Reference: 2020-15-INF-3500-v1
Target: Público
Date: 04.05.2021

Created by: CERT11
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2020-15**
TOE	**NXP San Jose**
Applicant	**17070621-NL800009782B01 - NXP Semiconductors B.V.**
References	

[EXT-5798] Certification Request

[EXT-6726] Evaluation Technical Report

Certification report of the site NXP San Jose, as requested in [EXT-5798] dated 05/02/2020, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-6726] received on 26/03/2021.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the site NXP San Jose.

The site is a single building location with two floors occupied by NXP Semiconductors. The development area is exclusively occupied by NXP with restricted need to know access controlled by NXP for authorized personnel only.

Developer/manufacturer: NXP Semiconductors B.V.

Sponsor: NXP Semiconductors B.V.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories.

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R5

To re-use in evaluations up to EAL6

Security Assurance Components: ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1, AST_INT.1, AST_CCL.1, AST_SPD.1, AST_OBJ.1, AST_ECD.1, AST_REQ.1 and AST_SSS.1.

Resistance to Attack Potential: High.

Evaluation end date: 12/04/2021.

Re-use expiration date: 15/06/2022[1].

All the assurance components required by the evaluation have been assigned a “PASS” verdict are resistant to attackers with a High attack potential. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied, as defined by the Common Criteria v3.1 R5, the supporting document guidance CCDB-2007-11-001 Site Certification [SCER] and the JIWG supporting document Minimum site security requirements [MSSR].

The assurance components are chosen in order to re-use the results in evaluations up to EAL6. It has been assumed that the security measures are resistant to attacks performed by attackers with a *High* attack potential.

[1] This audit was performed as a virtual site audit according to [IT-013] and [JIL-COVID] policies, and therefore the re-use of evaluation activities is limited at most to 18 months since de site audit date.

Considering the obtained evidences during the instruction of the certification request of the site NXP San Jose, a positive resolution is proposed.

SITE SUMMARY

The NXP San Jose is located at

NXP Semiconductors

411 East Plumeria Drive

San Jose, CA 95134

United States

The site comprises the following areas within the scope of the evaluation:

- Yellow areas (Level 2: RS Enhanced Security Zone): Moderate security areas with basic stop detection layers.
- Red areas (Level 3: HS High Security Zone): High security areas with enhanced stop and detection layers.

Within those areas, only members of the IT department, development group and test team are entitled to access sensitive information like secure shipments, source code, confidential development documentation and samples. To enforce such access restriction, a combination of physical, procedural, personnel and logical measurements have been installed.

SITE DESCRIPTION

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

- The site participates in the development and testing of software for secure integrated circuits.
- The site participates in the hardware development and testing of secure integrated circuits.
- The site uses a shipment method such that assurance of integrity is assured throughout transport of physical security objects.
- Supporting services:
    - The site is involved in the NXP datacenters security supervision

TYPICAL LIFE CYCLE OF SUPPORTED TOEs

It is assumed that product certifications which refer to this certificate are related to a TOE that follows a TOE life-cycle according to [PP84], chap. 1.2.3. The NXP San Jose covers Phase 1 (IC Embedded Software Development) and Phase 2 (IC Development) according to [PP84].

SECURITY ASSURANCE REQUIREMENTS

The site was evaluated with all the evidence required to fulfil the evaluation activities resistant to attackers with a **High** attack potential, according to Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5.

The assurance components are chosen in order to re-use the results in evaluations up to EAL6. Therefore, it has been assumed that the security measures are resistant to attacks performed by attackers with a High attack potential.

Assurance Class	Assurance Components
AST: Site Security Target Evaluation	AST_INT.1 SST introduction
	AST_CCL.1 Conformance claims
	AST_SPD.1 Security problem definition
	AST_OBJ.1 Security objectives
	AST_ECD.1 Extended components definition
	AST_REQ.1 Security assurance requirements
	AST_SSS.1 Site summary specification
ALC: Life-cycle support	ALC_CMC.5 Advanced support
	ALC_CMS.5 Development tools CM coverage
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model

Please note that ALC_DEL.1 has been excluded from the SST since this site does not perform external deliveries and ALC_DEL.1 is therefore not applicable.

IDENTIFICATION

Site Name	NXP San Jose
Site Location	NXP Semiconductors 411 East Plumeria Drive San Jose, CA 95134 United States
Areas in the scope of the certificate as declared in the SST	See section 1.3 of Site Security Target.
Activities in the product development	Life cycle phases: • Phase 1 (IC Embedded Software Development) • Phase 2 (IC Development)
Site Security Target	Site Security Target NXP San Jose. NXPOMS-1719007347-4559, v6.1, 03/25/2021.
Evaluation Level	Common Criteria v3.1 R5 To re-use activities in evaluations up to EAL6
Security Assurance Components	ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1, AST_INT.1, AST_CCL.1, AST_SPD.1, AST_OBJ.1, AST_ECD.1, AST_REQ.1 and AST_SSS.1.
Attack Potential	High

SECURITY POLICIES

The use of the product NXP San Jose shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Site Security Target [SST], chapter 3.3 (Organizational Security Policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

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

The detail of the assumptions considered to be applicable is documented in the Site Security Target [SST], chapter 3.4 (Assumptions).

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the site NXP San Jose, although the agents implementing attacks have a High attack potential for the Security Assurance Requirements ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1, AST_INT.1, AST_CCL.1, AST_SPD.1, AST_OBJ.1, AST_ECD.1, AST_REQ.1 and AST_SSS.1, and always fulfilling the assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the site security properties and the associated certificate, do not guarantee any resistance.

The detail of these threats is documented in the Site Security Target [SST], chapter 3.2 (Threats).

DOCUMENTS

The site evaluation has been based on the evidences listed in the chapter 5 (Evaluation evidence) of the Evaluation Technical Report of NXP San Jose [EXT-6726].

These evidences describe the global procedures and security measures in the site. For each specific TOE, some accessory documents including specific characteristics of the TOE should be provided in addition to the above evidences.

The above evidences should be made available to ITSEFs in order to re-use the results of this certificate.

EVALUATION RESULTS

The site NXP San Jose has been evaluated against the Security Target [SST].

All the assurance components required by the evaluation have been assigned a “PASS” verdict are resistant to attackers with a High attack potential. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied, as defined by the Common Criteria v3.1 R5, the supporting document guidance CCDB-2007-11-001 Site Certification [SCER] and the JIWG supporting document Minimum site security requirements [MSSR].

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the site are provided. These have been collected along the evaluation process and are detailed to be considered.

- The current PASS verdict is conditioned by the certificate of NXP Headquarters (whose Site evaluated under CC methodology is identified as NXP Hamburg) certified by the BSI. A revocation of the certificate of NXP Hamburg would imply the revocation of this certificate. Configuration Management services provided by NXP Hamburg and consumed by NXP Semiconductors San Jose are covered by the certificate [BSI-DSZ-CC-S-0124-2019]. Evaluations reusing the results of NXP Semiconductors San Jose shall ensure the existence of a valid certificate covering the consumed services provided by NXP Hamburg.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the site NXP San Jose, a positive resolution is proposed.

This Certification Report only applies to the site and its evaluated scope as indicated. The confirmed assurance components is only valid on the condition that all assumptions and preconditions required by the site, as given in this report and in the Site Security Target, are observed.

The owner of the certificate is obliged:

1. when advertising the Site Certificate or the fact of the Site Certification, to refer to the Site Certification Report as well as to provide the Site Certification Report and the Site Security Target and documentation mentioned herein to any client for the application and proper usage of the certified site,
2. to inform this Certification Body immediately about vulnerabilities of the site that have been identified by the sponsor or applicant or any third party after issuance of the certificate,
3. to inform this Certification Body immediately about security relevant changes in the scope of the evaluated site, e.g. changes related to the logical and physical development and production environment, to processes, and to services of the site.

In case of changes to the certified site, the validity can be extended to the changed site, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified site, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

RE-USE OF THE SITE CERTIFICATE

The re-use of this Site Certificate is limited to the extent defined in the Spanish Certification Body (CCN) Technical Interpretation "IT-003 Instrucción técnica: reutilización de resultados mediante la certificación de centros de desarrollo" [IT003], the Supporting Document Guidance Site Certification [SCER] and the SOG-IS Smartcard and similar devices supporting documents, such as the Minimum site security requirements [MSSR].

The results from a site certification can be re-used for product certifications. For each specific TOE, accessory documents including specific TOE characteristics should be evaluated in addition to the above specified documents. These evidences shall rely and shall be consistent with the evidences used in the site certificate evaluation and in the Site Security Target.

Currently the Recognition Agreements in place do not cover the recognition of Site Certificates. However, the evaluation process performed was outlined according to the rules of the agreements and by using the agreed supporting document on Site Certification [SCER] and [MSSR]. Therefore, the results of this evaluation and certification procedure can be re-used by the issuing scheme in a subsequent product evaluation and certification procedure.

When re-using the results of the activities that uphold this site certificate in a product evaluation, the scheme responsible for certifying the product may decide to fully recognize the results or contact this scheme to query about specific assurance activities carried out in the scope of this site certification.

SITE CERTIFICATE VALIDITY REVIEW

In this case, and according to arrangements in SOG-IS Smart Card and similar devices technical domain, to re-use the evaluation activities that uphold this Site Certificate in a product specific evaluation, a reassessment of the assurance activities validity should be done at most 18 months after the site audit date as virtual site audit procedure of [IT-013] and [JIL-COVID] policies has been applied. Therefore a reassessment of the assurance activities validity should be done before 15/06/2022.

According to [JIL-COVID], despite from the 18 months mentioned, a "virtual audit" should be replaced by a regular on-site audit as soon as the restrictions of the pandemic situation and scheduling of the parties involved allows for.

SHARED TECHNICAL AUDIT REPORT (STAR)

The evaluation activities carried out in this site certification dossier have been summarized in a Shared Technical Audit Report (STAR). This STAR has been validated by this Certification Body according to [ASAREP]. The reference of the STAR is:

- **Report name**: SITE TECHNICAL AUDIT REPORT (STAR). NXP San Jose
- **Report ID**: CCENXP004-STAR-M0
- **Version**: M0
- **Issue Date**: 26/03/2021
- **SHA-256**: 036761E2A0E08AD02E9DA2EADD54DDB3927A37F775F4F82F7B6D1C346AEC85B1
- **Issuing ITSEF**: Applus Laboratories
- **Site audit dates**: 14/12/2020 – 15/12/2020

The STAR report constitutes an evaluation evidence, therefore according to article 25 of Presidential Order PRE/2740/2007 which regulates the CCN Certification Body, written authorization must be requested by Applus Laboratories to the Certification Body to share any information of this certification dossier (including the STAR report) with third parties.

It is expected that if the applicant NXP Semiconductors B.V. is willing to share the STAR report with any third party, they may contact Applus Laboratories to perform an authorization request to the CCN Certification Body to distribute this report.

SITE SECURITY TARGET

Along with this certification report, the complete site security target (SST) of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- Site Security Target NXP San Jose. NXPOMS-1719007347-4559, v6.1, 03/25/2021.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ITSEF	Information Technology Security Evaluation Facility
JIWG	Joint Interpretation Working Group of SOG-IS
OC	Organismo de Certificación

SOG-IS	Senior Officials Group Information Systems Security
SST	Site Security Target
TOE	Target of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[ASAREP] ISCI WG1 - ALC Site Audit Reuse Exchange Procedure, draft version 1.1. March 2018.

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[IT-003] Instrucción técnica: reutilización de resultados mediante la certificación de centros de desarrollo. Versión 2. November 2014.

[IT-013] Instrucción técnica temporal para la realización de actividades de evaluación con motivo del coronavirus COVID-19, versión 3.0. August 2020.

[JIL-COVID] JIL Temporary Covid19 pandemic operational SOGIS evaluation and certification policy and rules, version 1.0, June 2020.

[MSSR] Joint Interpretation Library. Minimum site security requirements. Version 3.0. Date February 2020.

[PP84] EUROSMART's protection profile "Security IC Platform Protection Profile with Augmentation packages. Version 1.0, 2014"

[SANT] Common Criteria Recognition Arrangement. ST sanitising for publication. Document number CCDB-2006-04-004, April 2006.

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

[SST] Site Security Target NXP San Jose. NXPOMS-1719007347-4559, v6.1, 03/25/2021.