Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2009/05

VSC-TOOAL v1.1

Paris, le 15 octobre 2009

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 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 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 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-2009/05

Nom du produit

VSC-TOOAL v1.1

Référence/version du produit

Version 1.1

Critères d'évaluation et version

CERTIFICATION SECURITE DE PREMIER NIVEAU (CSPN, Version expérimentale)

Développeur(s)

MEDISCS
Espace Concorde B1
Parc d'activité Aéroport
120 impasse Jean-Baptiste SAY
34470 Pérols
France

Commanditaire

MEDISCS
Espace Concorde B1
Parc d'activité Aéroport
120 impasse Jean-Baptiste SAY
34470 Pérols
France

Centre d'évaluation

AQL Groupe Silicomp
4 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 :

- L'agence 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 « VSC-TOOAL v1.1 » développé par la société MEDISCS.

Sa principale fonctionnalité est d'automatiser l'accès à un service Internet sécurisé utilisant des certificats X509 en réalisant les opérations que devrait faire l'utilisateur pour accéder à ce service (installer le certificat associé à ce service, ouvrir son navigateur avec l'URL du service, s'authentifier, effacer le certificat).

Il se présente sous la forme d'un mini CD R, contenant l'application. Ce mini CD est le média physique, détenu par l'utilisateur, qui mémorise les informations et les programmes nécessaires à la réalisation de la fonction d'authentification.

A ce titre, il doit assurer la protection de certaines des informations nécessaires à la réalisation de ces fonctionnalités et en particulier, assurer la confidentialité des clés privées de l'utilisateur.

Pour ce faire, il s'appuie sur des mécanismes cryptographiques permettant le chiffrement des données sensibles et sur l'authentification de l'utilisateur permettant de déverrouiller l'accès à ces données lorsque nécessaire.

A la différence d'une carte à puce, le produit ne comporte aucune capacité de traitement ni de confinement des données sensibles dans une enceinte sécurisée lorsqu'elles sont utilisées. Les traitements sont réalisés sur l'ordinateur de l'utilisateur, ce qui implique que cet ordinateur soit considéré comme sûr.

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

1.2.2. Identification du produit

L'identification du produit peut se faire par lecture du support physique (voir illustration, ici, V1.1).

Si cette information n'est pas visible sur le support physique, il est également possible de vérifier le n° de version du produit en affichant les propriétés Windows du fichier VSCTooal.exe présent sur le CD-R.

1.2.3. Services de sécurité

Le principal service de sécurité du produit est de permettre à un utilisateur de disposer des secrets lui permettant de se connecter à un service internet sécurisé sur un support portable (un CD-ROM) tout en assurant leur confidentialité.

Par contre, la fonctionnalité et le service de sécurité proposés impliquent la mise en œuvre de fonctions et de mécanismes de sécurité pour protéger les informations sensibles manipulées. Ce sont certaines de ces fonctions et mécanismes qui ont fait l'objet de la présente évaluation.

Les mécanismes de sécurité permettent d'assurer :

- la confidentialité des clés manipulées par le processus de connexion au service internet sécurisé ;
- la confidentialité du code PIN permettant à l'utilisateur de s'authentifier vis-à-vis de l'application embarquée dans le support VSC-TOOAL ;
- l'intégrité de l'application embarquée et de la procédure de connexion.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

- phase 1 : développement du produit réalisé par Mediscs ;
- phase 2 : personnalisation du produit réalisée par Mediscs à partir des informations fournies par l'initialisateur (voir les rôles dans [ST]) et distribution à l'utilisateur ;
- phase 3 : utilisation du produit par l'utilisateur final.

Le produit faisant l'objet de la présente évaluation est celui issu de la phase 2 du cycle de vie.

1.2.5. Configuration évaluée

Sans objet.

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

Le produit a fait l'objet de deux évaluations consécutives pour répondre à des remarques formulées à l'issue de la première évaluation. La charge de travail totale a été de 44 h.j, y compris la charge d'évaluation de la cryptographie. L'évaluation de la version certifiée s'est déroulée en juillet 2009.

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 [ST] (chapitre « Argumentaire »).

2.3.1.2.Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [ST] (chapitre « Description des biens sensibles que le produit doit protéger »).

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

Conforme à la cible de sécurité [ST] (chapitre « Description des menaces »).

2.3.1.4.Fonctions de sécurité

Conforme à la cible de sécurité [ST] (chapitre « Description des fonction de sécurité du produit »).

2.3.1.5.Utilisateurs typiques

Conforme à la cible de sécurité [ST] (chapitre « Argumentaire »).

2.3.2. Installation du produit

2.3.2.1.Plate-forme de test

Le produit a été évalué sur la plate-forme suivante :

- un PC disposant d'une CPU Intel 1.7 GHz, de 2 Go RAM, équipé d'un lecteur de CD-ROM standard ;
- le système d'exploitation Windows XP Pro SP 2 de Microsoft ;
- le navigateur Internet Explorer 7.0 de Microsoft.

L'éditeur du produit annonce que le produit fonctionne également sous Windows XP SP3 et sous Windows Vista, mais ces configurations n'ont pas été testées lors de l'évaluation.

Le produit n'est pas prévu pour fonctionner avec d'autres navigateurs qu'Internet Explorer.

2.3.2.2.Particularités de paramétrage de l'environnement

Conforme à la cible de sécurité [ST] (chapitre « Description de l'environnement technique dans lequel le produit doit fonctionner »).

2.3.2.3.Options d'installation retenues pour le produit

Le produit ne nécessite pas d'installation.

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

Sans objet.

2.3.2.5.Durée de l'installation

Sans objet.

2.3.2.6.Notes et remarques diverses

Si le produit ne nécessite pas d'installation particulière, l'application VSC-TOOAL doit néanmoins pouvoir s'exécuter. Si l'auto exécution automatique (*autorun*) est activée, le produit se lance automatiquement lorsque le support VSC-TOOAL est inséré dans le lecteur de CD-ROM. Dans le cas contraire, il faut cliquer sur l'icône de l'application.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit. Il a effectué une rapide revue et n'a pas identifié de non-conformité.

La documentation utilisateur est claire et il n'a pas été relevé de non-conformité.

2.3.4. Revue du code source

Les évaluateurs ont eu accès au code source. Le développeur utilise une version récente du compilateur, permettant de générer du code robuste vis à vis des problèmes de gestion mémoire. Le code de l'application est bien structuré et convenablement commenté.

2.3.5. Fonctionnalités testées

OK : résultat conforme.
KO : résultat non-conforme.

Fonctionnalité	Résultat
Authentification utilisateur du produit	OK
« Blocage » du produit après 5 échecs d'authentification avec code PIN utilisateur.	OK
S'assurer que la position des chiffres sur le clavier virtuel est modifiée entre des authentifications successives à échec du code PIN utilisateur.	OK
S'assurer que la position des chiffres sur le clavier virtuel est modifiée à chaque nouveau lancement de l'application.	OK
Vérification de la fonction C et RAZ du clavier virtuel.	OK
Vérification de la touche « annuler » du clavier virtuel.	OK
Vérification de la touche « valider » du clavier virtuel.	OK
Connexion au site de test proposé par Mediscs.	OK
Authentification au site de test proposé par Mediscs à travers un serveur proxy.	OK
Vérifier l'échec de la connexion suite à la non-installation de l'AC racine.	OK
Authentification sans la connexion Internet.	OK
Vérifier que le certificat est bien effacé du système à la fin de la procédure d'authentification.	OK
Vérifier l'arrêt de l'application si l'utilisateur ne répond pas à la requête d'installation du certificat de l'AC.	OK
Vérification du temps de réponse pour une authentification avec code PIN utilisateur.	OK
Vérification du temps de réponse pour une authentification avec code PIN utilisateur, avec un CDROM virtuel.	OK
Vérifier la fermeture de l'application quand l'éjection du CD est forcée.	**KO**
Vérifier que la longueur du code PIN correspond à la stratégie définie.	OK
Vérifier que la stratégie du code PIN est respectée (caractères utilisés).	OK
Vérifier que le certificat est bien importé dans le système.	OK
Vérifier que le certificat est inutilisable après un arrêt brutal de l'application.	OK
Vérifier la latence entre deux saisies de code PIN.	OK
Vérifier l'arrêt de l'application automatiquement après 300 secondes d'exécution.	OK
Modification date système pendant la procédure d'authentification.	OK
Vérifier le message d'alerte dans le cas d'une attaque par mimétisme au clavier virtuel.	OK
Vérifier que le certificat est bien effacé du système si l'application s'arrête après 5 minutes d'exécution.	OK
Vérifier que l'application s'arrête si elle n'est pas exécutée dans l'environnement prévu.	OK
Vérifier le message d'alerte dans le cas d'une attaque par mimétisme.	OK
Vérifier le message d'alerte dans le cas d'une attaque à la séquence de sécurité.	OK

2.3.6. Fonctionnalités non testées

Tester l'application avec un lecteur de carte à puce installé sur le poste hôte.
Tester le délai d'attente de l'application à la demande de la carte à puce.

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

La seule non-conformité identifiée concerne la non-terminaison de l'application après éjection du CD-ROM.

2.3.8. Avis d'expert sur le produit

A une exception près, le produit est conforme à ses spécifications.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1.Liste des fonctions et des mécanismes testés - résistance

Pour un avis sur la résistance des mécanismes, voir 2.3.9.3.

Fonction et mécanismes
Initialisation / personnalisation
Protection des données sensibles
Sécurisation de la mémoire
Effacement des données sensibles
Protection de l'exécution des procédures de connexion
Protection de la clé privée
Contrôle du temps d'exécution
Temps minimum sécurisé de saisie
Limite du nombre de saisie
Protection clavier virtuel
Contrôle de l'environnement d'exécution
Protection des données d'authentification en mémoire
Contrôle d'intégrité
Export sécurisé du certificat et de la clé privée associée vers le CSP de Windows
Protection de la clé privée résidente dans le CSP
Suppression des données

2.3.9.2. Liste des fonctions et des mécanismes non testés - résistance

Déverrouillage : validation du code PIN en un temps incompressible : ce mécanisme a été testé fonctionnellement et est conforme. Sa résistance n'a pas été évaluée.

2.3.9.3.Avis d'expert sur la résistance des mécanismes

Les mécanismes de sécurité qui s'appuient sur la cryptographie font l'objet d'une analyse théorique particulière dont les principales conclusions sont données au chapitre 2.4.

Hors utilisation (utilisateur non authentifié), la carte VSC-TOOAL protège correctement les biens sensibles qu'elle mémorise.

En utilisation (utilisateur authentifié, application VSC-TOOAL en exécution), les mécanismes de sécurité, qui sont tous implantés en logiciel, s'exécutent sur l'ordinateur de l'utilisateur.

Ils sont tous potentiellement vulnérables à des attaques si les précautions d'emplois (valables pour tous les logiciels) ne sont pas respectés (poste sain par exemple).

L'évaluateur n'a pas identifié de dégradation de la sécurité introduite par le produit par rapport à une authentification à des services sécurisés que serait faite manuellement avec les outils disponibles sous Windows.

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 ce produit particulier. Par contre, le produit peut être sensible à des vulnérabilités existantes dans les environnements sur lesquels il s'appuie (Windows, Internet explorer, le CSP de Microsoft, etc.).

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

Les évaluateurs ont identifié des vulnérabilités potentielles et ont tenté d'en exploiter certaines. Ces vulnérabilités ne sont pas exploitables si les conditions d'utilisation (en particulier, poste sain) sont respectées.

2.3.11. Accès aux développeurs

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Au cours 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 (dans la journée) 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

Néant.

2.3.12.2. Recommandations pour une utilisation sûre du produit

L'utilisation du produit doit être faite sur un PC hébergeant un système d'exploitation dont les mises à jour de sécurité sont faites de manière rigoureuse. Il doit être au minimum protégé par un produit anti-virus (avec bases d'information à jour et proposant des fonctions de détection

des infections informatiques furtives - anti-spyware, anti-rootkit, etc.) et un pare-feu correctement configuré.

Le produit ne devrait pas être utilisé si le moindre doute subsiste quant à la compromission du système.

Il est à noter que, dans ce dernier cas, la même recommandation peut être faite pour une connexion manuelle par l'utilisateur au service Internet sécurisé (donc sans l'aide de VSC-TOOAL).

Pour assurer la confidentialité des informations sensibles, le code PIN de l'utilisateur doit avoir une longueur d'au moins 10 caractères (lettres et/ou chiffres) et être non trivial.

Il est recommandé de ranger sa carte et de ne pas la laisser à la vue de tous.

En cas de perte ou de vol du support, l'utilisateur doit avertir l'opérateur du service sécurisé associé à son support afin que le certificat correspondant au support soit révoqué.

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

Lorsque l'utilisateur procède lui-même à l'éjection du CD-ROM, des données sensibles sont susceptibles de rester en mémoire après arrêt du PC ou terminaison forcée des processus de l'application. Il est donc conseillé à l'utilisateur de laisser l'application éjecter le CD-ROM elle-même.

L'application VSC-TOOAL gère automatiquement certains pop-up sans l'intervention de l'utilisateur. Cependant, dans certains cas, l'application ne peut pas gérer tous les pop-up à la place de l'utilisateur. Par exemple, si un *proxy* demande une authentification avant de permettre la connexion vers l'Internet, l'application VSC-TOOAL affiche le pop-up de saisie du login et du mot de passe à l'utilisateur. Le pop-up affiché n'est pas toujours visible par l'utilisateur puisqu'il est parfois caché derrière la fenêtre principale de l'application CSV-TOOAL que l'on ne peut pas réduire. La seule solution pour afficher le pop-up est de taper `ALT + TAB`. Une amélioration possible du produit pourrait consister à afficher les pop-up de manière visible.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre pour protéger les clés secrètes ainsi que le mécanisme de déverrouillage sont conformes au référentiel [RGS_B_1] de l'ANSSI.

2.5. Analyse du générateur d'aléas

Le générateur d'aléa a fait l'objet d'une analyse et est conforme au référentiel [RGS_B_1] de l'ANSSI.

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 « VSC-TOOAL v1.1 » 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] et suivre les recommandations énoncées dans le présent rapport de certification.

Annexe 1. Références documentaires du produit évalué

[ST]	*Cible de sécurité CSPN v3.3* ; TOOAL.VSC1.1.Cible_de_securite_CSPN_v3-3
[RTE]	*Rapport Technique d'Evaluation – Certification de Sécurité de Premier Niveau Carte VSC-TOOAL* ; CSPN_VSC-TOOAL_RTE_v1.3
[GUIDES]	*Guide utilisateur* ; TOOAL.VSC1.1.Guide_Utilisateur

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.
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, v1.11