PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2012/02

Librairie ClearBUS Secure
Version 1.1

Paris, le 27 mars 2012

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

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 doit 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 et de la sécurité 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-2012/02**
Nom du produit **Librairie ClearBUS Secure**
Référence/version du produit **1.1**
Catégorie de produit **Communication sécurisée**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur(s) **ClearBUS** **6, rue Irvoy** **38000 Grenoble** **France**
Commanditaire **ClearBUS** **6, rue Irvoy** **38000 Grenoble** **France**
Centre d'évaluation **Oppida** **4-6, avenue du Vieil Etang - Bât B** **78180 Montigny Le Bretonneux** **Tél : 01 30 14 19 00, mél : cesti@oppida.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 modifié. Ce décret indique que :

- L'agence nationale 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 la librairie « ClearBUS Secure version 1.10 » développée par la société ClearBUS.

Ce produit est destiné à être utilisé dans le cadre du service postal dématérialisé ClearBUS. Ce dernier est composé :

- d'une interface web pour la gestion des utilisateurs et des abonnés ;
- d'un client de dépôt et de réception du courrier ;
- d'un logiciel spécifique installé sur le serveur pour la gestion du stockage sécurisé, du routage, de l'horodatage et de l'authentification des abonnés.

La librairie évaluée est utilisée par le client de dépôt et de réception de courrier pour la gestion de la communication sécurisée avec le serveur, l'authentification et l'intégrité des échanges. Les autres composants du logiciel et de la solution n'entrent pas dans le cadre de cette certification.

La librairie ClearBus Secure est destinée à être utilisée par des développeurs souhaitant proposer les fonctionnalités d'envoi et de réception de courrier dématérialisé à leur application. Elle constitue une solution technique permettant l'interopérabilité avec les services ClearBus.

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

La version du produit certifiée est la version 1.10.

Elle est identifiable par l'ensemble des empreintes des fichiers suivants :

Nom du fichier	**Empreinte SHA512**
\outils\OpenSSLFactory_base.cpp	a132c22cbd3236e06177b944dedf960cf9d7bc33ab418afdd 4230096ebb24cf6dc06b214624ac973d98f62ed8495bae78d e4beccacc00e6d6ee73dbebee2302d
\trace\Trace_base.cpp	679f4e8f69df2dbf803136dd8fa9db85cb82b4f2156dd9624b e0ab5022abdd0628c25653eba722092761b9e6c155c6261c4 248c45bcc2009e5703cafcbe56a72
\connexion\Connexion_base.cpp	2b83712d898c2d376f946d2c0fa8f84ca6339ae620d8473c7f fff6b4903a1b45db575e57b13d44994ca8a443beadc81afa3f 1a76cca8b2222eab44005f01e7e2
\erreur\ExceptionsClearBusSecure.cpp	ae5e93eef1e2d62ba2d776b332d042ffe95eaa9cd2787c2c3f a0bbfbe94a80ee080ee3a8cd17e1b5a7ca4e3eef1dbffc63d4b 27865eca8676fd96377126af1a7
\include\OpenSSLFactory_base.h	50a5d6b2e07698dc388464bbc02c85acb20c6909dd975009 9f89a970c3ea0bef5933fb0bd9e8b5d180da49932821528e6 de60375910fc74e24ea297c812cd21d
\include\Trace_base.h	be53baf9702b617be72e643a217db73de0b31475afc318328 b1ab3c22111b1ec96132bcef511b7565ed547fdbdd0c63475 6e2c8037a846c15e844a8dde5391e8
\include\Connexion_base.h	08a41a5bb4b290218f435e67617cc68920d09f99336009408 d78d9fada5269166e9111835a3252d5dfab29dcf7ae0b87fd9 d2a39d5b1acd9f536a657f566245d
\include\ExceptionsClearBusSecure.h	66b879faedd823672c65b247a0c863919232ff886f97a82efa 37ae2299f422b369648a34e493d38f7ee2967cac1a4e8b945 ab7827f634984f182c28f8775043b

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- Authentification du serveur ;
- Protection des données lors de la transmission ;
- Signature électronique.

1.2.4. Configuration évaluée

La configuration évaluée est celle par défaut.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau. Les références des documents se trouvent en annexe 2.

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

La durée de l'évaluation a été conforme à la charge de travail prévue lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN] pour un produit comportant des mécanismes cryptographiques, soit 35 hommes x jours.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] 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 [CDS] (chapitre 2 « Argumentaire »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 4 « 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 [CDS] (chapitre 5 « Description des menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 6 « Description des fonctions de sécurité de la librairie »).

2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 2.2 « Description de l'environnement prévu d'utilisation du service »).

2.3.2. Installation du produit

2.3.2.1. Particularités de paramétrage de l'environnement

L'installation de la librairie ClearBUS Secure est dépendante des librairies et logiciels suivants :

- Trolltech QT ;
- MinGW ;
- OpenSSL.

Les versions des dépendances utilisées dans le cadre de l'évaluation sont indiquées dans le tableau suivant :

Trolltech	4.7
MinGW	4.4
OpenSSL	1.0.0f

2.3.2.2. Options d'installation retenues pour le produit

Sans objet.

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

Sans objet.

2.3.2.4. Durée de l'installation

Sans objet.

2.3.2.5. Notes et remarques diverses

Sans objet.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est claire et aucune non-conformité n'a été relevée.

2.3.4. Revue du code source (facultative)

L'évaluateur a évalué l'intégralité du code source de la librairie ClearBUS Secure. Le code est clair et les bonnes pratiques de programmation y sont globalement respectées.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Authentification du serveur	**Réussite**
Authentification de l'émetteur du message	**Réussite**
Protection en confidentialité d'un message lors de sa transmission	**Réussite**
Signature électronique	**Réussite**

2.3.6. Fonctionnalités non testées

Sans objet.

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

L'ensemble des fonctionnalités détaillées dans la cible de sécurité [CDS] ont été testées. Aucune non-conformité n'a été relevée.

2.3.8. Avis d'expert sur le produit

Le produit est fonctionnellement conforme à la cible de sécurité [CDS]. Son installation et son utilisation sont simples. L'API fournie par la TOE est claire et non-ambiguë, mais peut être complexe à prendre en main par un développeur externe.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Fonction et mécanisme
Mécanisme d'authentification du serveur Web ClearBUS
Mécanisme d'authentification des utilisateurs par identifiant et mot de passe
Mécanisme de chiffrement des communications entre le client et le serveur
Mécanisme de signature des courriers envoyés

2.3.9.2. Avis d'expert sur la résistance des mécanismes

Ces fonctions s'appuient sur des mécanismes cryptographiques détaillés dans le §2.4. Leur implémentation est jugée robuste par l'évaluateur.

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.

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

Aucune vulnérabilité n'a été trouvée dans le cadre d'utilisation du produit défini par la cible de sécurité [CDS] et respectant les recommandations du §2.3.12.2.

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 bonne maîtrise de son produit et a été en mesure de répondre rapidement 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

La sécurité du produit peut être remise en cause si le développeur utilisant la librairie ClearBUS Secure ne respecte pas les bonnes pratiques de programmation et notamment s'il ne suit pas les recommandations présentes dans [GUIDES] et dans le §2.3.12.2.

2.3.12.2. Recommandations pour une utilisation sûre du produit

Développeur

Le développeur désirant intégrer les fonctions de la librairie ClearBUS Secure au sein de son application doit veiller à respecter les bonnes pratiques en matière de programmation sécurisée.

Il doit notamment veiller à ce que l'utilisateur final du produit ait des droits d'accès limités à la lecture au fichier *prngseed.dat* ainsi qu'au fichier représentant son certificat de signature.

Il doit également veiller à utiliser la fonction *nettoyer()* de la librairie ClearBUS Secure afin de s'assurer d'un effacement des secrets en mémoire conforme à [REF-CRY].

Utilisateur final du produit basé sur la librairie ClearBus Secure

L'utilisation finale du produit doit être faite sur un PC hébergeant un système d'exploitation à jour concernant les correctifs de sécurité et correctement administré. 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 en cas de doute sur la sécurité du système.

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

Le public cible de la TOE est constitué des développeurs souhaitant intégrer les fonctionnalités de ClearBus Secure dans leur application. L'API de la librairie est claire et simple d'utilisation. La remontée d'erreur à l'exécution est efficace, ainsi que la création de traces applicatives

2.3.12.4. Notes et remarques diverses

Sans objet.

2.4. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par l'évaluateur. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] qui a conclu à la conformité à [REF-CRY] des mécanismes cryptographiques suivants :

- authentification par certificat ;
- authentification par mot de passe ;
- chiffrement des communications ;
- signature des courriers envoyés.

2.5. Analyse du générateur d'aléas

La fonction de génération d'aléa utilisée par le produit provient de la librairie OpenSSL. L'utilisation sous-jacente du générateur d'aléa fourni par les systèmes Windows nécessite de prendre en compte les attaques réalisées sur celui-ci et d'appliquer les contre-mesures détaillés dans [GUIDES].

3. La certification

3.1. Conclusion

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

Ce certificat atteste que le produit « Librairie ClearBUS Secure**,** 1.10 **»** soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

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 [CDS] et suivre les recommandations énoncées dans le présent rapport.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN - ClearBUS : Application cliente pour la communication sécurisée ;* Référence : *CBUS-CS-1.12-20111125* ; Date : *25/11/2011*
[RTE]	*Rapport Technique d'Évaluation (RTE) CSPN - ClearBus Secure ;* Référence : *OPPIDA/2011/DIC/659/1.2* ; Date : *27/02/2012*
[ANA-CRY]	*Rapport Technique d'Evaluation (RTE) CRYPTO CSPN - ClearBus Secure ;* Référence : *OPPIDA/DOC/2011/CSPN/CRYPTO/ClearBUS* ; Date : *13/01/2012*
[GUIDES]	Description de la solution : *Description & architecture de ClearBUS Secure* Date : *02/12/2011* Guide d'utilisation : *Guide utilisateur ClearBUS ;* Date : *22/11/2011* Guide de développement : *Manuel de documentation de l'API de la TOE 1.1*

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur www.ssi.gouv.fr
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur www.ssi.gouv.fr