Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF

Août 2019

Vote électronique – test public d'intrusion 2019

Rapport final du comité de pilotage

Système testé : système complètement vérifiable de la Poste Suisse (version de février 2019)

Table des matières

1 Objectif du document

Le présent rapport résume l'organisation, le déroulement et les conclusions du test public d'intrusion 2019 (*public intrusion test,* PIT) auquel a été soumis le système de vote électronique de la Poste Suisse.

2 Contexte

En se fondant sur l'art. 8*a* de la loi fédérale sur les droits politiques (LDP, RS 161.1), les cantons organisent depuis 2004 des essais de vote électronique dans le cadre du projet Vote électronique (VE) de la Confédération et des cantons. Au niveau du droit fédéral, les conditions de test sont réglées dans l'ordonnance sur les droits politiques (ODP, RS 161.11) et dans l'ordonnance de la Chancellerie fédérale sur le vote électronique (OVotE, RS 161.116).

Au total, quinze cantons ont d'ores et déjà permis à diverses reprises à une partie des électeurs de voter par Internet lors de scrutins fédéraux. Les systèmes utilisés depuis 2015 offrent la vérifiabilité individuelle. Toutefois pour étendre davantage le vote électronique, le système doit garantir la vérifiabilité complète. Afin d'autoriser l'utilisation d'un tel système, l'OVotE exige une certification préalable et la publication du code source.

La Confédération et les cantons ont par ailleurs décidé en avril 2017 que les systèmes de vote électronique proposant la vérifiabilité complète devaient être soumis à un test public d'intrusion réalisé au titre de projet pilote. Un tel test permet de vérifier la sécurité d'un système en l'exposant à des attaques. Pour délivrer une certification, l'OVotE exige déjà un test d'intrusion mené par un organe accrédité. Un test public d'intrusion offre quant à lui la possibilité de tester le système à des personnes intéressées du monde entier.

La réalisation d'un test public d'intrusion répond à plusieurs objectifs. L'avis des participants contribue directement à améliorer la sécurité. Un tel test permet également à des spécialistes indépendants de s'approprier des connaissances et des compétences dans le domaine du vote électronique. Cette méthode permet ainsi de prévenir sur le long terme la dépendance à l'égard de certaines personnes ou organisations, tout en contribuant au débat public. Le test est également un instrument de transparence visant à instaurer la confiance. Sa réussite repose sur la collaboration active d'un nombre aussi important que possible de personnes compétentes. Le débat public que suscite ce type de test dans les médias et dans le monde politique démontre la culture de l'erreur qui règne dans le domaine du vote électronique.

3 Système soumis au test

Ces dernières années, deux systèmes de vote électronique permettant la vérifiabilité individuelle ont été utilisés en Suisse : le système de La Poste suisse (utilisé dernièrement par les cantons de Fribourg, de Neuchâtel, de Thurgovie et de Bâle-Ville) et celui du canton de Genève (utilisé dernièrement par les cantons de Berne, de Lucerne, de St-Gall[1], d'Argovie, de Vaud et de Genève).

Le 28 novembre 2018, les autorités genevoises ont annoncé qu'elles cesseraient d'exploiter leur système au plus tard au mois de février 2020. Elles ont par conséquent abandonné le développement de la vérifiabilité complète, rendant ainsi caduc un test public d'intrusion.

Le seul système soumis au PIT a ainsi été le futur système permettant la vérifiabilité complète proposé par La Poste suisse (la Poste). Il ne s'agissait donc pas du système qu'elle utilise actuellement mais de celui que les autorités pourront utiliser pour les scrutins fédéraux dès lors qu'il respectera toutes les exigences du droit fédéral et qu'il aura obtenu l'autorisation d'exploitation définitive.

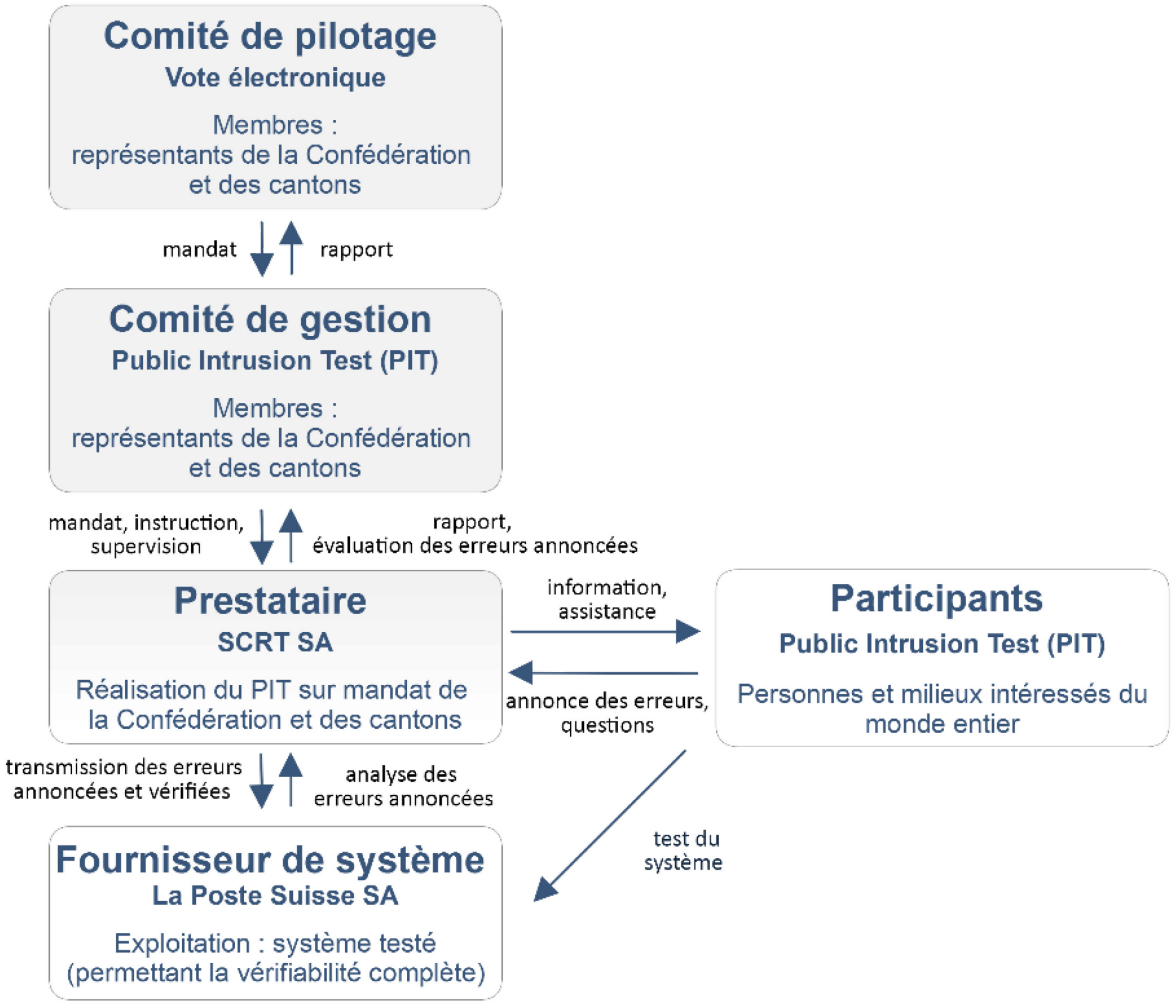
La structure du système utilisé pour le PIT était la réplique exacte de celle du système productif. Seule la configuration de sécurité permettant de bloquer des adresses IP suspectes au moyen de l'application fail2ban était désactivée afin de ne pas restreindre inutilement l'accès des participants.

4 Dispositif de test et organisation

La Confédération et les cantons ont décidé d'agir en commun dans le domaine des tests publics d'intrusion et ont fixé ensemble les exigences à l'attention du fournisseur de système[2]. Ils ont par ailleurs soutenu ledit test dans le cadre du plan stratégique E-Government Suisse de la Confédération, des cantons et des communes par une participation de 250 000 francs répartis entre la poste (150 000 fr.) et la société SCRT (100 000 fr.) en sa qualité de prestataire de la Confédération et des cantons.

[1] À l'avenir, le canton de St-Gall prévoit d'utiliser le système de La Poste suisse.
[2] https://www.bk.admin.ch/dam/bk/fr/dokumente/pore/Exigences%20de%20la%20Conf%C3%A9d%C3%A9ration%20et%20des%20cantons_tests%20d%E2%80%99intrusion%20publics.pdf.download.pdf/Exigences%20de%20la%20Conf%C3%A9d%C3%A9ration%20et%20des%20cantons_tests%20d%E2%80%99intrusion%20publics.pdf

Organisation PIT



La Poste a mis le système à disposition pour le PIT du 25 février au 24 mars 2019 et en a géré le fonctionnement. Elle disposait d'une enveloppe globale de 150 000 francs pour offrir une récompense pouvant aller de 100 francs à 50 000 francs aux participants qui lui soumettraient des avis pertinents. Les participants avaient la possibilité de consulter les critères d'indemnisation sur un site Internet dédié exclusivement au test, la plateforme du PIT[3].

Le comité de gestion (CG) de la Confédération et des cantons a supervisé et encadré le PIT sur mandat du comité de pilotage Vote électronique (CP VE). Il était l'interlocuteur de la Confédération et des cantons pour les questions au sujet du test. Pendant le test, le CG était chargé de ponctuellement donner des informations sur l'état actuel. Il coordonnait la communication entre les parties prenantes et élaborait les éléments de la communication officielle destinée au public.

Pour la réalisation du PIT, la Confédération et les cantons ont mandaté la société SCRT, spécialisée dans le domaine, qui opérait sous l'égide du CG. Elle était chargée de la communication avec les participants : elle s'occupait de leur recrutement, de leur enregistrement et de

[3] https://www.onlinevote-pit.ch/

leur accompagnement, collectait leurs rapports et les évaluait, le tout au moyen de la plateforme du PIT.

Le PIT s'adressait à des personnes du monde entier. En s'inscrivant sur la plateforme, ces personnes prenaient connaissance du code de conduite défini par la Poste auquel elles devaient adhérer (convention avec la Poste). Ce code régissait le champ d'application du test et la conduite à tenir en cas de découverte d'une faille ; il garantissait en outre l'impunité pour autant que les règles aient été respectées.

Le dispositif de test a essuyé certaines critiques de la part du public.

- Conformément aux exigences de la Confédération et des cantons, la Poste a limité le test aux attaques contre son infrastructure de vote électronique et fixé le code de conduite en conséquence, interdisant de fait toute attaque contre les infrastructures des cantons, les imprimeries ou les autres services de la Poste. Les attaques visant un déni de service, qui aurait empêché les électeurs d'accéder au système, étaient également exclues, de même que les attaques lancées contre les plateformes utilisateur des électeurs. Il était également interdit d'essayer de pousser les participants à s'écarter des procédures prévues, au moyen notamment de messages falsifiés (techniques d'ingénierie sociale). La Confédération et les cantons ont réagi à la critique (voir chap. 5).

- Les exigences fixées par la Confédération et les cantons contraignaient la Poste à publier le code source du système avant le PIT, conformément à l'art. 7*a* et suivant OVotE, afin que les participants aient la possibilité de se préparer. La Poste a soumis l'accès à ce code source à des conditions d'utilisation particulières. Les critiques ont porté d'une part sur ces conditions d'utilisation et, d'autre part, sur la préparation du code source. En effet, certaines personnes ont critiqué le fait que les conditions d'utilisation prévoyaient des restrictions inadmissibles au droit d'étudier, de modifier, de compiler et d'exécuter le code source mais aussi de rédiger des études en la matière et de les publier, droit qui figure à l'art. 7*b*, al. 4, OVotE. La Poste contrevenait également à l'art. 7*b*, al. 1, OVotE en publiant un code source difficile à lire et une documentation insuffisante. La Chancellerie fédérale a invité la Poste à revoir et adapter ses conditions générales de publication du code source.[4]

5 Déroulement

Le 7 février 2019, la Chancellerie fédérale et les cantons de Fribourg, des Grisons, de Neuchâtel, de St-Gall et de Thurgovie ont publié un communiqué de presse pour annoncer le PIT[5]. Dès lors, les personnes intéressées ont pu s'enregistrer anonymement sur la plateforme du PIT. La société SCRT a annoncé le test aux milieux spécialisés sur Twitter et en passant par d'autres canaux. Ce même jour, la Poste a rendu accessible le code source.

Les médias ayant manifesté un grand intérêt pour le PIT, la Chancellerie fédérale les a invités à une séance d'information organisée le 25 février 2019 à l'occasion du lancement du test. Des représentants de la Confédération, des cantons et de la Poste ont distribué des fiches

[4] https://www.bk.admin.ch/bk/fr/home/documentation/communiques.msg-id-74307.html
[5] https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-73898.html

d'information et répondu aux questions[6]. Les fiches portaient sur les objectifs du PIT et sur son champ d'application. Elles représentaient la réponse de la Confédération et des cantons aux nombreuses critiques sur les modalités du test. Des explications sur le sujet étaient également mises en ligne sur le site de la Chancellerie fédérale sous la rubrique Questions et réponses.[7]

Durant le test, les participants pouvaient se rendre sur la plateforme du PIT afin de se procurer des cartes de légitimation pour le vote, de poser des questions et de soumettre leurs rapports. La société SCRT triait les rapports et informait les participants des résultats de son analyse. Lorsque le rapport indiquait une possible vulnérabilité, SCRT informait le CG et la Poste. SCRT et La Poste soumettaient en outre périodiquement au CG leur évaluation des rapports, évaluation qui n'a suscité aucun désaccord entre les parties quels qu'ils soient.

6 Résultats

À la fin du test, le 24 mars 2019, 3186 participants issus de 137 pays[8] s'étaient enregistrés. Parmi eux, 1090 personnes ou équipes s'étaient effectivement connectées sur la plateforme du PIT et 822 personnes avaient demandé des cartes de légitimation pour le vote dans le cadre du test. En fin de compte, 80 personnes ont soumis 173 rapports sur la plateforme du PIT. Dans seize rapports, SCRT a constaté des manquements de la Poste aux meilleures pratiques de sécurité.[9] La Poste a indemnisé les participants en conséquence pour un montant total de 2000 francs. Le PIT n'a révélé aucune intrusion dans l'infrastructure, aucune manipulation des voix ni aucune remise en cause du secret du vote.

Des chercheurs, qui ont étudié la documentation relative au système fournie dans le cadre de la publication du code source, ont identifié trois failles majeures du système.[10] Ces découvertes ne sont pas directement liées au PIT. L'une d'elles touchait également le système offrant la vérifiabilité individuelle déjà en service. À la suite de cette découverte, la Poste a renoncé à utiliser son système lors de la votation du 19 mai 2019. La Chancellerie fédérale a en outre annoncé qu'elle ferait un point de la situation afin de prévenir de telles erreurs en temps utile à l'avenir. Aucune attaque contre le système qui aurait utilisé l'une de ces failles n'a été constatée. Étant donné que ces failles n'ont pas été décelées au moyen d'une attaque lancée contre le système testé, les rapports n'entraient pas dans le champ du PIT.

7 Conclusions

Le fait qu'un grand nombre de personnes compétentes issues du monde entier a participé activement au test constitue un véritable succès. Leur travail a permis d'éliminer des failles dans la catégorie des meilleures pratiques et donc d'améliorer la sécurité de l'ensemble du système. Ces personnes bénéficient désormais d'une expérience dans le domaine du vote électronique en Suisse qu'elles pourront peut-être faire valoir en d'autres occasions en s'occupant par exemple de questions de sécurité ou en participant au débat public.

[6] https://www.bk.admin.ch/bk/fr/home/droits-politiques/groupe-experts-vote-electronique/oeffentlicher_intrusionstest.html
[7] https://www.bk.admin.ch/bk/fr/home/droits-politiques/groupe-experts-vote-electronique/oeffentlicher_intrusionstest.html
[8] Selon les déclarations des participants eux-mêmes
[9] Ch. 4.3 de l'annexe et https://www.onlinevote-pit.ch/stats/
[10] https://www.bk.admin.ch/bk/fr/home/documentation/communiques.msg-id-74508.html

Il est probable que les participants n'étaient pas tous des experts, mais qu'il y avait parmi eux aussi des citoyens intéressés. Le PIT leur a donné la possibilité de se familiariser avec un système de vote électronique qui sera peut-être un jour utilisé dans leur canton.

La Poste a rempli la majorité des exigences de la Confédération et des cantons. À grand renfort de ressources et de personnel qualifié, elle a mis sur pied un PIT concluant. Le test a notamment révélé qu'il fallait maintenant s'atteler sérieusement à la question de la préparation et de la publication du code source.

Les nombreuses critiques exprimées au sujet du champ d'application du PIT devront être exploitées. Le point de la situation que fera la Chancellerie fédérale, notamment en ce qui concerne les aspects liés à la sécurité qui ne peuvent pas être traités dans le cadre d'un PIT, devra se concentrer sur les actions susceptibles de favoriser et de structurer un dialogue constructif avec des experts indépendants. Pour ce qui est du développement du système et des vérifications d'assurance qualité, il faudra davantage faire appel à des experts indépendants.

Les rapports les plus utiles ont été ceux qui dénonçaient les failles majeures décelées dans le code source. Aucune tentative aboutie de pénétrer dans le système n'a été annoncée. À l'avenir, il faudra examiner la possibilité de créer des incitations en vue d'obtenir des informations utiles sur le code source et la documentation. Les expériences faites dans ce contexte sont prometteuses en ce qui concerne la mise en place d'une culture de la qualité et de l'erreur dans le domaine du vote électronique.

Il est fort probable que la médiatisation du PIT a contribué à faire augmenter le nombre de personnes qui ont participé à l'analyse du code source.

Le test public d'intrusion réalisé cette année était le premier en son genre en ce qui concerne le vote électronique. Il servira d'expérience en cas de nouveaux tests.

8 Documentation complémentaire, rapports, renvois

Informations de la Confédération, des cantons et de la société SCRT (prestataire chargé de l'exécution) sur le test public d'intrusion.

Documents, rapports, renvois	lien
Page de la Confédération consacrée au test public d'intrusion 2019	https://www.bk.admin.ch/bk/fr/home/droits-politiques/groupe-experts-vote-electronique/oeffentlicher_intrusionstest.html
Exigences fixées par la Confédération et les cantons pour les tests publics d'intrusion	https://www.bk.admin.ch/dam/bk/fr/dokumente/pore/Exigences%20de%20la%20Conf%C3%A9d%C3%A9ration%20et%20des%20cantons_tests%20d%E2%80%99intrusion%20publics.pdf.download.pdf/Exigences%20de%20la%20Conf%C3%A9d

	%C3%A9ration%20et%20des%20cantons_tests%20d%E2%80%99intrusion%20publics.pdf
Fiche d'information de la Chancellerie fédérale – PIT	https://www.bk.admin.ch/dam/bk/fr/dokumente/pore/PIT_Factsheet%20BK_FR.pdf.download.pdf/PIT_Factsheet%20BK_FR.pdf
Fiche d'information du comité de gestion – PIT	https://www.bk.admin.ch/dam/bk/fr/dokumente/pore/PIT_Factsheet%20Leitungsausschuss_FR.pdf.download.pdf/PIT_Factsheet%20Leitungsausschuss_FR.pdf
Plateforme d'enregistrement PIT pour les personnes intéressées et les participants	https://www.onlinevote-pit.ch/
Questions et réponses sur le PIT (FAQ) pour les personnes intéressées et les participants	https://www.onlinevote-pit.ch/faq/
Rapports PIT acceptés et publiés	https://www.onlinevote-pit.ch/stats/

Informations du fournisseur du système, la Poste, sur le test public d'intrusion.

Documents, rapports, renvois	lien
Rapport technique final détaillé de l'opérateur du système (Poste CH SA)	https://www.post.ch/-/media/post/evoting/dokumente/abschlussbericht-oeffentlicher-intrusionstest-post.pdf?la=fr&vs=1
Terms, Conditions and Code of Conduct Public Intrusion Test (PIT)	https://www.onlinevote-pit.ch/conduct/
Page consacrée au test public d'intrusion 2019	https://www.post.ch/fr/solutions-commerciales/vote-electronique/publications-et-code-source#test-d-intrusion-public-2019
Article du blog spécialisé sur le test public d'intrusion	https://www.evoting-blog.ch/fr/pages/2019/test-de-piratage-public-du-systeme-de-vote-electronique-de-la-poste
Article du blog spécialisé sur la publication du code source	https://www.evoting-blog.ch/fr/pages/2019/la-poste-divulgue-le-code-source-de-son-systeme-de-vote-electronique
Système de démonstration de vote électronique	https://www.evoting.ch/fr

Accès au code source depuis le site Internet de la Poste	https://www.post.ch/fr/solutions-commerciales/vote-electronique/publications-et-code-source#publicationcodesource

9 Annexe

Public Intrusion Test, Final Report, SCRT SA, 2019