

Reference: 2024-21-INF-4582-v1
Target: Limitada al expediente
Date: 16.07.2025

Created by: CERT16
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	2024-21
TOE	Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, Line S3, MR2, SR1, SR3 and DSR-B building)
Applicant	Samsung Electronics Co., Ltd.
References	[EXT-9046] 2024-05-03_2024-21_solicitud_certificacion [EXT-9592] 2025-04-08_2024-21_ETR_vM0

Certification report of the site Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, Line S3, MR2, SR1, SR3 and DSR-B building), as requested in [EXT-9046] dated 23/04/2024, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-4580] received on 08/04/2025.

CONTENTS

EXECUTIVE SUMMARY	3
SITE SUMMARY.....	4
SITE DESCRIPTION	4
TYPICAL LIFE CYCLE OF SUPPORTED TOEs.....	6
SECURITY ASSURANCE REQUIREMENTS	6
IDENTIFICATION	7
SECURITY POLICIES.....	8
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT	8
CLARIFICATIONS ON NON-COVERED THREATS	8
DOCUMENTS	8
EVALUATION RESULTS	9
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM	9
CERTIFIER RECOMMENDATIONS	9
RE-USE OF THE SITE CERTIFICATE	10
SITE CERTIFICATE VALIDITY REVIEW	11
SHARED TECHNICAL AUDIT REPORT (STAR)	11
SITE SECURITY TARGET.....	11
GLOSSARY.....	12
BIBLIOGRAPHY	12

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the site Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, Line S3, MR2, SR1, SR3 and DSR-B building)

Developer/manufacturer: SAMSUNG Electronics Co. Ltd

Sponsor: SAMSUNG Electronics Co. Ltd.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R5

To re-use ALC certified security assurance components in evaluations up to EAL6

Security	Assurance	Components:
	ALC_CMC.5,ALC_CMS.5,ALC_DVS.2,ALC_LCD.1,ALC_TAT.3,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: 17/07/2025

Re-use expiration date: 18/01/2027¹.

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 ALC certified security assurance components 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.

Considering the obtained evidences during the instruction of the certification request of the site Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, Line S3, MR2, SR1, SR3 and DSR-B building), a positive resolution is proposed.

¹ This audit was performed as a on site audit according to [IT-013] policy, and therefore the re-use of evaluation activities is limited at most to 30 months since the site audit date (18/01/2027).

SITE SUMMARY

The Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, Line S3, MR2, SR1, SR3 and DSR-B building) is located at:

- Samsung Electronics. Co., Ltd. (Hwaseong), DSR building
1-1, Samsungjeonja-ro, Hwaseong-si, Gyeonggi-do,
18448 Republic of Ko-rea
- Samsung Electronics. Co., Ltd. (Giheung),
Samsung-ro, Giheung-gu, Yongin-si, Gyeonggi-do,
17113 Republic of Korea

The following buildings are included as part of the physical scope:

Site / Building	Purpose	Asset
Hwaseong Plant/ DSR Building (DSR-B 17 th floor)	Design Center (GDS integration, Ebeam generation and engineer testing)	Design-related Data
Giheung Plant/ SR3 Building (6 th floor)	Test program development	Test program
Giheung Plant/ Line 5 (2 th floor)	Bump Fabrication	Process Data and Spec., Wafers/scrap in TEST mode, Mask (Reticle), Scrap(Reject) Mask
Giheung Plant/ Line 3 (2 th floor)	Wafer EDS Test	Wafer in TEST mode Packaged wafer
Giheung Plant/ SR1 Building (2 th floor)	Data preparation	Data
Hwaseong Plant/ DSR Building (DSR-B 2 nd floor)	Security Operation Center DSR Building	CCTV Records & access control logs
Giheung Plant/ Control Building (2 nd floor)	Security Operation Center Giheung	CCTV Records & access control logs
Giheung Plant/ Line 6 (6 th floor)	Data center Giheung	Production data + test data
Hwaseong Plant/ DSR Building (DSR-B 5 th floor)	Data center DSR Building	Development data

SITE DESCRIPTION

The following services and/or processes provided by Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, Line S3, MR2, SR1, SR3 and DSR-B building) are in the scope of the site evaluation process:

- Giheung:
 - Bump fabrication

- Wafer EDS test
- Test program development
- Data handling and preparation
- Hwaseong:
 - Integration of GDS files for full AP chip
 - GDS file checking and optimization for mask data generation (Ebeam generation)
 - Engineer testing

The process flow of security product fabricated by the site is as follows. The client transfers the encrypted GDS files to Hwaseong DSR-B and then, the GDS integration and the Ebeam generation is performed in this building.

The Ebeam is transferred by SFTP to Giheung SR1 for the data handling and preparation, then it is sent by FTP to customer for the mask production. Depending on the type of mask, they are sent to Giheung Line 5 directly, where the bump fabrication is performed or they are sent to customer first, where the wafer fabrication is performed.

The engineer testing for analyzing in the testing lab room.

Finally, the wafers arrive to Giheung Line 3 where the wafer EDS tests are performed. This test are developed in Giheung SR3.

The complete logical flow explained previously is covered by the SST. In addition, the management of the Security IC modules for AP and IT Security Products processes and the site security are covered by the SST. The product flow of the Security IC modules for AP and IT Security Products on the site starts with the receipt of parts of the TOE (raw materials) up to the yield measurement and handover for shipment of the finished goods for Security IC modules for AP and IT Security Products.

Security Controlled Access: (Security-Guard, IC-Card, CCTV) When the intrusion happened at the external or secured doors using un-authorized IC-Card, the real-time alarm is informed to the Central security system.

Shipment Transport Control: (Access Control, CCTV Surveillance Systems, Patrol Officers). Service and delivery vehicles are tracked and only verified forwarder are used.

Stock Control: Security guard surveillances cover the loading dock 24hours / 7days. Only authorized employees and escorted visitors are permitted to access to the Stock.

Automation Control: Possible human errors during the following life cycle phases of the Security IC modules for Smart Card, NFC (Near field communication) and IT Security Products are fended off by the automation of the handling procedure.

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 Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, Line S3, MR2, SR1, SR3 and DSR-B building) covers the Phase 2 (IC Development) and Phase 3 (IC Manufacturing) 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 ALC certified security assurance components 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.

<Revisar>

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
	ALC_TAT.3 Compliance with implementation standards – all parts

Please note that the evaluation does not cover the ALC_DEL family because the site does not provide deliveries to the end-user. Deliveries from this site are internal and have been evaluated as part of the ALC_DVS.2 family.

Please note that the evaluation scope of this site includes ALC_TAT.3 family, but the dependency with ADV_IMP.1 is partially fulfilled since there is not a specific TOE while evaluating/certifying a site. This work must be completed while evaluating ADV_IMP during the evaluation of a product.

IDENTIFICATION

Site Name	Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, Line S3, MR2, SR1, SR3 and DSR-B building)
Site Location	See section 2.1 of [SST]
Areas in the scope of the certificate as declared in the SST	Refer to section 2.3 Site Description in [SST]
Activities in the product development	Life cycle phases: • Phase 2 (IC Development) • Phase 3 (IC Manufacturing)
Site Security Target	Site Security Target of Samsung Electronics Giheung & Hwaseong Version/Date: Version 1.7/15.02.2025
Evaluation Level	Common Criteria v3.1 R5 To re-use ALC certified security assurance components in evaluations up to EAL6
Security Assurance Components	ALC_CMC.5,ALC_CMS.5,ALC_DVS.2,ALC_LCD.1,ALC_TAT.3,AST_INT.1,AST_CCL.1,AST_SPD.1,AST_OBJ.1,AST_ECD.1,AST_REQ.1,AST_SSS.1.
Attack	High

Potentia I	
---------------	--

SECURITY POLICIES

Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, Line S3, MR2, SR1, SR3 and DSR-B building) 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 4.3 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 4.4 Assumptions.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the site Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, Line S3, MR2, SR1, SR3 and DSR-B building), 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,ALC_TAT.3,AST_INT.1,AST_CCL.1,AST_SPD.1,AST_OB J.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], chapter 4.2 Threats.

DOCUMENTS

The site evaluation has been based on the evidences listed in the chapter 5 (Evaluation evidence) of the Evaluation Technical Report of Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, Line S3, MR2, SR1, SR3 and DSR-B building) [EXT-9592].

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 Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, Line S3, MR2, SR1, SR3 and DSR-B building) 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 evaluation team makes the following security recommendations:

- The evaluation scope of this site does not include ALC_DEL.1 family; however, all the internal deliveries and the deliveries to external sites are covered by the evaluation of ALC_DVS.2 family.
- The evaluation scope of this site includes ALC_TAT.3 family. The dependency with ADV_IMP.1 is partially fulfilled since there is not a specific TOE while evaluating/certifying a site. This work must be completed while evaluating ADV_IMP during the evaluation of a product.
- The evaluation does not cover the ALC_FLR family, as it was not included in the evaluation scope of this site.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the site Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, Line S3, MR2, SR1, SR3 and DSR-B building), 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 30 months after the site audit date as this site has been previously certified by means of an on-site audit by this Certification Body. Therefore, a reassessment of the assurance activities validity should be done before <18/01/2027>.

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 [START]. The reference of the STAR is:

- **Report name:** Site technical audit report (STAR). Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, Line S3, MR2, SR1, SR3 and DSR-B building)
- **Report ID:** CCESAM013R1-STAR-M0.
- **Version:** M0.
- **Issue Date** 14/03/2025
- **Issuing ITSEF:** Applus Laboratories
- **Site audit dates:** 15-17/07/2024.

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 SAMSUNG Electronics Co. Ltd 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 of Samsung Electronics Giheung & Hwaseong, version 1.7.

The public version of this document constitutes the SST Lite. The SST Lite has also been reviewed for the needs of publication according to sanitation [SANT], and it is published along with this certification report in the Certification Body. The SST Lite identifier is:

- Site Security Target-lite of Samsung Electronics Giheung & Hwaseong, version 1.0.

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:

CC v3.1 R5

[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 3. Date 07-11-2019.

[MSSR] Joint Interpretation Library. Minimum site security requirements. Version 3.1, December 2023.

[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 of Samsung Electronics Giheung & Hwaseong, version 1.7.

[START] Joint Interpretation Library. Site Technical Audit Report Template. Version 1.0. February 2018.