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-2012/81

MetaPKI, version 9.2.5

Paris, le 6 décembre 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-CC-2012/81**
Nom du produit **MetaPKI**
Référence/version du produit **Version 9.2.5**
Conformité à un profil de protection **Néant**
Critères d'évaluation et version **Critères Communs version 3.1 révision 3**
Niveau d'évaluation **EAL 3 augmenté** **ALC_FLR.3, AVA_VAN.3**
Développeur(s) **BULL** **Rue Jean Jaures, 78340 Les Clayes sous Bois, France**
Commanditaire **BULL** **Rue Jean Jaures, 78340 Les Clayes sous Bois, France**
Centre d'évaluation **Amossys** **4 bis allée du bâtiment, 35000 Rennes, France**
Accords de reconnaissance applicables **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

1.1. Présentation du produit

Le produit évalué est « MetaPKI, version 9.2.5 » développé par BULL.

Ce produit permet de mettre en œuvre une infrastructure de gestion de clés publiques (ou PKI pour *Public Key Infrastructure*). Il fournit une solution de gestion des certificats (demande, création, renouvellement, révocation), qu'il s'agisse des certificats de chiffrement, d'authentification ou de signature, et une gestion des listes de révocation. Le produit permet de définir une autorité de certification racine, des autorités de certification subalternes et des autorités d'enregistrement.

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.

La cible de sécurité s'inspire du profil de protection [PP CIMC].

1.2.2. Identification du produit

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

La version certifiée du produit (9.2.5) et de ses prérequis[1] (4.8.0) sont identifiables par les éléments suivants :

- sur les CD ROM de livraison et leurs bons de livraison associé, émis séparément (qui contiennent également l'empreinte SHA-1 du produit) ;
- depuis l'interface web du produit, dans le menu « Informations/ Versions ».

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la gestion des utilisateurs du produit et de leurs droits (authentification et contrôle d'accès) ;
- la gestion de politiques de certification ;
- la création et la publication de certificats numériques conformes aux standards X509v3 et RFC-5280 ;
- la création et la publication de liste de révocation de certificats ;
- le traitement de requêtes OCSP[2] (analyse, réponse) ;
- le séquestre et le recouvrement de clés ;

[1] Composants Linux additionnels requis pour l'utilisation de MetaPKI.
[2] *Online Certificate Status Protocol.*

- la journalisation et l'audit ;
- le stockage sécurisé des mots de passe utilisateurs ;
- la sauvegarde et la restauration des données applicatives.

1.2.4. Architecture

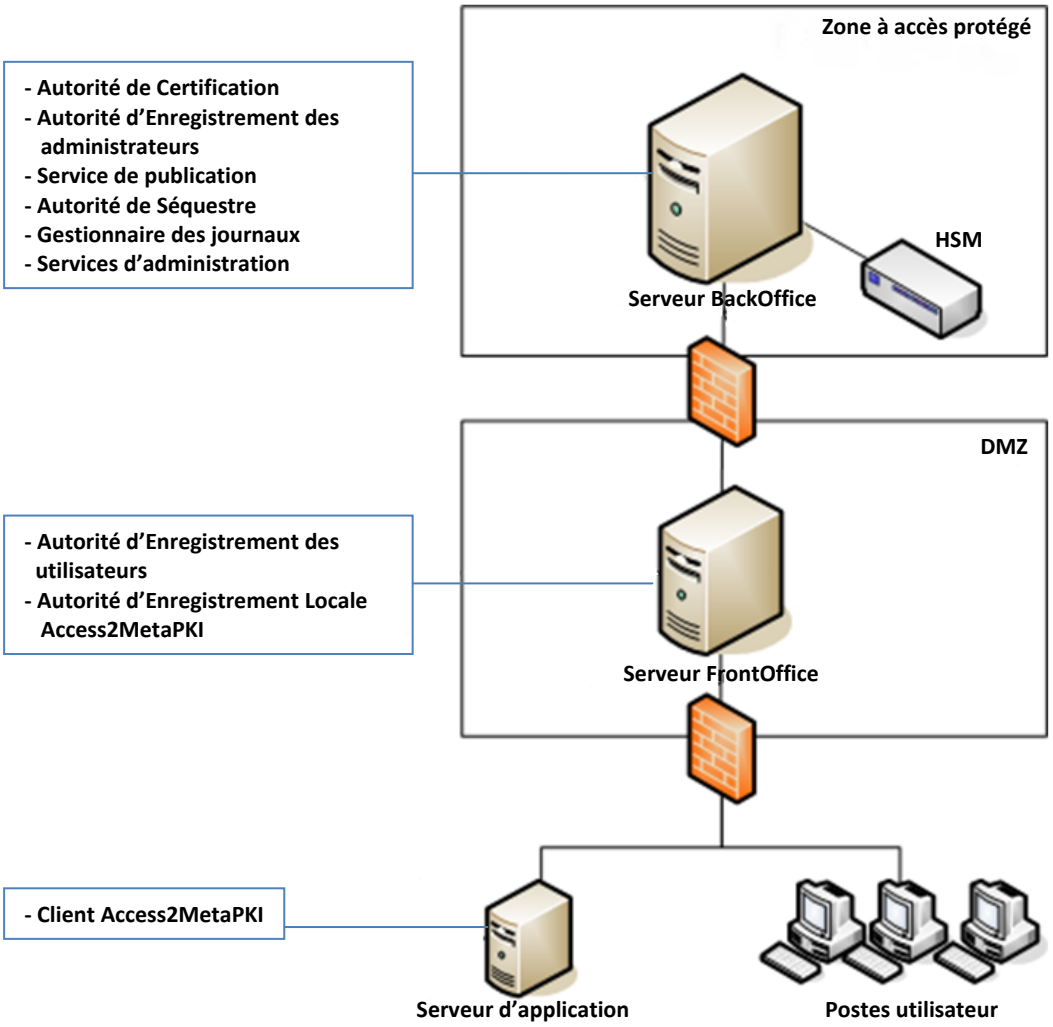
Le produit MetaPKI constitue une architecture client/serveur distribuée de type application web.
Dans le cadre de l'évaluation, ces fonctionnalités sont mises en œuvre depuis un serveur BackOffice situé en zone sécurisée, non accessible depuis l'extérieur. Un serveur FrontOffice fait le lien entre les utilisateurs et ce serveur.

Le produit MetaPKI est composé des principales entités suivantes :

- des Autorités d'Enregistrement[1] (AE et AEL) qui sont chargées de la validation des demandes de certificat ; AE et AEL peuvent être mis en œuvre soit par le biais d'une interface web ou via une API (Access2MetaPKI) ;
- des Autorités de Certification (AC) racine et déléguée qui sont chargées de la validation des demandes de certification et de la génération des certificats et des listes de révocation qui sont signés par le HSM[2] de l'AC concernée ;
- une entité de génération des clés qui disposent des deux modes suivants :
    - une génération centrale où les bi-clés sont générés par le HSM de l'AC et exportées avec leur certificat associés au format PKCS#12 (protégé par un mot de passe) ;
    - une génération locale où les bi-clés sont générées par des cartes à puce, en ce cas seules les clés publiques sont extraites des cartes en vue de leur signature par le HSM de l'AC ;
- une entité de publication qui publie les certificats et les listes de révocation sur le serveur Web de MetaPKI ;
- un guichet de retrait qui permet l'exportation des clés privées générées en central et des certificats générés par l'AC ;
- une Autorité de Séquestre qui fait appel au HSM pour les opérations de séquestre des clés privées générées en central et leur recouvrement ;
- un répondeur OCSP qui transmet les requêtes OSCP à l'AC qui a généré le certificat et qui signe les réponses OCSP à l'aide du HSM ;
- un gestionnaire de journaux qui signe périodiquement les évènements journalisés à l'aide du HSM.

[1] *Registration Authority (RA).*
[2] *Hardware Security Module.*

La figure suivante décrit un exemple de déploiement du produit MetaPKI.



Ici les entités décrites ci-dessus sont créées et hébergées sur le serveur BackOffice. Lorsqu'elles doivent être visibles sur le FrontOffice, une entité de type proxy est créée et associée à l'entité d'origine. Il y a donc autant d'entités de type proxy que d'entités devant être visibles sur le serveur FrontOffice.
Toutes les entités disposent d'un certificat et d'une paire de clés afin de s'authentifier entre elles. Leurs bi-clés sont générées par le HSM et exportées sur le serveur BackOffice au format PKCS#12. Les communications entre les serveurs BackOffice et FrontOffice sont protégées par :

- authentification mutuelle et protocole TLS 1.0 ;
- ou par canal SSH pour l'installation et la mise à jour du produit, et les opérations d'administration distantes (changement de périodicité de la journalisation, modification de politiques de certification…).

La communication entre le HSM et le serveur BackOffice (tous deux devant être colocalisés dans une zone sécurisée) se fait par un réseau Ethernet dédié, sans chiffrement (liaison point à point).

1.2.5. Cycle de vie

Le produit a été développé sur le site suivant :

BULL

Rue Jean Jaures
78340 Les Clayes sous Bois
France

1.2.6. Configuration évaluée

La plateforme de test mise en œuvre par le CESTI correspond à l'architecture logique de déploiement présentée en 1.2.4, les serveurs BackOffice et FrontOffice étant installés sur un même serveur physique dans deux machines virtuelles VMWare.

Le tableau suivant décrit l'environnement de test pris en compte dans le cadre de cette évaluation :

	Serveur	Clients
OS	Red Hat 6 ES (Hardened version) MetaPKI Pre-requistes, version 4.8.0	Windows XP SP3 (32 bits)
Supports cryptographiques	BULL TRUSTWAY PCI CRYPTOGRAPHIC, version S507-RSA 4096 *Certifié par l'ANSSI sous la référence ANSSI-2010-09*	MultiApp ID IAS ECC *Certifié par l'ANSSI sous la référence ANSSI-2009-56* Middleware Classic Client 6.1_005
Lecteur de carte		CCID Teo by XIRING
SGBD	PostgreSQL v9.0.6	
LDAP	openldap client v2.4.29	
Navigateur web		Internet explorer 8.0

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [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 30 novembre 2012, 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

Le produit ne comporte pas de mécanismes cryptographiques entrant dans le périmètre d'évaluation. En effet, ces mécanismes sont implémentés par des éléments de l'environnement du produit MetaPKI : HSM, carte à puce, et librairie OpenSSL.

2.4. Analyse du générateur d'aléas

Le produit ne comporte pas de générateur d'aléas entrant dans le périmètre d'évaluation.

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 « MetaPKI, version 9.2.5 » 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 :

- le système d'exploitation Linux utilisé pour héberger les serveurs doit faire l'objet d'un durcissement. Les mesures minimales à appliquer au moment de la certification sont décrites dans le guide d'installation et de déploiement fourni par le développeur. Le client final doit mettre en place une veille technique concernant les composants fournis dans les prérequis de MetaPKI et les mettre à jour en cas de vulnérabilité publique avérée ;
- lorsque certaines fonctions de MetaPKI doivent être accessibles depuis Internet, et afin de réduire au maximum la surface d'attaque, il est recommandé de limiter au strict minimum les accès et de renforcer les dispositifs sécuritaires de l'environnement hébergeant MetaPKI ;
- pour une mise en œuvre du produit conforme au RGS, les supports cryptographiques utilisés (HSM et cartes à puce) doivent avoir eux-mêmes fait l'objet d'une qualification et être utilisés conformément aux termes de leurs qualifications respectives ;
- AC et HSM doivent être installés dans une zone à accès protégé.

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]	Cible de sécurité de référence pour l'évaluation : - « Security Target METAPKI », référence EVALCC-MPKI-ST-01, version 1.2.
[RTE]	Rapport technique d'évaluation : - « METAPKI - rapport technique d'évaluation », référence BUL001-RTE01, version 2.01.
[CONF]	Liste de configuration documentaire : - Liste-Fourniture-Documentaire, version 5. Liste de configuration logicielle : - configurationList-MetaPKI-9_2_5.odt ; - configurationList-MetaPKI-9_2_5.xml.
[GUIDES]	Guide d'installation du produit : - « Guide d'installation et de déploiement de MetaPKI », référence METAPKI-INST-GDE-01, version1.11. Guide d'administration du produit : - « Manuel d'administration de MetaPKI », référence METAPKI-ADM-GDE-01, version 4.13 ; - « Description des formulaires porteurs », référence METAPKI-ADM-GDE-02, version 2.0. Guide d'utilisation du produit : - « Guide utilisateur de la TOE », référence METAPKI-UTIL-GDE-01, version1.4.
[PP CIMC]	Certificate Issuing and Management Components (CIMC) Security Level 3 Protection Profile, Version 1.0, 31 octobre 2001.

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, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[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 Janvier 2010, Management Committee.