Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF

Section des droits politiques

Révision partielle de l'ordonnance sur les droits politiques et révision totale de l'ordonnance de la ChF sur le vote électronique (restructuration de la phase d'essai)

Rapport explicatif en vue de l'entrée en vigueur au 1er juillet 2022

Table des matières

1. Rappel des faits

Le vote électronique en Suisse, qui est en phase d'essai depuis 2004, est un maillon de la Stratégie suisse de cyberadministration de la Confédération et des cantons. Les bases légales sur lesquelles se fondent les essais sont l'art. 8*a* de la loi fédérale sur les droits politiques (LDP ; RS 161.1), les art. 27*a* à 27*q* de l'ordonnance sur les droits politiques (ODP ; RS 161.11) et l'ordonnance de la Chancellerie fédérale (ChF) sur le vote électronique (OVotE ; RS 161.116). Le principe qui veut que « la sécurité prime la vitesse » est appliqué depuis que le projet a été lancé. En Suisse, seuls sont autorisés les systèmes de vote électronique qui répondent aux exigences de sécurité sévères qui figurent dans le droit fédéral.

Depuis 2004, 15 cantons au total ont créé les bases légales nécessaires à l'utilisation du vote électronique, et ont proposé ce canal à une partie de leurs électeurs dans le cadre de plus de 300 essais réussis. Tous ont ouvert les essais aux électeurs suisses de l'étranger, et certains d'entre eux ont étendu cette participation à une partie des électeurs résidant en Suisse. Au cours des dernières années, les cantons avaient le choix entre deux systèmes de vote électronique : d'une part, le système du Canton de Genève, et, d'autre part, celui de La Poste Suisse. Ces fournisseurs ayant tous deux retiré leur système à la mi-2019, le vote électronique n'est plus possible en Suisse actuellement.

Le Conseil fédéral a décidé le 19 décembre 2018 d'ouvrir la procédure de consultation relative à la mise en exploitation du canal de vote électronique. La révision partielle proposée de la LDP aurait ainsi mis fin à la phase d'essai et fait du vote électronique le troisième canal de vote. La consultation a montré qu'une majorité significative des cantons et des partis étaient favorables à l'instauration du vote électronique. La Conférence des gouvernements cantonaux et 19 cantons ont même approuvé le passage à la mise en exploitation. Les partis qui étaient a priori favorables au vote électronique ont toutefois estimé que le temps n'était pas encore venu de franchir ce pas.

Le Conseil fédéral a ensuite décidé le 26 juin 2019 de renoncer momentanément à la révision de la LDP, tenant ainsi compte notamment des développements concernant les deux systèmes disponibles à ce moment-là. Il a par ailleurs chargé la ChF de concevoir avec les cantons une restructuration de la phase d'essai du vote électronique[1]. Ce faisant, il a fixé les objectifs de cette restructuration, qui sont les suivants :

1. Poursuite du développement des systèmes
2. Surveillance et contrôles efficaces
3. Renforcement de la transparence et de la confiance
4. Renforcement des liens avec les milieux scientifiques

À l'issue d'un vaste dialogue avec les milieux scientifiques, la Confédération et les cantons ont établi un rapport final assorti d'un catalogue de mesures complet. Le comité de pilotage Vote électronique (CoPil VE) a adopté le 30 novembre 2020 ce rapport final sur la restructuration de la phase d'essai et la reprise des essais[2]. La mise en œuvre des mesures proposées vise à répondre à la nécessité d'agir identifiée dans les quatre objectifs fixés par le Conseil fédéral. La mise en œuvre des mesures se fera par étapes. La première concerne la reprise des essais. Ces derniers pourront ainsi reprendre dans une mesure limitée, pendant que la mise en œuvre des objectifs à moyen et à long termes fera parallèlement l'objet de travaux en continu.

Le Conseil fédéral a pris acte le 18 décembre 2020 du rapport final du CoPil VE. Il a en outre chargé la ChF de mettre en œuvre progressivement et en collaboration avec les cantons les mesures indispensables à la restructuration, et de lui soumettre en vue de l'organisation d'une consultation un projet portant sur les modifications à apporter à l'ODP et à l'OVotE. L'objectif du Conseil fédéral est que les cantons puissent de nouveau mener des essais de vote électronique limités. La sécurité du vote électronique sera garantie par des exigences de sécurité plus précises, par des règles de transparence plus rigoureuses,

[1] Communiqué de presse du Conseil fédéral du 27 juin 2019, consultable sur www.bk.admin.ch > Droits politiques > Vote électronique > Communiqués de presse.

[2] Le rapport final et l'ensemble des documents concernant le dialogue avec les milieux scientifiques figurent sur le site Internet de la ChF : www.bk.admin.ch > Droits politiques > Vote électronique > Rapports et études.

par une collaboration plus étroite avec des experts indépendants et par un contrôle efficace effectué sur mandat de la Confédération[3].

La procédure de consultation sur la révision partielle de l'ODP et la révision totale de l'OVotE dans le cadre de la restructuration de la phase d'essai a été ouverte le 28 avril 2021 et a pris fin le 18 août 2021. 25 cantons, 1 commune, 8 partis politiques, 29 organisations et plusieurs particuliers se sont exprimés sur le projet. Les orientations et les objectifs de la restructuration ont été majoritairement salués. L'accent mis sur le développement des systèmes, sur un contrôle et une surveillance efficaces, sur le renforcement de la transparence et de la confiance et sur le renforcement des liens avec les milieux scientifiques ont été largement approuvés, de même que le renforcement du rôle de la Confédération dans le contrôle indépendant des systèmes et de leur exploitation. D'autre part, certaines questions de fond ont également été soulevées, notamment en ce qui concerne les compétences de la Confédération, des cantons et des fournisseurs de systèmes, ainsi que l'obligation de publier le code source des systèmes de vote électronique sous licence open source. Les avis reçus et le rapport de consultation ont été publiés[4].

Le 10 décembre 2021, le Conseil fédéral a pris acte des résultats de la procédure de consultation et chargé la ChF de finaliser les ordonnances en tenant compte des réactions circonstanciées suscitées par les différentes dispositions, de sorte que les cantons puissent reprendre les essais[5]. Les réserves fondamentales émises lors de la consultation doivent être prises en compte à moyen et à long terme selon le catalogue de mesures de la Confédération et des cantons, conformément au rapport final du CoPil VE du 30 novembre 2020.

2. Aperçu de la révision 2022 des bases légales

La révision 2022 des bases légales comprend une révision partielle de l'ODP ainsi qu'une révision totale de l'OVotE et de son annexe, qui entrent en vigueur au 1er juillet 2022. Ces révisions correspondent à la première étape de la mise en œuvre des mesures de restructuration de la phase d'essai.

Les grands axes de la révision sont les suivants :

- **Poursuite de la phase d'essai :**
  Le vote électronique restera en phase d'essai. Jusqu'à présent, les dispositions du droit fédéral prévoyaient trois plafonds pour la participation de l'électorat, en fonction du degré de développement des systèmes. Lors de la prochaine phase d'essai, la participation aux essais sera limitée à 30 % de l'électorat cantonal et à 10 % de l'électorat national, même en cas d'utilisation de systèmes à vérifiabilité complète. Ces plafonds seront revus régulièrement à la lumière des développements intervenus en matière de vote électronique. Les électeurs suisses de l'étranger continueront de ne pas être comptabilisés dans le calcul des plafonds (art. 27*f*, al. 3, ODP). Tel sera nouvellement aussi le cas pour les électeurs qui, en raison d'un handicap, ne peuvent exprimer leur suffrage de manière autonome et dans le respect du secret du vote.

- **Renforcement de la sécurité :**
  À l'avenir, la Confédération n'autorisera plus que des systèmes à vérifiabilité complète. Il s'agit là d'une mesure importante pour garantir la sécurité du vote électronique : la vérifiabilité complète permet d'identifier les manipulations des suffrages exprimés par voie électronique. La sécurité des systèmes de vote électronique sera encore renforcée par des exigences de sécurité et de qualité plus précises qui s'appliqueront aux systèmes et à leur développement.

- **Répartition des compétences entre la Confédération et les cantons :**
  Chaque canton continuera de déterminer s'il souhaite mener des essais de vote électronique. L'acquisition des systèmes restera aussi du ressort des cantons, lesquels pourront – comme c'était le cas jusqu'à présent – exploiter leur propre système, utiliser le système d'un autre canton ou faire

[3] Communiqué de presse du Conseil fédéral du 21 décembre 2020, consultable sur www.bk.admin.ch > Droits politiques > Vote électronique > Communiqués de presse.

[4] Consultable sur www.admin.ch > Droit fédéral > Procédures de consultation > Procédures de consultation terminées > 2021 > Chancellerie fédérale suisse.

[5] Communiqué de presse du Conseil fédéral du 10 décembre 2021, consultable sur www.bk.admin.ch > Droits politiques > Vote électronique > Communiqués de presse.

appel à une entreprise privée (art. 27*k*^{bis}, let. b, ODP). La Confédération continuera de fixer le cadre réglementaire et de délivrer les autorisations.

- **Contrôles indépendants :**
  La certification des systèmes et de leur exploitation qui était exigée jusqu'à présent sera remplacée par un audit indépendant effectué sur mandat de la Confédération, lequel garantira un contrôle efficace de la sécurité, et donc des conditions d'autorisation, tout en permettant d'identifier des améliorations potentielles pour l'avenir. Le présent projet de révision prévoit dès lors que la plupart des contrôles seront désormais effectués sur mandat de la ChF, et non plus des cantons ou de l'exploitant du système.

- **Transparence, participation du public et collaboration avec les milieux scientifiques :**
  Des prescriptions plus sévères en matière de transparence et le recours accru à des experts indépendants pour concevoir, développer et contrôler les systèmes de vote électronique contribueront à établir un processus d'amélioration continue. Le public aura accès à toutes les informations relatives au système et à son exploitation, mais aussi aux rapports d'audit, et sa participation aux travaux sera encouragée. Cela permettra de poser les fondements d'un contrôle public continu, les milieux scientifiques ayant eux aussi un rôle important à jouer à cet égard. Les anciennes exigences applicables à la publication du code source des systèmes de vote électronique sont par ailleurs précisées, et la mise en place d'un programme de *bug bounty*, avec rétributions financières récompensant les personnes ayant fourni de précieuses informations, devient obligatoire.

3. Conséquences pour la Confédération, les cantons et d'autres acteurs

La sécurité est capitale pour le vote électronique, ce qui n'est pas sans conséquences financières pour les autorités et les fournisseurs de systèmes. La couverture des coûts se fera en fonction de la répartition des tâches entre la Confédération et les cantons dans le domaine des droits politiques, la plus grande partie des coûts restant à la charge des cantons.

La mise en œuvre de la première étape de mesures, qui interviendra en 2021 et en 2022, engendrera des coûts supplémentaires de 1,2 à 1,5 million de francs pour les cantons, d'après les estimations qu'ils ont réalisées. Les frais d'exploitation annuels augmenteront vraisemblablement de quelque 50 000 à 70 000 francs. Quant à la mise en œuvre des mesures à moyen et à long termes, elle entraînera des coûts supplémentaires de 3,4 à 4,1 millions de francs selon les estimations. Ces mesures feront augmenter les frais d'exploitation annuels de quelque 0,9 à 1,1 million de francs. Il s'agit, pour les estimations susmentionnées, de coûts totaux pour tous les cantons.

La Confédération estime les surcoûts uniques durant la première étape à quelque 1,25 million de francs. Ces coûts, prévus pour la période 2021-2022, comprennent notamment les audits indépendants des systèmes de vote électronique, qui seront désormais réalisés sur mandat de la ChF. Il faut par ailleurs s'attendre à des coûts récurrents à moyen et à long termes. La restructuration n'entraînera pas de besoins de ressources humaines supplémentaires.

Les coûts devront vraisemblablement être pris en charge par quelques cantons seulement pendant une période assez longue. Si la pérennité du vote électronique doit être assurée, la Confédération devra participer plus largement à la couverture des coûts inhérents à la phase d'essai qui sont à la charge des cantons. Aussi le Conseil fédéral estime-t-il pertinent que la Confédération participe aux coûts de développement, et il s'emploiera à ce que cette participation intervienne via l'Administration numérique suisse (ANS). L'ANS a du reste déjà approuvé dans le cadre du plan actuel de mise en œuvre (2021–2023) une première demande visant à couvrir les besoins de financement supplémentaires.

Les mesures de restructuration auront par ailleurs un impact sur La Poste Suisse, qui est pour l'heure le seul fournisseur d'un système de vote électronique. La Confédération n'a pas connaissance de coûts qui pourraient être à la charge de La Poste Suisse et qui dépasseraient les estimations précitées des coûts à la charge de la Confédération et des cantons.

4. Commentaire des dispositions

4.1 Ordonnance sur les droits politiques (ODP)

La révision partielle de l'ODP concerne en particulier les modifications qui touchent la mise en œuvre de la restructuration de la phase d'essai du vote électronique (modification de la section 6*a*, voir chap. 4.1.1). Elle prévoit en outre la mise à jour de plusieurs dispositions de la section 3 et de l'annexe 3*a* (voir chap. 4.1.2).

4.1.1 Modification de la section 6*a*, consacrée aux essais de vote électronique

Art. 27b, let. b

Les essais de vote électronique sont soumis à une procédure d'autorisation en deux étapes : les cantons doivent d'abord obtenir de la part du Conseil fédéral une autorisation générale, qui est délivrée pour plusieurs scrutins ou pour l'élection du Conseil national (art. 27*a* ODP), et ensuite, de la part de la ChF, un agrément pour chaque scrutin considéré individuellement (art. 27*e* ODP). Il est à noter que le Conseil fédéral ne peut délivrer une autorisation générale que si les exigences prévues dans l'OVotE sont remplies. Le respect de ces exigences est vérifié par la ChF dans le cadre de la procédure d'agrément. En d'autres termes, la procédure d'autorisation générale comprend toujours une procédure d'agrément. Pour clarifier le rapport entre ces deux procédures, leur articulation a été précisée à la let. b, et l'ajout concerné n'entraîne donc aucune conséquence pratique.

Art. 27c, al. 2

Cet alinéa peut être abrogé suite à la modification de l'art. 27*b*, let. b, ODP.

Art. 27d, let. c

Le Conseil fédéral indique dans l'autorisation générale aussi bien le territoire que la part de l'électorat – autrement dit le pourcentage des électeurs – concernés par le recours au vote électronique. Il a besoin de connaître le nombre d'électeurs qui seront autorisés à voter par voie électronique pour contrôler le respect des plafonds fixés à l'art. 27*f*, al. 1, ODP.

Art. 27e, al. 1 à 2

Comme précédemment dans le cadre de la phase d'essai, un agrément de la ChF est nécessaire pour chaque scrutin. Comme le Conseil fédéral délivre les autorisations générales pour plusieurs essais (à l'exception de l'élection du Conseil national), la ChF vérifie pour chaque scrutin que les exigences pour obtenir l'agrément sont encore remplies. Ces exigences sont précisées dans l'OVotE.

Al. 1 et 1bis : Ces alinéas comprennent l'ancien al. 1, complété par la mention selon laquelle la ChF fixe les exigences applicables au système de vote électronique et à son exploitation. Cette délégation de compétence, qui figurait à l'art. 27*f*, est désormais réglée à cet endroit.

Al. 2 : Adaptation rédactionnelle.

Art. 27f Plafonds

Al. 1 : Jusque-là, les différents plafonds étaient liés à la mise en œuvre des exigences de sécurité. Pour les systèmes à vérifiabilité complète, le Conseil fédéral aurait pu ne pas fixer de plafond. Durant la phase d'essai écoulée, il n'y a encore aucun canton qui a pu remplir les conditions pour permettre à plus de 30 % de son électorat de voter par voie électronique. Et le plafond de 10 % de l'électorat national n'a jamais été atteint lui non plus[6]. Désormais, les plafonds sont fixés à 30 % de l'électorat cantonal et à 10 %

[6] S'agissant de l'électorat national, le pourcentage le plus élevé a été atteint lors du scrutin du 10 février 2019, quand près de 2,5 % des électeurs résidant en Suisse ont pu voter par voie électronique.

de l'électorat national, même en cas d'utilisation de systèmes à vérifiabilité complète. En fixant un plafond qui correspond à l'ancien plafond le plus bas, on souligne le caractère expérimental du vote électronique.

Le contrôle du respect du plafond cantonal continuera d'incomber aux cantons, qui seront libres de choisir la manière de garantir le respect du plafond fixé pour les électeurs résidant en Suisse. Jusqu'à présent, ils l'ont fait en recourant par exemple à une procédure d'annonce ou à des communes-pilotes.

La responsabilité du respect du plafond au niveau national incombera à la Confédération. Si, en raison du plafond national, il n'est pas possible de délivrer une autorisation générale à tous les cantons qui en font la demande, le renouvellement des autorisations générales déjà accordées sera prioritaire par rapport aux demandes d'autorisation générale nouvellement déposées. En d'autres termes, priorité sera donnée aux cantons qui ont déjà utilisé le vote électronique et qui souhaitent pérenniser le recours à ce canal de vote par rapport aux cantons qui déposent une première demande.

Al. 2 : La limitation fixée à l'al. 1 s'appliquera à la prochaine étape de la phase d'essai. Il s'agit de donner aux cantons la possibilité de rassembler des expériences avec les systèmes à vérifiabilité complète pendant que les essais resteront limités. Le réexamen régulier des plafonds permettra de tenir compte des évolutions entourant le vote électronique. Il devra prendre en considération l'utilisation du vote électronique par les cantons à ce moment-là et ultérieurement, le contexte politique, la stabilité de la phase d'essai et le degré de confiance de la population. La ChF peut procéder à un tel réexamen de sa propre initiative ou à la demande des cantons. Si, après avoir pris en compte ces aspects, la ChF estime indiqué d'adapter les plafonds, elle soumettra au Conseil fédéral une proposition visant à modifier l'al. 1.

Al. 3 : L'ancien al. 2 a subi la modification suivante : il n'y a pas que les électeurs suisses de l'étranger qui constituent des groupes cibles particuliers du vote électronique, il y a aussi les électeurs qui ne peuvent pas exprimer leur suffrage de manière autonome, dans le respect du secret du vote, en raison d'un handicap. L'ajout fait à l'al. 3 garantit que ces deux groupes cibles ne seront pas comptabilisés dans le calcul des plafonds. Les cantons auront ainsi la possibilité de proposer le vote électronique à ces deux groupes cibles sans que la limitation de l'électorat constitue à cet égard un obstacle. La mise en œuvre des exceptions incombe aux cantons. S'agissant des électeurs handicapés, les cantons feront appel dans la mesure du possible à des spécialistes de la politique en faveur des personnes handicapées et des questions liées à l'accessibilité.

Art. 27i, titre et al. 1 et 2, Vérifiabilité et établissement de la plausibilité du vote électronique

La fiabilité du vote électronique fait l'objet de l'art. 27*j* ODP. L'art. 27*i* ODP règle la traçabilité considérée comme la possibilité de vérifier que les suffrages ont été correctement traités et que les résultats sont exacts et plausibles. L'ancienne formulation de l'art. 27*i*, al. 1 et 2, se réfère à la possibilité de permettre à une partie ou à l'ensemble de l'électorat de voter par voie électronique. Comme l'art. 27*f*, al. 1, ODP ne prévoit plus la possibilité de permettre à l'ensemble de l'électorat de voter par voie électronique durant la prochaine phase d'essai, il faut adapter la formulation. Par ailleurs, les deux alinéas ont été intervertis afin de faire passer la vérifiabilité avant l'établissement de la plausibilité.

Al. 1 : La vérifiabilité du vote électronique est la mesure majeure destinée à garantir la sécurité du vote électronique, car elle permet d'identifier toute manipulation des suffrages exprimés par voie électronique. La vérifiabilité consiste à pouvoir vérifier :

- si le suffrage a été exprimé conformément à l'intention de son auteur,
- s'il a été enregistré comme il a été exprimé,
- s'il a été décompté comme il a été enregistré.

La réglementation exigeait précédemment la vérifiabilité complète uniquement lorsque l'essai concernait l'ensemble de l'électorat. Elle est désormais exigée quelle que soit la part de l'électorat autorisée à prendre part au vote électronique.

Al. 2 : L'établissement de la plausibilité des résultats des scrutins durant lesquels le vote électronique est utilisé vise à fournir des indices donnant à penser que des erreurs ont été commises involontairement dans l'établissement des résultats ou que ceux-ci ont été manipulés. Les cantons pourront continuer d'utiliser plusieurs méthodes pour procéder à l'établissement de la plausibilité. Ils pourront par exemple

comparer les résultats avec ceux du vote par correspondance ou à l'urne, comparer les suffrages électroniques décomptés avec ceux qui figurent dans les fichiers journaux des serveurs des votations ou des élections ou procéder à des vérifications au moyen de suffrages de contrôle émis par exemple par les représentants des électeurs. Des méthodes statistiques pourront aussi être utilisées lors des essais, à condition qu'elles soient disponibles et que la base de données le permette. La Confédération et les cantons se sont entendus dans le cadre du rapport final du CoPil VE pour développer l'établissement de la plausibilité des résultats du vote électronique[7].

Les al. 3 et 4 ne changent pas.

Art. 27k^{bis}, al. 2

Cet alinéa peut être abrogé étant donné que la ChF sera désormais dégagée des relations contractuelles. La relation contractuelle entre les cantons et d'éventuelles entreprises privées découle de l'al. 1.

Art. 27l Contrôle des systèmes et des modalités d'exploitation

Al. 1 : Il reprend le précédent al. 2 et énumère les motifs qui déclenchent un contrôle. Voir aussi les dispositions du ch. 26 de l'annexe de l'OVotE relatives à la date du contrôle.

Al. 2 : Les objets du contrôle sont les mêmes que précédemment. La vérification ne porte plus sur les seules « exigences de sécurité », mais sur toutes les exigences fixées par la ChF, ce qui correspond à la pratique. Par ailleurs, l'auditeur et l'audité doivent être indépendants l'un de l'autre.

Al. 3 et 4 : La ChF règle dans son ordonnance les éléments à contrôler, la périodicité des contrôles, les conditions que doivent remplir les entités mandatées et les compétences en matière d'octroi de mandats. Depuis la révision des bases légales en 2013, le contrôle des systèmes de vote électronique a été exigé dans la plupart des cas par des entités externes accréditées. Les cantons étaient chargés non seulement de mandater une entité ou de la faire mandater par l'exploitant d'un système pour qu'elle établisse la certification requise, mais aussi d'apporter les preuves exigées dans le cadre de la procédure d'autorisation. L'expérience de 2019 a montré que les anciennes exigences en matière de contrôle des systèmes et des processus n'ont pas eu les effets souhaités. La publication du code source et un examen indépendant réalisé ultérieurement ont révélé des failles de sécurité graves que les audits et certifications précédents n'avaient pas permis de détecter. Les compétences et la conception des contrôles des systèmes sont modifiées afin de garantir l'efficacité et la crédibilité des contrôles[8]. L'indépendance entre l'organisme d'audit et l'entité auditée joue un rôle important dans le cadre de cette modification des compétences. C'est pourquoi la répartition des responsabilités entre la Confédération et les cantons sont revue de façon que la Confédération assume davantage de responsabilités et un rôle plus direct dans l'audit des systèmes.

Art. 27l^{bis} Publicité des informations concernant le système et son exploitation

Al. 1 : La publication d'informations relatives au système de vote électronique et à son exploitation sert à permettre une bonne compréhension des opérations. Il s'agit de tenir compte des destinataires que sont les spécialistes ainsi que les personnes ne disposant pas de connaissances spécialisées.

Al. 2 : La mesure centrale est ici la publication du code source et de la documentation en la matière (let. a et b). Les anciennes art. 7*a* et 7*b* OVotE exigeaient déjà des cantons qu'ils publient le code source du logiciel d'un système à vérifiabilité complète destiné au vote électronique, accompagné d'une documentation suffisante. Le code source permet de voir comment le système enregistre et traite les votes. La let. c demande que soit également publiée la documentation du processus de développement. Le processus de développement est compris ici comme l'ensemble des processus de création du code source

[7] Voir mesure B.8 du rapport final du CoPil VE du 30 novembre 2020, accessible sous www.bk.admin.ch > Droits politiques > Vote électronique > Rapports et études.

[8] Voir mesure B.1 du rapport final du CoPil VE du 30 novembre 2020, accessible sous www.bk.admin.ch > Droits politiques > Vote électronique > Rapports et études.

ainsi que de ses mécanismes de contrôle et de sa mise à disposition. Les exigences relatives au processus de développement sont définies aux ch. 24.1 et 24.3 à 24.5 de l'annexe de l'OVotE. Elles comprennent en particulier le cycle de vie, les outils de développement, les méthodes de développement, la gestion des modifications, la gestion de configuration ainsi que la compilation et le déploiement fiables et vérifiables. Ils ne comprennent toutefois pas les produits qui découlent de ces processus (comme les demandes de changement, les listes de configuration ou l'historique des changements). La let. d prévoit que soit désormais également publié une pièce justificative attestant que le code source publié est également celui qui est mis en œuvre par le système lors de son utilisation.

Les principes de la transparence et de la vérifiabilité sont suffisamment importants pour être inscrits dans l'ODP. Les informations publiées permettent aux spécialistes de s'investir dans le processus, ce qui sera propice à la sécurité et à la qualité des systèmes, mais aussi à la confiance. La publication d'informations relatives au système, à savoir en particulier son code source, et à son exploitation contribue à instaurer un débat objectif et factuel. La disponibilité des informations limite la dépendance à l'égard de personnes ou d'organisations particulières. La ChF continuera d'apporter les précisions nécessaires dans son ordonnance.

Al. 3 : Lorsque cela est justifié, il est possible de renoncer à une publication. Si la publication porte atteinte à des intérêts publics ou privés prépondérants, il convient d'examiner si une forme de publication alternative est possible (par ex. caviardage de certains passages ou description sommaire des contenus). Ce n'est que si aucune forme de publication alternative ne permet de protéger les intérêts prépondérants qu'il y a lieu de renoncer à une publication. Les exceptions s'appuient généralement sur les législations sur la transparence et sur la protection des données. Il s'agira à cet égard de mettre à chaque fois en balance l'intérêt public à une publication et l'intérêt public ou privé à la confidentialité. On peut s'attendre à ce que l'intérêt public à une publication, notamment pour ce qui est des informations en lien avec la sécurité, sera élevé. À l'appui de l'intérêt à la confidentialité, il est notamment possible de faire valoir des directives internes, la protection des intérêts de l'entreprise ou encore la protection des données de tiers.

Art. 27l^{ter} Participation du public

Al. 1 : Pour associer le public et les milieux spécialisés aux travaux, la ChF et les cantons mettent en œuvre des mesures qui peuvent comprendre par exemple l'organisation de colloques ou de conférences scientifiques, de concours d'idées et de hackathons, la gestion de plateformes d'information et la mise sur pied de projets dans le domaine des sciences participatives. En outre, la ChF se charge ici, entre autres, d'expliquer ce qu'est la vérifiabilité, les cantons se chargeant pour leur part et en vertu de l'art. 27*m*, al. 1, ODP d'expliquer la mise en œuvre de cette notion.

Al. 2 : Les cantons sont notamment chargés de créer les incitations nécessaires à la participation de spécialistes issus de la société civile, par exemple au moyen de la mise en place d'un programme de *bug bounty* (art. 13 OVotE).

Art. 27m Informations des électeurs et publication des résultats du vote électronique

Al. 1 : Il a subi de légères modifications rédactionnelles. Les cantons devront informer les électeurs, comme c'était le cas précedemment. Il s'agit notamment des informations figurant sur le matériel de vote, qui décrivent le déroulement précis du vote électronique et la procédure à suivre en cas d'irrégularités ou de problèmes. On considère par ailleurs qu'il est important d'expliquer aux électeurs la mise en œuvre de la vérifiabilité. Car la procédure de vérifiabilité ne permet d'identifier des irrégularités que si les électeurs y ont recours. La vérifiabilité complète ne peut avoir un impact positif sur la confiance que si l'on comprend véritablement son utilité.

Al. 2 : Il correspond, sur le fond, à l'ancien al. 2. La disposition a été précisée en ce sens qu'on y explique que la possibilité d'observation porte sur les opérations qui ponctuent le déroulement d'un scrutin (par ex. la procédure de dépouillement ainsi que le chiffrement et le déchiffrement de l'urne). Cette disposition continue d'assurer la transparence vis-à-vis des électeurs et de ne pas exiger des cantons qu'ils mettent en place des structures permanentes destinées à représenter les électeurs, par exemple des commissions électorales. En principe, il suffit par exemple qu'un bureau électoral institué par l'autorité compétente puisse suivre les procédures et les opérations, car celui-ci est généralement composé de personnes

ayant le droit de vote dans le canton. Par ailleurs, il ne s'agit pas de donner accès à *toutes* les étapes et de publier *tous* les documents. Si des motifs prépondérants militent contre un accès ou une publication, il restera possible de rejeter la demande. À cet égard, on pourrait recourir aux exceptions figurant dans la législation sur la transparence, laquelle est applicable. Par ailleurs, le renvoi à la loi du 17 décembre 2004 sur la transparence, qui est désormais superflu, peut être supprimé. Ce qui est déterminant, c'est que le scrutin se déroule en temps voulu ; à aucun moment ce déroulement ne doit être mis en péril en raison de cette disposition.

Al. 3 : Les cantons sont tenus de publier les résultats du vote électronique, ce qui constitue une nouveauté, avant tout dans un souci de transparence.

Les résultats ci-après doivent être publiés :

- dans le cas des votations : le nombre de oui, de non et de suffrages blancs.
- dans le cas des élections : le nombre de suffrages exprimés par voie électronique pour chaque candidat (suffrages nominatifs) et pour chaque liste (suffrages de liste).

Les données doivent être publiées d'une manière aussi détaillée que possible. Dans le cas des votations, il faut chercher à fournir des indications par commune ; dans le cas des élections, par arrondissement électoral. La publication ne doit pas mettre en péril le secret du vote. Celui-ci serait menacé par la publication si, par exemple, seuls les électeurs suisses de l'étranger pouvaient voter par voie électronique et si, dans une commune, seule une personne vivant à l'étranger était habilitée à voter. Si le secret du vote était menacé par la publication, il ne faudrait généralement pas renoncer au principe de publication, mais examiner la possibilité de recourir à d'autres solutions, par exemple déterminer si l'on pourrait procéder à la publication moyennant l'adaptation du degré de détail des informations, en regroupant par exemple les résultats de plusieurs communes, et, dans l'affirmative, comment. Il convient de renoncer à une publication si aucune forme alternative de publication ne permet de garantir le secret du vote.

La publication ne doit pas avoir lieu dans la Feuille officielle ; il suffit de la faire sur le site Internet du canton. Les informations doivent être facilement accessibles et réexploitables.

Art. 27o Recours à des experts indépendants et suivi scientifique

Al. 1 : Les autorités doivent recourir davantage à des experts indépendants dans les domaines où cet accompagnement présente une plus-value, par exemple si cela permet d'acquérir des connaissances dans le domaine de la sécurité du vote électronique. Les experts devraient être indépendants de l'exploitant du système et, si possible, des autorités. Le recours à des experts peut englober l'octroi de mandats portant sur des prestations de services ou de conseil précises, comme l'audit du système, l'assistance et le conseil lors de la mise en place d'un système d'appréciation des risques, l'audit et le conseil en matière de convivialité et d'accessibilité ou la collaboration dans le cadre de l'exploitation, notamment pour l'évaluation des résultats de la vérification ou pour des enquêtes de suivi.

Al. 2 : La ChF doit en outre veiller à ce que les essais de vote électronique fassent l'objet d'un suivi scientifique. Cette disposition porte sur les travaux de recherche effectués par les milieux scientifiques, travaux qui, par rapport à ceux visés à l'al. 1, ne doivent pas servir directement aux travaux des autorités qui sont absolument indispensables à la tenue des scrutins. Ce suivi doit favoriser la création d'une assise qui servira à l'évaluation et qui permettra de donner des orientations en vue de l'amélioration de la phase d'essai. Les let. a et b pourraient par exemple permettre des travaux de recherche sur les thèmes suivants :

- conditions préalables à la confiance et à l'acceptation
- utilisation du canal de vote électronique
- renforcement de la vérifiabilité
- méthodes formelles pour la formulation d'exigences et des spécifications du système
- convivialité et accessibilité

L'*al. 3* correspond à l'ancien al. 2.

Al. 4 : Ancien al. 3.

4.1.2 Modification de la section 3 et de l'annexe 3*a*

Art. 8a, al. 1

Cette disposition a subi des modifications rédactionnelles. Depuis le 1er novembre 2015, les cantons qui connaissent le système proportionnel doivent fixer la date limite du dépôt des listes de candidats à un lundi du mois d'août de l'année de l'élection (RO **2015** 543). Dans les cantons qui connaissent le système majoritaire avec dépôt des listes de candidats, on pourrait toutefois envisager aussi de fixer désormais la date limite du dépôt des listes au début du mois de septembre.

Art. 8d, al. 3

En pratique, on n'utilise plus le télécopieur pour effectuer ces communications. La disposition peut donc être corrigée en conséquence.

Annexe 3a et verso de l'annexe 3a

Diverses adaptations faites à la suite de la modification de la LDP du 26 septembre 2014 (RO **2015** 543).

4.2 Ordonnance de la ChF sur le vote électronique (OVotE)

4.2.1 Partie principale

Art. 1 Objet

Les définitions ont été déplacées dans la partie principale de l'OVotE (voir l'art. 2 OVotE).

Art. 2 Définitions

Al. 1 : Il reprend pour l'essentiel les définitions de l'ancienne annexe de l'OVotE, dans la mesure où elles sont pertinentes pour la partie principale.

Commentaire des définitions :

Let. a : La « réalisation d'un scrutin électronique » comprend également la préparation et le suivi, dans la mesure où ces travaux concernent spécifiquement le vote électronique. N'en font pas partie les processus administratifs préalables, tels que les éventuelles procédures d'enregistrement des électeurs pour l'obtention du matériel de vote permettant de prendre part au vote en ligne.

Le système comprend :

- La fonctionnalité de lecture des données du registre des électeurs nécessaire à l'organisation de scrutins électroniques.
- L'infrastructure nécessaire à l'impression du matériel de vote spécialement conçu pour le vote électronique.
- Les composants dotés de fonctions spéciales qui sont importantes pour la vérifiabilité du vote électronique. Il s'agit de ce que l'on appelle les composants de contrôle, les composants de configuration, les composants d'impression et les dispositifs techniques des vérificateurs.

Ne font pas partie du système la tenue du registre des électeurs, car il ne concerne pas spécifiquement le vote électronique, ni le logiciel de compilation des résultats partiels provenant des différents canaux de vote.

Let. b : Ne font pas partie du système en ligne les composants du système qui sont utilisés pour la préparation et le dépouillement (tels que l'imprimerie et le composant de configuration).

Let. c : Un protocole cryptographique doit garantir qu'en cas de dysfonctionnement ou même d'attaque, les manipulations des suffrages (modification, ajout, suppression) puissent être détectées même si un seul composant de contrôle par groupe fonctionne correctement. De même, le secret des votes doit être préservé même si un seul composant de contrôle par groupe fonctionne correctement. Les modalités

détaillées figurent aux art. 5 à 8, à l'annexe, ch. 2, ainsi que dans les explications détaillées. Le ch. 3 de l'annexe contient des dispositions relatives à la mise en œuvre technique et au fonctionnement des composants de contrôle, qui visent à ce que tous les composants de contrôle d'un groupe fonctionnent effectivement de manière correcte. Plus il y a de composants de contrôle dans un groupe, plus leur mise en œuvre technique diffère, plus ils sont exploités indépendamment les uns des autres et plus ils sont protégés contre les attaques, plus il est probable qu'au moins l'un d'entre eux fonctionne correctement.

Let. d : Les exigences destinées à garantir une conception et une exploitation indépendantes figurent dans l'annexe au ch. 3.

Let. h : Le recours à des vérificateurs sert la transparence. Les électeurs doivent pouvoir présumer que les vérificateurs attireront en cas de doute leur attention sur une irrégularité. Le recours à des vérificateurs vus comme les représentants des électeurs répond à l'art. 27*m*, al. 2, ODP (voir le commentaire correspondant). L'organisation et la forme de ce recours à des vérificateurs sont régies par le droit cantonal.

Let. i : La plate-forme utilisateur ne fait pas partie de l'infrastructure.

Let. j : Concerne en particulier la mise en œuvre des éléments suivants :

- génération des éléments cryptographiques secrets
- vérification du droit de vote (il s'agit de vérifier au moyen des données d'authentification serveur si l'émetteur du vote est autorisé à voter ; cette vérification peut être effectuée de manière anonyme)
- contrôle de validité
- enregistrement des suffrages entrants
- mélange cryptographique des suffrages enregistrés
- déchiffrement des suffrages
- génération des preuves qui, grâce à l'utilisation des composants de contrôle, résultent de la garantie de la vérifiabilité individuelle et de la vérifiabilité universelle

Let. m : Dans ce contexte, la partie fiable du système fait référence à un groupe de composants de contrôle appartenant au système en ligne.

Let. o, ch. 1 : Dans une élection au système majoritaire, les champs de texte libre sont toujours considérés comme ayant été remplis conformément au système.

Let. p : Sur la base des données d'authentification client, le dispositif technique utilisé crée un message d'authentification (par exemple, la signature du suffrage) qui est envoyé à l'infrastructure ; au moyen du message d'authentification et des données d'authentification serveur (par exemple, une clef publique permettant de vérifier la signature), l'infrastructure authentifie l'émetteur d'un vote en tant que personne autorisée à voter. Les données d'authentification client doivent être difficiles à deviner.

Let. r : Il doit être impossible en pratique de générer un message d'authentification valide sans avoir connaissance des données d'authentification client.

Let. s : Il peut s'agir par exemple d'un certificat ISO 27001.

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

Phrase introductive, let. a et c : Les dispositions ont été revues sous l'angle rédactionnel. À la let. a a en outre été ajoutée la vérifiabilité, désormais exigée aux termes de l'art. 27*i*, al. 1, ODP pour toute utilisation d'un système de vote électronique.

Let. a : Concerne notamment les exigences fixées aux art. 4 à 9 OVotE.

Let. b : Lors de la mise en œuvre de cette disposition, il convient notamment de veiller à ce que le système soit conçu de manière à prendre en compte les besoins spécifiques des personnes handicapées (art. 27*g*, al. 1, ODP). Ainsi, le portail de vote électronique doit être accessible et conforme à la norme d'accessibilité eCH-0059 – à l'exception de son chapitre 2.4 – et être vérifié par un organisme compétent (cf. ch. 25.7.3 de l'annexe; contrôle de conformité selon ch. 26.2.1 de l'annexe). Des indications visant à améliorer l'accessibilité du système peuvent être déposées en vertu de l'art. 13, al. 1, OVotE. En outre, l'ODP prévoit

que des allègements peuvent être autorisés pour les personnes handicapées lors de la mise en œuvre des exigences, pour autant que la sécurité ne s'en trouve pas sensiblement réduite (cf. art. 27*g*, al. 2, ODP).

Let. c : Concerne notamment les exigences fixées aux art. 10 à 12 OVotE.

Let. d : L'ancienne disposition a été complétée par l'obligation de donner accès au public à des informations adaptées et sur la participation du public (en vertu notamment des art. 27*l*^{bis} et 27*l*^{ter} ODP et 13 OVotE). Cet ajout souligne l'importance de la transparence et de la participation du public aux travaux qui concernent le vote électronique. Les informations à fournir et leur forme sont fonction des groupes cibles visés, soit notamment le grand public et les milieux spécialisés.

Art. 4 Appréciation des risques

Al. 1 : Pour obtenir un agrément, les cantons doivent, comme précédemment, procéder à des appréciations des risques dans le domaine qui relève de leurs compétences. Tous les risques qui menacent la réalisation des objectifs de sécurité doivent être identifiés au moyen d'une appréciation des risques. Il faut par ailleurs apprécier les risques qui concernent l'environnement du vote électronique au sein de l'administration et dans le public.

L'appréciation des risques doit également tenir compte de la confiance et de l'acceptation du public à l'égard du vote électronique. Ces préoccupations générales doivent être intégrées de manière transversale dans tous les objectifs et risques de sécurité. Exemples d'application :

- Exemple 1 : Il est expliqué comment procéder au cas où la vérification du résultat de la votation ou de l'élection serait négative (par ex. à l'aide du dispositif technique des vérificateurs ; cf. art. 5, al. 3, let. b, OVotE). Il s'agit ainsi de prévenir tout doute quant à l'exactitude.
- Exemple 2 : Même si seuls sont découverts des défauts insignifiants, il existe un risque que cela porte atteinte à la confiance du public. Pour y remédier, il est possible de faire appel à des experts indépendants pour la classification des défauts découverts (évaluation des défauts, communication).

Les appréciations des risques doivent être menées selon une méthode comprenant les activités suivantes : identifier les risques ; analyser les risques ; estimer les risques. Les détails de la méthode utilisée et les critères de tolérance des risques imposés par le canton doivent être documentés. Les appréciations des risques doivent être revues au moins une fois par an et à chaque fois que le système fait l'objet d'une modification majeure. Il faut également s'assurer avant chaque scrutin si des nouveaux risques existent ou si des risques déjà existants se sont accrus.

Dans le cadre de l'évaluation qu'elle fait de la situation, la ChF peut établir sa propre appréciation des risques pour son domaine de compétences. Si une appréciation des risques effectuée par la ChF n'implique nullement la délivrance d'un agrément aux cantons, elle peut toutefois être prise en compte dans la décision d'accorder ou non cet agrément. Elle est envoyée aux cantons pour information afin qu'ils puissent en tenir compte. La ChF consulte les appréciations effectuées par les cantons pour établir sa propre appréciation des risques.

La ChF fournit aux cantons un guide qui indique comment effectuer les appréciations des risques. Toutes les appréciations des risques doivent refléter la situation du moment, et les derniers développements et connaissances en date doivent y être intégrés en continu.

Al. 2 : L'exploitant ou le fabricant du système doit désormais préparer sa propre appréciation des risques, notamment lorsqu'il a recours à un système externe. Pour les autres prestataires dont les services sont liés à la sécurité, tels que les imprimeries, les fournisseurs de dispositifs techniques destinés aux vérificateurs ou de composants de contrôle, le canton doit vérifier s'il suffit qu'il effectue lui-même l'appréciation des risques ou si une appréciation supplémentaire des risques par le prestataire est nécessaire. Les prestataires de services établissent les appréciations des risques à l'intention du canton. Celui-ci les prend en compte pour effectuer sa propre appréciation des risques, qu'il soumet à la Confédération dans le cadre de la procédure d'autorisation.

Al. 3 : La phrase introductive et les objectifs de sécurité (let. a à e) sont revus sur le plan linguistique. L'objectif de sécurité figurant à la lettre f est précisé afin de mieux éclairer sa finalité. L'achat de votes, par exemple, entre dans le champ de cet objectif de sécurité.

Al. 4 : Correspond essentiellement au précédent al. 2. L'obligation de démontrer que les risques sont jugés suffisamment faibles a été reprise à l'al. 1.

L'ancien al. 3 peut être supprimé puisque les éléments visés à l'art. 11 OVotE doivent être publiés, ce qui lui enlève une bonne partie de sa signification.

Art. 5 Exigences applicables à la vérifiabilité complète

La vérifiabilité complète permet de détecter, sans compromettre le secret du vote, une éventuelle défaillance système qui se produirait pendant la procédure de vote en raison d'une erreur logicielle, d'une erreur humaine ou d'une tentative de manipulation. Elle prévoit que l'électeur obtienne la preuve que son suffrage est parvenu à la partie fiable du système sans avoir fait l'objet d'aucune altération, provoquée par exemple par un logiciel malveillant installé sur l'ordinateur utilisé. Les vérificateurs peuvent s'assurer, indépendamment du système utilisé, que tous les suffrages dont il a été vérifié qu'ils avaient été émis correctement par les votants, ont également été dépouillés correctement, c.-à-d. conformément à la preuve obtenue par les votants. La mise en œuvre de la vérifiabilité doit se fonder sur des méthodes cryptographiques reconnues.

À l'avenir, la Confédération n'autorisera plus que des systèmes à vérifiabilité complète. Les exigences précédemment prévues aux art. 4 et 5 sont reprises aux art. 5 à 8 OVotE avec quelques modifications.

Al. 2 : La vérifiabilité individuelle permet aux électeurs de constater toute utilisation abusive, commise intentionnellement ou non, qui serait faite de leur droit de vote. Cette opération doit aussi être possible si la plate-forme utilisateur et le canal de transmission ne sont pas fiables. Il faut considérer a priori que la plate-forme utilisateur et le canal de transmission sont infectés par des virus indétectables ou exposés à d'autres risques. Le suffrage tel qu'il a été saisi sur la plate-forme utilisateur par le votant correspond toujours à la volonté du votant, sauf erreur de saisie commise par ce dernier.

Al. 3 : La vérifiabilité universelle permet de détecter toute manipulation, commise intentionnellement ou non, dans l'infrastructure (modification, ajout, suppression). À la différence de la vérifiabilité individuelle, la vérifiabilité universelle ne doit cependant pas être impérativement proposée aux électeurs : il est en effet possible de recourir pour cela à des vérificateurs. Le processus de vérification doit être observable, ce qui signifie que les vérificateurs doivent être en mesure de comprendre autant que possible la signification et les résultats des différentes étapes. À cette fin, ils doivent pouvoir attester la bonne exécution des étapes ainsi que les résultats des tests, par exemple en se rendant sur le lieu de l'exécution.

Art. 6 Caractère concluant des preuves

Aucune preuve ne permet de confirmer avec une certitude absolue que tous les suffrages ont été correctement traités au sens des exigences prévues à l'art. 5, al. 2 et 3, OVotE. Les preuves doivent donc être interprétées à la lumière de leur caractère concluant. L'art. 6 énonce à cet égard des exigences minimales, auxquelles les personnes amenées à interpréter une preuve doivent pouvoir se fier. Plus le caractère est concluant, et plus la falsifiabilité est faible. On trouvera dans l'annexe de l'OVotE des précisions et des exigences supplémentaires (ch. 2.9.1, 2.9.2 et 2.11). La liste visée aux let. a à c de l'art. 6 est exhaustive. Le caractère concluant des preuves visées à l'art. 5 est donc exclusivement déterminé par la fiabilité de ces éléments.

Un électeur qui bénéficie de la vérifiabilité individuelle devrait pouvoir être certain, sur la base de la référence de vérifiabilité reçue par la poste, que son vote est très probablement arrivé à destination, à condition que la génération et l'impression des données pour la référence de vérifiabilité ait fonctionné correctement et que l'un des quatre composants de contrôle ait fonctionné correctement (voir commentaire du ch. 2 de l'annexe). Si l'électeur ne croit pas que ces conditions sont remplies, le résultat de l'examen de la preuve n'aurait logiquement pour lui aucune signification ou seulement une signification limitée. Pour le dire autrement : la preuve n'aurait pour lui qu'un « caractère insuffisamment concluant ».

Le bon fonctionnement de la plate-forme utilisateur des électeurs et des moyens de transmission ne doit pas constituer un présupposé pour le caractère concluant de la preuve au sens de l'art. 5, al. 2, let. a, OVotE. Cela signifie que la preuve doit être concluante même dans le cas où une plateforme utilisateur manipulée ou un *man-in-the-middle*[9] manipule discrètement le suffrage – la preuve visée à l'art. 5, al. 2 OVotE permet malgré tout à l'électeur de détecter la manipulation.

De manière analogue au caractère concluant des preuves selon l'al. 3 : la preuve est concluante si elle permet aux vérificateurs de détecter des manipulations dans le cadre des hypothèses de confiance données. Cela empêche l'attaquant de tromper les vérificateurs en utilisant les composants non fiables du système pour fabriquer une preuve légitimant un résultat manipulé. Tant que les vérificateurs ont la certitude que l'un des quatre composants de contrôle et le dispositif technique qu'ils utilisent pour tester les preuves (généralement un ordinateur portable) fonctionnent correctement, les preuves sont concluantes.

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

Pour garantir le secret du vote et rendre impossible l'établissement de résultats partiels anticipés, le système doit être conçu de manière à ce qu'il faille prendre le contrôle de tous les composants de contrôle pour mener une attaque réussie après que le suffrage a été émis. Des exigences plus sévères s'appliquent au système en ligne, si celui-ci est exploité par un opérateur privé. Des précisions à cet égard figurent dans l'annexe de l'OVotE (ch. 2.9.3).

Art. 8 Exigences applicables à la partie fiable du système

Ces exigences visent à garantir qu'un accès non autorisé réussi ne confère pas, dans la mesure du possible, un avantage dans la tentative d'accéder discrètement à un autre composant de contrôle.

Art. 9 Mesures supplémentaires visant à réduire les risques

Correspond à l'ancien art. 6 de l'OVotE, avec quelques modifications linguistiques. Cet article prévoit que des mesures supplémentaires doivent être prises si les risques ne sont pas suffisamment faibles malgré les mesures prises pour répondre aux exigences de l'OVotE, en vertu notamment des art. 3 et 5 à 8 de l'OVotE. La notion de « suffisamment faibles » s'inspire des critères d'évaluation et d'acceptation des risques définis par les cantons et la ChF.

Art. 10 Exigences applicables au contrôle

Afin de renforcer l'efficacité des contrôles et l'indépendance de l'organe de contrôle par rapport à l'organe contrôlé, la répartition des tâches entre la Confédération et les cantons est adaptée de manière à donner à la Confédération une responsabilité accrue et un rôle plus direct dans le contrôle des systèmes. À l'avenir, la plupart des contrôles seront commandés par la ChF (al. 1 ; cf. aussi le commentaire de l'art. 27*l*, al. 3 et 4, ODP). Il sera renoncé dans ces domaines à une certification par des services accrédités par le Service d'accréditation suisse (SAS). Comme précédemment, le canton veille à ce qu'un contrôle du bon fonctionnement du système soit effectué dans le centre de calcul de l'exploitant (al. 2). Les autres exigences, telles que l'objet, les responsabilités et les dates des contrôles, continuent d'être précisées dans l'annexe de l'OVotE (ch. 26).

Al. 1, let. b : Adaptation de la dénomination : il est nouvellement question de « logiciel du système ». Ce contrôle comprend le précédent, visé à l'annexe aux ch. 5.2 (Fonctionnalités) et 5.4 (Composants de contrôle). Avec la nouvelle formulation, les logiciels de l'ensemble du système et des composants de contrôle sont testés ensemble.

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

Al. 1, let. c : Les exigences applicables aux imprimeries relèvent désormais de la disposition « sécurité de l'infrastructure et de l'exploitation ». L'infrastructure et l'exploitation peuvent être réparties entre l'exploitant du système et les cantons. Cette répartition dépend du système choisi et du modèle de collaboration. Tous les éléments de l'infrastructure et tous les aspects de l'exploitation sont examinés. La vérification est effectuée auprès de l'organisme responsable de l'élément concerné.

Al. 2 : L'exploitation du système dans le centre de calcul de l'exploitant du système doit être certifiée conformément à la norme ISO 27001. Cette vérification est laissée à l'appréciation des cantons, puisqu'elle repose sur une norme reconnue et qu'il existe une méthode établie pour la mettre en œuvre. Un canton qui n'exploite pas lui-même un système peut se faire certifier pour les processus cantonaux selon la norme ISO 27001, mais il n'est pas obligé de le faire.

Al. 3 : La ChF et les organes mandatés pour les contrôles visés à l'al. 1 doivent avoir accès aux documents nécessaires détenus par le canton et ses prestataires de services. Cela comprend tous les documents requis pour les contrôles prévus à l'al. 1 et tous les rapports disponibles (y compris les rapports de certification), les pièces justificatives et les certificats (certificat ISO 27001 au sens de l'al. 2 et toutes les certifications cantonales, s'il y en a).

Al. 4 :

- Les résultats des audits qui sont pertinents pour l'autorisation sont publiés. L'organe compétent publie les pièces et les certificats qui ont été établis dans le cadre des contrôles conformément aux al. 1 et 2. Le terme « pièces justificatives » recouvre également les rapports d'audit. Pour les audits visés à l'al. 2, il y a lieu de publier au moins la Déclaration d'applicabilité (Statement of Applicability, SoA), ou, à défaut, les résultats complets.
- Les résultats des audits qui sont publiés doivent être compréhensibles. S'il y est fait référence à d'autres documents, ceux-ci doivent en règle générale être eux aussi publiés. S'il n'est pas possible de publier des documents supplémentaires, les résultats des audits doivent être rendus compréhensibles au moyen d'une description sommaire des aspects pertinents de la documentation non publiée.
- Si l'entité auditée rédige une réplique à un rapport d'audit et souhaite qu'elle soit publiée, la réplique est publiée par l'entité compétente en vertu des al. 1 et 2.
- L'organe compétent pour la publication est celui qui a commandé l'audit. Il s'agit de la ChF pour les contrôles visés à l'al. 1 et du canton ou de l'exploitant du système pour les contrôles visés à l'al. 2.
- En ce qui concerne l'exception au principe de la publication, voir les explications relatives à l'art. 27*l*^{bis}, al. 3, ODP.

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

Les exigences précédemment applicables à la publication du code source et de la documentation relative au système et à son exploitation sont précisées. L'al. 1 contient désormais une liste des éléments qui doivent être publiés. Ci-après un commentaire de certains des termes utilisés:

Al. 1, let. a : Les « paramètres pertinents » comprennent toutes les informations et données nécessaires pour que les personnes interéssées puissent mettre le système en service chez soi.

Al. 1, let. c : La documentation du logiciel comprend notamment le protocole cryptographique, la spécification et l'architecture, les instructions, les concepts de test, les rapports consacrés aux failles et aux mesures correctives et les résultats des audits menés dans le cadre du développement du système (revues de code, rapports de test).

Al. 1, let. d : Comprend les documents qui décrivent le processus de développement (cf. le commentaire de l'art. 27*l*^{bis}, al. 2, let. c, ODP.

Al. 1, let. e : Comprend les documents qui facilitent la mise en service du système en vue de le tester (par exemple des instructions, une FAQ, etc.).

Al. 1, let. f : Par « principaux composants », on entend les composants dont le fonctionnement correct est important pour la réduction des risques, notamment les composants fiables selon le ch. 2 de l'annexe.

Les spécifications techniques comprennent le nom du fabricant et la désignation du produit, ainsi que les informations pertinentes pour l'identification des failles de sécurité (par ex. la version du système d'exploitation ou du micrologiciel, la version de l'environnement Java Runtime).

Al. 1, let. g : Comprend les documents qui documentent la conformité aux exigences de l'OVotE. Cela inclut également ceux qui documentent les mesures essentielles de réduction des risques mentionnées dans l'appréciation des risques. Le principe qui prévaut est le suivant: plus la documentation concerne l'exploitation, l'entretien ou la sécurité d'un composant dit fiable au sens du ch. 2 de l'annexe ou la manipulation d'un support de données contenant des données critiques, plus il est important de publier. Les dispositions de la législation sur la transparence qui concernent les exceptions s'appliquent au surplus.

Al.1, let. h : Si l'exploitant du système a connaissance d'une erreur dans le code source publié ou dans la documentation, il doit l'indiquer. Il décrit l'erreur et les mesures éventuellement prévues pour y remédier. Cela contribue à la compréhension, à la transparence et à la coopération avec le public.

Al. 2, let. c : Comme il a été dit dans le commentaire de l'art. 27*l*bis, al. 3, ODP, les exceptions justifiées se fondent sur les législations sur la transparence et sur la protection des données. En outre, s'agissant de la publication selon l'art. 11, si des motifs particuliers le justifient, il est possible de ne pas publier les documents peu ou pas pertinents pour la sécurité du système et son exploitation. Il s'agit par exemple de descriptions de processus opérationnels sans rapport direct avec le système ou de simples précisions pas ou peu déterminantes pour la sécurité ou dont il est possible de supposer qu'elles seront mises en œuvre correctement. Si des exceptions sont demandées, il convient de procéder à une pesée des intérêts (cf. le commentaire de l'art. 27*l*bis, al. 3, ODP).

Art. 12 Modalités de publication

Les exigences en matière de transparence et d'accessibilité des informations relatives au système et à son fonctionnement sont a priori élevées. L'OVotE n'exige pas que les documents soient publiés sous une licence open source. Mais la Confédération et les cantons se sont prononcés en 2020 pour une publication sous licence open source des futurs systèmes et composants de système[10]. La présente réglementation de l'OVotE sur la publication des documents vise à ce que le plus grand nombre possible d'experts indépendants se penchent sur les documents publiés.

Al. 1 : Les éléments concernés doivent être publiés sur toutes les plate-formes courantes. Les fichiers doivent être organisés conformément à la pratique établie, compte tenu de leur taille et de leur complexité.

Al. 2 : Les documents publiés doivent pouvoir être obtenus de manière anonyme et le propriétaire du code source ne doit pas inviter les personnes intéressées à s'enregistrer pour obtenir ces documents. Si une personne a droit à une rétribution financière conformément à l'art. 13 OVotE, le propriétaire peut demander les informations nécessaires à sa remise. On considère qu'il est judicieux de faire intervenir la publication six mois environ avant le déploiement prévu du système, de façon à permettre un examen public efficace.

Al. 3 : L'échange avec d'autres personnes et la citation d'informations publiées doivent être autorisés, notamment pour faciliter la recherche de failles par les spécialistes.

Al. 4, let. b : Afin de garantir une publication responsable (*Responsible Disclosure*), le propriétaire peut inviter les participants à respecter les règles suivantes :

- Signaler immédiatement les failles au propriétaire du code source.
- Attendre avant de signaler publiquement une faille ; un embargo donné devra à cet égard être respecté.
- Adopter une attitude responsable à propos des informations concernant des défauts présumés. Ne pas diffuser inutilement des informations concernant des failles de sécurité potentielles. Les informations en la matière ne doivent être partagées et discutées qu'avec des personnes supposées aptes et disposées à traiter ces questions, et qui adopteront elles aussi une attitude responsable.

[10] Voir mesure C.2 du rapport final du CoPil VE du 30 novembre 2020, accessible sous www.bk.admin.ch > Droits politiques > Vote électronique > Rapports et études.

Al. 5 : Si le propriétaire du code source fixe des conditions d'utilisation du code source et de la documentation (par ex. exclusion d'une utilisation commerciale par un tiers) ou des conditions fondées sur l'al. 4, let. b (conditions pour la fourniture d'indications selon l'art. 13, al. 1, OVotE), les violations de ces conditions ne peuvent être sanctionnées que dans les cas exceptionnels mentionnés à l'al. 5 (utilisation de tout ou partie du code source à des fins commerciales ou productives). Le propriétaire du code source doit, dans les conditions d'utilisation, attirer l'attention des participants sur les restrictions relatives aux possibilités de sanction. Il convient par ailleurs de renoncer à demander une déclaration d'intention aux utilisateurs.

Art. 13 Participation du public

Cet article arrête les principes d'un programme de *bug bounty*, c.-à-d. de versement d'une prime pour détection d'une faille, qui est une mesure de mise en œuvre de l'art. 27*l*ter ODP. Dans la mesure du possible, les cantons devraient prendre des mesures supplémentaires pour fournir des incitations tant financières que non financières.

Al. 1 : En principe, les cantons veillent à ce que le public intéressé puisse soumettre des indications pour améliorer le système (programme de *bug bounty*). Ce programme de *bug bounty* devrait être lancé bien avant la présentation au Conseil fédéral d'une demande d'autorisation générale. Un délai d'environ six mois avant le déploiement prévu est considéré comme raisonnable. Le programme de *bug bounty* prévoit un programme récurrent de recherche d'erreurs (let. a) et un test internet (let. b).

Al. 1, let. a : Recherche d'erreurs dans la documentation ou le code source publiés et recherche de failles par analyse du système dans sa propre infrastructure. Ce programme de recherche de défauts fonctionne en continu.

Al. 1, let. b : Ce « test Internet » vise exclusivement à pénétrer dans l'infrastructure. Les attaques par déni de service (DoS) et par ingénierie sociale peuvent être exclues du programme de *bug bounty*. Le test Internet peut être mis en œuvre soit comme un programme permanent, soit comme un test récurrent de durée limitée.

La participation au programme de *bug bounty* est régie par l'art. 12 OVotE.

Le service à désigner pour gérer le programme de *bug bounty* peut être un service du canton lui-même, l'exploitant du système ou une société externe.

Al. 2 : Ce service permet la mise en œuvre du programme, reçoit les indications et assure la communication avec la personne qui a fourni l'indication. Il doit être informé des décisions relatives à l'issue qui sera donnée à l'indication fournie et des mesures qui pourront être prises.

Devront en outre être publiées les informations sur les indications reçues. Les informations suivantes devront ainsi être publiées : informations sur le contenu de l'indication, source de l'indication (pour autant que la personne ou l'institution qui l'a fournie soit d'accord), évaluation faite par le service responsable du programme de *bug bounty* et informations sur les mesures éventuellement prises sur la base de l'indication.

Al. 3 : Les indications qui ont un rapport direct, mais aussi celles qui ont un rapport indirect, avec la sécurité doivent être rétribuées, à condition qu'elles contribuent à l'amélioration du système. Les indications ayant un lien indirect avec la sécurité sont, par exemple, celles qui améliorent la qualité du code source. La qualité du code source, en effet, est notamment déterminante pour la lisibilité et donc aussi pour la probabilité de pouvoir trouver des erreurs. Le montant de la rétribution est à fixer en fonction de l'importance de la faille, et devra être suffisamment incitatif pour encourager réellement le public disposant des connaissances nécessaires à participer.

Les bases juridiques de la ChF définissent simplement le cadre du programme de *bug bounty*. Les modalités précises du programme, par exemple la définition de catégories permettant d'évaluer le caractère de gravité des failles ou encore la détermination du montant de la rétribution financière, relèvent de la compétence des cantons ou de l'exploitant du système. La Confédération vérifie dans le cadre de la procédure d'autorisation dans quelle mesure la procédure choisie par les cantons et le service compétent en vertu de l'al. 1 a permis d'atteindre les objectifs du programme de *bug bounty*.

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

Les tâches et les compétences étaient précédemment définies dans l'annexe. Leur répartition est désormais réglée dans la partie principale de l'OVotE.

Al. 2 : Cette disposition s'applique notamment aux tâches suivantes :

- Tâches du service compétent au niveau cantonal selon l'al. 3.
- Détermination de la conception du matériel de vote ainsi que des informations qu'il contient.
- Exploitation du composant de configuration et d'au moins un composant de contrôle du groupe contenant une partie de la clé de déchiffrement des suffrages (ch. 3.1 de l'annexe).
- Déchiffrement et dépouillement des suffrages (ch. 11.2 de l'annexe).
- Communication avec les électeurs sur des questions concrètes liées au vote.

À l'exception des tâches importantes, le canton peut déléguer les tâches principales à des entités extérieures, même s'il continue d'en assumer la responsabilité générale au sens de l'al. 1. Ainsi, il assume par exemple intégralement les risques liés à l'exécution d'une tâche, même si celle-ci a donné lieu à délégation. Par dérogation aux tâches importantes qui doivent être exécutées par le canton, la communication sur les questions relatives au fonctionnement du système peut faire l'objet d'une délégation s'il s'agit de questions de nature particulièrement technique qui nécessitent des connaissances très spécialisées.

Al. 3 : Les tâches du service compétent au niveau cantonal étaient précédemment définies dans l'annexe. Elles sont désormais réglées dans la partie principale de l'OVotE.

Al. 3, let. a : La directive globale sur la sécurité de l'information peut être une directive générale du canton ou une directive applicable spécifiquement au vote électronique. Elle définit les objectifs, le cadre et les responsabilités en matière de sécurité de l'information. Elle comporte également un catalogue de directives pour la sécurité de l'information de niveau inférieur et précise les modalités de sa gestion. Elle est communiquée à tous les collaborateurs et doit être revue et adaptée à intervalles planifiés.

Al. 3, let. b : La directive sur la classification et le traitement de l'information définit un cadre de sécurité contraignant pour l'exploitation du système dans son ensemble. Elle est communiquée aux collaborateurs concernés et doit être revue et adaptée à intervalles planifiés.

Al. 3, let. c : La directive sur la gestion du risque définit notamment le champ d'application et les limites de la gestion des risques liés à la sécurité de l'information, l'organisation de la gestion des risques, les critères d'acceptation des risques et la méthode à appliquer pour effectuer l'appréciation des risques. Elle doit être revue et adaptée à intervalles planifiés.

Al. 3, let. d : Exemples de mesures : réalisation de l'appréciation des risques, contrôle de la conformité avec les directives sur la sécurité de l'information, révision de directives sur la sécurité de l'information, mise à disposition d'outils appropriés.

Al. 3, let. f : Par « actions et opérations critiques », on entend notamment la préparation du scrutin (ch. 5 de l'annexe), l'ouverture et la fermeture du vote électronique (ch. 9 de l'annexe), le dépouillement de l'urne électronique (ch. 11 de l'annexe) et la destruction des données après la validation des résultats du scrutin (ch. 12.8 de l'annexe).

Al. 3, let. h : La détermination des vérificateurs et l'organisation et la forme concrètes du recours aux vérificateurs sont régies par le droit cantonal. Le service compétent au niveau cantonal accompagne l'intervention des vérificateurs et les instruit. En plus de la formation, l'instruction des vérificateurs comprend l'exécution d'exercices.

Al. 3, let. i : Avec d'autres indicateurs, le nombre et le type des anomalies signalées par les électeurs au canton, notamment, doivent être communiqués aux vérificateurs conformément au ch. 11.10 de l'annexe.

Al. 4 : Les unités d'exploitation agissent sur instruction du canton et répondent devant celui-ci des compétences qu'elles assument.

Al. 5 : L'organisation et la forme concrètes du recours aux vérificateurs sont régies par le droit cantonal.

Art. 15 Documents à joindre aux demandes

Al. 1 : Suite à la modification de l'article 27*b*, let. b, ODP, seule est réglée ici la question des documents à joindre aux demandes d'agrément. Les informations supplémentaires à fournir en vue d'une procédure d'autorisation générale sont définies à l'art. 27*c* ODP.

Le canton peut faire valoir la validité de résultats d'audit ou de pièces justificatives sur plusieurs scrutins (concernant la notion de « validité », cf. aussi le commentaire de l'al. 2). Il explique alors pourquoi il n'y a pas lieu de procéder à un nouvel audit pour le scrutin actuel. Il indique toutes les modifications apportées ou qu'il est prévu d'apporter au système ou aux processus d'exploitation ou d'entretien, jusqu'au moment où aura lieu le scrutin. Il démontre par là qu'il s'agit de modifications mineures qui n'ont pas d'impact négatif sur l'appréciation des risques.

Les informations actuelles sur l'utilisation prévue du vote électronique qui doivent être fournies dans le cadre de la procédure d'agrément comprennent par exemple les versions du système et des composants du système à utiliser, la description et l'explication des éventuelles différences par rapport aux versions contrôlées, les calendriers du scrutin prévu ainsi que des informations actuelles sur l'organisation concrète de la cellule de crise.

En ce qui concerne les justificatifs relatifs au respect des exigences légales, il convient notamment de fournir, dans le cadre de la procédure d'agrément, des justificatifs qui ne font pas partie de la vérification effectuée sur mandat de la ChF. Cela concerne par exemple les informations relatives à la communication prévue avec les électeurs selon l'art. 27*m*, al. 1, ODP, l'établissement de la plausibilité prévu ou déjà effectué selon l'art. 27*i*, al. 2, ODP et la publication prévue ou déjà effectuée des résultats du vote électronique selon l'art. 27*m*, al. 3, ODP ainsi que les pièces justificatives mentionnées aux let. a à e. Cette liste des pièces justificatives comprend – avec des adaptations aux nouvelles dispositions de l'OVotE – l'ancien art. 8, al. 1, OVotE ainsi que la liste figurant à l'ancien ch. 6 de l'annexe de l'OVotE, de sorte qu'il n'y ait plus qu'une seule liste de pièces justificatives. Les délais exacts et d'autres modalités seront fixés à chaque fois par la ChF dans un document séparé.

Al. 1, let. a : Le canton remet les appréciations des risques à jour du canton et, le cas échéant, de ses prestataires de services, conformément à l'art. 4 OVotE. Le canton s'engage à signaler immédiatement tout changement dans l'appréciation des risques.

Al. 1, let. b : Conformément aux compétences en matière de vérification des systèmes et de leur exploitation, les cantons remettent les certificats et leurs annexes qu'ils ont établis dans le cadre des vérifications auxquelles ils ont procédé en vertu de l'art. 10, al. 2, OVotE ainsi que les pièces justificatives permettant de satisfaire à l'obligation de publication prévue à l'art. 10, al. 4, OVotE.

Al. 1, let. c : Le canton présente des pièces justificatives pour confirmer que les éléments visés à l'art. 11 OVotE ont été publiés. Il informe également la ChF des dates auxquelles ils ont été publiés. Il communique également des informations sur les indications reçues du public, parmi lesquelles une liste des indications reçues, l'évaluation faite respectivement par le canton ou l'organe compétent, le montant de la rétribution versée et une description des mesures prises sur la base de ces indications.

Al. 1, let. d : Reprise du ch. 6.3 de l'ancienne annexe de l'OVotE. Le canton soumet d'autres protocoles de test si un test n'est effectué que peu de temps avant le scrutin. Si le système présente des failles dont le canton ou l'exploitant du système ont connaissance, la ChF doit être informée de ces failles, de leurs effets et des mesures prévues.

Al. 2 : Le qualificatif « valides » s'entend aussi bien au sens strict du terme (comme par exemple pour la validité d'un certificat) que dans son acception plus large (documents qui n'ont pas été adaptés et qui n'ont pas à l'être, par exemple parce que la conception du système, l'état des connaissances techniques ou les bases juridiques n'ont pas changé). En cas de renvoi, il devra être établi et confirmé que les documents sont toujours valides.

Art. 16 Autres dispositions

Al. 2 : Un canton peut exceptionnellement être dispensé de remplir certaines exigences, à condition de remplir trois conditions, énumérées aux let. a à c. Il doit notamment exposer de manière intelligible les

raisons pour lesquelles il n'a pas rempli ces exigences. Par exemple, dans un scrutin au système majoritaire, il n'y a pas d'obligation de se conformer aux exigences liées à la vérifiabilité individuelle si, pour émettre le suffrage, il faut entrer un nom dans un champ de texte libre.

4.2.2 Annexe contenant les exigences techniques et administratives applicables au vote électronique

Observations générales

La référence au profil de protection de l'Office fédéral de la sécurité des techniques de l'information (BSI Allemagne ; ch. 3.15 dans la version précédente) a été supprimée, car celui-ci n'est plus géré par le BSI et a été archivé. Les exigences pertinentes du profil de protection ont été incluses de manière sélective dans les exigences existantes ou dans de nouvelles exigences.

Commentaire de dispositions choisies

Ch. 1 Définitions

Ch. 1.3 : Le votant compare les codes affichés à l'écran avec les codes de la référence de vérification.

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

Entre son émission et son dépouillement, un suffrage électronique parvient depuis les plates-formes utilisateur jusqu'au canton, en passant par l'Internet et les nombreux serveurs de l'exploitant du système. Les différents éléments de l'infrastructure utilisée sont nombreux et difficiles à contrôler. Les protocoles cryptographiques permettent de ramener au minimum le nombre des éléments qui pourraient faciliter la tâche à un attaquant qui pourrait modifier les suffrages sans se faire remarquer ou pour compromettre le secret du vote. Les mesures visant à empêcher un attaquant de prendre un élément sous son contrôle peuvent ainsi être concentrées sur un nombre limité d'éléments. Ceux-ci sont donc particulièrement dignes d'être protégés et, idéalement, peuvent également l'être de manière particulièrement efficace et convaincante. Les exigences prévues au ch. 3 s'appliquent à cet égard.

Ces éléments, qui se trouvent parmi les participants du système et les canaux de communication énumérés aux ch. 2.1 et 2.2, sont qualifiés de « fiables ». À première vue, cela peut paraître surprenant : pourquoi qualifier de « fiable » un élément particulièrement digne de protection ? L'explication réside dans le fait que les protocoles cryptographiques ne visent pas à protéger ces éléments. Le qualificatif « fiable » signale aux auteurs et aux lecteurs du document dans lequel le protocole cryptographique est spécifié qu'ils n'ont pas à s'inquiéter d'éventuelles attaques dans lesquelles un attaquant prendrait ces éléments sous son contrôle. Du fait de leur caractère fiable, les participants du système refusent de coopérer avec un attaquant. Le protocole doit être défini de telle sorte que, tant que les participants fiables du système s'en tiennent au protocole, l'attaquant ne parviendra pas à ses fins, même s'il met sous son contrôle les autres participants, non fiables, du système. L'utilisation de ce terme est basée sur la littérature spécialisée.

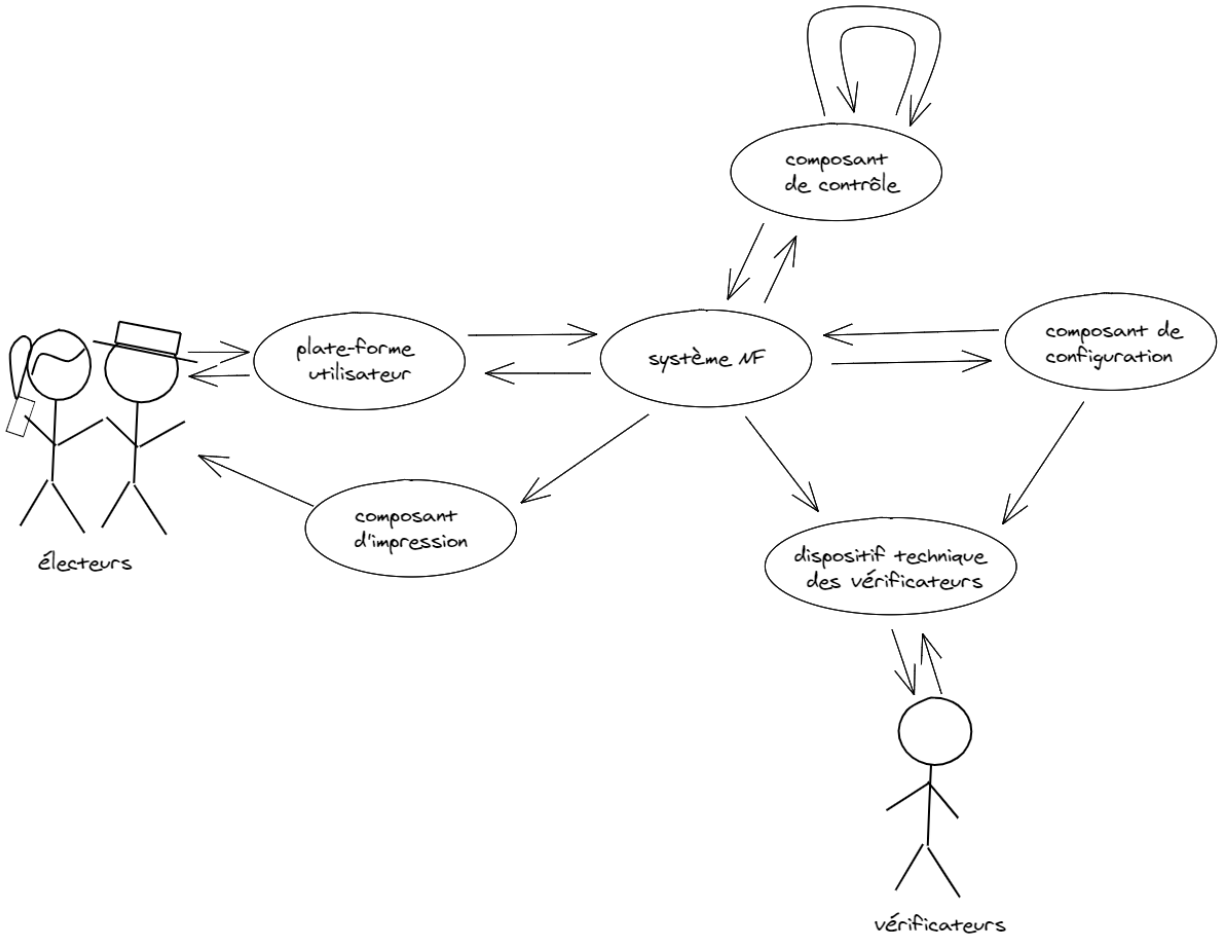
Le protocole cryptographique consiste en des instructions abstraites, écrites en langage mathématique, destinées à tous les participants du système et indiquant les calculs qu'ils doivent effectuer lors de la réception des différents messages, les données qu'ils doivent stocker et les messages qu'ils doivent envoyer via quels canaux. Le protocole est conforme à l'OVotE si l'attaquant au sens du ch. 2.3 ne peut empêcher la réalisation des objectifs visés aux ch. 2.5 à 2.8 dans les conditions prévues aux ch. 2.11 et 2.12 malgré le contrôle qu'il exerce sur les participants du système et les canaux de communication non fiables énumérés aux ch. 2.1, 2.2, 2.9 et 2.10. Le ch. 2.13 exige à cet égard que soient utilisés des éléments cryptographiques sûrs (par ex. des algorithmes de chiffrement) et que les instructions données aux participants du système soient claires et suffisamment précises. Le ch. 2.14 exige des preuves mathématiques de la conformité du protocole (preuves de conformité), comme le veut la pratique scientifique usuelle.

Le développement du système repose sur le protocole cryptographique. Celui-ci ne peut être pleinement efficace que si les instructions des éléments fiables sont correctement mises en œuvre sous forme logicielle et si les composants sur lesquels le logiciel s'exécute sont suffisamment protégés. C'est pourquoi l'OVotE prévoit plusieurs exigences à cet égard. Voir également le commentaire des ch. 2.3 et 2.4.

Ch. 2.1 :

- électeur / votant : les électeurs reçoivent par la poste et avant le scrutin de la part du canton ou de l'imprimerie leurs données d'authentification client confidentielles et leur référence de vérification. Pour pouvoir émettre leur suffrage, ils saisissent leurs données d'authentification client et leur suffrage dans la plate-forme utilisateur. Pour pouvoir faire usage de la vérifiabilité individuelle au sens de l'art. 5 en rel. avec le ch. 2.5, ils vérifient au moyen de la référence de vérification les preuves affichées par la plate-forme utilisateur à destination du votant.
- plate-forme utilisateur : la plate-forme utilisateur génère le message d'authentification et l'envoie au système NF avec le suffrage chiffré et d'autres messages nécessaires pour permettre la vérifiabilité. Elle utilise à cet effet le logiciel, y compris les paramètres publics, qu'elle a reçu auparavant du système NF. Elle affiche à destination du votant les messages envoyés par le système NF, comme par ex. les preuves au sens du ch. 2.5.
- composant de configuration : le composant de configuration est exploité dans l'infrastructure du canton (voir le ch. 3.1). Le canton prépare au moyen de ce composant les données en vue de l'exécution du scrutin. Il s'agit notamment de données dont le caractère aléatoire et la confidentialité sont essentiels pour satisfaire aux exigences du protocole cryptographique énoncées aux ch. 2.5, 2.7 et 2.8, comme par ex. la référence de vérification des électeurs. Ce terme abstrait peut lui aussi inclure différents dispositifs techniques tels que des ordinateurs portables et des supports de données.
- système non fiable (système NF) : le système NF sert de nœud de communication entre les autres participants du système. Il doit être considéré comme non fiable en ce qui concerne toutes les exigences applicables au protocole cryptographique (voir ch. 2.9).
- composant d'impression : il imprime la référence de vérification à l'intention des électeurs. Ce terme abstrait comprend la mise sous pli et l'envoi aux électeurs. Il recouvre également tous les dispositifs techniques utilisés pour l'impression. Outre la machine à imprimer proprement dite, le terme peut également désigner un ordinateur portable permettant de déchiffrer les données d'impression et une clef USB permettant de stocker les données chiffrées.
- un ou plusieurs groupes de composants de contrôle : les composants de contrôle interagissent avec les autres composants de contrôle de leur groupe de telle sorte que les exigences applicables au protocole cryptographique au sens des ch. 2.5, 2.6 et 2.7 sont remplies même si un seul d'entre eux est fiable et fonctionne donc correctement.
- vérificateurs : les vérificateurs reçoivent après le dépouillement de la part du système NF une preuve au sens du ch. 2.6, qui confirme l'établissement correct du résultat. Ils vérifient cette preuve au moins une fois après l'établissement du résultat avec un dispositif technique. Ils peuvent également vérifier des résultats intermédiaires avant ou pendant le scrutin. Ils peuvent notamment assumer avec leur dispositif technique des tâches de vérification du composant de configuration pendant la phase de paramétrage.
- dispositif technique des vérificateurs : les vérificateurs ont besoin d'un dispositif technique pour pouvoir évaluer la preuve au sens du ch. 2.6.

Ch. 2.2 :



Ch. 2.3 : En ce qui concerne les exigences applicables au protocole cryptographique, aucune distinction n'est faite entre des attaquants ayant des moyens ou un bagage technique différents : qu'un attaquant prenne sous son contrôle des participants du système en usant de menaces, de piratage ou d'ingénierie sociale est sans importance pour la définition du protocole cryptographique. Le préalable est plutôt que l'attaquant doit avoir pris sous son contrôle les participants du système et les canaux de communication non fiables. Le protocole cryptographique doit être défini de telle façon que l'attaquant ne puisse causer aucun dommage malgré des attaques réussies sur de tels participants du système et canaux de communication. Cela suppose implicitement que l'attaquant n'est pas capable de casser les éléments cryptographiques et leur mise en œuvre dans le code source. C'est cet objectif que visent les exigences prévues aux ch. 2.13 et 2.14 et les exigences applicables à la qualité du développement du logiciel au sens des ch. 24 et 25.

Ch. 2.3.2 : L'attaquant peut introduire des messages par des canaux non fiables, par exemple en modifiant ou en reproduisant à son avantage des messages échangés par d'autres acteurs.

Le ch. 2.3.2 définit les hypothèses à formuler sur les capacités des attaquants (« que peuvent obtenir les attaquants en tout cas »). Le ch. 2.4 définit dans quelle mesure les capacités peuvent être considérées comme limitées (« que ne peuvent pas forcément obtenir les attaquants »).

Ch. 2.4 : Les participants au système et les canaux de communication fiables sont considérés comme protégés contre l'attaquant. Moins il y a d'éléments considérés comme fiables, et plus la protection offerte par le protocole cryptographique doit être étendue (cf. commentaire introductif du ch. 2). Le chiffre 2.9 définit les participants au système et les canaux de communication qui peuvent être considérés comme fiables au regard des exigences des ch. 2.5 à 2.8.

Il est a priori souhaitable de considérer les participants au système et les canaux de communication comme non fiables même si cela n'est pas nécessaire selon le ch. 2.9. Cette possibilité est toutefois limitée. Par exemple, il ne serait pas possible de constater des manipulations selon le ch. 2.6 si tous les vérificateurs n'étaient pas fiables et agissaient donc selon les instructions de l'auteur de l'attaque. Les

possibilités de renforcer encore la vérifiabilité en réduisant les hypothèses de confiance doivent être examinées en collaboration avec la science sur la base du catalogue de mesures de la Confédération et des cantons[11], et les systèmes devront être adaptés en conséquence.

Les exigences applicables à l'exploitation des composants fiables figurent au ch. 3.

On peut supposer que les messages envoyés par des canaux fiables ne sont pas manipulés. Le récepteur du message peut ainsi se fier à ce que l'émetteur est bien le participant du système spécifié par la définition du canal.

Ch. 2.5 : Les preuves ne peuvent déployer leur efficacité que si les votants les vérifient effectivement et s'ils s'adressent à l'autorité compétente en cas de doute. La recherche et le suivi scientifique pourraient étudier dans quelle mesure ils le font et quelles mesures pourraient inciter les votants à vérifier les preuves conformément aux instructions. Certaines exigences de l'OVotE pourraient contribuer à faire des preuves un outil efficace. Par ex., la répartition des preuves en preuves partielles conformément aux ch. 2.12.5 à 2.12.10 doit permettre aux votants de mettre fin à leur vote avant qu'il ne soit définitif pour se tourner vers le vote par correspondance ou à l'urne au cas où ils rencontreraient des difficultés liées à la vérification. Contrairement à ce qui est le cas avec les premières preuves partielles, la vérification de la preuve partielle confirmant le vote définitif doit être particulièrement facile à effectuer. L'exigence prévue au ch. 8.8 vise à rendre plus difficiles les attaques par ingénierie sociale destinées à empêcher les votants de procéder correctement à la vérification des preuves. Le ch. 8 prévoit au surplus des exigences supplémentaires en matière d'information et d'assistance aux électeurs. Les attaques par ingénierie sociale doivent être évaluées dans le cadre de l'appréciation des risques conformément au ch. 13.

Une preuve correcte confirme aux votants qu'au moins le composant de contrôle qui peut être considéré comme fiable en vertu du ch. 2.9.1 a enregistré le suffrage comme ayant été émis conformément à la procédure prévue par le système. En vérifiant les preuves selon le ch. 2.6, les vérificateurs établissent que le suffrage a également été comptabilisé correctement et donc conformément à la preuve prévue au ch. 2.5, qui a été affichée à l'intention des votants. Pour que la vérification de la preuve visée au ch. 2.6 soit réussie, tous les composants de contrôle doivent avoir enregistré les mêmes suffrages comme ayant été émis conformément à la procédure prévue par le système. Les cas où les composants de contrôle présenteraient à cet égard des incohérences doivent être anticipés conformément au ch. 11.11 et la marche à suivre doit être déterminée au préalable.

La disposition ne prescrit pas comment interpréter les cas où une preuve serait affichée de manière incorrecte ou pas du tout. Ainsi, il ne serait pas illicite que le groupe des composants de contrôle enregistre un suffrage comme ayant été émis conformément à la procédure prévue par le système alors que tel n'est pas le cas. Le ch. 2.6 impose toutefois que ces suffrages soient mis à part ultérieurement afin de permettre aux vérificateurs de s'assurer que l'attaquant n'a pas inséré de suffrages non émis conformément à la procédure prévue par le système. Enfin, en vertu du ch. 10, le système NF (pas nécessairement le groupe des composants de contrôle) doit détecter ces suffrages au moment de leur émission et il ne doit pas les assimiler à des suffrages émis conformément à la procédure prévue par le système.

En ce qui concerne la précision « 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 », une telle preuve serait d'une utilité limitée pendant le scrutin, car l'attaquant aurait encore le temps d'émettre un suffrage. Aussi est-il suffisant que les électeurs puissent demander cette preuve après le scrutin. Pour des raisons d'efficacité, il suffit que le service cantonal compétent confirme à l'électeur qu'aucun suffrage n'a été émis en son nom. Pour ce qui est de la vérification par le service compétent, les hypothèses de confiance énoncées au ch. 2.9.1 s'appliquent, le dispositif technique des vérificateurs pouvant lui aussi être considéré comme fiable. Cette exigence va au-delà du modèle de confiance dans la mesure où l'attaquant au sens du ch. 2.8 ne doit en aucune façon pouvoir accéder aux données d'authentification client. En ce qui concerne la présente exigence, il faut supposer que l'attaquant a accès aux données d'authentification client de certains électeurs.

Ch. 2.6 : Un vote n'est considéré comme ayant été émis conformément à la procédure prévue par le système que si les données d'authentification client utilisées correspondent à des données d'authentifi-

[11] Voir mesures A.5 et A.6 du rapport final du CoPil VE du 30 novembre 2020, accessible sous www.bk.admin.ch > Droits politiques > Vote électronique > Rapports et études.

cation serveur ayant été définies et « attribuées » à un électeur pendant la phase de préparation du scrutin. La preuve doit donc inclure la confirmation qu'aucunes données d'authentification non attribuées n'ont été créées pour l'émission de suffrages. À cette fin, les composants de contrôle ou les vérificateurs doivent avoir reçu lors de la préparation du scrutin des données correspondantes destinées à servir de moyen de comparaison. Les vérificateurs doivent établir que le nombre des données d'authentification correspond au nombre (officiel) des électeurs autorisés à voter. Dans ce cas, on peut considérer que les données d'authentification ont été « attribuées » à un électeur. Il est vrai que cela ne garantit pas que des données d'authentification client d'électeurs fiables n'ont pas été utilisées abusivement pour émettre un suffrage conformément à la procédure prévue par le système. Toutefois, selon le ch. 2.5, les électeurs doivent être en mesure de le déterminer.

Ch. 2.7.2 : Moins il y a de voix comptées dans un cercle électoral, plus grande est la probabilité que toutes les voix soient identiques. Si un attaquant a accès au résultat d'un cercle électoral avec des voix identiques et qu'il parvient en outre à connaître l'identité des votants, il pourrait compromettre le secret du vote sans effort supplémentaire. Il pourrait aussi apprendre comment les votants n'ont pas voté. Cette situation se présente aussi bien pour le vote classique que pour le vote électronique. Comme pour le vote classique, la présente ordonnance ne règle pas la taille minimale des cercles électoraux.

Dans les grands cercles électoraux, les attaques sont plus difficiles. On part néanmoins ici de l'hypothèse d'un attaquant qui tente de compromettre le secret du vote de manière similaire. Tout d'abord, il devrait faire en sorte que seul un petit nombre de voix soit comptabilisé en contrôlant des participants au système qui ne sont pas fiables. Par exemple, il pourrait essayer de manipuler le système NF de manière à ce que la plupart des suffrages ne soient pas transmis au composant de contrôle après avoir été émis. Si l'attaque réussit, seuls les suffrages de personnes sous le contrôle de l'attaquant ou dont il tente de compromettre le secret de vote seront enregistrés après la fermeture (éventuellement provisoire) du canal de vote électronique. Sur la base de la fiabilité d'au moins un composant de contrôle, il est recommandé aux cantons d'examiner, en tenant compte du nombre de suffrages enregistrés par les composants de contrôle, si une attaque semble possible et si le secret du vote pourrait être menacé par le dépouillement. Les cantons décident si les suffrages doivent être dépouillés. Les cantons déterminent, sur la base de l'expérience croissante en matière de vote électronique, le nombre maximal de suffrages qui pourrait suggérer une attaque.

Ch. 2.7.3 : On peut supposer que la manipulation du logiciel du serveur est sans effet sur la fiabilité de la plate-forme utilisateur pendant la vérification.

S'il y a pour cela de bonnes raisons, la base de comparaison utilisée pour la vérification peut également être publiée sur une plateforme externe sûre et considérée comme fiable. Une telle plateforme ainsi que le canal de communication correspondant peuvent notamment être considérés comme fiables au sens des ch. 2.9.3.2 et 2.10.2.

Les possibilités de protéger les plates-formes utilisateur contre les risques d'abus sont beaucoup plus faibles que pour les composants dans un environnement protégé. C'est cependant délibérément, dans un souci de convivialité, qu'on n'a pas voulu utiliser le protocole cryptographique pour garantir le secret du vote et l'impossibilité d'établir des résultats partiels anticipés. Le protocole doit toutefois offrir une protection là où les suffrages sont conservés de manière centralisée. Qualifier la plate-forme utilisateur de « fiable » indique qu'il n'y a pas lieu de prendre en compte d'attaque contre la plate-forme utilisateur lors du développement et de l'analyse du protocole cryptographique (voir le commentaire introductif du ch. 2).

Ch. 2.9.3 : L'une des conséquences est que la clef nécessaire au déchiffrement des suffrages doit être répartie entre quatre composants de contrôle différents. Au moins un de ces composants de contrôle doit être exploité par le canton (comme cela est dit expressément au ch. 3.1).

Une proportion importante des électeurs doit être considérée comme non fiable afin que le système NF puisse apprendre en collaboration avec un électeur non fiable le contenu d'un suffrage émis. À cette fin, il faut s'assurer que cet électeur ne puisse faire passer pour sien un suffrage chiffré émis, même après adaptation externe, dans le but d'apprendre le contenu du suffrage au moyen de la preuve obtenue dans le cadre de la vérification de la preuve prévue au ch. 2.5. Un attaquant pourrait essayer avant le dépouillement de marquer des suffrages avec l'aide des participants non fiables du système pour ensuite compromettre le secret du vote au moyen des suffrages décryptés. Après le dépouillement, les vérificateurs

pourraient constater que les suffrages n'ont pas été traités conformément à leur saisie, mais sous une forme marquée. À ce stade, cependant, le secret du vote aurait déjà été compromis. Il s'agit de prévenir une telle situation au moyen d'un groupe de composants de contrôle garantissant avant le dépouillement qu'aucun suffrage marqué ne sera traité. En ce qui concerne le qualificatif « fiable » appliqué à la plate-forme utilisateur, voir le commentaire du ch. 2.7.3 (deuxième paragraphe).

Ch. 2.9.3.3 : Ainsi, aucun exploitant du système privé ne dispose des données qui seraient nécessaires pour compromettre le secret du vote ou obtenir des résultats partiels anticipés.

Ch. 2.11.1 : L'une des conséquences de cette disposition est qu'une preuve doit pouvoir prendre au moins 1000 valeurs différentes (pour un code numérique, par ex., toutes les valeurs entre 000 et 999). Ainsi, la probabilité pour l'attaquant de deviner correctement une preuve serait exactement de 0,1%. En recueillant des informations sur les participants du système et les canaux de communication non fiables, il pourrait se procurer un avantage qui lui permettrait de ne plus avoir à deviner le code entièrement au hasard, ce qui augmenterait d'autant la probabilité précitée. Eu égard à ces éventualités, un code doit pouvoir prendre a priori des valeurs en nombre suffisant pour que la probabilité ne dépasse pas 0,1%.

Ch. 2.11.3 : On admet à titre d'hypothèse que ladite probabilité est de 1 %. En ce cas, il y aurait lieu de répéter les décomptes jusqu'à ramener cette probabilité à moins de 1 %. Une répétition de ces décomptes doit ainsi permettre de réduire cette probabilité autant que nécessaire.

Ch. 2.12.4 : Cette déclaration n'implique pas que le suffrage a été définitivement émis. Tout d'abord, le votant doit avoir la possibilité de vérifier sa transmission correcte au moyen d'une première preuve partielle. Ensuite, il doit pouvoir mettre fin à l'opération de vote pour se rabattre sur un canal de vote classique.

Ch. 2.12.5 : L'objectif de la division de la preuve en sous-preuves est de la rendre plus facile à utiliser par le votant. Cette division ne vise pas un renforcement de la validité.

Il n'est pas permis de faire effectuer aux votants une vérification pour des raisons purement psychologiques si le résultat de la vérification n'est pas pertinent pour évaluer si le suffrage a été manipulé.

Ch. 2.12.8 : Au cas où deux preuves partielles sont utilisées pour se conformer au ch. 2.5, l'avant-dernière preuve partielle est équivalente à la première preuve partielle. En outre, on peut déduire du ch. 2.8 que les votants doivent saisir avec la déclaration de volonté prévue au ch. 2.12.8 un élément secret qui n'a pas encore été saisi dans la plate-forme utilisateur. L'élément secret peut simultanément être compris comme une donnée d'authentification client.

Ch. 2.12.11 : Les composants de configuration et les composants d'impression sont destinés a priori à être utilisés pour la préparation du scrutin. Mais leur utilisation à un moment ultérieur, par exemple, n'est ici pas interdite. Le traitement des suffrages ou des autres données qui ne sont pas générées avant le scrutin ne devrait cependant pas pouvoir intervenir en étant fondé sur l'hypothèse que ces composants sont fiables. Si ces composants sont utilisés pour le traitement de telles données, ils ne doivent donc pas être considérés comme fiables.

Ch. 2.14.1 : Dans les cas où le ch. 2.9.3.3 s'applique, l'exclusion prévue au ch. 2.7.2 permet de formuler des hypothèses différentes de celles des ch. 2.9.3.1 et 2.9.3.2 pour prouver la conformité avec le ch. 2.7. Par exemple, on peut supposer qu'un composant de contrôle enregistre correctement un nombre suffisant de suffrages d'électeurs fiables, tels qu'ils ont été envoyés par la plate-forme utilisateur fiable, et qu'il ne les efface pas par la suite. Ou alors, il serait permis de supposer que le secret du vote n'est pas menacé lorsqu'ont été dépouillés une seule fois non pas tous les suffrages exprimés, mais une partie quelconque d'entre eux.

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

Le présent chapitre dresse la liste des exigences applicables aux composants qui, conformément au protocole cryptographique, sont réputés fiables afin que soit remplie au moins l'une des exigences prévues aux ch. 2.5 à 2.8. Il peut s'agir des composants suivants :

- composants de configuration
- composants d'impression

- composants de contrôle
- dispositifs techniques des vérificateurs

Ch. 3.1 : Font partie de l'exploitation la mise en place (système d'exploitation, environnement d'exécution, logiciel de vote électronique), la vérification de la conformité des fichiers avec le logiciel de vote électronique, la mise à jour, la configuration et la sécurisation du composant concerné. Voir également le commentaire du ch. 2.9.3.

Ch. 3.2 : La base de sélection des valeurs aléatoires (*seed*) doit accumuler suffisamment d'entropie pour que les éléments de base cryptographiques selon le ch. 15.4 soient efficaces. Cela peut être favorisé par l'agrégation de valeurs aléatoires provenant de différents composants indépendants. Dans tous les cas, il convient d'utiliser des fonctions et des bases dont la fiabilité est généralement reconnue. Le cas échéant, il convient de veiller à ce que les conditions nécessaires soient réunies. Ces conditions peuvent inclure le fait qu'un système d'exploitation ne calcule pas de valeur aléatoire tant que les sources utilisées (qui peuvent inclure, par exemple, le mouvement du curseur de la souris) n'ont pas contribué suffisamment à l'entropie.

Ch. 3.4 : L'organisation et les modalités concrètes du recours aux vérificateurs dépendent du droit cantonal. Voir aussi à cet égard le commentaire de l'art. 27*m*, al. 2, ODP.

Ch. 3.6 : Le processus de vérification doit être observable, ce qui signifie que les personnes qui pourraient assister au processus doivent pouvoir comprendre autant que possible la signification et les résultats des différentes étapes. Elles doivent pour cela avoir la possibilité de témoigner de l'exécution correcte de ces étapes, par exemple en se rendant sur le lieu d'exécution. En ce qui concerne l'installation du logiciel, il convient de tenir compte du ch. 24.3.

Ch. 3.7 : Il s'agit non seulement du logiciel de vote électronique, mais aussi des logiciels de l'infrastructure, comme les systèmes d'exploitation. Il convient de s'assurer que le logiciel provient d'une source officielle et fiable.

Ch. 3.14 : Contrairement à une forme plus faible du double contrôle, il faut garantir que personne ne puisse pas accéder à des données critiques sans qu'une autre personne ne le remarque. Il ne suffit donc pas de limiter le double contrôle à l'exécution des étapes du processus. Pour assurer un double contrôle strict, la conservation sécurisée de données critiques pourrait consister à stocker les données sous forme chiffrée sur un support et à conserver celui-ci dans un coffre-fort, la première personne connaissant le code d'accès au coffre-fort et l'autre la clé pour déchiffrer les données.

Ch. 3.15 : Il est suffisant d'utiliser le même logiciel pour tous les composants de contrôle. Des logiciels indépendants du fournisseur seront utilisés à l'avenir pour certains composants de contrôle, selon le catalogue de mesures de la Confédération et des cantons[12].

Ch. 3.18 : Un logiciel indépendant du fournisseur pour le dispositif technique des vérificateurs sera utilisé à l'avenir selon le catalogue de mesures de la Confédération et des cantons[13].

Ch. 4 Procédure de vote

Ch. 4.9 : Cette disposition autorise le canton à offrir la fonctionnalité correspondante. Mais le canton n'y est pas obligé.

Ch. 4.10 : En l'occurrence, on peut faire dépendre le caractère concluant des preuves de la fiabilité de la plate-forme utilisateur. Cela permet par ex. de numériser la référence de vérification avant le vote. Ces facilités sont réservées à un petit groupe d'électeurs qui ne pourraient pas interpréter la preuve sans elles. Les électeurs auxquels ce cas ne s'applique pas doivent être incités à vérifier les preuves conformément à la procédure prévue.

Ch. 4.11 : Les votants sont tenus d'informer l'autorité cantonale compétente en cas d'affichage incorrect d'une preuve ou d'incertitude à cet égard. Le vote par correspondance ou à l'urne reste possible tant

[12] Voir mesure A.4 du rapport final du CoPil VE du 30 novembre 2020, accessible sous www.bk.admin.ch > Droits politiques > Vote électronique > Rapports et études.

[13] Voir mesure A.4 du rapport final du CoPil VE du 30 novembre 2020, accessible sous www.bk.admin.ch > Droits politiques > Vote électronique > Rapports et études.

qu'aucun suffrage électronique n'a été enregistré. Pour le vérifier, les cantons disposent de la possibilité prévue au ch. 11.6.

Ch. 4.12 : La confirmation de l'émission définitive du suffrage conformément au ch. 2.12.8 doit être effectuée à l'aide d'un élément secret n'ayant pas encore été saisi dans la plate-forme utilisateur. Il n'est pas exclu d'utiliser une e-ID comme substitut à cet élément secret. Cette possibilité devrait s'appuyer sur une appréciation des risques. Toutefois, l'e-ID ne pourra pas remplacer l'envoi par la poste de la référence de vérification. L'envoi postal du matériel de vote restera nécessaire dans un premier temps.

Par ailleurs, la disposition selon laquelle la possibilité d'utiliser une e-ID doit être examinée sur la base d'une appréciation des risques, s'applique même si cette e-ID est délivrée ou reconnue par l'État.

Ch. 7 Exigences applicables aux imprimeries

Les exigences applicables aux imprimeries ne sont plus réglementées dans un catalogue d'exigences distinct, mais figurent directement dans l'annexe. Ces dispositions s'appliquent en plus des dispositions du ch. 3.

Ch. 7.4 : Par ex., le support de données et l'élément secret nécessaire au déchiffrement doivent être conservés séparément l'un de l'autre dans un endroit sûr (par ex. un coffre-fort). La personne qui détient l'élément secret permettant de déchiffrer les données ne doit pas pouvoir ouvrir le coffre sans que nul ne s'en rende compte. Le déchiffrement et le traitement des données ainsi que le processus d'impression doivent être effectués selon le principe du double contrôle. Il doit être impossible que les données soient présentes sur un composant sous une forme non chiffrée sans qu'au moins deux personnes surveillent ce composant et informent au besoin d'un abus qui aurait éventuellement été commis.

Si le principe du double contrôle ne peut être mis en œuvre de manière continue lors du traitement de données critiques, par ex. en raison d'une interruption relativement longue, les données doivent être détruites.

Ch. 7.6 : Si de bonnes raisons le justifient, la destruction des données peut être reportée au plus tard jusqu'à ce que les exigences légales applicables à la conservation et à la traçabilité soient remplies.

Ch. 8 Information et assistance

Ch. 8.8 : Cette règle s'applique également lorsque la première preuve partielle selon le ch. 2.12.5 était erronée et que l'électeur a interrompu en conséquence le processus de vote.

Ch. 8.9 : Cette disposition vise à éviter les cas où des tiers utilisent abusivement le matériel de vote d'autres personnes pour voter. Il convient de tenir compte du fait que les détenteurs du matériel de vote ne peuvent pas nécessairement détecter un vote abusif sans consulter le système au sens du ch. 2.5 (deuxième tiret). En outre, il faut tenir compte du fait qu'un vote peut rester possible même après l'affichage de la première preuve partielle selon le ch. 2.12.5.

Ch. 8.11 : Les votant doivent connaître la procédure correcte pour émettre leur suffrage afin d'être protégés contre les attaques par ingénierie sociale. En envoyant les instructions par la poste et en recommandant de suivre ces instructions en cas de doute et de s'adresser au besoin au service cantonal compétent, les autorités rendent plus difficiles les attaques par ingénierie sociale. La recherche et le suivi scientifique pourraient s'intéresser à l'efficacité de cette procédure ainsi qu'à des procédures alternatives d'orientation des électeurs.

Ch. 10 Contrôle de conformité et enregistrement des suffrages définitifs

Seuls des suffrages émis conformément à la procédure prévue par le système doivent être enregistrés en vue du dépouillement. Cette fonctionnalité peut également être assurée au moyen d'un composant non fiable au sens du ch. 2.

On entend par urne électronique une zone de stockage contenant les suffrages prévus pour le dépouillement. L'urne électronique peut être mise en œuvre au moyen des composants de contrôle visés au ch. 2.

Il est également possible de prévoir une zone de stockage supplémentaire, auquel cas l'urne électronique doit dans tous les cas être considérée comme non fiable au sens du ch. 2.4.

Ch. 11 Dépouillement de l'urne électronique

Ch. 11.1 : Le déchiffrement au sens du ch. 11.2 doit avoir lieu le dimanche du vote. Des déchiffrements effectués en amont chez l'exploitant du système peuvent déjà commencer dès la fermeture du canal de vote électronique. L'efficacité du chiffrement doit rester élevée malgré les déchiffrements en amont.

Ch. 11.2 : Si c'est le système d'un autre canton qui est utilisé, le déchiffrement et le dépouillement peuvent également avoir lieu dans le canton qui fournit le système.

Ch. 11.6 : Il n'est pas possible de déterminer si un suffrage émis par correspondance ou à l'urne est un vote double ou même multiple en utilisant uniquement les suffrages émis électroniquement comme base de comparaison. La fonctionnalité prévue au ch. 11.6 n'en entre pas moins dans le champ d'application de l'OVotE. Toutefois, il n'est pas nécessaire de spécifier la fonctionnalité en se référant aux hypothèses de confiance au sens du ch. 2.

Ch. 11.7 : Les vérificateurs doivent en principe se trouver sur le lieu d'exécution. En outre, il est possible de proposer à des vérificateurs supplémentaires de suivre le déroulement des processus, par exemple via une retransmission en direct.

Ch. 12 Données confidentielles

Ch. 12.7 : La Confédération ne règle pas la taille minimale des cercles électoraux, et donc pas non plus notamment des circonscriptions électorales (cf. commentaire du ch. 2.7.2). Si la garantie du secret du vote l'exige, les résultats des petites circonscriptions électorales doivent être traités de manière confidentielle. Lorsque les circonscriptions électorales sont divisées en cercles électoraux, cette exigence s'applique par analogie.

Ch. 12.8 : En ce qui concerne notamment les composants du système dont la fiabilité est déterminante pour la garantie du secret du vote selon le ch. 2.9.3, il faut s'assurer que les données ont été irrémédiablement effacées.

Ch. 13 Menaces

Les objectifs de sécurité (voir art. 4, al. 3, OVotE) ne pourront pas être atteints à coup sûr. Il est en tout cas possible d'identifier des risques en matière de sécurité. Il faut, sur la base d'une appréciation méthodique des risques (voir art. 4, al. 1, OVotE), apporter la preuve que les risques sont suffisamment faibles.

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

La liste des menaces a été adaptée en fonction des connaissances acquises au cours des dernières années et de l'utilisation de systèmes entièrement vérifiables. Les acteurs de la menace ont fait l'objet d'une nouvelle définition et de nouvelles dénominations afin de clarifier les scénarios.

Ch. 13.12 : Le protocole exige que les votants vérifient les preuves conformément au ch. 2.5. Selon cette disposition, il est nécessaire d'évaluer le risque qu'un attaquant externe modifie les informations fournies par le canton afin d'inciter les votants à s'écarter des étapes à suivre pour procéder à cette vérification. Il ne s'agit pas ici de prendre en compte les fausses informations qui pourraient être diffusées sur les réseaux sociaux.

Ch. 13.13, 13.14 et 13.15 : Par moyen électronique, on entend ici un moyen qui permet d'accéder à des informations importantes sans que l'attaquant ait à être physiquement présent. Il peut par ex. s'agir de logiciels malveillants.

Par moyen physique, on entend ici un moyen qui permet à l'attaquant d'accéder à des informations importantes en se rendant personnellement sur place.

L'ingénierie sociale est une méthode qui permet à un attaquant d'accéder à des informations importantes en induisant une personne en erreur afin qu'elle lui fournisse directement les informations souhaitées ou qu'elle lui accorde un accès physique ou électronique.

Ch. 13.16, 13.17 et 13.18 : Le protocole cryptographique définit certains paramètres, algorithmes et procédures. Les menaces mentionnées ici exploiteraient une vulnérabilité présente dans un ou plusieurs de ces éléments.

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

Les systèmes de vote électronique doivent permettre de détecter et d'investiguer efficacement les incidents, tels que les soupçons de manipulation des votes ou les attaques contre le système. Il y a lieu de définir le contenu et l'étendue des journaux système de manière à garantir ces possibilités en garantissant simultanément le secret du vote.

Il faudra par ailleurs mettre en place un processus d'amélioration continue dans le cadre de la détection et de l'investigation des incidents. Ce faisant, il y aura lieu de tenir compte notamment des aspects suivants :

- Un échange ouvert aura lieu entre la Confédération, les cantons et les exploitants des systèmes.
- Des analyses portant sur l'adéquation des systèmes de monitoring et d'investigation seront effectuées régulièrement. Elles prendront en compte les scénarios définis dans la convention de crise. La participation d'experts en forensique à ces analyses permettra d'apporter des améliorations plus efficaces.
- Les éléments résultant de l'analyse seront pris en compte dans le cadre de l'amélioration des instruments et des processus.

L'aspect technique de ces exigences s'adresse principalement à l'exploitant du système. Le service compétent au niveau cantonal doit comprendre le contenu des journaux système et être en mesure de réagir à un signalement transmis par son exploitant de système.

Ch. 14.2 : Les processus de journalisation, d'identification et d'authentification, qui sont particulièrement sensibles, nécessitent une surveillance particulière tant dans la partie du système exploitée par le canton que dans la partie exploitée par l'exploitant du système. L'identification désigne l'opération qui permet d'identifier une personne, par exemple au moyen d'un nom d'utilisateur ou d'une carte à puce. L'authentification désigne quant à elle l'opération qui permet au système de délivrer le droit d'accès, par exemple au moyen de la vérification d'un mot de passe.

Ch. 14.7 : Il s'agit de s'assurer que les suffrages sont traités et décomptés correctement. À cet effet, les suffrages de contrôle sont traités selon les mêmes procédures que les suffrages émis conformément à la procédure prévue par le système. Les suffrages de contrôle ne doivent pas être pris en compte dans le résultat final en tant que suffrages émis conformément à la procédure prévue par le système.

Ch. 14.9 : Cette disposition ne concerne pas nécessairement le système en ligne uniquement. Elle peut également concerner des composants mis en œuvre dans le cadre de la préparation ou du suivi des scrutins.

Ch. 15 Utilisation de mesures cryptographiques et gestion des clefs

Ch. 15.3 : Le chiffrement au niveau du logiciel, indispensable en vertu du ch. 2, n'est pas suffisant pour remplir cette exigence.

Ch. 16 Échange d'informations électronique et physique sûr

Ch. 16.2 : Le système doit être séparé logiquement ou physiquement de toutes les autres activités. Toutefois, certains éléments de l'infrastructure (par exemple, la surveillance, le pare-feu) peuvent être partagés avec d'autres activités si cela n'augmente pas de manière significative les risques du système tout en présentant un avantage substantiel.

Ch. 17 Tests du système

Ch. 17.2 : Les interfaces désignent les éléments qui permettent au logiciel d'échanger des informations avec son environnement. Il peut s'agir d'interfaces graphiques, de lignes de commande ou d'interfaces de programmation (API).

Ch. 17.3 : Dans le cas de cette exigence, on tient compte de deux niveaux dans la structure du logiciel :

- Un module, qui constitue le niveau le plus bas de la structure, regroupe une série de classes du code source qui ont un objectif commun clairement défini.
- Un sous-système est constitué d'un ensemble de modules qui fournissent une fonctionnalité du système, par exemple la gestion d'une votation, l'établissement d'une carte de légitimation ou l'enregistrement d'un vote.

Ch. 22 Gestion de la communication et de l'exploitation

Ch. 22.3 : La vérification du bon fonctionnement de la sauvegarde des données s'effectue au minimum par un test de restauration des données. Il peut être complété par d'autres vérifications visant à une amélioration continue des processus de sauvegarde des données.

Ch. 24 Développement et maintenance de systèmes d'information

La qualité des systèmes de vote électronique doit être garantie tout au long du processus de développement. Afin de renforcer l'assurance qualité, on a précisé les exigences au moyen des objectifs suivants :

- Les modifications apportées au système doivent être traçables et contrôlables.
- La traçabilité entre les différents éléments de la documentation (protocole, spécification, architecture, etc.) et le code source doit pouvoir être assurée de manière continue et dans les deux sens.
- Les résultats des processus de contrôle sont intégrés dans le développement.
- La conformité aux exigences légales est garantie et maintenue tout au long du cycle de vie.

Désormais, les exigences des *Common Criteria* (critères communs) du degré EAL 4 s'appliqueront à l'ensemble du système, et non plus aux seuls composants de contrôle. Elles ont par ailleurs été complétées par des exigences des degrés supérieurs à celles des *Common Criteria* du degré EAL 4, lesquelles s'appliqueront si elles apportent une contribution majeure à la réalisation des objectifs de sécurité et si elles vont dans le sens des objectifs figurant dans le paragraphe précédent.

Ch. 24.1 : Les fonctions de sécurité sont d'une importance capitale pour le logiciel. Elles doivent donc faire l'objet d'un soin particulier et être traçables à toutes les étapes du processus de développement. Il importe de s'assurer que toutes les fonctions de sécurité prévues dans la conception du logiciel sont présentes à tous les niveaux, jusqu'au code source. La notion de code source comprend ici également les éventuelles bibliothèques externes.

Les outils de développement dont il est question ici sont les outils qui revêtent une importance pour la sécurité du développement du logiciel. Il s'agit notamment des outils de l'IDE (*Integrated Development Environment*), des outils de construction (*Build Tools*) et des outils de gestion de la configuration, mais aussi des options de configuration qui peuvent avoir une influence sur la sécurité du développement.

Comme il a été précise au ch. 17.2, les interfaces sont les éléments qui permettent au logiciel d'échanger des informations avec son environnement. Il peut s'agir d'interfaces graphiques, de lignes de commande ou d'interfaces de programmation (API).

Une liste de configuration est un groupe d'éléments de configuration cohérents entre eux qui représentent l'état du logiciel et de la documentation à un moment donné. Dans l'idéal, il permet de reconstituer une version précédente du logiciel.

Ch. 24.3 : Il s'agit de garantir la mise à disposition correcte du système depuis le code source jusqu'à son installation en production (construction et déploiement). Il incombe à cet égard à l'exploitant du système d'utiliser une méthode de construction et de déploiement à la fois éprouvée et traçable, laquelle permettra d'atteindre les objectifs suivants :

- s'assurer que le logiciel utilisé est conforme à la version publiée, testée et autorisée ;
- en plus de cette traçabilité, empêcher autant que possible toute manipulation des composants du système ;
- éviter que les outils de développement et librairies utilisés n'introduisent des vulnérabilités pertinentes pour le logiciel qui rendraient le système vulnérable aux attaques.

Pour ce faire, on a fixé de nouvelles exigences, lesquelles se fondent sur les directives de l'État américain du Colorado qui régissent l'utilisation des systèmes de vote électronique[14], sur la documentation de l'entreprise GitHub relative au *Trusted Build* (construction fiable)[15] et sur la documentation intitulée « *Reproducible Builds* », qui est issue du projet éponyme[16].

Ch. 24.3.3 : Concernant la précision « Cette compilation démontre en particulier que toutes les signatures cryptographiques des dépendances ont été vérifiées sur la base d'une référence établie, publique et fiable » : Il peut par exemple s'agir du dépôt central de Maven.

Ch. 24.4 : Les utilisateurs sont toutes les personnes qui entrent en contact avec le logiciel de quelque façon que ce soit. Il peut s'agir de collaborateurs du canton, d'électeurs, de testeurs et, en fin de compte, de toutes les personnes qui portent un intérêt au système.

Pour que le développeur puisse traiter de façon appropriée les rapports qu'il reçoit concernant des failles et mener une activité de communication efficace dans ce domaine, il est important que les utilisateurs sachent comment lui transmettre ces rapports et comment s'enregistrer auprès de lui pour obtenir les informations en la matière.

Pour contribuer à améliorer la sécurité d'un système, il faut dresser une liste aussi complète que possible des vulnérabilités supposées et les traiter de manière systématique. Les exigences en la matière viennent compléter la publication du code source (art. 11 et 12 OVotE) et la mise en place d'un programme de *bug bounty* (art. 13 OVotE).

Ch. 25 Qualité du code source et de la documentation

La qualité du code source et de la documentation est un élément capital pour la sécurité du vote électronique. Les anciennes bases légales

imposent plusieurs exigences en la matière. Il s'agit toutefois plutôt de descriptions générales, telles que l'obligation de préparer et de documenter le code source conformément aux bonnes pratiques et de mettre en œuvre certains éléments des *Common Criteria*. Aussi a-t-il fallu préciser les critères de qualité qui s'appliquaient précedemment. Des critères clairs devront garantir une qualité élevée des systèmes de vote électronique, ce qui profitera à la sécurité, car cela facilitera les contrôles effectués par tous les acteurs et par le public. Pour définir ces critères de qualité, on a établi un modèle de qualité pour les systèmes de vote électronique. Ce modèle repose sur la norme ISO 25010 et sur le modèle de qualité développé par McCall[17]. Les critères ont été choisi en fonction de la contribution qu'ils peuvent apporter aux objectifs de sécurité et de qualité qui ont été définis.

Ch. 25.7.3 : Le portail de vote électronique doit être accessible et conforme à la norme d'accessibilité eCH-0059. Les contenus de la norme sont obligatoires, à l'exception des exigences relatives aux formes

[14] Colorado Election Rules [8 CCR 1505-1] Rule 1. Definitions, 2020 et Colorado Voting Systems Trusted Build Procedures, 2020

[15] GitHub How to: Trusted builds, 2017

[16] https://reproducible-builds.org/

[17] FACTORS IN SOFTWARE QUALITY - Vol. 1: Concept and Definitions of Software Quality - Jim A. McCall, Paul K. Richards, Gene F. Walters (1977)

de communication alternatives (cf. chap. 2.4 de la norme). La mise à disposition d'informations en langue facile à lire et en langue des signes n'est pas soumise à des exigences plus sévères que celles qui s'appliquent au vote par correspondance ou au vote à l'urne, en particulier en ce qui concerne les informations sur l'objet de la votation, telles que les explications ou les instructions de vote. La preuve que le portail de vote électronique est conforme aux exigences de la norme eCH-0059 comprend soit un certificat, soit un rapport d'audit établi par un organisme spécialisé.

Ch. 25.13.2 : Cette exigence vise à éviter tout comportement inattendu pour toutes les parties du logiciel et pour toutes les valeurs possibles. À cet effet, au moins une valeur doit être testée pour chaque ensemble de valeurs conduisant à des résultats différents. Au sein d'un ensemble de valeurs, il n'y a pas lieu de tester toutes les valeurs. Les situations d'erreur doivent elles aussi être testées.

Ch. 26 Critères de contrôle pour les systèmes et leur exploitation

Les compétences ont été modifiées pour garantir l'efficacité et la crédibilité des contrôles. La répartition des responsabilités entre la Confédération et les cantons a été revue de sorte que la Confédération assume davantage de responsabilités et un rôle plus direct dans le contrôle des systèmes.

La Confédération aura la compétence de vérifier que les exigences relatives au système et aux processus sous-jacents sont remplies, ce qui favorisera notamment le fait que les connaissances issues des audits viendront alimenter de façon ciblée la suite du déroulement de la phase d'essai. Des experts externes seront chargés de procéder aux audits.

Le canton ou l'exploitant du système continuera d'être responsable des contrôles liés à l'exploitation du système dans ses centres informatiques (certification ISO 27001).

Il est renoncé à demander une certification plus poussée aux services accrédités par le Service d'accréditation suisse (SAS).