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-2011/08

## Middleware IAS ECC
## Version 2.08 pour Windows mobile 6.1

*Paris, le 10 juin 2011*

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

Patrick Pailloux
**[ORIGINAL SIGNE]**

SÉCURITÉ CERTIFICATION

# 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 doit 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 présupposées 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

*Référence du rapport de certification*

# ANSSI-CSPN-2011/08

*Nom du produit*

# Middleware IAS ECC

*Référence/version du produit*

## Version 2.0 révision 8 pour Windows mobile 6.1

*Critères d'évaluation et version*

## CERTIFICATION DE SECURITE DE PREMIER NIVEAU

## *(CSPN, Phase expérimentale)*

*Développeur(s)*


## Gemalto S.A.

**Avenue du Pic de Bertagne BP100**

**13881 Gémenos Cedex**

**France**

## Dictao S.A.

**152, avenue de Malakoff**

**75116 Paris**

**France**


*Commanditaire*


## Agence Nationale des Titres Sécurisés

**5 rue de l'Eglise**

**08000 Charleville-Mézières**

**France**


*Centre d'évaluation*


## Thales Security Systems and Services SAS

**18, avenue Edouard Belin BPI 1414**

**31401 Toulouse Cedex 9**

**Tél : 562882801, mél : nathalie.feyt@thalesgroup.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 modifié. Ce décret indique que :

- L'agence nationale 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

## 1.1. Présentation du produit

Le produit évalué est « Middleware IAS ECC**,** 2.0 révision 8 pour Windows mobile 6.1 **»** (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 d'interface, aussi appelé API (*Application Programming Interface*), qui permet à des applications d'accéder aux services cryptographiques et aux différentes fonctionnalités d'une carte à puce de type IAS ;
- d'un outil connexe, IASDiag (v2.0.16), directement utilisable par les utilisateurs finaux utilisant l'API *middleware* IAS-ECC, permettant aux utilisateurs de diagnostiquer la bonne installation et le bon fonctionnement du *middleware* IAS-ECC en générant un rapport technique d'installation et d'analyse du fonctionnement.

Contrairement aux versions développées pour Windows XP, 2000, Vista & 7, pour MacOS et pour Linux, la version pour Windows Mobile ne possède pas d'outils de « changement de code secret » et de « lecture du contenu de la carte ».

On entend par « carte à puce IAS » une carte à puce conforme à la spécification « IAS-ECC V1.01 » élaborée par le Gixel [GIXEL].

Le middleware IAS-ECC implémente les normes **PKCS11** [PKCS] et CryptoAPI [CRYPTO-API] pour le traitement des demandes de services cryptographiques de la part du logiciel. Il offre en plus une bibliothèque spécifique « **IAS-API** » [IAS-API] qui permet d'effectuer via un « secure messaging » des opérations d'accès en lecture à la structure de la carte, d'administration du contenu de la carte, et de signature qualifiée

## 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*

| |
|---|
| ☐ 1 - détection d'intrusions |
| ☐ 2 - anti-virus, protection contre les codes malicieux |
| ☐ 3 – firewall |
| ☐ 4 - effacement de données |
| ☐ 5 - administration et supervision de la sécurité |
| ☒ 6 - identification, authentification et contrôle d'accès |
| ☐ 7 - communication sécurisée |

| |
|---|
| ☐ 8 - messagerie sécurisée |
| ☐ 9 – stockage sécurisé |
| ☐ 10 - matériel et logiciel embarqué |
| ☐ 99- Autres |

### *1.2.2. Identification du produit*

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

Afin d'assurer l'intégrité du package d'installation (cf. §2.3.12.2), il est recommandé de vérifier que le haché du package d'installation correspond à celui présent dans le guide d'installation [GUIDES].

Voici la valeur contenue dans le guide d'installation :

- le sha256 calculé sur le fichier IAS_ECC_Middleware.cab (version 2.08) est :
  **aa1a8d9087d12c4ab38dcf9005efe5fcc019b5d787c72092e12868cffce8cf4d**

La version d'IASDiag peut être vérifiée en cliquant sur « A propos » dans le menu « ? ».

### *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 saisie 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 de la protection du PIN que 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*

Sans objet.

# 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

La charge de travail totale a été de 15 h.j au lieu des 25 h.j normalement prévus car l'évaluateur a pu s'appuyer sur les résultats des évaluations des versions Windows XP [CSPN-2010/02], Linux [CSPN-2010/04], MacOS [CSPN-2011/06] et Windows 2000, Vista & 7 [CSPN-2011/07].

## 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 (description) du produit »).

#### 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

Pour tester les différentes fonctionnalités et s'assurer de la compatibilité des différents blocs de la chaîne, les évaluateurs ont eu à leur disposition un terminal PSION WAP e-ID G3 sur lequel Windows Mobile 6.1 Classique était installé.

Plusieurs types de cartes ont été utilisées pour tester le logiciel (Carte Gemalto / Profil CNIE / Carte PVE / Carte gendarmerie nationale).

#### 2.3.2.2. Particularités de paramétrage de l'environnement

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

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

L'administrateur est libre d'installer l'application sur l'appareil ou en RAM.
Les deux installations ont été effectuées et les tests de conformité et de vulnérabilité ont été joués sur chacun des deux cas. Aucune différence n'a été constatée.

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

Sans objet.

#### 2.3.2.5. Durée de l'installation

L'installation du package se déroule au travers d'une interface conviviale en quelques secondes.

#### 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 (facultative)*

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

### *2.3.5. Fonctionnalités testées*

| Fonctionnalité | Résultat |
|---|---|
| Test de l'outil de diagnostique du *middleware* IAS | Réussite |

### *2.3.6. Fonctionnalités non testées*

La cible [CDS] précise que le terminal sur lequel est installé le middleware ne doit pas être connecté à internet. De plus, les applications présentes sur le terminal sont installées et configurées sous contrôle d'une autorité de confiance. Les fonctions de tests suivantes n'ont donc pas été testées :

- Changement du PIN en utilisant les navigateurs Firefox et Internet Explorer ;

- Accès aux certificats via Firefox ;
- Utilisation des bibliothèques tierces.

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

Les fonctions testées lors de cette évaluation ainsi que celles testées lors des évaluations précédentes 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

L'avis sur la résistance des mécanismes est donné au §2.3.9.3.

| Fonction et mécanisme |
|---|
| Protection du code PIN de signature en mémoire |
| Protection du code PIN global en mémoire |
| Effacement du code PIN en mémoire |
| Effacement du code PIN global en mémoire cache |
| Intégrité du package d'installation |

#### 2.3.9.2. Avis d'expert sur la résistance des mécanismes

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'emploi et les hypothèses d'environnement ne sont pas respectées (cf. §2.3.12.2.).

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. Il est donc important de respecter les recommandations décrites dans le paragraphe 2.3.12.2 du présent document.

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

Une vulnérabilité résiduelle a été découverte lors de l'évaluation : un attaquant qui cible le circuit d'approvisionnement du *middleware* peut remplacer le package par une version illégitime du logiciel.

Il est donc nécessaire de vérifier l'intégrité du package d'installation avant de l'installer (cf. §2.3.12.2).

### *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 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

Intégrité du package d'installation

L'administrateur doit vérifier l'intégrité du package d'installation avant d'installer le *middleware*. Le haché sha256 du package d'installation est disponible dans le guide d'installation [GUIDES] et dans le paragraphe 1.2.2 du présent document.

Recommandations pour le poste

Le middleware IAS-ECC est installé sur un système (terminal mobile durci) supposé sain et sécurisé. En particulier, les mesures de sécurité suivantes seront déployées :

- Une procédure de durcissement est appliquée qui ne permet pas l'installation ni l'exécution d'un code non approuvé par l'autorité d'administration (DPICA) ou Microsoft (signature à clé publique des applications et package d'installation) :
  - Application de gestion des PV-e (DPICA) ;
  - Middleware IAS ;
  - Mise à jour Windows (Microsoft) ;
- L'accès aux tâches d'administration du système est réservé à un compte d'administrateur ; il existe également un compte utilisateur, doté de privilèges restreints, et réservé à l'utilisation courante du système.

Recommandations générales

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.

L'utilisateur doit être vigilant à ne pas quitter son poste en ayant une procédure de changement de mot de passe en cours.

#### 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.

#### 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 et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « Middleware IAS ECC**,** 2.0 révision 8 pour Windows mobile 6.1 **»** soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS].

## 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 [CDS] et suivre les recommandations énoncées dans le présent rapport.

# Annexe 1. Références documentaires du produit évalué

| | |
|---|---|
| [CDS] | *Cible de sécurité CSPN - Middleware IAS-ECC V2.0 pour environnement Windows mobile 6.1 ;* Référence : ; Date : *10/10/2010* |
| [RTE] | *Rapport d'évaluation CSPN, Projet : CSPNIAS ;*<br>Référence : *CIASW_CSPN* ; Date : *07/01/2011* |
| [GUIDES] | Guide d'installation :<br>*Spécifications fonctionnelles de l'installateur ;*<br>Référence : *dictao_ants_MWIAS_setup_sfg* ; Date : *24/01/2011*<br><br>Guide d'utilisation :<br>*Spécification fonctionnelle de l'outil de diagnostic ;*<br>Référence : *dictao_ants_MWIAS_IADdiag_sfg.pdf* ; Date : *24/01/2011* |
| [GIXEL] | *European Card for e-Services and National e-ID applications - Technical Specifications*; IAS ECC, Revision: 1.01<br>[http://www.gixel.fr/accesCAT.asp?cat_id=44] |
| [PKCS] | Additional PKCS#11 Mechanisms; PKCS #11 v2.01<br>Cryptographic Token Interface Standard; PKCS #11 v2.01 |
| [IAS-API] | Middleware IAS - PKCS#11 - Crypto API - Guide de programmation |
| [CSPN-2010/02] | Rapport de certification ANSSI-CSPN-2010/02 – Middleware IAS-ECC V.2.0.12 pour Windows<br>Date : 07/05/2010<br>[http://www.ssi.gouv.fr/site_rubrique54_certificat_cspn_2010_02.html] |
| [CSPN-2010/04] | Rapport de certification ANSSI-CSPN-2010/04 – Middleware IAS-ECC V.2.0 pour Linux<br>Date : 22/10/2010<br>[http://www.ssi.gouv.fr/site_rubrique54_certificat_cspn_2010_04.html] |
| [CSPN-2011/06] | Rapport de certification ANSSI-CSPN-2011/06 – Middleware IAS-ECC Version 2.08 pour MacOS<br>Date : 20/05/2010 |
| [CSPN-2011/07] | Rapport de certification ANSSI-CSPN-2011/07 – Middleware IAS-ECC Version 2.017 pour Windows 2000, Vista & 7 |

# Annexe 2. Références à la certification

| | |
|---|---|
| Décret 2002-535 du 18 avril 2002 modifié 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.<br><br>Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1. 4.<br><br>Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1. 3.<br><br>Documents disponibles sur www.ssi.gouv.fr |
| [REF-CRY] | Référentiel général de sécurité, version 1.0, annexe B1 :<br>Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20.<br><br>Documents disponibles sur www.ssi.gouv.fr |