Ordonnance de la ChF sur le vote électronique (OVotE)

du 25 mai 2022 (État le 1er juillet 2022)

La Chancellerie fédérale suisse (ChF),
vu les art. 27*e*, al. 1bis, 27*g*, al. 2, 27*i*, al. 3, et 27*l*, al. 3 et 4,
de l'ordonnance du 24 mai 1978 sur les droits politiques (ODP)[1],
arrête:

Art. 1 Objet

La présente ordonnance fixe les conditions régissant l'octroi de l'agrément pour les essais de vote électronique.

Art. 2 Définitions

1 On entend par:

a. s*ystème:* terme générique qui recouvre le logiciel et les infrastructures utilisés pour réaliser un scrutin électronique;

b. s*ystème en ligne:* partie du système qui est utilisée pour vérifier le droit de vote, pour envoyer le suffrage chiffré et pour conserver le suffrage chiffré;

c. *partie fiable du système:* partie du système comprenant un ou plusieurs groupes de composants de contrôle; la fiabilité de cette partie du système résulte de ce qu'il est possible de détecter les abus même si un seul des composants de contrôle d'un groupe fonctionne correctement;

d. *composants de contrôle:* composants du système indépendants qui diffèrent les uns des autres dans leur conception, sont exploités par des personnes différentes et sont sécurisés par des mesures spécifiques;

e. *exploitant du système:* autorité ou entreprise privée qui, agissant sur instructions du canton, exploite le système en ligne lors de la tenue d'un scrutin et assure sa maintenance;

f. *exploitation:* toutes actions à caractère technique, administratif ou juridique ainsi que les activités dirigeantes menées par un canton, un exploitant du système ou une imprimerie qui sont nécessaires pour la réalisation d'un scrutin électronique, y compris la maintenance;

g. *unités d'exploitation:* unités responsables de l'exploitation, comme une chancellerie d'État, un exploitant d'un système ou une imprimerie;

RO **2022** 336
1 RS **161.11**

h. *vérificateurs:* personnes qui, sur mandat du canton, s'assurent du bon déroulement du scrutin;

i. *infrastructure:* matériel informatique, logiciels de composants tiers au sens de l'art. 11, al. 2, let. a, éléments de réseau, locaux, services et moyens d'exploitation de toute nature des unités d'exploitation, qui sont nécessaires à une exploitation sûre du vote électronique;

j. *logiciel:* pleine implémentation à partir du protocole cryptographique nécessaire à la vérifiabilité complète du processus de vote électronique telle qu'elle a été mise en œuvre par le développeur du système;

k. *protocole cryptographique:* protocole doté de fonctions de sécurité cryptographiques destiné à assurer la conformité aux exigences visées à l'annexe, ch. 2; le protocole cryptographique est implanté au niveau du modèle et ne contient donc pas d'instructions d'implémentation directes, mais uniquement des fonctions de sécurité abstraites;

l. *plate-forme utilisateur:* appareil multifonctionnel programmable relié à Internet et qui permet de voter, tel qu'un ordinateur standard, un ordiphone ou une tablette tactile;

m. *suffrage enregistré:* suffrage dont la partie fiable du système a reçu confirmation de son caractère définitif;

n. *suffrage partiel:*
   1. dans le cadre d'une votation: suffrage émis relativement à un projet, à un contre-projet ou à une question subsidiaire,
   2. dans le cadre d'une élection: suffrage émis en faveur d'une liste ou d'un candidat;

o. *suffrage émis conformément à la procédure prévue par le système:* suffrage qui répond aux quatre conditions suivantes:
   1. il est conforme aux règles applicables au remplissage d'un bulletin de vote,
   2. il a été émis de manière définitive,
   3. les données pertinentes 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,
   4. il a été émis au moyen de données d'authentification client qui n'ont pas déjà été utilisées pour émettre un suffrage que la partie fiable du système en ligne aurait enregistré précédemment;

p. *donnée d'authentification client:* information mise à la disposition de l'électeur, comme un NIP, et dont celui-ci, le cas échéant conjointement avec d'autres données d'authentification client, a besoin pour voter;

q. *donnée d'authentification serveur:* information qui, le cas échéant conjointement avec d'autres données d'authentification serveur, est nécessaire pour authentifier l'émetteur d'un suffrage en sa qualité d'électeur au moyen de messages d'authentification;

r. *messages d'authentification:* ensemble des informations qu'une plate-forme utilisateur envoie au système en ligne après introduction des données d'authentification client pour que l'infrastructure authentifie l'émetteur d'un suffrage en sa qualité d'électeur;

s. *certificat:* document qui atteste qu'un élément contrôlé est conforme à un cadre de référence ou à une norme;

t. *certificat électronique:* ensemble de données qui atteste de certaines caractéristiques de personnes ou d'objets et dont l'authenticité et l'intégrité peuvent être vérifiées par des procédés cryptographiques; le certificat électronique est principalement utilisé pour identifier et authentifier le titulaire et pour chiffrer les transmissions;

u. *actions et opérations critiques:* activités au cours desquelles des données critiques sont traitées;

v. *données critiques:* données dont l'intégrité ou la confidentialité sont déterminantes pour le respect des exigences du protocole cryptographique.

2 Sont applicables au surplus les définitions qui figurent au ch. 1 de l'annexe.

Art. 3 Conditions à remplir pour obtenir l'agrément en vue de la tenue d'un scrutin électronique

L'agrément doit être demandé pour chaque scrutin électronique; il est accordé si les conditions suivantes sont remplies:

a. le système est conçu et exploité de façon à garantir un scrutin électronique vérifiable, sûr et fiable;

b. le système est facile à utiliser par les électeurs; il tient compte autant que possible des besoins particuliers de chacun;

c. le système et les processus d'exploitation sont conçus et documentés de façon à ce qu'il soit possible de vérifier et de comprendre dans le détail leurs aspects techniques et organisationnels;

d. le public a accès à des informations adaptées sur le fonctionnement du système et sur ses processus d'exploitation, et des mesures sont prises pour inciter les personnes disposant des connaissances nécessaires à participer à l'amélioration du système.

Art. 4 Appréciation des risques

1 Le canton démontre au moyen d'une appréciation des risques que les risques pour la sécurité sont suffisamment faibles dans le domaine qui relève de sa compétence. Il tient compte de la confiance et de l'acceptation du public à l'égard du vote électronique.

2 Il examine s'il lui est possible d'apprécier les risques dans les domaines qui relèvent de ses prestataires ou si ceux-ci doivent le faire eux-mêmes. Le cas échéant, il leur demande de procéder à une telle appréciation et de la lui remettre.

3 Les risques sont appréciés sous l'angle des objectifs de sécurité suivants:

a. l'exactitude des résultats est garantie;

b. le secret du vote est garanti et il est impossible d'établir des résultats partiels anticipés;

c. le vote électronique est accessible et opérationnel;

d. les informations personnelles des électeurs sont protégées;

e. les informations destinées aux électeurs sont protégées contre les manipulations;

f. il est impossible de faire un usage abusif des preuves relatives au comportement de vote.

4 Chaque risque doit être identifié et décrit clairement au moyen de la documentation du système et de son exploitation, sous l'angle des aspects suivants:

a. objectifs de sécurité;

b. données éventuellement liées aux objectifs de sécurité;

c. menaces;

d. vulnérabilités.

Art. 5 Exigences applicables à la vérifiabilité complète

1 Toute manipulation de nature à fausser les résultats doit pouvoir être détectée sans qu'il soit porté atteinte au secret du vote (vérifiabilité complète). Tel est réputé être le cas lorsque sont remplies les exigences applicables et à la vérifiabilité individuelle et à la vérifiabilité universelle.

2 La vérifiabilité individuelle est soumise aux exigences suivantes:

a. tout votant dispose de la possibilité de détecter si le suffrage qu'il a émis, tel qu'il l'a saisi sur la plate-forme utilisateur, a été manipulé ou intercepté sur la plate-forme utilisateur ou pendant la transmission; tout votant reçoit à cet effet la preuve que la partie fiable du système (art. 8) a enregistré son suffrage tel qu'il l'a saisi sur la plate-forme utilisateur, et que ce suffrage a été émis conformément à la procédure prévue par le système; la preuve atteste, pour chaque suffrage partiel, que l'enregistrement a été effectué correctement;

b. tout électeur qui n'a pas voté par voie électronique peut demander, une fois fermé le canal de vote électronique et avant l'échéance des délais de recours légaux, la preuve que la partie fiable du système n'a pas enregistré de suffrage émis au moyen de ses propres données d'authentification client.

3 La vérifiabilité universelle est soumise aux exigences suivantes:

a. les vérificateurs reçoivent la preuve que les résultats ont été établis correctement; cette preuve atteste que ceux-ci ont été établis en prenant en compte:

1. tous les suffrages qui ont été émis conformément à la procédure prévue par le système et qui ont été enregistrés par la partie fiable du système,

2. uniquement les suffrages qui ont été émis conformément à la procédure prévue par le système,
3. tous les suffrages partiels correspondant à la preuve générée dans le cadre de la vérifiabilité individuelle;

b. les vérificateurs doivent évaluer cette preuve au cours d'un processus observable; ils mettent en œuvre à cet effet des dispositifs techniques indépendants et séparés du reste du système.

Art. 6 Caractère concluant des preuves

Le caractère concluant des preuves visées à l'art. 5 dépend de la fiabilité:

a. de la partie fiable du système, pour les preuves visées à l'art. 5, al. 2 et 3;

b. de la procédure utilisée pour générer et imprimer le matériel de vote, pour les preuves visées à l'art. 5, al. 2, et

c. des dispositifs techniques que les vérificateurs mettent en œuvre aux fins de contrôle, pour les preuves visées à l'art. 5, al. 3.

Art. 7 Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés

Sont déterminantes pour garantir le secret du vote et l'impossibilité d'établir des résultats partiels anticipés au sein de l'infrastructure:

a. la fiabilité de la partie fiable du système;

b. la fiabilité de la procédure utilisée pour générer et imprimer le matériel de vote.

Art. 8 Exigences applicables à la partie fiable du système

1 La partie fiable du système comprend un ou plusieurs groupes de composants de contrôle.

2 Les preuves sont concluantes (art. 6) et le secret du vote est garanti (art. 7) même si, dans chaque groupe, il n'y a qu'un seul composant de contrôle à fonctionner correctement.

3 Pour que la fiabilité de la partie fiable du système soit garantie, il faut que les composants de contrôle diffèrent les uns des autres dans leur conception et que leur exploitation et leur surveillance soient indépendantes.

Art. 9 Mesures supplémentaires visant à réduire les risques

Si les risques ne sont pas suffisamment faibles malgré les mesures prises, il convient de prendre des mesures supplémentaires afin de les réduire. Cette règle s'applique même lorsque toutes les exigences prévues dans l'annexe ont déjà été mises en œuvre.

Art. 10 Exigences applicables au contrôle

1 Des organes indépendants mandatés par la ChF vérifient la conformité:

a. du protocole cryptographique (annexe, ch. 26.1);

b. du logiciel du système (annexe, ch. 26.2);

c. de la sécurité de l'infrastructure et de l'exploitation (annexe, ch. 26.3);

d. de la protection contre les tentatives d'intrusion dans l'infrastructure (annexe, ch. 26.4).

2 Le canton s'assure que l'exploitant du système dispose d'un système de management de la sécurité de l'information (SMSI) et que celui-ci est audité par des organes indépendants (annexe, ch. 26.5). Le SMSI porte au moins sur les processus et les éléments de l'infrastructure de l'exploitant du système qui sont pertinents pour atteindre les objectifs de sécurité.

3 Le canton s'assure que la ChF et les organes indépendants qu'elle a mandatés ont accès au système et à tous les documents nécessaires de façon à pouvoir procéder aux contrôles visés à l'al. 1.

4 Les autorités responsables des contrôles en vertu des al. 1 et 2 publient les pièces justificatives et les certificats. Ils publient en outre tous documents pertinents pour la compréhension de ces derniers. Ne doivent pas obligatoirement être publiés les documents ou parties de documents qui échappent à l'obligation de publication parce que des motifs particuliers le justifient, notamment tirés de la législation sur la protection des données ou de la législation sur la transparence.

Art. 11 Publication du code source et de la documentation du système et de son exploitation

1 Le canton veille à ce que soient publiés les éléments suivants:

a. le code source du logiciel du système, y compris les fichiers contenant les paramètres pertinents;

b. une pièce justificative attestant que les programmes lisibles par machine ont été créés au moyen du code source du logiciel tel qu'il a été publié;

c. la documentation du logiciel;

d. la documentation du processus de développement;

e. les guides et autres documentations complémentaires, afin que les personnes disposant des connaissances nécessaires puissent compiler, faire fonctionner et analyser le système dans leur propre infrastructure au moyen du code source;

f. les spécifications techniques des principaux composants du système;

g. la documentation des processus d'exploitation, de maintenance et de sécurité du système;

h. les informations et descriptifs concernant les failles identifiées.

2 Ne doivent pas obligatoirement être publiés:

a. le code source de composants tiers tels que des systèmes d'exploitation, des bases de données, des serveurs web et des serveurs d'application, des systèmes de gestion des droits, des pare-feu et des routeurs, pour autant que ces composants soient utilisés à grande échelle et qu'ils soient mis à jour en permanence;

b. le code source des portails de cyberadministration qui sont reliés au système;

c. les documents ou parties de documents qui échappent à l'obligation de publication parce que des motifs particuliers le justifient, notamment tirés de la législation sur la protection des données ou de la législation sur la transparence.

Art. 12 Modalités de publication

1 Les éléments à publier conformément à l'art. 11 doivent être préparés et documentés de façon à faciliter autant que possible leur lecture et leur analyse.

2 Pour permettre au public d'apprécier les éléments à publier, il est fait en sorte que ceux-ci:

a. soient accessibles en ligne facilement, gratuitement et sans obligation d'enregistrement, et

b. soient disponibles suffisamment longtemps avant l'utilisation prévue du système.

3 Toute personne a le droit d'examiner, de modifier, de compiler et d'exécuter le code source à des fins idéales et de lui consacrer des études. Elle peut publier des études et des constatations sur les failles. Elle a également le droit d'échanger avec d'autres personnes pour rechercher des failles et de citer tout ou partie des informations publiées.

4 Le propriétaire du code source peut:

a. autoriser l'utilisation du code source à d'autres fins;

b. soumettre à des conditions particulières la fourniture d'indications sur les moyens d'améliorer le système; il peut ainsi inviter à signaler toute faille au plus vite et à observer un certain délai pour les publications consacrées à des failles supposées.

5 S'il soumet le code source et la documentation à des conditions d'utilisation ou s'il prévoit des conditions au sens de l'al. 4, let. b, il ne peut poursuivre leur violation civilement ou pénalement que si le code source est utilisé en tout ou partie à des fins commerciales ou productives. Les conditions précitées doivent préciser ce point.

Art. 13 Participation du public

1 Le canton désigne un service auquel le public peut fournir des indications sur les moyens d'améliorer le système, notamment:

a. des indications concernant des erreurs dans les éléments qui doivent être publiés en vertu de l'art. 11;

b. des indications reposant sur des tentatives d'intrusion dans le système en ligne effectuées dans le cadre de tests publics.

2 Le service visé à l'al. 1 évalue les indications reçues et informe les personnes qui les ont fournies des conclusions qu'il en a tirées et des mesures qui pourront être prises à partir de ces indications. Ces informations sont publiées.

3 Le canton veille à ce que les indications qui touchent à la sécurité et qui permettent d'améliorer le système soient rémunérées de manière équitable.

Art. 14 Responsabilité et compétences à l'égard du bon déroulement du scrutin électronique

1 Le canton assume la responsabilité générale du bon déroulement du scrutin électronique.

2 Il exécute lui-même les tâches principales. Il peut déléguer à des entités extérieures le développement du logiciel utilisé, les tâches liées à l'exploitation et la communication sur le fonctionnement du système.

3 Il désigne un service compétent au niveau cantonal qui assume la responsabilité générale du scrutin et veille notamment à la bonne exécution des tâches suivantes:

a. établir une directive globale sur la sécurité de l'information;

b. établir une directive sur la classification et le traitement de l'information pour les ressources informationnelles identifiées;

c. établir une directive sur la gestion du risque;

d. définir et mettre en œuvre les mesures permettant d'assurer la conformité aux directives visées aux let. a à c;

e. mandater l'exploitant d'un système et définir les exigences applicables à sa surveillance et à son contrôle;

f. fixer les délais applicables à l'exécution d'actions et d'opérations critiques;

g. surveiller et vérifier les travaux effectués par l'exploitant du système;

h. accompagner et instruire les vérificateurs;

i. évaluer et communiquer l'exactitude des résultats du scrutin sur la base des preuves visées à l'art. 5 et d'autres indicateurs.

4 Pendant la tenue d'un scrutin, les unités d'exploitation répondent devant le canton du bon fonctionnement du vote électronique et de la bonne gestion de ses aspects techniques.

5 Les vérificateurs compétents selon le droit cantonal répondent du bon fonctionnement de leurs dispositifs techniques.

Art. 15 Documents à joindre aux demandes

[1] Aux demandes présentées en vertu de l'art. 27*e* ODP devront être joints les informations concernant l'utilisation prévue du système de vote électronique et les documents qui attestent que les exigences légales sont remplies. Il s'agit notamment des documents suivants:

a. les appréciations des risques les plus récentes au sens de l'art. 4, y compris les éléments nécessaires à leur compréhension;

b. les certificats, y compris leurs annexes, qui ont été établis dans le cadre de l'art. 10, al. 2, et les informations attestant de leur publication conformément à l'art. 10, al. 4;

c. les informations concernant la publication des éléments visés à l'art. 11 et les indications fournies par le public en vertu de l'art. 13;

d. les protocoles des tests qui ont été effectués par le canton, et les indications suggérant l'existence de failles affectant le système;

e. les raisons pour lesquelles certaines exigences n'ont pas été remplies et les mesures de remplacement prévues, conformément à l'art. 16, al. 2.

[2] Lorsque la ChF a déjà en sa possession les documents visés à l'al. 1 et qu'ils sont encore valides, il pourra suffire d'y renvoyer.

Art. 16 Autres dispositions

[1] Les exigences techniques et administratives à remplir pour organiser un scrutin électronique sont détaillées dans l'annexe.

[2] La ChF peut exceptionnellement dispenser un canton de remplir certaines exigences s'il respecte les trois conditions suivantes:

a. il signale comme telles dans la demande les exigences qu'il n'a pas remplies;

b. il expose de manière plausible les raisons pour lesquelles il n'a pas rempli ces exigences;

c. il décrit les mesures de remplacement qu'il prendra et, s'agissant de l'appréciation des risques, indique les raisons pour lesquelles il considère que ceux-ci sont suffisamment faibles.

Art. 17 Abrogation d'un autre acte

L'ordonnance de la ChF du 13 décembre 2013 sur le vote électronique[2] est abrogée.

Art. 18 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er juillet 2022.

2 [RO **2013** 5371; **2018** 2279]

Annexe
(art. 2, al. 1, let. k, et 2, 9, 10, al. 1 et 2, et 16, al. 1)

Exigences techniques et administratives applicables au vote électronique

1. Définitions

En complément de l'art. 2, on entend par:

1.1 *garantie du secret du vote:* situation qui prévaut lorsque aucune personne et aucun composant n'a accès aux données suivantes:

1.1.1. suffrages émis ou données permettant de déduire le contenu de suffrages émis,

1.1.2. données permettant d'identifier le votant (données concernant les électeurs), et

1.1.3. données permettant d'attribuer les données concernant les électeurs aux suffrages émis;

1.2 *impossibilité d'établir des résultats partiels anticipés:* situation qui prévaut lorsque aucune personne et aucun composant n'a accès de manière anticipée aux suffrages émis ou à des données permettant de déduire les suffrages émis;

1.3 *référence de vérification:* informations fournies avec le matériel de vote qui doivent permettre aux électeurs de vérifier conformément à l'art. 5, al. 2, en rel. avec le ch. 2.5 de l'annexe, que leur suffrage a été émis correctement (par ex. une liste contenant un code pour chaque réponse possible);

1.4 *attaquant externe:* personne ou groupe de personnes externe à la conception et à l'exploitation du système et disposant de ressources et de compétences techniques moyennes et qui mène une attaque; ses motivations peuvent comprendre l'activisme ou l'appât du gain;

1.5 *attaquant interne:* personne ou groupe de personnes impliqués dans la conception ou l'exploitation du système et qui mène une attaque; ses motivations peuvent comprendre l'activisme, l'appât du gain ou la volonté de nuire à son employeur;

1.6 *organisation hostile:* groupe de personnes disposant de moyens étendus et menant une attaque, qu'il soit soutenu par un État ou non; ses compétences, ou du moins celles de ses membres, sont élevées; elle peut avoir pour motivations la collecte de données à des fins de profilage, la perturbation d'un scrutin ou l'altération de ses résultats;

1.7 *attaquant:* personne, groupe de personnes ou organisation au sens des ch. 1.4 à 1.6;

1.8 *urne électronique:* zone de stockage dans laquelle les suffrages émis sont conservés jusqu'au déchiffrement et au dépouillement;

1.9 *journal système:* journal créé par les éléments de l'infrastructure et destiné à permettre la surveillance du fonctionnement du système et l'analyse des incidents.

2. Exigences applicables au protocole cryptographique pour la vérifiabilité complète (art. 5)

2.1 Participants du système

Le protocole cryptographique doit régler les tâches des participants abstraits suivants:

- électeur / votant
- plate-forme utilisateur
- composant de configuration
- système non fiable (composants quelconques, à l'exclusion des autres composants énumérés sous le présent chiffre; système NF)
- composant d'impression
- un ou plusieurs groupes de composants de contrôle
- vérificateurs
- dispositif technique des vérificateurs

2.2 Canaux de communication

Le protocole cryptographique peut prévoir les canaux de communication suivants pour l'échange de messages entre les participants du système:

- électeur / votant ↔ plate-forme utilisateur
- plate-forme utilisateur ↔ système NF
- composant de configuration ↔ système NF
- composant de contrôle ↔ système NF
- système NF → composant d'impression
- système NF → dispositif technique des vérificateurs
- composant d'impression → électeur / votant
- composant de configuration → dispositif technique des vérificateurs
- vérificateurs ↔ dispositif technique des vérificateurs
- canaux bidirectionnels pour la communication entre les composants de contrôle

2.3 Attaquant

2.3.1 Le protocole cryptographique doit protéger contre un attaquant qui tente d'influer abusivement sur les suffrages et sur le résultat, de compromettre le secret du vote ou d'établir des résultats partiels de manière anticipée (ch. 2.5 à 2.8).

2.3.2 Il doit reposer sur l'hypothèse qu'un attaquant possède les capacités suivantes:

- Il peut prendre sous son contrôle tous les participants non fiables du système (voir ch. 2.4) de façon à les amener à partager avec lui toutes les données secrètes et à agir selon toutes ses instructions.
- Il peut lire ou supprimer tous les messages qui sont échangés sur des canaux non fiables et envoyer des messages à loisir.

2.4 Participants du système et canaux de communication fiables et non fiables

2.4.1 Les participants du système et les canaux de communication sont considérés soit comme «fiables» soit comme «non fiables». Les hypothèses de confiance licites pour les différents participants du système sont réglées au ch. 2.9.

2.4.2 Les participants du système et les canaux de communication fiables sont considérés comme protégés contre un attaquant. Les hypothèses suivantes, notamment, peuvent s'appliquer au protocole cryptographique:

- Les participants fiables du système conservent de façon sécurisée les données confidentielles et n'effectuent que les opérations prescrites dans le protocole cryptographique.
- Les canaux de communication fiables conservent de façon sécurisée les messages transmis et les protègent contre toute manipulation.

2.5 Exigence applicable au protocole cryptographique: vérifiabilité individuelle

L'électeur reçoit des preuves au sens de l'art. 5, al. 2, en rel. avec l'art. 6, let. a et b, qui attestent qu'un attaquant:

- n'a modifié ou fait disparaître aucun suffrage partiel de l'électeur jusqu'à son enregistrement en tant que suffrage émis conformément à la procédure prévue par le système;
- n'a pas abusivement émis au nom de l'électeur de suffrage ayant ensuite été enregistré et comptabilisé en tant que suffrage émis conformément à la procédure prévue par le système.

2.6 Exigence applicable au protocole cryptographique: vérifiabilité universelle

Les vérificateurs reçoivent des preuves au sens de l'art. 5, al. 3, let. a, en rel. avec l'art. 6, let. a et c, qui attestent qu'un attaquant:

- n'a modifié ou fait disparaître aucun suffrage partiel jusqu'au calcul des résultats, après que les suffrages correspondants ont été enregistrés comme ayant été émis conformément à la procédure prévue par le système;
- n'a ajouté ni suffrage ni suffrage partiel non émis conformément à la procédure prévue par le système, qui ont été pris en compte dans le calcul des résultats.

2.7 Exigences applicables au protocole cryptographique: secret du vote et impossibilité d'établir des résultats partiels anticipés

2.7.1 Un attaquant ne doit pouvoir ni compromettre le secret du vote ni établir des résultats partiels de manière anticipée sans devoir en plus prendre sous son contrôle les électeurs ou leurs plates-formes utilisateur.

2.7.2 Il n'est pas obligatoire d'empêcher les attaques qui limitent le nombre des suffrages dépouillés de telle manière que tous les suffrages partiels soient les mêmes pour une question soumise au vote, une liste ou un candidat.

2.7.3 Un attaquant ne doit pas pouvoir prendre sous son contrôle de manière inaperçue les plates-formes utilisateur en manipulant sur le serveur le logiciel pour les plates-formes utilisateur. Le votant doit à cet égard avoir la possibilité de vérifier si sa plate-forme utilisateur a reçu du serveur le logiciel correct avec les paramètres corrects, notamment la clef publique destiné à chiffrer le suffrage.

2.8 Exigence applicable au protocole cryptographique: authentification efficace

Un attaquant ne doit pouvoir émettre de suffrage conformément à la procédure prévue par le système sans prendre sous son contrôle les électeurs correspondants.

2.9 Liste des participants fiables et non fiables du système

2.9.1 Concernant le caractère concluant des preuves au sens du ch. 2.5

2.9.1.1 Les participants du système suivants sont considérés comme non fiables:

- plate-forme utilisateur
- système NF
- trois des quatre composants de contrôle par groupe, sans qu'il soit nécessaire de déterminer lesquels
- un pourcentage significatif des électeurs
- les vérificateurs
- les dispositifs techniques des vérificateurs

2.9.1.2 Les participants du système suivants peuvent être considérés comme fiables:

- composant de configuration
- composant d'impression
- un des quatre composants de contrôle par groupe, sans qu'il soit nécessaire de déterminer lequel

2.9.2 Concernant le caractère concluant des preuves au sens du ch. 2.6

2.9.2.1 Les participants du système suivants sont considérés comme non fiables:

- plate-forme utilisateur
- système NF
- trois des quatre composants de contrôle par groupe, sans qu'il soit nécessaire de déterminer lesquels
- un pourcentage significatif des électeurs
- composant de configuration
- composant d'impression

2.9.2.2 Les participants du système suivants peuvent être considérés comme fiables:
- un des quatre composants de contrôle par groupe, sans qu'il soit nécessaire de déterminer lequel
- un vérificateur d'un groupe, sans qu'il soit nécessaire de déterminer lequel
- un dispositif technique d'un vérificateur fiable, sans qu'il soit nécessaire de déterminer lequel

2.9.3 Concernant le secret du vote et l'impossibilité d'établir des résultats partiels anticipés au sens du ch. 2.7

2.9.3.1 Les participants du système suivants sont considérés comme non fiables:
- système NF
- trois des quatre composants de contrôle par groupe, sans qu'il soit nécessaire de déterminer lesquels
- un pourcentage significatif des électeurs
- les vérificateurs
- les dispositifs techniques des vérificateurs

2.9.3.2 Les participants du système suivants peuvent être considérés comme fiables:
- composant de configuration
- composant d'impression
- plate-forme utilisateur
- un des quatre composants de contrôle par groupe, sans qu'il soit nécessaire de déterminer lequel

2.9.3.3 Si un groupe entier de composants de contrôle est mis en œuvre par un exploitant du système privé, aucun de ces composants ne peut être considéré comme fiable.

2.9.4. Concernant l'efficacité de l'authentification au sens du ch. 2.8

2.9.4.1 Les participants du système suivants sont considérés comme non fiables:
- système NF
- trois des quatre composants de contrôle par groupe, sans qu'il soit nécessaire de déterminer lesquels
- un pourcentage significatif des électeurs
- les vérificateurs
- les dispositifs techniques des vérificateurs
- plate-forme utilisateur

2.9.4.2 Les participants du système suivants peuvent être considérés comme fiables:
- composant de configuration
- composant d'impression
- un des quatre composants de contrôle par groupe, sans qu'il soit nécessaire de déterminer lequel

2.10 Liste des canaux de communication fiables et non fiables

2.10.1 Les canaux de communication suivants sont considérés comme non fiables:

- plate-forme utilisateur ↔ système NF
- composant de configuration ↔ système NF
- composant de contrôle ↔ système NF
- système NF → composant d'impression
- système NF → dispositif technique des vérificateurs
- canaux bidirectionnels pour la communication entre les composants de contrôle

2.10.2 Les canaux de communication suivants peuvent être considérés comme fiables:

- électeur / votant ↔ plate-forme utilisateur
- dispositif technique des vérificateurs ↔ vérificateurs
- composant de configuration → dispositif technique des vérificateurs
- composant d'impression → électeur / votant

2.11 Exigences supplémentaires applicables au caractère concluant des preuves

2.11.1 La probabilité qu'un attaquant puisse falsifier une preuve au sens du ch. 2.5 en modifiant un suffrage partiel, en faisant disparaître un suffrage partiel ou en émettant un suffrage au nom d'un tiers, ne peut dépasser 0,1 %.

2.11.2 La probabilité qu'un attaquant puisse falsifier une preuve au sens du ch. 2.6 en modifiant ou en faisant disparaître un suffrage émis conformément à la procédure prévue par le système ou en ajoutant un suffrage non émis conformément à cette procédure de façon que le résultat établi s'écarte de 0,1 % du résultat correct ne peut dépasser 1 % par projet, choix de liste ou choix d'un candidat sur une liste.

2.11.3 Si la probabilité qu'un attaquant puisse falsifier une preuve au sens du ch. 2.6 n'est pas négligeable au sens cryptographique[3], la probabilité qu'il réussisse doit pouvoir être réduite à loisir au moyen de plusieurs décomptes, les vérificateurs devant recevoir pour chaque décompte une preuve supplémentaire et indépendante au sens du ch. 2.6.

2.12 Exigences fonctionnelles applicables au processus de vote ayant des incidences sur le protocole cryptographique

2.12.1 Les données d'authentification qui sont attribuées à un électeur ne permettent d'émettre qu'un seul suffrage.

2.12.2 Le votant saisit son suffrage dans la plate-forme utilisateur.

2.12.3 Le votant peut modifier et vérifier au moyen d'une vue d'ensemble son suffrage jusqu'à ce qu'il décide de l'émettre.

[3] Correspond à peu près à la probabilité de décrypter, sans connaître la clef, une valeur ayant été chiffrée avec un algorithme réputé sûr et un paramétrage correspondant.

2.12.4 Une fois que le votant a eu la possibilité de vérifier son suffrage au moyen de la vue d'ensemble, il indique dans la plate-forme utilisateur qu'il souhaite émettre son suffrage tel qu'il l'a saisi.

2.12.5 Les preuves que le suffrage a été correctement émis au sens du ch. 2.5 doivent se structurer en au moins deux preuves partielles séquentielles. Chacune des indications présentées comme une preuve partielle doit constituer une véritable contribution au caractère concluant des preuves au sens du ch. 2.5.

2.12.6 La plate-forme utilisateur indique au votant la première preuve partielle après que celui-ci a saisi dans la plate-forme utilisateur son intention d'émettre son suffrage.

2.12.7 La plate-forme utilisateur n'indique au votant la seconde preuve partielle qu'une fois que celui-ci a confirmé au moyen d'une saisie dans la plate-forme utilisateur que la preuve partielle précédente était correcte.

2.12.8 En confirmant que l'avant-dernière preuve partielle était correcte, le votant déclare vouloir émettre son suffrage de manière définitive.

2.12.9 Dès qu'il a reçu confirmation que le votant veut émettre son suffrage de manière définitive, le groupe de composants de contrôle enregistre le suffrage comme ayant été émis conformément à la procédure prévue par le système.

2.12.10 Lorsque le votant a vérifié la dernière preuve partielle et si le résultat est positif, l'opération de vote est terminée. La dernière preuve partielle doit être particulièrement facile à vérifier, cette vérification consistant autant que possible dans l'affichage correct d'un code unique ou de toute autre indication simple.

2.12.11 Si des données de vote sont importées, un composant de configuration ou un composant d'impression ne peut plus à partir de ce moment être considéré comme fiable.

2.13 Exigences applicables à la définition et à la description du protocole cryptographique

2.13.1 On utilisera lorsque cela sera possible des éléments qui sont largement utilisés dans le monde et qui ont été vérifiés de manière approfondie par des personnes compétentes. De même, on pourra faire appel à titre de comparaison à des standards, des projets de référence et des publications scientifiques. Tout écart par rapport à la norme ou toute incertitude seront traités à part dans le cadre de l'appréciation des risques visés à l'art. 4.

2.13.2 Les instructions doivent être suffisamment précises: chacune d'elles devra limiter les possibilités de mise en œuvre de telle sorte que chaque mise en œuvre autorisée par l'instruction correspondante soit également conforme aux exigences applicables au protocole cryptographique.

2.13.3 Les canaux fiables peuvent être utilisés pour la distribution de certificats électroniques entre les participants au système. Le ch. 3.8 s'applique.

2.14 Preuves de conformité aux exigences applicables au protocole cryptographique

2.14.1 Une preuve de conformité symbolique et une preuve de conformité cryptographique doivent attester que le protocole cryptographique respecte les exigences visées aux ch. 2.1 à 2.12.

2.14.2 Ces preuves de conformité doivent se référer directement à la description du protocole qui sert de base pour le développement du système.

2.14.3 En ce qui concerne les éléments de base cryptographiques, les preuves de conformité peuvent être administrées dans le cadre d'hypothèses et de constructions de sécurité généralement admises (comme le modèle de l'oracle aléatoire, l'hypothèse décisionnelle de Diffie-Hellman ou l'heuristique de Fiat-Shamir).

3. Exigences applicables aux composants fiables au sens du ch. 2 et à leur exploitation

3.1 L'exploitation du composant de configuration et d'au moins un composant de contrôle du groupe contenant une partie de la clef destinée à déchiffrer les suffrages doit relever directement du canton et intervenir dans son infrastructure. Toute sous-traitance à l'exploitant d'un système privé est interdite.

3.2 On veillera à utiliser une entropie suffisante pour le choix de valeurs aléatoires concernant, notamment, les composants de configuration et les composants de contrôle.

3.3 Les vérificateurs doivent contrôler au moins une fois les preuves au sens du ch. 2.6 et utiliser à cet effet un dispositif technique au sens du ch. 2.

3.4 Les exigences d'exploitation pour les composants de configuration visés au ch. 3 s'appliquent également aux dispositifs techniques des vérificateurs. Ceux-ci peuvent prévoir des dérogations dans le cadre de leurs compétences telles qu'elles sont définies par le droit cantonal.

3.5 À l'exception des composants mentionnés aux ch. 3.1 et 3.3, le canton peut déléguer l'exploitation de n'importe quelle partie du système, y compris les composants de contrôle et le composant d'impression, à des prestataires de services privés. Un exploitant privé du composant d'impression ne peut effectuer que les tâches opérationnelles qui constituent une condition préalable à la préparation, au conditionnement et à la livraison.

3.6 Les composants fiables (composants de configuration, composants d'impression, dispositifs techniques des vérificateurs et composants de contrôle) doivent être mis en place, mis à jour, configurés et sécurisés dans un processus observable.

3.7 Avant d'installer un logiciel, il faut vérifier pour tous les programmes au moyen d'une source fiable officielle si la version des fichiers est bien la version correcte et non modifiée.

3.8 Lorsque sont installés des certificats électroniques provenant d'autres participants au système, l'authenticité doit être garantie. Il y a lieu à cet effet de prévoir un processus manuel, avec des personnes qui transfèrent les certificats électroniques d'une machine à l'autre via un support de données physique au sens du ch. 3.13.

3.9 La date de mise à jour de l'ensemble des logiciels des composants fiables doit être choisie de manière que les avantages attendus l'emportent sur les risques potentiels.

3.10 Les composants de configuration, les composants d'impression et les dispositifs techniques des vérificateurs qui sont impliqués d'une manière ou d'une autre dans le traitement des données critiques doivent être surveillés physiquement selon le principe du double contrôle pendant toute la durée du calcul et jusqu'à la suppression de toute donnée critique ou jusqu'au stockage sécurisé de ces composants et dispositifs. Ils peuvent être interconnectés tout au plus par des câbles physiques visibles, afin qu'il soit autant que possible visible jusqu'à la destruction des données confidentielles qu'aucune autre machine ne peut y accéder.

3.11 Les composants fiables ne doivent pas être connectés à Internet pour installer ou mettre à jour des logiciels.

3.12 En principe, les données critiques doivent être détruites après usage. S'il existe de bonnes raisons à cela, un stockage sécurisé du support de données est également autorisé comme solution alternative.

3.13 Les supports destinés à l'échange ou à la conservation de données, tels que les clefs USB, doivent être retirés après le téléchargement des données vers le composant fiable et ne peuvent être réutilisés avant la destruction des données que si le composant fiable était vierge de données critiques avant le téléchargement.

Avant toute utilisation, les supports d'échange de données doivent être reformatés, et toutes les données détruites, au moyen d'un composant exploité conformément aux exigences applicables aux composants fiables.

3.14 Aucun accès logique ou physique à des composants fiables ou à des supports contenant des données critiques ne doit être possible sans qu'une autre personne en soit informée, par ex. en prévoyant que cet accès ne soit possible qu'avec son concours (double contrôle strict).

3.15 Un accès non autorisé réussi à un composant de contrôle ne doit pas, autant que possible, conférer un avantage dans la tentative d'accéder discrètement à un autre composant de contrôle. En plus des autres exigences prévues au ch. 3, on appliquera les exigences suivantes:

- Si une personne dispose d'un accès physique ou logique à un composant de contrôle, elle ne doit avoir accès à aucun autre composant de contrôle.
- Le matériel, les systèmes d'exploitation et les systèmes de surveillance des composants de contrôle doivent autant que possible être différents.
- Les composants de contrôle doivent être connectés à plusieurs réseaux locaux différents.

– Un composant de contrôle doit être matérialisé par un appareil physique. Une virtualisation réalisée au moyen de plusieurs appareils physiques n'est pas admise.

3.16 Les composants de contrôle doivent être conçus pour détecter les accès non autorisés et alerter les personnes responsables. Les personnes responsables doivent prévoir des mesures de surveillance externe, telles que la surveillance et l'enregistrement inviolable du trafic réseau ou la surveillance physique au moyen de caméras placées sous leur contrôle. Les personnes responsables doivent être considérées comme particulièrement loyales et dignes de confiance.

3.17 Les composants fiables ne doivent effectuer que les opérations prévues.

3.18 Le logiciel du dispositif technique des vérificateurs doit provenir d'un autre développeur de système que celui qui a développé la plupart des logiciels des autres composants du système. La publication du logiciel du dispositif technique sous une licence répondant aux critères des logiciels libres[4] peut justifier une exception. Si les vérificateurs utilisent plusieurs dispositifs techniques, cette disposition vaut pour au moins l'un des dispositifs.

3.19 Toutes les procédures impliquant des composants fiables doivent être documentées par écrit et d'une manière facile à comprendre pour les personnes concernées.

3.20 Tout accès et toute utilisation d'un composant fiable ou d'un support de données contenant des données critiques doivent être consignés.

4. Procédure de vote

4.1 Le votant déclare avoir pris connaissance des règles du vote électronique et de la responsabilité qui lui incombe.

4.2 Avant de voter, le votant est informé qu'il prend part au scrutin de la même manière que s'il votait par correspondance ou à l'urne. Le votant ne peut émettre son suffrage qu'une fois qu'il a confirmé qu'il en a été informé.

4.3 Lors du vote, le votant est prié de vérifier les preuves au sens du ch. 2.5 au moyen de la référence de vérification et de signaler au canton tout doute qu'il pourrait avoir sur leur exactitude.

4.4 Tant qu'il n'a pas émis définitivement son suffrage par la voie électronique, l'électeur peut voter via un canal de vote classique.

4.5 Le système client tel qu'il se présente à l'électeur n'influence pas la prise de décision de ce dernier.

4.6 La navigation n'encourage pas un vote hâtif ou irréfléchi.

4 Voir la définition dans le guide intitulé «Praxis-Leitfaden Open Source Software in der Bundesverwaltung» (en langue allemande), version 1.0 du 19.12.2019, chap. 1; disponible auprès de: Chancellerie fédérale suisse, CH-3003 Berne; www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Architecture de la Confédération > Open Source Software (OSS).

4.7 Le système ne propose pas au votant une fonction lui permettant d'imprimer ou de sauvegarder son suffrage.

4.8 Une fois le vote terminé, le votant ne reçoit aucune information sur le contenu du suffrage chiffré qu'il a émis.

4.9 En ce qui concerne les électeurs qui ne sont pas en mesure de voter parce que des tiers ont utilisé indûment leur matériel de vote pour émettre un suffrage, les cantons peuvent les autoriser à voter malgré tout en déclarant nul le suffrage indûment émis. Le secret du vote au sens du ch. 2.7 doit être garanti.

4.10 En ce qui concerne les électeurs souffrant d'un handicap, il peut être prévu des facilités pour la vérification des preuves. Dans ce cas uniquement, il peut être dérogé aux exigences prévues au ch. 2.9.1.

4.11 Tant que le système n'a pas enregistré de confirmation du vote définitif, un électeur peut voter au moyen d'un canal de vote classique.

4.12 L'utilisation d'une méthode d'authentification indépendante du vote électronique est autorisée. Les effets sur l'intégrité de la vérification de la qualité d'électeur et la garantie du secret du vote doivent être examinés en détail dans le cadre de l'appréciation des risques.

5. Préparation du scrutin

5.1 Si les données du registre des électeurs sont importées depuis un système tiers qui n'est pas sous le contrôle du canton, les données doivent être chiffrées et signées. La signature doit être vérifiée à leur réception. Pour la livraison à l'imprimeur, les dispositions du ch. 7 priment.

5.2 Les données nécessaires à la vérification des preuves conformément au ch. 2.6 sont remises aux vérificateurs.

6. Exigences applicables aux cartes de légitimation

6.1 Les cartes de légitimation doivent être conçues dans la mesure du possible de manière à permettre aux électeurs handicapés d'utiliser facilement le vote électronique.

6.2 Il n'est possible d'utiliser des éléments de sécurité sur la carte de légitimation (par ex. un champ à gratter) que s'il a été attesté que les informations dissimulées sont bien protégées contre toute lecture non autorisée.

6.3 S'il n'est pas utilisé d'éléments de sécurité pour protéger les informations confidentielles sur la carte de légitimation, il faut mettre en place des processus organisationnels pour en garantir la sécurité.

7. Exigences applicables aux imprimeries

7.1 Les fichiers d'impression destinés à la production des cartes de légitimation sont envoyés sous forme chiffrée et signée. Il est également possible de remettre personnellement à l'imprimeur un support de données contenant ces fichiers. En ce cas, le support de données est remis à l'imprimeur par deux personnes qui l'ont surveillé ensemble pendant le transport et jusqu'à la remise (double contrôle).

7.2 Le chiffrement doit répondre aux exigences de la norme eCH 0014[5], chap. 7.5. En cas de chiffrement symétrique, l'élément secret permettant le déchiffrement est envoyé aux responsables de l'imprimerie via un canal secondaire sécurisé.

7.3 Les responsables de l'imprimerie qui reçoivent le support de données signent un accusé de réception.

7.4 Le support de données contenant les données d'impression, le composant sur lequel les données critiques sont déchiffrées et tous les composants qui traitent les données critiques sont soumis aux dispositions du ch. 3 relatives au composant d'impression.

7.5 Les responsables de l'imprimerie effectuent un contrôle de la quantité de matériel.

7.6 Après avoir imprimé les cartes de légitimation, l'imprimerie détruit les données reçues.

7.7 Si l'imprimerie se charge également de la mise sous pli et de l'expédition des cartes de légitimation, celles-ci doivent être mises sous pli avec le matériel de vote immédiatement après l'impression.

7.8 Le canal entre les imprimeries et les électeurs ne peut être considéré comme fiable que si les organes compétents en vertu du droit cantonal remettent le matériel de vote sous pli aux électeurs par voie postale ou s'assurent qu'il soit remis en mains propres.

8. Information et assistance

8.1 Le service compétent au niveau cantonal élabore une stratégie pour informer les citoyens sur le vote électronique.

8.2 Cette stratégie garantit que les informations sont autorisées par les organes compétents.

8.3 Sont publiés sur Internet des conseils et des guides sur la manière de voter, ainsi que des informations sur les responsabilités qui incombent aux électeurs. Ils préviennent tout vote hâtif ou irréfléchi.

5 eCH-0014: «Normes et architectures pour les applications de cyberadministration en Suisse (SAGA.ch) », version 9.0 du 09.12.2019; disponible gratuitement auprès de: Association eCH, Mainaustrasse 30, Postfach, 8034 Zürich, www.ech.ch.

8.4 La vérifiabilité, les autres mesures de sécurité et les procédures à suivre en cas d'anomalie sont expliquées aux électeurs de manière aisément compréhensible.

8.5 Les électeurs sont informés de ce à quoi ils doivent faire attention pour pouvoir voter en toute sécurité.

8.6 Il est expliqué aux électeurs comment supprimer après le vote leur suffrage dans tous les espaces mémoire de la plate-forme utilisateur sur laquelle ils ont saisi leur vote.

8.7 Les électeurs peuvent demander une assistance en matière de vote électronique.

8.8 Les électeurs sont invités à signaler au service compétent au niveau cantonal les preuves au sens du ch. 2.5, comme les codes de vérification, qui sont affichées de manière incorrecte, ou les autres vérifications dont les résultats sont négatifs. Cette invitation est également diffusée avec le matériel de vote.

8.9 Les électeurs sont invités à conserver de façon sécurisée le matériel de vote contenant les éléments de sécurité visés au sens du ch. 2.5, jusqu'à ce qu'ils aient émis leur vote de manière définitive ou que le scrutin soit clos.

8.10 Les électeurs reçoivent les informations nécessaires pour vérifier l'authenticité du site Internet utilisé pour voter, du serveur ainsi que du logiciel. La pertinence d'une vérification réussie doit être étayée par l'utilisation de moyens cryptographiques conformes aux meilleures pratiques.

8.11 Les informations essentielles pour garantir un vote sécurisé sont envoyées avec le matériel de vote. Il est expliqué aux électeurs qu'en cas de doute, ils doivent se référer aux informations qui sont fournies avec le matériel de vote et non à celles qui s'affichent sur la plate-forme utilisateur.

8.12 Il est expliqué aux électeurs par quels moyens le secret du vote est assuré.

8.13 Toute faille identifiée et les mesures qu'elle appelle sont communiquées de manière transparente.

8.14 Les vérificateurs doivent être informés et formés de manière adéquate sur les processus dont dépendent l'exactitude du résultat, la garantie du secret du vote et l'impossibilité d'établir des résultats partiels anticipés (par ex. la génération des clefs, l'impression du matériel de vote, le déchiffrement et le dépouillement). Ils sont capables de comprendre les points essentiels des processus et leur signification.

9. Ouverture et fermeture du canal de vote électronique

Le canal de vote électronique n'est disponible que pendant la période autorisée.

10. Contrôle de conformité et enregistrement des suffrages définitifs

Un suffrage qui n'a pas été émis conformément à la procédure prévue par le système n'est pas enregistré dans l'urne électronique.

11. Dépouillement de l'urne électronique

11.1 Le déchiffrement et le dépouillement des suffrages ne peuvent commencer avant le dimanche de l'élection ou de la votation.

11.2 Le canton effectue le déchiffrement et le dépouillement dans sa propre infrastructure.

11.3 Le canton veille à ce que le déchiffrement et le dépouillement des suffrages donnent lieu à procès-verbal. Le service compétent au niveau cantonal approuve ce procès-verbal.

11.4 Depuis le déchiffrement des suffrages jusqu'à la transmission du résultat du scrutin, tout accès au système ou à l'un de ses composants est effectué par au moins deux personnes; il est consigné par écrit et doit pouvoir être contrôlé par les vérificateurs.

11.5 Si les données de résultats sont envoyées à un système tiers qui n'est pas sous le contrôle du canton, ces données sont chiffrées et signées.

11.6 Le système permet d'utiliser la carte de légitimation pour déterminer si une personne a émis un suffrage par voie électronique.

11.7 Les vérificateurs sont présents pendant le déchiffrement et le dépouillement. Les cantons peuvent permettre des travaux de contrôle à distance.

11.8 Les composants utilisés pour le dépouillement des suffrages sont soumis aux mêmes exigences que celles qui s'appliquent aux composants de configuration au sens du ch. 3 s'ils ne sont pas fiables au sens du ch. 2.4.

11.9 Les vérificateurs exercent leurs responsabilités conformément au droit cantonal lorsqu'ils procèdent à la vérification des preuves au sens du ch. 2.6.

11.10 Le service compétent au niveau cantonal soumet aux vérificateurs tous les indicateurs pertinents pour l'exactitude du résultat. Outre les preuves au sens du ch. 2.6, il s'agit notamment du nombre et du type d'anomalies signalées au canton par les électeurs.

11.11 Le canton anticipe les anomalies éventuelles et élabore, en concertation avec les acteurs concernés, un plan d'urgence précisant la conduite à tenir. Il veille à la transparence vis-à-vis du public.

11.12 Dans la mesure où elles sont disponibles et où la base de données le permet, des méthodes statistiques seront utilisées pour établir la plausibilité des résultats.

12. Données confidentielles

12.1 Il est fait en sorte que ni les collaborateurs ni les personnes extérieures n'aient connaissance de données permettant d'établir un lien entre l'identité du votant et le suffrage qu'il a émis.

12.2 Il est fait en sorte que ni les collaborateurs ni les personnes extérieures n'aient connaissance avant le déchiffrement des suffrages de données permettant d'établir des résultats partiels de manière anticipée.

12.3 Le canton ne peut pas transmettre à des entreprises privées la part de la clef de déchiffrement des suffrages qu'il détient en vertu du ch. 3.1 sur le composant de contrôle qu'il exploite.

12.4 Le canton traite les résultats du scrutin de manière confidentielle depuis le moment où les suffrages sont déchiffrés jusqu'à celui de la publication.

12.5 Le canton fait en sorte que soient traitées de manière confidentielle les données qui permettent de déterminer si un électeur a voté par voie électronique.

12.6 Le canton traite les différents suffrages de manière confidentielle après le dépouillement.

12.7 Le canton veille à ce que les résultats des votations et des élections organisées dans les circonscriptions de petite taille soient traités de manière confidentielle.

12.8 Après la validation sont détruites selon un processus préétabli et documenté, toutes les données qui ont été créées au cours du scrutin électronique, qui concernent les différents suffrages enregistrés et qui sont classées comme confidentielles.

13. Menaces

13.1 Les menaces énumérées aux ch. 13.3 à 13.40 sont des menaces d'ordre général et constituent un socle qu'il y a lieu de compléter. Elles se rapportent aux objectifs de sécurité et doivent être prises en compte dans le cadre de l'identification des risques. Selon les vulnérabilités du système qui seront détectées et compte tenu des appréciations des risques des différents services, il y aura lieu de préciser et de compléter cette liste au vu de la constellation en présence et des menaces effectives.

13.2 Sont réputées menaces potentielles:

- les menaces accidentelles ou délibérées émanant d'acteurs humains internes ou externes utilisant des moyens électroniques ou physiques;
- les menaces résultant d'un dysfonctionnement du système ou des éléments de support du système.

	Description	Objectif de sécurité concerné (au sens de l'art. 4, al. 3)
13.3	Un logiciel malveillant modifie le suffrage sur la plate-forme de l'utilisateur.	Exactitude des résultats

	Description	Objectif de sécurité concerné (au sens de l'art. 4, al. 3)
13.4	Un attaquant externe détourne le suffrage au moyen d'un empoisonnement du cache DNS[6].	Exactitude des résultats
13.5	Un attaquant externe modifie le suffrage au moyen de la technique de «l'homme du milieu», ou «MITM»[7].	Exactitude des résultats
13.6	Un attaquant externe envoie au moyen d'une attaque MITM des données corrompues qui sont nécessaires pour émettre le suffrage et qui proviennent du système en ligne (par ex. un fichier Javascript).	Exactitude des résultats
13.7	Un attaquant interne manipule le logiciel, qui n'enregistre alors plus les suffrages.	Exactitude des résultats
13.8	Un attaquant interne modifie, supprime ou multiplie les suffrages.	Exactitude des résultats
13.9	Un attaquant interne ajoute des suffrages dans l'urne électronique.	Exactitude des résultats
13.10	Une organisation hostile pénètre dans le système pour fausser le résultat.	Exactitude des résultats
13.11	Un attaquant interne copie du matériel de vote et l'utilise.	Exactitude des résultats
13.12	Un attaquant externe utilise des méthodes relevant de l'ingénierie sociale pour détourner l'attention du votant des mesures de sécurité (vérifiabilité individuelle).	Exactitude des résultats
13.13	Un attaquant externe pénètre électroniquement, physiquement ou au moyen de procédés d'ingénierie sociale dans l'infrastructure du canton et manipule les composants de configuration ou s'empare de données de sécurité.	Exactitude des résultats

6 L'«empoisonnement du cache DNS » (Domain name server spoofing) est une attaque au cours de laquelle le lien entre un nom d'hôte et l'adresse IP correspondante est faussé.

7 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 logiquement entre les deux partenaires d'une communication et prend totalement le contrôle du trafic de données entre eux ou entre plusieurs périphériques réseau. Il peut consulter les informations à loisir et même les manipuler.

	Description	Objectif de sécurité concerné (au sens de l'art. 4, al. 3)
13.14	Un attaquant externe pénètre électroniquement, physiquement ou au moyen de procédés d'ingénierie sociale dans l'infrastructure de l'imprimerie et s'empare des codes des cartes de légitimation.	Exactitude des résultats
13.15	Un attaquant externe pénètre électroniquement, physiquement ou au moyen de procédés d'ingénierie sociale dans l'infrastructure de La Poste et s'empare de cartes de légitimation.	Exactitude des résultats
13.16	Une erreur se produit dans la vérifiabilité individuelle.	Exactitude des résultats
13.17	Une erreur se produit dans la vérifiabilité universelle.	Exactitude des résultats
13.18	Un dispositif technique des vérificateurs comporte une erreur.	Exactitude des résultats
13.19	Une «porte dérobée»[8] est introduite dans le système via une dépendance logicielle et est mise à profit par un attaquant externe pour accéder au système.	Exactitude des résultats, garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés, accessibilité et capacité opérationnelle du vote électronique, protection contre les manipulations des informations destinées aux électeurs, pas d'usage abusif des preuves relatives au comportement de vote
13.20	Un logiciel malveillant installé sur la plateforme utilisateur envoie le suffrage à une organisation hostile.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés
13.21	Le suffrage est détourné au moyen d'un empoisonnement du cache DNS.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés
13.22	Un attaquant externe lit le suffrage au moyen d'une attaque MITM.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés
13.23	Un attaquant interne utilise la clef et déchiffre des suffrages non anonymisés.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés

8 Dans un logiciel, une «porte dérobée » (backdoor) est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel.

	Description	Objectif de sécurité concerné (au sens de l'art. 4, al. 3)
13.24	Le secret du vote est violé lors de la vérification de l'exactitude du traitement et du dépouillement.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés
13.25	Un attaquant interne lit des suffrages de manière anticipée sans devoir les déchiffrer.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés
13.26	Une organisation hostile pénètre dans le système pour violer le secret du vote ou pour établir des résultats partiels de manière anticipée.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés
13.27	Une erreur dans le processus de chiffrement rend celui-ci inopérant ou réduit son efficacité.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés
13.28	Un attaquant interne manipule le logiciel et celui-ci divulgue les suffrages.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés
13.29	Un logiciel malveillant installé sur l'ordinateur de l'électeur empêche ce dernier de voter.	Accessibilité et capacité opérationnelle du canal de vote
13.30	Une organisation hostile mène une attaque du type «déni de service» (DOS)[9].	Accessibilité et capacité opérationnelle du canal de vote
13.31	Un attaquant interne configure mal le système; le dépouillement ne peut pas se faire.	Accessibilité et capacité opérationnelle du canal de vote
13.32	Un attaquant interne falsifie les preuves cryptographiques de la vérifiabilité universelle.	Accessibilité et capacité opérationnelle du canal de vote
13.33	Une défaillance technique du système fait que le système n'est pas disponible au moment du dépouillement.	Accessibilité et capacité opérationnelle du canal de vote
13.34	Un dispositif technique des vérificateurs ne fonctionne pas au moment du dépouillement.	Accessibilité et capacité opérationnelle du canal de vote

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

	Description	Objectif de sécurité concerné (au sens de l'art. 4, al. 3)
13.35	Une organisation hostile 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.	Accessibilité et capacité opérationnelle du canal de vote, protection contre les manipulations des informations destinées aux électeurs, pas d'usage abusif des preuves relatives au comportement de vote
13.36	Un attaquant interne vole les données concernant les adresses des électeurs.	Protection des informations personnelles concernant les électeurs
13.37	Un logiciel malveillant influence des électeurs pendant qu'ils se forgent une opinion.	Protection contre les manipulations des informations destinées aux électeurs
13.38	Un attaquant interne manipule le site Internet d'information ou le portail de vote et sème la confusion dans l'esprit des électeurs.	Protection contre les manipulations des informations destinées aux électeurs
13.39	Un attaquant interne prescrit à des électeurs si et comment ils doivent voter. Après le déchiffrement, il trouve dans l'infrastructure des pièces justificatives prouvant que les électeurs se sont tenus aux instructions.	Pas d'usage abusif des preuves relatives au comportement de vote
13.40	Un attaquant externe prescrit à des électeurs si et comment ils doivent voter et leur demande une pièce justificative prouvant qu'ils se sont tenus aux instructions.	Pas d'usage abusif des preuves relatives au comportement de vote

14. Détection et annonce d'incidents et de vulnérabilités en matière de sécurité; gestion des incidents en matière de sécurité et des améliorations

14.1 Un système de monitoring de l'infrastructure détecte les incidents qui pourraient menacer la sécurité du système, y compris sa disponibilité, et alerte le personnel compétent. Le personnel en question 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.

Les erreurs d'écriture lors de l'enregistrement d'un suffrage dans les composants de contrôle et dans l'urne sont détectées. Des informations supplémentaires en rapport avec l'erreur doivent être disponibles afin de permettre de

détecter et de corriger l'erreur. Les incidents constatés doivent être signalés au service compétent au niveau cantonal.

14.2 Des procès-verbaux dont la collecte, la transmission et le stockage résistent aux manipulations sont établis dans l'infrastructure (journaux système). Ils sont cohérents entre eux et permettent de retracer les événements pertinents dans le cadre de l'examen de manipulations ou d'erreurs supposées. Ils servent à cet égard de preuve de la prise en compte complète, non falsifiée et exclusive de l'intégralité des suffrages émis conformément à la procédure prévue par le système ainsi que de preuve de la garantie du secret du vote et de l'impossibilité d'établir des résultats partiels anticipés.

Le contenu des procès-verbaux couvre au moins les événements suivants:

- démarrage et arrêt des processus de journalisation, d'identification et d'authentification
- démarrage, redémarrage et fin de la phase de vote
- démarrage du dépouillement comprenant l'établissement des résultats
- réalisation d'éventuels autotests et résultats de ces derniers
- dysfonctionnements qui ont été identifiés dans les éléments de l'infrastructure informatique et qui compromettent la capacité opérationnelle

Il documente par ailleurs la date et l'heure, le type d'événement, l'auteur potentiel et le résultat, en termes d'échec ou de réussite.

Les journaux système sont mis à la disposition du service compétent au niveau cantonal sous une forme qui lui permette d'en interpréter les informations.

14.3 Le monitoring et l'établissement des procès-verbaux sont soumis à un processus d'amélioration continue. Ce processus inclut un dialogue ouvert entre les parties prenantes et une évaluation objective régulière de l'efficacité des instruments et des processus mis en œuvre. Les résultats des évaluations sont pris en compte dans ce cadre.

14.4 Le monitoring et la collecte des journaux système ne compromettent en aucun cas l'efficacité des mesures destinées à garantir le secret du vote.

14.5 Il est garanti que les suffrages et les données qui prouvent le bon fonctionnement de la procédure de dépouillement des suffrages sont, en cas de panne, enregistrés dans l'infrastructure sans subir d'altérations.

14.6 Après une panne du système ou une défaillance des moyens de communication ou d'enregistrement, le système passe dans un mode «reprise sur panne» qui donne la possibilité de retourner à un mode de fonctionnement sûr. En particulier, les procédures de vote qui ont débuté sont interrompues. Le votant ne peut reprendre la procédure de vote que lorsque le système est de nouveau dans un mode de fonctionnement sûr.

14.7 Il est 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 est consigné dans un procès-verbal. Les suffrages de contrôle dépouillés sont comparés avec ceux qui sont consignés dans les procès-verbaux.

Il est garanti non seulement que les suffrages de contrôle seront traités dans toute la mesure du possible de manière similaire aux suffrages émis conformément à la procédure prévue par le système, mais aussi qu'ils ne seront pas comptabilisés.

14.8 La disponibilité de l'infrastructure est contrôlée et consignée dans un procès-verbal à des intervalles déterminés.

14.9 Toutes les parties du système de vote sont régulièrement mises à jour moyennant un processus préétabli et documenté afin que les vulnérabilités identifiées soient éliminées.

14.10 Les mesures qui servent à la surveillance et à l'établissement des procès-verbaux de l'utilisation du système et des activités des administrateurs, ainsi qu'à l'établissement des procès-verbaux des dysfonctionnements, sont décrites de manière détaillée, mises en œuvre, suivies et vérifiées.

15. Utilisation de mesures cryptographiques et gestion des clefs

15.1 Les certificats électroniques sont gérés selon les meilleures pratiques.

15.2 Des mesures cryptographiques efficaces correspondant à l'état de la technique garantissent l'intégrité des données sous-tendant l'exactitude des résultats et la confidentialité des données critiques, y compris des données d'identification et d'authentification concernant les autorités.

15.3 Dans l'infrastructure, des mesures cryptographiques efficaces correspondant à l'état de la technique garantissent la confidentialité des données critiques. Ces données sont toujours enregistrées sur des supports sous une forme chiffrée.

15.4 Des éléments de base cryptographiques sont utilisés uniquement quand la longueur des clefs et les algorithmes correspondent aux normes courantes (par ex. NIST, ECRYPT, SCSE). La signature électronique satisfait aux exigences d'une signature électronique avancée au sens de la loi du 18 mars 2016 sur la signature électronique (SCSE)[10]. La vérification de la signature se fait au moyen d'un certificat électronique délivré par un fournisseur de services de certification reconnu au sens de la SCSE.

16. Échange d'informations électronique et physique sûr

16.1 Tous les composants de l'infrastructure sont exploités dans une zone réseau séparée. Cette zone est protégée par rapport au reste du réseau au moyen d'un contrôle de routage adéquat.

16.2 Le vote électronique est de manière générale clairement séparé de l'ensemble des autres applications.

10 RS **943.03**

17. Tests du système

17.1 Les fonctions pertinentes pour la sécurité du système (fonctions de sécurité) sont testées. Les tests sont documentés au moyen de plans de test et au moyen des résultats attendus et des résultats effectifs des tests.

Le plan de test:

- détermine les tests qui doivent être exécutés;
- décrit les scénarios de chaque test, y compris les éventuelles dépendances par rapport aux résultats d'autres tests.

Les résultats attendus doivent montrer les résultats escomptés d'une exécution réussie des tests.

Les résultats effectifs doivent correspondre aux résultats attendus.

17.2 Une analyse de la couverture des tests est réalisée. Elle démontre:

- que les tests définis dans la documentation de test et les spécifications fonctionnelles des interfaces correspondent;
- que toutes les interfaces ont été complètement testées.

17.3 Une analyse de la profondeur des tests est réalisée. Elle démontre:

- que les tests définis dans la documentation de test et les sous-systèmes relatifs aux fonctions de sécurité et aux modules ayant un rôle dans la garantie de la sécurité correspondent;
- que tous les sous-systèmes relatifs aux fonctions de sécurité figurant dans les spécifications ont été testés;
- que tous les modules ayant un rôle dans la garantie de la sécurité ont été testés.

18. Organisation de la sécurité des informations

18.1 Tous les rôles et toutes les responsabilités concernant l'exploitation du système sont précisément définis, attribués et communiqués.

18.2 La configuration initiale de l'infrastructure, qu'il s'agisse du matériel, du logiciel ou des droits d'accès, et toute modification doivent avoir été approuvées au préalable.

18.3 Les risques liés à des tiers (mandataires tels que fournisseurs et prestataires) sont identifiés et réduits autant que nécessaire moyennant la conclusion de conventions contractuelles adéquates. Le respect de ces conventions est surveillé et vérifié de manière appropriée pendant leur durée de validité.

19. Gestion des ressources matérielles ou immatérielles

19.1 Toutes les ressources matérielles ou immatérielles qui correspondent à un actif 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[11] et qui sont pertinentes pour le vote électronique (organisation dans son ensemble, en particulier les processus organisationnels et les informations traitées dans le cadre de ces processus; les supports de données; les installations de traitement des données de l'infrastructure; les locaux de l'infrastructure) sont répertoriées dans un inventaire. Une liste recensant le personnel doit être dressée. L'inventaire et la liste du personnel sont tenus à jour. Chaque ressource matérielle ou immatérielle est attribuée à une personne qui en prend la responsabilité.

19.2 L'utilisation licite de ressources matérielles ou immatérielles est définie.

19.3 Des directives régissant la classification des informations sont édictées et communiquées.

19.4 Des procédures régissant le marquage et la gestion des informations sont définies.

20. Fiabilité du personnel

20.1 Pour garantir la fiabilité du personnel avant, pendant et après la période d'engagement ou en cas de changement de rôle, des directives et des procédures adéquates sont élaborées et diffusées.

20.2 Les décideurs du personnel assument l'entière responsabilité de la garantie de la fiabilité du personnel.

20.3 L'ensemble du personnel possède une sensibilité marquée en matière de sécurité des informations. À cette fin est mis en place et lancé un programme de formation et d'entraînement qui soit adapté aux tâches.

21. Sécurité physique et sécurité liée à l'environnement

21.1 Les périmètres de sécurité des différents locaux de l'infrastructure sont clairement définis.

21.2 Des autorisations d'accès sont définies, créées et contrôlées de manière adéquate pour l'accès physique aux différents locaux de l'infrastructure.

21.3 Pour garantir la sécurité des appareils à l'intérieur et à l'extérieur des locaux de l'infrastructure, des directives et des procédures adéquates sont définies et leur respect est surveillé et vérifié.

21.4 Toutes les données sont traitées, notamment conservées, exclusivement en Suisse.

11 Le texte peut être consulté ou obtenu contre paiement auprès de: Secrétariat central de l'Organisation internationale de normalisation (ISO), Chemin de Blandonnet 8, CP 401, 1214 Vernier, www.iso.org.

22. Gestion de la communication et de l'exploitation

22.1 Les obligations et les domaines de responsabilité sont 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 aux risques.

22.2 Des mesures de protection appropriées sont prises contre les logiciels malveillants.

22.3 Un plan détaillé pour la sécurisation des données est établi et mis en œuvre. Le bon fonctionnement de la sécurisation des données est vérifié à intervalles réguliers.

22.4 Des mesures adéquates sont définies et mises en œuvre pour assurer la protection du réseau contre les menaces qui ont été identifiées dans l'appréciation des risques visée à l'art. 4 en rel. avec le ch. 13, ainsi que la sécurité des services du réseau.

22.5 Les procédures relatives à l'utilisation de supports de données amovibles et à l'élimination de supports de données sont réglées en détail.

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

23.1 Pendant le scrutin, il est garanti que toute modification des droits d'accès apportée ultérieurement ne pourra être effectuée qu'en accord avec le service compétent au niveau cantonal.

23.2 L'accès à l'infrastructure et au logiciel est réglé et documenté en détail sur la base d'une appréciation des risques. Le principe du double contrôle s'applique dans les domaines présentant des risques élevés et pour toutes les opérations manuelles en rapport avec l'urne (par ex. ouverture du canal de vote, fermeture du canal de vote et début du dépouillement).

Les opérations manuelles en rapport avec l'urne électronique (par ex. ouverture du canal de vote, fermeture du canal de vote et début du dépouillement) sont authentifiées explicitement.

23.3 Il est impossible, à moins de 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.

23.4 Pendant le scrutin, aucune intervention étrangère ne peut avoir lieu dans l'infrastructure.

23.5 Il est garanti qu'aucun des éléments des données d'authentification client ne pourra être systématiquement intercepté, modifié ou détourné au moment de la remise. L'authentification se fait au moyen de mesures et de technologies permettant de réduire suffisamment le risque d'abus systématique par des tiers.

24. Développement et maintenance de systèmes d'information

24.1 Développement

24.1.1 Il est défini un modèle de cycle de vie. Celui-ci:
- est utilisé pour le développement et la maintenance du logiciel;
- prévoit les contrôles nécessaires dans le développement et la maintenance du logiciel;
- est documenté.

24.1.2 Une liste des outils de développement utilisés et de leurs options de configuration sélectionnées pour la mise en œuvre de chaque outil est établie.

24.1.3 La documentation de chaque outil de développement:
- contient une définition de l'outil;
- définit toutes les conventions et directives utilisées dans la mise en œuvre de l'outil;
- définit sans ambiguïté la signification de toutes les options de configuration pour l'utilisation de l'outil.

24.1.4 Les standards d'implémentation sont définis et appliqués.

24.1.5 Le logiciel est spécifié et implémenté de telle sorte que les fonctions de sécurité ne puissent pas être contournées.

24.1.6 Les fonctions de sécurité sont spécifiées et implémentées de telle sorte qu'elles soient protégées contre les manipulations.

24.1.7 L'architecture de sécurité du logiciel est documentée. La documentation:
- possède un niveau de détail correspondant à la description des fonctions de sécurité;
- décrit les domaines de sécurité qui reposent sur les fonctions de sécurité;
- décrit la manière dont les procédures d'initialisation sont sécurisées;
- démontre que les exigences fixées aux ch. 24.1.5 et 24.1.6 sont remplies.

24.1.8 Les spécifications fonctionnelles sont documentées. La documentation:
- représente l'entier du logiciel;
- décrit l'objectif et le mode d'utilisation de toutes les interfaces;
- identifie et décrit tous les paramètres associés aux interfaces;
- décrit toutes les actions associées aux interfaces;
- décrit tous les messages d'erreur directs pouvant résulter de l'appel de chaque interface.

24.1.9 La traçabilité entre les spécifications fonctionnelles et les exigences de sécurité est garantie et va jusqu'au niveau des interfaces.

24.1.10 Toutes les fonctions de sécurité sont implémentées dans le code source.

24.1.11 La traçabilité entre l'entier du code source et les spécifications des fonctions de sécurité doit être garantie, et leur correspondance est manifeste.

24.1.12 Les fonctions de sécurité sont conçues et implémentées de telle sorte qu'elles soient bien structurées. La structure interne est décrite et comprend une justification:

- qui indique les caractéristiques utilisées pour évaluer les notions de «bien structuré» et de «complexe»;
- qui démontre que toutes les fonctions de sécurité sont bien structurées et qu'elles ne sont pas trop complexes.

24.1.13 Les spécifications:

- décrivent la structure du logiciel en termes de sous-systèmes;
- décrivent les fonctions de sécurité en tant que modules, l'objectif de chaque module et les relations que chaque module a avec les autres modules; la description des modules ayant un rôle dans le renforcement de la sécurité comprend en plus les interfaces disponibles, les valeurs de retour de ces interfaces et les interfaces des autres modules utilisés pour interagir avec eux;
- décrivent tous les sous-systèmes relatifs aux fonctions de sécurité, y compris les interactions qu'ils peuvent avoir entre eux;
- démontrent par une représentation claire des sous-systèmes associés aux fonctions de sécurité que toutes les interfaces sont conformes au comportement décrit dans la spécification; la représentation doit comporter un niveau de détail allant au moins jusqu'aux modules.

24.1.14 Le logiciel est muni d'une référence univoque.

24.1.15 La documentation de la gestion de la configuration:

- décrit la manière dont les éléments de configuration sont identifiés;
- contient un plan de gestion de la configuration qui décrit comment le système de gestion de la configuration est utilisé dans le cadre du développement du logiciel et quelles sont les procédures appliquées pour la reprise de modifications ou de nouveaux éléments;
- démontre que les procédures de reprise des modifications dans un élément de configuration prévoient un contrôle adéquat de ces dernières pour tous les éléments de configuration.

24.1.16 Le système de gestion de la configuration:

- identifie chacun des éléments de configuration de manière univoque;
- fournit des mesures automatisées de sorte que seules les modifications autorisées soient apportées aux éléments de configuration;
- soutient le développement du logiciel par des procédures automatisées;
- garantit que la personne chargée d'accepter l'élément de configuration n'est pas celle qui l'a développé;
- identifie les éléments de configuration qui composent les fonctions de sécurité;
- soutient par des moyens automatisés le contrôle de tous les changements apportés au logiciel, y compris en consignant le nom de l'auteur de la modification ainsi que la date et l'heure de cette dernière;

- fournit une procédure automatisée pour l'identification de tous les éléments de configuration concernés par la modification d'un élément de configuration déterminé;
- est capable d'identifier la version du code source sur la base de laquelle le logiciel est généré.

24.1.17 Tous les éléments de configuration sont répertoriés dans le système de gestion de la configuration.

24.1.18 Le système de gestion de la configuration est utilisé conformément au plan de gestion de la configuration.

24.1.19 Il est établi une liste de configuration contenant les éléments ci-après:

- le logiciel proprement dit;
- les preuves des contrôles nécessaires au respect de la sécurité;
- les parties qui composent le logiciel;
- le code source;
- l'historique des changements[12];
- les rapports relatifs aux failles de sécurité et à l'état d'avancement des mesures prises pour y remédier.

Le développeur de chaque élément pertinent pour les fonctions de sécurité est mentionné. Chaque élément est identifié de manière univoque.

24.1.20 La documentation de la sécurité du développement du logiciel:

- décrit les mesures de sécurité physiques, procédurales, relatives au personnel et autres qui sont nécessaires pour protéger le logiciel et l'intégrité de sa conception et de son implémentation dans leur environnement de développement;
- démontre que les mesures de sécurité assurent le niveau de protection nécessaire au maintien de l'intégrité du logiciel.

24.2 Exploitation

24.2.1 Il est établi un guide opérationnel. Pour chaque rôle utilisateur, celui-ci:

- décrit les fonctions auxquelles l'utilisateur a accès et les autorisations qui doivent être contrôlées dans un environnement sécurisé, y compris les avertissements en la matière;
- décrit comment utiliser les interfaces disponibles de manière sécurisée;
- décrit les fonctions et interfaces disponibles, en particulier tous les paramètres de sécurité qui se trouvent sous le contrôle de l'utilisateur, en indiquant les valeurs pertinentes pour la sécurité;
- présente de façon précise chaque type d'événement de sécurité en rapport avec les fonctions accessibles à l'utilisateur qui doivent être exécutées, y

12 L'historique des changements (Commit History) consiste en une liste ordonnée de toutes les modifications apportées à un référentiel, avec pour chaque modification le motif qui la justifie.

compris les modifications des caractéristiques de sécurité des éléments sous le contrôle des fonctions de sécurité;
- décrit les mesures de sécurité à mettre en œuvre pour atteindre les objectifs de sécurité opérationnels.

24.2.2 Le guide opérationnel identifie tous les modes d'exploitation possibles du logiciel, y compris la reprise de l'exploitation après la découverte d'erreurs et la description des conséquences et implications de ces erreurs pour le maintien d'une exploitation sûre.

24.2.3 Le guide opérationnel est précis et adéquat.

24.3 Compilation et déploiement fiables et vérifiables

24.3.1 La procédure de préparation décrit toutes les étapes nécessaires:
- à une réception sûre des composants du système dans le respect de la procédure de livraison;
- à une préparation sûre de l'environnement d'exploitation dans le respect des objectifs de sécurités opérationnels;
- à une installation sûre du logiciel dans l'environnement d'exploitation.

24.3.2 La livraison du logiciel ou de parties du système est documentée et comprend toutes les procédures qui sont nécessaires au maintien de la sécurité lors de la livraison du logiciel.

24.3.3 Il est réalisé une compilation fiable et vérifiable au moyen de mesures de sécurité adéquates pour garantir que le code exécutable est une représentation vérifiable et fidèle du code source qui a été soumis à un contrôle public et à des audits indépendants. Cette compilation permet d'établir une chaîne de preuves pour la vérification du logiciel, et démontre en particulier:
- que l'environnement de compilation est tel que décrit sur la plate-forme publique (ensemble des outils avec leur version, système d'exploitation et configurations éventuelles); les divergences qui pourraient exister sont documentées et justifiées;
- que le logiciel a été compilé selon les instructions disponibles sur la plate-forme publique; si un défaut est détecté dans les instructions au moment de la compilation, il doit être consigné, et la documentation adaptée par la suite;
- que le code source soumis au contrôle public et audité est bien celui utilisé pour la compilation;
- qu'aucun autre élément que ceux prévus dans les instructions n'a été introduit;
- que toutes les signatures cryptographiques des dépendances ont été vérifiées sur la base d'une référence établie, publique et fiable;
- qu'une analyse des vulnérabilités concernant les dépendances a été conduite et, si des vulnérabilités pertinentes pour le logiciel existent, qu'elles ne le rendent pas vulnérable aux attaques;

– que les éventuels paramètres qui ont été introduits ne rendent pas le système vulnérable.

24.3.4 Il est réalisé un déploiement fiable et vérifiable au moyen de mesures de sécurité adéquates, qui garantit:

1. que le code déployé en production soit une représentation vérifiable et fidèle du code source qui a été soumis à un contrôle public et à des audits indépendants, et
2. que l'environnement de production soit conforme à celui qui a été soumis au contrôle public et aux audits indépendants.

Le déploiement permet d'établir une chaîne de preuves pour la vérification du logiciel. Il démontre en particulier:

– que l'environnement de production est conforme à celui qui a été soumis au contrôle public et aux audits indépendants; les éventuelles divergences (version du *firmware*, fichiers de configuration, etc.) sont documentées et justifiées;
– que le logiciel déployé dans l'environnement de production est bien celui qui a été produit au cours de la procédure de compilation fiable et vérifiable;
– que les éventuels paramètres qui ont été introduits ne rendent pas le système vulnérable.

24.3.5 La qualité des preuves de la compilation fiable et vérifiable et du déploiement fiable et vérifiable doit être attestée par la présence d'au moins deux témoins issus d'organisations différentes ou par des procédés techniques propres à établir la vérité en fonction de l'état des connaissances scientifiques et de l'expériences acquise.

24.3.6 La chaîne de preuves de la compilation fiable et vérifiable et du déploiement fiable et vérifiable est rendue publique.

24.4 Correction systématique des failles

24.4.1 Il est défini des procédures de correction des failles. Ces procédures:

– comprennent une documentation, en particulier en ce qui concerne la traçabilité des failles pour chaque version du logiciel et les méthodes utilisées pour fournir aux utilisateurs du système des informations sur les failles, les corrections et les mesures correctives possibles;
– exigent une description de la nature et des effets de chaque faille de sécurité ainsi que des informations sur l'état des travaux visant à trouver un correctif et sur les mesures correctives qui ont été arrêtées;
– décrivent les moyens par lesquels les utilisateurs du système peuvent porter à la connaissance du développeur du logiciel des rapports et des requêtes concernant des failles supposées affecter le logiciel;
– comprennent une procédure exigeant une réponse rapide et l'envoi automatique de rapports sur les failles de sécurité et les correctifs en la matière aux utilisateurs du système enregistrés qui pourraient être affectés par la faille de sécurité.

24.4.2 Il est défini une procédure de traitement des failles signalées. Cette procédure:
- garantit que toute faille signalée et confirmée sera corrigée et que les procédures de correction seront communiquées aux utilisateurs du système;
- prévoit des mesures garantissant que toute correction de failles de sécurité n'entraînera pas de nouvelles failles.

24.4.3 Il est défini des directives régissant le signalement et le traitement des failles. Ces directives:
- fournissent aux utilisateurs du système des instructions sur la manière de signaler au développeur toute faille de sécurité supposée;
- fournissent aux utilisateurs du système des instructions sur la manière de s'enregistrer auprès du développeur pour recevoir les rapports sur les faille de sécurité et les correctifs;
- indiquent les services à contacter pour l'envoi des rapports et des demandes de renseignements sur les problèmes de sécurité concernant le logiciel.

24.5 Assurance qualité

Il est vérifié régulièrement et objectivement que les processus exécutés et les produits associés correspondent à la description des processus, des normes et des procédures qui doivent être mis en œuvre. Les divergences font l'objet d'un suivi jusqu'à leur élimination.

25. Qualité du code source et de la documentation

Le code source et la documentation répondent au moins aux critères suivants:

25.1 Traçabilité

25.1.1 Définition: propriété du logiciel qui fournit un fil conducteur depuis les exigences jusqu'à la mise en œuvre.

25.1.2 Toutes les exigences applicables au protocole cryptographique sont traçables pour l'ensemble des résultats des opérations de travail liés au processus de développement du logiciel.

25.1.3 Le lien entre les exigences juridiques et le protocole cryptographique, les spécifications et la documentation de l'architecture est décrit.

25.2 Complétude

25.2.1 Définition: propriété du logiciel qui permet la mise en œuvre complète des fonctions requises.

25.2.2 Le logiciel ne contient pas de références ambigües (entrée, fonction, sortie). Le même terme est utilisé partout où un même élément est référencé.

25.2.3 Toutes les données référencées et toutes les fonctions utilisées sont définies dans les spécifications.

25.2.4 Toutes les fonctions définies dans les spécifications sont utilisées.

25.2.5 Toutes les variantes possibles sont définies dans les spécifications pour chaque élément de décision (par ex. exécution conditionnelle).

25.2.6 Tous les paramètres sont définis dans les spécifications et validés (pas de passage implicite de paramètres).

25.2.7 Toutes les erreurs graves qui ont été signalées sont corrigées avant le passage à l'étape suivante du cycle de développement.

25.2.8 Le protocole cryptographique, la spécification, l'architecture et le code source sont alignés.

25.3 Cohérence

25.3.1 Définition: propriété du logiciel qui fournit des techniques et une notation uniformes dans la conception et la mise en œuvre.

25.3.2 Les représentations figurant dans la documentation suivent une convention établie par le développeur du logiciel.

25.3.3 Les fonctions et les variables suivent une convention de nommage établie par le développeur du logiciel.

25.3.4 Le traitement des entrées et des sorties des fonctions suit une convention établie par le développeur du logiciel.

25.3.5 Le traitement des erreurs suit une convention établie par le développeur du logiciel.

25.3.6 Les types de variables utilisés sont cohérents.

25.4 Uniformité de la communication

25.4.1 Définition: propriété du logiciel qui permet l'utilisation de protocoles et de routines d'interface standardisés.

25.4.2 Les règles régissant la communication avec d'autres systèmes sont définies.

25.4.3 La communication repose sur des méthodes standardisées.

25.5 Uniformité des données

25.5.1 Définition: propriété du logiciel qui permet d'utiliser une représentation standardisée des données.

25.5.2 La représentation standardisée des données pour la communication avec d'autres systèmes est définie de manière formelle.

25.5.3 Des normes de conversion entre les différentes représentations sont définies.

25.5.4 Les fonctions de conversion sont centralisées dans un seul module.

25.6 Facilité d'apprentissage

25.6.1 Définition: propriété du logiciel qui permet à l'utilisateur de se familiariser facilement avec son fonctionnement.

25.6.2 Les personnes qui exploitent et utilisent le système sont formées et reçoivent la documentation nécessaire.

25.6.3 La formation comprend la possibilité de s'entraîner sur un système prévu à cet effet.

25.6.4 Des aides techniques sont facilement accessibles.

25.7 Opérabilité

25.7.1 Définition: propriété du logiciel qui facilite les interactions entre les utilisateurs et le système.

25.7.2 Le logiciel est convivial. La navigation se fait selon des schémas connus.

25.7.3 La partie client du système, telle qu'elle se présente à l'électeur, est conforme à la norme d'accessibilité eCH-0059[13], à l'exception des exigences de la norme relatives aux formes alternatives de communication prévues au chapitre 2.4. Les cantons veillent à ce que cela soit attesté par un service techniquement compétent.

25.8 Tolérance aux erreurs

25.8.1 Définition: propriété du logiciel qui permet la continuité des opérations dans des conditions exceptionnelles.

25.8.2 Les erreurs sont détectées et traitées de sorte que le programme puisse continuer de fonctionner sans interruption.

25.8.3 Le traitement des erreurs, y compris l'enregistrement dans le procès-verbal, est fait au niveau le plus pertinent pour la continuité des opérations. Une erreur qui ne peut être traitée à un niveau donné est transférée au niveau supérieur.

25.8.4 Des conditions de validité sont définies pour les paramètres d'entrée.

25.8.5 Tous les paramètres d'entrée sont vérifiés avant le début de l'exécution.

25.9 Modularité

25.9.1 Définition: propriété du logiciel qui fournit une structure comprenant des modules hautement indépendants.

25.9.2 Chaque module possède une responsabilité bien définie.

25.9.3 La responsabilité d'un module doit être restreinte et ciblée. Les responsabilités de deux modules ne doivent pas se chevaucher.

25.9.4 Les modules ne partagent pas de données par le biais d'une mémoire volatile commune (par ex. variable globale).

13 eCH-0059: Accessibility Standard, version 3.0 du 25.06.2020; disponible gratuitement auprès de: association eCH, Mainaustrasse 30, Postfach, 8034 Zürich, www.ech.ch.

25.10 Simplicité

25.10.1 Définition: propriété du logiciel qui permet la mise en œuvre des fonctions de la manière la plus compréhensible possible. En général, il s'agit d'éviter les pratiques qui augmentent la complexité.

25.10.2 Une approche top-down (structure hiérarchique) est adoptée dans la conception.

25.10.3 La conception ne prévoit pas de fonction dupliquée entre les modules.

25.10.4 La conception ne prévoit pas de données de portée globale, c.-à-d. de données pouvant être utilisées partout sans être passées en paramètres.

25.10.5 Les combinaisons booléennes complexes sont évitées autant que possible dans le code source.

25.10.6 Les variables ne sont pas réutilisées pour d'autres usages que ceux prévus initialement dans le code source.

25.10.7 Le nombre d'imbrications est limité autant que possible dans le code source.

25.10.8 La complexité cyclomatique et cognitive est limitée autant que possible dans le code source.

25.11 Concision

25.11.1 Définition: propriété du logiciel qui permet la mise en œuvre dans le code source d'une fonction avec le moins possible d'instructions.

25.11.2 Le code source ne contient pas de code mort.

25.11.3 Le code source ne contient pas de variables inutiles.

25.11.4 Le code source ne devrait pas contenir de duplications.

25.12 Intelligibilité

25.12.1 Définition: propriété du logiciel qui permet aux destinataires d'en déterminer les objectifs, les hypothèses, les contraintes, les entrées, les sorties, les composants et le statut.

25.12.2 Les classes, les fonctions et les étapes de traitement complexes sont commentées dans le code source selon une convention établie par le développeur du logiciel.

25.12.3 Les variables et les fonctions ont des noms évocateurs.

25.12.4 Le code source comprend une instruction par ligne, sauf si une répartition sur plusieurs lignes permet d'améliorer la lisibilité. On évitera de saisir plusieurs instructions sur une seule ligne.

25.13 Instrumentation

25.13.1 Définition: propriété du logiciel qui permet d'en mesurer l'utilisation ou d'identifier des erreurs.

25.13.2 Les tests unitaires[14] couvrent tous les chemins possibles et les limites entre valeurs autorisées et valeurs non autorisées des paramètres d'entrée.

25.13.3 Les tests d'intégration couvrent tous les modules.

25.13.4 Les scénarios de test système couvrent tous les modules.

25.13.5 Les erreurs et les informations nécessaires sont consignées dans des fichiers journaux.

26. Critères de contrôle pour les systèmes et leur exploitation

26.1 Contrôle du protocole cryptographique (art. 10, al. 1, let. a)

26.1.1 Objet: Il est examiné:

- si les exigences figurant à l'art. 5 en rel. avec les art. 6 à 8 et avec le ch. 2 de l'annexe sont remplies; cette évaluation doit se faire notamment à l'aide des preuves de conformité cryptographiques et symboliques;
- si le protocole cryptographique repose sur des protocoles et des éléments existants qui ont fait leurs preuves et dans quelle mesure;
- si des approfondissements et des améliorations peuvent contribuer à renforcer la sécurité, et lesquels.

26.1.2 Compétences: Le contrôle est effectué par des experts en cryptographie. Il est commandé par la ChF, qui vérifie qu'il est exécuté dans le respect du mandat.

26.1.3 Date du contrôle:

- Un contrôle complet est effectué avant la première mise en service.
- Le contrôle est répété après deux ou trois ans.
- Le protocole cryptographique est soumis à un nouveau contrôle:
  - à chaque fois qu'il est modifié, ou
  - lorsque la recherche fait émerger de nouvelles connaissances pertinentes relatives à la sécurité des éléments cryptographiques utilisés ou à la menace.

26.2 Contrôle du logiciel du système (art. 10, al. 1, let. b)

26.2.1 Objet: Il est examiné:

- si le protocole cryptographique contrôlé en vertu du ch. 26.1 est mis en œuvre; la mise en œuvre correcte des fonctions des composants fiables sera soumise à un contrôle particulièrement approfondi;
- si le logiciel du système remplit les exigences de la présente ordonnance et contribue à la réalisation des objectifs fixés;
- si la partie du système, telle qu'elle se présente à l'électeur, est conforme à la norme eCH-0059 comme le prévoit le ch. 25.7.3; la vérification peut

14 Un test unitaire consiste pour le programmeur à tester un module, indépendamment du reste du programme, afin de s'assurer qu'il répond aux spécifications fonctionnelles et qu'il fonctionne correctement en toutes circonstances. Cette vérification est considérée comme essentielle pour les applications critiques.

s'appuyer sur un certificat valide ou sur un rapport d'audit ayant été établi par une institution reconnue par la ChF et attestant de la conformité avec ladite norme.

26.2.2 Compétences: Le contrôle doit être effectué par des experts en cryptographie et en développement de logiciels. Il est commandé par la ChF.

26.2.3 Date du contrôle:

- Un contrôle complet est effectué avant la première mise en service.
- Le contrôle est répété après deux ou trois ans.
- Le logiciel du système est soumis à un nouveau contrôle à chaque modification majeure est opérée, notamment:
  - après toute modification du protocole cryptographique;
  - après toute modification, dans le code source, des fonctions dont la fiabilité est déterminante pour le caractère concluant des preuves prévues dans le cadre de la vérifiabilité;
  - lorsque la recherche fait émerger de nouvelles connaissances pertinentes relatives à la sécurité des éléments cryptographiques utilisés ou à la menace;
  - lorsqu'il est renoncé à recourir à des mécanismes garantissant le fonctionnement sûr de composants fiables au sens du ch. 2, ou que des modifications majeures sont apportées à ces mécanismes.

26.3 Contrôle de la sécurité de l'infrastructure et de l'exploitation (art. 10, al. 1, let. c)

26.3.1 Objet: Il est examiné:

- si le système et son exploitation par le canton, par l'exploitant du système et par l'imprimerie répondent aux exigences de la présente ordonnance et contribuent de façon appropriée à la réalisation des objectifs fixés;
- si les composants de base, comme le logiciel qui concourt à l'utilisation sûre et indépendante des composants de contrôle, les systèmes d'exploitation utilisés ou les serveurs utilisés correspondent aux meilleurs standards reconnus.

26.3.2 Compétences: Le contrôle est effectué par des experts en cryptographie et en exploitation de systèmes hautement sécurisés. Il est commandé par la ChF.

26.3.3 Date du contrôle:

- Un contrôle complet est effectué avant la première mise en service.
- Le contrôle est répété après deux ou trois ans.
- Un nouveau contrôle est effectué chaque fois qu'une modification majeure est opérée, notamment:
  - après une modification du protocole cryptographique;
  - lorsqu'il est renoncé à recourir à des mécanismes garantissant le fonctionnement sûr de composants fiables au sens du ch. 2, ou que des modifications majeures sont apportées à ces mécanismes;
  - en cas de modification majeure des processus ou de l'infrastructure.

– Si des nouvelles versions de composants de base sont utilisés (nouveau serveur, patchs pour le système d'exploitation ou pour le logiciel qui concourt à l'utilisation sûre et indépendante de composants fiables au sens du ch. 2), il n'est pas nécessaire d'effectuer un nouveau contrôle pour autant que les composants de base correspondent toujours aux meilleurs standards reconnus.

26.4 Contrôle de la protection contre les tentatives d'intrusion dans l'infrastructure (art. 10, al. 1, let. d)

26.4.1 Objet: Il est examiné si des experts mandatés par la ChF parviennent dans le cadre de la participation à un test à pénétrer dans l'infrastructure du système en ligne et ainsi à se ménager l'accès à des données importantes ou à prendre le contrôle de fonctions importantes.

Les tests sont réalisés sur la base de vulnérabilités potentielles découvertes à la suite d'une analyse méthodique des documents qui ont été publiés, en vertu notamment de l'art. 11.

26.4.2 Compétences: Le contrôle est effectué par des experts en sécurité. Il est commandé par la ChF.

26.4.3 Date du contrôle:

– Un contrôle complet est effectué avant la première mise en service.
– Le contrôle est répété après deux ou trois ans.
– Le contrôle est effectué à chaque modification majeure de l'infrastructure.
– Le contrôle est effectué en cas d'émergence de nouvelles connaissances pertinentes relatives à la sécurité des moyens d'exploitation utilisés ou à la menace.

26.5 Contrôle du système de management de la sécurité de l'information (art. 10, al. 2)

26.5.1 Objet: Il est examiné si le SMSI de l'exploitant du système est conforme à 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 englobe toutes les unités organisationnelles de l'exploitant du système qui sont responsables du système sur les plans juridique, administratif et opérationnel.

26.5.2 Compétences: L'organisme de certification est accrédité par le Service d'accréditation suisse (SAS) pour pouvoir effectuer des audits 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 contrôle est commandé par le canton ou par l'exploitant du système; le canton veille à ce qu'il soit effectué.

26.5.3 Durée de validité d'une pièce justificative: Les audits de renouvellement sont effectués aux intervalles prescrits par la norme ISO/IEC 27001:2013, Technologies de l'information – Techniques de sécurité – Systèmes de

management de la sécurité de l'information – Exigences. Un certificat valide et la déclaration d'applicabilité (*Statement of Applicability*) sont présentés à chaque utilisation. Si une nouvelle version de la norme ISO/IEC 27001:2013, Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences est publiée, la preuve que le SMSI dispose d'une certification valide conforme à la nouvelle version doit être apportée au plus tard à l'échéance du délai transitoire. Le champ d'application du SMSI ne peut être restreint à la faveur de cette nouvelle certification.