CIBLE DE SECURITE CSPN

DE L'APPLICATION

TEOPAD

POUR TERMINAUX MOBILES

Prepared by :
THALES Communications & Security S.A.S
4 Avenue des Louvresses 92622 GENNEVILLIERS - FRANCE

CHANGES

Revision	Description
-A	Création du document
-B	Prise en compte des remarques de l'ANSSI
-C	Prise en compte des remarques d'AMOSSYS
-D	Prise en compte des remarques de l'ANSSI
-E	

Ind. + Date	-A 09-10-2012	-B 19-10-2012	-C 16-11-2012	-D 11-06-2013	-E	-F
Written by						
Name						
Role						
Signature						
Checked by						
Name						
Role						
Signature						
Approved by						
Name						
Role						
Signature						

TABLE DES MATIERES

1. INTRODUCTION

Le présent document est la cible de sécurité pour l'évaluation CSPN du produit identifié au §1.1

1.1. IDENTIFICATION DU PRODUIT

Nom du produit: TEOPAD

Nom commercial du produit: TEOPAD

Version soumis à évaluation: 1.1.06

Produit évalué sur: Android 4.0.3, sur terminal mobile Samsung S3

Développeur: THALES Communications and Security (TCS)

Catégorie du produit : Matériel et logiciel embarqué

Nota : *Par la suite l'emploi des termes « produit », « TEOPAD », « application TEOPAD » se réfèrent à l'application sur le terminal mobile. Les termes « solution TEOPAD » se réfèrent au système dans sa globalité incluant l'application sur le terminal mobile et les serveurs installés dans le SI de l'entreprise.*

1.2. STRUCTURE DU DOCUMENT

Le présent document est conforme à la structure des cibles de sécurité CSPN [CSPN] :

– Le chapitre 1 décrit le produit soumis à évaluation.

– Le chapitre 2 présente la définition de la problématique de sécurité, à savoir la liste des biens sensibles protégés, la liste des utilisateurs du produit et la liste des menaces que le produit contre.

– Le chapitre 3 donne les fonctions de sécurité implémentées par le produit pour contrer les menaces.

– Le chapitre 4 fournit les recommandations de mise en œuvre du produit.

1.3. REFERENCES

	Titre	Référence	Version	Classification
CSPN	Certification de Sécurité de Premier Niveau	1417/ANSSI/SR	1	Public
RGS_B_1	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques Annexe B1 du Référentiel Général de Sécurité	N/A	1.20	Public

Tableau 1:Références

1.4. GLOSSAIRE

TMC	TEOPAD Management Center
TMA	TEOPAD Management Agent
SE	Security Element
SEM	Secure Element Manager
SCM	Secure Configuration Manager
SAM	Secure Application Manager
TMP	TEOPAD Market Place
RVP	ReVerse Proxy
MDM	Mobile Device Management
DSI	Direction des Systèmes d'Information
PKI	Public Key Infrastructure
VSE	Virtual Secure Element
PRNG	Pseudo-Random Number Generator

1.5. DESCRIPTION DE LA SOLUTION TEOPAD

1.5.1. PRINCIPES GENERAUX DE LA SOLUTION TEOPAD

TEOPAD est une solution de sécurisation des applications professionnelles sur les smartphones et les tablettes, développée par Thales et destinée au monde de l'entreprise et des administrations.

La solution TEOPAD permet de créer sur le terminal un environnement professionnel de confiance qui peut cohabiter avec un contexte personnel ouvert. Cet environnement professionnel se présente sous la forme d'une application qui peut être lancée après une authentification forte 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 complètement isolé de la partie personnelle et native par une technologie de sandboxing brevetée.

Cette partie entièrement chiffrée et contrôlée, 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 déployées dans l'environnement professionnel proviennent obligatoirement du « TEOPAD Market Place » privatif de l'organisation et ne peuvent en aucun cas être téléchargées à partir d'un kiosque public.

Par ailleurs, la connexion aux ressources de l'entreprise (Intranet, messagerie, serveurs de fichiers, etc.) se fait obligatoirement de façon chiffrée et authentifiée à travers les réseaux opérateurs. 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 SI 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.

1.5.2. ARCHITECTURE GLOBALE DE LA SOLUTION TEOPAD

La solution TEOPAD est constituée des éléments suivants :

– Pour l'utilisateur
  - L'application TEOPAD à installer sur le terminal mobile.
  - L'application client TEOPAD Market Place

– Pour l'entreprise

  L'infrastructure TEOPAD est particulièrement légère puisqu'elle ne requiert aucun élément propriétaire pour connecter les utilisateurs au système d'information.

  Elle permet un déploiement puis une exploitation centralisés et industrialisés de TEOPAD. Les outils permettent notamment de créer des profils génériques ou personnalisés, et donc de s'adapter à des flottes de grande dimension ou spécialisées par métiers.

L'infrastructure de gestion comprend les modules suivants :

– TEOPAD Management Center (TMC)

  TMC permet d'enrôler et de gérer les utilisateurs TEOPAD. Cette station s'interface avec les éléments existants du système d'information (annuaire et PKI) en utilisant des protocoles standards (LDAP, XKMS), ce qui facilite l'intégration dans le système d'information. Le TMC dispose de 3 fonctions :
  - Secure Element Manager (SEM) permet de personnaliser le support d'authentification de l'utilisateur;
  - Secure Configuration Manager (SCM) permet de générer les fichiers de paramétrage des applications professionnelles sécurisées (par exemple adresses des serveurs, comptes de messagerie, bookmarks, etc.);
  - Secure Application Manager (SAM) permet le traitement des applications prises sur étagère pour les sécuriser dans l'environnement professionnel de TEOPAD;

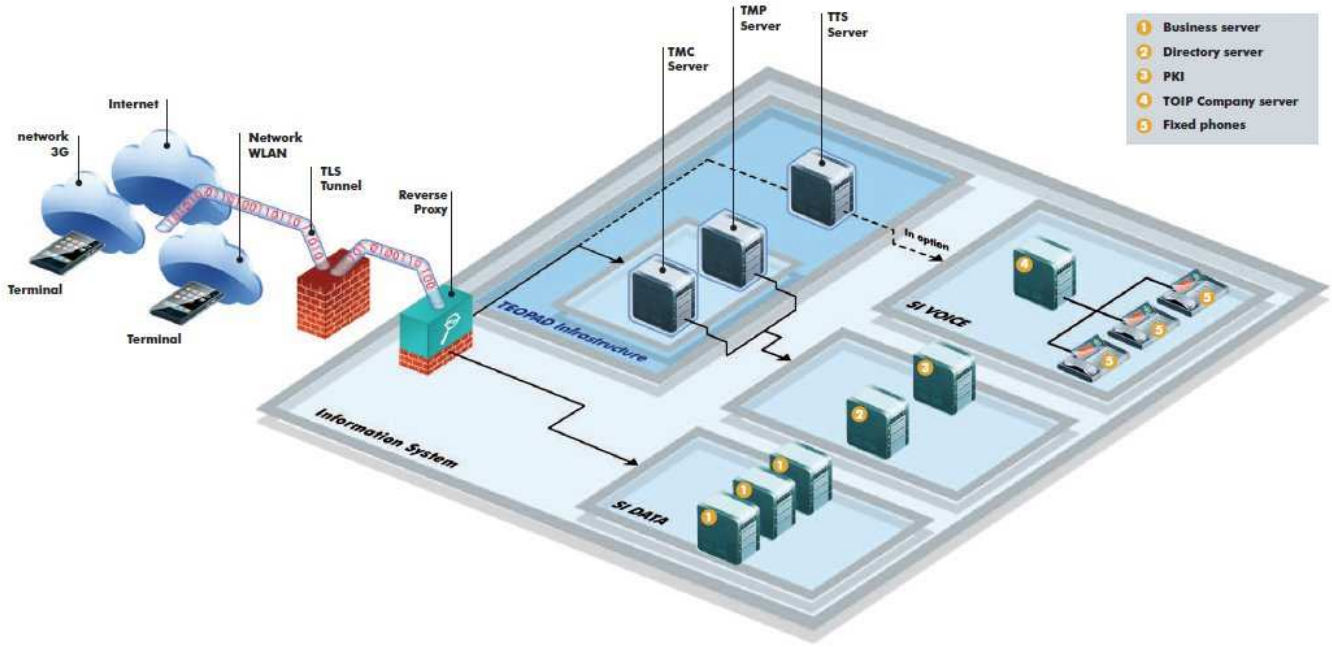
– TEOPAD Market Place (TMP)

  Le TMP est le magasin d'applications dédié aux applications professionnelles sécurisées par TEOPAD. Il est sous contrôle de l'organisation et permet de mettre à disposition des utilisateurs, selon leur métier, des applications sécurisées et les paramètres de configuration de celles-ci. Ce système permet de gérer les différentes versions d'une même application, les mises à jours, les dépendances des applications et la création de « bundle » d'applications.

– ReVerse Proxy (RVP)

  Point d'entrée unique des flux entrants et sortants des applications TEOPAD, le serveur reverse proxy
  - vérifie la validité des demandes de connexion au système d'information grâce à un mécanisme d'authentification mutuelle avec le terminal. Ce mécanisme est basé sur une vérification de certificats;
  - termine les tunnels TLS établis par les terminaux;
  - masque l'infrastructure du système d'information;

- effectue une rupture protocolaire;



La solution TEOPAD est par ailleurs compatible et peut s'interfacer avec les outils de Mobile Device Management (MDM) du marché.

1.5.3. DEPLOIEMENT DE LA SOLUTION TEOPAD

1.5.3.1. Côté de l'entreprise

Le déploiement de la solution TEOPAD se décompose en deux étapes :

– préparation du déploiement par l'organisation;

– enrôlement des utilisateurs.

<u>Préparation du déploiement</u>

– Sécurisation des applications à déployer :

  La DSI (Direction des Systèmes d'Information) de l'organisation séléctionne les applications professionnelles qu'elle souhaite mettre à disposition des utilisateurs. Puis,via le module SAM du TEOPAD Management Center (TMC), elle les sécurise, les signe et les publie sur le TEOPAD Market Place.

  Les applications sont signées à l'aide d'un certificat délivré par la PKI de l'organisation ou par un certificat auto-généré par le TMC.

– Préparation de profils :

  - Un profil de sécurité contient la politique de sécurité définie par la DSI.

TEOPAD permet de gérer plusieurs politiques de sécurité affectées à différents groupes d'utilisateurs.

Les profils contiennent par exemple les données suivantes :

– taille et format du code d'authentification;
– nombre de tentatives d'authentification avant blocage du terminal;
– durée de la session TEOPAD;
– type d'élément de sécurité;
– etc.

- Création de profils de configuration.

  Cette phase concerne la création de profils de configuration pour chacune des applications. Un profil contient un formulaire pour les données propres à chaque utilisateur, ainsi que les informations communes à tous les utilisateurs.

  Par exemple :

  – FQDN du serveur mail;
  – paramètres du service TLS;
  – etc.

Enrôlement des utilisateurs

Cette étape consiste à inscrire l'utilisateur au service TEOPAD.

Elle comprend la génération d'un élément de sécurité (logiciel ou matériel) et la configuration de l'environnent TEOPAD propre à chaque utilisateur. Suite à cette étape :

– l'élément de sécurité et le code d'authentification TEOPAD sont transmis à l'utilisateur final;
– les données de configuration utilisateur sont publiées sur le TMP.

1.5.3.2. Côté utilisateur

– Installation du client TEOPAD Market Place

  Le client TMP peut être déployé de différentes manières sur les terminaux via :

  - la carte microSD, si ce format est retenu pour l'élément de sécurité;
  - le portail web de l'organisation;
  - un outil de management de flotte (MDM).

– Installation des applications

  Dès qu'il possède l'application client TMP sur son terminal, l'utilisateur est en mesure de télécharger puis d'installer l'application TEOPAD et les applications professionnelles sécurisées mises à sa disposition par l'organisation.

  Le client TMP lancera automatiquement l'installation et la préconfiguration :

  - de l'application professionnelle sécurisée choisie;
  - des dépendances de celle-ci.

1.6. DESCRIPTION DU PRODUIT

1.6.1. PÉRIMÈTRE ÉVALUÉ

Le produit soumis à évaluation est l'application TEOPAD installée sur un terminal mobile munis du système Android.

Le terminal mobile utilisé et la version d'Android pour l'évaluation sont identifiés au §1.1.

Le §1.8 indique la plateforme d'évaluation précise, en particulier :

– Le SE fourni pour les tests est Giesecke & Devrient Mobile Security Card SE 1.0.

– Les tests de communications sont faits sur l'interface Wifi.

1.6.2. PRINCIPALES FONCTIONNALITÉS DU PRODUIT

Les principales fonctionnalités de sécurité du produit sont :

– Le sandboxing :

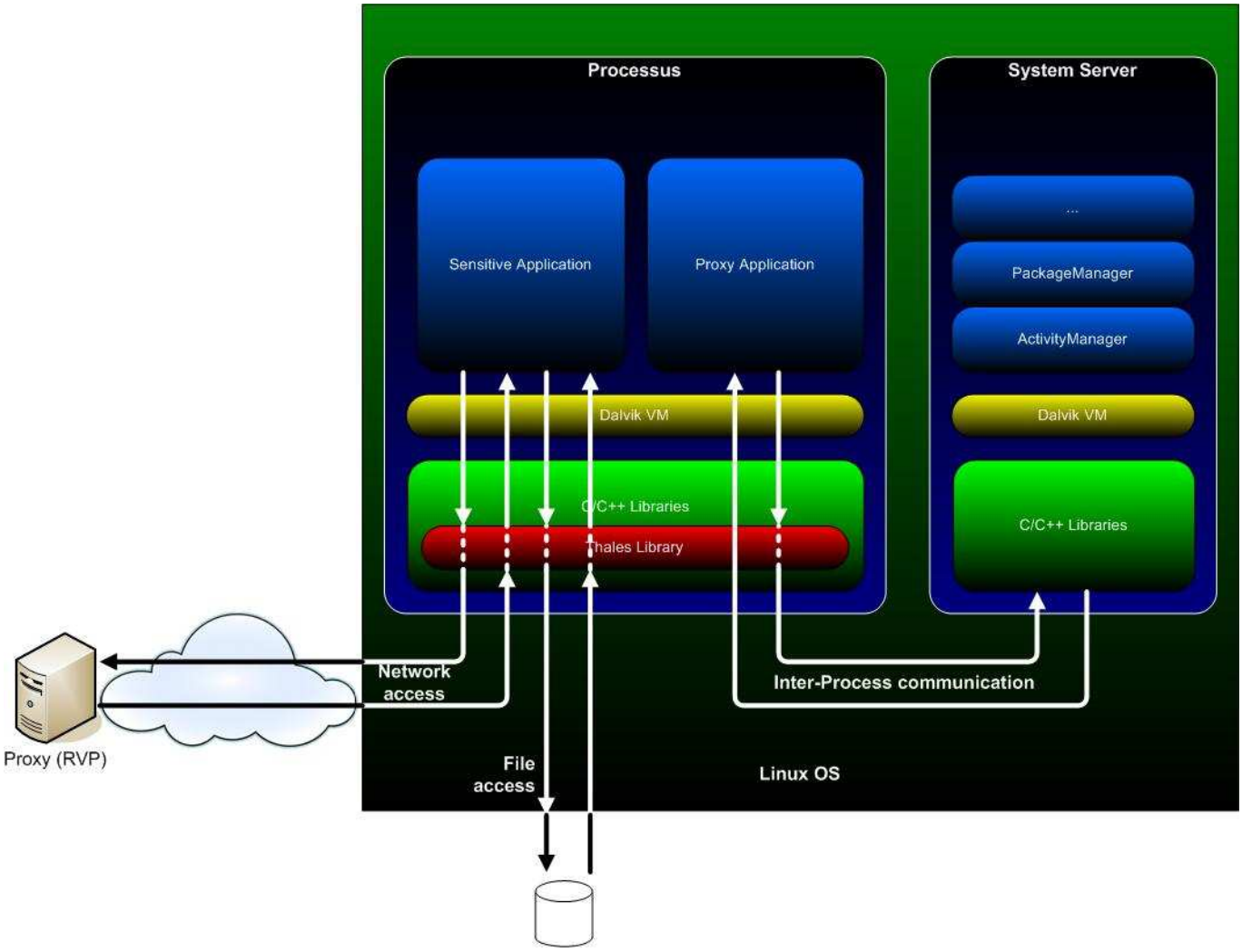
- Contrôle de l'intégrité des applications sécurisées
- Environnement d'exécution sécurisé
- Protection des données stockées en confidentialité et intégrité (AES 128 ou 256 bits en mode GCM)

– La protection des canaux de communication réseaux :
  - TLS
  - SIP-TLS, SRTP

1.7. ARCHITECTURE

Le produit est utilisé sur un système d'exploitation Android. Les mécanismes de sécurité apportés par le produit et son environnement sont les suivants :

– Le produit fournit un bac à sable pour les applications sensibles. Ce bac à sable apporte 3 principaux mécanismes :
  - Le premier garantit que tous les fichiers des applications sensibles sont protégés en confidentialité et en intégrité.
  - Le deuxième garantir que toutes les communications réseaux externes entre Internet et une application sensible utilisent un tunnel sécurisé et passent par un Proxy RVP de l'entreprise.
  - Le dernier contrôle et filtre tous les échanges une application sensible et une application externe..
– L'accès au bac à sable et aux applications sensibles est contrôlé via une authentification forte de l'utilisateur et par l'utilisation d'une clé cryptographique. L'authentification de l'utilisateur est faite sur un élément externe appelé « Secure Element » (SE). Après une authentification réussie, le SE donne l'accès aux clés cryptographiques utilisées par TEOPAD :
  - Une clé secrète pour la protection locale des données stockées et du fichier de configuration de TEOPAD..
  - Une clé privée avec son certificat permettant à TEOPAD de s'authentifier auprès du Proxy RVP lors de l'établissement d'un tunnel sécurisé.
  - Un certificat d'authentification du Proxy RVP permettant à TEOPAD d'authentifier le Proxy RVP lors de l'établissement d'un tunnel sécurisé.
– Par ailleurs les mécanismes de permissions d'Android (permissions basées sur la signature) sont utilisés pour assurer une défense en profondeur. Ces mécanismes assurent au niveau du système d'exploitation Android une ségrégation des accès aux fichiers et des environnements d'exécution.



1.8. PLATEFORME DE TEST

L'évaluation de l'application TEOPAD se fait sur les plateformes indiquées au §1.1.

A ces terminaux sont joints :

– Un Secure Element (SE) externe packagé dans une SDCard, du fournisseur Giesecke & Devrient. Le SE est composé d'un micro-contrôleur certifié CC EAL5+ et la carte à puce dans son ensemble (i.e. avec l'ensemble JavaCard) est certifié CC EAL4+. Le SE est personnalisé par TCS à l'aide de son centre de gestion (TMC).

– Un Virtual Secure Element (VSE). Le VSE intègre les mêmes données de sécurité que le SE mais se présente sous la forme d'un fichier chiffré. Comme pour le SE, le VSE est personnalisé par TCS à l'aide de son centre de gestion (TMC).

La liste des applications sécurisées installées est la suivante :

– Application d'initialisation :

Application	Version
TEOPAD installer	1.1.05
Driver G&D	2.4.0-02
Application de ressources TEOPAD	1.1.06
TEOPAD Management Agent	0.4.07

– Et les applications suivantes :

Application	Version
Email Pro	4.0.3
Exchange Pro	4.0.3
Calendar	4.0.3
Contacts	4.0.3
Download	4.0.3
KingSoft Office	4.5
Notepad Color Note	3.1.14
Astro	3.1.383.std

Pour l'évaluation, TCS met à disposition du centre d'évaluation son propre système TEOPAD (composé du RVP, d'un TMC, d'un TMP et d'un serveur Mail) en version de test.

2. DEFINITION DE LA PROBLEMATIQUE DE SECURITE

Ce chapitre présente la définition de la problématique de sécurité du produit. Il fournit les biens sensibles et les menaces.

2.1. BIENS SENSIBLES

Pour chaque bien sont indiqués les besoins de sécurité.

2.1.1. DONNÉES SENSIBLES DU PRODUIT

Alias	Description	Besoins de sécurité
D.CONFIGURATION	Fichier de configuration du produit.	Confidentialité Intégrité
D.SSK	Clé cryptographique secrète utilisée pour protéger les données stockées en locale. Il s'agit d'une copie en mémoire volatile de la clé secrète se trouvant dans le SE.	Confidentialité
D.PRIV_KEY	Clé cryptographique privée utilisée par la TOE pour s'authentifier auprès du RVP Il s'agit d'une copie en mémoire volatile de la clé privée se trouvant dans le SE.	Confidentialité
D.RVP_CERT	Certificat du RVP utilisé par la TOE pour authentifier le RVP. Il s'agit d'une copie en mémoire volatile du certificat se trouvant dans le SE.	Intégrité
D.KEYS	Toute autre clé et élément cryptographique temporaire en mémoire : – Graine du PRNG – Clés cryptographiques générées ou négociées	Confidentialité
D.USER_SECRET	Secret utilisé par le SE pour authentifier l'utilisateur (code PIN)	Confidentialité

2.1.2. DONNEES DES APPLICATIONS SENSIBLES

Alias	Description	Besoins de sécurité
D.SENSITIVE_APPLICATIONS_DATA	Données des applications sensibles, à savoir : – Données de configuration – Données d'authentification – Données de l'utilisateur – Etc…	Confidentialité Intégrité

2.2. MENACES

Dans les menaces ci-dessous, les attaquants et logiciels malveillants n'ont pas un accès privilégié ni de droits particuliers sur le terminal.

Libellé	Description	Couverture
T.PERMISSIONS	Une application malveillante téléchargée et installée sur le terminal mobile par l'utilisateur exploite ses propres permissions (qu'elles soient basées sur l'approbation de l'utilisateur ou sur signature) pour accéder à des données sensibles	– F.RESTRICTIVE_ACCESS – F.INTENT_PERMISSIONS – F.ROOT
T.ACCESS_RIGHTS	Une application malveillante téléchargée et installée sur le terminal mobile par l'utilisateur exploite ses droits Linux pour accéder à des données sensibles.	– F.SANDBOX – F.ZEROISATION
T.DATA	Un attaquant accède au terminal mobile (suite à un vol ou à une perte du terminal) et tente d'accéder aux données sensibles stockées dans le terminal	– F.USER_AUTH_FAILURE – F.SANDBOX – F.DEBUG
T.SPOOFING	Un attaquant déploie un faux point d'accès réseau sans fil (WiFi) auquel l'utilisateur se connecte via son terminal mobile afin d'intercepter toutes les communications	– F.TLS
T.COMMUNICATIONS	Un attaquant intercepte les échanges sans fil entre le terminal mobile et un point d'accès	– F.TLS
T.TMP_MASQUERADING	Un attaquant usurpe le TEOPAD Market Place faisant croire à l'utilisateur qu'il se connecte à son TMP légitime. L'attaquant utilise ce moyen pour déployer une application malveillante alors que l'utilisateur pense télécharger et installer une application sécurisée légitime	– F.TLS

3. FONCTIONS DE SECURITE

3.1. JOURNALISATION ET ALARME

F.AUDIT - AUDIT RECORD GENERATION

TEOPAD enregistre les événements d'audit en utilisant le mécanisme fourni par Android.

F.ALARM - ALARM NOTIFICATION

TEOPAD avertit immédiatement l'utilisateur lors de la survenance d'une alarme. L'avertissement se fait sous la forme d'une fenêtre de type « pop-up ».

3.2. CRYPTOGRAPHIE

F.KEYS - CRYPTOGRAPHIC KEYS

TEOPAD utilise les clés stockées dans le SE pour la protection des données locales et pour l'établissement des canaux de communication sécurisés.

Les clés cryptographiques ne sont utilisées qu'en mémoire volatile.

Les longueurs de clés sont

– Pour D.SSK: 128 ou 256 bits

– Pour D.PRIV_KEY: 2048 bits

– Pour la clé publique dans D.RVP_CERT: 2048 bits

– Pour les clés de sessions D.KEYS: 128 ou 256 bits

3.3. AUTHENTIFICATION DE L'UTILISATEUR

F.USER_AUTH_FAILURE - E.SE'S USER AUTHENTICATION FAILURE

Lorsque TEOPAD est informé par le SE que le *nombre maximum prédéfini de tentatives d'authentification* sur le SE a été atteint, il applique la politique de sécurité *Kill&Exit*.

3.4. CANAL DE COMMUNICATION SÉCURISÉ

F.TLS - TRUSTED CHANNEL

Pour toutes les communications réseaux entre une application sensible et un serveur, TEOPAD requièrent que celles-ci passent par un canal sécurisé établit entre le terminal mobile et un équipement distant prédéterminé (alias Proxy) au travers du protocole :

– Protocole TLS version 1.0 protégeant les données échangées en confidentialité et rejeu et permettant de détecter leur modification.

Lors de l'établissement du canal, TEOPAD :

– Requiert que l'équipement distant s'authentifie. Il utilise alors le certificat D.RVP_CERT ;

– Et s'authentifie auprès de l'équipement. Il utilise la clé privée D.PRIV_KEY.

Le canal de communication sécurisé est établit que le réseau utilisé soit Wifi ou la liaison data de réseau mobile.

F.PROTECT_COMM - CRYPTOGRAPHIC OPERATIONS: TRUSTED CHANNEL PROTECTION

TEOPAD utilise les algorithmes suivants pour la protection des canaux de communication :

– RSA-2048

– AES-CBC

– HMAC-SHA-1

Note : les suites cryptographiques TLS correspondantes sont : TLS_RSA_WITH_AES_128_CBC_SHA et TLS_RSA_WITH_AES_256_CBC_SHA

3.5. PROTECTION DES DONNEES ET DES PROCESSUS

F.SANDBOX - SANDBOX

TEOPAD fournit un bac à sable aux applications sensibles assurant une isolation à différents niveaux :

– Lors de l'exécution de l'application sensible, celle-ci ne partageant de contextes qu'avec les autres applications sensibles ;

– Lors du stockage de leurs données, celles-ci étant systématiquement chiffrées et protégées en intégré ;

– Lors de communications inter-applications, TEOPAD assurant un filtrage supplémentaire sur les IPC (Inter-Process Communication) ;

– Lors de communications externes, TEOPAD assurant que celles-ci passent par un canal sécurisé (cf F.TLS).

F.PROTECT_CONFIGURATION - CRYPTOGRAPHIC OPERATIONS: CONFIGURATION PROTECTION

TEOPAD protège ses données de configuration (D.CONFIGURATION) lors de leur stockage en utilisant AES-GCM.

F.PROTECT_APP_DATA - CRYPTOGRAPHIC OPERATIONS: APPLICATIONS DATA PROTECTION

TEOPAD protège les données des applications sensibles (D.SENSITIVE_APPLICATIONS_DATA) lors de leur stockage en utilisant AES-GCM.

F.ZEROISATION - ZEROISATION

TEOPAD assure l'écrasement de données stockées en mémoire volatile (mécanisme d'écriture de 0), lorsque les données sensibles ne sont plus utilisées et lors de l'exécution de la politique de sécurité *Kill&Exit*.

3.6. FONCTIONS DE SECURITE SPECIFIQUES A ANDROID

F.RESTRICTIVE_ACCESS - RESTRICTIVE ACCESS

TEOPAD donne à ses composants et à ceux des applications sensibles (*Activity*, *BroacastReceivers*, *Services*) des droits d'accès restreints pour les applications externes.

F.INTENT_PERMISSIONS - PERMISSIONS

TEOPAD donne à ses composants pouvant être appelés par un *Intent* et à ceux des applications sensibles des droits d'accès restreints (*Android's permissions*) dans leur *manifest*.

3.7. POLITIQUES DE SÉCURITÉ

F.K&E_POLICY - KILL&EXIT POLICY DESCRIPTION

La politique de sécurité *Kill&Exit* est la suivante:

– Lorsque TEOPAD est en cours d'exécution
  - Il ferme la session avec le SE
  - Il effectue un écrasement des données sensibles en mémoire volatile (F.ZEROISATION)
  - Il termine les processus des applications sensibles
  - Il se termine

– Lorsque TEOPAD est en cours de démarrage, il se termine immédiatement.

3.8. FONCTIONS SUPPORT

F.DEBUG - DEBUG MODE DETECTION

TEOPAD détecte lorsque le mode *debug* est actif. En cas de détection, il exécute la politique de sécurité *Kill&Exit*.

F.ROOT - ROOT MODE DETECTION

TEOPAD détecte lorsque le mode *root* est actif. En cas de détection, il exécute la politique de sécurité *Kill&Exit*.

4. RECOMMANDATIONS POUR L'ENVIRONNEMENT

4.1. RECOMMANDATIONS POUR L'UTILISATEUR

OE.USER - USER

Il est recommandé de sensibiliser les utilisateurs de TEOPAD aux menaces et des risques spécifiques aux terminaux mobiles, en particulier

– Du risque d'installer des applications inconnues

– Du risque de passer un terminal Android en mode « root » ou « debug »

– De ne pas utiliser depuis un ordinateur la capacité de stockage de masse USB du terminal pour y stocker des données sensibles car celles-ci ne seront pas protégées puisque ne passant pas par TEOPAD ni une application sécurisée.

Concernant les applications du domaine personnel :

L'utilisateur ne doit installer que des applications « réputées de confiance » dans son espace personnel. La confiance peut s'acquérir au travers de la notoriété d'une application, d'informations prises sur des forums ou auprès des administrateurs du SI de l'organisation de rattachement de l'utilisateur, …

Durant l'installation d'une application, l'utilisateur doit s'assurer que les permissions Android qu'elle demande sont en cohérence avec les services qu'elle propose.

Les applications du domaine personnelle ne doivent pas disposer de droits root ou permettre des élévations de privilèges intentionnelles.

Il est recommandé de toujours utiliser la dernière version disponible des applications (pro et perso).

4.2. RECOMMANDATIONS POUR L'ORGANISATION

OE.APPS.UPDATE - UPDATE OF SENSITIVE APPLICATIONS

Il est recommandé de mettre à disposition des utilisateurs la dernière version disponible de chaque application sécurisée.

OE.ORG.STARTUP - MOBILE DEVICE PREPARATION

Il est recommandé de transmettre aux utilisateurs des terminaux mobiles neufs. Si un terminal a déjà été utilisé par un précédent collaborateur, une opération de retrait de service assurant l'écrasement des données doit être préalablement réalisée.

OE.ORG.STARTUP - MOBILE DEVICE END OF LIFE

Lorsqu'un terminal est retiré de la flotte de terminaux de l'organisation, celui-ci doit faire l'objet d'une opération de retrait de service assurant en particulier l'écrasement des données. Si un SE (physique) était associé au terminal il est recommandé de le détruire.

OE.ORG.MOBILE_CONFIGURATION - MOBILE DEVICE CONFIGURATION

Il est recommandé de configurer le système Android de la manière suivante:

– Screen timeout: 2 minutes maximum
– Set up screen lock: yes (pattern, PIN code or password)
– USB debugging: disabled
– Stay awake: disabled
– Back up my data: disabled

OE.SIM_AUTHENTICATION - SIM CARD AUTHENTICATION

Il est recommandé de configurer le Secure Element (SE) de telle manière qu'il requiert la saisie d'un code PIN d'au moins 6 digits.

OE.ORG.UNKNOWN_SOURCE – UNKNOW SOURCE

Il est recommandé de configurer le système Android de la manière à ce que l'installation d'applications auto-signées ne soit pas permise (en fonction des cas de figure il peut cependant être nécessaire de désactiver ce paramètre afin d'installer TEOPAD ou une application sécurisée).