Comité Français d'Accréditation 52, rue Jacques Hillairet 75012 Paris SIRET : 397 897 487 00031 Téléphone : +33 (0)1.44.68.82.20 Site internet : www.cofrac.fr	**Attestation d'accréditation** *Accreditation certificate*	**N° 1-1294** **Rev. 13**

Bénéficiaire / *Beneficiary:* COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
Opérant sous le nom / *Operating as:* CESTI Leti

Identifiant légal / *Legal identifier: N°* 775685019
Adresse / *Address:* CEA-Leti, MINATEC Campus, DRT/LETI/DSYS/SSSEC/CESTI, 17 AVENUE DES MARTYRS, 38054, GRENOBLE Cedex 9, FRANCE

Le Comité Français d'Accréditation (Cofrac) atteste que l'organisme satisfait aux exigences de la norme **NF EN ISO/IEC 17025 : 2017** et aux règles d'application du Cofrac pour son activité Essai / Analyse, pour les activités et sites précisées dans l'annexe technique ci-après, à l'exclusion des activités réalisées dans les pays listés dans le document GEN INF 16, dont la version en vigueur est disponible sur le site internet du Cofrac (www.cofrac.fr). / *The French Committee for Accreditation (Cofrac) certifies that the body fulfils the requirements of the standard* ***NF EN ISO/IEC 17025 : 2017*** *and Cofrac's application rules for its activity of Testing, for the activities and locations described in the following technical annex, excluding activities performed in the countries listed in the document GEN INF 16, the current version of which is available on Cofrac's website (www.cofrac.fr).*

Le Cofrac est signataire de l'accord de reconnaissance multilatéral de l'European co-operation for Accreditation (EA) pour les activités objets de la présente attestation. / *Cofrac is signatory of the European Co-operation for Accreditation (EA) multilateral agreement for the activities covered by this certificate.*
Cette version de l'attestation remplace toute version précédemment émise / *This version of the certificate supersedes all previously issued versions.*
Seul le texte en français engage la responsabilité du Cofrac / *Cofrac's liability applies only on the French text.*

Date de prise d'effet / *Valid from*: **12/03/2026**
Date de fin de validité / *Valid until*: **30/09/2026**

Approuvé par / *Approved by*:

DocuSigned by:
Florence SIMONUTTI
1E72B235B6AD4A0...

L'accréditation peut être retirée, suspendue ou sa portée modifiée 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 withdrawn, suspended or its scope modified at any time. For a proper use the scope of accreditation and its validity should be checked on Cofrac's website (www.cofrac.fr).*

Annexe technique / *Technical annex*

ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / *ELECTRONIC, COMPUTING AND TELECOMMUNICATIONS*

Sites intervenant dans le cadre de l'accréditation de l'organisme / *Locations included in the organisation's accreditation*:

Désignation	**Adresse complète**
CESTI Leti	CEA-Leti, MINATEC Campus, DRT/LETI/DSYS/SSSEC/CESTI, 17 AVENUE DES MARTYRS, 38054, GRENOBLE Cedex 9, FRANCE

CESTI Leti, CEA-Leti, MINATEC Campus, DRT/LETI/DSYS/SSSEC/CESTI, 17 AVENUE DES MARTYRS, 38054, GRENOBLE Cedex 9, FRANCE

# ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / COMPOSANTS ELECTRONIQUES, MICROELECTRONIQUES ET LOGICIELS EMBARQUES / Evaluation de la sécurité des technologies de l'information / LAB REF 34			
Code	**Objet**	**Caractéristiques mesurées ou recherchées**	**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
SAGW	Profils de protection	Conformité aux exigences des composants CC : APE_CCL.1, APE_ECD.1, APE_INT.1, APE_OBJ.2, APE_REQ.2, APE_SPD.1	Évaluation de conformité, de complétude et de cohérence
SAGX	PP-modules et PP-configurations	Conformité aux exigences des composants CC de la classe ACE	Évaluation de conformité, de complétude et de cohérence
SAGY	Cible de sécurité Rapport d'évaluation pour composition	Conformité aux exigences des composants CC : ACO_COR.1 ACO_DEV.2 ACO_REL.2 ACO_CTT.2 ACO_VUL.2	Évaluation de produits en composition

# ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / COMPOSANTS ELECTRONIQUES, MICROELECTRONIQUES ET LOGICIELS EMBARQUES / Evaluation de la sécurité des technologies de l'information / LAB REF 34			
Code	**Objet**	**Caractéristiques mesurées ou recherchées**	**Principe de la méthode**
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.6 ADV_TDS.6 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

# ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / COMPOSANTS ELECTRONIQUES, MICROELECTRONIQUES ET LOGICIELS EMBARQUES / Evaluation de la sécurité des technologies de l'information / LAB REF 34			
Code	**Objet**	**Caractéristiques mesurées ou recherchées**	**Principe de la méthode**
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 ANSSI-NOTE-06 ANSSI-NOTE-09 ANSSI-NOTE-10 PME.4.010
SAGW	Profils de protection		CEM PME.4.010
SAGX	PP-modules et PP-configurations		CEM PME.4.010
SAGY	Cible de sécurité Rapport d'évaluation pour composition	Évaluation de produits en composition	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 ANSSI-NOTE-13 PME.4.010

# **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**
SAH0	Mesures et dispositifs de sécurité physiques et organisationnels Sites de développements	Évaluation de la mise en œuvre et de l'efficacité	CEM ANSSI-NOTE-02 ANSSI-NOTE-17 JIL MSSR PME.4.007
SAH1	Documentation d'installation, d'administration et d'utilisation	Évaluation de la complétude et de la cohérence	CEM PME.4.010
SAH2	Documentation technique d'architecture et de design, spécifications fonctionnelles	Évaluation de la conception de haut-niveau (documentation technique)	CEM PME.4.010
SAH3	Langages C/C++, Java Card, assembleur	Echantillonnage et audit de code Analyse manuelle et automatisée	CEM PME.4.011 PME.4.014 PME.4.021
SAH4	Modèles formels Preuves formelles	Vérification de la modélisation de la politique de sécurité	CEM ANSSI-NOTE-12 PME.4.010 PME.4.018
SAH5	Documentation de tests Résultats des tests fonctionnels	Évaluation des procédures et jeux de tests du développeur Tests indépendants	CEM PME.4.010
SAH6	Générateurs physiques de nombres aléatoires Algorithmes de comparaison biométrique	Tests fonctionnels Tests statistiques	ANSSI-NOTE-05 PME.4.012 PME.4.019 ANSSI-NOTE-24

# **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	Cryptographie État de l'art des mécanismes cryptographiques approuvés	Analyse cryptographique	RGS SOG-IS Agreed Cryptographic Mechanims PME.4.009
SAH6	Composants sécurisés et cartes à puces Architectures matérielles des composants	Techniques d'attaques maitrisées [A1] Tests fonctionnels Analyse de vulnérabilités Attaques non-invasives Attaques semi-invasives Attaques invasives	JIL Application of Attack Potential to smartcards
SAH6	Composants sécurisés et cartes à puces Sécurité des plateformes et applications Natif, JavaCard	Techniques d'attaques maitrisées [A2] Tests fonctionnels Analyse de vulnérabilités Attaques non-invasives Attaques semi-invasives Attaques invasives Attaques logicielles, Java Card	JIL Application of Attack Potential to smartcards
SAH6	Equipement matériel avec boîtiers sécurisés Hardware Security Module (HSM)	Techniques d'attaques maitrisées [A3] Tests fonctionnels Analyse de vulnérabilités Ouverture de boîtiers sécurisés Attaques non-invasives Attaques semi-invasives Attaques invasives Attaques logicielles	JIL Application of Attack-Potential to Hardware Devices with Security Boxes

FLEX3 : 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.

Accréditation rendue obligatoire dans le cadre réglementaire français. # Mandatory accreditation in the French legislative framework.

La liste détaillée des prestations réalisées par l'organisme est disponible sur le site internet www.cofrac.fr ou directement auprès de l'organisme.