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-CSPN-2017/06

6TZEN contenant les modules logiciels HUB version 1.0.36.FINAL, DEMATREE version 1.05.08.FINAL3 et ADMIMAIL version 3.02.09.FINAL3.

Paris, le 28 mars 2017

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

Guillaume POUPARD
[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 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@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2017/06**
Nom du produit **6TZEN**
Référence/version du produit **HUB version 1.0.36.FINAL** **DEMATREE version 1.05.08.FINAL3** **ADMIMAIL version 3.02.09.FINAL3**
Catégorie de produit Identification, authentification et contrôle d'accès
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Adminext** **17, rue Gazan, 75014 Paris, France**
Centre d'évaluation **Oppida** **4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France**
Fonctions de sécurité évaluées **Authentification des usagers** **Communications sécurisées** **Authentification des administrateurs fonctionnels, des chefs de service et des agents** **Gestion des droits** **Traçabilité**
Fonction(s) de sécurité non évaluées **Néant**
Restriction(s) d'usage Oui (cf. §3.2)

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 CSPN 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 EVALUE 8
1.2.1. Catégorie du produit 8
1.2.2. Identification du produit 8
1.2.3. Fonctions de sécurité 9
1.2.4. Configuration évaluée 9

2. L'EVALUATION 10

2.1. REFERENTIELS D'EVALUATION 10
2.2. CHARGE DE TRAVAIL PREVUE ET DUREE DE L'EVALUATION 10
2.3. TRAVAUX D'EVALUATION 10
2.3.1. Installation du produit 10
2.3.2. Analyse de la documentation 10
2.3.3. Revue du code source (facultative) 11
2.3.4. Analyse de la conformité des fonctions de sécurité 11
2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité 11
2.3.6. Analyse des vulnérabilités (conception, construction, etc.) 11
2.3.7. Accès aux développeurs 11
2.3.8. Analyse de la facilité d'emploi et préconisations 11
2.4. ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES 12
2.5. ANALYSE DU GENERATEUR D'ALEAS 12

3. LA CERTIFICATION 13

3.1. CONCLUSION 13
3.2. RESTRICTIONS D'USAGE 13

1. Le produit

1.1. Présentation du produit

Le produit évalué est « 6Tzen » développé par *ADMINEXT*.
Il est constitué de trois modules logiciels :

- « l'ADMIMAIL », version 3.02.09.FINAL3 qui met en oeuvre le portail « 6Tzen Portail » et permet la gestion des dossiers ;
- le « HUB », version 1.0.36.FINAL responsable de l'envoi des mails sur instruction du module « ADMIMAIL » ;
- le « DEMATREE », version 1.05.08.FINAL3 qui met en œuvre « 6Tzen Admin ». Il permet la gestion des rôles de l'intranet que sont les administrateurs « DEMATREE », les administrateurs fonctionnels, les chefs de service et les agents.

Ce produit est une solution intégrée de dématérialisation des échanges avec l'administration, qui s'adresse à la fois aux citoyens par le biais d'un portail de démarches en ligne, et aux agents publics par le biais d'une application de gestion et d'instruction des demandes.
La solution met à disposition des utilisateurs les deux interfaces, **6Tzen Portail** et **6Tzen Admin**.

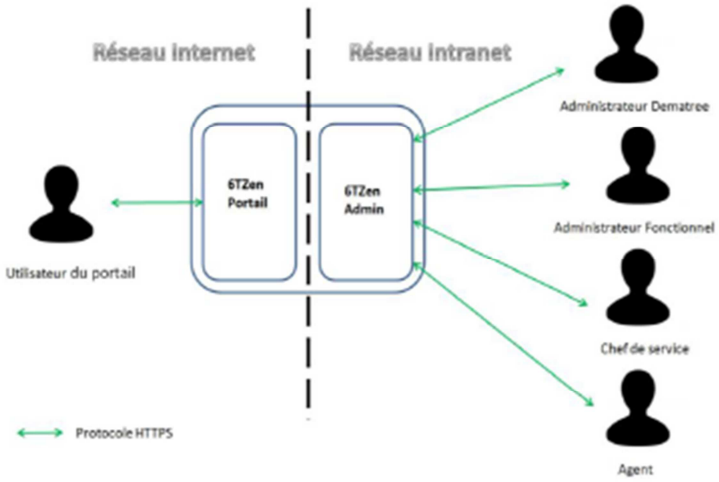

Figure 1 : Architecture fonctionnelle

6Tzen portail
Il s'agit du portail destiné aux usagers pour :

- accéder à une liste de démarches en ligne ;
- effectuer une démarche / remplir un formulaire en ligne ;
- soumettre la demande à l'administration ;
- suivre l'état de la demande en temps réel ;
- échanger avec les agents directement sur le portail ;
- gérer son porte-documents et y stocker ses pièces justificatives ;
- accéder aux réponses de l'Administration.

6Tzen Admin

Il s'agit du portail mis à disposition des agents publics pour :

- prendre en charge les demandes ;
- qualifier et diffuser les demandes entrantes pour traitement par un agent instructeur ;
- échanger avec l'usager directement via l'application ;
- piloter le portefeuille de demandes ;
- instruire la demande en gérant notamment un statut ;
- communiquer le statut des demandes à l'usager.

Les trois modules logiciels, objet de cette évaluation doivent être déployés dans une infrastructure classique de mise à disposition de services web.

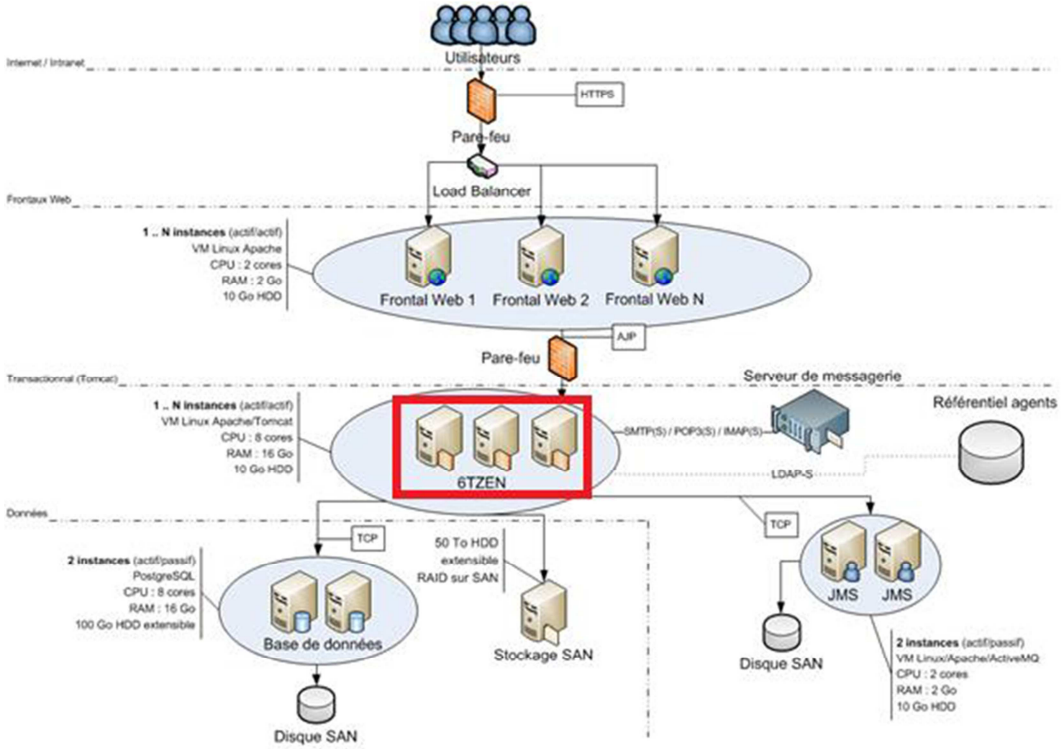

Figure 2 : Déploiement classique de 6Tzen (en rouge, périmètre de l'évaluation)

Les modules « ADMIMAIL, DEMATREE et HUB » ont besoin pour fonctionner des composants suivants :

- un système d'exploitation de type *LINUX* ;
- un serveur web *APACHE* ;
- un serveur d'application *TOMCAT* ;
- un serveur de base de données *POSTGRESQL* ;
- un serveur *ACTIVEMQ* pour le dépôt des messages par l'application ;
- un serveur *SMTP* pour l'envoi des mails.

1.2. Description du produit évalué

La cible de sécurité [CDS] 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 – pare-feu
☐ 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 – environnement d'exécution sécurisé
☐ 11 – terminal de réception numérique (*Set top box*, STB)
☐ 12 – matériel et logiciel embarqué
☐ 13 – automate programmable industriel
☐ 99 – autre

1.2.2. Identification du produit

Nom du produit	6Tzen
Numéro de la version évaluée	HUB version 1.0.36.FINAL DEMATREE version 1.05.08.FINAL3 ADMIMAIL version 3.02.09.FINAL3

Les versions des modules évalués «ADMIMAIL » et « DEMATREE » sont visualisables sur les interfaces web des applications « 6Tzen Admin et Dematree » :

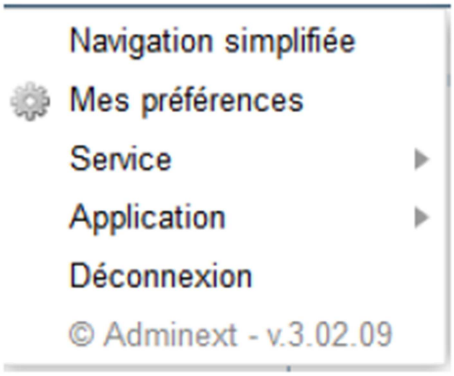

Figure 3 : Version Admimail

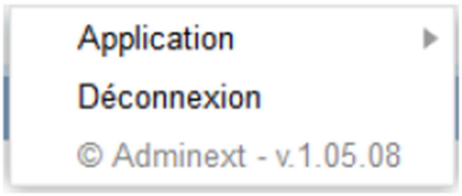

Figure 4 : Version Dematree

Une autre possibilité pour s'assurer que les versions installées correspondent bien à celles évaluées, est offerte une fois le déploiement de l'application sur le serveur *TOMCAT* effectuée :

```
root@oppida-6tzen:~# cat /etc/adminext/version/admimail
3.02.09.FINAL3
root@oppida-6tzen:~# cat /etc/adminext/version/dematree
1.05.08.FINAL3
root@oppida-6tzen:~# cat /etc/adminext/version/hub
1.0.36.FINAL
root@oppida-6tzen:~#
```

Figure 5 : Versions émanant du serveur Tomcat

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- l'authentification des utilisateurs du portail ;
- la communications sécurisées entre les utilisateurs du portail et l'administration ;
- l'authentification des administrateurs fonctionnels, des administrateurs *DEMATREE*, des chefs de service et des agents ;
- la gestion des droits ;
- la traçabilité.

1.2.4. Configuration évaluée

La plateforme de test déployée pour les tests d'évaluation, est une architecture mono-serveur, sous système d'exploitation Debian « Jessie » 8 64 bits (système de base, sans composants additionnels hormis « Serveur SSH » et utilitaires usuels du système).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. 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 est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3. Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1. Installation du produit

2.3.1.1. Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

L'environnement progiciel nécessaire au fonctionnement de 6Tzen s'installe, se met à jour et se configure via un script de déploiement qui est exécuté depuis une machine tierce (voir [INSTALL]).

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

L'installation se fait à l'aide du script de déploiement décrit dans le document [INSTALL]. Ce script se connecte en ssh/scp afin d'effectuer les opérations nécessaires sur les différents composants applicatifs que sont le serveur web Apache, le serveur *J2EE TOMCAT* ainsi que la base de données.

2.3.1.3. Durée de l'installation

Deux journées sont nécessaires pour l'installation.

2.3.1.4. Notes et remarques diverses

Dans le cas d'une architecture de type 3-tiers, l'application n'est pas directement accessible à la suite du déploiement. Il est nécessaire de mettre à jour la configuration *APACHE* afin de permettre les communications avec le serveur *TOMCAT*.

2.3.2. Analyse de la documentation

La documentation est jugée suffisamment complète pour permettre une prise en main du produit.

2.3.3. Revue du code source (facultative)

L'évaluation n'a pas fait l'objet d'une revue de code source.

2.3.4. Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1. Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

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

Il n'a pas été découvert de vulnérabilité du produit qui puisse remettre en cause la sécurité du produit.

2.3.7. Accès aux développeurs

Sans objet.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées. Les utilisateurs doivent se conformer aux documents [PREREQUIS], [INSTALL], et [GUIDES] fournis. Il est recommandé également d'utiliser les paramètres de configuration listés dans [PARAM].
L'évaluateur a mis en avant une restriction d'usage à respecter pour une utilisation sécurisée du produit : utiliser un identifiant à usage unique lors de l'accès à une application via le mécanisme du SSO[1].

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

L'utilisation du produit est simple et intuitive, l'accès aux fonctionnalités est immédiat.

[1] *Single Sign-On.*

2.3.8.4. Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le RTE.

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN. Celle-ci n'a pas identifié de non-conformité au [RGS], ni de vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

Le produit n'implémente pas de générateur d'aléa. Le générateur d'aléa utilisé est le générateur d'OpenSSL (conforme au [RGS]) qui fait appel à /dev/urandom.

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 « 6Tzen, contenant les modules logiciels HUB en version 1.0.36.FINAL, DEMATREE en version 1.05.08.FINAL3 et ADMIMAIL en version 3.02.09.FINAL3 » 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.

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées. Les utilisateurs doivent se conformer aux documents [PREREQUIS], [INSTALL], et [GUIDES] fournis. Il est recommandé également d'utiliser les paramètres de configuration listés dans [PARAM].
De plus, l'évaluateur a mis en avant une restriction d'usage pour une utilisation sécurisée du produit : utiliser un identifiant à usage unique lors de l'accès à une application via le mécanisme du SSO[1].

[1] *Single Sign-On.*

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN – 6TZEN* Version : 3.0 ; Date : 08/03/2017 ; *ADMINEXT.*
[RTE]	Rapport Technique d'Evaluation CSPN 6Tzen3 – 6TZEN, Référence : OPPIDA/CESTI/6Tzen3/RTE/1.4 ; Version : 1.4 ; Date : 24/03/2017 ; *OPPIDA.*
[SPEC-CRY]	*Description des mécanismes cryptographiques* Version : 2.0 ; Date : 08/03/2017 ; *ADMINEXT.*
[PARAM]	*Annexe : liste des paramètres de configuration utilisés pour l'évaluation* Version : 3.0 ; Date : 08/03/2017 ; *ADMINEXT.*
[PREREQUIS]	*Prérequis et installation* Version 4.0 ; Date : 08/03/2017 ; *ADMINEXT.*
[INSTALL]	*Installation, mise à jour et paramétrage de 6TZEN* Version : 3.0 ; Date : 08/03/2017 ; *ADMINEXT.*
[GUIDES]	*Livret d'utilisation : démo assistée du Portail Usager* Version 2.0 ; Date : 29/03/2016 ; *ADMINEXT.* *Livret d'utilisation : administration du portail de démarches* Version 3.0 ; Date : 08/03/2017 ; *ADMINEXT.* *Procédures et API de maintenance* Version 2.0 ; Date : 08/03/2017 ; *ADMINEXT.*

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 des produits (CSPN) des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur www.ssi.gouv.fr/
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr/