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-2013/06

TEOPAD
Version 1.1.06

Paris, le 13/06/2013

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-2013/06**
Nom du produit **TEOPAD**
Référence/version du produit **1.1.06**
Catégorie de produit **Environnement d'exécution sécurisé**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur **Thales Communications & Security** **152, avenue Malakoff** **92622 Gennevilliers** **France**
Commanditaire **Thales Communications & Security** **152, avenue Malakoff** **92622 Gennevilliers** **France**
Centre d'évaluation **AMOSSYS** **4 bis Allée du Bâtiment** **35000 Rennes** **France**

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 TEOPAD, version 1.1.06 développé par la société Thales Communications & Security. TEOPAD est une solution permettant de déployer des applications sécurisées sur les *smartphones* et les tablettes dans un contexte professionnel.

La solution TEOPAD permet de créer sur un terminal mobile un environnement professionnel sécurisé qui peut cohabiter avec un contexte personnel ouvert. Cet environnement professionnel se présente sous la forme d'une application qui peut être lancée après authentification de l'utilisateur et à partir d'une simple icône sur le bureau natif du terminal. L'utilisateur a alors accès à un second bureau qui constitue son environnement professionnel. Celui-ci est isolé de la partie personnelle et native par une technologie de bac à sable (*sandboxing*) propriétaire. Cette partie, contient l'ensemble des applications, données et paramètres nécessaires à l'utilisateur dans le cadre de son activité professionnelle :

- applications de tous types : navigateur web, client courriel, visionneuses, bloc-notes, client phonie, applications métier, etc. ;
- documents, base de contacts, agenda, archives de courriels, etc.

Les applications nécessitant une connexion à un service extérieur (navigation web, courriel, phonie) utilisent un canal sécurisé vers l'infrastructure de l'entreprise qui est chargée de router ces connexions (recommandation n° 18 de [REC-ANSSI]).

Les applications déployées dans l'environnement professionnel proviennent obligatoirement du TEOPAD Market Place (TMP) privatif de l'organisation et ne peuvent en aucun cas être téléchargées à partir d'un kiosque public. TEOPAD permet ainsi de faciliter la mise en œuvre de politiques de sécurité centralisées lors du déploiement d'applications utilisées dans un environnement professionnel (recommandation n° 12 de [REC-ANSSI]).

L’accès direct à des sites internet publics n’est donc pas possible à partir du bureau professionnel, mais doit dans ce cas se faire par rebond à partir du système d’information de l’entreprise. Il est alors soumis à la politique de sécurité de cette dernière. Par contre cet accès direct à des sites internet publics reste potentiellement autorisé pour l’utilisateur dans le cadre de son usage privé et à partir d’un navigateur présent sur son environnement personnel, auquel TEOPAD ne change rien et n’apporte aucune sécurité.

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 : environnement d'exécution sécurisé**

1.2.2. Identification du produit

La version du produit utilisée peut être vérifiée à travers les options de l'application TEOPAD dans les menus du système ANDROID comme le montre la figure suivante.

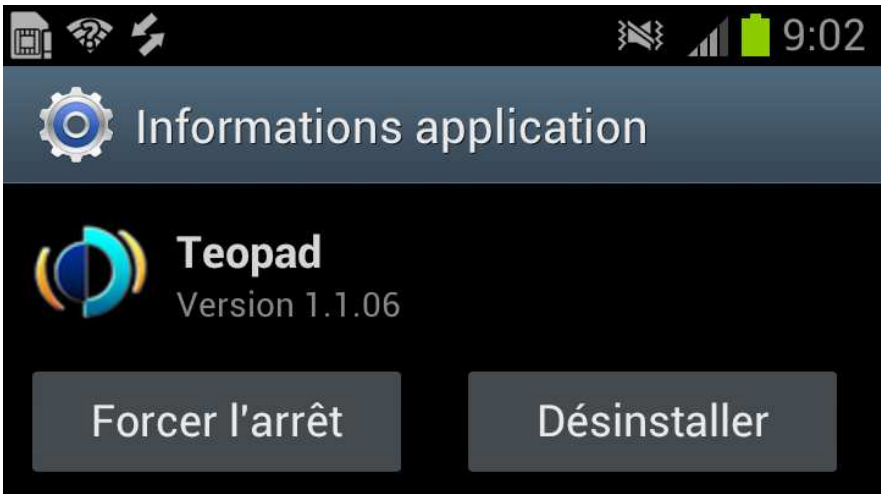

Figure 1 - Identification de la version de l'application TEOPAD

La version certifiée du produit est celle évaluée. Elle correspond à la version 1.1.06.

1.2.3. Services de sécurité

Les services de sécurité fournis par le produit qui font l'objet de l'évaluation sont :

- l'authentification de l'utilisateur avant toute utilisation de l'environnement TEOPAD ;
- le chiffrement des fichiers et données manipulés à l'intérieur de l'environnement TEOPAD ;
- le chiffrement des communications entre les applications exécutées dans l'environnement TEOPAD et le SI de l'entreprise de l'utilisateur ;
- l'isolement applicatif au sein de l'environnement professionnel TEOPAD vis-à-vis des applications non-privilégiées de l'environnement ANDROID dit « personnel » ;
- le stockage des clés cryptographiques dans un élément de sécurité matériel (ou *Secure Element*, SE) ;
- l'effacement des secrets en RAM lors de l'arrêt de TEOPAD ;
- la journalisation d'évènements et l'émission d'alarmes.

1.2.4. Configuration évaluée

La configuration évaluée correspond à la version décrite au chapitre précédent, déployée sur un terminal *Galaxy SIII* de *Samsung* embarquant un système ANDROID en version 4.0.4, et équipé du SE matériel Mobile Security Card SE 1.0 (inclus dans une carte au format Micro-SD) développé par *G&D* et certifié au niveau EAL4 augmenté des composants ADV_IMP.2 et AVA_VLA.4.

Dans la configuration évaluée, le canal sécurisé entre le produit et l'infrastructure de l'entreprise était monté sur l'interface Wifi du téléphone, l'établissement de ce canal sur le réseau de l'opérateur n'a pas été évalué.

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 3 « Argumentaire »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 3.4 « Biens à protéger »).

2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre 3.5 « Menaces considérées »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 4 « Fonctions de sécurité »).

2.3.1.5. Utilisateurs typiques

Un seul type d'utilisateur est prévu pour TEOPAD. En effet l'installation du produit sur le terminal mobile ne nécessite aucune intervention d'un administrateur. L'utilisateur ne doit pas disposer de compétence technique évoluée ni d'une connaissance précise du système d'information lié au produit.

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

Le terminal utilisé pour l'évaluation est un *smartphone* Galaxy SIII de Samsung dont les caractéristiques sont listées ci-après :

Catégorie	Descriptions
Noyau	GNU/Linux 32bit 3.0.15-782020-user
OS	`Android` 4.0.4
Processeur	2x ARMv7 Processor rev0 (v7l)
RAM	800MB
Stockage interne	11GB
Réseau	*WiFi* ; Aucune carte SIM installée

Pour l'évaluation, les applications suivantes sont installées par défaut dans l'application TEOPAD des terminaux mobiles :

- *Email Pro,* version 4.0.3 ;
- *Exchange Pro,* version 4.0.3 ;
- *Agenda Pro,* version 4.0.3 ;
- *Contacts Pro,* version 4.0.3 ;
- *Gestionnaire de téléchargement Pro,* version 4.0.3 ;
- *Kingsoft Office,* version 4.5 ;
- *ColorNote,* version 3.1.4 ;
- *ASTRO,* version 3.1.383.std.

2.3.2.2. Particularités de paramétrage de l'environnement

Le produit ne peut être installé et utilisé que dans le cadre d'une organisation ayant déployé l'ensemble de la solution TEOPAD et disposant d'un centre de gestion TEOPAD (*TEOPAD Management Center).* Aucun paramétrage particulier n'est requis.

2.3.2.3. Options d'installation retenues pour le produit

Aucune option d'installation n'est disponible.

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

La procédure d'installation est destinée à être effectuée par l'utilisateur du périphérique mobile. La description fournie se positionne ainsi du point de vue de l'utilisateur de l'environnement TEOPAD.
L'évaluateur a pu constater que l'installation s'est déroulée conformément à la procédure décrite dans les guides.

2.3.2.5. Durée de l'installation

Sans objet.

2.3.2.6. Notes et remarques diverses

Sans objet.

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

Les fonctions suivantes ont été soumises à des tests de conformité :

Fonctionnalité	Résultat
Enregistrement des évènements dans le journal	**Réussite**
Gestion des alarmes	**Réussite**
Détection du mode *débogage USB* et exécution de la politique adéquate	**Réussite**
Détection du mode *ROOT* et exécution de la politique adéquate	**Réussite**
Isolation des applications sensibles	**Réussite**
Protection des données stockées par chiffrement	**Réussite avec remarque**
Gestion du *Secure Element*	**Réussite**
Conformité de l'algorithme cryptographique utilisé pour le canal TLS	**Réussite**

2.3.6. Fonctionnalités non testées

Du fait que le CESTI n'a pas eu la possibilité de *dumper* la mémoire volatile, il n'a pas pu s'assurer du bon fonctionnement des fonctionnalités suivantes :

- effacement sécurisé des clés en mémoire ;
- effacement sécurisé des données en mémoire.

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

Plusieurs tests menés par le CESTI ont démontré l'existence de cas où le produit ne chiffrait pas correctement les données. Ces problèmes sont contournés par l'application des recommandations du §2.3.12.2 du présent rapport.

2.3.8. Avis d'expert sur le produit

L'analyse a montré que le produit est majoritairement conforme aux spécifications techniques présentées dans sa cible de sécurité.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Les fonctions suivantes ont été soumises à des tests de pénétration :

Fonction et mécanisme
Détection du mode *root*
Détection du mode *debug*
Authentification
Stockage sécurisé
Isolation entre les deux environnements

2.3.9.2. Avis d'expert sur la résistance des mécanismes

L'évaluateur est parvenu à contourner les détections des modes *root* et *debug*. Cependant, ces fonctions de sécurité sont des fonctions supports fournies par le système d'exploitation et non par le produit en lui-même et leur contournement ne permet pas, à lui seul, d'accéder aux biens sensibles protégés par le produit dans le cadre de l'évaluation.

Comme indiqué dans la cible de sécurité [CDS], le produit s'exécutant sans privilège particulier, l'isolation entre les deux environnements peut être outrepassée par un attaquant ou une application malveillante ayant des droits privilégiés.

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 cette version du produit.

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

L'analyse de la résistance de la fonction de bac à sable a permis d'identifier qu'une application malveillante installée dans l'environnement TEOPAD pouvait partiellement contourner le bac à sable et compromettre des informations de l'environnement TEOPAD vers l'environnement personnel. Cependant, les applications présentes dans l'environnement TEOPAD étant considérées sûres, cette vulnérabilité n'est pas exploitable dans le contexte décrit dans la cible de sécurité [CDS].

2.3.11. Accès aux développeurs

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Lors 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

Le produit requiert la désactivation de la fonction de vérification des sources des applications, offerte par le système ANDROID, afin de pouvoir installer et mettre à jour les applications professionnelles destinées à l'environnement TEOPAD. Ce comportement a pour conséquence d'abaisser le niveau global de sécurité du dispositif et doit être contrôlé conformément aux recommandations énoncées dans le §2.3.12.2.

Enfin, bien que le produit permette l'utilisation aussi bien d'un élément de sécurité matériel (SE) que logiciel (VSE), la sécurité d'une solution à base de VSE ne peut être considérée équivalente à celle d'une solution à base de SE. Le présent certificat ne porte donc que sur la configuration où l'application TEOPAD est associée à un élément de sécurité matériel.

2.3.12.2. Recommandations pour une utilisation sûre du produit

1) Il est recommandé de laisser la vérification des sources des applications activée par défaut et de ne la désactiver que ponctuellement lorsqu'il est nécessaire de procéder à une mise à jour du jeu d'applications TEOPAD. L'utilisateur devra ainsi, après tout téléchargement de logiciel depuis le *TEOPAD Market Place*, veiller à réactiver manuellement cette fonction.

2) L'encapsulation dans un tunnel chiffré des données échangées entre les applications TEOPAD et le monde extérieur utilise un certificat auto-signé. Aucune vérification sur l'authenticité du certificat n'est faite par le produit ni par le système. Par conséquent, l'utilisateur doit avoir connaissance de l'empreinte cryptographique du certificat afin de pouvoir vérifier manuellement son authenticité.

3) Les secrets cryptographiques sont partagés entre toutes les applications de l'environnement TEOPAD. Ainsi, la sécurité du produit repose essentiellement sur l'isolation faite entre l'environnement personnel ANDROID et l'environnement professionnel TEOPAD. Ce mécanisme de sécurité peut-être mis à mal par une application malveillante et dans ce cas, toutes les applications de l'environnement TEOPAD sont accessibles à un attaquant. L'utilisateur doit s'assurer que les applications qu'il charge sur son environnement personnel sont de confiance. En cas de doute, il devrait s'abstenir de charger des applications externes ou non validées par l'organisation.

4) Du fait de l'architecture de TEOPAD, il ne peut être exclu la possibilité de piégeage logiciel du terminal en cas de perte, même brève, de ce dernier. Ainsi, comme indiqué dans la recommandation n°6 de [REC-ANSSI], tout appareil équipé avec TEOPAD et qui échapperait à la vigilance de l'utilisateur devrait être considéré comme ayant été usurpé, et retourné au « *TEOPAD Management Center* » afin d'être réinitialisé avant toute nouvelle utilisation sur le terrain.

5) L'effacement des secrets en mémoire ne se fait qu'à l'extinction de TEOPAD ou de l'appareil. L'utilisateur doit donc conserver l'appareil sous son contrôle jusqu'à son extinction.

6) Des non-conformités liées au chiffrement des fichiers ayant été constatées lors de l'utilisation de l'application de gestion de fichiers *Astro*, cette application ne doit pas être

utilisée depuis l'environnement TEOPAD pour éditer un fichier créé depuis l'environnement ANDROID personnel.

7) Lors de la mise à jour et de l'installation d'une application dans l'environnement TEOPAD, l'application est également installée dans l'environnement personnel de l'utilisateur. Il est conseillé à l'utilisateur de vérifier dans son gestionnaire d'application que le couple d'application concerné possède le même numéro de version. Dans le cas contraire, il est conseillé à l'utilisateur de désinstaller cette mise à jour ou cette application pour éviter de mettre le produit dans un état instable.

8) Il convient de s'assurer que l'utilisation du produit est faite sur un dispositif hébergeant un système ANDROID à jour concernant les correctifs de sécurité et n'ayant pas été modifié. Plus particulièrement, l'environnement TEOPAD ne se protégeant pas contre des applications ayant des privilèges particuliers, le téléphone ne doit pas être « rooté » et, comme indiqué dans la recommandation n°9 de [REC-ANSSI], une étude de réputation doit être réalisée par l'utilisateur avant d'installer une application sur l'environnement Android dit « personnel » pour valider que cette dernière n'est pas malveillante et ne permet pas une escalade de privilège.

9) Le produit ne devrait pas être utilisé en cas de doute sur la sécurité du terminal. De manière générale, l'installation et l'exploitation du dispositif doivent être effectuées conformément aux bonnes pratiques en matière de sécurité des terminaux mobiles, telles que celles décrites dans le document [REC-ANSSI].

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

Sans objet.

2.3.12.4. Notes et remarques diverses

Aucune.

2.4. Analyse de la résistance des mécanismes cryptographiques

Certains mécanismes cryptographiques mis en œuvre par le produit ne suivent pas les recommandations du référentiel [REF-CRY]. Cependant, les écarts constatés ne remettent pas en cause le niveau de résistance aux attaques visé par la CSPN.

2.5. Analyse du générateur d'aléas

Le produit s'appuie sur le générateur d'aléas de la bibliothèque OpenSSL non conforme au référentiel de l'ANSSI [REF-CRY]. Cependant, les moyens mis en œuvre pour le retraitement des nombres aléatoires 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 « TEOPAD, version 1.1.06 », 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]	*CIBLE DE SECURITE CSPN DE L'APPLICATION TEOPAD POUR TERMINAUX MOBILES ;* Référence : *62905976 - 305 - rev-D - TEOPAD - CDS CSPN ;* Révision : D ; Date : *11/06/2013 ;*
[RTE]	*Rapport Technique d'Evaluation CSPN - TEOPAD version 1.1.06 sur terminal mobile Samsung S3 (Android 4.0.4);* Référence : *CSPN-RTE-TEOPAD-1.01*; Date : *16/01/2013.*
[SPEC-CRY]	*Teopad Spécifications cryptologiques;* Référence : *TCS/RSS/ISS/DDV/SCC/LCH,2011/46 – Rév D;* Date : *02/12/2011.*
[ANA-CRY]	*Evaluation CSPN du produit TEOPAD - Analyse des mécanismes cryptographiques;* Référence : *CSPN-CRYPTO-TEOPAD-1.01;* Version : *1.3 ;* Date : *06/03/2013.*
[GUIDES]	Guide d'installation : *Note d'installation et d'usage de la solution Teopad* Version : *D ;* Date : *06/02/2012.* Guide de déploiement : *Teopad – Note de déploiement* Date *: 06/02/2012.*

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
[REC-ANSSI]	Recommandations de sécurité relatives aux Ordiphones, version 1.0 du 15 mai 2013, ANSSI. Document disponible sur www.ssi.gouv.fr