



**PREMIER  
MINISTRE**

*Liberté  
Égalité  
Fraternité*

**Secrétariat général de la défense  
et de la sécurité nationale**

Agence nationale de la sécurité  
des systèmes d'information

# Rapport de certification ANSSI-CC-SITE-2025/08

## ST Grenoble

Paris, le 17/11/2025 | 15:25 CET

Vincent Strubel



## AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le site dans les restrictions d'usage définies dans ce même rapport. Les résultats de cette évaluation de site peuvent ainsi être réutilisés par les développeurs de produits qui utilisent ce site dans le cycle de vie de leur produit. Dans tous les cas le rapport devra être utilisé conjointement avec la cible de sécurité du site.

La certification ne constitue pas en soi une recommandation de l'agence nationale de la sécurité des systèmes d'information (ANSSI).

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale  
Agence nationale de la sécurité des systèmes d'information  
Centre de certification  
51, boulevard de la Tour Maubourg  
75700 Paris cedex 07 SP

[certification@ssi.gouv.fr](mailto:certification@ssi.gouv.fr)

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	<b>ANSSI-CC-SITE-2025/08</b>
Nom du site	<b>ST Grenoble</b>
Adresse du site	<b>12 rue Jules Horowitz, BP 217, 38019 Grenoble Cedex – France</b>
Critère d'évaluation et version	<b>Critères Communs version 2022 révision 1</b>
Tâches génériques liées aux critères d'assurance ALC	<b>ALC_CMC.5 ALC_CMS.5 ALC_DVS.2 ALC_LCD.1 ALC_TAT.3 ALC_FLR.2</b>
Commanditaire	<b>STMICROELECTRONICS</b> ZI, 190 avenue Celestin Coq 13106 Rousset CEDEX France
Centre d'évaluation	<b>SERMA SAFETY &amp; SECURITY</b> 14 rue Galilée, CS 10071, 33608 Pessac Cedex, France

## PREFACE

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

La certification de site constitue un sous-ensemble des travaux requis pour une certification de produit.

Les procédures de certification sont disponibles sur le site Internet [cyber.gouv.fr](http://cyber.gouv.fr).

## TABLE DES MATIERES

1	Le projet .....	6
1.1	Identification du site .....	6
1.2	Étapes du cycle de vie .....	6
1.3	Périmètre de l'évaluation.....	6
2	L'évaluation.....	7
2.1	Référentiels d'évaluation .....	7
2.2	Travaux d'évaluation .....	7
3	La certification .....	8
3.1	Conclusion.....	8
3.2	Restrictions d'usage.....	8
ANNEXE A.	Références documentaires du site évalué.....	9
ANNEXE B.	Références liées à la certification .....	10

# 1 Le projet

## 1.1 Identification du site

Les éléments constitutifs du site sont identifiés dans la liste de configuration [CONF].

Le site évalué est le suivant :

ST Grenoble

12 rue Jules Horowitz, BP 217, 38019 Grenoble Cedex – France

## 1.2 Étapes du cycle de vie

Le site de production identifié au paragraphe 1.1 est en charge du développement matériel et des *firmwares*, y compris des activités de test et de validation. Le site héberge également des serveurs de développements.

Les activités suivantes entrent dans le cadre de cette certification :

- développement matériel et *firmware* ;
- tests ;
- validation ;
- hébergement de serveurs de développement ;
- prototypage.

Ce site de production intervient en phase 1, 2 et 4 du cycle de vie décrit par le profil de protection [PP0084].

## 1.3 Périmètre de l'évaluation

Conformément à la cible de sécurité du site [SST], le certificat porte sur le site identifié dans le chapitre 1.1 et couvre les activités listées dans le chapitre 1.2.

## 2 L'évaluation

### 2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2022 révision 1** [CC], à la méthodologie d'évaluation définie dans le manuel [CEM], à [SITE\_CER], et en conformité avec [MSSR].

Les travaux d'évaluation ont été réalisés conformément à [NOTE02]. Cet audit est valide jusqu'au 5 décembre 2027.

### 2.2 Travaux d'évaluation

Le rapport technique d'évaluation du site [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI (voir date en bibliographie), détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation des classes ALC et AST sont à « **réussite** ».

Le guide [GUIDE\_FLR] décrit les modalités de communication au développeur des défauts identifiés par les utilisateurs des produits développés sur ce site.

### 3 La certification

#### 3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le site « ST Grenoble » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [SST] pour les tâches génériques<sup>1</sup> des composants d'assurance ALC\_CMC.5, ALC\_CMS.5, ALC\_DVS.2, ALC\_LCD.1, ALC\_TAT.3 et ALC\_FLR.2.

Toutes les exigences de [MSSR] sont satisfaites.

Ce site, pour les composants d'assurance cités ci-dessus, est donc adapté pour les certifications de produits visant un niveau d'assurance jusqu'à EAL6 augmenté de ALC\_FLR.2. Ce niveau comprend les exigences classiquement requises pour les produits de type microcircuits du domaine « cartes à puces et dispositifs similaires » pouvant faire l'objet d'une reconnaissance selon les accords [SOG-IS]<sup>2</sup> et [CCRA]<sup>3</sup>.

#### 3.2 Restrictions d'usage

Ce certificat porte sur le site spécifié au chapitre 1.1 du présent rapport de certification.

Les utilisateurs de ce site doivent analyser la cohérence de ce présent certificat avec les exigences de développement de leur produit et notamment s'assurer du respect des hypothèses, telles que spécifiées dans la cible de sécurité du site [SST].

---

<sup>1</sup> Des tâches génériques sont des tâches qui peuvent s'effectuer indépendamment d'un produit particulier tel qu'identifié dans [AIS38].

<sup>2</sup> Reconnaissance jusqu'au niveau EAL7 dans le cadre de cet accord.

<sup>3</sup> Reconnaissance jusqu'au niveau EAL2 dans le cadre de cet accord.



**ANNEXE A. Références documentaires du site évalué**

[SST]	Cible de sécurité du site de référence pour l'évaluation : <ul style="list-style-type: none"><li>- <i>Site security target of ST Grenoble</i>, référence SMD_ST_GRENOBLE_SST_25_001, version 2, 12 septembre 2025.</li></ul>
[RTE]	Rapport technique d'évaluation : <ul style="list-style-type: none"><li>- <i>Evaluation Technical Report Site_ST_Grenoble_25 Site Certification project</i>, référence Site_ST_Grenoble_25_ETR_v1.0, version 1.0, 24 septembre 2025.</li></ul> Rapport de réutilisation : <ul style="list-style-type: none"><li>- <i>Site Technical Audit Report ST Grenoble</i>, référence Site_ST_Grenoble_25_STAR_v1.0, version 1.0, 24 septembre 2025.</li></ul>
[CONF]	Liste de configuration du site : <ul style="list-style-type: none"><li>- <i>ST Grenoble Site Certification Configuration List</i>, référence ST_GNB_Certif_Config_List, version 2.0, 14 mars 2025.</li></ul>
[GUIDE_FLR]	Guide utilisateur lié à ALC_FLR : <ul style="list-style-type: none"><li>- <i>CONNECTED SECURITY DEFECTS &amp; CHANGES MANAGEMENT GUIDELINES</i>, référence DM00262458, version 3.0, 5 juin 2023.</li></ul>

**ANNEXE B. Références liées à la certification**

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER-P-01]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0.
[CC]	<p><i>Information technology — Security techniques — Evaluation criteria for IT security</i></p> <ul style="list-style-type: none"> <li>- Part 1: Introduction and general model : ISO/IEC 15408-1:2022 ;</li> <li>- Part 2: Security functional components: ISO/IEC 15408-2:2022 ;</li> <li>- Part 3: Security Assurance components: ISO/IEC 15408-3:2022 ;</li> <li>- Part 4: Framework for the specification of evaluation methods and activities: ISO/IEC 15408-4:2022 ;</li> <li>- Part 5: Pre-defined packages of security requirements: ISO/IEC 15408-5:2022.</li> </ul> <p>Equivalent à la version CCRA :</p> <ul style="list-style-type: none"> <li>- Common Criteria for Information Technology Security Evaluation, version CC:2022, rev. 1, vol. 1 -&gt; 5, ref. CCMB-2022-11-001 -&gt; CCMB-2022-11-005.</li> </ul>
[CEM]	<p><i>Information technology — Security techniques — Evaluation criteria for IT security, ISO/IEC 18045:2022</i></p> <p>Equivalent à la version CCRA :</p> <p><i>Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, version CC:2022, rev. 1, ref. CCMB-2022-11-006</i></p>
[CC-Errata]	<i>Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), ref. 002, version 1.1, 22/07/2024.</i>
[CC2022-Transition]	<i>Transition policy to CC:2022 and CEM:2022, ref. CCMC-2023-04-001, 20/04/2023.</i>
[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.</i>
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.</i>
[MSSR]	<i>Joint Interpretation Library – Minimum Site Security Requirements, version 3.1, décembre 2023.</i>
[SITE_CER]	<i>Site Certification, version 1.0, révision 1, Octobre 2007, référence CCDB-2007-11-001, BSI (Bundesamt für Sicherheit in der Informationstechnik).</i>
[NOTE02]	Note d'application : Visite de l'environnement de développement, ANSSI-CC-NOTE-02, version 6.2, 27 mars 2025.

[PP0084]	<p><i>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014.</i></p> <p>Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-PP-0084-2014.</p>
----------	---