Direction centrale de la sécurité des systèmes d'information

Profil de Protection
Machine à voter
(PP-CIVIS)

Date de publication	**:**	21 juin 2006
Référence	**:**	PP-CIVIS
Version	**:**	1.0

Table des matières

1 Introduction

1.1 Identification

Titre :	Profil de protection – Machine à voter
Référence :	PP-CIVIS, version 1.0, 21 juin 2006
Auteur :	Oppida

1.2 Contexte

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).

L'objet du présent document est de présenter les exigences de sécurité sur ces machines à voter.

1.3 Présentation générale de la cible d'évaluation

1.3.1 Type de TOE

La machine à voter est une borne sur laquelle un électeur peut faire son choix pour un ou plusieurs scrutins électoral.

1.3.2 Particularités / caractéristiques de sécurité de la TOE

L'Article L57-1 du code électoral précise au sujet des machines à voter :
« Des machines à voter peuvent être utilisées dans les bureaux de vote des communes de plus de 3 500 habitants figurant sur une liste fixée dans chaque département par arrêté du représentant de l'Etat (modification dans une ordonnance de fin 2004).
Les machines à voter doivent être d'un modèle agréé par arrêté du ministre de l'intérieur et satisfaire aux conditions suivantes :

- comporter un dispositif qui soustrait l'électeur aux regards pendant le vote ;
- permettre plusieurs élections de type différent le même jour à compter du 1 janvier 1991 ;
- permettre l'enregistrement d'un vote blanc ;
- ne pas permettre l'enregistrement de plus d'un seul suffrage par électeur et par scrutin ;
- totaliser le nombre de votants sur un compteur qui peut être lu pendant les opérations de vote ;
- totaliser les suffrages obtenus par chaque liste ou chaque candidats ainsi que les votes blancs, sur des compteurs qui ne peuvent être lus qu'après la clôture du scrutin ;

- ne pouvoir être utilisées qu'à l'aide de deux clés différentes, de telle manière que, pendant la durée du scrutin, l'une reste entre les mains du président du bureau de vote et l'autre entre les mains de l'assesseur tiré au sort parmi l'ensemble des assesseurs. »

1.3.3 Eléments matériels de la TOE

Borne

La machine à voter est essentiellement constituée d'une borne matérielle disposant d'un écran, de touches permettant aux électeurs de faire leurs choix et d'un dispositif d'impression des résultats.

Dispositifs d'authentification du président du bureau de vote ou d'un assesseur

Pour s'authentifier, le président du bureau de vote et un assesseur disposent de dispositifs matériels (carte à puce, jeton ou simplement clé normale).

Dispositif d'activation de la machine à voter (« droit de vote »)

L'activation de la machine à voter juste avant le vote d'un électeur peut être, dans certains systèmes, directement réalisée par l'électeur au moyen d'un dispositif matériel de type carte de vote ou autre.

1.3.4 Eléments logiciels de la TOE

Logiciel de la machine à voter

Un logiciel dédié pour les machines à voter est installé sur les bornes pour constituer les machines à voter.

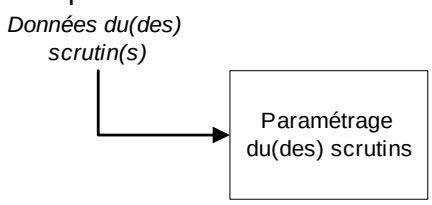
1.3.5 Fonctions essentielles de la machine à voter

1.3.5.1 Fonction : Paramétrage du(des) scrutin(s)

La machine à voter permet aux agents de la commune de charger les données nécessaires au déroulement du(des) scrutin(s) et de la configurer en fonction du nombre et de la nature des élections prévues. La machine doit notamment permettre de charger les candidatures telles qu'elles figurent sur la liste adressée par le préfet.
Le paramétrage peut être réalisé directement sur la machine ou via une station distincte sur un média inséré ensuite dans la machine.
Durant cette phase, toutes les modifications peuvent être réalisées car un contrôle d'intégrité des données du scrutin se déroulera à l'ouverture du scrutin.

Les informations nécessaires pour la réalisation de cette fonction sont :

- Les données relatives au(x) scrutin(s) : nature et date de l'élection, nom de la commune, heures d'ouverture et de clôture du scrutin, numéro du bureau de vote, circonscription, liste des candidats ou question posée.



1.3.5.2 Fonction : Ouverture du(des) scrutin(s) par le président du bureau de vote

Conformément aux articles L. 63 et R. 55-1 du code électoral, les membres du bureau doivent constater avant l'ouverture du scrutin que :

- la machine à voter fonctionne correctement (voyants, procédure manuelle de test, autodiagnostic, etc.). Cette vérification est prévue par le règlement technique ;
- les compteurs des suffrages sont à la graduation zéro ;
- les candidatures mentionnées par la machine à voter correspondent à celles indiquées par la liste adressée par le préfet au maire de la commune.

Un procès-verbal dit d'« initialisation de la machine » peut être imprimé.

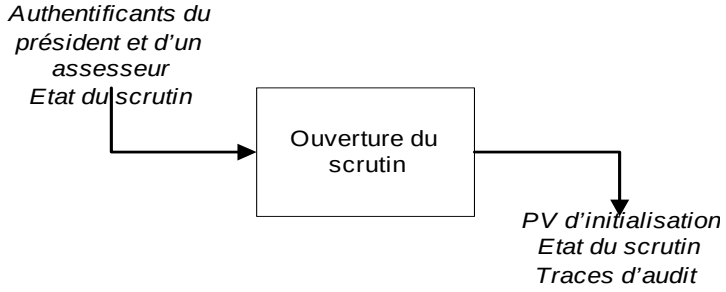
Le président du bureau peut alors ouvrir le(s) scrutin(s), par l'activation d'un double dispositif d'ouverture actionné par le président du bureau de vote et un assesseur. Ce dispositif est constitué d'un dispositif matériel (carte à puce, jeton ou simplement clé normale) détenu par le président du bureau de vote et d'une autre détenue par un assesseur. Un double du dispositif d'authentification de l'assesseur doit pouvoir être détenu par un autre assesseur.

Les informations nécessaires pour la réalisation de cette fonction sont :

- Authentifiants du président du bureau de vote et d'un assesseur,
- Etat du scrutin : clos,

Les informations produites par la réalisation de cette fonction sont :

- PV d'initialisation de la machine,
- Etat du scrutin : ouvert,
- Traces d'audit.



1.3.5.3 Fonction : Activation de la machine pour un(plusieurs) scrutin(s)

La machine à voter ne doit être utilisable que par un électeur dont le droit de vote a été reconnu par les membres du bureau de vote. Pour ce faire, après vérification de l'identité et de l'inscription sur la liste électorale de l'électeur par les membres du bureau de vote, la machine à voter doit être « activée » afin de permettre à cet électeur, et à celui-là seul, de voter.

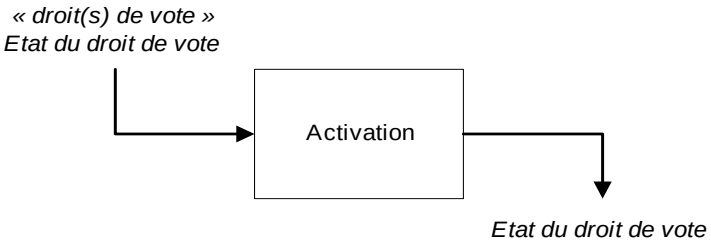
La machine est activée à l'aide d'un dispositif d'activation qui contient le « droit de vote » qui est mis à disposition du président ou directement de l'électeur. Dans le cas de la mise à disposition du président, ce dispositif peut être confondu avec son dispositif d'authentification.

En cas de scrutins multiples, l'électeur ne peut voter que pour les scrutins pour lesquels il est électeur (un droit de vote pour chacun des scrutins) :

- si l'activation de la machine est effectuée par le président du bureau de vote, la machine n'est activée que pour le(s) scrutin(s) pour lesquels l'électeur est autorisé à voter ;
- si l'activation de la machine est effectuée par une action de l'électeur sur la machine (introduction d'un « droit de vote »), ce « droit de vote » ne doit actionner que le(s) scrutin(s) pour lesquels l'électeur est autorisé à voter.

Les informations nécessaires pour la réalisation de cette fonction sont :
- Le(s) « droit(s) de vote »,
- L'état du droit de vote : clos.

Les informations produites par la réalisation de cette fonction sont :
- Droit de vote : ouvert.



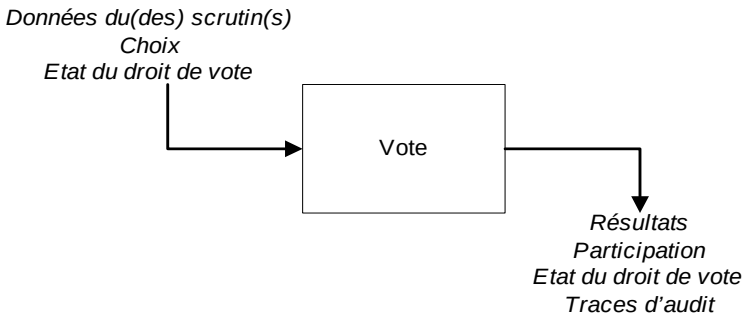
1.3.5.4 Fonction : Vote pour un scrutin

La machine à voter permet à l'électeur :
- d'effectuer un choix parmi les propositions présentées (candidats, listes de candidats, oui/non) ou de sélectionner un vote blanc ;
- de pouvoir modifier à tout moment du processus le choix effectué, jusqu'à la confirmation du vote ;
- de confirmer le choix effectué, ce qui provoque son enregistrement dans la machine.

Dès l'enregistrement du vote d'un électeur pour un des scrutins pour lequel il dispose du droit de vote, le droit de vote est rendu « inactif » pour le scrutin pour lequel l'électeur a voté.
Si la machine a été activée pour plusieurs scrutins, l'électeur peut faire son choix pour les autres scrutins.

Les informations nécessaires pour la réalisation de cette fonction sont :
- Les données du(des) scrutin(s),
- Le choix de l'électeur (bulletin de vote) pour un scrutin,
- L'état du droit de vote : ouvert.

Les informations produites par la réalisation de cette fonction sont :
- Les résultats d'un scrutin pour la machine,
- La participation d'un scrutin pour la machine,
- L'état du droit de vote : clos,
- Des traces d'audit en cas d'erreur de maniement d'un utilisateur ou d'une anomalie de fonctionnement.

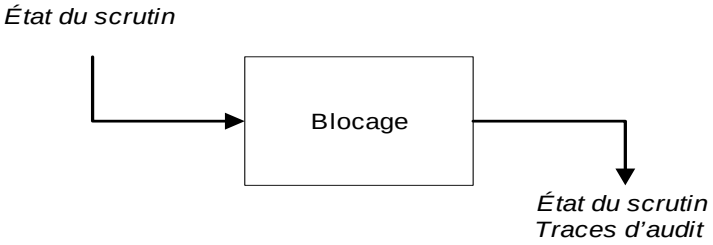


1.3.5.5 Fonction : Blocage de la machine (clôture d'un scrutin)

Les machines à voter doivent être bloquées à la déclaration de clôture d'un scrutin par le président du bureau de vote. Cette action rend inefficace toute action sur l'une des touches ou commandes de la machine pour le scrutin clos.

Les informations nécessaires pour la réalisation de cette fonction sont :
- Etat du scrutin : ouvert.

Les informations produites par la réalisation de cette fonction sont :
- Etat du scrutin : clos,
- Traces d'audit.



1.3.5.6 Fonction : Affichage des résultats pour un scrutin

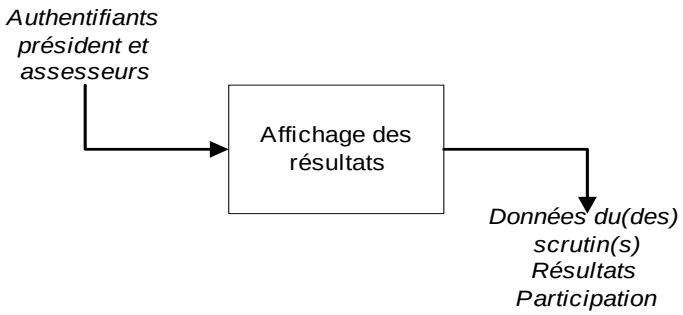
Conformément à l'article R. 66-1 du code électoral, le dépouillement des suffrages est assimilé au dénombrement des suffrages enregistrés par les machines à voter.
La lecture des résultats contenus dans la machine à voter n'est possible qu'après la mise en œuvre d'un double dispositif matériel (carte à puce, jeton ou simplement clé normale), actionné par le président du bureau de vote et un assesseur.
Les résultats et les informations nécessaires à l'édition du procès-verbal, dont les heures d'ouverture et de clôture du scrutin, sont visualisés et imprimés. En cas de scrutin multiple, le dépouillement s'effectue scrutin par scrutin.

La lecture des résultats ne doit pas effacer les données :
- la possibilité d'une relecture des résultats doit être préservée ;
- les résultats doivent être stockés de manière inaltérable, au moins jusqu'à l'épuisement des délais de recours contre les résultats.

Après restitution des résultats, la machine à voter est bloquée ; elle ne peut être utilisée de nouveau, après authentification des intervenants, que pour une relecture des données ou une réinitialisation pour prise en compte des données relatives à un nouveau scrutin.

Les informations nécessaires pour la réalisation de cette fonction sont :
- Les authentifiants du président du bureau de vote et d'un assesseur.

Les informations produites par la réalisation de cette fonction sont :
- Les données du(des) scrutins
- Les résultats d'un scrutin pour la machine,
- La participation d'un scrutin pour la machine.



1.3.5.7 Etat de la machine

Le référentiel technique définit un « état de la machine » prenant pour valeurs « active » ou « inactive ».
Cet état est en fait la combinaison des différents états suivants :

- Etat du scrutin : état d'un des scrutins réalisés sur la machine (prends deux valeurs : « ouvert » / « clos ») ;
- Droit de vote : état fonction de la présentation du droit de vote d'un électeur pour un scrutin donné (« ouvert » / « clos »).

La machine est « active » uniquement lorsque le scrutin et le droit de vote sont « ouverts ». Lorsque l'électeur a voté ou a décidé de ne pas voter, la machine repasse à l'état « inactive » jusqu'à la présentation d'un nouveau droit de vote.

1.3.6 Environnement matériel et logiciel

Les machines à voter sont autonomes. Elles peuvent fonctionner sur secteur ou sur batteries. Elles sont déconnectées de tout réseau.

1.4 Déclarations de conformité

Le présent profil de protection se veut conforme aux Critères Communs version 3.0. [CC1][CC2][CC3]

Les cibles de sécurité (ST) qui se voudront conformes au présent profil de protection devront déclarer une conformité *démontrable*.

Les produits qui se voudront conformes au profil de protection devront se conformer également aux exigences de la qualification standard de la DCSSI. [QUALIF_STD] [CRYPTO_STD].

2 Définition du problème de sécurité

2.1 Utilisateurs

Les différentes personnes qui accèdent aux machines à voter sont les suivantes.

2.1.1 Le président du bureau de vote

Le président du bureau de vote est responsable du bon déroulement du scrutin. Il déclare notamment l'ouverture et la clôture du scrutin et supervise le dépouillement.

2.1.2 Les assesseurs

Les assesseurs assistent le président du bureau pour assurer le bon déroulement du scrutin. Ils peuvent notamment vérifier les identités des électeurs.

2.1.3 Les électeurs

Pour voter, l'électeur doit être inscrit sur la liste électorale du bureau de vote où il se présente. Dans les communes de moins de 5 000 habitants, il peut présenter sa carte électorale ou une pièce d'identité. En revanche, dans les communes de 5 000 habitants et plus, il doit nécessairement présenter une pièce d'identité.

2.1.4 Les agents de la commune

Les agents de la commune ont pour rôle de préparer le bureau de vote et donc de réceptionner, de stocker et d'installer la machine à voter.

2.2 Hypothèses

2.2.1 Contrôle visuel

H.CONTROLE_VISUEL

Lors du scrutin, la machine est constamment sous le contrôle visuel du président du bureau de vote ou d'un de ses assesseurs. Cette hypothèse permet de limiter tous les risques liés à d'éventuelles tentatives de réalisation d'actions malveillantes sur la machine à voter de type vandalisme ou intrusion physique.

Note : de la même façon, si un électeur vole le dispositif d'authentification du président, il n'est pas en mesure de l'utiliser sans se faire repérer.

2.2.2 Contrôle des opérations de maintenance

H.OPERATIONS_MAINTENANCE

Toute opération de maintenance sur les machines est interdite au cours du scrutin pour éviter toute tentative de fraude. En cas de problème, une autre machine doit être utilisée.

2.2.3 Connexions réseau

H.CONNEXIONS_RESEAUX_INEXISTANTES

Les machines à voter ne sont connectées à aucun réseau lors du scrutin.

2.2.4 Isoloir

H.ISOLOIR

Les machines à voter disposent d'un mécanisme assurant la confidentialité du vote au moment du vote. Pour les machines ne disposant pas d'un tel mécanisme, la confidentialité du vote est assurée par un isoloir.

2.2.5 Dimensionnement de la machine

H.MEMOIRE_SUFFISANTE

Les machines à voter disposent de suffisamment d'espace mémoire pour enregistrer tous les votes et tous les évènements (erreurs, anomalies,...) intervenant au cours du scrutin.

2.3 Menaces

2.3.1 Clôture du scrutin

Clôture du scrutin par un électeur

Un électeur clôt le scrutin durant son déroulement.
Cet acte peut avoir pour conséquence l'indisponibilité du vote jusqu'à ce que le président ouvre de nouveau le scrutin.

2.4 Politiques de sécurité organisationnelles (OSP)

P.EAL

La TOE doit être évaluée au niveau EAL2 augmenté des composants ADV_TDS.3, ADV_IMP.1, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1, AVA_VAN.3.

P.04-OUVERTURE

Avant l'ouverture du scrutin, une procédure d'autotest doit permettre aux membres du bureau de vote de vérifier que seuls les composants matériels et logiciels agréés sont activés lors du scrutin et que la machine à voter fonctionne correctement (voyants, procédure manuelle de test, autodiagnostic, etc.).

P.07-OUVERTURE

A l'ouverture du scrutin, la machine à voter doit être débloquée par le biais d'un double dispositif d'authentification électronique actionné par le président du bureau de vote et un assesseur. Ce dispositif est constitué d'une clé[1] détenue par le président du bureau de vote et d'une autre détenue par un assesseur. Un double de la clé de l'assesseur doit pouvoir être détenu par un autre assesseur.

P.08-ACTIVATION

La machine à voter doit pouvoir être rendue « active », soit par une action de l'électeur sur la machine elle-même (introduction d'un code, d'une carte magnétique ou à puce par

[1] La notion de clé est à interpréter au sens large ; le dispositif de déblocage peut également prendre la forme d'un dispositif électronique de type carte à puce ou télécommande infrarouge.

exemple), soit par une commande à disposition du président du bureau de vote, agissant sur le terminal.

P.17-CLOTURE
Le blocage de la dernière machine bloque l'ensemble du dispositif. Ce blocage interdit toute modification, par qui que ce soit, des mémoires contenant les résultats du scrutin[2].

P.18-DEPOUILLEMENT
La lecture des résultats contenus dans la machine à voter ne doit pouvoir être possible qu'après la mise en oeuvre d'un double dispositif d'authentification électronique, constitué de deux clés actionnées par le président du bureau de vote et un assesseur.

P.20-DEPOUILLEMENT
La lecture des résultats ne doit pas effacer les données :
- la possibilité d'une relecture des résultats doit être préservée ;
- les résultats doivent être stockés de manière inaltérable, au moins jusqu'à l'épuisement des délais de recours contre les résultats.

P.21-DEPOUILLEMENT
Après restitution des résultats, la machine à voter doit être bloquée ; elle ne doit pouvoir être utilisée de nouveau, après authentification des intervenants, que pour une relecture des données ou une réinitialisation pour prise en compte des données relatives à un nouveau scrutin.

P.44-CONCEPTION
La machine à voter doit être une machine dédiée. Sa conception ne doit pas comporter de spécificités propres aux règles des différents scrutins. Ses capacités doivent se résumer à des fonctions de stockage de données, d'affichage, de sélection d'un choix, de comptage des suffrages et de transmission des résultats, ainsi que les fonctions normales d'administration.

P.45-CONCEPTION
Les programmes nécessaires à la réalisation de ces fonctions doivent être des modules indépendants et stockés sous forme inaltérable. Les mémoires destinées au stockage des informations propres au scrutin doivent être amovibles, avec verrouillage physique d'accès durant le scrutin, afin d'éviter toute manipulation frauduleuse.

P.46-CONCEPTION
La machine à voter doit comprendre une horloge interne qui permette de dater les divers événements et comptes-rendus mémorisés au cours d'un scrutin. Les données heure-minute-seconde doivent pouvoir être ajustées par les membres du bureau de vote avant l'ouverture du scrutin.
Un dispositif complémentaire, interne à la machine, doit permettre d'enregistrer et de dater tous les événements, qu'il s'agisse d'actions effectuées durant ou hors d'un scrutin, de manière à garder une trace de toutes les interventions sur la machine et d'en vérifier l'imputabilité en cas de contrôle ou de contentieux.

P.47-CONCEPTION
De l'ouverture à la clôture du scrutin, les bulletins de vote sont stockés dans la machine de façon à ce que la lecture de leur contenu soit impossible, même si une intervention sur la

[2] Cette OSP s'applique jusqu'à l'expiration des délais de recours sauf en cas d'authentification du président et d'un assesseur (cf P.21-DEPOUILLEMENT)

machine est nécessaire. Il ne doit pas être possible de connaître le résultat provisoire du scrutin.

P.48-CONCEPTION
La machine à voter doit mémoriser, visualiser, et restituer à la demande :
- les messages découlant d'une erreur de maniement d'un utilisateur, ou d'une anomalie de fonctionnement ;
- les actions d'un utilisateur ayant entraîné une modification de l'état de la machine.
Ces informations sont datées et rédigées de façon à être compréhensibles par un personnel du bureau de vote qui ne possède pas de compétences techniques particulières.

P.49-EMPLOI
La machine doit pouvoir être installée de façon à protéger l'électeur des regards extérieurs, garantissant ainsi la confidentialité de son vote.

P.53-EMPLOI
La machine à voter doit signaler, à l'électeur et aux membres du bureau de vote, les anomalies de fonctionnement de la machine ayant pour origine, soit un dysfonctionnement de l'un de ses composants, soit une manipulation erronée d'un utilisateur.

P.65-CONFIDENTIALITE_VOTE
Si l'utilisation d'une machine à voter doit être interrompue en cours de scrutin (panne, remplacement de la machine), aucune indication sur le choix qui a été effectué par l'électeur ne doit être visible.

P.66-CONFIDENTIALITE_VOTE
Les bulletins de vote doivent être enregistrés de façon aléatoire, pour qu'il ne soit pas possible lors du dépouillement de reconstituer la chronologie des votes.

P.68-INTEGRITE_DONNEES
Si l'utilisation d'une machine à voter doit être interrompue en cours de scrutin (panne, remplacement de la machine), il doit être possible de s'assurer si l'électeur a ou non enregistré son vote avant l'incident, tout en respectant l'exigence 65.

P.69-INTEGRITE_DONNEES
Si l'utilisation d'une machine à voter doit être interrompue en cours de scrutin (panne, remplacement de la machine), les informations mémorisées relatives aux votes (nombre de votants, bulletins de vote) doivent pouvoir être récupérées sans altération par les membres du bureau de vote, tout en respectant l'exigence 65.

P.70-INTEGRITE_DONNEES
La machine à voter doit être protégée durant les opérations électorales contre tout type d'intrusion frauduleuse, à l'aide de multiples dispositifs de sécurité.

P.72-DISPONIBILITE
La machine à voter doit permettre de détecter et de localiser, par autotests, une avarie.

P.79-ALIMENTATION_DE_SECOURS
Le dispositif d'alimentation de secours doit assurer un bon fonctionnement de la machine à voter durant au moins 12 heures (ce dispositif peut être interne ou externe). En cas de

basculement sur le dispositif d'alimentation de secours, la machine à voter ne doit subir aucune perte d'informations ni de détérioration de fonctionnement[3].

[3] On entend par perte d'information le cas où la participation aurait été incrémentée alors que le choix de l'électeur n'aurait pas été enregistré (et inversement). La machine pourrait s'arrêter en cas de coupure électrique mais une procédure permettrait de récupérer les votes non enregistrés.

3 Objectifs de sécurité

3.1 Objectifs de sécurité pour la TOE

3.1.1 Identification et authentification des opérateurs

OT.AUTHENTIFICATION_PRESIDENT
La TOE doit identifier et authentifier le président du bureau de vote et les assesseurs avant les opérations d'ouverture et de clôture du scrutin et pour le dépouillement.

OT.AUTHENTIFICATION_DROIT_VOTE
La TOE doit identifier et authentifier la présentation du « droit de vote ».

3.1.2 Enregistrement des évènements

OT.TRACES_AUDIT
La TOE doit mémoriser, visualiser, et restituer à la demande :

- les actions d'un utilisateur ayant entraîné une modification de l'état de la machine (ouverture du(des) scrutin(s), activation de la machine, vote[4], clôture du scrutin) ;
- les messages découlant d'une erreur de maniement d'un utilisateur, ou d'une anomalie de fonctionnement.

OT.HORLOGE
La TOE doit disposer d'une horloge interne lui permettant de dater les évènements enregistrés.

3.1.3 Protection du système

OT.ACCES_OUVERTURE
La TOE doit limiter l'accès aux fonctions d'ouverture du(des) scrutin(s) aux seuls président et assesseurs authentifiés.

OT.ACCES_ACTIVATION
La TOE doit limiter l'activation de la machine à la présentation d'un « droit à voter » authentifié.

OT.DESACTIVATION
La TOE doit empêcher la vue du choix d'un électeur par l'électeur suivant.

OT.ACCES_CLOTURE
La TOE doit limiter l'accès aux fonctions de clôture du(des) scrutin(s) aux seuls président et assesseurs authentifiés.

OT.ACCES_AFFICHAGE_RESULTATS
La TOE doit restreindre l'affichage des résultats aux seuls président et assesseurs authentifiés et uniquement lorsque le scrutin est clos.

[4] L'enregistrement de la participation permet l'enregistrement des actions de vote.

OT.AUTOTEST
Un mécanisme d'autotest doit être implémenté pour détecter automatiquement une panne ou un dysfonctionnement d'un des éléments de la machine.

3.1.4 Protection des données

OT.ENREGISTREMENT_ALEATOIRE
La TOE doit enregistrer les votes dans un ordre aléatoire afin qu'il ne soit pas possible de reconstituer la chronologie des votes.

3.2 Objectifs de sécurité pour l'environnement de développement

3.2.1 Evaluation de sécurité

OD.EAL
La TOE doit être évaluée au niveau EAL2 augmenté des composants ADV_TDS.3, ADV_IMP.1, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1, AVA_VAN.3.

3.3 Objectifs de sécurité pour l'environnement opérationnel

3.3.1 Contrôle de la machine et du vote

OE.CONTROLE_VISUEL
Lors du scrutin, la machine doit être constamment sous le contrôle visuel du président du bureau de vote ou d'un de ses assesseurs.

3.3.2 Contrôle des opérations de paramétrage de la machine

OE.AUTHENTIFICATION_COMMUNE
L'environnement de la TOE doit identifier et authentifier les agents de la commune avant les opérations de paramétrage du(des) scrutin(s).

OE.ACCES_PARAMETRAGE
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.

3.3.3 Contrôle des opérations de maintenance

OE.OPERATIONS_MAINTENANCE
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.

3.3.4 Disponibilité du scrutin

OE.RESULTATS_PARTIELS

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.BATTERIE
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.

3.3.5 Usage dédié

OE.MACHINE_DEDIEE
La machine et son logiciel ne doivent pouvoir réaliser que les fonctionnalités nécessaires au déroulement du scrutin.

3.3.6 Connexions réseau

OE.CONNEXIONS_RESEAU_INEXISTANTES
La machine à voter ne doit pas être connectée à un réseau lors du scrutin.

3.3.7 Utilisation d'un isoloir

OE.ISOLOIR
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.

3.3.8 Dimensionnement de la machine

OE.MEMOIRE_SUFFISANTE
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.

3.3.9 Contrôles d'intégrité

OE.CONTROLE_INTEGRITE_MATERIEL
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_LOGICIEL
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_DONNEES_SCRUTIN
Avant l'ouverture du scrutin, le président doit vérifier que les données du scrutin stockées dans la machine correspondent bien aux données officielles.

OE.SCELLES

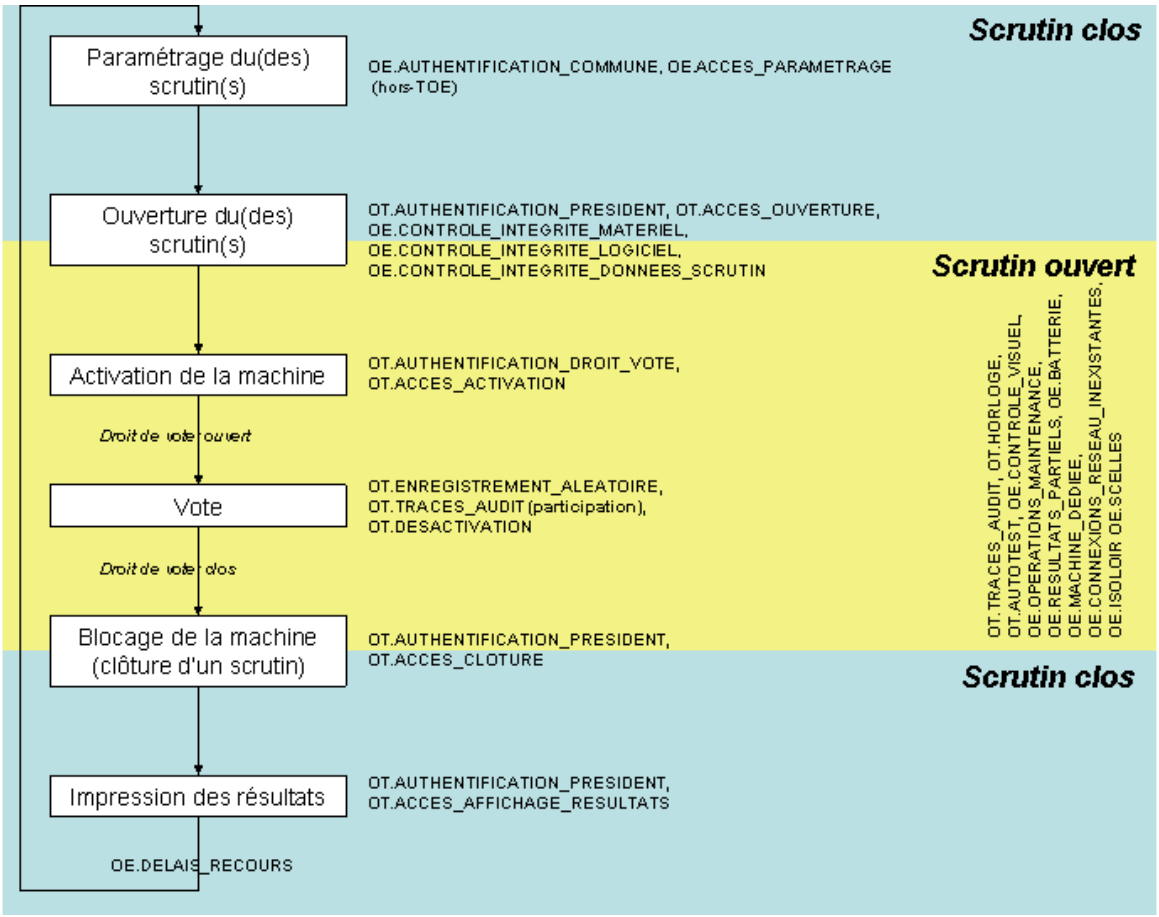
Des scellés doivent être déposés à l'issue de contrôle d'intégrité du matériel et du logiciel pour détecter toute tentative de piégeage de la machine. Ces scellés doivent être contrôlés régulièrement.

3.3.10 Délais de recours

OE.DELAIS_RECOURS

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.

3.4 Récapitulatifs des objectifs de sécurité



4 Exigences de sécurité des TI

4.1 Introduction

4.1.1 Sujets

Un sujet est une entité active de la TOE ; les sujets réalisent des opérations dans la TOE. Les sujets sont distincts des entités actives qui se trouvent hors de la TOE (par exemples les utilisateurs).

President

Il s'agit du président du bureau de vote.
Ses attributs de sécurité sont les suivants :

- Authenticated : prends la valeur « True » si le président s'est authentifié et « False » dans le cas contraire.

Assessor

Il s'agit d'un des assesseurs du président.
Ses attributs de sécurité sont les suivants :

- Authenticated : prends la valeur « True » si l'assesseur s'est authentifié et « False » dans le cas contraire.

Elector

Il ne s'agit pas de l'électeur en lui-même mais de son droit de vote (anonyme).
Ses attributs de sécurité sont les suivants :

- Authenticated : prends la valeur « True » si le droit de vote a été présenté et « False » dans le cas contraire.

4.1.2 Objets

Un objet est une entité passive de la TOE ; ce sont les entités sur lesquelles sont réalisées les opérations.

Scrutiny

Il s'agit du scrutin en lui-même.
Ses attributs de sécurité sont les suivants :

- status : L'état du scrutin peut prendre pour valeur : « close » (par défaut) ou « open » lorsque le scrutin est ouvert.

Vote access

Il s'agit de l'accès à l'opération de vote.
Ses attributs de sécurité sont les suivants :

- status : L'état du vote prend pour valeur « close » par défaut, « open » lorsque le droit de vote a été présenté.

Audit tracks files (fichiers de traces d'audit)

Il s'agit des fichiers contenant les informations enregistrées au cours du fonctionnement de la machine et pouvant être utiles en cas d'audit.
L'objet n'a pas d'attribut de sécurité.

Clock (horloge interne)

Il s'agit de l'horloge interne de la machine.
L'objet n'a pas d'attribut de sécurité.

Participation files (fichiers de la participation)

Il s'agit des fichiers qui contiennent la participation au(x) scrutin(s).
L'objet n'a pas d'attribut de sécurité.

Results files (fichiers des résultats)

Il s'agit des fichiers qui contiennent les résultats du(des) scrutin(s) pour la machine.
L'objet n'a pas d'attribut de sécurité.

4.1.3 Opérations

Une opération est une action spécifique d'un sujet sur un objet de la TOE.

Scrutiny opening

Il s'agit de l'opération d'ouverture du scrutin (cf 1.3.5).

Les sujets et les objets impliqués sont les suivants :

- Sujets : President, Assessor
- Objets : Scrutiny

Machine activation

Il s'agit de l'opération d'activation de la machine (cf 1.3.5).

Les sujets et les objets impliqués sont les suivants :

- Sujets : Elector
- Objets : Vote access

Vote

Il s'agit de l'opération de vote par un électeur (cf 1.3.5).

Les sujets et les objets impliqués sont les suivants :

- Sujets : Elector
- Objets : Results files, Participation files, vote access

Participation display

Il s'agit de l'opération d'affichage de la particiaption.

Les sujets et les objets impliqués sont les suivants :

- Sujets : Anybody (Elector, President, Assessor,...)
- Objets : Participation files

Scrutiny closing

Il s'agit de l'opération de clôture du scrutin (cf 1.3.5).

Les sujets et les objets impliqués sont les suivants :

- Sujets : President, Assessor
- Objets : Scrutiny

Results display

Il s'agit de l'opération d'affichage des résultats ainsi que des traces d'audit enregistrées au cours du scrutin (cf 1.3.5).

- Sujets : President, Assessor
- Objets : Results files, Audit tracks files

4.2 Définition des composants étendus

Aucun composant étendu n'a été défini.

4.3 Exigences de sécurité fonctionnelles pour la TOE

Les opérations de sélection et d'affectation sont soulignées.
La notation « X.attribut » correspond à l'attribut de sécurité associé au sujet ou à l'objet X.

La TOE doit identifier et authentifier le président du bureau de vote et les assesseurs avant les opérations d'ouverture et de clôture du scrutin et pour le dépouillement.

FIA_UAU.1/President : User authentication by TSF

FIA_UAU.1.1: The TSF shall authenticate a user before the user can bind to President.

FIA_UID.2/President : User identification

FIA_UID.2.1: The TSF shall identify a user before the user can bind to President.

FIA_USB.1/President : User-subject binding

FIA_USB.1.1: Upon binding a user to President the TSF shall change the values of security attributes of that subject as follows: the security attribute "authenticated" of President shall be set to "True"

FIA_UAU.1/Assessor : User authentication by TSF

FIA_UAU.1.1: The TSF shall authenticate a user before the user can bind to Assessor.

FIA_UID.2/Assessor : User identification
FIA_UID.2.1: The TSF shall identify a user before the user can bind to Assessor.

FIA_USB.1/Assessor : User-subject binding
FIA_USB.1.1: Upon binding a user to Assessor the TSF shall change the values of security attributes of that subject as follows: the security attribute “authenticated” of Assessor shall be set to “True”

La machine doit identifier et authentifier la présentation du « droit de vote ».

FIA_UAU.1/Elector : User authentication by TSF
FIA_UAU.1.1: The TSF shall authenticate a user before the user can bind to Elector.

FIA_UID.2/Elector : User identification
FIA_UID.2.1: The TSF shall identify a user before the user can bind to Elector.

FIA_USB.1/Elector : User-subject binding
FIA_USB.1.1: Upon binding a user to Elector the TSF shall change the values of security attributes of that subject as follows: the security attribute “authenticated” of Elector shall be set to “True”

La machine à voter doit mémoriser, visualiser, et restituer à la demande :
- les actions d'un utilisateur ayant entraîné une modification de l'état de la machine (ouverture du(des) scrutin(s), activation de la machine, vote, clôture du scrutin) ;
- les messages découlant d'une erreur de maniement d'un utilisateur, ou d'une anomalie de fonctionnement.

FAU_GEN.2/audit : Audit data generation with time
FAU_GEN.2.1: The TSF shall store an audit record in Audit tracks files of the following events: Scrutiny opening, Machine activation, Vote, Scrutiny closing.

FAU_GEN.2.2: The TSF shall record within each audit record the following information:

a) Date and time of the event, type of event, values of Scrutiny.status and Vote access.status, the success and the failure of the event; and

b) nothing else.

FAU_GEN.1/Participation: Audit data generation without time

FAU_GEN.1.1: The TSF shall store an audit record in Participation files of the following events: Vote.

FAU_GEN.1.2: The TSF shall record within each audit record the following information:

a) Type of event, values of nothing of the subject(s) associated with the event, the success of the event; and

b) nothing else.

Note d’application: il s’agit de l’incrémentation de la participation si l’électeur a fait son choix.

FDP_ACC.1/participation: Access control

FDP_ACC.1.1: The TSF shall [selection: allow, disallow] an operation of a subject on an object [selection: if, if and only if] [assignment: rules for operations, based on security attributes of the subjects and objects].

Raffinement: The TSF shall allow the operation "participation display" on the object "participation files" at any time to anybody.

La machine doit disposer d'une horloge interne lui permettant de dater les évènements enregistrés.

FMI_TIM.1 : Time stamps

FMI_TIM.1.1: The TSF shall maintain the current time in Clock to an accuracy of seconds.

La TOE doit limiter l'accès aux fonctions d'ouverture du(des) scrutin(s) aux seuls président et assesseurs authentifiés.

FDP_ACC.2/Opening: Access control with automatic modification of security attributes

FDP_ACC.2.1: The TSF shall [selection: allow, disallow] an operation of a subject on an object [selection: if, if and only if] [assignment: rules for operations, based on security attributes of the subjects and objects].

Raffinement: The TSF shall allow the operation "Scrutiny opening" on the object scrutiny if and only if (president.authenticated=True AND assessor.authenticated = True).

FDP_ACC.2.2: The TSF shall change the security attributes of subjects and/or objects involved in operations as follows: Scrutiny.status must be set to "open" if the scrutiny opening is allowed

FDP_ISA.1/scrutiny : Security attribute initialisation

FDP_ISA.1.1 : The TSF shall assign the value "Close" to the security attribute status whenever a scrutiny is created.

La TOE doit limiter l'activation de la machine à la présentation d'un « droit à voter » authentifié.

FDP_ACC.2/Activation: Access control with automatic modification of security attributes

FDP_ACC.2.1: The TSF shall [selection: allow, disallow] an operation of a subject on an object [selection: if, if and only if] [assignment: rules for operations, based on security attributes of the subjects and objects].

Raffinement: The TSF shall allow the operation "Machine activation" if and only if (elector.authenticated=True).

FDP_ACC.2.2: The TSF shall change the security attributes of subjects and/or objects involved in operations as follows: Vote access.status must be set to "open" if the vote is allowed

FDP_ISA.1/vote access : Security attribute initialisation

FDP_ISA.1.1 : The TSF shall assign the value "Close" to the security attribute status whenever a Vote access object is created.

La TOE doit empêcher la vue du choix d'un électeur par l'électeur suivant.

FIA_LOB.2: User-initiated locking out

FIA_LOB.2.1 The TSF shall allow a user to lock-out a binding of that user to elector by clearing or overwriting display and/or communication devices and setting the attribute Vote access.status to "Close".

FIA_LOB.2.2 The TSF shall unlock the binding after a new activation.

La TOE doit limiter l'accès aux fonctions de clôture du(des) scrutin(s) aux seuls président et assesseurs authentifiés.

FDP_ACC.2/Closing: Access control with automatic modification of security attributes

FDP_ACC.2.1: The TSF shall [selection: allow, disallow] an operation of a subject on an object [selection: if, if and only if] [assignment: rules for operations, based on security attributes of the subjects and objects].

Raffinement: The TSF shall allow the operation "Scrutiny closing" on the object scrutiny if and only if (president.authenticated=True AND assessor.authenticated = True).

FDP_ACC.2.2: The TSF shall change the security attributes of subjects and/or objects involved in operations as follows: Scrutiny.status must be set to "close" if the scrutiny closing is allowed

La TOE doit restreindre l'affichage des résultats aux seuls président et assesseurs authentifiés et uniquement lorsque le scrutin est clos.

FDP_ACC.1/display: Access control

FDP_ACC.1.1: The TSF shall [selection: allow, disallow] an operation of a subject on an object [selection: if, if and only if] [assignment: rules for operations, based on security attributes of the subjects and objects].

Raffinement: The TSF shall allow the operation "Results display" on the objects Results files and Audit tracks files if and only if (president.authenticated=True AND assessor.authenticated = True AND scrutiny.status=close).

Un mécanisme d'autotest doit être implémenté pour détecter automatiquement une panne ou un dysfonctionnement d'un des éléments de la machine.

FPT_TST.1 : TSF self-testing

FPT_TST.1.1: The TSF shall run a suite of tests immediately after installation, during each start-up, periodically during normal operation, at the request of a subject to demonstrate the correct operation of the TSF.

La TOE doit enregistrer les votes dans un ordre aléatoire afin qu'il ne soit pas possible de reconstituer la chronologie des votes.

FDP_UNL.3 : Unlinkability of objects

FDP_UNL.3.1: The TSF shall ensure that anybody is unable to determine whether Results files are related as follows: list of votes with list of electors.

Application note: Il s'agit d'éviter de pouvoir associer une opération de vote avec un résultat ; par exemple en enregistrant les votes dans un ordre aléatoire.

4.4 Exigences de sécurité d'assurance pour la TOE

4.4.1 Pour une qualification au niveau standard

Le paquet d'assurance prévu pour une qualification au niveau standard est le suivant.

Classe d'assurance	Classe d'assurance	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**

* L'échantillon de l'implémentation doit contenir tous les mécanismes de nature cryptographique de la TOE.

** La description de la conception de la TOE en termes de modules doit être limitées aux mécanismes de nature cryptographique de la TOE.

5 Argumentaire

5.1 Objectifs de sécurité / Problème de sécurité

5.1.1 Couverture des objectifs de sécurité

	H.CONTROLE_VISUEL	H.OPERATIONS_MAINTENANCE	H.CONNEXIONS_RESEAUX_INEXISTANTES	H.ISOLOIR	H.MEMOIRE_SUFFISANTE	Clôture du scrutin par un électeur	P.EAL	P.04-OUVERTURE	P.07-OUVERTURE	P.08-ACTIVATION	P.17-CLOTURE	P.18-DEPOUILLEMENT	P.20-DEPOUILLEMENT	P.21-DEPOUILLEMENT	P.44-CONCEPTION	P.45-CONCEPTION	P.46-CONCEPTION	P.47-CONCEPTION	P.48-CONCEPTION	P.49-EMPLOI	P.53-EMPLOI	P.65-CONFIDENTIALITE_VOTE	P.66-CONFIDENTIALITE_VOTE	P.68-INTEGRITE_DONNEES	P.69-INTEGRITE_DONNEES	P.70-INTEGRITE_DONNEES	P.72-DISPONIBILITE	P.79-ALIMENTATION_DE_SECOURS
OT.AUTHENTIFICATION_PRESIDENT						X			X		X	X		X														
OT.AUTHENTIFICATION_DROIT_VOTE										X																		
OT.TRACES_AUDIT																	X		X					X				
OT.HORLOGE																	X											
OT.ACCES_OUVERTURE									X																			
OT.ACCES_ACTIVATION										X																		
OT.DESACTIVATION																				X								
OT.ACCES_CLOTURE						X																						
OT.ACCES_AFFICHAGE_RESULTATS											X	X		X								X						
OT.AUTOTEST								X													X						X	
OT.ENREGISTREMENT_ALEATOIRE																							X					
OD.EAL							X																					
OE.CONTROLE_VISUEL	X																											
OT.AUTHENTIFICATION_COMMUNE											X			X														
OT.ACCES_PARAMETRAG											X			X														

	H.CONTROLE_VISUEL	H.OPERATIONS_MAINTENANCE	H.CONNEXIONS_RESEAUX_INEXISTANTES	H.ISOLOIR	H.MEMOIRE_SUFFISANTE	Clôture du scrutin par un électeur	P.EAL	P.04-OUVERTURE	P.07-OUVERTURE	P.08-ACTIVATION	P.17-CLOTURE	P.18-DEPOUILLEMENT	P.20-DEPOUILLEMENT	P.21-DEPOUILLEMENT	P.44-CONCEPTION	P.45-CONCEPTION	P.46-CONCEPTION	P.47-CONCEPTION	P.48-CONCEPTION	P.49-EMPLOI	P.53-EMPLOI	P.65-CONFIDENTIALITE_VOTE	P.66-CONFIDENTIALITE_VOTE	P.68-INTEGRITE_DONNEES	P.69-INTEGRITE_DONNEES	P.70-INTEGRITE_DONNEES	P.72-DISPONIBILITE	P.79-ALIMENTATION_DE_SECOURS
E																												
OE.OPERATIONS_MAINTENANCE		X														X		X										
OE.RESULTATS_PARTIELS																									X			
OE.BATTERIE																												X
OE.MACHINE_DEDIEE															X													
OE.CONNEXIONS_RESEAU_INEXISTANTES			X																									
OE.ISOLOIR				X																X								
OE.MEMOIRE_SUFFISANTE					X																							
OE.CONTROLE_INTEGRITE_MATERIEL								X																				
OE.CONTROLE_INTEGRITE_LOGICIEL								X																				
OE.CONTROLE_INTEGRITE_DONNEES_SCRUTIN								X																				
OE.SCELLES																X										X		
OE.DELAIS_RECOURS											X		X															

5.1.2 Couverture des menaces par les objectifs de sécurité

Il est possible de réduire le risque en mettant en place des mesures de protection (réduire). Si cette mesure de protection n'est pas assez efficace ou inexistante, il faut pouvoir détecter l'occurrence de l'évènement redouté (détecter) et réagir le cas échéant (réagir) ; à défaut de détection, il faut pouvoir limiter impact de l'occurrence de l'évènement.

Menaces	Argumentaires
Clôture du scrutin par un électeur	Protection: la capacité de clôture du scrutin doit limitée au président en présence d'un des assesseurs (OT.ACCES_CLOTURE). La présence d'un double mécanisme d'authentification (OT.AUTHENTIFICATION_PRESIDENT) permet cela. Limitation de l'impact: - Détection: Evident (le scrutin est clos) Réaction: -

5.1.3 Couverture des hypothèses par les objectifs de sécurité

Hypothèses	Argumentaires
H.CONTROLE_VISUEL	L'hypothèse est directement traduite en objectif sur l'environnement OE.CONTROLE_VISUEL.
H.OPERATIONS_MAINTENANCE	L'hypothèse est directement traduite en objectif sur l'environnement OE.OPERATIONS_MAINTENANCE.
H.CONNEXIONS_RESEAUX_INEXISTANTES	L'hypothèse est directement traduite en objectif sur l'environnement OE.CONNEXIONS_RESEAU_INEXISTANTES.
H.ISOLOIR	L'hypothèse est directement traduite en objectif sur l'environnement OE.ISOLOIR.
H.MEMOIRE_SUFFISANTE	L'hypothèse est directement traduite en objectif sur l'environnement OE.MEMOIRE_SUFFISANTE.

5.1.4 Couverture des OSP par les objectifs de sécurité

OSP	Argumentaires
P.EAL	Les évaluations à réaliser doivent être du niveau EAL2+ pour obtenir une qualification standard par la DCSSI (OD.EAL).
P.04-OUVERTURE	La vérification qu'il s'agit bien de la machine agréée se fait par le contrôle du matériel (OE.CONTROLE_INTEGRITE_MATERIEL) et du logiciel (OE.CONTROLE_INTEGRITE_LOGICIEL). A l'ouverture, il faut également bien s'assurer que les données relatives au scrutin ont bien été insérées dans la machine (OE.CONTROLE_INTEGRITE_DONNEES_SCRUTIN). Enfin, le

	fonctionnement correct des éléments de la machine est vérifié par un mécanisme d'autotest (OT.AUTOTEST).
P.07-OUVERTURE	L'ouverture n'est possible (OT.ACCES_OUVERTURE) qu'après l'authentification du président et d'un des assesseurs. (OT.AUTHENTIFICATION_PRESIDENT)
P.08-ACTIVATION	L'activation de la machine n'est possible (OT.ACCES_ACTIVATION) qu'après authentification du « droit à voter » (OT.AUTHENTICATION_DROIT_VOTE).
P.17-CLOTURE	Après le blocage de la machine, les résultats ne doivent pas être accessibles sauf : - pour un affichage des résultats (OT.ACCES_AFFICHAGE_RESULTATS) après la double authentification du président et d'un des assesseurs (OT.AUTHENTIFICATION_PRESIDENT) - ou pour le paramétrage d'un nouveau scrutin (OE.ACCES_PARAMETRAGE) par un agent de la commune (OE.AUTHENTIFICATION_COMMUNE) mais après l'expiration des délais de recours (OE.DELAIS_RECOURS).
P.18-DEPOUILLEMENT	L'objectif OT.ACCES_AFFICHAGE_RESULTATS permet de limiter la possibilité d'affichage aux seules personnes autorisées. Le dispositif d'authentification (OT.AUTHENTIFICATION_PRESIDENT) permet de garantir que seuls le président avec un assesseur ont la possibilité de dépouiller.
P.20-DEPOUILLEMENT	Les seules opérations permettant d'altérer les résultats sont la maintenance de la machine et le paramétrage d'un nouveau scrutin. Ces opérations doivent être interdites tant que les délais de recours ne sont pas épuisés. (OE.DELAIS_RECOURS)
P.21-DEPOUILLEMENT	Après le blocage de la machine, les résultats ne doivent pas être accessibles sauf : - pour un affichage des résultats (OT.ACCES_AFFICHAGE_RESULTATS) après la double authentification du président et d'un des assesseurs (OT.AUTHENTIFICATION_PRESIDENT) - ou pour le paramétrage d'un nouveau scrutin (OE.ACCES_PARAMETRAGE) par un agent de la commune (OE.AUTHENTIFICATION_COMMUNE).
P.44-CONCEPTION	La machine à voter doit être une machine dédiée (OE.MACHINE_DEDIEE).
P.45-CONCEPTION	Au cours du scrutin, la maintenance de la machine doit être interdite (OE.OPERATIONS_MAINTENANCE) et un scellé doit être posé (OE.SCELLES) afin d'empêcher et de détecter toute tentative d'altération de la TOE.
P.46-CONCEPTION	La machine doit comporter une horloge (OT.HORLOGE) afin d'assurer l'horodatage des traces d'audit (OT.TRACES_AUDIT).
P.47-CONCEPTION	La lecture des résultats ne doit être possible que lorsque le scrutin est clos (OT.ACCES_AFFICHAGE_RESULTATS). De plus, il faut interdire toute maintenance de la machine lors du scrutin (OE.OPERATIONS_MAINTENANCE).
P.48-CONCEPTION	La machine doit enregistrer les problèmes au cours du fonctionnement (OT.TRACES_AUDIT).
P.49-EMPLOI	Il doit être impossible de voir le choix des électeurs ; pendant le vote par l'utilisation d'un isoloir (OE.ISOLOIR) et par l'effacement de

	l'écran lorsque l'électeur a fait son choix (OT.DESACTIVATION).
P.53-EMPLOI	La machine doit détecter et indiquer tout dysfonctionnement (OT.AUTOTEST).
P.65-CONFIDENTIALITE_VOTE	En cas de panne, le choix de l'électeur ne doit pas être visible sauf après authentification du président et d'un assesseur (OT.ACCES_AFFICHAGE_RESULTATS).
P.66-CONFIDENTIALITE_VOTE	L'OSP est directement traduite en objectif sur la TOE (OT.ENREGISTREMENT_ALEATOIRE).
P.68-INTEGRITE_DONNEES	L'acte de vote faisant partie des informations enregistrées par le biais de l'enregistrement de la participation, OT.TRACES_AUDIT permet de s'assurer que l'électeur a enregistré ou non son vote avant l'incident.
P.69-INTEGRITE_DONNEES	Les informations mémorisées jusqu'à l'interruption sont effectivement disponible grâce par exemple à l'utilisation de mémoires extractibles dont le contenu peut être relu sur une autre machine. (OE.RESULTATS_PARTIELS)
P.70-INTEGRITE_DONNEES	La machine peut être difficilement protégée contre des intrusions. En revanche, les intrusions peuvent être détectées grâce à des scellés (OE.SCELLES).
P.72-DISPONIBILITE	La machine doit disposer d'une fonction d'autotest (OT.AUTOTEST).
P.79-ALIMENTATION_DE_SECOURS	En cas de coupure électrique, la machine doit pouvoir fonctionner sur batterie (OE.BATTERIE).

5.2 Exigences de sécurité / Objectifs de sécurité

5.2.1 Couverture des exigences de sécurité

	OT.AUTHENTIFICATION_PRESIDENT	OT.AUTHENTIFICATION_DROIT_VOTE	OT.TRACES_AUDIT	OT.HORLOGE	OT.ACCES_OUVERTURE	OT.ACCES_ACTIVATION	OT.DESACTIVATION	OT.ACCES_CLOTURE	OT.ACCES_AFFICHAGE_RESULTATS	OT.AUTOTEST	OT.ENREGISTREMENT_ALEATOIRE
FIA_UAU.1/president	X										
FIA_UID.2/president	X										
FIA_USB.1/president	X										
FIA_UAU.1/assessor	X										
FIA_UID.2/assessor	X										
FIA_USB.1/assessor	X										
FIA_UAU.1/elector		X									
FIA_UID.2/elector		X									
FIA_USB.1/elector		X									
FAU_GEN.2/audit			X								
FAU_GEN.1/participation			X								
FAU_ACC.1/participation			X						X		
FMI_TIM.1			X	X							

	OT.AUTHENTIFICATION_PRESIDENT	OT.AUTHENTIFICATION_DROIT_VOTE	OT.TRACES_AUDIT	OT.HORLOGE	OT.ACCES_OUVERTURE	OT.ACCES_ACTIVATION	OT.DESACTIVATION	OT.ACCES_CLOTURE	OT.ACCES_AFFICHAGE_RESULTATS	OT.AUTOTEST	OT.ENREGISTREMENT_ALEATOIRE
FDP_ACC.2/Opening					X						
FDP_ISA.1/scrutiny					X						
FDP_ACC.2/Activation						X					
FDP_ISA.1/vote access						X					
FIA_LOB.2							X				
FDP_ACC.2/Closing								X			
FDP_ACC.1/display			X						X		
FPT_TST.1										X	
FDP_UNL.3											X

5.2.2 Couverture des objectifs de sécurité pour la TOE par les exigences de sécurité

Objectifs sur la TOE	Argumentaires
OT.AUTHENTIFICATION_PRESIDENT	Le composant FIA_UAU.1/president a été sélectionné pour l'authentification du président et le composant FIA_UID.2/president pour son identification. Le composant FIA_UAU.1/assessor a été sélectionné pour l'authentification d'un des assesseurs et le composant FIA_UID.2/assessor pour son identification. Les dépendances de ces composants ont aussi été sélectionnées : - FIA_USB.1/president et FIA_USB.1/assessor pour associer la personne qui se connecte au profil adéquat et passer leur attribut de sécurité à « authenticated ».
OT.AUTHENTIFICATION_DROIT_VOTE	Le composant FIA_UAU.1/Elector a été sélectionné pour l'authentification des « droits à voter » et le composant FIA_UID.2/Elector pour leur identification. Les dépendances de ces composants ont aussi été sélectionnées : - FIA_USB.1/Elector pour associer la personne qui se connecte au profil adéquat et passer leur attribut de sécurité à « authenticated ».
OT.TRACES_AUDIT	Le composant FAU_GEN.2/audit a été

	sélectionné pour l'enregistrement de traces d'audit horodatées en cas de problèmes. Le composant FAU_GEN.1/participation a été sélectionné pour l'incrémentation du fichier de participation lorsque l'électeur a fait un choix. Les dépendances de ces composants ont aussi été sélectionnées : - FMI_TIM.1 pour la disponibilité d'une horloge permettant d'horodater les évènements. - FDP_ACC.1/display pour ne permettre l'affichage des traces d'audit que lorsque le président et un assesseur se sont authentifiés car l'impression des traces est faite au moment de l'impression des résultats. - FDP_ACC.1/participation pour définir l'accès au fichier de participation
OT.HORLOGE	Le composant FMI_TIM.1 a été sélectionné pour la disponibilité d'une horloge.
OT.ACCES_OUVERTURE	Le composant FDP_ACC.2/Opening a été sélectionné pour limiter la possibilité d'ouverture du scrutin aux seuls président et assesseurs authentifiés simultanément. Les dépendances de ces composants ont aussi été sélectionnées : - FDP_ISA.1/scrutiny pour l'initialisation du statut à « close » lors de la création d'un scrutin.
OT.ACCES_ACTIVATION	Le composant FDP_ACC.2/Activation a été sélectionné pour limiter la possibilité d'activation à la présentation du « droit à voter ». Les dépendances de ces composants ont aussi été sélectionnées : - FDP_ISA.1/vote pour l'initialisation du statut à « close » lors de la création de l'objet « vote access ».
OT.DESACTIVATION	Le composant FIA_LOB.2 a été sélectionné pour assurer que l'écran de la machine est effacé lorsque l'électeur a fait son choix et pour éviter que l'électeur suivant ne puisse voir son choix.
OT.ACCES_CLOTURE	Le composant FDP_ACC.2/Closing a été sélectionné pour limiter la possibilité de clôture du scrutin aux seuls président et assesseur authentifiés simultanément.

	-
OT.ACCES_AFFICHAGE_RESULTATS	Le composant FDP_ACC.2/display a été sélectionné pour ne permettre l'affichage des résultats (resultats et traces d'audit) que lorsque le président et un assesseur se sont authentifiés et uniquement en dehors du scrutin. La participation est accessible librement tout au long du scrutin. (FDP_ACC.1/participation)
OT.AUTOTEST	Le composant FPT_TST.1 a été sélectionné pour la vérification automatique du fonctionnement de la machine
OT.ENREGISTREMENT_ALEATOIRE	Le composant FDP_UNL.3 a été sélectionné pour s'assurer qu'il est impossible d'associer un résultat avec un vote en particulier. Même si l'électeur n'est pas personnellement identifié, il serait possible de recouper l'information entre une observation visuelle (« qui a voté à quelle heure » ou « dans quel ordre ont votés les électeurs ») et le résultat enregistré.

5.2.3 Couverture des objectifs de sécurité pour l'environnement de développement par les exigences de sécurité

L'objectif de sécurité pour l'environnement de développement OD.EAL est directement couvert par le niveau d'évaluation EAL2+ sélectionné.

5.3 Dépendances

Exigences fonctionnelles	Dépendances exigées	Satisfaction/Argumentaires
FIA_UAU.1/president	FIA_UID.2	OK : FIA_UID.2 /president
	FIA_URE.2	NOK: Il est considéré que les utilisateurs sont définis une fois pour toute dans la machine à sa conception et qu'il n'est pas nécessaire de créer de nouveaux utilisateurs au cours de la vie de la machine.
FIA_UID.2/president	FIA_USB.1	OK : FIA_USB.1/president
FIA_USB.1/president	-	OK
FIA_UAU.1/assessor	FIA_UID.2	OK : FIA_UID.2 / assessor

	FIA_URE.2	NOK: Il est considéré que les utilisateurs sont définis une fois pour toute dans la machine à sa conception et qu'il n'est pas nécessaire de créer de nouveaux utilisateurs au cours de la vie de la machine.
FIA_UID.2/ assessor	FIA_USB.1	OK : FIA_USB.1/ assessor
FIA_USB.1/assessor	-	OK
FIA_UAU.1/elector	FIA_UID.2	OK : FIA_UID.2 / elector
	FIA_URE.2	NOK: Il est considéré que les utilisateurs sont définis une fois pour toute dans la machine à sa conception et qu'il n'est pas nécessaire de créer de nouveaux utilisateurs au cours de la vie de la machine.
FIA_UID.2/ elector	FIA_USB.1	OK : FIA_USB.1/ elector
FIA_USB.1/elector	-	OK
FAU_GEN.2/audit	FMI_TIM.1	OK : FMI_TIM.1
	FDP_ACC.1	OK : La consultation des fichiers d'audit est réalisée via l'impression du ticket contenant les résultats. L'accès au fichier d'audit est donc lié à la fonction d'affichage des résultats. (FDP_ACC.1/display)
	FPT_RSA.1	NOK : il est considéré que les ressources mémoire sont largement suffisantes pour traiter toutes les données générées au cours du scrutin. (cf H.MEMOIRE_SUFFISANTE)
FAU_GEN.1/participation	FDP_ACC.1	OK : FDP_ACC.1/participation
	FPT_RSA.1	NOK : il est considéré que les ressources mémoire sont largement suffisantes pour traiter toutes les données générées au cours du scrutin. (cf H.MEMOIRE_SUFFISANTE)
FDP_ACC.1/participation	FDP_ISA.1	NOK : l'objet « participation files » n'a pas d'attribut de sécurité et n'a donc pas besoin d'être initialisé.
FMI_TIM.1	FDP_ACC.1	NOK : La mise à jour de l'horloge se fait lors du paramétrage du(des) scrutin(s) qui est hors-TOE.
FDP_ACC.2/Opening	FDP_ISA.1	OK : FDP_ISA.1/scrutiny
FDP_ACC.2/Activation	FDP_ISA.1	OK : FDP_ISA.1/vote access
FIA_LOB.2	FIA_USB.1	OK : FIA_USB1/elector
FDP_ACC.2/Closing	FDP_ISA.1	NOK : Il n'y a pas de création d'objet à la clôture du scrutin.

FDP_ACC.1/display	FDP_ISA.1	NOK : les objets « results files », « participation files » et « audit tracks files » n'ont pas d'attributs de sécurité et n'ont donc pas besoin d'être initialisés
FDP_ISA.1/scrutiny	-	OK
FDP_ISA.1/vote access	-	OK
FPT_TST.1	-	OK
FDP_UNL.3	-	OK

5.4 Conformité à un PP

Ce profil de protection ne se veut pas conforme à un autre profil de protection.

5.5 Composants étendus

Aucun composant étendu n'est utilisé.

Annexe A Compléments de description de la TOE et de son environnement

A.1 Eléments relatifs à la conception

A.1.1 Relations Entités / Eléments

	Personnes				Matériels			Logiciels
	Président du bureau de vote	Assesseurs	Electeurs	Agents de la commune	Borne	Dispositifs président/assesseurs	Dispositif d'activation	Logiciel de la machine
Fonctions								
Paramétrage du(des) scrutin(s)				X	X			X
Ouverture du(des) scrutin(s)	X	X			X	X		X
Activation du(des) scrutin(s)	(X)		(X)		X		X	X
Vote			X		X			X
Blocage de la machine	X	X			X	X		X
Impression des résultats	X	X			X	X		X
Informations								
Données du(des) scrutin(s)				X	X			X
Authentifiants président/assesseurs	X	X			X	X		X
PV d'initialisation	X	X			X			X
Etat de la machine					X			X
Droit de vote	X		X		X		X	X
Choix de l'électeur			X		X			X
Résultats pour un scrutin	X	X			X			X
Participation pour un scrutin	X	X	X		X			X
Traces d'audit					X			X

(X) selon la méthode d'activation

A.2 Eléments de justification du problème de sécurité

Une analyse de risque a été réalisée pour la machine à voter. Les résultats de cette analyse sont disponibles dans le document [FEROS].

A.2.1 Biens

A.2.1.1 Echelle de besoins

	Disponibilité	Intégrité	Confidentialité
Niveaux			
0	Indisponibilité même le jour du scrutin acceptable	Altération acceptable (il est simple de retrouver l'information par une autre source)	Information publique
1	Indisponibilité toute la journée du scrutin	Intégrité préférable (il est possible de	-

	inacceptable	retrouver l'information par une autre source mais l'opération est complexe et/ou fastidieuse)	
2	Indisponibilité supérieure à 1 heure le jour du scrutin inacceptable	-	Information qui doit rester secrète jusqu'à la proclamation des résultats
3	Indisponibilité supérieure à 5 minutes le jour du scrutin inacceptable	Altération inacceptable (il est impossible de retrouver les données par une autre source)	Information qui doit rester tout le temps secrète

A.2.1.2 Recueil des besoins de sécurité

	Disp.	Int.	Conf.	Impacts
Fonctions				
Paramétrage du(des) scrutin(s)	2	0	0	L'indisponibilité de la fonction de paramétrage porterait atteinte au bon déroulement du scrutin (incapacité à utiliser la machine le jour du scrutin).
Ouverture du(des) scrutin(s)	2	1	0	L'indisponibilité de la fonction pour plus d'une heure porterait atteinte au bon déroulement du scrutin. L'altération de la fonction porterait également atteinte au bon déroulement du scrutin puisque la machine se déclarerait opérationnelle alors qu'elle ne le serait pas.
Activation de la machine pour un(des) scrutin(s)	3	3	0	L'indisponibilité de la fonction pour plus d'une minute porterait atteinte au bon déroulement du scrutin puisque l'électeur ne pourrait pas voter jusqu'à l'activation de la machine. L'altération de la fonction porterait également atteinte au bon déroulement du scrutin puisque l'électeur penserait la machine active alors qu'elle ne le serait pas.
Vote	3	3	0	L'indisponibilité de la fonction pour plus d'une minute porterait atteinte au bon déroulement du scrutin car l'électeur devrait attendre avant de pouvoir voter. L'altération de la fonction porterait atteinte à l'exactitude des résultats.
Blocage de la machine	2	0	0	L'indisponibilité de la fonction pendant plus d'une heure porterait atteinte au bon déroulement du scrutin puisque les résultats ne pourraient pas être imprimés.
Impression des résultats	2	3	0	L'indisponibilité de la fonction pendant plus d'une heure porterait atteinte au bon déroulement du scrutin puisqu'il faudrait attendre l'impression pour pouvoir proclamer

	Disp.	Int.	Conf.	Impacts
				les résultats. L'altération de la fonction porterait atteinte à l'exactitude des résultats.
Informations				
Données relatives au(x) scrutin(s)	2	1	0	L'indisponibilité des données pour l'ouverture du scrutin porterait atteinte au bon déroulement du scrutin. L'altération des données (par exemple une modification des données relatives aux candidatures) porterait atteinte à l'exactitude des résultats.
Authentifiants du président et des assesseurs	2	3	3	L'indisponibilité des clés pendant plus d'une heure porterait notamment atteinte au bon déroulement du scrutin (notamment pour le dépouillement). La perte totale des clés porterait atteinte à l'exactitude des résultats puisque les votes exprimés sur la machine ne pourraient pas être décomptés. La divulgation des clés porterait atteinte au bon déroulement du scrutin puisque qu'une personne malintentionnée pourrait se faire passer pour le président ou un de ses assesseurs.
PV d'initialisation	2	3	0	L'indisponibilité du PV d'initialisation pendant plus d'une heure porterait atteinte au bon déroulement du scrutin car le scrutin ne pourrait pas être ouvert. L'altération du PV porterait atteinte à l'exactitude des résultats car la machine pourrait être en état de dysfonctionnement lors du scrutin.
Etat de la machine	2	1	0	L'indisponibilité de l'information de l'état du scrutin pendant plus d'une heure porterait atteinte au bon déroulement du scrutin. L'altération de l'état porterait également atteinte au bon déroulement du scrutin .
Droit de vote	2	1	2	L'indisponibilité de l'autorisation pendant plus d'une heure porterait atteinte au bon déroulement du scrutin. L'altération porterait également atteinte au bon déroulement car il faudrait régénérer une autorisation qui ne fonctionne pas. La divulgation de l'autorisation porterait atteinte à l'exactitude des résultats car un électeur pourrait activer la machine pour voter plusieurs fois et même lors de scrutins ultérieurs si les données ne sont pas changées à l'issue du

	Disp.	Int.	Conf.	Impacts
				scrutin.
Choix de l'électeur	3	3	3	L'indisponibilité du choix de l'électeur porterait atteinte à l'exactitude des résultats. Son altération porterait également atteinte à l'exactitude des résultats. La divulgation porterait atteinte au secret du vote.
Résultats pour un scrutin	3	3	2	L'indisponibilité des résultats pour la machine porterait atteinte à l'exactitude des résultats. Son altération porterait également atteinte à l'exactitude des résultats. La divulgation porterait atteinte au secret du vote (il suffirait de faire la différence entre les résultats avant le vote d'un électeur et les résultats après pour déterminer le choix).
Participation pour un scrutin	1	1	0	L'indisponibilité ou l'altération de la participation porterait atteinte au bon déroulement du scrutin (il faudrait déterminer la participation à partir des registres des électeurs).
Traces d'audit	3	3	0	L'indisponibilité ou l'altération des traces d'audit porterait atteinte à la capacité de contrôle.

A.2.2 Prise en compte des menaces

Les menaces « Bogue informatique », « Piégeage de la machine lors de sa conception, de sa fabrication ou de sa livraison », « programme pernicieux » ne sont pas reprises de l'analyse de risque car déjà prises en compte par l'OSP P.QUALIFICATION-STANDARD.

Les menaces « Altération par le personnel de maintenance », « Destruction ou perte du dispositif d'authentification du président », « Dysfonctionnement du dispositif d'activation », « Dysfonctionnement du dispositif d'authentification du président », « Erreur lors d'une opération de maintenance », « Piégeage de la machine par un électeur lors de son utilisation », « Reniement d'activité de maintenance », « Usurpation des droits du personnel de maintenance », « Vandalisme », « Vol du dispositif d'activation des machines à voter », « Vol du dispositif d'authentification du président » identifiées lors de l'analyse de risque n'étant couvertes que par des mesures sur l'environnement de la TOE, ces dernières n'ont pas été reprises dans le PP. De ce fait, les objectifs sur l'environnement « OE.CHANGEMENT_CLES », « OE.OPERATIONS_MAINTENANCE », « OE.CONTROLE_VISUEL », « OE.CONTROLE_VOTE », « OE.RETOUR_DISPOSITIFS_ACTIVATION » présents dans l'analyse de risque n'apparaissent pas non plus dans le PP.

A.3 Eléments pour la rédaction de la ST

La cible de sécurité qui se voudra conforme au présent profil de protection devra présenter la plate-forme d'évaluation retenue.

Annexe B Définitions et acronymes

Cible de sécurité (ST) : document servant de référence à l'évaluation de la cible d'évaluation : le certificat délivré par la DCSSI attestera de la conformité du produit et de sa documentation aux exigences formulées dans la cible de sécurité.

Cible d'évaluation (TOE) : le produit à évaluer et sa documentation associée

Annexe C Références

[FEROS] Fiche d'Expression Rationnelle des Objectifs de sécurité pour la machine à voter, version 1.1.

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, June 2005, Version 3.0, Revision 2, CCMB-2005-07-001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, July 2005, Version 3.0, Revision 2, CCMB-2005-07-002.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, July 2005, Version 3.0, Revision 2, CCMB-2005-07-003.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, July 2005, Version 3.0, Revision 2, CCMB-2005-07-004.

[QUA-STD] Définition des paquets d'assurance pour la qualification standard et la qualification renforcée suivant les CC version 3 – Document du 8 février 2006

[CRYPT-STD] Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse *standard* ou *renforcé*. Version 1.0, mai 2003. DCSSI, 001064/SGDN/DCSSI/SDS/AsTeC.