Cible de sécurité CSPN
Logiciel Trusted Foundations pour environnement OMAP4

Statut du document

Date d'application	Sans objet
Version actuelle	1.1.1

	Développeurs	**Commanditaire**	**Évaluateur**
Organisme(s)	Trusted Logic Mobility	Trusted Logic Mobility	Amossys

Diffusion

Nom ou rôle	**Organisation**
Développeurs Trusted Foundations	Trusted Logic Mobility
Consultants (CSPN TF/OMAP4)	Trusted Labs
Évaluateurs (CSPN TF/OMAP4)	Amossys
Certificateurs (CSPN TF/OMAP4)	ANSSI

Historique des versions

Date	**Version**	**Commentaire**
2012-06-27	1.0	Émission
2012-06-29	1.0.1	Mise à jour de la bibliographie
2012-12-03	1.1.0	Prise en compte des remarques de l'ANSSI : expliciter que le GDA est hors périmètre ; terminologie jeton -> identifiant ; définitions de confidentialité et authenticité (§4.1) ; intégrité de la HUK (G1) ; confidentialité des identifiants clients (G2)
2012-12-05	1.1.1	définitions plus habituelles des propriétés de sécurité (§4.1) ; terminologie : HUK -> MFK

Sommaire

1 Introduction

1.1 IDENTIFICATION DE LA CIBLE DE SÉCURITÉ

Cette cible de sécurité a été élaborée en vue d'une évaluation CSPN [RD1].

1.2 IDENTIFICATION DU PRODUIT

Catégorie	Identification
Nom commercial du produit	Trusted Foundations
Numéro de la version évaluée	SMCAG01.06.36315
Catégorie de produit	Logiciel embarqué

1.3 RÉFÉRENCES

Code	Référence	Nom
[RD1]	N°915/SGDN/DCSSI/SDR du 25 avril 2008	Certification de sécurité de premier niveau des technologies de l'information
[RD2]	CP-2010-RT-533-V1.0	Trusted Foundations™ — Developer Reference Manual (APIs V3.0)
[RD3]	Site internet ARM	http://www.arm.com/products/processors/technologies/trustzone.php

2 Argumentaire du produit

2.1 DESCRIPTION GÉNÉRALE DU PRODUIT

Le produit Trusted Foundations (TF) est un Système d'Exploitation sécurisé destiné à s'exécuter sur un dispositif portable tel qu'un téléphone mobile ou une tablette graphique.

Trusted Foundations apporte des services dédiés permettant de sécuriser le dispositif portable sans en perturber son fonctionnement.

Il partage son environnent d'exécution avec d'autres applications non-sécurisées en tirant avantage des fonctions d'isolation matérielle entre deux mondes d'exécution mises à disposition par le processeur sur lequel il s'exécute :

- Le monde normal où s'exécute un Système d'Exploitation Classique, comme Android, Linux, Windows Mobile, Symbian OS, ou tout autre OS ;
- Le monde sécurisé où s'exécute le système d'exploitation sécurisé TF qui se défend contre le monde normal, supposé hostile.

Communication entre le monde sécurisé et le monde normal :

Un moyen unique appelé SChannel est dédié aux échanges entre le monde normal et le monde sécurisé. Il s'agit d'un protocole de communication dédié qui sait gérer plusieurs requêtes concurrentes issues d'applications différentes et/ou multi-instanciées (*multithread*).

Le **Trusted Foundations Secure World** (*TFSW*) est la partie logicielle qui s'exécute dans le monde sécurisé. Elle s'accompagne d'une bibliothèque de fonctions qui s'intègre au système d'exploitation dans le monde normal qui propose les interfaces (*API*) pour invoquer les services disponibles dans le TFSW grâce à SChannel.

Description du TFSW :

Le TFSW propose un ensemble de services aux applications du monde normal. Il n'intervient que sur demande et se comporte en mode client / serveur. Il peut traiter en parallèle plusieurs requêtes provenant potentiellement de clients différents.

Le TFSW dispose de moyens calculatoires et de mémoire vive sécurisée pour répondre aux demandes des applications, mais il ne dispose pas de moyen de stockage rémanent pour sauvegarder les informations issues des applications, ou des données de travail (e.g. contexte). Il délègue ces fonctions de stockage au monde normal tout en assurant l'authenticité et la confidentialité des données sauvegardées, ainsi que l'impossibilité de les utiliser en dehors du dispositif portable où elles sont stockées.

Les applications clientes sont identifiées individuellement, et les données et services d'une application ne sont pas accessibles par une autre application.

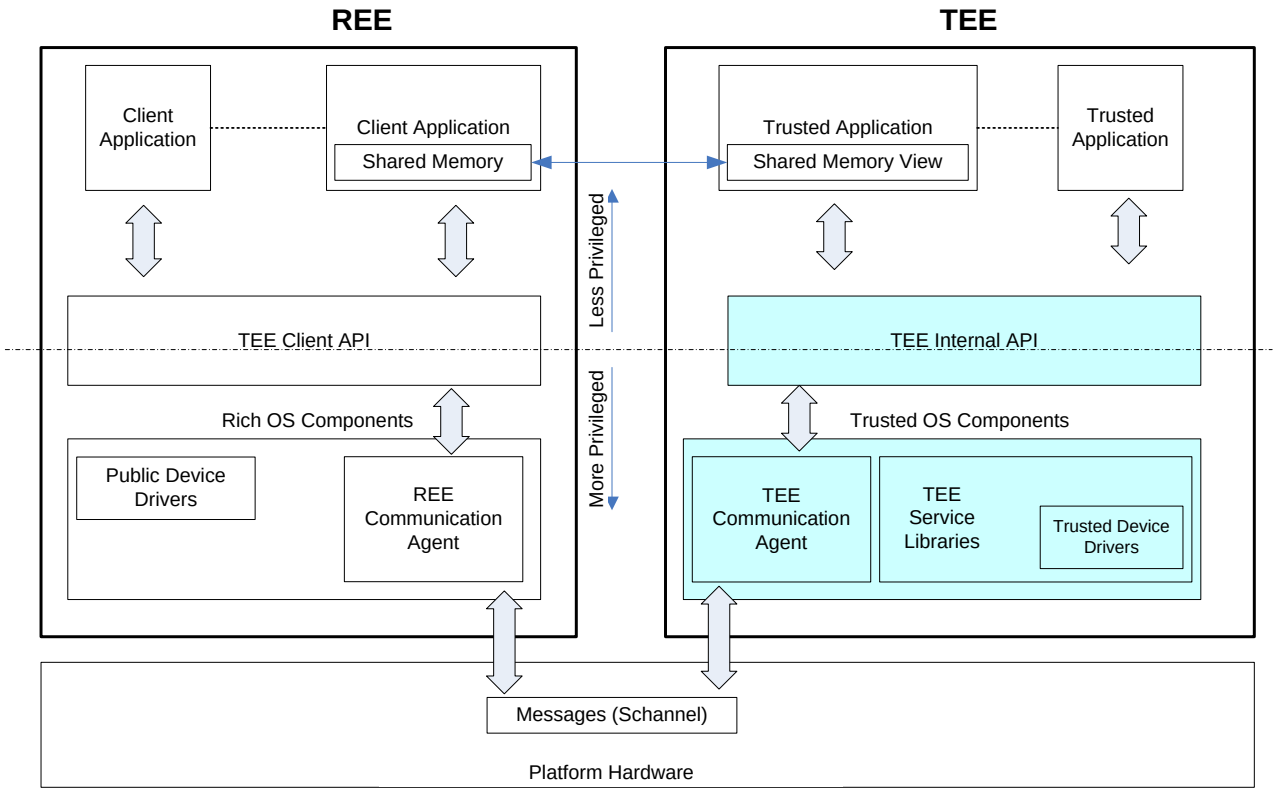
Les services de base suivants sont proposés au monde normal :

- Système de fichiers : ce service chiffre et signe à la volée les données stockées dans le système de fichiers (confidentialité et authenticité). Si une application venait à accéder aux données stockées pour une autre application (lecture mémoire flash, etc.), elle ne pourrait pas les exploiter ;
- Cryptographie : ce service protège notamment la confidentialité des données sensibles (clés) contre le monde normal. Le service de cryptographie offre une large étendue d'algorithmes symétriques et asymétriques ainsi que des fonctions de génération de clés et de stockage rémanent de clés.

Le TFSW contient également un service de délégation de stockage qui assure le stockage de données au sein du monde normal pour le compte du monde sécurisé.

Optionnellement, le TFSW peut embarquer d'autres services (Trusted Applications), par exemple un service Digital Right Management (*DRM*) pour gérer l'accès aux services de télévision à péage. En pareil cas, le service DRM est chargé lors de la phase d'intégration.

La figure suivante présente l'architecture globale du système d'exploitation Trusted Foundations dans son environnement : TEE (Trusted Execution Environment) et REE (Rich Execution Environment) sont les termes génériques utilisés pour désigner l'environnement sécurisé d'exécution (ici TF) et l'environnement normal d'exécution, respectivement.



2.2 DESCRIPTION DE L'UTILISATION DU PRODUIT

Le produit n'est pas immédiatement fonctionnel après qu'il ait été généré. Il doit être intégré et paramétré pour le dispositif portable où il s'exécutera. C'est après cette étape qu'il sera activé et utilisé (démarrage du matériel).

Intégration :

Le logiciel Trusted Foundations est mis à disposition d'un intégrateur sous un format binaire accompagné des instructions et outils permettant de configurer le logiciel sur le dispositif portable.

- L'intégrateur active le dispositif d'amorçage sécurisé (*secure bootloader*) résidant en partie dans la ROM du processeur et en partie dans la mémoire programmable de l'appareil.
- Il utilise l'outil de configuration fourni par Trusted Logic (appelé *postlinker*) pour produire le logiciel exécutable prêt à fonctionner sur le dispositif portable.

Usage final :

Trusted Foundations met ses services à disposition des applications du monde normal, supposé hostile.

2.3 DESCRIPTION DE L'ENVIRONNEMENT D'UTILISATION PRÉVU

Intégration :

La phase d'intégration est réalisée dans les locaux de l'intégrateur lors de la production du dispositif portable.

Utilisation :

Le dispositif portable est disponible pour l'utilisateur final qui peut l'utiliser à sa guise. En particulier, il peut charger des applications dans le monde normal, lesquelles pourront interagir avec TFSW.

2.4 DESCRIPTION DES HYPOTHÈSES SUR L'ENVIRONNEMENT

Hypothèses lors de la phase d'intégration :

La phase d'intégration consiste à charger TFSW sur le processeur, accompagné des autres logiciels utiles au bon fonctionnement du dispositif portable. C'est lors de cette étape qu'il convient de paramétrer correctement l'ensemble afin d'en garantir la sécurité en usage final.

Les hypothèses sont les suivantes :

- L'intégrateur est considéré comme non hostile.
- Trusted Foundations est intégré et installé sur microprocesseur autorisé par Trusted Logic.
- L'intégrateur suit scrupuleusement les instructions de Trusted Logic afin d'assurer :
    - que le composant matériel dispose d'un code en mémoire morte (Secure ROM) correspondant à la version attendue du processeur ;
    - que la partie réinscriptible de la mémoire rémanente contient les mises à jour pour la Secure ROM fournies par le fournisseur du processeur et attendues par TFSW ;
    - que TFSW est initialement copié dans la mémoire sécurisée par le secure bootloader qui vérifie sa signature et que son espace de travail réside en mémoire sécurisée (découpage de la mémoire).
- Les logiciels s'exécutant en mode sécurisé (outre TFSW) sont conçus pour :
    - interdire l'exécution en mode sécurisé de tout autre logiciel en dehors de la Secure ROM, des mises à jour mentionnées ci-dessus et de TFSW ;
    - assurer l'intégrité des paramètres de fonctionnement du composant, en particulier le partage de la mémoire entre le monde sécurisé et le monde normal.
- En particulier, aucun logiciel non fourni par le fournisseur du processeur ou par Trusted Logic n'est autorisé à s'exécuter dans le mode sécurisé, ce qui signifie que l'intégrateur ne rajoute pas de service (*Trusted Application*).
- Les moyens matériels ou logiciels de déverminage disponibles sur le processeur sont désactivés.
- La clé maîtresse du composant (MFK : Master Fuse Key) est protégée en intégrité et en authenticité par le processeur OMAP sur lequel TFSW fonctionne.
- Il n'existe pas de moyen pour changer la configuration lorsque la phase d'intégration est terminée.

- L'authenticité du TFSW est vérifiée lors du démarrage du dispositif par un code sécurisé qui ne peut être remplacé ou trompé.

Usage final :

Pas d'hypothèse (environnement supposé hostile).

2.5 DESCRIPTION DES DÉPENDANCES

TF doit être exécuté sur une plateforme matérielle avec les caractéristiques suivantes :

- Processeur OMAP4 type HS (« High Security ») ;
- Les mises à jour pour la Secure ROM ;
- Système d'exploitation Android Gingerbread.

L'intégrateur produit le dispositif portable tel que :

- La clé maîtresse du composant (MFK d'au moins 128 bits), brûlée dans des fusibles lors de l'intégration est unique à chaque dispositif portable, et est conservée secrète par l'intégrateur. Elle n'est pas modifiable et n'est accessible que par le monde sécurisé (caractéristique intrinsèque du composant) ;
- Un dispositif d'amorçage sécurisé (« secure bootloader ») contrôle l'intégrité du produit lors de son démarrage et assure que seuls les logiciels autorisés peuvent s'exécuter dans le monde sécurisé. Ce dispositif réalise également les opérations suivantes :
    - Il réserve une zone de mémoire RAM qui est accessible uniquement par le monde sécurisé.
    - Il copie TFSW dans la mémoire sécurisée, et lui communique l'adresse d'un espace de travail dans la mémoire sécurisée qui lui est réservé.
- Le logiciel chargé de gérer les transitions intervenant lorsque le dispositif portable est mis en veille (mode hibernation), éteint, active ou désactive certains de ses composants ou certaines parties de ses composants, assure que seuls les logiciels autorisés peuvent s'exécuter dans le monde sécurisé (gestion de l'énergie).

2.6 DESCRIPTION DES UTILISATEURS TYPIQUES

Le logiciel Trusted Foundations est utilisé par le système d'exploitation et les applications existant sur le dispositif portable où il est installé. Ces utilisateurs sont les clients du TF et sont identifiés à l'aide d'identifiants dédiés.

2.7 DESCRIPTION DU PÉRIMÈTRE DE L'ÉVALUATION

L'évaluation porte sur logiciel Trusted Foundations Secure World s'exécutant sur une plateforme OMAP4 telle que décrite chapitre 2.5, où seuls les services de base sont inclus.

Le générateur aléatoire du processeur OMAP est hors du périmètre de l'évaluation.

3 Description de l'environnement technique de fonctionnement

TF est un système d'exploitation conçu pour fonctionner sur un processeur OMAP4 (voir liste des dépendances au chapitre 2.5), embarqué dans un dispositif portable tel qu'un téléphone cellulaire ou une tablette graphique. Il cohabite avec d'autres systèmes d'exploitation et logiciels requis pour le bon fonctionnement du dispositif portable.

Il fonctionne donc dans un environnement logiciel ouvert, ou des applications hostiles peuvent être chargées (selon le système d'exploitation principal du dispositif portable).

Toutefois, TF est protégé par la technologie « TrustZone® » [RD3] présente dans le processeur où il fonctionne. Cette technologie permet une isolation matérielle entre deux « mondes d'exécution » :

- Le monde normal exécute un Système d'Exploitation Classique, comme Android, Linux, Windows Mobile, Symbian OS, ou tout autre OS ;
- Le monde sécurisé exécute le Produit et se défend contre le monde normal, supposé hostile.

Ces deux mondes s'exécutent sur le même processeur et partagent les unités de calcul et l'accès au ressources du composant (caches, mémoires, périphériques, etc.).

4 Description des biens sensibles que le produit doit protéger

4.1 PROPRIÉTÉS FONDAMENTALES

Les propriétés fondamentales des biens sensibles sont les suivantes :

- Confidentialité : Un bien est confidentiel lorsqu'il n'est accessible qu'à ceux dont l'accès est autorisé.
- Intégrité : Un bien est protégé en intégrité lorsqu'il ne peut être modifié que par ceux qui y sont autorisés.
- Authenticité : Un bien est protégé en authenticité lorsque son origine et son contenu sont vérifiés et ne sont pas modifiables.

Pour chaque bien protégé par TF, un tableau indique les protections qui s'y appliquent.

4.2 BIENS PROTÉGÉS PAR TF

Les biens sensibles protégés par TF sont:

- G1 : Master Fuse Key (128 random bits minimum).

  ☑ Confidentialité ☑ Intégrité ☐ Authenticité

  Chargée par l'intégrateur, TFSW s'assure qu'elle ne peut être dévoilée par son intermédiaire et ne permet pas de la modifier.

- G2 : Identifiant d'accès de l'application cliente.

  ☑ Confidentialité ☑ Intégrité ☐ Authenticité

  Une application s'identifie auprès du TFSW grâce à un identifiant d'accès, choisi par le monde normal. Lorsqu'une application tente d'accéder à une donnée protégée (fichier ou objet cryptographique), TFSW s'assure que l'identifiant d'accès fourni par l'application requérante correspond à l'identifiant d'accès propriétaire de cette donnée. TFSW assure en particulier l'intégrité des identifiants indiqués comme propriétaire d'une donnée. De plus, TFSW ne dévoile jamais l'identifiant d'une application au monde normal.

- G3 : Système de fichiers sécurisé.

  ☑ Confidentialité ☐ Intégrité ☑ Authenticité

  Automatiquement crée par TFSW, il est constitué de plusieurs fichiers chiffrés à l'aide de clés connues de TF seul. Il est stocké dans une zone du monde normal et peut être lu ou modifié par un attaquant. Pour cette raison, il est protégé en confidentialité et en authenticité.

  L'ensemble des données à protéger y sont stockées. Des zones réservées aux applications clients et à TF y sont crées sur demande.

  Le système de fichiers n'est protégé qu'en authenticité et non en intégrité, dans la mesure où un attaquant peut le remplacer dans son ensemble par une ancienne version du système de fichiers sur le même dispositif. TF assure l'authenticité globale de cette ancienne version.

- G4 : Données confidentielles des applications clientes et de TF (sauvegardé dans le système de fichier sécurisé G3).

  ☑ Confidentialité ☑ Intégrité ☑ Authenticité

  TFSW s'appuie sur le système de fichiers sécurisé pour garantir la confidentialité et l'authenticité des données des applications clientes et accepte les requêtes de plusieurs applications sans relations entre elles. À l'aide d'un identifiant d'accès (cf. G2) il détermine quelles données et service sont accessibles à quelle application.

  TFSW garantit la séparation des informations application par application, interdisant à une application cliente d'accéder aux données d'une autre application. Cette garantie couvre à la fois la bonne utilisation du système de fichiers sécurisé et la protection des données en mémoire vive.

- G5 : Objets et tokens de clés cryptographiques

  ☑ Confidentialité ☑ Intégrité ☑ Authenticité

  L'API cryptographique de TFSW permet de stocker des clés de manière rémanente. Un tel matériel cryptographique rémanent est appelé token. TFSW s'appuie sur le système de fichiers sécurisé (c.f. G3) pour garantir la confidentialité, l'intégrité et l'authenticité des tokens de clés cryptographiques. Chaque token est lié à un propriétaire (TFSW ou une application cliente). TFSW détermine les autorisations d'utilisation d'un token en utilisant un identifiant d'accès (c.f. G2).

  TF garantit la séparation des informations application par application, interdisant à une application d'accéder aux données d'une autre application.

5 Description des menaces

Les menaces considérées sont les suivantes :

- **M1. Attaque directe par accès mémoire :**
  le monde normal réussit à subvertir le cloisonnement entre les deux mondes et lit ou modifie directement des données. La subversion des mécanismes de cloisonnement peut utiliser tout moyen à disposition du monde normal ;
- **M2. Attaque indirecte par les protocoles :**
  le monde normal émet des commandes incorrectes ou mal formées et réussit à amener le produit à lui retourner la valeur de données confidentielles ou à modifier des données protégées ;
- **M3.Attaque indirecte par les API TF :**
  le monde normal inclut des paramètres avec des caractéristiques non prévues pour provoquer des erreurs non gérées, et réussit à amener le produit à lui retourner la valeur de données confidentielles, à modifier des données protégées, à réaliser des calculs en utilisant des secrets qui ne lui sont pas associés, à réaliser un calcul interdit avec la clé courante ;
- **M4. Attaque sur le stockage de données dans le monde normal :**
  TFSW s'appuie sur le monde normal pour stocker et lire ses données préalablement chiffrées et signées. Le monde normal peut manipuler à tout moment ces données et donc les attaquer ; L'attaque consiste à modifier tout ou partie des informations stockées dans le monde normal, et de parvenir ensuite à les présenter de nouveau au monde sécurisé sans qu'il ne s'aperçoive des changements ;

- **M5. Contournement des contrôles d'accès :**
  une application cliente réussit à obtenir ou modifier les données privées d'une autre application cliente, alors qu'elle n'est pas capable de présenter l'identifiant de l'autre application. On notera que la protection des identifiants au sein du monde normal ne relève pas de la présente cible de sécurité ;
- **M6. Attaque sur la gestion de l'énergie :**
  le monde normal requiert une mise en veille (extinction des processeurs, avec maintien des données en mémoire vive) et en manipulant les données de sauvegarde ou de contrôle lors du redémarrage, réussit à accéder aux données confidentielles ou à modifier des données protégées en intégrité.

6 Description des fonctions de sécurité du produit

Les fonctions de sécurité du produit sont les suivantes :

- **FS1 : cloisonnement mémoire entre les deux mondes**

  TFSW assure la confidentialité et l'authenticité des opérations qu'il réalise et des données qu'il manipule dans le monde sécurisé où il est installé. Ces propriétés s'appuient sur des fonctionnalités de la plate-forme (TrustZone®).

  Lors d'opérations prédéterminées (chiffrement/déchiffrement d'un flux par exemple), TFSW accède directement à la mémoire du monde normal tout en assurant que seules les données prévues y soient écrites ou lues (passage de paramètres, retour du résultat d'exécution d'un service).

- **FS2 : robustesse du protocole de communication SChannel**

  TFSW assure que l'implémentation du protocole SChannel filtre toutes les requêtes en vérifiant systématiquement leur syntaxe. Une commande non conforme soit est rejetée, soit provoque un mutisme du monde sécurisé jusqu'au redémarrage complet du matériel (mise hors tension puis mise sous tension).

- **FS3 : Mutisme**

  Quand TFSW détecte un comportement susceptible de dénoter une attaque, mais qui peut aussi bien être une mauvaise utilisation par inadvertance, il essaye d'abord de répondre par un code d'erreur. Si, pour une raison quelconque, il n'y parvient pas, il existe un mécanisme de mutisme qui rend le monde sécurisé inopérant jusqu'au prochain démarrage du matériel (mise hors tension puis sous tension).

- **FS4 : stockage sécurisé des données des clients**

  TFSW propose un système de fichiers sécurisé qui assure la confidentialité et l'authenticité des données qui y sont stockées. Les commandes disponibles sont celles habituellement proposées en pareil cas : Open, Close, Read, Write, Rename, Delete, …

  Chaque client dispose de son espace de stockage inaccessible aux autres. Les clients sont identifiés par leur identifiant d'accès. Ce service chiffre et signe à la volée les données stockées dans le système de fichiers (confidentialité et authenticité). Outre les données utilisateurs contenues dans des fichiers, le système de fichiers sécurisé stocke aussi des tokens de clés cryptographiques utilisables avec l'API cryptographique (cf. FS5).

  La sécurité est assurée à l'aide d'algorithmes cryptographiques. Les données sont protégées en confidentialité et en authenticité à l'aide de clés secrètes. L'authenticité du stockage est assurée globalement (et pas seulement fichier par fichier) en utilisant un arbre de condensats (« digests ») pour vérifier l'intégrité et l'authenticité. Les algorithmes utilisés sont SHA-256 pour

les contrôles d'intégrité, AES-CBC pour la confidentialité et HMAC-SHA-256 pour l'authenticité.

Si la sécurité du système de fichier n'est plus assurée, TFSW en bloque l'accès ou le reformate.

- **FS5 : Services cryptographiques**

  Lorsqu'une application cliente souhaite utiliser les services cryptographiques de TF, elle doit tout d'abord créer un matériel cryptographique (transitoire ou rémanent) contenant la clé cryptographique ainsi que des attributs déterminant son mode d'utilisation. Un objet cryptographique se trouve verrouillé immédiatement après sa création, et ne peut être modifié ensuite.

  TFSW garantit que chaque objet cryptographique ne pourra être utilisé que selon les attributs qui lui ont été attribués au moment de sa création.

- **FS6 : Authentification par identifiant et gestion des autorisations**

  TFSW garantit que chaque application cliente n'a accès qu'aux objets cryptographiques rémanents qu'elle a elle-même stocké. Les applications clientes sont identifiées par leur identifiant d'accès. Quant aux objets cryptographiques transitoires, TFSW garantit qu'ils ne sont accessibles qu'au sein de la session (qui lie uniquement une application cliente et TFSW) dans laquelle ils ont été créés.

  L'accès peut aussi être demandé en mode public. Aucun identifiant n'est requis dans ce cas, mais aucun accès ou stockage de données rémanentes n'est possible.