Nomenclature et expression des lignes de portée d'accréditation pour les essais en vue de l'évaluation de la cybersécurité des produits TIC dans le cadre du schéma de certification européen EUCC

LAB INF 34 - Révision 00

Préambule

L'objectif de ce document d'information élaboré par des experts des essais concernés est de proposer une nomenclature des essais pouvant servir de base à l'élaboration des portées d'accréditation des laboratoires réalisant des essais en vue de l'évaluation de la sécurité des technologies de l'information dans le cadre du schéma de certification européen EUCC ou candidats à l'accréditation, pour le niveau d'assurance « substantiel ».

L'accréditation est délivrée pour une portée définie par le laboratoire correspondant à ses besoins et suivant les différentes options décrites dans le document LAB REF 08 (expression et évaluation des portées d'accréditation).

Les portées de ce document d'information ne sont pas exhaustives.

Les champs grisés sont à préciser par le laboratoire.

Portée flexible FLEX3

Portée d'accréditation générale

# ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / COMPOSANTS ELECTRONIQUES, MICROELECTRONIQUES ET LOGICIELS EMBARQUES / Essais pour l'évaluation de la cybersécurité des produits TIC (LAB REF 34)				Portée minimale attendue
N°	**Objet**	**Caractéristique mesurée**	**Principe de la méthode**	**Caractéristique mesurée**
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.x, APE_ECD.x, APE_INT.x, APE_OBJ.x, APE_REQ.x, APE_SPD.x		APE_CCL.1, APE_ECD.1, APE_INT.1, APE_OBJ.2, APE_REQ.2, APE_SPD.1
SAGX	PP-modules et PP-configurations	Conformité aux exigences des composants CC de la classe ACE		/
SAGY	Cible de sécurité Rapport d'évaluation pour composition	Conformité aux exigences des composants CC : ACO_COR.x ACO_DEV.x ACO_REL.x ACO_CTT.x ACO_VUL.x	Évaluation de produits en composition	ACO_COR.1, ACO_DEV.2, ACO_REL.2, ACO_CTT.2, ACO_VUL.2.

# ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / COMPOSANTS ELECTRONIQUES, MICROELECTRONIQUES ET LOGICIELS EMBARQUES / Essais pour l'évaluation de la cybersécurité des produits TIC (LAB REF 34)				Portée minimale attendue
N°	**Objet**	**Caractéristique mesurée**	**Principe de la méthode**	**Caractéristique mesurée**
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.x ALC_CMS.x ALC_DEL.x ALC_FLR.x ALC_LCD.x ALC_TAT.x	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	ALC_CMC.3 ALC_CMS.3 ALC_DEL.1 ALC_FLR.1 ALC_LCD.1
SAH0	Mesures et dispositifs de sécurité physiques et organisationnels Sites de développements	Conformité aux exigences du composant CC : ALC_DVS.x	Évaluation de la mise en œuvre et de l'efficacité	ALC_DVS.1
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.x ADV_FSP.x ADV_TDS.x ADV_INT	Évaluation de la conception de haut-niveau (documentation technique)	ADV_ARC.1 ADV_FSP.3 ADV_TDS.2
SAH3	Code source du produit	Conformité aux exigences du composant CC : ADV_IMP.x	Echantillonnage et audit de code	/
SAH4	Modèles formels Preuves formelles	Conformité aux exigences du composant CC : ADV_SPM.x	Vérification de la modélisation de la politique de sécurité	/

# ELECTRONIQUE, INFORMATIQUE ET TELECOMMUNICATIONS / COMPOSANTS ELECTRONIQUES, MICROELECTRONIQUES ET LOGICIELS EMBARQUES / Essais pour l'évaluation de la cybersécurité des produits TIC (LAB REF 34)				Portée minimale attendue
N°	**Objet**	**Caractéristique mesurée**	**Principe de la méthode**	**Caractéristique mesurée**
SAH5	Documentation de tests Résultats des tests fonctionnels	Conformité aux exigences des composants CC : ATE_COV.x ATE_DPT.x ATE_FUN.x ATE_IND.x	Évaluation des procédures et jeux de tests du développeur Tests indépendants	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
SAH6	Produit	Conformité aux exigences des composants CC : ATE_IND.x AVA_VAN.2	Tests fonctionnels Analyse de vulnérabilités Tests de robustesse	/

L'accréditation est délivrée également selon la norme ISO/IEC TS 23532-1 "Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences relatives aux compétences des laboratoires d'essais et d'évaluation de la sécurité TI — Partie 1 : Évaluation pour l'ISO/IEC 15408", en tant que référentiel d'accréditation complémentaire applicable, en plus de la norme NF EN ISO/IEC 17025.

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 Méthode et/ou outil mis en œuvre [à définir par le laboratoire]
SAGW	Profils de protection		CEM Méthode et/ou outil mis en œuvre [à définir par le laboratoire]
SAGX	PP-modules et PP-configurations		CEM Méthode et/ou outil mis en œuvre [à définir par le laboratoire]
SAGY	Cible de sécurité Rapport d'évaluation pour composition	Évaluation de produits en composition	CEM Méthode et/ou outil mis en œuvre [à définir par le laboratoire]
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 Méthode et/ou outil mis en œuvre [à définir par le laboratoire]
SAH0	Mesures et dispositifs de sécurité physiques et organisationnels Sites de développements	Évaluation de la mise en œuvre et de l'efficacité	CEM Méthode et/ou outil mis en œuvre [à définir par le laboratoire]

# 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**
SAH1	Documentation d'installation, d'administration et d'utilisation	Évaluation de la complétude et de la cohérence	CEM Méthode et/ou outil mis en œuvre [à définir par le laboratoire]
SAH2	Documentation technique d'architecture et de design, spécifications fonctionnelles	Évaluation de la conception de haut-niveau (documentation technique)	CEM Méthode et/ou outil mis en œuvre [à définir par le laboratoire]
SAH3	Langages [à définir par le laboratoire]	Echantillonnage et audit de code [à définir par le laboratoire] Analyse manuelle ou automatisée	CEM Méthode et/ou outil mis en œuvre [à définir par le laboratoire]
SAH4	Modèles formels Preuves formelles	Vérification de la modélisation de la politique de sécurité	CEM Méthode et/ou outil mis en œuvre [à définir par le laboratoire]
SAH5	Documentation de tests Résultats des tests fonctionnels	Évaluation des procédures et jeux de tests du développeur Tests indépendants	CEM Méthode et/ou outil mis en œuvre [à définir par le laboratoire]
SAH6	Technologies mises en œuvre dans les produits évalués [à définir par le laboratoire – cf. tableau ci-dessous]	Techniques d'attaques maitrisées [A1] Recherche de vulnérabilités génériques Fuzzing Utilisation d'exploits publics Développements d'exploits basiques	CEM Méthode et/ou outil mis en œuvre [à définir par le laboratoire]
SAH6	Technologies mises en œuvre dans les produits évalués [à définir par le laboratoire – cf. tableau ci-dessous]	Techniques d'attaques maitrisées [A2] 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 Méthode et/ou outil mis en œuvre [à définir par le laboratoire]

# 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	Technologies mises en œuvre dans les produits évalués [à définir par le laboratoire – cf. tableau ci-dessous]	Techniques d'attaques maitrisées [A3] 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 Méthode et/ou outil mis en œuvre [à définir par le laboratoire]

Identification des types de technologies :

	Types de technologies		
Architectures matérielles et logicielles, OS et sécurité applicative (S)	1	Architectures matérielles	X86, ARM, autres (à préciser)
	2	Sécurité des postes de travail et serveurs	Windows/linux/BSD, autres (à préciser)
	3	Systèmes embarqués, micronoyaux	TEE, OS temps réel, autres (à préciser)
	4	Virtualisation	VMware, Microsoft, Citrix, autres (à préciser)
	5	Sécurité applicative	A préciser
	6	Bases de données	A préciser
	7	Technologies web	A préciser
Réseau & sans-fil (N)	1	Protocoles réseau	tcp, udp, ip, dhcp etc.
	2	Protocoles communication	ssh, https etc.
	3	Bas-niveau	USB, SPI, autres (à préciser)
	4	Sans-fil	Wifi, BlueTooth/BLE, NFC, LoRa, ZigBee, autres (à préciser)
	5	Protocoles composants	SCP GlobalPlatform, TCG, autres (à préciser)
	6	Téléphonie et VoIP	
	7	Réseaux mobiles 3/4/5G	
	8	Filtrage	
	9	Détection d'intrusion	
Composants sécurisés et cartes à puces (H)	1	Architectures matérielles des composants	
	2	Capteurs matériels, technologie réactive	
	3	Sécurité des plateformes et applications	Natif, JavaCard, Multos, autres (à préciser)
Cryptographie (C)	1	État de l'art des mécanismes cryptographiques approuvés	