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-2016/15

Discretio entreprise pour Android
Version 1.2.0

Paris, le 24 novembre 2016

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

Guillaume POUPARD
[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-2016/15**
Nom du produit **Discretio entreprise pour Android**
Référence/version du produit **Version 1.2.0**
Catégorie de produit **Communication sécurisée**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **MBDSYS** **187 Boulevard Anatole France** **93200 Saint-Denis** **France**
Centre d'évaluation **Oppida** **4-6 avenue du vieil étang, Bâtiment B,** **78180 Montigny le Bretonneux,** **France**
Fonctions de sécurité évaluées **Chiffrement des communications entre le terminal et le serveur de signalisation** **Chiffrement des communications entre le terminal et le service d'enregistrement** **Chiffrement des communications audio** **Authentification des utilisateurs et des serveurs** **Protection des clés de chiffrement**
Fonction(s) de sécurité non évaluées **N.A.**
Restriction(s) 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 la solution de protection des communications téléphoniques « Discretio entreprise pour Android, version 1.2.0 » développée par *MBDSYS*. Cette solution permet l'authentification des utilisateurs de terminaux mobiles équipés entre eux, ainsi que la protection des communications en confidentialité et intégrité.
Elle se compose d'une application Discretio, exécutée sur un terminal mobile Android, et d'un serveur, livré pour les besoins de l'évaluation sous la forme d'une appliance, hébergeant notamment un serveur de signalisation (Kamailio), une infrastructure de clés publiques comprenant une autorité de certification et une autorité d'enregistrement, un proxy SIP et un pare-feu.

La figure suivante présente l'architecture générale du produit.

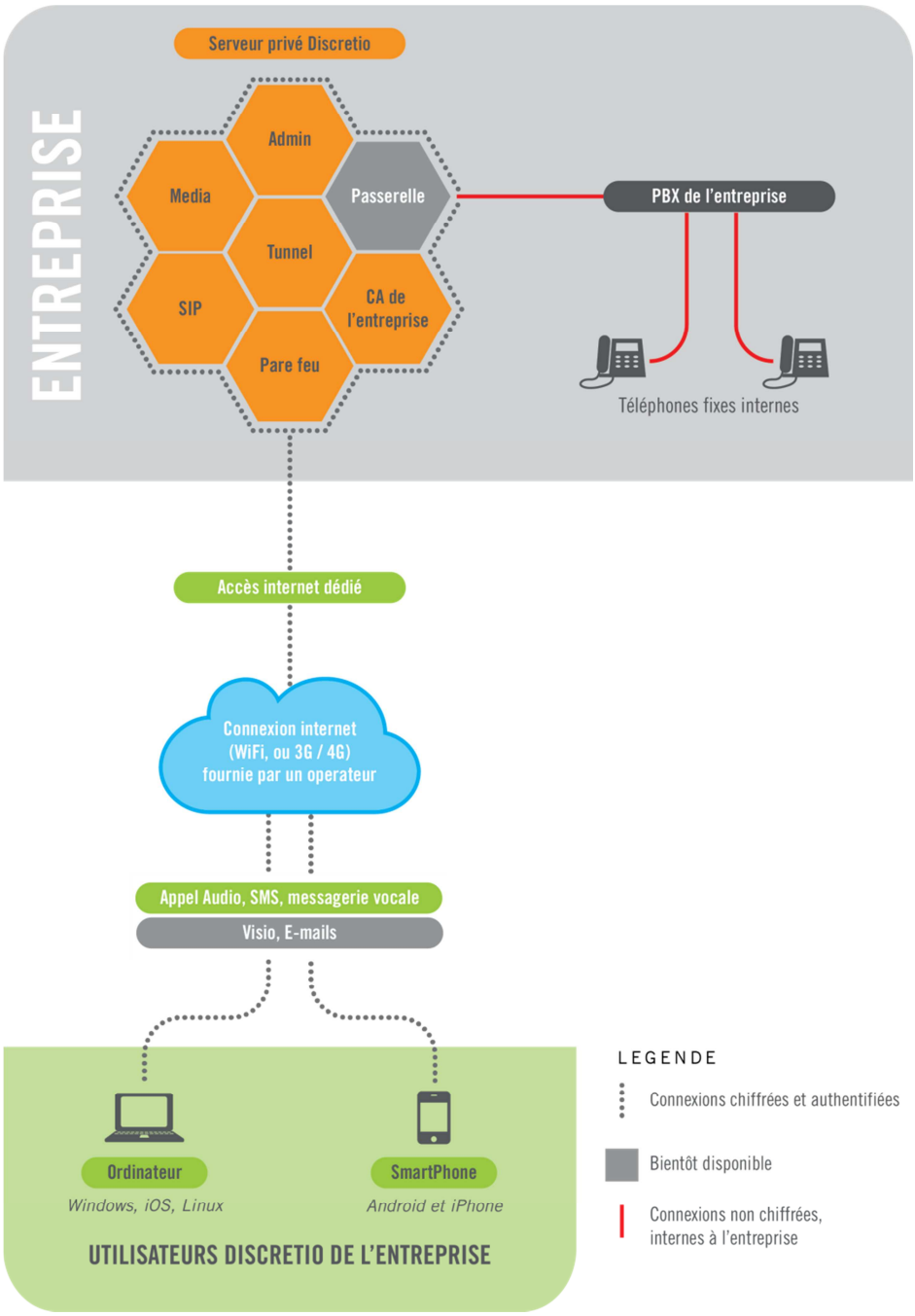

Figure 1 - Architecture de la solution.

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
☐ 14 – autre

1.2.2. Identification du produit

Nom du produit	Discretio entreprise pour Android
Numéro de la version évaluée	1.2.0 (application Android)

La version certifiée de l'application peut être identifiée sur le terminal Android depuis les paramètres du système, sur l'interface des applications installées, en sélectionnant l'application « Discretio ».

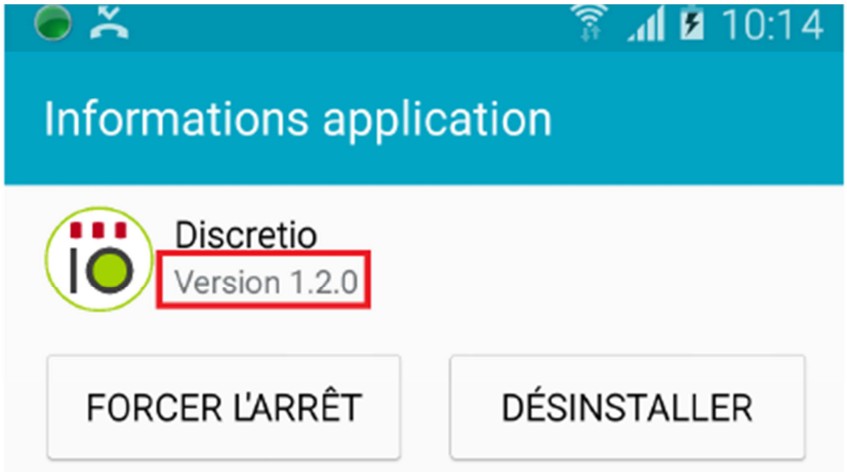

Figure 2 - Identification de la version mobile installée

De son côté, la version de l'appliance utilisée peut être identifiée depuis l'onglet « Informations » accessible sur l'interface web. La version utilisée pour l'évaluation est celle identifiée ci-après :

Figure 3 - Identification de la plateforme depuis l'interface web

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- l'authentification des utilisateurs et des serveurs ;
- l'authentification des utilisateurs entre eux ;
- la protection du flux d'enregistrement ;
- la protection du flux de signalisation ;
- la protection de la voix ;
- la protection de la clef.

1.2.4. Configuration évaluée

Aucune option d'installation particulière n'a été retenue pour l'évaluation. Une *appliance* a été livrée et configurée par le développeur conformément au guide d'installation.
L'application Android est récupérée depuis le téléphone sous la forme d'un APK[1], généré par le développeur.

La plateforme de test est constituée des éléments suivants :

- une « Discretio Box » (PC de type « shuttle ») ;
- un point d'accès (routeur WiFi,) permettant aux téléphones de se connecter au serveur ;
- deux téléphones *SAMSUNG* Galaxy S4.

[1] *Android Package*.

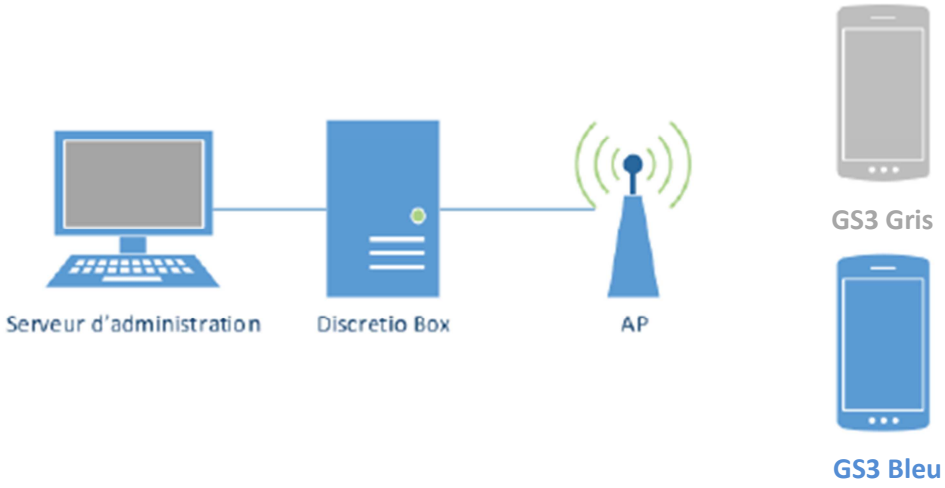

Figure 4 - plateforme de tests.

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, menaces, utilisateurs et 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.
L'architecture choisie, conforme au guide d'installation, est présentée comme « démo » et permet de tester le produit sans être connecté au réseau Internet.
Les certificats, préalablement générés par l'expert, étaient inclus dans l'APK.

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

L'*appliance* a été livrée et configurée par une personne de la société *MBDSYS*. Les certificats ont été générés par *MBDSYS*, et saisis sur le serveur ainsi que la licence.

L'application Android est générée et signée par *MBDSYS* après intégration des données issues de la personnalisation.
L'installation de l'application nécessite d'autoriser l'installation à partir de sources inconnues.

Pour pouvoir utiliser l'application, il est nécessaire de disposer de l'application ainsi que d'un *token* généré par l'administrateur.
L'administrateur doit avoir préalablement renseigné l'utilisateur dans la base de données via l'interface d'administration, puis ensuite communiquer le *token* à l'utilisateur.
L'enrôlement auprès du service nécessite la saisie du *token* et d'un mot de passe.

2.3.1.3. Durée de l'installation

L'installation est simple et rapide et ne nécessite que quelques minutes, du moment que l'APK a correctement été générée. Cette opération doit être réalisée conjointement avec le développeur de la solution.

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. L'évaluateur note toutefois l'absence de détails techniques relatifs à la plateforme utilisée (serveur) et le paramétrage (liste des ports à ouvrir, ports ouverts pour l'administration) ainsi qu'à la modification de certaines options de durcissement dans la documentation administrateur.

2.3.3. Revue du code source (facultative)

Le code source de la solution n'a pas été fourni à l'évaluateur. Celui-ci a toutefois pu accéder à certaines parties du code, par décompilation de l'application Java pour Android, et grâce à un accès *root* sur le serveur mis à disposition pour les besoins de l'évaluation.

L'évaluateur a effectué une revue du code décompilé et estime que le celui-ci est clairement organisé et respecte les bonnes pratiques de programmation.

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

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces. Cependant dans le contexte défini par la cible de sécurité [CDS] et les conditions d'utilisation prévues, aucune d'entre elles n'est exploitable.

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

Il n'a été découvert aucune vulnérabilité propre à l'architecture du produit, ni aucune liée à son implémentation qui puisse remettre en cause la sécurité du produit.

2.3.7. Accès aux développeurs

Sans objet.

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'évaluateur recommande à l'utilisateur du produit de mettre en œuvre les mesures suivantes :

- le *token* doit être fourni à l'utilisateur au travers d'un canal de communication sécurisé ;
- l'option « autoriser les sources inconnues » doit être désactivée après installation de l'application.

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 pour un l'utilisateur final.

2.3.8.4. Notes et remarques diverses

Sans objet.

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN. Des non-conformités au RGS ont été constatées, cependant celles-ci ne constituent pas des vulnérabilités exploitables dans le contexte d'utilisation du produit.

2.5. Analyse du générateur d'aléas

Le PRNG utilisé pour la génération d'aléas cryptographique n'est pas reconnu conforme au RGS, pour autant il n'a pas été identifié de chemin d'attaque exploitable lié à son utilisation dans le contexte visé et pour le niveau d'attaquant considéré.

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 « Discretio entreprise, version 1.2.0 » 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, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations énoncées dans le présent rapport (voir 2.3.8.2).

Annexe 1. Références documentaires du produit évalué

[CDS]	Cible de sécurité - Discretio entreprise Version : *1.2* ;
[RTE]	Rapport Technique d'Évaluation (RTE) CSPN DISCRETIO2 Référence : OPPIDA/CESTI/DISCRETIO2/RTE/1.0 ; Version : 1.0 ;
[SPEC-CRY]	Discretio - Caractéristiques techniques Version : 1.2 ;
[GUIDES]	Discretio Android 1.2.0 - Guide d'utilisation Version : 0.02 ; Discretio Entreprise 1.2.0 - Document d'installation Version : 1.2 ;

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. 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. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur www.ssi.gouv.fr/
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr.