Site Security Target - Toppan Round Rock

Revision	1.6

Table of content

Table of Figures

1. SST Introduction

1 The chapters 1 to 7 of this document is based upon the Eurosmart Site Security Target Template [1] with adaptions such that it fits the site.

1.1 SST Reference

2 Title: Site Security Target - Toppan Round Rock

3 Ref, Version, date: NXPOMS-1719007347-4653, v1.6, 10 Dec 2021

1.2 Site Reference

4 The site belongs to Toppan Photomask Inc. and is located at:

Toppan Round Rock
400 Texas Avenue
Round Rock
TX 78664
United States

1.3 Site Description

The Toppan building specified in Section 1.2 is in the scope of the SST. The surroundings of this building are not in the scope of the SST. Therefore the walls of this building form the physical boundary of the site.

5 The site is not directly involved with any onsite activities of the life cycle phases described into [5] but is supporting Phase 3 activities (IC manufacturing) for sites using this service.

6 The Toppan building supports activities of many other organisations but is described here for **IT support operations** only. Activities are performed through IT room (IT1).

- Global IT administration and infrastructure support through secure remote connections (encrypted VPN) to all Toppan mask shops (incl. AMTC Dresden).

7 This service ensures that for supported sites, the security of the network infrastructure and the IT administration are well protected. Therefore, the confidentiality and integrity of TOE related data handled in those sites are fully covered.

2. Conformance Claim

8 This SST is conformant with Common Criteria Version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017, [2]
- Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 5, April 2017,[3]

9 For the evaluation, the following methodology will be used:

- Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology; Version 3.1, revision 5, April 2017, [4]
- Minimum Site Security Requirements [8]

10 This SST is CC Part 3 conformant.

11 There are no extended components required for this SST for the Toppan Site.

12 The evaluation of the site comprises the following assurance components:

13 ALC_CMC.5, ALC_CMS.5, ALC_DVS.2

14 The assurance level chosen for the SST is compliant to the Security IC Platform Protection Profiles [5] and is therefore suitable for the evaluation of Security ICs.

15 The activities of the site are not directly related to designing, testing, producing, shipping etc. of secure products. Therefore, this site does not claim conformance to ALC_DEL, ALC_TAT and ALC_LCD.

16 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 a high attack potential are assumed. Therefore this site supports product evaluations up to EAL6.

3. Security Problem Definition

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

18 Where necessary the items in this section have been re-worked to fit the site.

3.1 Assets

19 The following section describes the assets handled at the site.

Physical security objects: The site has physical security objects e.g. network and IT equipment. Both the integrity and the confidentiality of these must be protected.

Account with specific rights: The site uses specific accounts which can give access to sensitive network hardware. The confidentiality of these accounts must be protected.

3.2 Threats

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of assets (1) Physical security objects (2) Account with specific rights. 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.

T.Rugged-Theft: An attacker with specialized equipment for burglary, who may be paid to perform the attack, tries to access sensitive areas and manipulate or steal assets (1) Physical security objects (2) Account with specific rights.

T.Computer-Net: A possibly paid hacker with substantial expertise using standard equipment attempts to remotely access sensitive network segments to get access to (1) physical security objects (2) Account with specific rights with the intention to violate confidentiality and possibly integrity.

T.Accident-Change: An employee, contractor or student trainee may remove security features to (1) physical security objects by accident.

T.Unauthorised-Staff: Employees or subcontractors not authorized to get access to assets by violating (1) Physical security objects (2) Account with specific rights.

T.Staff-Collusion: An attacker tries to get access to assets by getting support from one employee through extortion or bribery. In this case electronic access with the intention to violate confidentiality and possibly integrity (1) Physical security objects (2) Account with specific rights.

3.3 Organizational Security Policies

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

P.Config-Items: The configuration management system shall be able to uniquely identify configuration items. This includes in this case the unique identification of items that are used at the site.

P.Config-Control: Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes.

P.Config-Process: The services and/or processes provided by the site are controlled and documented. This comprises the documentation that describes the services and/or processes provided by the site.

21 The documentation with the process descriptions and the security measures of the site are under version control. Measures are in place to ensure that the evaluated status is ensured. Tools are used to support the processes at the site. This comprises a commercial data base system.

P.Transfer-Data: Line used for administration of the supported IT equipment client is using encryption to ensure confidentiality and integrity of the manipulations.

3.4 Assumptions

A.network_Available: In order to perform the IT administration of remote IT equipment; the equipement must be switched on.

22 The assumptions are outside the sphere of influence of SST Toppan Round Rock.

4. Security Objectives

23 The Security Objectives are related to physical, technical, and organizational security measures, the configuration management.

24 O.Physical-Access: 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 unauthorised people. The access control measures ensure that only registered employees can access restricted areas. Assets are handled in restricted areas only.

25 O.Security-Control: Assigned personnel of the site operate the systems for access control. Out of hour surveillance and respond to alarms is contracted to a 3rd party security company. Technical security measures like motion sensors and similar kind of sensors support the enforcement of the access control. Toppan personnel are also responsible for registering and ensuring escort of visitors, contractors and suppliers.

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

27 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 audit is performed every year to control the application of the security measures.

28 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 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.

29 O.Logical-Access: The site enforces a logical separation between the internal network and the internet including a firewall. The security measures ensure that only defined services and defined connections are accepted on the internal network. The internal network is appropriately separated to prevent interference between the different environments (office, development and production environments). Additional specific networks for

production and configuration are physically separated from any internal network to enforce access control. Access to the production network and associated systems is restricted to authorized employees working in the related area or involved in the configuration tasks of the production systems. Every user of an IT system has his/her own user account and password.

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

31 O.Config-Items: Toppan has a configuration management system that assigns a unique internal of internal procedures and guidance are covered by the configuration management.

32 O.Config-Control: The services and/or processes can be changed by authorised personnel only. Automated systems support configuration management and production control.

33 O.Config-Process: The site controls its services and/or processes using a configuration management plan. The configuration management is controlled by tools and procedures for the documentation that describes the services and/or processes provided by a site.

34 O.Staff-Engagement: 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. All contractors and visitors must be escorted by a trained employee at all times.

O.Transfer-Data: The site uses encryption to perform remote administration of IT equipment.

4.1 Security Objectives Rationale

35 The SST includes a Security Objective Rationale with two parts. The first part includes the tracing which shows how the threats and OSPs are covered by the Security Objectives. The second part includes a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives (see column “Rationale” of table 1)

Threat and OSP	Security Objective(s)	Rationale
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	O.Physical-Access ensures that the Secure Room is physically partitioned off, so that a burglar cannot just walk in. O.Security-Control ensures that an attacker will be detected when trying to reach the assets through the Secure Room 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 O.Internal-Monitor O.Maintain-Security	O.Physical-Access ensures that the Secure Areas are physically partitioned off, so that a burglar cannot just walk in. O.Security-Control ensures that an attacker will be detected when trying to reach the assets through the Secure Room 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.Logical-Operation O.Logical-Access O.Internal-Monitor O.Maintain-Security O.Staff-Engagement	O.Logical-Operation ensures that all computer systems used to manage the network are kept up to date minimizing IT weaknesses. O.Logical-Access ensures protection of the production environment from the external. O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). Together, these objectives will therefore counter T.Computer-Net.
T.Accident-Change	O.Logical-Access O.Staff-Engagement O.Config-Items O.Config-Control O.Config-Process	O.Logical-Access ensures protection of the production environment from the external O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Config-Items ensures that all procedures have their own identifier. O.Config-Control and O.Config-Process ensure that only authorized people are able to change process.

T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Logical-Access O.Config-Control O.Config-Process	O.Security-Control ensures that all unauthorized people who have a legitimate need to visit the Secure Areas are always accompanied. O.Physical-Access, O.Security-Control and O.Alarm-Response ensures that the unauthorized people cannot circumvent this O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Logical-Access ensures protection of the production environment due to user account and password. O.Config-Control and O.Config-Process ensure that only authorized people are able to change process. Together, these objectives will therefore counter T.Unauthorised-Staff.
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement	O.Internal-Monitor and O.Maintain-Security ensure that physical accesses is well managed and maintained. O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). Together, these objectives will therefore counter T.Staff-Collusion.
P.Config-Items	O.Config-Items	The Security Objectives enforce the OSP. O.Config-Items ensures that all procedures have their own identifier. These objectives are sufficient to meet P.Config-Items.
P.Config-Control	O.Config-Items O.Config-Control O.Config-Process O.Logical-Access	The Security Objectives enforce the OSP. O.Config-Items ensures that all procedures have their own identifier. O.Config-Control and O.Config-Process ensure that only authorized people are able to change process. O.Logical-Access ensures protection of the production environment due to user account and password. These objectives are sufficient to meet P.Config-Control.

P.Config-Process	O.Config-Process O.Logical-Access	O.Config-Process ensures that documentation is under configuration management. O.Logical-Access ensures protection of the IT environment due to user account and password. These objectives are sufficient to meet P.Config-Process.
P.Transfer-Data	O.Transfer-Data	O.Transfer-Data ensures that the site uses encrypted lines to ensure confidentiality and integrity. This objective is sufficient to meet P.Transfer-Data

Table 1 Threats and OSP - Security Objectives Rationale

5. Extended Assurance Components Definition

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

6. Security Assurance Requirements

37 Toppan using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Eurosmart Protection Profiles [5].

38 The Security Assurance Requirements are chosen from the class ALC (Life-cycle support) as defined in [3]:

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

39 The Security Assurance Requirements listed above fulfill the requirements of [6] because hierarchically higher components than the defined minimum site requirements (ALC_CMC.3, ALC_CMS.3, ALC_DVS.1, see section 3.2.3 of [6]) are used in this Site Security Target.

6.1 Application Notes and Refinements

40 The description of the site certification process [6] includes specific application notes. The main item is that a product that is considered as intended TOE is not available during the evaluation. Since the term “TOE” is not applicable in the Site Security Target, the associated processes for the handling of products, or “intended TOEs” are in the scope of this Site Security Target and are described in this document. These processes are subject of the evaluation of the site.

6.1.1 CM Capabilities (ALC_CMC.5)

41 According to [6] the processes rather than a TOE are in the focus of the CMC examination.

42 The configuration items are listed in section 3.1. and in ALC_CMS.5. The CM documentation of the site must be able to maintain the items listed for the relevant life-cycle step and the CM system must be able to track the configuration items.

43 A CM system has to be employed to guarantee the traceability and completeness of the different configuration items. Appropriate administration procedures have to be provided in order to maintain the integrity and confidentiality of the configuration items.

44 For further details refer to subsection ‘Application Notes for Site Certification’ in [6] 5.1 ‘Application Notes for ALC_CMC’.

6.1.2 CM Scope (ALC_CMS.5)

45 Refer to subsection ‘Application Notes for Site Certification’ in [6] 5.2 ‘Application Notes for ALC_CMS’.

46 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 processed and produced at the site.

6.1.3 Development Security (ALC_DVS.2)

47 Refer to subsection ‘Application Notes for Site Certification’ in [6] 5.4 ‘Application Notes for ALC_DVS’.

48 If the transfer of configuration items between two site involved in the production flow is included in the scope of the evaluation (life-cycle covered by the product evaluation) this is considered as internal shipment. In general, the security requirements for confidentiality and integrity are the same but it must clearly distinguished to ensure the correct subject of the evaluation.

49 As ALC_DVS is relatively broad, and the security objectives are more specific, the following refinements are applied to ensure that ALC_DVS.2 will meet the objectives:

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

- **Assigned personnel of the site operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, unauthorized Toppan employees, contractors and suppliers.**

- **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 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 every year 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 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.**

- **The computer systems for production are kept up-to-date (software updates, security patches, virus protection, spyware protection).**

- **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.**

6.2 Security Requirements Rationale

6.2.1 Security Requirements Rationale - Dependencies

50 The dependencies for the assurance requirements are as follows (see [3], appendix C):

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

51 Some of the dependencies are not fulfilled:

- ALC_LCD.1 is not included as the site is not related to development.

52 Refinements introduced into the SAR are in *italic*.

6.2.2 Security Requirements Rationale – Mapping

SAR	Security Objective	Rationale	Reference
ALC_CMC.5.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labeling*.	O.Config-Items	Appropriate and consistent labelling and use of the site configuration management systems (O.Config-Items).	[7_2] [7_8]
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Config-Items O.Config-Control O.Config-Process	Labeling is mapped to the internal identification as defined by O.Config-Items. O.Config-Control ensures that handling of each item is released based on a defined process. The	[7_3] [7_4] [7_5] [7_6] [7_8]

		configurations can only be done by authorized person. O.Config-Process provides a configured and controlled process.	
ALC_CMC.5.3C: The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.	O.Config-Items O.Config-Process	Labeling is mapped to the internal identification as defined by O.Config-Items. O.Config-Process provides a configured and controlled process..	[7_3] [7_4] [7_8]
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	O.Config-Items	O.Config-Items includes the internal unique identification of all items..	[7_3] [7_6] [7_8]
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config-Items O.Config-Control O.Config-Process	Labeling is mapped to the internal identification as defined by O.Config-Items. O.Config-Control ensures that handling of each item is released based on a defined process. The configurations can only be done by authorized person. O.Config-Process provides a configured and controlled process.	[7_3] [7_8]
ALC_CMC.5.6C: The CM system shall support the production of the *intended* TOE by automated means.	O.Config-Items O.Config-Process	Labeling is mapped to the internal identification as defined by O.Config-Items. O.Config-Process provides a configured and controlled process.	[7_3] [7_8]
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-Items O.Config-Process	Labeling is mapped to the internal identification as defined by O.Config-Items. O.Config-Process provides a configured and controlled process.	[7_3] [7_8]
ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the TSF.	O.Config-Items	Labeling is mapped to the internal identification as defined by O.Config-Items. that comprise the TSF.	[7_3] [7_8]

ALC_CMC.5.9C: The CM system shall support the audit of all changes to the *intended* TOE by automated means, including the originator, date, and time in the audit trail.	O.Config-Items O.Config-Process	Labeling is mapped to the internal identification as defined by O.Config-Items. O.Config-Process provides a configured and controlled process.	[7_3] [7_8]
ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O.Config-Items O.Config-Process	Labeling is mapped to the internal identification as defined by O.Config-Items. O.Config-Process provides a configured and controlled process.	[7_3] [7_8]
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the *intended* TOE is generated.	O.Config-Items	Labeling is mapped to the internal identification as defined by O.Config-Items	[7_3] [7_8]
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.Config-Process	O.Config-Process ensures the reliability of the processes and tools based on dedicated CM plans.	[7_3] [7_8]
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the *intended* TOE.	O.Config-Process	O.Config-Process describes how documentation are built by the site.	[7_3] [7_8]
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of an *intended* TOE.	O.Config-Process	O.Config-Process ensures the automated control of released items.	[7_3] [7_8]
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are	O.Config-Process	The objectives O.Config-Process ensure that all procedures, documentations are processed under the configuration system.	[7_3] [7_8]

being maintained under the CM system.			
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.Config-Process	The objectives O.Config-Process ensure that all procedures, documentations are processed under the configuration system.	[7_3] [7_8]

Table 2 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale	Reference
ALC_CMS.5.1C: The configuration list includes the following: *clear instructions how to consider these items in the list*; the evaluation evidence required by the SARs *of the life cycle*; *development and production tools* and security flaw reports and resolution status.	O.Config-Items O.Config-Process	O.Config-Items ensure unique part IDs including a list of all items O.Config-Process ensure that all procedures, documentations are processed under the configuration system.	[7_8] [9]
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.Config-Items O.Config-Process	Items and processes are uniquely identified by the data base system according to O.Config-Items. Unique identification is supported by automated tools according to O.Config-Process.	[7_8] [9]
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer of the item.	O.Config-Items	The CI-List (O.Config-Items) indicates the developer for each configuration items (Toppan).	[7_8] [9]

Table 3 Rationale for ALC_CMS.5

SAR	Security Objective	Rationale	Reference
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural,	O.Physical-Access O.Security-Control	The development security documentation describes the physical (O.Physical-Access, O.Security-Control, O.Alarm-Response), procedural (O.Internal-	[7_1] [7_2] [7_4] [7_6]

SAR	Security Objective	Rationale	Reference
personnel, and other security measures that are necessary to protect the confidentiality and integrity of the *intended* TOE design and implementation in its development environment.	O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Logical-Access O.Logical-Operation O.Transfer-Data	Monitor, O.Maintain-Security), personnel (O.Staff-Engagement), and logicaly (O.Logical-Operation, O.Logical-Access, O.Transfer-Data) 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 *intended* TOE.	O.Internal-Monitor O.Logical-Operation O.Maintain-Security	The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. The associated control and continuous justification is subject of the objectives O.Internal-Monitor, O.Logical-Operation and O.Maintain-Security.	[7_1] [7_2] [7_4] [7_6]

Table 4 Rationale for ALC_DVS.2

7. Site Summary Specification

7.1 Preconditions required by the Site

53 This section provides background information on the assumptions defined in chapter 3.4

54 The sites using this service must provide appropriate information as mentionned in chapter 1.3.

Assumption	How the assumption is met with this site
A.network_Available	The remote equipment must be swithed on

55 Applicable policies and processes are documented and available.

7.2 Services of the Site

56 The site provides services to external sites and especially

- to provide Global IT adminsitration and infrastructure support through secure remote connections (encrypted VPN) to all Toppan mask shops (including AMTC Dresden).

7.3 Security Assurance Rationale

7.3.1 CM capabilities (ALC_CMC.5)

57 Configuration Management is described in [6].

58 For full detail and evidences please view Section 6.2.2

7.3.2 CM scope (ALC_CMS.5)

59 Configuration Management is described in [6].

60 For full detail and evidences please view Section 6.2.2

7.3.3 Development Security (ALC_DVS.2)

61 Development Security is described in [6].

62 For full detail and evidences please view Section 6.2.2

7.4 Obejctives Rationale

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

64 O.Physical-Access: The site implements a “need to know” principle by separation measures using a combination of physical partitioning together with technical and organisational

security measures. The access control measures support the enforcement of the separation and the “need to know” principle. The handling of assets is restricted to separates security areas. By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

65 O.Security-Control: The site is using dedicated personnel for guard services. This personnel is responsible for operation of the access control systems, for the enforcement of the access control, for the surveillance of the technical alarm sensors and the responses to incidents and for the escort of visitors. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff.

66 O.Alarm-Response: In case of an access attempt to an asset by an unauthorized person the site has an alarm system in place. After the alarm is triggered the unauthorised person still has to overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff.

67 O.Internal-Monitor: The established physical and logical security measures of the site are regularly reviewed by security management meetings and internal audits. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.

68 O.Maintain-Security: Technical security measures are maintained regularly. This ensures that the systems are working correctly and are configured as required to ensure the protection of the networks and computer systems. Hence, this helps to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.

69 O.Logical-Access: The used workstations for IT administration purposes are using authentication measures for the users of these systems. Hence the threats T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff is prevented and the OSP P.Config-Control and P.Config-Process addressed.

70 O.Logical-Operation: The network used at the site is connected only to dedicated trustworthy systems. All network segments are separated and the computer systems are kept up-to-date. This prevents the threats T.Computer-Net.

71 O.Config-Items: All documents are labelled with a unique number. This prevents the threat T.Accident-Change and directly addresses the OSP P.Config-Items as well as the OSP P.Config-Control.

72 O.Config-Control: The site applies a release procedure for the setup of documentation. In addition, the site has a process to classify and introduce changes for documentation. The services and/or processes can be changed by authorised personnel only. By the combination of these measures the threat T.Accident-Change and T.Unauthorised-Staff can be prevented and directly addresses the OSP P.Config-Control.

73 O.Config-Process: The site controls its services and/or processes using a configuration management plan. This T.Accident-Change, T.Unauthorised-Staff and the OSPs P.Config-Process, P.Config-Control.

74 O.Staff-Engagement: The site has established personnel security measures: 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. This helps to prevent the threats T.Unauthorised-Staff, T.Staff-Collusion, T.Accident-Change and T.Computer-Net.

75 O.Transfer-Data: During transport of logical assets, protection against disclosure and modification is ensured by cryptographic means which are appropriate to resist against high attack potential. Cryptographic keys and passwords are protected against unauthorised access. The OSP P.Transfer-Data is addressed.

7.4.1 Security Objectives and security requirements

76 The following section provides a rationale for each security objective for the development environment (as defined in chapter 4), why each of the assigned SARs (as given in section 7.3 is suitable to meet the security objective.

77 The justification is given at the level of SAR content elements (see Table 1 to Table 6).

7.4.2 O.Physical-Access

78 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.4.3 O.Security-Control

79 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.4.4 O.Alarm-Response

80 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.4.5 O.Internal-Monitor

81 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. ALC_DVS.2.2C require the development security documentation to justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby these SARs are suitable to meet the security objective.

7.4.6 O.Maintain-Security

82 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. ALC_DVS.2.2C require the development security documentation to justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby these SARs are suitable to meet the security objective.

7.4.7 O.Logical-Access

83 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.4.8 O.Logical-Operation

84 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. ALC_DVS.2.2C require the development security documentation to justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby these SARs are suitable to meet the security objective.

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

7.4.9 O.Config-Items

86 ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products. ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configura tion items. ALC_CMC.5.3C requires the CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items. ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system. ALC_CMC.5.5C requires the CM system to provide automated measures such that only authorised changes are made to the configuration items. ALC_CMC.5.6C requires the CM system to support the production of the intended TOE by automated means. ALC_CMC.5.7C requires the CM system to ensure that the person responsible for accepting a configuration item into CM is not the person who developed it. ALC_CMC.5.8C requires the CM system to identify the configuration items that comprise the TSF. ALC_CMC.5.9C requires the CM system to support the audit of all changes to the intended TOE by automated means, includng the originator, date, and time in the audit trail. ALC_CMC.5.10C requires the CM system to provide an automated means to identify all other configuration items that are affected by the change of a given configuration item. ALC_CMC.5.11C requires the CM system to be able to identify the version of the implementation representation from which the product is generated.

87 ALC_CMS.5.1C requires that the configuration list shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_CMS.5.3C requires for each

TSF relevant configuration item, that the configuration list indicated the developer of the item.

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

7.4.10 O.Config-Control

89 ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.5C requires the CM system to provide automated measures such that only authorised changes are made to the configuration items. .

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

7.4.11 O.Config-Process

91 ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires requires the CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items. ALC_CMC.5.5C requires the CM system to provide automated measures such that only authorised changes are made to the configuration items. ALC_CMC.5.6C requires the CM system to support the production of the product by automated means. ALC_CMC.5.7C requires the CM system to ensure that the person responsible for accepting a configuration item into CM is not the person who developed it. ALC_CMC.5.9C requires the CM system to support the audit of all changes to the intended TOE by automated means, includng the originator, date, and time in the audit trail. ALC_CMC.5.10C requires the CM system to provide an automated means to identify all other configuration items that are affected by the change of a given configuration item. ALC_CMC.5.12C requires the CM documentation to include a CM plan. ALC_CMC.5.13C requires the CM plan to describe how the CM system is used for the development of the product. ALC_CMC.5.14C requires the CM plan to describe the procedures used to accept modified or newly created configuration items as part of the product. ALC_CMC.5.15C requires evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMC.5.16C requires the evidence to demonstrate that the CM system is being operated in accordance with the CM plan.

92 ALC_CMS.5.1C requires that the configuration list shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C requires that the configuration list shall uniquely indetify the configurantion items.

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

7.4.12 O.Staff-Engagement

94 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.4.13 O.Transfer-Data

95 ALC_DVS.2.1C ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are

necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

8. References

8.1 Literature

[1] „Site Security Target Template, Version 1.0, published by Eurosmart,“ Eurosmart, 21.06.2009.

[2] Common Criteria, „Common Criteria for Information Technology Security Evaluations, Part 1: Introduction and General Model; Version 3.1, Revision 5,“ April 2017.

[3] Common Criteria, „Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 5,“ April 2017.

[4] Common Criteria, „Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5,“ April 2017.

[5] „Security IC Platform Protection Profile with Augmentation Packages Version 1.0 (BSI-PP-0084),“ Eurosmart, 13.01.2014

[6] Common Criteria, “Supporting Document, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001,” October 2007.

[7_1] GLIS-2850_ISO 27001_ISManualForEmployee

[7_2] GLIT-2408_IT EmployeeManual.

[7_3] GLQA-6029_QualityManagementSystemManual

[7_4] GLIT-2409_InformationTechnology

[7_5] GLQA-7580_ChangeControlManual

[7_6] RRIS-4600_RR_SITE_INF_SECURITY_INSTRUCTIONS

[7_7] GLQA-2410 - Global Internal Audit Manual

[7_8] GLQA-2402 - Global Document Control Manual

[8] Minimum Site Security Requirements v3.0 Feb 2020

[9] Toppan Round Rock Configuration List v2.0

8.2 Definitions

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

Production Process — “Production Process” here refers to the processes and flows that are set up for internal shipment and external delivery (forwarding or storing and shipping of items).

8.3 List of Abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
IC	Integrated Circuit
IP	Intellectual Property
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SST	Site Security Target
ST	Security Target
TOE	Target of Evaluation

8.4 Revision History

Revision	Description	Author	Approval - Date
1.1	Site security target aligned with SST v 2.2	Christophe Bouly	06/26/2019
1.2	Site security target aligned with SST v 2.3	Christophe Bouly	07/09/2019
1.3 (Not released)	New reference, version to align with NXP policy (only PUBLIC version) and deletion of production service with associated SST elements.	Christophe Bouly	10/01/2021
1.4	Updates related to evaluator comments (chapters 1.2, 3.2, 6.1.1, 6.2.2, 7.1, 7.2, 7.4.1, 7.4.13, 8, 8.4)	Christophe Bouly	10/21/2021
1.5	Changed content chapters 1.1, 1.3, 8.1, 8.4	Christophe Bouly	10/25/2021
1.6	Improvement regarding logical service wording chap 1.3	Christophe Bouly	12/10/2021