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-2012/03

Librairie nCode iwlib Java
Version 2.1

Paris, le 10 avril 2012

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 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-2012/03**
Nom du produit **nCode iwlib Java**
Référence/version du produit **Version 2.1**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur(s) **In-Webo Technologies SAS** **25, rue de Navarin** **75009 Paris** **France**
Commanditaire **In-Webo Technologies SAS** **25, rue de Navarin** **75009 Paris** **France**
Centre d'évaluation **Amossys** **4 bis, allée du Batiment** **35000 Rennes** **Tél : 02 99 23 15 79, mél : frederic.remi@amossys.fr**

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 la librairie « nCode iwlib Java version 2.1 » développé par In-Webo Technologies SAS.

L'application nCode est un générateur de mots de passe à usage unique (OTP) pour plates-formes mobiles. Elle permet, avec plus de fiabilité que la présentation d'un couple nom d'utilisateur/mot de passe, de discriminer les utilisateurs autorisés à accéder à un service de ceux non-autorisés à y accéder. L'application nCode fonctionne de façon autonome, c'est-à-dire sans connexion ni échange de données avec un serveur distant.

La librairie évaluée est au cœur de l'application nCode d'In-Webo. Elle est disponible en langages C et Java. La version Java, sujet de l'évaluation, est destinée à être déployée sur tout système d'exploitation mobile supportant le Java (téléphones ou tablettes Android, Blackberry, Java midp2.0, Windows mobile).

1.2. Description du produit évalué

La cible de sécurité [ST] 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

La version certifiée du produit est identifiable dans l'écran « A propos » du menu Outils. Cet écran identifie à la fois la version du logiciel utilisé (2.5.1 dans le cadre de cette évaluation) et la version de la librairie iwlib sur laquelle il s'appuie (2.1).

1.2.3. Services de sécurité

Le principal service de sécurité fourni par le produit est la génération d'OTP.

Cependant, pour assurer la protection en confidentialité et en intégrité des biens sensibles protégés par le produit, il assure les fonctions suivantes :

- blocage du PIN ;
- protection en confidentialité et en intégrité des clés stockées et utilisées lors de la génération d'un OTP et de la mise en œuvre d'une fonction de service ;
- protection contre le *key-logging* du PIN (hors périmètre de la présente évaluation).

1.2.4. Configuration évaluée

Lors de l'évaluation, la génération d'un OTP pour accéder à un service donné se faisait avec **présentation systématique du code PIN**.
Les services ne demandant pas la présentation systématique du code PIN n'entrent pas dans le périmètre de cette évaluation.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau. 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 a été conforme à la charge de travail prévue lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN] pour un produit comportant des mécanismes cryptographiques, soit 35 hommes x jours.

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 2 « Argumentaire »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 4 « 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 5 « Description des menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 6 « Description des fonctions de sécurité du produit »).

2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 2.6 « Argumentaire – Description des utilisateurs typiques concernés et de leur rôle particulier dans l'utilisation du produit »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

L'évaluation du produit s'est déroulée sur l'environnement Android 2.3.3 suivant deux modes de fonctionnement :

- en émulation : produit utilisé depuis un ordinateur (sous Windows 7 Pro) avec un émulateur Android fourni par le SDK Android ;
- en mode réel : produit installé sur un *smartphone* de type « Samsung Nexus S ».

2.3.2.2. Particularités de paramétrage de l'environnement

Sans objet.

2.3.2.3. Options d'installation retenues pour le produit

Sans objet.

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

En mode émulation

L'application a été livrée à l'évaluateur sous la forme d'un projet Eclipse afin qu'il puisse générer lui-même l'applicatif et vérifier que la librairie nCode iwlib soit bien utilisée lors de la génération de l'application.

Dans ce cas, l'installation se déroule en deux temps :

1. installation du SDK d'Android ;
2. installation du projet Eclipse.

En mode réel

L'application nCode est disponible directement depuis l'Android Market et peut également être installée à partir du fichier *nCode.apk* fourni par le développeur.

L'installation de cette application nécessite les permissions suivantes pour fonctionner :

- INTERNET ;
- READ_PHONE_STATE ;
- WRITE_EXTERNAL_STORAGE.

2.3.2.5. Durée de l'installation

En mode réel, le téléchargement de l'application et son installation nécessitent moins de 10 minutes.

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

Le produit ne dispose pas de documentation à proprement parler, la Foire Aux Questions [FAQ] présente sur le site internet d'In-Webo fait office de guide d'utilisation et d'installation de l'application nCode.

Cette FAQ est jugée suffisante, claire, compréhensible et ne peut pas conduire à de mauvaises interprétations.

2.3.4. Revue du code source (facultative)

Les évaluateurs ont eu accès à l'ensemble du code source de la librairie. Bien que le code ne soit pas beaucoup documenté, il est lisible et compréhensible grâce aux noms des fonctions et variables.

L'audit de code n'a pas permis de mettre en évidence l'utilisation de pratiques dangereuses et a permis de s'assurer que les permissions nécessaires à l'installation de l'application (§2.3.2.4) ne sont pas utilisées à des fins de diffusions malveillantes d'information.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Génération d'OTP	**Réussite**
Blocage du PIN	**Réussite**

2.3.6. Fonctionnalités non testées

La fonction de « Protection contre le *key-loggin* du PIN » n'a pas été évaluée car elle n'était pas implémentée dans la version du produit évaluée.

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

Sans objet.

2.3.8. Avis d'expert sur le produit

L'application nCode est simple d'utilisation et son interface est intuitive. Aucune compétence particulière n'est demandée à l'utilisateur final.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Fonction et mécanisme
Protection en confidentialité des clés stockées
Protection en confidentialité des clés échangées lors de la mise en œuvre d'une fonction de service
Protection en confidentialité des clés utilisées dans le calcul des OTP
Protection en intégrité des biens sensibles.

2.3.9.2. Avis d'expert sur la résistance des mécanismes

Le bilan global de l'analyse de résistance des fonctions et mécanismes mis en œuvre par l'application nCode est positif. Ils s'appuient sur des mécanismes cryptographiques détaillés dans le §2.4. Leur implémentation est jugée robuste par l'évaluateur.

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.

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

Plusieurs vulnérabilités ont permis à un attaquant de générer des OTP valides pour un service ne demandant pas la présentation systématique du code PIN. Ces vulnérabilités ne permettaient pas d'accéder directement aux biens sensibles protégés par le produit et n'étaient pas exploitables dans le cadre d'utilisation du produit défini par la cible de sécurité [CDS] et respectant les recommandations du §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

Lorsqu'un service ne demande pas la présentation systématique du code PIN, la sécurité de la solution peut être remise en cause si l'attaquant a un accès physique à la plate-forme de la victime.

2.3.12.2. Recommandations pour une utilisation sûre du produit

<u>Développeur de services utilisant la solution nCode</u>
Les services utilisant la solution nCode doivent être configurés pour forcer la demande systématique du code PIN pour la génération de l'OTP.

<u>Utilisateur de l'application</u>
L'utilisation de l'application nCode doit être faite sur une plate-forme 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.).

Le code PIN utilisé pour l'application nCode doit rester sous contrôle exclusif de l'utilisateur.

En cas de perte ou de vol du terminal mobile, l'utilisateur doit réinstaller l'application nCode sur un nouveau téléphone et lancer une synchronisation avec le serveur In-Webo. A défaut il doit faire une demande de suppression de son compte auprès d'un administrateur sur le site internet d'In-Webo.

L'utilisateur doit activer, sur sa plate-forme d'utilisation, le verrouillage de l'écran par schéma, code PIN ou mot de passe.

Le produit ne devrait pas être utilisé en cas de doute sur la sécurité du système.

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

Moyennant le respect des recommandations évoquées précédemment, l'évaluateur n'a pas identifié de cas ou le produit serait configuré ou utilisé de façon non sûre mais qu'un utilisateur pourrait raisonnablement croire sûre.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par l'évaluateur. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] qui a conclu à la conformité à [REF-CRY] des mécanismes cryptographiques suivants :

- chiffrement / déchiffrement ;
- calcul de hachés.

2.5. Analyse du générateur d'aléas

Les moyens mis en œuvre pour la génération et le retraitement des nombres aléatoires qui sont utilisés dans la librairie nCode permettent d'atteindre le niveau de résistance aux attaques visé par la CSPN.

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 « nCode iwlib Java**,** 2.1 » 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 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]	*nCode iwlib 2.1 - Cible de sécurité – v1.0 ;* Date : *17/11/2011*
[RTE]	*Rapport Technique d'Evaluation In-Webo - nCode iwlib Java ;* Référence : *RTE-nCode-1.20* ; Date : *03/02/2012*
[ANA-CRY]	*Evaluation CSPN de la bibliothèque nCode iwlib - Cotation des mécanismes cryptographiques ;* Date : *12/01/2012*
[FAQ]	Guide d'utilisation : *Foire Aux Questions (FAQ)* http://www.in-webo.com/fr/faq

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 1, n° 1414/ANSSI/SR du 30 mai 2011. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur www.ssi.gouv.fr
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur www.ssi.gouv.fr