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-2017/17

# Middleware IAS-ECC pour MAC OS
# Version 3.1

*Paris, le 21 août 2017*

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

Emmanuel GERMAIN
[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@ssi.gouv.fr

*Référence du rapport de certification*

**ANSSI-CSPN-2017/17**

*Nom du produit*

**Middleware IAS-ECC pour MAC OS**

*Référence/version du produit*

**Version 3.1**

*Catégorie de produit*

**Identification, authentification et contrôle d'accès**

*Critères d'évaluation et version*

**CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**

*Commanditaire*

**Agence Nationale des Titres Sécurisés**
**18 rue Irénée Carré**
**08000 Charleville-Mézières**
**France**

*Développeur*

**Safran Identity & Security**
**18 Chaussé Jules César**
**95520 Osny**

*Centre d'évaluation*

**THALES (TCS – CNES)**
**290 allée du Lac**
**31670 Labège, France**
**France**

*Fonctions de sécurité évaluées*

**Protection du PIN lors de sa saisie via l'interface propre du middleware**
**Protection du PIN lors de son traitement par le middleware et sa transmission au sous-système carte à puce du système d'exploitation**
**Protection du PIN lors de sa saisie via l'outil de management de code secret**
**Protection du PIN lors de la lecture des informations sur la carte à puce IAS ECC**
**Protection du PIN en mémoire**

*Fonction de sécurité non évaluées*

**Néant**

| *Restriction d'usage* |
| --- |
| **Oui (cf. §3.2)** |

# 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 CSPN 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 le « Middleware IAS-ECC pour MAC OS, version 3.1 » (ci-après, middleware IAS-ECC, IAS-ECC étant les acronymes pour Identification-Authentification-Signature *European-Citizen-Card*) développé par *SAFRAN IDENTITY AND SECURITY*.

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

- du middleware IAS-ECC, 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 ;
- 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 leur 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.

Le *middleware* IAS-ECC implémente la norme PKCS11 [PKCS] pour le traitement des demandes de services cryptographiques de la part du logiciel.

## 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 – pare-feu |
| ☐ 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 – environnement d'exécution sécurisé |
| ☐ 11 – terminal de réception numérique (*Set top box*, STB) |
| ☐ 12 – matériel et logiciel embarqué |
| ☐ 13 – automate programmable industriel |
| ☐ 99 – autre |

### *1.2.2. Identification du produit*

| | |
|---|---|
| Nom du produit | Middleware IAS-ECC pour MAC OS |
| Numéro de la version évaluée | 3.1 |

L'empreinte MD5 suivante correspond au package « Middleware-3.1.2-osx-installer-signed.app » à installer : 4c43cbef0dbdc361bf2a30d1ff1c010d.

### *1.2.3. Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- protection du PIN lors de sa saisie via l'interface propre du *middleware* ;
- protection du PIN lors de son traitement par le *middleware* et sa transmission au sous-système carte à puce du système d'exploitation ;
- protection du PIN lors de sa saisie via l'outil de management de code secret ;
- protection du PIN lors de la lecture des informations sur la carte à puce IAS ECC ;
- protection du PIN en mémoire.

### *1.2.4. Configuration évaluée*

La configuration évaluée correspond au produit identifié au chapitre 1.2.2.

# 2. L'évaluation

## 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe 2.

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

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

## 2.3. Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

### *2.3.1. Installation du produit*

#### 2.3.1.1. Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.3 et exécuté sur les plateformes suivantes :

- Mac OS *Mountain Lion* 10.8.5, avec mise à jour de sécurité 2015-006 ;
- Mac OS *Mavericks* 10.9.5, avec mise à jour de sécurité 2016-004 ;
- Mac OS *Yosemite* 10.10.5, avec mise à jour de sécurité 2016-006.

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

Le guide d'installation [GUIDE] décrit les étapes à suivre pour l'installation de la TOE[1].
L'installation se fait par interface graphique et aucune option de configuration n'est proposée.

#### 2.3.1.3. Durée de l'installation

Non applicable.

#### 2.3.1.4. Notes et remarques diverses

Sans objet.

### *2.3.2. Analyse de la documentation*

La documentation est jugée suffisamment complète pour permettre une prise en main efficace du produit. Cependant, les guides ne reprennent pas certaines recommandations correspondant aux hypothèses d'environnement figurant dans la cible, ainsi qu'énoncé au paragraphe 2.3.8.2, l'utilisateur doit se conformer strictement à ces hypothèses.

[1] *Target Of Evaluation* : périmètre de l'évaluation

La documentation a également mis en avant des configurations pouvant avoir un impact sur les fonctions de sécurité, comme le mode parapheur, qui inhibe l'effacement du PIN après utilisation. Ce mode a toutefois été pris en compte dans l'évaluation et ne remet pas en cause la sécurité du produit.

### *2.3.3. Revue du code source (facultative)*

L'évaluation n'a pas fait l'objet d'une revue de code source.

### *2.3.4. Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

### *2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

### *2.3.6. Analyse des vulnérabilités (conception, construction, etc.)*

#### 2.3.6.1. Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

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

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

### *2.3.7. Accès aux développeurs*

Le centre d'évaluation a eu accès aux développeurs pour préciser les conditions d'utilisation du produit.

### *2.3.8. Analyse de la facilité d'emploi et préconisations*

#### 2.3.8.1. Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

#### 2.3.8.2. Recommandations pour une utilisation sûre du produit

L'administrateur doit vérifier l'intégrité du package d'installation avant d'installer le *middleware*. Le haché MD5 du package est disponible dans le guide d'installation [GUIDE] et dans le paragraphe 1.2.2 du présent document.

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées (notamment les hypothèses sur l'environnement) et les utilisateurs doivent se conformer au [GUIDE] fourni.

#### 2.3.8.3. Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté.

#### 2.3.8.4. Notes et remarques diverses

Le [RTE] ne contient aucune note ni remarque.

## 2.4. Analyse de la résistance des mécanismes cryptographiques

Le produit n'a fait l'objet d'une analyse des mécanismes cryptographiques au titre de cette évaluation CSPN.

## 2.5. Analyse du générateur d'aléas

Le produit n'implémente pas de générateur d'aléas.

# 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 pour MAC OS, version 3.1 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

## 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 spécifiés dans la cible de sécurité [CDS], et mettre en œuvre la recommandation énoncée dans le présent rapport (voir 2.3.8.2).

Cependant l'évaluation a mis en avant des restrictions d'usage à respecter pour une utilisation sécurisée du produit décrites ci-après :

- exécuter la TOE avec un compte utilisateur sans droit administrateur ;
- gérer les logiciels installés sur l'ordinateur exécutant la TOE ;
- désactiver les « *Core Dumps* » de Mac OS.

# Annexe 1. Références documentaires du produit évalué

| | |
|---|---|
| [CDS] | *Middleware IAS ECC v3.1 – Cible de sécurité CSPN pour MAC OS MAC OS 10.8 – MAC OS 10.9 – MAC OS 10.10*<br>Référence : 2016_2000015475 ;<br>Version : 1.0 ;<br>Date : *17 mai 2016* |
| [RTE] | *Rapport Technique d'Evaluation CSPN – Projet CSPN_MW_IAS_ECC_OSX*<br>Référence : MW_IAS_OSX_CSPN_RTE ;<br>Version : 1.0 ;<br>Date : 27 janvier 2017 |
| [GUIDE] | *Middleware IAS ECC - Guide d'installation MacOS*<br>Référence : 2016_2000020474 ;<br>Version : 2.0 ;<br>Date : *décembre 2016* |
| [PKCS] | Additional PKCS#11 Mechanisms; PKCS #11 v2.01<br>Cryptographic Token Interface Standard; PKCS #11 v2.01 |

# 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 des produits (CSPN) des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014.<br><br>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014.<br><br>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014.<br><br>Documents disponibles sur www.ssi.gouv.fr/ |