Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification PP/0309

Profil de protection « Cryptographic Module for CSP Signing Operations without Backup » Version 0.28

Paris, le 18 décembre 2003

Le Directeur central de la sécurité des systèmes d'information

Henri Serres

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport atteste la conformité de la version évaluée du profil de protection aux critères d'évaluation.
Un profil de protection est un document public qui définit pour une catégorie de produits un ensemble d'exigences et d'objectifs de sécurité indépendants de leur technologie et de leur implémentation. Les produits ainsi définis satisfont les besoins de sécurité communs à un groupe d'utilisateurs.
La certification d'un profil de protection ne constitue pas en soi une recommandation de ce profil de protection par le centre de certification.

Table des matières

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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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 selon les ITSEC et les Critères Communs sont publiques et disponibles en français sur le site Internet :

www.ssi.gouv.fr

Le site international concernant la certification selon les Critères Communs est accessible à l'adresse Internet :

www.commoncriteria.org

1. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : Cryptographic Module for CSP Signing Operations without Backup
Version : 0.28
Date : 27 octobre 2003

1.2. Rédacteur

Ce profil de protection a été rédigé par le groupe « WS/E-Sign Project Team D2 » du CEN/ISSS (Comité Européen de Normalisation / Information Society Standardization System), dans le cadre de l'initiative européenne pour la standardisation sur la signature électronique (EESSI) :

CEN/ISSS WS/E-Sign Project Team D2

Rue de Stassart 36
1050 Brussels
Belgique

1.3. Description du profil de protection

1.3.1. Généralités

Ce profil de protection définit les exigences de sécurité d'un module cryptographique utilisé par un prestataire de service de certification (CSP) comme un élément de son système sûr pour fournir des services de signature, tels que le service de génération de certificats ou les services d'information sur le statut d'un certificat.

1.3.2. Périmètre de la cible d'évaluation

La cible d'évaluation (TOE) est un module cryptographique, utilisé pour la création des bi-clés du CSP, et leur utilisation pour la création et la vérification des signatures électroniques avancées des certificats qualifiés ou des certificats d'information sur le statut des certificats.

1.4. Exigences fonctionnelles

Les **exigences fonctionnelles de sécurité** sont les suivantes :

- Audit data generation (FAU_GEN.1)
- User identity association (FAU_GEN.2)
- Guarantees of audit data availability (FAU_STG.2/TOE)
- Cryptographic key generation (FCS_CKM.1)
- Cryptographic key destruction (FCS_CKM.4)
- Cryptographic operation (FCS_COP.1/SIGN)
- Quality metrics for random numbers (FCS_RND.1)
- Subset access control (FDP_ACC.1/CRYPTO)
- Subset access control (FDP_ACC.1/AUDIT)
- Security attribute based access control (FDP_ACF.1/CRYPTO)

- Security attribute based access control (FDP_ACF.1/AUDIT)
- Export of user data without security attributes (FDP_ETC.1)
- Subset information flow control (FDP_IFC.1/CRYPTO)
- Partial elimination of illicit information flows (FDP_IFF.4/Crypto)
- Subset residual information protection (FDP_RIP.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- Authentication failure handling (FIA_AFL.1)
- User attribute definition (FIA_ATD.1)
- Verification of secrets (FIA_SOS.1)
- Timing of authentication (FIA_UAU.1)
- Timing of identification (FIA_UID.1)
- Management of security attributes (FMT_MSA.1/ROLE_CRYPTO)
- Management of security attributes (FMT_MSA.1/ROLE_AUDIT)
- Secure security attributes (FMT_MSA.2)
- Static attribute initialisation (FMT_MSA.3)
- Management of TSF data (FMT_MTD.1/ACCESS_CONTROL)
- Management of TSF data (FMT_MTD.1/USER_Crypto)
- Management of TSF data (FMT_MTD.1/USER_AUDIT)
- Management of TSF data (FMT_MTD.1/RAD)
- Management of TSF data (FMT_MTD.1/AUDIT)
- Specification of Management Functions (FMT_SMF.1)
- Security roles (FMT_SMR.1)
- Abstract machine testing (FPT_AMT.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Notification of physical attack (FPT_PHP.2)
- Resistance to physical attack (FPT_PHP.3)
- Manual recovery (FPT_RCV.1)
- TSF testing (FPT_TST.1)
- Trusted path (FTP_TRP.1/TOE)

Ces exigences fonctionnelles du profil de protection sont extraites de la partie 2 des Critères Communs [CC] à l'exception de FCS_RND.1.

1.5. Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau **EAL4**[1] **augmenté des composants d'assurance suivants**, conformes à la partie 3 des Critères Communs :

Composants	Descriptions
ADV_IMP.2	Implementation of the TSF
AVA_CCA.1	Covert channel analysis
AVA_VLA.4	Highly resistant

Tableau 1 - Augmentations

Le niveau de résistance exigé pour les fonctions de sécurité est **élevé** (**SOF-High**).
Toutes les exigences d'assurance du profil de protection sont extraites de la partie 3 des Critères Communs [CC].

1.6. Objectifs de sécurité sur l'environnement

Les objectifs de sécurité sur l'environnement sont les suivants :

- les applications qui utilisent le produit doivent réaliser les vérifications de sécurité nécessaires sur les données qui sont échangées avec le produit. Les applications doivent également réaliser les authentifications des utilisateurs nécessaires et les fonctions de contrôle d'accès qui ne peuvent pas être réalisées au sein du produit. Les contrôles de sécurité dans l'environnement du produit doivent aussi empêcher les manipulations non autorisées des données soumises au produit.
- l'environnement doit assurer la disponibilité des traces d'audit générées et exportées par le produit. Ces traces doivent être examinées.
- lorsque l'application le permet, les données échangées entre un utilisateur et le produit doivent être protégées en confidentialité et en intégrité.
- les personnes utilisant les services du produit doivent être informées de leurs responsabilités civiles, financières et légales, aussi bien que des obligations spécifiques à leur rôle. Le personnel doit être formé pour utiliser correctement le produit.
- le produit doit être protégé par des mesures physiques, logiques et organisationnelles, afin d'empêcher toute modification du produit et la divulgation des biens à protéger. Ces mesures doivent restreindre l'utilisation du produit aux seules personnes autorisées.
- des plans et des procédures de récupération doivent exister, permettant une récupération sécurisée et opportune en cas de problème majeur avec le produit (c'est-à-dire lorsque le produit est bloqué dans son état sécurisé après une défaillance, une discontinuité du service ou après détection d'une altération physique).

[1] Annexe 1 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

- des procédures et des contrôles dans l'environnement du produit doivent être définis et appliqués, permettant une installation et une initialisation sécurisées du produit pour la génération de signatures pour des certificats qualifiés ou des certificats d'information sur le statut. Cela inclut la génération de la clé, l'importation de la clé, la configuration initiale des autres données de la TSF (rôles, utilisateurs) et les informations d'authentification des utilisateurs.
- des procédures et des contrôles dans l'environnement du produit doivent être définis, permettant l'exploitation du produit au sein d'un système d'une autorité de certification conforme aux exigences de la Directive européenne et de la politique pour les autorités de certification émettant des certificats qualifiés.
- le CSP doit définir les obligations et les services de gestion et les rôles opératoires pour le produit. Le CSP doit informer et former le personnel suivant leur rôle. Le CSP doit informer le personnel utilisant le produit de ses responsabilités civiles, financières et légales.

2. L'évaluation

2.1. Centre d'évaluation

SERMA Technologies

30 avenue Gustave Eiffel
33608 Pessac
France

Téléphone : +33 (0)5 57 26 08 64

Adresse électronique : m.dus@serma.com

2.2. Commanditaire

Bull S.A.

68 route de Versailles
78430 Louveciennes
France

2.3. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et aux interprétations finales suivantes : 008, 013, 019, 043, 049, 051, 058, 064, 065, 084, 085, 098, 138.

2.4. Evaluation du profil de protection

L'évaluation du profil de protection a été menée sur la base des exigences de la classe APE définie dans la partie 3 des Critères Communs [CC] :

Class APE	Protection profile evaluation
APE_DES.1	TOE description
APE_ENV.1	Security environment
APE_INT.1	ST introduction
APE_OBJ.1	Security objectives
APE_REQ.1	IT security requirements
APE_SRE.1	Explicitly stated IT security requirements

Tableau 2- Composants d'assurance de la classe APE

3. Conclusions de l'évaluation

3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats détaillés de l'évaluation du profil de protection.

3.2. Niveau d'évaluation

Pour tous les composants de la classe APE, les verdicts suivants ont été émis :

Class APE	Protection profile evaluation	
APE_DES.1	TOE description	Réussite
APE_ENV.1	Security environment	Réussite
APE_INT.1	ST introduction	Réussite
APE_OBJ.1	Security objectives	Réussite
APE_REQ.1	IT security requirements	Réussite
APE_SRE.1	Explicitly stated IT security requirements	Réussite

Tableau 3 - Composants et verdicts associés

3.3. Recommandations et limitations d'usage

Le certificat d'un profil de protection ne s'applique qu'à la version évaluée du profil de protection.

3.4. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que le profil de protection Cryptographic Module for CSP Signing Operations without Backup identifié au paragraphe 1.1 du présent rapport **est conforme** aux exigences de la classe APE. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique d'évaluation [RTE].

Annexe 1. Niveaux d'assurance prédéfinis CC

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 2. Références

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CC]	Critères Communs pour l'évaluation de la sécurité des technologies de l'information: ▪ Part 1: Introduction and general model, august 1999, version 2.1, ref CCIMB-99-031 ; ▪ Part 2: Security functional requirements, august 1999, version 2.1, ref CCIMB-99-032 ; ▪ Part 3: Security assurance requirements, august 1999, version 2.1, réf: CCIMB-99-033.
[CEM]	Méthodologie d'évaluation de la sécurité des technologies de l'information: ▪ Part 2: Evaluation Methodology, august 1999, version 1.0, ref CEM- 99/045.
[RTE]	Evaluation Report, Référence CMCSO-PP_ APE, version 2.5, Serma Technologies.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr