Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-CC-2014/36

# ZonePoint
# version 3.0, build 330

*Paris, le 22 avril 2014*

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

[Original signé]

Guillaume POUPARD

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 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*<br>**ANSSI-CC-2014/36** |
| *Nom du produit*<br>**ZonePoint** |
| *Référence/version du produit*<br>**version 3.0, build 330** |
| *Conformité à un profil de protection*<br>**Néant** |
| *Critères d'évaluation et version*<br>**Critères Communs version 3.1 révision 4** |
| *Niveau d'évaluation*<br>**EAL 3 augmenté**<br>**ALC_FLR.3, AVA_VAN.3** |
| *Développeur*<br>**Prim'X Technologies**<br>**10 place Charles Béraudier,**<br>**69428 Lyon Cedex 03,**<br>**France** |
| *Commanditaire*<br>**Prim'X Technologies**<br>**10 place Charles Béraudier,**<br>**69428 Lyon Cedex 03,**<br>**France** |
| *Centre d'évaluation*<br>**Amossys**<br>**4 bis allée du bâtiment, 35000 Rennes, France** |
| *Accords de reconnaissance applicables*<br>**CCRA** **SOG-IS** |

# 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 ..... 6**

1.1. PRESENTATION DU PRODUIT ..... 6
1.2. DESCRIPTION DU PRODUIT ..... 6
*1.2.1. Introduction ..... 6*
*1.2.2. Identification du produit ..... 6*
*1.2.3. Services de sécurité ..... 7*
*1.2.4. Architecture ..... 7*
*1.2.5. Cycle de vie ..... 7*
*1.2.6. Configuration évaluée ..... 8*

**2. L'EVALUATION ..... 9**

2.1. REFERENTIELS D'EVALUATION ..... 9
2.2. TRAVAUX D'EVALUATION ..... 9
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI ..... 9
2.4. ANALYSE DU GENERATEUR D'ALEAS ..... 10

**3. LA CERTIFICATION ..... 11**

3.1. CONCLUSION ..... 11
3.2. RESTRICTIONS D'USAGE ..... 11
3.3. RECONNAISSANCE DU CERTIFICAT ..... 12
*3.3.1. Reconnaissance européenne (SOG-IS) ..... 12*
*3.3.2. Reconnaissance internationale critères communs (CCRA) ..... 12*

**ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT ..... 13**

**ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE ..... 14**

**ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION ..... 15**

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est « ZonePoint, version 3.0, *build* 330 » développé par Prim'X Technologies.

Ce produit est destiné à gérer des zones de stockage chiffrées au sein de bibliothèques de documents SharePoint. ZonePoint réalise le chiffrement et le déchiffrement local (sur le poste de l'utilisateur) et « à la volée » des documents téléchargés depuis ou transmis vers les bibliothèques de documents chiffrés.
Il permet, pour chaque zone chiffrée, de définir et gérer des accès, via des secrets détenus par les utilisateurs.

ZonePoint se décline en deux *packages* :

- une édition contenant le produit complet ;
- une édition, appelée « *Light* », ne permettant pas d'effectuer d'opération de gestion des zones et des accès. Cette édition permet, à partir d'un navigateur, de télécharger et déchiffrer ou chiffrer des documents, depuis ou vers une zone chiffrée sur le serveur SharePoint. Cette zone chiffrée doit avoir été préalablement créée avec l'édition complète de ZonePoint.

## 1.2. Description du produit

### *1.2.1. Introduction*

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

### *1.2.2. Identification du produit*

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

Sur le site *web* de Prim'X Technologies, le numéro de la version du produit est intégré au nom des fichiers d'installation, comme par exemple « Setup ZonePoint 3.0 x86 (b330).exe » ou « ZonePoint Light 3.0 x86 (b330).msi ».

Après installation de la TOE et une fois qu'elle est opérationnelle, ZonePoint édition *Light* affiche directement le *build* du produit installé sur le poste et, pour la version complète, le menu « A propos de ZonePoint… » permet de connaitre la version ainsi que le *build* du produit installé sur le poste. Le guide d'installation détaille la « lecture de la version de ZonePoint », voir [GUIDES].

### *1.2.3. Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la gestion de zones chiffrées au sein de bibliothèques de documents SharePoint (tirage de la clé de zone, chiffrement, déchiffrement, transchiffrement, affichage des informations de zone) ;
- le contrôle d'accès aux zones chiffrées (interface obligatoire entre l'utilisateur et les zones chiffrées, qui autorise ou refuse l'accès) ;
- la gestion des clés d'accès (renouvellement, ajout, suppression, rôle associé) ;
- la journalisation des événements liés aux opérations réalisées par le produit ;
- l'administration du produit (initialisation et modification de la configuration).

### *1.2.4. Architecture*

Le produit de l'édition complète est constitué par :

- un gestionnaire de bibliothèque ZonePoint, installé sur le serveur ;
- un ensemble logiciel, installé sur les postes clients, avec en particulier un *plugin* pour le navigateur web. Cet ensemble inclut un module « commandes administratives » dédié à l'administrateur.

Le produit de l'édition *Light* est constitué par un ensemble logiciel, installé sur les postes clients. Cet ensemble n'inclut pas les « commandes administratives ».

### *1.2.5. Cycle de vie*

Le cycle de vie du produit est le suivant :

- phase d'expression de besoin : elle fixe le contenu de la version du produit à développer ;
- phase d'implémentation et de validation ;
- phase d'intégration et de mise en ligne, à l'issue de laquelle la version du produit est disponible pour livraison aux utilisateurs ;
- phase de support aux utilisateurs et de maintenance.

Le produit a été développé sur le site suivant :

**Prim'X Technologies**

10 place Charles Béraudier
69428 Lyon Cedex 03
France

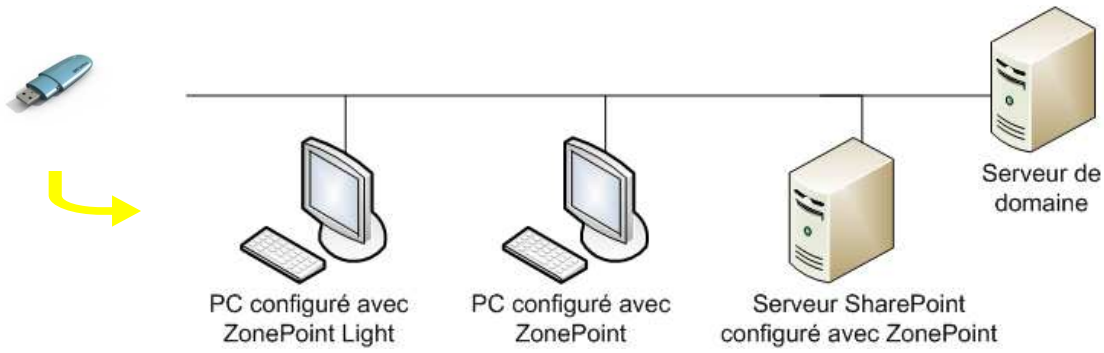
Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit les personnes réalisant les opérations d'administration de la sécurité conformément aux [GUIDES], et comme utilisateur du produit les personnes accédant, également conformément aux [GUIDES], en lecture ou écriture aux documents placés dans les zones chiffrées.

### *1.2.6. Configuration évaluée*

Le certificat porte sur les configurations suivantes :

- contrôleur de domaine Windows 2008 ;
- serveur SharePoint 2010 installé sur une machine Windows 2008 Server ;
- postes clients sur Windows 7 (architectures 32 et 64 bits) avec les navigateurs Internet Explorer (10), Firefox (24) et Chrome (30) ;
- les deux types de clés d'accès aux zones chiffrées : mot de passe et clé RSA (sur *token* USB Aladdin).

La figure suivante décrit l'environnement de test mis en œuvre par le CESTI.



# 2. L'évaluation

## 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

## 2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 24 mars 2014, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

## 2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les utilisateurs (administrateurs en particulier) de ZonePoint doivent suivre notamment les recommandations suivantes, fournies dans les guides [GUIDES] :

- l'algorithme de chiffrement RSA est reconnu de niveau standard s'il est employé avec un module de taille supérieure ou égale à 2048 bits pour une utilisation n'allant pas au-delà de 2020, et si les exposants publics sont supérieurs à 65536 ;
- outre la recommandation ci-dessus, les clés RSA générées à l'extérieur du produit puis embarquées dans des fichiers de clés ou des objets physiques (pour être utilisées en tant que clés d'accès) doivent être générées conformément aux règles et recommandations de l'ANSSI ;
- la politique P292 doit être configurée avec la valeur SHA-256.

Quoi qu'il en soit, les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

Dans le cadre du processus de qualification standard, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI [ANA-CRY]. Ces résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

## 2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires du produit a été évalué. Comme requis dans le référentiel cryptographique de l'ANSSI ([REF]), la sortie de son alimentation en bruit subit un retraitement de nature cryptographique.
Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

# 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. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « ZonePoint, version 3.0, *build* 330 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté des composants ALC_FLR.3 et AVA_VAN.3.

## 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, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment celles relatives aux mécanismes cryptographiques citées au §2.3, ainsi que celles liées à la tenue à jour de Microsoft SharePoint Server, à l'utilisation de *https* pour la connexion sécurisée au serveur, et au choix par l'utilisateur de mots de passe robustes.

## 3.3. Reconnaissance du certificat

### *3.3.1. Reconnaissance européenne (SOG-IS)*

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

### *3.3.2. Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

# Annexe 1. Niveau d'évaluation du produit

| Classe | Famille | Composants par niveau d'assurance | | | | | | | Niveau d'assurance retenu pour le produit | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | EAL 1 | EAL 2 | EAL 3 | EAL 4 | EAL 5 | EAL 6 | EAL 7 | EAL 3+ | Intitulé du composant |
| **ADV Développement** | ADV_ARC | | **1** | 1 | 1 | 1 | 1 | 1 | **1** | Security architecture description |
| | ADV_FSP | **1** | **2** | **3** | **4** | **5** | 5 | **6** | **3** | Functional specification with complete summary |
| | ADV_IMP | | | | **1** | 1 | **2** | 2 | | |
| | ADV_INT | | | | | **2** | **3** | 3 | | |
| | ADV_SPM | | | | | | **1** | 1 | | |
| | ADV_TDS | | **1** | **2** | **3** | **4** | **5** | **6** | **2** | Architectural design |
| **AGD Guides d'utilisation** | AGD_OPE | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Operational user guidance |
| | AGD_PRE | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Preparative procedures |
| **ALC Support au cycle de vie** | ALC_CMC | **1** | **2** | **3** | **4** | 4 | **5** | 5 | **3** | Authorisation controls |
| | ALC_CMS | **1** | **2** | **3** | **4** | **5** | 5 | 5 | **3** | Implementation representation CM coverage |
| | ALC_DEL | | **1** | 1 | 1 | 1 | 1 | 1 | **1** | Delivery procedures |
| | ALC_DVS | | | **1** | 1 | 1 | **2** | 2 | **1** | Identification of security measures |
| | ALC_FLR | | | | | | | | **3** | Systematic flaw remediation |
| | ALC_LCD | | | **1** | 1 | 1 | 1 | **2** | **1** | Developer defined life-cycle model |
| | ALC_TAT | | | | **1** | **2** | **3** | 3 | | |
| **ASE Evaluation de la cible de sécurité** | ASE_CCL | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Conformance claims |
| | ASE_ECD | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Extended components definition |
| | ASE_INT | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | ST introduction |
| | ASE_OBJ | **1** | **2** | 2 | 2 | 2 | 2 | 2 | **2** | Security objectives |
| | ASE_REQ | **1** | **2** | 2 | 2 | 2 | 2 | 2 | **2** | Derived security requirements |
| | ASE_SPD | | **1** | 1 | 1 | 1 | 1 | 1 | **1** | Security problem definition |
| | ASE_TSS | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | TOE summary specification |
| **ATE Tests** | ATE_COV | | **1** | **2** | 2 | 2 | **3** | 3 | **2** | Analysis of coverage |
| | ATE_DPT | | | **1** | 1 | **3** | 3 | **4** | **1** | Testing: basic design |
| | ATE_FUN | | **1** | 1 | 1 | 1 | **2** | 2 | **1** | Functional testing |
| | ATE_IND | **1** | **2** | 2 | 2 | 2 | 2 | **3** | **2** | Independent testing: sample |
| **AVA Estimation des vulnérabilités** | AVA_VAN | **1** | **2** | 2 | **3** | **4** | **5** | 5 | **3** | Focused vulnerability analysis |

# Annexe 2. Références documentaires du produit évalué

| | |
|---|---|
| [ST] | ZonePoint version 3.0 – Cible de sécurité Critères Communs niveau EAL3+, PX128371 v1r9, février 2014, Prim'X Technologies. |
| [RTE] | Evaluation « ZonePoint » version 3.0, rapport technique d'évaluation, RTE-ZonePoint3-1.01, 24 mars 2014, Amossys. |
| [ANA-CRY] | Evaluation CC EAL3+ du produit ZonePoint version 3.0, Analyse des mécanismes cryptographiques, CRY-ZonePoint3-1.01, 24 mars 2014, Amossys. |
| [CONF] | ZonePoint version 3.0 Build 330 - Liste de configuration, PX13A429, v1r3, 21 février 2014, Prim'X Technologies. |
| [GUIDES] | – Guide d'installation - ZonePoint for MS SharePoint 2010 version 3.0, PX12A388 rev4, octobre 2013, Prim'X Technologies ;<br>– Manuel des politiques, PX104202 rev16, octobre 2013, Prim'X Technologies ;<br>– Guide de mise en oeuvre ZonePoint version 3.0, PX12A386 rev7, 2014, Prim'X Technologies ;<br>– Guide d'utilisation ZonePoint édition Light version 3.0, PX132403 rev2, octobre 2013, Prim'X Technologies. |

# Annexe 3. Références liées 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. | |
| [CER/P/01] | Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI. |
| [CC] | Common Criteria for Information Technology Security Evaluation :<br>Part 1: Introduction and general model,<br>September 2012, version 3.1, revision 4, ref CCMB-2012-09-001;<br>Part 2: Security functional components,<br>September 2012, version 3.1, revision 4, ref CCMB-2012-09-002;<br>Part 3: Security assurance components,<br>September 2012, version 3.1, revision 4, ref CCMB-2012-09-003. |
| [CEM] | Common Methodology for Information Technology Security Evaluation : Evaluation Methodology,<br>September 2012, version 3.1, révision 4, ref CCMB-2012-09-004. |
| [CC RA] | Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000. |
| [SOG-IS] | « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 January 2010, Management Committee. |
| [REF] | Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr. |
| | Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité (RGS_B_2), voir www.ssi.gouv.fr. |
| | Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_3), voir www.ssi.gouv.fr. |