VSC-TOOAL 1.1

Cible de Sécurité CSPN

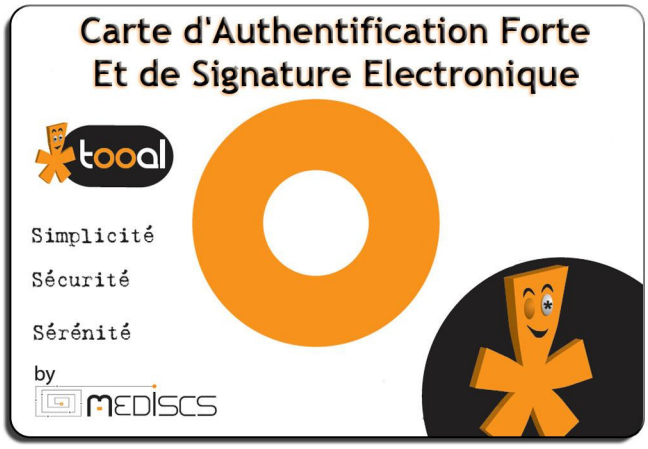
1 Identification du produit

Organisation éditrice	MEDISCS
Lien vers l'organisation	www.mediscs.com
Nom commercial du produit	VSC-TOOAL
Numéro de la version évaluée	1.1
Catégorie de produit	Dispositif d'authentification

2 Argumentaire du produit

2.1 Description générale du produit

Le produit VSC-TOOAL se présente sous la forme d'un mini CD R, au format proche d'une carte de visite, contenant une application qui est le moteur du produit VSC-TOOAL. Ce mini CD est le média physique, détenu par l'utilisateur, qui lui permet de s'authentifier à des services sécurisés, en réalisant le meilleur compromis entre sécurité des données, coût, facilité de déploiement et simplicité d'utilisation.



Le produit embarque un certificat électronique avec sa clé privée dans le fichier coffre-fort enregistré dans une zone masquée du fichier ISO 9660. Le certificat électronique avec sa clé privée sont sous format PKCS#12. Le fichier coffre-fort est un fichier chiffré avec l'algorithme AES 256 bits. .

Le produit automatise l'accès à un service internet sécurisé en réalisant les opérations que devrait faire l'utilisateur pour accéder à ce service, c'est-à-dire : installer le certificat associé à ce service (authentification), ouvrir son navigateur avec l'URL du service, authentifier l'utilisateur, effacer le certificat. Une fois ces étapes effectuées, le CD s'éjecte automatiquement de l'ordinateur.

Le produit ne demande pas au concepteur d'un service Internet d'adapter son service à l'utilisation du produit VSC-TOOAL, mais c'est elle qui s'adapte au service existant en reproduisant les actions que devrait réaliser l'utilisateur pour y accéder (assistant de connexion).

2.2 Description de la manière d'utiliser le produit

L'utilisateur introduit sa carte VSC-TOOAL dans le lecteur CD de son poste. Si l'auto exécution (autorun) est activée, l'application se lance automatiquement, sinon l'utilisateur doit cliquer sur l'icône de l'application.

L'utilisation de l'application est conditionnée par la saisie d'un « code PIN[1] », connu uniquement de l'utilisateur, qui assure la protection des données sensibles contenues dans le produit VSC-TOOAL.

2.3 Description de l'environnement prévu pour son utilisation

Le produit VSC-TOOAL, qui s'appuie sur une technologie à base de CD-Rom, répond aux besoins d'authentification par certificat X509 des utilisateurs sur un service internet sécurisé. Il se veut une alternative innovante face aux solutions existantes utilisant des certificats « X509 logiciels » ou des cartes à puce cryptographique. Il rend le certificat logiciel portable et facile à déployer.

Le produit fonctionne sous Windows XP ou Windows Vista et utilise un lecteur de CD-Rom standard. Il allie simplicité d'utilisation (aucune installation de logiciel n'est nécessaire, installation/effacement du certificat X509 automatique) et sécurité (authentification de l'utilisateur, protection de la clé privée transitant dans le conteneur personnel de Windows du poste hôte, certificat supprimé de l'ordinateur hôte à la fin de chaque session d'authentification et éjection automatique de la carte VSC-TOOAL).

Exemple d'utilisation : Authentification sur le service de sa banque online.

> La carte VSC-TOOAL est spécifiquement configurée pour ce service (utilisant une procédure de connexion) et initialisée pour un utilisateur. Le propriétaire reçoit sa VSC-TOOAL et le code PIN d'utilisation.
>
> L'utilisateur (propriétaire) introduit sa carte dans le lecteur CD du poste de travail (poste qui suit les recommandations du guide d'utilisation du produit) à partir duquel il veut consulter ses comptes bancaires. Si l'auto exécution est activée, l'application se lance automatiquement, sinon il doit cliquer sur l'icône de l'application.
>
> L'application fait apparaître un clavier virtuel à partir duquel l'utilisateur saisit son « code PIN » de protection. Si le « code PIN » saisi est le bon, l'application enchaîne les étapes permettant d'accéder à son service bancaire. L'utilisateur peut suivre le déroulement de ces étapes sur son écran. A la fin de cette procédure de connexion, il est sur l'espace de confiance du service bancaire. L'application supprime le certificat du magasin utilisateur et éjecte la carte VSC TOOAL.

[1] Code PIN : Mot de passe nécessaire au déverrouillage du produit.

2.4 Description des hypothèses sur l'environnement

H.INITIALISATION

Il est supposé que l'initialiseur et le personnalisateur soient non hostiles et compétents. L'initialiseur est la personne qui génère le fichier au format ISO 9660 spécifique à chaque carte VSC-TOOAL et le personnalisateur est la personne qui grave le fichier ISO sur CD-ROM (voir les rôles décrits dans le chapitre 2.6). Ils possèdent les ressources requises pour ces tâches et sont formés pour conduire les activités dont ils sont responsables.

L'initialisation s'effectue sur un serveur, et il est supposé que ce serveur est sécurisé physiquement et logiquement par les mesures organisationnelles appropriées.

La personnalisation s'effectue sur un système, et il est supposé que ce système est sécurisé physiquement et logiquement par les mesures organisationnelles appropriées.

Le produit et les données nécessaires à son utilisation (code PIN associé) sont supposés être transmis à l'utilisateur final par un canal organisationnel sécurisé.

H.UTILISATEUR

Les utilisateurs du produit doivent assurer la confidentialité de leurs données d'authentification personnelles (code PIN).

Les utilisateurs sont avertis des risques liés à la divulgation de leurs données et n'enregistrent pas de copies de celles-ci en clair.

Le poste de l'utilisateur suivra les recommandations indiquées dans le guide d'utilisation du produit. Ces recommandations concernent la protection de l'ordinateur (pare-feu correctement configuré, antivirus avec base de données à jour, anti-spyware, anti-rootkit, etc.)

H.CERTIF_AUTH

Il est supposé que l'autorité de certification, émettant le certificat, permettant l'authentification de l'utilisateur, implémente des pratiques conformes à une politique de certification approuvée.

H.CRYPTO

Il est supposé que la génération des bi-clés à l'extérieur du produit est effectuée par une personne autorisée s'assurant de la confidentialité et de l'intégrité des clés.

2.5 Description des dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système qui ne sont pas fournis avec le produit

Aucune contrainte particulière (voir 3.2).

2.6 Description des utilisateurs typiques concernés (utilisateurs finaux, administrateurs, experts…) et de leur rôle particulier dans l'utilisation du produit.

Le produit comporte 3 rôles intervenants à des phases différentes du cycle de vie :

- Le rôle initialiseur qui génère le fichier au format ISO 9660 spécifique à chaque produit ainsi que le code PIN et le certificat associé. L'initialiseur a en charge la distribution sécurisée du code PIN (dans la pratique, il s'agit d'une entité cliente qui reçoit le code PIN et le distribue à ses propres utilisateurs).
- Le rôle personnalisateur qui grave le fichier ISO 9660 sur le CD-ROM. Après gravure de la CD carte avec le fichier ISO 9660, le personnalisateur a ensuite en charge la distribution du produit à l'utilisateur.
- Le rôle utilisateur qui se sert du produit pour s'authentifier dans un service sur internet.

2.7 Définition du périmètre de l'évaluation, à savoir les caractéristiques de sécurité du produit concernées par l'évaluation.

Le produit représenté par le fichier au format ISO 9660 gravé sur le CD carte est constitué de plusieurs composants fichiers :

- Application principale pilotant l'ensemble des fonctions du produit
- Fichier permettant l'auto exécution du produit
- Fichier gérant l'icône de l'application
- Fichiers contenant les informations de configuration du produit
- Fichiers contenant les données sensibles

Le produit est divisé en quatre modules principaux eux mêmes subdivisés en plusieurs composants. Nous indiquons le module d'interface homme-machine (IHM) et le module d'Automatisation des procédures Internet Explorer (IE) qui ne font pas partie du périmètre d'évaluation du produit puisque ce sont des modules optionnels.

Le principal objectif de la cible de sécurité CSPN est de valider le service de confinement des données sensibles sur le support du produit.

2.7.1 Module IHM

L'IHM est la partie publique et visible par l'utilisateur de l'application.

Le module IHM instancie le pavé virtuel alphanumérique de capture du code PIN. Il gère ensuite l'accès aux services sécurisés du produit lorsque l'utilisateur a été authentifié (dans la VSC-TOOALv1.1, il n'y a pas d'interface de gestion).

2.7.2 Module Automatisation des procédures Internet Explorer (IE)

Ce module est responsable de la gestion des procédures de connexion et de leur exécution. Le module est constitué de deux composants :

- IEManager qui coordonne la lecture des instructions de connexion à suivre provenant d'un fichier XML de procédures et leur exécution dans IE.
- WindowControl dans sa partie gestion des fenêtres IE: ce composant permet d'automatiser la gestion des fenêtres pop-up générées par le navigateur IE.

2.7.3 Module fonctions de sécurité

Ce module implémente les fonctions de sécurité du produit. Le module est constitué des composants suivants :

- WindowControl dans sa partie gestion des fenêtres de sécurité. Il permet d'ordonnancer et de traiter un ensemble de fenêtres selon une séquence prédéfinie. Ce module intervient également dans la gestion de la clé de session.
- Security Center : ce composant est responsable de tous les appels aux opérations cryptographiques assurant la protection des données sensibles dans le produit et lors de leur transfert dans le système d'exploitation. Le choix des algorithmes et des longueurs des clés suit les recommandations de la DCSSI.
- Gestion des certificats : ce composant permet de manipuler(en particulier installer et supprimer) les certificats du système d'exploitation.
- Gestion du pavé virtuel : composant qui contient le pavé virtuel alphanumérique de capture du code PIN muni de certaines protections de saisies.

2.7.4 Module ISO

Ce module assure la gestion des fichiers au format ISO 9660. Le module est constitué du composant responsable de la lecture du fichier ISO (notamment certaines plages cachées).

3 Description de l'environnement technique dans lequel le produit doit fonctionner

3.1.1 Matériel compatible ou dédié

- Matériel : PC compatible, architecture X86 (Pentium ou supérieur) avec un lecteur de CR-ROM,
- Une connexion à Internet est nécessaire.

3.1.2 Système d'exploitation compatible : type, version, correctifs…

Système d'exploitation : Windows XP (à partir du SP2) ou Windows VISTA. En particulier, le produit utilise les services cryptographiques (CSP) Microsoft Enhanced Cryptographic Provider v1.0 et la CryptoAPI pour réaliser les opérations cryptographiques d'installation du certificat et de la clé privée dans le CSP personnel de Microsoft Windows.

Internet Explorer 7.0 : le produit s'appuie sur les fonctionnalités d'Internet Explorer, principalement l'objet COM IWebBrowser2 pour créer une instance cachée d'Internet Explorer et exécuter automatiquement la procédure de connexion. Le protocole SSL (TSL) doit être actif.

4 Description des biens sensibles que le produit doit protéger

D.CLE_PRIVEE

Ce bien utilisateur correspond à la clé privée générée à l'extérieur du produit et importée dans le produit. Cette clé privée est associée à un certificat et à la clé publique contenue dans ce certificat. La clé privée doit rester cohérente avec la clé publique correspondante.
Protection : intégrité et confidentialité

D.CERTIFICAT

Ce bien utilisateur correspond au certificat édité par l'autorité de certification et qui contient en particulier les éléments d'information suivants :

- la désignation de l'autorité de certification émettrice du certificat
- le nom du titulaire de la clé publique
- la valeur de la clé publique
- la période de validité au-delà de laquelle il sera suspendu ou révoqué
- des informations complémentaires optionnelles :
  - restrictions d'usage des clés (signature, chiffrement, certification …)

    - politique de certification appliquée pour obtenir le certificat
    - etc.
  - la signature du certificat généré par l'autorité de certification

Protection : intégrité

D.RAD

Ce bien utilisateur correspond aux données stockées dans le produit (aussi nommé RAD pour « Reference Authentication Data ») et permettant de vérifier le code PIN entré par l'utilisateur pour s'authentifier :

- Tableau d'Aléa
- bloc ID du fichier coffre-fort
- fichier configuration

Protection : intégrité (Tableau d'Aléa), intégrité et confidentialité (bloc ID et fichier configuration)

D.PIN

Ce bien utilisateur correspond au code PIN (parfois aussi nommé VAD pour Verification Authentication Data) entré par l'utilisateur pour s'authentifier auprès du produit.

Protection : confidentialité

D.APPLICATION

Ce bien est nécessaire au fonctionnement du produit et correspond à la partie applicative du produit.

Protection : intégrité

D.XML

Ce bien utilisateur correspond à la procédure de connexion (sous format XML) qui permet la connexion automatique aux services sécurisés distants.

Protection : intégrité et confidentialité

D.CLES

Clés nécessaires au fonctionnement du produit :

- Clé coffre-fort
- Cette clé est utilisée pour déchiffrer le fichier coffre-fort.
- Clé PKCS#12
- Cette clé correspond au mot de passe du fichier PKCS#12 stocké dans le coffre-fort du produit.
- Clés protection1
- Clés pour déchiffrer le certificat contenu dans le fichier PKCS#12
- Clés protection2
- Clés pour déchiffrer la clé privée contenue dans le fichier PKCS#12
- Clé session
- Cette clé est utilisée comme mot de passe de protection d'une clé privée dans le CSP de Microsoft.
- Clé processus
- Cette clé permet de chiffrer la clé session, la clé PKCS#12 et la clé coffre-fort dans la mémoire sécurisée du produit.

Protection : confidentialité

5 Description des menaces

Les agents menaçant considérés sont des attaquants essayant d'utiliser illégitimement le produit ou essayant de se faire passer pour l'utilisateur légitime du produit auprès de services distants. Les attaques nécessitent le vol préalable du produit ou l'interception de données transitant hors du produit.

L'initialiseur et le personnalisateur ne sont pas considérés comme des attaquants, par hypothèse.

5.1 Menaces relatives à l'authentification utilisateur

M.MODIFICATION_RAD

Un attaquant modifie illégitimement ou détruit les données qui permettent l'authentification de l'utilisateur auprès du produit. Par exemple, un attaquant peut importer des RAD dans le produit correspondantes à des PIN connus afin de pouvoir utiliser le produit et s'authentifier auprès d'un service distant comme l'utilisateur légitime.
Biens concernés : D.RAD (intégrité)

M.DIVULGATION_RAD

Un attaquant accède illégitimement aux données permettant l'authentification de l'utilisateur et en déduit la valeur du code PIN permettant de s'authentifier comme l'utilisateur légitime.
Biens concernés : D.RAD (bloc ID et fichier configuration en confidentialité)

M.DIVULGATION_PIN

Un attaquant accède illégitimement aux données entrées par l'utilisateur pour s'authentifier (à l'aide d'un enregistreur de frappe) et en déduit la valeur du code PIN.
Biens concernés : D.PIN (confidentialité)

5.2 Menaces relatives à la gestion des clés

M.MODIFICATION_CLE_PRIVEE

Un attaquant modifie la valeur de la clé privée quand elle est stockée dans le produit ou durant son transfert dans et en dehors du produit (remplacement de la clé privée par exemple).
Biens concernés : D.CLE_PRIVEE (intégrité)

M.DIVULGATION_CLE_PRIVEE

Un attaquant accède à la valeur de la clé privée afin, par exemple, de s'authentifier en tant qu'utilisateur légitime auprès d'un agent distant.
La clé privée peut être divulguée lorsqu'elle est stockée dans le produit (suite à un vol du produit par exemple) ou bien lorsqu'elle réside sur le PC hôte.
Biens concernés : D.CLE_PRIVEE (confidentialité)

M.ARRET_PC

Un arrêt brutal du PC hôte (coupure d'alimentation, « plantage » système…) empêche la fermeture « propre » de la session de l'utilisateur connecté, ce qui permet, après le redémarrage du PC, l'accès à certaines données sensibles qui ne sont plus protégées par le produit.
Biens concernés : Tous ceux qui sont protégés en confidentialité (D.CLE_PRIVEE, D.RAD, D.PIN, D.XML, D.CLES)

5.3 Menaces relatives à la gestion des certificats

M.MODIFICATION_CERTIFICAT

Un attaquant modifie un certificat quand il est stocké dans le produit ou durant son transfert dans et en dehors du produit (l'impact est un déni de service par altération des données).
Biens concernés : D.CERTIFICAT (intégrité)

5.4 Menaces relatives à l'administration du produit

M.MODIFICATION_APPLICATION

Un attaquant modifie l'application pour modifier le comportement ultérieur du produit (insertion d'un cheval de Troie par exemple).
Biens concernés : D.APPLICATION (intégrité)

M.COMPROMISSION_XML

Un attaquant prend connaissance et/ou modifie les procédures XML de connexion afin de détourner leur utilisation (connexion à un site malveillant par exemple). Un utilisateur légitime compromet ses données de connexion par une mauvaise utilisation de procédures XML.
Biens concernés : D.XML (confidentialité et intégrité)

6 Description des fonctions de sécurité du produit

La fonction principale du produit est de protéger les données d'authentification de l'utilisateur au travers des services de gestion et de protection des certificats et clés associées.

6.1 Services assurés par le produit

Export de certificat :
Ce service assure l'export sécurisé d'un certificat du produit vers le CSP de Windows.

Protection du certificat :
Ce service assure la protection en confidentialité et intégrité des certificats sur le produit (garantissant notamment une protection en cas de fermeture brutale de la session ou de vol du produit).

Export de la clé privée :
Ce service assure l'export sécurisé de la clé privée (associée à un certificat) du produit vers le CSP de Windows. La clé privée est par ailleurs marquée comme non exportable.

Le produit fournit une clé de session de 248 bits afin de prévenir l'utilisation de la clé privée du CSP Windows par un autre processus durant le temps de la session.

Protection des clés :
Ce service assure la protection en confidentialité des clés (clé privée et clés nécessaires au fonctionnement du produit), garantissant notamment une protection en cas de fermeture brutale de la session ou de vol du produit.

Authentification utilisateur :
Ce service assure l'authentification sécurisée de l'utilisateur avant toute utilisation du produit (protection contre les key-loggers). L'authentification utilisateur s'effectue au travers d'un chemin de confiance basé sur l'entrée d'un code PIN saisi à partir d'un clavier virtuel alphanumérique affiché à l'écran.

Protection des procédures de connexion XML :
Ce service assure la protection (intégrité et confidentialité) des procédures de connexion sous le support du produit. De même, les procédures de connexion sont protégées dans la mémoire sécurisée du produit.

Protection des informations rémanentes
Ce service assure la protection des données rémanentes sensibles dans les mémoires du PC hôte.

6.2 Services nécessaires au fonctionnement du produit

Initialisation :
L'initialisation consiste à utiliser un code PIN pour initialiser le produit (création d'un fichier ISO 9660). Cette phase déclenche entre autre la génération de données secrètes nécessaires à la protection des données de l'utilisateur.

Ce service est assuré par une application externe au produit VSC-TOOAL. Cette application est hors périmètre d'évaluation.