Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Chancellerie fédérale ChF**

Section des droits politiques

# Dialogue avec les milieux scientifiques 2020

## Abrégé du rapport de synthèse

### 1. Contexte et procédure

Dans le cadre du mandat que le Conseil fédéral lui a confié le 26 juin 2019, la Chancellerie fédérale (ChF), en collaboration avec différents cantons, a conduit un dialogue avec des experts issus du monde scientifique. Il visait à fournir des éléments au sous-groupe de travail de la ChF et des cantons en vue de l'élaboration de recommandations. La ChF a examiné avec 23 experts issus de la recherche et de l'industrie des questions liées au vote électronique[1]. Le dialogue s'est concentré sur des questions techniques. La plupart des experts disposaient de connaissances dans le domaine des sciences exactes et trois d'entre eux avaient un bagage en sciences sociales.

Le 14 février 2020, la ChF a soumis aux experts un questionnaire composé d'une soixantaine de questions[2]. Se fondant sur les réponses obtenues, la ChF a mené un dialogue en ligne par écrit, du 5 mai au 17 juillet 2020. Pour chaque bloc de discussion, le modérateur a fourni un résumé des travaux précédents aux experts participants. Le résumé des blocs de discussion et le résumé des réponses ont été intégrés dans le document de synthèse du dialogue avec les experts (« Summary of the Expert Dialog »).

### 2. Evaluation générale

Les experts estiment qu'il faut intervenir en ce qui concerne la sécurité, la transparence et le contrôle indépendant. Ils sont néanmoins d'avis que des progrès significatifs ont été accomplis au courant des 15 dernières années. Ils recommandent d'analyser également la sécurité des autres canaux de vote. Ils invitent en outre à approfondir la question de la création d'un climat de confiance.

Les experts soulignent l'importance d'associer en tout temps les spécialistes - en particulier des experts issus du monde scientifique - à la conception, au développement et au contrôle des systèmes de vote électronique. La création d'un comité scientifique a été évoquée à plusieurs reprises.

### 3. Mise à disposition d'un système sûr

#### 3.1 Les prescriptions en matière de sécurité doivent rester la prérogative des autorités

Les experts estiment que l'évaluation des risques et le cas échéant la prescription de mesures doivent rester l'affaire des autorités. Un comité scientifique pourrait les assister dans ce domaine.

#### 3.2 Standardisation des composants cryptographiques

Les preuves de sécurité dans le domaine de la cryptographie déjà exigées aujourd'hui sont cruciales. Il convient de les adapter constamment à l'état de la science et des connaissances. Les experts recommandent en outre aux autorités d'œuvrer à la standardisation des composants cryptographiques.

[1] Liste des experts mandatés: www.bk.admin.ch > Droits politiques > Vote électronique
[2] Questionnaire: www.bk.admin.ch > Droits politiques > Vote électronique

### 3.3 Garantir la qualité et la vérifiabilité du code source

Il faut veiller à ce que la documentation du système et le code source soient disponibles sous une forme qui permette un contrôle efficace de leur conformité avec les exigences légales. Les experts ont cité plusieurs standards qui pourraient servir de base aux processus de développement. La simplicité doit être la règle maîtresse de la conception du système.

### 3.4 Plus de diversité comme condition fondamentale de la fiabilité

Les experts estiment que la diversité des composants importants pour la vérifiabilité (composants de contrôle et de vérification) est une condition fondamentale de la fiabilité d'un système. Grâce au fonctionnement correct d'autres composants, les erreurs dans certains composants ne devraient pas affecter la vérifiabilité (gain de sécurité exponentiel). Le logiciel fait partie des éléments à diversifier. Les experts voient également un potentiel d'amélioration dans la génération des paramètres système (par ex. des codes de contrôle pour la vérifiabilité individuelle), qui devrait être vérifiable et distribuée. Ils ont ébauché des solutions d'impression partagée des cartes de légitimation. Si les experts sont bien conscients du fait que la diversité augmente les coûts et la complexité de l'exploitation, ils soulignent néanmoins la plus-value qu'elle apporte.

### 3.5 Tableau d'affichage public au service de la vérifiabilité

La possibilité de recourir à un tableau d'affichage public (*Public Bulletin Board*) - instrument évoqué dans la littérature sur le vote électronique - afin de développer la vérifiabilité et d'améliorer son indépendance a été examinée. Les experts estiment qu'un tel instrument est susceptible de contribuer à la confiance mais relèvent que celle-ci pourrait être affectée en cas d'erreur de conception et de réalisation. Les besoins des votants, notamment en matière de communication, de présentation visuelle et de convivialité, doivent être établis et pris en compte suffisamment tôt.

## 4. Contrôle sur mandat et contrôle public

### 4.1 Contrôle sur mandat

La certification des systèmes n'est pas considérée comme déterminante. Une certification (selon la norme ISO27001) pourrait néanmoins s'avérer judicieuse dans le cadre du contrôle de l'exploitation. Les autorités devraient privilégier les contrôles indépendants effectués par des personnes dotées des compétences nécessaires plutôt que recourir à des certifications. Il faut faire appel à des cryptographes également pour le contrôle du code source et de l'exploitation. Le contrôle doit reposer sur un concept global afin d'éviter les lacunes. Il doit faire l'objet d'une commande de la Confédération ou d'un comité indépendant.

### 4.2 Contrôle public

Les experts attachent une grande importance au contrôle public. Ils préconisent de remplacer le test public d'intrusion mené en 2019 par un programme *Bug Bounty* (PBB) permanent, donnant droit à une compensation financière. Le PBB ne doit pas se limiter à pirater l'infrastructure du fournisseur, mais viser à détecter les erreurs dans la documentation du système et le code source. La définition des objectifs et des modalités ainsi que la haute surveillance sur le PBB doivent être arrêtées par la Confédération ou un comité indépendant.

D'autres mesures, telles que des hackathons, visant à associer le public sont envisageables en plus du PBB. Il pourrait également être judicieux de faire appel à des personnes sans bagage technique, par exemple dans le cadre d'un projet de sciences participatives consacré à la convivialité.

## 4.3 Transparence et publication du code source

La transparence est la condition *sine qua non* d'un contrôle public efficace. Les experts estiment qu'il faut absolument renoncer à exiger une déclaration de confidentialité lors de la publication du code source.

Tous les documents nécessaires pour comprendre comment le système fonctionne et est exploité doivent être publiés avec le code source. Il doit en outre être possible aux participants de tester le système sur leur ordinateur. Si les adaptations du code source ne sont pas immédiatement publiées, les experts recommandent de procéder à une première itération des contrôles internes afin d'éviter des erreurs susceptibles de saper la confiance.

Il faut publier les failles et répondre aux remarques du public. Il appartient à la Confédération de préciser les modalités à cet égard. La plupart des experts recommandent en outre de publier les rapports de contrôle. Ils ont cependant été nombreux à signaler que des rapports de mauvaise qualité pourraient affecter la confiance.

Les experts sont d'avis qu'une publication même sans licence libre[3] permet de mener un contrôle public adéquat. Ils estiment néanmoins qu'une publication sous licence libre offre de meilleures garanties de succès.

## 4.4 Procédure en cas de non-conformités

Idéalement, le contrôle a lieu suffisamment tôt pour que les non-conformités puissent être découvertes et éliminées avant l'exploitation du système. Des processus décisionnels doivent être mis en place pour les non-conformités découvertes plus tard.

Il n'est pas nécessaire d'interrompre l'exploitation d'un système de vote électronique pour n'importe quelle non-conformité. Les experts estiment qu'il est raisonnable d'accepter des risques mineurs. Toute la difficulté réside dans l'appréciation correcte du risque. Il peut être utile de faire une comparaison avec des risques qui ont déjà été acceptés. Il faut également tenir compte du fait que sans le vote électronique les Suisses de l'étranger perdent de fait une partie de leur droit de vote et que renoncer à ce canal implique de recourir davantage au vote par correspondance, qui n'est pas non plus exempt de risque. Plus une non-conformité affecte le système et moins elle est circonscrite aux processus environnants, plus il est nécessaire de l'éliminer. En principe, les erreurs dans le protocole cryptographique ou dans sa mise en œuvre dans le code source ne doivent pas être acceptées.

# 5. Appréciation du dialogue par les experts

De l'avis des experts, le dialogue avec les milieux scientifiques pose un jalon important. Il a permis d'obtenir des résultats précieux et devrait servir de base à un échange permanent.

[3] Les licences libres permettent d'utiliser un logiciel dans n'importe quel but.