Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-CSPN-2008/01

TRANGO Hypervisor version 1.5.61 sur plate-forme OMAP 2430

Paris, le 11 septembre 2008

Le Directeur central 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 devrait 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 la Direction centrale de la sécurité des systèmes d'information (DCSSI), 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 nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.gouv.fr

Référence du rapport de certification

DCSSI-CSPN-2008/01

Nom du produit

TRANGO Hypervisor version 1.5.61 sur plate-forme OMAP 2430

Référence/version du produit

Version 1.5.61 - build 7224

Critères d'évaluation et version

CERTIFICATION SECURITE DE PREMIER NIVEAU (CSPN, Version expérimentale)

Développeur(s)

TRANGO Virtual Processors
22, avenue Doyen Louis Weil
38000 – Grenoble
France

Commanditaire

TRANGO Virtual Processor
22, avenue Doyen Louis Weil
38000 – Grenoble
France

Centre d'évaluation

AQL Groupe Silicomp
1 rue de la châtaigneraie, CS 51766, 35513 Cesson Sévigné Cedex, France
Tél : +33 (0)2 99 12 50 00, mél : cesti@aql.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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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

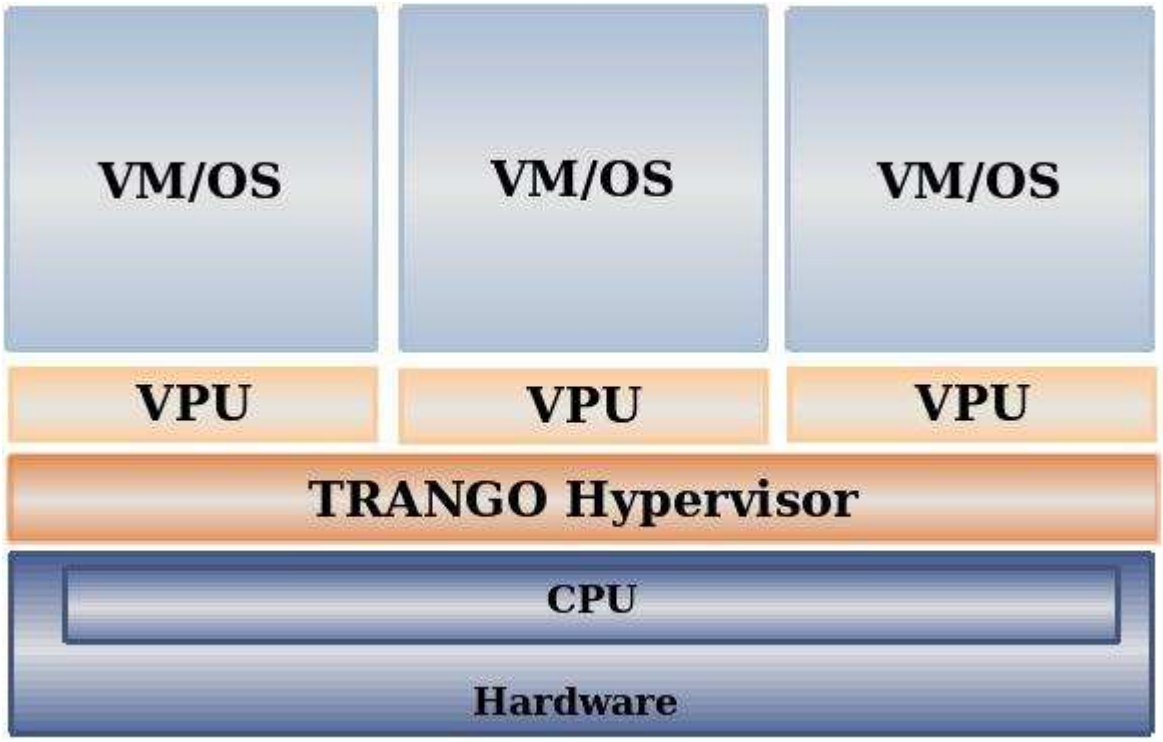
1. Le produit

1.1. Présentation du produit

Le produit évalué est « TRANGO Hypervisor version 1.5.61 sur plate-forme OMAP 2430 » développé par TRANGO Virtual Processors.

La principale fonctionnalité de sécurité de cet hyperviseur est de permettre l'exécution simultanée et sécurisée de plusieurs machines virtuelles (VM pour Virtual Machine) sur une plate-forme mono ou multi-coeurs.

L'hyperviseur virtualise les ressources matérielles et assure leur partage entre plusieurs VMs. Ces VMs peuvent faire fonctionner tout programme qui s'exécute normalement sur un processeur réel : applications autonomes, systèmes d'exploitation temps réel, etc. Le partitionnement créé par l'hyperviseur assure le cloisonnement entre les différentes VMs.



VM/OS pour Virtual Machine/Operating System, VPU pour Virtual Processor Unit, CPU pour Central Processor Unit.

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 : systèmes d'exploitation et de virtualisation**

1.2.2. Identification du produit

L'identification du produit peut-être réalisée par la lecture du registre VPR_RO.vmm_version lors de l'exécution d'une VM. Le numéro renvoyé est le numéro de « build » (ici, 7224).

1.2.3. Services de sécurité

TRANGO Hypervisor fournit les services suivants aux VMs :

- partage sécurisé des ressources (mémoire, unité centrale ou CPU (Central Processor Unit), périphériques) ;
- canaux de communication sécurisés inter-VMs ;
- gestion dynamique des VMs: création, destruction, gestion des ressources de l'unité centrale, débogage.

TRANGO Hypervisor est capable de gérer jusqu'à plusieurs centaines de VMs, suivant la plate-forme matérielle.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

- Phase 1 : développement de l'hyperviseur, réalisé par TRANGO Virtual Processors ;
- Phase 2 : développement / intégration de VMs utilisant TRANGO Hypervisor sur le produit matériel cible ;
- Phase 3 : utilisation du produit résultant.

Le produit faisant l'objet de la présente évaluation est celui issu de la phase 1 du cycle de vie.

1.2.5. Configuration évaluée

Le périmètre de l'évaluation couvre l'hyperviseur « TRANGO Hypervisor » à l'exception des fonctions suivantes qui seront désactivées par l'intégrateur dans le fichier de configuration du système, durant la phase d'intégration :

- supervision (modification des paramètres d'exécution autorisés) ;
- monitoring et micro-monitoring (lecture d'informations du système) ;
- débogage (déroutement du flot d'instruction) ;
- gestion de l'énergie (arrêt de certaines fonctionnalités et/ou VMs).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de Sécurité de Premier Niveau en phase expérimentale. Les références des documents se trouvent en annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La charge de travail prévue lors de la demande de certification était conforme à la charge de travail préconisée dans [CSPN] pour un produit ne comportant pas de mécanismes cryptographiques, soit 20 homme.jour. L'évaluation s'est déroulée de fin juin 2008 à fin juillet 2008.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [ST] 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.

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité.

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

Conforme à la cible de sécurité. Toutefois, l'évaluateur a été amené à préciser la portée de certaines des menaces. Ainsi, les attaques par canaux auxiliaires, les attaques physiques sur le composant, les attaques utilisant d'éventuelles non-conformités du composant ont été identifiées mais ont été exclues du périmètre de l'évaluation.

Le périmètre de l'évaluation couvre uniquement les menaces mises en œuvre par des attaques logicielles réalisées au travers de l'interface de l'hyperviseur.

En particulier, l'hyperviseur ne propose pas de mécanismes pour éviter la fuite d'informations critiques, lorsqu'elles circulent sur les bus mémoire ni de mécanismes pour éviter la fuite d'informations critiques (attaques basées sur l'analyse des temps d'exécution de l'ordonnanceur ou des manipulations du cache).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité. L'évaluateur a observé que le produit proposait également les fonctions de sécurité suivantes :

- Protection contre les attaques par déni de service (flot d'interruptions illicites inter-VMs, comportement du contrôleur d'interruption, allocation de toute la mémoire par une VM, utilisation de toute la ressource de l'unité centrale).
- L'hyperviseur propose un mécanisme de recouvrement qui assure qu'il ne risque pas de se retrouver dans un état non sûr en cas de défaillance matérielle.

2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité.

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

Pour l'évaluation, le produit TRANGO Hypervisor a été testé sur une carte matérielle correspondant à un téléphone mobile[1] complété par un module de Reset fourni par TRANGO Virtual Processors et une carte de débogage fournie par le fabricant du téléphone mobile.

Cette plate-forme est architecturée autour d'un processeur embarqué OMAP2430 (TI) basé sur un processeur de type ARMv6 en révision r0p6. Divers composants fonctionnels gravitent autour de ce processeur :

- un contrôleur mémoire (DRAM et FLASH), connecté via un bus mémoire ;
- un affichage de type « cristaux liquides », connecté via un bus RGB et un bus SPI ;
- un gestionnaire Radio-Baseband, connecté via un bus SPI ;
- un gestionnaire d'alimentation et clavier, connecté via un bus I2C.

Les interfaces externes sont :

- une liaison série de type série asynchrone (UART), normalement utilisée uniquement pour la mise au point ;
- une liaison USB (servant aussi de support à une liaison Ethernet) ;
- un canal radio.

2.3.2.2. Particularités de paramétrage de l'environnement

S'agissant d'une part, d'un produit destiné à des développeurs/intégrateurs, et d'autre part, d'une évaluation qui s'est déroulée sur une plate-forme de test, il est normal que certaines adaptations du processus général d'installation décrit dans les documents fournis par la société TRANGO Virtual Processors soient nécessaires. L'évaluateur a été amené à modifier certains fichiers de paramétrage de la chaîne de développement. Ces modifications sont considérées comme mineures et à la portée d'un développeur/intégrateur.

[1] La référence exacte du téléphone mobile est confidentielle : à la date de réalisation de l'évaluation, le modèle de téléphone utilisé était en cours de développement.

2.3.2.3. Options d'installation retenues pour le produit

Les options d'installation sont précisées dans les guides. S'agissant d'un produit très technique, il n'a pas été jugé pertinent de les rappeler dans le présent rapport.

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

Il n'a pas été relevé de non-conformité aux adaptations près réalisées par l'évaluateur et qui ne sont pas considérées ici comme des non-conformités.

2.3.2.5. Durée de l'installation

L'installation, la configuration et la prise en main du *framework* complet requièrent au moins une journée.

Deux évaluateurs ont participé à la formation, à l'installation et à la prise en main du produit, sur trois jours.

2.3.2.6. Notes et remarques diverses

Néant.

2.3.3. Analyse de la conformité

2.3.3.1. Analyse de la documentation

La documentation est complète et très lisible. La documentation fournie étant importante, l'évaluateur a privilégié l'analyse des documents suivants :

- la cible de sécurité [ST] ;
- le guide utilisateur [GUIDES] ;
- la documentation d'installation [GUIDES] ;
- le manuel de référence technique [GUIDES].

L'évaluateur n'a pas identifié de non-conformité dans la documentation du produit.

2.3.3.2. Revue du code source

Le code source n'a pas été fourni.

2.3.3.3. Fonctionnalités testées

Fonctionnalité	**Description**
Identification, authentification et contrôle d'accès VPHY	Accès depuis le mode noyau virtuel à différentes zones de la mémoire et contrôle de conformité des exceptions qui sont levées.
	Positionnement des droits d'accès des pages et contrôle de la valeur de retour des hypercalls. Tentative de lecture ou d'écriture dans ces pages et contrôle de conformité de ces opérations.
	Affichage et contrôle de conformité de l'information contenue dans les registres virtuels.

	Gestion dynamique des pages et contrôle de conformité du type et des propriétés des pages obtenues. Test de robustesse sur la gestion et l'accès à ces pages.
	Contrôle d'accès aux différentes zones mémoires.
	Contrôle de la mémoire utilisée par le biais des informations fournies par l'hyperviseur.
	Test de conformité de la fonctionnalité permettant d'obtenir les propriétés d'une page.
	Contrôle de cohérence du cache après libération de mémoire.
	Contrôle du comportement et des propriétés d'accessibilité des objets gérant le mapping mémoire.
	Création/désallocation sans erreur d'une page servant à la création dynamique de VM.
	Contrôle de l'évolution des informations de management d'objet de l'hyperviseur.
	Contrôle de la cohérence des données de statut mémoire lors de la création dynamique d'une VM.
	Contrôle de la politique d'allocation et de libération de la mémoire.

Fonctionnalité	**Description**
Identification, authentification et contrôle d'accès VLOGK	Contrôle des droits des pages mémoire VLOGK et contrôle de la conformité des tentatives d'accès.
	Contrôle en robustesse des services de mapping mémoire.
	Contrôle des dépendances entre objets lors d'opération de mapping.

Fonctionnalité	**Description**
Identification, authentification et contrôle d'accès VLOGU	Contrôle du champ utilisateur des objets de gestion du mapping mémoire.
	Contrôle de cohérence des droits d'accès avec les pages VLOG et VPHY.
	Contrôle de robustesse des hypercalls relatifs au mapping.
	Droits d'accès à la mémoire VLOGU par 6 Vms.
	Attachement des objets de gestion du mapping à VLOGU.
	Conformité de la gestion des sous domaines mémoire.
	Contrôle de l'effet des droits d'exécution dans VLOGU .

Fonctionnalité	**Description**
Auto protection interruptions	Installation d'un environnement minimal de gestion des interruptions. Utilisation du masque, activation/désactivation des interruptions.
	Utilisation des sources d'interruption périodique virtualisées.
	Conformité de la reconfiguration dynamique des sources d'interruption périodique.
	Contrôle de la bonne restauration du contexte après traitement d'une interruption.

	Contrôle de conformité des objets gérant le contrôle des interruptions: Un gestionnaire d'interruptions traite toutes les interruptions en attente avant de rendre la main.
	Contrôle de robustesse du mécanisme des interruptions par tentative de corruption des données de gestion.
	Contrôle de robustesse du mécanisme des interruptions par débordement en modifiant leur nombre de manière agressive.
	Contrôle de conformité de la fonctionnalité permettant de forcer le déclenchement d'une interruption.
	Contrôle de conformité du masque des interruptions.
	Contrôle de conformité des droits associés aux sources d'interruptions.
	Contrôle de conformité du mécanisme des interruptions avec des sources timer SoC.
	Contrôle de conformité du mécanisme des interruptions avec des sources Watchdog.

Fonctionnalité	**Description**
Autoprotection Exceptions	Contrôle de conformité du traitement des différents types d'exceptions pour l'architecture ARM.

Fonctionnalité	**Description**
Cache	Contrôle de cohérence du cache en situation normale et en situation d'accès concurrents.

Fonctionnalité	**Description**
Hypercalls de déboguage	Contrôle de conformité et de robustesse (débordement de tampon) des hypercalls d'entrée/sortie de déboguage (PutChar, GetChar)
	Contrôle de conformité et de robustesse (débordement de tampon) de l'UART virtuel.
	Conformité du reset logiciel.

Fonctionnalité	**Description**
Communication sécurisée Communication inter-VMs	Conformité du mécanisme de communication entre VMs.

Fonctionnalité	**Description**
Robustesse	Contrôle de robustesse de l'allocation de mémoire VPHY entre plusieurs VMs.
	Contrôle de robustesse par exécution d'hypercalls choisis aléatoirement avec des arguments aléatoires.
	Contrôle de robustesse des droits d'accès aux pages de types relatifs aux entrées/sorties.
	Contrôle de robustesse de l'allocation de mémoire VPHY, en atteignant ou en modifiant les limitations.

	Contrôle de robustesse des pages de confiance de l'hyperviseur.
	Contrôle de robustesse de l'allocation de mémoire.

Fonctionnalité	**Description**
Identification, authentification et contrôle d'accès Contrôle des droits en mode VUSER	Contrôle des droits en mode VUSER.

Fonctionnalité	**Description**
Ordonnanceur	Contrôle de conformité de l'ordonnanceur.

Fonctionnalité	**Description**
Administration et supervision de la sécurité	Contrôle de conformité de la gestion des VMs.

2.3.3.4. Fonctionnalités non testées

Fonctionnalité	**Description**
supervision	Cette fonctionnalité autorise la modification des paramètres d'exécution.
monitoring	Cette fonctionnalité permet la lecture d'informations de haut niveau du système.
déboguage	Cette fonctionnalité est dédiée à la mise au point et permet de dérouter le flot d'exécution.
gestion de l'énergie	Cette fonctionnalité permet par exemple la mise en veille de la plateforme.

2.3.3.5. Synthèse des fonctionnalités testés / non testées et des non-conformités

Le document CSPN_ENTRIES [GUIDE] décrit les non-conformités connues lors de l'évaluation. Celles-ci n'ont pas d'impact sur la sécurité du produit.

2.3.3.6. Avis d'expert sur le produit

La documentation est complète et très lisible. Les tests de conformité fournis par TRANGO Virtual Processors permettent de couvrir de nombreux aspects tant fonctionnels que liés à la sécurité. Dans le contexte de cette évaluation, il n'a pas été détecté d'impact sur la sécurité liée aux non-conformités détectées et déjà tracées par TRANGO Virtual Processors.

2.3.4. Analyse de la résistance des mécanismes et des fonctions

2.3.4.1. Liste des fonctions testées et résistance

Les fonctions de sécurité FS1 à FS7 de la cible de sécurité ont été testées. Elles sont rappelées ici pour mémoire :

- FS1 : Cloisonnement inter VMs
- FS2 : Contrôle du mode privilégié
- FS3 : Sécurité du contrôleur des interruptions
- FS4 : Sécurité du code et des données de l'hyperviseur
- FS5 : Sécurité de la MMU
- FS6 : Destruction des informations rémanentes (non réutilisation d'objets)
- FS7 : Sécurité du fichier de configuration

2.3.4.2. Avis d'expert sur la résistance des mécanismes

Peu de tests de robustesse autres que ceux proposés par TRANGO Virtual Processors ont été réalisés par l'évaluateur. Le jeu de tests de robustesse proposé par TRANGO Virtual Processors permet de couvrir un large spectre de mécanismes de sécurité. Des tests complémentaires ont été conçus par l'évaluateur concernant l'accès direct aux registres du processeur ARM :

- modification des registres de contrôle et de statut permettant par exemple d'accéder aux informations concernant le niveau de privilège courant de l'unité centrale ;
- modification des registres du coprocesseur P15 gérant le gestionnaire de mémoire (MMU pour Memory Management Unit) ;
- lecture de données résiduelles dans les registres de l'unité centrale afin de confirmer les résultats obtenus par les tests conçus par TRANGO Virtual Processors).

D'autres idées de tests sont envisagées par l'évaluateur concernant :

- les tests aux limites concernant les arguments passés aux hypercalls ;
- les possibilités d'usurpation d'identité de VM ;
- les possibilités d'accéder aux composants matériels de l'OMAP 2430 et l'incidence sur la sécurité des VMs et de l'hyperviseur ;
- la mise en oeuvre d'une attaque de type *Simple Branch Prediction Analysis* (SBPA), ou par canaux cachés en logiciel.

2.3.5. Analyse des vulnérabilités (conception, construction…)

2.3.5.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues sur ce produit particulier. Les vulnérabilités génériques associées aux produits de cette catégorie sont hors du champ de la présente évaluation. En particulier :

- les attaques portant sur le matériel sont hors du champ de la présente évaluation ;
- il n'a pas été identifié de non-conformités matérielles permettant d'envisager un chemin d'attaque ;
- le produit n'offre pas de mécanisme de protection contre les attaques par canaux auxiliaires.

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

D'une manière générale, il existe un risque potentiel d'élévation de privilège par utilisation des modules matériels du chipset OMAP 2430. C'est en particulier le cas pour le module initiateur USB (qui peut effectuer directement des requêtes d'écriture et de lecture). On notera que dans la version évaluée de TRANGO Hypervisor, l'USB est désactivé dans la séquence d'initialisation de l'hyperviseur.

Il existe un risque potentiel de mise en œuvre d'une attaque de type SBPA. L'évaluateur n'a pas réalisé de test pour confirmer la validité de ce risque. Il rappelle que si besoin est, le *branch predictor* de l'unité centrale ARMv6 peut être désactivé.

Les vulnérabilités potentielles concernant l'utilisation des ressources matérielles ou des composants de l'OMAP 2430 sont théoriquement couvertes par les hypothèses d'environnement, car l'accès aux ressources matérielles est protégé par droits d'intégration (*credentials*) dont on suppose que la gestion est sûre (l'intégrateur système est considéré comme non hostile, il est formé pour exécuter les opérations dont il a la responsabilité en suivant les recommandations du guide d'utilisation de l'hyperviseur, il dispose de moyens de contrôle des paramètres de configuration lui permettant de les intégrer de manière sûre).

2.3.6. Analyse de la facilité d'emploi et préconisations

2.3.6.1. Cas où la sécurité est ambiguë

L'évaluateur n'a pas identifié de cas où une VM peut être configurée d'une manière qui n'est pas sûre, mais que l'intégrateur pourrait raisonnablement croire sûre.

Pour des raisons de performance, les pages mémoires allouées par une VM et rendues volontairement au système ne sont pas nettoyées. Il s'agit d'un choix de conception dont l'utilisateur est averti. Voir à ce sujet la remarque au chapitre 2.3.6.2. Il ne s'agit pas d'une vulnérabilité au sens propre du terme mais il a été jugé nécessaire d'introduire cette précision à la fonction de sécurité FS6 (destruction des informations rémanentes) dans le présent rapport.

2.3.6.2. Recommandations pour une utilisation sûre du produit

Le chapitre 18 du guide d'utilisation [GUIDES] donne des recommandations pour le développement sécurisé de VMs de confiance. Ils proposent en particulier des indications de codage/paramétrage (contre mesures) pour éviter :

- les débordements de tampon,
- la présence de données résiduelles sensibles,

et sécuriser la communication inter-VMs.

Il est recommandé de suivre scrupuleusement les indications fournies par le développeur de VM et par l'intégrateur.

En particulier, il est de la responsabilité des VM d'effacer les pages mémoires qu'elles rendent au système si cela est utile. A noter que lorsqu'une VM est détruite, les pages mémoires qui lui sont allouées sont effacées.

TRANGO Hyperviseur n'intégrant pas les drivers des différents coupleurs matériels, il est recommandé que ces drivers soient implémentés dans des VM de confiance. Si une VM qui n'est pas de confiance doit accéder à ces ressources, il est recommandé qu'elle passe par une VM de confiance via les moyens de communication entre VM. Voir également à ce sujet 0 à propos du risque potentiel d'élévation de privilèges liés à certains modules matériels du chipset OMAP 2430.

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

Le module de l'IDE (Integrated Development Environment) Eclipse développé par la société TRANGO Virtual Processors permet de paramétrer une VM par le biais d'une interface graphique et doit faciliter la tâche de l'intégrateur. Cette interface de développement n'a pas été testée lors de l'évaluation. Cependant, la séparation des paramètres sur deux fichiers (tgo : structure de la mémoire physique, tgi : définition des droits) est bien pensée et rend aisée le paramétrage manuel de VM embarquant une simple application, comme par exemple celles utilisées dans les tests de conformité et de robustesse.

Le développement d'applications embarquées est supporté par une documentation de développement et de description des interfaces de programmation applicatifs (API pour Application Programming Interface) de l'hyperviseur de bonne qualité permettant de prendre en main progressivement le *framework* de développement de VMs et de réaliser facilement leur intégration.

Une bonne connaissance en informatique système est cependant nécessaire.

2.3.6.4. Notes et remarques diverses

Néant.

2.3.7. Accès aux développeurs

L'évaluateur a eu accès à TRANGO Virtual Processors et a pu bénéficier d'une formation au produit et d'un contact technique compétent.

2.4. Analyse de la résistance des mécanismes cryptographiques

Le produit évalué ne comporte pas de mécanismes cryptographiques.

2.5. Analyse du générateur d'aléas

Le produit évalué ne comporte pas de générateurs d'aléas.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles en vigueur, avec la compétence et l'impartialité requise pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « TRANGO Hypervisor version 1.5.61 sur plate-forme OMAP 2430 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST].

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 [ST], suivre les recommandations énoncées dans le présent rapport de certification ainsi que celles se trouvant dans les guides fournis [GUIDES] avec le produit.

Annexe 1. Références documentaires du produit évalué

[ST]	TGO-QUA-0438-CSPN_SECURITY_TARGET, version 1.1, 17 juin 2008
[RTE]	TVP003-RTE01, version 1, révision 0, 25 juillet 2008.
[GUIDES]	Guide d'installation du produit : PROC_INSTALL_OMAP2430. Guides d'utilisation : TRANGO ARMv6 Hypervisor User's Guide , TGO-MAN-OMAP2430_UG, CSPN-1.5.61, 27 juin 2008. Manuel de référence du produit : TRANGO ARMv6 Hypervisor Reference Manual, TGO-MAN-OMAP2430_RM, version CSPN-1.5.61, 27 juin 2008. Dossiers de test du produit : TRANGO ARMv5 Test Description, TGO-TST-0346-ARMV6_TEST_DESCRIPTION, version CSPN-1.5.61, 27 juin 2008. Entrées CSPN TRANGO, CSPN_ENTRIES, version 1.0, 30 juin 2008. Présentation de la sécurité du produit : Security overview, TGO-QUA-0304-SEC_OVERVIEW, draft, 27 février 2008.

Annexe 2. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CSPN-CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 2.4, phase expérimentale, n°915/SGDN/DCSSI/SDR/CCN, 25 avril 2008. Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1.4. Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1.3.