



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2010/02

Middleware IAS-ECC V. 2.0.12 pour Windows

Paris, le 07 mai 2010

*Le Directeur général de l'agence nationale
de la sécurité des systèmes d'information*

Patrick PAILLOUX
[ORIGINAL SIGNE]



Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification devrait être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présumées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

<i>Référence du rapport de certification</i>	ANSSI-CSPN-2010/02
<i>Nom du produit</i>	Middleware IAS-ECC V. 2.0.12 pour Windows
<i>Référence/version du produit</i>	Version 2.0.12
<i>Critères d'évaluation et version</i>	CERTIFICATION DE SECURITE DE PREMIER NIVEAU
<i>Commanditaires</i>	Agence Nationale des Titres Sécurisés 5, rue de l'Eglise 08000 Charleville-Mézières France
<i>Développeurs</i>	DICTAO 152, avenue de Malakoff 75116 Paris France GEMALTO Avenue du Pic de Bertagne BP 100 13881 Gémenos Cedex France
<i>Centre d'évaluation</i>	SOGETI Infrastructure Services 6 - 8, Rue Duret, 75016 Paris, France Tél : +33 (0)1 58 44 55 66, mél : edouard.jeanson@sogeti.com

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- L'agence centrale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. LE PRODUIT	7
1.1. PRESENTATION DU PRODUIT	7
1.2. DESCRIPTION DU PRODUIT EVALUE	7
1.2.1. <i>Catégorie du produit</i>	8
1.2.2. <i>Identification du produit</i>	8
1.2.3. <i>Services de sécurité</i>	8
1.2.4. <i>Configuration évaluée</i>	9
2. L’EVALUATION	10
2.1. REFERENTIELS D’EVALUATION	10
2.2. CHARGE DE TRAVAIL PREVUE ET DUREE DE L’EVALUATION	10
2.3. TRAVAUX D’EVALUATION	10
2.3.1. <i>Fonctionnalités, environnement d’utilisation et de sécurité</i>	10
2.3.1.1. <i>Spécification de besoin du produit</i>	10
2.3.1.2. <i>Biens sensibles manipulés par le produit</i>	10
2.3.1.3. <i>Description des menaces contre lesquelles le produit apporte une protection</i>	10
2.3.1.4. <i>Fonctions de sécurité</i>	10
2.3.1.5. <i>Utilisateurs typiques</i>	10
2.3.2. <i>Installation du produit</i>	11
2.3.2.1. <i>Plate-forme de test</i>	11
2.3.2.2. <i>Particularités de paramétrage de l’environnement</i>	11
2.3.2.3. <i>Options d’installation retenues pour le produit</i>	11
2.3.2.4. <i>Description de l’installation et des non-conformités éventuelles</i>	11
2.3.2.5. <i>Durée de l’installation</i>	11
2.3.2.6. <i>Notes et remarques diverses</i>	11
2.3.3. <i>Analyse de la documentation</i>	11
2.3.4. <i>Revue du code source</i>	12
2.3.5. <i>Fonctionnalités testées</i>	12
2.3.6. <i>Fonctionnalités non testées</i>	12
2.3.7. <i>Synthèse des fonctionnalités testés / non testées et des non-conformités</i>	12
2.3.8. <i>Avis d’expert sur le produit</i>	12
2.3.9. <i>Analyse de la résistance des mécanismes et des fonctions</i>	12
2.3.9.1. <i>Liste des fonctions et des mécanismes testés - résistance</i>	12
2.3.9.2. <i>Liste des fonctions et des mécanismes non testés - résistance</i>	13
2.3.9.3. <i>Avis d’expert sur la résistance des mécanismes</i>	13
2.3.10. <i>Analyse des vulnérabilités (conception, construction...)</i>	13
2.3.10.1. <i>Liste des vulnérabilités connues</i>	13
2.3.10.2. <i>Liste des vulnérabilités découvertes lors de l’évaluation et avis d’expert</i>	13
2.3.11. <i>Accès aux développeurs</i>	13
2.3.12. <i>Analyse de la facilité d’emploi et préconisations</i>	14
2.3.12.1. <i>Cas où la sécurité est remise en cause</i>	14
2.3.12.2. <i>Recommandations pour une utilisation sûre du produit</i>	14
2.3.12.3. <i>Avis d’expert sur la facilité d’emploi</i>	14
2.3.12.4. <i>Notes et remarques diverses</i>	14
2.4. ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES	14
2.5. ANALYSE DU GENERATEUR D’ALEAS	15
3. LA CERTIFICATION	16



3.1.	CONCLUSION	16
3.2.	RESTRICTIONS D'USAGE.....	16
ANNEXE 1. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE		17
ANNEXE 2. REFERENCES LIEES A LA CERTIFICATION		18

1. Le produit

1.1. Présentation du produit

Le produit évalué est le « [Middleware IAS-ECC V. 2.0.12 pour Windows](#) » (ci-après, *Middleware IAS-ECC*, IAS-ECC étant les acronymes pour Identification, Authentification, Signature – *European Card Citizen*) développé par les sociétés DICTAO et GEMALTO.

Il s'agit d'un *package* logiciel composé :

- du middleware IAS-ECC qui est un logiciel fournissant des API (*Application Programming Interface*), qui vont:
 - permettre d'effectuer des opérations sur les données d'une carte à puce dite « IAS » conforme à la spécification IAS-ECC V1.01 élaborée par le Gixel (cf. référence [1]) :
 - lire des objets (c.f références [GUIDES]) dont le contrôle d'accès est en lecture libre ou protégée par un code personnel ou PIN (*Personal Identification Number*).
 - consulter les contrôles d'accès des différents objets.
 - administrer la carte par un canal transparent (mode permettant d'envoyer directement des APDU (*Application Protocol Data Unit*) à la carte en passant par l'API IAS).
 - permettre aux applications d'accéder aux interfaces PKCS#11 (cf. références [2]) ou CryptoAPI [3] directement au travers utilisant des API du middleware IAS-ECC.
- des outils associés, directement utilisables par les utilisateurs finaux utilisant les API du *middleware* IAS-ECC, permettant aux utilisateurs de :
 - changer leur code personnel (PIN) si le profil le permet ;
 - lire le contenu de sa carte ;
 - diagnostiquer la bonne installation et le bon fonctionnement du *middleware* IAS-ECC en générant un rapport technique d'installation et d'analyse du fonctionnement.

1.2. Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

<input type="checkbox"/>	1 - détection d'intrusions
<input type="checkbox"/>	2 - anti-virus, protection contre les codes malicieux
<input type="checkbox"/>	3 - firewall
<input type="checkbox"/>	4 - effacement de données
<input type="checkbox"/>	5 - administration et supervision de la sécurité
<input checked="" type="checkbox"/>	6 - identification, authentification et contrôle d'accès
<input type="checkbox"/>	7 - communication sécurisée
<input type="checkbox"/>	8 - messagerie sécurisée
<input type="checkbox"/>	9 - stockage sécurisé
<input type="checkbox"/>	10 - matériel et logiciel embarqué
<input type="checkbox"/>	99- Autres

1.2.2. Identification du produit

Le nom et la version du produit sont inscrites sur le CDROM d'installation et précisés à la première ligne du fichier « ReadMe_Fr.txt » présent au niveau du dossier racine de l'installation (par défaut « C:\Program Files\IAS ECC *Middleware* »).

1.2.3. Services de sécurité

Les fonctions de sécurité concernent la protection du PIN (code PIN global d'authentification et code PIN pour la signature qualifiée). Il s'agit des fonctions suivantes :

1. Protection du PIN en mémoire lors de sa saisie via l'interface propre du *middleware* ;
2. Protection du PIN en mémoire lors de son traitement par le *middleware* et sa transmission au lecteur de carte à puce ;
3. Protection du PIN en mémoire lors de sa saisie via l'outil de management de code secret ;
4. Protection du PIN en mémoire lors de la lecture des informations sur la carte à puce IAS.

On distingue trois cas de figure en fonction du mode de saisi du PIN.

Le PIN est saisi par un *PINpad* (clavier de saisie du PIN) associé à un lecteur de carte : la saisie est donc garantie par le matériel lecteur de la carte.

Le PIN est saisi via un logiciel utilisateur : la saisie doit être garantie par le logiciel utilisateur. Le logiciel transmet le PIN à l'interface PKCS11 du *middleware* IAS-ECC. C'est typiquement le cas lors de la saisie du PIN global d'authentification d'une carte. Le *middleware* n'est alors responsable que de la confidentialité et de l'intégrité du PIN lors de son traitement et sa transmission au matériel lecteur de carte à puce.

Le PIN est saisi via le *middleware* IAS-ECC lui-même : la saisie est alors effectuée grâce aux fonctions spécifiques du *middleware*. Dans ce cas, le *middleware* est responsable de la confidentialité et de l'intégrité du PIN lors de sa saisie, de son traitement et jusqu'au moment de sa transmission au logiciel de contrôle du lecteur de la carte à puce.

1.2.4. Configuration évaluée

La configuration évaluée est celle par défaut.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de Sécurité de Premier Niveau en phase expérimentale. Les références des documents se trouvent en annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

Le produit a fait l'objet de trois évaluations consécutives pour répondre à des remarques formulées à l'issue de la première évaluation. La charge de travail totale a été de 37 h.j. L'évaluation de la version certifiée s'est déroulée entre décembre et février 2010.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1. *Fonctionnalités, environnement d'utilisation et de sécurité*

2.3.1.1. *Spécification de besoin du produit*

Conforme à la cible de sécurité [CDS] (chapitre « Argumentaire »).

2.3.1.2. *Biens sensibles manipulés par le produit*

Conforme à la cible de sécurité [CDS] (chapitre « Description des biens sensibles que le produit doit protéger »).

2.3.1.3. *Description des menaces contre lesquelles le produit apporte une protection*

Conforme à la cible de sécurité [CDS] (Chapitre « Description des menaces »)

2.3.1.4. *Fonctions de sécurité*

Conforme à la cible de sécurité [CDS] (chapitre « Description des fonction de sécurité du produit »).

2.3.1.5. *Utilisateurs typiques*

Conforme à la cible de sécurité [CDS] (chapitre « Argumentaire »).

2.3.2. *Installation du produit*

2.3.2.1. *Plate-forme de test*

La plate-forme de test pour l'évaluation du produit a été constituée de machines virtuelles, fonctionnant sur le logiciel « VMware Workstation » dans sa version 6.5.3 build-185404. La machine virtuelle utilisée est un poste standard sur lequel est installé **Windows XP Professionnel, version 5.1 (2600), Service Pack 3**, possédant l'ensemble des mises à jour disponibles au début de l'évaluation.

L'installation et les tests fonctionnels ont également été reproduits sur une seconde machine virtuelle, sous **Windows Vista Enterprise**, possédant l'ensemble des mises à jour disponibles au début de l'évaluation.

Certains tests fonctionnels ont été réalisés à l'aide des logiciels Thunderbird (client mail), Internet Explorer et Firefox (navigateur Web).

La carte à puce IAS utilisée dispose d'un profil CNIe v0.11.1.

2.3.2.2. *Particularités de paramétrage de l'environnement*

Il faut disposer des droits d'administrateur pour installer le middleware.

Le fonctionnement de celui-ci requiert aussi que le système implémente :

- une interface PC/SC (*Personal Computer/Smart Card*) opérationnelle ;
- un lecteur de carte à puce correctement installé dans l'environnement PC/SC ;
- une carte à puce IAS émise dans un format compatible avec le *middleware* (Profil « Adèle » ou profil « CNIe » (Carte Nationale d'Identité électronique)).

2.3.2.3. *Options d'installation retenues pour le produit*

L'installation du produit s'effectue par l'exécution du package d'installation nommé « IAS ECC Middleware.msi ». Une installation standard a été effectuée, les répertoires et la configuration par défaut ont été conservés.

2.3.2.4. *Description de l'installation et des non-conformités éventuelles*

Sans objet.

2.3.2.5. *Durée de l'installation*

Sans objet.

2.3.2.6. *Notes et remarques diverses*

L'installation est simple et ne requiert aucune configuration de la part de l'utilisateur.

2.3.3. *Analyse de la documentation*

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est claire et aucune non-conformité n'a été relevée.

2.3.4. *Revue du code source*

Les évaluateurs n'ont pas eu accès au code source.

2.3.5. *Fonctionnalités testées*

Fonctionnalité	Résultat
Changement du PIN en utilisant les navigateurs Firefox et Internet Explorer	Réussite
Test de l'outil de diagnostique du <i>middleware</i> IAS	Réussite
Test de l'outil de consultation du contenu des cartes du <i>middleware</i> IAS	Réussite
Test de l'outil de changement du code secret du <i>middleware</i> IAS	Réussite

2.3.6. *Fonctionnalités non testées*

L'environnement de tests mis à disposition de l'évaluateur n'a pas permis de tester les fonctionnalités suivantes :

- authentification forte auprès d'un site Web distant ;
- authentification Windows avec carte à puce ;
- utilisation des certificats pour signer un courriel.

2.3.7. *Synthèse des fonctionnalités testées / non testées et des non-conformités*

L'environnement de test n'a pas permis de tester certaines fonctionnalités du produit ; toutefois, la recette fonctionnelle prononcée par l'ANTS en confirmera le bon fonctionnement.

Les fonctions testées couvrent de manière suffisante les opérations nécessaires à l'analyse de la résistance des mécanismes et fonctions définies dans la cible de sécurité.

2.3.8. *Avis d'expert sur le produit*

Le produit est conforme à ses spécifications.

2.3.9. *Analyse de la résistance des mécanismes et des fonctions*

2.3.9.1. *Liste des fonctions et des mécanismes testés - résistance*

Pour avis sur la résistance des mécanismes voir 2.3.9.3.

Fonction et mécanisme
Utilisation des certificats pour signer un courriel
Changement du PIN en utilisant le navigateur Firefox
Test de l'outil de diagnostique du <i>middleware</i> IAS

Test de l'outil de consultation du contenu des cartes du <i>middleware IAS</i>
Test de l'outil de changement du code secret du <i>middleware IAS</i>
Protection du code PIN en mémoire
Protection du code PIN global en mémoire cache
Effacement du code PIN en mémoire
Effacement du code PIN global en mémoire cache

2.3.9.2. Liste des fonctions et des mécanismes non testés - résistance

Sans objet.

2.3.9.3. Avis d'expert sur la résistance des mécanismes

Hors utilisation (utilisateur non authentifié), le *middleware IAS-ECC* ne compromet pas les biens sensibles qu'il est censé protéger (PIN).

En utilisation (utilisateur authentifié, *middleware IAS-ECC* en exécution), le *middleware* traite correctement les biens sensibles qu'il manipule afin d'éviter leur compromission ultérieure. On notera que les mécanismes de sécurité mis en œuvre pour atteindre ces objectifs étant tous implantés en logiciel, ils sont tous potentiellement vulnérables si les précautions d'emplois et les hypothèses d'environnement ne sont pas respectés (poste sain par exemple. De manière générale, cette remarque s'applique à tous les mécanismes implantés en logiciel).

Enfin, l'évaluateur n'a pas identifié de cas où le *middleware* dégraderait la sécurité du poste de travail sur lequel il s'exécute du fait de sa présence.

2.3.10. Analyse des vulnérabilités (conception, construction...)

2.3.10.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues sur ce produit particulier. Par contre, le produit peut être sensible à des vulnérabilités existantes dans les environnements sur lesquels il s'appuie (Windows, Internet explorer, le CSP de Microsoft, etc.).

2.3.10.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Aucune

2.3.11. Accès aux développeurs

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Au cours des échanges techniques qui ont eu lieu, le développeur a fait preuve d'une très bonne maîtrise de son produit et a été en mesure de répondre rapidement (dans la journée) aux questions posées.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

Néant.

2.3.12.2. Recommandations pour une utilisation sûre du produit

L'utilisation du produit doit être faite sur un PC hébergeant un système d'exploitation à jour concernant les correctifs de sécurité et correctement administré. Il doit être au minimum protégé par un produit anti-virus (avec bases d'information à jour et proposant des fonctions de détection des infections informatiques furtives - anti-*spyware*, anti-*rootkit*, etc.) et un pare-feu correctement configurés.

Le produit ne devrait pas être utilisé en cas de doute concernant la compromission du système.

L'utilisateur doit porter une attention particulière à la confidentialité du PIN de sa carte. Pour prendre une référence connue, il devrait attacher une même importance à la sécurité de sa carte IAS qu'à celle de sa carte bancaire.

En cas de perte ou de vol du support, l'utilisateur doit avertir l'opérateur du service sécurisé associé à son support afin que le certificat correspondant au support soit révoqué.

2.3.12.3. Avis d'expert sur la facilité d'emploi

Le *middleware* IAS-ECC n'est pas à proprement dit un logiciel destiné à un utilisateur final. Il est d'abord destiné à fournir une interface de « haut-niveau » à des applications informatiques. Néanmoins, l'utilisateur est susceptible d'interagir directement avec le produit dans certains cas :

- lors de l'installation
- lors de la saisie d'un PIN
- lorsqu'il utilise les outils associés.

Dans aucun de ces cas, il n'a été noté que l'utilisateur final pourrait se trouver en situation où la sécurité proposée par le produit pourrait être remise en cause.

Par ailleurs, la documentation fournie pour l'utilisation des API est claire et explicite. Des exemples de programmes de tests sont disponibles dans le SDK fourni.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

Sans objet.



2.5. Analyse du générateur d'aléas

Sans objet.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles en vigueur, avec la compétence et l'impartialité requise pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « [Middleware IAS-ECC V. 2.0.12 pour Windows](#) » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST].

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [ST] et suivre les recommandations énoncées dans le présent rapport de certification.

Annexe 1. Références documentaires du produit évalué

[CDS]	<i>Cible de sécurité CSPN v1.2 ;</i>
[RTE]	K08-DI-PRE-520-2009 v1.1, SOGETI-ESEC, 23 février 2009
[GUIDES]	<i>Middleware IAS - PKCS#11 - Crypto API - Guide de programmation;</i> MDWIAS_SF_PKCS11CAPIF version 1.1 <i>Middleware IAS Outil de changement de code secret - Spécifications fonctionnelles ;</i> MDWIAS_SF_PINManagementF_v1.01 <i>Middleware IAS Explorateur de fichiers de la carte IAS - Spécifications fonctionnelles ;</i> MDWIAS_SF_FileBrowserF_v1.01 <i>Middleware IAS - API IAS - Guide de programmation ;</i> MDWIAS_SF_IASAPIF_v1 09_MS
[1]	<i>European Card for e-Services and National e-ID applications - Technical Specifications;</i> IAS ECC, Revision: 1.01
[2]	Additional PKCS#11 Mechanisms; PKCS #11 v2.01 Cryptographic Token Interface Standard; PKCS #11 v2.01
[3]	Microsoft CryptoAPI

Annexe 2. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

[CSPN]

Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 2. 4, phase expérimentale, n° 915/SGDN/DCSSI/SDR/CCN du 25 avril 2008.

Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1. 4.

Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1. 3.

Documents disponibles sur www.ssi.gouv.fr