



**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-2026/01

IDQ20MC1
(8214-4657-Wafer1-Split1B)

Paris, le 2/2/2026 | 18:36 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 produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présumées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

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

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

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 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).

Les procédures de certification sont disponibles sur le site Internet www.cyber.gouv.fr.

TABLE DES MATIERES

1	Résumé	5
2	Le produit.....	7
2.1	Présentation du produit.....	7
2.2	Description du produit.....	7
2.2.1	Introduction	7
2.2.2	Services de sécurité.....	7
2.2.3	Architecture	7
2.2.4	Identification du produit.....	7
2.2.5	Cycle de vie	7
2.2.6	Configuration évaluée	7
3	L'évaluation.....	8
3.1	Référentiels d'évaluation	8
3.2	Travaux d'évaluation	8
3.3	Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI	8
4	La certification	9
4.1	Conclusion.....	9
4.2	Restrictions d'usage	9
4.3	Reconnaissance du certificat.....	10
4.3.1	Reconnaissance européenne (SOG-IS).....	10
4.3.2	Reconnaissance internationale critères communs (CCRA)	10
ANNEXE A.	Références documentaires du produit évalué	11
ANNEXE B.	Références liées à la certification	12

1 Résumé

Référence du rapport de certification	ANSSI-CC-2026/01
Nom du produit	IDQ20MC1
Référence/version du produit	8214-4657-Wafer1-Split1B
Type de produit	Cartes à puce et dispositifs similaires
Conformité à un profil de protection	<i>Aucun profil</i>
Critère d'évaluation et version	Critères Communs version CC:2022, révision 1
Niveau d'évaluation	EAL2 augmenté ADV_FSP.4, ADV_TDS.3, ALC_TAT.1, ADV_IMP.1, ATE_DPT.2
Référence du rapport d'évaluation	<i>Evaluation Technical Report (full ETR) - SYRAX</i> <i>LETI.CESTI.SYR.FULL.001-v1.2</i> <i>6 janvier 2026</i>
Fonctionnalité de sécurité du produit	voir 2.2.2 Services de sécurité
Exigences de configuration du produit	voir 4.2 Restrictions d'usage
Hypothèses liées à l'environnement d'exploitation	voir 4.2 Restrictions d'usage
Développeur	ID QUANTIQUE SA Rue Eugène-Marziano 25 CH - 1227 Acacias, Genève, Switzerland
Commanditaire	ID QUANTIQUE SA Rue Eugène-Marziano 25 CH - 1227 Acacias, Genève, Switzerland
Centre d'évaluation	CEA – LETI 17 avenue des martyrs, 38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables



Ce certificat est reconnu au niveau EAL2.

SOG-IS



2 Le produit

2.1 Présentation du produit

Le produit évalué est « IDQ20MC1, en version 8214-4657-Wafer1-Split1B » développé par ID QUANTIQUE SA.

Ce produit est destiné à être utilisé comme générateur de nombres aléatoires dans des satellites artificiels.

2.2 Description du produit

2.2.1 Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

2.2.2 Services de sécurité

Les principaux services de sécurité fournis par le produit sont mentionnés à la section 1.3.1 « *Usage and major security features of the TOE* » de la cible de sécurité.

2.2.3 Architecture

Le produit est constitué d'une source physique de bruit et d'un module de retraitement déterministe, comme illustré en figure 4 de la cible de sécurité.

2.2.4 Identification du produit

La version certifiée du produit est identifiable par les éléments détaillés dans la cible de sécurité [ST] en Table 1 « *IDQ20MC1 TOE reference* ».

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire, selon la procédure d'identification décrite dans les [GUIDES] ; cette procédure comporte par ailleurs des mesures organisationnelles mises en place lors de la livraison de la TOE (TOE Delivery) relatives à l'authenticité du produit.

2.2.5 Cycle de vie

Le cycle de vie du produit est décrit à la section 1.6 « *Target of Evaluation Life Cycle* » de la cible de sécurité. Le point de livraison correspond à l'issue de la phase 4.

2.2.6 Configuration évaluée

Le certificat porte sur les configurations permises par la cible de sécurité, pourvu que les exigences des [GUIDES] soient remplies.

3 L'évaluation

3.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

Pour répondre aux spécificités des cartes à puce et dispositifs similaires, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

3.2 Travaux d'évaluation

Le rapport technique d'évaluation [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 sont à « **réussite** ».

3.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

Le produit comporte un générateur d'aléa ; la cible de sécurité [ST] comporte une SFR FCS_RNG visant la classe PTG.3 définie par [AIS20/31]. Ce générateur a été analysé conformément à la méthode d'évaluation [AIS20/31] ainsi qu'aux dispositions de la note d'application [NOTE-24].

4 La certification

4.1 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 produit soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé (voir chapitre 1 Résumé).

Le certificat associé à ce rapport, référencé ANSSI-CC-2026/01 a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de cinq ans à partir de cette date.

4.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 2.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

4.3 Reconnaissance du certificat

4.3.1 Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



4.3.2 Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires², des certificats Critères Communs.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

² La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - QRNG IDQ20MC1 <i>Security Target</i>, IDQ20MC1_QRNG_ST, v1.18, 5 janvier 2026. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - QRNG IDQ20MC1 <i>Security Target Lite</i>, IDQ20MC1_QRNG_ST_LITE, v1.1, 5 janvier 2026.
[RTE]	Rapport technique d'évaluation : - <i>Evaluation Technical Report (full ETR)</i> SYRAX, LETI.CESTI.SYR.FULL.001 - v1.2, 6 janvier 2026.
[GUIDES]	Les documents référencés en Table 2 de la cible de sécurité.

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, ou les profils de protection, référence ANSSI-CC-CER-P-01, version <Si EUCC> 5.1 <sinon> 5.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[CC]	<i>Information technology — Security techniques — Evaluation criteria for IT security</i> - <i>Part 1: Introduction and general model</i> : ISO/IEC 15408-1:2022 ; - <i>Part 2: Security functional components</i>: ISO/IEC 15408-2:2022 ; - <i>Part 3: Security Assurance components</i>: ISO/IEC 15408-3:2022 ; - <i>Part 4: Framework for the specification of evaluation methods and activities</i>: ISO/IEC 15408-4:2022 ; - <i>Part 5: Pre-defined packages of security requirements</i>: ISO/IEC 15408-5:2022. Equivalent à la version CCRA: <i>Common Criteria for Information Technology Security Evaluation</i>, version CC:2022, révision 1, parties 1 à 5, références CCMB-2022-11-001 à CCMB-2022-11-005.
[CEM]	<i>Information technology — Security techniques — Evaluation criteria for IT security, ISO/IEC 18045:2022</i> Equivalent à la version CCRA: <i>Common Methodology for Information Technology Security Evaluation, Evaluation Methodology</i>, version CC:2022, révision 1, référence CCMB-2022-11-006.
[CC-Errata]	<i>Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1)</i> , référence 002, version 1.1, 22 juillet 2024.
[IIWG IC] *	<i>Mandatory Technical Document – The Application of CC to Integrated Circuits</i> , version 3.0, février 2009.
[IIWG AP] *	<i>Mandatory Technical Document – Application of attack potential to smartcards and similar devices</i> , version 3.2.1, février 2024.
[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security</i> , 2 juillet 2014.

[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates</i> , version 3.0, 8 janvier 2010, Management Committee.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[AIS20/31]	<i>A proposal for: Functionality classes for random number generators</i> , AIS20/AIS31, version 2.0, 18 septembre 2011, BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>).
[NOTE-24]	Note d'application – Evaluation de générateurs d'aléa selon AIS20/31 dans le schéma français, référence ANSSI-CC-NOTE-24, version en vigueur.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.