PROJET version 00 rev_7

PROGRAMME D'ACCREDITATION POUR DES TESTS SUR LES CARTES A PUCE IAS ET LECTEURS ASSOCIES

Document LAB REF 2X

Révision 00 – Mois 2007

Section Laboratoires

SOMMAIRE

1 OBJET DU DOCUMENT

L'objet du document est de définir les exigences techniques à satisfaire dans le cadre du programme de conformité en vue du référencement des cartes à puce basées sur le socle IAS, et lecteurs associés par la Direction Générale de la Modernisation de l'Etat (DGME), et ce, en accord avec les textes réglementaires en vigueur en vue d'obtenir l'accréditation pour ces activités : décret XXX ou arrêté n°XXX.

2 REFERENCES BIBLIOGRAPHIQUES ET DEFINITIONS

2.1 REFERENCES BIBLIOGRAPHIQUES

Le présent document fait référence ou s'appuie sur les documents suivants :

- NF EN ISO/CEI 17025 (2005) : Prescriptions générales concernant la compétence des laboratoires d'étalonnages et d'essais,
- LAB Réf 02 (révision 03 – novembre 2006) : Accréditation des laboratoires selon la norme NF EN ISO/CEI 17025 – Prescriptions,
- PKCS #11 : Public-Key Cryptographic Standard #11,
- MS-CAPI : Microsoft CryptoAPI,
- ISO/CEI 10373-1 (1998) : Identification cards – Test methods – General characteristics tests,
- ISO/CEI 10373-3 (2001) : Identification cards – Test methods – Integrated circuit(s) cards with contacts and related interface devices (§ 1-5),
- ISO/CEI 7816-1 (1998) : Identification cards -- Integrated circuit(s) cards with contacts - Part 1 : Physical Characteristics,
- ISO/CEI 7816-2 (1999) : Identification cards -- Integrated circuit(s) cards with contacts - Part 2 : Dimensions and location of the contacts,
- ISO/CEI 7816-3 (1997) : Identification cards -- Integrated circuit(s) cards with contacts - Part 3 : Electronic signals and transmission protocols,
- EMV2000 : ICC Specification for Payment Systems - Book 1 – Version,
- Spécifications générales « IAS Contact Niveau 1 » et références des méthodes de test associées disponibles sur le site de la DGME (www.synergies.modernisation.gouv.fr),
- Plate-forme commune pour l'e-administration rév 1.01 Premium disponible sur le site du Gixel (www.gixel.fr).

2.2 DEFINITIONS

Pour les besoins du présent document les termes et définitions ci-après s'appliquent :

- carte à puce : carte au format ISO ID-1, conforme aux normes ISO/CEI 7816-1, -2 et -3, intégrant au moins un microcontrôleur et fournissant des capacités de calculs cryptographiques et de stockage d'information

- lecteur : appareil électronique acceptant des cartes à puce et faisant l'interface pour sa lecture

- lecteur transparent contact IAS : lecteur transparent à contact, avec ou sans PIN/PAD PC/SC 2.0

- middleware : logiciels présents sur un ordinateur, pilotant la carte à puce et offrant des interfaces standards (MS-CAPI, PKCS#11…) pour les applications

- e-administration : ensemble des acteurs et moyens permettant la dématérialisation des procédures administratives.

- PKCS#11 : standard développé par RSA Laboratories en coopération avec un consortium, auquel participent Apple, Microsoft, DEC, Sun, MIT et Lotus ; PKCS#11 définit une interface de programmation indépendante de la technologie, appelée Cryptoki, pour des matériels comme des cartes à puce ou des cartes PCMCIA.

2.3 SIGLES

- DGME : Direction Générale de la Modernisation de l'Etat,
- ADELE : ADministration ELEctronique,
- APDU : Application Protocol Data Unit,
- ATR : Answer to Reset,
- CNIe : Carte Nationale d'Identité Electronique,
- CVQ : Carte de Vie Quotidienne,
- I/O : Input/Output,
- MS-CAPI : Microsoft CryptoAPI,
- IAS : Identification/Authentification/Signature,
- PC/SC : Personal Computer / Smart Card,
- PCD : Proximity Coupling Device,
- PKCS : Public Key Crytographic Standard,
- PICC : Proximity Integrated Circuit Card,
- PIN/PAD : Personal Identification Number / PIN Accepting Device,
- PPS : Protocol Parameters Selection,
- RST : Reset,
- Vcc ; Tension d'alimentation en courant continu.

3 DOMAINE D'APPLICATION

Le champ d'application du présent programme concerne les méthodes d'essais à mettre en œuvre dans le cadre du programme de conformité en vue du référencement par la DGME des cartes à puce IAS, et lecteurs associés. Ce programme s'adresse :

- aux laboratoires d'essais sur les cartes à puce IAS, et lecteurs associés accrédités ou candidats à l'accréditation ;
- aux auditeurs du Cofrac, et constitue une base d'harmonisation à leur usage ;
- aux membres des instances décisionnelles du Cofrac (Comité de Section, Commission Technique d'Accréditation "Electricité - Rayonnements - Technologies de l'Information", Commission Interne d'Examen des Rapports d'Audit).

Ce programme correspond à l'état des référentiels de test au jour de sa sortie. Il est de la responsabilité du laboratoire d'essais de prendre en compte les évolutions des référentiels de test lors de l'utilisation du présent programme.
Les référentiels de tests et les spécifications en vigueur sont disponibles sur le site de la DGME.

4 MODALITES D'APPLICATION

Ce programme est applicable à compter du XXX

5 SYNTHESE DES MODIFICATIONS

Il s'agit de la première version du document, aucune marque de modification n'est donc indiquée.

6 MODALITE DE REEXAMEN

Les dispositions du présent document seront amenées à être modifiées ou complétées, pour tenir compte de l'évolution des pratiques et de "l'état de l'art", notamment techniques. A ce titre, ce document est revu au moins tous les 3 ans et révisé si nécessaire par la section Laboratoires.

7 EXIGENCES DU PROGRAMME

L'aptitude d'un laboratoire à être accrédité par le Cofrac au titre du présent programme est examinée au regard du respect :

- des exigences générales relatives à la compétence des laboratoires d'essais contenues dans la norme NF EN ISO/CEI 17025 et les prescriptions du document Cofrac LAB Ref 02
- des référentiels de tests détaillés au § 8 du présent document,
- au regard des exigences particulières définies en collaboration avec la DGME.

Chaque ligne numérotée du tableau du § 8 constitue un tout indissociable correspondant à un test. Le laboratoire a le choix des lignes donc des tests pour lesquels il postule à une accréditation.

Un laboratoire accrédité pour les tests d'intéropérabilité sur les cartes à puces (respectivement sur les lecteurs) prononce la conformité globale de l'échantillon en s'appuyant sur les résultats des rapports d'essais émis par les laboratoires accrédités pour les autres tests sur les cartes (respectivement sur les lecteurs).
(Exigence à justifier en regard du document Cofrac LAB REF 02)

8 REFERENTIELS DE TESTS

N°	Objet soumis à essai	Caractéristiques mesurées ou testées	Principe de la méthode de test et principaux moyens d'essais utilisés		Spécifications générales	Référence de la méthode de test
1	Carte à puce à contact *(15 cartes profil ADELE 1 ou 2)*	Tests de post-caractérisation électrique:	Méthode d'essai sur composant masqué	Banc de tests : Lecteur et instruments de mesure	IAS CONTACT NIVEAU 1	IAS CARTE POST-CARACTERISATION
2	Carte à puce à contact *(2 cartes profil ADELE 1 ou 2)*	Caractéristiques électriques : • Vcc : tension min/max, courant max • Clk :rapports cycliques min/max • Clk, Rst, I/O : temps de montée + niveaux min/max	Exécution de scripts Interprétation des résultats	Simulateur de lecteur Instruments de mesure	IAS CONTACT NIVEAU 1	IAS CARTE ELECTRIQUE
3	Carte à puce à contact *(2 cartes profil ADELE 1 ou 2)*	Caractéristiques protocolaires : • Réponse au reset • Protocole T=0 ou T=1 • PPS	Exécution de scripts Interprétation des résultats	Simulateur de lecteur Instruments de mesure	IAS CONTACT NIVEAU 1	IAS CARTE PROTOCOLAIRE
4	Carte à puce à contact *(50 cartes profil IAS)*	Caractéristiques fonctionnelles : • Tests nominaux • Tests des cas d'erreurs • Tests destructifs	• Emission d'APDU vers la carte et réception des réponses. • Vérification de la réponse obtenue par rapport à la réponse attendue.	• PC avec lecteur de référence et carte réelle • Application pour émission / réception d'APDU • Outil de	Spécification IAS : Plateforme commune pour l'e-administration rév 1.01 Premium	IAS CARTE FONCTIONNEL Validation du cycle de vie Commandes administratives Commandes associées au système de fichiers Commandes applicatives

N°	Objet soumis à essai	Caractéristiques mesurées ou testées	Principe de la méthode de test et principaux moyens d'essais utilisés		Spécifications générales	Référence de la méthode de test
				comparaison • Simulateur de carte (générateur de profil d'usage) • Librairie cryptographique de référence • Générateur de signaux • Appareil pour mesurer le temps d'exécution des APDU		Commandes liées à l'authentification Services cryptographiques Génération de clés, nombres aléatoires Intégrité (mode transactionnel) Définition générique de la carte (liste des fichiers, contenu et attributs des fichiers, applications) Messages d'erreur (comportement du produit, conformité des codes) Blocage de la carte (self-test) Validation de la fin de vie de la carte
5	Carte à puce à contact *(10 cartes profil ADELE1, 10 cartes profil ADELE2)*	Tests d'interopérabilité : Fonctionnement de la carte en environnement approuvé	Exécution de transactions	Panel de lecteurs de référence et middleware IAS	Spécification IAS : Plateforme commune pour l'e-administration rév 1.01 Premium	IAS INTER-OPERABILITE

N°	Objet soumis à essai	Caractéristiques mesurées ou testées	Principe de la méthode d'essai ou de test et principaux moyens d'essais utilisés		Spécifications générales	Référence de la méthode	Limites d'adaptation de la méthode
6	Lecteur transparent contact IAS *(3 lecteurs transparents)*	Tests mécaniques : • Acceptation des sondes • Pression des contacts	Mesures directes	Banc de tests : • Sondes aux dimensions max (embossage) et min • Capteur de mesure d'effort	IAS CONTACT NIVEAU 1	IAS LECTEUR MECANIQUE	Non applicable (portée 1)
7	Lecteur transparent contact IAS *(3 lecteurs transparents)*	Tests électriques : • Court-circuit • Séquences d'activation, de désactivation et de reset • Caractéristiques des signaux Clk, Vcc, Rst, I/O	Mesures : • directes • indirectes • à l'oscilloscope	Banc de tests : • Simulateur de cartes • Oscilloscope	IAS CONTACT NIVEAU 1	IAS LECTEUR ELECTRIQUE	Non applicable (portée 1)
8	Lecteur transparent contact IAS *(3 lecteurs transparents)*	Tests protocolaires : • ATR • PPS • Protocole T=0 ou T=1	Mesures indirectes Interprétation du résultat	Banc de tests : • Simulateur de cartes	IAS CONTACT NIVEAU 1	IAS LECTEUR PROTOCOLAIRE	Non applicable (Définir tests PPS pour une portée 1)
9	Lecteur transparent contact IAS *(3 lecteurs transparents)*	Tests d'interopérabilité : Fonctionnement du lecteur en environnement approuvé	Exécution de transactions	Banc de tests : • Panel de cartes et middleware IAS	IAS INTER-OPERABILITE	IAS INTER-OPERABILITE	Ajout de cartes et de lecteurs de référence