

Sécurité des systèmes de vote par internet : la CNIL actualise sa recommandation de 2010

09 juillet 2019

Avec l'entrée en application RGPD et suite à la consultation auprès des professionnels et experts afin d'améliorer la sécurité des solutions de vote par correspondance électronique, notamment via Internet, la CNIL a mis à jour sa recommandation sur ces dispositifs.

Le 25 avril 2019, la CNIL a adopté une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet. Elle présente aux responsables de traitement souhaitant recourir à un tel système de vote une approche par niveau de risque et par objectifs de sécurité à atteindre.

La recommandation s'accompagne d'une fiche pratique qui présente une méthodologie en deux temps :

- une grille d'analyse pour déterminer le niveau de sécurité que le système de vote par correspondance électronique, notamment via Internet, doit respecter ;
- des niveaux d'objectifs de sécurité avec des exemples de moyens , non limitatifs, à mettre en œuvre pour atteindre ces objectifs.

Etape 1 : remplir la grille d'analyse

La grille suivante, basée sur des questions fermées, a pour objet d'aider les responsables de traitement à déterminer le niveau de sécurité que leur système doit atteindre.

	Vrai (0)	Faux (1)
Question 1 : Le scrutin peut être reporté, par exemple en cas d'incident.		
Question 2 : Le scrutin concerne moins de 50 personnes.		

<p>Question 3 : Le scrutin concerne moins de 1 000 personnes.</p>		
<p>Question 4 : D'autres voies de vote sont possibles (à l'urne, à distance, etc.).</p>		
<p>Question 5 : Les personnes élues n'ont pas de pouvoir décisionnel.</p>		
<p>Question 6 : Les votants sont tous sur le territoire national.</p>		
<p>Question 7 : Les votants sont tous sur le territoire européen.</p>		
<p>Question 8 : Aucun élément laissant penser que le bon déroulement de l'élection puisse être affecté (menaces particulières, etc.) n'a été décelé.</p>		
<p>Question 9 : La validation du scrutin ne nécessite pas de preuves formelles de bon déroulé.</p>		
<p>Question 10 : L'organisation du scrutin n'est pas une obligation légale.</p>		
<p>Total</p>		

Le responsable de traitement compte « 1 » pour chaque réponse où il inscrit « faux ». La somme des « 1 » lui permet d'obtenir un score et ainsi de déterminer le niveau de solution attendu :

- entre 0 et 2 points, la solution doit répondre aux objectifs de niveau 1 ;
- entre 3 et 6 points, la solution doit répondre aux objectifs de niveau 2 ;
- entre 7 et 10 points, la solution doit répondre aux objectifs de niveau 3.

Une fois cette étape franchie, le responsable de traitement peut déterminer les objectifs de sécurité que la solution de vote doit atteindre.

Etape 2 : déterminer les objectifs de sécurité

Les industriels, fournisseurs de solutions de système de vote, sont ainsi libres de fournir tout moyen adéquat permettant de répondre à l'objectif. L'expertise indépendante de la solution devra mettre en évidence si la solution proposée est pertinente afin d'y répondre.

Les industriels qui le souhaitent peuvent faire parvenir à la CNIL une description des moyens qu'ils jugent acceptables et qu'ils proposent dans leur solution afin de répondre aux objectifs présentés dans la recommandation. La CNIL pourra les étudier et mettre à jour, le cas échéant, la présente fiche.

La Commission tient à souligner que le moyen de répondre à un objectif est valable seulement si sa mise en œuvre opérationnelle est réalisée de manière pertinente et correcte. La Commission rappelle de nouveau que seule l'étude réalisée par les experts indépendants permettra d'assurer au responsable de traitement que l'objectif de sécurité énoncé est pleinement et correctement atteint.

Objectifs de sécurité de niveau 1

- Objectif de sécurité n° **1-01** : mettre en œuvre une solution technique et organisationnelle de qualité ne présentant pas de faille majeure (faille publiée par l'éditeur et/ou rendue publique par des tiers).

Solution : Utiliser les dernières versions stables et mises à jour des systèmes d'exploitation, des serveurs Web, des solutions de chiffrement et des bases de données mobilisées dans la solution. Il convient également d'utiliser des protocoles et algorithmes publics de chiffrement réputés « forts ».

- Objectif de sécurité n° **1-02** : définir le vote d'un électeur comme une opération atomique comprenant le choix, la validation, l'enregistrement du bulletin dans l'urne, l'émargement et la délivrance d'un récépissé.

Solution : Dès lors que l'électeur a validé de manière définitive son choix de vote, l'ensemble des opérations précitées doit s'enchaîner sans discontinuité jusqu'à l'achèvement de la dernière action, c'est-à-dire jusqu'à la délivrance d'un récépissé. L'échec d'une action entraîne l'échec de toute la chaîne et, a contrario, la réussite de la chaîne n'est possible que de par le bon déroulement de chacune des actions unitaires.

- Objectif de sécurité n° **1-03** : authentifier les électeurs en s'assurant que les risques majeurs liés à une usurpation d'identité sont réduit de manière significative.

Solution : L'électeur s'authentifie à l'aide d'un couple identifiant et mot de passe personnel qui lui a été remis de manière sécurisée (par deux canaux de communications séparés). Le fichier des électeurs comportant les éléments d'authentification est conservé de manière sécurisée. En cas de perte ou de vol de ses moyens d'authentification, une procédure permet à l'électeur d'effectuer son vote et rend les moyens d'authentification perdus ou volés inutilisables.

- Objectif de sécurité n° **1-04** : assurer la stricte confidentialité du bulletin dès sa création sur le poste du votant.

Solution : Chiffrer le bulletin sur le poste du votant, coté client et avant son émission, à l'aide d'un algorithme public réputé « fort ».

- Objectif de sécurité n° **1-05** : assurer la stricte confidentialité et l'intégrité du bulletin pendant son transport.

Solution : Utiliser un canal sécurisé afin d'acheminer le bulletin, lui-même déjà chiffré (voir objectif de sécurité n° 1-02), du poste du votant jusqu'à l'urne électronique. Dans le cas de recours à des certificats, les choisir et les utiliser, au niveau 2, si possible conformément aux préconisations du RGS et, au niveau 3, conformément aux préconisations du RGS.

- Objectif de sécurité n° **1-07** : assurer l'étanchéité totale entre l'identité de votant et l'expression de son vote pendant toute la durée du traitement.

Solution : Ne disposer d'aucun lien entre le votant et son bulletin chiffré dès lors que le vote est exprimé. Le bulletin n'est pas horodaté, contrairement à la liste d'émargement, et le bulletin et la liste sont conservés dans des espaces de stockage distincts.

- Objectif de sécurité n° **1-08** : renforcer la confidentialité et l'intégrité des données en répartissant le secret permettant le dépouillement exclusivement au sein du bureau électoral et garantir la possibilité de dépouillement à partir d'un seuil de secret déterminé.

Solution : Générer a minima trois clés et exiger que deux de ces clés a minima soient indispensables afin de permettre le dépouillement. La génération des clés doit être réalisée de manière publique et ces dernières doivent être stockées sur un support sécurisé en possession uniquement du président du bureau et de ses assesseurs.

- Objectif de sécurité n° **1-09** : définir le dépouillement comme une fonction atomique utilisable seulement après la fermeture du scrutin.

Solution : L'option de dépouillement ne doit être activable qu'après la fermeture du scrutin et le scellement de l'urne et de la liste d'émargement. L'opération de dépouillement, une fois activée, ne peut être interrompue avant d'être entièrement exécutée et terminée. Un dépouillement partiel ne peut ainsi être réalisé.

- Objectif de sécurité n° **1-10** : assurer l'intégrité du système, de l'urne et de la liste d'émargement.

Solution : S'assurer que le dispositif déployé est identique à celui audité par l'expert indépendant qui a effectué l'expertise commanditée par le responsable de traitement. Des empreintes des éléments doivent être calculées par l'expert et pouvoir être recalculées sur le système afin de les comparer et de les vérifier. L'urne et la liste d'émargement doivent être scellées et une empreinte calculée dès le scellement.

- Objectif de sécurité n° **1-11** : s'assurer que le dépouillement de l'urne puisse être vérifié a posteriori.

Solution 1 : Possibilité de rejouer le dépouillement : pour cela, conserver l'ensemble des éléments nécessaires pour pouvoir prouver que l'urne dépouillée est bien celle contenant les votes des électeurs qui se sont exprimés (des votants) et uniquement ceux-là ; conserver les éléments nécessaires pour dérouler à nouveau la procédure de décompte des votes.

Solution 2 : Possibilité de prouver que le dépouillement s'est déroulé sans erreur : pour cela, conserver l'ensemble des éléments nécessaires à la vérification de la preuve cryptographique démontrant que l'urne dépouillée est celle contenant les votes des électeurs qui se sont exprimés (des votants) et uniquement ces derniers et que celle-ci a été correctement dépouillée.

Objectifs de sécurité de niveau 2

- Objectif de sécurité n° **2-01** : assurer une haute disponibilité de la solution.

Solution : Disposer d'une infrastructure dimensionnée pour supporter l'élection et la charge attendue. Il est prévu un système de redondance par un dispositif de secours susceptible de prendre le relais en cas de panne du système principal et offrant les mêmes garanties et caractéristiques.

- Objectif de sécurité n° **2-02** : assurer un contrôle automatique de l'intégrité du système, de l'urne et de la liste d'émargement.

Solution : Calculer à intervalles non réguliers et non prévisibles une empreinte des éléments précités et les comparer à la valeur de référence calculée en amont (voir objectif de sécurité n° 1-08).

- Objectif de sécurité n° **2-03** : permettre le contrôle automatique par le bureau électoral de l'intégrité de la plateforme de vote pendant tout le scrutin.

Solution : Mettre à disposition du bureau électoral un dispositif lui permettant de vérifier directement la mise en œuvre de l'objectif de sécurité n° 2-02 depuis un écran de contrôle.

- Objectif de sécurité n° **2-04** : authentifier les électeurs en s'assurant que les risques majeurs et mineurs liés à une usurpation d'identité sont réduits de manière significative.

Solution 1 : L'électeur s'authentifie à l'aide d'un certificat électronique, choisi et utilisé conformément aux

préconisations du RGS.

Solution 2 : L'électeur s'authentifie à l'aide d'un couple identifiant et mot de passe personnel qui lui a été remis de manière sécurisée (deux canaux séparés) et répond à une question défi-réponse non triviale (sont ainsi exclus la date de naissance et tout autre élément facilement décelable) dont il est le seul à connaître la réponse (avec le responsable de traitement).

En cas de perte ou de vol de ses moyens d'authentification, une procédure permet à l'électeur d'effectuer son vote et rend les moyens d'authentification perdus ou volés inutilisables.

- Objectif de sécurité n° **2-06** : utiliser un système d'information mettant en œuvre les mesures de sécurité physique et logique recommandées par les éditeurs et l'ANSSI.

Solution : Appliquer les bonnes pratiques mises en avant dans les documentations par les éditeurs, notamment les éditeurs de solutions de vote, mais également les éditeurs de serveur web, de serveurs d'application et les éditeurs de base de données. Appliquer, selon les cas d'espèce, les bonnes pratiques de l'ANSSI énoncées dans les guides « [Recommandations pour la sécurisation des sites web](#) », « [Recommandations de sécurité relatives à TLS](#) », « [Recommandations de sécurité relatives à IPsec](#) », « [Recommandations de configuration d'un système GNU/Linux](#) », « [Recommandations de sécurité relatives à un système GNU/Linux](#) », « [Recommandations de sécurité relatives aux environnements d'exécution Java sur les postes de travail Microsoft Windows](#) » et s'inspirer du document « [La défense en profondeur appliquée aux systèmes d'information](#) » et du [guide d'hygiène](#).

- Objectif de sécurité n° **2-07** : assurer la transparence de l'urne pour tous les électeurs.

Solution : Rassurer autant que possible les votants qui n'ont pas accès à l'expertise de la solution de vote, garante du bon fonctionnement du dispositif et de la sincérité et intégrité du vote dans son ensemble. Il s'agit de permettre aux électeurs de s'assurer que leur bulletin a été pris en compte dans l'urne et que les bulletins de vote sont construits de manière correcte.

Pour ce faire :

Chaque récépissé de vote contient une information unique, totalement décorrélée de l'identité du votant (empreinte numérique, numéro aléatoire, « preuve à divulgation nulle de connaissance », etc.) qui est calculée au moment où le votant valide son choix de vote. La plateforme de vote électronique est destinataire de l'information et la publie afin de la rendre accessible à tous les électeurs. Chaque électeur peut ainsi avoir la garantie que son bulletin est bien dans l'urne.

De plus, la solution de vote permet aux votants d'accéder à un espace de test où il est possible d'effectuer différents votes de tests et de voir ce qui ressort de l'ouverture du bulletin sur le serveur, le but étant de s'assurer que les bulletins sont correctement construits.

Objectifs de sécurité de niveau 3

- Objectif de sécurité n° **3-02** : permettre la transparence de l'urne pour tous les électeurs à partir d'outils tiers.

Solution : Procéder de la même manière que pour l'objectif de sécurité n° 2-07 en effectuant de surcroît les vérifications sur une machine tierce, mise en œuvre par un partenaire externe au vote.

- Objectif de sécurité n° **3-03** : assurer une très haute disponibilité de la solution de vote en prenant en compte les risques d'avarie majeure.

Solution : Disposer d'une infrastructure dimensionnée pour supporter la charge attendue induite par le processus électoral. Il est prévu un système de redondance par un dispositif de secours susceptible de prendre le relais en cas de panne du système principal et offrant les mêmes garanties et caractéristiques. Prévoir une redondance de l'alimentation de chaque machine, ainsi que des accès à Internet de l'infrastructure. Les sites hébergeant l'infrastructure principale et de secours doivent être suffisamment distants et correctement placés afin de couvrir les risques naturels.

- Objectif de sécurité n° **3-04** : permettre le contrôle automatique et manuel par le bureau électoral de l'intégrité de la plateforme pendant tout le scrutin.

Solution : Donner la possibilité au bureau de déclencher manuellement un contrôle de l'intégrité de la plateforme en supplément du contrôle automatique énoncé par l'objectif n° 2-03.

Pour approfondir

- [Cybersécurité](#)
 - [Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet](#)
 - [Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via internet \(rectificatif\)](#)
-