RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

RECOMMANDATIONS POUR LA MISE EN ŒUVRE DU VOTE PAR INTERNET POUR LES ÉLECTIONS NON POLITIQUES

GUIDE ANSSI

ANSSI-PA-118
2026-04-24

PUBLIC VISÉ :

Développeur **Administrateur** RSSI **DSI** Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI s'intitule **« Recommandations pour la mise en œuvre du vote par Internet pour les élections non politiques »**. Il est téléchargeable sur le site `cyber.gouv.fr`.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
0.1	2025-03-10	Version pour consultation publique
1.0	2026-04-24	Version publiée

Table des matières

1
Introduction

Ce guide s'inscrit dans le cadre d'une collaboration avec la Commission Nationale de l'Informatique et des Libertés (CNIL) et de la mise à jour en 2026 [72] de sa recommandation relative à la sécurité des systèmes de vote par correspondance électronique, appelé aussi *vote par Internet*. Ce guide a fait l'objet d'une consultation publique ayant permis de recueillir les retours de chercheurs dans le domaine, d'organisateurs de scrutins, de prestataires fournisseurs de solutions de vote par correspondance électronique ainsi que d'experts indépendants.

Le vote par correspondance électronique est utilisé en France pour deux catégories d'élections : les élections *non politiques* et les élections *politiques*.

Élections non politiques. Le vote par correspondance électronique est utilisé depuis plusieurs années dans de nombreuses élections professionnelles, au sein des entreprises et au sein de la fonction publique. Ce mode de scrutin est également utilisé pour d'autres élections, par exemple : assemblées générales d'actionnaires ou de copropriétaires, élections organisées par des ordres professionnels, fédérations sportives, associations, universités. En complément, ce mode de scrutin est utilisé en France pour les primaires organisées par les partis politiques : le contexte de ces élections est bien politique, mais elles ne sont pas considérées dans le présent document comme des élections politiques.

Élections politiques. Une élection politique permet soit de désigner des responsables politiques, soit de consulter les électeurs sur des projets de résolutions ou de textes (référendums). C'est une élection pour laquelle les listes électorales sont extraites du Répertoire électoral unique tenu par l'INSEE [1]. Le vote par correspondance électronique est utilisé en France dans le cadre des élections politiques, pour des cas très précis décrits dans le code électoral [2], à savoir les votes des Français résidant à l'étranger pour les élections législatives et les élections des conseillers et des délégués des Français de l'étranger.

Attention

Le présent guide fournit des recommandations techniques pour la mise en œuvre du vote par correspondance électronique pour les **élections non politiques** . En effet, les élections politiques nécessitent des mesures de sécurité complémentaires non abordées dans ce guide.

L'objet de ce guide est d'approfondir la délibération 2026 de la CNIL [72], en formulant des recommandations techniques associées à chaque objectif de cette délibération. Ce guide remplace la page [41] du site Web de la CNIL qui, jusqu'en 2026, remplissait ce rôle.

1. https://www.insee.fr/fr/information/3539086
2. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070239/

2
À qui s'adresse ce guide ?

Ce guide s'adresse en premier lieu aux organisateurs de scrutin qui sont tenus d'en garantir la conformité réglementaire et le respect des principes fondamentaux qui commandent les opérations électorales, notamment par la conformité à la délibération 2026 de la CNIL « portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet » [72]. Cette délibération fait référence aux organisateurs de scrutin en tant que responsables de traitement [40].

Au regard des rôles essentiels qu'ils jouent dans la conformité et la sécurité du vote par correspondance électronique, les prestataires (fournisseurs de solutions de vote) sont également invités à prendre connaissance de ce guide. Les recommandations techniques formulées leur permettront de garantir et/ou de fournir les moyens permettant de démontrer que leurs produits et/ou leurs services sont sûrs et conformes à la délibération de la CNIL.

Enfin, les tiers intervenant dans la vérification de la conformité des scrutins, par exemple les experts indépendants (au sens de la délibération de la CNIL), sont aussi invités à prendre connaissance de ce guide. Les recommandations techniques formulées leur permettront de vérifier la conformité des scrutins à la délibération de la CNIL.

Attention

Les recommandations techniques proposées dans ce guide reposent sur le modèle d'un organisateur du scrutin achetant un service à un prestataire spécialisé dans le vote par correspondance électronique, souvent fourni clé en main (modèle *Software as a Service, SaaS*). Dans le cas d'une autre situation (par exemple, l'organisateur du scrutin développe lui-même sa propre solution de vote), les responsabilités devront être adaptées.

Ce guide contient plusieurs annexes qui, selon le sujet traité, s'adressent en premier lieu aux prestataires spécialisés dans le vote par correspondance électronique ainsi qu'aux tiers intervenant dans la vérification de la conformité des scrutins. Ces annexes fournissent des détails techniques, notamment sur certains mécanismes cryptographiques.

3
Présentation et enjeux du vote par correspondance électronique

Une élection [3] est un choix exprimé au travers d'un vote. Un scrutin désigne l'ensemble des opérations constituant un vote. Un suffrage est l'expression du vote de l'électeur. Un scrutin peut être public (le vote des électeurs n'est pas confidentiel) ou secret (le vote des électeurs est confidentiel). Différentes modalités de vote peuvent être mises en œuvre : d'une part, le vote à l'urne dans un bureau de vote et d'autre part, le vote par correspondance. Le vote par correspondance peut être postal ou électronique.

Attention

Ce guide concerne le vote par correspondance électronique dans le contexte d'un **scrutin secret**.

3.1 Opérations nécessaires à la réalisation d'un scrutin

Un scrutin comporte un nombre important d'opérations rendant sa réalisation complexe. Ces opérations peuvent être réparties dans une chronologie en trois étapes, selon qu'elles aient lieu avant, pendant ou après la période de vote. Les opérations sont gérées par l'organisateur du scrutin qui est responsable de la conformité réglementaire du scrutin et du respect des principes fondamentaux qui commandent les opérations électorales. La Figure 1 présente les opérations décrivant la majorité des scrutins, certaines d'entre elles n'étant pas réalisées pour des scrutins à petite échelle.

Avant la période de vote

- Gestion des listes électorales
- Gestion des options de vote
- Gestion du découpage électoral
- Gestion des moyens d'authentification des électeurs
- Diffusion de la propagande électorale

Pendant la période de vote

- Authentification de l'électeur
- Contrôle de l'appartenance à la liste électorale
- Présentation des options de vote
- Réalisation du choix
- Émargement
- Contrôle de la liste d'émargement
- Contrôle de l'urne

Après la période de vote

- Vérifications diverses
- Dénombrement des émargements
- Dénombrement des choix réalisés
- Dépouillement
- Proclamation des résultats

FIGURE 1 – Opérations constituant la réalisation d'un scrutin

3. Les hyperliens renvoient au Glossaire.

Avant la période de vote

- L'organisateur du scrutin gère les listes électorales, les options de vote (le cas échéant l'éligibilité des candidats, les listes des candidats), le découpage électoral et choisit un ou plusieurs modes de scrutin : ces opérations fournissent une configuration de l'élection. Il gère également (éventuellement via des sous-traitants) les moyens d'authentification des électeurs et la diffusion de la propagande électorale.

Pendant le vote

- Les électeurs sont authentifiés, leur appartenance à la liste électorale est contrôlée, les options de vote leur sont présentées. Par exemple, dans le cas du vote à l'urne, l'authentification peut être réalisée par le contrôle d'une pièce d'identité officielle et le contrôle de l'inscription à la liste électorale est réalisé directement à partir de cette liste.
- L'organisateur du scrutin doit s'assurer que l'ensemble des options de vote est bien présenté et doit permettre aux électeurs de réaliser leur choix et d'émarger. Par exemple, dans le cas du vote à l'urne, l'électeur choisit son option de vote dans un isoloir, le choix de l'électeur est un bulletin papier qu'il met dans une enveloppe opaque. Ensuite il dépose cette enveloppe dans une urne surveillée. L'émargement est enregistré (souvent par la signature de la liste d'émargement).
- Le bureau de vote surveille le déroulement du scrutin. En particulier, il contrôle l'urne et la liste d'émargement.

Après la période de vote

- Les différents acteurs impliqués (organisateur du scrutin, assesseurs, bureau de vote) dénombrent les émargements et les choix exprimés, comparent le nombre d'émargements et le nombre de choix exprimés, réalisent le dépouillement et proclament les résultats. Par exemple, dans le cas du vote à l'urne, le nombre d'émargements et le nombre d'enveloppes sont comparés, les enveloppes sont dépouillées et le résultat est proclamé au niveau du bureau de vote.
- Des vérifications sont effectuées par les différents acteurs, notamment que le résultat proclamé correspond à celui observé (par exemple, un électeur peut constater que le résultat proclamé correspond au résultat constaté dans un bureau de vote).

3.2 Impacts de la numérisation

Dans le cas d'un vote par correspondance *non électronique*, le matériel de vote envoyé aux électeurs (options de vote, enveloppes) est physique et l'électeur réalise son choix par voie postale [4]. Par analogie, dans le cas du vote par correspondance *électronique*, le matériel de vote est dématérialisé et l'organisateur du scrutin met en place un téléservice pour que les électeurs puissent voter depuis un équipement connecté à Internet. Suivant les contextes, ce type de vote est appelé « élection

4. Certaines étapes peuvent faire intervenir des moyens électroniques. Par exemple, la lecture de code-barres.

dématérialisée », « vote par Internet », « vote en ligne », « vote par voie électronique à distance » ou simplement « vote électronique » (bien que ce terme soit ambigu et désigne parfois les machines à voter).

Attention

Comme illustré dans la Figure 2, les termes suffrage et bulletin ont des significations différentes dans le vote à l'urne et le vote par correspondance électronique. Dans le cas du vote à l'urne, l'électeur choisit un bulletin papier correspondant à son suffrage et le dépose dans une enveloppe. Dans le cas du vote par correspondance électronique, le suffrage est numérisé, le client de vote construit le bulletin en chiffrant le suffrage : un bulletin numérique contient donc le suffrage chiffré et correspond plus à la notion d'enveloppe du vote à l'urne.

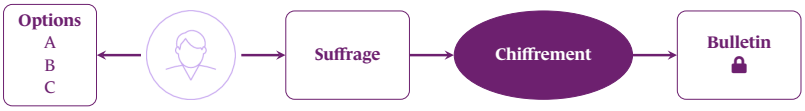

FIGURE 2 – Notions de suffrage et de bulletin

3.2.1 Opérations numérisées par le vote par correspondance électronique

La Figure 3 présente en noir les opérations le plus souvent numérisées dans le vote par correspondance électronique. Le périmètre de la numérisation est important, car il intègre des contrôles renforçant la sincérité des opérations électorales : authentification de l'électeur, contrôle de l'appartenance à la liste électorale, émargement, vérifications. Parmi les opérations préalables, il est possible que la propagande électorale soit dématérialisée.

Avant la période de vote

- Gestion des listes électorales
- Gestion des listes de candidats
- Gestion du découpage électoral
- Gestion des moyens d'authentification des électeurs
- Diffusion de la propagande électorale [a]

a. Selon les scrutins

Pendant la période de vote

- Authentification de l'électeur
- Contrôle de l'appartenance à la liste électorale
- Présentation des bulletins
- Réalisation du vote
- Dépôt du bulletin dans l'urne
- Émargement
- Contrôle de l'urne
- Contrôle de la liste d'émargement

Après la période de vote

- Vérifications diverses
- Dénombrement des émargements
- Dénombrement des bulletins
- Dépouillement des bulletins
- Proclamation des résultats

FIGURE 3 – Opérations numérisées par le vote par correspondance électronique

Avant la période de vote

- La solution de vote est généralement conçue et développée par un prestataire spécialisé, prestataire de l'organisateur du scrutin. La solution est ensuite installée sur une infrastructure qui sera exposée sur Internet pour permettre aux électeurs de voter. Suivant les situations, cette infrastructure peut être sous la responsabilité de l'organisateur du scrutin ou d'un prestataire, ce qui nécessite de définir

précisément les conditions d'exploitation et d'accès à la solution (incluant les procédures et les responsabilités contractuelles et légales). Les clés nécessaires aux mécanismes cryptographiques sont générées et distribuées conformément aux procédures de la solution de vote.

- Un ou des secrets d'authentification sont transmis aux électeurs, soit par le prestataire, soit par l'organisateur du scrutin, soit par un sous-traitant spécifiquement chargé de la gestion de l'authentification.
- Le bureau électoral contrôle l'intégrité et la bonne configuration du système de vote avant le début du scrutin, ainsi que la vacuité des urnes et des listes d'émargement.

Pendant le vote

- Lorsqu'un électeur se présente, la solution l'authentifie, contrôle son droit à voter et présente les choix de vote en fonction de la configuration de l'élection.
- L'électeur réalise son choix, son bulletin de vote est formé sur un équipement connecté à Internet, qui réalise les opérations visant à garantir le secret du scrutin et l'intégrité du suffrage exprimé. La solution de vote réalise l'émargement et enregistre son bulletin dans l'urne électronique.
- La solution fait l'objet d'une surveillance active pendant le scrutin par le bureau électoral. Elle peut également permettre aux électeurs ou à des tiers (observateurs, experts ou auditeurs) de vérifier certaines informations, comme la présence de bulletins dans l'urne.
- À la clôture du scrutin, la solution de vote ne doit plus permettre de voter.

Après la période de vote

- Sous l'autorité du bureau électoral, la solution réalise le dépouillement et affiche les résultats.
- La solution peut également permettre aux électeurs ou à des tiers (observateurs, experts ou auditeurs) de vérifier certaines informations attestant du respect des principes fondamentaux qui commandent les opérations électorales.

3.2.2 Enjeux de la numérisation des opérations

Dans sa délibération de 2026 [72], la CNIL rappelle que le recours au vote par correspondance électronique doit s'inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales concernées : le secret du scrutin sauf pour les scrutins publics, le caractère personnel du vote, le caractère libre du vote, la sincérité des opérations électorales, l'intégrité des suffrages exprimés, l'accès au vote pour tous les électeurs, la surveillance effective du vote et la possibilité de contrôle *a posteriori* de l'élection par un juge. De ces principes découlent les objectifs de sa délibération.

Attention

Un système de vote électronique ne peut pas être appréhendé comme un système d'information classique, car ces principes doivent être mis en œuvre par des moyens qui peuvent être compromis *y compris par l'entité qui les opère, et qui peut retirer un bénéfice de cette compromission* (par exemple influencer le résultat). De plus, le secret du scrutin peut rendre difficile la détection des cas de compromission.

En lien avec ces principes, les points suivants doivent ainsi être pris en compte pour estimer les risques liés à la mise en place d'un système de vote électronique.

Secret du scrutin

Dans le cadre du vote par correspondance électronique, les bulletins de vote sont dématérialisés. Afin d'assurer le secret du scrutin, le système de vote peut *par exemple* utiliser un mécanisme de chiffrement asymétrique. Dans ce cas, il réalise le chiffrement local du suffrage avec une clé publique unique, commune à tous les électeurs (appelée dans ce cas clé publique de l'élection), qui fait partie de la configuration de l'élection. Ensuite le bulletin (chiffré du suffrage) est transmis à un serveur de vote lequel intègre ce bulletin dans une urne électronique. Le dépouillement s'effectue dans ce cas notamment en déchiffrant les données contenues dans l'urne (ou une somme de ces données) grâce à la clé privée de l'élection.

Une particularité importante du vote par correspondance électronique est la numérisation conjointe de l'authentification des électeurs et du traitement des bulletins. Lors d'un vote à l'urne, ces opérations sont réalisées par les membres du bureau de vote et de manières indépendantes : contrôle d'une pièce d'identité et de l'inscription sur la liste électorale, mise sous enveloppe du bulletin anonyme et ajout dans l'urne de l'enveloppe. Il est alors impossible, ou très difficile, de relier les bulletins présents dans l'urne physique aux électeurs.

Dans le cadre du vote par correspondance électronique, le système de vote est à la fois responsable d'authentifier l'électeur, de générer le bulletin de vote à partir de son suffrage, de stocker ce bulletin et de le dépouiller. Il est donc possible que le système de vote permette l'établissement d'un lien entre l'identité de l'électeur et son suffrage, portant ainsi atteinte au secret du scrutin. Pour s'assurer que le secret du scrutin est respecté, une solution de vote par correspondance électronique doit garantir l'étanchéité entre l'identité de l'électeur et l'expression de son vote.

Vérifiabilité individuelle et universelle

Lorsque le vote à l'urne a lieu dans un bureau de vote, la simplicité et la visibilité des moyens utilisés (isoloir, urne transparente [5], surveillance effective par le bureau de vote) favorisent la compréhension des opérations par les électeurs et la confiance dans le résultat. Le vote à l'urne permet aussi à tout électeur ou observateur d'assister au scrutin et d'en contrôler visuellement la bonne tenue. Proposer un équivalent à ces moyens dans le cadre du vote par correspondance électronique est toujours un sujet de recherche actif, car les systèmes de vote (et la cryptographie nécessaire au secret du scrutin) sont complexes, difficiles à comprendre et à vérifier.

Afin de s'en approcher, deux notions de vérifiabilité ont été proposées [31, 43]. D'une part, la vérifiabilité individuelle qui signifie que l'électeur peut contrôler que son bulletin a été enregistré

5. En France, dans le cadre des élections politiques.

dans l'urne, d'autre part, la vérifiabilité universelle qui signifie que tout le monde doit pouvoir constater que le résultat proclamé (le nombre de voix pour chaque option de vote) correspond au contenu de l'urne. Ces notions intègrent la notion de vérifiabilité de la légitimité, qui signifie que tout le monde doit pouvoir vérifier que les bulletins proviennent d'électeurs légitimes. Ensemble, ces deux notions mettent en œuvre le principe fondamental d'indépendance logicielle : il doit être possible de vérifier la validité du résultat d'une élection sans reposer sur l'hypothèse que le système de vote est de confiance.

Transparence

Même si les mécanismes déployés pour assurer le secret et la vérifiabilité sont complexes, il est nécessaire d'être transparent sur leur choix, leur utilisation et leur mise en œuvre. La transparence signifie qu'il existe un support accessible publiquement (par exemple une page Web accessible sans restriction depuis Internet) dans lequel ces informations sont disponibles. Cette transparence concerne en particulier les mécanismes cryptographiques utilisés pour traiter le suffrage de l'électeur, depuis l'expression du vote jusqu'au dépouillement, ainsi que le protocole de vote mis en œuvre [6].

Surveillance

Pour tous les modes de scrutin, il est nécessaire de détecter et d'alerter de tout événement pouvant altérer la sincérité des opérations électorales. Ces événements peuvent relever de dysfonctionnements ou d'actes de malveillance (fraude).

Pour le vote par correspondance électronique, cette surveillance se traduit par de la journalisation (la collecte des journaux d'événements) et de la supervision du système de vote. Ce besoin de surveillance est amplifié par la durée de la période de vote, souvent plusieurs jours, ainsi que par la centralisation de l'infrastructure : une attaque sur le serveur de vote aura potentiellement un impact sur une proportion élevée d'électeurs (contrairement à un incident dans un bureau de vote lors lors d'un vote à l'urne dont les électeurs se répartissent sur plusieurs bureaux de vote). Cette surveillance peut impliquer des acteurs techniques (administrateurs et exploitants) et non techniques (membres du bureau électoral), voire des tiers (observateurs, experts ou auditeurs).

Sécurité de l'équipement et de l'environnement de l'électeur

Une autre particularité importante du vote par correspondance électronique est l'impossibilité de garantir la sécurité de l'équipement connecté à Internet (ordinateur, mobile multifonction, etc.) que l'électeur utilise pour voter, ainsi que son environnement. L'équipement peut être vulnérable à des attaques en écoute passive ou en intrusion active, visant à divulguer ou modifier le suffrage de l'électeur. L'environnement peut également être vulnérable à des attaques visant à divulguer ou modifier les données transmises du serveur de vote vers l'équipement (en particulier le client de vote) ou de l'équipement vers le serveur de vote (en particulier le bulletin de vote).

De plus, le vote n'étant pas réalisé dans un isoloir comme pour le vote à l'urne, l'électeur peut être victime de coercition, c'est-à-dire de vote sous contrainte. Le risque d'achat de vote est également amplifié pour ce mode de scrutin (comme pour le vote par correspondance non électronique). Ces

6. Selon le principe fondamental de Kerckhoffs.

deux risques font l'objet de recherche active et les solutions proposées pour y répondre sont complexes et n'ont pas de maturité suffisante. En particulier, certaines solutions mises en œuvre dans d'autres pays reposent sur le revote (la faculté de pouvoir voter plus d'une fois à un même scrutin) pour couvrir ces risques. Cette possibilité n'est pas usuelle pour les votes par correspondance électronique en France, encore très calqués sur le vote à l'urne. De plus, elle nécessite d'identifier précisément les bulletins des électeurs, ce qui peut aller à l'encontre de l'étanchéité entre l'identité de l'électeur et l'expression de son vote si des mécanismes cryptographiques appropriés ne sont pas utilisés.

Transition vers la cryptographie post-quantique

Les mécanismes de cryptographie asymétrique utilisés aujourd'hui sont vulnérables à la menace quantique. Ainsi, le but de la transition post-quantique est de les remplacer par des mécanismes de cryptographie asymétrique dite post-quantique, supposée résistante à des attaques qui seraient réalisées sur un ordinateur classique et sur un ordinateur quantique.

Dans le contexte du vote par correspondance électronique, un éventuel ordinateur quantique pourrait porter atteinte au secret du scrutin pour les élections organisées actuellement, par des attaques de type *store now, decrypt later* : conservation des bulletins émis maintenant par les électeurs et déchiffrement plus tard avec un ordinateur quantique [7]. Un éventuel ordinateur quantique, une fois disponible, pourrait également porter atteinte aux autres principes fondamentaux qui commandent les opérations électorales.

Pendant la transition post-quantique, l'hybridation est recommandée par l'ANSSI [13, 15]. L'hybridation combine l'utilisation d'un mécanisme de cryptographie asymétrique classique éprouvé, mais vulnérable à des attaques quantiques, et celle d'un mécanisme de cryptographie asymétrique supposé résistant aux attaques quantiques, mais pour lequel l'assurance de robustesse vis-à-vis des attaques réalisées à l'aide d'ordinateurs classiques et quantiques est moindre.

Dans le contexte du vote par correspondance électronique, l'élaboration de tels mécanismes fait l'objet d'une recherche académique active, complexifiée par les propriétés à atteindre, telles que présentées dans ce guide. A l'heure de la rédaction de ce guide, ces mécanismes ne sont pas mis en œuvre par les systèmes de vote.

Attention

Le présent guide fournit des recommandations techniques pour la mise en œuvre du vote par correspondance électronique, pour les scrutins dont on cherche à protéger le secret uniquement à court terme (par exemple, pour les 5 prochaines années). En effet, les scrutins dont le secret doit être garanti à moyen ou long terme (au-delà de 5 ans) nécessitent des mesures de sécurité complémentaires non abordées dans ce guide.

7. Le déchiffrement des bulletins ne permet pas seul de porter atteinte au secret du scrutin. Il faut également conserver d'autres éléments permettant d'associer les bulletins aux électeurs.

3.3 Objectifs de sécurité fixés par la CNIL

Il n'existe pas de labellisation de solutions de vote par correspondance électronique [8]. Cependant, le lien entre vote et données à caractère personnel (dont les opinions politiques et syndicales) est évident. Le vote par correspondance électronique a donc fait l'objet d'une attention particulière de la CNIL dès 2003. La CNIL a publié plusieurs recommandations successives [9]. La dernière version précise notamment certains objectifs de sécurité relatifs à la vérifiabilité et à la transparence.

Afin de répondre aux problématiques spécifiques à la numérisation des opérations de vote, la CNIL propose depuis la délibération de 2019 une démarche axée sur l'estimation des risques organisationnels et techniques. Cette démarche est reprise pour la version de 2026.

Cette estimation des risques conduit à l'affectation d'un niveau au scrutin : le **niveau 1** pour un scrutin de risque faible, le **niveau 2** pour un scrutin de risque modéré et le **niveau 3** pour un scrutin comportant des risques significatifs. La Section 3 de la recommandation de la CNIL [72] décrit les différents niveaux et fournit des exemples de types de scrutins pour chaque niveau. Ces descriptions et ces exemples sont repris dans ce guide aux Sections 4.1, 4.2, 4.3. La Section 4 de la recommandation de la CNIL [72] précise que le responsable de traitement « identifie le niveau correspondant à sa situation en fonction des risques organisationnels et techniques soulevés par son scrutin ».

À chaque niveau est associée une liste d'**objectifs de sécurité** que devrait atteindre une solution de vote, déclinant les principes fondamentaux qui commandent les opérations électorales (3.2.2). L'objet du présent document est de proposer des recommandations pour approfondir les objectifs fixés par la délibération. Ces recommandations n'ont pas de caractère normatif.

Attention

Les prestataires sont libres de proposer tous moyens qu'ils estiment adéquats pour répondre à chacun des objectifs de sécurité fixés par la CNIL. L'expertise indépendante de la solution devra évaluer si les moyens proposés apportent une réponse pertinente.

Les prestataires qui le souhaitent peuvent faire parvenir à l'ANSSI une description des moyens qu'ils estiment adéquats et qu'ils proposent dans leur solution afin de répondre aux objectifs de sécurité fixés par la CNIL. L'ANSSI pourra les étudier et mettre à jour, le cas échéant, le présent guide.

Les commentaires peuvent être adressés par e-mail à conseil.technique@ssi.gouv.fr.

8. Au contraire des machines à voter, qui font l'objet d'un agrément [75].
9. 2003 (https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000017653831/), 2010 (https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000023124205/), 2019 (https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038661239/) et 2026 [72].

4
Recommandations pour la mise en œuvre des objectifs de sécurité fixés par la CNIL

Chaque section du présent chapitre est consacrée à un des trois niveaux de scrutin identifiés par la CNIL. La section rappelle d'abord la description de ce niveau, et en décrit le modèle de confiance associé. Elle liste ensuite l'ensemble des objectifs de sécurité associés au niveau.

Puis les recommandations sont présentées par objectif. Des commentaires sont fournis, donnant des explications sur l'objectif ou sur les recommandations. **Ces commentaires sont à visée pédagogique**.

Attention

Pour chacune des recommandations de ce guide, l'utilisation du verbe *devoir* est volontairement plus prescriptive que la formulation *il est recommandé*. Dans les deux cas, les recommandations n'ont aucun caractère normatif.

Recommandations de niveau 1, 2 ou 3

Les recommandations sont directement associées à un niveau de scrutin, figuré par le nombre d'étoile (★). Ces recommandations sont **cumulables** : toutes les recommandations du niveau 1 (respectivement des niveaux 1 et 2) doivent être prises en compte pour le niveau 2 (respectivement pour le niveau 3). Ces recommandations sont présentées de la manière suivante :

Recommandation de niveau 1

Cette recommandation répond à un objectif de sécurité de niveau 1 fixé par la CNIL **et s'applique aux scrutins de niveaux 1, 2 et 3**.

Recommandation de niveau 2

Cette recommandation répond à un objectif de sécurité de niveau 2 fixé par la CNIL **et s'applique aux scrutins de niveaux 2 et 3**.

Recommandation de niveau 3

Cette recommandation répond à un objectif de sécurité de niveau 3 fixé par la CNIL **et s'applique aux scrutins de niveau 3**.

Pour répondre aux recommandations, les encadrés suivants mettent en avant des exemples de pratiques compatibles avec tous les niveaux de scrutin :

Pratique compatible avec les scrutins de niveaux 1, 2 ou 3

Cette pratique est compatible avec les scrutins de niveaux 1, 2 et 3 car elle peut être adaptée aux risques et menaces plus élevés de ces niveaux. Aussi **il est recommandé que l'organisateur du scrutin privilégie l'usage d'un système de vote qui met en œuvre cette pratique**.

Recommandations complémentaires

Des recommandations complémentaires sont fournies en Section 4.4. Elles proposent des mesures allant au-delà de celles requises par les objectifs de sécurité de niveau 3. Elles peuvent être retenues pour répondre à des risques identifiés par une analyse de risque (objectif 3-01).

Ces recommandations renforcent la sincérité des opérations électorales et le secret du scrutin contre une compromission du serveur de vote, limitant la confiance à accorder au serveur et à ses administrateurs. Ces recommandations sont plus difficiles à mettre en œuvre car elles peuvent nécessiter l'intervention de tiers indépendants ou des moyens informatiques supplémentaires. Ces recommandations sont accompagnées d'un signe plus (+) et présentées de la manière suivante :

Recommandation complémentaire au niveau 3

En fonction de l'analyse des risques (3-01), cette recommandation propose une mesure complémentaire à celles requises par les objectifs de sécurité de niveau 3.

La liste récapitulative des recommandations est disponible en page 125.

Risques non couverts

Enfin, la Section 4.5 expose des risques qui ne sont pas complètement couverts par les recommandations de ce guide. Ces risques concernent des attaquants qui peuvent disposer de ressources importantes (comme un État), de complicités internes chez l'organisateur ou son prestataire, ou présenter de fortes motivations (dont la déstabilisation).

4.1 Objectifs de sécurité de niveau 1

Définition de la CNIL [72] : **Niveau 1 (risques faibles)** : *les sources de menace (parmi les votants, les organisateurs du scrutin, les fournisseurs du système de vote, les personnes extérieures, etc.) ont peu de ressources et peu de motivations. L'administrateur (ou les administrateurs) du système d'information n'est ni votant, ni candidat. Il est considéré comme neutre par toutes les parties. Ce niveau s'applique principalement pour les scrutins qui impliquent un faible nombre de votants, qui se déroulent dans un cadre non conflictuel, qui ne révèlent ni les orientations politiques, ni les opinions syndicales des personnes, et à l'issue desquels les personnes élues auront, le cas échéant, peu de pouvoirs. Il peut par exemple s'agir d'élections de représentants de parents d'élèves dans les établissements scolaires, ou de scrutins organisés au sein d'associations locales.*

Modèle de confiance : Pour ce niveau, le système de vote, le prestataire et l'organisateur du scrutin sont supposés de confiance. Le risque de compromission externe (au système de vote) est jugé faible, et une assurance minimale est apportée en suivant des recommandations basiques. Enfin, aucune transparence ni aucun élément de preuve ne sont requis pour ce niveau. La Figure 4 présente les objectifs de sécurité de la CNIL correspondant à des scrutins de niveau 1.

1-01	Mettre en œuvre une solution technique et organisationnelle ne présentant pas de faille majeure (faille publiée par l'éditeur et/ou rendue publique par des tiers) et respectant les recommandations de déploiement et d'utilisation émanant de l'éditeur du système de vote électronique retenu et de l'ANSSI.
1-02	Définir le vote d'un électeur comme une opération comportant de manière indivisible la validation de son suffrage, l'enregistrement du bulletin dans l'urne, l'émargement et la délivrance d'un récépissé.
1-03	Authentifier les électeurs en s'assurant que les risques majeurs liés à une usurpation d'identité sont réduits de manière significative. Si une procédure de recouvrement des accès à la plateforme de vote est mise en place, s'assurer que celle-ci n'abaisse pas le niveau de sécurité de l'authentification des électeurs.
1-04	Assurer la stricte confidentialité de l'expression du vote dès la création du bulletin sur le poste du votant.
1-05	Assurer la stricte confidentialité et l'intégrité du bulletin pendant son transport.
1-06	Assurer, de manière organisationnelle et/ou technique, la stricte confidentialité et l'intégrité du bulletin pendant son traitement et son stockage dans l'urne jusqu'au dépouillement.
1-07	Assurer l'étanchéité totale entre l'identité de l'électeur et l'expression de son vote (le contenu déchiffré de son bulletin de vote) pendant toute la durée de traitement, y compris lors du dépouillement et, le cas échéant, lors de l'archivage des données du scrutin.
1-08	Renforcer la confidentialité des bulletins de vote en répartissant le secret permettant leur dépouillement, notamment au sein du bureau électoral, et garantir la possibilité de dépouillement à partir d'un seuil de secret déterminé.
1-09	Assurer que le dépouillement d'une urne n'est réalisable que sur l'ensemble des bulletins qu'elle contient et après la fermeture du scrutin.
1-10	Assurer l'intégrité du système de vote électronique et la vacuité de l'urne et de la liste d'émargement avant l'ouverture du scrutin.
1-11	Assurer que le bon dépouillement de l'urne peut être vérifié *a posteriori*.

FIGURE 4 – Objectifs de sécurité de niveau 1

Attention

Bien que le système de vote, le prestataire et l'organisateur du scrutin eux-mêmes puissent porter atteinte aux principes fondamentaux qui commandent les opérations électorales, ces risques de compromission interne sont *acceptés* comme résiduels au niveau 1.

Objectif n° 1-01

Mettre en œuvre une solution technique et organisationnelle ne présentant pas de faille majeure (faille publiée par l'éditeur et/ou rendue publique par des tiers) et respectant les recommandations de déploiement et d'utilisation émanant de l'éditeur du système de vote électronique retenu et de l'ANSSI.

Le système de vote est constitué de l'ensemble des moyens physiques (matériels) et logiques (logiciels) utilisés pour le vote électronique et la solution de vote comprend le système de vote ainsi que ses procédures d'exploitation et de sécurisation.

La sincérité des opérations électorales dépend de la qualité de la solution mise en œuvre, sur les aspects organisationnels comme techniques. Si certaines mesures ne sont pas mises en œuvre ou respectées, la solution de vote peut contenir des failles de sécurité.

D'un côté, l'organisateur du scrutin est responsable du respect des procédures prévues pour les parties qu'il exécute et de la mise en place de la surveillance effective du scrutin par le bureau électoral. Il doit également maîtriser les développements spécifiques qu'il demande, et leurs impacts sur la sécurité. De l'autre, le prestataire doit fournir les procédures adaptées, choisir des mécanismes cryptographiques conformes aux référentiels de l'ANSSI, cartographier le système de vote et le maintenir à jour.

R1 ★

Fournir des procédures détaillées de déploiement et d'utilisation du système de vote

Le prestataire doit fournir des procédures détaillées, notamment pour le déploiement, l'utilisation et la surveillance du système, par le bureau électoral, pour la tenue des cérémonies ou pour la gestion des supports contenant des clés cryptographiques (1-08).

Ces procédures doivent être revues par l'expert indépendant, au sens de la délibération de la CNIL [72].

Une fois revues et stabilisées, ces procédures doivent être respectées par l'ensemble des acteurs impliqués, notamment l'organisateur du scrutin et le prestataire, et tout écart doit être identifié.

Afin de répondre aux besoins du scrutin, l'organisateur peut demander au prestataire des développements spécifiques qui seront ajoutés à la solution standard. Ces ajouts peuvent dégrader la sécurité de la solution de vote existante. Il faut donc que ces développements soient clairement identifiés et spécifiés. Leurs impacts sur la sécurité doivent être analysés.

R2 ★

Identifier et analyser les développements spécifiques

L'organisateur du scrutin doit identifier et analyser les développements spécifiques à ajouter à la solution de vote standard proposée par le prestataire. Si une analyse de risque est réalisée (3-01), elle doit tenir compte de ces développements.

Ces développements spécifiques peuvent notamment concerner :

- Le recouvrement des secrets d'authentification (1-03).
- Le pastillage (1-04, Annexe E).
- La prise en compte de configurations d'élection particulières, par exemple à cause du découpage électoral, à cause de contraintes réglementaires (par exemple le vote avec rature autorisé dans le Code du travail [10]) ou bien à cause de statuts particuliers (autorisant par exemple le vote pondéré ou le panachage).
- La production de statistiques spécifiques sur le déroulement du scrutin pour sa surveillance (2-02).
- La prise en compte de format spécifique de données pour la configuration de l'élection ou l'exportation des émargements et des résultats.
- En fonction de l'analyse des risques (3-01), la vérification d'une signature numérique externe (Section 4.4), la séparation en modules d'une application monolithique, en prévision de l'installation de ces modules sur des machines distinctes (Section 4.4), ou l'intégration de mécanismes cryptographiques post-quantiques (Section 4.5).

Les mécanismes cryptographiques constituent le cœur d'une solution de vote par correspondance électronique. Ils doivent être conformes à l'état de l'art.

R3 ★

Assurer la conformité des mécanismes cryptographiques

Le système de vote doit mettre en œuvre des mécanismes cryptographiques conformes aux *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* [18].

Ces mécanismes peuvent notamment faire partie de la liste suivante :

- La génération et la dérivation des secrets d'authentification (1-03).
- Le chiffrement et la signature numérique des données transmises aux sous-traitants assurant l'envoi des secrets d'authentification aux électeurs (1-03).
- La protection des communications, par exemple avec le protocole TLS (1-03, 1-05).
- Le chiffrement des bulletins (1-04).
- Les mécanismes assurant la validité des suffrages et des bulletins (1-06).
- La signature numérique et le chaînage des bulletins pour en détecter les modifications illégitimes (1-06).
- L'accumulation, le mélange cryptographique et le déchiffrement des bulletins (1-07, 1-11).
- La fragmentation de la clé privée de déchiffrement et le chiffrement des fragments (1-08).
- Le contrôle d'intégrité des données (1-10).

10. https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006072050/

Pour les niveaux 2 et 3, cette liste peut être complétée avec les mécanismes identifiés à ces niveaux (2-02, 2-07, 2-08, 2-09, 3-02, 3-04).

Comme évoqué explicitement par l'objectif 1-01, la sécurité de la solution repose également sur l'absence de failles connues et directement exploitables par un attaquant. Pour cela, l'ensemble des matériels et logiciels composant le système de vote doit être connu et cartographié, puis être maintenu « à jour », en condition de sécurité.

R4 ⋆

Cartographier le système de vote

Le prestataire doit réaliser une cartographie de l'ensemble des composants techniques du système de vote.

La cartographie doit couvrir au minimum les équipements réseaux (y compris les moyens de communication externes tels que les accès à Internet), l'envoi des moyens d'authentification aux électeurs, les équipements de sécurité, les logiciels d'infrastructure (serveurs Web, serveurs applicatifs), le ou les logiciels exécutés sur l'équipement de l'électeur, les composants logiciels tiers (bibliothèques, cadriciels - ou *framework*, y compris ceux relatifs à la cryptographie), les bases de données, les serveurs et leurs systèmes d'exploitation, les solutions de virtualisation et les supports de stockage (de masse ou amovible), en particulier pour les fragments de la clé privée de l'élection.

R5 ⋆

Maintenir à jour les composants du système de vote

Le prestataire de vote doit utiliser les dernières versions stables (incluant les correctifs de sécurité) des composants du système de vote, tels que cartographiés.

Pratique compatible avec les scrutins de niveaux 1, 2 ou 3

Une mise en œuvre conforme de la recommandation R5⋆ est de considérer la classification standardisée CVSS [56] pour les failles de sécurité (none, low, medium, high, critical). Il est recommandé que tous les composants du système de vote, ainsi que leurs dépendances, ne contiennent aucune faille publique de criticité supérieure ou égale à **medium**. De même, il est recommandé que tous les composants du système de vote exposés sur Internet ne contiennent aucune faille publique de criticité supérieure ou égale à **low**. Cela inclut notamment les terminaisons TLS exposées aux électeurs (1-05) et le client de vote (1-04).

À l'approche du début du scrutin, un équilibre doit être trouvé entre prise en compte des mises à jour de sécurité récentes et stabilité du système de vote.

L'absence de faille majeure sur le système de vote peut être finalement vérifiée par un audit de configuration. Cet audit peut être réalisé dans le cadre de l'expertise indépendante (au sens de la délibération de la CNIL [72]), ou plus fréquemment à l'initiative du prestataire.

R6 ★

Auditer la configuration du système de vote

Le système de vote doit être audité, notamment sur les points suivants :

- Les versions des composants du système de vote.
- La correction des failles de sécurité.
- La conformité des mécanismes cryptographiques aux *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* [18].
- La conformité des mécanismes d'authentification des électeurs, en particulier lors du transfert des secrets à des sous-traitants (1-03).
- La conformité des liaisons TLS (1-05).
- Le développement, le durcissement, l'administration et la sécurité physique du système de vote (2-06).
- Sur demande de l'organisateur du scrutin, la conformité au cahier des charges du projet.

L'audit doit être réalisé en conformité avec les recommandations de la CNIL ([72], section 7) : pour chaque scrutin de niveau 3, et éventuellement en réutilisant des expertises réalisées dans les 12 derniers mois pour les scrutins de niveau 2 et dans les 24 derniers mois pour les scrutins de niveau 1.

Pour cet audit, il est possible de faire appel à un *Prestataire d'Audit de la Sécurité des Systèmes d'Information* (PASSI), qualifié par l'ANSSI. Dans ce cas, le prestataire doit être qualifié pour les activités suivantes : audit d'architecture, audit de configuration, audit de code source, test d'intrusion, audit organisationnel et physique. Le *Référentiel d'exigences* [20] présente les exigences pour la qualification et la page Web *Produit et services qualifiés* [5] fournit la liste des PASSI mise à jour.

Pour aller plus loin

L'objectif 1-01 est renforcé par l'objectif 2-06 relatif à la mise en œuvre de mesures de sécurité recommandées par les éditeurs et l'ANSSI.

Objectif n° 1-02

Définir le vote d'un électeur comme une opération comportant de manière indivisible la validation de son suffrage, l'enregistrement du bulletin dans l'urne, l'émargement et la délivrance d'un récépissé.

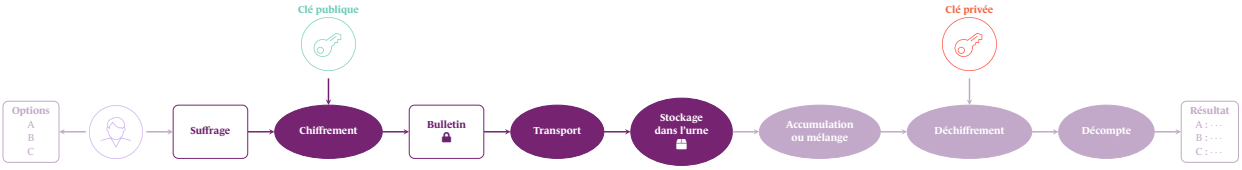

FIGURE 5 – Traitements de l'opération de vote

Cet objectif signifie qu'une fois que l'électeur a validé son choix, l'ensemble des traitements qui suivent, réalisés par le système de vote, réussit ou bien échoue complètement : enregistrer le bulletin dans l'urne, ajouter l'électeur à l'émargement et délivrer un récépissé. En cas de succès, l'électeur reçoit un récépissé matérialisant sa participation. En cas d'échec, il peut recommencer et voter à nouveau.

Comme illustré à la Figure 5, l'opération de vote est composée des traitements suivants :

- La validation par l'électeur de son choix (choix d'un candidat par exemple) dans le client de vote. L'expression du vote de l'électeur constitue le suffrage.
- La génération par le client de vote du bulletin contenant le suffrage chiffré, la génération éventuelle des preuves à divulgation nulle de connaissance associées au bulletin et éventuellement la signature numérique du bulletin, telles que prévues dans le protocole de vote (1-04, 2-09).
- Le transport du bulletin, du client de vote au serveur de vote (1-05).
- La validation du bulletin par le serveur de vote, y compris la vérification des éventuelles preuves associées au bulletin (1-06) et la vérification de son éventuelle signature.
- Le stockage du bulletin dans l'urne électronique, ou dans les urnes en cas de pastillage (1-04, Annexe E), et la mise à jour de la liste d'émargement par le serveur de vote.
- La délivrance d'un récépissé de vote à l'électeur.

Les recommandations suivantes concernent la fiabilité des traitements de l'opération de vote, dès lors que l'électeur a exprimé son choix.

R7 ★

Enchaîner les traitements de l'opération de vote sans discontinuité

Dès lors que l'électeur a exprimé et validé son choix, le système de vote doit enchaîner l'ensemble des traitements constituant l'opération de vote sans discontinuité jusqu'à l'achèvement du dernier traitement, la délivrance d'un récépissé.

L'échec d'un traitement entraîne l'échec de toute l'opération et, a contrario, la réussite de l'opération n'est possible que de par le succès de chacun des traitements unitaires.

Les traitements les plus critiques sont le dépôt du bulletin dans l'urne et l'émargement, qui doivent être réalisés de manière indissociable afin d'assurer leur cohé-

rence [11].

Enfin, comme explicitement demandé dans l'objectif 1-02, le système de vote doit délivrer un récépissé à l'électeur.

R8 ★

Délivrer un récépissé à l'électeur

Le système de vote doit délivrer un récépissé à l'électeur à la fin de l'opération de vote.

Il est acceptable que le récépissé soit généré dans le cadre de l'opération de vote, puis délivré de façon asynchrone par messagerie électronique.

Le récépissé doit contenir les informations requises par la réglementation encadrant le scrutin (suivant les cas, un identifiant de l'électeur, l'horodatage de l'opération de vote ainsi que le ou les scrutins auxquels l'électeur a participé). Le récépissé ne doit pas contenir d'informations liées au bulletin de l'électeur, informations présentes dans la preuve de vote (R58★★).

Une propriété importante d'un système de vote par correspondance électronique est la propriété appelée receipt-freeness (R30★), également expliquée en Annexe D. Malgré son nom, cette propriété ne signifie pas *sans récépissé*, mais exprime que les données publiées par le système de vote ne portent pas atteinte au caractère personnel du vote.

Pour aller plus loin

L'objectif 1-02 est renforcé par l'objectif 2-04 qui concerne la mise en place d'alerte en cas de dysfonctionnement dans l'opération de vote, l'objectif 1-07 qui concerne l'étanchéité entre l'identité de l'électeur et l'expression de son vote ainsi que l'objectif 2-07 qui concerne la preuve de vote.

11. Dans le contexte des bases de données SQL, cela correspond à une transaction.

Objectif n° 1-03

Authentifier les électeurs en s'assurant que les risques majeurs liés à une usurpation d'identité sont réduits de manière significative. Si une procédure de recouvrement des accès à la plateforme de vote est mise en place, s'assurer que celle-ci n'abaisse pas le niveau de sécurité de l'authentification des électeurs.

L'usurpation d'identité d'un électeur permet de soumettre un vote à sa place. Cela porte atteinte au caractère personnel du vote ainsi qu'à la sincérité des opérations électorales et peut entraîner l'annulation du scrutin. L'authentification des électeurs limite ces risques majeurs, car elle doit assurer que seuls les électeurs **légitimes** peuvent effectivement voter. De plus, l'authentification rend plus difficile la « délégation » de vote (une autre personne vote à la place de l'électeur).

Cependant, la nature des moyens d'authentification disponibles et leur caractère dédié au scrutin sont souvent contraints. Dans le contexte du vote par correspondance électronique, par nature événementiel, il peut être très complexe de déployer en tant que moyen d'authentification un facteur de possession ou un facteur inhérent dédié au vote.

Information

Comme indiqué dans le guide *Authentification multifacteurs et mots de passe* [22], un facteur de possession doit être un *équipement* attribué à chaque électeur. Cet équipement peut être une carte à puce contenant une clé privée, un mobile de type smartphone contenant une application implémentant un protocole d'authentification basé sur un OTP, une carte SIM d'un téléphone mobile comportant des données d'identification, etc. De même, un facteur inhérent est de nature biométrique.

Ainsi, ni une messagerie électronique ni une messagerie instantanée ne peuvent être considérées comme des facteurs de possession (tout au plus elles peuvent être considérées comme des facteurs de connaissance - du mot de passe d'accès à ces messageries).

Ainsi, il est souvent plus simple de recourir à un facteur de connaissance, qui est un secret d'authentification. Il est possible de s'appuyer soit sur une solution d'authentification existante adaptée aux contraintes du scrutin, soit sur un secret d'authentification dédié au scrutin.

Recours à une solution d'authentification existante

Le recours à une solution d'authentification existante, indépendante du scrutin, peut assurer l'authentification de l'électeur. Ce type de solution présente trois intérêts pour l'autorité organisatrice (et pour les électeurs) :

- Elle renforce l'authentification sans la complexifier par la manipulation d'un nouveau secret.
- Elle évite la génération et l'envoi à l'électeur d'un secret d'authentification, dans un contexte où les canaux d'envoi utilisables sont rares ou difficiles à sécuriser.
- Parce que le secret associé à cette solution peut donner accès à des ressources (données ou applications) plus larges que celles liées au scrutin, l'électeur (rationnel) hésitera davantage à partager ce secret avec un tiers lui proposant de voter à sa place. Ainsi cette mesure peut dissuader un électeur de vendre ou déléguer ses secrets d'authentification.

Lorsqu'une solution d'authentification existante, externe à la solution de vote, est utilisée, elle doit présenter des garanties suffisantes.

R9 ★

Utiliser une solution d'authentification externe présentant des garanties suffisantes

L'organisateur du scrutin doit s'assurer, qu'en cas de recours à une solution d'authentification externe, indépendante du scrutin, cette solution présente les garanties suivantes :

- Chaque électeur peut être authentifié. S'il faut utiliser plusieurs solutions différentes pour couvrir l'ensemble des électeurs, il faut toutes les intégrer au système de vote.
- Elle est accessible sur l'ensemble des équipements depuis lesquels les électeurs sont autorisés à voter. En particulier, si le recours à un équipement personnel est autorisé, alors la solution doit être exposée et utilisable depuis Internet.
- La réglementation et les conditions générales d'utilisation de la solution permettent son utilisation dans le contexte du scrutin.
- La solution renvoie une identité pivot qui peut être mise en relation de façon univoque avec la liste des électeurs du système de vote.
- L'engagement de disponibilité de la solution est compatible avec les besoins du scrutin.

Il existe plusieurs types de solutions d'authentification externes à la solution de vote. Toutes ne sont pas adéquates :

- **Les solutions d'authentification proposées par des fournisseurs de services numériques en ligne** (réseaux sociaux par exemple). Les identités associées à ces services sont souvent déclaratives, voire sans aucun lien avec l'état civil de la personne physique. Elles ne peuvent pas être considérées comme suffisantes pour s'assurer que « les risques majeurs liés à une usurpation d'identité sont réduits de manière significative ».
- **Les solutions d'authentification internes à l'entité organisatrice du scrutin** (SSO d'entreprise par exemple). Ces solutions permettent au quotidien l'authentification des utilisateurs du système d'information de l'entité, et peuvent être considérées comme suffisamment robustes pour le contexte du vote - mais elles sont cependant à la portée de l'organisateur et de ses administrateurs. En revanche, si le vote doit être possible depuis un équipement personnel (cela dépend de la réglementation applicable), il faut que la solution d'authentification soit également disponible depuis un équipement personnel.
- **Les solutions d'identité numérique** certifiées (telles que FranceConnect+) ou non certifiées (telles que FranceConnect). Elles assurent un lien avec l'état civil de l'utilisateur avec des niveaux d'assurance variables, parfois évalués par l'ANSSI. La section suivante étudie les possibilités et les limitations de ce type de solution.

Identité numérique et niveau de scrutin

Cette section décrit le rôle que peuvent jouer les identités numériques dans l'authentification des

électeurs, seules ou en complément d'autres solutions. Chaque identité numérique offre un *niveau de garantie*, relatif à un règlement européen nommé eIDAS [21]. Il y a trois niveaux : faible, substantiel et élevé.

Le niveau faible est le niveau par défaut, notamment quand le service n'a pas fait l'objet d'une certification. Pour les niveaux substantiel et élevé, le service doit faire l'objet d'une certification par l'ANSSI, selon le *Référentiel d'exigences de sécurité pour les moyens d'identification électronique* [3] [12].

Une identité numérique de niveau faible (non évaluée) ne peut pas, seule, répondre aux objectifs 1-03 et 2-08. Il n'est acceptable d'y recourir qu'en complément d'un secret d'authentification dédié au scrutin (R10★).

Une identité numérique de niveau substantiel ou élevé (évaluée par l'ANSSI) pourrait répondre seule aux objectifs 1-03 et 2-08, sans recours à un secret dédié au scrutin. Cette affirmation doit cependant être tempérée, car elle ne tient compte que de l'aspect sécurité. En pratique, les identités numériques de niveau substantiel ou élevé sont disponibles, en France, à travers le service FranceConnect+. Le recours à ce service est contraint par plusieurs facteurs :

- La réglementation [13] restreint les services, notamment privés, qui peuvent utiliser FranceConnect.
- La même réglementation précise que l'utilisation de FranceConnect doit être facultative pour l'usager. En pratique, l'organisateur du scrutin devrait proposer une alternative aux électeurs, et donc maintenir une autre solution d'authentification.

Recours à une solution d'authentification dédiée au scrutin

Vu les contraintes liées au recours à une solution d'authentification externe (R9★), il peut être plus pratique et plus réaliste d'avoir recours à une solution d'authentification dédiée au scrutin. Dans ce cas, la recommandation suivante peut être utilisée à la place de la recommandation R9★.

R10 ★

Utiliser à défaut un secret d'authentification dédié au scrutin

À défaut d'une solution d'authentification existante adaptée, le système de vote doit utiliser un facteur de connaissance, tel qu'un mot de passe, dédié au scrutin, pour authentifier les électeurs.

Attention

Les deux recommandations R9★ et R10★ sont applicables aux scrutins de niveau 1 mais doivent être complétées pour les scrutins de niveaux 2 et 3 : une déclinaison (au niveau 2) est proposée dans ce guide, via la recommandation R60★★. Autrement dit, pour les scrutins de niveaux 1, l'utilisation d'un seul secret d'authentification est suffisante ; pour les scrutins de niveaux 2 et 3, il est recommandé d'utiliser deux secrets d'authentification, transmis par deux canaux différents.

12. Une certification selon ce référentiel assure une conformité au référentiel eIDAS et un niveau de sécurité vérifié par l'ANSSI (audits PASSI).
13. Voir notamment l'Arrêté du 8 novembre 2018 relatif au téléservice dénommé « FranceConnect » créé par la direction interministérielle du numérique et du système d'information et de communication de l'État [70].

Conformité des mécanismes d'authentification aux guides de l'ANSSI

De façon générale, les mécanismes d'authentification (c'est-à-dire l'ensemble des moyens permettant de générer, transmettre et vérifier les secrets d'authentification) devraient être conformes aux recommandations du guide *Authentification multifacteurs et mots de passe* [22].

R11 ⋆

Assurer la conformité des mécanismes d'authentification des électeurs

Le système de vote doit mettre en œuvre des mécanismes d'authentification des électeurs conformes aux recommandations du guide *Authentification multifacteurs et mots de passe* [22]. Notamment :

- Les secrets d'authentification doivent être générés avec suffisamment d'entropie.
- Les secrets d'authentification doivent être générés au sein d'un environnement maîtrisé afin de prévenir tout accès illégitime à ces secrets.
- Les fichiers contenant ces secrets doivent être protégés en confidentialité et en intégrité.
- Les secrets d'authentification doivent être envoyés aux électeurs en garantissant leur confidentialité et leur intégrité (ils ne doivent notamment pas être envoyés en clair).
- Le système de vote doit vérifier l'authentification des électeurs au moyen de données dérivées à partir des secrets d'authentification, et non directement au moyen de ces secrets.
- Le système de vote doit être protégé contre les attaques par recherche d'authentifiants (attaques par force brute, par arrosage de mots de passe ou *password spraying*, par saisie d'authentifiants volés ou *credential stuffing* [2]). Ce type de protection peut s'appuyer sur un délai d'attente incompressible et croissant après plusieurs présentations de mots de passe erronés ou sur un CAPTCHA.
- Le système de vote doit imposer une déconnexion automatique de l'électeur après un certain délai d'inactivité. L'électeur doit être informé de la déconnexion.

Transmission des secrets d'authentification à des sous-traitants

Cette section concerne la transmission des secrets d'authentification à des sous-traitants, qui vont réaliser l'envoi de ces secrets aux électeurs. Il est nécessaire de protéger ces secrets contre la divulgation et la modification, car ces attaques peuvent porter atteinte au caractère personnel du vote et à la sincérité des opérations électorales, en permettant à des personnes non légitimes de voter. De nombreux sous-traitants, en particulier ceux spécialisés dans l'envoi d'e-mail et de SMS, exposent des API, qui peuvent être directement appelées par le système de vote (voir la page Web de la CNIL *Interfaces de Programmation d'Application - API* [38]).

R12 ⋆

Protéger la transmission des secrets d'authentification à des sous-traitants

Lorsque le système de vote transmet des secrets d'authentification à des sous-traitants pour leur envoi aux électeurs (postal, par messagerie électronique, par SMS ou par

messagerie instantanée), cette transmission doit assurer la confidentialité et l'intégrité des secrets.

Une fois les secrets d'authentification des électeurs transmis au sous-traitant, celui-ci doit les protéger en confidentialité et en intégrité jusqu'à leur envoi aux électeurs. Le sous-traitant ne doit pas communiquer ces secrets à d'autres entités. Une fois les secrets envoyés, le sous-traitant doit supprimer toute copie de ces secrets (le sous-traitant n'a pas à conserver les secrets pour un éventuel recouvrement, voir la recommandation R14★).

Cette transmission peut être réalisée par échange de fichiers ou en utilisant des API exposées par le sous-traitant.

Pratique compatible avec les scrutins de niveaux 1, 2 ou 3

Lorsque la transmission des secrets d'authentification à des sous-traitants s'effectue par échange de fichiers :

- Les fichiers doivent être chiffrés dès leur constitution et ne doivent être déchiffrables que par le sous-traitant destinataire au moyen d'un mécanisme de chiffrement conforme aux *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* [18].
- Les fichiers doivent être protégés en intégrité au moyen d'une signature numérique ou une empreinte numérique, conforme aux *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* [18].
- Les fichiers doivent être protégés en confidentialité et en intégrité avant leur échange (la confidentialité et l'intégrité des fichiers ne doivent pas être assurées par le moyen réalisant l'échange).

Pratique compatible avec les scrutins de niveaux 1, 2 ou 3

Lorsque la transmission des secrets d'authentification à des sous-traitants utilise des API exposées par ces sous-traitants :

- Le sous-traitant doit suivre l'état de l'art et les bonnes pratiques pour le déploiement d'API, par exemple les recommandations de l'*OWASP API Security Project* [80].
- La transmission doit être protégée par TLS, conformément aux *Recommandations de sécurité relatives à TLS* [8].
- Le secret d'authentification (mot de passe ou jeton d'authentification) utilisé pour accéder aux API doit être robuste, non prédictible, et dédié au scrutin, ou, à défaut, être renouvelé régulièrement.
- Le secret d'authentification (mot de passe ou jeton d'authentification) utilisé pour accéder aux API ne doit pas être commun aux environnements de production, de développement et de recette.
- Si les appels à l'API sont journalisés, les événements du journal ne doivent pas

contenir les secrets d'authentification (secrets d'authentification des électeurs et secret d'authentification à l'API).

Envoi des secrets d'authentification aux électeurs

La Recommandation R11★ demande la protection en confidentialité et en intégrité du secret d'authentification lors de son envoi à l'électeur. En pratique, les moyens d'envoi à disposition des organisateurs (email, SMS) n'offrent pas cette protection.

Une alternative à l'envoi du secret est l'envoi d'un lien à usage unique permettant à l'électeur de prendre connaissance du secret d'authentification, ou de le définir. Ce lien apporte une meilleure protection en confidentialité ; il permet de détecter un usage illégitime du lien et un accès illégitime au secret.

Cependant, les liens à usage unique peuvent être difficiles à utiliser, notamment par les électeurs moins familiers avec le numérique, et empêcher ces derniers de voter. L'organisateur du scrutin doit trouver un équilibre entre la sécurité de l'authentification et une participation plus élevée, les deux aspects contribuant à la sincérité des opérations électorales [14].

Information

Des alternatives au SMS apparaissent avec le standard RCS (*Rich communication service*) ou les messageries instantanées :

- RCS permet en théorie le chiffrement de bout en bout des échanges. Cependant, ce chiffrement n'est pas toujours mis en œuvre, en particulier entre équipements d'écosystèmes différents (Android et iOS), ou lorsque l'échange n'est pas entre deux individus, mais entre un émetteur institutionnel et un individu. Le gain en sécurité attendu grâce au chiffrement n'est donc pas toujours réalisé.
- Certaines messageries instantanées indiquent mettre en œuvre du chiffrement de bout en bout. Cependant, imposer l'usage d'une application particulière à l'ensemble des électeurs peut être difficile ou impossible. De plus, comme pour RCS, le chiffrement de bout en bout n'est pas toujours mis en œuvre pour les envois institutionnels.

Par ailleurs, pour le choix des canaux d'envoi des secrets d'authentification, il est préférable de privilégier les canaux hors de portée de l'organisateur du scrutin et des parties ayant un intérêt dans le scrutin (les candidats par exemple), afin de limiter le risque d'usurpation d'identité.

Par exemple, pour l'élection de représentants du personnel, des risques d'usurpation d'identité existent dans les cas suivants :

- Un secret envoyé sur une adresse de messagerie professionnelle peut être accédé par un administrateur de la messagerie.
- Un secret envoyé par SMS sur un téléphone professionnel peut être accédé par un administrateur de la flotte des téléphones à travers le service de gestion des terminaux mobiles - MDM.

14. Si des électeurs qui veulent voter ne sont pas en mesure de le faire, le résultat ne reflétera pas la volonté des électeurs.

- Un secret sous pli (remis en main propre ou distribué par le courrier interne) peut être accédé par une personne chargée de la distribution.

Cependant, en pratique, identifier et utiliser un canal d'envoi hors de portée de l'organisateur du scrutin est parfois difficile.

Un tel canal peut reposer sur des données personnelles, telles qu'une adresse email personnelle ou un numéro de téléphone personnel. Pour commencer, l'organisateur ne dispose pas forcément de ces données pour l'ensemble des électeurs avant le vote. Le système de vote peut alors collecter ces données pendant la session de vote (saisie d'un numéro de téléphone pour recevoir un code à usage unique). Dans ce cas, l'apport à la sécurité de l'authentification est limité par la valeur purement déclarative des données [15]. Enfin, l'usage de données personnelles peut être jugé disproportionné, typiquement dans le contexte des élections professionnelles (voir l'avis de la CNIL sur la page Web *Élections professionnelles et données personnelles : questions–réponses* [37], question 10).

L'organisateur doit donc trouver un équilibre entre :

- d'une part le risque d'usurpation d'identité dû à un accès aux secrets d'authentification par l'organisateur du scrutin ou des parties ayant un intérêt dans le scrutin,
- et d'autre part l'apport réel à la sécurité de l'usage des données personnelles, ainsi que le risque d'usage disproportionné de ces données.

À titre illustratif, la CNIL propose, pour le contexte des élections professionnelles, la liste des canaux d'envoi suivants (voir la page Web *Élections professionnelles et données personnelles : questions–réponses* [37], question 8) :

- la remise en main propre sur le lieu de travail ;
- l'envoi sur une adresse e-mail professionnelle ou un téléphone professionnel ;
- l'envoi postal au domicile de l'électeur ;
- le dépôt sur un intranet professionnel ou un coffre-fort numérique accessible au seul salarié. Dans le contexte de la fonction publique d'État, l'Espace Numérique Sécurisé de l'Agent Public (ENSAP) [52] est un exemple d'un tel coffre-fort numérique, accessible seulement par les agents.

Cette liste peut servir de base de réflexion pour estimer les risques en fonction du contexte de l'élection. Une fois les risques identifiés, ils peuvent être traités à travers l'analyse des risques (R62★★★).

Envoi des secrets d'authentification par courrier postal ou remise en main propre

L'envoi par courrier postal ou la remise d'un courrier en main propre doit assurer la confidentialité du secret d'authentification qui figure dans le courrier. La protection de la confidentialité est particulièrement importante si le courrier est traité ou distribué au sein de l'entité organisatrice du scrutin (remise en main propre). À défaut de la garantir, il doit être possible de détecter les atteintes à cette confidentialité pour que l'électeur puisse demander le recouvrement d'un secret qui aurait pu être compromis.

15. Ce mécanisme de saisie d'un numéro peut être vu comme un moyen de limiter la fraude, en contraignant chaque électeur à disposer d'un numéro unique. L'efficacité de cette mesure doit être analysée, car il existe sur Internet des services mettant à disposition des numéros à usage unique pour recevoir des SMS.

R13 ★

Assurer la confidentialité des secrets transmis par courrier papier

En cas d'envoi par courrier postal ou de remise en main propre d'un moyen d'authentification, il est recommandé que le système de vote assure la confidentialité de ce moyen en empêchant la lecture du secret sans ouverture de l'enveloppe.

Pratique compatible avec les scrutins de niveaux 1, 2 ou 3

Une réponse à la recommandation R13★ peut être réalisée par un des mécanismes suivants :

- Masquage du secret sous une couche opaque à gratter.
- Masquage du secret sous une languette opaque à décoller.
- Masquage du secret par un carré opaque situé ailleurs sur le courrier, mais au-dessus lors du pliage.
- Utilisation d'une enveloppe avec un motif de brouillage sur sa face intérieure.

Les deux premiers mécanismes permettent en outre une détection de lecture du secret. Les deux derniers n'ont pas cette propriété, mais coûtent généralement moins cher.

Le système de vote peut également recourir à des enveloppes sécurisées pour l'envoi postal, principalement pour rendre plus difficile l'accès au secret sans détection de la compromission par l'électeur. Ces enveloppes combinent en général un caractère indéchirable et opaque avec un témoin d'ouverture.

Recouvrement des secrets d'authentification

Le recouvrement permet aux électeurs qui n'ont pas reçu ou qui ont perdu un secret d'authentification (notamment celui spécifique au système de vote) d'en obtenir un nouveau. Le recouvrement est un moyen essentiel pour assurer la participation des électeurs, car la non-réception, la perte et l'oubli d'un secret d'authentification sont des risques avérés.

R14 ★

Fournir un recouvrement de secret d'authentification n'abaissant pas la sécurité

Lorsque le système de vote met en place un recouvrement des secrets d'authentification, celui-ci ne doit pas abaisser la sécurité de l'envoi initial de ces secrets.

Par défaut, les canaux utilisés pour l'envoi initial des secrets doivent être réutilisés pour le recouvrement.

Le système de vote doit notifier l'électeur du recouvrement de son secret d'authentification par tous les canaux disponibles n'ayant pas servi au recouvrement. Cette notification permet à l'électeur d'être informé d'une demande de recouvrement illégitime faite en son nom.

Le système de vote doit rendre **inutilisables** les secrets d'authentification précédents.

Dans certains cas, la réutilisation du canal d'origine pour le recouvrement n'est pas possible : soit pour des contraintes temporelles (par exemple si le premier envoi a été réalisé par courrier postal), soit parce que l'adresse de messagerie ou le numéro de téléphone n'est pas ou plus valable (l'électeur n'a plus accès à cette boite aux lettres ou a changé de numéro de téléphone). L'organisateur du scrutin doit trouver un équilibre entre une sécurité stricte et interdire la saisie d'une nouvelle adresse, limitant le risque d'usurpation d'identité, et favoriser la participation en autorisant la saisie d'une nouvelle adresse de messagerie ou d'un nouveau numéro de téléphone. Dans le cas où cette seconde option est choisie, la recommandation suivante s'applique.

R15 ★

Réduire les risques liés à l'impossibilité d'usage du canal d'origine

Si l'organisateur du scrutin veut favoriser la participation en autorisant la saisie d'un nouveau moyen d'adressage (nouvelle adresse de messagerie, nouveau numéro de téléphone) pour le recouvrement d'un secret d'authentification :

- Il est recommandé que le système de vote authentifie l'électeur de façon renforcée, par exemple en utilisant une authentification externe (système d'authentification de l'entité à laquelle appartiennent les électeurs, identité numérique [39], vérification d'identité à distance [4]) ou grâce à un défi-réponse conforme au guide *Authentification multifacteurs et mots de passe* [22].
- Si l'authentification renforcée réussit, si le défi réussit ou encore si l'absence d'authentification renforcée ou de défi-réponse est jugée acceptable par l'organisateur du scrutin, le système de vote permet à l'électeur de saisir un nouveau moyen d'adressage.
- Le système de vote électronique renouvelle le secret et l'envoie vers le nouveau moyen d'adressage.

Pour aller plus loin

L'objectif 1-03 est renforcé par l'objectif 2-04 qui concerne la mise en place d'alertes, notamment en cas de détection d'attaque par recherche d'authentifiants et par l'objectif 2-08 qui concerne la mise en place de deux moyens d'authentification.

Objectif n° 1-04

Assurer la stricte confidentialité de l'expression du vote dès la création du bulletin sur le poste du votant.

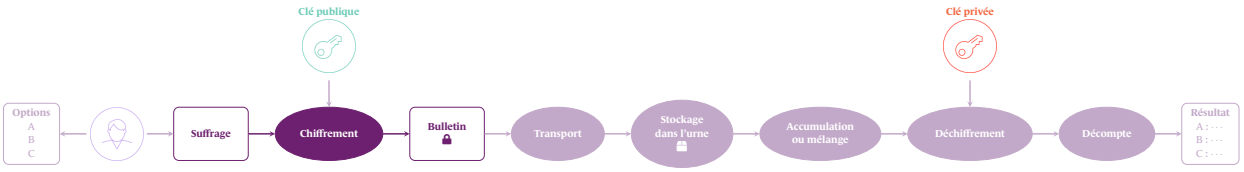

FIGURE 6 – Création du bulletin

Comme illustré en Figure 6, lorsque l'électeur saisit son suffrage sur le client de vote, ce dernier crée un bulletin contenant le suffrage chiffré.

D'abord, le client de vote doit protéger le suffrage en confidentialité. Ensuite, le client de vote peut également détecter les caractéristiques techniques de l'équipement connecté à Internet utilisé par l'électeur pour voter. Enfin, le chiffrement du suffrage doit s'appuyer sur des mécanismes cryptographiques adaptés aux besoins du vote par correspondance électronique. Le cas particulier du pastillage est évoqué en fin de section.

Protection en confidentialité du suffrage au sein du client de vote

La protection du secret du suffrage implique d'abord que le chiffrement doit avoir lieu dès que possible. En effet, comme expliqué à la Section 3.2.2, le secret du scrutin est un des principes fondamentaux qui commandent les opérations électorales. C'est donc au client de vote, et pas au serveur de vote, de réaliser ce chiffrement.

De plus, pour protéger le suffrage pendant sa manipulation en mémoire sur l'équipement utilisé par l'électeur, le client de vote ne doit pas faire appel à des ressources tierces qui ne seraient pas maîtrisées [16]. Ainsi, le recours à un service de CAPTCHA d'un site Web tiers et le recours à un service de CDN, en particulier pour des ressources statiques mais critiques comme les scripts **JavaScript**, doivent être proscrits.

La création du bulletin (le suffrage chiffré) implique l'usage d'aléa par le client de vote (R18★), dont la confidentialité doit être assurée comme le suffrage. Ainsi le client de vote manipule deux données sensibles en confidentialité : le suffrage de l'électeur et l'aléa utilisé pour son chiffrement. Ces données sensibles ne doivent pas être stockées temporairement (par exemple dans un fichier), être mises en cache, accédées par d'autres onglets du navigateur ou retrouvées dans l'historique.

R16 ★

Assurer la confidentialité du suffrage dans le client de vote

Le système de vote doit présenter aux électeurs un client de vote assurant la confidentialité du suffrage, notamment :

- Le client de vote doit réaliser le chiffrement du suffrage au moyen de mécanismes cryptographiques implémentés conformément au *Guide de sélection d'al-*

16. Maîtrisées au sens d'hébergées sur le serveur de vote et auditées (par exemple soumises à l'expertise indépendante, au sens de la délibération de la CNIL [72]).

gorithmes cryptographiques [10]. En particulier, lorsque le client de vote fait appel à des bibliothèques cryptographiques (par exemple du navigateur), ces bibliothèques doivent être éprouvées et les appels à ces bibliothèques doivent être réalisés conformément aux préconisations des fournisseurs de ces bibliothèques.

- Le client de vote ne doit pas faire appel à des ressources tierces en ligne non maîtrisées.
- Le client de vote doit maîtriser l'accès aux données sensibles (suffrage, aléa utilisé pour le chiffrement du suffrage) au sein et en dehors du navigateur, puis assurer leur effacement dès que le bulletin est créé.

Le client de vote est communément un script JavaScript intégré à la page Web présentée à l'électeur et exécuté par le navigateur utilisé par l'électeur. Dans ce contexte, les *Recommandations pour la mise en œuvre d'un site Web : maîtriser les standards de sécurité côté navigateur* [11] s'appliquent, en particulier celles recommandant de ne pas stocker de données sensibles dans les cookies ou les bases de données IndexedDB. Ces recommandations concernant le stockage peuvent être complétées au moyen de mécanismes influençant le cache, expliqués en Annexe F.

Détection des caractéristiques techniques de l'équipement utilisé par l'électeur

Comme exposé en Section 3.2.2, la sécurité de l'environnement et de l'équipement utilisé par l'électeur ne peuvent pas être garantis, car l'électeur doit pouvoir soumettre son vote depuis n'importe quel équipement (connecté à Internet). Aussi les risques de divulgation ou de modification du suffrage doivent être estimés. Concernant l'équipement, il est possible de mettre en place des mécanismes de détection de certaines de ses caractéristiques techniques et ainsi prévenir le lancement du client de vote si le risque de compromission est trop élevé.

Attention

La détection de caractéristiques techniques de l'équipement utilisé par l'électeur pourrait permettre d'identifier un équipement compromis par un attaquant de niveau basique. Cependant un équipement compromis par un attaquant de niveau élevé pourrait toujours contourner ces détections (c'est-à-dire renvoyer un faux positif).

Le risque de compromission de l'équipement utilisé par l'électeur fait ainsi partie de la liste des « risques non couverts » par les recommandations de ce guide (voir Section 4.5).

R17 ⋆

Détecter les caractéristiques techniques de l'équipement utilisé par l'électeur

Lorsque le client de vote est un JavaScript intégré à la page Web présentée à l'électeur et exécuté par son navigateur, il est recommandé que le système de vote intègre des mécanismes de détection des caractéristiques techniques de l'équipement utilisé par l'électeur pour réaliser son vote (version de navigateur, moteur JavaScript, activation de la sandbox, mode debug). Ces détections doivent permettre au client de vote :

- D'empêcher son exécution sur un navigateur ou un moteur JavaScript incompa-

tibles car n'ayant pas les caractéristiques requises. Par exemple, le client de vote ne devrait pas s'exécuter sur une version de navigateur ayant une CVE connue permettant la fuite de données ou n'implémentant pas une version de TLS compatible (1-05).

- De lier son exécution à l'activation de mécanismes d'isolation afin de restreindre la modification ou la récupération illégitime de données.
- D'empêcher son exécution lorsque le mode debug du moteur JavaScript ou du navigateur est activé, afin de restreindre la modification ou la récupération illégitime de données.

L'Annexe F fournit des exemples de mécanismes de détection, basés sur la construction d'heuristiques dédiées.

Information

Il est envisageable de considérer un client de vote de type « client lourd » ou application mobile, installés sur l'équipement de l'électeur.

Protection du suffrage par des mécanismes cryptographiques

Le mécanisme cryptographique assurant la confidentialité du suffrage est le chiffrement qui, dans le contexte du vote par correspondance électronique, doit persister jusqu'au dépouillement, pendant lequel le déchiffrement est réalisé. En conséquence, il ne peut pas reposer exclusivement sur le chiffrement des échanges réseau par le protocole TLS mis en œuvre par le serveur de vote (objectif 1-06).

Il est nécessaire d'utiliser un mécanisme de chiffrement probabiliste. En effet, si le mécanisme de chiffrement est déterministe – c'est-à-dire qu'il n'utilise pas d'aléa – deux suffrages identiques donneraient le même bulletin. Cela porterait atteinte au secret du scrutin car il serait possible d'identifier les électeurs ayant le même suffrage.

Il est également nécessaire d'utiliser un mécanisme de chiffrement non-malléable : un mécanisme de chiffrement est malléable s'il est possible d'effectuer des opérations sur les données chiffrées (par exemple, les multiplier entre elles) pour obtenir le chiffrement d'autres données que celles initialement chiffrées. Si le chiffrement est malléable, il est possible de modifier le bulletin afin qu'il contienne une autre donnée que le suffrage exprimé par l'électeur, le bulletin restant valide [17]. Cela porterait atteinte à l'intégrité des suffrages exprimés et à la sincérité des opérations électorales.

Enfin, le consensus actuel est d'utiliser un mécanisme de chiffrement asymétrique. En effet, ce type de mécanisme permet la transmission d'une même donnée publique (la clé publique de l'élection) aux électeurs, aux fins de chiffrement de leur suffrage, et le contrôle de la donnée secrète associée (la clé privée de l'élection), lors du déchiffrement des bulletins. Cette asymétrie renforce le secret du scrutin, à l'inverse d'un mécanisme de chiffrement symétrique.

17. Les notions de *validité du suffrage* et de *validité du bulletin* sont expliquées dans le contexte du mécanisme de chiffrement ElGamal en Annexe C.

R18 ★

Utiliser un chiffrement asymétrique probabiliste non-malléable

Le client de vote doit effectuer le chiffrement du suffrage de l'électeur au moyen d'un mécanisme de chiffrement asymétrique probabiliste non-malléable, dès que l'électeur a validé son suffrage.

Dans ce cas, le client de vote doit être en mesure de générer suffisamment d'aléa localement et de le combiner si nécessaire avec une source d'aléa externe maîtrisée (par exemple en provenance du serveur de vote).

Pratique compatible avec les scrutins de niveaux 1, 2 ou 3

Le mécanisme de chiffrement asymétrique ElGamal, basé sur le groupe multiplicatif d'un corps fini ou basé sur le groupe des points rationnels d'une courbe elliptique est asymétrique et probabiliste. Utilisé seul, ce mécanisme est malléable et il est nécessaire de le composer avec un autre mécanisme afin de le rendre non-malléable. La composition avec des preuves à divulgation nulle de connaissance assure cette non-malléabilité et fournit un mécanisme conforme à la recommandation R18★ (voir également l'Annexe A).

Conformité du mécanisme de chiffrement des suffrages vis-à-vis d'autres mécanismes cryptographiques

		Conforme pour Niveau		
	Choix de mécanisme cryptographique	1	2	3
Confidentialité de l'expression du vote	Chiffrement symétrique, déterministe ou malléable	✗	✗	✗
	Chiffrement asymétrique, probabiliste et non-malléable	✓	✓	✓
Étanchéité entre l'identité de l'électeur et l'expression de son vote	Pas de mélange cryptographique	✗	✗	✗
	Mélange cryptographique	✓	✓	✗
	Mélange cryptographique vérifiable	✓	✓	✓
	Accumulation	✓	✓	✓
Répartition du secret permetttant le dépouillement	Pas de partage du secret	✗	✗	✗
	Partage de secret à seuil	✓	✓	✓
Dépouillement vérifiable *a posteriori*	Nouvelle exécution du déchiffrement et du décompte	✓	✓	✗
	Déchiffrement vérifiable	✓	✓	✓

FIGURE 7 – Conformité des mécanismes cryptographiques par niveau

Le choix du mécanisme de chiffrement des suffrages peut avoir un impact sur d'autres mécanismes cryptographiques mis en œuvre pour répondre à d'autres objectifs, notamment l'étanchéité entre l'identité de l'électeur et l'expression de son vote (1-07), la répartition du secret permettant le déchiffrement (1-08) et la vérification du dépouillement *a posteriori* (1-11 et 3-02).

En effet, suivant le mécanisme de chiffrement des suffrages choisi, les mécanismes cryptographiques répondant aux objectifs ci-dessus peuvent être mis en œuvre de manière sûre et efficace. La Figure 7 précise la conformité des mécanismes cryptographiques présentés dans ce guide, par niveau de scrutin.

Il est donc recommandé d'analyser précisément la conformité du mécanisme de chiffrement des suffrages à ces mécanismes, et ne pas limiter l'analyse à la seule fonction de chiffrement. Cette analyse doit permettre au prestataire d'identifier les scrutins que sa solution peut réaliser.

R19 ★

Analyser la conformité du mécanisme de chiffrement des suffrages

Il est recommandé que le prestataire analyse la conformité du mécanisme de chiffrement des suffrages avec les mécanismes cryptographiques suivants :

- L'accumulation des bulletins.
- Le mélange cryptographique (et le mélange vérifiable) des bulletins.
- Le partage de secret à seuil.
- Le déchiffrement vérifiable.

Il est recommandé que cette analyse s'appuie sur des travaux académiques de référence, c'est-à-dire publiés à des conférences ou dans des journaux scientifiques reconnus en cryptographie ou en sécurité informatique.

Pratique compatible avec les scrutins de niveaux 1, 2 ou 3

Le mécanisme de chiffrement ElGamal, basé sur le groupe multiplicatif d'un corps fini ou basé sur le groupe des points rationnels d'une courbe elliptique et composé avec une preuve à divulgation nulle de connaissance de l'aléa, est asymétrique, probabiliste et non-malléable. Il permet de mettre en œuvre de manière sûre et efficace les mécanismes d'accumulation, de mélange cryptographique (y compris vérifiable), de déchiffrement vérifiable, de partage de secret à seuil (y compris vérifiable) décrits dans ce guide.

Il est donc envisageable d'utiliser un système de vote basé sur le mécanisme ElGamal pour le chiffrement du suffrage pour **les niveaux de scrutin 1, 2 et 3**, ainsi que pour les recommandations complémentaires exposées à la Section 4.4.

L'annexe A fournit de nombreux exemples de systèmes de vote s'appuyant sur le mécanisme de chiffrement ElGamal.

Mise en œuvre du pastillage

Le pastillage consiste en une association d'attributs à un électeur, qui doivent suivre l'expression de son vote, pour fournir des résultats complémentaires pour des scrutins dits « indirects ». La notion de pastillage et sa mise en œuvre sont expliquées en Annexe E. Deux solutions sont possibles :

- associer les attributs au suffrage de l'électeur et à *les chiffrer avec ce suffrage*, ou
- *ne pas* associer les attributs au suffrage, mais les associer au bulletin (le chiffré du suffrage).

Comme exposé en Annexe E, la mise en œuvre du pastillage associant les attributs au suffrage plutôt qu'au bulletin comporte un risque majeur sur le secret du scrutin et la sincérité des opérations électorales, aussi elle doit être écartée. De plus, comme exposé à la Section 6 « Information des

électeurs et accessibilité du vote » de la délibération de la CNIL [72], l'électeur doit être informé des traitements réalisés dans ce contexte.

R20 ★

Utiliser un pastillage associant les attributs au bulletin

En cas de pastillage, le système de vote doit associer les attributs de l'électeur au bulletin chiffré. De plus :

- La mise en œuvre du pastillage ne doit pas porter atteinte au secret du scrutin.
- L'électeur doit être informé sur les scrutins indirects auxquels il participe et des moyens lui permettant de vérifier la prise en compte de son suffrage pour tous ces scrutins.
- La mise en œuvre du pastillage doit permettre de détecter tout déplacement d'un bulletin d'une urne à l'autre.

Pratique compatible avec les scrutins de niveaux 1, 2 ou 3

Le mécanisme de chiffrement asymétrique ElGamal, basé sur le groupe multiplicatif d'un corps fini ou basé sur le groupe des points rationnels d'une courbe elliptique, permet de réaliser l'accumulation et le mélange cryptographique des bulletins, tout en étant composable avec des preuves à divulgation nulle de connaissance assurant la validité du bulletin et du suffrage (voir l'objectif 1-06). Ce mécanisme est donc adapté pour la mise en œuvre du pastillage consistant à associer les attributs au bulletin, car le contexte de ces preuves peut être complété avec ces attributs. Avec cette composition, il est ainsi possible de détecter un éventuel déplacement de bulletin qui porterait atteinte au secret du scrutin [50].

L'organisateur du scrutin peut donc envisager **les niveaux de scrutin 1, 2 et 3** avec un système de vote basé sur le mécanisme ElGamal pour le chiffrement du suffrage, lorsqu'un pastillage est mis en œuvre.

Pour aller plus loin

L'objectif 1-04 est renforcé par l'objectif 1-07 relatif à l'étanchéité entre l'identité de l'électeur et l'expression de son vote, les objectifs 1-11 et 3-02 relatifs à la vérification du dépouillement, l'objectif 2-09 relatif à la publication du protocole de vote et l'objectif 3-05, relatif à la publication du code source du client de vote.

Objectif n° 1-05

Assurer la stricte confidentialité et l'intégrité du bulletin pendant son transport.

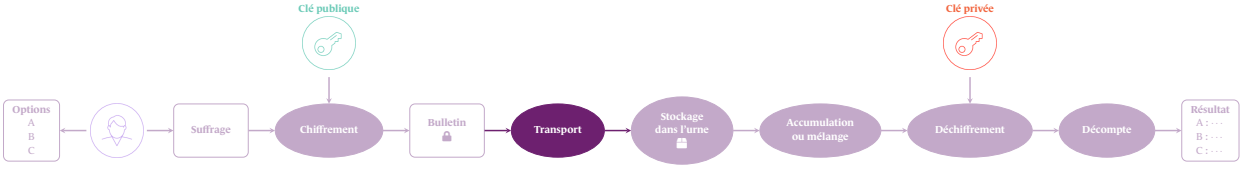

FIGURE 8 – Transport du bulletin

Cet objectif concerne le transport du bulletin depuis le client de vote jusqu'à l'urne électronique hébergée par le serveur de vote, illustré en Figure 8. La solution la plus répandue consiste à mettre en place une liaison TLS entre ces deux composants.

Or, en pratique, la liaison TLS établie par le client de vote se termine bien en amont de l'urne électronique : sur des composants de sécurité tels qu'un pare-feu applicatif [18], ou sur le serveur Web assurant la couche de présentation d'une architecture « trois tiers » [19].

Dans ce cas, il est nécessaire de s'assurer qu'une ou plusieurs autres liaisons TLS prennent le relais de la liaison établie par le client de vote, pour assurer la confidentialité et l'intégrité du bulletin jusqu'à l'urne. Pour cela, il faut déjà connaître et décrire le chemin du bulletin jusqu'à l'urne électronique.

R21 ★

Décrire le chemin du bulletin jusqu'à l'urne électronique

Le prestataire doit décrire précisément le chemin complet du bulletin de vote du client de vote jusqu'à l'urne électronique.

Cette description doit contenir l'ensemble des composants du système de vote par lesquels transitent les bulletins une fois qu'ils sont traités par la terminaison TLS exposée aux électeurs, jusqu'à l'urne électronique, notamment en cas de mise en œuvre d'une architecture « trois tiers ». Le prestataire doit identifier clairement les terminaisons TLS et les points de rupture du protocole sur ce chemin.

La mise en œuvre de chaque liaison TLS doit être conforme aux *Recommandations de sécurité relatives à TLS* [8]. De plus :

- Un élément de configuration important d'une liaison TLS est de mettre en place (ou non) l'authentification de la partie cliente : la partie serveur est nécessairement **authentifiée**, et des fonctions additionnelles permettent l'**authentification du client**, si nécessaire.
- Il peut exister un petit nombre d'électeurs utilisant des équipements ou des navigateurs obsolètes, reposant sur des versions du protocole TLS non conformes aux recommandations [8] [20],

18. Dans ce cas là, il s'agit d'un équilibre renforçant la protection du système de vote contre les attaques Web au prix d'une exposition plus grande du bulletin de vote.
19. Une architecture « trois tiers » sépare notamment la couche de présentation (le serveur Web et le serveur applicatif) et la couche d'*accès aux données* (la base de données). L'urne appartient à la couche d'accès aux données.
20. Ne pas utiliser SSLv2, SSLv3, TLS 1.0 et TLS 1.1. La version TLS 1.3 doit être prise en charge et privilégiée. La version TLS 1.2 est également acceptée sous condition de suivre les recommandations de [8].

ou bien n'implémentant pas des mécanismes cryptographiques récents. Malgré l'impact (minime) sur la participation, il est recommandé de conserver la stricte conformité au guide TLS et d'exclure de fait ces équipements et navigateurs obsolètes.

R22 ★

Protéger avec TLS les connexions initiées par le client de vote

Le système de vote doit mettre en place des liaisons TLS conformes aux *Recommandations de sécurité relatives à TLS* [8] pour l'ensemble des flux initiés par le client de vote. Le client de vote doit authentifier le serveur de vote grâce à un certificat (authentification simple).

La négociation des liaisons TLS doit être paramétrée de façon stricte et exclure les versions de TLS et les mécanismes cryptographiques obsolètes.

Lorsque le *Référentiel Général de Sécurité* [19] s'applique, le système de vote doit mettre en place un certificat conforme aux préconisations de ce référentiel [21].

Attention

Le recours à un service de CDN est à proscrire dès lors que ce service procéderait à un déchiffrement des flux entre le client de vote et le serveur de vote, ou servirait des ressources statiques mais critiques comme les Javascript.

R23 ★

Protéger les flux internes au système de vote par TLS à double authentification

Il est recommandé que le système de vote mette en place des liaisons TLS à double authentification (comportant l'authentification du serveur et l'authentification du client) conformes aux *Recommandations de sécurité relatives à TLS* [8] pour l'ensemble des flux sur le chemin entre la terminaison TLS exposée aux clients de vote et l'urne électronique.

21. Par exemple, l'obligation faite à l'article R.211-511 du code général de la Fonction publique pour les élections professionnelles de la fonction publique.

Objectif n° 1-06

Assurer, de manière organisationnelle et/ou technique, la stricte confidentialité et l'intégrité du bulletin pendant son traitement et son stockage dans l'urne jusqu'au dépouillement.

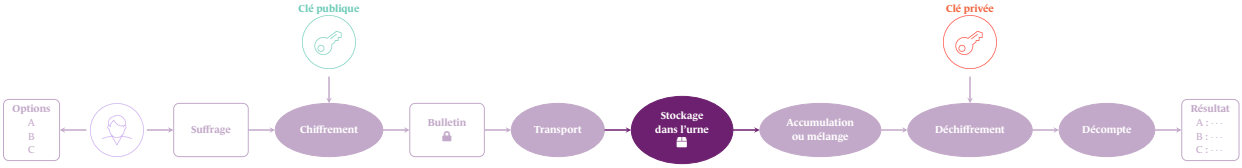

FIGURE 9 – Stockage du bulletin dans l'urne

Cet objectif concerne le traitement et le stockage du bulletin transmis par le client de vote de l'électeur, comme illustré en Figure 9.

Dans le modèle de confiance d'un scrutin de niveau 1, un attaquant peut transmettre des bulletins invalides qui pourraient porter atteinte à la sincérité des opérations électorales. Aussi il est nécessaire que le système de vote puisse se protéger dès ce niveau contre de telles attaques.

Validité du bulletin et validité du suffrage

Il est recommandé que le système de vote vérifie la validité du bulletin créé ainsi que la validité du suffrage contenu dans le bulletin. Sans ces vérifications, il est possible que le déchiffrement du bulletin renvoie un message d'erreur, ou bien que le déchiffrement renvoie une donnée non conforme à la configuration de l'élection.

Attention

En l'absence de mécanisme attestant de la validité du suffrage ou bien si cette validité n'est pas vérifiée lors de la réception du bulletin, il est possible d'insérer dans l'urne électronique un bulletin contenant un suffrage invalide. Cela peut avoir comme conséquence de compromettre la sincérité des opérations électorales.

Il est donc recommandé que la validité du bulletin et la validité du suffrage soient vérifiés directement à la réception du bulletin transmis par l'électeur, avant son insertion dans l'urne électronique. *A minima*, cette vérification peut porter sur le format du bulletin.

R24 ★

Vérifier la validité du bulletin et du suffrage

Il est recommandé que le système de vote mette en œuvre un mécanisme de vérification de la validité des bulletins transmis par les électeurs ainsi qu'un mécanisme de vérification du suffrage contenu dans le bulletin, sans divulguer le suffrage ni l'aléa utilisé pour le chiffrement.

Dans ce cas, le serveur de vote doit vérifier cette validité à la réception du bulletin et le rejeter si la vérification échoue.

En cas d'accumulation des bulletins (1-07) pour assurer l'étanchéité bulletin/suffrage, un mécanisme attestant de la validité du suffrage sans le divulguer est **obligatoire**.

Les Annexes A et B fournissent des exemples de mécanismes assurant la validité du bulletin et la validité du suffrage, adaptés au mécanisme de chiffrement ElGamal.

Disponibilité des bulletins

Une fois que les bulletins sont déposés dans l'urne, il est nécessaire de prévenir et détecter leur perte jusqu'au dépouillement, consécutive à un dysfonctionnement ou une erreur.

Information

La perte de données maximale admissible (PDMA) d'un système d'information est une durée qui mesure la fenêtre de temps avant un incident pendant laquelle des données pourraient être perdues.

La PDMA peut être nulle (0 seconde) si les données sont répliquées en temps réel, de façon synchrone, sur deux systèmes indépendants. Elle peut être de quelques minutes si la réplication est asynchrone, par exemple exécutée toutes les 5 minutes.

La PDMA peut également être infinie s'il n'existe aucune sauvegarde ou réplication du système d'information : en cas d'incident détruisant les données, elles sont irrémédiablement perdues.

La perte de données maximale admissible (PDMA) du système de vote devrait être nulle : aucun bulletin reçu par le système de vote ne devrait être perdu, quel que soit l'incident ou la panne qui touche le système de vote.

R25 ★

Fournir une PDMA nulle

Il est recommandé que le système de vote fournisse une PDMA nulle : aucun bulletin ne doit être perdu pendant le scrutin.

Cette recommandation doit être mise en œuvre dans un contexte adapté au niveau du scrutin. Pour des scrutins de niveau 1 ou 2, la réplication synchrone peut être réalisée sur deux systèmes au sein d'un même centre de données – on accepte alors le risque d'une perte des bulletins en cas d'incident majeur touchant ce centre de données. Pour des scrutins de niveau 3, une réplication synchrone entre deux centres de données distincts est requise, car elle couvre le risque de perte d'un centre de données suite à un incident majeur.

Information

La disponibilité des données par réplication est nécessaire mais pas suffisante pour que le système dans son ensemble soit hautement disponible. La disponibilité du système est abordée dans l'objectif 2-01.

Si le système de vote ne permet pas d'atteindre une PDMA nulle (réplication asynchrone), alors des bulletins peuvent être perdus. Dans ce cas, il est nécessaire de communiquer vers l'ensemble des électeurs sur le fait que des bulletins émis à une certaine période ont pu être perdus afin que ceux dont le ou les bulletins sont susceptibles d'avoir été perdus puissent à voter à nouveau.

Confidentialité et intégrité des bulletins

Une fois la disponibilité des bulletins assurée, il faut également assurer leur confidentialité et leur intégrité : créés par les électeurs, les bulletins ne doivent plus être modifiés et les accès à ces bulletins doivent être contrôlés. Pour cela, il est nécessaire de restreindre les accès au système de vote pendant le scrutin et de détecter la modification des bulletins.

R26 ★

Restreindre les accès techniques au système de vote pendant le scrutin

Le prestataire doit restreindre ses accès techniques au système de vote pendant le scrutin aux opérations de gestion et de maintenance strictement nécessaires au maintien en condition opérationnelle et en condition de sécurité du système de vote.

Information

Les accès techniques doivent également faire l'objet d'une journalisation au titre de la recommandation R38★, et d'alertes au titre de la recommandation R52★★.

R27 ★

Détecter la modification illégitime des bulletins

Le système de vote doit permettre de détecter toute perte ou modification illégitime des bulletins transmis par les électeurs, traités par le serveur de vote et stockés dans l'urne électronique, jusqu'au dépouillement.

Il est recommandé d'utiliser une signature numérique ou un chaînage des bulletins : une telle modification est détectable, car elle rend la signature ou le chaînage invalide.

La signature numérique, comme le chaînage, doivent être réalisés au moyen de mécanismes conformes au *Guide de sélection d'algorithmes cryptographiques* [10]. Ces deux mécanismes sont appliqués par le serveur de vote après la réception et la vérification des bulletins (R24★), aussi les secrets associés à ces mécanismes (par exemple la clé privée d'une signature asymétrique ou la clé secrète d'un code d'authentification de message de type HMAC [23]) sont totalement sous son contrôle. Le serveur de vote est donc en mesure de porter atteinte à l'intégrité des suffrages exprimés et ces mécanismes ont plus pour objet de détecter une perte ou une altération de bulletin suite à un problème technique que de détecter un bourrage d'urne par le serveur de vote.

Protection contre le bourrage d'urne par le serveur de vote

En fonction de l'analyse des risques (R62★★★), si le risque de bourrage d'urne par le serveur est identifié, il peut être estimé nécessaire de renforcer la signature ou le chaînage des bulletins en faisant intervenir un tiers horodateur ou en réalisant l'export des calculs de signature ou de chaînage vers un système de journalisation (R38★).

L'ajout de ces traitements dans l'opération de vote peut avoir un impact sur la disponibilité du système (R7★) et l'accès au vote pour tous les électeurs. De plus, cet ajout n'a de sens que si la *vérification* de ces mécanismes est réalisable par un tiers, sur la base des données traitées par le système de vote. Aussi, il est nécessaire que tous les éléments entrant dans les calculs de vérification de la

signature, du chaînage ou de l'horodatage soient clairement identifiés, disponibles et permettent effectivement leur vérification.

Attention

Même lorsque la recommandation R27★ est correctement mise en œuvre et que les vérifications sont correctement effectuées, elle ferait l'hypothèse que l'intégralité des équipements susceptibles de modifier les bulletins est connue, maîtrisée, auditable et de confiance.

Reposer exclusivement sur cette recommandation et les vérifications associées pour analyser la protection du scrutin contre le bourrage d'urne est donc un compromis qui fait l'hypothèse que le système de vote est de confiance.

De manière générale, reposer exclusivement sur des mécanismes mis en œuvre par le serveur de vote lui-même, après la réception et la vérification des bulletins, ne protège pas contre un bourrage d'urne par le serveur de vote, qui serait indétectable. Cette impossibilité peut être dépassée en réalisant une signature des bulletins dès leur émission sur le client de vote et en assurant que cette signature ne peut pas être réalisée par les entités qui ont les moyens techniques de modifier les bulletins sur le serveur de vote (le prestataire, l'organisateur du scrutin).

Pour aller plus loin

L'objectif 1-06 est renforcé par l'objectif 1-10 qui porte sur l'intégrité globale du système de vote, l'objectif 2-04 et la mise en place d'alertes à destination du bureau électoral en cas de détection de modification illégitime de bulletin et les recommandations complémentaires concernant la signature des bulletins (Section 4.4, recommandation R70★★★+).

Objectif n° 1-07

Assurer l'étanchéité totale entre l'identité de l'électeur et l'expression de son vote (le contenu déchiffré de son bulletin de vote) pendant toute la durée de traitement, y compris lors du dépouillement et, le cas échéant, lors de l'archivage des données du scrutin.

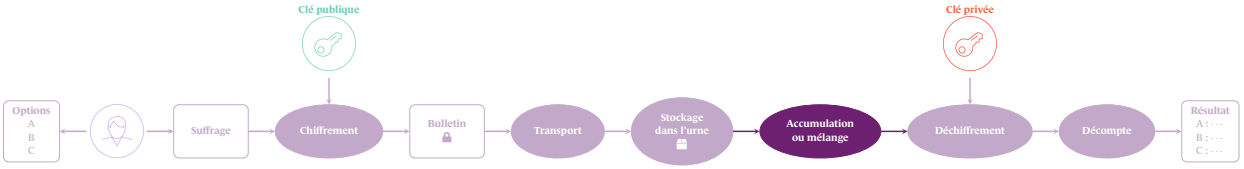

FIGURE 10 – Étanchéité entre l'identité de l'électeur et l'expression de son vote

Cet objectif, illustré en Figure 10, est central pour le secret du scrutin : il doit être impossible de mettre en relation l'identité de l'électeur avec l'expression de son vote. Cette mise en relation nécessite deux étapes : associer un électeur avec un bulletin (chiffré), puis associer ce bulletin avec l'expression du vote (le suffrage, en clair), par exemple lors du déchiffrement. Pour protéger le secret, le système de vote peut donc assurer l'étanchéité électeur/bulletin ou assurer l'étanchéité bulletin/suffrage.

Étanchéité électeur/bulletin

Pour la première étanchéité électeur/bulletin, une pratique répandue est de s'appuyer sur l'absence d'horodatage du bulletin. En effet, puisque l'émargement de chaque électeur est horodaté, si le bulletin est également horodaté, on peut rapprocher facilement le bulletin de l'électeur à travers leur horodatage.

R28 ★

Renoncer à l'horodatage individuel des bulletins

Il est recommandé que le système de vote ne réalise pas d'horodatage individuel des bulletins transmis par les électeurs, c'est-à-dire qu'il ne produise pas de trace horodatée contenant soit le bulletin, soit une information calculée de manière déterministe à partir du bulletin (par exemple une empreinte du bulletin).

Cela implique en particulier que les journaux d'événements établis aux fins de surveillance du système de vote (R37★) ne contiennent pas de bulletin ni aucune information calculée de manière déterministe à partir du bulletin.

Cette recommandation fournit un premier niveau d'étanchéité électeur/bulletin. Cependant, si elle peut être maîtrisable sur un périmètre réduit, il est difficile de l'assurer sur l'ensemble des traitements impliqués dans l'opération de vote (R21★ en fournit une première liste, restreinte au chemin entre le client de vote et le serveur de vote) et, d'autre part, tout traitement laisse des traces techniques. C'est le cas typiquement des équipements réalisant les échanges réseau entre le client de vote et le serveur de vote, de l'horodatage du système de fichiers sur disque, des journaux transactionnels des bases de données. Ces équipements peuvent aussi potentiellement *ne pas* être opérés par le prestataire et être hors du périmètre des audits, aussi l'absence d'horodatage ne peut pas être attestée. Enfin, il peut exister des données corrélées avec l'identité de l'électeur, autres que l'émargement, qui seraient horodatées.

Attention

S'appuyer exclusivement sur la recommandation R28★ pour assurer l'étanchéité électeur/bulletin ferait l'hypothèse que l'intégralité des équipements susceptibles de tracer les bulletins et que l'intégralité des données corrélées avec l'identité de l'électeur et horodatées sont connues, maîtrisées, auditables et de confiance.

Sans cette hypothèse, cette recommandation *à elle seule* n'assure pas l'étanchéité électeur/bulletin. De plus, elle n'est non plus pas *suffisante* pour assurer le secret du scrutin car il peut y avoir d'autres moyens que l'horodatage pour corréler un électeur et son bulletin (identifiants, métadonnées par exemple).

Étanchéité bulletin/suffrage

En complément ou en remplacement de l'absence d'horodatage du bulletin, des dispositions peuvent être prises pour assurer l'étanchéité entre le bulletin et le suffrage. Les premières sont bien sûr l'utilisation d'un chiffrement robuste (1-04) et la protection de la clé privée de l'élection (1-08). Elles évitent qu'il soit possible de déchiffrer le bulletin en dehors du déchiffrement légitime réalisé lors du dépouillement.

Mais ces dispositions sont inefficaces si les bulletins sont déchiffrés un par un, établissant un lien évident entre le bulletin et le suffrage. C'est le rôle de l'accumulation ou du mélange cryptographique que d'éviter ce lien.

L'accumulation consiste à générer le chiffré du résultat à partir des bulletins, sans déchiffrer les bulletins individuels. Cette notion et sa mise en œuvre sont expliquées en Annexe C.

Le mélange consiste à réordonner les bulletins de l'urne électronique. Cette notion et sa mise en œuvre sont expliquées en Annexe C. Deux solutions sont possibles :

- utiliser un mélange *non cryptographique*, ou
- utiliser un mélange *cryptographique*.

Comme exposé en Annexe C, la mise en œuvre d'un mélange non cryptographique comporte un risque majeur sur le secret du scrutin, aussi elle doit être écartée.

R29 ★

Assurer l'étanchéité par accumulation ou mélange cryptographique des bulletins

Le système de vote doit assurer l'étanchéité entre l'identité de l'électeur et l'expression de son vote par accumulation ou mélange cryptographique des bulletins.

Dans les deux cas, le mécanisme mis en œuvre doit être compatible avec le mécanisme de chiffrement des suffrages (R19★).

La solution de vote doit assurer que seuls les bulletins accumulés ou mélangés, sont déchiffrés :

- En cas d'accumulation, l'accumulation ne peut être réalisée qu'après vérification individuelle de la validité des suffrages (sans divulgation de ceux-ci) contenus dans les bulletins et le déchiffrement ne peut être réalisé que sur l'accumulation pro-

duite et pas sur les bulletins d'origine.

- En cas de mélange cryptographique incluant le déchiffrement, le mélange ne peut être réalisé qu'après vérification individuelle de la validité des bulletins.
- En cas de mélange cryptographique n'incluant pas de déchiffrement, le mélange ne peut être réalisé qu'après vérification individuelle de la validité des bulletins, et le déchiffrement ne peut être réalisé que sur les bulletins issus du mélange.

Information

Le mécanisme de chiffrement asymétrique ElGamal permet l'accumulation des bulletins, car c'est un chiffrement homomorphe. De plus, la malléabilité du mécanisme permet la mise en place d'un mélange cryptographique *par rechiffrement* des bulletins (voir Annexe C).

- En cas d'accumulation, chaque bulletin **doit** contenir un ensemble de preuves à divulgation nulle de connaissance attestant de la validité du suffrage (preuve à divulgation nulle de connaissance de chiffrement de 0 ou 1, preuve à divulgation nulle de connaissance de chiffrement d'entier dans un intervalle), dont le contexte est éventuellement complété avec les attributs des électeurs en cas de pastillage (R20★). Ces preuves doivent être vérifiées avant l'accumulation.
- En cas de mélange cryptographique, chaque bulletin **doit** contenir une preuve à divulgation nulle de connaissance attestant de la validité du bulletin (preuve à divulgation nulle de connaissance de l'aléa utilisé pour le chiffrement du suffrage), dont le contexte est éventuellement complété avec les attributs des électeurs en cas de pastillage (R20★). Ces preuves doivent être vérifiées avant le mélange.

Mise en œuvre de la propriété receipt-freeness

L'étanchéité entre l'identité de l'électeur et l'expression de son vote doit être assurée y compris vis-à-vis d'un électeur qui veut utiliser le système de vote pour *prouver* à un attaquant son suffrage [22].

Pour cela, l'électeur qui souhaite prouver son suffrage va utiliser toutes les données transmises ou affichées par le système de vote ou bien effectuer des manipulations sur ces données pour en obtenir d'autres, afin d'obtenir une preuve. Dans des modèles de sécurité plus forts, des contraintes peuvent en plus être exercées par un attaquant sur l'électeur. Comme expliqué à l'Annexe D, selon les informations auxquelles l'électeur a accès, les actions qu'il peut réaliser et les contraintes auxquelles il est exposé, les propriétés attendues du système de vote seront différentes :

- La propriété de receipt-freeness est la plus basique (l'électeur n'effectue pas de manipulation sur les données, n'est pas contraint et l'attaquant a accès aux données transmises ou affichées par le système de vote), aussi cette propriété doit être assurée par le système de vote pour tous les niveaux de scrutin.
- Les propriétés de résistance à l'achat de vote et à la coercition, renforçant, respectivement, le caractère personnel du vote et le caractère libre du vote, sont plus difficiles à mettre en œuvre,

22. L'électeur peut toujours divulguer son suffrage à un tiers. Il s'agit ici d'utiliser le système de vote pour le prouver.

tant par le système de vote que par les électeurs, aussi elles sont envisageables en fonction de l'analyse de risque (objectif 3-01).

Attention

La propriété de receipt-freeness pourrait empêcher un électeur de prouver son suffrage à un attaquant basique. Cependant un attaquant exerçant des contraintes sur l'électeur pourrait obtenir cette preuve.

Les risques d'achat de vote et de coercition font ainsi partie de la liste des « risques non couverts » par les recommandations de ce guide (voir Section 4.5).

R30 ★

Assurer la propriété de receipt-freeness

Le système de vote doit assurer la propriété de receipt-freeness : l'ensemble des données transmises ou affichées par le système de vote ne doivent pas permettre à l'électeur de prouver son suffrage à un attaquant, également destinataire de ces données [23].

Pour aller plus loin

L'objectif 1-07 est renforcé par l'objectif 3-04 qui recommande de ne pas traiter la clé privée de l'élection sur la même machine que celle stockant l'urne électronique.

23. En prenant l'hypothèse que l'électeur n'effectue pas de manipulation supplémentaire à celles prévues par le protocole de vote, comme intervenir sur son client de vote pour enregistrer l'aléa utilisé lors du chiffrement du suffrage.

Objectif n° 1-08

Renforcer la confidentialité des bulletins de vote en répartissant le secret permettant leur dépouillement, notamment au sein du bureau électoral, et garantir la possibilité de dépouillement à partir d'un seuil de secret déterminé.

Comme expliqué aux objectifs 1-04, 1-07 et 1-11, l'accès à la clé privée de l'élection permet de réaliser le dépouillement, mais également de porter atteinte au secret du scrutin si cette clé est utilisée de manière illégitime ou si elle est compromise.

Afin de réduire ce risque, il est recommandé de répartir la connaissance du secret qu'est la clé privée de l'élection, en fragmentant cette clé grâce à un mécanisme de partage de secret, et en attribuant les fragments, notamment aux membres du bureau électoral.

Fragmentation et stockage de la clé privée de l'élection

Une collusion des attributaires des fragments de la clé privée de l'élection permet en théorie de la reconstituer. Aussi, ce risque est minimisé (et accepté) en choisissant un nombre de fragments suffisant ainsi que des attributaires ayant des intérêts divergents. Un risque inhérent à cette pratique est que la perte d'un fragment ou l'absence d'un attributaire empêche le déchiffrement et donc le dépouillement. Pour cela, un mécanisme de partage de secret à seuil [24] doit être utilisé.

R31 ★

Fragmenter la clé privée au moyen d'un mécanisme de partage de secret à seuil

Le système de vote doit fragmenter la clé privée de déchiffrement des bulletins au moyen d'un mécanisme de partage de secret à seuil, compatible avec le mécanisme de chiffrement des suffrages (R19★). Le partage doit être effectif (il y a strictement plus de deux fragments) et le seuil doit être effectif (il doit être strictement plus grand que 1).

Le déchiffrement ne doit être possible qu'avec un nombre de fragments supérieur ou égal au seuil, y compris lorsque ce déchiffrement intervient afin d'exécuter un nouveau décompte (R40★).

La description de la fragmentation (les porteurs de fragments, le seuil utilisé) doit être publique.

Le **partage de secret à seuil** de Shamir [89] est communément utilisé. Ce mécanisme a l'avantage d'être compatible avec n'importe quel mécanisme de chiffrement utilisé, mais il impose la génération de la clé privée de l'élection (et donc son existence, même temporaire) sur un même équipement. De plus, il ne permet pas de détecter un éventuel détournement de ce partage en faveur d'un des attributaires qui disposerait de la clé privée entière. Ainsi il existe un risque sur le secret du scrutin car l'usage de la clé privée de l'élection ne serait plus contrôlé. Suivant l'analyse

24. L'organisateur définit un seuil ou nombre minimal de fragments à rassembler, seuil strictement plus grand que un ; cela oblige à disposer effectivement de plusieurs fragments pour déchiffrer. Le seuil peut également être strictement plus petit que le nombre total de fragments, pour pouvoir se passer du fragment d'un (ou de plusieurs suivant la marge prise) attributaire absent ou non coopératif. Exemple, pour 5 fragments créés, le seuil pourrait être fixé à 3.

de risque (R62★★★), il peut être envisagé de renforcer le partage de clé en utilisant un partage de clé distribué (R72★★★+) ou vérifiable (R74★★★+).

L'Annexe A fournit des exemples de partages de la clé privée de l'élection adaptés au mécanisme de chiffrement ElGamal, **à seuil maximal** (tous les fragments de clé sont nécessaires pour réaliser le déchiffrement des bulletins) ou **à seuil** (un nombre de fragments strictement inférieur au nombre total de fragments de clé est suffisant pour réaliser le déchiffrement des bulletins).

R32 ★

Stocker les fragments de clés de manière sécurisée

Le système de vote doit stocker les fragments de la clé privée de l'élection en respectant les points suivants :

- La clé privée entière (non fragmentée) ne doit jamais être stockée.
- À chaque fragment de la clé privée doit être associé un code d'activation, seulement connu de l'attributaire.
- Le système de vote doit imposer une règle de composition du code d'activation afin de le rendre conforme aux *Recommandations relatives à l'authentification multifacteur et aux mots de passe* [22]. Cette règle doit tenir compte de l'utilisation du code dans la protection du fragment de clé privée (code permettant de dériver une clé symétrique de chiffrement ou bien code PIN d'activation de support matériel).
- Chaque fragment de la clé privée est enregistré individuellement en étant chiffré. Cet enregistrement peut être réalisé dans le système de vote électronique, ou sur un support physique qui est alors remis à l'attributaire du fragment.
- L'enregistrement protège le fragment en intégrité et en confidentialité et le fragment ne peut être déchiffré et utilisé qu'en connaissant le code d'activation.
- Les codes d'activation ne sont pas enregistrés par le système de vote électronique.
- Les codes d'activation ne doivent pas être rassemblés sous le contrôle d'un nombre plus réduit d'acteurs (organisateur ou prestataire) que le seuil.

Une pratique répandue consiste à organiser une cérémonie au cours de laquelle les fragments de la clé privée de l'élection sont générés et chaque attributaire choisit un code d'activation. Cette cérémonie permet de réunir le bureau électoral et de réaliser d'autres actions comme la mise en œuvre de scellements.

Comme exprimé à la recommandation R1★, le prestataire doit fournir la procédure de la cérémonie adaptée au contexte de l'organisateur du scrutin, cette procédure doit être revue par l'expert indépendant (au sens de la délibération de la CNIL [72]) et une fois stabilisée, l'organisateur du scrutin doit respecter cette procédure.

Information

La recommandation R32★ indique que les codes d'activation ne doivent pas être rassemblés sous le contrôle d'un nombre plus réduit d'acteurs (que le seuil). Elle ne s'op-

pose pas à la mise en œuvre d'une éventuelle obligation réglementaire de pouvoir exécuter un décompte (R40★). En effet, si pour répondre à cette obligation réglementaire, les fragments de clés et les codes d'activation sont archivés, alors la procédure d'archivage doit s'assurer que ces éléments ne seront accessibles (et accédés) que dans le cadre d'un nouveau décompte, ordonné par le juge de l'élection.

Pour aller plus loin

L'objectif 1-08 est renforcé par l'objectif 3-04 qui recommande de ne pas traiter la clé privée de l'élection sur la même machine que celle stockant l'urne électronique.

Objectif n° 1-09

Assurer que le dépouillement d'une urne n'est réalisable que sur l'ensemble des bulletins qu'elle contient et après la fermeture du scrutin.

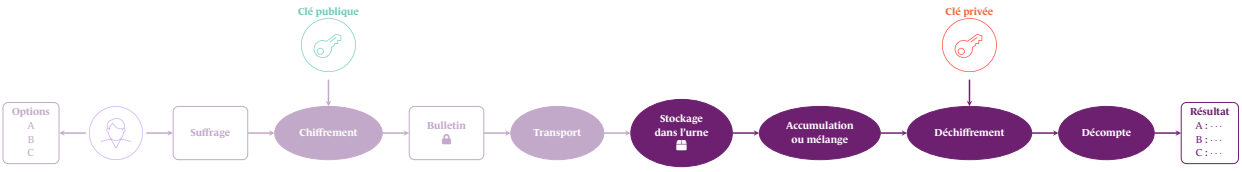

FIGURE 11 – Dépouillement

Le dépouillement, dernière étape du scrutin, réalise, le cas échéant, l'accumulation ou le mélange cryptographique des bulletins, le déchiffrement, exécute un décompte des suffrages et produit le résultat de l'élection, comme illustré à la Figure 11.

S'il est possible d'effectuer le dépouillement sur des ensembles de bulletins arbitraires, une atteinte au secret du scrutin est possible [25] : il doit être impossible de dépouiller d'autres ensembles de bulletins que ceux prévus par l'élection, ou de le faire avant la clôture du scrutin.

Une pratique répandue consiste à organiser une cérémonie au cours de laquelle les fragments de la clé privée de l'élection sont utilisés par les attributaires pour réaliser le déchiffrement, le décompte et afficher les résultats. De manière analogue à la cérémonie de génération (1-08), cette cérémonie permet de réunir le bureau électoral et de réaliser d'autres actions comme la vérification du scellement. Comme exprimé à la recommandation R1★, le prestataire doit fournir la procédure de la cérémonie adaptée au contexte de l'organisateur du scrutin, cette procédure doit être revue par l'expert indépendant (au sens de la délibération de la CNIL [72]) et une fois stabilisée, l'organisateur du scrutin doit respecter cette procédure.

R33 ★

Détecter tout dépouillement illégitime

La solution de vote doit détecter (de façon organisationnelle ou technique) toute tentative de réaliser le dépouillement avant la clôture du scrutin et toute tentative de réaliser le dépouillement sur d'autres ensembles de bulletins que ceux prévus par l'élection.

En cas de pastillage, les urnes électroniques à dépouiller sont celle du scrutin direct et celles des scrutins indirects.

Comme expliqué à l'objectif 1-07, le déchiffrement nécessite l'accès aux fragments de la clé privée de l'élection. L'accès à ces fragments de clé permet de réaliser le déchiffrement de n'importe quelle donnée chiffrée avec la clé publique de chiffrement, aussi il est nécessaire que les opérations réalisées soient contrôlées. De plus, l'ordonnancement des opérations d'accumulation ou de mélange, de déchiffrement et de décompte après la clôture du scrutin doit tenir compte des temps de traitement de chaque opération.

25. À l'extrême, un ensemble peut être constitué d'un bulletin et cela divulgue le suffrage d'un électeur.

Pour aller plus loin

L'objectif 1-09 est renforcé par l'objectif 2-04 et la mise en place d'alerte.

Objectif n° 1-10

Assurer l'intégrité du système et de la vacuité de l'urne et de la liste d'émargement avant le début du scrutin.

L'intégrité du système de vote est une condition nécessaire à l'intégrité des suffrages exprimés et à la sincérité des opérations électorales. Le système de vote doit être expertisé pour analyser sa conformité à la délibération de la CNIL [72]. Une fois expertisé, il ne doit pas être modifié : son intégrité doit pouvoir être contrôlée.

De plus, le résultat de l'élection ne sera valide que si l'urne électronique et la liste d'émargement sont vides au début du scrutin et restent cohérentes pendant le scrutin.

Intégrité de l'application de vote

La référence du contrôle d'intégrité est produite par l'expert indépendant lors de l'analyse du code source prévue à la section 7 « Expertise de la solution de vote par correspondance électronique » de la délibération de la CNIL. L'expertise vérifie que le système de vote est conforme à la délibération.

Idéalement, l'intégrité est assurée pour l'ensemble du système de vote, y compris son hébergement. Cependant, la vérification de l'intégrité peut se concentrer sur l'application de vote et la configuration de l'élection.

La délibération de la CNIL recommande également que l'expert indépendant « vérifie que les différents composants logiciels sur lesquels a porté l'expertise n'ont pas été modifiés sur le système utilisé durant le scrutin ». Cela peut être réalisé par les étapes suivantes :

- La compilation du code source analysé en application exécutable de manière reproductible [67, 86], au sens où le résultat de cette compilation est déterministe [26].
- La prise d'empreinte numérique de l'application exécutable issue de la compilation du code source expertisé.
- La vérification que l'application déployée sur le système de vote correspond à celle expertisée, en comparant son empreinte à celle issue de la compilation du code source expertisé.

R34 ★

Fournir une compilation reproductible

Il est recommandé que le prestataire fournisse une compilation reproductible [67, 86] du code source de l'application de vote en fichiers exécutables déployés sur le système de vote.

La compilation de l'application de vote doit pouvoir être reproduite de manière indépendante par un tiers (par exemple l'expert indépendant au sens de la délibération de la CNIL [72]) et générer les mêmes fichiers exécutables que dans l'environnement de compilation du prestataire. Le résultat de la compilation reproductible peut être identifié par une prise d'empreinte numérique.

26. [85] fournit un exemple de compilation reproductible dans le contexte du vote par correspondance électronique.

R35 ★

Permettre le contrôle de l'intégrité de l'application de vote

Le système de vote doit permettre à un expert indépendant (au sens de la délibération de la CNIL [72]) de contrôler que les fichiers exécutables de l'application de vote correspondent au résultat de la compilation du code source objet de l'expertise.

L'intégrité de ces fichiers exécutables doit pouvoir être vérifiée par un calcul d'empreinte numérique et une comparaison avec l'empreinte de référence, issue de la compilation reproductible (R34★).

De plus, l'application de vote peut inclure des scripts ou des fichiers non exécutables (par exemple, le schéma de la base de données) dont l'intégrité doit pouvoir être vérifiée, également par comparaison d'empreinte numérique.

Attention

Même lorsque les recommandations R34★ et R35★ sont correctement mises en œuvre, le prestataire peut toujours installer une application illégitime sur le serveur de vote et porter atteinte à l'intégrité des suffrages exprimés et à la sincérité des opérations électorales.

Reposer sur la conformité du code source de l'application de vote pour analyser l'intégrité des suffrages exprimés et la sincérité des opérations électorales est donc un compromis qui fait l'hypothèse que le prestataire ainsi que le système de vote sont de confiance.

Cette hypothèse peut être dépassée en appliquant le principe d'indépendance logicielle, décliné aux objectifs 2-07 (recorded-as-cast) et 3-02 (tallied-as-recorded).

Cohérence de l'urne électronique et de la liste d'émargement

Comme l'urne électronique et la liste d'émargement seront modifiées légitimement pendant le scrutin, il faut en assurer la cohérence.

R36 ★

Permettre le contrôle de la cohérence de l'urne électronique et de la liste d'émargement

Le système de vote doit permettre au prestataire de contrôler la cohérence de l'urne électronique et de la liste d'émargement tout au long du scrutin. Elles doivent être vides à l'ouverture du scrutin, elles ne doivent qu'augmenter pendant le scrutin et elles doivent comporter à tout moment le même nombre d'éléments. En cas de pastillage, la cohérence doit être vérifiée sur l'urne du scrutin direct et les urnes des scrutins indirects.

La cohérence doit pouvoir être contrôlée par requêtes directes, qui doivent donner le nombre exact d'entrées dans l'urne et dans la liste d'émargement de chaque scrutin.

Journalisation et détection

L'intégrité du système de vote peut enfin s'appuyer sur la journalisation et la détection des événements qui concernent le fonctionnement du système, ou qui peuvent avoir un impact sur l'intégrité

des suffrages exprimés et la sincérité des opérations électorales.

R37 ★

Mettre en place un système de journalisation et de détection des événements

Il est recommandé que le prestataire mette en œuvre un système de journalisation des événements, par exemple en suivant les *Recommandations de sécurité pour l'architecture d'un système de journalisation* [14].

Dans ce cas, les événements journalisés ne doivent *pas* contenir les données suivantes :

- Les secrets d'authentification des électeurs (1-04).
- Les secrets ou clés privées de signature numérique ou de chaînage des bulletins (1-06).
- Les fragments de la clé privée de l'élection et les codes d'activation des attributaires (1-08).
- Les secrets ou clés privées utilisés pour le scellement du système de vote (2-02).
- Les bulletins des électeurs ou toute information calculée de manière déterministe à partir des bulletins (par exemple une empreinte numérique des bulletins).
- Les informations présentes dans les preuves de vote (2-07).

De plus, il est recommandé que le prestataire soit en mesure d'analyser les journaux *en temps réel* pour contrôler le fonctionnement correct du système de vote et *a posteriori* pour analyser les causes d'un éventuel dysfonctionnement.

R38 ★

Journaliser les événements de fonctionnement du système de vote

Il est recommandé que le système de vote journalise les événements relatifs à son fonctionnement, notamment :

- Toute opération de maintenance et de gestion réalisée sur le système de vote.
- Le déploiement de la configuration de l'élection et des fichiers exécutables (1-10).
- La génération des secrets d'authentification des électeurs.
- L'envoi (dont l'envoi initial s'il est réalisé par le système de vote) et le recouvrement de secret d'authentification des électeurs ; le changement de moyen d'adressage des secrets d'authentification des électeurs (1-03, R15★).
- La génération des clés privées ou des secrets de signature numérique ou de chaînage, (1-06, 2-02) et de la clé privée de signature numérique des preuves de vote (2-07).
- La génération des fragments de la clé privée de l'élection (1-08).
- L'ouverture, la suspension, l'arrêt et la fermeture du scrutin (2-05).
- Les traces générées par le chaînage (1-06).

- La réalisation du dépouillement, y compris le lancement et la clôture des opérations d'accumulation, de mélange cryptographique et de déchiffrement (1-09).
- Le scellement et toute vérification de scellement du système (2-02).
- Les alertes transmises au bureau électoral (2-04).

R39 ★

Journaliser les événements ayant un impact sur le secret, l'intégrité et la sincérité

Il est recommandé que le système de vote journalise les événements ayant un impact direct ou indirect sur le secret du scrutin, l'intégrité des suffrages exprimés et la sincérité des opérations électorales, notamment :

- Accès illégitime à la clé privée de l'élection ou un de ses fragments.
- Échec d'un traitement de l'opération de vote (1-02).
- Dépôt d'un bulletin dans une urne électronique sans émargement ou émargement sans dépôt de bulletin dans une urne électronique (1-02).
- Attaque par recherche d'authentifiants (1-03).
- Détection de modification de bulletin transmis par un électeur, traité par le serveur de vote et stocké dans l'urne électronique (1-06).
- Indisponibilité du système de vote (2-01).
- Attaque en déni de service sur le système de vote (2-01).
- Rupture d'un scellement (2-02).

Pour aller plus loin

L'objectif 1-10 est renforcé par l'objectif 2-04 qui concerne la mise en place d'alertes à destination du bureau électoral.

Objectif n° 1-11

Assurer que le bon dépouillement de l'urne peut être vérifié a posteriori.

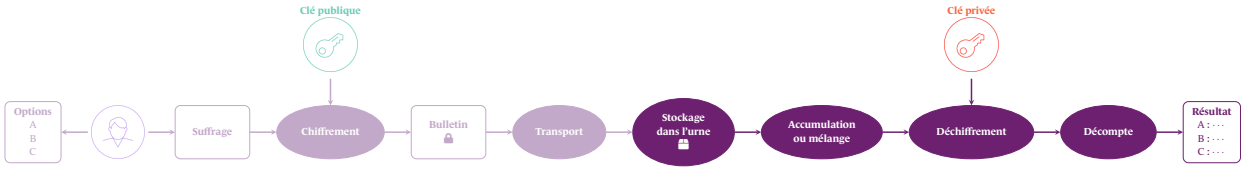

FIGURE 12 – Vérification du dépouillement *a posteriori*

Le dépouillement, dernière étape du scrutin, réalise, le cas échéant, l'accumulation ou le mélange cryptographique des bulletins, le déchiffrement, exécute un décompte des suffrages et produit le résultat de l'élection, comme illustré à la Figure 12. Si ce résultat est contesté, il doit pouvoir être contrôlé *a posteriori* par le juge de l'élection (voir la Section 3.2.2).

Pour cela, deux solutions sont couramment envisagées (voir par exemple [71]) : exécuter un nouveau décompte ou prouver de façon irréfutable que le résultat correspond effectivement au contenu de l'urne électronique au moyen de preuves mathématiques. La première solution est décrite en réponse à l'objectif 1-11. La seconde est abordée dans l'objectif 3-02.

Vérification du dépouillement par l'exécution d'un nouveau décompte

La première solution est donc l'exécution d'un nouveau décompte. Deux options sont possibles :

- Partir du résultat du déchiffrement.
- Partir de l'urne électronique stockée, non mélangée ou non accumulée, et non déchiffrée.

Attention

Partir du résultat du déchiffrement ne permet aucunement de vérifier le dépouillement car cela revient à ignorer les bulletins transmis par les électeurs. Cette option doit donc être écartée.

Ainsi, le point de départ *doit* être l'urne électronique et l'exécution d'un nouveau décompte nécessite la réalisation des opérations y menant, c'est-à-dire, le cas échéant, l'accumulation ou le mélange cryptographique, et le déchiffrement.

L'exécution d'un nouveau décompte s'impose lorsque le mélange cryptographique des bulletins ou le déchiffrement sont *non vérifiables* : le seul moyen de les vérifier est de les exécuter à nouveau. Elle s'impose également dans certains contextes réglementaires [27].

Dans ces cas, l'organisateur du scrutin doit :

- Conserver l'urne électronique d'origine (non mélangée, non accumulée) et de façon générale la configuration de l'élection. Cette conservation est de toute façon obligatoire [28].

27. Par exemple, à la date de rédaction du présent guide, l'exécution d'un nouveau décompte est requise pour les votes par correspondance électronique régis par le Code du travail (art. R2122-70 et art. R2314-17), par le Code de commerce (art. R.713-21 et art. R713.25), le Code rural et de la pêche maritime (art. R242-19, art. R511-48-2 et art. R723-84-1), le Code de l'artisanat (art. R322-39), le Code de la santé publique (art. R4031-35 et art. R4311.81) et le Code de l'action sociale et des familles (art. R211-2-10).

28. Voir la section « Conservation des données portant sur l'opération électorale » de la délibération de la CNIL [72]. Cette section utilise la notion de matériel de vote.

- Conserver les fragments de la clé privée de l'élection.
- Prévoir un moyen assurant que suffisamment de codes d'activation associés aux fragments de clé soient disponibles lors du nouveau déchiffrement (voir plus bas).
- Pouvoir recourir à une fonction du système de vote réalisant une nouvelle accumulation ou un nouveau mélange, un nouveau déchiffrement et un nouveau décompte (parfois des mois après le scrutin, alors que le système de vote pourrait avoir été sauvegardé puis démantelé) à partir des données conservées.

R40 ★

Permettre l'exécution d'un nouveau décompte, le cas échéant

En l'absence de déchiffrement vérifiable ou en cas de contrainte réglementaire, le système de vote doit permettre la vérification du dépouillement par l'exécution d'un nouveau décompte. Cette vérification part de l'urne électronique d'origine et exécute à nouveau, le cas échéant l'accumulation ou le mélange cryptographique, et le déchiffrement.

Dans ce cas, la procédure de conservation des fragments de la clé privée de l'élection et des codes d'activation associés doit assurer le secret du scrutin.

Disponibilités des codes d'activation

Pour qu'un nouveau décompte puisse être exécuté et en l'absence de déchiffrement vérifiable, un nouveau déchiffrement est nécessaire. Pour cela, il faut disposer de suffisamment de fragments de la clé privée de l'élection et des codes d'activation associés.

Il serait tentant pour l'organisateur du scrutin de simplement conserver, en plus des fragments de la clé privée de l'élection, les codes d'activation de ces fragments, dans le but d'être autonome en cas de requête du juge de l'élection.

Cependant, cette conservation crée un risque important pour le secret du scrutin. L'organisateur pourrait en effet déchiffrer, seul, les bulletins individuels de l'urne électronique d'origine, rentrant ainsi en contradiction avec la recommandation R31★. Cela rendrait caduques de nombreuses mesures de sécurité mises en œuvre pendant le scrutin, comme le partage de la clé privée, ou le recours à un mélange cryptographique ou à l'accumulation. Cela irait enfin à l'encontre de la délibération de la CNIL [72] qui cite parmi les garanties minimales qu'il faut pouvoir « prouver que les clés de chiffrement/déchiffrement ne sont connues que de leurs seuls détenteurs. »

Attention

En conservant la possibilité d'un nouveau décompte alors que la surveillance du bureau électoral est relâchée après le scrutin, on augmente le risque d'une atteinte au secret du scrutin.

Des alternatives plus protectrices du secret du scrutin sont envisageables :

- Obtenir la coopération d'assez d'attributaires de ces fragments pour qu'ils acceptent d'utiliser leur code d'activation lors de la nouvelle exécution du décompte (et que ces attributaires se souviennent de leur code d'activation).

- Conserver les codes d'activation séparément de l'urne et des fragments de clé, en les confiant à un tiers de confiance tel qu'un huissier.
- Conserver les codes d'activation sur des supports rendant visible un accès à leur contenu, tel que des enveloppes de sécurité scellées. L'idée est qu'une utilisation du code hors d'une demande légitime puisse être détectée.

Les mesures ci-dessus ont pour objet de ne pas affaiblir le secret du scrutin lors de la conservation des fragments de la clé privée de l'élection (ou des codes d'activation de ces fragments). Cependant, elles supposent que l'utilisation de ces fragments (ou de ces codes) est contrôlée et circonscrite à la ré-utilisation d'une fonction du système de vote réalisant un nouveau déchiffrement, sous le contrôle du bureau électoral. Ces mesures sont insuffisantes pour l'objectif 3-02 qui requiert la vérification du dépouillement au moyen d'un *outil tiers*.

Portée de l'exécution d'un nouveau décompte

En plus du risque sur le secret du scrutin exposé précédemment, la portée de l'exécution d'un nouveau décompte est limitée.

En effet, ré-utiliser une fonction du système de vote utilisé pour le scrutin ne constitue aucunement un décompte indépendant de celui exécuté pour le dépouillement. Ainsi l'exécution d'un nouveau mélange, d'un nouveau déchiffrement et d'un nouveau décompte ne permet pas de vérifier la sortie de la fonction de mélange ou de déchiffrement, mais permet par exemple de détecter la publication d'un résultat différent de celui issu du mélange ou du déchiffrement (l'organisateur du scrutin ignore le mélange ou le déchiffrement et publie un résultat invalide)[29].

Attention

S'appuyer sur l'exécution d'un nouveau mélange, d'un nouveau déchiffrement et d'un nouveau décompte pour vérifier le dépouillement est donc un compromis qui fait l'hypothèse que le système de vote est de confiance.

Cette hypothèse peut être dépassée en appliquant le principe d'indépendance logicielle, décliné aux objectifs 2-07 (propriété recorded-as-cast) et 3-02 (propriété tallied-as-recorded).

Pour aller plus loin

Cet objectif est renforcé par les objectifs objectifs 2-07 (propriété recorded-as-cast) et 3-02 (propriété tallied-as-recorded).

29. À titre de comparaison, un nouveau décompte indépendant peut être réalisé dans le contexte des machines à voter avec trace papier : il existe deux ensembles de bulletins distincts, de formes distinctes (dématérialisée et papier) ; un décompte indépendant de celui réalisé sur les bulletins dématérialisés peut être réalisé au moyen des bulletins papier.

4.2 Objectifs de sécurité de niveau 2

Définition de la CNIL [72] : **Niveau 2 (risques modérés)** : *les sources de menace (parmi les votants, les organisateurs du scrutin, les fournisseurs du système de vote, les personnes extérieures, etc.) peuvent présenter des ressources moyennes ou des motivations moyennes. Ce niveau s'applique principalement à des scrutins qui impliquent un nombre modéré de votants et qui présentent un enjeu moyen pour les candidats dans un contexte dépourvu de conflictualité particulière. Il s'agit par exemple des élections de représentants du personnel au sein d'organismes de petite taille ou de taille moyenne.*

Modèle de confiance : Pour ce niveau, le prestataire et l'organisateur du scrutin peuvent porter atteinte à la sécurité du système de vote. En conséquence, les recommandations de ce niveau complètent celles du niveau 1 et visent à renforcer la sincérité des opérations électorales par le durcissement du système de vote, et la surveillance effective du vote. Les enjeux plus élevés des scrutins de niveau 2 justifient des moyens supplémentaires pour en assurer la disponibilité ainsi qu'une plus grande transparence. La vérifiabilité individuelle est introduite. L'authentification des électeurs est renforcée. La Figure 13 présente les objectifs de sécurité de la CNIL correspondant à des scrutins de niveau 2.

2-01	Assurer, durant la période d'ouverture du scrutin, une haute disponibilité du système de vote électronique et des services tiers pouvant être nécessaires à son fonctionnement (notamment pour l'authentification et l'émargement des électeurs, le contrôle par le bureau de vote, etc.).
2-02	Mettre en œuvre, sous la surveillance du bureau électoral, un contrôle automatique de l'intégrité du système de vote et de la cohérence entre le contenu de l'urne et le nombre d'émargements pendant toute la durée du scrutin.
2-03	Permettre le déclenchement manuel par le bureau électoral des contrôles mentionnés dans l'objectif 2-02. Prévoir la formation du bureau électoral au fonctionnement des outils de contrôle dont il dispose.
2-04	Assurer que le bureau électoral soit alerté automatiquement et immédiatement de tout incident de sécurité et de toute intervention de gestion ou de maintenance survenant sur le système de vote électronique et dispose d'un accès à un journal de ces alertes.
2-05	Assurer un cloisonnement entre les systèmes de vote électronique de chaque scrutin de sorte qu'aucune donnée ne puisse être échangée entre ces systèmes et qu'il soit possible de suspendre ou de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours.
2-06	Utiliser un système d'information mettant en œuvre les mesures de sécurité physique et logique recommandées par les éditeurs des briques applicatives constituant la solution de vote, par la CNIL et par l'ANSSI.
2-07	Permettre aux électeurs de vérifier la présence de leur bulletin dans l'urne pendant le scrutin ainsi que sa présence dans l'urne utilisée pour le dépouillement jusqu'à expiration des délais de recours.
2-08	Authentifier les électeurs en s'assurant que la vraisemblance d'une usurpation d'identité est négligeable.
2-09	Favoriser la transparence et l'auditabilité de la solution de vote en rendant public, en amont du scrutin, le protocole de vote ainsi que les propriétés de sécurité garanties par ce protocole et le moyen de les atteindre.

FIGURE 13 – Objectifs de sécurité de niveau 2

Attention

La conformité au niveau 2 ne fournit pas de protection contre un attaquant disposant de ressources importantes permettant de porter atteinte à la disponibilité du système de vote, ou de remettre en cause la sincérité des opérations électorales ou l'intégrité des suffrages exprimés. Pour ce niveau d'attaquant, des mesures complémentaires doivent être envisagées.

Objectif n° 2-01

Assurer, durant la période d'ouverture du scrutin, une haute disponibilité du système de vote électronique et des services tiers pouvant être nécessaires à son fonctionnement (notamment pour l'authentification et l'émargement des électeurs, le contrôle par le bureau de vote, etc.).

L'indisponibilité de la solution peut porter atteinte à l'accès au vote pour tous les électeurs et à la sincérité des opérations électorales car elle peut défavoriser une partie de l'électorat. Les enjeux plus élevés des scrutins de niveau 2 justifient des moyens supplémentaires pour en assurer la disponibilité.

Attention

La disponibilité de la solution de vote peut dépendre d'autres systèmes, que le système de vote, qui ne sont pas directement opérés par le prestataire (sous-traitants pour les envois d'email et de SMS, l'horodatage, solution d'authentification, fournisseur d'accès à Internet). Ces autres systèmes doivent être considérés lors de la mise en œuvre des recommandations répondant à l'objectif 2-01.

R41 ★★

Dimensionner correctement le système de vote

Le système de vote doit être correctement dimensionné pour supporter l'élection et la charge attendue. Cela concerne l'ensemble du système de vote, tel qu'il a été cartographié (R4★).

L'organisateur du scrutin doit fournir au prestataire les éléments lui permettant de réaliser ce dimensionnement, notamment :

- Le nombre d'électeurs a un impact sur la charge du système de vote avant et pendant le vote, et sur le volume des échanges, des données produites et des traces générées par le système de vote.
- Le nombre d'options de vote (ex. : candidats) et le pastillage (1-04) ont un impact sur les traitements réalisés par le client de vote.
- Le nombre d'électeurs et le nombre d'options de vote ont un impact sur les traitements nécessaires pour réceptionner, traiter, accumuler ou mélanger, et déchiffrer les bulletins.

Si des ressources sont partagées entre le système de vote et d'autres systèmes (serveurs, stockage, réseau), le prestataire doit s'assurer des ressources nécessaires au fonctionnement du système de vote, indépendamment du fonctionnement des autres systèmes.

R42 ★★

Mettre en œuvre un système de vote redondant

Le prestataire doit fournir un système secondaire susceptible de prendre le relais en cas d'incident sur le système principal, et offrant les mêmes garanties et les mêmes caractéristiques.

De plus, il est recommandé que chaque système (principal ou secondaire) s'appuie sur une redondance d'infrastructure technique.

Au niveau 2, il est acceptable que les deux systèmes, principal et secondaire, soient hébergés dans le même centre de données (pour un *cloud* public, cela correspond à une unique zone de disponibilité au sein d'une région). Certains risques conduisant à une indisponibilité prolongée du centre de données ne sont alors pas couverts et doivent être acceptés. Au niveau 3, une réplication dans un second centre de données est exigée par l'objectif 3-03.

R43 ★★

Surveiller l'état du système de vote

Il est recommandé que le prestataire effectue une supervision technique de l'état du système de vote, notamment des éléments suivants : l'état des serveurs et des équipements réseau (utilisation du CPU et de la RAM), l'état des disques (volume occupé), l'état du réseau (volume des données échangées) et l'état des services (serveurs Web et applicatifs, serveur de base de données...).

Dans ce cas, le prestataire doit avoir accès à ces information en *temps réel* pour contrôler le fonctionnement correct du système de vote.

Une attaque par déni de service peut rendre indisponible le système de vote, alors que la période de vote peut être courte et sa clôture fixée par des dispositions juridiques. Aussi, il est recommandé de prévenir ces attaques, et de réagir afin d'en limiter l'impact pendant la période de vote.

R44 ★★

Protéger le système de vote contre les attaques par déni de service

Il est recommandé que le système de vote soit protégé contre les attaques par déni de service afin de limiter leur impact pendant la période de vote, par exemple en appliquant les *Essentiels de l'ANSSI - Dénis de service distribués* [16] ainsi que les *Fiches Réflexes du CERT-FR* [33, 34].

Comme rappelé aux objectifs 1-04 et 1-05, le recours à un service de protection contre les dénis de services distribués doit exclure l'utilisation d'un CDN.

Pour aller plus loin

Cet objectif est renforcé par l'objectif 2-04 et la mise en place d'alerte en cas d'indisponibilité du système ou de détection d'attaque en déni de service, et par l'objectif 3-03 qui concerne la réplication complète du système de vote dans un second centre de données.

Objectif n° 2-02

Mettre en œuvre, sous la surveillance du bureau électoral, un contrôle automatique de l'intégrité du système de vote et de la cohérence entre le contenu de l'urne et le nombre d'émargements pendant toute la durée du scrutin.

Cet objectif renforce l'objectif 1-10 relatif à l'intégrité des suffrages exprimés et à la sincérité des opérations électorales : aux contrôles initiaux de l'intégrité du système et de la vacuité de l'urne électronique et de la liste d'émargement, il ajoute l'automatisation de ces contrôles pendant toute la durée du scrutin. Cette automatisation renforce la surveillance effective du vote et s'appuie notamment sur des scellements.

Information

Le scellement d'un contenu numérique consiste à prendre une empreinte numérique de ce contenu, ou à apposer un cachet sur ce contenu. Il est ensuite possible de contrôler l'intégrité du contenu (l'absence de modification) en recalculant l'empreinte numérique pour la comparer à la valeur initiale ou au cachet. Du point de vue technique, l'empreinte numérique s'appuie sur une fonction de hachage cryptographique résistante aux collisions, et le cachet sur la combinaison d'une empreinte générée par une telle fonction et d'une signature numérique. Un scellement peut concerner un ensemble de fichiers.

Le terme scellement fait référence aux sceaux de cire sur les parchemins ou aux scellés judiciaires placés sur des éléments dont on veut pouvoir détecter l'ouverture ou la modification.

Les recommandations suivantes complètent les recommandations relatives à l'application de vote (R35★). Les empreintes calculées par ces deux recommandations sont recalculées et comparées automatiquement et régulièrement. Les empreintes sont également étendues à d'autres éléments du système de vote, notamment la configuration de l'élection.

R45 ★★ Mettre en œuvre des scellements sur le système de vote

Le système de vote doit mettre en œuvre des scellements, par exemple en suivant les *Recommandations de configuration d'un système GNU/LINUX* [7] : une opération de scellement d'un système de fichiers peut consister en l'installation puis la configuration d'un service qui aura pour objectif de vérifier périodiquement les modifications faites au niveau d'une arborescence.

Dans ce cas, les scellements doivent être conformes aux *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* [18] et notamment porter sur les éléments suivants :

- Avant l'ouverture du scrutin :
  - Les données relatives à l'application de vote (R35★).
  - Les données relatives à la configuration de l'élection. La configuration inclut notamment le découpage électoral, les options de vote et l'ordre dans lequel elles sont présentées aux électeurs, la liste électorale, les heures d'ouverture et

de fermeture du scrutin, la clé publique de l'élection et les éventuels secrets de signature numérique (en particulier des preuves de vote quand elles sont mises en œuvre), de chaînage ainsi que le pastillage.

- À la clôture du scrutin : sur l'urne électronique et la liste d'émargement.
- À la fin du dépouillement sur l'ensemble des données générées (fichiers de résultats, procès-verbaux, preuves générées par le système de vote, le cas échéant).

R46 ★★

Vérifier les scellements périodiquement et aléatoirement

Le système de vote doit vérifier périodiquement les scellements mis en œuvre.

Dans ce cas, le déclenchement de cette vérification doit être aléatoire afin de rendre les contrôles non prévisibles. La fréquence des contrôles doit dissuader une tentative d'intervention non autorisée sur le système de vote et doit assurer une détection rapide de toute altération.

En plus des scellements, le contrôle de l'intégrité du système est assuré par de la supervision de l'état du système de vote (R43★★) et des accès au système de vote, déjà limités (R26★).

R47 ★★

Surveiller les accès au système de vote

Il est recommandé que le prestataire effectue une supervision technique des accès au système de vote, notamment les accès distants aux serveurs, au système de gestion des bases de données et aux équipements réseau.

Enfin, l'objectif 2-02 requiert la mise à disposition du bureau électoral du résultat du contrôle de cohérence entre l'urne électronique et la liste d'émargement et des scellements, et la mise à disposition du journal des événements.

R48 ★★

Fournir au bureau électoral les résultats des contrôles d'intégrité

Le prestataire doit fournir au bureau électoral les résultats des différents contrôles d'intégrité mis en œuvre par le système de vote :

- Contrôle de l'intégrité de l'application de vote (R35★).
- Contrôle de cohérence entre l'urne et la liste d'émargement décrit (R36★).
- Contrôle des scellements (R46★★).

R49 ★★

Permettre l'analyse du journal des événements par un tiers

Le prestataire doit permettre à un tiers d'analyser les journaux collectés pendant les opérations, contenant les événements relatifs au fonctionnement du système de vote (R38★) ainsi que les événements ayant un impact sur la sincérité du scrutin (R39★).

Le prestataire doit s'assurer que les libellés des événements sont suffisamment compréhensibles pour que le tiers puisse en réaliser l'analyse en toute autonomie. Le

prestataire doit être en mesure de fournir une explication sur l'ensemble des événements enregistrés, à la demande du tiers.

Le prestataire doit également s'assurer que lorsque ces événements intègrent les résultats des opérations de signature numérique, de chaînage ou d'horodatage des bulletins (R27★), il rend disponible toute donnée nécessaire à leur vérification et fournit toute explication permettant au tiers de la réaliser.

Pour aller plus loin

Cet objectif est renforcé par l'objectif 2-03 sur la surveillance du système par le bureau électoral et par l'objectif 2-04 sur la mise en place d'alerte en cas de détection de rupture de scellement ou de détection d'incident lors de la supervision du système.

Objectif n° 2-03

Permettre le déclenchement manuel par le bureau électoral des contrôles mentionnés dans l'objectif 2-02. Prévoir la formation du bureau électoral au fonctionnement des outils de contrôle dont il dispose.

Cet objectif renforce l'objectif 2-02 relatif à la surveillance effective du vote. Il donne la possibilité au bureau électoral de déclencher manuellement et en autonomie un contrôle de l'intégrité sur le système de vote.

Ces contrôles doivent être possibles pendant toute la période pendant laquelle des scellements sont posés sur le système de vote, depuis la pose des scellements qui précède l'ouverture du scrutin, jusqu'à la pose des scellements qui suit le dépouillement (voir R45★★).

R50 ★★

Permettre au bureau électoral de déclencher manuellement les contrôles d'intégrité

Le prestataire doit permettre au bureau électoral de déclencher manuellement et en autonomie (sans intervention du prestataire ni de l'organisateur du scrutin) les contrôles d'intégrité prévus à l'objectif 2-02 :

- Contrôle de l'intégrité de l'application de vote (R35★).
- Contrôle de cohérence entre l'urne électronique et la liste d'émargement (R36★).
- Contrôle des scellements (R45★★).

Les contrôles manuels doivent pouvoir être déclenchés pendant toute la période de vote.

Pour aller plus loin

Cet objectif est renforcé par l'objectif 2-04 sur la mise en place d'alerte en cas de détection de rupture de scellement ou de détection d'incident lors de la supervision du système.

Objectif n° 2-04

Assurer que le bureau électoral soit alerté automatiquement et immédiatement de tout incident de sécurité et de toute intervention de gestion ou de maintenance survenant sur le système de vote électronique et dispose d'un accès à un journal de ces alertes.

Cet objectif renforce la surveillance effective du vote des objectifs 2-02 et 2-03. Il concerne la mise en place d'alertes *à destination* du bureau électoral en cas d'incident de sécurité sur le système de vote. Les alertes concernent directement le secret du scrutin, la sincérité des opérations électorales, l'intégrité des suffrages exprimés, l'accès au vote pour tous les électeurs ou concernent des événements qui peuvent avoir un impact sur ces principes.

R51 ★★ Alerter le bureau électoral en cas d'incident de sécurité sur le système de vote

Le système de vote doit émettre des alertes à destination du bureau électoral pour tout événement ou incident relatif à la sécurité du système de vote, ayant un impact sur le secret du scrutin, la sincérité des opérations électorales, l'intégrité des suffrages exprimés, l'accès au vote pour tous les électeurs

Ces alertes doivent être générées et être transmises automatiquement et sans délai par le système de vote, sans que le prestataire n'ait à intervenir pour qu'elles parviennent au bureau électoral. Toute modification du système d'alerte doit également générer une alerte automatique au bureau électoral.

Le système de vote (dont le système de détection mis en œuvre au titre de la R37★) doit générer une alerte à destination du bureau électoral notamment dans les cas suivants :

- Échec d'un traitement de l'opération de vote (1-02, R7★).
- Incohérence entre l'urne électronique et la liste d'émargement (1-02, R36★).
- Attaque par recherche d'authentifiants (1-03, R11★).
- Accès illégitime au système de vote (2-02, R47★★).
- Modification de bulletin transmis par un électeur, traité par le serveur de vote et stocké dans l'urne électronique (1-06, R27★).
- Modification de clé privée ou de secret de signature numérique, de chaînage ou de scellement (1-06, 2-02) ou de signature des preuves de vote (2-07).
- Modification des données publiques intervenant dans la vérification des mécanismes cryptographiques mis en œuvre pour contrôler la validité ou l'intégrité des données (signature, chaînage, horodatage, preuves à divulgation nulle de connaissance) (1-04, 1-07, 1-08, 1-11).
- Tentative de dépouillement illégitime : dépouillement avant la clôture ou dépouillement sur un ensemble de bulletins non autorisé (1-09, R33★).
- Indisponibilité, attaque en déni de service sur le système de vote (2-01, R43★★, R44★★).
- Rupture d'un scellement (2-02, R46★★).

Le prestataire doit trouver un équilibre évitant de trop nombreuses alertes superflues (ex. : un électeur s'est trompé en entrant son mot de passe) tout en signalant des évènements significatifs pour la sécurité (ex. : incohérence entre l'urne et l'émargement).

R52 ★★

Alerter le bureau électoral de toute intervention de gestion et de maintenance

Le prestataire doit mettre en œuvre un système d'alerte à destination du bureau électoral, l'informant de toute intervention de gestion et de maintenance sur le système de vote.

Ces alertes doivent être générées et être transmises automatiquement par le système de vote, sans que le prestataire n'ait à intervenir pour qu'elles parviennent au bureau électoral. Toute modification du système d'alerte doit également générer une alerte automatique vers le bureau électoral.

Attention

Même lorsque les recommandations R51★★ et R52★★ sont correctement mises en œuvre, le prestataire peut toujours réaliser des actions ne générant pas d'alerte et porter atteinte aux principes fondamentaux qui commandent les opérations électorales.

Reposer sur les alertes pour vérifier ces principes est donc un compromis qui fait l'hypothèse que le système de vote est de confiance.

Pour les principes d'intégrité des suffrages exprimés et de sincérité des opérations électorales, cette hypothèse peut être dépassée en appliquant le principe d'indépendance logicielle, décliné aux objectifs 2-07 (vérifiabilité individuelle) et 3-02 (vérifiabilité universelle).

Pour aller plus loin

Cet objectif est renforcé par les objectifs objectifs 2-07 (propriété recorded-as-cast) et 3-02 (propriété tallied-as-recorded).

Objectif n° 2-05

Assurer un cloisonnement entre les systèmes de vote électronique de chaque scrutin de sorte qu'aucune donnée ne puisse être échangée entre ces systèmes et qu'il soit possible de suspendre ou de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours.

Le bureau électoral doit avoir toute liberté pour décider de suspendre ou de stopper un scrutin sans que cela empêche d'autres scrutins de continuer [30]. Les autres scrutins sont d'abord ceux du même organisateur, mais également ceux d'autres clients du prestataire.

Information

Le pastillage (Objectif 1-04, Annexe E) introduit la notion de scrutin *direct* et de scrutin *indirect*. Seuls les scrutins *directs* peuvent être suspendus ou stoppés. Les scrutins *indirects* dépendent de l'état du scrutin direct auquel ils sont associés.

Les différents types de cloisonnement

Pour suspendre ou stopper un scrutin sans que cela ait un impact sur d'autres scrutins se déroulant en même temps, la solution la plus courante est de séparer les scrutins au niveau de l'application de vote. Le système de vote est ainsi conçu pour gérer plusieurs scrutins indépendamment les uns des autres, en distinguant notamment l'état de chacun (par exemple : à venir, en cours, stoppé, clos). On parle dans ce cas de *cloisonnement applicatif*.

D'autres types de cloisonnement peuvent être mis en œuvre pour compléter le cloisonnement applicatif. Les scrutins de différents clients du même prestataire peuvent être gérés par des instances distinctes du système de vote, chacune exécutée par des ressources virtuelles (ex. : machines virtuelles) dédiées au client. On parle alors de *cloisonnement logique*.

Dans d'autres cas, les ressources dédiées à chaque client du prestataire peuvent être physiquement distinctes : des serveurs physiques différents sont attribués à chaque système de vote. On parle dans ce cas de *cloisonnement physique*. Ce type de cloisonnement peut se justifier d'abord par l'ampleur du ou des scrutins du client (nombre important de votants) et parfois en tant que mesure de sécurité avancée.

Risques associés aux différents types de cloisonnement

Le type d'hébergement choisi pour la solution de vote peut avoir un impact sur le cloisonnement entre scrutins. En reprenant la description des offres fournie dans les *Recommandations pour l'hébergement dans le Cloud des systèmes d'information sensibles* [6], et en fonction du modèle de confiance, le choix de l'offre sera adapté aux besoins de l'organisateur du scrutin et, le cas échéant, aux conclusions de l'analyse des risques (3-01).

Une offre s'appuyant sur un cloisonnement *applicatif*, mutualisant les scrutins de plusieurs organisateurs sur un seul système de vote, crée des contraintes opérationnelles significatives. Par

30. Tant que le scrutin est suspendu ou dès qu'il est stoppé, les électeurs ne peuvent plus enregistrer leur vote.

exemple, si un problème applicatif est détecté et qu'il affecte les scrutins d'un organisateur particulier, il peut être nécessaire d'intervenir sur le système de vote pour mettre en œuvre un correctif. Cette intervention pourrait entraîner une interruption technique de tous les scrutins, et devrait déclencher une alerte à tous les organisateurs de scrutin (2-04). Ces contraintes opérationnelles doivent être évaluées et acceptées.

Une offre s'appuyant sur un cloisonnement *logique*, dédiant un système de vote virtuel à chaque organisateur, n'est pas sujette aux mêmes contraintes opérationnelles. Chaque système virtuel peut être opéré – démarré, corrigé, stoppé – indépendamment suivant les besoins et contraintes de l'organisateur. Ce cloisonnement logique semble plus adapté que du cloisonnement applicatif pour des scrutins de niveau 3.

Enfin, une offre s'appuyant sur un cloisonnement *physique* va limiter les possibilités de latéralisation d'un attaquant par rapport à un cloisonnement logique. Par exemple, si deux applications partagent un même serveur physique, l'attaquant ayant compromis une des applications pourrait se latéraliser à travers l'hyperviseur du serveur physique et compromettre la seconde application. Si le système de vote dispose d'un serveur physique dédié, ce type de latéralisation n'est pas possible.

Cependant, si l'application gérant les différents scrutins est la même, et si l'exposition des différents scrutins à Internet est similaire, alors le cloisonnement physique n'est pas pertinent : si un des systèmes est compromis, les autres peuvent probablement l'être aussi par le même moyen. En revanche, si le serveur physique pouvait être commun à des systèmes de vote et à d'autres usages (hébergement dans un Cloud public), alors le choix de dédier le serveur physique à des systèmes de vote peut être mieux justifié.

Ainsi, pour des scrutins de niveau 3, si une offre mutualisée est choisie, il convient d'intégrer ses spécificités à l'analyse de risques. Si l'analyse conclut à la compatibilité d'une telle offre avec les objectifs de sécurité, alors l'offre devient acceptable pour cet usage. Il convient alors d'accepter les risques résiduels associés à la mutualisation : compromission par d'autres clients du prestataire de vote ou d'autres clients de l'hébergeur, compromission par l'hébergeur lui-même.

Si ces risques ne sont pas acceptables, alors un hébergement sur un Cloud de confiance (par exemple qualifié SecNumCloud) ou un hébergement internalisé et sécurisé peuvent fournir des alternatives.

R53 ★★

Rendre indépendant le déroulement des différents scrutins

Le système de vote doit gérer le déroulement des différents scrutins de façon à pouvoir stopper totalement un scrutin sans que cela ait un impact sur les autres scrutins en cours [31].

Le cloisonnement entre les scrutins peut être applicatif ou logique ou (optionnellement) physique, en fonction des besoins de l'organisateur.

31. « Autres scrutins » signifie les autres scrutins de l'organisateur et les autres scrutins gérés par le prestataire pour d'autres clients que l'organisateur.

Objectif n° 2-06

Utiliser un système d'information mettant en œuvre les mesures de sécurité physique et logique recommandées par les éditeurs des briques applicatives constituant la solution de vote, par la CNIL et par l'ANSSI.

Le présent document a déjà renvoyé à des guides de l'ANSSI décrivant des bonnes pratiques applicables au système de vote : les mécanismes cryptographiques (1-01), l'authentification (1-03), la mise en place de TLS (1-05), la sauvegarde et la journalisation (1-06), la protection contre les attaques en déni de service (2-01). L'objectif 2-06 ajoute des références à des bonnes pratiques pour le développement, le durcissement, l'administration et la sécurité physique du système de vote.

Attention

La sécurité de la solution de vote peut dépendre d'autres systèmes qui ne sont pas directement opérés par le prestataire (sous-traitants pour les envois d'email et de SMS, horodatage, solution d'authentification). Le prestataire, ou l'organisateur le cas échéant, doivent cependant s'assurer, notamment contractuellement, de la sécurité de ces autres systèmes.

Le guide *Recommandations pour la mise en œuvre d'un site Web* [11] fournit des règles en matière de sécurité des applications Web, applicables au serveur de vote et au client de vote. Un point d'attention est que toutes les recommandations de ce guide reposent sur l'hypothèse que le navigateur est de confiance (plus largement, que l'équipement connecté à Internet utilisé par l'électeur est de confiance, voir 3.2.2). Dans le contexte du vote par Internet, cette hypothèse peut être précisée : les fonctions appelées par le client de vote respectent la confidentialité et l'intégrité de l'expression du vote, et les mécanismes cryptographiques implémentés par le navigateur et appelés par le client de vote sont conformes à l'état de l'art.

En complément, la page Web *OWASP Top 10* [82] est un rapport mis à jour régulièrement par l'organisation OWASP, qui se concentre sur les 10 risques les plus critiques des applications Web. Ce rapport fournit également les bonnes pratiques pour se prémunir contre ces risques. Ces bonnes pratiques renforcent le secret du scrutin, la sincérité des opérations électorales, l'intégrité des suffrages exprimés, l'accès au vote pour tous les électeurs car elles protègent le système de vote contre des attaques internes et externes.

R54 ★★

Suivre les bonnes pratiques pour le développement du système de vote

Il est recommandé que le prestataire suive les bonnes pratiques pour développer le système de vote, telles que les *Recommandations pour la mise en œuvre d'un site Web : maîtriser les standards de sécurité côté navigateur* [11] de l'ANSSI et les recommandations du *TOP 10 OWASP* [82].

Le prestataire doit durcir la configuration système de l'ensemble des composants techniques du système de vote, composants identifiés par la cartographie (R4★). Pour cela, en application du principe de défense en profondeur, le prestataire doit suivre les bonnes pratiques applicables fournies par les éditeurs ou par des tiers.

Pour les systèmes reposant sur LINUX, les *Recommandations de configuration d'un système GNU/LINUX* [7] fournissent des indications pour les durcir avec des niveaux cumulatifs : minimal, intermédiaire, renforcé et élevé. Les mesures de niveau minimal sont de l'ordre de l'hygiène informatique et peuvent être appliquées directement. Certaines mesures de niveau expert, concernant l'intégrité des systèmes, peuvent également être prises en compte. Les autres mesures de niveau expert nécessitent des compétences fortes en administration système et reviennent à la conception d'un système dédié pour le vote électronique qui devra faire l'objet d'un suivi spécifique, aussi elles ne sont pertinentes que si de telles compétences sont réellement mobilisables. Un durcissement analogue peut être effectué sur l'ensemble des composants sur lesquels transitent les bulletins, d'une part, et sur lesquels sont stockés les bulletins, d'autre part.

R55 ★★

Suivre les bonnes pratiques pour le durcissement du système de vote

Il est recommandé que le prestataire suive les bonnes pratiques de durcissement des systèmes, telles que les *Recommandations de configuration d'un système GNU/LINUX* [7].

Il est recommandé que le prestataire suive les bonnes pratiques de durcissement des composants techniques du système de vote identifiés par la cartographie (R4★), telles que les recommandations des éditeurs des briques applicatives, celles issues de la liste *National Checklist Program for IT Product* [79] ou celles émises par le *Center for Internet Security* [32].

Les administrateurs du système de vote (qu'ils soient du prestataire ou de l'organisateur du scrutin) ont un rôle essentiel pour assurer le secret du scrutin, la sincérité des opérations électorales, l'intégrité des suffrages exprimés, l'accès au vote pour tous les électeurs. Les *Recommandations relatives à l'administration sécurisée des systèmes d'information* [12] fournissent des indications pour mettre en œuvre leurs accès privilégiés au système de vote.

R56 ★★

Suivre les bonnes pratiques pour l'administration du système de vote

Il est recommandé que le prestataire et l'organisateur du scrutin suivent les bonnes pratiques pour l'administration du système de vote, telles que les *Recommandations relatives à l'administration sécurisée des systèmes d'information* [12].

En cas d'administration partagée entre l'organisateur du scrutin et le prestataire pour assurer les opérations de gestion et de maintenance, les accès au système de vote doivent suivre la même politique de sécurité, notamment concernant la journalisation des événements (R38★, R39★) et les alertes (R52★★).

Enfin, la sécurité physique des composants techniques est essentielle pour assurer le secret du scrutin, la sincérité des opérations électorales, l'intégrité des suffrages exprimés, l'accès au vote pour tous les électeurs, car un accès physique illégitime donne accès en lecture ou en modification aux données sensibles (notamment les fragments de la clé privée de l'élection, l'urne électronique, la liste d'émargement, la configuration de l'élection, l'application de vote). Les *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection* [9] fournissent des indications pour mettre en œuvre des contrôles d'accès physique à ces composants.

R57 ★★

Suivre les bonnes pratiques pour la sécurité physique du système de vote

Il est recommandé que le prestataire et l'organisateur du scrutin suivent les bonnes pratiques pour assurer la sécurité physique des composants techniques du système de vote, telles que les *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection* [9].

Objectif n° 2-07

Permettre aux électeurs de vérifier la présence de leur bulletin dans l'urne pendant le scrutin ainsi que sa présence dans l'urne utilisée pour le dépouillement jusqu'à expiration des délais de recours.

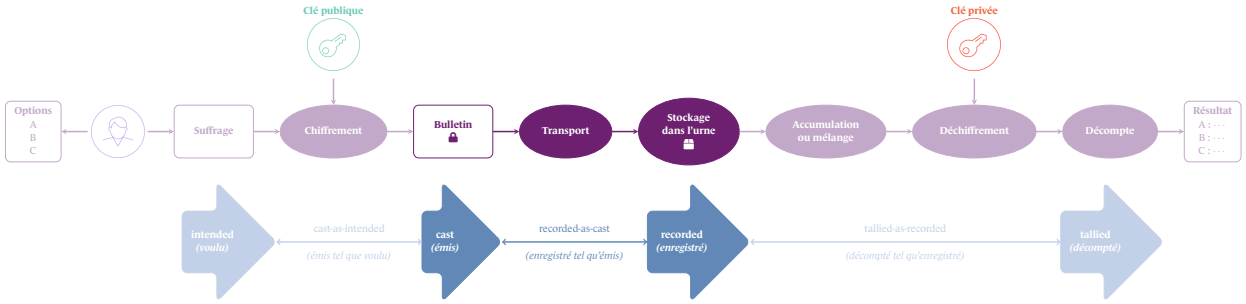

FIGURE 14 – Propriété recorded-as-cast

Cet objectif, illustré en Figure 14, correspond à la propriété appelée recorded-as-cast (le bulletin est *enregistré dans l'urne électronique* tel qu'*émis* par l'électeur), qui constitue une partie de la vérifiabilité individuelle. Sa mise en œuvre repose sur la fourniture d'une preuve de vote et la publication des données associées [32]. Cet objectif renforce la sincérité des opérations électorales, l'intégrité des suffrages exprimés ainsi que la surveillance effective du vote et constitue une mise en œuvre du principe d'indépendance logicielle.

Le système de vote doit fournir à l'électeur une preuve de vote contenant une référence calculée à partir de son bulletin. Le système de vote doit également rendre publiques l'ensemble des données permettant aux électeurs de vérifier la présence de leur bulletin dans l'urne. La preuve de vote n'a pas le même objet que le récépissé de vote [33]. Comme expliqué à la recommandation R8★, la preuve de vote, associée au récépissé, ne doit pas porter atteinte au secret du scrutin.

R58 ★★

Fournir aux électeurs une preuve de vote pour la vérification de présence dans l'urne

Le client de vote doit générer une preuve de vote, permettant à l'électeur de vérifier la présence de son bulletin dans l'urne. L'électeur peut conserver la preuve de vote.

La preuve de vote contient une référence cryptographiquement liée au bulletin (par exemple une empreinte numérique du bulletin ou bien une preuve à divulgation nulle de connaissance), calculée au moment où le votant valide son suffrage.

La preuve de vote ne doit pas contenir l'identité de l'électeur ni l'horodatage de son vote. La preuve de vote ne doit pas non plus contenir de données qui, seules ou ajoutées aux informations fournies par le récépissé de vote, portent atteinte au secret du scrutin ou facilitent l'achat de vote.

La référence est transmise au serveur de vote pour publication.

Il est recommandé que la preuve de vote contienne également une signature de cette

32. L'objectif ne concerne par contre pas la propriété appelée cast-as-intended (le bulletin est *émis* tel que *voulu* par l'électeur), qui constitue l'autre partie de la vérifiabilité individuelle.
33. L'objectif 1-02 mentionne la délivrance d'un récépissé. Ce récépissé a pour objet de matérialiser l'émargement de l'électeur, et pas de fournir à l'électeur un moyen de vérifier la présence de son bulletin dans l'urne.

référence par le serveur de vote.

Attention

La preuve de vote doit être générée et présentée à l'électeur par le client de vote et pas par le serveur de vote. Cela assure au client de vote (et à l'électeur) que la preuve de vote correspond bien au bulletin qu'il vient de générer et pas à un autre bulletin.

Par ailleurs, la signature numérique de la référence par le serveur de vote est fortement recommandée. Le serveur de vote calcule et retourne la signature au client de vote à la fin de l'opération de vote (R7★). Cette condition assure l'authenticité de la preuve de vote : un client de vote ne peut pas générer de preuve de vote authentique pour un bulletin qui n'est pas enregistré par le serveur de vote.

Lorsque le serveur de vote réalise la signature numérique des bulletins (R27★), ce service peut être utilisé pour réaliser la signature des preuves de vote.

R59 ★★

Publier les informations nécessaires à la vérification de présence dans l'urne

Le serveur de vote doit rendre publique une liste des références présentes dans les preuves de vote transmises par les clients de vote sur une page Web accessible sans restriction depuis Internet.

Le serveur de vote doit également rendre publique la clé publique de vérification de la signature des références dans les preuves de vote, également sur sur une page Web accessible sans restriction depuis Internet.

Pendant le scrutin et jusqu'à expiration des délais de recours, les électeurs doivent disposer d'un moyen pour contrôler que la référence présente dans leur preuve de vote et correspondant à leur bulletin est bien présente dans la liste des références rendue publiquement disponible par le système de vote et que sa signature est correcte.

Pour aller plus loin

Cet objectif est complété par l'objectif 3-02 relatif à la propriété tallied-as-recorded, et renforcé par l'objectif 3-05 qui concerne la publication du code source du client de vote.

Objectif n° 2-08

Authentifier les électeurs en s'assurant que la vraisemblance d'une usurpation d'identité est négligeable.

Les deux recommandations R9★ et R10★ sont applicables aux scrutins de niveau 1 mais doivent être complétées pour les scrutins de niveaux 2 : il est recommandé d'utiliser deux secrets d'authentification.

L'objectif 1-03 rappelle que l'usurpation d'identité peut porter atteinte au caractère personnel du vote et à la sincérité des opérations électorales. Afin d'en diminuer la vraisemblance, cet objectif renforce l'objectif 1-03 en imposant, en pratique, un second facteur d'authentification, en plus de celui imposé par les deux recommandations R9★ et R10★. Suivant la recommandation mise en œuvre, ce second facteur peut être lui aussi dédié au scrutin, ou bien relever d'une solution d'authentification existante, externe à la solution de vote.

R60 ★★

Combiner deux secrets d'authentification dont un dédié au scrutin

Pour renforcer l'authentification des électeurs, le système de vote doit combiner deux secrets d'authentification, dont un dédié au scrutin. Les cas suivants sont possibles :

- Utiliser une solution d'authentification externe combinée avec un secret d'authentification dédié au scrutin.
- Utiliser deux secrets d'authentification dédiés au scrutin, transmis par deux canaux différents.

Comme rappelé à l'objectif 1-03 :

- *Une identité numérique de niveau faible* (non évaluée) ne peut pas, seule, répondre à l'objectif 2-08. Il n'est acceptable d'y recourir qu'en complément d'un secret d'authentification dédié au scrutin (R10★).
- *Une identité numérique de niveau substantiel ou élevé* (évaluée par l'ANSSI) pourrait répondre seule à l'objectif 2-08, sans recours à un secret dédié au scrutin.

Pour aller plus loin

Pour en savoir plus sur l'identité numérique, se reporter au dossier thématique de la CNIL consacré à ce sujet [39].

Objectif n° 2-09

Favoriser la transparence et l'auditabilité de la solution de vote en rendant public, en amont du scrutin, le protocole de vote ainsi que les propriétés de sécurité garanties par ce protocole et le moyen de les atteindre.

Pour les scrutins de niveau 2, une première étape de transparence est demandée au prestataire : rendre publics le protocole de vote utilisé, les propriétés de sécurité prétendument atteintes, ainsi que le modèle de confiance associé. Le protocole de vote est une modélisation théorique des opérations réalisées par un électeur, via le client de vote et le serveur de vote qui réceptionne et traite l'ensemble des bulletins des électeurs. Cette transparence renforce la sincérité des opérations électorales, l'intégrité des suffrages exprimés ainsi que la surveillance effective du vote.

L'usage d'un protocole de vote non éprouvé académiquement doit ainsi être évité. Aussi le prestataire doit fournir les références académiques correspondant au protocole qu'il met en œuvre. Des exemples de spécifications publiques de protocoles de vote sont fournis dans [1, 45, 49, 57, 66, 85, 92].

R61 ★★

Rendre public le protocole de vote

En amont du scrutin, le prestataire doit rendre public le protocole de vote qu'il met en œuvre dans le système de vote sans préjudice de la propriété intellectuelle du prestataire. Cette publication peut typiquement s'effectuer sur une page Web accessible sans restriction depuis Internet. Cette publication doit notamment comprendre :

- Les messages échangés entre tous les acteurs, l'ordre dans lequel ces messages sont échangés, les traitements effectués à chaque étape par chaque acteur (notamment la récupération ou le stockage de données intermédiaires, l'affichage ou la demande d'information à l'utilisateur, la vérification de signature numérique, les preuves à divulgation nulle de connaissance, les tests d'égalité). La description doit être aussi précise que possible pour chaque acteur.
- Les éventuelles références académiques sur lesquelles s'appuie le protocole utilisé, ainsi que les éventuels écarts avec ces références.
- Les mécanismes cryptographiques mis en œuvre pour assurer la confidentialité et l'intégrité des données tout au long du scrutin.
- Les propriétés de sécurité prétendument atteintes, leur modèle de confiance et un argumentaire décrivant comment ces propriétés sont atteintes.
- Les composants et acteurs intervenant dans l'élection (notamment client de vote, serveur de vote, électeur, bureau électoral).
- La description des cérémonies, notamment celles faisant intervenir le bureau électoral.

La description des échanges doit permettre à un tiers de contrôler que les propriétés de sécurité prétendument atteintes le sont réellement. Cette analyse de sécurité doit être autorisée pour *tout tiers* (et pas seulement l'expert indépendant au sens de la délibération de la CNIL [72]), sur la base des spécifications publiées. Un point de

contact doit être identifié pour rendre possible la divulgation responsable d'éventuelles faiblesses identifiées par les tiers.

Attention

La conception et l'évaluation de protocoles cryptographiques interactifs, tels que les protocoles de vote, sont des tâches très spécialisées. L'invention de protocoles originaux est fortement déconseillée à des non-spécialistes : en effet, même si les mécanismes cryptographiques utilisés par le système de vote sont conformes à l'état de l'art, un mauvais *agencement* de ces mécanismes peut porter atteinte aux principes fondamentaux qui commandent les opérations électorales, en particulier le secret du scrutin, la sincérité des opérations électorales et l'intégrité des suffrages exprimés.

De plus, selon le principe fondamental de Kerckhoffs, la sécurité des protocoles cryptographiques, tels que les protocoles de vote, doit être assurée, y compris face à un attaquant disposant de leurs spécifications.

4.3 Objectifs de sécurité de niveau 3

Définition de la CNIL [72] : **Niveau 3 (risques significatifs)** : *les sources de menace (parmi les votants, les organisateurs du scrutin, les prestataires du système de vote, les personnes extérieures, etc.) peuvent présenter des ressources importantes ou de fortes motivations. Ce niveau concerne principalement les scrutins qui impliquent un nombre de votants important et qui présentent un enjeu élevé pour les candidats ou se déroulent dans un climat potentiellement conflictuel. Il peut par exemple s'agir d'élections organisées au sein d'ordres professionnels réglementés, des primaires de partis politiques, ou d'élections de représentants du personnel au sein d'organisations importantes.*

Modèle de confiance : Pour ce niveau, le système de vote peut être attaqué par des attaquants internes ou externes, avec des ressources importantes. Les recommandations de ce niveau complètent celles du niveau 2 et visent à renforcer la sincérité des opérations électorales par la vérifiabilité universelle et à renforcer le secret du scrutin par la maîtrise de la clé privée de l'élection. La vérifiabilité individuelle, le contrôle par le bureau électoral, la disponibilité du système et la transparence, initiés aux niveaux 1 et 2, sont également renforcés. La Figure 15 présente les objectifs de sécurité de la CNIL correspondant à des scrutins de niveau 3.

3-01	Effectuer une analyse de risque selon une méthode éprouvée afin de définir les mesures les plus adéquates au contexte spécifique du scrutin.
3-02	Assurer que le bon dépouillement de l'urne peut être vérifié *a posteriori*, y compris par un outil tiers, sans affaiblir le secret du scrutin.
3-03	Assurer, durant la période d'ouverture du scrutin, une très haute disponibilité du système de vote électronique et des services tiers nécessaires à son fonctionnement, en prenant notamment en compte les risques d'avarie majeure comme la perte d'un centre de données.
3-04	Renforcer le caractère secret du scrutin en ne manipulant jamais le secret permettant leur dépouillement sur un serveur qui serait en capacité de rapprocher l'identité des électeurs et leur bulletin.
3-05	Favoriser la transparence de la solution de vote et la confiance des électeurs en rendant public, en amont du scrutin, le code source des éléments du système de vote ayant vocation à être exécutés sur le terminal de l'électeur, y compris dans un navigateur.

FIGURE 15 – Objectifs de sécurité de niveau 3

Attention

La conformité au niveau 3 ne fournit pas de protection contre un attaquant disposant de ressources élevées (comme un État), de complicités internes chez l'organisateur ou chez le prestataire, ou présentant de fortes motivations (dont la déstabilisation). Pour ce niveau d'attaquant, des mesures complémentaires doivent être envisagées (cf. 4.4).

Objectif n° 3-01

Effectuer une analyse de risque selon une méthode éprouvée afin de définir les mesures les plus adéquates au contexte spécifique du scrutin.

L'organisateur du scrutin peut réaliser une première estimation de la sensibilité de son scrutin avec la grille d'analyse fournie dans la délibération de la CNIL [72]. Lorsque l'application de cette grille donne un niveau de risque égal à 3, l'organisateur du scrutin doit compléter cette première analyse au moyen d'une méthode plus fine telle que la méthode EBIOS-RM, détaillée dans le guide *La méthode EBIOS Risk Manager* [17].

Le contexte spécifique du scrutin peut influer sur plusieurs hypothèses de l'analyse de risque :

- Les sources de menace (parmi les votants, les organisateurs du scrutin, les prestataires du système de vote, les personnes extérieures, etc.) présentent des ressources ou des motivations plus importantes, par exemple en lien avec un contexte social conflictuel.
- Les procédures et les cérémonies habituellement prévues par le prestataire ne sont finalement pas réalisables pour le scrutin.
- Le succès de l'élection repose sur des parties prenantes insuffisamment fiables ou maîtrisées.

L'analyse de risques doit tenir compte des différents audits et du rapport de l'expert indépendant. Tout écart par rapport aux objectifs de sécurité fixés par la CNIL et plus généralement aux principes fondamentaux qui commandent les opérations électorales doit être étudié et si possible réduit, pour ne pas s'exposer à des contentieux.

Une fois les risques évalués, l'organisateur doit concevoir et mettre en œuvre un plan de traitement des risques. Des mesures de sécurité complémentaires peuvent réduire la vraisemblance ou la gravité de chaque risque. L'organisateur en déduit finalement les risques résiduels.

R62 ★★★

Effectuer une analyse de risque selon une méthode éprouvée

L'organisateur du scrutin doit effectuer une analyse de risque selon une méthode éprouvée, telle que la méthode EBIOS-RM, portant sur la solution de vote.

L'organisateur doit tenir compte du contexte spécifique du scrutin, des différents audits et du rapport de l'expert indépendant (au sens de la délibération de la CNIL [72]) dans l'évaluation des sources de menaces et des risques, et dans la conception du plan de traitement de risques.

Pour aller plus loin

La Section 4.4 propose des recommandations complémentaires permettant de traiter certains risques spécifiques.

Objectif n° 3-02

Assurer que le bon dépouillement de l'urne peut être vérifié *a posteriori*, y compris par un outil tiers, sans affaiblir le secret du scrutin.

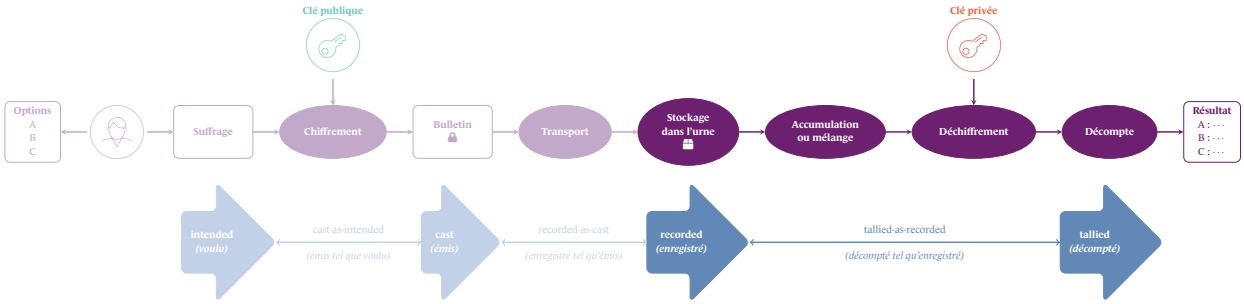

FIGURE 16 – Propriété tallied-as-recorded

Cet objectif, illustré en Figure 16, correspond à la propriété appelée tallied-as-recorded (le bulletin est *décompté* tel qu'*enregistré* dans l'urne), qui constitue une partie de la vérifiabilité universelle [34]. Par rapport à l'objectif 1-11, cet objectif renforce le secret du scrutin, la sincérité des opérations électorales, l'intégrité des suffrages exprimés ainsi que la surveillance effective du vote, en particulier car il introduit la notion d'*outil tiers*.

L'objectif 1-11 expose les limites de l'exécution d'un nouveau décompte, notamment à cause de sa portée et du risque sur le secret du scrutin. La portée de l'exécution d'un nouveau décompte peut être renforcée par l'utilisation d'un outil tiers, cependant, afin de ne pas affaiblir le secret du scrutin, les hypothèses suivantes doivent être satisfaites en cas d'utilisation d'un tel outil :

- L'urne électronique, ainsi que la clé privée de l'élection, doivent pouvoir être fournies à un tiers exécutant le nouveau décompte, sans que cette fourniture ne porte atteinte au secret du scrutin. Le point de départ étant l'urne électronique, cela suppose que le déchiffrement des bulletins stockés dans l'urne électronique ne porte pas atteinte au secret du scrutin, c'est-à-dire que l'étanchéité électeur/suffrage repose entièrement sur l'étanchéité électeur/bulletin et pas du tout sur l'étanchéité bulletin/suffrage. Cette hypothèse est discutée à l'objectif 1-07.
- Un électeur doit pouvoir fournir son bulletin à un tiers disposant de la clé privée de l'élection, ou même récupérer cette clé, sans que cette fourniture ou cette récupération ne lui permettent de prouver son suffrage (propriété receipt-freeness R30★). Cela suppose que le déchiffrement d'un bulletin *lié à l'identité de l'électeur* ne permet pas de rapprocher son contenu (le suffrage) de cette identité.

Une alternative à l'exécution d'un nouveau décompte reposant sur ces hypothèses est la *vérification* que le résultat issu du dépouillement (englobant donc l'accumulation ou le mélange, le déchiffrement et le décompte) correspond à l'urne électronique.

- Si le système de vote met en œuvre l'accumulation des bulletins, cette opération ne nécessitant pas de secret ou d'aléa, elle est vérifiable : il suffit de la répéter à l'identique.
- Si le système de vote met en œuvre un mélange cryptographique, celui-ci n'est pas forcément vérifiable : il peut être étendu afin de générer un ensemble de preuves mathématiques que le

34. L'objectif ne concerne par contre pas la propriété appelée vérifiabilité de la légitimité, qui constitue l'autre partie de la vérifiabilité universelle. Cette dernière propriété est évoquée à la Section 4.4.

mélange ne modifie pas les suffrages inclus dans les bulletins de l'urne électronique. On parle alors de mélange vérifiable.

- Enfin, le déchiffrement des bulletins n'est également pas forcément vérifiable : il peut aussi être étendu afin de générer un ensemble de preuves mathématiques que le résultat généré correspond à l'urne électronique. On parle alors de déchiffrement vérifiable.

Que ce soit pour le mélange ou pour le déchiffrement vérifiables, les vérifications ne nécessitent pas d'accéder aux clés secrètes ou privées utilisées pour réaliser ces opérations. Ces vérifications peuvent donc être réalisées **sans affaiblir le secret du scrutin**, au moyen d'un outil tiers.

Mise en place d'un mélange vérifiable

Un mélange cryptographique (R29★) est un mécanisme générant un nouvel ensemble de données décorrélées des bulletins de l'urne électronique. Il est donc possible de fournir en sortie de mélange des données sans rapport avec l'urne en entrée, et de porter atteinte à l'intégrité des suffrages exprimés et à la sincérité des opérations électorales. Un mélange vérifiable permet de détecter une telle manipulation. Un tel mélange produit une preuve à divulgation nulle de connaissance que l'ensemble des bulletins mélangés contient exactement le même ensemble de suffrages que l'ensemble des bulletins avant chaque mélange.

R63 ★★★

Assurer l'étanchéité par accumulation ou mélange vérifiable des bulletins

Le système de vote doit assurer l'étanchéité entre l'identité de l'électeur et l'expression de son vote par accumulation ou mélange vérifiable des bulletins.

Dans ce cas, le mécanisme doit être compatible avec le mécanisme de chiffrement des bulletins.

Mise en place d'un déchiffrement vérifiable

Le déchiffrement doit assurer que l'information déchiffrée correspond bien aux suffrages contenus dans les bulletins chiffrés. Or le déchiffrement, seul, ne permet pas la détection de la production d'un résultat invalide (c'est-à-dire un résultat ne correspondant pas aux suffrages exprimés contenus dans les bulletins de l'urne électronique). En effet, comme exposé à l'objectif 1-10, même en cas d'analyse de conformité du code source correspondant à la fonction de déchiffrement, cette analyse repose *in fine* sur l'hypothèse que le serveur de vote est de confiance ; si cette hypothèse n'est pas satisfaite, l'utilisation d'une fonction de déchiffrement compromise est possible. Un déchiffrement vérifiable permet de détecter une telle compromission.

R64 ★★★

Utiliser un déchiffrement vérifiable

Le système de vote doit mettre en œuvre un déchiffrement vérifiable des bulletins au moyen de preuves à divulgation nulle de connaissance, que le résultat du déchiffrement correspond bien au contenu des bulletins avant déchiffrement.

Dans ce cas, la vérification de ces preuves doit pouvoir être réalisée par un tiers sans utilisation des fragments de la clé privée de l'élection.

Conservation des informations nécessaires à la vérification des preuves

Pour que la vérification puisse être effectivement réalisée, il faut que l'organisateur conserve les éléments nécessaires à la vérification des preuves. Cette conservation des données peut être réalisée avec le concours du prestataire.

Information

Le terme « preuve » regroupe plusieurs données, générées par le système de vote à différentes étapes :

- Les moyens de vérifier la validité des bulletins ou des suffrages générés par le client de vote (R24★). Par exemple, dans le cas du mécanisme de chiffrement ElGamal, il s'agit, pour la validité des bulletins, d'une preuve à divulgation nulle de connaissance de l'aléa et pour la validité des suffrages, d'une preuve à divulgation nulle de connaissance de chiffrement de 0 ou 1 et d'une preuve à divulgation nulle de connaissance de chiffrement d'entier dans un intervalle (voir Annexe B).
- Les informations publiées par le serveur de vote, correspondant aux références des bulletins contenues dans les preuves de vote, générées par le client de vote, permettant de vérifier que l'urne correspond aux bulletins transmis par les électeurs (R59★★).
- Les preuves mathématiques générées lors d'un mélange et un déchiffrement vérifiables, permettant de vérifier que les résultats proclamés correspondent à l'urne déchiffrée. Par exemple, dans le cas du mécanisme de chiffrement ElGamal, il s'agit d'une preuve de déchiffrement correct (voir Annexe B).

R65 ★★★

Conserver les éléments nécessaires à la vérification des preuves

L'organisateur du scrutin doit conserver l'ensemble des éléments nécessaires à la vérification des preuves générées par le système de vote :

- La configuration de l'élection.
- La clé publique de l'élection.
- L'urne électronique d'origine avec les bulletins (incluant leur **preuve de validité**) non accumulés ou non mélangés.
- L'ensemble des **références des bulletins de vote**, contenues dans les preuves de vote, telles que publiées par le serveur de vote (2-07) aux fins de vérifiabilité individuelle par les électeurs.
- En cas de mélange vérifiable, le résultat de chaque mélange réalisé par chaque mélangeur et les preuves générées lors de chaque mélange.
- Les preuves générées par le déchiffrement vérifiable de l'urne électronique.
- Les résultats de l'élection.

Ces éléments peuvent être enrichis par d'autres preuves générées à d'autres étapes, par exemple les preuves générées par le partage vérifiable de la clé privée de l'élection.

Vérification des preuves au moyen d'un outil tiers

La vérification des preuves générées par le système de vote requiert l'accès aux éléments conservés (R65★★★), notamment l'urne électronique d'origine. En plus de ces éléments, cette vérification nécessite également l'utilisation d'un outil indépendant du système de vote, développé par un tiers indépendant du prestataire de la solution de vote. Cet outil doit pouvoir être développé sur la base de spécifications publiques élaborées par le prestataire.

R66 ★★★

Publier les spécifications d'un outil de vérification des preuves

Suffisamment en amont du scrutin et en complément de la publication du protocole de vote (R61★★), le prestataire doit rendre publique, typiquement sur une page Web accessible sans restriction depuis Internet, une spécification d'un outil de vérification des informations suivantes :

- Les preuves de validité des bulletins.
- La cohérence entre les références publiées par le serveur de vote, aux fins de vérifiabilité individuelle, et l'urne électronique.
- Les preuves du mélange vérifiable (lorsque le système de vote les génère) et les preuves du déchiffrement vérifiable, aux fins de vérifiabilité universelle.

Cet outil doit permettre, à partir des éléments spécifiés en R65★★★, de réaliser les vérifications dès le dépouillement de l'urne électronique.

Ces spécifications doivent notamment décrire :

- Le format de l'urne électronique et des bulletins.
- Les mécanismes cryptographiques utilisés pour générer les preuves de validité des bulletins, les données nécessaires pour leur vérification.
- Le format des références des bulletins publiées par le serveur de vote, les mécanismes cryptographiques utilisés pour générer ces références et en réaliser la signature numérique, les données nécessaires pour la vérification de ces signatures et la vérification de la cohérence de ces références avec les bulletins contenus dans l'urne électronique, le format de la clé publique de vérification de la signature des références des bulletins et les modalités d'accès à cette clé, le format de la page Web publiant les informations des bulletins dans l'urne (R59★★) et les modalités d'accès à cette page.
- Les mécanismes cryptographiques utilisés pour le chiffrement des suffrages, pour l'accumulation ou le mélange vérifiable des bulletins, le format des preuves du déchiffrement vérifiable, des preuves du mélange vérifiable, les données nécessaires pour la vérification de ces preuves, le format de la clé publique de l'élection et des clés publiques intervenant dans le mélange, et les modalités d'accès à ces clés.

Le prestataire doit également fournir des jeux de données de tests permettant à un tiers de valider son implémentation.

Information

Il est essentiel pour la sincérité des opérations électorales, l'intégrité des suffrages exprimés et la surveillance effective du vote, qu'un tiers puisse s'approprier les spécifications du prestataire, développer un outil de vérification indépendant et le publier en source ouverte.

La fourniture par le prestataire lui-même d'un outil de vérification n'offre pas la même indépendance.

Objectif n° 3-03

Assurer, durant la période d'ouverture du scrutin, une très haute disponibilité du système de vote électronique et des services tiers nécessaires à son fonctionnement, en prenant notamment en compte les risques d'avarie majeure comme la perte d'un centre de données.

Cet objectif complète l'objectif 2-01, qui concerne la redondance des composants du système de vote au sein d'un unique centre de données. En cas de perte de ce centre de données, le système de vote est indisponible et cela peut porter atteinte à l'accès au vote pour tous les électeurs et à la sincérité des opérations électorales. Pour couvrir ce risque, une réplication du système de vote dans un second centre de données peut prendre le relais.

R67 ★★★

Répliquer le système de vote dans un second centre de données

Le prestataire doit fournir une réplication du système de vote dans un second centre de données, prenant le relais en cas d'avarie majeure du système principal. Les sites hébergeant l'infrastructure principale et de secours doivent être suffisamment distants et correctement placés afin de couvrir les risques naturels jugés pertinents par l'analyse de risque. Pour un *cloud* public, cela correspond à l'utilisation de zones de disponibilité différentes au sein d'une région.

Le système de secours doit prendre automatiquement et sans délai le relais en cas de panne ou d'incident technique n'entraînant pas d'altération des données.

L'expression « sans délai » peut être modulée selon les besoins (et les moyens) de l'organisateur du scrutin. Une indisponibilité courte – quelques minutes, voire une heure – peut-être jugée acceptable par rapport à la période de vote. Il faut cependant prendre en compte des indisponibilités pouvant se produire juste avant la clôture du scrutin.

Comme expliqué à l'objectif 1-06, la perte de données maximale admissible (PDMA) doit être nulle : aucun bulletin ne doit être perdu quels que soient l'incident ou la panne qui touche le système de vote. Cette recommandation est plus difficile à réaliser en cas de sinistre majeur impliquant une bascule vers le dispositif de secours car le choix du mode de réplication (synchrone / asynchrone) dépend fortement de la distance et de la qualité de la liaison entre les sites.

Objectif n° 3-04

Renforcer le caractère secret du scrutin en ne manipulant jamais le secret permettant leur dépouillement sur un serveur qui serait en capacité de rapprocher l'identité des électeurs et leur bulletin.

Cet objectif renforce l'objectif 1-08 en séparant à tout moment les bulletins (tant qu'ils sont non mélangés et non accumulés) de la clé privée de l'élection. Cela renforce le secret du scrutin (cf. 1-07) car les bulletins non mélangés ou non accumulés ne seront pas déchiffrés illégitimement.

Pour mettre en œuvre cet objectif, la clé privée de l'élection ne doit être ni générée, ni reconstituée sur le serveur qui stocke les bulletins non mélangés et non accumulés.

R68 ★★★

Séparer la clé privée de l'élection des bulletins non mélangés ou non accumulés

Le système de vote doit séparer strictement les bulletins non mélangés ou non accumulés de la clé privée de l'élection.

La génération de la clé privée de l'élection et l'utilisation de la clé pour déchiffrer les bulletins (une fois mélangés ou accumulés) doivent être réalisées hors du serveur (applicatif) stockant les bulletins non mélangés ou non accumulés, par exemple dans le navigateur d'un poste client réservé au bureau électoral, connecté à ce serveur et bénéficiant des mêmes conditions de sécurité que le serveur.

Information

Le déport du déchiffrement sur un poste client implique que les données à déchiffrer soient transmises à ce poste client. Il est donc nécessaire de prendre en compte les traitements à réaliser pour estimer la compatibilité de l'architecture (voir l'Annexe B, en particulier la partie relative aux preuves du déchiffrement vérifiable).

Si le système de vote met en œuvre l'accumulation des bulletins, le volume de données et le temps de traitement seront limités et compatibles avec une telle architecture.

Si le système de vote s'appuie sur un mélange vérifiable intégrant le déchiffrement, alors celui-ci repose sur un ensemble de serveurs (mélangeurs) qui réalisent aussi le déchiffrement et aucun mélange ne peut être réalisé sur un poste client.

Enfin, si le système de vote s'appuie sur un mélange vérifiable n'intégrant pas le déchiffrement, alors celui-ci repose sur un ensemble de serveurs (mélangeurs) réalisant seulement le mélange. À l'issue du mélange, les bulletins doivent être récupérés du dernier mélangeur et déchiffrés. Le déchiffrement sur un poste client n'est de fait compatible qu'avec un nombre limité de bulletins. Si le nombre de bulletins est important, il est nécessaire de réaliser le déchiffrement sur une machine ayant les capacités de calcul d'un serveur équivalent à ceux utilisés pour le mélange.

La Section 4.4 propose des alternatives à l'utilisation d'un poste client : d'une part le recours à un serveur hors ligne, d'autre part la génération et le déchiffrement distribués. Ces alternatives

peuvent être mises en œuvre si l'analyse de risque (R62★★) conclut sur le besoin de renforcer la confidentialité de la clé privée de l'élection, ou si le déport des traitements sur un navigateur n'est pas compatible avec les contraintes du scrutin.

Objectif n° 3-05

Favoriser la transparence de la solution de vote et la confiance des électeurs en rendant public, en amont du scrutin, le code source des éléments du système de vote ayant vocation à être exécutés sur le terminal de l'électeur, y compris dans un navigateur.

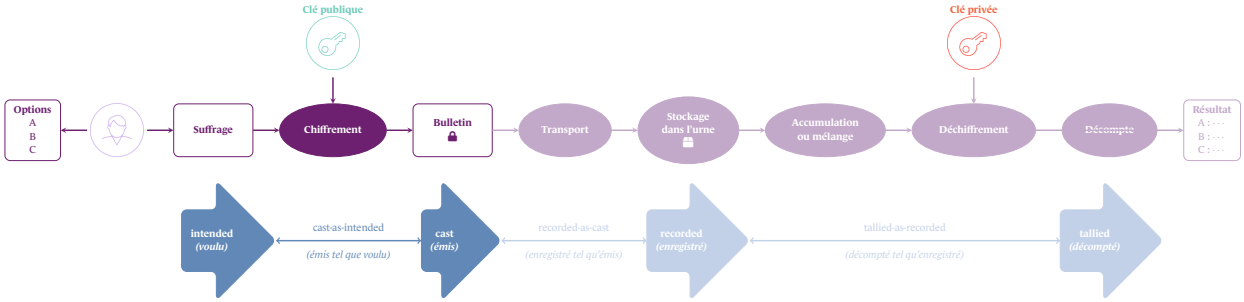

FIGURE 17 – Propriété cast-as-intended

Cet objectif renforce la sincérité des opérations électorales, l'intégrité des suffrages exprimés et la surveillance effective du vote. Il constitue une partie de la vérifiabilité individuelle : publier le code source du client de vote fournit un premier niveau d'assurance que ce client de vote respecte bien l'intention de l'électeur (Propriété cast-as-intended, illustrée à la Figure 17).

Dans le détail, la publication du code source non offusqué du client de vote permet à tous, avant l'élection, de vérifier que le client est conçu pour émettre un bulletin correspondant à l'intention de vote de l'électeur. Le jour de l'élection, il est possible de constater que le client de vote fourni à tous les électeurs correspond à celui qui a été rendu public.

Publier le code source du client de vote

R69 ★★★

En amont du scrutin, le prestataire doit rendre public le code source du client de vote utilisé par les électeurs, sans préjudice de la propriété intellectuelle du prestataire.

Le code source publié doit être complet, lisible, ne pas faire l'objet d'offuscation et doit correspondre à celui transmis aux électeurs par le serveur de vote. La publication peut typiquement être réalisée sur une page Web accessible sans restriction depuis Internet.

N'importe qui doit pouvoir constater que le client de vote transmis par le serveur de vote correspond au code source publié, aussi le client de vote doit être entièrement chargé *avant l'authentification* de l'électeur.

Cette publication de code doit permettre à un tiers d'en analyser la sécurité ainsi que celle du protocole de vote. Cette analyse doit être autorisée pour *tout tiers*, sur la base du code publié. Un point de contact doit être identifié pour rendre possible la divulgation responsable d'éventuelles faiblesses identifiées par les tiers.

Comme évoqué dans [50], la publication du code source du client de vote peut être facilitée par l'utilisation d'application monopage (*Single Page Application*) [77]. Comme exposé à l'objectif 1-04, le client de vote est communément un script JavaScript intégré à la page Web présentée à l'électeur

et exécuté par le navigateur. Dans ce cas, la publication du code source du client de vote consiste à publier ce script Javascript ainsi que ses dépendances.

Information

Les limitations de cette approche sont que l'électeur n'est pas autonome pour faire les vérifications et que l'honnêteté de son équipement, qui exécute le client de vote via un navigateur, n'est pas garantie. Cette propriété de cast-as-intended fait toujours l'objet de recherche active. Historiquement le mécanisme appelé Challenge de Benaloh [26] a été proposé, mais sa mise en œuvre pratique ainsi que sa portée font l'objet d'analyses [47, 63, 65, 73, 87].

4.4 Recommandations complémentaires

En fonction de l'analyse des risques (R62★★★), l'organisateur d'un scrutin de niveau 3 peut être confronté à des risques spécifiques, dépassant ceux envisagés par les objectifs de sécurité fixés par la CNIL. Par exemple, l'application de vote ou plus généralement le serveur de vote ne sont pas jugés complètement de confiance.

Cette section propose des recommandations mises en œuvre dans différents systèmes de votes [27, 44, 45, 93], limitant les impacts de situations où le serveur de vote pourrait permettre :

- Le bourrage d'urne (ajout de bulletins illégitimes dans l'urne), portant atteinte à la sincérité des opérations électorales. La protection peut reposer sur la vérifiabilité de la légitimité.
- La conservation illégitime ou la fuite de la clé privée de l'élection, portant atteinte au secret du scrutin. La protection peut reposer sur la génération hors ligne de la clé (impliquant un déchiffrement hors ligne).
- La génération d'une clé privée de l'élection favorisant un des attributaires, portant atteinte au secret du scrutin. La protection peut reposer sur :
  - la génération distribuée de la clé privée (impliquant un déchiffrement distribué),
  - la vérification de la génération et du partage de clé par des preuves à divulgation nulle de connaissance.

Attention

Ces recommandations sont délicates à mettre en œuvre, car pour que les garanties de sécurité qu'elles apportent soient effectives, elles peuvent nécessiter que les équipements sur lesquels la génération des clés ou le déchiffrement s'effectuent ne soient pas sous le contrôle de l'organisateur du scrutin ni du prestataire, ou nécessiter l'établissement d'une communication privée entre les attributaires. Ces recommandations nécessitent donc de traiter le sujet de la fourniture de ces équipements, de leur sécurité, de la fourniture du code réalisant les opérations et de sa performance.

Vérifiabilité de la légitimité

La propriété de vérifiabilité de la légitimité (tous les bulletins proviennent d'électeurs légitimes et seulement de ceux-ci) constitue une partie de la vérifiabilité universelle. Cette propriété permet de détecter un bourrage d'urne, y compris par le serveur de vote.

Cette propriété ne peut pas être atteinte avec la recommandation R27★ (le système de vote contrôle la clé privée ou la clé secrète de signature numérique ou de chaînage des bulletins). En effet, dans ce cas, le système de vote dispose des moyens de modifier l'urne électronique et la liste d'émargement et d'ajouter des bulletins à l'insu des électeurs.

Si le risque de bourrage d'urne par le serveur de vote n'est pas acceptable, une solution consiste à faire réaliser la signature numérique des bulletins par les électeurs, sur le client de vote, au cours de l'opération de vote, au moyen d'une clé privée de signature numérique *délivrée par une entité*

indépendante de l'organisateur du scrutin et du prestataire. Cette recommandation est de niveau supérieur au niveau 3 de la CNIL, car sa mise en œuvre est difficile : le fournisseur des clés de signature devrait être indépendant de l'organisateur du scrutin et du prestataire, et le prestataire doit intégrer la vérification de signature dans le système de vote.

R70 ★★ ★+

Signer les bulletins avec une clé indépendante de la solution de vote

En fonction des conclusions de l'analyse de risque (R62★★), il est recommandé qu'une entité indépendante de l'organisateur du scrutin et du prestataire fournisse une clé individuelle privée de signature numérique des bulletins à chaque électeur et fournisse les clés publiques de vérification de signature au système de vote.

Dans ce cas, les clés publiques de vérification de signature doivent être associées de manière universellement vérifiable aux identités des électeurs légitimes. La signature du bulletin doit être réalisée dans le client de vote ; à réception du bulletin, le système de vote doit en vérifier la signature numérique au moyen de la clé publique fournie par l'entité indépendante et doit vérifier l'association des clés publiques aux identités des électeurs.

i

Information

La mise en place d'une signature officialise le lien électeur/bulletin. Dans ce cas, le secret du scrutin reposera entièrement sur l'absence de lien bulletin/suffrage, en particulier si la signature n'est pas anonyme. Il est possible théoriquement d'obtenir la légitimité des bulletins (et donc une protection contre le bourrage d'urne), en utilisant, à la place de leur signature, des preuves à divulgation nulle de connaissance adaptées [42], cette analyse théorique repose sur des preuves plus complexes que celles exposées dans ce guide en Annexe B.

Génération hors ligne de la clé privée de l'élection et déchiffrement hors ligne

Pour la génération de la clé privée de l'élection et pour le déchiffrement, une alternative à l'utilisation d'un poste connecté au serveur de vote est le recours à un serveur hors ligne, distinct du serveur de vote stockant les bulletins. Ce serveur hors ligne est chargé de manipuler le secret le plus sensible de l'élection, la clé privée de l'élection. Sa position hors ligne, déconnectée d'Internet, le rend plus difficile à compromettre par un acteur malveillant.

Cependant, cette architecture complexifie aussi les cérémonies, puisque des transferts physiques d'informations sont à mettre en œuvre : clé publique de l'élection vers le serveur de vote, bulletins mélangés ou accumulés vers le serveur hors ligne, et résultat du décompte vers le serveur de vote.

R71 ★★ ★+

Réaliser les opérations impliquant la clé privée de l'élection sur un serveur dédié hors ligne

En fonction des conclusions de l'analyse de risque (R62★★), il est recommandé que le système de vote utilise un serveur hors ligne dédiée aux opérations impliquant la clé privée de l'élection, à savoir la génération des fragments de cette clé (R31★) et le

déchiffrement des bulletins (R64★★★).

Enfin, même si elle renforce la protection de la clé privée de l'élection, cette architecture centralise toujours sa génération ainsi que son utilisation pour le déchiffrement des bulletins. Comme exposé à l'objectif 1.10, même en cas d'analyse de la conformité du code source de l'application de vote, cette analyse repose *in fine* sur l'hypothèse que le serveur de vote est de confiance. Sans cette hypothèse, la compromission de la clé privée de l'élection est toujours possible, car celle-ci est calculable à partir des fragments de clés qui sont centralisés. Si ce risque n'est pas acceptable, la génération de clé et le déchiffrement distribués peuvent être envisagés.

Génération distribuée de la clé privée de l'élection

Si le risque de compromission de la clé privée de l'élection par le système de vote n'est pas acceptable, il est nécessaire de renforcer la génération de la clé et son usage pour le déchiffrement. Une solution consiste à réaliser une génération de clé et un déchiffrement distribués.

La **génération de clé distribuée** consiste à faire générer localement par chaque attributaire une paire clé privée/clé publique. L'ensemble des clés publiques permet de construire la clé publique de l'élection, sans avoir à regrouper les clés privées de chaque attributaire. Ainsi, les fragments de la clé privée de l'élection ne sont jamais regroupés sur un même équipement, contrairement aux architectures précédentes.

R72 ★★★+

Générer la clé privée de l'élection de manière distribuée

En fonction des conclusions de l'analyse de risque (R62★★★), il est recommandé que le système de vote mette en œuvre une génération distribuée de la paire clé privée/clé publique de l'élection. Cette génération doit assurer que les fragments de la clé privée de l'élection ne sont jamais présents sur le même équipement.

Dans ce cas, le prestataire doit fournir la procédure de génération adaptée au contexte de l'organisateur du scrutin pour assurer la sécurité de la génération et l'organisateur du scrutin doit respecter les contraintes opérationnelles du prestataire.

Afin de ne pas dégrader la sécurité obtenue avec la génération de clé distribuée, le déchiffrement des bulletins ne doit pas non plus s'appuyer sur une reconstitution de la clé privée de l'élection.

Pour cela, il est possible que chaque attributaire réalise un déchiffrement vérifiable *distribué* des bulletins. Chaque déchiffrement partiel génère une preuve à divulgation nulle de connaissance de déchiffrement correct. L'ensemble des déchiffrés partiels est ensuite combiné pour générer le résultat de l'élection. Ce mécanisme est aussi délicat à mettre en œuvre, car, comme pour la génération distribuée des clés, il peut nécessiter que les équipements sur lesquels les déchiffrements partiels s'effectuent ne soient pas sous le contrôle de l'organisateur du scrutin ni du prestataire.

R73 ★★★+

Utiliser un déchiffrement vérifiable distribué

En fonction des conclusions de l'analyse de risque (R62★★★), il est recommandé que le système de vote mette en œuvre un déchiffrement vérifiable distribué des bulletins

au cours duquel les attributaires des fragments de la clé privée de l'élection réalisent chacun un déchiffrement partiel, assurant que la clé privée n'a jamais besoin d'être explicitement reconstituée. Chaque déchiffrement partiel doit générer une preuve à divulgation nulle de connaissance de déchiffrement correct.

Dans ce cas, le prestataire doit fournir la procédure de déchiffrement adaptée au contexte de l'organisateur du scrutin pour assurer la sécurité des déchiffrements partiels, et l'organisateur du scrutin doit respecter les contraintes opérationnelles du prestataire.

Vérification de la génération et du partage de clé par des preuves mathématiques

Le **partage de secret à seuil** de Shamir [89], communément utilisé en réponse à la recommandation (R31★) repose sur l'hypothèse que l'ensemble des participants impliqués (attributaires, organisateur, prestataire) exécute correctement les procédures de génération, de partage, de conservation et de reconstitution de la clé : il ne permet pas de détecter un éventuel dysfonctionnement. Cette hypothèse peut être remise en cause, soit à cause d'une erreur de manipulation, soit suite à une action volontaire. En particulier, comme expliqué dans [61] (Chapitre 7), il est possible qu'un attributaire dispose de la clé privée de l'élection correspondant à la clé publique de l'élection publiée, sans que cela soit détecté. Ainsi, le secret du scrutin pourrait être compromis car l'usage de la clé privée de l'élection ne serait pas contrôlé.

Afin de traiter ce risque, un **partage de secret à seuil *vérifiable*** assure que la clé publique de l'élection publiée est bien celle qui est issue des manipulations réalisées par les attributaires, et que chacun dispose bien de seulement d'un seul fragment de la clé privée de l'élection correspondante.

Pour cela, il est possible d'inverser les opérations de génération et de fragmentation : chaque porteur génère un fragment de la clé privée de l'élection, ainsi qu'un fragment de clé publique de l'élection correspondant. La clé publique de l'élection est calculée en combinant l'ensemble des fragments de clé publique générés. Chaque fragment de clé publique est associé à une preuve à divulgation nulle de connaissance de clé secrète, assurant que ce fragment de clé publique est bien lié au fragment de clé privée qui est généré par l'attributaire. La vérification de cette preuve est réalisable avec le fragment de clé publique générée.

R74 ★★★+

Utiliser un partage de secret à seuil vérifiable

En fonction des conclusions de l'analyse de risque (R62★★★), il est recommandé que le système de vote mette en œuvre un partage de secret à seuil vérifiable, compatible avec le mécanisme de chiffrement des bulletins. Ce partage doit générer un ensemble de preuves à divulgation nulle de connaissance, permettant de vérifier que la clé publique de l'élection publiée correspond aux fragments de clés publiques générés par les attributaires.

Le prestataire doit rendre publique une spécification détaillant la constitution des preuves de bonne génération et de bon partage et une spécification d'un outil permettant de vérifier ces preuves. Ces spécifications doivent permettre à un tiers de développer un outil de vérification des preuves, indépendant du système de vote,

complétant l'outil de vérification des preuves du déchiffrement vérifiable (R64★★) et du mélange vérifiable (R63★★). Cette publication peut typiquement être réalisée sur une page Web sans authentification.

4.5 Risques non couverts

Les recommandations détaillées dans le guide ne répondent d'une part qu'aux objectifs de sécurité fixés par la CNIL et d'autre part qu'aux risques décrits dans la section 4.4 (bourrage d'urne, fuite de la clé privée de l'élection, génération de la clé privée de l'élection favorisant un des attributaires). Ainsi, même en appliquant l'ensemble des recommandations du guide, il subsiste des risques résiduels :

- Aucune recommandation n'empêche la copie illicite de la clé privée de l'élection (ou de fragments de celle-ci) et de porter atteinte au secret du scrutin. Les recommandations R31★ et R74★★+ fournissent une première réponse par le partage de la clé privée de l'élection. Cependant, la génération d'une copie non maîtrisée de la clé privée reste possible, par exemple s'il y a collusion entre suffisamment d'attributaires.
- Aucune recommandation n'assure complètement la résistance à l'achat de vote ou la résistance à la coercition. La recommandation R30★ (receipt-freeness), rend plus difficile pour un électeur de prouver son suffrage grâce au système de vote. Elle ne fournit par contre aucune protection contre un électeur qui pourrait effectuer des manipulations techniques lors de son vote, ni à un électeur qui devrait voter sous contrainte, portant atteinte au caractère personnel du vote ou au caractère libre du vote.
- Aucune recommandation n'assure la vérifiabilité de l'intention de l'électeur (cast-as-intended). La recommandation R69★★★, relative à la publication du code source du client de vote, constitue une première réponse, portant sur les opérations réalisées par le client de vote. Elle ne protège pas de la compromission de l'intention de l'électeur par d'autres éléments techniques de l'équipement utilisé par l'électeur (navigateur, système d'exploitation...), qui porterait atteinte à l'intégrité des suffrages exprimés et à la sincérité des opérations électorales.
- Aucune recommandation ne traite de la résistance à un ordinateur quantique et de la mise en œuvre de la confidentialité persistante (everlasting-privacy). Cela concerne en particulier les mécanismes liés au chiffrement du suffrage (R18★, R19★). Les mécanismes de chiffrement asymétriques actuels, dont ElGamal, sont vulnérables à une attaque *store now, decrypt later*, portant atteinte au secret du scrutin dans le futur, pour une élection réalisée aujourd'hui.
- Aucune recommandation ne traite de la résistance à la déstabilisation : il est toujours possible de prétendre que le résultat n'est pas valide et porter atteinte à la sincérité des opérations électorales. Les recommandations relatives à la transparence (R61★★, R69★★★) et à l'indépendance logicielle, notamment la vérifiabilité individuelle et la vérifiabilité universelle (R58★★, R59★★, R63★★★, R64★★★, R65★★★, R66★★★) fournissent une première réponse. Cependant, elles n'offrent pas de garanties face à une diffusion massive de fausses informations.

Attention

À l'issue de l'analyse des risques (R62★★★), lorsque l'organisateur d'un scrutin de niveau 3 estime que des risques exposés dans la présente section ne sont pas couverts, d'autres mesures que celles décrites dans ce guide doivent être mises en œuvre.

De façon plus pragmatique, si les risques ne peuvent être ni réduits, ni acceptés, alors le vote par correspondance électronique peut être abandonné et le scrutin peut être réalisé par vote à l'urne.

Annexe A
Mise en œuvre du chiffrement ElGamal

Cette annexe s'adresse en premier lieu aux prestataires spécialisés dans le vote par correspondance électronique ainsi qu'aux tiers intervenant dans la vérification de la conformité des scrutins. Elle fournit des explications sur la mise en œuvre du mécanisme de chiffrement ElGamal. Ce mécanisme est largement utilisé dans les systèmes de vote actuels, par exemple ceux décrits dans [1, 27, 36, 45, 46, 49, 57, 68, 69, 85, 88]. Cependant, son utilisation ne fait l'objet d'aucune standardisation. Cette annexe a une vocation pédagogique et vise à faciliter l'utilisation du mécanisme de chiffrement ElGamal ou une transition vers ce mécanisme. Comme le reste du document, cette annexe n'a aucun caractère normatif.

Les algorithmes sont décrits dans le cas générique d'un groupe cyclique $\mathbb{G}$, de générateur g, de cardinal premier q. Ce groupe doit être choisi conformément à la recommandation R3*, c'est-à-dire que le problème du logarithme discret est difficile à résoudre dans $\mathbb{G}$. Le *Guide de sélection d'algorithmes cryptographiques* [10] fournit des recommandations et des notes d'implémentation pour le choix du groupe multiplicatif d'un corps fini ou les paramètres de courbes elliptiques pour lesquels ce problème est difficile.

La sécurité sémantique du chiffrement ElGamal repose sur le fait que le message à chiffrer (dans le contexte du vote par Internet, une représentation du suffrage de l'électeur), est un élément du groupe, c'est-à-dire un message de la forme $M = g^m$ pour un certain entier $m < q$. Il y a deux manières de réaliser le codage du suffrage :

- Représenter le suffrage par un élément du groupe $\mathbb{G}$. C'est exactement le cas présenté précédemment : il existe un entier m tel que le suffrage soit représenté par l'élément de groupe $M = g^m$. Dans ce cas, le résultat du déchiffrement d'un bulletin est exactement l'élément de groupe M, qui représente le suffrage. On parle alors de codage classique.
- Représenter le suffrage par un entier $m < q$, tel que $M = g^m$ soit l'élément de groupe chiffré. Dans ce cas, le déchiffrement d'un bulletin vaut M, qui ne *représente pas* le suffrage : une opération additionnelle doit être réalisée, i.e. $m = \log(M)$ afin d'obtenir la donnée qui représente le suffrage, c'est-à-dire l'entier m. On parle alors de codage exponentiel.

Ainsi, dans les deux cas, le codage assure la sécurité sémantique du chiffrement, cependant, le suffrage sera représenté différemment.

Attention

Le mécanisme de chiffrement ElGamal (à codage classique ou exponentiel) n'assure pas *seul* le secret du scrutin ni l'intégrité des suffrages exprimés car il est **malléable** : il n'atteint que la propriété IND-CPA et cette propriété est insuffisante. Des attaques exploitant la malléabilité du chiffrement ElGamal pour porter atteinte au secret du scrutin sont par exemple décrites dans [78].

Lorsque le mécanisme d'accumulation est utilisé pour assurer l'étanchéité entre l'identité de l'électeur et l'expression de son vote, le codage exponentiel est utilisé et il est nécessaire de vérifier que le bulletin contient un suffrage valide, sans dévoiler ce suffrage (R24★) car cela renforce la sincérité des opérations électorales et l'intégrité des suffrages exprimés. Le mécanisme de chiffrement ElGamal *seul* ne permet pas de réaliser cette vérification.

Toutes les versions (à codage classique ou exponentiel, centralisé, distribué) du déchiffrement des bulletins n'assurent pas *seules* que celui-ci respecte le suffrage des électeurs (et donc n'assurent pas *seules* la sincérité des opérations électorales et l'intégrité des suffrages exprimés) en cas de compromission de l'application de vote (une attaque directe est par exemple décrite dans [61]).

La génération de clé (identique pour les codages classique ou exponentiel), peut être déclinée de manière centralisée ou distribuée, avec ou sans seuil (R31★). Ce mécanisme *seul* n'assure *pas* le secret du scrutin en cas de compromission de l'application de vote (une attaque directe est par exemple décrite dans [61]).

En conséquence, il est nécessaire d'adapter le mécanisme de chiffrement ElGamal aux étapes de génération de la clé, de chiffrement et de déchiffrement afin de renforcer le secret du scrutin, l'intégrité des suffrages exprimés ainsi que la sincérité des opérations électorales :

- Une première adaptation, **nécessaire dès le niveau 1**, consiste à composer le chiffrement du suffrage avec une preuve à divulgation nulle de connaissance de l'aléa. Cette composition empêche d'exploiter la malléabilité et permet d'atteindre la propriété de sécurité NM-CPA, qui, elle, assure le secret du scrutin et l'intégrité du suffrage exprimé.
- Une seconde adaptation, **nécessaire dès le niveau 1 en cas d'accumulation des bulletins**, consiste à composer le chiffrement du suffrage avec des preuves à divulgation nulle de connaissance de chiffrement de 0 ou 1 et de chiffrement d'entier dans un intervalle, dont la conjonction assure la validité du suffrage. Cette composition renforce le secret du scrutin, l'intégrité du suffrage exprimé et la sincérité des opérations électorales.
- Une troisième adaptation, **nécessaire au niveau 3**, consiste à composer le déchiffrement (centralisé ou distribué, avec ou sans seuil) des bulletins avec une preuve à divulgation nulle de connaissance de déchiffrement correct. Cette preuve met en œuvre un déchiffrement vérifiable et au final renforce la sincérité des opérations électorales et l'intégrité des suffrages exprimés.
- Une quatrième adaptation, **à prendre en compte en fonction de l'analyse des risques**, consiste à composer la génération de clé (centralisée ou distribuée, avec ou sans seuil) avec une preuve à divulgation nulle de connaissance de clé secrète.

Des exemples classiques [29] de preuves compatibles avec l'algorithme ElGamal sont présentées en Annexe B.

Validité du bulletin, validité du suffrage

Lorsque le mécanisme de chiffrement ElGamal est utilisé, un chiffré est un couple $(g^r, g^m K^r)$, où g est un générateur du groupe $\mathbb{G}$ dans lequel le problème du logarithme discret est difficile, r est un aléa, g^m est le codage du suffrage et K est la clé publique de l'élection.

Un **bulletin valide** signifie que les deux termes du couple (g^r et $g^m K^r$) sont bien des éléments du groupe $\mathbb{G}$, que le même aléa r est utilisé dans les deux termes et que la clé publique de l'élection est bien celle utilisée (K) pour réaliser le chiffrement. La composition du chiffrement avec une preuve à divulgation nulle de connaissance de l'aléa (voir Annexe B), assure, en plus de la non-malléabilité du chiffrement, que ces conditions sont satisfaites et vérifiables sans divulgation de l'aléa r. Cela ne signifie par contre *pas* que le suffrage est valide : la conformité du terme g^m à la configuration de l'élection n'est ni assurée ni vérifiée.

Un **suffrage valide** signifie que le terme g^m est bien conforme à la configuration de l'élection. Cela signifie que ce terme correspond bien à une option que l'électeur peut choisir et seulement à une telle option. Lorsque l'électeur doit sélectionner plusieurs options, la conjonction des deux preuves suivantes permet d'assurer et de vérifier la validité du suffrage sans le divulguer (voir Annexe B) :

- Une preuve à divulgation nulle de connaissance de chiffrement de 0 ou 1.
- Une preuve à divulgation nulle de connaissance de chiffrement d'entier dans un intervalle.

Cette conjonction de preuves assure la validité du suffrage, la validité du bulletin et la non-malléabilité du chiffrement. Lorsque la configuration de l'élection est plus complexe, ou lorsque le nombre d'options est trop élevé, d'autres preuves doivent être mises en œuvre (voir Annexe B).

La vérification de ces preuves doit être réalisée directement dès réception du bulletin (R24★).

Génération centralisée de clé non fragmentée, codage classique

Les algorithmes 1, 2 et 3 décrivent le mécanisme de chiffrement ElGamal à codage classique, c'est-à-dire, dans le contexte du vote par Internet, que le suffrage est représenté par un élément du groupe $\mathbb{G}$.

Attention

Ces algorithmes sont décrits pour illustrer la différence entre codage classique et codage exponentiel. Ils ne peuvent pas être utilisés tels quels car ils contredisent la recommandation R31★ (fragmentation de la clé privée de déchiffrement).

Algorithme 1 : Génération centralisée de clé non fragmentée

Entrée : g, q (générateur de groupe, ordre du groupe)
Sortie : (k, K) (clé privée, clé publique)

1 $k \xleftarrow{\$} \mathbb{Z}_q$
2 $K := g^k$
3 Return (k, K).

Dans le cas du codage classique, le suffrage est représenté par un élément du groupe $\mathbb{G}$, noté ici M : il existe un entier m tel que $M = g^m$.

Algorithme 2 : Chiffrement à codage classique

Entrée : g, q, K, M (générateur de groupe, ordre du groupe, clé publique, élément de groupe représentant le suffrage)
Sortie : (α, β) (chiffré)

1 $r \xleftarrow{\$} \mathbb{Z}_q$
2 Return $(\alpha, \beta) = (g^r, MK^r)$

Algorithme 3 : Déchiffrement centralisé à clé non fragmentée, codage classique

Entrée : k, (α, β) (clé privée, chiffré)
Sortie : M (élément de groupe représentant le suffrage)

1 Return $M = \beta / \alpha^k$

Ainsi le codage classique fournit un homomorphisme *multiplicatif* : si l'on considère deux chiffrés ElGamal de deux messages M_1 et M_2 avec la même clé publique K, $(\alpha_1, \beta_1) = (g^{r_1}, M_1 K^{r_1})$ et $(\alpha_2, \beta_2) = (g^{r_2}, M_2 K^{r_2})$, alors le produit défini par $(\alpha, \beta) = (\alpha_1 \times \alpha_2, \beta_1 \times \beta_2)$ est le chiffré du message $M_1 \times M_2$.

Information

Lorsque le chiffrement ElGamal à codage classique est utilisé pour réaliser le mélange des bulletins, le bulletin de vote produit par le client de vote ne contient qu'un seul chiffré ElGamal, composé avec la preuve de connaissance de l'aléa.

Génération centralisée de clé non fragmentée, codage exponentiel

L'accumulation des bulletins peut être réalisée si l'algorithme de chiffrement des suffrages fournit un homomorphisme *additif*, ce qui est le cas lorsque ElGamal utilise le codage exponentiel. Une opération additionnelle est nécessaire lors du déchiffrement (log), par rapport au codage classique, afin de retrouver le suffrage exprimé.

Les algorithmes 4, 5 décrivent le chiffrement et le déchiffrement de l'algorithme ElGamal à codage exponentiel. La génération de clé est identique au cas du codage classique, seuls le chiffrement et le déchiffrement sont différents.

Attention

Ces algorithmes sont décrits pour illustrer la différence entre codage classique et codage exponentiel. Ils ne peuvent pas être utilisés tels quels car ils contredisent la recommandation R31⋆ (fragmentation de la clé privée de déchiffrement).

Algorithme 4 : Chiffrement à codage exponentiel

Entrée : g, q, K, m (générateur de groupe, ordre du groupe, clé publique, entier représentant le suffrage)

Sortie : (α, β) (chiffré)

1 $r \xleftarrow{\$} \mathbb{Z}_q$

2 Return $(\alpha, \beta) = (g^r, g^m K^r)$

Algorithme 5 : Déchiffrement centralisé à clé non fragmentée, codage exponentiel

Entrée : k, (α, β) (clé privée, chiffré)

Sortie : m (entier représentant le suffrage)

1 $M = \beta / \alpha^k$

2 Return $m = \log(M)$ i.e m tel que $M = g^m$

Avec le codage exponentiel, le mécanisme de chiffrement ElGamal fournit un homomorphisme *additif* qui est donc adapté pour l'accumulation des bulletins : si l'on considère deux chiffrés ElGamal de deux messages m_1 et m_2 avec la même clé publique K, $(\alpha_1, \beta_1) = (g^{r_1}, g^{m_1} K^{r_1})$ et $(\alpha_2, \beta_2) = (g^{r_2}, g^{m_2} K^{r_2})$, alors le produit défini par $(\alpha, \beta) = (\alpha_1\,\alpha_2, \beta_1\,\beta_2)$ est le chiffré du message $g^{m_1+m_2}$, et après décodage cela fournit $m_1 + m_2$.

Information

Lorsque le chiffrement ElGamal à codage exponentiel est utilisé pour réaliser l'accumulation des bulletins, le bulletin de vote produit par le client de vote contient autant de chiffrés ElGamal qu'il y a d'options proposées aux électeurs, composés avec les preuves à divulgation nulle de connaissance décrites dans l'annexe B.

Une fois le vote clos, le nombre de voix par option est calculable d'abord en effectuant le produit de l'ensemble des chiffrés correspondant à cette option et ensuite en en réalisant le déchiffrement. Ainsi le décodage est borné par le nombre d'électeurs participant à l'élection et est réalisable en temps raisonnable [90].

Génération centralisée de clé fragmentée, à seuil maximal

La génération de clé ainsi que le déchiffrement (à codage classique ou exponentiel) peuvent être adaptées pour mettre en œuvre une fragmentation de la clé privée de déchiffrement des bulletins entre l'ensemble des attributaires (dans les algorithmes ci-dessous, N représente le nombre d'attributaires), telle que l'**ensemble des fragments de clé est nécessaire pour réaliser le déchiffrement des bulletins**.

Le chiffrement (à codage classique ou exponentiel) sont identiques aux cas précédents, seuls la génération de clé et le déchiffrement sont différents. Les algorithmes 6, 7, 8 décrivent la génération centralisée de clé fragmentée, le déchiffrement centralisé classique ou avec codage exponentiel au moyen de la clé fragmentée.

Attention

Ce mécanisme peut être composé avec une preuve à divulgation nulle de connaissance de déchiffrement correct afin de fournir un déchiffrement vérifiable (R64$^{\star\star}_{\star}$) et suivant l'analyse de risque (R62$^{\star\star}_{\star}$), une preuve de connaissance de clé secrète afin de fournir un partage secret à seuil vérifiable (R74$^{\star\star}_{\star+}$). Voir l'Annexe B.

Algorithme 6 : Génération centralisée de clé fragmentée à seuil maximal

Entrée : g, q, N (générateur du groupe, ordre du groupe, nombre de fragments)
Sortie : $(k_1, \ldots, k_N, K)$ (N fragments de la clé privée, clé publique)

for i *from* 1 *to* N **do**
  $k_i \xleftarrow{\$} \mathbb{Z}_q$
  $K_i := g^{k_i}$
$K = \prod_i K_i$ Return $(k_1, \ldots, k_N, K)$.

Algorithme 7 : Déchiffrement centralisé à clé fragmentée à seuil maximal, codage classique

Entrée : $(k_1, \ldots, k_N)$, (α, β) (N fragments de la clé privée, chiffré)
Sortie : M (élément de groupe représentant le suffrage)

for i *from* 1 *to* N **do**
  $\gamma_i = \alpha^{k_i}$
Return $M = \beta / \prod_i \gamma_i$

Algorithme 8 : Déchiffrement centralisé à clé fragmentée à seuil maximal, codage exponentiel

Entrée : $(k_1, \ldots, k_N)$, (α, β) (N fragments de la clé privée, chiffré)
Sortie : m (entier représentant le suffrage)

for i *from* 1 *to* N **do**
  $\gamma_i = \alpha^{k_i}$
$M = \beta / \prod_i \gamma_i$
Return $m = \log(M)$ i.e m tel que $M = g^m$

Attention

La clé privée de déchiffrement n'a pas besoin d'être explicitement reconstruite, cependant elle peut être facilement recalculée à partir des fragments qui sont bien centralisés (avec les notations de l'algorithme 6, elle vaut $\sum_i k_i$) aussi les algorithmes 6, 7, 8 ne permettent *que de résoudre le problème de mise en place d'une fragmentation de la clé*.

Génération centralisée de clé fragmentée à seuil

La génération de clé ainsi que le déchiffrement (à codage classique ou exponentiel) peuvent être adaptés pour mettre en œuvre une fragmentation à seuil de la clé privée de déchiffrement des bulletins entre l'ensemble des attributaires, telle que **seul un sous-ensemble de ces fragments soit suffisant pour réaliser le déchiffrement**. Dans les algorithmes ci-dessous, N désigne le nombre d'attributaires, $(k_1, \ldots, k_N)$ l'ensemble des fragments de la clé privée, t désigne le seuil et $K_t \subsetneq (k_1, \ldots, k_N)$ désigne n'importe quel sous-ensemble de t fragments de la clé privée. Le chiffrement (à codage classique ou exponentiel) est identique aux cas précédents, seuls la génération de clé et le déchiffrement sont différents.

Attention

Ce mécanisme peut être composé avec une preuve à divulgation nulle de connaissance de déchiffrement correct afin de fournir un déchiffrement vérifiable (R64$^{\star\star}_{\star}$) et suivant l'analyse de risque (R62$^{\star\star}_{\star}$), une preuve de connaissance de clé secrète afin de fournir un partage secret à seuil vérifiable (R74$^{\star\star}_{\star+}$). Voir l'Annexe B.

Algorithme 9 : Génération centralisée de clé fragmentée à seuil

Entrée : g, q, N, t (générateur du groupe, ordre du groupe, nombre de fragments, seuil)
Sortie : $(k_1, \ldots, k_N, K)$ (N fragments de la clé privée, clé publique)

1 $f(X) \xleftarrow{\$} \mathbb{Z}_q[X]$, tel que $deg(f) = t - 1$ et $f(0) = k$ (k : clé privée de l'élection)
2 $K := g^k$
3 **for** i *from* 1 *to* N **do**
4 $\quad k_i := f(i)$
5 Return $(k_1, \ldots, k_N, K)$.

Algorithme 10 : Déchiffrement centralisé à clé fragmentée à seuil, codage classique

Entrée : K_t, (α, β) (sous-ensemble de t fragments de la clé privée, chiffré)
Sortie : M (élément de groupe représentant le suffrage)

1 **for** $k_i \in K_t$ **do**
2 $\quad \gamma_i = \alpha^{k_i}$
3 $D = \prod_i \gamma_i^{a_i}$, where $a_i = \prod_{j!=i}(j)/(j-i)$ (Interpolation de Lagrange)
4 Return $M = \beta / D$

Algorithme 11 : Déchiffrement centralisé à clé fragmentée à seuil, codage exponentiel

Entrée : K_t, (α, β) (sous-ensemble de t fragments de la clé privée, chiffré)
Sortie : j (entier représentant le suffrage)

1 **for** $k_i \in K_t$ **do**
2 $\quad \gamma_i = \alpha^{k_i}$
3 $D = \prod_i \gamma_i^{a_i}$, where $a_i = \prod_{j!=i}(j)/(j-i)$ (Interpolation de Lagrange)
4 $M = \beta / D$
5 Return $m = \log(M)$ i.e m tel que $M = g^m$

Attention

Comme dans le cas précédent (sans seuil), la clé privée de déchiffrement n'a pas besoin d'être explicitement reconstruite, cependant elle peut être facilement recalculée à partir des fragments qui sont bien centralisés, aussi les algorithmes 9, 10, 11 ne permettent *que de résoudre le problème de mise en place d'une fragmentation de clé à seuil*.

Génération distribuée de clé fragmentée, à seuil maximal

La génération de clé ainsi que le déchiffrement (à codage classique ou exponentiel) peuvent être adaptés pour mettre en œuvre une génération distribuée de la clé privée de déchiffrement des bulletins entre l'ensemble des attributaires (dans les algorithmes ci-dessous, N représente le nombre d'attributaires), telle que l'**ensemble des fragments de clé est nécessaire pour réaliser le déchiffrement des bulletins**.

Le chiffrement (à codage classique ou exponentiel) est identique aux cas précédents, seuls la génération de clé et le déchiffrement sont différents. Les algorithmes 12, 13 décrivent la génération de fragment de clé par un attributaire et la génération de la clé publique de chiffrement à partir des fragments générés par les attributaires.

Contrairement au déchiffrement centralisé, le déchiffrement distribué est réalisé en deux étapes. Chaque fragment de la clé privée réalise un *déchiffrement partiel* du chiffré ElGamal. Ensuite tous les déchiffrés sont combinés pour calculer le message en clair. Cette seconde opération ne nécessite pas de fragment de clé de déchiffrement (ni la clé complète).

Les algorithmes 14, 15, 16 décrivent le déchiffrement partiel par un attributaire d'un chiffré ElGamal, la finalisation du déchiffrement au moyen des déchiffrés partiels pour les codages classique et exponentiel.

Attention

Ce mécanisme peut être composé avec une preuve à divulgation nulle de connaissance de déchiffrement correct afin de fournir un déchiffrement vérifiable (R64$^{\star\star}_{\star}$) et suivant l'analyse de risque (R62$^{\star\star}_{\star}$), une preuve de connaissance de clé secrète afin de fournir un partage secret à seuil vérifiable (R74$^{\star\star}_{\star+}$). Voir l'Annexe B.

Algorithme 12 : Génération de fragment de clé fragmentée à seuil maximal

Entrée : i, g, q (identifiant d'attributaire, générateur du groupe, ordre du groupe)
Sortie : (k_i, K_i) (fragment de la clé privée, fragment de la clé publique)

1 $k_i \xleftarrow{\$} \mathbb{Z}_q$
2 $K_i := g^{k_i}$
3 out(K_i) (publication du fragment de clé publique)
4 Return (k_i, K_i).

Algorithme 13 : Génération distribuée de la clé de chiffrement à seuil maximal

Entrée : N (nombre d'attributaires)
Sortie : K (clé publique de chiffrement ElGamal)

1 **for** i *from* 1 *to* N **do**
2 in(K_i) (récupération des fragments de clé publique)
3 Return $K = \prod_i K_i$.

Algorithme 14 : Déchiffrement partiel à seuil maximal

Entrée : $i, k_i, (\alpha, \beta)$ (identifiant d'attributaire, clé privée d'attributaire, chiffré)
Sortie : γ_i (déchiffrement partiel)

1 $\gamma_i = \alpha^{k_i}$
2 out(γ_i) (publication du déchiffré partiel)

Algorithme 15 : Génération distribuée du déchiffrement à seuil maximal, codage classique

Entrée : $N, (\alpha, \beta)$ (nombre d'attributaires, chiffré)
Sortie : M (élément de groupe représentant le suffrage)

1 **for** i *from* 1 *to* N **do**
2 in(γ_i) (récupération des déchiffrés partiels)
3 Return $M = \beta / \prod_i \gamma_i$

Algorithme 16 : Génération distribuée du déchiffrement à seuil maximal, codage exponentiel

Entrée : $N, (\alpha, \beta)$ (nombre d'attributaires, chiffré)
Sortie : m (entier représentant le suffrage)

1 **for** i *from* 1 *to* N **do**
2 in(γ_i) (récupération des déchiffrés partiels)
3 $J = \beta / \prod_i \gamma_i$
4 Return $m = \log(M)$ i.e m tel que $M = g^m$

Attention

Les algorithmes 12, 13, 14, 15, 16 n'ont pas vocation à être utilisés de manière centralisée car cela impliquerait qu'un même équipement contient l'ensemble des fragments de la clé de déchiffrement.

Génération distribuée de clé fragmentée à seuil

La génération de clé ainsi que le déchiffrement (à codage classique ou exponentiel) peuvent être adaptés pour mettre en œuvre une génération distribuée de la clé privée de déchiffrement des bulletins entre l'ensemble des attributaires, telle que **seul un sous-ensemble de ces fragments soit suffisant pour réaliser le déchiffrement**. Dans les algorithmes ci-dessous, N désigne le nombre d'attributaires et I_t désigne n'importe quel sous-ensemble de t attributaires.

Le chiffrement (à codage classique ou exponentiel) est identique aux cas précédents, seuls la génération de clé et le déchiffrement sont différents. Les algorithmes 17, 18 décrivent la génération de clé fragmentée à seuil par un attributaire et la génération de la clé de chiffrement au moyen des morceaux de clé publique.

Attention

Le partage des fragments de clés par les attributaires nécessite l'établissement d'un canal sécurisé entre ces attributaires (instructions in$(i,*)$ et out$(j,*)$ de l'algorithme 17).

Algorithme 17 : Génération de fragment de clé fragmentée à seuil

Entrée : i, t, N, g, q (identifiant d'attributaire, seuil, nombre d'attributaires, générateur du groupe, ordre du groupe)

Sortie : (k_i, K_i) (fragment de la clé privée, fragment de la clé publique)

1 $f_i(X) \xleftarrow{\$} \mathbb{Z}_q[X]$, tel que $deg(f_i) = t-1$ et $f_i(0) = z_i$
2 $K_i = g^{z_i}$
3 out(K_i) (publication du fragment de clé publique)
4 **for** j *from* 1 *to* N **do**
5 $\quad z_{i,j} := f_i(j)$
6 $\quad$ out$(j \neq i, z_{i,j})$ (transmission sur canal sécurisé aux autres attributaires)
7 $\quad$ in$(i \neq j, z_{j,i})$ (réception sur canal sécurisé en provenance des autres attributaires)
8 $k_i = \sum_j z_{i,j}$ Return (k_i, K_i).

Attention

Ce mécanisme peut être composé avec une preuve à divulgation nulle de connaissance de déchiffrement correct afin de fournir un déchiffrement vérifiable (R64$^{\star\star}_{\star}$) et suivant l'analyse de risque (R62$^{\star\star}_{\star}$), une preuve de connaissance de clé secrète afin de fournir un partage secret à seuil vérifiable (R74$^{\star\star}_{\star+}$), voir l'Annexe B.

Algorithme 18 : Génération distribuée de la clé de chiffrement à seuil

Entrée : N (nombre d'attributaires)

Sortie : K (clé publique de chiffrement ElGamal)

1 **for** i *from* 1 *to* N **do**
2 $\quad$ in(K_i) (récupération des fragments de clé publique)
3 Return $K = \prod_i K_i$.

Contrairement au déchiffrement centralisé, le déchiffrement distribué à seuil est réalisé en deux étapes. Chaque fragment de la clé privée réalise un *déchiffrement partiel* du chiffré ElGamal, le nombre de déchiffrements partiels à réaliser étant égal au seuil. Ensuite les déchiffrés sont combinés pour calculer le message en clair. Cette seconde opération ne nécessite pas de fragment de clé de déchiffrement (ni la clé complète).

Les algorithmes 19, 20, 21 décrivent le déchiffrement partiel par un attributaire d'un chiffré ElGamal, la finalisation du déchiffrement au moyen des déchiffrés partiels pour les codages classique et exponentiel.

Algorithme 19 : Déchiffrement partiel à seuil

Entrée : $i \in I_t, k_i, (\alpha, \beta)$ (identifiant d'attributaire pris dans le sous-ensemble I_t, fragment de clé privée, chiffré)

Sortie : γ_i (déchiffrement partiel)

1 $\gamma_i = \alpha^{k_i}$

2 out(γ_i) (publication du déchiffré partiel)

Algorithme 20 : Génération distribuée du déchiffrement à seuil, codage classique

Entrée : $I_t, (\alpha, \beta)$ (sous-ensemble de t identifiants d'attributaires, chiffré)

Sortie : M (élément de groupe représentant le suffrage)

1 **for** $i \in I_t$ **do**

2 in(γ_i) (récupération des déchiffrés partiels)

3 $D = \prod_i \gamma_i^{a_i}$, where $a_i = \prod_{k \neq i}(k)/(k-i)$ (Interpolation de Lagrange)

4 Return $M = \beta / D$

Algorithme 21 : Génération distribuée du déchiffrement à seuil, codage exponentiel

Entrée : $I_t, (\alpha, \beta)$ (sous-ensemble de t identifiants d'attributaires, chiffré)

Sortie : m (entier représentant le suffrage)

1 **for** $i \in I_t$ **do**

2 in(γ_i) (récupération des déchiffrements partiels)

3 $D = \prod_i \gamma_i^{a_i}$, where $a_i = \prod_{k \neq i}(k)/(k-i)$ (Interpolation de Lagrange)

4 $M = \beta / D$

5 Return $m = \log(M)$, i.e m tel que $M = g^m$

Attention

Les algorithmes 17, 18, 19, 20, 21 n'ont pas vocation à être utilisés de manière centralisée car cela impliquerait qu'un même équipement contient l'ensemble des fragments de la clé de déchiffrement.

Annexe B
Preuves à divulgation nulle de connaissance

Cette annexe s'adresse en premier lieu aux prestataires spécialisés dans le vote par correspondance électronique ainsi qu'aux tiers intervenant dans la vérification de la conformité des scrutins. Elle fournit des exemples de preuves à divulgation nulle de connaissance [25, 55].

Les preuves décrites dans cette annexe reposent sur l'utilisation du mécanisme de chiffrement ElGamal pour le chiffrement du suffrage, détaillé à l'Annexe A. Elles fournissent des exemples répondant à plusieurs recommandations de ce guide :

- Les recommandations R18★ et R20★ : la composition du mécanisme avec une preuve à divulgation nulle de connaissance de l'aléa assure la validité du bulletin, la non-malléabilité du mécanisme et renforce l'intégrité des suffrages exprimés ; l'adaptation du contexte de ces preuves avec les attributs du pastillage renforce le secret du scrutin.
- Les recommandations R18★, R20★ et R24★ : la composition du mécanisme avec une preuve à divulgation nulle de connaissance de chiffrement de 0 ou 1 et une preuve à divulgation nulle de connaissance de chiffrement d'entier dans un intervalle assure la validité du suffrage, la non-malléabilité du mécanisme et renforce l'intégrité des suffrages exprimés en cas d'accumulation ; l'adaptation du contexte de ces preuves avec les attributs du pastillage renforce le secret du scrutin.
- La recommandation R64★★★ : la composition du mécanisme avec une preuve à divulgation nulle de connaissance de déchiffrement correct assure la validité du résultat et renforce l'intégrité des suffrages exprimés ainsi que la sincérité des opérations électorales.
- La recommandation R74★★★+ : la composition du mécanisme avec une preuve à divulgation nulle de connaissance de clé secrète renforce le secret du scrutin.

Attention

Les preuves décrites dans cette annexe ne permettent pas d'atteindre certaines propriétés allant au delà du niveau 3 de la CNIL (en particulier la protection contre l'achat de vote, la résistance à la coercition ou la propriété everlasting-privacy). Ces preuves ne sont pas non plus adaptées à des configurations complexes (typiquement le vote avec rature, car le nombre de preuves à calculer est linéaire en le nombre de choix proposés à l'électeur) ou à des modèles de sécurité plus fort (prenant en compte par exemple des attaques adaptatives). Aussi d'autres types de preuves devront être utilisées en fonction de l'analyse de risque (3-01) ou de la configuration de l'élection, par exemple [30, 59, 62, 69, 83, 84, 88].

Cette annexe a pour objet d'expliquer comment les générer et les vérifier, dans le cas générique suivant :

- Un groupe cyclique $\mathbb{G}$, de générateur g, de cardinal premier q (identique au groupe utilisé pour le mécanisme de chiffrement ElGamal).
- Une fonction de hachage cryptographique hash à valeur dans $\mathbb{Z}_q$.

Ces mécanismes doivent être choisis conformément à la recommandation R3★, c'est-à-dire que le problème du logarithme discret est difficile à résoudre dans $\mathbb{G}$ et que la fonction de hachage hash est résistante aux collisions, aux calculs de pré-images, et plus généralement suffisamment solide pour qu'on puisse la modéliser par un oracle aléatoire.

Tous les calculs de preuve à divulgation nulle de connaissance sont faits dans un *contexte*. Ce contexte prend la forme d'une chaîne de caractères ctx qui doit identifier aussi précisément que possible l'environnement où cette preuve est construite, afin qu'elle ne puisse pas être rejouée ailleurs (Typiquement, le contexte contient une chaîne de caractères pour le nom de l'élection, le nom de l'urne, lorsque différentes urnes sont déchiffrées, par exemple suivant les collèges ; il contient aussi le chiffré ElGamal - en entier - sur lequel porte la preuve, ainsi que les informations sur le groupe et le générateur utilisé. Cette liste n'est pas exhaustive et doit être aussi précise que possible).

Dans ce qui suit, on ajoute explicitement à chaque fois le type de preuve au contexte, sous forme d'une chaîne de caractère supplémentaire.

Pour chaque preuve, on présente deux algorithmes : celui qui permet de créer la preuve, et celui qui permet de la vérifier. À chaque fois, on liste les « données publiques », c'est-à-dire la connaissance commune au prouveur et au vérifieur. Quant aux données secrètes, seul le prouveur y a accès ; il utilise ces données secrètes pour l'algorithme de génération, et il a la garantie que la preuve qu'il produit ne révèle rien sur ces données secrètes.

Attention

Cette annexe ne décrit pas les mécanismes de validation des entrées des algorithmes. Il est de bon usage, et parfois crucial pour la sécurité de s'assurer que les éléments de $\mathbb{G}$ appartiennent bien au groupe, et que les éléments de $\mathbb{Z}_q$ sont bien normalisés comme les entiers dans $[0, q-1]$.

Des vulnérabilités ont été identifiées car le contexte des preuves à divulgation nulle de connaissance n'était pas assez complet [29], aussi il est nécessaire d'être vigilant sur sa définition suivant les cas d'usage des preuves.

Les preuves expliquées dans cette annexe sont adaptées à un type de scrutin (l'électeur a la possibilité de sélectionner une ou plusieurs option(s) parmi ℓ), représentatif de la majorité des scrutins organisés en France. Dans le cas de scrutins plus complexes, des preuves supplémentaires devraient être envisagées, aussi leur conception et leur efficacité devraient faire l'objet d'une analyse fine [51, 74], car elles jouent un rôle essentiel pour assurer la sincérité des opérations électorales et l'intégrité des suffrages exprimés.

Preuve de connaissance de clé secrète

Cette preuve est générée par l'application de vote lors de la génération d'une paire de clés de chiffrement ElGamal par un attributaire. Lors de cette création, l'application de vote permet à l'attributaire d'annoncer sa clé publique et de prouver qu'il connaît la clé privée associée.

Données publiques : $\mathcal{D}_{\mathsf{pub}} = \{K, \mathsf{ctx}\}$, où $K \in \mathbb{G}$ est une clé publique.

Données secrètes : $\mathcal{D}_{\mathsf{sec}} = \{k\}$, où $k \in \mathbb{Z}_q$ est tel que $K = g^k$.

Algorithme 22 : Génération de preuve de connaissance de clé secrète

Entrée : $\mathcal{D}_{\mathsf{pub}}$, $\mathcal{D}_{\mathsf{sec}}$
Sortie : $\pi = (c, v)$

1 $\xi \xleftarrow{\$} \mathbb{Z}_q$
2 $A := g^{\xi}$
3 $c := \mathsf{hash}(\text{"zkp\_sec"}, \mathsf{ctx}, K, A)$
4 $v := (\xi - k\,c) \bmod q$
5 Return $\pi = (c, v)$.

Algorithme 23 : Vérification de preuve de connaissance de clé secrète

Entrée : $\mathcal{D}_{\mathsf{pub}}$, $\pi = (c, v)$

1 $A := g^v\, K^c$
2 $c' := \mathsf{hash}(\text{"zkp\_sec"}, \mathsf{ctx}, K, A)$
3 Check $c == c'$.

Preuve de connaissance de l'aléa

Cette preuve est générée par le client de vote après le chiffrement du suffrage par l'algorithme ElGamal avec le codage classique ou avec le codage exponentiel (Annexe A). Elle permet de prouver que le chiffrement est réalisé de manière correcte, c'est-à-dire que le chiffré généré est bien celui correspondant au suffrage. Pour cela, le client de vote génère une preuve de connaissance de l'aléa utilisé dans ce chiffré, car la connaissance de l'aléa implique la connaissance du suffrage.

Données publiques : $\mathcal{D}_{\mathsf{pub}} = \{K, (\alpha, \beta), \mathsf{ctx}\}$, où $K \in \mathbb{G}$ est une clé publique, et $(\alpha, \beta) \in \mathbb{G} \times \mathbb{G}$ est un chiffré ElGamal.

Données secrètes : $\mathcal{D}_{\mathsf{sec}} = \{M, r\}$, où $r \in \mathbb{Z}_q$ est tel que $(\alpha, \beta) = (g^r, MK^r)$, avec $M \in \mathbb{G}$ le message clair associé au chiffré.

Algorithme 24 : Génération de preuve de connaissance de l'aléa

Entrée : $\mathcal{D}_{\mathsf{pub}}, \mathcal{D}_{\mathsf{sec}}$
Sortie : $\pi = (c, v)$

1 $\xi \xleftarrow{\$} \mathbb{Z}_q$
2 $A := g^{\xi}$
3 $c := \mathsf{hash}(\text{"zkp\_enc"}, \mathsf{ctx}, K, \alpha, \beta, A)$
4 $v := (\xi - r\,c) \bmod q$
5 Return $\pi = (c, v)$.

Algorithme 25 : Vérification de preuve de connaissance de l'aléa

Entrée : $\mathcal{D}_{\mathsf{pub}}, \pi = (c, v)$

1 $A := g^v\,\alpha^c$
2 $c' := \mathsf{hash}(\text{"zkp\_enc"}, \mathsf{ctx}, K, \alpha, \beta, A)$
3 Check $c == c'$.

Preuve de chiffrement de 0 ou 1

Cette preuve est générée par le client de vote après le chiffrement du suffrage par l'algorithme ElGamal utilisant le codage exponentiel (Annexe A). Elle permet de prouver que ce chiffrement est effectué de manière correcte, c'est-à-dire que le message clair est soit g^0, soit g^1. Cette preuve se combine avec la précédente : au passage, elle prouve la connaissance de l'aléa utilisé pour le chiffrement ElGamal. Comme expliqué à l'Annexe C, cette preuve est nécessaire dès lors que le mécanisme d'accumulation est mis en œuvre.

Données publiques : $\mathcal{D}_{\mathsf{pub}} = \{K, (\alpha, \beta), \mathsf{ctx}\}$, où $K \in \mathbb{G}$ est une clé publique, et $(\alpha, \beta) \in \mathbb{G} \times \mathbb{G}$ est un chiffré ElGamal.

Données secrètes : $\mathcal{D}_{\mathsf{sec}} = \{M, r\}$, où $M \in \{g^0, g^1\}$ est le message clair associé au chiffré, et $r \in \mathbb{Z}_q$ est tel que $(\alpha, \beta) = (g^r, MK^r)$.

Algorithme 26 : Génération de preuve de chiffrement de 0 ou 1

Entrée : $\mathcal{D}_{\mathsf{pub}}, \mathcal{D}_{\mathsf{sec}}$
Sortie : $\pi = ((c_0, v_0), (c_1, v_1))$

if $m == g^0$ **then**
- $\xi \xleftarrow{\$} \mathbb{Z}_q$; $c_1 \xleftarrow{\$} \mathbb{Z}_q$; $v_1 \xleftarrow{\$} \mathbb{Z}_q$
- $A_0 := g^{\xi}$; $B_0 := K^{\xi}$
- $A_1 := g^{v_1}\, \alpha^{c_1}$; $B_1 := K^{v_1}\, (\beta/g)^{c_1}$
- $c_0 := \mathsf{hash}(\text{"zkp\_enc\_01"}, \mathsf{ctx}, K, \alpha, \beta, A_0, B_0, A_1, B_1) - c_1 \bmod q$
- $v_0 = (\xi - r\, c_0) \bmod q$

if $m == g^1$ **then**
- $\xi \xleftarrow{\$} \mathbb{Z}_q$; $c_0 \xleftarrow{\$} \mathbb{Z}_q$; $v_0 \xleftarrow{\$} \mathbb{Z}_q$
- $A_0 := g^{v_0}\, \alpha^{c_0}$; $B_0 := K^{v_0}\, \beta^{c_0}$
- $A_1 := g^{\xi}$; $B_1 := K^{\xi}$
- $c_1 := \mathsf{hash}(\text{"zkp\_enc\_01"}, \mathsf{ctx}, K, \alpha, \beta, A_0, B_0, A_1, B_1) - c_0 \bmod q$
- $v_1 = (\xi - r\, c_1) \bmod q$

Return $\pi = ((c_0, v_0), (c_1, v_1))$.

Algorithme 27 : Vérification de preuve de chiffrement de 0 ou 1

Entrée : $\mathcal{D}_{\mathsf{pub}}, \pi = ((c_0, v_0), (c_1, v_1))$

- $A_0 := g^{v_0}\, \alpha^{c_0}$
- $A_1 := g^{v_1}\, \alpha^{c_1}$
- $B_0 := K^{v_0}\, \beta^{c_0}$
- $B_1 := K^{v_1}\, (\beta/g)^{c_1}$
- $c' := \mathsf{hash}(\text{"zkp\_enc\_01"}, \mathsf{ctx}, K, \alpha, \beta, A_0, B_0, A_1, B_1) \bmod q$
- Check $c' == c_0 + c_1 \bmod q$.

Preuve de chiffrement d'entier dans un intervalle

Cette preuve est générée par le client de vote après le chiffrement du suffrage par l'algorithme ElGamal utilisant le codage exponentiel (Annexe A) et après la génération de preuve de chiffrement correct (de 0 ou 1). En reprenant les notations de l'Annexe A, chaque électeur génère une liste ordonnée de chiffrés ElGamal, $\mathcal{L} = (\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots, (\alpha_\ell, \beta_\ell)$, telle que $(\alpha_i, \beta_i) = (g^{r_i}, g^0 K^{r_i})$ si l'option i n'a pas été sélectionnée ou $(\alpha_i, \beta_i) = (g^{r_i}, g^1 K^{r_i})$ si l'option i a été sélectionnée. Le client de vote accumule tous les chiffrés ElGamal et prouve que le chiffré ElGamal obtenu, $(\alpha, \beta) = (\prod_i \alpha_i, \prod_i \beta_i)$, est le chiffré d'un entier dans un intervalle fixé par la configuration de l'élection. Comme expliqué à l'Annexe A, cette preuve est nécessaire dès lors que le mécanisme d'accumulation est mis en œuvre.

Deux cas sont décrits : le cas simple et le cas général. Dans le cas simple, une seule option peut être sélectionnée par l'électeur, dans le cas général, plusieurs options peuvent être sélectionnées par l'électeur : le nombre d'options sélectionnées doit être compris dans un intervalle.

Cas simple : une et une seule option doit être sélectionnée

Données publiques : $\mathcal{D}_{\text{pub}} = \{K, (\alpha, \beta), \mathcal{L}, \text{ctx}\}$, où $K \in \mathbb{G}$ est une clé publique, $\mathcal{L}$ est la liste ordonnée des chiffrés ElGamal $(\alpha_1, \beta_1), \ldots, (\alpha_\ell, \beta_\ell)$ et $\alpha, \beta = \prod_i \alpha_i, \prod_i \beta_i$ est leur accumulation.

Données secrètes : $\mathcal{D}_{\text{sec}} = \{r\}$, où $r \in \mathbb{Z}_q$ est tel que $(\alpha, \beta) = (g^r, g^1 K^r)$.

Algorithme 28 : Génération de preuve de sélection d'une et une seule option

Entrée : $\mathcal{D}_{\text{pub}}, \mathcal{D}_{\text{sec}}$
Sortie : $\pi = (c, v)$

1 $\xi \xleftarrow{\$} \mathbb{Z}_q$
2 $A := g^\xi$
3 $B := K^\xi$
4 $c = \text{hash}(\text{"zkp\_enc\_simple"}, \text{ctx}, K, \alpha, \beta, \mathcal{L}, A, B) v = (\xi - r\, c) \bmod q$
5 Return $\pi = (c, v)$

Algorithme 29 : Vérification de preuve de sélection d'une et une seule option

Entrée : $\mathcal{D}_{\text{pub}}, \pi = (c, v)$

1 $A := g^v\, \alpha^c$
2 $B := K^v\, (\beta / g)^c$
3 $c' := \text{hash}(\text{"zkp\_enc\_simple"}, \text{ctx}, K, \alpha, \beta, \mathcal{L}, A, B) \bmod q$
4 Check $c' == c \bmod q$.

Information

L'inclusion de la liste ordonnée des chiffrés $\mathcal{L} = (\alpha_1, \beta_1, \ldots, \alpha_\ell, \beta_\ell)$ dans le contexte de la preuve à divulgation nulle de connaissance permet d'associer à cette preuve l'ordre de ces chiffrés et ainsi d'en détecter une éventuelle permutation. Si un mécanisme de signature des bulletins est mis en œuvre, l'inclusion de cette liste n'est pas nécessaire car l'ordre des chiffrés serait alors garanti par cette signature.

Cas général : le nombre d'options sélectionnées doit être compris dans un intervalle

Données publiques : $\mathcal{D}_{\text{pub}} = \{K, (\alpha, \beta), (\alpha_1, \beta_1), \ldots, (\alpha_\ell, \beta_\ell), \text{ctx}\}$, où $K \in \mathbb{G}$ est une clé publique, $\mathcal{L}$ est la liste ordonnée des chiffrés ElGamal $(\alpha_1, \beta_1), \ldots, (\alpha_\ell, \beta_\ell)$ et $\alpha, \beta = \prod_i \alpha_i, \prod_i \beta_i$ est leur accumulation.

Données secrètes : $\mathcal{D}_{\text{sec}} = \{i_{\text{choisi}}, r\}$, où $i_{\text{choisi}} \in \{i_{\min}, i_{\min}+1, \ldots, i_{\max}\}$ est l'entier codé par le message clair associé au chiffré, et $r \in \mathbb{Z}_q$ est tel que $(\alpha, \beta) = (g^r, g^{i_{\text{choisi}}} K^r)$.

Algorithme 30 : Génération de preuve de chiffrement d'entier dans un intervalle

Entrée : $\mathcal{D}_{\text{pub}}$, $\mathcal{D}_{\text{sec}}$
Sortie : $\pi = ((c_{i_{\min}}, v_{i_{\min}}), (c_{i_{\min}+1}, v_{i_{\min}+1}), \ldots, (c_{i_{\max}}, v_{i_{\max}}))$

for i *from* $i_{\min}$ *to* $i_{\max}$ **do**
  if $i == i_{\text{choisi}}$ **then**
    $\xi \xleftarrow{\$} \mathbb{Z}_q$
    $A_{i_{\text{choisi}}} := g^{\xi}$
    $B_{i_{\text{choisi}}} := K^{\xi}$
  else
    $c_i \xleftarrow{\$} \mathbb{Z}_q$
    $v_i \xleftarrow{\$} \mathbb{Z}_q$
    $A_i := g^{v_i}\, \alpha^{c_i}$
    $B_i := K^{v_i}\, (\beta / g^i)^{c_i}$
$c_{i_{\text{choisi}}} = \text{hash}(\text{"zkp\_enc\_int"}, \text{ctx}, K, \alpha, \beta, \mathcal{L}, A_{i_{\min}}, B_{i_{\min}}, A_{i_{\min}+1}, B_{i_{\min}+1}, \ldots, A_{i_{\max}}, B_{i_{\max}}) - (\sum_{i \neq i_{\text{choisi}}} c_i) \bmod q$
$v_{i_{\text{choisi}}} = (\xi - r\, c_i) \bmod q$
Return $\pi = ((c_{i_{\min}}, v_{i_{\min}}), (c_{i_{\min}+1}, v_{i_{\min}+1}), \ldots, (c_{i_{\max}}, v_{i_{\max}}))$

Algorithme 31 : Vérification de preuve de chiffrement d'entier dans un intervalle

Entrée : $\mathcal{D}_{\text{pub}}$, $\pi = ((c_{i_{\min}}, v_{i_{\min}}), (c_{i_{\min}+1}, v_{i_{\min}+1}), \ldots, (c_{i_{\max}}, v_{i_{\max}}))$

for i *from* $i_{\min}$ *to* $i_{\max}$ **do**
  $A_i := g^{v_i}\, \alpha^{c_i}$
  $B_i := K^{v_i}\, (\beta / g^i)^{c_i}$
$c' := \text{hash}(\text{"zkp\_enc\_int"}, \text{ctx}, K, \alpha, \beta, \mathcal{L}, A_{i_{\min}}, B_{i_{\min}}, A_{i_{\min}+1}, B_{i_{\min}+1}, \ldots, A_{i_{\max}}, B_{i_{\max}}) \bmod q$
Check $c' == (\sum_i c_i) \bmod q$.

Information

L'inclusion de la liste ordonnée des chiffrés $\mathcal{L} = (\alpha_1, \beta_1, \ldots, \alpha_\ell, \beta_\ell)$ dans le contexte de la preuve à divulgation nulle de connaissance permet d'associer à cette preuve l'ordre de ces chiffrés et ainsi d'en détecter une éventuelle permutation. Si un mécanisme de signature des bulletins est mis en œuvre, l'inclusion de cette liste n'est pas nécessaire car l'ordre des chiffrés serait alors garanti par cette signature.

Preuve de déchiffrement correct

Cette preuve est générée par l'application de vote lors du déchiffrement d'un chiffré ElGamal par un attributaire. Lors de ce déchiffrement, l'application de vote permet à l'attributaire de prouver (sans dévoiler sa clé secrète) qu'il a effectué ce déchiffrement de manière correcte.

Données publiques : $\mathcal{D}_{\mathsf{pub}} = \{K, (\alpha, \beta), M, \mathsf{ctx}\}$, où $K \in \mathbb{G}$ est une clé publique, $(\alpha, \beta) \in \mathbb{G} \times \mathbb{G}$ est un chiffré ElGamal, et $M \in \mathbb{G}$ est le message clair correspondant.

Données secrètes : $\mathcal{D}_{\mathsf{sec}} = \{k\}$, où $k \in \mathbb{Z}_q$ est tel que $K = g^k$.

Algorithme 32 : Génération de preuve de déchiffrement correct

Entrée : $\mathcal{D}_{\mathsf{pub}}, \mathcal{D}_{\mathsf{sec}}$
Sortie : $\pi = (c, v)$

1 $\xi \xleftarrow{\$} \mathbb{Z}_q$
2 $A := g^{\xi}$
3 $B := \alpha^{\xi}$
4 $c := \mathsf{hash}(\text{"zkp\_dec"}, \mathsf{ctx}, K, \alpha, \beta, M, A, B)$
5 $v := (\xi - k\,c) \bmod q$
6 Return $\pi = (c, v)$.

Algorithme 33 : Vérification de preuve de déchiffrement correct

Entrée : $\mathcal{D}_{\mathsf{pub}}, \pi = (c, v)$

1 $A := g^v\, K^c$
2 $B := \alpha^v\, (\beta / M)^c$
3 $c' := \mathsf{hash}(\text{"zkp\_dec"}, \mathsf{ctx}, K, \alpha, \beta, M, A, B)$
4 Check $c == c'$.

Information

Lorsque l'accumulation des bulletins est mise en œuvre afin d'assurer l'étanchéité entre l'identité de l'électeur et l'expression de son vote (1-07), le nombre de preuves de déchiffrement correct à générer (et à vérifier) est égal au nombre d'options proposées aux électeurs. Lorsqu'un mélange vérifiable est mis en œuvre, le nombre de preuves de déchiffrement correct à générer (et à vérifier) est égal au nombre de votants.

Annexe C
Accumulation, mélange cryptographique, mélange vérifiable

Cette annexe s'adresse aux organisateurs de scrutin, aux prestataires spécialisés dans le vote par correspondance électronique ainsi qu'aux tiers intervenant dans la vérification de la conformité des scrutins. Elle fournit des explications sur les notions d'accumulation, de mélange cryptographique et de mélange vérifiable.

L'accumulation et le mélange cryptographique sont les deux mécanismes mentionnés dans ce guide pour assurer l'étanchéité entre l'identité de l'électeur et l'expression de son vote, c'est-à-dire le contenu déchiffré de son bulletin (1-07). **Ces mécanismes sont requis pour les scrutins de niveau 1 et 2.**

Attention

Un mélange *non cryptographique* consiste à utiliser une permutation (secrète) pour ré-ordonner les bulletins contenus dans l'urne électronique, sans modifier ces bulletins : la sortie du mélange est le même ensemble de bulletins, dans un ordre différent. Ainsi, il est possible de lier chaque bulletin issu du mélange à un bulletin de l'urne électronique, y compris si la permutation reste secrète. Après déchiffrement des bulletins issus du mélange, il est donc possible de relier chaque suffrage avec un bulletin de l'urne électronique. Cela porte atteinte au secret du scrutin, aussi **ce type de mélange ne doit pas être utilisé pour assurer l'étanchéité entre l'identité de l'électeur et son suffrage.**

À l'inverse, un mélange cryptographique consiste à utiliser à la fois une permutation et une clé ou un aléa (secrets) pour générer un ensemble *décorrélé* de l'urne électronique. Ainsi chaque élément de ce nouvel ensemble ne peut pas être lié aux bulletins de l'urne électronique, sauf à disposer de la clé ou de l'aléa utilisé. Il y a classiquement deux types de mélange cryptographique, le mélange par **déchiffrement** et le mélange par **re-chiffrement**, expliqués ci-dessous.

Comme un mélange cryptographique est un mécanisme générant un ensemble décorrélé de l'urne électronique, il est possible de fournir en sortie du mélange un ensemble ne correspondant pas aux suffrages de l'ensemble de bulletins de l'urne. Un mélange vérifiable permet de détecter une telle manipulation, aussi **ce mécanisme doit remplacer un mélange cryptographique non vérifiable pour les scrutins de niveau 3.**

L'accumulation étant un mécanisme déterministe, donc vérifiable, est compatible avec les scrutins de niveau 3.

Accumulation des bulletins

Ce mécanisme est adapté lorsque les suffrages sont chiffrés avec un mécanisme de chiffrement homomorphe additif, ce qui est par exemple le cas lorsque le mécanisme de chiffrement ElGamal avec le codage exponentiel est utilisé pour le chiffrement du suffrage.

Information

L'accumulation ne nécessite pas la clé privée de l'élection, elle peut donc être réalisée sur le serveur contenant l'urne électronique, le résultat de l'accumulation pouvant ensuite être transféré vers l'équipement chargé du déchiffrement (3-04).

Les bulletins n'étant pas individuellement déchiffrés (et donc le suffrage qu'ils contiennent n'étant pas individuellement validé), il est nécessaire de vérifier leur validité, ainsi que la validité du suffrage qu'ils contiennent, avant de les accumuler (voir Annexe A).

Par exemple, dans le cas du mécanisme de chiffrement ElGamal (Annexe A), sans cette vérification, un électeur peut fournir deux types de bulletins invalides :

- Un bulletin pour lequel une option a été sélectionnée plusieurs fois au lieu d'une seule. Dans le cas du codage exponentiel, cela signifie que pour cette option, le message chiffré est g^a, avec $a > 1$ au lieu de g^1 (l'électeur atribue par exemple a voix à un candidat au lieu d'une seule).
- Un bulletin contenant plus (ou moins) d'options que le nombre prévu par la configuration de l'élection. Par exemple, pour le codage exponentiel, , cela signifie que la liste des chiffrés générée par le client de vote, $(\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots, (\alpha_\ell, \beta_\ell)$, contient un nombre de chiffrés du message g^1 strictement inférieur ou strictement supérieur à celui prévu (l'électeur sélectionne par exemple plusieurs candidats au lieu d'un seul).

Des exemples de systèmes de vote mettant en œuvre le mécanisme d'accumulation basé sur le mécanisme de chiffrement ElGamal à codage exponentiel sont décrits dans [1, 27, 45, 49].

Mélange cryptographique des bulletins

Les preuves décrites en Annexe B s'appliquent dans le cas où un électeur doit choisir une ou plusieurs options parmi ℓ. Lorsque la configuration de l'élection est plus complexe (typiquement lorsque le nombre d'options proposées aux électeurs est élevé, par exemple dans le cas du vote avec rature [35]) ou bien d'autres possibilités sont fournies à l'électeur (par exemple le vote pondéré ou le panachage), les preuves à divulgation nulle de connaissance nécessaires pour l'accumulation des bulletins peuvent être nombreuses ou difficiles à mettre en œuvre dans le client de vote (si par exemple le nombre de preuves à calculer est linéaire en le nombre de choix proposés à l'électeur). Dans ce cas, il est nécessaire soit d'adapter les preuves pour continuer à utiliser l'accumulation des bulletins, soit de basculer sur un autre mécanisme que l'accumulation pour assurer l'étanchéité entre l'identité de l'électeur et l'expression de son vote. Le mélange cryptographique assure cette étanchéité, tout en ne requérant pas autant de preuves liées au bulletin, allégeant ainsi les traitements du client de vote. La contrepartie est que les traitements à réaliser sur l'urne électronique sont plus complexes que l'accumulation.

35. Le vote avec rature est explicitement autorisé pour l'élection de la délégation du personnel au comité social économique (CSE) [76].

Un équipement qui réalise un mélange est un *mélangeur* ; lorsque plusieurs de ces équipements sont mis en œuvre, on parle de *réseau de mélangeur* ou *mix-net*.

Il y a classiquement deux types de mélange cryptographique, le mélange par **déchiffrement** et le mélange par **re-chiffrement** :

- Dans le premier cas, chaque mélangeur effectue une partie du déchiffrement, qui est donc complètement réalisé à l'issue du dernier mélange. Les traitements réalisés par les mélangeurs doivent en général être réalisés dans un ordre donné.
- Dans le second cas, chaque mélangeur ne contribue « que » au mélange : à l'issue de celui-ci le déchiffrement des bulletins doit être réalisé.

Le mélange par déchiffrement a été initialement décrit dans [35], il a l'avantage d'être compatible avec n'importe quel mécanisme de chiffrement asymétrique des suffrages. Un exemple de système de vote mettant en œuvre un mélange par déchiffrement est décrit dans [66].

Le mélange par re-chiffrement peut quant à lui être mis en œuvre en exploitant la malléabilité du mécanisme de chiffrement des suffrages. Le mécanisme de chiffrement ElGamal dispose de cette propriété, aussi il est adapté à ce mélange, cependant cette propriété constitue aussi une vulnérabilité (recommandation R18★) : il est nécessaire de composer le chiffrement avec une preuve à divulgation nulle de connaissance de l'aléa afin de la rendre non-exploitable (voir Annexe A). Une fois cette preuve vérifiée, le mélange peut être réalisé.

Il existe de nombreux exemples de systèmes de vote mettant en œuvre un mélange par re-chiffrement, basé sur le mécanisme de chiffrement ElGamal (voir la liste ci-dessous donnée pour la mise en œuvre d'un mélange vérifiable par re-chiffrement).

Mélange vérifiable des bulletins

Un mélange cryptographique est un mécanisme générant un nouvel ensemble de données décorrélées des bulletins de l'urne électronique. Il est donc possible de fournir en sortie de mélange des données sans rapport avec l'urne, et de porter atteinte à l'intégrité des suffrages exprimés et à la sincérité des opérations électorales. Un mélange vérifiable permet de détecter une telle manipulation.

Un tel mélange produit une preuve à divulgation nulle de connaissance que l'ensemble des bulletins mélangés contient exactement le même ensemble de suffrages que l'ensemble des bulletins avant chaque mélange. Ces preuves (de mélange correct) ne sont pas génériques et dépendent fortement du mélange réalisé et de l'algorithme de chiffrement utilisé.

De plus, la mise en place d'un mélange vérifiable est délicate car il faut définir le nombre de mélangeurs et statuer sur le niveau de confiance apporté à chaque (serveur implémentant un) mélangeur [60]. Enfin, la réalisation du mélange peut nécessiter des délais importants incompatibles avec sa tenue au cours d'une cérémonie publique de dépouillement dès la clôture du scrutin.

Des exemples de systèmes de vote mettant en œuvre un mélange vérifiable par re-chiffrement, basé sur le mécanisme de chiffrement ElGamal sont décrits dans [36, 45, 57, 69, 88, 91, 92, 93, 94]. Une description complète est par exemple fournie dans [58].

Annexe D
Receipt-freeness, protection contre l'achat de vote, résistance à la coercition

Cette annexe s'adresse aux organisateurs de scrutin, aux prestataires spécialisés dans le vote par correspondance électronique ainsi qu'aux tiers intervenant dans la vérification de la conformité des scrutins. Elle fournit des explications sur les notions de receipt-freeness, de protection contre l'achat de vote et de résistance à la coercition.

La propriété de receipt-freeness est **requise pour tous les niveaux de scrutin**, la protection contre l'achat de vote et de résistance à la coercition sont envisageables en fonction de l'analyse de risque (3-01).

Dans les grandes lignes, la propriété de receipt-freeness [28] consiste à empêcher les votants honnêtes qui auraient suivi le protocole de vote, de prouver à un attaquant comment ils ont voté. En particulier, les votants ne sauvegardent que les données qu'ils voient et qu'ils reçoivent. Il est nécessaire (et possible) de mettre en œuvre cette propriété en s'assurant que le récépissé de vote, la preuve de vote, les affichages réalisés par le client de vote à l'électeur ainsi que les données publiées par le système de vote ne contiennent pas d'information qui *à elles seules* portent atteinte au secret du scrutin (par exemple, ces données ne doivent pas contenir le suffrage en clair ou contenir la clé clé privée de l'élection, ou bien le client de vote ne doit pas afficher à l'électeur l'aléa généré pour chiffrer le bulletin). C'est l'objet de la recommandation R30★.

La protection contre l'achat de vote est une propriété plus forte que la propriété receipt-freeness, renforçant le caractère personnel du vote : l'électeur est considéré capable d'effectuer des manipulations, par exemple d'extraire des données intervenant dans la constitution de son bulletin et de s'en servir pour prouver son vote au moyen des données publiées par le système de vote. En considérant un électeur avec cette capacité, la vérifiabilité individuelle pourrait être remise en cause : pour assurer la protection contre l'achat de vote, le système de vote devrait assurer que les données publiées dépendent d'un secret non connu de l'électeur, tout en assurant la propriété de vérifiabilité individuelle. Cette contradiction peut être levée en utilisant des protocoles de vote spécifiques, aussi cette mise en œuvre est envisageable en fonction de l'analyse de risque (3-01).

Enfin, la résistance à la coercition est une propriété plus forte que la protection contre l'achat de vote, renforçant le caractère libre du vote : l'électeur peut être contraint pendant une partie de l'opération de vote. Cette propriété nécessite également l'utilisation de protocoles de vote spécifiques, aussi elle est également envisageable en fonction de l'analyse de risque (3-01).

Du fait de ces spécificités, l'achat de vote et la coercition sont des risques identifiés comme non couverts par les recommandations de ce guide (Section 4.5).

Annexe E
Mise en œuvre du pastillage

Cette annexe s'adresse aux organisateurs de scrutin, aux prestataires spécialisés dans le vote par correspondance électronique ainsi qu'aux tiers intervenant dans la vérification de la conformité des scrutins. Elle fournit des explications sur la notion de pastillage.

Le pastillage consiste à rendre possible des extractions d'informations complémentaires à un scrutin dit « scrutin direct » :

- Soit pour constituer d'autres instances dans un périmètre qui est inférieur à celui du scrutin direct, telles que les formations spécialisées. On parle alors de « scrutin indirect constitutif ».
- Soit à des fins statistiques ou informatives destinées à l'organisateur du scrutin ou d'autres entités (par exemple pour obtenir représentativité des candidats dans des sous-ensembles de l'électorat). On parle alors de « scrutin indirect informatif ».

Exemple

Dans une association communale, les statuts exigent que le conseil central d'administration soit élu par l'ensemble des adhérents, et que le même vote élise aussi des conseillers par quartier. Les listes candidates souhaitent également connaître leur représentativité parmi les électeurs actifs et retraités au niveau de la commune.

Dans ce cas, à chaque électeur sont associés deux attributs : son quartier de résidence et son statut actif ou retraité. Pour cette élection, on aura un seul vote par électeur, mais plusieurs scrutins : le scrutin direct au niveau communal, un scrutin indirect constitutif par quartier pour élire les conseils de quartier, et deux scrutins indirects informatifs donnant les résultats pour les actifs et pour les retraités.

La mise en œuvre du pastillage consiste en l'association d'attributs à un électeur, qui doivent suivre son bulletin. Ces attributs sont utilisés pour produire des résultats à des scrutins indirects. Ces résultats partiels sont calculés de la même manière que le résultat de l'élection, c'est-à-dire en additionnant les suffrages, mais sur un sous-ensemble des bulletins qui disposent d'un ou plusieurs attributs, correspondants au scrutin indirect. La mise en œuvre doit également empêcher :

- la génération d'un autre résultat que ceux du scrutin direct et ceux des scrutins indirects, correspondant à d'autres attributs, car ces résultats illicites peuvent porter atteinte au secret du scrutin ;
- la fourniture, par un électeur, d'une autre liste d'attributs que la sienne, car cette possibilité peut porter atteinte à la sincérité des opérations électorales ou lui permettre de prouver son vote.

Exemple

Dans l'exemple précédent, cela signifie que :

- il doit être impossible de générer un scrutin indirect informatif donnant les résultats pour les actifs et les retraités *au niveau d'un quartier*, et,
- il doit être impossible, pour un électeur *actif*, d'utiliser un attribut *retraité* (ou l'inverse), ou d'utiliser un attribut arbitraire l'identifiant de manière certaine.

Une première mise en œuvre possible du pastillage consiste à associer les attributs au suffrage de l'électeur et à *les chiffrer avec ce suffrage*, sans les associer au bulletin. Il n'est pas possible d'accumuler les bulletins car la donnée chiffrée n'est plus additionnable, aussi seul un mélange cryptographique est possible. De plus, les attributs n'étant pas associés au bulletin, il est impossible de les vérifier, sans divulguer le suffrage.

Les attributs ne sont pas associés au bulletin (c'est à dire le chiffré du suffrage). Dans ce cas, il n'existe qu'une seule urne, correspondant au scrutin direct, qui est dépouillée. Après le mélange et le déchiffrement, on exécute le décompte correspondant à chaque scrutin indirect en sélectionnant les suffrages associés au scrutin d'après leurs attributs.

Attention

Cette mise en œuvre comporte un risque majeur sur le secret du scrutin ainsi que sur la sincérité des opérations électorales. Elle doit être écartée.

En effet, même si au final un seul attribut est utilisé pour produire chaque résultat partiel, chaque suffrage reste bien lié à la conjonction des attributs d'origine et cette conjonction persiste sur le suffrage quel que soit le mélange effectué. Cela implique que lorsque la liste contient beaucoup d'attributs, il est possible de retrouver le lien suffrage/électeur : le secret du scrutin peut être compromis. Dans l'exemple précédent, cela signifie que chaque suffrage est lié au quartier de résidence de l'électeur **et** à son statut, *alors que cette conjonction n'est aucunement nécessaire pour chacun des deux scrutins indirects envisagés*.

De plus, comme les attributs ne sont connus qu'après déchiffrement, il est tout à fait possible de renseigner une fausse liste d'attributs, telle que le nombre de suffrages exprimés pour le scrutin direct soit correct et pour autant le nombre de suffrages exprimés dans un des scrutins indirects soit incorrect. Cela pourrait porter atteinte à la sincérité des opérations électorales et entraîner l'annulation de l'élection. Dans l'exemple précédent, cela signifie par exemple qu'un électeur ayant le statut *actif* le remplace par *retraité*, ou bien modifie l'attribut correspondant à son quartier de résidence : le dépouillement du scrutin direct reste valide, cependant les scrutins indirects seraient invalides.

Une seconde mise en œuvre possible du pastillage consiste à *ne pas* associer les attributs au suffrage mais à les associer au bulletin (le chiffré du suffrage). Dans ce cas il y a une urne électronique correspondant au scrutin direct et autant d'urnes électroniques qu'il y a de scrutins indirects, dans lesquelles les bulletins sont déposés en fonction des attributs. Pour autant, il y a une seule liste

d'émargement : la cohérence entre l'urne et l'émargement (1.10) est vérifiable pour les scrutins direct et indirects en filtrant cette unique liste d'émargement sur les attributs.

Si l'accumulation des bulletins est mise en œuvre dans chaque urne, le bulletin contient, en plus du chiffré du suffrage, un moyen de vérifier la validité de ce suffrage, sans le dévoiler (R24★). Par exemple, dans le cas du mécanisme de chiffrement ElGamal, cela peut être la conjonction des preuves à divulgation nulle de connaissance de chiffrement de 0 ou 1 et de chiffrement d'entier dans un intervalle. Le contexte de ces preuves peut être complété avec les attributs, afin de lier sans ambiguïté les bulletins aux urnes électroniques des scrutins indirects.

Si l'accumulation des bulletins n'est pas mise en œuvre et que l'étanchéité entre l'identité de l'électeur et l'expression de son vote est assurée par mélange cryptographique, il y a deux possibilités :

- Le bulletin contient, en plus du chiffré du suffrage, un moyen permettant de vérifier la validité de ce bulletin. Par exemple, dans le cas du mécanisme de chiffrement ElGamal, cela peut être la preuve à divulgation nulle de connaissance de l'aléa utilisé (voir Annexe B).
- Il n'existe pas un tel moyen et le bulletin ne contient « que » le chiffré du suffrage.

Dans le cas où le bulletin contient un moyen de vérifier sa validité, par exemple une preuve à divulgation nulle de connaissance de l'aléa, le contexte de la preuve peut être complété avec les attributs des électeurs. Comme pour l'accumulation, afin de détecter un déplacement de bulletin, cette preuve doit être vérifiée avant le dépôt du bulletin dans chaque urne et avant le mélange des bulletins (R20★).

Dans le cas où le bulletin ne contient « que » le chiffré, il est nécessaire de le lier avec les attributs par un mécanisme qui assure que cette liaison ne peut pas être modifiée et qu'elle puisse être vérifiée, comme l'assurerait une preuve à divulgation nulle de connaissance.

Dans les deux cas (preuve à divulgation nulle de connaissance ou autre mécanisme), les bulletins sont mélangés et déchiffrés d'une part dans l'urne du scrutin direct et d'autre part dans chaque urne de scrutin indirect, chacune correspondant à un ensemble d'attributs.

Une fois que l'accumulation ou le mélange cryptographique est réalisé, le déchiffrement de l'urne du scrutin direct et des urnes des scrutins indirects peut être réalisé. Chaque bulletin de l'urne du scrutin direct est bien lié à l'ensemble de ses attributs, cependant les accumulations ou les mélanges réalisés assurent que ce lien n'est plus lié aux suffrages exprimés.

Information

Un taux de participation faible peut porter atteinte au secret du scrutin, en particulier dans le cas des scrutins indirects *informatifs*. Ce risque peut être réduit en définissant un seuil, relatif au nombre de suffrages *exprimés*, à partir duquel le dépouillement du scrutin indirect peut être réalisé. La décision de procéder au dépouillement pour ces scrutins indirects est donc prise en fonction de la participation.

Annexe F
Renforcement du client de vote

Cette annexe s'adresse en premier lieu aux prestataires spécialisés dans le vote par correspondance électronique ainsi qu'aux tiers intervenant dans la vérification de la conformité des scrutins.

Cette annexe présente des mécanismes qui peuvent être mis en œuvre par un client de vote JavaScript afin de renforcer le secret du suffrage, d'une part en contrôlant les données mises en cache (R16★) et d'autre part en détectant les caractéristiques de l'équipement utilisé par l'électeur (R17★).

Contrôle des données mises en cache

Certains mécanismes peuvent influencer le cache, sachant qu'il est impossible en JavaScript d'interagir avec la gestion de la mémoire d'une variable. Ces mécanismes ne permettent cependant pas de contrôler le cache au niveau du navigateur ou au niveau du système d'exploitation.

Il est possible en JavaScript d'utiliser les techniques suivantes, qui ont un impact sur le cache (pour toutes ces techniques, voir la documentation [77]) :

- Contrôler le cache HTTP via des entêtes : les entêtes « Cache-Control », « Expires » ou « Etag » sont définis côté serveur et peuvent empêcher le client de placer la réponse en cache.
- Utiliser l'API « Cache Web ». Cette API specifique au contexte des « Service Workers » permet de supprimer une réponse du cache.
- Remplir la mémoire d'un grand nombre d'objets afin de provoquer l'exécution du « Garbage Collector ».
- Contrôler le cache CPU via l'utilisation de « SharedArrayBuffer ».

Contrôle de l'équipement utilisé par l'électeur

Pour les caractéristiques suivantes, il n'existe pas d'API JavaScript permettant de les déterminer, cependant il est possible de construire des heuristiques de détection, à implémenter au niveau du client de vote (voir également la documentation [77]) :

- Nom et version du moteur JavaScript : heuristique basée sur les différences d'implémentation connues entre navigateurs. Cette technique est délicate car elle nécessite de construire et maintenir à jour une base de données complexe, suivant les changements entre versions des moteurs.
- Activation de la « Sandbox » et niveau de restriction : heuristique basée sur l'accès à des ressources bloquées lorsque la sandbox est activée (notamment système). Des différences lors de l'utilisation des « Iframes » peuvent également apparaître lorsque la sandbox est activée.
- Activation du mode debug : heuristique basée sur le temps d'exécution de certaines requêtes.

Pour le système d'exploitation et le navigateur : le « UserAgent » est une donnée envoyée lors d'une requête HTTP qui contient des informations sur le système d'exploitation et le navigateur utilisés par le client. Le langage JavaScript peut interroger ces informations, via l'API navigator.userAgent en ReadOnly. Ces informations ne sont pour autant pas fiables, car elles peuvent être facilement altérées.

Liste des figures

Liste des recommandations

Glossaire

Accumulation Mécanisme cryptographique assurant l'étanchéité bulletin/suffrage. Ce mécanisme consiste à calculer le chiffrement de la somme des suffrages en additionnant (ou multipliant suivant les cas) les bulletins entre eux. Il nécessite l'utilisation d'un chiffrement additivement homomorphe. 15, 33, 42, 43, 53, 55, 79, 81, 84, 95, 115, 121

Accès au vote pour tous les électeurs Un des principes fondamentaux qui commandent les opérations électorales, qui exprime que l'organisation des opérations électorales doit permettre à chaque électeur d'exprimer son vote [72]. 6, 39, 58, 64, 68, 69, 83

Achat de vote (protection contre l') Propriété d'un système de vote assurant que l'électeur ne peut pas prouver l'expression de vote à un tiers. 8, 43, 93, 107, 118

API (Application Programming Interface) Interface logicielle qui permet de « connecter » un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et d'utiliser des fonctionnalités [38]. 23, 122

Application de vote Logiciel installé sur le serveur de vote traitant les bulletins transmis par les électeurs. 50, 51, 60, 63, 66, 69, 88

Authentification Processus consistant à vérifier la preuve d'une identité précédemment annoncée grâce à un moyen d'authentification [2, 22]. Dans le contexte d'un scrutin, processus permettant de vérifier l'identité et la légitimité d'un électeur. 4, 5, 20, 68

Bourrage d'urne Dépôt illégitime de bulletins dans l'urne électronique. 39, 88, 93

Bulletin Donnée contenant le suffrage de l'électeur chiffré. Cette notion correspond à la notion d'enveloppe dans le vote à l'urne. 5, 18, 29, 37, 41, 52, 62, 74, 84, 115, 118, 119

Bureau de vote Désigne à la fois le lieu où s'exerce le droit de vote (dans le cas du vote à l'urne) et l'entité responsable des opérations de vote (voir Bureau électoral). 4

Bureau électoral Entité responsable du contrôle des opérations de vote par voie électronique. 6, 46, 48, 53, 61, 63–66, 74, 84

Cachet Signature numérique. 60

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) Test automatisé permettant de différencier un utilisateur humain d'un ordinateur. Mesure de protection visant notamment à limiter les attaques par force brute automatisées. 23, 29

Caractère libre du vote Un des principes fondamentaux qui commandent les opérations électorales, qui exprime que les membres du corps électoral doivent être à l'abri de toute pression, et les parties prenantes à l'organisation de l'élection doivent être neutres et objectives, garantissant notamment l'égalité entre les candidats. Le respect de ce principe peut dépendre de facteurs extérieurs au système de vote par correspondance électronique [72]. 6, 43, 93, 118

Caractère personnel du vote Un des principes fondamentaux qui commandent les opérations électorales, qui exprime que le risque de recours à la délégation de vote, et donc à l'achat de vote, ainsi que le risque d'usurpation d'identité, doivent pouvoir être limités [72]. 6, 19, 20, 23, 43, 73, 93, 118

Cast-as-intended Vérifiabilité de l'intention – le suffrage *émis* est conforme à l'*intention* de l'électeur : propriété faisant partie de vérifiabilité individuelle qui signifie que l'électeur doit pouvoir vérifier que son bulletin contient bien l'expression de son vote. 71, 86, 87, 93

CDN (Content Delivery Network) Groupe de serveurs reliés en réseau mettant à disposition du contenu [77]. 29, 36, 59

Chaînage Mécanisme cryptographique utilisant des signatures ou des empreintes numériques liant entre eux des ensembles de données et permettant de détecter leur modification. 15, 39, 52, 61, 62, 64, 88

Chiffrement Mécanisme cryptographique assurant la confidentialité d'une donnée. 15, 31, 42, 81, 93

Chiffrement asymétrique Chiffrement consistant à chiffrer une donnée avec une clé publique et la déchiffrer avec une clé privée. 7, 31, 117

Chiffrement homomorphe Chiffrement permettant de manipuler les données chiffrées pour obtenir le chiffré d'une combinaison des données en clair correspondantes. Dans le contexte du vote électronique, la propriété recherchée est la génération d'une donnée chiffrée contenant la somme des suffrages, ce que permet le codage exponentiel. 43, 116

Chiffrement probabiliste Chiffrement utilisant un aléa permettant de différentier deux chiffrements de deux données identiques. 31

Client de vote Partie logicielle du système de vote exécutée sur l'équipement utilisé par l'électeur pour lui permettre d'exprimer son vote. En général, application JavaScript exécutée dans un navigateur. 5, 16, 18, 29, 30, 35, 41, 72, 74, 86, 88, 93, 116, 118

Clé privée de l'élection Lorsque le chiffrement du suffrage est réalisé par un mécanisme de chiffrement asymétrique, une paire de clé publique/privée est générée et la partie privée est utilisée pour réaliser le déchiffrement. La clé privée est alors appelée clé privée de l'élection. 7, 16, 31, 42, 44–48, 52, 53, 55, 69, 76, 79, 80, 84, 85, 88–91, 93, 116, 118, 126

Clé publique de l'élection Lorsque le chiffrement du suffrage est réalisé par un mécanisme de chiffrement asymétrique, une paire de clé publique/privée est générée et la partie publique est transmise aux électeurs pour leur permettre de chiffrer leur suffrage. La clé publique est alors appelée clé publique de l'élection. 7, 31, 61, 80, 81, 89–91, 96

Codage classique Codage consistant à représenter le suffrage par un élément de groupe. 94

Codage exponentiel Codage consistant à représenter le suffrage par un entier. 94, 116

Coercition (résistance à la) Propriété d'un système de vote assurant que l'électeur peut réaliser son vote librement même en étant sous la contrainte. 8, 43, 93, 107, 118

Configuration de l'élection Ensemble des données caractérisant une élection (notamment : dates d'ouverture et de clôture, liste électorale, options de vote, découpage électoral, pastillage, données de vérification de l'authentification des électeurs, clé publique de chiffrement des suffrages). 4, 7, 15, 37, 50, 52, 54, 60, 69, 80, 96, 107, 116

CPU (Central Processing Unit) Processeur d'un ordinateur. 59, 122

CVE (Common Vulnerabilities and Exposures) Programme d'identification, de qualification et de publication de vulnérabilités informatiques [48]. 31

CVSS (Common Vulnerability Scoring System) Méthode permettant de qualifier la criticité d'une vulnérabilité [56]. 16

Divulgation responsable Modèle de divulgation de vulnérabilité informatique dans lequel les parties prenantes s'engagent à laisser un délai avant la divulgation de la vulnérabilité afin de permettre sa correction avant cette divulgation [81]. 75, 86

Durcissement (d'un système d'information) Consiste à modifier sa configuration initiale pour renforcer la sécurité du système. Exemples : désactiver des services inutiles, activer des fonctions de sécurité, modifier des mots de passe par défaut, etc.. 17, 68, 69

Déchiffrement vérifiable Déchiffrement permettant de vérifier que la donnée déchiffrée correspond à la donnée en clair contenue dans la donnée chiffrée. 33, 55, 79–81, 84, 90, 92, 95

Décompte Opération incluse dans le dépouillement, intervenant après le déchiffrement, au cours de laquelle les suffrages exprimés sont décomptés ou totalisés afin de produire le résultat de l'élection. 48, 54–56, 78

Dépouillement Opération intervenant après la clôture du scrutin, incluant l'accumulation ou le mélange des bulletins, le déchiffrement et le décompte, au cours de laquelle la clé privée de l'élection est utilisée pour déchiffrer les bulletins et obtenir le résultat de l'élection. 4, 6, 31, 42, 48, 53, 54, 64, 81, 117, 121

Dérivation Mécanisme cryptographique permettant de calculer une ou plusieurs clés à partir d'un secret maître. 15

EBIOS-RM (Expression des Besoins et Identification des Objectifs de Sécurité Risk Manager) Méthode d'analyse de risque française de référence, permet aux organisations de réaliser une appréciation et un traitement des risques [17]. 77

eIDAS electronic Identification, Authentication and Trust Services [21]. 22

Élection Choix exprimé au travers d'un vote. 3

ElGamal Mécanisme de chiffrement asymétrique, basé sur le groupe multiplicatif d'un corps fini ou basé sur le groupe des points rationnels d'une courbe elliptique, dont la sécurité repose sur la difficulté de résolution du problème du logarithme discret [54]. 32–34, 38, 43, 46, 93, 94, 96, 107, 116, 117

Éligibilité (des candidats) Aptitude à être élu(e). 4

Émargement Dans le cas du vote à l'urne, signature par l'électeur d'un fichier appelé liste d'émargement après le dépôt de son bulletin dans l'urne, attestant de ce dépôt. Dans le cas du vote par correspondance électronique, mise à jour par le serveur de vote d'un fichier appelé liste d'émargement. 4, 5, 53

Empreinte numérique Donnée calculée au moyen d'une fonction de hachage cryptographique. 50–52, 60, 71

Entropie Mesure de la quantité d'aléa contenu dans un système, une application ou une information. 23

Etanchéité Stricte séparation entre deux informations qui implique l'impossibilité ou la difficulté à les rapprocher. 7, 9, 13, 19, 32, 34, 37, 41–43, 78, 79, 95, 114–116, 121, 125, 126

Everlasting privacy Propriété signifiant que le secret du scrutin est garanti de manière inconditionnelle, y compris en particulier vis-à-vis d'une attaque du type « store now, decrypt later » menée au moyen d'un ordinateur quantique [59]. 93, 107

Expert indépendant Personne ou entité réalisant pour le compte de l'organisateur du scrutin le contrôle de la conformité de la solution de vote à la délibération de la CNIL [72]. 14, 46, 48, 50, 51, 74, 77

Fonction de hachage Mécanisme cryptographique calculant une donnée unique de petite taille à partir de toute donnée, fournissant les propriétés de résistance aux collisions. 60

HTTP Hyper Text Transfer Protocol. 122

IND-CPA INDistinguishability under Chosen Plaintext Attack [24]. 94

Indépendance logicielle Principe selon lequel une modification ou une erreur non détectée du logiciel du système de vote ne doit pas causer une modification ou une erreur non détectée dans le résultat. En d'autres termes, il doit être possible de vérifier la sincérité du résultat sans reposer sur l'hypothèse que le système de vote est de confiance. C'est l'objet de la vérifiabilité individuelle et universelle. Ce principe est expliqué dans le Chapitre 1 *Software Independence Revisited* du livre *Real-World Electronic Voting : Design, Analysis and Deployment* [61]. 8, 51, 56, 65, 71, 93

INSEE Institut national de la statistique et des études économiques. 1

Intégrité des suffrages exprimés Un des principes fondamentaux qui commandent les opérations électorales, qui exprime que le choix d'un électeur ne doit pas pouvoir être modifié entre son émission et sa prise en compte au moment du décompte des suffrages [72]. 6, 31, 39, 50, 51, 53, 60, 64, 65, 68, 69, 71, 74, 75, 78, 79, 82, 86, 93–95, 107, 117

Journalisation Collecte des journaux d'évènements [14]. 8, 51, 52, 68, 69

Kerckhoffs (principe de) Principe selon lequel la sécurité d'un mécanisme ou d'un protocole cryptographique est assurée face un attaquant disposant de ses spécifications [64]. 8, 75

Latéralisation Accès à d'autres systèmes depuis un système compromis. 67

Liste d'émargement Liste des électeurs ayant participé à un vote. 4, 18, 50, 51, 60, 61, 63, 64, 69, 88, 120

Liste électorale Liste des électeurs pouvant participer à un vote. 4, 5

Malléabilité (du chiffrement) Propriété d'un mécanisme de chiffrement permettant d'effectuer des opérations sur les données chiffrées pour obtenir le chiffrement d'autres données que celles initialement chiffrées. 43, 94, 117

Matériel de vote Dans le cas du vote à l'urne, désigne les bulletins, les enveloppes, les isoloirs et l'urne physique utilisés par les électeurs ; dans le cas du vote par correspondance électronique, désigne la configuration de l'élection, l'urne électronique, la liste d'émargement ainsi que l'ensemble des traces générées par le système de vote. 4, 54

MDM (Mobile Device Management) Service de gestion des terminaux mobiles. 25

Modèle de confiance Description des hypothèses sur lesquelles s'appuie la sécurité d'un système de vote. 11, 13, 37, 57, 66, 74, 76

Moyen d'authentification Élément qui est généralement connu ou possédé uniquement par l'utilisateur et qui permet de l'authentifier de manière unique (comme un mot de passe, une clé privée d'un certificat électronique, etc.). Il s'agit d'une preuve utilisée pour démontrer son identité [22]. 4

Mélange cryptographique Mécanisme cryptographique assurant l'étanchéité dntre le bulletin et le suffrage. 15, 33, 42, 43, 53, 55, 79, 115, 116, 121

Mélange vérifiable Mélange cryptographique permettant de vérifier qu'un mélange d'un ensemble de bulletins correspond au même ensemble de suffrages. 33, 79–81, 84, 92, 115, 117

NM-CPA Non-Malleability under Chosen Plaintext Attack [24, 53]. 95

Offuscation (ou obscurcissement ou *obfuscation*, en anglais, du code source) Technique visant à rendre difficile l'interprétation d'un programme, par exemple pour protéger la propriété intellectuelle (secret industriel) associée. 86

Opération de vote Ensemble des traitements permettant à un électeur de déposer un bulletin dans l'urne électronique. 18, 39, 41, 53, 64, 72, 88

Organisateur du scrutin Entité responsable de l'organisation et de la conformité du scrutin. La délibération de la CNIL [72] fait référence aux organisateurs de scrutin en tant que responsables de traitement [40]. 3, 46, 66, 88

OTP (One Time Password) Code à usage unique utilisé pour une authentification. Il peut être envoyé à la demande à l'utilisateur, ou généré à intervalle régulier par un équipement ou une application spécifique. 20

OWASP Fondation à but non lucratif dédiée à la sécurité des applications Web. 68

Partage vérifiable Partage de secret permettant de vérifier que chaque attributaire ne dispose que d'un fragment du secret. 80

Pastillage Extraction d'informations complémentaires à un scrutin, soit pour constituer d'autres instances sur un périmètre inférieur, soit à des fins statistiques. 15, 18, 33, 43, 48, 51, 119

PIN (Personal Identification Number) Code numérique comportant au moins 4 chiffres, destiné à authentifier l'attributaire d'un fragment de clé stocké sur carte à puce. 46

Preuve de vote Information anonyme et non horodatée contenant une référence cryptographiquement liée au bulletin de vote. La preuve de vote permet à l'électeur de vérifier la présence de son bulletin dans l'urne. La preuve de vote est distincte du récépissé de vote. 52, 61, 64, 71, 72, 80, 118

Preuve à divulgation nulle de connaissance Mécanisme cryptographique permettant de prouver qu'une proposition est vraie sans révéler d'autre information que la véracité de la proposition [25, 51, 55, 74]. 18, 32–34, 43, 64, 71, 74, 79, 80, 88–91, 95, 96, 99, 101, 103, 105, 107, 116, 117, 121

Protocole de vote Modélisation théorique des opérations réalisées par un électeur et une entité (serveur de vote) qui réceptionne et traite l'ensemble des bulletins des électeurs. 8, 18, 74, 118

Période de vote Période pendant laquelle les électeurs peuvent voter. 3, 59, 63, 83

RAM (Random Access Memory) Composant d'un ordinateur stockant les données de manière temporaire pour un accès plus rapide. 59

Receipt-freeness Propriété d'un système de vote qui signifie que les données publiées par le système de vote ne portent pas atteinte au secret du scrutin [28]. 19, 43, 93, 118

Récépissé de vote Information transmise aux électeurs à la fin de l'opération de vote, contenant l'heure de dépôt du bulletin dans l'urne électronique. Le récépissé de vote est distinct de la preuve de vote. 18, 71, 118

Recorded-as-cast Propriété faisant partie de la vérifiabilité individuelle qui signifie que le bulletin est *enregistré* dans l'urne électronique tel qu'*émis* par l'électeur. 51, 56, 65, 71

Recouvrement (de secret d'authentification) Renouvellement par un électeur d'un secret d'authentification perdu ou compromis. De façon annexe, désigne aussi le masquage d'un secret par un dispositif physique opaque lorsque ce secret est imprimé pour sa transmission par courrier postal. 15, 26, 27, 52

Redondance Duplication de composants techniques pour en assurer la disponibilité en palliant d'éventuelles pannes. 59, 83

Revote Faculté de pouvoir voter plus d'une fois à un même scrutin. Cette fonctionnalité implique de devoir traiter les différents bulletins remis par un même électeur. 9

Réplication Copie et stockage de données sur un système primaire et un système secondaire. La réplication peut être synchrone ou asynchrone. 38, 59, 83

Scellement Apposition d'un cachet ou d'une empreinte numérique garantissant l'intégrité d'un contenu numérique et permettant de contrôler l'intégrité d'un contenu numérique en détectant toute modification ultérieure de ce contenu. 46, 48, 52, 53, 60, 61, 63, 64

Scrutin Ensemble des opérations constituant un vote. 3, 66

Secret d'authentification Secret partagé entre l'électeur et le système de vote, permettant au système de vote de vérifier l'identité et la légitimité de l'électeur. 6, 15, 20, 52

Secret du scrutin Un des principes fondamentaux qui commandent les opérations électorales, qui exprime que aucun lien ne doit pouvoir être établi entre un votant et l'expression de son vote (c'est-à-dire le contenu de son bulletin), afin de garantir, d'une part, la confidentialité du choix réalisé par le votant, et d'autre part, l'anonymat du vote, afin de limiter le risque d'intimidation, de manipulation ou de corruption des votants [72]. 6, 7, 12, 29, 31, 33, 34, 41, 42, 45, 48, 53, 55, 56, 64, 68, 69, 71, 75, 76, 78, 84, 88, 89, 91, 93–95, 107, 115, 118–121

Serveur de vote Partie centralisée du système de vote. Elle est au moins en partie exposée sur Internet pour recueillir les votes des électeurs. 7, 12, 18, 35, 39, 41, 72, 74, 80, 86, 88, 89

Signature numérique Mécanisme cryptographique permettant de détecter la modification d'une donnée et d'assurer son authenticité. 15, 18, 39, 52, 61, 62, 64, 72, 74, 81, 88, 89

Sincérité des opérations électorales Un des principes fondamentaux qui commandent les opérations électorales, qui exprime que le vote ne doit être accessible qu'aux électeurs inscrits sur les listes électorales, et le résultat des opérations de vote doit représenter la volonté exprimée des votants [72]. 5, 6, 8, 12, 14, 20, 23, 25, 31, 37, 50–53, 57, 58, 60, 64, 65, 68, 69, 71, 73–76, 78, 79, 82, 83, 86, 88, 93, 95, 107, 117, 119, 120

SMS Short Message Service. 23, 25, 26, 58, 68

Solution de vote Comprend le système de vote ainsi que ses procédures d'exploitation et de sécurisation. 5, 14, 42, 48, 77

SQL Structured Query Language. 19

SSO Single Sign On. 21

Suffrage Expression du vote de l'électeur, c'est-à-dire le choix de cet électeur parmi les options de vote (candidat(s), liste(s), réponse à une question, etc.). Le suffrage chiffré est contenu dans le bulletin. 3, 5, 18, 29, 37, 41, 48, 54, 71, 93, 94, 119

Surveillance effective du vote Un des principes fondamentaux qui commandent les opérations électorales, qui exprime que l'organisation et le déroulement des opérations électorales doivent faire l'objet d'un contrôle régulier, indépendant et objectif [72]. 6, 57, 60, 63, 64, 71, 74, 78, 82, 86

Système de vote Ensemble des moyens physiques (matériels) et logiques (logiciels) utilisés pour le vote électronique. 14, 50, 51, 63–66, 83, 84, 90, 118

Tallied As Recorded Propriété faisant partie de vérifiabilité universelle qui signifie que tout le monde doit pouvoir vérifier que le résultat proclamé (décompte ou *tally* en anglais) correspond aux suffrages contenus dans les bulletins de l'urne. 51, 56, 65, 72, 78

Tiers (vérificateur) Personne ou entité qui contribue à une mission de vérification de la sincérité d'un scrutin. Cette mission peut inclure en particulier un service de vérification de la présence d'un bulletin dans l'urne (2-07), et un service de vérification des preuves de bon déchiffrement de l'urne (3-02). Idéalement, le tiers vérificateur est indépendant de l'organisateur du scrutin et du prestataire fournissant le système de vote. 61, 74, 79, 81, 82, 86, 91, 115, 119

TLS (Transport Layer Security) Protocole cryptographique assurant la confidentialité et l'intégrité des données, l'authentification des participants et la protection contre le rejeu [8]. 15–17, 31, 35, 36, 68

Urne électronique Dispositif technique (c.-à-d. base de données, fichier, etc.) assurant le stockage des bulletins. 6, 18, 35, 44, 47, 48, 50, 51, 53–55, 60, 61, 63, 64, 69, 80, 81, 88, 115, 116, 120

Vérifiabilité de la légitimité Propriété faisant partie de vérifiabilité universelle qui signifie que tout le monde doit pouvoir vérifier que les bulletins proviennent d'électeurs légitimes. 8, 78, 88

Vérifiabilité individuelle Propriété d'un système de vote signifiant que tout électeur est en mesure de vérifier que son suffrage a été enregistré en respectant l'intention de l'électeur (tel que voulu). Cette propriété se décompose en deux propriétés : « cast-as-intended » et « recorded-as-cast ». 7, 65, 71, 80, 81, 86, 93, 118

Vérifiabilité universelle Propriété d'un système de vote signifiant que tout de monde doit pouvoir constater que le résultat proclamé (le nombre de voix pour chaque option) correspond au contenu de l'urne. Cette propriété se décompose en deux propriétés : « tallied-as-recorded » et « vérifiabilité de la légitimité ». 8, 65, 78, 81, 88, 93

Bibliographie

[1] Ben Adida.
Helios : Web-based Open-Audit Voting.
In Paul C. van Oorschot, editor, *USENIX Security 2008 : 17th USENIX Security Symposium*, pages 335–348, San Jose, CA, USA, juillet 28 – août 1, 2008. USENIX Association.

[2] ANSSI.
CyberDico.
https://cyber.gouv.fr/cyberdico/.

[3] ANSSI.
Les moyens d'identification électronique et leur certification.
https://cyber.gouv.fr/reglementation/reglementation-identite-confiance-numerique/securite-echanges-voie-electronique/services-introduits-par-republique-numérique/les-moyens-didentification-electronique-et-leur-certification/.

[4] ANSSI.
Prestataires de vérification d'identité à distance (PVID).
https://cyber.gouv.fr/prestataires-de-verification-didentite-distance-pvid.

[5] ANSSI.
Produits et services qualifiés.
https://cyber.gouv.fr/produits-services-qualifies.

[6] ANSSI.
Recommandations pour l'hébergement dans le Cloud des systèmes d'information sensibles.
https://cyber.gouv.fr/publications/recommandations-pour-lhebergement-des-si-sensibles-dans-le-cloud.

[7] *Recommandations de sécurité relatives à un système GNU/Linux*.
Guide ANSSI-BP-028 v2.0, ANSSI, octobre 2022.
https://cyber.gouv.fr/guide-linux.

[8] *Recommandations de sécurité relatives à TLS*.
Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020.
https://cyber.gouv.fr/guide-tls.

[9] *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection*.
Guide ANSSI-PA-072 v2.0, ANSSI, mars 2020.
https://cyber.gouv.fr/guide-controle-acces-videoprotection.

[10] *Guide de sélection d'algorithmes cryptographiques*.
Guide ANSSI-PA-079 v1.0, ANSSI, mars 2021.
https://cyber.gouv.fr/publications/mecanismes-cryptographiques.

[11] *Recommandations pour la mise en œuvre d'un site Web : maîtriser les standards de sécurité côté navigateur*.

Guide ANSSI-PA-009 v2.1, ANSSI, avril 2021.
https://cyber.gouv.fr/guide-sites-web.

[12] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.
https://cyber.gouv.fr/guide-admin-si.

[13] *Avis scientifique et technique de l'ANSSI sur la migration vers la cryptographie post-quantique*.
Avis scientifique et technique ANSSI-PA-093 v1.0, ANSSI, avril 2022.
https://cyber.gouv.fr/publications/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique.

[14] *Recommandations de sécurité pour l'architecture d'un système de journalisation*.
Guide DAT-PA-012 v2.0, ANSSI, janvier 2022.
https://cyber.gouv.fr/guide-journalisation.

[15] *Avis de l'ANSSI sur la migration vers la cryptographie post-quantique (suivi 2023)*.
Avis scientifique et technique ANSSI-PA-098 v1.0, ANSSI, décembre 2023.
https://cyber.gouv.fr/publications/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique-0.

[16] *Dénis de service distribués (DDoS)*.
Essentiels Version 2.0, ANSSI, avril 2024.
https://cyber.gouv.fr/publications/denis-de-service-distribues-ddos.

[17] *La méthode EBIOS Risk Manager - Le Guide*.
Guide ANSSI-PA-048 v1.5, ANSSI, mars 2024.
https://cyber.gouv.fr/ebios-rm.

[18] *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*.
Guide ANSSI-PG-083 v3.0, ANSSI, mars 2026.
https://cyber.gouv.fr/publications/mecanismes-cryptographiques.

[19] *Référentiel général de sécurité (RGS)*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://cyber.gouv.fr/rgs.

[20] *Prestataires d'audit de la sécurité des systèmes d'information. Référentiel d'exigences*.
Référentiel Version 2.1, ANSSI, octobre 2015.
https://cyber.gouv.fr/referentiels-dexigences-pour-la-qualification.

[21] *Le règlement eIDAS - liste nationale de confiance*.
Référentiel Version 1.0, ANSSI, juillet 2016.
https://cyber.gouv.fr/eidas.

[22] *Authentification multifacteurs et mots de passe*.
Guide ANSSI-PG-078 v1.0, ANSSI, octobre 2021.
https://cyber.gouv.fr/guide-authentification.

[23] Mihir Bellare, Ran Canetti, and Hugo Krawczyk.
Keying Hash Functions for Message Authentication.
In Neal Koblitz, editor, *Advances in Cryptology – CRYPTO'96*, volume 1109 of *Lecture Notes*

in Computer Science, pages 1–15, Santa Barbara, CA, USA, août 18–22, 1996. Springer Berlin Heidelberg, Germany.

[24] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway.
Relations Among Notions of Security for Public-Key Encryption Schemes.
In Hugo Krawczyk, editor, *Advances in Cryptology – CRYPTO'98*, volume 1462 of *Lecture Notes in Computer Science*, pages 26–45, Santa Barbara, CA, USA, août 23–27, 1998. Springer Berlin Heidelberg, Germany.

[25] Mihir Bellare and Phillip Rogaway.
Random Oracles are Practical : A Paradigm for Designing Efficient Protocols.
In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93 : 1st Conference on Computer and Communications Security*, pages 62–73, Fairfax, Virginia, USA, novembre 3–5, 1993. ACM Press.

[26] Josh Benaloh.
Simple Verifiable Elections.
In *2006 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 06)*, Vancouver, B.C., août 2006. USENIX Association.

[27] Josh Benaloh, Michael Naehrig, Olivier Pereira, and Dan S. Wallach.
ElectionGuard : a Cryptographic Toolkit to Enable Verifiable Elections.
In Davide Balzarotti and Wenyuan Xu, editors, *33rd USENIX Security Symposium, USENIX Security 2024, Philadelphia, PA, USA, August 14-16, 2024*. USENIX Association, 2024.

[28] Josh Cohen Benaloh and Dwight Tuinstra.
Receipt-free secret-ballot elections (extended abstract).
In *26th Annual ACM Symposium on Theory of Computing*, pages 544–553, Montréal, Québec, Canada, mai 23–25, 1994. ACM Press.

[29] David Bernhard, Olivier Pereira, and Bogdan Warinschi.
How Not to Prove Yourself : Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios.
In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology – ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 626–643, Beijing, China, décembre 2–6, 2012. Springer Berlin Heidelberg, Germany.

[30] Philippe Bulens, Damien Giry, and Olivier Pereira.
Running Mixnet-Based Elections with Helios.
In *2011 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 11)*, San Francisco, CA, août 2011. USENIX Association.

[31] Bundesamt für Sicherheit in der Informationstechnik.
A Study of Mechanisms for End-to-End Verifiable Online Voting.
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Cryptography/End-to-End-Verifiable_Online-Voting.html.

[32] Center For Internet Security.
Center For Internet Security Benchmarks.
https://www.cisecurity.org/cis-benchmarks-overview.

[33] CERT-FR.
Fiche réflexe du CERT-FR. Déni de service réseau - Endiguement.
https://www.cert.ssi.gouv.fr/fiche/CERTFR-2024-RFX-010/.

[34] CERT-FR.
Fiche réflexe du CERT-FR. Déni de service réseau - Qualification.
https://www.cert.ssi.gouv.fr/fiche/CERTFR-2024-RFX-009/.

[35] David L. Chaum.
Untraceable electronic mail, return addresses, and digital pseudonyms.
Commun. ACM, 24(2) :84–90, février 1981.

[36] Michael R. Clarkson, Stephen Chong, and Andrew C. Myers.
Civitas : Toward a Secure Voting System.
In *2008 IEEE Symposium on Security and Privacy*, pages 354–368, Oakland, CA, USA, mai 18–21, 2008. IEEE Computer Society Press.

[37] CNIL.
Élections professionnelles et données personnelles : questions–réponses.
https://www.cnil.fr/fr/elections-professionnelles-et-donnees-personnelles-questions-reponses.

[38] CNIL.
Interface de programmation d'application (API).
https://www.cnil.fr/fr/definition/interface-de-programmation-dapplication-api.

[39] CNIL.
La CNIL publie son premier dossier thématique dédié à l'identité numérique.
https://www.cnil.fr/fr/la-cnil-publie-son-premier-dossier-thematique-dedie-lidentite-numerique.

[40] CNIL.
Responsable de traitement.
https://www.cnil.fr/fr/definition/responsable-de-traitement.

[41] CNIL.
Sécurité des systèmes de vote par internet : la CNIL actualise sa recommandation de 2010.
https://www.cnil.fr/fr/securite-des-systemes-de-vote-par-internet-la-cnil-actualise-sa-recommandation-de-2010.

[42] Véronique Cortier, Alexandre Debant, Anselme Goetschmann, and Lucca Hirschi.
Election Eligibility with OpenID : Turning Authentication into Transferable Proof of Eligibility.
In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 3783–3800, Philadelphia, PA, août 2024. USENIX Association.

[43] Véronique Cortier, Alexandre Debant, Ralf Küsters, Florian Moser, Johannes Müller, and Melanie Volkamer.
On a Study of Mechanisms for End-to-End Verifiable Online Voting (StuVe).
In *EVote-ID 2025 - 10th International Joint Conference on Electronic Voting*, Nancy, France, 2025. Springer.

[44] Véronique Cortier, David Galindo, Stéphane Glondu, and Malika Izabachene.
Distributed ElGamal à la Pedersen - Application to Helios.
In *Workshop on Privacy in the Electronic Society (WPES 2013)*, Berlin, Germany, 2013.

[45] Véronique Cortier, Pierrick Gaudry, and Stéphane Glondu.
Belenios : A Simple Private and Verifiable Electronic Voting System.
In Joshua D. Guttman, Carl E. Landwehr, José Meseguer, and Dusko Pavlovic, editors, *Foundations of Security, Protocols, and Equational Reasoning : Essays Dedicated to Catherine A. Meadows*, pages 214–238, Cham, 2019. Springer International Publishing.

[46] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers.
A Secure and Optimally Efficient Multi-Authority Election Scheme.
In Walter Fumy, editor, *Advances in Cryptology – EUROCRYPT'97*, volume 1233 of *Lecture Notes in Computer Science*, pages 103–118, Konstanz, Germany, mai 11–15, 1997. Springer Berlin Heidelberg, Germany.

[47] Chris Culnane and Vanessa Teague.
Strategies for Voter-Initiated Election Audits.
In Quanyan Zhu, Tansu Alpcan, Emmanouil Panaousis, Milind Tambe, and William Casey, editors, *Decision and Game Theory for Security*, pages 235–247, Cham, 2016. Springer International Publishing.

[48] CVE.
CVE Program Mission.
https://www.cve.org/.

[49] Olivier de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater.
Electing a University President Using Open-Audit Voting : Analysis of Real-World Use of Helios.
In *2009 Electronic Voting Technology Workshop/ Workshop on Trustworthy Elections (EVT/WOTE 09)*, Montreal, Quebec, août 2009. USENIX Association.

[50] Alexandre Debant and Lucca Hirschi.
Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol.
In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 6737–6752, Anaheim, CA, août 2023. USENIX Association.

[51] Henri Devillez, Olivier Pereira, and Thomas Peters.
How to Verifiably Encrypt Many Bits for an Election ?
In Vijayalakshmi Atluri, Roberto Di Pietro, Christian Damsgaard Jensen, and Weizhi Meng, editors, *ESORICS 2022 : 27th European Symposium on Research in Computer Security, Part II*, volume 13555 of *Lecture Notes in Computer Science*, pages 653–671, Copenhagen, Denmark, septembre 26–30, 2022. Springer, Cham, Switzerland.

[52] Direction générale des Finances publiques.
Espace Numérique Sécurisé des Agents Publics (ENSAP).
https://ensap.gouv.fr/.

[53] Danny Dolev, Cynthia Dwork, and Moni Naor.
Non-Malleable Cryptography (Extended Abstract).
In *23rd Annual ACM Symposium on Theory of Computing*, pages 542–552, New Orleans, LA, USA, mai 6–8, 1991. ACM Press.

[54] Taher ElGamal.
A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.
In G. R. Blakley and David Chaum, editors, *Advances in Cryptology – CRYPTO'84*, volume 196

of *Lecture Notes in Computer Science*, pages 10–18, Santa Barbara, CA, USA, août 19–23, 1984. Springer Berlin Heidelberg, Germany.

[55] Amos Fiat and Adi Shamir.
How to Prove Yourself : Practical Solutions to Identification and Signature Problems.
In Andrew M. Odlyzko, editor, *Advances in Cryptology – CRYPTO'86*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194, Santa Barbara, CA, USA, août 1987. Springer Berlin Heidelberg, Germany.

[56] FIRST.
Common Vulnerability Scoring System SIG.
https://www.first.org/cvss/.

[57] Rolf Haenni, Reto E. Koenig, Philipp Locher, and Eric Dubuis.
CHVote System Specification.
Cryptology ePrint Archive, Report 2017/325, 2017.

[58] Rolf Haenni, Philipp Locher, Reto E. Koenig, and Eric Dubuis.
Pseudo-Code Algorithms for Verifiable Re-encryption Mix-Nets.
In Michael Brenner, Kurt Rohloff, Joseph Bonneau, Andrew Miller, Peter Y. A. Ryan, Vanessa Teague, Andrea Bracciali, Massimiliano Sala, Federico Pintore, and Markus Jakobsson, editors, *FC 2017 Workshops*, volume 10323 of *Lecture Notes in Computer Science*, pages 370–384, Sliema, Malta, avril 7, 2017. Springer, Cham, Switzerland.

[59] Thomas Haines, Rafieh Mosaheb, Johannes Müller, and Ivan Pryvalov.
SoK : Secure E-Voting with Everlasting Privacy.
Proceedings on Privacy Enhancing Technologies, 2023(1) :279–293, janvier 2023.

[60] Thomas Haines and Johannes Müller.
SoK : Techniques for Verifiable Mix Nets.
In Limin Jia and Ralf Küsters, editors, *CSF 2020 : IEEE 33rd Computer Security Foundations Symposium*, pages 49–64, Boston, MA, USA, juin 22–26, 2020. IEEE Computer Society Press.

[61] Feng Hao and Peter Y. A. Ryan.
Real-World Electronic Voting : Design, Analysis and Deployment.
Series in Security, Privacy and Trust. CRC Press, 2016.
https://realworldevoting.com/.

[62] Nicolas Huber, Ralf Küsters, Julian Liedtke, and Daniel Rausch.
ZK-SNARKs for Ballot Validity : A Feasibility Study.
In David Duenas-Cid, Peter Roenne, Melanie Volkamer, Jurlind Budurushi, Michelle Blom, Adrià Rodríguez-Pérez, Iuliia Spycher-Krivonosova, Jordi Castellà Roca, and Jordi Barrat Esteve, editors, *Electronic Voting*, pages 107–123, Cham, 2025. Springer Nature Switzerland.

[63] Wojciech Jamroga.
Pretty Good Strategies for Benaloh Challenge.
In Melanie Volkamer, David Duenas-Cid, Peter B. Rønne, Peter Y. A. Ryan, Jurlind Budurushi, Oksana Kulyk, Adrià Rodriguez Pérez, and Iuliia Spycher-Krivonosova, editors, *Electronic Voting : 8th International Joint Conference, E-Vote-ID 2023, Luxembourg City, Luxembourg, October 3-6, 2023, Proceedings*, volume 14230 of *Lecture Notes in Computer Science*, pages 106–122. Springer, 2023.

[64] Auguste Kerckhoffs.
La cryptographie militaire.
Journal des sciences militaires, IX :5–38, Feb 1883.

[65] Oksana Kulyk and Melanie Volkamer.
Usability is not Enough : Lessons Learned from 'Human Factors in Security' Research for Verifiability.
In *Third International Joint Conference on Electronic Voting (E-Vote-ID 2018)*. TUT Press, 2018.

[66] Ralf Küsters, Johannes Müller, Enrico Scapin, and Tomasz Truderung.
sElect : A Lightweight Verifiable Remote Voting System.
In Michael Hicks and Boris Köpf, editors, *CSF 2016 : IEEE 29th Computer Security Foundations Symposium*, pages 341–354, Lisbon, Portugal, juin 27–1, 2016. IEEE Computer Society Press.

[67] Chris Lamb and Stefano Zacchiroli.
Reproducible Builds : Increasing the Integrity of Software Supply Chains.
IEEE Software, 39(2) :62–70, mars 2022.

[68] Philipp Locher and Rolf Haenni.
Receipt-free remote electronic elections with everlasting privacy.
Annals of Telecommunications, 71(7–8), May 2016.

[69] Philipp Locher, Rolf Haenni, and Reto E. Koenig.
Coercion-Resistant Internet Voting with Everlasting Privacy.
In Jeremy Clark, Sarah Meiklejohn, Peter Y. A. Ryan, Dan S. Wallach, Michael Brenner, and Kurt Rohloff, editors, *FC 2016 Workshops*, volume 9604 of *Lecture Notes in Computer Science*, pages 161–175, Christ Church, Barbados, février 26, 2016. Springer Berlin Heidelberg, Germany.

[70] Légifrance.
Arrêté du 8 novembre 2018 relatif au téléservice dénommé «FranceConnect» créé par la direction interministérielle du numérique et du système d'information et de communication de l'État.
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037611479.

[71] Légifrance.
Décret n° 2024-1038 du 6 novembre 2024 relatif aux dispositions réglementaires des livres Ier et II du code général de la fonction publique.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000050510977.

[72] Légifrance.
Délibération n° 2026-045 du 19 mars 2026 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique et abrogeant les délibérations n° 2010-371 du 21 octobre 2010 et n° 2019-053 du 25 avril 2019.
https://www.legifrance.gouv.fr/.

[73] Karola Marky, Oksana Kulyk, Karen Renaud, and Melanie Volkamer.
What Did I Really Vote For ? On the Usability of Verifiable E-Voting Schemes.
In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–13, New York, NY, USA, 2018. Association for Computing Machinery.

[74] Ueli M. Maurer.
Unifying Zero-Knowledge Proofs of Knowledge.

In Bart Preneel, editor, *AFRICACRYPT 09 : 2nd International Conference on Cryptology in Africa*, volume 5580 of *Lecture Notes in Computer Science*, pages 272–286, Gammarth, Tunisia, juin 21–25, 2009. Springer Berlin Heidelberg, Germany.

[75] Ministère de l'Intérieur.
Machines à voter.
https://www.interieur.gouv.fr/Elections/Comment-voter/Machines-a-voter.

[76] Ministère du Travail, de la Santé, des Solidarités et des Familles.
L'élection de la délégation du personnel au CSE.
https://travail-emploi.gouv.fr/lelection-de-la-delegation-du-personnel-au-cse.

[77] Mozilla Developer Network (MDN).
Web technology for developers.
https://developer.mozilla.org/en-US/docs/Web.

[78] Johannes Müller.
Breaking and Fixing Vote Privacy of the Estonian E-Voting Protocol IVXV.
In Shin'ichiro Matsuo, Lewis Gudgeon, Ariah Klages-Mundt, Daniel Perez Hernandez, Sam Werner, Thomas Haines, Aleksander Essex, Andrea Bracciali, and Massimiliano Sala, editors, *FC 2022 Workshops*, volume 13412 of *Lecture Notes in Computer Science*, pages 325–334, Grenada, mai 6, 2022. Springer, Cham, Switzerland.

[79] National Institute of Standard and Technology.
National Checklist Program for IT Products.
https://ncp.nist.gov/repository.

[80] OWASP.
OWASP API Security Project.
https://owasp.org/www-project-api-security/.

[81] OWASP.
OWASP Cheat Sheet Series - Vulnerability Disclosure Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html.

[82] OWASP.
OWASP TOP 10.
https://owasp.org/Top10/.

[83] David Pointcheval.
Linearly-Homomorphic Signatures for Short Randomizable Proofs of Subset Membership.
In *Eighth International Joint Conference on Electronic Voting (E-Vote-ID '23)*, Luxembourg, Luxembourg, octobre 2023.

[84] David Pointcheval.
Efficient Universally-Verifiable Electronic Voting with Everlasting Privacy.
In Clemente Galdi and Duong Hieu Phan, editors, *SCN 24 : 14th International Conference on Security in Communication Networks, Part I*, volume 14973 of *Lecture Notes in Computer Science*, pages 323–344, Amalfi, Italy, septembre 11–13, 2024. Springer, Cham, Switzerland.

[85] Swiss Post.
Protocol of the Swiss Post Voting System - Computational Proof of Complete Verifiability and Privacy.
https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/master.

[86] Reproductible-Builds.
Reproducible builds are a set of software development practices that create an independently-verifiable path from source to binary code.
https://reproducible-builds.org.

[87] Peter B. Rønne, Peter Y. A. Ryan, and Ben Smyth.
Cast-as-Intended : A Formal Definition and Case Studies.
In Matthew Bernhard, Andrea Bracciali, Lewis Gudgeon, Thomas Haines, Ariah Klages-Mundt, Shin'ichiro Matsuo, Daniel Perez, Massimiliano Sala, and Sam Werner, editors, *FC 2021 Workshops*, volume 12676 of *Lecture Notes in Computer Science*, pages 251–262, Virtual Event, mars 1–5, 2021. Springer Berlin Heidelberg, Germany.

[88] Peter Y. A. Ryan, Peter B. Rønne, and Vincenzo Iovino.
Selene : Voting with Transparent Verifiability and Coercion-Mitigation.
In Jeremy Clark, Sarah Meiklejohn, Peter Y. A. Ryan, Dan S. Wallach, Michael Brenner, and Kurt Rohloff, editors, *FC 2016 Workshops*, volume 9604 of *Lecture Notes in Computer Science*, pages 176–192, Christ Church, Barbados, février 26, 2016. Springer Berlin Heidelberg, Germany.

[89] Adi Shamir.
How to Share a Secret.
Communications of the Association for Computing Machinery, 22(11) :612–613, novembre 1979.

[90] Daniel Shanks.
Class Number, a Theory of Factorization, and Genera.
In Donald J. Lewis, editor, *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 415–440. American Mathematical Society, Providence, RI, 1971.

[91] Björn Terelius and Douglas Wikström.
Proofs of Restricted Shuffles.
In Daniel J. Bernstein and Tanja Lange, editors, *AFRICACRYPT 10 : 3rd International Conference on Cryptology in Africa*, volume 6055 of *Lecture Notes in Computer Science*, pages 100–113, Stellenbosch, South Africa, mai 3–6, 2010. Springer Berlin Heidelberg, Germany.

[92] Tomasz Truderung.
POLYAS 3.0 Verifiable E-Voting System.
https://github.com/polyas-voting/core3-verifiable-doc/.

[93] Douglas Wikström.
Verificatum Mix-Net.
https://www.verificatum.org/.

[94] Douglas Wikström.
A Commitment-Consistent Proof of a Shuffle.

In Colin Boyd and Juan Manuel González Nieto, editors, *ACISP 09 : 14th Australasian Conference on Information Security and Privacy*, volume 5594 of *Lecture Notes in Computer Science*, pages 407–421, Brisbane, Australia, juillet 1–3, 2009. Springer Berlin Heidelberg, Germany.

Version 1.0 - 2026-04-24 - ANSSI-PA-118

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité