# Cible de sécurité CSPN

# Middleware IAS-ECC V2.0 pour environnement MAC OS

## Statut du document

| | |
|---|---|
| **Date d'application** | Sans objet |
| **Version actuelle** | 1.2 |

| | **Développeurs** | **Commanditaire** | **Evaluateur** |
|---|---|---|---|
| **Organisme(s)** | Dictao<br>Gemalto | ANTS | Sogeti |

## Diffusion

| **Nom** | **Organisation** |
|---|---|
| Pascal Chour | ANSSI |
| Emmanuel Sohier | ANSSI |
| Gérard Bonningue | ANTS |
| Sébastien Gelgon | AMO ANTS |
| Olivier Clémot | Dictao |
| Florence Defrance | Gemalto |
| Michael Guerassimo | Gemalto |
| Sébastien Valette | Thales |

## Historique des versions

| **Date** | **Version** | **Commentaire** |
|---|---|---|
| 05/07/10 | 1.0 | Version initiale |
| 13/09/10 | 1.1 | Ajout de la fonction de sécurité n°5 §4.2 |
| 10/10/10 | 1.2 | Suppression de la diffusion restreinte, correction du pied de page et modification du § 4.2 |

# Sommaire

# 1. Synthèse

## 1.1. Identification de la cible de sécurité

Cette cible de sécurité a été élaborée en vue d'une évaluation CSPN [1].

## 1.2. Identification du produit

| Catégorie | Identification |
|---|---|
| Nom commercial du produit | Middleware IAS-ECC |
| Numéro de la version évaluée | 2.0 |
| Catégorie de produit | Middleware de gestion de carte à puce |

## 1.3. Références

| Code | Référence | Nom |
|---|---|---|
| [1] | N°915/SGDN/DCSSI/ SDR du 25 avril 2008 | Certification de sécurité de premier niveau des technologies de l'information |
| [2] | IAS ECC, Revision: 1.01 | European Card for e-Services and National e-ID applications - Technical Specifications [http://www.gixel.fr/accesCAT.asp?cat_id=44] |
| [3] | PKCS #11 v2.01 | Cryptographic Token Interface Standard |
| [4] | PKCS #11 v2.01 | Additional PKCS#11 Mechanisms |
| [5] | MDWIAS_SF_PKCS11 CAPIF version 1.1 | Middleware IAS - PKCS#11 - Crypto API - Guide de programmation |
| [6] | MDWIAS_SF_PINMan agementF_v1.01 | Middleware IAS Outil de changement de code secret Spécifications fonctionnelles |
| [7] | MDWIAS_SF_FileBrow serF_v1.01 | Middleware IAS Explorateur de fichiers de la carte IAS Spécifications fonctionnelles |

# 2. Argumentaire (description) du produit

## 2.1. Description générale du produit

Le middleware IAS-ECC est package logiciel composé :

- Du middleware IAS-ECC qui est un logiciel d'interface, aussi appelé API (*Application Programming Interface*), permettant à des applications d'accéder aux services cryptographiques et aux différentes fonctionnalités d'une carte à puce de type IAS.
- Des outils connexes, directement utilisables par les utilisateurs finaux utilisant l'API 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 fonctionnement du middleware IAS-ECC en générant un rapport technique d'installation et d'analyse du fonctionnement.

On entend par « carte à puce IAS » une carte à puce conforme à la spécification « IAS-ECC V1.01» élaborée par le Gixel (cf. référence [2]).
Dans la suite du document, on nommera ce package logiciel « middleware IAS-ECC ». Le fonctionnement de celui-ci requiert que le système implémente :

- Un PC/SC opérationnel ;
- 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).

Le middleware IAS-ECC implémente les normes PKCS11 (cf. références [3] et [4]) pour le traitement des demandes de services cryptographiques de la part du logiciel. Il offre en plus une librairie spécifique « IAS-API » [5], qui permet d'effectuer des opérations d'accès en lecture à la structure de la carte, d'administration du contenu de la carte, et de signature qualifiée en utilisant les mécanismes de « secure messaging » des cartes IAS ECC.

## 2.2. Description de l'utilisation du produit

La cible d'évaluation étant un package logiciel, composé de plusieurs briques fonctionnelles, nous pouvons considérer deux types d'utilisateurs :

- Dans le cadre de la brique fonctionnelle API middleware IAS-ECC, les utilisateurs seront les logiciels qui feront appel à l'API middleware IAS-ECC ;
- Pour les briques fonctionnelles utilisant l'API middleware IAS-ECC (Changement du code PIN, lecture du contenu de la carte, diagnostique de l'installation et de bon fonctionnement) ce seront des utilisateurs finaux.

Pour accéder aux données privées de la carte à puce, le middleware IAS-ECC va requérir le code PIN de la carte. Celui-ci peut être « saisi » par le middleware de plusieurs façons :

- À l'aide d'un lecteur de carte disposant d'une interface de saisie du PIN (PINpad) ;
- Par un logiciel utilisateur, par exemple un navigateur Web, qui envoie ensuite le PIN à l'interface PKCS11 du middleware IAS-ECC ;
- Par le middleware lui-même à l'aide de fonctions propres.

Une fois l'accès autorisé, les utilisateurs finaux peuvent, via les outils connexes du middleware IAS-ECC :

- Gérer le changement des codes secret par l'intermédiaire de l'outil « Outil de Changement de code secret » ;
- Lire la structure de fichiers et les contrôles associés via l'application « Explorateur de fichier de la carte IAS » ;
- Diagnostiquer la bonne installation du produit via l'application de diagnostique incluse dans le package middleware IAS-ECC.

## 2.3. Description de l'environnement d'utilisation prévu

Le middleware IAS-ECC est destiné à être installé sur tout poste de travail d'un utilisateur qui voudrait utiliser une carte à puce IAS ECC.
Une version du middleware est disponible pour les systèmes d'exploitation les plus courants, à savoir Microsoft Windows, Linux et Mac OS. Cette cible ne concerne que la distribution Mac OS.

Les pré-requis nécessaires pour l'utilisation du middleware IAS-ECC sont les suivants :

- Un lecteur de carte à puce et une implémentation PC/SC
- Une carte à puce IAS ECC;
- Optionnellement, le lecteur de carte à puce peut intégrer un dispositif de saisie du code PIN (PINpad) ;
- Un système d'exploitation Mac OS 10.5 & 10.6

## 2.4. Description des hypothèses sur l'environnement

**Système :**

Le middleware IAS-ECC est installé sur un système supposé sain et sécurisé. En particulier, les mesures de sécurité suivantes sont supposées être déployées :

- Le système est protégé des virus et ne permet pas l'exécution de code malveillant ;
- Toutes les mises à jour de sécurité disponibles sont installées ;

- Les échanges de données avec le réseau sont contrôlés par un pare-feu correctement configuré ;
- Il existe un compte utilisateur, doté de privilèges restreints, et réservé à l'utilisation courante du système ;
- L'accès aux tâches d'administration du système est réservé à un compte d'administrateur (root) ou au compte utilisateur via la commande « sudo ». Cette commande devant être configurée pour être utilisée avec un mot de passe interactif valide pour une seule commande.
- L'installation et la mise à jour des logiciels sont sous le contrôle du compte administrateur ;
- L'installation et la configuration logiciel « Middleware IAS ECC » sont réalisées suivant les recommandations données par le guide utilisateur.
- Seuls des utilisateurs de confiance ont accès aux comptes du système.

**Matériels :**

Le lecteur de carte à puce est supposé être connecté de façon sécurisée au poste de travail : on ne peut pas intercepter les informations qui circulent entre le lecteur de carte et le poste de travail. Par exemple, si le lecteur de carte est relié par un port USB, il n'y a pas de moyen matériel d'interception des données sur ce port USB.
De plus, le lecteur de carte est supposé traiter correctement les données APDU qui lui sont envoyées par le middleware IAS-ECC et les relayer à la carte à puce en garantissant leur intégrité. De même, il est supposé garantir l'intégrité des réponses de la carte.
Si le lecteur de carte à puce comporte un dispositif de lecture de code PIN (PINpad), il est supposé garantir la confidentialité et l'intégrité du PIN lors de sa saisie et de sa transmission à la carte IAS ECC. Enfin, le lecteur ne stocke aucune information transmise à la carte ou au middleware.

**Logiciels utilisateurs :**

Les logiciels utilisateurs du middleware IAS-ECC sont supposés de confiance : leur intégrité est garantie et en particulier ils ne sont ni infectés, ni corrompus par des logiciels malveillants.
En cas de gestion de la saisie du code PIN par le logiciel utilisateur, le logiciel est supposé garantir la confidentialité de la saisie et de son envoi au middleware IAS-ECC.

## 2.5. Description des dépendances

Pour fonctionner correctement, le middleware IAS-ECC est dépendant de l'ensemble des éléments de son environnement indiqués au paragraphe 2.3.

## 2.6. Description des utilisateurs typiques

Dans le cadre de cette évaluation, il y a deux types d'utilisateurs :

- Les logiciels qui vont requérir les services du middleware IAS-ECC pour l'accès à une carte IAS ECC, que ce soit pour des opérations cryptographiques d'authentification, de signature, d'identification ou encore pour des tâches de lecture ou d'administration de la carte. Un logiciel utilisateur typique est un navigateur Web comme Firefox, qui demande, pour l'accès à un e-service, une authentification forte par carte à puce.
- Les utilisateurs finaux qui utiliseront les outils connexes pour changer leur code PIN, lire les informations de leur carte à puce IAS, diagnostiquer l'installation et le fonctionnement du logiciel.

En d'autres termes, un utilisateur sera :

- Soit le logiciel qui va utiliser les API PKCS11
- Soit le logiciel de diagnostic qui instrumentera l'ensemble des fonctions des API ;
- Soit le logiciel de Management des codes secrets ;
- Soit le logiciel d'Exploration de fichiers de la carte IAS ;
- Soit les utilisateurs finaux qui utiliseront les outils connexes.

## 2.7. Description du périmètre de l'évaluation

L'évaluation porte sur l'intégralité des fonctionnalités du middleware IAS-ECC, et uniquement sur ces fonctionnalités.

# 3. Description de l'environnement technique de fonctionnement

## 3.1. Matériel compatible ou dédié

Aucune contrainte matérielle particulière.

## 3.2. Système d'exploitation retenu

Dans le cadre de cette évaluation du middleware IAS-ECC V2.0, l'ensemble des tâches d'évaluation est effectué sur un environnement Mac OS 10.5 & 10.6.

# 4. Description des biens sensibles que le produit doit protéger

Les biens sensibles protégés par le middleware IAS-ECC sont les deux codes PIN de la carte IAS ECC:

- Code PIN global d'authentification ;
- Code PIN pour la signature qualifiée.

## 4.1. Description des menaces

En tenant compte des hypothèses d'environnement, on considère qu'il n'y a pas de menaces particulières sur le produit.

## 4.2. Description des fonctions de sécurité du produit

Les fonctions de sécurité concernent la protection du code PIN :

1. Garantie de la confidentialité du code PIN lors de sa saisie via l'interface propre du middleware ;
2. Garantie de la confidentialité du code PIN lors de son traitement par le middleware et sa transmission au lecteur de carte à puce.
3. Garantie de la confidentialité du code PIN lors de sa saisie via l'outil de management de code secret.
4. Garantie de la confidentialité du code PIN lors de la lecture des informations sur la carte à puce IAS ECC.
5. Garantie de la confidentialité du code PIN en mémoire et de son effacement aussitôt qu'il n'est plus utile de le stocker.

On distingue plusieurs cas de figures en fonction du mode de saisie du PIN :

**Le code PIN est capturé par un PINpad :**
La saisie est donc garantie par le matériel lecteur de la carte.

**Le code PIN est saisi par un logiciel utilisateur :**
La saisie est 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. Le middleware est alors responsable de la confidentialité et de l'intégrité du code PIN lors de son traitement et sa transmission au matériel lecteur de carte à puce.

**Le code PIN est saisi par 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 code PIN lors de sa saisie, de son traitement et jusqu'au moment de sa transmission au driver du lecteur de la carte à puce.