Data Center Akquinet Hamburg

Site Security Target

Rev. v2.4 — 6 June 2024

NXPOMS-1719007347-3816

Evaluation document

PUBLIC

Document information

Information	Content
Keywords	Common Criteria, Data Center, Akquinet Hamburg, Site Security Target
Abstract	Site Security Target for the site certification of the site Akquinet Hamburg (DE)

1 Document Information

1.1 Reference

Title:	Site Security Target - Akquinet Hamburg
Version:	v2.4
Date:	6 June 2024
Company:	Akquinet AG
Name of the site:	Akquinet Hamburg
Site Type:	Datacenter
EAL:	SARs taken from EAL6

1.2 Revision History

Rev.	Date	Description	Author	Owner
2.0	2022-07-22	Initial release in DITA Oxygen XML Author v 17.1 All revisions prior to 1.5 were archived. New Design, New Template Site Certification - Site Security Target	Michael Sandu Gordon Caffrey	Monique Franssen
2.1	2022-11-15	Change Author from Gordon Caffrey to Michael Sandu Removed O.Config-Control, as wrong selected for Datacenter	Michael Sandu	Monique Franssen
2.2	2022-11-23	Corrected the linking any typo in 5.1.2 Objectives Rationale - O.Logical-Access - O.Config-Items Linked the correct Security Objective with Rational to the correct class (ALC_CMC, ALC_CMS, ALC_DVS) in Chapter 7.2.1	Michael Sandu	Monique Franssen
2.3	2022-12-07	Update of dependencies of the SARs in Chapter 7 Update of Bibliography to Eurosmart Template v2.0 form 15. April 2021	Michael Sandu	Monique Franssen
2.4	2024-06-06	Update of the NXP Design Update of Name and Typo correction	Michael Sandu	Monique Franssen

2 SST Introduction

This document is based on the Eurosmart Site Security Target Template [1] with adaptations such that it fits the site.

This Site Security Target is intended to be used by only one specific client, namely NXP Semiconductors B.V.. Therefore, the term 'client' in this document refers directly to NXP Semiconductors B.V..

Definitions of the color coded areas and handling instructions for classified material can be found here [2]

In the following chapters you will find several times statements like 'this and/or that'. The applicability is given by the 'type of site' and the definition of assets.

2.1 Identification of the Site

The site Akquinet Hamburg is located at:

```
akquinet data center competence GmbH
Ulzburger Strasse 201
22850 Norderstedt
Hamburg, Germany
```

2.2 Site Description

2.2.1 Physical Scope

The entire building specified in Section 2.1 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.

All areas in scope are classified as YELLOW and RED areas. The terms YELLOW area and RED area are defined in the NXP internal document NXPOMS-1719007347-2404 "CCC&S Security Requirements overview".

Those locations contain security areas with restricted access under control of NXP where only authorized persons can enter. Authorized persons can be NXP personnel or authorized subcontractors. They perform only the physical activities listed earlier. This personnel is therefore not directly involved in designing, testing, producing, shipping etc. of NXP products.

2.2.2 Logical Scope

The following life-cycle phases as defined in 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084) are subject of the SST:

- Phase I: IC Embedded Software Development
- Phase II: IC Development
- Phase III: IC Manufacturing
- Phase IV: IC Packaging
- Phase V: Composite Product Integration
- Phase VI: Personalisation
- Phase VII: Operational Usage

To perform its development activities the site uses the NXP CCC&S provided and managed remote IT-infrastructure. Locally available IT equipment like workstations or VPN router is also provided and managed by NXP CCC&S directly. The site works as per NXP CCC&S processes. CCC&S is the abbreviation for ‘Competence Center Crypto & Security’.

The security-relevant system is only connected with other systems through VPN router provided by and remotely managed by the NXP Business Line to whom the data belongs. During processing, servers can manipulate encrypted and unencrypted data. The only connection to the outside world is protected through so that no unencrypted content is leaving the Secure Cage. Only the NXP Business Line has the keys to encrypt/ decrypt.

Data are stored in specialized and specific data servers. Secure data are encrypted with hard disk encryption.

All logical activities in the cage are performed remotely. Example: an NXP employee in e.g. Glasgow performs some design work on a security IC: the actual work is done in Glasgow, but logically and physically in the Cage. Administration of the servers in the secure cage are performed remotely using encrypted lines.

2.2.3 List of services in Scope

The following services and/or processes provided by the site are in the scope of the site evaluation process. Some processes are directly part of the phases presented before and others are supporting processes which can be involved at any phase of the development. The services are detailed in section Section 8.2.

- Data hosting

DC Akquinet Site Services releated to life cycle phases:

- Operational Usage (IT/Infrastructure) (Phase VII)

3 Conformance Claim

The SST is conformant to Common Criteria Version 3.1 ([4], [5]).

For the evaluation the following methodology will be used:

- Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology; Version 3.1 ([6])

The evaluation of the site comprises the following assurance components:

- **ALC_CMC.5**
- **ALC_CMS.5**
- **ALC_DVS.2**

The assurance level chosen for the SST is compliant to the Security IC Platform Protection Profile [3] and is therefore suitable for the evaluation of (software for) Security ICs.

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.

4 Security Problem Definition

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 of the TOE and the security management of the site.

4.1 Assets

Depending on the setup of the Site, the protection of the following assets is needed:

Physical Security Objects: The site has physical security objects in relation to the "intended TOEs". Both the integrity and the confidentiality of these must be protected.

- Data Storage
  - Active and accessible data on running file servers
  - Inactive but accessible unencrypted data
  - Defect but holding unencrypted data

Development Data: The site has access to or even copies of electronic development data in relation to developed TOEs. Both the integrity and the confidentiality of these electronic documents must be protected.

- Development Data

Cryptographic Keys: The site creates, receives and/or handles cryptographic keys. Both the integrity and the confidentiality of these electronic data must be protected.

- Cryptographic Keys

Production Data: The site has access to production data in relation to intended TOEs.

- Production Data

Site Certification Data: The site has access to documentation needed to successfully pass a site certification. Both the integrity and the confidentiality of this data must be protected.

- Site Security Manual
- Document list

4.2 Threats

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive 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. In addition, the attacker may be able to use specific working clothes of the site to camouflage the intention.

T.Rugged-Theft: An experienced thief with specialised equipment for burglary, who may be paid to perform the attack tries to access sensitive areas and manipulate or steal sensitive assets.

T.Computer-Net: A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get access to development and/or production systems with the intention to modify the development and/or production process thus violating integrity and possibly confidentiality.

T.Unauthorised-Staff: Unauthorised employees or subcontractors get access to assets or systems used for development, configuration management and/or production, so that the confidentiality and/or the integrity of the "intended TOE" is violated. This can apply to any development and/or production step and any asset related to the "intended TOE" or its configuration.

T.Staff-Collusion: An attacker tries to get access to assets handled at the site. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery.

4.3 Organisational Security Policies

P.Config-Items: The configuration management system shall be able to uniquely identify all 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-Process: The services and/or processes provided by the site are controlled in the configuration management plan. This comprises incoming items, tools used for the development and/or production of the product, the management of flaws and optimizations of the process flow as well as the documentation that describes the services and/or processes provided by the site. A released production/development process is defined and under version control.

4.4 Assumptions

Each site operating in a production flow must rely on preconditions provided by the previous site. Each site must rely on the information received by the previous site/client. This is reflected by the assumptions that must be defined for the interface.

A.Secure-IT-Provisioning: The local IT equipment (e.g. workstations, servers, HSMs) is connected to a secure remote IT-Infrastructure through a secure (encrypted) network connection. The local secure IT-infrastructure together with the remote secure IT-infrastructure and the secure connection between them will satisfy all relevant ALC requirements and are provided and managed by the client. The workstations are configured such that any logical assets are contained within encrypted containers.

NXP rationale for usage of this site: *The secure connection is established by using a VPN tunnel between the two sites. The underlying connection is a rented line which additionally provides an encryption on its own. The evaluator was informed during connection of this site to the security certified network infrastructure. The correctness of the implementation was checked during the virtual Master IT audit. Please refer to the site visit report [8]. The standard NXP Semiconductors PC/Laptop stream developed during the 'Tightening security project' supports the usage of encrypted containers. The usage of this tool is introduced to every user during the Advanced Security Awareness Training.*

5 Security Objectives

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.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 site enforces two or three levels of access control to sensitive areas of the site. The access control measures ensure that only registered and authorized people can access restricted areas. Sensitive products and data are handled in restricted areas only. Network cabling is protected according to classification of the transferred data by avoiding routes through public areas or by usage of appropriate cryptographic measures.

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 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, 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 sensitive configuration item (assets). 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. Sensitive processes may be controlled within a shorter time frame to ensure a sufficient protection.

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.Logical-Access: The site implements a firewall system to enforce a logical separation between the internal network and the internet. The firewall system ensures that only defined services and defined connections are accepted. Furthermore, the internal network is separated into production networks, office and administration network. Specific networks for production and configuration/administration are further logically separated from other internal network to enforce access control. Access to the production network and related systems is restricted to authorised employees involved in the configuration tasks of the production systems. Every user of an IT system has its own user account and password. An authentication using a unique 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 backup of sensitive data and security relevant logs is applied according to the classification of the stored data.

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

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 development and production of the product, for the management of flaws and optimisations of the process flow as well as for the documentation that describes the services and/or processes provided by a site.

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/development flow are checked regarding security concerns and have to sign a nondisclosure agreement. Furthermore, all employees are trained and qualified for their job.

5.1 Security Objectives Rationale

The SST includes a Security Objectives 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.

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

5.1.1 Mapping of Security Objectives

All the given security objective(s) in the table below counter(s) the threat / OSP.

Table 1. Security Problem Definition mapping to Security Objective

Security Problem Definition / Threats	Security Objective
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security
T.Computer-Net	O.Maintain-Security O.Logical-Access
T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Operation O.Staff-Engagement
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement
Security Problem Definition / Policies	**Security Objective**
P.Config-Items	O.Config-Items
P.Config-Process	O.Config-Process

5.1.2 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 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 separate security areas.

By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

O.Security-Control: The site is using dedicated, trained security personnel for guard services. These personnel are responsible for operation of the access control and alarm systems, performing patrol rounds, visitor registration, physical key management, the surveillance of the technical alarm sensors and the responses to incidents.

By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

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 must overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack.

By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

O.Internal-Monitor: Regular meetings are implemented to monitor security incidences as well as changes or updates of security relevant systems and processes. This includes the assessment of security alarms and associated logs of the physical and logical protection. In addition, results of internal audits and assessments are reviewed.

This helps to prevent the threat(s) T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff and T.Staff-Collusion.

O.Maintain-Security: The security related surveillance and alarm systems are maintained on a regular basis. The physical and logical access permission are reviewed and updated if needed. Logs of the associated systems are reviewed to support the work.

This helps to prevent the threat(s) T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.

O.Logical-Access: The secure IT network is split in several segments according to different security level and purpose (development, administration, lab, manufacturing). The protection of network segments is implemented according to the classification of the processed data. The separation is enforced by firewalls and additional network components. Network services are limited to prevent the misuse and the access to network segments. User accounts are limited to the access rights required by the job task following a strict "need to know principle".

This helps to prevent the threat(s) T.Computer-Net.

O.Logical-Operation: Virus protection and patch management for operating systems and applications ensure the secure operation of the computer systems and the defense against malfunctions provoked by malicious software. Furthermore, backup of the production control system and data processing tools is implemented and the classified data from the client is excluded from the backup.

This helps to prevent the threat(s) T.Unauthorised-Staff.

O.Config-Items: The different items part of an "intended TOE" and the "intended TOE" itself is under configuration management. This configuration management system assigns unique identification numbers.

This helps to address the OSP(s) P.Config-Items.

This helps to address the OSP(s) .

O.Config-Process: The control of the released production/development processes and the controlled introduction of changes ensure a reproducible and consistent production/development. Procedures for setting up the production/development process as well as changes to the released processes and documents are in place. Changes can only be done by authorised personnel. A team of specialists ensures that all aspects are covered for the introduction of new processes and for the assessment of changes. All documentation is under configuration management.

This helps to address the OSP(s) P.Config-Process.

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. This provides legal liability to protect the assets against disclosure. Furthermore, all employees are qualified for their job, are trained and had to pass a questionnaire to check the security awareness.

This helps to prevent the threat(s) T.Unauthorised-Staff and T.Staff-Collusion.

6 Extended Assurance Components Definition

No extended components are defined in this Site Security Target.

7 Security Assurance Requirements

Clients using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Eurosmart Protection Profile [3].

The Security Assurance Requirements (SAR) are:

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

The Security Assurance Requirements listed above fulfil the requirements of [7] because hierarchically higher components than the defined minimum site requirements (ALC_CMC.3, ALC_CMS.3, ALC_DVS.1) are used in this Site Security Target.

In addition, the minimum set of SARs is extended by SAR of the assurance components for "CM capabilities" (ALC_CMC.5), "CM scope" (ALC_CMS.5), .

The dependencies for the assurance requirements are as follows

- 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

All included except ALC_LCD.1. ALC_LCD.1 is not included as it is related to development where this site is not involved in development

7.1 Application Notes and Refinements

The description of the site certification process [7] 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.

The SST in hand has been refined to consider "intended TOEs" rather than specific TOEs. All other refinements as stipulated by the corresponding subsections in "Application Notes for Site Certification" [7], chapter 5 of the chosen Assurance Classes have been applied as well. In addition, the relevant refinements of the Eurosmart PP [3] have been considered.

7.2 Security Assurance Rationale

The Security Assurance Rationale maps the content elements of the selected assurance components of [5] to the Security Objectives defined in this SST. The refinements described above are considered.

The site has a process in place to ensure an appropriate and consistent identification of the products. If the site already receives configuration items, this process is based on the assumption that the received configuration items are appropriately labelled and identified.

Note: The content elements that are changed from the original CEM [6] according to the application notes in the process description [7] are written in italic. The term TOE can be replaced by "configuration items" in most cases. In specific cases it is replaced by "intended TOE". "Configuration items" is used here in the sense that these are items contributing to build or to produce the TOE.

The SAR Rationale does not explicitly address the developer action elements defined in [5] 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. This includes the requirement that the procedures are applied as written and explained in the documentation.

7.2.1 Rationales, Aspects and References for ALC_CMC.5

ALC_CMC.5.1C - *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*

Security Objective	Rational
O.Config-Items	The CM system and it’s CM-Plan, which is mandatory for each project, ensure appropriate and consistent labeling through its application.

Aspects	Reference
The sources are labelled in the version control system, which is owned by CCC&S. Documents are labelled with a DOC-number, -title, -owner and date. Configuration Items are identified via the identifiers that are automatically provided by the system as well as the baseline labels that are given by the configuration manager.	- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management - Configuration Management References and Templates

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

Security Objective	Rational
O.Config-Items	The method used to uniquely identify the configuration items is described in the CM-Plan.

Aspects	Reference
All items can be uniquely identified by the version control system, which is owned by CCC&S. Documents can be uniquely identified using the labelling described above. Configuration Items are identified via the identifiers that are automatically provided by the system as well as the baseline labels that are given by the configuration manager.	- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management - Configuration Management References and Templates

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.

Security Objective	Rational
O.Config-Items	The adequate and appropriate acceptance procedures for configuration items are described in the CM-Plan.

Aspects	Reference
Review board is in place for every project. Steering is done by CCC&S.	- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management, Change Control Board - CCB & Change Control Process Outline - NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management, slide on NPI 3.0 Key Review overview - NPI Lifecycle - Configuration Management References and Templates - NXPOMS-1719007347-2486 - L-BL CS Gate Checklist

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

Security Objective	Rational
O.Config-Items	The configuration management system is ensuring uniqueness of the identification.
O.Config-Process	Unique identification of all configuration items is realized by performing the configuration management activities.

Aspects	Reference
All items can be uniquely identified by the version control system, which is owned by CCC&S.	- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management - Configuration Management References and Templates

ALC_CMC.5.5C - The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

Security Objective	Rational
O.Config-Items	The CM system ensure unique identification.
O.Config-Process	Mandates a CM-Plan for each project, and ensures that only authorized changes are made to the configuration items.

Aspects	Reference
Different CM tools like DesignSync, CollabNet as well as EnoviaNXP provide automated measures to only allow authorized changes to configuration items. Restricted access allows only authorized persons to do changes and the authorization for the change is approved by the Change Control Board using the change process.	- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management - Configuration Management References and Templates - NXPOMS-999116894-4839 - Project Setup in Collabnet Instructions

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

Security Objective	Rational
O.Config-Items	The CM system ensure unique identification.
O.Config-Process	Mandates a CM-Plan for each project.

Aspects	Reference
Different CM tools like DesignSync, CollabNet as well as EnoviaNXP support the development of the "intended TOE" by automated means.	- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management - Configuration Management References and Templates - NXPOMS-999116894-4839 - Project Setup in Collabnet Instructions - NXPOMS-1719007347-2657 - L-BL CS Design Environment Maintenance

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.

Security Objective	Rational
O.Config-Process	Mandates a CM-Plan for each project.

Aspects	Reference
Specific roles in tools are defined in a way that the person responsible for accepting a configuration item into CM is not the person who developed it. E.g. the role 'Documentation Office' publishes a document written by an 'Author' or the 'Integrator' generates the release of the "intended TOE", while the 'Developer' is responsible for the development of the "intended TOE" but cannot release it.	- NXPOMS-999116894-4839 - Project Setup in CollabNet instructions - Configuration Management Procedure - NXPOMS-999116894-14314 - L-BL CS Project Role Descriptions

ALC_CMC.5.8C - The CM system shall identify the configuration items that comprise the TSF.

Security Objective	Rational
O.Config-Items	The CM system ensure unique identification.
O.Config-Process	Mandates a CM-Plan for each project.

Aspects	Reference
Per [7] there is no specific TOE in the focus, therefore, this is only applicable to the CM documentation. The documentation can be identified in the tool EnoviaNXP.	- Product/project specific CM plans and the CI list that is used for CC evaluation

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.

Security Objective	Rational
O.Config-Items	The CM system ensure unique identification.
O.Config-Process	Mandates a CM-Plan for each project.

Aspects	Reference
Different CM tools like DesignSync or CollabNet provide automated means to support the audit of all changes. Documents stored in EnoviaNXP or NXPOMS are under version control.	- NXPOMS-1719007347-2015 - Enovia Basic Type Lifecycle Management - NXPOMS-1719007347-2524 - BL CS Configuration and Data Management Procedure - NXPOMS-999116894-4839 - Project Setup in Collabnet Instructions - NXPOMS-1719007347-3034 - Classic OMS Admin Work Instructions

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.

Security Objective	Rational
O.Config-Items	The CM system ensure unique identification.
O.Config-Process	Mandates a CM-Plan for each project.

Aspects	Reference
In case a source file has been changed, the code is compiled again, and all affected items are identified as they are marked as 'changed' compared with the version in the CM system.	- NXPOMS-1719007347-2524 - BL CS Configuration and Data Management Procedure - NXPOMS-999116894-4839 - Project Setup in Collabnet Instructions - Configuration Management Procedure - Requirements Engineering Procedure

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.

Security Objective	Rational
O.Config-Items	The CM system ensure unique identification.
O.Config-Process	Mandates a CM-Plan for each project.

Aspects	Reference
Different CM tools like DesignSync or CollabNet provide means to tag (baseline) a released version from which the "intended TOE" is generated. The version information of documents is stored in EnoviaNXP or NXPOMS.	- NXPOMS-1719007347-2015 - Enovia Basic Type Lifecycle Management - NXPOMS-1719007347-2524 - BL CS Configuration and Data Management Procedure - NXPOMS-999116894-4839 - Project Setup in Collabnet Instructions - NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slides referring to Baselines - Configuration Management Procedure - Requirements Engineering Procedure

ALC_CMC.5.12C - The CM documentation shall include a CM plan.

Security Objective	Rational
O.Config-Process	Mandates a CM-Plan for each project.

Aspects	Reference
Each project must have a project specific CM plan.	- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management - Product specific configuration management plan (CMP) available

ALC_CMC.5.13C - The CM plan shall describe how the CM system is used for the development of the *intended* TOE.

Security Objective	Rational
O.Config-Process	The CM-Plan describes how the CM system is used for the development of the product.

Aspects	Reference
The development environment used is set up centrally as documented. Each project must create a project specific CM plan.	- NXPOMS-999116894-4839 - Project Setup in CollabNet instructions - NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management - Product specific configuration management plan (CMP) available

ALC_CMC.5.14C - The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *intended* TOE.

Security Objective	Rational
O.Config-Process	The acceptance procedures for modified or newly created configuration items are described in the CM-Plan.

Aspects	Reference
The development environment used is set up centrally to ensure 'separation of duties'. Each project must have a project specific CM plan where the project specific CCB is described. Documents are managed centrally after initial creation by the 'Documentation Officer'.	- NXPOMS-999116894-4839 - Project Setup in CollabNet instructions - NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management and Change Control Board - CCB - Product specific configuration management plan (CMP) available

ALC_CMC.5.15C - The evidence shall demonstrate that all configuration items are being maintained under the CM system.

Security Objective	Rational
O.Config-Process	Ensures, that all configuration items are under version control.

Aspects	Reference
The development environment used is set up centrally to ensure 'separation of duties'. Each project must have a project specific CM plan where the project specific processes are described. Documents are stored in project vaults. Evidences can be provided during a site visit.	- NXPOMS-999116894-4839 - Project Setup in CollabNet instructions - NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management - Product specific configuration management plan (CMP) available and documentation

ALC_CMC.5.16C - The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Security Objective	Rational
O.Config-Process	Ensures, that all configuration items are under version control.

Aspects	Reference
After the development environment used is set up centrally, each project must have a project specific CM plan where the project specific processes are described. Documents are stored in project vaults. Evidences can be provided during a site visit.	- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management - Product specific configuration management plan (CMP) available and documentation

The security assurance requirements of the assurance class "CM capabilities" listed above are suitable to support the production of complex products due to the formalized acceptance process and the automated support. The identification of all configuration items supports an automated and industrialized production process. The requirement for authorized changes supports the integrity and confidentiality required for the products. Therefore, this assurance level meets the requirements for the configuration management.

7.2.2 Rationales, Aspects and References for ALC_CMS.5

The scope of the evaluation according to the assurance class ALC_CMS comprises the security products, the complete documentation of the site provided for the evaluation and the configuration and initialization data as well as associated tools. The specifications and descriptions provided by the client are not part of the configuration management at the certified site.

ALC_CMS.5.1C - The configuration list includes the following: the *intended* TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the *intended* TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.

Security Objective	Rational
O.Config-Items	The CM system ensures that all configuration items are under version control including a CI-list. The CI-list contains all items of this content element.

Aspects	Reference
In terms of site certification, the configuration list is represented by the list of all applicable documents including this SST.	- SST - Document list/Bibliography

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

Security Objective	Rational
O.Config-Items	The CI-List uniquely identifies the configurations items per version, date, NXPOMS number, Collabnet ID (whatever is applicable per CI).

Aspects	Reference
All configuration items are maintained in the CM systems. Every document can be uniquely identified by version, date, NXPOMS number, Collabnet ID (whatever is applicable per CI).	- NXPOMS-1719007347-3034 - Classic OMS Admin Work Instructions - CollabNet TeamForge - User & Administration Guide

ALC_CMS.5.3C - For each TSF relevant configuration item, the configuration list shall indicate the developer/ *subcontractor* of the item.

Security Objective	Rational
O.Config-Items	The CI-List indicates the developer/subcontractor/author for each configuration item.

Aspects	Reference
In terms of site certification, the CI-list is the list of all applicable documents. In the CI-List the author of each item is listed.	- Document list/Bibliography

The security assurance requirements of the assurance class "CM scope" listed above support the control of the production and test environment. This includes product related documentation and data as well as the documentation for the configuration management and the site security measures. Since the site certification process focuses on the processes based on the absence of a concrete TOE these assurance requirements are suitable.

7.2.3 Rationales, Aspects and References for ALC_DVS.2

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 *intended* TOE design and implementation in its development environment.

Security Objective	Rational
O.Physical-Access	This covers the physical measures.
O.Security-Control	This covers the organizational measures of the guard team.
O.Alarm-Response	This covers the physical measures and their alarm follow up by the guard team.
O.Internal-Monitor	This covers organizational measures by reviews and management attention.
O.Maintain-Security	This covers organizational measures by maintenance.
O.Logical-Operation	This covers logical measures and the user interaction with the security systems.
O.Logical-Access	This covers logical measures in the area of firewall and virus protection as well at patch management.
O.Staff-Engagement	This covers personnel measures.

Aspects	Reference
- Access control to development areas inside the building, surveillance, alarm system and guard services to prevent access to the security area for unauthorized persons - Operation of the physical security system, emergency procedures, incident handling and reporting - Tracing and control of Visitors, external suppliers and cleaning personnel	- NXPOMS-1281972304-3130 - DVS Master Document DC Akquinet Hamburg

Aspects	Reference
- Internal storage of products in a strong room, handling of physical objects, zero balancing, disposal of security products - Trustworthiness and training of staff - Organizational measures to enforce security and alarm tracing - Personal accountability for products - Policies and procedures for the internal handling of confidential information - Network security measures to ensure logical protection and authentication to computer systems using username and password - Maintenance of security measures - Protection of the internal shipment - Destruction of sensitive documents, data, products and other items	

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.

Security Objective	Rational
O.Config-Process	The development security documentation justifies, that the security measures providethe necessary level of protection to maintain the confidentiality and integrity of the"intended TOE".

Aspects	Reference
The justification is provided in this site security target because it shows that all threats are addressed by the measures. In addition, the measures are monitored to control the effectiveness. Besides this the lifecycle documentation also provides a justification from a different angle.	- This SST, see chapter 7.2 Security Assurance Rationale

The security assurance requirements of the assurance class "Development security" listed above are required since a high attack potential is assumed for potential attackers. The configuration items and information handled at the site during development, production, testing, assembly and pre-personalization or personalization of the "intended TOE" can be used by potential attackers for the development of attacks. Any keys loaded into the "intended TOE" also support the security during the internal shipment or the external delivery. Therefore, the handling and storage of electronic keys must also be protected. Further on the Protection Profile [3] requires this protection for sites involved in the lifecycle of Security ICs development and production.

8 Site Summary Specification

Please refer for the rationales, aspects and references to the subchapters in Section 7.2 for the different ALC classes.

8.1 Preconditions Required by the Site

This section includes justifications for the assumptions defined in the SST. These assumptions are relevant for the splicing process since they must be examined during the product evaluation. Especially aspects like the classification of items and the appropriate provision of specifications for the site must be verified by checking appropriate evidence (e.g. the set of specifications provided to the site with a site certificate) during the product evaluation.

Please also refer to the site visit checklist [8].

The following table explains the preconditions of the client that are required to ensure the security measures of the site in order to protect its assets.

Table 2. Preconditions of Assumptions

Assumption	Precondition
A.Secure-IT-Provisioning	To enable that the site participates in the development of products the client provides services to setup and maintain the necessary development environment (e.g. workstations, tools, test samples) and configuration management systems (e.g. user accounts in project repositories). The client also provides a secure connection between the IT equipment of the site and a secure remote IT infrastructure of the client. These services are provided by the client in a secure way in order to properly protect the assets of the site. This includes the enforcement of a trustworthy access policy to the site equipment and data using the secure connection based on a "need-to-know" principle.

8.2 Services of the Site

Table 3. Services of the Site

Service of the Site	Explanation of the Service
S.Secure_Area	The site provides a secure physical environment (RED and/or YELLOW area) for classified IT infrastructure and equipment installed by the client at the site according to Common Criteria requirements. *Dependencies:* none *Assumptions:* none

9 Bibliography

[1] Eurosmart. Site Security Target Template, Version 2.0, 15. April 2021.

[2] a.) NXP Semiconductors. "CCC&S Security Objects", NXPOMS-1719007347-2401, 29. January 2024.
b.) NXP Semiconductors. "CCC&S Security Objects Master", NXPOMS-1719007347-2402, 17. January 2023.

[3] Eurosmart. Security IC Platform Protection Profile with Augmented Packages (BSI-CC-PP-0084-2014), Version 1.0, 2014.

[4] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

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

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

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

[8] NXP Semiconductors. "Security Checklist for Site Visit", NXPOMS-1719007347-16672, 15. May 2023.

10 Glossary

CA – Certificate Authority

CC – Common Criteria

CCC&S – Competence Center Crypto & Security

CI – Configuration Item

CKC – Customer Key Creation (system for key creation and post-shipment services)

CL – Configuration List

CM – Configuration Management

CSH – China Secure High Confidential

CSM – China Secure Main Confidential

CSR – Certificate Signing Requests

CTO – Chief Technology Organization

CSx – China Secure - Main or High Confidential

DDS – Data Delivery Service

DiT – Data Intake and Translation

DIT – Data Intake

DMZ – Demilitarized Zone

DNV – Dynamic Non-volatile

EAL – Evaluation Assurance Level

FH – Fabkey Helpdesk (old name of DNV desk)

FS – Facility Secure

FAE – Field Application Engineer

HS – High Secure

HSM – Hardware Security Module

IC – Integrated Circuit

IP – Intellectual Property

KDS – Key Delivery Services

KIS – Key Insertion Server

MBK – Master Backup Key

NPIT – New Product Introduction Team

OEF – Order Entry Form

OSP – Organizational Security Policy

PP – Protection Profile

PS – Production Secure

PS-HS – Production Secure-High Secure

PS-RS – Production Secure-Restricted Secure

PMP – Project Management Plan

PQE – Product Quality Engineer

RCS – ROM Code System

ROM – Read-Only Memory

RS – Restricted Secure

SAR – Security Assurance Requirement

SNV – Static Non-Volatile

SNR – Serial Number Server

SSM – Site Security Manual

SST – Site Security Target

ST – Security Target

TOE – Target of Evaluation

TP – Trust Provisioning

TSM – Trusted Service Manager

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

Tab. 1. Security Problem Definition mapping to Security Objective 9

Tab. 2. Preconditions of Assumptions 23

Tab. 3. Services of the Site 23

Contents

1 Document Information 2
1.1 Reference 2
1.2 Revision History 2
2 SST Introduction 3
2.1 Identification of the Site 3
2.2 Site Description 3
2.2.1 Physical Scope 3
2.2.2 Logical Scope 3
2.2.3 List of services in Scope 4
3 Conformance Claim 5
4 Security Problem Definition 6
4.1 Assets 6
4.2 Threats 6
4.3 Organisational Security Policies 7
4.4 Assumptions 7
5 Security Objectives 8
5.1 Security Objectives Rationale 9
5.1.1 Mapping of Security Objectives 9
5.1.2 Objectives Rationale 10
6 Extended Assurance Components Definition 12
7 Security Assurance Requirements 13
7.1 Application Notes and Refinements 13
7.2 Security Assurance Rationale 13
7.2.1 Rationales, Aspects and References for ALC_CMC.5 14
7.2.2 Rationales, Aspects and References for ALC_CMS.5 20
7.2.3 Rationales, Aspects and References for ALC_DVS.2 21
8 Site Summary Specification 23
8.1 Preconditions Required by the Site 23
8.2 Services of the Site 23
9 Bibliography 24
10 Glossary 25
Legal information 27

© 2024 NXP B.V. All rights reserved.