Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF

Section des droits politiques

Annexe à l'ordonnance de la ChF du 13 décembre 2013 sur le vote électronique (OVotE, RS 161.116)

Exigences techniques et administratives applicables au vote électronique

Version : 2.0
Entrée en vigueur : 1.7.2018

Table des matières

1. Généralités

1.1. Documents de référence

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

1.1.2 Ordonnance du 24 mai 1978 sur les droits politiques (ODP; RS 161.11)

1.1.3 « Vote électronique : catalogue de critères pour les imprimeries » (document établi par la Chancellerie fédérale)

1.1.4 Common criteria protection profile for basic set of security requirements for online voting products, version 1.0 (BSI-CC-PP-0037-2008)

1.1.5 Norme ISO/IEC 27001:2013

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

1.1.7 eCH-0059: Norme d'accessibilité, version 2.0, 13.04.2011

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 suisse 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 Deutschland https://www.bsi.bund.de
Normes eCH	Association eCH Mainaustrasse 30 Case postale CH-8034 Zurich http://www.ech.ch

1.2. Sigles

BSI	Office fédéral allemand de la sécurité des techniques de l'information (*Bundesamt für Sicherheit in der Informationstechnik*)
CC	Critères communs (*common criteria*)
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 (*protection profile*)
SAS	Service d'accréditation suisse
SFR	Exigences fonctionnelles de sécurité (*security functional requirements*)

1.3. Définitions

1.3.1 Authentification

1.3.1.1 Données d'authentification client

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. 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 authentifie l'expéditeur d'un suffrage en tant qu'électeur. Les données d'authentification client doivent être difficiles à découvrir.

1.3.1.2 Données d'authentification serveur

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

1.3.1.3 Message d'authentification

Ensemble des informations qu'une plate-forme utilisateur envoie à l'infrastructure après l'introduction des données d'authentification client pour que l'infrastructure authentifie l'expéditeur d'un suffrage en tant qu'électeur. En pratique, il doit être impossible de générer un message d'authentification sans connaître les données d'authentification client.

1.3.2 Parties du système

1.3.2.1 Système

Terme générique recouvrant les fonctionnalités et l'infrastructure. La partie client du système est la partie qui comprend la plate-forme utilisateur et le logiciel client gérant les fonctionnalités. La partie serveur du système est la partie qui comprend la plate-forme serveur et le logiciel serveur gérant les fonctionnalités.

1.3.2.2 Infrastructure (I)

Matériel informatique, logiciels, éléments de réseau, locaux, services et moyens d'exploitation en tout genre nécessaires à l'exploitation des fonctionnalités côté serveur dans le respect de toutes les exigences de sécurité.

1.3.2.3 Fonctionnalités (F)

Logiciel serveur et logiciel client sur la plate-forme utilisateur qui ont été developpés spécialement pour le vote électronique afin que toutes les exigences de sécurité soient remplies.

1.3.2.4 Plate-forme utilisateur

Appareil multifonctionnel programmable qui est relié à Internet et qui sert à voter. Il s'agit généralement d'un ordinateur standard, d'un ordiphone ou d'une tablette tactile.

1.3.3 Suffrage

1.3.3.1 Suffrage tel qu'il a été exprimé par l'électeur sur la plate-forme utilisateur

Suffrage dont le contenu correspond à la saisie que le votant a effectuée sur la plate-forme utilisateur et qui n'a en particulier pas été manipulé depuis ce moment. Il corrrespond toujours à la volonté du votant, à moins que ce dernier se soit trompé lors de la saisie.

1.3.3.2 Suffrage enregistré

Suffrage enregistré une fois que l'infrastructure a pris connaissance du vote définitif.

1.3.3.3 Suffrage partiel

Projet, contre-projet ou question subsidiaire dans le cas d'une votation; choix d'une liste ou choix d'un candidat dans une liste dans le cas d'une élection.

1.3.3.4 Suffrage exprimé conformément à la procédure prévue par la système

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'authentification 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.

1.3.4 Appréciation des risques

Terme générique recouvrant les activités suivantes, qui doivent être effectuées successivement: identifier les risques, analyser les risques et estimer les risques.

1.3.5 Exploitant du système

Organisation (autorité ou entreprise privée) qui assume, lors d'un scrutin, l'entière responsabilité de la gestion de tous les aspects techniques du vote. Elle met à disposition le personnel, l'organisation et l'infrastructure nécessaires. Toutes les activités de direction de nature technique, administrative et juridique qui sont menées par l'exploitant du système constituent l'exploitation. L'exploitant du système travaille sous les ordres du responsable cantonal.

1.3.6 Données et informations classifiées

1.3.6.1 Données et informations confidentielles

Données et informations dont seules certaines personnes dont le nom est connu peuvent prendre connaissance.

1.3.6.2 Données et informations secrètes

Données et informations confidentielles dont personne ne peut prendre connaissance. En font partie au moins les données et les informations qui, prises dans leur intégralité, permettent de violer le secret du vote ou d'établir des résultats partiels de manière anticipée. La présente définition peut déroger à d'autres normes.

2. Exigences concernant l'aménagement des processus élémentaires

Les chiffres ci-après regroupent les exigences concernant l'aménagement des processus élémentaires. La colonne de droite indique lors de quel contrôle l'exigence considérée joue un rôle important (I: contrôle de l'infrastructure et de l'exploitation; F: contrôle des fonctionnalités).

2.1. Procédure de vote

2.1.1	Le système doit être convivial. La navigation doit se faire selon des schémas connus.	F
2.1.2	L'accessibilité du système client doit être contrôlée conformément à la norme eCH-0059 (version 2.0) par un service dont les compétences techniques sont reconnues par la Chancellerie fédérale.	F
2.1.3	Les votants déclarent avoir pris connaissance des règles du vote électronique et de leurs responsabilités.	F
2.1.4	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 du message qu'il a reçu.	F
2.1.5	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
2.1.6	Le votant saisit son suffrage sur la plate-forme utilisateur et l'envoie dans l'urne électronique au moyen des données d'authentification client.	F
2.1.7	L'apparence du système client ne doit pas influencer le votant dans son choix.	F,I
2.1.8	Le votant peut modifier son suffrage jusqu'au moment où il décide de l'exprimer de façon définitive. Le canal de vote conventionnel reste à sa disposition jusqu'à ce moment.	F
2.1.9	La navigation ne doit pas inciter à voter de manière hâtive ou irréfléchie.	F
2.1.10	Le système 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

2.1.11	Le système offre à l'électeur la possibilité d'interrompre à tout moment le processus de vote sans pour autant perdre le droit de voter.	F,I
2.1.12	Le système n'offre au votant aucune fonction permettant d'imprimer le suffrage.	F
2.1.13	Le votant doit pouvoir constater sur la plate-forme utilisateur que son suffrage a été transmis avec succès. Il se voit confirmer que le suffrage exprimé est bien parvenu à destination.	F,I
2.1.14	Après le vote, le votant ne doit recevoir aucune information sur le suffrage exprimé.	F
2.1.15	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 des autres paramètres du système

2.2.1	Le registre des électeurs est importé dans l'infrastructure.	F,I
2.2.2	Les questions du scrutin (par exemple les objets soumis au vote ou les listes de candidats) pour tous les niveaux du système fédéraliste et arrondissements électoraux concernés sont importées et enregistrées dans l'infrastructure.	F,I
2.2.3	Les données d'authentification serveur de chaque électeur sont préparées et enregistrées dans l'infrastructure.	F
2.2.4	En cas de besoin, les données d'authentification client de chaque électeur sont préparées et enregistrées temporairement dans l'infrastructure. (Cela n'est nécessaire que dans les cas où aucun moyen d'authentification externe n'est utilisé).	F
2.2.5	Les clés cryptographiques utilisées sont préparées et enregistrées dans l'infrastructure.	F
2.2.6	L'exploitant du système définit les paramètres techniques pertinents pour la réalisation d'un scrutin.	I

2.3. Informations et soutien

2.3.1	Le responsable cantonal élabore à l'attention des citoyens une stratégie d'information sur le vote électronique.	I
2.3.2	La stratégie garantit que les informations ont été autorisées par les organes compétents.	I
2.3.3	Des conseils, des règles concernant le vote et des informations sur la responsabilité des électeurs peuvent être consultés sur Internet. Ils doivent contribuer à ce que l'électeur ne vote pas de manière hâtive ou irréfléchie.	F,I
2.3.4	L'électeur reçoit des explications compréhensibles sur les mesures de sécurité, ce qui renforce la confiance dans le vote électronique.	F
2.3.5	L'électeur reçoit des explications sur les points auxquels il doit faire attention afin de pouvoir voter en toute sécurité.	F
2.3.6	L'électeur reçoit des explications sur la procédure à suivre pour effacer le suffrage dans toutes les mémoires de la plate-forme utilisateur employée pour voter.	F
2.3.7	L'électeur peut demander un soutien technique.	I
2.3.8	Les vérificateurs, par exemple une commission de vérification, doivent être informés et formés de manière à connaître les processus qui sous-tendent l'exactitude des résultats, 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 déchiffrement et le dépouillement). Ils doivent être en mesure de comprendre les processus et leur signification.	I

2.4. Préparation à l'impression du matériel de vote

2.4.1	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
2.4.2	Le fichier nécessaire à l'impression du matériel de vote est préparé; les données d'authentification client y sont éventuellement intégrées.	F
2.4.3	Le fichier nécessaire à l'impression est transmis à l'imprimerie.	F,I

2.5. Ouverture et fermeture du canal de vote électronique

2.5.1	L'exploitant du système initialise le système. (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[1].)	I
2.5.2	Le canal de vote électronique est ouvert pour les électeurs.	F,I
2.5.3	Il doit être interdit d'ouvrir ou de fermer prématurément le canal de vote électronique.	I
2.5.4	Le canal de vote électronique est fermé pour les électeurs.	F,I

2.6. Contrôle de la conformité et enregistrement des suffrages définitifs

2.6.1	Au moyen du message d'authentification reçu et des données d'authentification serveur, le système authentifie l'expéditeur du suffrage exprimé en tant que personne autorisée à voter.	F
2.6.2	Le système vérifie si un suffrage a déjà été déposé dans l'urne électronique sous le nom du même électeur.	F
2.6.3	Quand le suffrage a été exprimé conformément à la procédure prévue par le système, ce dernier enregistre le suffrage dans l'urne électronique et informe l'électeur du succès du vote. Les suffrages non valables ne sont pas enregistrés dans l'urne électronique. Un suffrage qui n'a pas été exprimé conformément à la procédure prévue par le système n'est pas enregistré dans l'urne électronique. (Tout comme l'expression conforme à la procédure prévue par le système, la bonne forme d'un suffrage[2] est un critère du succès du vote.)	F

2.7. Dépouillement de l'urne électronique

2.7.1	Après la fermeture du canal de vote électronique, mais au plus tôt le dimanche au cours duquel a lieu la votation, le responsable cantonal lance le déchiffrement des suffrages contenus dans l'urne électronique.	F,I
2.7.2	*Abrogé*[3]	
2.7.3	Le responsable cantonal rédige un procès-verbal à propos du processus de déchiffrement des suffrages et du dépouillement.	I

[1] L'urne électronique désigne la zone de stockage dans laquelle les suffrages exprimés sont déposés jusqu'au déchiffrement et au dépouillement.

[2] Un suffrage bien formé est une manière précise de remplir un bulletin de vote. Il est possible de définir à l'avance si et comment les suffrages qui ne sont pas bien formés 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 « blanc » peuvent avoir une influence sur le résultat du scrutin. Une réponse telle que « je ne veux pas voter » aurait pour conséquence que le suffrage ne serait pas bien formé. Il faut définir avant le scrutin si les suffrages qui ne sont pas bien formés pourront 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.

[3] Nouvelle teneur selon ch. II de la modification du 30 mai 2018 de l'ordonnance de la ChF sur le vote électronique (RO *2018* 2279).

2.7.4	Entre le déchiffrement des suffrages et la transmission des résultats du scrutin, tout accès au système ou à l'un de ses composants doit être le fait d'au moins deux personnes; il doit être consigné par écrit et pouvoir être contrôlé par des représentants de l'autorité compétente.	F,I
2.7.5	Les résultats du scrutin sont transmis 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
2.7.6	Le système met les informations nécessaires à disposition pour qu'on puisse constater, au moyen d'une carte de légitimation, si l'électeur concerné qui veut voter en personne ou par correspondance a déjà voté par voie électronique. Si des essais de vote électronique sont menés avec un électorat très limité (par exemple avec des Suisses de l'étranger uniquement), il n'est pas permis, dans le souci de protéger le secret du vote, de remettre à un service extérieur à l'infrastructure des listes qui permettraient d'identifier les électeurs qui ont voté par voie électronique. Au lieu de cela, il faut confirmer, sur demande, si un électeur particulier a voté. Autre possibilité: le système peut générer une liste contenant des codes anonymes qui correspondent aux cartes de légitimation utilisées.	F,I
2.7.7	Le déchiffrement et le dépouillement des suffrages ont lieu en présence de parties ou d'organes indépendants qui peuvent ainsi attester du bon déroulement de la procédure.	I

2.8. Données confidentielles ou secrètes

2.8.1	Il faut garantir que ni des collaborateurs ni des personnes externes n'auront connaissance de données qui permettent d'établir un lien entre l'identité des votants et le suffrage qu'ils auront exprimé.	F,I
2.8.2	Il faut garantir que ni des collaborateurs ni des personnes externes n'auront connaissance, avant le moment du déchiffrement des suffrages, de données permettant d'établir des résultats partiels de manière anticipée.	F,I
2.8.3	Il faut garantir que les résultats du scrutin seront traités confidentiellement entre le moment du déchiffrement des suffrages et le moment de la publication.	F,I
2.8.4	Il faut garantir que les données permettant de constater si des électeurs ont voté par voie électronique seront traitées confidentiellement.	F,I
2.8.5	Il faut garantir que les données personnelles issues du registre des électeurs seront traitées confidentiellement.	F,I
2.8.6	Il faut garantir que les suffrages seront aussi traités confidentiellement après le dépouillement.	I
2.8.7	Il faut garantir que les résultats du scrutin seront traités confidentiellement au cas où une faible part seulement des électeurs d'un arrondissement électoral auraient le droit de voter par voie électronique.	F,I
2.8.8	Après la validation, l'exploitant du système détruit, conformément à un processus consigné par écrit, toutes les données créées dans le cadre du vote électronique qui se rapportent aux suffrages enregistrés et qui sont classifiées confidentielles ou secrètes.	I

2.9. Devoirs du responsable cantonal

	Le responsable cantonal est la personne physique qui assume l'entière responsabilité d'un scrutin par voie électronique. Il doit en particulier: a. définir, approuver et mettre en œuvre les mesures concernant la sécurité des informations (directive en matière de sécurité des informations, critères de base pour la gestion des risques en matière de sécurité des informations, champ d'application et limites de la gestion des risques en matière de sécurité des informations, organisation de la gestion des risques); b. rédiger le contrat relatif à l'exécution du scrutin et fixer les exigences en matière de surveillance et de vérification; c. charger un exploitant de système de l'exécution du scrutin; d. fixer les délais applicables à l'exécution d'actions et d'opérations critiques, et e. surveiller et vérifier l'exécution du scrutin par l'exploitant de système qui a été mandaté. Il peut être impliqué dans le déroulement d'un scrutin par voie électronique.	I

3. Exigences de sécurité

Les objectifs de sécurité (voir art. 3, 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 appréciation méthodique des risques (voir art. 3, al. 2, et ch. 6.4), apporter la preuve que les risques sont suffisamment faibles.

Il est possible d'identifier un risque au moyen de menaces et de vulnérabilités du système. Il y a risque quand une vulnérabilité du système peut être exploitée par une menace et quand 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.

Le ch. 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 vulnérabilités identifiées du système, ils doivent être concrétisés et complétés si nécessaire.

Les exigences de sécurité des ch. 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 vulnérabilités du système 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 ch. 2). Ceci aide à comprendre à quelles vulnérabilités il faut prêter attention lors de la mise en œuvre d'une exigence de sécurité. D'autres vulnérabilités du système doivent être identifiées, et les exigences de sécurité doivent s'y rapporter de manière analogue.

Le ch. 3.15 comprend les exigences de sécurité du profil de protection (PP) du Bundesamt für Sicherheit in der Informationstechnik (BSI), 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 ch. 3.15.

3.1. Menaces

	Description	Objectif de sécurité concerné
3.1.1	Un logiciel malveillant modifie le suffrage sur la plate-forme de l'utilisateur	Exactitude des résultats
3.1.2	Un attaquant détourne le suffrage au moyen d'un empoisonnement du cache DNS[4].	Exactitude des résultats
3.1.3	Un attaquant modifie le suffrage au moyen de la technique de « l'homme du milieu »[5].	Exactitude des résultats
3.1.4	Un attaquant envoie des bulletins de vote corrompus au moyen d'une attaque MITM.	Exactitude des résultats
3.1.5	Un administrateur manipule le logiciel, qui n'enregistre alors plus les suffrages.	Exactitude des résultats
3.1.6	Un administrateur modifie des suffrages.	Exactitude des résultats
3.1.7	Un administrateur ajoute des suffrages dans l'urne électronique.	Exactitude des résultats
3.1.8	Une organisation criminelle pénètre dans le système pour falsifier le résultat.	Exactitude des résultats (ici en relation avec les ch. 3.1.5/6/7/9)
3.1.9	Un administrateur copie du matériel de vote et l'utilise.	Exactitude des résultats
3.1.10	Un logiciel malveillant installé sur la plate-forme de l'utilisateur envoie le suffrage de ce dernier à une organisation criminelle.	Protection du secret du vote et impossibilité d'établir des résultats partiels de manière anticipée
3.1.11	Le suffrage est détourné au moyen d'un empoisonnement du cache DNS.	Protection du secret du vote et impossibilité d'établir des résultats partiels de manière anticipée
3.1.12	Un attaquant lit le suffrage au moyen d'une attaque MITM.	Protection du secret du vote et impossibilité d'établir des résultats partiels de manière anticipée
3.1.13	Un administrateur utilise la clé et déchiffre des suffrages non anonymisés.	Protection du secret du vote et impossibilité d'établir des résultats partiels de manière anticipée
3.1.14	Le secret du vote est violé lors de la vérification de l'exactitude du traitement / dépouillement.	Protection du secret du vote et impossibilité d'établir des résultats partiels de manière anticipée
3.1.15	Un administrateur consulte de manière anticipée des suffrages non chiffrés.	Protection du secret du vote et impossibilité d'établir des résultats partiels de manière anticipée

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

[5] L'homme du milieu désigne 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 s'immisce 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 consulter les informations à loisir et même les manipuler.

3.1.16	Une organisation criminelle pénètre dans le système pour violer le secret du vote ou pour établir des résultats partiels de manière anticipée.	Protection du secret du vote et impossibilité d'établir des résultats partiels de manière anticipée (ici en relation avec des menaces, ch. 3.1.13/14/15).
3.1.17	Un logiciel malveillant installé sur l'ordinateur de l'électeur empêche ce dernier de voter.	Disponibilité des fonctionnalités
3.1.18	Un logiciel malveillant influence des électeurs pendant qu'ils se forgent une opinion.	Protection des informations destinées aux électeurs
3.1.19	Une organisation criminelle mène une attaque du type « déni de service » (DOS)[6].	Disponibilité des fonctionnalités
3.1.20	Un administrateur configure mal le système; le dépouillement ne peut pas se faire.	Disponibilité des fonctionnalités
3.1.21	Un administrateur manipule le site Internet d'information / le portail de vote et sème la confusion dans l'esprit des électeurs.	Protection des informations destinées aux électeurs
3.1.22	Après le déchiffrement, un administrateur cherche les bulletins de vote remplis selon des instructions de tiers (n'est possible que pour les élections).	Impossibilité d'obtenir, dans l'infrastructure, des preuves relatives au comportement de vote
3.1.23	Une organisation criminelle pénètre dans le système pour en perturber l'exploitation, pour manipuler les informations destinées aux électeurs ou pour obtenir des preuves relatives au comportement de vote des électeurs.	Disponibilité des fonctionnalités, protection des informations destinées aux électeurs, impossibilité d'obtenir, dans l'infrastructure, des preuves relatives au comportement de vote (ici en relation avec des menaces, ch. 3.1.20/21/22)
3.1.24	Un administrateur vole les données concernant les adresses des électeurs.	Protection des informations concernant les électeurs

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

3.2.1	Un système de monitoring de l'infrastructure 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 - 2.2.1/2/3/4/5/6 - 2.3.3/4/5/ - 2.5.2/3/4 - 2.6.1/2/3 - 2.7.1/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
3.2.2	Des procès-verbaux des suffrages entrés doivent être établis dans l'infrastructure 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 exprimés conformément à la procédure prévue par le système. En cas de divergence, ils doivent servir à en chercher la cause.	F,I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/20/22/23

[6] Un déni de service (denial of service, DOS) correspond à l'impossibilité d'accéder, lors du traitement numérique de données, à un service qui devrait en principe être disponible.

3.2.3	Des procès-verbaux des accès au système qui soient impossibles à manipuler doivent être établis dans l'infrastructure 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 exprimés conformément à la procédure prévue par le système 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 - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
3.2.4	Les suffrages exprimés et dépouillés par voie électronique doivent, à des fins d'établissement de la plausibilité des résultats, être comparés avec les procès-verbaux des suffrages entrés dans l'infrastructure.	F,I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/20/22/23
3.2.5	Il faut garantir que les suffrages et les données qui prouvent le bon fonctionnement de la procédure de dépouillement des suffrages sont, en cas de panne, enregistrés sans altérations dans l'infrastructure.	F,I - 2.1.6/13 - 2.2.1/2/3/4/5/6 – 2.4.2 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/20/23
3.2.6	Il doit être possible, au moyen de données d'authentification, d'envoyer des suffrages de contrôle qui ne sont attribués à aucun électeur. Le contenu de ces suffrages de contrôle doit être consigné dans un procès-verbal. Les suffrages de contrôle dépouillés doivent être comparés avec les procès-verbaux des suffrages de contrôle envoyés. Il faut garantir que les suffrages de contrôle seront traités dans toute la mesure du possible de manière similaire aux suffrages exprimés conformément à la procédure prévue par le système; il faut en même temps garantir qu'ils ne seront pas comptabilisés.	F,I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/4 - 2.8.1/2/3/4/5/6/8 - 3.1.1/2/3/4/5/6/7/8/9/13/14/15/16/17/18/21/23
3.2.7	La disponibilité de l'infrastructure doit être contrôlée et consignée dans un procès-verbal à intervalles déterminés.	I - 3.1.19/20/23
3.2.8	Des méthodes statistiques doivent pouvoir être utilisées pour l'établissement de la plausibilité des résultats dans la mesure où la base de données le permet.	I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4 - 2.8.1/2/3/4/5/6/8 - 3.1.5/6/7/8/9/13/14/15/16/20/22/23
3.2.9	Les parties du système de vote accessibles par Internet doivent être régulièrement actualisées moyennant un processus documenté afin que les vulnérabilités identifiées soient éliminées.	I - 3.1.5/6/7/8/9/13/14/15/16/19/21/22/23/24

3.3. Utilisation de mesures cryptographiques et gestion des clés

3.3.1	Les certificats électroniques doivent être gérés selon les meilleures pratiques.	I 2.2.13 - 2.2.5/6 - 2.4.3 - 2.7.5 - 3.1.2/3/4/8/12/16/20/23
3.3.2	Des mesures cryptographiques efficaces qui correspondent aux dernières évolutions de la technique doivent garantir l'intégrité des données sous-tendant l'exactitude des résultats.	I,F - 2.1.6 – 2.2.1/3/4/5/6 - 2.4.3 - 2.5.1 - 2.6.1/2/3 - 2.7.1/2/5/6 - 3.1.5/6/7/8/9/14/16
3.3.3	Des mesures cryptographiques efficaces qui correspondent aux dernières évolutions de la technique doivent garantir la confidentialité des données sous-tendant le secret du vote et l'absence de résultats partiels anticipés.	I,F - 2.1.6 - 2.2.1/3/4/5/6 - 2.4.2/3 - 2.5.1 - 2.6.1/2/3 - 2.7.1/2/5/6 - 2.8.1/2/3/4/6/7/8 3.1.12/13/14/15/16

3.3.4	Les suffrages ne doivent en aucun cas être enregistrés ou transmis sous une forme non chiffrée entre le moment de leur saisie et celui du dépouillement.	I,F 2.1.6/13 - 2.4.2/3 - 2.6.1/2/3 - 2.7.1 - 2.8.1/2 - 3.1.3/4/5/6/7
3.3.5	Chiffrement et signature sont de rigueur lors de l'échange des données des registres électoraux et des résultats. La signature et l'intégrité des données doivent être vérifiées au moment de la réception de telles données.	I,F 2.2.1/2 - 2.4.3 - 2.7.5 - 2.8.3/7
3.3.6	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, ECRYPT, SCSE). La signature électronique doit satisfaire aux exigences d'une signature électronique avancée au sens de la SCSE. 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
3.3.7	Les électeurs reçoivent les informations nécessaires au contrôle de l'authenticité du site Internet utilisé pour voter 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 2.1.13 - 2.2.5 - 3.1.2/3/4/11/12

3.4. Echange d'informations électronique et physique sûr

3.4.1	Tous les composants de l'infrastructure doivent être exploités dans une zone réseau séparée. Cette zone doit être protégée par rapport au reste du réseau au moyen d'un contrôle de routage adéquat.	I 2.8.1/2/3/4/5/6/7 - 3.1.6/7/8/9/13/14/15/ 16/20/22/23/24
3.4.2	Les systèmes doivent être protégés contre des attaques (quels que soient le type ou la provenance des menaces).	I
3.4.3	Au sein de la zone réseau dans laquelle l'infrastructure est exploitée, le système de dépouillement des suffrages doit être exploité dans une sous-zone réseau propre qui doit être séparée des autres sous-zones réseau de façon sécurisée.	I 7.2.1/2/3/4/5/6/7 - 2.8.1/2/3/4/5/6/7 3.1.6/7/8/9/13/14/ 15/16/20/22/23
3.4.4	Les traitements en rapport avec le vote par voie électronique doivent être clairement séparés de l'ensemble des autres applications.	I 2.8.1/2/3/4/5/6/7 - 3.1.6/7/8/9/13/14/15/16/ 20/22/23/24

3.5. Tests des fonctionnalités

3.5.1	Un schéma de test doit garantir que les fonctionnalités sont conformes 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 procès-verbaux et de la rédaction des rapports. 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.	I,F

3.6. Directive concernant la sécurité des informations

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

3.7. Organisation de la sécurité des informations

3.7.1	Tous les rôles et les responsabilités pour l'exploitation du système doivent être précisément définis, attribués et communiqués.	I - 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23
3.7.2	Un processus d'autorisation doit être mis en place pour toute installation de moyens de traitement des informations dans l'infrastructure.	I - 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23
3.7.3	Les risques liés à des tiers (mandataires en tout genre tels que fournisseurs, prestataires, etc.) doivent être identifiés et réduit autant que nécessaire moyennant des conventions contractuelles adéquates. Le respect de ces conventions doit être surveillé et vérifié de manière appropriée pendant leur durée de validité.	I

3.8. Gestion des ressources matérielles ou immatérielles

3.8.1	Toutes les ressources matérielles ou immatérielles pertinentes qui correspondent à un actif au sens de la norme ISO/IEC 27001:2013 et qui sont en rapport avec le vote électronique (organisation en tant que tout, en particulier les processus organisationnels et les informations traitées dans le cadre de ces processus; le personnel; les supports de données; les installations de traitement des données de l'infrastructure; les locaux de l'infrastructure) doivent être saisies dans un inventaire. Une liste recensant le personnel doit être dressée. L'inventaire et la liste du personnel doivent être tenus à jour. Chaque ressource matérielle ou immatérielle doit être attribuée à une personne qui en prend la responsabilité.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.8.2	L'utilisation licite de ressources matérielles ou immatérielles doit être définie.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.8.3	Des directives régissant la classification des informations doivent être édictées et communiquées.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.8.4	Des procédures régissant le marquage et la gestion des informations doivent être définies.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24

3.9. Fiabilité du personnel

3.9.1	Pour garantir que le personnel ne menacera pas la sécurité 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 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23
3.9.2	Les décideurs du personnel doivent assumer l'entière responsabilité pour garantir que le personnel ne menacera pas la sécurité.	I 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23

3.9.3	L'ensemble du personnel doit posséder une sensibilité marquée en matière de sécurité des informations. A cette fin, il faut mettre en place et exploiter un programme de formation et d'entraînement qui soit adapté aux tâches.	I 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23

3.10. Sécurité physique et sécurité liée à l'environnement

3.10.1	Les périmètres de sécurité des différents locaux de l'infrastructure (locaux pour les différents groupes de personnes du personnel, locaux pour les serveurs, etc.) doivent être clairement définis.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/21/22/23/24
3.10.2	Des autorisations d'accès doivent être définies, créées et contrôlées de manière adéquate pour l'accès physique aux différents locaux de l'infrastructure.	I 3.1.5/6/7/8/9/13/14/ 15/16/23
3.10.3	Pour garantir la sécurité des appareils à l'intérieur et à l'extérieur des locaux de l'infrastructure, il faut définir des directives et des procédures adéquates ainsi que surveiller et vérifier qu'elles sont respectées.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/21/22/23/24

3.11. Gestion de la communication et de l'exploitation

3.11.1	Les étapes de l'utilisation doivent être décrites de manière détaillée pour les principales activités du système.	I 2.2.1/2/3/4/5/6 - 2.3.8 - 2.4.2/3 - 2.5.1/2/3 - 2.7.1/2/3/4/5/6/7 - 3.1.20
3.11.2	Les systèmes de production peuvent uniquement être modifiés conformément à une procédure documentée de gestion des modifications.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.11.3	Les obligations et les domaines de responsabilité doivent être répartis de telle sorte que les risques émanant du personnel qui sont liés à l'exploitation et à la communication soient réduits de façon à ce qu'ils ne constituent plus que des risques résiduels compatibles avec les critères de tolérance des risques.	I - 2.2.1/2/3/4/5/6 - 2.3.8 - 2.4.2/3 - 2.5.1/2/3 - 2.7.1/2/3/4/5/6/7 - 3.1.20
3.11.4	Des mesures de protection appropriées doivent être prises contre les logiciels malveillants.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.11.5	Il faut établir et mettre en œuvre un plan détaillé pour la sécurisation des données. Le bon fonctionnement de la sécurisation des données doit être vérifié à intervalles réguliers.	I 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.4.2 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/20/23
3.11.6	Des mesures adéquates doivent être définies et mises en œuvre pour assurer la protection du réseau et la sécurité des services du réseau.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.11.7	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 - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/9 - 3.1.13/14/15/16 - 3.1.22/23/24
3.11.8	Les mesures en rapport avec la surveillance et l'établissement des procès-verbaux de l'utilisation du système et des activités des administrateurs, mais aussi en rapport avec l'établissement des procès-verbaux des incidents, doivent être décrites de manière détaillée, mises en œuvre, suivies et vérifiées.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2/3 - 2.5.1/2/3/4 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23/24

3.12. Attribution, gestion et retrait des droits d'accès

3.12.1	Pendant le scrutin, il faut garantir que toute modification envoyée ultérieurement ne pourra être effectuée qu'en accord avec le responsable cantonal.	F,I - 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.4 - 3.1.5/6/7/8/20/23
3.12.2	L'accès à l'infrastructure et aux fonctionnalités doit être réglé et documenté en détail sur la base d'une appréciation des risques. Le principe dit des « quatre yeux » doit valoir dans les domaines présentant des risques élevés.	I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2 - 2.5.1 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.12.3	Il doit être impossible, sans disposer d'une autorisation en ce sens, de modifier des informations sur le portail du vote électronique ou sur des sites d'information concernant le vote électronique.	F,I 2.3.3/3/4/5/6 - 3.1.21/23
3.12.4	Pendant le scrutin, aucune intervention étrangère au vote en cours ne doit pouvoir être effectuée.	F,I 2.2.1/2/3/4/5/6 - 2.3.2/3/4/5/6 - 2.4.2/3 - 2.5.1/2/3/4 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/ 15/16/20/21/22/23/24
3.12.5	Il faut garantir qu'aucun des éléments des données d'authentification client ne pourra 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 – 2.1.5/6/15 - 2.2.3/4 - 2.4.1/2/3 - 2.6.1/2 - 2.7.1/2/4/5/6 - 2.8.1/4/5 - 3.1.5/6/7/8/9/13/14/15/16

3.13. Exigences applicables aux imprimeries

3.13.1	Les imprimeries doivent accomplir leurs tâches en respectant les dispositions figurant dans le catalogue de critères pour les imprimeries.	

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

3.14.1	Des procédures adéquates doivent être décrites de manière détaillée et mises en œuvre pour l'installation de logiciels sur les systèmes de production.	I 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24
3.14.2	Des procédures adéquates doivent être décrites de manière détaillée et mises en œuvre pour le traitement des vulnérabilités techniques. Une attention particulière doit être portée aux parties de l'infrastructure qui sont accessibles par Internet.	I - 3.1.5/6/7/8/9/13/14/ 15/16/19/20/21/22/23/24

3.15. Exigences découlant du profil de protection du BSI

Les exigences découlant du profil de protection du BSI [1.1.4] doivent être mises en œuvre en plus 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 l'OVotE, c'est cette dernière qui fait foi.

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

3.15.1	*OE.ElectionPreparation*[7] prévoit notamment que les électeurs vérifient les données figurant sur la liste des personnes autorisées à voter et peuvent, le cas échéant, demander que les données soient corrigées. En l'occurrence, cette exigence ne doit pas être mise en œuvre pour les électeurs.
3.15.2	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.
3.15.3	*OE.ServerRoom* prévoit que seuls les responsables électoraux ont le droit d'entrer dans la pièce abritant le serveur. Cette exigence peut être interprétée de manière moins stricte: seules des personnes désignées par le responsable cantonal peuvent entrer dans la pièce; elles sont surveillées.
3.15.4	*O.Correction* prévoit que les électeurs peuvent corriger leur suffrage aussi souvent qu'ils le souhaitent avant sa remise définitive. Cette exigence peut être assouplie de la façon suivante: les votants peuvent modifier leur suffrage jusqu'au moment où ils décident de l'exprimer de façon définitive (le ch. 2.1.8 prime.)
3.15.5	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).

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 de la présente ordonnance.

O.UnauthorisedVoter	F,I 2.1.5 - 2.2.1/2/3/4 - 2.4.2 - 2.6.1 - 3.1.7/8/9
O.Proof	F,I 2.1.12 - 3.1.22
O.IntegrityMessage	F – 2.1.6/13 – 2.2.5 – 2.4.3 – 3.1.2/3/4
O.SecrecyOfVoting	F – 2.1.6 – 2.2.5 – 2.8.1/2 – 3.1.12/13
O.SecretMessage	F - 2.1.6 - 2.2.5 - 2.8.1/4 - 3.1.9
O.AuthenticityServer	F,I - 2.1.6 - 2.2.5 - 2.4.2 - 3.1.2/3/4/12
O.ArchivingIntegrity	F,I - 2.2.5 - 2.7.2/3/4 - 3.1.6/7/8
O.ArchivingSecrecyOfVoting	F,I - 2.7.2 - 2.8.1/6/8 - 3.1.13/14/16/22
O.Abort	F - 2.1.11
O.EndingElection	F - 2.5.3/4 - 3.1.20
O.EndOfElection	F - 2.5.4 - 3.1.20
O.SecrecyOfVotingElectionOfficers	F - 2.7.2 - 2.8.1/6/7 - 3.1.13/14/16
O.IntegrityElectionOfficers	F - 2.5.1/2/4 - 2.7.4 - 3.1.5/6/7/8
O.IntermediateResult	F - 2.7.1 - 2.8.2/3 - 3.1.15/16
O.OverhasteProtection	F - 2.1.10
O.Correction	F - 2.1.8
O.Acknowledgement	F - 2.1.13 - 3.1.17
O.Failure	F,I - 2.2.6 - 2.5.1 - 3.1.19/20
O.Audit	F,I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9 - 3.1.13/14/15/16/19/20/21/22/23/24
O.OneVoterOneVote	F,I - 2.1.5/8/11/13/15 - 2.2.1/2/3/4 - 2.4.1 - 2.6.1/2/3 - 2.7.6 - 3.1.7/8/17
O.AuthElectionOfficers	F - 2.2.1/2/3/4/5/6 - 2.4.2 - 2.5.1/2/4 - 2.7.1/2/4/5 - 2.8.1/2/3/4/5/6/7

[7] Les exigences mentionnées ici, qui découlent du profil de protection, commencent soit par « O. », qui vient de « security objective », soit par « OE. », qui vient de « security objectives for the operational environment ».

O.StartTallying	F - 2.5.4 - 2.7.1/2 - 3.1.15/16
O.Tallying	F - 2.2.6 - 2.5.1 - 2.7.2 - 3.1.5/7/8 - 3.1.20
OE.ElectionPreparation	F,I - 2.2.1/2/3/4/5/6 - 2.3.1/3 - 2.4.2/3 - 2.5.1 - 2.8.1/2/3/4/5/6/7/8 - 3.1.7/8/20
OE.Observation	F - 2.1.6
OE.ElectionOfficers	I - 2.2.1/2/6 - 2.3.2 - 2.5.1/2/4 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/20/21/22/23/24
OE.AuthData	F,I - 2.2.1/2/3/4 - 2.4.2/3 - 2.8.1/5 - 3.1.8/9
OE.VoteCastingDevice	F,I - 2.1.3 - 2.3.3/4 - 3.1.1 - 3.1.10
OE.ElectionServer	I - 3.1.8 - 3.1.16 - 3.1.23
OE.Availability	I - 3.1.19
OE.ServerRoom	I - 3.1.5/6/7/8/9/13/14/15/16/23
OE.DataStorage	I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.4.2 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/3/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.8/20/23
OE.SystemTime	I - 2.1.6/13 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4 - 2.8.1/2/3/4/6/8 - - 3.1.5/6/7/8/9/13/14/15/16/20/22/23
OE.AuditTrailProtection	I - 2.1.6/13 - 2.2.1/2/3/4/5/6 - 2.5.1/2/4 - 2.6.1/2/3 - 2.7.1/2/4/5/6 - 2.8.1/2/3/4/5/6/7/8 - 3.1.5/6/7/8/9/13/14/15/16/19/20/21/22/23/24
OE.AuthenticityServer	F - 2.3.3/4/5 - 2.4.2 - 3.1.2/3/4/12
OE.ArchivingIntegrity	F,I - 2.2.5 - 2.7.2/3/4 - 3.1.6/7/8
OE.ArchivingSecrecyOfVoting	F,I - 2.7.2 - 2.8.1/6/8 - 3.1.13/14/16/22
OE.ProtectedCommunication	I - 3.1.5/6/7/8/9/13/14/15/16/22/23/24
OE.Buffer	F - 2.3.6

4. Vérifiabilité

Les art. 4 et 5 contiennent les dispositions consacrées à la vérifiabilité. Le présent chiffre expose ces dispositions d'une manière plus formelle afin d'expliciter les critères applicables aux deux formes de vérifiabilité.

Pour ce faire, le ch. 4.1 définit un modèle abstrait réduit pour décrire le déroulement d'un scrutin. Se fondant sur ce modèle, le ch. 4.2 contient des explications concernant l'art. 4 et des dispositions qui complètent ce dernier. Le ch. 4.3 présente le modèle abstrait complet. Le ch. 4.4, enfin, contient des commentaires concernant l'art. 5 et des dispositions qui complètent ce dernier.

4.1. Modèle abstrait réduit relatif à l'art. 4

Dans le modèle abstrait utilisé, un scrutin est défini par un protocole cryptographique[8] constitué par les échanges d'informations entre les composants du système suivants:

Electeurs / votants	Les électeurs reçoivent du système 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 avec le suffrage chiffré. Pour ce faire, elle utilise les paramètres publics qu'elle a reçus auparavant du système. Elle affiche au besoin, pour les votants, les messages envoyés par la partie serveur du système.
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 (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 chiffré. Il détermine si les suffrages ont été exprimés conformément à la procédure prévue, il déchiffre 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 vérification). Le système 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
- système ↔ imprimerie
- imprimerie → électeurs

Soit les composants du système et les canaux de communication sont fiables, soit ils ne le sont pas. Les composants du système qui sont fiables conservent de façon sécurisée toutes les données

[8] Un protocole cryptographique est un protocole doté de fonctions de sécurité cryptographiques qui sert à atteindre des objectifs de sécurité. Les protocoles cryptographiques sont implantés au niveau du modèle, si bien qu'ils ne contiennent pas de fonctions d'implémentation directes, mais uniquement des fonctions de sécurité abstraites.

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 le composant du système qui est prescrit dans la définition du canal.
Qui plus est, le modèle abstrait prévoit un attaquant qui peut corrompre tous les composants du système et les canaux de communication qui ne sont pas fiables et en prendre le contrôle. Les composants 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 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 » et « système ↔ 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 dans la mise en œuvre:

le système met en œuvre 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 composants du système et les canaux de communication sont fiables est justifiée par des mesures de sécurité correspondantes.

Le ch. 4.2 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 composants du système et aux canaux de communication considérés comme fiables dans le modèle abstrait.

4.2. Dispositions complémentaires concernant la vérifiabilité individuelle

4.2.1	(ad art. 4, al. 2) 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.
4.2.2	(ad art. 4, al. 2) Cette exigence doit être mise en oeuvre de telle sorte que le risque d'un achat de suffrages ne s'accroisse pas de manière significative par rapport au vote par correspondance.
4.2.3	(ad art. 4, al. 3) L'objectif consiste à empêcher que des composants 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.

4.2.4	(ad art. 4, 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 composants du système qui ne sont pas fiables, une preuve faisant croire aux votants que le suffrage qu'ils ont exprimé sur la plate-forme utilisateur a été enregistré en tant que suffrage exprimé conformément à la procédure prévue par le système. 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 %.
4.2.5	(ad art. 4, 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.
4.2.6	(ad art. 4, al. 5) Si les votants se servent d'un dispositif technique particulier 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.
4.2.7	(ad art. 4, al. 5) 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 non chiffrées ou non signées inhérentes à la référence de vérification 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.
4.2.8	(ad art. 4, al. 5) La partie serveur du système ne fait pas l'objet de dispositions supplémentaires. Lors de la mise en oeuvre des exigences relatives à l'aménagement des processus élémentaires et des exigences de sécurité (voir art. 2 et ch. 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 vérification 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.
4.2.9	(ad art. 4, al. 4) Le canal entre l'imprimerie et les électeurs ne peut être considéré comme fiable que si les informations sont remises par la Poste suisse, ou si les personnes concernées se les remettent en mains propres.

4.3. Modèle abstrait complet relatif à l'art. 5

Le modèle abstrait complet considère que le système 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 composants du système supplémentaires ci-après:

Composant de contrôle	Il interagit avec le système 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 une preuve attestant que les résultats ont été établis correctement.
Dispositif technique 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
- système ↔ 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. 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. 5 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 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
- 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 établir des résultats partiels de manière anticipée 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 dans la mise en œuvre: elle est régie par les dispositions applicables à la vérifiabilité individuelle.

Le ch. 4.4 met en relation les dispositions de l'art. 5 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 composants du système et aux canaux de communication considérés comme fiables dans le modèle abstrait.

4.4. Dispositions complémentaires concernant la vérifiabilité complète

4.4.1	(ad art. 5, 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.
4.4.2	(ad art. 5, al. 3) Forts des informations figurant dans la partie fiable du système (le suffrage chiffré 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 chiffrés 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 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 peuvent 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. 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.*
4.4.3	(ad art. 5, al. 3, let. b) L'objectif consiste à empêcher que des composants 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.
4.4.4	(ad art. 5, al. 3, let. c) La confidentialité des données relatives à une éventuelle référence de vérification ne peut donc dépendre, même au sein de l'infrastructure, que de la partie fiable du système.
4.4.5	(ad art. 5, al. 4) Le fait que le dispositif technique doit 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. 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 ou par les vérificateurs. Ces derniers 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.

4.4.6	(ad art. 5, al. 4, let. a et b) Un suffrage n'est considéré comme ayant été exprimé conformément à la procédure prévue par le système 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 attribuées dans le but d'exprimer des suffrages. 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 exprimer un suffrage conformément à la procédure prévue par le système, 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. 5, al. 3, let. b.
4.4.7	(ad art. 5, al. 5) 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 vérificateurs en confectionnant, à l'aide des composants 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 qui a été exprimé conformément à la procédure prévue par le système et qui a été enregistré par la partie fiable du système. Les vérificateurs doivent pouvoir identifier tous les cas dans lesquels on ajoute un suffrage 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[9], il faut pouvoir réduire suffisamment le risque en procédant à plusieurs dépouillements en utilisant de nouvelles valeurs aléatoires.
4.4.8	(ad art. 5, al. 5) Si l'application utilisée sur la plate-forme utilisateur pour le chiffrement du suffrage est mise à disposition par le système, elle doit être attribuée aussi à la partie serveur du système. Il faut 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 chiffrée 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.
4.4.9	(ad art. 5, al. 5) Conformément à l'objectif de sécurité, il faut éviter que la partie serveur du système 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 chiffré 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.

[9] Il s'agit de la probabilité de déchiffrer, sans connaître la clé, une valeur chiffrée avec un algorithme réputé sûr et paramétré en conséquence.

4.4.10	(ad art. 5, al. 5) En raison de l'exigence qui veut que le secret du vote soit garanti et qu'aucun résultat partiel ne soit établi de manière anticipée, aucun composant du système ne doit avoir accès aux clés privées servant à déchiffrer les 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 déchiffrement, 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 chiffrement 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 de manière anticipée, il n'est pas permis que des suffrages se trouvent en dehors de la plate-forme utilisateur, sous une forme non chiffrée, à quelque moment que ce soit pendant la durée d'ouverture du canal permettant de voter par voie électronique.
4.4.11	(ad art. 5, al. 6) L'identification de dysfonctionnements sérieux du système 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 anticipé de résultats partiels. 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 sérieux du système. 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 rechiffrer correctement – selon une méthode démontrable – des suffrages (pour les rendre anonymes; chaque « trustee » correspond au nœud mélangeur d'un réseau de rechiffrement), à gérer un tableau d'affichage électronique fiable, à mettre en place une infrastructure à clés publiques et à déchiffrer 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.
4.4.12	(ad art. 5, al. 6) Le logiciel des composants de contrôle doit être simple à analyser et ne disposer, si possible, que de fonctions cryptographiques élémentaires.
4.4.13	(ad art. 5, al. 6) Les composants de contrôle doivent être installés, actualisés, configurés et sécurisés au cours d'un processus observable.
4.4.14	(ad art. 5, al. 6) 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 illicitement 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. 4.4.12). 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 peuvent 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 identifiées et signalées au responsable des composants de contrôle en question.

4.4.15	(ad art. 5, al. 6) 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.
4.4.16	(ad art. 5, al. 6) 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.
4.4.17	(ad art. 5, al. 6) 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 contrôler le logiciel, mais aussi de s'assurer qu'il a été installé correctement.

5. Critères de contrôle pour les systèmes et leur exploitation (permettre à plus de 30 % de l'électorat cantonal de voter par voie électronique)

Chacun des ch. 5.1 à 5.6 correspond à un contrôle externe du système. Si le résultat du contrôle est un succès, les organisations responsables établissent une pièce justificative à l'attention du canton qui les a mandatées pour effectuer le contrôle. Le canton joint la pièce justificative à la demande d'agrément qu'il présente à la ChF. Les pièces justificatives à joindre figurent au ch. 6.

5.1. Contrôle du protocole cryptographique

5.1.1	Critères de contrôle: le protocole doit être conforme à l'objectif de sécurité et aux hypothèses de confiance figurant dans le modèle abstrait décrit au ch. 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 » et « Fiat-Shamir heuristic »). Le protocole doit se fonder si possible sur des protocoles éprouvés.
5.1.2	Compétences: les preuves doivent être apportées ou contrôlées 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 à la ChF le recours à un nouveau protocole ou la modification du protocole existant. Il peut proposer une institution, voire une personne, susceptible de procéder au contrôle; 2. la ChF examine la proposition; 3. la ChF fait part de sa décision au canton. Dans le cas de systèmes 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.
5.1.3	Durée de validité d'une pièce justificative: la première mise en service doit être précédée d'un contrôle complet. Le protocole doit être soumis à un nouveau contrôle s'il est modifié et si la recherche fait émerger de nouvelles connaissances importantes concernant la sécurité des éléments cryptographiques utilisés.

5.2. Contrôle des fonctionnalités

5.2.1	Critères de contrôle: les fonctionnalités doivent répondre aux exigences énumérées aux ch. 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. 4 ou 5. 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 doivent être contrôlées sur la base des critères principaux EAL2 des Critères communs (Common Criteria [CC]).
5.2.2	Compétences: le contrôle doit être effectué par une institution accréditée par le Service d'accréditation suisse (SAS).
5.2.3	Durée de validité d'une pièce justificative: les fonctionnalités doivent être soumises à un nouveau contrôle lors de chaque modification fondamentale, notamment en cas de modification du protocole cryptographique.

5.3. Contrôle de l'infrastructure et de l'exploitation

5.3.1	Critères de contrôle: le système et son exploitation doivent répondre aux exigences énumérées aux ch. 2, 3 et 4, mais aussi contribuer de façon appropriée à la réalisation des objectifs fixés. La sécurité des informations concernant le système 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 27001:2013 (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 du système qui sont responsables du système de vote électronique sur les plans juridique, administratif et opérationnel.
5.3.2	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 27001:2013. L'organisme de certification doit en outre attester que les exigences figurant aux ch. 2, 3 et 4 sont remplies si elles ne sont pas déjà couvertes par l'audit au sens de la norme ISO/IEC 27001:2013. L'organisme de certification doit être accrédité par le SAS pour pouvoir effectuer des audits au sens de la norme ISO/IEC 27001:2013.
5.3.3	Durée de validité d'une pièce justificative: les audits de renouvellement doivent être effectués aux intervalles prescrits dans la norme ISO 27001:2013. 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 fondamentale. Si une nouvelle version de la norme ISO/IEC 27001:2013 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. Contrôle des composants de contrôle

5.4.1	Critères de contrôle: les composants de contrôle doivent répondre aux exigences énumérées au ch. 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 contrôlées 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 doivent être contrôlées 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.
5.4.2	Compétences: le contrôle doit être effectué par une institution accréditée par le SAS.
5.4.3	Durée de validité d'une pièce justificative: les composants de contrôle doivent être soumis à un nouveau contrôle 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 fondamentales à des mécanismes de ce type; – si l'on recourt à un HSM, il faut, dans tous les cas, procéder, dans le cadre d'un contrôle, 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 n'est pas impératif de procéder à un nouveau contrôle pour autant que les composants de base correspondent toujours aux meilleures normes existantes.

5.5. Contrôle de la protection contre les tentatives d'intrusion dans l'infrastructure

5.5.1	Critères de contrôle: les personnes lançant une attaque depuis Internet ne doivent pas pouvoir pénétrer dans l'infrastructure 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, à l'aide de la documentation relative au système, en exploitant des vulnérabilités connues que présentent 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 contrôler au moins les vulnérabilités recensées dans le *Open Web Application Security Project* (OWASP).
5.5.2	Compétences: le contrôle doit être effectué par une institution accréditée par le SAS.
5.5.3	Durée de validité d'une pièce justificative: un nouveau contrôle doit être effectué au bout de trois ans.

5.6. Contrôle concernant les imprimeries

5.6.1	Critères de contrôle: l'imprimerie concernée doit mettre en œuvre l'exigence fixée au ch. 4.2.5 en plus des dispositions figurant dans le catalogue de critères pour les imprimeries.
5.6.2	Compétences: le contrôle doit être effectué par une institution accréditée par le SAS.
5.6.3	Durée de validité d'une pièce justificative: un nouveau contrôle doit être effectué au bout de deux ans. Un nouveau contrôle doit être effectué dans les cas où la décision est prise de renoncer à une mesure ou de modifier une mesure de manière fondamentale.

6. Pièces justificatives à l'appui des demandes

6.1	Le canton requérant envoie les pièces justificatives relatives aux contrôles (voir art. 7) qu'il a obtenues des institutions compétentes. La pièce justificative relative au contrôle visé au ch. 5.3 doit être un certificat valable au sens de la norme ISO/IEC 27001:2013.
6.2	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 du contrôle correspondant. Il indique toutes les modifications apportées au système, 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'appréciation des risques.
6.3	Le canton remet tous les protocoles des tests qui ont résulté de la mise en œuvre du schéma de test (ch. 3.5). Il s'engage à remettre des protocoles de tests supplémentaires au cas où un test serait mené peu avant le scrutin.
6.4	Le canton remet son actuelle appréciation des risques (art. 3) et s'engage à informer immédiatement qui de droit de tout changement dans l'évaluation des risques. Tous les risques qui menacent la réalisation des objectifs de sécurité doivent être identifiés moyennant une appréciation des risques. Il faut de plus apprécier les risques qui concernent l'environnement du vote électronique au sein de l'administration et dans le public. L'appréciation doit être menée selon une méthode comprenant les activités suivantes: -- identification des risques; -- analyse des risques; -- estimation des risques. Les détails de la méthode utilisée et les critères de tolérance des risques imposés par le canton doivent être documentés. Pour les risques qui découlent de l'exploitation du système, il faut, lors l'identification des risques dans les cas ou l'on permet à plus de 30 % de l'électorat cantonal de voter par voie électronique, respecter en tous points les exigences méthodologiques de la norme ISO/IEC 27001:2013.