Table of contents

Publication Summary

Reference Number (NXPOMS-ID)	NXPOMS-1719007347-2661
Reference Title	Site Security Target Lite – GlobalLogic, Slovakia, Zilina
Publisher	Business Unit Security & Connectivity
Classification	PUBLIC
Author	Lubos Kocvara
Owner	Lubos Kocvara
Archive Numbers	See reference number

1. Objectives / Purpose

See chapter 4.0.

2. Scope

This document is applicable to the following organisation(s): BU Security and Connectivity

3. Document Introduction

3.1 Reference

Title:	Site Security Target Lite – GlobalLogic, Slovakia, Zilina
Date:	See history
Company:	GlobalLogic s.r.o.
Name of site:	GlobaLlogic Zilina
EAL:	SARs taken from EAL6

4. SST Introduction

1 This document is based upon the Eurosmart Site Security Target Template [1] with adaptions such that it fits the site (i.e. development site, no production, no direct delivery to customers of the user of the site).

4.1 SST Reference

2 Title Site Security Target Lite – GlobalLogic, Slovakia, Zilina

3 Date See history

4.2 Site Reference

4 The site belongs to GlobalLogic and is located at:

5 GlobalLogic, s.r.o.

6 Antona Bernoláka 334/72

7 010 01 Žilina

8 Slovakia

4.3 Site Description

9 The site is inside 4 floors building where 2 top floor are occupied by Globallogic only. The entire site is in-scope for this SST.

10 The activities (and areas where they are performed) are:

Activity	Area
Development and testing* of software for secure integrated circuits.	217, 218, 219, 220, 221, 221a, 223

* Through simulation or remotely on physical objects at another site.

11 The site is used by NXP Business Unit Security & Connectivity (BUS&C) to participate in the development and testing of software[1] for secure IC hardware products. To perform its activities the site uses the NXP provided remote IT-infrastructure and local IT equipment (workstations, router) and works according to BUS&C processes.

[1] Software means in this case: IC Embedded Software Development (Phase 1) and/or IC Dedicated Software Development (Phase 2) as defined in 'Security IC Platform Protection Profile' (PP-0035) and 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084)

12 The site provides a secure physical environment for HS & RS IT infrastructure and equipment meeting A-Inherit-secure-IT.

5. Conformance Claim

13 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 Requirements; Version 3.1, 5, April 2017, [3]

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

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

15 This SST is CC Part 3 conformant.

16 The evaluation of the site comprises the following assurance components[2]:

17 ALC_CMC.5, ALC_CMS.5, ALC_DVS.2 (at AVA_VAN.5 level), ALC_LCD.1, and ALC_TAT.3.

18 The assurance level chosen for the SST is compliant to the Security IC Platform Protection Profile [5] and is therefore suitable for the evaluation of (software for) Security ICs.

19 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 potentially augmented product evaluations up to EAL6.

[2] The activities of the site are not directly related to production and shipping of secure products. Therefore this site does not claim conformance to ALC_DEL.

6. Security Problem Definition

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

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

6.1 Assets

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

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.

Development computers: 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.

Physical security objects: The site has physical security objects (samples, printed documents, etc) in relation to developed TOEs. Both the integrity and the confidentiality of these must be protected.

6.2 Threats

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of assets. 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 specialised equipment for burglary, who may be paid to perform the attack, tries to access sensitive areas and manipulate or steal assets.

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) development data with the intention to violate confidentiality and possibly integrity or (2) development computers with the intention to modify the development process.

T.Unauthorised-Staff: Employees or subcontractors not authorised to get access to assets get access to assets violating the confidentiality and possibly the integrity of products.

T.Staff-Collusion: An attacker tries to get access to assets by getting support from one employee through extortion or bribery.

T.Attack-Transport: An attacker tries to get access to shipped physical security objects when shipped in or out of the site with the intention to compromise confidentiality and/or integrity of the product design data, customer and/or consumer data like code and data (including personalisation data and/or keys) stored in the ROM and/or EEPROM or classified product documentation.

6.3 Organizational Security Policies

P.Config_IT-env: The site uses software on development workstations and servers in addition to configuration management systems for file versioning and problem tracking. For file versioning unique repositories shall be used to support proper management of multiple products and the site internal procedures.

P.LifeCycle-Doc: The site uses life cycle documentation that describes: (1) Description of configuration management systems and their usage; (2) A configuration items list; (3) Site security; (4) The development process; (5) The development tools.

P.Config_Activities: The activities of the site shall be performed in accordance with the life cycle documentation (P.Config_IT-env) using the IT-environment (P.LifeCycle-Doc).

6.4 Assumptions

A.Inherit-secure-IT: The local IT equipment (e.g. workstations) is connected to a secure remote IT-Infrastructure through a secure (encrypted) network connection. The local workstations, the remote secure IT-infrastructure and the secure connection to it satisfy all relevant ALC requirements and are provided and managed by the client. The workstations are configured such that any assets are contained within encrypted containers.

A.Shared-Docs: In case of necessary updates to the life cycle documentation[3] the site and the client cooperate.

A.Setup-Projects: To enable that the site participates in the development of products the client provides services to setup the necessary development computers (tools, user accounts, etc.) and configuration management systems (user accounts, repositories etc.).

A.Shipment: To enable the site to realize shipment such that assurance of integrity is assured throughout transport of physical security objects the client will adhere to the shipment method as described in the life cycle documentation.

[3] Part of the life cycle documentation is written in corporation with the client where other parts are provided by the client.

A.Product-Setup: The site participates in the development of products. To define the participation of the site in the development while maintaining quality, for each product the site and the client agree on the activities to be performed by the site, the specifications of the input for the site and the acceptance of the results by the client.

7. Security Objectives

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

O.Config_IT-env: The site uses software on development workstations and servers in addition to configuration management systems for file versioning and problem tracking. For file versioning unique repositories are used to support proper management of multiple products and the site internal procedures.

O.LifeCycle-Doc: The site uses life cycle documentation that describes: (1) Description of configuration management systems and their usage; (2) A configuration items list; (3) Site security; (4) The development process; (5) The development tools.

O.Config_Activities: The activities of the site are performed in accordance with the life cycle documentation (O.Config_IT-env) using the IT-environment (O.LifeCycle-Doc).

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.

O.Security-Control: Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like 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, contractors and suppliers.

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.

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.

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.

O.Network-separation: The (plain-text) development network of the site exists within the secured areas of the site only. It is connected only to: (1) The encryption equipment employs encrypted VPNs to the secure network provided by the client; (2) the development workstations provided by the client; (3) Additional equipment (e.g. a printer) approved by the client.

O.Logical-Operation: Development computers enforce that every user authenticates using a password and has a unique user ID.

O.Control-Shipment: The site has measures in place to provide assurance of integrity throughout transport of physical security objects.

O.Control-Scrap: The site has measures in place to either securely destruct assets (e.g. paper shredder) or return them to the client.

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.

7.1 Security Objectives Rationale

Threat	Security Objective(s)	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 organizational measures detects unauthorized access and allows for appropriate response on the threat.
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat.
T.Computer-Net	O.Network-separation	The development network is not connected to anything that an attacker could use to set up a remote connection.

T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Operation O.Staff-Engagement O.Control-Scrap	Physical and logical access control prohibits access to assets. Secure destruction of scrap limits the amount of assets
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Control-Scrap	The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees limits unauthorized access to assets.
T.Attack-Transport	O.Control-Shipment O.LifeCycle-Doc	The shipment method and the organizational measures ensure that integrity changes of shipped objects are detected and appropriately responded upon.

Table 1 Threats - Security Objectives Rationale

OSP	Security Objective(s)	Rationale
P.Config_IT-env	O.Config_IT-env	The Security Objective directly enforces the OSP.
P.LifeCycle-Doc	O.LifeCycle-Doc	The Security Objective directly enforces the OSP.
P.Config_Activities	O.Config_Activities	The Security Objective directly enforces the OSP.

Table 2 OSP - Security Objectives Rationale

8. Extended Assurance Components Definition

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

9. Security Assurance Requirements

25 Clients using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL6+, potentially claiming conformance with the Eurosmart Protection Profile [5].

26 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)
- Life-cycle definition (ALC_LCD.1)
- Tools and techniques (ALC_TAT.3)

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

- [6] 3.2.3 ‘Minimum Site Requirements’
- [5] Eurosmart Protection Profile.

28 In addition, the minimum set of SAR as defined in [6] 3.2.3 ‘Minimum Site Requirements’ is augmented by assurance components from ‘Life-cycle definition’ (ALC_LCD.1) and ‘Tools and techniques’ (ALC_TAT.3).

9.1 Application Notes and Refinements

29 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.

9.1.1 CM Capabilities (ALC_CMC.5)

30 Refer to subsection ‘Application Notes for Site Certification’ in [6] 5.1 ‘Application Notes for ALC_CMC’.

9.1.2 CM Scope (ALC_CMS.5)

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

9.1.3 Development Security (ALC_DVS.2)

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

9.1.4 Life-cycle Definition (ALC_LCD.1)

33 Refer to subsection 'Application Notes for Site Certification' in [6] 5.6 'Application Notes for ALC_LCD'.

34 Refer to '*Application Note 26*' in 6.2.1.2 'Refinements regarding Development Security (ALC_DVS)' in the Eurosmart PP [5].

35 Refer to subsection *'Refinement'* in 6.2.1.2 'Refinements regarding Development Security (ALC_DVS)' in the Eurosmart PP [5].

9.1.5 Tools and Techniques (ALC_TAT.3)

36 Refer to subsection 'Application Notes for Site Certification' in [6] 5.7 'Application Notes for ALC_TAT'.

9.2 Security Requirements Rationale

9.2.1 Security Requirements Rationale - Dependencies

37 The dependencies for the assurance requirements are as follows:

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

38 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 [6] 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 [6] 5.7 'Application Notes for ALC_TAT'.

-

9.2.2 Security Requirements Rationale – Mapping

SAR	Security Objective	Rationale
ALC_CMC.5.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labeling.	O.Config_IT-env O.LifeCycle-Doc O.Config_Activities	Appropriate and consistent labelling is ensured through the application (O.Config_Activities) of the CM-Plan (O.LifeCycle-Doc) and the use of the configuration management systems (O.Config_IT-env).
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.LifeCycle-Doc	The method used to uniquely identify the configuration items is described in the CM-Plan (O.LifeCycle-Doc).
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.LifeCycle-Doc	The adequate and appropriate acceptance procedures for configuration items are described in the CM-Plan (O.LifeCycle-Doc).
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	O.Config_IT-env O.LifeCycle-Doc O.Config_Activities	Unique identification of all CIs is realized by performing the CM activities (O.Config_Activities) in accordance with the CM-Plan (O.LifeCycle-Doc) using the Configuration management systems (C.Config_IT-env)
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config_IT-env O.LifeCycle-Doc O.Config_Activities	The configuration management systems (O.Config_IT-Env) used (O.Config_Activities) according to the CM-Plan (C.Config_CM-Plan) enforces automated measures such that only authorized changes are made to the configuration items

SAR	Security Objective	Rationale
ALC_CMC.5.6C: The CM system shall support the production of the product by automated means.	O.Config_IT-env O.LifeCycle-Doc O.Config_Activities	The software on the development computers (O.Config_IT-env) supports automated production of products when used (O.Config_Activities) in accordance with the CM-Plan (O.LifeCycle-Doc)
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.LifeCycle-Doc O.Config_Activities	As described in the CM-Plan (O.LifeCycle-Doc) the activities performed (O.Config_Activities) are such that the person responsible for accepting a configuration item into CM is not the person who developed it.
ALC_CMC.5.8C: The CM system shall clearly identify the configuration items that comprise the TSF.	O.Config_IT-env O.LifeCycle-Doc	The CM-Plan (O.LifeCycle-Doc) identifies the configuration items that comprise the TSF possibly supported by the configuration management system (O.Config_IT-env)
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_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configuration management systems (O.Config_IT-env) are configured such that an audit trail (showing originator, date and time) is automatically generated.
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_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configurations management system and software installed on the development workstations and servers (O.Config_IT-env) provide automated means to identify all other configuration items that are affected by the change of a given configuration item.

SAR	Security Objective	Rationale
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_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configurations management system (O.Config_IT-env) identifies the version of the implementation representation from which the TOE is generated through baselines.
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) includes a CM-Plan.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the TOE.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) describes how the CM system is used for the development of the product.
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.LifeCycle-Doc	The acceptance procedures for modified or newly created configuration items are described in the CM-Plan (O.LifeCycle-Doc).
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.LifeCycle-Doc	All configuration items are listed in the CI-list (O.LifeCycle-Doc)
ALC_CMC.5.16C: The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.	O.Config_IT-env O.LifeCycle-Doc	The CI-list (O.LifeCycle-Doc) is generated from the configuration management systems (O.Config_IT-env)

Table 3 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
ALC_CMS.5.1C: The configuration list includes the following: the TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the TOE; the implementation representation; security flaws; and development tools and related information. The CM documentationshall include a CM plan.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) includes a CM-Plan and a CI-List with the items required by ALC_CMS.5.1C
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.LifeCycle-Doc	The CI-List (O.LifeCycle-Doc) uniquely identifies the configurations items as described in the CM-Plan (O.LifeCycle-Doc).
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.	O.LifeCycle-Doc	The CI-List (O.LifeCycle-Doc) indicates the developer/subcontractor for each configuration items as described in the CM-Plan (O.LifeCycle-Doc).

Table 4 Rationale for ALC_CMS.5

SAR	Security Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	O.LifeCycle-Doc O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Network-separation O.Logical-Operation O.Control-Shipment O.Control-Scrap	The development security documentation (O.LifeCycle-Doc) describes the physical (O.Physical-Access, O.Security-Control, O.Alarm-Response), procedural (O.Internal-Monitor, O.Maintain-Security, O.Control-Shipment, O.Control-Scrap), personnel (O.Staff-Engagement), and other(O.Network-separation, O.Logical-Operation,) security measures that are necessary to protect the

SAR	Security Objective	Rationale
	O.Staff-Engagement	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.	O.LifeCycle-Doc	The development security documentation (O.LifeCycle-Doc) justifies the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

Table 5 Rationale for ALC_DVS.2

SAR	Security Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.	O.LifeCycle-Doc	The model used to develop the TOE is described in the life cycle documentation (O.LifeCycle-Doc)
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	O.LifeCycle-Doc	The life cycle model as described in the life cycle documentation (O.LifeCycle-Doc) provides for the necessary control over the development and maintenance of the TOE.

Table 6 Rationale for ALC_LCD.1

SAR	Security Objective	Rationale
ALC_TAT.3.1C: Each development tool used for implementation shall be well-defined.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) shows that the development tools used for implementation are well-defined.
ALC_TAT.3.2.C: The documentation of each development tool shall unambiguously define the meaning of all	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) together with the documentation of the development tools

SAR	Security Objective	Rationale
statements as well as all conventions and directives used in the implementation.		unambiguously defines 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.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) together with the documentation of the development tools unambiguously defines the meaning of all implementation-dependent options.

Table 7 Rationale for ALC_TAT.3

10. Site Summary Specification

10.1 Preconditions required by the Site

39 The site activities are performed using an IT infrastructure consisting of development workstations, servers and configuration management systems. All of these are provided, configured and maintained by the client.

40 The IT infrastructure consists of local and remote equipment connected using an encrypted connection. The client provides, configures and maintains the local workstations and router (used for the encrypted connection) and all remote equipment such that they are secure. The workstations are configured such that any assets are contained within encrypted containers.

41 Remote access on RS hardware is limited to the classification of CC Restricted

42 In case of necessary updates to the life cycle documentation[4] the site and the client will cooperate.

43 To enable that the site participates in the development of products the client provides services to setup the necessary development computers (tools, user accounts, etc.) and configuration management systems (user accounts, repositories etc.).

44 To enable the site to realize shipment such that assurance of integrity is assured throughout transport of physical security objects the client will adhere to the shipment method.

45 In case the site is unable to securely destruct certain physical assets the assets will be securely shipped to the client for destruction.

46 To define the participation of the site in the development while maintaining quality, for each product the site and the client agree on the activities to be performed by the site, the specifications of the input for the site and the acceptance of the results by the client.

10.2 Services of the Site

47 The site participates in the development and testing of software[5] for secure integrated circuits.

48 The site uses a shipment method such that assurance of integrity is assured throughout transport of physical security objects.

[4] Part of the life cycle documentation is written in corporation with the client where other parts are provided by the client.

[5] Software means in this case: IC Embedded Software Development (Phase 1) and/or IC Dedicated Software
Development (Phase 2) as defined in 'Security IC Platform Protection Profile' (PP-0035) and 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084)

10.3 Aspects of the SARs

10.3.1 CM capabilities (ALC_CMC.5)

49 Configuration Management is described in [7] and [8].

ALC_CMC.5.1C The TOE shall be labelled with its unique reference.

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

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.

ALC_CMC.5.4C 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.

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 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.

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.

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

ALC_CMC.5.12C 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.

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.

ALC_CMC.5.15C The evidence shall demonstrate that all configuration items are 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.

10.3.2 CM scope (ALC_CMS.5)

50 Configuration Management is described in [7] and [8].

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.

10.3.3 Development Security (ALC_DVS.2)

51 Development Security is described in [9]

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.

10.3.4 Life-cycle definition (ALC_LCD.1)

52 Life-cycle definition is described in [7] and [8].

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

10.3.5 Tools and techniques (ALC_TAT.3)

Tools and techniques is described in [7] and [8].

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.

11. References

11.1 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, Part3: Security Assurance Requirements; 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 Version 1.0," Eurosmart, 15.06.2007.

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

[7] G.Caffrey, „BU ID ALC-CM Common Criteria Documentation, NXPOMS-1719007347-2549," 09.04.2014.

[8] L. Kocvara, „ALC-CM GlobalLogic Zilina, NXPOMS-1719007347-2714," 09.02.2018.

[9] L. Kocvara, „Site Security Manual – GlobalLogic Zilina, NXPOMS-1719007347-2651," 15.03.2018.

11.2 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.

11.3 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

11.4 Revision History

Document Author	Date	Description of Change	Document Owner
Lubos Kocvara	04/18/2018	Removed references to document version	Lubos Kocvara
Lubos Kocvara	03/19/2018	Reference to new version of SSM updated	Lubos Kocvara
Lubos Kocvara	03/13/2018	Area in section 4.3 updated (not released)	Lubos Kocvara
Lubos Kocvara	2/09/2018	References updated, document ID changed, document template updated	Lubos Kocvara
Lubos Kocvara	1/27/2018 (not released)	Update for new building in Zilina	Lubos Kocvara
Lubos Kocvara	10/26/2016	Updated Reference [5] 2017-03-08: migration to NXP OMS, adaption to OMS template, no content change	Lubos Kocvara
In case of questions or change proposals please contact the latest document author or owner.			

Old revision history:

Revision	Description	Author	Approval - Date
V1.1	Updated Reference [5]	Lubos Kocvara	2016-10-26
V1.0	Creation of SST Lite	Lubos Kocvara	2016-10-13

Approvers

Sequence	Role	Name
Approval	Site Security GlobalLogic Zilina	Christophe Bouly