Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF
Section des droits politiques

Vote électronique

Catalogue des mesures de la Confédération et des cantons

Adopté par le Comité de pilotage Vote électronique (CoPil VE) le 20 février 2023

Table des matières

1. Contexte

Dans le cadre de la restructuration de la phase d'essai du vote électronique, la Confédération et les cantons ont adopté un rapport final assorti d'un grand catalogue de mesures[1]. La restructuration de la phase d'essai doit permettre aux cantons de reprendre les essais et de lancer une phase d'essai stable avec des systèmes de vote électronique de la dernière génération. La première étape de la restructuration comprenait de nombreuses mesures, qui ont notamment été mises en œuvre par la révision des bases légales, laquelle est entrée en vigueur en juillet 2022. Cette révision a pris la forme d'une révision partielle de l'ordonnance sur les droits politiques (ODP ; RS 161.11) et d'une révision totale de l'ordonnance de la Chancellerie fédérale (ChF) sur le vote électronique (OVotE ; RS 161.116)[2].

La sécurité des systèmes de vote électronique a été renforcée par cette révision dans la mesure où les exigences en matière de sécurité et de qualité vis-à-vis des systèmes, de leur développement et de leur exploitation ont été précisées et augmentées. De plus, ne sont plus autorisés que des systèmes comportant la vérifiabilité complète qui ont fait l'objet d'un contrôle par des experts indépendants sur mandat de la Confédération. Ils ne peuvent être utilisés que par maximum 30% de l'électorat cantonal et 10% de l'électorat national. L'amélioration continue des systèmes de vote électronique et de leurs modalités d'exploitation est au cœur de la nouvelle phase d'essai, l'objectif étant de développer et de renforcer la sécurité en continu. Les enseignements tirés de la pratique doivent également être intégrés dans ce processus d'amélioration continue. Ce principe est pris en compte dans la procédure d'autorisation. En vertu de l'art. 16, al. 2, OVotE, la ChF peut même autoriser des systèmes de vote électronique si les cantons font valoir des exceptions au respect des exigences. Les exceptions de ce type doivent être justifiées par les cantons, les éventuelles mesures de remplacement doivent être décrites, et l'élimination éventuelle de la non-conformité doit être annoncée. Quand un besoin d'action subsiste, le système de vote électronique ne peut être utilisé que si les risques inhérents à son utilisation sont malgré tout suffisamment faibles.

La Poste Suisse a publié le code source et la documentation de son nouveau système à vérifiabilité complète dès 2021. Depuis, le système et son exploitation ont été vérifiés à plusieurs reprises par des experts indépendants et par le public, en ce qui concerne ce dernier dans le cadre d'un programme de *bug bounty* et d'un test d'intrusion public, permettant ainsi à la Poste de les améliorer considérablement. Ce système devrait être utilisé par les cantons de Bâle-Ville, Saint-Gall et Thurgovie pour la reprise des essais de vote électronique tels que prévus par l'ODP.

Des besoins d'action supplémentaires ont été identifiés, notamment lors du contrôle indépendant mandaté par la ChF. Ils comprennent quelques points qualifiés de non-conformité ainsi que des points appelant des améliorations supplémentaires pour un respect plus efficace des exigences. Afin de répondre aux besoins existants et d'aborder et de mettre en évidence les développements nécessaires dans le domaine du vote électronique, la Confédération et les cantons gèrent en commun le présent catalogue de mesures (voir la mesure A.8 figurant au ch. 2.2). Ce catalogue est réexaminé, adapté et publié à intervalles réguliers. La mise en œuvre des mesures fait l'objet, dans toute la mesure du possible, d'un calendrier. Les coûts engendrés par la mise en œuvre des mesures sont analysés et intégrés dans la planification financière commune de la Confédération et des cantons. La mise en œuvre des mesures sera en outre soutenue par des moyens de l'Administration numérique suisse.

[1] Rapport final du Comité de pilotage Vote électronique (CoPil VE) du 30 novembre 2020 sur la restructuration et la reprise des essais ; voir sous www.chf.admin.ch > Droits politiques > Vote électronique > Rapports et études.

[2] Communiqué du Conseil fédéral du 25 mai 2022 ; voir sous www.chf.admin.ch > Droits politiques > Vote électronique > Communiqués de presse.

2. Catalogue des mesures

2.1 Mesures en suspens

Le tableau suivant contient l'état des mesures en suspens selon la décision du CoPil VE du 20 février 2023. Les informations adaptées sont indiquées en italique.

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
A.	**Poursuite du développement des systèmes**				
A.4	Utilisation de composants indépendants du fournisseur (« Verifier », composants contrôle)	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Etude et proposition composants de contrôle en ligne au CoPil VE : *2024* Mise en œuvre sous réserve : *2028*	Etude composants de contrôle en ligne : Cantons, avec la participation de la ChF	Planifié
A.5	Réduction des hypothèses de confiance dans le processus d'impression et le logiciel qui génère les paramètres cryptographiques	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Approfondissement et adaptation du protocole cryptographique, établissement du calendrier de la mise en œuvre : *2023 / 2024* Proposition au CoPil VE : *2025* Mise en œuvre sous réserve : *2025 / 2026*	Clarification des questions ouvertes concernant les exigences : ChF Mise en œuvre : Cantons *et fournisseur du système*	Planifié
A.6	Approfondissement des informations servant de base à l'introduction d'un mécanisme de vérifiabilité supplémentaire dont l'efficacité ne repose pas sur les hypothèses de confiance actuelles	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Etude : *2025* Proposition au CoPil VE : *2025*	Etude : ChF avec la participation des cantons	Planifié
A.9	Finalisation de la spécification du système dans le domaine de l'authentification des électeurs	Les spécifications servent d'instructions pour le développement du système. Elles constituent en outre des fondements pour la réalisation d'analyses de la conformité du système avec les exigences légales. Le système doit être spécifié de manière suffisamment précise (ch. 2.13.2 annexe OVotE).	2e trimestre 2023 (utilisation à partir de l'élection du CN en 2023)	Cantons et fournisseur du système	Nouveau

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
		Dans le système de vote électronique de la Poste[3], les électeurs sont authentifiés avant de voter en vertu du ch. 2.8 de l'annexe de l'OVotE, mais cette authentification n'est pas entièrement spécifiée. La spécification dans le domaine de l'authentification des électeurs est finalisée au moyen de la présente mesure et prise en compte dans les preuves de conformité visées au ch. 2.14 de l'annexe de l'OVotE dans la mesure où cela se révèle judicieux. Les parties spécifiées du système, les vérifications effectuées sur le système et les explications fournies par la Poste permettent de conclure, en l'occurrence, que les risques inhérents à la spécification incomplète peuvent être considérés comme suffisamment faibles. Voir l'annexe pour de plus amples informations sur la présente mesure.			
A.10	Réduction des dépendances vis-à-vis de logiciels externes dans le système de la Poste	L'intégration de logiciels externes dans le système de vote électronique peut être judicieuse, notamment pour des raisons de sécurité. C'est en particulier le cas si un logiciel est largement utilisé dans le monde entier, tout en étant constamment testé et amélioré. Plus le logiciel est contrôlé, moins il est probable que des attaquants parviennent à introduire un code malveillant dans le système sans être détectés. La Poste a déjà mis en place un processus visant à réduire le plus possible les risques inhérents à l'utilisation de logiciels externes. La présente mesure permettra à la Poste de réduire davantage sa dépendance vis-à-vis de logiciels externes, notamment de bibliothèques logicielles externes dans le client JavaScript. Les bibliothèques externes ne sont utilisées que si des raisons valables le justifient.	En continu ; client JavaScript : 2e trimestre 2023 (utilisation à partir de l'élection du CN en 2023)	Cantons et fournisseur du système	Nouveau
A.11	Publication du code source du logiciel de génération des fichiers PDF pour l'impression des cartes de légitimation	La publication du logiciel est exigée à l'art. 11 OVotE. Elle contribue à la détection d'éventuelles erreurs ou vulnérabilités. En application de l'art. 11 OVotE, les cantons ont déjà publié le logiciel qui génère les données brutes pour l'impression des cartes de légitimation. Les données brutes contiennent les codes pour le vote et la vérification par les votants dans le but de garantir la vérifiabilité individuelle visée au ch. 2.5 de l'annexe de l'OVotE. Pour convertir les données brutes en documents PDF prêts à être imprimés, les cantons de BS et de TG utilisent le logiciel de la Poste baptisé « Voting Card Printing Service (VCPS) ». Ce logiciel n'est pas publié. Le logiciel utilisé pour générer les fichiers PDF destinés à l'impression des cartes de légitimation sera désormais publié.	2024	Cantons et fournisseur du système	Nouveau

[3] Les besoins identifiés dans le présent catalogue de mesures se réfèrent à la version du système de la Poste qui sera utilisée pour la première fois en juin 2023.

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
		L'étendue des fonctions, les mesures opérationnelles et les contrôles effectués sur le code source permettent de conclure que le fait de ne pas publier le logiciel pour l'instant présente un risque suffisamment faible. Voir l'annexe pour de plus amples informations sur la présente mesure.			
A.12	Les preuves symboliques de la conformité du protocole cryptographique sont développées	Des preuves de sécurité sont générées par ordinateur sur la base de modèles symboliques. Le ch. 2.14.1 de l'annexe de l'OVotE dispose que des preuves de sécurité de ce type doivent attester qu'un protocole cryptographique respecte les exigences en matière de vérifiabilité, de secret du vote et d'authentification. La Poste a établi un modèle symbolique et utilise le programme ProVerif pour générer les preuves en question. Pour que ProVerif puisse produire un résultat en temps utile, il est d'usage de saisir les propriétés réelles du système sous une forme simplifiée dans des modèles symboliques, ce qui entre inévitablement en conflit avec la pertinence d'une preuve. Les contrôles effectués sur le système de la Poste permettent de conclure que les modèles disponibles sont de bonne qualité et que les preuves apportées pour démontrer la conformité du protocole cryptographique ont un contenu substantiel. Dans l'optique d'une amélioration continue pendant la phase d'essai, la prochaine étape consistera à continuer d'étoffer le contenu des preuves dans la mesure où cela est possible et judicieux. Les modèles seront complétés comme suit pour qu'ils reproduisent les propriétés du système de la manière la plus fidèle possible à la réalité : - Dans la mesure où cela est judicieux, l'authentification sera modélisée sur la base de la spécification et prise en compte dans les preuves symboliques (voir également la mesure A.9). - D'autres compléments seront examinés en détail puis mis en œuvre, à moins que l'abandon de la procédure se justifie du point de vue matériel (voir les recommandations 4.1 et 4.2.1 figurant dans le rapport d'audit de l'Université de Surrey du 17.10.2022[4]). En outre, dans la mesure où cela se révèle judicieux, des preuves supplémentaires seront apportées pour démontrer que les modèles sont adaptés à la détection des non-conformités (voir la recommandation 4.2.3 figurant dans le rapport d'audit de l'Université de Surrey du 17.10.2022).	Authentification : 2e trimestre 2023 (utilisation à partir de l'élection du CN en 2023) Autres points : 2025	Cantons et fournisseur du système	Nouveau

[4] Voir sous www.chf.admin.ch > Droits politiques > Vote électronique > Contrôles des systèmes.

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
A.13	Renonciation au problème du SGSP[5] comme hypothèse de sécurité	Le ch. 2.14.1 de l'annexe de l'OVotE dispose que des preuves de sécurité cryptographiques doivent attester que le protocole cryptographique respecte les exigences en matière de vérifiabilité, de secret du vote et d'authentification. Dans l'administration de leurs preuves, les protocoles cryptographiques sont mis en relation avec des problèmes cryptographiques élémentaires. Si la preuve est administrée correctement, à savoir si les relations sont établies correctement, et si les hypothèses de sécurité s'appliquent, à savoir si les problèmes cryptographiques élémentaires sont « difficiles à résoudre » et donc, de facto, insolubles, un protocole peut être considéré comme sûr au sens de l'OVotE. Le ch. 2.14.3 de l'annexe de l'OVotE dispose que les preuves de sécurité cryptographiques peuvent être administrées dans le cadre d'hypothèses de sécurité généralement admises. Le protocole cryptographique de la Poste utilise une construction qui, dans la preuve de sécurité cryptographique, est mise en relation avec ce que l'on appelle le problème du SGSP. Il s'agit en l'occurrence d'un problème cryptographique élémentaire qui s'apparente au problème de Diffie-Hellman[6] en tant qu'hypothèse de sécurité généralement admise. Bien qu'il s'apparente au problème de Diffie-Hellman, le problème du SGSP est considéré comme peu étudié. La Poste adapte son protocole cryptographique de manière à ce que sa conformité ne dépende pas de l'impossibilité - de facto - de résoudre le problème du SGSP. Voir l'annexe pour de plus amples informations sur la présente mesure.	2025 / 2026 (en même temps que la mesure A.5)	Cantons et fournisseur du système	Nouveau
A.14	Renonciation au champ d'application de la qualité d'électeur comme critère obligatoire pour la constitution de bureaux de dépouillement	La conception technique du système de la Poste fait que les suffrages des électeurs ayant des qualités d'électeur différentes ne peuvent pas être mélangés et décomptés ensemble. Ainsi, pour les objets fédéraux, l'établissement des résultats concernant les suffrages des électeurs suisses de l'étranger doit obligatoirement se faire dans un bureau de dépouillement distinct, pour autant qu'ils n'aient pas la qualité d'électeur pour les objets cantonaux ou communaux du même scrutin. Plus les suffrages sont mélangés et décomptés ensemble, plus la protection du secret du vote est grande. Les exigences du droit fédéral ne prescrivent pas aux cantons de taille minimale pour les bureaux de dépouillement ; il en va de même pour le vote électronique. Par conséquent, la solution choisie par la Poste est	2025 / 2026 (en même temps que la mesure A.5)	Cantons et fournisseur du système	Nouveau

[5] Subgroup Generated by Small Primes.

[6] Problème concernant l'hypothèse décisionnelle de Diffie-Hellman.

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
		conforme aux exigences du droit fédéral. Toutefois, eu égard aux cantons où les suffrages des électeurs suisses de l'étranger sont traités de manière décentralisée, une plus grande flexibilité dans la constitution des bureaux de dépouillement est souhaitable. En particulier, des raisons relevant de la conception technique ne doivent pas constituer des obstacles. Pour les projets au niveau fédéral, les cantons auront à l'avenir la possibilité de mélanger et de décompter les suffrages des électeurs suisses de l'étranger avec ceux des autres électeurs de la même commune. La Poste adapte son système en conséquence.			
A.15	L'implémentation des primitives cryptographiques est régie de façon accrue par les principes de conception de la programmation orientée objet	L'application systématique de principes de conception lors de l'implémentation facilite la maintenabilité et permet de lutter contre les erreurs. Les primitives cryptographiques du système de la Poste sont un ensemble d'algorithmes qui effectuent des opérations cryptographiques de base. L'implémentation est régie par les principes de la programmation orientée objet. Elle est publiée sous une licence open source. Les contrôles effectués sur le système de la Poste aboutissent à la conclusion qu'il existe un potentiel dans certains domaines pour tirer davantage profit des principes de conception de la programmation orientée objet. Il existe notamment un potentiel d'amélioration dans la dénomination des classes et des interfaces, dans l'application systématique de critères sémantiques lors de la création de hiérarchies (héritage de classes, implémentation d'interfaces), dans la définition de méthodes appropriées à un niveau d'abstraction élevé et dans l'utilisation efficace de ces dernières. Des adaptations seront effectuées dans les domaines suivants (voir également le ch. 3.2.1 du rapport d'audit de la Haute école spécialisée bernoise [BFH] du 23.02.2023[7]) : - implémentation de groupes algébriques - implémentation de tuples, de vecteurs et de matrices - interface « Hashable » comme base pour le calcul des valeurs de hachage cryptographiques Il est possible de ne pas tenir compte des recommandations dans la mesure où les objectifs qui sous-tendent les observations figurant dans le rapport d'audit sont atteints d'une autre manière.	2025	Cantons et fournisseur du système	Nouveau

[7] Voir sous www.chf.admin.ch > Droits politiques > Vote électronique > Contrôles des systèmes.

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
A.16	La Poste examine les possibilités de réduire la complexité du système et met en œuvre les simplifications appropriées	En principe, les constructions qui se caractérisent par leur simplicité favorisent la détection et la correction précoces des erreurs. Par ailleurs, les systèmes de vote électronique qui sont sûrs ont par nature une étendue substantielle. Les systèmes devraient être aussi étendus que nécessaire et aussi simples que possible. Le système de la Poste n'est pas conçu de façon inutilement compliquée. Néanmoins, la Poste examinera les possibilités de simplifier davantage le système, pour autant qu'on puisse les mettre en œuvre sans compromettre les caractéristiques de sécurité implémentées et que la mise en œuvre se révèle judicieuse (voir également le ch. 1.4, intitulé « Potential for Simplifications », qui figure dans le rapport d'audit de la BFH du 23.02.2023[8]). Elle met notamment en œuvre des simplifications dans les domaines suivants : - Le processus d'authentification des électeurs se fait par un échange de messages qui comprend plusieurs tours. On recourt à des certificats qui ne satisfont certes pas aux exigences du droit fédéral en matière de certificats, mais dont l'utilisation ne joue aucun rôle pour la conformité du système. On renoncera aux messages et aux certificats pour lesquels aucune valeur ajoutée substantielle n'est documentée. Les simplifications correspondantes sont effectuées dans le cadre de l'élaboration de la spécification de l'authentification (voir également la mesure A.9). - Outre le suffrage exprimé, des éléments nécessaires à la génération des codes de vérification par le système en ligne sont envoyés en tant que partie intégrante de l'ensemble des données de vote. Ces éléments sont envoyés sous forme chiffrée, bien que cela ne soit pas nécessaire (voir également le ch. 5.1.4 du Swiss Post Voting System - System Specification Version 1.2.0[9]). On renoncera à tout chiffrement inutile.	Simplification de l'authentification : 2e trimestre 2023 (utilisation à partir l'élection du CN en 2023) Renonciation aux chiffrements inutiles dans l'ensemble des données de vote et simplifications supplémentaires en cas de besoin : 2025 / 2026 (en même temps que la mesure A.5)	Cantons et fournisseur du système	Nouveau
A.17	La Confédération, les cantons et le fournisseur du système qu'est la Poste harmonisent leur terminologie	La Confédération, les cantons et la Poste utilisent parfois des termes différents pour désigner les mêmes réalités (concepts, objets, etc.), alors que les documents des parties prenantes présentent des liens matériels forts entre eux. L'utilisation de termes différents peut, d'une manière générale, rendre plus difficile la compréhension des documents. La Confédération, les cantons et la Poste établissent un tableau expliquant les termes utilisés par toutes les parties prenantes. Ils étudient la	Tableau et plan : 2024	ChF avec la participation des cantons et du fournisseur du système	Nouveau

[8] Voir sous www.chf.admin.ch > Droits politiques > Vote électronique > Contrôles des systèmes.

[9] Voir sous https://gitlab.com/swisspost-evoting > E-Voting > E-Voting documentation > System.

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
		possibilité de mettre le tableau à la disposition du public pour l'aider à comprendre les documents publiés. Sur la base de ce tableau, la Confédération, les cantons et la Poste décident des uniformisations possibles et établissent un plan de mise en œuvre. L'objectif est d'utiliser une terminologie aussi unifiée que possible dans les documents établis ou adaptés en vue de l'utilisation de la version 2.0 du système de la Poste.			
A.18	Les cantons documentent les liens entre leurs instructions d'exploitation, le protocole cryptographique et les exigences figurant dans l'OVotE	Le protocole cryptographique définit pour tous les participants au système, sur la base du modèle de confiance figurant au ch. 2 de l'annexe de l'OVotE, les opérations qui doivent être effectuées. Pour l'exécution de certaines opérations, des mesures d'exploitation sont nécessaires, lesquelles seront prises par des personnes, par exemple la définition de mots de passe (voir ch. 4.2.2 du Swiss Post Voting System - System Specification Version 1.2.0[10]). Par ailleurs, le ch. 3 de l'annexe de l'OVotE contient des exigences supplémentaires applicables à l'exploitation des composants dont le bon fonctionnement est capital pour la réalisation des objectifs de sécurité (ce qu'on appelle les « composants fiables »). L'OVotE dispose par exemple qu'il faut veiller à utiliser une entropie suffisante pour le choix de valeurs aléatoires (ch. 3.2 annexe OVotE). Par cette mesure, les cantons mettent l'accent sur la documentation des liens entre leurs instructions d'exploitation, le protocole cryptographique et les exigences figurant dans l'OVotE. Cette façon de procéder contribue à la mise en œuvre correcte et pérenne des mesures opérationnelles importantes, notamment en cas d'adaptation au protocole cryptographique ou à l'OVotE.	2025	Les cantons, moyennant le soutien du fournisseur du système et de la ChF	Nouveau
A.19	La Confédération et les cantons examinent l'usage que les votants font des éléments de vérification et définissent, si nécessaire, des mesures pour encourager leur utilisation	L'OVotE exige que les électeurs disposent de plusieurs possibilités de vérification pour pouvoir identifier les attaques et y réagir : - vérifier si le suffrage a été enregistré correctement (ch. 2.5 annexe OVotE) ; - vérifier si un suffrage a été exprimé de manière abusive au nom de l'électeur (ch. 2.5 annexe OVotE) ; - vérifier si le bon logiciel est exécuté sur la plate-forme utilisateur avec les paramètres de chiffrement corrects (ch. 2.7.3 annexe OVotE) ;	Analyse et, si nécessaire, définition de mesures : 2025	ChF avec la participation des cantons et du fournisseur du système	Nouveau

[10] Voir sous https://gitlab.com/swisspost-evoting > E-Voting > E-Voting documentation > System.

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
		- vérifier l'authenticité du site Internet utilisé pour voter (ch. 8.10 annexe OVotE). Le ch. 8 de l'annexe de l'OVotE contient en outre une série d'exigences minimales en matière d'information et d'assistance à l'intention des électeurs. Les possibilités de vérification ne déploient leurs effets que si les électeurs en font usage. Les services qui participent à l'exploitation utilisent les messages concernant les résultats négatifs des vérifications effectuées par les électeurs comme indices de l'existence d'attaques systématiques potentielles. Il est aussi dans leur intérêt que les électeurs fassent un usage suffisant des possibilités de vérification. La phase d'essai doit constituer le cadre permettant d'analyser l'usage que les électeurs font des possibilités de vérification et, le cas échéant, d'apporter des améliorations à leur conception ainsi qu'à la communication. La ChF et les cantons analysent l'usage que les votants font des éléments de vérification et définissent, si nécessaire, des mesures pour encourager leur utilisation.			
A.20	Lors du contrôle public, des scrutins peuvent être organisés à partir des fichiers eCH	À partir du code source publié, des personnes peuvent installer le système de la Poste dans leur propre infrastructure et simuler des scrutins à l'aide de fichiers tests prédéfinis. Dans le cadre du programme de *bug bounty* de la Poste, le signalement de failles pertinentes est rémunéré. Afin de garantir aux personnes intéressées une plus grande flexibilité dans la simulation de scrutins, la Poste étudie des mesures telles que l'organisation de scrutins à partir des fichiers eCH contenant les paramètres techniques (objets de la votation, listes et candidats, électeurs).	Premières améliorations : 2e trimestre 2023 (utilisation à partir de l'élection du CN en 2023) Améliorations supplémentaires : 2024	Cantons et fournisseur du système	Nouveau
A.21	Implémentation du « dispute resolver » spécifié	Pour traiter les incohérences potentielles dans les composants de contrôle concernant la question de savoir quels suffrages doivent être décomptés, la Poste a spécifié ce que l'on appelle le « dispute resolver » (voir également les explications relatives à la mesure A.24 dans l'annexe). Il s'agit maintenant d'implémenter ce dernier afin que les cantons ou la Poste puissent l'utiliser directement en cas de besoin. La probabilité qu'il existe des incohérences peut être considérée comme faible. En amont de l'implémentation du « dispute resolver », l'existence d'incohérences avant la mise en œuvre de la présente mesure aurait pour conséquence qu'il faudrait implémenter la fonctionnalité nécessaire à court terme en cas de besoin en tenant compte de la transparence et de la traçabilité nécessaires. Cela pourrait avoir pour conséquence que la résolution de l'incohérence prendrait plusieurs	2024	Cantons et fournisseur du système	Nouveau

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
		jours. Le risque inhérent à l'absence provisoire d'implémentation du « dispute resolver » peut être considéré comme suffisamment faible.			
A.22	Adaptation des tâches des vérificateurs afin qu'ils n'aient pas de tâches opérationnelles à assumer	Dans le cadre de la phase de configuration d'un scrutin, le canton définit les paramètres cryptographiques pour le scrutin. Il s'agit d'une tâche opérationnelle qui ne relève donc pas vraiment de la compétence des vérificateurs. Les opérations nécessaires à cet effet prennent beaucoup de temps. Dans le but d'optimiser les processus, les cantons et la Poste ont placé l'une des étapes particulièrement chronophages sous la responsabilité des vérificateurs au sens de l'art. 2, al. 1, let. h, OVotE. Pour ces travaux, les vérificateurs utilisent l'ordinateur portable qui leur a été attribué. Ainsi, cette étape peut être effectuée parallèlement à d'autres travaux. Étant donné que l'ordinateur portable utilisé par les vérificateurs est conservé par le service cantonal responsable et exploité selon les mêmes modalités que l'ordinateur portable qui serait en fait prévu pour cette étape, la solution doit être considérée comme équivalente du point de vue de la sécurité. La présente mesure vise à faire en sorte que les vérificateurs n'assument pas de tâches opérationnelles. Lors de l'élaboration de la mesure A.5, il convient notamment de veiller à ce que l'exécution de tâches opérationnelles ne dépende pas, ou pas uniquement, du bon fonctionnement de l'ordinateur portable des vérificateurs. Voir l'annexe pour de plus amples informations sur la présente mesure.	2025 / 2026 (en même temps que la mesure A.5)	Cantons et fournisseur du système	Nouveau
A.23	Poursuite du développement du processus de développement, en particulier ce qui relève du cycle de vie du développement sécurisé (secure development lifecycle)	Le rapport d'audit de la société SCRT du 02.11.2022 relatif au processus de développement de la Poste[11] contient des propositions d'améliorations dans le domaine des mesures de sécurité lors du développement logiciel. La Poste a déjà commencé à mettre en œuvre ces propositions dans le cadre du processus d'amélioration continue. Cette mesure établit que les recommandations des rapports d'audit seront prises en compte et que l'état des mesures de sécurité à ce moment-là sera soumis à la ChF pour les contrôles périodiques. Les résultats seront disponibles en 2024 pour un premier contrôle.	En continu ; mise en œuvre et fourniture pour un premier contrôle : 2024	Cantons et fournisseur du système	Nouveau
A.24	Poursuite de l'amélioration du caractère concluant des preuves de conformité cryptographiques et augmentation de la pertinence de leur contenu	Le ch. 2.14.1 de l'annexe de l'OVotE dispose que des preuves de sécurité cryptographiques doivent attester que le protocole cryptographique respecte les exigences en matière de vérifiabilité, de secret du vote et d'authentification. Dans l'administration de leurs preuves, les protocoles cryptographiques sont mis en relation avec des problèmes	2024	Cantons et fournisseur du système	Nouveau

[11] Voir sous www.chf.admin.ch > Droits politiques > Vote électronique > Contrôles des systèmes.

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
		cryptographiques élémentaires. Si la preuve est administrée correctement, à savoir si les relations sont établies correctement, et si les hypothèses de sécurité s'appliquent, à savoir si les problèmes cryptographiques élémentaires sont « difficiles à résoudre » et donc, de facto, insolubles, un protocole peut être considéré comme sûr au sens de l'OVotE. Le rapport d'audit de Haines, Pereira et Teague du 13.02.2023[12] montre qu'il faut encore améliorer le caractère concluant des preuves et, par conséquent, l'argumentation expliquant en quoi le protocole cryptographique a été correctement associé aux problèmes élémentaires. Pour améliorer le caractère concluant des preuves, il faut, dans quelques cas, approfondir les arguments avancés. Dans certains cas, des arguments erronés ou trompeurs qui ont déjà été suffisamment approfondis doivent être corrigés. La pertinence du contenu des preuves ne doit pas être considérée comme fondamentalement trop faible. Toutefois, elle serait augmentée si d'autres éléments du système, qui n'apparaissent pas actuellement dans les preuves de sécurité, étaient pris en compte. Désormais, les preuves tiendront compte de ces éléments du système dans la mesure où cela est judicieux. Voir l'annexe pour de plus amples informations sur la présente mesure.			
A.25	Poursuite de l'amélioration de la qualité de la spécification et du logiciel	Le respect des critères de qualité dans la spécification et dans le logiciel contribue de manière décisive à prévenir les erreurs ou les vulnérabilités, ou du moins à les détecter et à les corriger à temps. L'OVotE pose différentes exigences de qualité, par exemple en ce qui concerne la traçabilité, la complétude, la cohérence, l'uniformité et l'intelligibilité (voir le ch. 25 de l'annexe de l'OVotE). La Poste a réussi à améliorer substantiellement la qualité de la spécification et du code source de son système. Néanmoins, des améliorations sont nécessaires. Des exemples d'améliorations figurent dans les rapports d'audit[13]. Certains sont mentionnés dans l'annexe. Dans le cadre du processus d'amélioration continue, des améliorations sont apportées en permanence. La présente mesure vise en outre à contribuer à ce que les améliorations qualitatives nécessaires qui ont été identifiées (état en février 2023) soient prises en compte et dans toute la mesure du possible mises en œuvre d'ici 2025. Dans le cadre	Améliorations : en continu Description des améliorations prévues : en continu, mais au plus tard au 1er trimestre 2024 Mise en œuvre des améliorations nécessaires qui ont été identifiés : 2025	Cantons et fournisseur du système	Nouveau

[12] Voir sous www.chf.admin.ch > Droits politiques > Vote électronique > Contrôles des systèmes.

[13] Voir sous www.chf.admin.ch > Droits politiques > Vote électronique > Contrôles des systèmes.

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
		de ces travaux, la Poste doit fournir à chaque fois à la ChF et aux cantons une description matérielle des améliorations prévues afin que celles-ci puissent être discutées avant leur mise en œuvre et, si nécessaire, adaptées, mais aussi afin que les éventuelles ambiguïtés et divergences puissent être levées, le cas échéant moyennant le recours à des experts externes. La description visée viendra par ailleurs alimenter le contrôle indépendant que la ChF doit effectuer en vertu de l'art. 10, al. 1, OVotE. Les risques liés à la nécessité d'améliorer la qualité peuvent être considérés comme suffisamment faibles. Voir l'annexe pour de plus amples informations sur la présente mesure.			
B.	**Surveillance et contrôle efficaces**				
B.6	Renouvellement de la gestion de crises avec conduite d'exercices de crise	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	ChF (lead), cantons et fournisseur du système	En cours
B.8	Poursuite du développement du contrôle de la plausibilité des résultats du vote électronique	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais : premier échange Examen d'une méthode standardisée : *jusqu'en 2023*	Cantons	En cours (un premier échange a eu lieu en 2022)
B.10	Examen à long terme des processus, rôles et des tâches	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Long terme	GT Avenir VE	En cours
B.11	Amélioration continue de la documentation sur les risques dont disposent les cantons	Les appréciations des risques que les cantons ont établies en 2022 reflètent la situation après la mise en œuvre des exigences figurant dans l'OVotE. Elles ont été élaborées conformément au guide de la CHF en la matière. La documentation sur les risques sera améliorée en continu, et l'accent sera mis sur la traçabilité, en documentant davantage les réflexions qui aboutissent à une appréciation. Se fondant sur la collaboration avec les cantons et sur la documentation existante, la ChF conclut que les cantons ont apprécié leurs risques de manière systématique et suffisante. La présente mesure vise uniquement à améliorer la documentation afin de rendre plus compréhensible la gestion des risques par les cantons.	En continu ; mise en œuvre des premières améliorations : 2024	Cantons	Nouveau

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
B.12	Amélioration de l'accessibilité et de la traçabilité de la documentation sur les risques dont dispose la Poste	Accessibilité : Dans le cadre des demandes d'agrément adressées à la ChF, les cantons doivent présenter leurs appréciations des risques et, le cas échéant, celles de leurs prestataires (comme l'exploitant du système) (art. 15, al. 1, let. a, OVotE). Ils doivent démontrer et justifier que les risques pour la sécurité sont suffisamment faibles (art. 4, al. 1 et 2, OVotE). La Poste procède à l'appréciation des risques conformément à ses directives internes, qui comprennent plusieurs niveaux : groupe, informatique et vote électronique. La documentation ne peut être consultée que dans les locaux de la Poste en raison de la classification de son contenu. Cette consultation, qui est coûteuse pour l'autorité chargée de l'octroi des autorisations, ne permet aucune flexibilité. La Poste et les cantons étudient comment offrir à la ChF une forme de consultation qui réponde aux besoins de toutes les parties prenantes et aux contraintes auxquelles elles sont soumises. L'accès doit garantir la traçabilité des différentes évaluations des risques. Traçabilité : Après avoir consulté la documentation de la Poste sur les menaces et les risques, la ChF arrive à la conclusion que les processus implémentés sont appropriés pour que les propriétaires des risques assument la responsabilité de l'identification, de l'évaluation et de la documentation des risques. Ces processus garantissent certes que les risques sont sous contrôle, mais la documentation soumise à la ChF peut être améliorée. Elle sera adaptée et complétée pour que la ChF dispose d'une vue d'ensemble consolidée de tous les risques et menaces (inhérents au développement ou à l'exploitation, de nature technique ou organisationnelle), avec un niveau de détail suffisant.	Détermination de la forme et du calendrier de l'amélioration de l'accessibilité et de la traçabilité : 3e trimestre 2023	Cantons et fournisseur du système	Nouveau
B.13	Amélioration des possibilités d'effectuer des enquêtes indépendantes portant sur des incidents	Les informations dont disposent les cantons pour enquêter sur des incidents dépendent du fournisseur du système qu'est la Poste (rapports comprenant des statistiques sélectionnées ; rapports d'enquête sur commande). Cette dépendance pourrait poser des problèmes lorsqu'il s'agit d'enquêter sur un comportement fautif relevant de la responsabilité de la Poste. Les cantons examinent dans quelle mesure un accès plus direct aux informations pertinentes pour de telles enquêtes est nécessaire et possible. Ils développement, au cours de la phase d'essai et en fonction des besoins identifiés lors des scrutins, des compétences destinées à la conduite des enquêtes sur des incidents. Compte tenu des conditions régissant la phase d'essai (notamment de la limitation du nombre d'électeurs autorisés), cette dépendance est acceptable jusqu'à la mise en œuvre des mesures d'amélioration. La	Première évaluation de la situation en 2024, puis définition des mesures	Cantons et fournisseur du système	Nouveau

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
		phase d'essai servira également à développer des compétences de ce type.			
B.14	Révision des bases légales afin de lever les ambiguïtés	Les bases légales fédérales, qui ont été révisées en 2022, s'appliqueront pour la première fois en 2023 à l'occasion de la reprise des essais. C'est la première fois que l'application des bases légales a soulevé une série de questions. On a constaté qu'il serait possible d'améliorer l'intelligibilité sur certains points en adaptant le libellé de l'OVotE ou en complétant, voire en précisant, les explications. Ainsi, une incohérence dans les bases légales a par exemple abouti à la nécessité d'invoquer, dans un rapport d'audit, le non-respect partiel d'une exigence, bien que la solution choisie par les cantons soit préférable du point de vue de la sécurité (voir le ch. 8, point 15.4, du rapport d'audit de la société SCRT du 17.02.2023 relatif à l'infrastructure et à l'exploitation dans les cantons[14]). La phase d'essai offrira un cadre permettant, notamment au regard des bases légales, de tirer des enseignements et de procéder à des adaptations propices à l'intelligibilité. Un réexamen de ce type sera entrepris dès qu'une nouvelle révision des bases légales sera agendée dans le cadre des prochaines étapes de la restructuration de la phase d'essai.	Lors de la prochaine révision des bases légales	ChF	Nouveau

C.	Renforcement de la transparence et de la confiance				
C.6	Une participation accrue du public	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Concept : *2023*	ChF avec la participation des cantons et fournisseur du système	En cours
C.7	Fourniture de documents supplémentaires pour aider à se forger une opinion sur la fiabilité et la sécurité	Les électeurs sans connaissances techniques mais aussi les spécialistes se posent des questions élémentaires sur la fiabilité et la sécurité du vote électronique. La transparence est une condition essentielle pour que les personnes intéressées puissent se forger une opinion et pour qu'un débat public fructueux et factuel puisse avoir lieu. La Confédération, les cantons et la Poste ont publié des documents relevant de leurs domaines de compétence respectifs et ont également préparé des documents explicatifs sur le vote électronique à l'intention des électeurs.	Ateliers ChF : 2023 Fourniture de documents : en continu et en fonction des besoins	ChF et cantons	Nouveau

[14] Voir sous www.chf.admin.ch > Droits politiques > Vote électronique > Contrôles des systèmes.

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
		Sur la base des prestations déjà fournies, la phase d'essai à venir permettra de déterminer quelles sont les questions capitales pour les électeurs et quels sont les besoins et les attentes en matière de contenu de la communication émanant des autorités et de leurs prestataires. Recensement des besoins : - En accord avec les cantons, la ChF organise des ateliers réunissant des personnes indépendantes issues du public. - La ChF et les cantons évaluent, en collaboration avec leurs prestataires, les réactions qui leur parviendront durant la phase d'essai. En cas de besoin, la ChF et les cantons mettent à la disposition du public des documents supplémentaires relevant de leurs domaines de compétence respectifs.			
D.	**Renforcement des liens avec les milieux scientifiques**				
D.1	Elaboration d'un concept pour le soutien scientifique des essais et le dialogue avec des experts externes	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Concept : *2023*	ChF avec la participation des cantons	En cours
D.2	Participation d'experts indépendants	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Dans le cadre des mesures individuelles	ChF avec la participation des cantons	En continu
D.3	Elaboration d'un concept pour la mise en place d'un comité scientifique	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Concept : *2023*	ChF avec la participation des cantons	En cours

2.2 Mesures terminées

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
A.	**Poursuite du développement des systèmes**				
A.1	Précision des critères qualité pour le code source et la documentation y relative	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	Exigences : ChF Mise en œuvre : Cantons, fournisseur du système	Terminé (cf. ch. 24 et 25 de l'annexe OVotE ; la mise en œuvre a été effectuée par les cantons et le fournisseur du système)
A.2	Renforcement de l'assurance qualité dans le processus de développement du système	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	Exigences : ChF Mise en œuvre : Cantons, fournisseur du système	Terminé (cf. ch. 17 et 24 de l'annexe OVotE ; la mise en œuvre a été effectuée par les cantons et le fournisseur du système)
A.3	Mise en œuvre d'une méthode éprouvée et vérifiable de construction et de déploiement	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	Exigences : ChF Mise en œuvre : Cantons, fournisseur du système	Terminé (cf. ch. 24.3 de l'annexe OVotE ; la mise en œuvre a été effectuée par les cantons et le fournisseur du système)
A.7	Amélioration des capacités de détection (monitoring) et d'investigation (investigation numérique) des incidents	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Définition des exigences et du processus d'amélioration : Reprise des essais	Exigences : ChF Processus d'amélioration : Fournisseur, cantons	Terminé (cf. ch. 14 de l'annexe de l'OVotE ; la mise en œuvre du processus d'amélioration est effectuée en continu par les cantons et le fournisseur du système)
A.8	Création d'un plan d'action commun de la Confédération et des cantons	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	ChF / cantons	Terminé (cf. le présent catalogue de mesures, qui est régulièrement vérifié, adapté et publié)
B.	**Surveillance et contrôle efficaces**				
B.1	Modification des compétences dans le cadre de l'évaluation de la conformité du système et des processus qui l'entourent	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	ChF	Terminé (cf. art. 27*l* ODP ainsi que art. 10 OVotE en rel. avec le ch. 26 de l'annexe OVotE)
B.2	Elaboration d'un concept d'audit pour l'évaluation de la conformité du système et des processus qui l'entourent	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	ChF en collaboration avec les cantons et le fournisseur du système	Terminé (cf. concept d'audit pour les contrôles indépendants sous www.chf.admin.ch > Droits politiques > Vote électronique > Contrôles des systèmes)

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
B.3	Elaboration et mise en œuvre d'un processus de traitement des non-conformités	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	ChF en collaboration avec les cantons et le fournisseur du système	Terminé (le processus de traitement des non-conformités a été défini par la ChF en collaboration avec les cantons et le fournisseur du système)
B.4	Renouvellement et amélioration du guide pour l'appréciation des risques	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	ChF en collaboration avec les cantons et le fournisseur du système	Terminé (cf. guide de la ChF sous www.chf.admin.ch > Droits politiques > Vote électronique > Exigences du droit fédéral)
B.5	Elaboration et mise en œuvre d'un nouveau processus d'appréciation des risques pour des systèmes complètement vérifiables	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	ChF, cantons, fournisseur du système	Terminé (cf. art. 4 OVotE ; les appréciations des risques de tous les acteurs sont disponibles ; l'appréciation des risques de la ChF est publiée)
B.7	Intégration du vote électronique dans les infrastructures critiques de la Confédération	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	ChF (lead), cantons et fournisseur du système	Terminé
B.9	Adaptations de la procédure d'autorisation	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	ChF avec la participation des cantons	Terminé (cf. guide de la ChF sous www.chf.admin.ch > Droits politiques > Vote électronique > Exigences du droit fédéral)
C.	**Renforcement de la transparence et de la confiance**				
C.1	Limitation de l'électorat admissible pour les systèmes complètement vérifiables	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	ChF	Terminé (cf. art. 27*f* ODP)
C.2	Précision des exigences concernant la publication du code source	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	Exigences : ChF Publication : Cantons, fournisseur du système	Terminé (cf. art. 27*f*^{bis} ODP et art. 11 et 12 OVotE ; la publication par les cantons et le fournisseur du système a été effectuée)
C.3	Gestion d'un programme de *bug bounty*	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	Exigences : ChF Mise en œuvre : Cantons, fournisseur du système	Terminé (cf. art. 27*f*^{ter} ODP et art. 13 OVotE ; la mise en œuvre par les cantons et les fournisseurs a été effectuée ; cf. Programme de la communauté | Evoting-Community (post.ch))

N°	Mesure	Description	Calendrier mise en œuvre	Responsabilité	État de la mise en œuvre
C.4	Publication des rapports d'audit pertinents pour l'autorisation	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	ChF, cantons, fournisseur du système	Terminé (cf. art. 10, al. 4, OVotE ; la publication par la ChF, les cantons et le fournisseur du système a été effectuée)
C.5	Lors des scrutins fédéraux, publication du résultat des votes exprimés à travers le vote électronique	Cf. description dans le catalogue des mesures du rapport final du CoPil VE du 30.11.2020.	Reprise des essais	Exigences : ChF Publication : Cantons	Terminé (cf. art. 27*m*, al. 3, ODP ; la publication sera effectuée par les cantons après les scrutins)

Annexe : informations complémentaires sur certaines mesures en suspens

N°	Mesure
A.9	**Finalisation de la spécification du système dans le domaine de l'authentification des électeurs**

L'authentification des électeurs se déroule en deux étapes. Pour chaque étape, les électeurs saisissent un code confidentiel qui figure sur leur carte de légitimation :

1. L'authentification initiale a lieu après la saisie du premier code confidentiel. Si elle réussit, le système en ligne envoie un paramètre confidentiel pour le vote à l'appareil de l'électeur. Sans ce paramètre, la plate-forme utilisateur ne peut pas transmettre de suffrage qui soit accepté par le système en ligne (une authentification est effectuée sur la base de l'ensemble des données de vote).
2. En saisissant un deuxième code confidentiel, le votant confirme qu'il a contrôlé la transmission correcte du suffrage à l'aide des codes de vérification pour la vérifiabilité individuelle, transmission qui s'est soldée par un résultat positif. Le code saisi peut également être considéré comme une caractéristique d'authentification grâce à laquelle l'électeur est authentifié (voir les explications du 25 mai 2022 relatives au ch. 2.12.8 de l'annexe de l'OVotE[15]).

Dans le système de la Poste, dont la première utilisation est prévue pour le mois de juin 2023, l'authentification initiale de la première étape n'est pas spécifiée.

On peut déduire de la présente spécification du système que la sécurité de ce dernier est liée à la confidentialité du paramètre confidentiel dans le sens suivant :

En supposant que des attaquants aient accès au paramètre, ils ne pourraient pas voter malgré tout. Il leur faudrait pour cela entrer le deuxième code confidentiel. De même, la vérifiabilité visée aux ch. 2.5 et 2.6 de l'annexe de l'OVotE ne serait pas remise en question en cas d'accès au paramètre. Ces deux éléments peuvent être déduits de la preuve de conformité cryptographique visée au ch. 2.14.1 de l'annexe de l'OVotE. L'accès au paramètre pourrait présenter des avantages lors de tentatives visant à connaître le contenu des suffrages exprimés de manière chiffrée. Pour que l'exigence figurant au ch. 2.7 de l'annexe de l'OVotE soit satisfaite, aucun accès ne doit être possible. Certes, pour tirer profit de leur connaissance du paramètre confidentiel, les attaquants devraient accéder à des informations supplémentaires collectées dans le système en ligne lors du vote. Toutefois, en vertu du ch. 2.7 de l'annexe de l'OVotE, l'accès à l'ensemble des données gérées dans le système en ligne ne doit pas permettre de tirer des conclusions sur le contenu des suffrages exprimés.

À propos de la confidentialité du paramètre confidentiel : le paramètre confidentiel envoyé lors de la première étape n'est disponible pour le système en ligne que sous forme chiffrée. Il en va de même pour les autres valeurs du système en ligne qui permettraient de déchiffrer le paramètre confidentiel. Le déchiffrement n'est possible que si le premier code confidentiel est connu. Par conséquent, la plate-forme utilisateur envoie ce code sous une forme modifiée qui ne permet pas le déchiffrement. Ainsi, les attaquants qui entreraient en possession des valeurs chiffrées du système en ligne ne pourraient pas déchiffrer malgré tout le paramètre confidentiel. Ces observations ne sont pas étayées par une spécification, mais uniquement par des déclarations de la Poste et par des observations faites sur le code source. La finalisation et le contrôle de la spécification permettront de procéder à une analyse plus structurée du code source et contribueront ainsi à accroître la sécurité en matière de respect des exigences figurant au ch. 2.7 de l'annexe de l'OVotE.

N°	Mesure
A.11	**Publication du code source du logiciel de génération des fichiers PDF pour l'impression des cartes de légitimation**

Pour l'efficacité du protocole cryptographique, qui répond aux exigences en matière de vérifiabilité individuelle, de respect du secret du vote et d'authentification, il est essentiel que les codes pour les cartes de légitimation restent confidentiels et soient repris correctement dans les fichiers PDF.

[15] Voir sous www.chf.admin.ch > Droits politiques > Vote électronique > Exigences du droit fédéral.

La réalisation d'un contrôle de sécurité et les considérations suivantes aboutissent à la conclusion qu'une renonciation provisoire à la publication du logiciel VCPS présente des risques suffisamment faibles :

- Les cantons concernés s'engagent à vérifier par sondage durant le fonctionnement que les bons codes ont été repris dans le document PDF.
- Le logiciel VCPS fonctionne sur un ordinateur portable dont l'exploitation est régie par le ch. 3 de l'annexe de l'OVotE et jouit donc d'une protection particulière. Il fonctionne par ailleurs sans connexion réseau.
- Aucune donnée critique au sens de l'art. 2, al. 1, let. v, OVotE n'est conservée sur l'ordinateur portable, à l'exception des données brutes nécessaires à l'impression.

N°	Mesure
A.13	**Renonciation au problème du SGSP comme hypothèse de sécurité**

Il n'est pas possible de quantifier une fois pour toutes la difficulté de résoudre le problème du SGSP à l'aide du problème de Diffie-Hellman. On peut donc considérer que le problème du SGSP est, au plus, aussi difficile à résoudre que celui de Diffie-Hellman. Qui plus est, on ne connaît pas d'approche qui indique une solution plus efficace (bien que non viable) pour le problème du SGSP que pour le problème de Diffie-Hellman, et encore moins une solution viable.

La conformité du protocole cryptographique avec les exigences en matière de vérifiabilité au sens des ch. 2.5 et 2.6 ainsi qu'en matière d'authentification au sens du ch. 2.8 de l'annexe de l'OVotE ne repose pas sur le problème du SGSP. Les attaquants qui parviendraient à s'introduire dans le système en ligne, à accéder aux données nécessaires et à résoudre le problème du SGSP seraient en mesure de déterminer le contenu des suffrages exprimés de manière chiffrée. Le protocole cryptographique contreviendrait ainsi au ch. 2.7 de l'annexe de l'OVotE : en vertu du ch. 2.7 de l'annexe de l'OVotE, l'ensemble des données gérées dans le système en ligne ne doit pas permettre de déterminer le contenu des suffrages exprimés, même en cas d'accès réussi.

La réflexion suivante permet de conclure que le maintien provisoire du problème du SGSP comme hypothèse de sécurité présente des risques suffisamment faibles : si une solution viable au problème du SGSP existait du point de vue mathématique, il faudrait très probablement mobiliser énormément de moyens non seulement dans la recherche de la solution, mais aussi dans l'application de cette dernière. À cela s'ajouterait le travail nécessaire pour obtenir les données requises pour l'attaque, qui sont générées dans le système en ligne à partir de l'ensemble des données de vote. Par ailleurs, l'utilité qui pourrait résulter du travail fourni serait faible, vu le nombre limité d'électeurs jusqu'à la mise en œuvre de la mesure.

N°	Mesure
A.22	**Adaptation des tâches des vérificateurs afin qu'ils n'aient pas de tâches opérationnelles à assumer**

Les vérificateurs doivent identifier les cas où des suffrages ont été manipulés, effacés ou décomptés à tort (voir le ch. 2.6 de l'annexe de l'OVotE). Pour ce faire, ils analysent les preuves cryptographiques qu'ils reçoivent en même temps que le résultat du scrutin. Leur outil est le Verifier, un logiciel publié sous licence open source. Ils effectuent le contrôle sur un ordinateur portable dédié.

Dans le système de la Poste, les vérificateurs effectuent en outre, pendant la phase de configuration, un contrôle dont l'exécution correcte est déterminante pour le respect des exigences relatives à la vérifiabilité individuelle visée au ch. 2.5, à la protection du secret du vote visée au ch. 2.7 et à l'authentification visée au ch. 2.8 de l'annexe de l'OVotE. Ce contrôle est une tâche opérationnelle qui relève de la responsabilité directe du service cantonal chargé du vote électronique. Un dispositif technique sous la forme d'un ordinateur portable individuel (appelé composant de configuration) est mis à la disposition du service cantonal chargé du vote électronique.

Étant donné que l'ordinateur portable des vérificateurs ne traite pas de données dont la confidentialité constitue une condition du respect des exigences susmentionnées et que les mêmes modalités s'appliquent à l'exploitation du composant de configuration et du dispositif technique des vérificateurs, la solution choisie par les cantons et la Poste peut être considérée comme équivalente du point de vue de la

sécurité. Le rapport explicatif relatif à la révision totale de l'OVotE en 2022[16] indique par ailleurs que les vérificateurs peuvent être appelés à effectuer des tâches pour lesquelles le composant de configuration est normalement prévu (voir les explications relatives au ch. 2.1 de l'annexe de l'OVotE).

Les tâches opérationnelles doivent également être exécutées à long terme en tenant compte des mesures nécessaires. Parallèlement, les vérificateurs doivent pouvoir bénéficier d'une plus grande indépendance, si cela est souhaité et si le droit cantonal le permet. Les tâches opérationnelles doivent donc être exécutées directement par le service responsable des scrutins. En revanche, ce sont les vérificateurs qui doivent identifier les éventuels dysfonctionnements opérationnels dans le cadre de leur domaine de compétence.

N°	Mesure
A.24	**Poursuite de l'amélioration du caractère concluant des preuves de conformité cryptographiques et augmentation de la pertinence de leur contenu**

Les preuves de sécurité cryptographiques servent à convaincre les personnes qui les lisent - et en premier lieu les personnes responsables de l'administration des preuves - que le protocole cryptographique satisfait aux exigences de vérifiabilité, de secret du vote et d'authentification. Certes, on ne doit pas déduire a priori du caractère non concluant de la preuve que le protocole cryptographique présente une vulnérabilité, et encore moins une vulnérabilité qui peut être utilisée pour une attaque. En amont d'une analyse plus approfondie, un caractère non concluant doit toutefois être considéré comme un indice potentiel d'une possible vulnérabilité. Il est donc important d'examiner les caractères non concluants et de les éliminer, en améliorant soit uniquement la preuve, soit, si nécessaire, le protocole cryptographique. La Poste a amélioré substantiellement l'administration des preuves. L'objectif de la présente mesure est de poursuivre le travail jusqu'à ce que les preuves puissent être considérées comme concluantes de bout en bout.

Le rapport d'audit de Haines, Pereira et Teague du 13.02.2023[17] présente des exemples d'arguments erronés ou trompeurs figurant dans les preuves (voir les ch. 2.5.1 et 2.5.2). Il s'agit de caractères non concluants que l'on peut éliminer facilement rien qu'en adaptant l'argumentation dans la preuve. Le protocole cryptographique ne renferme pas de vulnérabilités cachées derrière les caractères non concluants, et il ne doit pas être adapté. Néanmoins, il est précieux et important de procéder à des adaptations de la preuve. Ainsi, les personnes qui lisent la preuve ne doivent pas investir le temps disponible dans des questions que d'autres ont déjà analysées. Elles peuvent au contraire examiner la preuve de manière ciblée à la recherche de nouveaux caractères non concluants et contribuer ainsi à ce que les éventuels besoins d'amélioration du protocole cryptographique soient identifiés et pris en compte à un stade précoce.

Au ch. 2.5, le même rapport d'audit indique qu'il faudrait développer davantage l'argumentation dans l'administration des preuves à différents endroits afin de pouvoir la comprendre et identifier les éventuelles erreurs ou lacunes qu'elle comporte. Sans les explications attendues, l'utilité des preuves peut être fortement limitée dans de tels cas de figure. Dans le souci de mettre en œuvre la présente mesure, l'argumentation sera développée davantage aux endroits concernés dans les preuves.

Par ailleurs, les preuves prendront en compte d'autres éléments du système. Dans les preuves de sécurité, il est courant de présenter les propriétés du système sous une forme simplifiée, ce qui entre inévitablement en conflit avec la pertinence d'une preuve. Toutefois, certaines fonctions qui revêtent une importance particulière au regard des propriétés de sécurité du protocole cryptographique qui ont été implémentées ne sont actuellement pas prises en compte. Pour que la preuve puisse démontrer de manière structurée que ces fonctions apportent l'avantage promis sans introduire de vulnérabilité dans le protocole, elles seront prises en compte dans la preuve. Cela vaut en particulier pour les éléments suivants du système :

- Avant le dépouillement, les suffrages sont mélangés et déchiffrés dans cinq composants différents dits de contrôle au sens de l'art. 2, al. 1, let. d, OVotE, en relation avec les ch. 2 et 3 de l'annexe de l'OVotE. Chaque composant de contrôle modifie l'ordre ainsi que le chiffrement des suffrages sans pour autant modifier ces derniers (c'est le chiffrement qui est modifié, et non pas le contenu du chiffrement). Après le mélange, chaque composant de contrôle effectue un déchiffrement partiel et transmet les suffrages mélangés et partiellement déchiffrés au composant de contrôle suivant. Les quatre premiers des cinq composants de contrôle se trouvent dans les locaux de la

[16] Voir sous www.chf.admin.ch > Droits politiques > Vote électronique > Exigences du droit fédéral.

[17] Voir sous www.chf.admin.ch > Droits politiques > Vote électronique > Contrôles des systèmes.

Poste. La clé privée pour le déchiffrement partiel est stockée dans les composants de contrôle. La confidentialité des clés privées est régie par les exigences figurant au ch. 3 de l'annexe de l'OVotE, et le principe du double contrôle doit être strictement respecté. Le cinquième composant de contrôle n'est autre qu'un ordinateur portable du canton, auquel s'applique également le ch. 3 de l'annexe de l'OVotE. Cependant, la clé privée pour le cinquième déchiffrement partiel - et donc pour le déchiffrement définitif des suffrages - n'est pas stockée dans cet ordinateur portable, car elle découle d'un long mot de passe réparti entre deux groupes de personnes auprès du canton. La répartition du mot de passe entre deux groupes de personnes permet d'éviter que le cinquième chiffrement partiel ne perde de facto son efficacité si une seule personne transmet le mot de passe nécessaire au déchiffrement. Les fonctions utilisées pour calculer la clé privée à partir des deux parties du mot de passe seront désormais prises en compte dans les preuves en raison de leur importance pour la sécurité. Il s'agit en particulier de démontrer que, dans les hypothèses de confiance servant à la protection du secret du vote au sens du ch. 2.7 de l'annexe de l'OVotE, l'une des deux parties du mot de passe ne permet pas à elle seule de procéder au cinquième déchiffrement partiel.

- Avant le mélange et le déchiffrement partiel, chaque composant de contrôle vérifie que tous les composants de contrôle précédents ont traité les suffrages correctement. Pour ce faire, ils vérifient tout d'abord les preuves mathématiques qui démontrent que les composants de contrôle précédents n'ont modifié aucun suffrage lors du mélange et du déchiffrement partiel. Ils vérifient ensuite que la liste des suffrages que le premier composant de contrôle a mélangés et déchiffrés partiellement est correcte. Les quatre composants de contrôle susmentionnés, qui se trouvent dans les locaux de la Poste, sont les mêmes machines qui génèrent les codes de vérification à partir des suffrages transmis en respectant la vérifiabilité individuelle au sens du ch. 2.5 de l'annexe de l'OVotE, et qui conservent les suffrages jusqu'au dépouillement. Leur vérification pour déterminer si le premier composant de contrôle a mélangé et déchiffré partiellement les suffrages corrects comprend une comparaison avec leur propre liste de suffrages à dépouiller. Si un composant de contrôle indique une incohérence entre sa propre liste et celle du premier composant de contrôle, une enquête doit être ouverte pour déterminer l'apparence correcte que devrait avoir la liste des suffrages à dépouiller. L'instrument nécessaire pour mener cette enquête n'est autre qu'un « dispute resolver » spécifié. La preuve de sécurité cryptographique tiendra désormais compte de l'utilisation éventuelle du « dispute resolver » et démontrera en particulier que la liste correcte des suffrages à dépouiller peut être trouvée dans le respect des hypothèses de confiance servant à la vérifiabilité individuelle au sens du ch. 2.5 de l'annexe de l'OVotE.

En plus de ces deux points, il existe d'autres éléments du système pour lesquels il convient de vérifier s'il pourrait être indiqué de les prendre en compte dans les preuves de sécurité cryptographiques ou, du moins, de justifier de manière informelle pourquoi ce n'est pas le cas (voir le ch. 2.1.3 du rapport d'audit de Haines, Pereira et Teague du 13.02.2023).

À l'heure actuelle, il n'existe pas d'éléments concrets laissant penser que les caractères non concluants ou les éléments du système non pris en compte dans les preuves cachent des vulnérabilités du protocole cryptographique. Les améliorations apportées aux preuves permettront d'en savoir plus sur les éventuelles vulnérabilités et sur les améliorations à apporter le cas échéant. Le protocole cryptographique a également fait l'objet d'un examen de conformité indépendamment de l'examen des preuves. Compte tenu du fait que l'électorat sera restreint jusqu'à la mise en œuvre de la présente mesure, le risque lié à la nécessité d'agir provisoirement sur les preuves cryptographiques peut être considéré comme suffisamment faible.

N°	Mesure
A.25	**Poursuite de l'amélioration de la qualité de la spécification et du logiciel**

Les points mentionnés ci-dessous mettent en évidence des besoins d'amélioration, auxquels il convient de remédier en continu, mais au plus tard lors de la mise en œuvre de la mesure A.5. La liste s'appuie en grande partie sur les résultats du contrôle indépendant commandé par la ChF.

En principe, tous les points sur lesquels portent les critiques formulées ici ou dans les rapports d'audit et qui concernent la qualité de la spécification et du logiciel doivent être pris en compte, à moins que la Poste ne démontre que les critiques ne sont pas justifiées. Dans les cas où la Poste propose des solutions de remplacement qui tiennent compte dans la même mesure de l'objectif qui sous-tend un point qui a fait l'objet d'une critique, des améliorations allant dans le sens des solutions de remplacement peuvent être mises en œuvre.

- Les documents de spécification doivent exprimer plus clairement la manière dont les variables créées par les participants au protocole et partiellement transmises entre eux doivent être utilisées au cours du protocole. Il s'agit notamment d'indiquer plus clairement avec quelles variables les algorithmes spécifiés en pseudocodes sont appelés. Il serait par ailleurs précieux de formuler de manière plus stricte dans la spécification les principes de vérification de la validité des variables transmises. Les principes devraient indiquer de manière complète et univoque quelles variables doivent être vérifiées, dans quels cas, par rapport à quelle base et pour quelle raison, mais aussi quelles variables peuvent être modifiées, dans quels cas et lesquelles ne peuvent jamais l'être. Les dérogations aux principes doivent être indiquées et justifiées clairement. Les principes doivent également régler l'utilisation des variables contextuelles, à savoir celles qui doivent être et rester immuables pendant un scrutin (voir également le ch. 3.1.2 du rapport d'audit de la BFH du 23.02.2023[18]). Les contrôles de validité et autres principes qui peuvent être déduits de la spécification doivent être mis en œuvre dans le code source d'une manière aussi uniforme que possible et être faciles à trouver.
- Le logiciel n'est pas suffisamment spécifié à certains endroits, de sorte que les documents de spécification ne précisent pas suffisamment comment l'implémentation dans le code source ou les étapes opérationnelles doivent être conçues. Par exemple, il est nécessaire de clarifier l'entropie minimale lors du choix des mots de passe pour le cinquième déchiffrement partiel (voir la mesure A.24). La procédure régissant la poursuite du scrutin, après qu'une incohérence a pu être résolue grâce au « dispute resolver » (voir la mesure A.24), n'est pas suffisamment claire. D'autres exemples figurent dans le rapport d'audit de la BFH du 23.02.2023 aux ch. 2.4.1 (« Election Use Cases »), 3.4.1, A.4.1 (3e section), A.4.2 et B.4, ainsi que dans le rapport d'audit de Haines, Pereira et Teague du 13.02.2023 au ch. 2.2.
- Des explications supplémentaires sur les décisions prises en toute connaissance de cause concernant la conception du système ainsi que sur les risques éventuels liés à ces décisions peuvent contribuer à un processus d'amélioration ciblé et doivent être fournies au moins lorsque l'on ne recourt pas à des normes courantes, à des pratiques évidentes ou à des recommandations explicites. Voir par exemple le rapport d'audit d'Essex du 21.11.2022 (ch. 5, « Clarify design choice of Bayer-Groth mixnet »), le rapport d'audit d'Essex du 13.02.2023 (ch. 2.2, 2.3 et 2.4), le rapport d'audit de Haines, Pereira et Teague du 13.02.2023 (ch. 3.1) et le rapport d'audit de la BFH du 23.02.2023 (ch. 2.2.7 et 3.1.1, certains points au ch. A.3.1, ch. A.3.2 dans les sections 1, 7 et 8, ch. B.3.2 et ch. B.3.6). Les explications doivent notamment être intégrées dans la description matérielle des améliorations prévues (voir la partie principale du présent document concernant la présente mesure). Sur cette base, un dialogue doit pouvoir être mené en vue de déterminer s'il ne serait pas judicieux d'aménager le système sur les différents points dans le sens d'une norme courante, d'une pratique évidente ou d'une recommandation explicite.
- Les précisions dans la notation qui pourraient prévenir des erreurs ou des malentendus devraient être mises en œuvre, de même que les petites erreurs devraient être corrigées ; voir par exemple le rapport d'audit d'Essex du 21.11.2022 (ch. 5, « Implied modular reduction in subscript » et « Improper quotation marks »), le rapport d'audit de la BFH du 23.02.2023 (ch. 3.1.5 et 3.2.2 [« Algorithm 3.1 », « Algorithm 3.8 », « Algorithm 3.9 » et « Algorithm 3.12 »], ch. 3.2.3 [« Algorithm 4.11 » et « Algorithm 4.13 »] ainsi que d'autres algorithmes aux ch. 3.2.5, 3.2.7, 3.2.8 et 3.3.1).

[18] Voir sous www.chf.admin.ch > Droits politiques > Vote électronique > Contrôles des systèmes.