Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF

Section des droits politiques

31.05.2013

Annexe du règlement technique de la Chancellerie fédérale du ... concernant le vote électronique (RS ...)

Entrée en vigueur: 1er janvier 2014

V. 0.9 / Mai 2013

Table des matières

1. Généralités

1.1. Références

[1] Loi fédérale du 17 décembre 1976 sur les droits politiques (LDP; RS 161.1)

[2] Ordonnance du 24 mai 1978 sur les droits politiques (ODP; RS 161.11)

[3] Catalogue de critères de la Chancellerie fédérale en matière de vote électronique pour les imprimeries

[4] Common Criteria: Protection profile for basic set of of security requirements for online voting products, version 1.0

[5] Norme ISO/IEC 27001

[6] Loi fédérale du 19 décembre 2003 sur les services de certification dans le domaine de la signature électronique (SCSE; RS 943.03)

Les documents susmentionnés peuvent être obtenus auprès des organisations suivantes:

Actes législatifs munis d'un numéro RS	Office fédéral des constructions et de la logistique (OFCL) Vente des publications de la Confédération CH-3003 Berne http://www.bundespublikationen.ch
Normes ISO	Secrétariat central de l'Organisation internationale de normalisation (ISO) Rue de Varembé 1 CH-1211 Genève http://www.iso.org
Catalogue de critères pour les imprimeries	Chancellerie fédérale CH-3003 Berne http://www.bk.admin.ch/themen/pore/evoting/07979/index.html?lang=fr
Common Criteria: Protection profile	Bundesamt für Sicherheit in der Informationstechnik Postfach 200362 D-53133 Bonn https://www.bsi.bund.de

1.2. Abréviations

BSI	Office fédéral allemand de la sécurité des techniques de l'information (*Bundesamt für Sicherheit in der Informationstechnik*)
CC	Critères Communs
ChF	Chancellerie fédérale
DNS	Serveur de noms de domaines (*domain name server*)
DOS	Déni de service (*denial of service*)
EAL	Niveau d'évaluation d'assurance (*evaluation assurance level*)
ISO	Organisation internationale de normalisation
LDP	Loi fédérale sur les droits politiques
MITM	Homme du milieu (*man in the middle*)
NIP	Numéro d'identification personnel
ODP	Ordonnance sur les droits politiques
PP	Profil de protection
SAS	Service d'accréditation suisse
SFR	Exigences fonctionnelles de sécurité (*security functional requirements*)
VE	Vote électronique

1.3. Définitions

message d'authentification: l'ensemble des informations qu'une plate-forme utilisateur envoie à l'infrastructure de VE après l'introduction des données d'authentification client pour que ces dernières authentifient l'expéditeur d'un suffrage en tant qu'électeur. Il doit être difficile de générer un message d'authentification sans connaître les données d'authentification client.

plate-forme utilisateur: un appareil multifonctionnel programmable qui est relié à Internet et sert à voter. Il s'agit généralement d'un ordinateur standard, d'un ordiphone ou d'une tablette tactile.

données d'authentification client: l'ensemble des informations mises à la disposition de chaque électeur et dont celui-ci a besoin pour voter (il peut s'agir par exemple d'un NIP dont l'introduction entraîne en fin de compte la signature du suffrage). Sur la base des données d'authentification client, le dispositif technique utilisé génère un message d'authentification (par exemple la signature du suffrage) qui est envoyé à l'infrastructure du VE. A l'aide du message d'authentification et des données d'authentification serveur (par exemple une clé publique permettant de contrôler la

signature), l'infrastructure du VE authentifie l'expéditeur d'un suffrage en tant qu'électeur. Il doit être difficile de découvrir les données d'authentification client.

déni de service: l'impossibilité d'accéder, lors du traitement numérique de données, à un service qui devrait en principe être disponible.

empoisonnement du cache DNS: une attaque au cours de laquelle le lien entre un nom d'hôte et l'adresse IP correspondante est falsifié.

urne électronique: la zone de stockage dans laquelle les suffrages exprimés conformément à la procédure prévue par le système sont déposés sous forme cryptée. Seuls des suffrages exprimés conformément à la procédure prévue par le système sont stockés dans l'urne électronique.

homme du milieu: l'attaquant dans une attaque de type « man-in-the-middle » (MITM). L'attaque MITM est une forme d'attaque qui trouve son application dans les réseaux informatiques. L'attaquant est physiquement ou, de nos jours la plupart du temps, logiquement entre les deux partenaires d'une communication et prend le contrôle complet du trafic de données entre eux ou entre plusieurs périphériques réseau. Il peut afficher des infomations à volonté et même les manipuler.

suffrage enregistré: le suffrage enregistré une fois que l'infrastructure du VE a pris connaissance du vote définitif.

évaluation des risques: le terme générique recouvrant la séquence des activités d'*identification des risques*, d'*analyse des risques* et d'*évaluation des risques* (remarque: la version 0.73 du règlement technique parle de façon erronée d'*analyse des risques*; l'erreur sera corrigée ultérieurement).

données d'authentification serveur: l'ensemble des informations qui permettent d'authentifier l'expéditeur d'un suffrage en sa qualité d'électeur au moyen d'un message d'authentification.

suffrage tel qu'il a été exprimé: un suffrage dont le contenu correspond au suffrage exprimé par l'électeur sur la plate-forme utilisateur et n'a en particulier pas été manipulé depuis ce moment. (Il correspond toujours à la volonté de l'électeur, à moins que celui-ci se soit trompé au moment du vote.)

suffrage exprimé conformément à la procédure prévue par le système: un suffrage

1. exprimé de manière définitive par l'expéditeur;
2. dont les **données d'authentification client** et le message d'authentification qui en résulte correspondent aux données d'identification serveur qui ont été définies et envoyées à l'électeur en amont du scrutin, et
3. qui est le seul suffrage déposé dans l'urne électronique au moyen des données d'authentification client de l'électeur.

suffrage partiel: lors de votations, un projet, un contre-projet ou une question subsidiaire; lors d'élections, le choix d'une liste ou le choix d'un candidat dans une liste.

exploitation du VE: toutes les activités de l'exploitant du système de VE. Aussi appelée « exploitation ».

fonctionnalités du VE: le logiciel serveur et le logiciel client sur la plate-forme utilisateur proposant les fonctionnalités nécessaires pour voter par voie électronique dans le respect de toutes les exigences de sécurité.

infrastructure du VE: le matériel informatique, les logiciels, les éléments de réseau, les locaux, les services et les moyens d'exploitation en tout genre nécessaires à l'exploitation des fonctionnalités du VE côté serveur dans le respect de toutes les exigences de sécurité. Aussi appelée « infrastructure ».

responsable cantonal du VE: le responsable cantonal d'un scrutin par voie électronique. Il définit et édicte des mesures concernant la sécurité de l'information (directives en matière de sécurité de l'information, critères de base pour la gestion des risques en matière de sécurité de l'information, champ d'application et limites de la gestion des risques en matière de sécurité de l'information, organisation de la gestion des risques), rédige le contrat relatif à l'exécution des mécanismes du scrutin (exigences en matière de surveillance et de vérification incluses) et charge un exploitant de système de VE de l'exécution des mécanismes du scrutin. Il peut aussi être impliqué dans l'exploitation du VE. Aussi appelé « responsable cantonal ».

organisation du VE: la structure organisationnelle (attribution des rôles et des responsabilités incluses), les processus organisationnels et les procédures organisationnelles de l'exploitant du système de VE qui sont nécessaires à l'exploitation des fonctionnalités du VE côté serveur dans le respect de toutes les exigences de sécurité. Aussi appelée « organisation ».

personnel du VE: le responsable de l'exploitation du système de VE, le préposé à la sécurité du VE, le responsable du personnel du VE, le responsable des fonctionnalités du VE, le chef technique du VE, les administrateurs du système de VE et du réseau de VE, les techniciens de bâtiment du VE, les tierces parties du VE qui participent à l'exploitation des fonctionnalités du VE côté serveur dans le respect de toutes les exigences de sécurité. Aussi appelé « personnel ».

responsable du personnel du VE: le responsable du personnel du VE auprès de l'exploitant du système de VE. Aussi appelé « responsable du personnel ».

préposé à la sécurité du VE: la personne responsable du respect des exigences en matière de sécurité de l'information auprès de l'exploitant du système de VE. Aussi appelé « préposé à la sécurité ».

système de VE: le terme générique recouvrant les fonctionnalités du VE, l'infrastructure du VE et l'exploitation du VE. Aussi appelé « système ».

administrateurs du système de VE et du réseau de VE: les responsables de la surveillance et de la maintenance quotidiennes des appareils et des installations de l'infrastructure du VE auprès de l'exploitant du système de VE. Aussi appelés « administrateurs du système et du réseau ».

exploitant du système de VE: l'organisation (autorité ou entreprise privée) qui assume, lors d'un scrutin, l'entière responsabilité de l'exécution des mécanismes du vote par voie électronique. Elle met à disposition le personnel, l'organisation et l'infrastructure nécessaires. Certaines tâches en rapport avec l'exploitation peuvent cependant être assumées par le responsable cantonal du VE. Aussi appelé « exploitant du système ».

responsable de l'exploitation du système de VE: le responsable général en charge de la conduite (communication interne et externe incluse), du respect des exigences légales et réglementaires ainsi que des obligations contractuelles, de l'organisation et de la technique auprès de l'exploitant du système de VE. Aussi appelé « responsable de l'exploitation du système ».

probabilité négligeable au sens cryptographique du terme: la probabilité de décrypter, sans connaître la clé, une valeur cryptée avec un algorythme réputé sûr et paramétré en conséquence.

suffrage bien formé: une manière précise de remplir un bulletin de vote. Il est possible de définir à l'avance si et comment les bulletins de vote qui n'ont pas été remplis correctement doivent être pris en compte dans le résultat final. On peut par exemple définir à l'avance que, dans le contexte d'une question posée en votation, seules les réponses prévues « oui », « non » ou « vierge » peuvent avoir une influence sur le résultat du scrutin. Une réponse telle que « je ne veux pas voter » aurait pour conséquence que le suffrage n'est pas bien formé. Il faut définir avant le scrutin si les suffrages qui ne sont pas bien formés peuvent être déposés ou non dans l'urne électronique, s'ils seront ignorés lors du dépouillement ou s'ils seront pris en compte dans le résultat final.

2. Exigences concernant l'aménagement des processus élémentaires

Les sous-chapitres ci-après regroupent des exigences concernant l'aménagement des processus fondamentaux. La colonne de droite contient des informations diverses; elle indique par exemple lors de quel examen une exigence particulière joue un rôle important (I: vérification de l'infrastructure et de l'exploitation du VE; F: vérification des fonctionnalités du VE).

2.1. Procédure de vote

A1.10	Le système de VE doit être convivial. La navigation doit se faire selon des schémas connus.	F
A 1.20	Le système de VE doit être facilement accessible. Lors du développement du système de VE, la Chancellerie fédérale fera à cette fin appel à un conseil reconnu. Celui-ci veillera, lors du développement du système de VE client et du développement du matériel de vote spécifique au VE, à ce que les besoins des électeurs handicapés soient pris en compte de manière appropriée. L'accessibilité du système de VE client doit être contrôlée par un service reconnu par l'expert en application de la norme eCH-0059. Lors de la vérification des fonctionnalités du VE, qui constitue l'une des conditions à l'octroi de l'approbation, le canton présentera une pièce justificative du conseil qui confirmera que ce dernier porte un jugement positif sur l'accessibilité du système de VE et du matériel de vote. Si le conseil émet des réserves, la Chancellerie fédérale décidera après l'avoir entendu si le canton peut utiliser le système de VE.	F
A 1.30	Les votants déclarent avoir pris connaissance des règles du VE et avoir été informés de leurs responsabilités.	F
A 1.32	Avant de voter, les électeurs doivent être expressément rendus attentifs au fait qu'ils participent en toute officialité à un vote populaire en envoyant leur suffrage à l'urne électronique. Toujours avant de voter, l'électeur doit confirmer qu'il a pris acte dudit message.	F
A 1.33	Pour voter par voie électronique, le votant doit prouver à l'autorité compétente qu'il est autorisé à voter. Il le fait au moyen des données d'authentification client.	F
A 1.35	Le votant saisit son suffrage et le dépose dans l'urne électronique au moyen des données d'authentification client.	F
A 1.37	L'apparence du système de VE client n'influence pas le votant dans son choix.	F,I
A 1.40	Le votant peut modifier son suffrage jusqu'au moment de le déposer dans l'urne électronique. Le canal de vote conventionnel reste à sa disposition jusqu'à ce moment.	F
A 1.42	La navigation ne doit pas inciter à voter de manière hâtive ou irréfléchie.	F
A 1.45	Le système de VE ne permet de voter qu'une fois que le votant a explicitement contrôlé et confirmé son suffrage. Ce dernier est affiché une nouvelle fois avant le vote définitif.	F
A 1.47	Le système de VE offre au votant la possibilité d'interrompre à tout moment le processus de vote sans pour autant perdre le droit de voter.	F,I
A 1.50	Le système de VE tient compte du fait que le suffrage exprimé ne peut pas être imprimé avec les données client utilisées. (Les fonctions qui permettent l'impression doivent être désactivées, pour autant que la technologie employée le permette.)	F

A 1.60	Le votant doit pouvoir constater sur l'appareil dont il s'est servi pour voter que son suffrage a bien été transmis. Il se voit confirmer que le suffrage exprimé est bien parvenu à destination.	F,I
A 1.70	Après le vote, le votant ne doit recevoir aucune information sur le suffrage exprimé.	F
A 1.80	Il doit être impossible de voter une seconde fois au moyen des mêmes données d'authentification client.	F,I

2.2. Préparation des données d'authentification client, des clés cryptographiques et d'autres paramètres du système

A 2.10	Le système de VE importe le registre des électeurs.	F,I
A 2.15	Le système de VE importe les questions du scrutin (par exemple les objets soumis au vote ou les listes de candidats) pour tous les niveaux du système fédéraliste et les arrondissements électoraux concernés, et les enregistre.	F,I
A 2.20	Le système de VE prépare, pour chaque électeur, les données d'authentification serveur et les enregistre.	F
A 2.30	Le système de VE prépare au besoin, pour chaque électeur, les données d'authentification client et les enregistre. (Cela n'est nécessaire que dans les cas où aucun moyen d'authentification externe n'est utilisé.)	F
A 2.40	Le système de VE prépare les clés cryptographiques utilisées et les enregistre.	F
A 2.50	L'exploitant du système de VE définit les paramètres techniques pertinents pour la réalisation d'un scrutin.	I

2.3. Informations et soutien

A 3.10	Le responsable cantonal du VE élabore une stratégie d'information sur le vote électronique à l'attention des citoyens.	I
A 3.15	La stratégie garantit que les informations ont été autorisées par les organes compétents.	I
A 3.20	Des conseils, des règles concernant le vote et des informations sur la responsabilité des électeurs sont consultables en ligne pour éviter que l'électeur ne vote de manière hâtive ou irréfléchie.	F,I
A 3.30	L'électeur reçoit des explications compréhensibles sur les mesures de sécurité, ce qui renforce la confiance dans le vote électronique.	F
A 3.40	L'électeur reçoit des explications sur les points auxquels il doit faire attention afin de pouvoir voter en toute sécurité.	F
A 3.45	L'électeur reçoit des explications sur la procédure à suivre pour effacer le suffrage dans toutes les mémoires de l'appareil utilisé pour voter.	F
A 3.50	L'électeur peut demander un soutien technique.	I
A 3.60	Des vérificateurs, par exemple une commission de vérification, doivent être informés et formés de manière à connaître les processus qui sous-tendent l'exactitude du résultat, le respect du secret du vote et l'absence de résultats partiels anticipés (par exemple la génération de clés, l'impression du matériel de vote, le décryptage et le dépouillement). Ils doivent pouvoir comprendre les processus et leur signification.	I

2.4. Préparation à l'impression du matériel de vote

A4.10	Le matériel de vote doit être conçu de manière à ce qu'il soit impossible de voter à deux reprises en passant par un canal de vote conventionnel.	F,I
A4.20	Le système de VE crée le fichier nécessaire à l'impression du matériel de vote, en incluant éventuellement les données d'authentification client.	F
A4.30	Le système de VE transmet à l'imprimerie le fichier nécessaire à l'impression.	F,I

2.5. Ouverture et fermeture du canal de vote électronique

A5.10	L'exploitant du système de VE initialise le système de VE. (L'initialisation englobe tous les réglages auxquels il faut procéder, selon la définition du processus, peu avant l'ouverture du canal de vote électronique et peut comprendre par exemple la mise en service de moniteurs système ou la réinitialisation de compteurs et de l'urne électronique.)	I
A5.20	L'exploitant du système de VE ouvre le canal de vote électronique pour les électeurs.	F,I
A5.30	Il doit être interdit d'ouvrir ou de fermer prématurément l'urne électronique.	I
A5.40	L'exploitant du système de VE ferme le canal de vote électronique.	F,I

2.6. Contrôle de la validité et enregistrement des suffrages définitifs

A6.10	Le système de VE authentifie l'expéditeur du suffrage exprimé en tant que personne autorisée à voter au moyen du message d'authentification reçu et des données d'authentification serveur.	F
A6.20	Le système de VE vérifie si un suffrage a déjà déposé dans l'urne électronique sous le nom du même électeur.	F
A6.30	Quand le suffrage est valable, le système de VE informe l'électeur du succès du vote et enregistre le suffrage dans l'urne électronique. Les suffrages non valables ne sont pas enregistrés dans l'urne électronique. (La bonne forme d'un suffrage est un exemple de critère supplémentaire du succès du vote.)	F

2.7. Dépouillement de l'urne électronique

A 7.10	Après la fermeture du canal de vote électronique et conformément à la législation cantonale, l'exploitant du système de VE lance le décryptage des suffrages contenus dans l'urne électronique.	F,I
A 7.15	L'exploitant du système de VE lance le dépouillement des suffrages décryptés et enregistre les résultats du scrutin pour chaque arrondissement électoral. Il est interdit de chercher à obtenir davantage de détails.	F,I
A 7.30	L'exploitant du système de VE rédige un compte rendu du processus de décryptage des suffrages et du dépouillement.	I
A 7.35	Pendant que l'urne électronique est ouverte, tout accès au système ou à l'un de ses composants doit être le fait d'au moins deux personnes; il doit être consigné et doit pouvoir être contrôlé par des représentants de l'autorité compétente.	F,I
A 7.40	L'exploitant du système de VE transmet les résultats du scrutin à un système tiers en vue de la poursuite du traitement des données, en particulier en vue de leur consolidation avec les suffrages exprimés au moyen des canaux de vote traditionnels.	F,I

A 7.50	Le système de VE remet à un système tiers les informations dont ce dernier a besoin pour constater, au moyen d'une carte de légitimation, si l'électeur concerné a déjà voté par voie électronique. Si des essais de vote électronique sont menés avec un électorat limité (par exemple avec des Suisses de l'étranger uniquement), il ne faut pas remettre à des services extérieurs à l'infrastructure du VE des listes qui permettraient d'identifier les électeurs qui ont voté par voie électronique. En lieu de cela, il faut confirmer, sur demande, si un électeur particulier a voté. Autre possibilité: le système de VE peut produire une liste contenant des codes anonymes qui correspondent aux cartes de légitimation utilisées.	F,I
A 7.60	Le décryptage et le dépouillement des suffrages doivent pouvoir avoir lieu en présence de parties ou d'organes indépendants qui peuvent ainsi attester du bon déroulement de la procédure.	I

2.8. Données confidentielles et données auxquelles il n'est pas permis d'accéder

A 8.10	Le système de VE garantit que ni des collaborateurs ni des personnes externes n'accèdent à des données qui permettent d'établir un lien entre l'identité des votants et leurs suffrages.	F,I
A 8.20	Le système de VE garantit que ni des collaborateurs ni des personnes externes n'accèdent, avant le moment du décryptage des suffrages, à des données qui permettent d'obtenir des résultats partiels anticipés.	F,I
A 8.25	Le système de VE garantit que les résultats du scrutin sont traités confidentiellement entre le moment du décryptage des suffrages et le moment de la publication.	F,I
A 8.30	Le système de VE garantit que les données permettant de constater si des électeurs ont voté par voie électronique sont traitées confidentiellement.	F,I
A 8.40	Le système de VE garantit que les données personnelles issues du registre des électeurs sont traitées confidentiellement.	F,I
A 8.50	Le système de VE garantit que les suffrages sont aussi traités confidentiellement après le dépouillement.	I
A 8.60	Le système de VE garantit que les résultats du scrutin sont traités confidentiellement au cas où une faible part seulement des électeurs d'un arrondissement électoral ont le droit de voter par voie électronique.	F,I
A 8.70	Après échéance du délai de validation, l'exploitant du système de VE détruit toutes les données créées dans le cadre du vote par voie électronique.	I

3. Exigences de sécurité

Les objectifs de sécurité (voir art. 2, al. 1) ne pourront pas être atteints à coup sûr. Il est en tout cas possible d'identifier des risques en matière de sécurité. Il faut, sur la base d'une évaluation méthodique des risques (voir chap. 6, ch. E 7.40), apporter la preuve que les risques sont suffisamment faibles (art. 2, al. 1).

Il est possible d'identifier un risque au moyen de menaces et de failles du système de VE. Il y a risque quand une faille du système de VE est exploitée par une menace et que la réalisation d'un objectif de sécurité s'en trouve potentiellement compromise. Des mesures de sécurité permettent de réduire les risques. Elles doivent satisfaire aux exigences de sécurité dans les domaines de l'infrastructure, des fonctionnalités et de l'exploitation de sorte que les risques identifiés puissent être réduits à un minimum acceptable.

Le sous-chapitre 3.1 comporte une liste de menaces d'ordre général et met celles-ci en rapport avec les objectifs de sécurité. Ces objectifs doivent être pris en compte lors de l'identification des risques. En fonction des failles identifiées du système de VE, ils doivent être concrétisés et complétés dans la mesure du nécessaire.

Les exigences de sécurité des sous-chapitres 3.2 à 3.15 peuvent être résumées comme suit:

- Elles se rapportent d'une part aux menaces. Des mesures de sécurité qui satisfont aux exigences de sécurité selon les meilleures pratiques sont à prévoir pour toutes les failles du système de VE exposées à des menaces, afin que les objectifs de sécurité puissent être atteints.
- Elles se rapportent d'autre part aux exigences relatives à l'aménagement des processus élémentaires (voir chap. 2). Ceci aide à comprendre à quelles failles il faut prêter attention lors de la mise en œuvre d'une exigence de sécurité. D'autres failles du système de VE doivent être identifiées et les exigences de sécurité doivent s'y rapporter de manière analogue.

Le sous-chapitre 3.15 comprend les exigences de sécurité du profil de protection (PP) du Bundesamt für Sicherheit in der Informationstechnik (BSI) [4], c'est-à-dire de l'office fédéral allemand de la sécurité des techniques de l'information. Il est cependant permis de s'en écarter dans certains cas. Les écarts et les références par rapport aux menaces, de même que les exigences relatives à l'aménagement des processus élémentaires, sont présentés au sous-chapitre 3.15.

3.1. Menaces

Men3.10	Un logiciel malveillant modifie le suffrage sur la plate-forme de l'électeur.	Objectif de sécurité (OS): exactitude du résultat
Men3.20	Le suffrage est détourné au moyen d'un empoisonnement du cache DNS.	OS: exactitude du résultat
Men3.30	Un « homme du milieu » (MITM) modifie le suffrage.	OS: exactitude du résultat
Men3.40	Un MITM envoie un bulletin de vote corrompu.	OS: exactitude du résultat
Men3.50	Un administrateur manipule le logiciel qui n'enregistre alors plus les suffrages.	OS: exactitude du résultat
Men3.60	Un administrateur modifie les suffrages.	OS: exactitude du résultat
Men3.70	Un administrateur ajoute des suffrages dans l'urne électronique.	OS: exactitude du résultat
Men3.80	Une organisation criminelle pénètre dans le système et y cause des dommages.	OS: exactitude du résultat (ici en relation avec les menaces Men3.50, Men3.60, Men3.70, Men3.90)
Men3.90	Un administrateur copie des bulletins de vote et les utilise.	OS: exactitude du résultat
Men2.10	Un logiciel malveillant installé sur la	OS: protection du secret du vote et

	plate-forme de l'utilisateur envoie le suffrage de ce dernier à une organisation criminelle.	impossibilité d'obtenir des résultats partiels anticipés
Men2.20	Un logiciel malveillant installé sur la plate-forme de l'utilisateur envoie le suffrage de ce dernier à une organisation criminelle.	OS: exactitude du résultat, protection du secret du vote et impossibilité d'obtenir des résultats partiels anticipés
Men2.30	Le suffrage est détourné au moyen d'un empoisonnement du cache DNS.	OS: exactitude du résultat, protection du secret du vote et impossibilité d'obtenir des résultats partiels anticipés
Men2.40	Un administrateur utilise la clé et décrypte des suffrages non anonymisés.	OS: exactitude du résultat, protection du secret du vote et impossibilité d'obtenir des résultats partiels anticipés
Men2.50	Le secret du vote est violé lors de la vérification de l'exactitude du traitement / dépouillement.	OS: protection du secret du vote et impossibilité d'obtenir des résultats partiels anticipés
Men2.60	Un administrateur consulte prématurément des suffrages non cryptés.	OS: protection du secret du vote et impossibilité d'obtenir des résultats partiels anticipés
Men2.70	Une organisation criminelle pénètre dans le système et y cause des dommages.	OS: protection du secret du vote et impossibilité d'obtenir des résultats partiels anticipés (ici en relation avec les menaces Men2.40, Men2.50, Men2.60).
Men1.10	Un logiciel malveillant installé sur la plate-forme de l'utilisateur empêche ce dernier de voter.	OS: disponibilité des fonctionnalités du VE
Men1.30	Un logiciel malveillant influence des électeurs pendant qu'ils se forment une opinion.	OS: protection des informations destinées aux électeurs
Men1.40	Une organisation criminelle mène une attaque du type « déni de service » (DOS).	OS: disponibilité des fonctionnalités du VE
Men1.50	Un administrateur configure mal le système de VE; le dépouillement ne peut pas se faire.	OS: disponibilité des fonctionnalités du VE
Men1.60	Un administrateur manipule le site Internet d'information / le portail du VE et embrouille les électeurs.	OS: protection des informations destinées aux électeurs
Men1.70	Après le décryptage, un administrateur cherche les bulletins de vote remplis selon des instructions de tiers (n'est possible que pour les élections).	OS: impossibilité d'obtenir des preuves sur le comportement de vote dans l'infrastructure du VE
Men1.80	Une organisation criminelle pénètre dans le système et y cause des dommages.	OS: disponibilité des fonctionnalités du VE, protection des informations destinées aux électeurs, impossibilité d'obtenir des preuves sur le comportement de vote dans l'infrastructure du VE (ici en relation avec les menaces Men1.50, Men1.60, Men1.70)
Men 1.90	Un administrateur vole les données concernant les adresses des électeurs.	OS: protection des informations personnelles concernant les électeurs

3.2. Constatation / découverte et annonce d'incidents et de failles en matière de sécurité; gestion des incidents en matière de sécurité et des améliorations

B 1.10	Un système de monitoring de l'infrastructure du VE doit détecter des incidents et alerter le personnel compétent. Le personnel gère les incidents selon des procédures prédéfinies. Des scénarios de crise et des plans de sauvetage servent de directives (ils comprennent un plan qui garantit que les activités en rapport avec le scrutin peuvent être poursuivies) et sont utilisés au besoin.	F,I - A2.10,15,20,30,40,50 - A3.20,30,40,45 - A5.20,30,40 - A6.10,20,30 - A7.10, A7.35 - A8.10,20,25,30,40,50,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,50,60,70,80,90
B 1.20	Des protocoles des suffrages entrés doivent être établis dans l'infrastructure du VE et au besoin être mis à disposition. Ils servent de preuve de la prise en compte non falsifiée et exclusive de l'intégralité des suffrages valables. En cas de divergence, ils doivent servir à en chercher la cause.	F,I - A1.35,60 - A5.10,20,40 - A6.10,20,30 - A7.10,35 - 8.10,20,25,30,40,50,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.50,70,80
B 1.30	Des protocoles des accès au système, impossibles à manipuler, doivent être établis dans l'infrastructure du VE et au besoin être mis à disposition. Ils servent de preuve de la prise en compte non falsifiée et exclusive de l'intégralité des suffrages valables ainsi que de preuve de la préservation du secret du vote et de l'absence de résultats partiels anticipés. En cas de divergence ou de doute, ils doivent servir à en chercher la cause.	F,I - A1.35, A1.60 - A2.10,15,20,30,40,50 - A5.10,20,40 - A6.10,20,30 - A7.10,15,35,40,50 - A8,10,20,25,30,40,50,60,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,50,60,70,80,90
B 1.40	Les suffrages exprimés et dépouillés par voie électronique doivent, à des fins de plausibilisation du résultat, être comparés avec les protocoles des suffrages entrés dans l'infrastructure du VE.	F,I - A1.35,60 - A5.10,20,40 - A6.10,20,30 - A7.10,15,35 - A8.10,20,25,30,40,50,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.50,70,80
B 1.50	Il faut garantir que les suffrages et les données qui prouvent le bon fonctionnement de la procédure de dépouillement des cartes de légitimation sont, en cas de panne, enregistrés sans altérations dans l'infrastructure du VE.	F,I - A1.35,60 - A2.10,15,20,30,40,50 - A4.20 - A5.10,20,40 - A6.10,20,30 - A7.10,15,30,35,40,50 - A8,10,20,25,30,40,50,60,70 - Men3.80 - Men1.50 - Men1.80
B 1.60	Il doit être possible, au moyen de données d'authentification, d'envoyer des suffrages-test qui ne sont attribués à aucun électeur. Le contenu de ces suffrages-test doit être protocolé dans l'infrastructure du VE. Les suffrages-test dépouillés doivent être comparés avec les protocoles des suffrages-test envoyés. Il faut garantir que les suffrages-test seront traités dans toute la mesure du possible de manière similaire à des suffrages valables; il faut en même temps garantir qu'ils ne seront pas comptés comme des suffrages valables.	F,I - A1.35,60 - A5.10,20,40 - A6.10,20,30 - A7.10,35 - A8.10,20,25,30,40,50,70 - Men3.10,20,30,40,50,60,70,80 - Men2.40,50,60,70 - Men1.10,30,60,80
B 1.70	La disponibilité de l'infrastructure du VE doit être vérifiée et protocolée à intervalles déterminés.	I - Men 1.40,50,80
B 1.80	Des méthodes statistiques doivent pouvoir être utilisées pour la plausibilisation du résultat dans la mesure où la base de données le permet.	I - A1.35,60 - A5.10,20,40 - A6.10,20,30 - A7.10,15,35 - A8.10,20,25,30,40,50,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.50,70,80
B 1.90	Les parties du système de vote accessibles par Internet doivent être régulièrement actualisées moyennant un processus documenté afin d'éliminer les failles identifiées.	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,60,70,80,90

3.3. Attribution, administration et retrait des droits d'accès

B 2.10	Pendant le scrutin, il faut garantir que toute modification envoyée ultérieurement est bloquée.	F,I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20 - A5.10 - A7.35 - Men3.50,60,70,80 - Men1.50,80
B 2.20	L'accès à l'infrastructure et aux fonctionnalités du VE doit être réglé et documenté sur la base d'une évaluation des risques. Le principe dit des « quatre yeux » doit valoir dans les domaines présentant des risques élevés.	I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20 - A5.10 - A7.10,15,35,40,50 - A8.10,20,35,30,40,50,60,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,50, 60,70,80,90
B 2.40	Il doit être impossible, sans disposer d'une autorisation en ce sens, de modifier des informations sur le portail du VE ou sur des sites d'information concernant le vote électronique.	F,I - A3.15,20,30,40,45 - Men1.60,80
B 2.55	Pendant le scrutin, aucune intervention étrangère au vote en cours ne peut être effectuée.	F,I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20,30 - A5.10,20,30,40 - A7.10,15,35,40,50- A8.10,20,35,30,40,50,60,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.50,60,70,80,90
B 2.60	Il faut garantir qu'aucun des éléments des données d'authentification client ne peut être systématiquement intercepté, modifié ou détourné au moment de la remise. L'authentification doit se faire au moyen de mesures et de technologies qui permettent de réduire suffisamment le risque d'abus systématique par des tiers.	F,I - A1.33,35,80 - A2.20,30 - A4.10,20,30 - A6.10,20 - A7.10,15,35,40,50 - A8.10,30,40 - Men3.50,60,70,80,90 - Men2.40,50,60,70

3.4. Utilisation de mesures cryptographiques et gestion des clés

B 3.10	Les certificats électroniques doivent être gérés selon les meilleures pratiques.	I - A1.60 - A2.40 - A2.50 - A 4.30 - A 7.40 - Men3.20,30,40,80 - Men2.30,70 - Men1.50,80
B 3.20	Des mesures cryptographiques adéquates doivent garantir l'intégrité des séquences de données sous-tendant l'exactitude du résultat.	I,F - A1.35 - A2.10,20,30,40,50 - A4.30 - A5.10 - A6.10,20,30 - A7.10,15,40,50 - Men3.50,60,70,80,90 - Men2.50,70
B 3.30	Des mesures cryptographiques adéquates doivent garantir la confidentialité des séquences de données sous-tendant le secret du vote et l'absence de résultats partiels anticipés.	I,F - A1.35 - A2.10,20,30,40,50 - A4.20,30 - A5.10 - A6.10,20,30 - A7.10,15,40,50 - A8.10,20,25,30,50,60,70 - Men2.30,40,50,60,70
B 3.40	Les suffrages ne doivent en aucun cas être enregistrés ou transmis sous une forme non cryptée entre le moment de leur saisie et celui du dépouillement.	I,F - A1.35,60 - A4.20,30 - A6.10,20,30 - A7.10 - A8.10,20 - Men2.30,40,50,60,70
B 3.50	Cryptage et signature sont de rigueur lors de l'échange des données des registres électoraux et des résultats. La signature et l'intégrité doivent être vérifiées au moment de la réception de telles données.	I,F - A 2.10,15 - A 4.30 - A 7.40 - A 8.25,60

B 3.60	Des éléments de base cryptographiques peuvent être utilisés uniquement quand la longueur des clés et les algorithmes correspondent aux normes courantes (par ex. FIPS 143-3, NIST, ENCRYPT, SCSE). La signature électronique doit satisfaire aux exigences d'une signature électronique avancée au sens de la loi fédérale du 19 décembre 2003 sur les services de certification dans le domaine de la signature électronique. La vérification de la signature doit se faire au moyen d'un certificat délivré par un fournisseur de services de certification reconnu au sens de la SCSE.	I,F
B 3.70	Les électeurs reçoivent les informations nécessaires au contrôle de l'authenticité du site Internet utilisé pour exprimer le suffrage et de celle du serveur. La pertinence d'une vérification réussie doit être soutenue par l'emploi de moyens cryptographiques conformément aux meilleures pratiques.	I,F - A 1.60 - A 2.40 - Men 3.20,30,40 - Men 2.20,30

3.5. Echange d'informations électronique et physique sûr

B 4.10	Le système de dépouillement des suffrages doit, au sein de la zone de réseau de l'infrastructure du VE, être exploité moyennant la mise en place d'une zone de réseau complètement séparée des autres composants de l'infrastructure du VE.	I - 7.10,15,30,35,40,50,60 - A8.10,20,25,30,40,50,60 - Men3.60,70,80,90 - Men2.40,50,60,70 - Men1.50,70,80
B 4.20	Les systèmes sur lesquels tourne le vote électronique doivent être protégés contre des attaques (indépendamment du type des attaques ou de leur provenance).	I
B 4.30	L'ensemble des composants de l'infrastructure du VE doit être exploité dans une zone de réseau séparée. Cette zone doit être protégée moyennant un contrôle de routage adéquat.	I - A8.10,20,25,30,40,50,60 - Men3.60,70,80,90 - Men2.40,50,60,70 - Men1.50,70,80,90
B 4.50	Les traitements en rapport avec le vote par voie électronique doivent être clairement séparés de l'ensemble des autres applications.	I - A8.10,20,25,30,40,50,60 - Men3.60,70,80,90 - Men2.40,50,60,70 - Men1.50,70,80,90

3.6. Tests des fonctionnalités du VE

B 5.10	Un schéma de test doit garantir que les fonctionnalités du VE fonctionnent conformément aux spécifications. Le schéma doit comprendre des scénarios de tests en tout genre. Il règle les responsabilités lors de l'exécution, de l'établissement des protocoles et de la rédaction des rapports à l'attention des responsables du VE. Il définit les conditions dans lesquelles un test doit être exécuté. Lors du développement, il faut au minimum tester chacune des fonctionnalités pertinentes du point de vue de la sécurité, même en cas de modifications minimes. Avant chaque scrutin, il faut procéder à un test de performance sur le système productif et tester la disponibilité de chaque fonction.	I,F

3.7. Directive concernant la sécurité de l'information

B 6.10	Le responsable cantonal du VE doit édicter et distribuer une directive concernant la sécurité de l'information qui définisse un cadre de sécurité contraignant pour l'ensemble de l'exploitation du système de VE. Cette directive doit être contrôlée à intervalles déterminés et adaptée au besoin.	I

3.8. Organisation de la sécurité de l'information

B 7.10	Tous les rôles et les responsabilités pour l'exploitation du système de VE doivent être précisément définis, attribués et communiqués.	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.50,60,70,80
B 7.20	Un processus d'autorisation doit être mis en place pour les installations de traitement des informations de l'infrastructure du VE.	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.50,60,70,80
B 7.30	Les risques liés à des tierces parties doivent être identifiés et traités moyennant des conventions contractuelles adéquates. Le respect de ces conventions doit être surveillé et vérifié de manière appropriée pendant leur durée de validité.	I

3.9. Gestion des biens sensibles

B 8.10	Tous les biens sensibles pertinents en rapport avec le VE (organisation du VE en tant que tout, en particulier les processus organisationnels et les informations traitées dans le cadre de ces processus; le personnel du VE; les supports de données; les installations de traitement des données de l'infrastructure du VE; les locaux de l'infrastructure du VE) doivent être saisis dans un inventaire à actualiser. Chaque bien sensible doit être attribué à une personne qui en prend la responsabilité.	I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20 - A5.10 - A7.10,15,35,40,50 - A8.10,20,35,30,40,50,60,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,50, 60,70,80,90
B 8.20	L'utilisation licite de biens sensibles doit être définie.	I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20 - A5.10 - A7.10,15,35,40,50 - 8.10,20,35,30,40,50,60,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,50, 60,70,80,90
B 8.30	Des directives de classification doivent être édictées et communiquées pour l'information.	I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20 - A5.10 - A7.10,15,35,40,50 - A8.10,20,35,30,40,50,60,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,50, 60,70,80,90
B 8.40	Des procédures doivent être définies pour la désignation et la gestion des informations.	I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20 - A5.10 - A7.10,15,35,40,50 - 8.10,20,35,30,40,50,60,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,50, 60,70,80,90

3.10. Sécurité personnelle

B 9.10	Pour garantir la sécurité personnelle avant, pendant et après la période d'engagement ou en cas de changement de rôle, il faut élaborer et diffuser des directives et des procédures adéquates.	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.50,60,70,80
B 9.20	Les décideurs du personnel du VE doivent assumer l'entière responsabilité pour garantir la sécurité personnelle.	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.50,60,70,80
B 9.30	Il faut, pour l'ensemble du personnel, mettre en place et exploiter un programme de formation et d'entraînement qui soit adapté aux tâches et renforce la sensibilité en matière de sécurité de l'information.	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.50,60,70,80

3.11. Sécurité physique et liée à l'environnement

B 10.10	Les périmètres de sécurité des différents locaux de l'infrastructure du VE (locaux pour les différents groupes de personnes du personnel du VE, locaux pour les serveurs, etc.) doivent être clairement définis.	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,60,70,80,90
B 10.20	Des autorisations d'accès doivent être définies, créées et contrôlées de manière adéquate pour l'accès physique aux différents locaux de l'infrastructure du VE.	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.80
B 10.30	Pour garantir la sécurité des appareils à l'intérieur et à l'extérieur des locaux de l'infrastructure du VE, il faut définir des directives et des procédures adéquates ainsi que surveiller et vérifier qu'elles sont respectées.	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,60,70,80,90

3.12. Gestion de la communication et de l'exploitation

B 11.10	Les étapes de l'utilisation doivent être décrites de manière détaillée pour les principales activités du système.	I - A2.10,15,20,30,40,50 - A3.60 - A4.20,30 - A5.10,20,30 - A7.10,15,30,35,40,50,60 - Men1.50
B 11.20	Les systèmes productifs peuvent uniquement être modifiés conformément à une procédure documentée de gestion des modifications.	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,50,60,70,80,90
B 11.30	Les obligations et les domaines de responsabilité doivent être répartis de manière appropriée.	I - A2.10,15,20,30,40,50 -- A3.60 - A4.20,30 - A5.10,20,30 - A7.10,15,30,35,40,50,60 - Men1.50
B 11.40	Des mesures appropriées doivent être prises contre les logiciels malveillants.	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,50,60,70,80,90
B 11.50	Il faut établir et mettre en œuvre un plan détaillé pour la sécurité des données. Le bon fonctionnement de la sécurité des données doit être vérifié à intervalles réguliers.	I - A1.35,60 - A2.10,15,20,30,40,50 - A4.20 - A5.10,20,40 - A6.10,20,30 - A7.10,15,30,35,40,50 - A8,10,20,25,30,40,50,60,70 - Men3.80 - Men1.50 - Men1.80
B 11.60	Des mesures adéquates doivent être définies et mises en œuvre pour assurer la protection du réseau et la sécurité des services du réseau.	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,50,60,70,80,90

B 11.70	Les procédures relatives à l'utilisation des supports de données amovibles et à l'élimination de supports de données doivent être réglées en détail.	I - A8.10,20,25,30,40,50,60,70 - Men3.80,90 - Men2.40,50,60,70 - Men1.70,80,90
B 11.80	Les mesures en rapport avec la surveillance et l'établissement des protocoles de l'utilisation du système, des activités des administrateurs et des incidents doivent être décrites de manière détaillée, mises en œuvre, suivies et vérifiées.	I - A2.10,15,20,30,40,50 - A3.15,20,30,40,45 - A4.20,30 - A5.10,20,30,40 - A7.10,15,35,40,50 - A8.10,20,35,30,40,50,60,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.50,60,70,80,90

3.13. Exigences à l'attention des imprimeries

B 12.10	Les imprimeries doivent remplir les conditions fixées dans le catalogue de critères de la Chancellerie fédérale en matière de vote électronique pour les imprimeries.	

3.14. Acquisition, développement et maintenance de systèmes d'information

B 13.10	Des procédures adéquates doivent être décrites de manière détaillée et mises en œuvre de manière scrupuleuse pour l'installation de logiciels sur les systèmes productifs.	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,50,60,70,80,90
B 13.20	Des procédures adéquates doivent être décrites de manière détaillée et mises en œuvre de manière scrupuleuse pour le traitement des failles techniques. Une attention particulière doit être portée aux parties de l'infrastructure du VE qui sont accessibles par Internet.	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,50,60,70,80,90

3.15. Exigences découlant du profil de protection du BSI

Les exigences découlant du profil de protection du BSI [4] doivent être mises en œuvre en sus des exigences décrites plus haut. La terminologie du profil de protection est déterminante lors de leur interprétation.

En cas de divergences entre les versions allemande et anglaise du profil de protection, ce sont les dispositions de la version anglaise qui font foi. En cas de divergences entre le profil de protection et le RT VE, c'est ce dernier qui fait foi.

Les divergences suivantes par rapport au profil de protection sont autorisées ou doivent être impérativement respectées:

B 14.10	OE.ElectionPreparation prévoit notamment que les électeurs vérifient les données figurant dans le registre des électeurs et peuvent, le cas échéant, demander que les données soient corrigées. Cette exigence ne doit pas être mise en œuvre pour les personnes autorisées à voter par voie électronique.
B 14.20	Il ne doit pas y avoir d'enregistrement des électeurs. Les données figurant dans le registre des électeurs sont déterminantes pour l'octroi de l'autorisation de voter.
B 14.30	OE.ServerRoom prévoit que seul le responsable électoral a le droit d'entrer dans la pièce abritant le serveur. Cette exigence peut être interprétée de manière moins stricte: seules des personnes nommées par le responsable cantonal peuvent entrer dans la pièce; elles sont surveillées.
B 14.40	Dans des cas solidement motivés, il est permis d'utiliser des mesures de sécurité TI alternatives (au sens de la terminologie selon les CC; *security functional requirements* en anglais).

Annexe du règlement technique de la Chancellerie fédérale du ... concernant le vote électronique (RS ...)

La liste ci-après met les objectifs de sécurité (au sens de la terminologie des CC; *security objectives* en anglais) en relation avec les menaces et les exigences concernant l'aménagement des processus élémentaires du présent règlement.

O.UnauthorisedVoter	F,I - A1.33 - A2.10,15,20,30 - A4.20 - A6.10 - Men3.70,80,90
O.Proof	F,I - A 1.50 - Men1.70
O.IntegrityMessage	F - A1.35,60 - A2.40 - A4.30 - Men3.20,30,40 - Men2.30
O.SecrecyOfVoting	F - A1.35 - A2.40 - A8.10,20 - Men2.30,40,70
O.SecretMessage	F - A1.35 - A2.40 - A8.10,30 - Men3.90
O.AuthenticityServer	F,I - A1.35 - A2.40 - A4.20 - Men3.20,30,40 - Men2.30
O.ArchivingIntegrity	F,I - A2.40 - A7.15,30,35 - Men3.60,70,80
O.ArchivingSecrecyOfVoting	F,I - A7.15 - A8.10,50,70 - Men2.40,50,70 - Men1.70
O.Abort	F - A1.47
O.EndingElection	F - A5.30,40 - Men1.50
O.EndOfElection	F - A5.40 - Men1.50
O.SecrecyOfVotingElectionOfficers	F - A7.15 - A8.10,50,60 - Men2.40,50,70
O.IntegrityElectionOfficers	F - A5.10,20,40 - A7.35 - Men3.50,60,70,80
O.IntermediateResult	F - A7.10 - A8.20,25 - Men2.60,70
O.OverhasteProtection	F - A1.45
O.Correction	F - A1.40
O.Acknowledgement	F - A1.60 - Men1.10
O.Failure	F,I - A2.50 - A5.10 - Men1.40,50
O.Audit	F,I - A1.35, A1.60 - A2.10,15,20,30,40,50 - A5.10,20,40 - A6.10,20,30 - A7.10,15,35,40,50 - A8,10,20,25,30,40,50,60,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,50,60,70,80,90
O.OneVoterOneVote	F,I - A1.33,40,47,60,80 - A2.10,15,20,30 - A4.10 - A6.10,20,30 - A7.50 - Men3.70,80 - Men1.10
O.AuthElectionOfficers	F - A2.10,15,20,30,40,50 - A4.20 - A5.10,20,40 - A7.10,15,35,40 - A8.10,20,25,30,40,50,60
O.StartTallying	F - A5.40 - A7.10,15 - Men2.60,70
O.Tallying	F - A2.50 - A5.10 - A7.15 - Men3.50,70,80 - Men1.50
OE.ElectionPreparation	F,I - A2.10,15,20,30,40,50 - A3.10,20 - A4.20,30 - A5.10 - A8.10,20,25,30,40,50,60,70 - Men3.70,80 - Men1.50
OE.Observation	F - A1.35
OE.ElectionOfficers	I - A2.10,15,50 - A3.15 - A5.10,20,40 - A7.10,15,3035,40,60 - A8.10,20,25,30,40,50,60,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.50,60,70,80,90
OE.AuthData	F,I - A2.10,15,20,30 - A4.20,30 - A8.10,40 - Men3.80,90
OE.VoteCastingDevice	F,I - A1.30 - A3.20,30 - Men3.10 - Men2.10
OE.ElectionServer	I - Men3.80 - Men2.70 - Men1.80
OE.Availability	I - Men1.40
OE.ServerRoom	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.80
OE.DataStorage	I - A1.35,60 - A2.10,15,20,30,40,50 - A4.20 - A5.10,20,40 - A6.10,20,30 - A7.10,15,30,35,40,50 - A8,10,20,25,30,40,50,60,70 - Men3.80 - Men1.50 - Men1.80

OE.SystemTime	I - A1.35,60 - A5.10,20,40 - A6.10,20,30 - A7.10,15,35 - A8.10,20,25,30,40,50,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.50,70,80
OE.AuditTrailProtection	I - A1.35, A1.60 - A2.10,15,20,30,40,50 - A5.10,20,40 - A6.10,20,30 - A7.10,15,35,40,50 - A8,10,20,25,30,40,50,60,70 - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.40,50,60,70,80,90
OE.AuthenticityServer	F - A3.20,30,40 - A4.20 - Men 3.20,30,40 - Men 2.30
OE.ArchivingIntegrity	F,I - A2.40 - A7.15,30,35 - Men3.60,70,80
OE.ArchivingSecrecyOfVoting	F,I - A7.15 - A8.10,50,70 - Men2.40,50,70 - Men1.70
OE.ProtectedCommunication	I - Men3.50,60,70,80,90 - Men2.40,50,60,70 - Men1.70,80,90
OE.Buffer	F - A3.45

4. Vérifiabilité

Les art. 3 et 4 contiennent les dispositions consacrées à la vérifiabilité. La présente annexe expose ces dispositions d'une manière plus formelle afin d'expliciter les critères applicables aux deux formes de vérifiabilité.

Pour ce faire, le sous-chapitre 4.1 définit un modèle abstrait réduit pour décrire le déroulement d'un scrutin. Se fondant sur ce modèle, le sous-chapitre 4.2 contient des explications concernant l'art. 3 et des dispositions qui complètent ce dernier. Le sous-chapitre 4.4 présente le modèle abstrait complet. Le sous-chapitre 4.4, enfin, contient des commentaires concernant l'art. 4 et des dispositions qui complètent ce dernier.

4.1. Modèle abstrait réduit relatif à l'art. 3

Dans le modèle abstrait utilisé, un scrutin est défini par un protocole cryptographique constitué par les échanges d'informations entre les éléments du système suivants:

Electeurs / votants	Les électeurs reçoivent du système de VE ou de l'imprimerie leurs données d'authentification client avant le scrutin. Pour pouvoir envoyer leur suffrage, ils communiquent leurs données d'authentification client et leur suffrage à la plate-forme utilisateur.
Plate-forme utilisateur	Elle génère le message d'authentification et l'envoie à la partie serveur du système de VE avec le suffrage crypté. Pour ce faire, elle utilise les paramètres publics qu'elle a reçus auparavant du système de VE. Elle affiche au besoin, pour les votants, les messages envoyés par la partie serveur du système de VE.
Dispositif technique fiable des électeurs	Les votants peuvent aussi saisir leur suffrage et/ou leurs données d'authentification client sur un dispositif technique fiable. Ce dernier peut effectuer n'importe quelle tâche dévolue à la plate-forme utilisateur.
Système de VE (il est ici toujours question de la partie serveur)	Il génère les données d'authentification client et les envoie aux électeurs avant le scrutin (éventuellement par l'entremise de l'imprimerie). Il génère également les paramètres publics et les envoie à la plate-forme utilisateur afin qu'elle puisse générer le message d'authentification et le suffrage crypté. Il évalue la validité des suffrages en fonction des règles connues, il décrypte les suffrages dans le respect du secret du vote et il calcule les résultats du scrutin.
Imprimerie	On peut faire appel à elle pour imprimer les données d'authentification client et les données confidentielles grâce auxquelles les votants pourront faire usage de la vérifiabilité individuelle (référence de vérifiabilité). Le système de VE envoie les données correspondantes à l'imprimerie, qui les envoie à son tour aux électeurs.

Le protocole peut prévoir les canaux de communication suivants pour l'échange de messages:

- votants ↔ plate-forme utilisateur
- votants ↔ dispositif technique fiable
- dispositif technique fiable ↔ plate-forme utilisateur
- plate-forme utilisateur ↔ système de VE
- système de VE ↔ imprimerie
- imprimerie → électeurs

Soit les éléments du système et les canaux de communication sont fiables, soit ils ne le sont pas. Les éléments du système qui sont fiables conservent de façon sécurisée toutes les données secrètes, sans exception, et n'effectuent que les opérations prescrites dans le protocole. Les canaux qui sont fiables doivent garantir que les messages transmis restent secrets. Par ailleurs, le destinataire d'un message peut avoir la certitude que l'expéditeur d'un message est l'élément du système qui est prescrit dans la définition du canal.

Qui plus est, le modèle abstrait prévoit un attaquant qui peut corrompre tous les éléments du système et les canaux de communication qui ne sont pas fiables et en prendre le contrôle. Les éléments du système qui sont corrompus communiquent toutes les données secrètes à l'attaquant et agissent librement en fonction des instructions de ce dernier. L'attaquant peut aussi consulter ou intercepter tous les messages échangés sur les canaux qui ne sont pas fiables, et même envoyer des messages à loisir.

Hypothèses de confiance dans le modèle abstrait (vérifiabilité individuelle du protocole): dans ce modèle, on part des trois hypothèses suivantes en ce qui concerne la vérifiabilité individuelle: premièrement, les dispositifs techniques fiables, le système de VE et l'imprimerie sont fiables; deuxièmement, les plates-formes utilisateurs et un pourcentage significatif d'électeurs ne sont pas fiables; troisièmement, les seuls canaux de communication à ne pas être fiables sont les deux canaux « plate-forme utilisateur ↔ système de VE » et « système de VE ↔ imprimerie ».

Objectif de sécurité dans le modèle abstrait (vérifiabilité individuelle du protocole): compte tenu des hypothèses de confiance qui ont été formulées, l'attaquant n'est pas en mesure d'atteindre les objectifs suivants sans qu'il y ait une grande probabilité qu'un votant s'aperçoive qu'une attaque a eu lieu:

- modifier le suffrage avant son enregistrement
- faire disparaître le suffrage avant son enregistrement
- exprimer un suffrage

Pour atteindre l'objectif de sécurité, il ne faut utiliser dans le protocole que des éléments cryptographiques qui sont réputés sûrs.

Vérifiabilité individuelle du système de VE dans la mise en oeuvre: le système de VE met en oeuvre un protocole cryptographique qui répond à l'objectif de sécurité relatif à la vérifiabilité individuelle dans le modèle abstrait. La où cela est nécessaire, l'hypothèse selon laquelle les éléments du système et les canaux de communication sont fiables est justifiée par des mesures de sécurité correspondantes.

Le sous-chapitre 4.2 met en relation les dispositions de l'art. 3 et l'objectif de sécurité dans le modèle abstrait tout en les explicitant là où cela est nécessaire. Il renferme par ailleurs des exigences de sécurité relatives aux éléments du système et aux canaux de communication considérés comme fiables dans le modèle abstrait.

4.2. Dispositions complémentaires concernant la vérifiabilité individuelle

D2.05	(ad art. 3, al. 1) La preuve ne doit pas forcément être apportée au cours d'une seule et unique transaction. Elle peut aussi être répartie entre plusieurs messages que le votant reçoit durant le processus de vote. (Dans ce cas, le dernier message confirme que le suffrage a été exprimé conformément à la procédure prévue par le système.) Si le votant décide d'interrompre le processus avant de procéder au vote définitif (et donc avant la réception du dernier message), il doit toujours avoir la possibilité de voter de façon traditionnelle.
D2.06	(ad art. 3, al. 2) L'objectif consiste à empêcher que des éléments du système qui ne sont pas fiables puissent exprimer un suffrage sans qu'on s'en aperçoive. Il faut interpréter cette disposition dans ce sens et vérifier le protocole en conséquence.
D2.07	(ad art. 3, al. 4) La preuve est concluante si elle permet aux votants d'identifier les manipulations de leur suffrage conformément à l'objectif de sécurité et compte tenu des hypothèse de confiance qui ont été formulées. L'attaquant n'est ainsi pas en mesure de tromper les votants en fabriquant, avec l'aide des éléments du système qui ne sont pas fiables, une preuve faisant croire aux votants que leur suffrage a été enregistré, tel qu'il a été exprimé, comme étant valable. La probabilité que l'attaquant réussisse à établir une telle preuve en devinant le choix des votants (au même titre que la preuve attestant qu'aucun suffrage n'a été exprimé) ne doit pas dépasser 0,1 %.
D2.08	(ad art. 3, al. 4) On peut prévoir des facilités pour permettre aux électeurs handicapés de vérifier les preuves fournies. C'est uniquement dans ce cas qu'on peut déroger à l'objectif de sécurité. En l'occurrence, on peut faire dépendre le caractère concluant des preuves de la fiabilité de la plate-forme utilisateur. Cela permet par exemple de numériser la référence de vérification avant le vote. Ces facilités sont réservées à un petit groupe d'électeurs qui, sans elles, ne pourraient pas interpréter la preuve dans tout son caractère

	concluant. Les électeurs auxquels ce cas ne s'applique pas doivent être incités à vérifier les preuves conformément à la procédure prévue.
D2.10	(ad art. 3, al. 4) Si les votants se servent d'un dispositif technique pour procéder à la vérification, ce dispositif doit avoir été conçu spécialement pour la sauvegarde sécurisée d'éléments secrets et pour l'exécution d'opérations cryptographiques, comme c'est le cas des appareils utilisés pour les transactions bancaires sécurisées depuis son domicile. Qui plus est, les votants doivent pouvoir acquérir la conviction que le dispositif fonctionne correctement en exprimant des suffrages-tests.
D2.20	(ad art. 3, al. 3 et 4) La disposition suivante s'applique en plus du catalogue de critères pour les imprimeries: tous les appareils que l'on utilise, sous quelque forme que ce soit, pour traiter des données inhérentes à la référence de vérifiabilité doivent faire l'objet d'une surveillance oculaire (principe des quatre yeux) pendant toute la durée des opérations de calcul. Seules sont autorisées les connexions au réseau dont les éléments sont reliés par des câbles physiques, de telle sorte qu'on puisse constater qu'aucun autre appareil n'est en mesure d'accéder aux données confidentielles jusqu'à leur destruction.
D2.30	(ad art. 3, al. 3 et 4) La partie serveur du système de VE ne fait pas l'objet de dispositions supplémentaires. Lors de la mise en oeuvre des exigences fondamentales et des exigences de sécurité (voir art. 1, al. 1, let. a, et annexe, chap. 2 et 3), il faut toutefois tenir compte du fait qu'il est impératif de faire en sorte que les données qui sont en relation avec la référence de vérifiabilité restent confidentielles pour garantir l'exactitude des résultats et le secret du vote, mais aussi pour éviter que des résultats partiels soient établis de manière anticipée.
D2.40	(ad art. 3, al. 3 et 4) La fiabilité du canal entre l'imprimerie et les électeurs n'est justifiée que par une instanciation, à savoir par la remise physique, notamment par la Poste suisse, ou par la remise en mains propres.

4.3. Modèle abstrait complet relatif à l'art. 4

Le modèle abstrait complet considère que le système de VE n'est pas fiable. Il prévoit des vérificateurs qui déterminent, sur la base d'un dispositif fiable et de « composants de contrôle » indépendants, si les résultats ont été établis correctement.
Ce modèle comporte ainsi les éléments supplémentaires suivants:

Composant de contrôle	Il interagit avec le système de VE et les autres composants de contrôle de telle sorte que le système peut, à l'issue du scrutin, générer une preuve concluante qui atteste que les résultats ont été établis correctement.
Vérificateurs	A l'issue du dépouillement, ils reçoivent du système de VE une preuve attestant que les résultats ont été établis correctement.
Dispositifs techniques des vérificateurs	Les vérificateurs peuvent utiliser un dispositif technique pour évaluer la preuve.

Le protocole cryptographique peut prévoir les canaux de communication supplémentaires suivants pour l'échange de messages:

- composant de contrôle ↔ système de VE
- système de VE ↔ dispositif technique des vérificateurs
- dispositif technique des vérificateurs ↔ vérificateurs
- canaux bidirectionnels destinés à la communication entre les composants de contrôle

Hypothèses de confiance dans le modèle abstrait (vérifiabilité complète du protocole): plusieurs composants de contrôle sont utilisés, qui sont rassemblés dans un groupe ou dans quelques groupes seulement. On doit partir de l'hypothèse qu'un seul et unique composant de contrôle n'est pas fiable, comme le système de VE. Il faut toutefois partir de l'hypothèse qu'il y a au moins un composant de contrôle fiable par groupe, mais sans déterminer lequel. La quantité de groupes de composants de contrôle constitue la partie fiable du système. La fiabilité de cette partie du système est définie par la fiabilité d'au moins un composant de contrôle dans chacun de ses groupes. Le caractère concluant de la preuve que reçoit un vérificateur en vertu de l'art. 4 ne doit dépendre que de la fiabilité de la partie fiable du système et du dispositif technique dont le vérificateur dispose. On part aussi de l'hypothèse selon laquelle il y a au moins un vérificateur fiable qui examine la preuve à l'aide d'un dispositif technique fiable. Les autres vérificateurs éventuels et leurs dispositifs techniques sont considérés

comme n'étant pas fiables. Par ailleurs, on part de l'hypothèse que, parmi les canaux de communication supplémentaires, le seul qui est fiable est celui qui relie les vérificateurs et leur dispositif technique. Le système de VE doit être considéré comme n'étant pas fiable.

Objectif de sécurité dans le modèle abstrait (vérifiabilité complète du protocole):

- compte tenu des hypothèses de confiance qui ont été formulées à propos de la vérifiabilité complète du protocole, l'attaquant n'est pas en mesure d'atteindre les objectifs suivants sans qu'il y ait une grande probabilité qu'un votant ou un vérificateur fiable s'aperçoive qu'une attaque a eu lieu:
  - modifier le suffrage avant son enregistrement par la partie fiable du système
  - faire disparaître le suffrage avant son enregistrement par la partie fiable du système
  - exprimer un suffrage
  - modifier un suffrage qui a été exprimé conformément à la procédure prévue par le système et qui a été enregistré par la partie fiable du système
  - faire disparaître un suffrage qui a été exprimé conformément à la procédure prévue par le système et qui a été enregistré par la partie fiable du système
  - ajouter un suffrage qui n'a pas été exprimé conformément à la procédure prévue par le système
- compte tenu des hypothèses de confiance qui ont été formulées à propos de la vérifiabilité complète du protocole, l'attaquant ne peut ni violer le secret du vote, ni collecter des résultats partiels anticipés sans corrompre les électeurs ou leurs plates-formes utilisateurs respectives.

Pour atteindre l'objectif de sécurité, il ne faut utiliser que des éléments cryptographiques qui sont réputés sûrs.

Vérifiabilité complète du système de VE dans la mise en oeuvre: elle est régie par les dispositions applicables à la vérifiabilité individuelle.

Le sous-chapitre 4.4 met en relation les dispositions de l'art. 4 et l'objectif de sécurité dans le modèle abstrait tout en les explicitant là où cela est nécessaire. Il renferme par ailleurs des exigences de sécurité relatives aux éléments du système et aux canaux de communication considérés comme fiables dans le modèle abstrait.

4.4. Dispositions complémentaires concernant la vérifiabilité complète

D4.10	(ad art. 4, al. 1) Le recours à des vérificateurs concourt à la transparence. Les électeurs doivent pouvoir partir de l'idée que les vérificateurs leur signaleraient toute irrégularité en cas de doute. C'est toutefois à dessein que l'on ne précise pas de quels milieux doivent venir les personnes mandatées pour revêtir le rôle de vérificateur.
D4.20	(ad art. 4, al. 2, let. a) Forts des informations figurant dans la partie fiable du système (le suffrage crypté lui-même peut s'y trouver), les vérificateurs peuvent déterminer si tel ou tel suffrage a été pris en compte, sous une forme non modifiée, pour l'établissement des résultats. Les votants doivent ainsi pouvoir se fier au fait que les données se trouvant dans la partie fiable du système n'en ont pas été retirées ou n'ont pas été manipulées. La littérature spécialisée contient à ce propos des propositions consistant à publier les suffrages cryptés sur un tableau d'affichage électronique (« public board » en anglais). Pour créer un tableau d'affichage, il faut y intégrer plusieurs composants fiables, de telle sorte que que les inscriptions ne puissent être supprimées ou modifiées sans qu'on s'en aperçoive que si plusieurs de ces composants sont corrompus. Grâce à une plate-forme utilisateur fiable, les votants peuvent constater à tout moment que leur suffrage se trouve dans la masse des suffrages exprimés. A l'issue de la votation, le tableau d'affichage contient les résultats et la preuve que les résultats ont été établis correctement, preuve qui est générée dans le cadre de la vérifiabilité universelle. Les votants pourraient, animés par la volonté d'avoir une transparence maximale, revêtir le rôle des « vérificateurs ». Plusieurs réflexions sur les risques, qui ont notamment un lien avec l'hypothèse concrète selon laquelle les plates-formes utilisateurs doivent être considérées comme n'étant pas fiables, peuvent militer en faveur de la publication restreinte des données pertinentes pour la vérifiabilité qui figurent dans la partie fiable du système. C'est la raison pour laquelle il est permis de ne fournir les données qu'à un

	nombre restreint de vérificateurs. Dans la terminologie utilisée dans la littérature spécialisée, cette exigence peut donc être comprise de la façon suivante: *les composants responsables du tableau d'affichage envoient aux votants la preuve attestant qu'ils ont reçu leur suffrage (ou les données qui sont suffisantes pour la vérification universelle). Le caractère concluant de cette preuve ne doit pas dépendre de la fiabilité d'une plate-forme utilisateur qui n'est pas fiable ou du système de VE. Les vérificateurs se voient octroyer, au plus tard après l'établissement des résultats (mais avant la publication), l'accès au tableau d'affichage et constatent que les résultats ont pris en compte chaque suffrage sur le tableau d'affichage, conformément aux règles en vigueur.*
D4.30	(ad art. 4, al. 2, let. b) L'objectif consiste à empêcher que des éléments du système qui ne sont pas fiables puissent exprimer un suffrage sans qu'on s'en aperçoive. Il faut interpréter cette disposition dans ce sens et vérifier le protocole en conséquence.
D4.40	(ad art. 4, al. 2, let. c) La confidentialité des données relatives à une éventuelle référence de vérification ne peut donc dépendre, même au sein de l'infrastructure du VE, que de la partie fiable du système.
D4.50	(ad art. 4, al. 3, let. a) Le fait que le dispositif technique doive être indépendant et séparé du reste du système a pour but de garantir que l'évaluation de la preuve ne pourra pas être influencée par le système de VE. C'est toutefois à dessein que la disposition ne précise pas si les dispositifs techniques et les programmes correspondants doivent être fournis par le système de VE ou par les vérificateurs. Les vérificateurs doivent néanmoins pouvoir déterminer facilement si le dispositif fonctionne correctement. Une solution consiste notamment à faire en sorte que les vérificateurs écrivent eux-mêmes les programmes ou puissent à tout le moins les analyser préalablement. Avant la vérification, ils pourraient installer le dispositif avec les responsables du système, puis compiler et installer les programmes de vérification. D'une manière générale, les programmes de vérification doivent être faciles à écrire dans un souci de transparence.
D4.60	(ad art. 4, al. 3, let. b) Un suffrage n'est valable que si les données d'authentification client correspondent aux données d'authentification serveur qui ont été établies durant la phase de préparation du scrutin et « attribuées » à un électeur. La preuve doit donc attester qu'on n'a pas établi de données d'authentification non atttribuées dans le but d'exprimer des suffrages non valables. C'est pourquoi il faut que des données correspondantes servant de base de comparaison aient été transmises aux composants de contrôle ou aux vérificateurs pendant la phase de préparation du scrutin. Les vérificateurs doivent constater que le nombre de données d'authentification correspond au nombre (officiel) d'électeurs autorisés à participer au scrutin. Dans ce cas, on peut considérer que les données d'authentification ont été « attribuées » à un électeur. Cette procédure ne donne certes pas encore la garantie qu'une personne n'a pas, pour voter valablement, utilisé abusivement les données d'authentification client d'un électeur fiable, mais l'électeur en question peut s'en rendre compte eu égard au point correspondant dans l'objectif de sécurité du modèle abstrait, mais aussi eu égard à l'art. 4, al. 2, let. b.
D4.70	(ad art. 4, al. 4) La preuve est concluante si elle permet aux votants ou aux vérificateurs d'identifier une manipulation des suffrages conformément à l'objectif de sécurité et compte tenu des hypothèses de confiance qui ont été formulées. Par conséquent, l'attaquant ne peut pas induire en erreur les éléments du système qui ont un rôle de vérification en confectionnant, à l'aide des éléments du système qui ne sont pas fiables, une preuve pour justifier des résultats manipulés, ou en influençant la confection de ladite preuve. Les dispositions suivantes s'appliquent dans le cadre de la vérifiabilité universelle: – Les vérificateurs doivent pouvoir identifier tous les cas dans lesquels on fait disparaître – sans le remplacer – un suffrage valable qui a été enregistré par la partie fiable du système. – Les vérificateurs doivent pouvoir identifier tous les cas dans lesques on ajoute un suffrage non valable sans qu'on ait fait disparaître un autre suffrage. – La probabilité de réussir à manipuler 0,1 % des suffrages partiels (par exemple en faisant disparaître des suffrages tout en en ajoutant), de telle sorte qu'ils ne restituent plus le contenu de la preuve générée dans le cadre de la vérification individuelle, ne doit pas dépasser 1 %. Si la probabilité n'est pas négligeable au sens cryptographique du terme, il faut pouvoir réduire suffisamment le risque en procédant à plusieurs dépouillements en utilisant de nouvelles valeurs aléatoires.
D4.80	(ad art. 4, al. 4) Si l'application utilisée sur la plate-forme utilisateur pour le cryptage du suffrage est mise à disposition par le système de VE, elle doit être attribuée aussi à la partie serveur du système de VE. Il s'agit d'éviter que, dans la partie serveur, une

	manipulation de l'application entraîne la violation du secret du vote par des votants fiables sans qu'il y ait eu corruption de leur plate-forme utilisateur. Les votants doivent donc avoir la possibilité de se convaincre, grâce à une plate-forme utilisateur fiable, que l'application enverra leur suffrage de façon cryptée avec la clé correcte. On peut par exemple y parvenir en recourant à une technologie de navigation qui permette de consulter le code source de l'application de l'utilisateur. Les votants peuvent ainsi se convaincre du fait que la clé publique utilisée correspond à celle du scrutin, mais aussi que l'application exécute exclusivement les opérations prévues. On pourrait aussi imaginer, à titre de variante, que le code source soit signé par un groupe de composants de contrôle.
D4.90	(ad art. 4, al. 4) Conformément à l'objectif de sécurité, il faut éviter que la partie serveur du système de VE puisse, en collaboration avec un électeur non fiable, accéder au contenu d'un suffrage exprimé. Pour y parvenir, il faut faire en sorte que cet électeur ne puisse pas faire passer pour le sien un suffrage crypté autre que le sien qui a été exprimé, même après l'avoir modifié extérieurement, son objectif étant de connaître le contenu du suffrage au moyen de la preuve qu'il reçoit dans le cadre de la vérifiabilité individuelle.
D4.A0	(ad art. 4, al. 4) En raison de l'exigence qui veut que le secret du vote soit garanti et qu'aucun résultat partiel ne soit établi ne manière anticipée, les éléments du système ne doivent pas avoir accès aux clés privées servant à décrypter des suffrages au moins tant que le canal permettant de voter par voie électronique est ouvert. Il est toutefois permis de calculer les clés privées en cas de recours à tous les composants de contrôle d'un groupe. Il est aussi permis de prévoir un groupe de composants de contrôle qui serait un groupe de personnes. Chaque membre de ce groupe pourrait détenir une partie de la clé privée sur un support d'enregistrement portable. Pour que le secret du vote soit préservé, la clé privée ne pourrait exister, après le décryptage, qu'à condition que les suffrages aient été exprimés anonymement et que, compte tenu des hypothèses de confiance formulées, il soit impossible d'établir un lien entre le cryptage d'un suffrage et l'identité d'un votant. Par ailleurs, eu égard à l'exigence qui veut qu'aucun résultat partiel ne soit établi à titre anticipé, il n'est pas permis que des suffrages se trouvent en dehors de la plate-forme utilisateur, sous une forme non cryptée, à quelque moment que ce soit pendant la durée d'ouverture du canal permettant de voter par voie électronique.
D4.B0	(ad art. 4, al. 5) L'identification de dysfonctionnements sérieux du système de VE dépend de la fiabilité de la « partie fiable du système ». Ces dysfonctionnements englobent notamment les erreurs de calcul qui influencent les résultats, la violation du secret du vote et l'établissement de résultats partiels anticipés. A cet égard, la mise en œuvre de propositions connues qui figurent dans la littérature spécialisée garantit une fiabilité particulièrement élevée. Ces propositions sont tellement poussées que c'est seulement dans les cas où tous les composants de contrôle d'un groupe ne fonctionnent pas correctement – par exemple à la suite de manipulations passées inaperçues – que l'on ne parvient pas à identifier des dysfonctionnements sérieux. Mais s'il n'y a qu'un seul composant de contrôle qui fonctionne correctement, il est possible d'identifier tout dysfonctionnement du système de VE. Les composants de contrôle sont souvent appelés « trustees » dans les modèles abstraits en anglais. Ce terme qualifie des entités capables d'effectuer des calculs complexes et de garder secrets des éléments privés. Les calculs peuvent consister à mélanger et à recrypter correctement – selon une méthode démontrable – des suffrages (pour les rendre anonymes; chaque « trustee » correspond au nœud mélangeur d'un réseau de recryptage), à gérer un tableau d'affichage électronique fiable, à mettre en place une infrastructure à clés publiques et à décrypter correctement les suffrages – selon une méthode démontrable – à l'aide d'une de ces clés publiques qui a été distribuée. Dans les modèles abstraits, les « trustees » sont souvent présentés comme des personnes qui peuvent calculer comme des machines. Le fait qu'ils conservent à l'abri les éléments secrets, ou qu'ils ne les utilisent pas pour envoyer des messages dont on peut faire un usage abusif, dépend uniquement de leur volonté de ne pas coopérer avec l'attaquant. En pratique, il faut certes faire une distinction entre la machine et la personne qui la configure et qui la surveille, mais la description du protocole cryptographique peut présenter les composants de sécurité comme des « trustees » autonomes.
D4.C0	(ad art. 4, al. 5) Le logiciel des composants de contrôle doit être simple à analyser et ne disposer, si possible, que de fonctions cryptographiques élémentaires
D4.D0	(ad art. 4, al. 5) Les composants de contrôle doivent être installés, actualisés, configurés et sécurisés au cours d'un processus observable.

D4.E0	(ad art. 4, al. 5) Les composants de contrôle doivent si possible se distinguer les uns des autres, mais aussi être gérés indépendamment les uns des autres, l'objectif étant de faire en sorte qu'une personne qui réussirait à accéder illictement à un composant de contrôle ne dispose pas, dans toute la mesure du possible, d'un avantage si elle tente d'accéder à d'autres composants sans qu'on s'en aperçoive (mise en place de « trustees »; voir ch. D4.B0). Cette façon de procéder permet de continuer d'assurer la fiabilité d'un groupe de composants de contrôle. Pour ce faire, il faut prévoir au moins les mesures suivantes: – la gestion et la surveillance des composants de contrôle doivent être confiées à plusieurs personnes. – le matériel informatique et les systèmes de surveillance des composants de contrôle doivent être distincts les uns des autres. – les composants de contrôle doivent être raccordés à plusieurs réseaux. – les composants de contrôle ne doivent être accessibles, physiquement et logiquement, qu'aux personnes chargées de la gestion et de la surveillance d'un composant de contrôle spécifique. Les tentatives d'accès par les responsables d'autres composants de contrôle doivent être identifées et signalées au responsable des composants de contrôle en question.
D4.F0	(ad art. 4, al. 5) Les composants de contrôle doivent exécuter exclusivement les opérations prévues. Ils doivent être conçus pour identifier les accès illicites et pour donner l'alerte aux personnes responsables. Ces dernières doivent prévoir des mesures de surveillance externes comme la surveillance du trafic sur le réseau et l'établissement des procès-verbaux relatifs à ce trafic selon une méthode résistant aux manipulations, ou comme la surveillance physique à l'aide de caméras placées sous leur contrôle. Les personnes responsables doivent être considérées comme particulièrement fiables et dignes de confiance.
D4.I0	(ad art. 4, al. 5) Il faut recourir, par groupe, à au moins quatre composants de contrôle dotés de systèmes d'exploitation distincts. Si les composants de contrôle sont des appareils qui ont été conçus et vérifiés spécifiquement pour l'exécution sécurisée d'opérations cryptographiques (module matériel de sécurité [HSM]), il peut y avoir un groupe de deux composants de contrôle issus de fabricants distincts. Les deux HSM peuvent utiliser le même système d'exploitation.
D4.J0	(ad art. 4, al. 5) Un HSM doit disposer d'un certificat fiable attestant que les éléments secrets sont inaccessibles et que le HSM enregistre chaque utilisation des éléments secrets de telle sorte que la personne responsable puisse identifier toute utilisation abusive. Le certificat doit correspondre, par analogie, au moins au degré EAL4 des Critères communs (Common Criteria [CC]) ou au niveau 3 de la norme FIPS 140-2. Il est permis de compléter un HSM par un logiciel qui fonctionne dans un périmètre protégé. Dans ce cas, le certificat doit aussi porter sur la fiabilité du périmètre protégé. Il s'agit de vérifier le logiciel, mais aussi de s'assurer qu'il a été installé correctement.

5. Critères de vérification (pour les systèmes de VE vérifiables individuellement ou complètement)

Chacun des sous-chapitres 5.1 à 5.6 correspond à une vérification externe du système de VE. Si le résultat de la vérification est positif, les organisations responsables établissent une pièce justificative à l'attention du canton qui les a mandatées pour effectuer la vérification. Le canton joint la pièce justificative à la demande d'approbation qu'il présente à la ChF. Les pièces justificatives à produire sont énumérées au chapitre 6.

5.1. Vérification du protocole cryptographique

E1.10	Critères de vérification: le protocole doit être conforme à l'objectif de sécurité et aux hypothèses de confiance figurant dans le modèle abstrait décrit au chapitre 4. Pour cela, il doit exister une preuve cryptographique et une preuve symbolique. En ce qui concerne les composants cryptographiques fondamentaux, les preuves peuvent être apportées sur la base des hypothèses de sécurité généralement admises (par exemple random oracle model, decisional Diffie-Hellman assumption, Fiat-Shamir heuristic). Le protocole doit se fonder si possible sur des protocoles éprouvés.
E1.20	Compétences: les preuves doivent être apportées ou vérifiées par des institutions hautement spécialisées. Le choix d'une organisation doit être avalisé au préalable par la ChF. La procédure à suivre est la suivante: 1. Le canton signale une modification du protocole à la ChF. Il peut proposer une institution, voire une personne, susceptible de procéder à la vérification. 2. La ChF examine la proposition. 3. La ChF fait part de sa décision au canton. Dans le cas de systèmes de VE vérifiables individuellement, il est possible de recourir à des protocoles simples si les hypothèses de confiance sont solides. La ChF peut alors se passer d'une organisation externe.
E1.30	Durée de validité d'une pièce justificative: la première mise en service doit être précédée d'une vérification complète. Le protocole doit subir une nouvelle vérification s'il est modifié et si la recherche fait émerger de nouvelles connaissances importantes concernant la sécurité des éléments cryptographiques utilisés.

5.2. Vérification des fonctionnalités du VE

E2.10	Critères de vérification: les fonctionnalités du VE doivent répondre aux exigences énumérées aux chapitres 2, 3 et 4, mais aussi contribuer de façon appropriée à la réalisation des objectifs fixés. Il se peut qu'il faille recourir à un protocole au sens de l'art. 3 ou 4. Il s'agit de garantir la mise en œuvre, à titre de mesures de sécurité, des *Security Functional Requirements* (SFR) figurant dans le profil de protection (PP) de l'office fédéral allemand de la sécurité des techniques de l'information (BSI), ou la mise en œuvre de moyens équivalents. Les fonctionnalités du VE doivent être vérifiées sur la base des critères principaux EAL2 des Critères communs (Common Criteria [CC]).
E2.20	Compétences: la vérification doit être effectuée par une institution accréditée par le Service d'accréditation suisse (SAS).
E2.30	Durée de validité d'une pièce justificative: les fonctionnalités du VE doivent être soumises à une nouvelle vérification lors de chaque modification significative, notamment en cas de modification du protocole cryptographique.

5.3. Vérification de l'infrastructure du VE et de l'exploitation

E3.10	Critères de vérification: le système de VE et son exploitation doivent répondre aux exigences énumérées aux chapitres 2, 3 et 4, mais aussi contribuer de façon appropriée à la réalisation des objectifs fixés. La sécurité de l'information concernant le système de VE et son exploitation doit être garantie par l'installation, l'implémentation, l'exploitation, la surveillance, la supervision, la maintenance et l'amélioration d'un système de management de la sécurité de l'information (SMSI) au sens de la norme ISO/IEC 27001:2005 (Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences). Le champ d'application du SMSI doit englober toutes les unités organisationnelles de l'exploitant qui sont responsables du système de VE sur les plans juridique, administratif et opérationnel.
E3.20	Compétences: l'efficacité et l'adéquation du SMSI doivent être attestées par la présentation du certificat établi par un organisme ayant procédé à la certification du SMSI conformément à la norme ISO/IEC 27001:2005. L'organisme de certification doit en outre attester que les exigences figurant aux chapitres 2, 3 et 4 sont remplies si elles ne sont pas déjà couvertes par l'audit au sens de la norme ISO/IEC 27001:2005. L'organisme de certification doit être accrédité par le SAS pour pouvoir effectuer des audits au sens de la norme ISO/IEC 27001:2005.
E3.30	Durée de validité d'une pièce justificative: les audits de renouvellement doivent être effectués aux intervalles prescrits dans la norme ISO 27001. Un certificat valable doit être présenté lors de chaque utilisation. Un audit de renouvellement doit aussi être effectué dans les cas où la décision est prise de renoncer à une mesure de surveillance qui sert à garantir le recours indépendant et sûr à des composants de contrôle, ou de modifier une telle mesure de manière significative. Si une nouvelle version de la norme ISO/IEC 27001:2005 est publiée, la preuve que le SMSI est valablement certifié conformément à la nouvelle version doit être apportée au plus tard à l'échéance du délai transitoire. Le champ d'application du SMSI ne peut pas être restreint à la faveur de cette nouvelle certification.

5.4. Vérification des composants de contrôle

E4.10	Critères de vérification: les composants de contrôle doivent répondre aux exigences énumérées au chapitre 4, mais aussi contribuer de façon appropriée à la réalisation des objectifs fixés. Les fonctions dont la fiabilité est déterminante pour le caractère concluant des preuves prévues dans le cadre de la vérifiabilité doivent être vérifiées en détail à l'aide du code source et du protocole cryptographique. Il s'agit de garantir la mise en œuvre, à titre de mesures de sécurité, des *Security Functional Requirements* (SFR) figurant dans le profil de protection (PP) de l'office fédéral allemand de la sécurité des techniques de l'information (BSI), ou la mise en œuvre de moyens équivalents. Les fonctionnalités du VE doivent être vérifiées sur la base des critères principaux EAL4 des Critères communs (Common Criteria [CC]). Les composants de base tels que le logiciel qui sert à l'utilisation sûre et indépendante de composants de contrôle, les systèmes d'exploitation utilisés ou les serveurs auxquels on a recours doivent correspondre aux meilleures normes existantes.
E4.20	Compétences: la vérification doit être effectuée par une institution accréditée par le SAS.
E4.30	Durée de validité d'une pièce justificative: les composants de contrôle doivent être soumis à une nouvelle vérification dans les cas suivants: – si l'on modifie le code source des fonctions dont la fiabilité est déterminante pour le caractère concluant des preuves prévues dans le cadre de la vérifiabilité; – si l'on renonce à utiliser des mécanismes qui servent à garantir le recours indépendant et sûr à des composants de contrôle, ou si l'on apporte des modifications significatives à des mécanismes de ce type; – si l'on recourt à un HSM, il faut, dans tous les cas, procéder, dans le cadre d'une vérification, à l'installation des fonctions dont la fiabilité est déterminante pour le caractère concluant des preuves prévues dans le cadre de la vérifiabilité. Si l'on utilise de nouvelles versions de composants de base (nouveaux serveurs, patches destinés à un système d'exploitation ou à un logiciel qui sert à garantir le recours indépendant et sûr à des composants de contrôle), il ne faut pas procéder à un nouveau contrôle pour autant que les composants de base correspondent toujours aux meilleures normes existantes.

5.5. Vérification de la protection contre les tentatives d'intrusion dans l'infrastructure du VE

E5.10	Critères de vérification: les personnes lançant une attaque depuis Internet ne doivent pas pouvoir pénétrer dans l'infrastructure du VE pour se ménager l'accès à des données importantes ou pour prendre le contrôle de fonctions importantes. Pour cela, une institution spécialisée doit tenter, à la faveur d'un test d'intrusion, de pénétrer dans l'infrastructure du VE, à l'aide de la documentation relative au système, en exploitant des failles connues que comportent les technologies utilisées. L'institution en question doit recevoir au moins, à titre de documentation, les documents relatifs à l'architecture, aux flux de données et aux technologies utilisées. Elle doit tester au moins les failles recensées dans le *Open Web Application Security Project* (OWASP).
E5.20	Compétences: la vérification doit être effectuée par une institution accréditée par le SAS.
E5.30	Durée de validité d'une pièce justificative: une nouvelle vérification doit être effectuée au bout de trois ans.

5.6. Vérification concernant les imprimeries

E6.10	Critères de vérification: l'imprimerie doit mettre en oeuvre l'exigence fixée au chiffre D2.20 en plus des dispositions figurant dans le catalogue de critères pour les imprimeries.
E6.20	Compétences: la vérification doit être effectuée par une institution accréditée par le SAS.
E6.30	Durée de validité d'une pièce justificative: une nouvelle vérification doit être effectuée au bout de deux ans. Une nouvelle vérification doit être effectuée dans les cas où la décision est prise de renoncer à une mesure ou de modifier une mesure de manière significative.

6. Pièces justificatives à l'appui des demandes d'octroi

E7.10	Le canton requérant envoie les pièces justificatives relatives aux vérifications (cf. art. 1, al. 2 et 3) qu'il a obtenues des institutions compétentes. La pièce justificative relative à la vérification visée au sous-chapitre 5.3 doit être un certificat valable au sens de la norme ISO/IEC 27001:2005.
E7.20	Le canton peut faire valoir la validité d'une pièce justificative sur plusieurs scrutins. Dans ce cas, il explique pourquoi il n'a pas procédé, s'agissant du scrutin actuel, à une répétition de la vérification correspondante. Il indique toutes les modifications apportées au système de VE, de même que les modifications prévues, jusqu'au moment du scrutin. Il montre ainsi qu'il s'agit de modifications mineures qui n'ont pas d'impact négatif sur l'évaluation des risques.
E7.30	Le canton remet tous les protocoles des tests qui ont résulté de la mise en œuvre du schéma de test (ch. B5.10). Il s'engage à remettre des protocoles de tests supplémentaires au cas où un test serait mené peu avant le scrutin.
E7.40	Le canton remet son actuelle évaluation des risques et s'engage à informer immédiatement qui de droit de tout changement dans l'estimation des risques. Tous les risques qui menacent la réalisation des objectifs de sécurité doivent être identifiés moyennant une évaluation des risques. Il faut de plus évaluer les risques qui concernent l'environnement du VE au sein de l'administration et dans le public. L'évaluation doit être menée selon une méthode comprenant les activités suivantes: – identification des risques; – analyse des risques; – évaluation des risques. Les détails de la méthode utilisée et les critères de tolérance de risques imposés par le canton doivent être documentés. Pour les risques qui découlent de l'exploitation du système de VE, il faut, lors l'identification des risques pour des systèmes vérifiables individuellement ou complètement, respecter en tous points les exigences méthodiques de la norme ISO/IEC 27001:2005.