Reference: 2021-17-INF-3723-v1
Target: Pública
Date: 14.03.2022

Created by: CERT8
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2021-17**
TOE	**NXP Toppan Round Rock**
Applicant	**17070621-NL800009782B01 - NXP Semiconductors B.V.**
References	

[EXT-6734] Certification Request

[EXT-7512] Evaluation Technical Report

Certification report of the site NXP Toppan Round Rock, as requested in [EXT-6734] dated 31/03/2021, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-7512] received on 22/12/2021.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the site NXP Toppan Round Rock.

The site is not directly involved with any onsite activities of the life cycle phases described into [PP84] but is supporting Phase 3 activities (IC manufacturing) for sites using this service.

The Toppan building supports activities of many other organisations but is described here for **IT support operations** only. Activities are performed through IT room (IT1). Global IT administration and infrastructure support through secure remote connections (encrypted VPN) to all Toppan mask shops (incl. AMTC Dresden).

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

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 EAL 6

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

Resistance to Attack Potential: High.

Evaluation end date: 22/12/2021.

Re-use expiration date: 20/01/2023[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

[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 the site audit date considering it a re-audit with major changes of the scope.

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 EAL 6. It has been assumed that the security measures are resistant to attacks performed by attackers with a *High* attack potential.

Considering the obtained evidences during the instruction of the certification request of the site NXP Toppan Round Rock, a positive resolution is proposed.

SITE SUMMARY

The NXP Toppan Round Rock is located at:

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

SITE DESCRIPTION

The Toppan building specified 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.

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. **This site is not directly involved with any onsite activities of the life cycle phases described into [PP84] but is supporting Phase 3 activities (IC manufacturing) for sites using this service.**

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 EAL 6. 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 Advance support
	ALC_CMS.5 Development tools CM coverage
	ALC_DVS.2 Sufficiency of security measures

The activities of the site are not directly related to designing, testing, producing, shipping, etc. of secure products. Therefore, this site does not claim conformance to ALC_DEL, ALC_TAT nor ALC_LCD.

IDENTIFICATION

Site Name	NXP Toppan Round Rock
Site Location	Toppan Round Rock 400 Texas Avenue Round Rock TX 78664 United States
Areas in the scope of the certificate as declared in the SST	The walls of this building form the physical boundary of the site.
Activities in the product development	Life cycle phases: • **supporting** Phase 3 activities (IC manufacturing) for sites using this service

Site Security Target	Site Security Target - Toppan Round Rock. NXPOMS-1719007347-4653, v1.6, 10 Dec 2021
Evaluation Level	Common Criteria v3.1 R5 To re-use activities in evaluations up to EAL 6
Security Assurance Components	ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, AST_INT.1, AST_CCL.1, AST_SPD.1, AST_OBJ.1, AST_ECD.1, AST_REQ.1, AST_SSS.1.
Attack Potential	High

SECURITY POLICIES

NXP Toppan Round Rock 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]: 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]: 3.4 Assumptions.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the site NXP Toppan Round Rock, although the agents implementing attacks have a High attack potential for the Security Assurance Requirements ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, AST_INT.1, AST_CCL.1, AST_SPD.1, AST_OBJ.1, AST_ECD.1, AST_REQ.1, 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]: 3.2 Threats.

DOCUMENTS

The site evaluation has been based on the evidences listed in the chapter 5 (List of evaluation evidence) of the Evaluation Technical Report of NXP Toppan Round Rock [EXT-7512 (ETR)].

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 Toppan Round Rock 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.

No specific recommendations reported.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the site NXP Toppan Round Rock, 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.

Additionally, this Certification Body wants to remark the following:

This site is not directly involved with any onsite activities of the life cycle phases described into [PP84].

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 (re-audit with major changes of the scope) 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 should be done before 20/01/2023.

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
- **Report ID**: CCENXP001R1-STAR-M1
- **Version**: M1
- **Issue Date**: 15/12/2021
- **Issuing ITSEF**: Applus Laboratories
- **Site audit dates**: 19/07/2021-20/07/2021

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 – Toppan Round Rock, version 1.6

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. Date 11-11-2014.

[IT-013] Instrucción técnica temporal para la realización de actividades de evaluación con motive del coronavirus COVID-19, versión 6. July 2021.

[JIL-COVID] JIL Temporary Covid19 pandemic operational SOGIS evaluation and certification policy and rules, version 1.3. October 2021.

[MSSR] Joint Interpretation Library. Minimum site security requirements. Version 2.1 Date December 2017.

[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. Date April, 2006.

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

[SST] Site Security Target – Toppan Round Rock, version 1.6