PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification PP 2006/04

Profil de Protection Machine à voter (PP-CIVIS)

Paris, le 11 juillet 2006.

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

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 sont publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

Accords de reconnaissance des certificats

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

La direction centrale de la sécurité des systèmes d'information passe aussi des accords de reconnaissance avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties. (article 9 du décret 2002-535)

Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance mutuelle 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] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.

[2] En juin 2006, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada, l'Australie-Nouvelle Zélande, le Japon, la Norvège, les Pays-Bas et la Corée du Sud ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Suède, la Turquie, la République Tchèque, Singapour, l'Inde et le Danemark.

1. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : Profil de Protection Machine à voter
Référence : PP-CIVIS[1]
Version : 1.0
Date : 21 juin 2006

1.2. Rédacteur

Ce profil de protection a été rédigé par :

4-6 avenue du Vieil Etang
Bât B
78180 MONTIGNY LE BRETONNEUX
FRANCE

Adresse électronique : cesti@oppida.fr

1.3. Description du profil de protection

1.3.1. Généralités

Le profil de protection a été rédigé dans le cadre d'un marché du SGDN/DCSSI. Il est le résultat de réunions avec les utilisateurs et les développeurs de ce type de produit.
Ce profil de protection est conforme aux préconisations pour la qualification de produits de sécurité au niveau standard selon la version 3.0 des CC [QS-QR].

1.3.2. Périmètre de la cible d'évaluation

Afin d'alléger les ressources humaines et financières nécessaires au déroulement des élections et de réduire la durée du dépouillement et de la centralisation des résultats, le code électoral permet l'utilisation de moyens de vote électronique nommés « machines à voter » (loi n 69-419 du 10 mai 1969 et loi n 88-1262 du 30 décembre 1988, codifiée notamment dans l'article L. 57-1 du code électoral).

La machine à voter est une borne sur laquelle un électeur peut faire son choix pour un ou plusieurs scrutins électoral.
L'objet de ce profil de protection est de spécifier les caractéristiques sécuritaires de la machine à voter.

[1] Lors de sa phase de développement, ce Profil de Protection était identifié à l'aide de la référence : OPPIDA/2006/DOC/529/2.0.

1.4. Exigences fonctionnelles

Les **exigences fonctionnelles de sécurité** définies par le profil de protection sont les suivantes :

- FAU_GEN.1 Audit data generation without time
- FAU_GEN.2 Audit data generation with time
- FDP_ACC.1 Access control
- FDP_ACC.2 Access control with automatic modification of security attributes
- FDP_ISA.1 Security attribute initialisation
- FDP_UNL.3 Unlinkability of objects
- FIA_UAU.1 User authentication by TSF
- FIA_UID.2 User identification
- FIA_USB.1 User-subject binding
- FIA_LOB.2 User-initiated locking out
- FMI_TIM.1 Time stamps
- FPT_TST.1 TSF self-testing

Toutes les exigences fonctionnelles du profil de protection sont extraites de la partie 2 des Critères Communs [CC].

1.5. Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau **EAL2[1] augmenté des composants d'assurance suivants** :

Composants	Descriptions
ADV_IMP.1*	Implementation representation of the TSF
ADV_TDS.3**	Basic modular design
ALC_DVS.1	Identification of security measures
ALC_FLR.3	Systematic flaw remediation
ALC_TAT.1	Well-defined development tools
AVA_VAN.3	Focused vulnerability analysis

Tableau 1 - Augmentations

** Le composant ADV_IMP.1 est raffiné de la façon suivante : The selected sample of the implementation representation shall embrace all the cryptographic mechanisms.*

*** Le composant ADV_TDS.3 est raffiné de la façon suivante : The description of the design of the TSF in terms of modules could be limited to the cryptographic mechanisms of the TOE.*

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

Le composant ADV_TDS.3** étant moins « exigeant » que ADV_TDS.3, seule une conformité au composant ADV_TDS.2 peut-être reconnue au titre des accords de reconnaissance.

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

1.6.1. Objectifs de sécurité sur l'environnement de développement

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

- La TOE doit être évalué au niveau de qualification standard défini par la DCSSI; soit un EAL2 augmenté des exigences d'assurance ADV_IMP.1*, ADV_TDS.3**, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1 et AVA_VAN.3.

* Le composant ADV_IMP.1 est raffiné de la façon suivante : The selected sample of the implementation representation shall embrace all the cryptographic mechanisms.

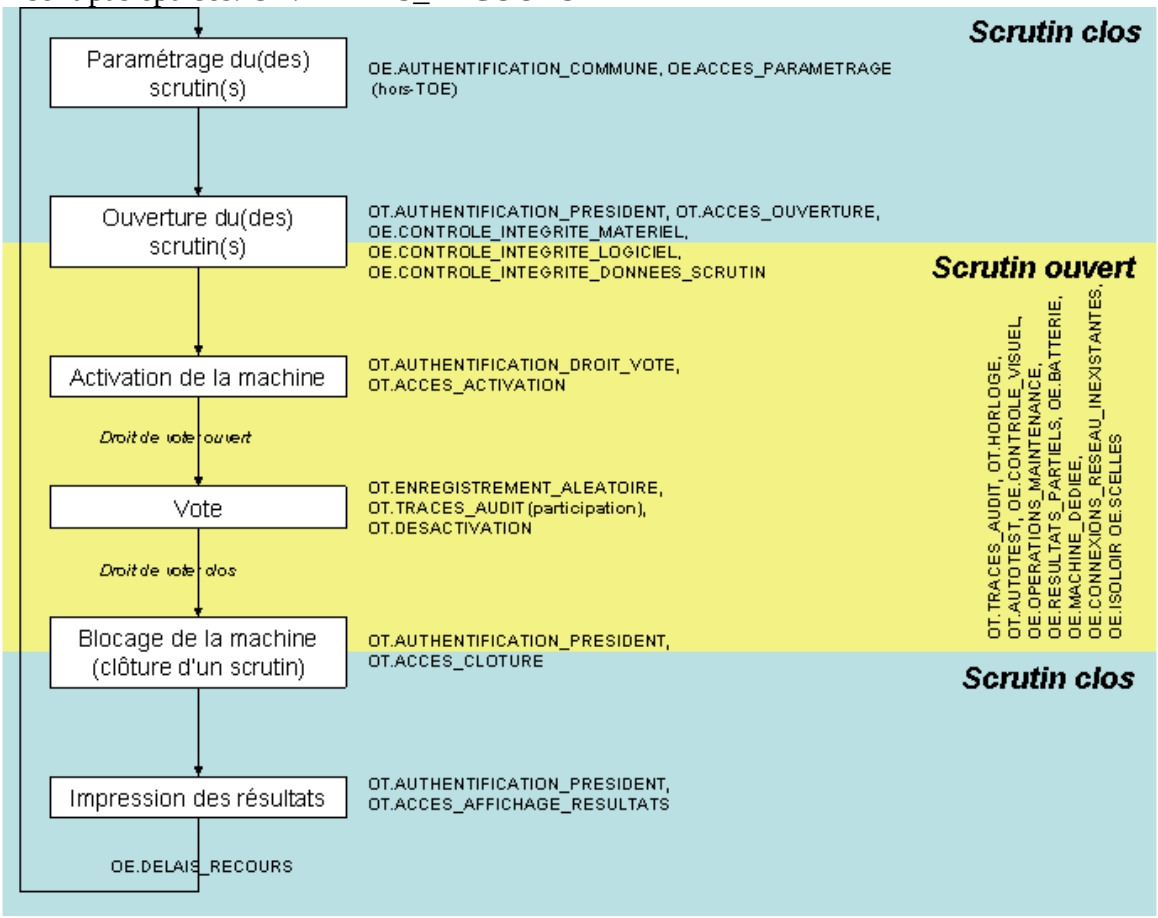
** Le composant ADV_TDS.3 est raffiné de la façon suivante : The description of the design of the TSF in terms of modules could be limited to the cryptographic mechanisms of the TOE.

1.6.2. Objectifs de sécurité sur l'environnement opérationnel

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

- Lors du scrutin, la machine doit être constamment sous le contrôle visuel du président du bureau de vote ou d'un de ses assesseurs. OE.CONTROLE_VISUEL
- L'environnement de la TOE doit identifier et authentifier les agents de la commune avant les opérations de paramétrage du(des) scrutin(s). OE.AUTHENTIFICATION_COMMUNE
- L'environnement de la TOE doit limiter aux seuls agents de la commune authentifiés l'accès aux fonctions de paramétrage du(des) scrutin(s) qui permettent notamment de réinitialiser les résultats et la participation. OE.ACCES_PARAMETRAGE
- Toute opération de maintenance sur les machines, qui permettent notamment de modifier les logiciels de la TOE, doit être interdite au cours du scrutin pour éviter toute tentative de fraude. En cas de problème, une autre machine doit être utilisée. OE.OPERATIONS_MAINTENANCE
- En cas de panne de la machine, la conception de la TOE doit permettre de récupérer les mémoires contenant les résultats afin de pouvoir comptabiliser ces « résultats partiels » à l'issue du scrutin. OE.RESULTATS_PARTIELS
- La machine doit pouvoir fonctionner sur batterie afin de pouvoir continuer le scrutin en cas de coupure électrique. Au redémarrage, le président doit bien vérifier si le dernier vote a été pris en compte avant la coupure (en vérifiant la participation). Si non, l'électeur doit de nouveau saisir son choix. OE.BATTERIE
- La machine et son logiciel ne doivent pouvoir réaliser que les fonctionnalités nécessaires au déroulement du scrutin. OE.MACHINE_DEDIEE

- La machine à voter ne doit pas être connectée à un réseau lors du scrutin. OE.CONNEXIONS_RESEAU_INEXISTANTES
- La machine doit être installée de façon à protéger l'électeur des regards extérieurs (par exemple dans un isoloir), garantissant ainsi la confidentialité de son vote. OE.ISOLOIR
- Les machines à voter doivent disposer de suffisamment d'espace mémoire pour enregistrer tous les votes et tous les évènements (erreurs, anomalies,…) intervenant au cours du scrutin. OE.MEMOIRE_SUFFISANTE
- La borne doit faire l'objet d'un contrôle d'intégrité juste avant l'ouverture du scrutin pour détecter la présence éventuelle d'un piège matériel introduit lors de sa fabrication, sa livraison ou son stockage. L'intégrité doit également être contrôlé régulièrement au cours du scrutin pour détecter tout acte de vandalisme ou problème matériel. OE.CONTROLE_INTEGRITE_MATERIEL
- Le logiciel de la machine doit faire l'objet d'un contrôle d'intégrité juste avant l'ouverture du scrutin pour détecter la présence éventuelle d'un programme pernicieux introduit lors de la fabrication de la machine, sa livraison ou son stockage. OE.CONTROLE_INTEGRITE_LOGICIEL
- Avant l'ouverture du scrutin, le président doit vérifier que les données du scrutin stockées dans la machine correspondent bien aux données officielles. OE.CONTROLE_INTEGRITE_DONNEES_SCRUTIN
- Des scellés doivent être déposés à l'issue de contrôle d'intégrité du matériel et du logiciel pour détecter toute tentative de piégeage de la machine. Ces scellés doivent être contrôlés régulièrement. OE.SCELLES
- Toute opération de maintenance ou de réinitialisation de la machine (paramétrage pour un nouveau scrutin) doit être interdite tant que les délais de recours pour le scrutin ne sont pas épuisés. OE.DELAIS_RECOURS



2. L'évaluation

2.1. Centre d'évaluation

SILICOMP - AQL

1 rue de la châtaigneraie
CS 51766
F 35513 Cesson Sévigné Cedex
France

Téléphone : +33 (0)2 99 12 50 00

Adresse électronique : cesti@aql.fr

2.2. Commanditaire

SGDN/DCSSI

51 boulevard de La Tour-Maubourg
75007 Paris

Adresse électronique : certification.dcssi@sgdn.pm.gouv.fr

2.3. Référentiels d'évaluation

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

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	Security Target evaluation
APE_INT.1	PP introduction
APE_CCL.1	Conformance claims
APE_SPD.1	Security problem definition
APE_OBJ.2	Security objectives
APE_ECD.1	Extended components definition
APE_REQ.2	Derived 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. Résultats d'évaluation

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

Class APE	Protection profile evaluation	
APE_INT.1	PP introduction	Réussite
APE_CCL.1	Conformance claims	Réussite
APE_SPD.1	Security problem definition	Réussite
APE_OBJ.2	Security objectives	Réussite
APE_ECD.1	Extended components definition	Réussite
APE_REQ.2	Derived 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 Profil de Protection Machine à voter (PP-CIVIS) 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].

3.5. Reconnaissance européenne (SOG-IS)

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

3.6. Reconnaissance internationale (CC RA)

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

Annexe 1. Niveaux d'assurance prédéfinis CC

Classe	Famille	Composants d'assurance par niveau d'évaluation							
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	QS
Development	ADV_ARC		1	1	1	1	1	1	**1**
	ADV_FSP	1	2	3	4	5	5	6	**2**
	ADV_IMP				1	1	2	2	**1***
	ADV_INT					2	3	4	
	ADV_SPM						1	1	
	ADV_TDS		1	2	3	4	5	6	**3****
Guidance documents	AGD_OPE	1	1	1	1	1	1	1	**1**
	AGD_PRE	1	1	1	1	1	1	1	**1**
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5	**2**
	ALC_CMS	1	2	3	4	5	5	5	**2**
	ALC_DEL		1	1	1	1	1	1	**1**
	ALC_DVS			1	1	1	2	2	**1**
	ALC_FLR								**3**
	ALC_LCD				1	2	2	3	
	ALC_TAT				1	2	3	3	**1**
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1	**1**
	ASE_ECD	1	1	1	1	1	1	1	**1**
	ASE_INT	1	1	1	1	1	1	1	**1**
	ASE_OBJ	1	2	2	2	2	2	2	**2**
	ASE_REQ	1	2	2	2	2	2	2	**2**
	ASE_SPD		1	1	1	1	1	1	**1**
	ASE_TSS	1	1	1	1	1	1	1	**1**
Tests	ATE_COV		1	2	2	2	3	3	**1**
	ATE_DPT			1	1	2	2	3	
	ATE_FUN		1	1	1	1	2	2	**1**
	ATE_IND	1	2	2	2	2	2	3	**2**
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5	**3**

* Le composant ADV_IMP.1 est raffiné de la façon suivante : The sample of the implementation representation shall contain all the cryptographic mechanisms of the TOE.
** Le composant ADV_TDS.3 est raffiné de la façon suivante : The description of the design of the TSF in terms of modules could be limited to the cryptographic mechanisms of the TOE.

Annexe 2. Références

<table>
<tr><td colspan="2">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.</td></tr>
<tr><td>[CC]</td><td>Critères Communs pour l’évaluation de la sécurité des technologies de l’information:
Part 1: Introduction and general model,
June 2005, version 3.0, revision 2, ref CCMB-2005-07-001;
Part 2: Security functional requirements,
July 2005, version 3.0, revision 2, ref CCMB-2005-07-002 ;
Part 3: Security assurance requirements,
July 2005, version 3.0, revision 2,ref CCMB-2005-07-003.</td></tr>
<tr><td>[CEM]</td><td>Méthodologie d’évaluation de la sécurité des technologies de l’information:
Evaluation Methodology,
June 2005, version 3.0, revision 2, ref CCMB-2005-07-004.</td></tr>
<tr><td>[RTE]</td><td>PROFIL DE PROTECTION CIVIS- Rapport Technique d’Evaluation, Réf. OPP001-CIVIS-RTE-1.00 v1.0, du 22 juin 2006</td></tr>
<tr><td>[QS-QR]</td><td>Définition des paquets d’assurance pour la qualification standard et la qualification renforcée suivant les CC version 3 – Document du 8 février 2006</td></tr>
<tr><td>[CC RA]</td><td>Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.</td></tr>
<tr><td>[SOG-IS]</td><td>«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.</td></tr>
</table>

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