Section Laboratoires

ATTESTATION D'ACCREDITATION

ACCREDITATION CERTIFICATE

N° 1-6098 rév. 12

Le Comité Français d'Accréditation (Cofrac) atteste que :
The French Committee for Accreditation (Cofrac) certifies that :

SERMA SAFETY AND SECURITY
N° SIREN : 812203479

Satisfait aux exigences de la norme **NF EN ISO/IEC 17025 : 2017**
Fulfils the requirements of the standard

et aux règles d'application du Cofrac pour les activités d'analyses/essais/étalonnages en :
and Cofrac rules of application for the activities of testing/calibration in :

ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / COMPOSANTS ELECTRONIQUES, MICROELECTRONIQUES ET LOGICIELS EMBARQUES
ELECTRONIC, COMPUTING AND TELECOMMUNICATIONS / ELECTRONIC, MICROELECTRONIC COMPONENTS AND EMBARKED SOFTWARE

réalisées par / *performed by* :

SERMA SAFETY & SECURITY
14 rue Galilée
33600 PESSAC

et précisément décrites dans l'annexe technique jointe
and precisely described in the attached technical appendix

L'accréditation suivant la norme internationale homologuée NF EN ISO/IEC 17025 est la preuve de la compétence technique du laboratoire dans un domaine d'activités clairement défini et du bon fonctionnement dans ce laboratoire d'un système de management adapté (cf. communiqué conjoint ISO-ILAC-IAF en vigueur disponible sur le site internet du Cofrac *www.cofrac.fr*)

Accreditation in accordance with the recognised international standard NF EN ISO/IEC 17025 demonstrates the technical competence of the laboratory for a defined scope and the proper operation in this laboratory of an appropriate management system (see current Joint ISO-ILAC-IAF Communiqué available on Cofrac web site www.cofrac.fr) .

Le Cofrac est signataire de l'accord multilatéral d'EA pour l'accréditation, pour les activités objets de la présente attestation.
Cofrac is signatory of the European co-operation for Accreditation (EA) Multilateral Agreement for accreditation for the activities covered by this certificate.

Date de prise d'effet / *granting date :* **21/03/2025**
Date de fin de validité / *expiry date :* **30/09/2029**

Pour le Directeur Général et par délégation
On behalf of the General Director

Le Responsable du Pôle Physique-Mécanique,
Pole manager - Physics-Mechanical,

DocuSigned by:
Stéphane RICHARD
694908483BDE4E5...

La présente attestation n'est valide qu'accompagnée de l'annexe technique.
This certificate is only valid if associated with the technical appendix.

L'accréditation peut être suspendue, modifiée ou retirée à tout moment. Pour une utilisation appropriée, la portée de l'accréditation et sa validité doivent être vérifiées sur le site internet du Cofrac (www.cofrac.fr).
The accreditation can be suspended, modified or withdrawn at any time. For a proper use, the scope of accreditation and its validity should be checked on the Cofrac website (www.cofrac.fr).

Cette attestation annule et remplace l'attestation N° 1-6098 Rév 11.
This certificate cancels and replaces the certificate N° 1-6098 Rév 11.

Seul le texte en français peut engager la responsabilité du Cofrac.
The Cofrac's liability applies only to the french text.

Comité Français d'Accréditation - 52, rue Jacques Hillairet 75012 PARIS
Tél. : +33 (0)1 44 68 82 20 – Fax : 33 (0)1 44 68 82 21 Siret : 397 879 487 00031 www.cofrac.fr

Section Laboratoires

ANNEXE TECHNIQUE

à l'attestation N° 1-6098 rév. 12

L'accréditation concerne les prestations réalisées par :

SERMA SAFETY & SECURITY
14 rue Galilée
33600 PESSAC

Dans son unité :

- CESTI MATERIEL

Elle est accordée selon le périmètre suivant :

 # ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / COMPOSANTS ELECTRONIQUES, MICROELECTRONIQUES ET LOGICIELS EMBARQUES

/ Evaluation de la sécurité des technologies de l'information (LAB REF 14)

Types de produits :

- Composants électroniques, microélectroniques, et leurs logiciels embarqués ;
- Equipements matériels avec boîtiers sécurisés – partie matérielle ;
- Sites de développement ou de fabrication ;

Critères d'évaluation maîtrisés :

- Critères communs version 3.1 et versions antérieures (ISO/IEC 15408) ;
- Critères communs version 2022 (ISO/IEC 15408)

 # ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / COMPOSANTS ELECTRONIQUES, MICROELECTRONIQUES ET LOGICIELS EMBARQUES

/ Essais pour l'évaluation de la cybersécurité des produits TIC (LAB REF 34)

Le laboratoire est reconnu compétent, dans le domaine couvert par la portée générale, pour adopter toute méthode reconnue et pour développer ou mettre en œuvre toute autre méthode dont il aura assuré la validation (FLEX3). La liste exhaustive des méthodes proposées sous accréditation est mise à disposition par le laboratoire

# **ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / COMPOSANTS ELECTRONIQUES, MICROELECTRONIQUES ET LOGICIELS EMBARQUES** / Evaluation de la sécurité des technologies de l'information (LAB REF 14)				
Objet	**Domaine d'application**	**Principe de la méthode**	**Principaux moyens utilisés**	**Référence de la Méthode**
Documents liés à l'environnement de développement (procédures, plans et documents de gestion de configuration, procédures de livraison, procédures d'installation, de génération et de démarrage, documents de sécurité du développement, procédures de correction d'erreurs, modèle et documents de cycle de vie, documents sur les outils de développement)	Politique de sécurité physique et organisationnelle, gestion de configuration	• Vérification de complétude • Analyse de cohérence • Analyse documentaire	/	CEMv3.1 et versions antérieures CEM:2022 JIL - Minimum Site Security Requirements
Sites de développement	Sécurité physique, sécurité logique	Vérification de l'application de procédures	/	CEMv3.1 et versions antérieures CEM:2022 ANSSI Note/02 – "Visite de l'environnement de développement" ANSSI Note/17 – "Réutilisation des composants d'assurance ALC" JIL - Minimum Site Security Requirements

# ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / COMPOSANTS ELECTRONIQUES, MICROELECTRONIQUES ET LOGICIELS EMBARQUES / Evaluation de la sécurité des technologies de l'information (LAB REF 14)				
Objet	**Domaine d'application**	**Principe de la méthode**	**Principaux moyens utilisés**	**Référence de la Méthode**
Documents liés au produit développé (profils de protection, cibles de sécurité, spécifications fonctionnelles, conceptions générales et détaillées, représentations de l'implémentation, modèle de politique de sécurité, structure de la conception, analyses de traçabilité, documentation de tests, analyses de vulnérabilité, guides)	Traçabilité des exigences fonctionnelles de la cible de sécurité	• Vérification de complétude • Analyse de cohérence • Analyse de traçabilité	/	CEMv3.1 et versions antérieures CEM:2022 ICES032 – Methodology for evaluation of CC v3.1 criteria
	Langages informatiques : C, C++, Java, JavaCard, Assembleurs	Analyse de code	Outils d'analyse de code logiciel : Understand C++, Eclipse, … Outils d'analyse de code de matériel (VHDL, Verilog) : HDL Designer	CEMv3.1 et versions antérieures CEM:2022 ICES032 – Methodology for evaluation of CC v3.1 criteria EMVCo – CAST – VCSP
	Langages formels : B, Coq, Isabelle, SPIN	Analyse de conception formelle	Outils d'édition de modèles formels, ProB, AtelierB, Isabelle, Coq, SPIN	CEMv3.1 et versions antérieures CEM:2022 ANSSI Note/12 "Modélisation formelle des politiques de sécurité d'une cible d'évaluation" ICES020 – Methodology for the Evaluation of Formal Models and Proofs
Produit développé	Compétences dans les domaines des systèmes d'exploitation, des réseaux, des architectures de systèmes d'information, de la cryptographie, des systèmes de gestion de base de données, de l'électronique, de la conception des circuits intégrés, des techniques analogiques et logiques, du logiciel embarqué, etc.	Tests fonctionnels	Outils d'exécution de tests, lecteurs de carte, compilateurs et bancs de tests	CEMv3.1 et versions antérieures CEM:2022 ICES032 – Methodology for evaluation of CC v3.1 criteria

Portée d'accréditation générale

# ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / COMPOSANTS ELECTRONIQUES, MICROELECTRONIQUES ET LOGICIELS EMBARQUES / Essais pour l'évaluation de la sécurité des technologies de l'information (LAB REF 34)			
N°	**Objet**	**Caractéristique mesurée**	**Principe de la méthode**
SAGV	Cible de sécurité	Conformité aux exigences des composants CC de la classe ASE	Évaluation de conformité, de complétude et de cohérence
SAGZ	Politique de sécurité physique et organisationnelle Procédures, plans et documents de gestion de configuration Procédures de livraison Procédures d'installation, de génération et de démarrage Documents de sécurité du développement Procédures de correction d'erreurs Modèle de cycle de vie Documentation des outils de développement Sites de développement	Conformité aux exigences des composants CC : ALC_CMC.5 ALC_CMS.5 ALC_DEL.1 ALC_FLR.3 ALC_LCD.2 ALC_TAT.3	Évaluation de la sécurité du cycle de vie et de l'environnement de développement d'un produit Évaluation de la mise en œuvre et de l'efficacité
SAH0	Mesures et dispositifs de sécurité physiques et organisationnels Sites de développements	Conformité aux exigences du composant CC : ALC_DVS.2	Évaluation de la mise en œuvre et de l'efficacité
SAH1	Documentation d'installation, d'administration et d'utilisation	Conformité aux exigences des composants CC : AGD_OPE.1 AGD_PRE.1	Évaluation de la complétude et de la cohérence
SAH2	Documentation technique d'architecture et de design, spécifications fonctionnelles	Conformité aux exigences des composants CC : ADV_ARC.1 ADV_FSP.5 ADV_TDS.5 ADV_INT.3	Évaluation de la conception de haut-niveau (documentation technique)
SAH3	Code source du produit	Conformité aux exigences du composant CC : ADV_IMP.2	Echantillonnage et audit de code
SAH4	Modèles formels Preuves formelles	Conformité aux exigences du composant CC : ADV_SPM.1	Vérification de la modélisation de la politique de sécurité
SAH5	Documentation de tests Résultats des tests fonctionnels	Conformité aux exigences des composants CC : ATE_COV.3 ATE_DPT.4 ATE_FUN.2 ATE_IND.3	Évaluation des procédures et jeux de tests du développeur Tests indépendants
SAH6	Produit	Conformité aux exigences des composants CC : ATE_IND.3 AVA_VAN.2	Tests fonctionnels Analyse de vulnérabilités Tests de robustesse

Portée d'accréditation détaillée

# ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / COMPOSANTS ELECTRONIQUES, MICROELECTRONIQUES ET LOGICIELS EMBARQUES / Essais pour l'évaluation de la sécurité des technologies de l'information (LAB REF 34)			
Référence portée générale	**Objet**	**Principe de la méthode**	**Référence de la méthode**
SAGV	Cible de sécurité	Évaluation de conformité, de complétude et de cohérence	CEM
SAGZ	Politique de sécurité physique et organisationnelle Procédures, plans et documents de gestion de configuration Procédures de livraison Procédures d'installation, de génération et de démarrage Documents de sécurité du développement Procédures de correction d'erreurs Modèle de cycle de vie Documentation des outils de développement Sites de développement	Évaluation de la sécurité du cycle de vie et de l'environnement de développement d'un produit Évaluation de la mise en œuvre et de l'efficacité	CEM MSSR
SAH0	Mesures et dispositifs de sécurité physiques et organisationnels Sites de développements	Évaluation de la mise en œuvre et de l'efficacité	CEM MSSR ANSSI-CC-NOTE-02
SAH1	Documentation d'installation, d'administration et d'utilisation	Évaluation de la complétude et de la cohérence	CEM
SAH2	Documentation technique d'architecture et de design, spécifications fonctionnelles	Évaluation de la conception de haut-niveau (documentation technique)	CEM
SAH3	Langages de description matériel, interprétés, natifs et assembleurs.	Echantillonnage et audit de code Analyse manuelle et automatisée	CEM ANSSI-CC-NOTE-26
SAH4	Modèles formels Preuves formelles	Vérification de la modélisation de la politique de sécurité	CEM ANSSI-CC-NOTE-12
SAH5	Documentation de tests Résultats des tests fonctionnels	Évaluation des procédures et jeux de tests du développeur Tests indépendants	CEM ICES022 – Methodology for evaluation of CC 2022 SAR classes/families out of CEM

# ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / COMPOSANTS ELECTRONIQUES, MICROELECTRONIQUES ET LOGICIELS EMBARQUES / Essais pour l'évaluation de la sécurité des technologies de l'information (LAB REF 34)			
Référence portée générale	**Objet**	**Principe de la méthode**	**Référence de la méthode**
SAH6	Architectures matérielles et logicielles, OS et sécurité applicative (S) : - Architectures matérielles – autres : HSM, POI	Identification de composants génériques sur un PCB Utilisation d'interfaces de *debug* (type JTAG ou UART) Ouverture de boîtiers sécurisés Attaques non-invasives /canaux auxiliaires (consommation électrique, rayonnement électromagnétique, temps d'exécution)	CEM ANSSI-CC-NOTE-19
SAH6	Composants sécurisés et cartes à puces : - Architectures matérielles des composants - Capteurs matériels, technologie réactive - Sécurité des plateformes et applications – Natif, JavaCard, Multos Cryptographie : - État de l'art des mécanismes cryptographiques approuvés	Attaques non-invasives/canaux auxiliaires (consommation électrique, rayonnement électromagnétique, temps d'exécution) Attaques semi-invasives simples (injection de lumière, injection électromagnétique, glitch d'alimentation/de fréquence d'horloge) Attaques invasives : préparation composants et *probing* basiques	CEM ANSSI-CC-NOTE-05 ANSSI-CC-NOTE-23 ANSSI-CC-NOTE-24

[#] *Accréditation rendue obligatoire dans le cadre réglementaire français précisé par le texte cité en référence dans le document Cofrac LAB INF 99 disponible sur www.cofrac.fr*

Date de prise d'effet : **21/03/2025** Date de fin de validité : **30/09/2029**

Cette annexe technique annule et remplace l'annexe technique 1-6098 Rév. 11.

Comité Français d'Accréditation - 52, rue Jacques Hillairet 75012 PARIS
Tél. : +33 (0)1 44 68 82 20 – Fax : 33 (0)1 44 68 82 21 Siret : 397 879 487 00031 www.cofrac.fr