are covered by the configuration management.

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

O. Organize-Product:

The development process (being part of client's production process) is applied as specified by the client. All process activities requiring justified change necessitates client's permission. The client's procedures define the exact rules in that matter.

This addresses the OSP P. Organise-Product.

O. Staff-Engagement:

All employees working at the site and having access to sensitive information or data have to sign a non-disclosure agreement to provide legal liability to protect sensitive information against disclosure. In addition, all employees are trained regarding security to support the security awareness.

This addresses the threats T. Computer-Net, T. Unauthorized-Staff and T. Staff-Collusion, T. Attack-Transport and support the OSP P. Reception-Control.

O. Internal-Shipment:

For every internal shipment expected from the development Sii by the client, the client has to provide the Sii with appropriate address data. This shall be address data for physical items and equivalent address data (e.g. email address) for the delivery or shipment of electronic items.

The threat T. Attack-Transport and the OSP P. Reception-Control and P. Product-Transport are addressed by the internal shipment.

O. Transfer-Data:

The integrity and confidentiality of the data transfer from/to the site and within the site is ensured by appropriate secure measures.

The threat T. Staff-Collusion and T. Attack-Transport as well as the OSP P. Reception-Control , P. Product-Transport and P. Transfer-Data.

8.4 Security Assurance Requirements Rationale

The Security Assurance Requirements rationale does not explicitly address the developer action elements defined in [2] because they are implicitly included in the content elements. This comprises the provision of the documentation to support the evaluation and the

preparation for the site visit. In addition, this includes that the procedures are applied as written and explained in the documentation.

8.4.1 ALC_CMC.5

The security assurance requirements of the assurance class "CM capabilities" listed below are suitable to support the secure and efficient development of products due to the formalized acceptance process and the automated support. The identification of all configuration items allows a parallel development of different products. The requirement for authorized changes support the integrity and confidentiality required for the products. Therefore this assurance level meets the requirements for the configuration management.

8.4.1.1 ALC_CMC.5.1C

The TOE shall be labelled with its unique reference.

8.4.1.2 ALC_CMC.5.2C

The CM documentation shall describe the method used to uniquely identify the configuration items.

8.4.1.3 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.

8.4.1.4 ALC_CMC.5.4C

8.4.1.5 The CM system shall uniquely identify all configuration items.ALC_CMC.5.5C

The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

8.4.1.6 ALC_CMC.5.6C

The CM system shall support the production of the TOE by automated means.

8.4.1.7 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.

8.4.1.8 ALC_CMC.5.8C

8.4.1.9 The CM system shall identify the configuration items that comprise the TSF.ALC_CMC.5.9C

The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.

8.4.1.10 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.

8.4.1.11 ALC_CMC.5.11C

The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.

8.4.1.12 ALC_CMC.5.12C

8.4.1.13 The CM documentation shall include a CM plan.ALC_CMC.5.13C

The CM plan shall describe how the CM system is used for the development of the TOE.

8.4.1.14 ALC_CMC.5.14C

The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

8.4.1.15 ALC_CMC.5.15C

The evidence shall demonstrate that all configuration items are being maintained under the CM system.

8.4.1.16 ALC_CMC.5.16C

The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

8.4.2 ALC_CMS.5

The security assurance requirements of the assurance class "CM scope" listed below are suitable to define a controlled environment for the product development. This includes the documentation of the site security and the procedures for the configuration management. Since the site certification process focuses on the processes based on the absence of a concrete TOE these assurance requirements are considered to be suitable.

8.4.2.1 ALC_CMS.5.1C

The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.

8.4.2.2 ALC_CMS.5.2C

8.4.2.3 The configuration list shall uniquely identify the configuration items.ALC_CMS.5.3C

For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

8.4.3 ALC_DEL

The ALC_DEL procedure is not applicable to this site.

8.4.4 ALC_DVS.2

The security assurance requirements of the assurance class "Development security" listed below are required since a high attack potential is assumed for potential attackers.
The information used at the site during the development of the product can be used by potential attackers for the development of attacks. This information is needed to apply an attack within considerable time and effort.

8.4.4.1 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.

8.4.4.2 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.

8.4.4.3 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.

8.4.5 ALC_LCD.1

The security assurance requirements of the assurance class "Life-cycle definition" listed below are suitable to support the controlled development process and maintenance of already developed products. This includes the documentation of these processes and the procedures for the configuration management. The site supports only the phases development (in the sense of the CC) of the described life cycle. The assurance requirements are considered to be suitable for this site.

8.4.5.1 ALC_LCD.1.1C

The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

8.4.5.2 ALC_LCD.1.2C

The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

8.4.6 ALC_TAT.3

The CC assurance components of family “Tools and Techniques” refer to the tools that are used to during development process. The client’s defines which tools and techniques have to be used by the site. The client provides the complete environment with all necessary tools preinstalled. The proper usage of the provided tools and defined techniques is verified be the client during audits.

8.4.6.1 ALC_TAT.3.1C

Each development tool used for implementation shall be well-defined.

8.4.6.2 ALC_TAT.3.2C

The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

8.4.6.3 ALC_TAT.3.3C

The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

8.5 Security Assurance Requirements

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.

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 including the initialization in its development environment.

O.Alarm-Response

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

O.Internal-Monitor

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 including the initialization in its development environment.

ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE design.

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.

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 and implementation including the initialization in its development 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 design.

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.Logical-Access

ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items.

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 including the initialization in its development environment.

Thereby this objective is suitable 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 and implementation including the initialization in its development environment.

Thereby this objective is suitable 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: The documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.

ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the TOE is generated. Additionally

ALC_CMC.5.15C: The evidence shall 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.

ALC_CMS.5.1C: The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.

ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.

ALC_CMS.5.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

The combination of these Security Assurance Requirements is suitable to meet the objective.

O.Config-Control

ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products.

ALC_CMC.5.2C: The documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.5.3C: The documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.

ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.

ALC_CMC.5.5C and ALC_CMC.5.6C requires that the CM system provides automated measures so that only authorised changes are made to the configuration items.

ALC_CMC.5.6C: The CM system shall support the production of the TOE by automated means.

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.

ALC_CMC.5.8C addresses the identification of the configuration items that comprise the TOE

security functionality (TSF).

ALC_CMC.5.9C requests the evidence by automated means of all changes to the TOE and supports the audit of all changes.

In addition ALC_CMC.5.10C requests the evidence by automated means of all other configuration items affected by a change.

ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the TOE is generated. Additionally ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.

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 product.

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.

ALC_CMS.5.1C: The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.

ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C: The model shall provide for the necessary control over the development and maintenance of the TOE.

The combination of these Security Assurance Requirements is suitable to meet the objective.

O.Organise-Product

ALC_CMC.5.6C: The CM system shall support the production of the TOE by automated means.

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.

ALC_CMC.5.8C addresses the identification of the configuration items that comprise the TOE security functionality (TSF).

ALC_CMC.5.9C requests the evidence by automated means of all changes to the TOE and supports the audit of all changes.

In addition ALC_CMC.5.10C requests the evidence by automated means of all other configuration items affected by a change.

ALC_CMC.5.13C requires that the CM plan describes how the CM system is used for the development (production) of the product.

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_LCD.1.1C: The documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C: The model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_TAT.3.1C: Each development tool used for implementation shall be well-defined.

ALC_TAT.3.2C: The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.3.3C: The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

Thereby the objective fulfils 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.

The objective meets the set of Security Assurance Requirements.

O.Internal-Shipment

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.

ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

ALC_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.

The objective meets the set of Security Assurance Requirements.

O.Transfer-Data

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.

ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

ALC_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.

Thereby this objective is suitable to meet the Security Assurance Requirement.

8.6 Mapping of the Evaluation Documentation

The mapping between the internal site documentation and the Security Assurance Requirements is only available within the full version of the Site Security Target.

9 References

9.1 Literature

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, September 2012

[3] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5, September 2012

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

[5] Site Security Target Template, June 2009, Version 1.0

[6] Minimum Site Security Requirements, December 2017, Version 2.1

[7] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, Eurosmart, 2014, BSI-CC-PP-0084-2014Related documents

[8] Guidance for Site Certification Version 1.1; 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik

9.2 Related documents

[9] Life-cycle Support, ALC_Sii_v 1.6, Version 1.6

[10] Sii Security Trainig, SII-Security-Training_v1.5-HQ, Version 1.5

9.3 Definition

None

9.4 List of Abbreviations

BKC - Best Known Configuration

CRS - Customer Requirement Specifications

CAT - Customer Acceptance Tests

CC – Common Criteria

IC – Integrated Circuit

OSP – Organizational Security Policy

SAR – Security Assurance Requirement

SDD - Software Detailed Design

SUTS - Software Unit Test Specification

SITS - Software Integration Test Specification

STS – Software Test Specification

SRS - Software Requirement Specifications

SE – Software Engineer

SW – Software

SST – Site Security Target

TOE – Target of evaluation