Tata Consultancy Services Hyderabad (IN-HYDT2)

Site Security Target

Rev. 4.1 — 28 June 2024 **Evaluation Document**

PUBLIC

Document information

Information	Content
Keywords	"Tata Consultancy Services, Hyderabad, IT Admin Site, Site Security Target"
Abstract	Site Security Target for the site certification of the site Tata Consultancy Services in India

1 Document Information

1.1 Reference

Title:	Site Security Target - Tata Consultancy Services Hyderabad (IN-HYDT2)
Version:	4.1
Date:	28 June 2024
Company:	Tata Consultancy Services Limited
Name of the site:	Tata Consultancy Services Hyderabad (IN-HYDT2)
Site Type:	Admin site Satellite site
EAL:	SARs taken from EAL6

1.2 Revision History

Rev.	Date	Description	Author	Owners/Approvers
1.0	2023-08-17	Version sent to Lab for evaluation	Prem Kumar	Paul Damean and Peter van Disseldorp
2.0	2024-01-05	Incorporated review feedback received from lab	Prem Kumar	Paul Damean and Peter van Disseldorp
3.0	2024-03-08	Incorporated review feedback received from lab	Prem Kumar	Paul Damean and Peter van Disseldorp
4.0	2024-04-17	Updated section 2.1 to reflect unique name of the site as recommended by Certifier	Prem Kumar	Paul Damean and Peter van Disseldorp
4.1	2024-06-28	Updated "Company" and "Name of the site" under section 1.1 Included a statement under section "SST Introduction" providing the clarification of the usage of short form of the site in rest of the SST Updated Gloassary with TCS Full Form	Prem Kumar	Gabor Hornyak

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.

The phrase "TCS Hyderabad" will also appear several times in this document. It should be read as "Tata Consultancy Services Hyderabad (IN-HYDT2)".

2.1 Identification of the Site

Tata Consultancy Services Hyderabad (IN-HYDT2) Site belongs to Tata Consultancy Services and the complete address is as follows :

```
Tata Consultancy Services Hyderabad (IN-HYDT2),
ODC 6, 5th Floor, Zone 6, Synergy Park-SEZ-Unit 2 - Phase II,
Premises No.2-56/1/36, Survey No.26, Gachibowli,
Serilingampally Mandal,
R R District Hyderabad, Telangana-500032
```

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.

The TCS Hyderabad site supports activities of several organizations, but the area where the relevant NXP IT Admin secure activities take place is limited to secure room in ODC 6, Core 2 - 5th Floor, Zone 6. The Secure Room provides 1st and/or 2nd and 3rd level technical support to NXP Business Units.

All areas in scope are classified as YELLOW or RED areas. The terms YELLOW area and RED area are defined in the NXP internal document NXPOMS-1719007347-2404 "CCC&S Security Requirements Overview". Activities of other organizations other than NXP **are not in scope of this SST**.

Those locations contain security areas with restricted access where only authorized persons can enter. Authorized persons can be TCS personnel or authorized subcontractors working for NXP. 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

The personnel in the Secure Room are not directly involved in designing, testing, producing, shipping etc. of NXP products. Therefore, there are no assets inside the site. However, the personnel have root level access to the electronic assets of the business units they manage and could therefore lead to threats of these assets. It is these threats that are the main subject of this Site Certification.

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.

The Secure Room provides 1st and/or 2nd & 3rd line IT support to NXP Business Lines (BLs). This consists of activities such as:

- Adding file storage space to existing NXP accounts
- Remote installation of operating systems
- General IT setup and maintenance
- Remote installation of software upgrades and patches
- User account creation, user account maintenance and revocation
- Implementing approved requests from the NXP Change Control Authority Board
- Resolving technical issues and responding to incidents

The site provides physical protection of the on-site IT infrastructure

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_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.

- IT Infrastructure (e.g. VPN, Switches, network components)

IT Security Objects: The site has IT security objects in relation IT infrastructure. Both the integrity and the confidentiality of these must be protected. Development data or keys hosted on the storages in the datacenter are **not** in scope of this SST, but of those for the datacenters.

- Admin account

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

- Router keys to establish a secure connection

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.Accident-Change: An employee, contractor or student trainee may exchange products of different production lots / different clients during production or changes tool configuration that have an impact on the "intended TOE" by accident.

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.

T.Attack-Transport: An attacker might try to get hold of any assets during the internal shipment and/or the external delivery. The target is to compromise confidential information or violate the integrity of the assets during the shipment/delivery process to allow a modification, cloning or the direct/indirect retrieval of confidential information.

4.3 Organisational Security Policies

P.Zero-Balance: The site ensures that all sensitive items (security relevant parts of the "intended TOEs" of different clients) are separated and traced on a device basis. For each handover, either an automated or an organizational "two-employees-acknowledgement" (four-eyes principle) is applied for functional and defect assets. As per the released production process the defect assets are either destroyed at the site or sent back to the client.

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

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

P.Scrap-Items: Any item that is defect, end-of-life or that does not comply with the quality requirements is shipped back to the client for destruction or is scrapped at the site in a way that the destructed item does not support any attacker.

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.

A.Client-Agreements [IT]: The site participates in the administration of the IT environment. The site and the client agree on the following items:

- the activities to be performed by the site including work instructions,
- in case of necessary updates to the life cycle documentation, the site and the client align.

The agreed methods and tools ensure the correct handling of theconfiguration items in terms of Common Criteria regarding the classes ALC_CMC, ALC_CMS.

NXP rationale for usage of this site: *Secure IT environment manager provides CM controlled work instructions to the site. As the employees at this site are considered as regular team members just located at another physical site, each change on the documents controlled in NXPOMS is accessible by them. All admin employees are trained concerning relevant security requirements using "Standard Security Awareness Training" or "Advanced Security Awareness Training" and work according to NXPOMS-1719007347-2401 "CCC&S Security Objects". Furthermore they have access to all relevant experts at the other secure IT locations worldwide.*

A.Client-Agreements [Satellite]: The site participates in the development of products. The site and the client agree on the following items:

- the activities to be performed by the site,
- the specifications of the input for the site including tools,
- the acceptance of the results by the client,
- the used configuration management methods, tools and their setup,
- the delivery and shipment details of any security relevant item,
- the necessary setup of computers, their configuration and user accounts,
- the handling of scrap configuration items: in case that scrap is not destroyed by the site, scrap configuration items are transferred back to the client,
- in case of necessary updates to the life cycle documentation, the site and the client align.

The agreed methods and tools ensure the correct handling of theconfiguration items in terms of Common Criteria regarding the classes ALC_CMC, ALC_CMS and ALC_TAT.

NXP rationale for usage of this site: *Whether the team members are located on an NXP premise or remotely on another secure site does not make any difference. They are part of the team and contribute in the same way as all team members do. All available security objects are handled according to NXPOMS-1719007347-2401 "CCC&S Security Objects". All activities per site are covered in the overall PMP, the sub-project PMP or the WBS in Sciforma as documented in NXPOMS-999116894-3989 "L-BL CS BCaM Handbook". The input for the site is handled during the project setup and the creation of the WBS for the engineers at the site. The acceptance of the results is defined during the project setup in the requirements development phase and checked during the gate reviews. The used configuration management methods and tools are documented in NXPOMS-1719007347-2524 "Configuration and Data Management Procedure". The delivery and shipment is covered by NXPOMS-1719007347-2354 "CCC&S Packing and Delivery Requirements for Security Products", while the return shipment (also scrap)*

from this site to NXP is covered in their ALC-DVS documentation. This site is supported by the NXP IT team to put in place and to configure development and production computers according to corporate and/or CCC&S rules. They use the usual configuration management tools which were certified during the virtual Master IT audit.

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

NXP rationale for usage of this site: *The site uses commonly used tools in NXP. They all were found suitable for proper configuration item handling and providing unique identifiers.*

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.Exclusive-Access: The only way to access the clients network is through management workstations connected to the encryption equipment provided by the client. There is no internal network access to the encryption equipment.

O.LifeCycle-Doc: The site uses life cycle documentation that describes:

1. A configuration items list;
2. Site security;

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.Network-Separation: The development network of the site exists within the secured areas of the site only. It is connected only to:

1. the VPN gateway that provides a secure connection to the remote secure network of the client;
2. the development workstations provided by the client;

3. additional equipment (e.g. a printer) approved by the client.

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.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.

O.Data-Transfer: Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorised employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secure measures and they are sufficiently protected.

O.Control-Scrap: The site has either measures in place to destruct sensitive documentation, erase electronic media and destroy sensitive configuration items so that they do not support an attacker, or the site returns the assets to be scrapped to the client, according to the secure shipment procedure of the client.

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.Exclusive-Access O.Maintain-Security O.Network-Separation O.Logical-Access
T.Accident-Change	O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Control-Scrap
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
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Control-Scrap
T.Attack-Transport	O.LifeCycle-Doc
Security Problem Definition / Policies	**Security Objective**
P.Zero-Balance	O.Staff-Engagement O.Control-Scrap
P.Organise-Product	O.Logical-Access O.Logical-Operation
P.Data-Transfer	O.Data-Transfer
P.Scrap-Items	O.Control-Scrap

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.Exclusive-Access: Using the protected security networks is only possible from inside the certified security areas or via VPN tunnel in specific cases. Administrative tasks can only be executed by authorized personnel from specific security rooms. No other possibility does exist to access or administrate the security networks.

This directly addresses the threat T.Computer-Net.

O.LifeCycle-Doc: Dedicated documents exist which define the use and the management of the configuration management systems, the configuration item list, the site security, the production/development process and the production/development tools. The site follows the procedures and instructions of these documents.

This directly addresses the threat T.Attack-Transport.

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.Network-Separation: The security network is located in a dedicated secured area. This network is connected only to dedicated trustworthy systems.

This directly addresses the threat T.Computer-Net.

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 address the OSP(s) and P.Organise-Product. T.Computer-Net and T.Accident-Change.

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 directly addresses the OSP P.Organise-Product. This helps to prevent the threat(s) T.Unauthorised-Staff and T.Accident-Change.

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 directly addresses the OSP P.Zero-Balance. This helps to prevent the threat(s) T.Accident-Change, T.Unauthorised-Staff and T.Staff-Collusion.

O.Data-Transfer: The integrity and confidentiality of the data transfer from/to the site is protected against modification and/or disclosure by cryptographic means during transfer. The selected cryptographic algorithms are appropriate to resist against high attack potential. Cryptographic keys and password used for secure communication are sufficiently protected against unauthorised access and disclosure.

This helps to address the OSP P.Data-Transfer.

O.Control-Scrap: The security of scrap handling is ensured by either securely destruct assets at the site (e.g. paper shredder) or return them to the client. Scrap material is stored, until destruction or shipment back to the client, in security environments. Procedures document the destruction process.

This helps to address the OSP(s) P.Zero-Balance P.Scrap-Items. This helps to prevent the threat(s) T.Accident-Change, 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:

- 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_DVS.1) are used in this Site Security Target.

Additionally, the chosen assurance components are derived from the assurance level EAL6 of the assurance class "Life-cycle Support". For the assessment of the security measures attackers with high attack potential are assumed. However, the activities of the site are not directly related to developing, managing, designing, testing, producing, shipping etc. of secure products. Therefore, this site does not claim conformance to ALC_CMC, ALC_CMS, ALC_DEL, ALC_TAT, or ALC_LCD.

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_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.LifeCycle-Doc	This covers the overall development security documentation.
O.Exclusive-Access	This covers the technical restrictions.
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.Network-Separation	This covers logical measures, esp. the network separation.
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.Control-Scrap	This covers procedural measures of secure destruction of security material.
O.Staff-Engagement	This covers personnel measures.
O.Data-Transfer	This covers logical measures related to cryptographic encryption and signature algorithms during electronic transfer of data.

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	- NXPOMS-1719007347-16903 - Site Security Manual - TCS Hyderabad

Aspects	Reference
- Tracing and control of Visitors, external suppliers and cleaning personnel - 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.Exclusive-Access	Ensures the integrity by authorized people

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 Security Assurance Rationale 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.
A.Client-Agreements [IT]	To allow the site to provide the IT administration service, it is necessary that the relevant work instructions and procedures are trained, shared and kept up to date. Furthermore, changes to the relevant procedures require a notification of the relevant people.

Table 2. Preconditions of Assumptions*...continued*

Assumption	Precondition
A.Client-Agreements [Satellite]	To enable the site to participate in the development of products, the client needs to provide services to setup and maintain the necessary development environment (e.g. workstations, development tools, test samples). Further, the client needs to setup and maintain the used configuration management systems and provide a project specific CM plan. This includes the setup and maintenance of user accounts in the project repositories and other required configuration management tools. The client needs to agree about the configuration management methods and the usage of the configuration management tools. The configuration management methods and tools by the client ensure the correct handling of the configuration items according to Common Criteria. For each project setup, the client needs to agree on the activities to be performed by the site, the specifications of the input for the site and the acceptance of the results from the site. Regarding a destruction of certain physical assets, the client need to specify whether the scrap need to be destroyed by the site or need to be sent back to the client. In the latter case the client is responsible for the secure destruction of the assets.
A.Item-Identification	Before sending items to this site, the previous site must label it uniquely. Those unique identifiers can come from EnoviaNXP, Collabnet or other tools.

8.2 Services of the Site

Table 3. Services of the Site

Service of the Site	Explanation of the Service
S.IT_Admin_Services (RS/HS/PS-RS/PS-HS/FS)	Administration of the listed MASTER IT services by • Resolving problems and responding to incidents • Implementing approved IT Changes • Implementing approved Service Request For the following services: • Client Systems and Workplace Services • Infrastructure services • System Box Infrastructure • Network Services • Monitoring Services • NXDI Infrastructue Services • Collaboration Services • Security Services • Monitoring Services *Dependencies:* **S.Secure_Area** must be fulfilled to ensure physical security *Assumptions:* **A.Secure-IT-Provisioning** must be fulfilled for secure networks **A.Client-Agreements [IT]** must be fulfilled

Table 3. Services of the Site*...continued*

Service of the Site	Explanation of the Service
S.IT_Admin_Services_CSx (CSM/CSH)	Administration of the listed MASTER IT services by • Resolving problems and responding to incidents • Implementing approved IT Changes • Implementing approved Service Request For the following services: • Client Systems and Workplace Services • Infrastructure services • System Box Infrastructure • Network Services • Monitoring Services • NXDI Infrastructue Services • Collaboration Services • Security Services • Monitoring Services *Dependencies:* **S.Secure_Area** must be fulfilled to ensure physical security *Assumptions:* **A.Secure-IT-Provisioning** must be fulfilled for secure networks **A.Client-Agreements [IT]** must be fulfilled
S.IT_Support	The site provides 1st and/or 2nd & 3rd level IT support to the client. This consists of activities such as: • Ticket creation or 1st level telephone hotline • Remote support 2nd and 3rd level • Installation of Client Operating Systems • Remote installation of software upgrades and patches • Resolving problems and responding to incidents • Implementing approved IT Changes • Implementing approved Service Request *Dependencies:* **S.Secure_Area** must be fulfilled to ensure physical security *Assumptions:* **A.Secure-IT-Provisioning** must be fulfilled for secure networks **A.Client-Agreements [IT]** must be fulfilled
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, 13. December 2021.
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] Check List for Site Visit NXP development site under site certification, Version 1.4, 26. February 2020.

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

TCS – Tata Consultancy Services Limited

TOE – Target of Evaluation

TP – Trust Provisioning

TSM – Trusted Service Manager

11 Legal information

11.1 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.

11.2 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 http://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 data sheet 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.

11.3 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

Contents

Date of release: 28 June 2024
Document identifier: NXPOMS-1719007347-16880