Règlement technique concernant le vote électronique (RT VE)

du xx XX 2013

La Chancellerie fédérale suisse (ChF),

vu les art. 27*e*, al. 2, 27*f*, al. 1, 27*g*, al. 2, 27*i*, al. 3, et 27*l*, al. 3, de l'ordonnance du 24 mai 1978[1] sur les droits politiques (ODP),

arrête:

Art. 1 Conditions générales régissant l'octroi de l'approbation pour un scrutin faisant appel au vote électronique

[1] L'approbation pour un scrutin faisant appel au vote électronique est octroyée si les conditions suivantes sont remplies:

a. l'aménagement de l'exploitation, de l'infrastructure et des fonctionnalités du système de vote électronique garantit la sûreté et la fiabilité du vote par voie électronique (annexe, chap. 2, 3 et 4);
b. le système de vote électronique garantit aux électeurs des fonctionnalités suffisantes, qui soient à la fois accessibles et faciles à utiliser.

[2] La Chancellerie fédérale peut faire en sorte qu'un service indépendant vérifie si les conditions sont remplies. Cette vérification englobe l'analyse des risques; elle est effectuée en particulier si le système de vote électronique et son exploitation ont subi des modifications non négligeables.

[3] Les éléments suivants afférents aux systèmes vérifiables individuellement ou complètement (art. 3 et 4) doivent être vérifiés à titre de condition supplémentaire:

1. le protocole cryptographique (annexe, sous-chap. 5.1);
2. les fonctionnalités (annexe, sous-chap. 5.2);
3. l'infrastructure et l'exploitation (annexe, sous-chap.5.3);
4. les composants de contrôle (annexe, sous-chap. 5.4);
5. la protection contre les tentatives d'intrusion dans l'infrastructure (annexe, sous-chap. 5.5);
6. les exigences applicables aux imprimeries (annexe, sous-chap. 5.6).

1 RS **161.11**

[4] Au besoin, il convient de prendre des mesures de sécurité supplémentaires qui ne découlent pas directement des exigences de sécurité (annexe, chap. 2) afin de réduire les risques.

Art. 2 Analyse des risques

[1] Il convient d'effectuer une analyse des risques visant à établir par écrit, de manière détaillée et compréhensible, que les risques pour la sécurité se situent à un niveau suffisamment bas. L'analyse doit porter sur les objectifs de sécurité suivants:

a. garantir l'exactitude des résultats;

b. protéger le secret du vote et faire en sorte que des résultats partiels ne soient pas établis de manière anticipée;

c. assurer la disponibilité des fonctionnalités du vote électronique;

d. protéger les informations personnelles concernant les électeurs;

e. protéger les informations destinées aux électeurs;

f. faire en sorte que des preuves relatives au comportement de vote ne soient pas établies.

[2] Chaque risque résiduel doit être identifié clairement compte tenu des objectifs de sécurité, des éventuelles séquences de données liées à ces objectifs, des menaces, des failles et de la documentation système concernant l'infrastructure, l'exploitation et les fonctionnalités du vote électronique. Le canton indique les raisons pour lesquelles il considère que les risques résiduels sont suffisamment faibles.

[3] En aucun cas l'objectif ne doit consister à garantir la sécurité en gardant secrètes des informations concernant le système.

Art. 3 Exigences à remplir pour que 50 pour cent de l'électorat cantonal puisse voter par voie électronique (vérifiabilité individuelle)

[1] Si un système de vote électronique permettant à 50 pour cent de l'électorat cantonal de voter par voie électronique est approuvé, les votants doivent avoir la possibilité de déterminer si le suffrage qu'ils ont exprimé a été manipulé ou intercepté sur la plateforme utilisateur ou pendant la transmission. Pour cela, ils doivent recevoir la preuve attestant que la partie serveur du système a enregistré le suffrage tel qu'il a été exprimé, en tant que suffrage exprimé conformément à la procédure prévue par le système. La preuve doit attester, pour chaque suffrage partiel, que la réponse choisie a été enregistrée correctement.

[2] Si les données d'authentification client sont envoyées par voie électronique, les votants doivent pouvoir demander, après la fermeture du canal permettant de voter par voie électronique, la preuve attestant que le système n'a pas enregistré de suffrages exprimés moyennant l'utilisation de leurs données d'authentification client.

[3] Le caractère concluant d'une preuve ne doit pas dépendre de la fiabilité de la plateforme utilisateur ou du canal de transmission.

[4] Le caractère concluant d'une preuve peut se fonder sur les éléments suivants, compte tenu des conditions figurant au sous-chapitre 4.2 de l'annexe:

a. la fiabilité de la partie serveur du système (ch. D2.30);

b. la fiabilité de dispositifs techniques particuliers des votants, qui doivent répondre à des exigences de sécurité particulièrement élevées (ch. D2.10);

c. la confidentialité de données envoyées sur support papier (référence de vérifiabilité); la confidentialité de ces données doit être garantie par des mesures particulières en dehors du cadre de l'infrastructure du VE (ch. D2.20 et D2.40).

Art. 4 Exigences à remplir pour que l'ensemble de l'électorat cantonal puisse voter par voie électronique (vérifiabilité complète)

[1] Si un système de vote électronique permettant à l'ensemble de l'électorat cantonal de voter par voie électronique est approuvé, il faut faire en sorte que les votants ou les vérificateurs puissent, dans le respect du secret du vote, identifier toute manipulation aboutissant à une falsification des résultats. Pour cela, il faut répondre à des exigences étendues en matière de vérifiabilité individuelle (al. 2) et à des exigences en matière de vérifiabilité universelle (al. 3 à 5).

[2] S'agissant de la vérifiabilité individuelle, les exigences suivantes s'appliquent en plus des exigences visées à l'art. 3:

a. la preuve doit, en plus, permettre aux votants de constater que les données pertinentes pour la vérification universelle sont parvenues dans la partie fiable du système (al. 5);

b. après la fermeture du canal permettant de voter par voie électronique, les votants doivent pouvoir demander la preuve attestant que la partie fiable du système n'a pas déjà enregistré un suffrage exprimé moyennant l'utilisation de leurs données d'authentification client;

c. le caractère concluant d'une preuve ne doit pas dépendre de l'ensemble de la partie serveur du système. Il peut toutefois se fonder sur la fiabilité de la partie fiable du système.

[3] S'agissant de la vérification universelle, les vérificateurs reçoivent une preuve attestant que les résultats ont été établis correctement. Ils doivent évaluer cette preuve au cours d'un processus observable. Pour ce faire, ils doivent utiliser des dispositifs techniques indépendants et séparés du reste du système. La preuve doit attester que l'établissement des résultats a pris en compte:

a. tous les suffrages qui ont été exprimés conformément à la procédure prévue par le système et qui ont été enregistrés par la partie fiable du système;

b. uniquement les suffrages qui ont été exprimés conformément à la procédure prévue par le système;

c. tous les suffrages partiels sans les modifier, c'est-à-dire conformément à la preuve générée dans le cadre de la vérification individuelle.

[4] Le caractère concluant de la preuve ne peut dépendre que de la fiabilité de la partie fiable du système et du dispositif technique utilisé pour la vérification. Par ailleurs,

la garantie du secret du vote et le fait que des résultats partiels ne doivent pas être établis de manière anticipée au sein de l'infrastructure du vote électronique ne peuvent dépendre que de la fiabilité de la partie fiable du système.

[5] La partie fiable du système comprend soit un groupe soit quelques groupes de composants indépendants sécurisés par des mesures particulières (composants de contrôle). L'utilisation de ces composants doit permettre d'identifier n'importe quel abus même si, dans chaque groupe, il n'y a qu'un composant de contrôle qui fonctionne correctement et qui n'est pas manipulé sans que cela se remarque. Pour garantir la fiabilité de la partie fiable du système, il est impératif que les composants de contrôle diffèrent les uns des autres de par leur conception, mais aussi que leur exploitation et leur surveillance soient indépendantes (chapitre 4 de l'annexe).

Art. 5 Pièces justificatives à l'appui des demandes d'octroi

[1] Les demandes d'octroi présentées en vertu de l'art. 27*c* ODP doivent être assorties de pièces justificatives attestant que le système de vote électronique a été vérifié sous l'angle des exigences fixées (art. 1, al. 2 et 3) et que toutes les exigences sont dûment remplies.

[2] Les pièces justificatives à l'appui des vérifications doivent être complétées par des pièces justificatives attestant que l'évaluation des risques menée avant un scrutin a démontré que les risques se situent à un niveau suffisamment bas.

Art. 6 Entrée en vigueur

Le présent règlement entre en vigueur le 1er janvier 2014.

xx 2013

Chancellerie fédérale suisse

Corina Casanova

Annexe du règlement technique de la Chancellerie fédérale concernant le vote électronique[2]

[2] Le texte de l'annexe du règlement technique concernant le vote électronique n’est pas publié au RO. Il peut être obtenu auprès de la Chancellerie fédérale, Section des droits politiques, Palais fédéral ouest, 3003 Berne.