Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère du budget, des comptes publics et de la fonction publique

==========

Référentiel de Tests
Cartes – Lecteurs IAS

IAS Interopérabilité

==========

VERSION 1.0

Référentiel de Tests Cartes - Lecteurs IAS	
IAS Interopérabilité	
Référence	**Date**
IAS INTEROPERABILITE V1 0.doc	15/11/2007
Identification d'objet (OID)	**Racine OID et gestionnaire**
1.2.250.1.137.2.3.3.6.1	1.2.250.1.137.2.3.3.6.1 SDAE
Responsable	**Version**
DGME/SDAE	**V1.0**
Critère de diffusion	**Nombre de pages**
PUBLIC	29

HISTORIQUE DES VERSIONS			
15/11/2007	1.0	Version initiale	DGME/SDAE FIME GIXEL

SOMMAIRE

1. Introduction

1.1. Présentation générale

Le Référentiel de Tests Cartes – Lecteurs IAS est un ensemble de documents décrivant les spécifications des tests que doivent passer avec succès les cartes et les lecteurs pour pouvoir être référencés.

Les produits référencés peuvent être utilisés pour accéder à l'ensemble des téléservices de l'administration électronique qui nécessitent l'utilisation de tels produits.

Ne peuvent être référencés que les produits conformes aux spécifications d'interopérabilité et de sécurité contenues dans le [RGI] et le [RGS] qui les concernent.

Le Référentiel de Tests Cartes – Lecteurs IAS ne porte que sur la conformité à des spécifications techniques.

Les tests de conformité des cartes et des lecteurs IAS doivent être exécutés par un laboratoire de tests accrédités par le Cofrac selon la norme NF EN ISO/CEI 17025 plus le programme d'accréditation correspondant.

Le Référentiel de Tests Cartes – Lecteurs IAS est le résultat d'un groupe de travail composé de membres du Gixel (Axalto, Gemplus, Oberthur Card Systems, Sagem), de FIME, du GIE SESAM Vitale et du DGME/SDAE.

Le but de ce document est de présenter les tests d'interopérabilité IAS (Carte et lecteur). A cet effet, la méthodologie, l'environnement de tests et plusieurs cas de tests proches d'une utilisation réelle, sont décrits.

1.2. Sigles

ADELE ADministration Electronique

ATR Réponse au reset (Answer To Reset)

Cofrac Comité Français d'Accréditation

DGME Direction Générale pour la Modernisation de l'Etat

GIXEL Groupement des Industriels de la Carte

IAS Identification, Authentification & Signature.

O.S. Système d'exploitation (Operating System)

PC Ordinateur compatible PC (Personal Computer)

SDAE Service du Développement de l'Administration Electronique

1.3. Définitions

Analyse	traitement d'un ensemble de données
Application	programme client ou serveur fournissant des fonctions de sécurité
Carte	support embarquant un microcontrôleur
Comité technique	comité constitué des membres ayant participé à l'écriture de ce référentiel de test et qui en assure la maintenance
Elément	élément de la plateforme de test
Elément de preuve	éléments enregistrés qui prouvent le résultat observé
Etat de livraison	état d'un produit à la livraison par le soumissionnaire ou l'industriel
Etat de référence	état d'un produit au démarrage de l'ensemble des tests
Etat initial	état d'un produit au démarrage d'un test
Inspection	examen visuel d'une application ou d'un document
Lecteur	dispositif permettant de lire des cartes
Middleware	élément logiciel qui permet de mettre en relation les applications clientes et la carte
Plateforme	ensemble des éléments matériels et logiciels permettant d'effectuer les tests
Téléservice	accès dématérialisé à une procédure d'administration
Test	exécution d'une application utilisant un équipement pour collecter les données à traiter

2. Méthodologie

2.1. Pré requis à la présentation d'un produit en test d'interopérabilité

Le produit carte doit avoir passé avec succès les tests suivants, prévus dans ce programme :

- Test de post-caractérisation électrique
- Tests électriques (tension, courant, rapport cyclique & temps de montée, court-circuit, reset et signaux)
- Tests protocolaires (ATR, type de protocole, PPS)
- Tests fonctionnels (tests nominaux, de cas d'erreurs et destructifs)

10 cartes personnalisées : [Profil ADELE 1] et 10 cartes personnalisées : [Profil ADELE 2] doivent être fournies.

Le produit lecteur doit avoir passé avec succès les tests suivants, prévus dans ce programme :

- Tests mécaniques (acceptation des sondes et pression des contacts, EMVCo Type Approval - Terminal Level 1 - Test cases)
- Tests électriques (tension, courant, rapport cyclique & temps de montée, court-circuit, reset et signaux)
- Tests protocolaires (ATR, type de protocole, PPS)

3 lecteurs doivent être fournis.

2.2. Formation au produit

A la demande du laboratoire de test, un support pourra être assuré, gratuitement, pendant la durée des tests par l'émetteur, sur les fonctionnalités du produit à tester.

2.3. Méthodes de vérification

Les résultats obtenus sont comparés aux résultats attendus et les éléments de preuve sont enregistrés.

Différentes cartes, lecteurs ou version de middleware sont utilisés et font appel à différentes techniques :

- Analyse (Génération et traitement de l'information)
- Démonstration
- Inspection (Documentation par rapport aux résultats obtenus)
- Test

2.4. Structure des tests

La structure des tests est construite selon le schéma suivant :

- Identification du test.
- Référence au point testé.
- Objectif du test.

- Configuration initiale et finale du test.
- Etat de référence du produit.
- Opération effectuée.
- Résultat attendu.
- Résultat observé.
- Eléments de preuve.
- Action en cas d'anomalie (*).

(*) Les actions seront traitées au cas par cas

2.5. Stratégie de test et enregistrement des éléments de preuves

Pour chaque test, le produit est supposé être dans un état de référence puis initial correspondant au besoin du test à exécuter. A l'issue du test, il est sensé être remis si possible à nouveau dans l'état de référence (hors tests destructifs).

Pour chaque test, la trace de l'exécution est mémorisée. Elle contient les opérations faites en préambule au test, pour amener le produit dans une configuration représentative du test, les opérations faites durant le test et les opérations faites en post ambule pour remettre le produit dans un état connu.

Les opérations manuelles effectuées sur la plateforme de référence seront aussi mémorisées.

2.6. Décision d'entrée du matériel testé dans le parc de référence

En fonction des résultats obtenus et de la représentativité du produit, le service en charge du référencement prendra la décision de son entrée ou non dans le parc de référence.

3. Environnement de test

3.1. Définition

Les tests sont effectués dans un environnement de laboratoire, c'est-à-dire :

- à température ambiante : 15-35°C
- à humidité ambiante : 30-70% humidité
- à pression atmosphérique : 860-1060 mbar
- sans interférences C.E.M.

Les tests ne prennent pas en compte les conditions d'utilisation extrême.

3.2. Matériels de la plateforme

Il n'est pas prévu de solution client/serveur utilisant un réseau externe pour valider la notion de téléservice. Le réseau utilisé sera indépendant et autonome. Seuls seront disponibles, un serveur de mail et un serveur http afin d'assurer la transmission de mails et la navigation internet.

La plateforme est constituée d'un ensemble de configurations différentes.

Chaque configuration comprendra au minimum :

- un ordinateur compatible PC/MAC/Linux, comprenant une interface PCMCIA et USB
- un lecteur de carte
- une carte IAS personnalisée avec un des profils demandés.

Pour être à jour, la plateforme devra contenir l'ensemble des configurations définies dans le plan de test.

3.3. Matrice de la plateforme d'interopérabilité

Les cartes et les lecteurs seront testés sur les 6 configurations décrites ci-dessous :

		Config 1	Config 2	Config 3	Config 4	Config 5	Config 6
OS		Windows Vista	Windows XP SP2	Windows 2000	MAC OS X 10.4	Linux Mandriva 2007	Linux Ubuntu 7.10
Navigateur		Internet Explorer 7.0	Internet explorer 6.0 SP1	Internet explorer 6.0 SP1	-	-	-
		Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1
Messagerie		Outlook 2003 Thunderbird 1.5.0.4	Outlook 2003 Thunderbird 1.5.0.4	Outlook Express v6 Thunderbird 1.5.0.4	Thunderbird 1.5.0.4	Mozilla Thunderbird v1.5.0.9	Mozilla Thunderbird v1.5.0.9
Application		**Application de test**					
Module crypto	**PKCS#11**	Oui	Oui	Oui	**Oui**	Oui	Oui
	CSP	Oui	Oui	Oui	**Non**	**Non**	**Non**
	IAS API	Oui	Oui	Oui	**Oui**	Oui	Oui
Profil Cartes		**Profil ADELE 1 et Profil Adèle 2**					

Figure 1 : Matrice de test interopérabilité

Dans le cas du test d'une nouvelle carte en cours référencement, celle-ci sera testée avec l'ensemble des lecteurs déjà référencés.

Dans le cas du test d'un nouveau lecteur en cours référencement, celui-ci sera testé avec l'ensemble des cartes IAS déjà référencées.

A la date de la publication de ce document, les versions des logiciels à utiliser sont listées dans le tableau ci-dessus. Ces versions pourront être modifiées par le comité technique.

La gestion et la traçabilité de la version des logiciels utilisés seront assurées (version des logiciels décrits ci-dessus avec la version du middleware correspondant au système d'exploitation et sa version).

3.4. Plateforme

La plateforme est installée indépendamment des produits à tester et de la mise à jour des panels décrits ci-dessous.

La désinstallation des lecteurs et de leurs pilotes devra s'effectuer de manière complète, c'est-à-dire qu'aucun fichier résiduel ne doit subsister sur le PC après une désinstallation. Ceci est de la responsabilité du fournisseur de lecteur.

3.4.1. Panel de plateforme de référence

Constitution et configuration de la plateforme

(Voir figure 1 dans le paragraphe 3.3)

3.4.2. Logiciel Middleware

Le middleware de référence est la version du logiciel Middleware IAS avec sa documentation distribué par la DGME.

Ce logiciel est disponible sur le site `pilotecarteIAS.referentiels-generaux.gouv.fr`

Le Middleware IAS est disponible sur les systèmes d'exploitation suivants:

- Windows 2OOO
- Windows XP
- Windows Vista
- Linux Mandriva 2007
- Linux UBUNTU 7.10
- Mac OS X 10.4

Le Middleware IAS est livré avec les utilitaires suivants :

- Explorateur de fichier
- Changement de code porteur
- Outil de propagation des certificats (Sur Windows 2000, Windows XP, Windows Vista)
- Mise à jour automatique

3.4.3. Panel de lecteur de référence

Les lecteurs de référence font partie de la liste des lecteurs référencés.

Cette liste est publiée sur le site du service en charge du référencement.

Ils sont fournis avec leur câble pour la communication, l'alimentation, les pilotes et la documentation

3.4.4. Panel de cartes de référence

Las cartes à puce de référence font partie de la liste des cartes référencées.

Cette liste est publiée sur le site du service en charge du référencement

Elles sont fournies avec leur documentation.

3.4.5. Téléservice ou application de test

Afin de réaliser les scenarii de tests décrits dans ce document, il est nécessaire de développer une ou des applications de test faisant appel aux interfaces des modules fournis par le middleware ou d'utiliser des produits du marché.

Le logiciel développé pour réaliser la recette du produit middleware IAS est mis à disposition par la DGME, il est conforme aux tests décrits ci-après.

Il est disponible dans les ateliers Adèle : https://www.ateliers.modernisation.gouv.fr/ Communauté A125 Ter Développement middleware IAS.

3.4.6. Mise à jour des éléments de la plateforme

Les éléments de la plateforme peuvent être mis à jour indépendamment des éléments testés.

Les mises à jours automatiques (telles que celles des OS) seront désactivées.

La version de la plateforme est dépendante de la version de chaque élément de la plateforme.

Le comité technique s'assurera de la bonne gestion et de la traçabilité de la version de chaque plateforme et de chaque élément de la plateforme.

3.5. Représentativité terrain

La représentativité terrain est limitée à l'utilisation des outils mis dans le panel de référence par l'utilisation des cas de test génériques définis par le service en charge du référencement.

Il n'a pas été spécifié de tests d'endurance dans ce programme.

4. Cas de test

Les cas d'usage décrits ci-dessous, permettent de rassembler l'ensemble minimum des fonctionnalités permettant l'interopérabilité.

Les cas de test peuvent être effectués par un navigateur, un client mail ou par une application dédiée.

Ces tests doivent être effectués avec des cartes personnalisées avec le [Profil ADELE 1] ou [Profil ADELE 2].

4.1. Identification & authentification

Utilisation des bi-clés et du certificat.

(Cf. Chapitre 1 du document [A])

4.1.1. Smartcard logon (serveur nécessaire) :

(Cf. document [B])

		Config 1	Config 2	Config 3	Config 4	Config 5	Config 6
OS		Windows Vista	Windows XP SP2	Windows 2000	MAC OS X 10.4	Linux Mandriva 2007	Linux Ubuntu 7.10
Navigateur		Internet Explorer 7.0	Internet explorer 6.0 SP1	Internet explorer 6.0 SP1	-	-	-
		Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1
Messagerie		Outlook 2003 Thunderbird 1.5.0.4	Outlook 2003 Thunderbird 1.5.0.4	Outlook Express v6 Thunderbird 1.5.0.4	Thunderbird 1.5.0.4	Mozilla Thunderbird v1.5.0.9	Mozilla Thunderbird v1.5.0.9
Application		**Smartcard logon**					
Module crypto	**PKCS#11**	Oui	Oui	Oui	**Oui**	Oui	Oui
	CSP	Oui	Oui	Oui	**Non**	**Non**	**Non**
	IAS API	Oui	Oui	Oui	**Oui**	Oui	Oui
Profil Cartes		**Profil ADELE 1 et Profil Adèle 2**					

Figure 2 : Matrice de test : Smartcard logon

En bleu : Elément applicable

4.1.2. Authentification SSL :

- Lecture du certificat de la carte (scénario de test via navigateur)

		Config 1	Config 2	Config 3	Config 4	Config 5	Config 6
OS		Windows Vista	Windows XP SP2	Windows 2000	MAC OS X 10.4	Linux Mandriva 2007	Linux Ubuntu 7.10
Navigateur		Internet Explorer 7.0	Internet explorer 6.0 SP1	Internet explorer 6.0 SP1	-	-	-
		Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1
Messagerie		Outlook 2003 Thunderbird 1.5.0.4	Outlook 2003 Thunderbird 1.5.0.4	Outlook Express v6 Thunderbird 1.5.0.4	Thunderbird 1.5.0.4	Mozilla Thunderbird v1.5.0.9	Mozilla Thunderbird v1.5.0.9
Application		**Application de test**					
Module crypto	**PKCS#11**	Oui	Oui	Oui	**Oui**	Oui	Oui
	CSP	Oui	Oui	Oui	**Non**	**Non**	**Non**
	IAS API	Oui	Oui	Oui	**Oui**	Oui	Oui
Profil Cartes		**Profil ADELE 1 et Profil Adèle 2**					

Figure 3 : Matrice de test : Authentification SSL

En bleu : Elément applicable

4.1.3. Authentification par une application de test :

		Config 1	Config 2	Config 3	Config 4	Config 5	Config 6
OS		Windows Vista	Windows XP SP2	Windows 2000	MAC OS X 10.4	Linux Mandriva 2007	Linux Ubuntu 7.10
Navigateur		Internet Explorer 7.0	Internet explorer 6.0 SP1	Internet explorer 6.0 SP1	-	-	-
		Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1
Messagerie		Outlook 2003 Thunderbird 1.5.0.4	Outlook 2003 Thunderbird 1.5.0.4	Outlook Express v6 Thunderbird 1.5.0.4	Thunderbird 1.5.0.4	Mozilla Thunderbird v1.5.0.9	Mozilla Thunderbird v1.5.0.9
Application		**Application de test**					
Module crypto	**PKCS#11**	Oui	Oui	Oui	**Oui**	Oui	Oui
	CSP	Oui	Oui	Oui	**Non**	**Non**	**Non**
	IAS API	Oui	Oui	Oui	**Oui**	Oui	Oui
Profil Cartes		**Profil ADELE 1 et Profil Adèle 2**					

Figure 4 : Matrice de test : Authentification par une application de test

En bleu : Elément applicable

4.2. Signature

Utilisation des différents types d'API et utilisation de tous les certificats.

4.2.1. Signature d'un message électronique:

(Cf. Chapitre 5.2 du document [B])

		Config 1	Config 2	Config 3	Config 4	Config 5	Config 6
OS		Windows Vista	Windows XP SP2	Windows 2000	MAC OS X 10.4	Linux Mandriva 2007	Linux Ubuntu 7.10
Navigateur		Internet Explorer 7.0	Internet explorer 6.0 SP1	Internet explorer 6.0 SP1	-	-	-
		Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1
Messagerie		Outlook 2003 Thunderbird 1.5.0.4	Outlook 2003 Thunderbird 1.5.0.4	Outlook Express v6 Thunderbird 1.5.0.4	Thunderbird 1.5.0.4	Mozilla Thunderbird v1.5.0.9	Mozilla Thunderbird v1.5.0.9
Application		**Application de test**					
Module crypto	**PKCS#11**	Oui	Oui	Oui	**Oui**	Oui	Oui
	CSP	Oui	Oui	Oui	**Non**	**Non**	**Non**
	IAS API	Oui	Oui	Oui	**Oui**	Oui	Oui
Profil Cartes		**Profil ADELE 1 et Profil Adèle 2**					

Figure 5 : Matrice de test : Signature d'un message électronique

En bleu : Elément applicable

4.2.2. Signature d'un document par une application de test :

(Cf Chapitre 5.2 du document [B])

		Config 1	Config 2	Config 3	Config 4	Config 5	Config 6
OS		Windows Vista	Windows XP SP2	Windows 2000	MAC OS X 10.4	Linux Mandriva 2007	Linux Ubuntu 7.10
Navigateur		Internet Explorer 7.0	Internet explorer 6.0 SP1	Internet explorer 6.0 SP1	-	-	-
		Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1
Messagerie		Outlook 2003 Thunderbird 1.5.0.4	Outlook 2003 Thunderbird 1.5.0.4	Outlook Express v6 Thunderbird 1.5.0.4	Thunderbird 1.5.0.4	Mozilla Thunderbird v1.5.0.9	Mozilla Thunderbird v1.5.0.9
Application		**Application de test**					
Module crypto	**PKCS#11**	Oui	Oui	Oui	**Oui**	Oui	Oui
	CSP	Oui	Oui	Oui	**Non**	**Non**	**Non**
	IAS API	Oui	Oui	Oui	**Oui**	Oui	Oui
Profil Cartes		**Profil ADELE 1 et Profil Adèle 2**					

Figure 6 : Matrice de test : Signature par une application de test

En bleu : Elément applicable

4.2.3. Signature qualifiée (avec utilisation du pin de signature et d'un certificat qualifié):

(Cf. Chapitre 6.3 du document [A])

		Config 1	Config 2	Config 3	Config 4	Config 5	Config 6
OS		Windows Vista	Windows XP SP2	Windows 2000	MAC OS X 10.4	Linux Mandriva 2007	Linux Ubuntu 7.10
Navigateur		Internet Explorer 7.0	Internet explorer 6.0 SP1	Internet explorer 6.0 SP1	-	-	-
		Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1
Messagerie		Outlook 2003 Thunderbird 1.5.0.4	Outlook 2003 Thunderbird 1.5.0.4	Outlook Express v6 Thunderbird 1.5.0.4	Thunderbird 1.5.0.4	Mozilla Thunderbird v1.5.0.9	Mozilla Thunderbird v1.5.0.9
Application		**Application de test**					
Module crypto	**PKCS#11**	Oui	Oui	Oui	**Oui**	Oui	Oui
	CSP	Oui	Oui	Oui	**Non**	**Non**	**Non**
	IAS API	Oui	Oui	Oui	**Oui**	Oui	Oui
Profil Cartes		**Profil ADELE 1 et Profil Adèle 2**					

Figure 7 : Matrice de test : Signature qualifiée

En bleu : Elément applicable

4.3. Déchiffrement

4.3.1. Déchiffrement d'un message électronique :

(Cf Chapitre 5.3 du document [B])

		Config 1	Config 2	Config 3	Config 4	Config 5	Config 6
OS		Windows Vista	Windows XP SP2	Windows 2000	MAC OS X 10.4	Linux Mandriva 2007	Linux Ubuntu 7.10
Navigateur		Internet Explorer 7.0	Internet explorer 6.0 SP1	Internet explorer 6.0 SP1	-	-	-
		Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1
Messagerie		Outlook 2003 Thunderbird 1.5.0.4	Outlook 2003 Thunderbird 1.5.0.4	Outlook Express v6 Thunderbird 1.5.0.4	Thunderbird 1.5.0.4	Mozilla Thunderbird v1.5.0.9	Mozilla Thunderbird v1.5.0.9
Application		**Application de test**					
Module crypto	**PKCS#11**	Oui	Oui	Oui	**Oui**	Oui	Oui
	CSP	Oui	Oui	Oui	**Non**	**Non**	**Non**
	IAS API	Oui	Oui	Oui	**Oui**	Oui	Oui
Profil Cartes		**Profil ADELE 1 et Profil Adèle 2**					

Figure 8 : Matrice de test : Déchiffrement d'un message électronique

En bleu : Elément applicable

4.3.2. Déchiffrement par une application de test:

(Cf Chapitre 6.4 du document [A])

		Config 1	Config 2	Config 3	Config 4	Config 5	Config 6
OS		Windows Vista	Windows XP SP2	Windows 2000	MAC OS X 10.4	Linux Mandriva 2007	Linux Ubuntu 7.10
Navigateur		Internet Explorer 7.0	Internet explorer 6.0 SP1	Internet explorer 6.0 SP1	-	-	-
		Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1
Messagerie		Outlook 2003 Thunderbird 1.5.0.4	Outlook 2003 Thunderbird 1.5.0.4	Outlook Express v6 Thunderbird 1.5.0.4	Thunderbird 1.5.0.4	Mozilla Thunderbird v1.5.0.9	Mozilla Thunderbird v1.5.0.9
Application		**Application de test**					
Module crypto	**PKCS#11**	Oui	Oui	Oui	**Oui**	Oui	Oui
	CSP	Oui	Oui	Oui	**Non**	**Non**	**Non**
	IAS API	Oui	Oui	Oui	**Oui**	Oui	Oui
Profil Cartes		**Profil ADELE 1 et Profil Adèle 2**					

Figure 9 : Matrice de test : Déchiffrement par une application de test

En bleu : Elément applicable

4.4. Tests de lecture/écriture de données

Cas de test en lecture et en écriture de données, en utilisant l'application dite Emetteur

(Cf Chapitre 7.2 et 7.3 du document [A])

		Config 1	Config 2	Config 3	Config 4	Config 5	Config 6
OS		Windows Vista	Windows XP SP2	Windows 2000	MAC OS X 10.4	Linux Mandriva 2007	Linux Ubuntu 7.10
Navigateur		Internet Explorer 7.0	Internet explorer 6.0 SP1	Internet explorer 6.0 SP1	-	-	-
		Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1
Messagerie		Outlook 2003 Thunderbird 1.5.0.4	Outlook 2003 Thunderbird 1.5.0.4	Outlook Express v6 Thunderbird 1.5.0.4	Thunderbird 1.5.0.4	Mozilla Thunderbird v1.5.0.9	Mozilla Thunderbird v1.5.0.9
Application		**Application de test**					
Module crypto	**PKCS#11**	Oui	Oui	Oui	**Oui**	Oui	Oui
	CSP	Oui	Oui	Oui	**Non**	**Non**	**Non**
	IAS API	Oui	Oui	Oui	**Oui**	Oui	Oui
Profil Cartes		**Profil ADELE 1 et Profil Adèle 2**					

Figure 10 : Matrice de test : Lecture/Ecriture de données

En bleu : Elément applicable

4.5. Arborescence

Parcours l'arborescence de l'ADF_{CIA} :

L'outil : Explorateur de fichier fourni avec le middleware IAS est utilisé pour vérifier l'arborescence de la carte conformément au [profil Adèle 1] ou [profil Adèle 2].

4.6. Lecture de données avec établissement d'un canal sécurisé

Création d'un canal sécurisé et lecture de données:

(Cf Chapitre 8 du document [A])

		Config 1	Config 2	Config 3	Config 4	Config 5	Config 6
OS		Windows Vista	Windows XP SP2	Windows 2000	MAC OS X 10.4	Linux Mandriva 2007	Linux Ubuntu 7.10
Navigateur		Internet Explorer 7.0	Internet explorer 6.0 SP1	Internet explorer 6.0 SP1	-	-	-
		Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1
Messagerie		Outlook 2003 Thunderbird 1.5.0.4	Outlook 2003 Thunderbird 1.5.0.4	Outlook Express v6 Thunderbird 1.5.0.4	Thunderbird 1.5.0.4	Mozilla Thunderbird v1.5.0.9	Mozilla Thunderbird v1.5.0.9
Application		**Application de test**					
Module crypto	**PKCS#11**	Oui	Oui	Oui	**Oui**	Oui	Oui
	CSP	Oui	Oui	Oui	**Non**	**Non**	**Non**
	IAS API	Oui	Oui	Oui	**Oui**	Oui	Oui
Profil Cartes		**Profil ADELE 1 et Profil Adèle 2**					

Figure 11 : Matrice de test : Création d'un canal sécurisé et lecture de données

En bleu : Elément applicable

4.7. Génération, renouvellement de Bi-clé et de certificat

La génération et le renouvellement des Bi-clés et des certificats de la carte IAS seront réalisés grâce à une application/télé service de test (modification du contenu de la carte en maintenant la cohérence de son application CIA).

- Chargement d'une bi-clé et d'un nouveau certificat
- Génération d'une bi-clé et chargement d'un nouveau certificat

En fonction des contrôles d'accès définis, certains de ces tests nécessitent l'établissement d'un canal sécurisé.

(Cf Chapitre 5.3 du document [A])

(Cf Chapitre 4 du document [B])

		Config 1	Config 2	Config 3	Config 4	Config 5	Config 6
OS		Windows Vista	Windows XP SP2	Windows 2000	MAC OS X 10.4	Linux Mandriva 2007	Linux Ubuntu 7.10
Navigateur		Internet Explorer 7.0	Internet explorer 6.0 SP1	Internet explorer 6.0 SP1	-	-	-
		Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1	Firefox 2.0.0.1
Messagerie		Outlook 2003 Thunderbird 1.5.0.4	Outlook 2003 Thunderbird 1.5.0.4	Outlook Express v6 Thunderbird 1.5.0.4	Thunderbird 1.5.0.4	Mozilla Thunderbird v1.5.0.9	Mozilla Thunderbird v1.5.0.9
Application		**Application de test**					
Module crypto	**PKCS#11**	Oui	Oui	Oui	**Oui**	Oui	Oui
	CSP	Oui	Oui	Oui	**Non**	**Non**	**Non**
	IAS API	Oui	Oui	Oui	**Oui**	Oui	Oui
Profil Cartes		**Profil ADELE 1 et Profil Adèle 2**					

Figure 12 : Matrice de test : Génération et renouvellement de bi-clés et de certificats

En bleu : Elément applicable

4.8. Changement de code porteur

Le changement de code porteur de la carte IAS sera réalisé grâce à l'outil fourni avec le middleware (changement de code porteur) (modification du contenu de la carte en maintenant la cohérence de son application CIA)

- Changement de code porteur
- Changement de code porteur utilisé pour la signature qualifiée.

Le nouveau code porteur sera vérifié en effectuant un test d'authentification voir § 4.1.2
Le nouveau code de signature qualifiée sera vérifiée en effectuant une opération de signature qualifiée avec ce nouveau code voir § 4.2.3

(Cf Chapitre 5.1 et 5.2 du document [A])

5. Annexe 1 : Evaluation des résultats et organisation de la certification

5.1. Evaluation des Résultats

5.1.1. Présentation des résultats

Le laboratoire de test doit rédiger un rapport avec son verdict et une synthèse.

Ce document présentera en synthèse un verdict pour les 7 cas de test décrits dans le chapitre IV et le détail des tests réalisés (couverture et résultats obtenus).

5.1.2. Analyse et expertise des résultats

Le laboratoire de test analyse et expertise les tests.

5.1.3. Validation des résultats

L'industriel peut contester les résultats.

5.1.4. Délivrance des rapports

Le rapport sera délivré au soumissionnaire et au service ministériel en charge du référencement (DGME).

5.2. Délivrance du certificat de conformité du produit au référentiel de tests IAS

5.2.1. Vérification des synthèses de l'ensemble des tests du référentiel de tests IAS

Après avoir vérifié la conformité des tests d'interopérabilité, le laboratoire rédige un rapport global incluant toutes les synthèses de tous les tests du référentiel de tests et prononce son verdict.

5.2.2. Délivrance du certificat de conformité au référentiel de tests IAS

Le certificat de conformité au référentiel de tests IAS est délivré à l'industriel et une notification est transmise au service ministériel en charge du référencement (DGME).

6. Annexe 2 : Documents cités en référence

6.1. Réglementation

Renvoi	Document
[REG_1]	Ordonnance n° 2005- 1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

6.2. Documents techniques

Renvoi	Document
[RGI]	Référentiel Général d'interopérabilité
[RGS]	Référentiel Général de Sécurité
[Profil Adèle 1]	Document de description du profil carte dit Adèle 1, fichier Profils Cartes IAS Adèle_v1.4.xls Disponible sur le site www.synergies-publiques.fr
[Profil Adèle 2]	Document de description du profil carte dit Adèle 2, fichier Profils Cartes IAS Adèle_v1.4.xls Disponible sur le site www.synergies-publiques.fr
[A]	MDWIAS_Scenarii_de_Test_Détaillés_IAS-API_V1.3.doc disponible dans les Ateliers Adèle : https://www.ateliers.modernisation.gouv.fr/ministeres/projets_adele/a125-ter-developpement/public
[B]	MDWIAS_Scenarii_de_Test_Détaillés_PKCS11-CSP_V1.3.doc disponible dans les Ateliers Adèle : https://www.ateliers.modernisation.gouv.fr/ministeres/projets_adele/a125-ter-developpement/public

6.3. Illustrations