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

GUIDE ANSSI

PUBLIC VISÉ :

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

Table des matières

Informations

Attention

Ce document rédigé par l'ANSSI présente les **« Recommandations pour la mise en œuvre du vote par Internet pour les élections non politiques »**. Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab [78].
Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.
Sauf disposition réglementaire contraire, ces recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
0.1	2025	Version pour consultation publique

1
Introduction

Ce guide s'inscrit dans le cadre d'une collaboration avec la Commission Nationale Informatique et Libertés (CNIL) et la mise à jour en 2025 [77] de la recommandation relative à la sécurité des systèmes de vote par correspondance électronique, appelé aussi *vote par Internet*. Ce guide a été élaboré avec le soutien de chercheurs dans le domaine du vote par correspondance électronique.

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 : le ministère de l'Éducation nationale ainsi que le ministère du Travail [1] depuis 2010, la fonction publique d'État depuis 2011, la fonction publique territoriale depuis 2014 et la fonction publique hospitalière depuis 2017. 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 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 (REU) tenu par l'INSEE [21]. 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 [5], à savoir les votes des Français résidant à l'étranger pour les élections législatives et les élections des conseillers des français de l'étranger (qui représentent les Français de l'étranger auprès des ambassades et des consulats).

Attention

Le présent guide fournit des recommandations techniques pour la mise en œuvre du vote par correspondance électronique pour les **élections non politiques**.

L'objet de ce guide est d'approfondir la délibération 2025 de la CNIL [77], en formulant des recommandations techniques associées à chaque objectif de cette délibération. Ce guide remplace la page [37] du site Web de la CNIL qui, jusqu'en 2025, remplissait ce rôle.

1. Pour l'élection syndicale TPE [9].

2
À qui s'adresse ce guide ?

Ce guide s'adresse en premier lieu aux organisateurs de scrutin qui sont tenus de garantir sa sincérité et sa conformité vis-à-vis de la recommandation de la CNIL [77]. Cette recommandation fait référence aux organisateurs de scrutin en tant que responsables de traitement [32].

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, chacun à leur niveau, de garantir et/ou de fournir les moyens nécessaires permettant de démontrer que leurs produits et/ou leurs services sont sûrs et conformes à la recommandation de la CNIL.

Enfin, les tiers intervenant dans la vérification de la sincérité 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, chacun à leur niveau, 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 une prestation à un prestataire spécialisé dans le vote par correspondance électronique. 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 sincérité des scrutins. Ces annexes fournissent des détails techniques, notamment sur certains mécanismes cryptographiques permettant d'assurer la sincérité du scrutin.

3
Présentation et enjeux du vote par correspondance électronique

Une **élection**[2] 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 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 **sincérité** du scrutin. La Figure 1 présente les opérations permettant de décrire 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 listes de candidats
- 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 bulletins
- Réalisation du vote
- Dépôt du bulletin dans l'urne
- Émargement
- Contrôle de la liste d'émargement
- Contrôle de l'urne

Après la période de vote

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

FIGURE 1 – Opérations constituant la réalisation d'un scrutin

2. Les termes **en gras** renvoient au Glossaire.

Avant la période de vote

- L'organisateur du scrutin gère les listes électorales, les candidats (éligibilité, 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 tiers prestataires) 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 bulletins de vote leur sont présentés. 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 bulletins est bien présenté et doit permettre aux électeurs de choisir leur option de vote (comme un candidat), de déposer leur bulletin dans l'urne et d'émarger.
- L'électeur fait son choix, son bulletin est déposé dans l'urne et l'émargement est enregistré.
- Le **bureau de vote** contrôle l'urne et la liste d'émargement.

Après la période 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).
- Les différents acteurs impliqués (organisateur du scrutin, assesseurs, bureau de vote) dénombrent les émargements, dénombrent les bulletins, comparent le nombre d'émargements et le nombre de bulletins, dépouillent les bulletins, totalisent les suffrages et proclament les résultats.

3.2 Impacts de la numérisation

Le vote par correspondance *non électronique* signifie que le **matériel de vote** envoyé aux électeurs (bulletins, enveloppes) est physique et que l'électeur envoie son bulletin de vote par voie postale. Par analogie, le vote par correspondance *électronique* signifie que le matériel de vote est dématérialisé et que l'organisateur du scrutin met en place un téléservice pour que les électeurs puissent voter depuis un **dispositif de vote** connecté à Internet. Suivant les contextes, ce type de vote est appelé « élection 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).

3.2.1 Opérations numérisées par le vote par correspondance électronique

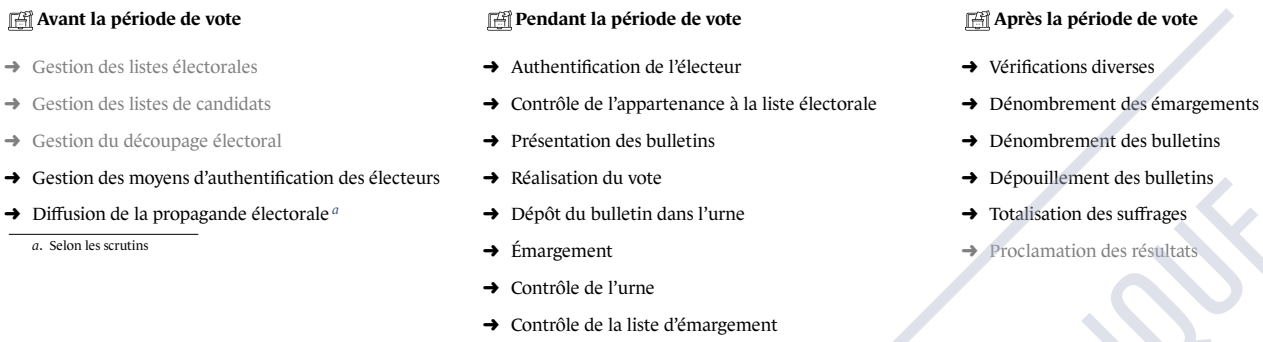

FIGURE 2 – Opérations numérisées par le vote par correspondance électronique

La figure 2 présente les opérations numérisées par le vote par correspondance électronique : le périmètre de la numérisation est important car il intègre des contrôles permettant d'assurer la sincérité du scrutin : 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

- La **solution de vote** est conçue et développée, en général 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 du 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 du prestataire.
- Un ou des **secrets d'authentification** sont transmis aux électeurs, soit par le prestataire, soit par l'organisateur du scrutin, soit par un tiers spécifiquement chargé de la gestion de l'authentification.

Pendant le vote

- À chaque fois qu'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 vote, 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. Elle peut également permettre aux électeurs ou à des tiers (observateurs, experts ou auditeurs) de vérifier certaines informations, comme la présence de bulletin 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 des bulletins, puis un décompte des suffrages, et affiche les résultats.
- La solution peut également permettre aux électeurs ou à des tiers (observateurs, experts ou auditeurs) de vérifier certaines informations permettant d'attester de la sincérité des résultats.

3.2.2 Enjeux de la numérisation des opérations

Dans sa recommandation de 2025 [77], 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 et 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.

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

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

Attention

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**[a] **obtient 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.

Secret du vote

Dans le cadre du vote par correspondance électronique, les bulletins de vote sont dématérialisés. Le secret du vote est assuré par des **mécanismes cryptographiques** : l'électeur peut par exemple utiliser un algorithme de chiffrement asymétrique et chiffrer son suffrage avec une clé publique unique, commune à tous les électeurs (appelée dans ce cas **clé publique de l'élection**), qui fait

a. Le client de vote est la partie logicielle du système de vote exécutée sur le dispositif de vote pour permettre à l'électeur d'exprimer son vote (voir le Glossaire).

partie de la **configuration de l'élection** et transmettre le bulletin chiffré à un **serveur de vote** lequel intègre ce bulletin numérisé dans une urne électronique. Le dépouillement s'effectue dans ce cas en déchiffrant les bulletins contenus dans l'urne (ou une somme de ces bulletins) grâce à la **clé privée de déchiffrement** correspondant à la clé publique de chiffrement.

Une particularité importante du vote par correspondance électronique est la numérisation conjointe de l'authentification de l'électeur et du traitement du bulletin. Lors d'un vote à l'urne, ces opérations sont réalisées par les membres du bureau de vote et indépendantes : contrôle d'une pièce d'identité et de l'inscription sur la liste électorale, ajout dans l'urne du bulletin anonyme et dans une 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 établisse un lien entre l'identité de l'électeur et son suffrage, créant un risque pour le secret du vote. De fait, la solution de vote doit garantir l'étanchéité entre l'identité de l'électeur et son suffrage.

Vérifiabilité individuelle et universelle

Lorsque le vote a lieu à l'urne dans un bureau de vote, la simplicité et la visibilité des dispositifs utilisés (isoloir, urne transparente, surveillance effective par le bureau de vote) favorisent la compréhension des opérations par les électeurs et la confiance dans le résultat. Elle permet aussi à tout électeur ou observateur d'assister au scrutin et d'en contrôler visuellement la bonne tenue. Proposer un équivalent à ces dispositifs 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 vote) sont bien plus complexes, difficiles à comprendre et donc à vérifier.

Afin de s'en approcher, des notions de vérifiabilité ont été proposées. D'une part, la **vérifiabilité individuelle** signifie que l'électeur peut contrôler que son bulletin a été compté, d'autre part, la **vérifiabilité universelle** signifie que tout le monde doit pouvoir constater que le résultat proclamé (le nombre de voix pour chaque candidat) 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.

Transparence

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

Surveillance

Pour tous les modes de scrutin, il est nécessaire de détecter et d'alerter de tout événement pouvant altérer la sincérité du scrutin. 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'évènements) et de la supervision du système de vote. Ce besoin est amplifié par la durée de la période de vote, souvent plusieurs jours, et aussi par la centralisation de l'infrastructure : une attaque sur le système de vote aura un impact sur une proportion élevée d'électeurs (contrairement à un incident dans un bureau de vote lors du vote à l'urne). Cette surveillance peut impliquer des acteurs techniques (administrateurs et exploitants) et non techniques (membres du bureau électoral).

Sécurité du dispositif de vote et de l'environnement de l'électeur

Une autre particularité importante du vote par correspondance électronique est l'impossibilité de garantir la sécurité du dispositif (ordinateur, mobile multifonction) que l'électeur utilise pour voter, ainsi que son environnement. Le dispositif 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 le dispositif de vote ou du dispositif de vote vers le serveur de vote, en particulier le client 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 cœrcition, 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 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 électeur/suffrage si des mécanismes cryptographiques appropriés ne sont pas utilisés.

Transition vers la cryptographie post-quantique

L'ANSSI a émis deux avis sur la transition vers la cryptographie post-quantique [53, 55]. Ces avis expriment des recommandations en termes d'algorithmes post-quantiques et de techniques d'hybridation. 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.

3.3 Délibérations de la CNIL

Il n'existe pas de labellisation de solutions de vote par correspondance électronique [3]. 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 délibérations successives [4]. La dernière version précise notamment les objectifs relatifs à la vérifiabilité et à la transparence.

3. Au contraire des machines à voter, qui font l'objet d'un agrément [24].
4. Délibérations publiées en 2003 [74], 2010 [75], 2019 [76] et en 2025 [77].

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 et reprise pour la version de 2025. Cette estimation 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.

À chaque niveau est associé une liste d'**objectifs** auxquels doit se conformer une solution de vote, déclinant les notions de secret du vote, d'authentification, de vérifiabilité, de transparence et de surveillance. L'objet du présent document est de proposer des recommandations pour atteindre les objectifs fixés par la délibération.

4
Recommandations en réponse aux objectifs de la délibération de la CNIL

Chaque section du présent chapitre est consacrée à un des trois niveaux de risques 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 associés au niveau.

Ensuite 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**.

Les recommandations sont cumulables par niveau, le guide présente également des pratiques limitées au niveau 1 ainsi que des pratiques compatibles avec les niveaux 1, 2 et 3. La présentation de ces pratiques a pour but de sensibiliser les acteurs concernés sur le fait que des choix de mise en œuvre ont un impact important sur la capacité d'une solution à répondre aux enjeux des scrutins de niveaux élevés.

Recommandations de niveau 1, 2 ou 3

La plupart des 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 :

R ★

Recommandation de niveau 1

Cette recommandation permet de répondre à un objectif de niveau 1 de la délibération de la CNIL **et doit être appliquée aux scrutins de niveaux 1, 2 et 3**.

R ★★

Recommandation de niveau 2

Cette recommandation permet de répondre à un objectif de niveau 2 de la délibération de la CNIL **et doit être appliquée aux scrutins de niveaux 2 et 3**.

R ★★ ★

Recommandation de niveau 3

Cette recommandation permet de répondre à un objectif de niveau 3 de la délibération de la CNIL **et doit être appliquée aux scrutins de niveau 3**.

De plus, pour certains objectifs de niveau 1 ou 2, des recommandations adaptées à ce niveau sont définies, mais également des recommandations adaptées à un niveau supérieur (2 ou 3). Cela per-

met de raffiner les recommandations d'un objectif de niveau 1 ou 2 lorsque cet objectif n'est pas décliné aux niveaux supérieurs mais qu'il convient de tenir compte de risques ou de menaces plus élevés.

Pratiques limitées au niveau 1 et pratiques compatibles avec les niveaux 1, 2 ou 3

Certaines pratiques, constatées dans les systèmes existants, devraient être limitées au niveau 1 et ne devraient pas être mises en œuvre pour des scrutins de niveau supérieur. Ce cas se présente en particulier dans le choix de mécanismes cryptographiques structurants (objectifs 1.04 à 1.11); certaines pratiques moins robustes sont acceptables pour des scrutins de niveau 1 mais pas au-delà. Ces pratiques sont présentées de la manière suivante :

Pratique limitée à un scrutin de niveau 1

Cette pratique a une portée limitée à un scrutin de niveau 1 car elle n'est pas adaptée aux risques et menaces plus élevés des niveaux supérieurs. Aussi **il est recommandé que l'organisateur du scrutin limite à un scrutin de niveau 1 l'usage d'un système de vote qui met en œuvre cette pratique et pas ses alternatives proposées pour les niveaux supérieurs**.

Inversement, en remplacement des pratiques limitées à des scrutins de niveau 1, il est possible de mettre en œuvre des pratiques qui sont bien compatibles avec tous les niveaux de scrutin. Ces pratiques sont présentées de la manière suivante :

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 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 au niveau 3

Enfin, des recommandations complémentaires au niveau 3 sont fournies. Elles proposent des mesures de sécurité allant au-delà de celles requises par les objectifs de niveau 3. Elles peuvent être retenues pour répondre à des risques identifiés par une analyse de risque (objectif 3.01). Elles permettent de renforcer la sincérité du scrutin en présence d'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).

Ces recommandations permettent de mieux protéger le 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 nécessitent 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

Cette recommandation propose une mesure de sécurité complémentaire à celles requises par les objectifs de niveau 3.

La liste récapitulative des recommandations est disponible en page 88.

4.1 Objectifs de sécurité de niveau 1

Définition de la CNIL [77] : **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 locale.*

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.

1-01	Mettre en œuvre une solution technique et organisationnelle de qualité ne présentant pas de faille majeure (faille publiée par l'éditeur et/ou rendue publique par des tiers) et respectant les bonnes pratiques de déploiement et d'utilisation du système de vote électronique retenu.
1-02	Définir le vote d'un électeur comme une opération atomique, c'est-à-dire comme comportant de manière indivisible le choix, la validation, 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 votant et l'expression de son vote (le contenu déchiffré de son bulletin de vote) pendant toute la durée du traitement.
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	Définir le dépouillement comme une opération atomique utilisable seulement sur l'ensemble des bulletins du scrutin et après sa fermeture.
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.

Tableau 1 – Objectifs de niveau 1

Attention

Bien que le système de vote, le prestataire et l'organisateur du scrutin eux-mêmes puissent porter atteinte à la sincérité du scrutin, ce risque de compromission interne est *accepté* comme résiduel.

Objectif n° 1-01

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

La sincérité du scrutin 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, le niveau de sécurité réel sera abaissé.

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

R1 ★

Respecter les procédures préconisées par le prestataire

L'organisateur du scrutin doit respecter les procédures préconisées par le prestataire, notamment pour le déploiement et la surveillance du système, la tenue des cérémonies ou la gestion des supports contenant des clés cryptographiques (1.08).

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 soit 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 spécifier 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 (Annexe B).
- La prise en compte de configuration d'élection complexe, par exemple dans le cas du vote avec rature (Annexe E).
- L'intégration de mécanismes cryptographiques post-quantiques.
- La vérification d'une signature externe (1.06).
- La production de statistiques spécifiques sur le déroulement du scrutin pour sa surveillance (2.03).
- La séparation en modules d'une application monolithique, en prévision de l'installation de ces modules sur des machines distinctes (3.07).

- La prise en compte de format spécifique de données pour la configuration de l'élection ou l'exportation des émargements et des résultats.

Les mécanismes cryptographiques constituent le cœur d'une solution de vote par correspondance électronique. Il est important de les choisir conformément à l'état de l'art.

R3 ⋆

Assurer la conformité des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le système de vote doivent être conformes aux *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* [49].

Les mécanismes cryptographiques mis en œuvre par le système de vote font notamment partie de la liste suivante :

- La génération et la dérivation des secrets d'authentification (1.03, 3.05)
- Le chiffrement et la signature des données transmises aux tiers 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 (1.04) des bulletins.
- Le chiffrement des bulletins, éventuellement vérifiable et distribué (1.09, 3.07).
- La signature et le chaînage des bulletins pour en détecter les modifications illégitimes (1.06).
- L'accumulation, le mélange vérifiable et le déchiffrement vérifiable (1.07, 1.11, 2.08, 3.02).
- La génération et la vérification des preuves à divulgation nulle de connaissance (1.07, 1.08, 1.09, 1.11), 2.08.
- La fragmentation, éventuellement distribuée, de la clé privée de déchiffrement et le chiffrement des fragments (1.08, 3.07).
- Le contrôle d'intégrité des données et les scellements (1.10).
- La génération de la preuve de vote et sa signature (2.07).
- Le protocole de vote (2.08).

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), les dispositifs d'envoi des moyens d'authentification aux électeurs, les équipements de sécurité, les logiciels d'infrastructure (serveurs Web, serveurs applicatifs), les composants logiciels tiers (librairies, 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 de déchiffrement.

R5 ★

Mettre 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 [39] 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 niveau supérieur ou égal à **medium**. De même, il est recommandé que tous les composants du système de vote exposés sur Internet ne contiennent aucune faille publique de niveau supérieur ou égal 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 devra 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 recommandation de la CNIL [77]), ou plus fréquemment.

R6 ★

Auditer la configuration du système de vote

Il est recommandé que le système de vote soit audité fréquemment, 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* [49].
- La conformité des mécanismes d'authentification des électeurs, en particulier les dispostifs de transfert des secrets à des tiers (1.03).
- La conformité des liaisons TLS (1.05).
- Le développement, le durcissement et l'administration du système de vote (2.06).

Il est recommandé que l'audit soit réalisé par un *Prestataire d'Audit de la Sécurité des Systèmes d'Information* (PASSI) [30, 57], qualifié pour les activités suivantes : audit d'architecture, audit de configuration, audit de code source, test d'intrusion, audit organisationnel et physique.

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 atomique, c'est-à-dire comme comportant de manière indivisible le choix, la validation, l'enregistrement du bulletin dans l'urne, l'émargement et la délivrance d'un récépissé.

Le terme **atomique** signifie qui ne peut être coupé, indivisible. Dans le contexte du vote, il implique qu'une fois que l'électeur a validé son choix, l'ensemble des opérations 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.

La transaction de vote est composée des opérations suivantes :

- L'expression, par l'électeur, de son vote (choix d'un candidat par exemple) et sa validation 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 du bulletin, telles que prévues dans le protocole de vote (1.04, 2.08).
- La transmission du bulletin par le client de vote au **serveur de vote** (1.05).
- La validation du bulletin par le serveur de vote, y compris la validation éventuelle des preuves associées au bulletin (1.06) et la vérification de son éventuelle signature.
- Le dépôt du bulletin dans l'urne, ou dans les urnes en cas de pastillage (1.04), et la mise à jour de la liste d'émargement par le serveur de vote.
- La délivrance d'un récépissé à l'électeur.

Les recommandations suivantes concernent la fiabilité des opérations de la transaction de vote.

R7 ★

Enchaîner les opérations de la transaction de vote sans discontinuité

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

L'échec d'une opération entraîne l'échec de toute la transaction et, a contrario, la réussite de la transaction n'est possible que de par le succès de chacune des opérations unitaires.

Les opérations les plus critiques de la transaction sont le dépôt du bulletin dans l'urne et l'émargement, qui doivent être réalisées de manière indissociable. Dans le contexte des bases de données et des transactions SQL [36], cela peut par exemple être réalisé par le protocole Two-Phase Commit [82].

R8 ★

Réaliser de manière indissociable l'émargement et le dépôt du bulletin dans l'urne

Le système de vote ne doit pas dissocier les opérations de dépôt du bulletin dans l'urne et d'émargement de l'électeur.

Enfin, comme explicitement demandé dans l'objectif 1.02, le système de vote doit délivrer un récépissé à l'électeur, qui peut être complété avec la **preuve de vote** (2.07).

R9 ★

Délivrer un récépissé à l'électeur

Le système de vote doit délivrer un récépissé à l'électeur à la fin de la transaction de vote. Le récépissé peut être transmis par messagerie électronique.

Le récépissé peut contenir l'identité de l'électeur, l'horodatage de son vote ainsi que le ou les scrutins auxquels l'électeur a participé.

Une propriété importante d'un système de vote par correspondance électronique est la propriété appelée **receipt-freeness** (R31★), également expliquée en Annexe C. Cette propriété ne signifie pas *sans reçu*, c'est à dire *sans récépissé*. Par ailleurs, cette propriété doit être vérifiée pour tous les niveaux de scrutin.

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 une opération constituant la transaction de vote, les objectifs 1.07 et 2.08 qui concerne l'étanchéité électeur/suffrage ainsi que l'objectif 2.07 qui concerne la preuve de vote.

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'authentification des électeurs consiste à s'assurer de l'identité des électeurs. Cette étape est critique pour la sincérité du scrutin, car elle garantit que seuls les électeurs **légitimes** peuvent effectivement voter. De plus, l'authentification peut contribuer à rendre 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 n'est pas envisageable 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* [58], 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**[5], une carte SIM d'un téléphone mobile comportant des données d'identification, une boite aux lettres postale. De même, un facteur inhérent est de nature biométrique.

Ainsi, ni une messagerie électronique ni une messagerie instantanée ne peuvent être considérés 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).

En revanche, il est possible de déployer un facteur de connaissance, qui est un **secret d'authentification** dont l'usage doit être *dédié* au scrutin.

R10 ★

Utiliser un secret d'authentification dédié au scrutin

Le système de vote doit utiliser un facteur de connaissance, tel qu'un mot de passe, dédié au scrutin, pour authentifier les électeurs. Ce facteur de connaissance dédié peut être complété par d'autres facteurs d'authentification.

Attention

La recommandation R10★ est applicable aux scrutins de niveau 1 **et aux scrutins de niveau 2**, mais doit être complétée pour les scrutins de niveau 3 : une déclinaison (au niveau 3) est proposée dans ce guide, via la recommandation R71★★★. Autrement dit, pour les scrutins de niveaux 1 et 2, l'utilisation d'un seul secret d'authentification dédié au scrutin est suffisante ; pour les scrutins de niveau 3, il est recommandé

5. Un OTP ou *one-time password* est un 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.

d'utiliser deux secrets d'authentification (dont toujours au moins un dédié au scrutin), transmis par deux canaux différents.

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 guides de l'ANSSI.

R11 ★

Assurer la conformité des mécanismes d'authentification des électeurs

Il est recommandé que le système de vote mette en œuvre des mécanismes d'authentification des électeurs conformes aux recommandations du guide *Authentification multifacteurs et mots de passe* [58]. Notamment :

- Les secrets d'authentification doivent être générés avec suffisamment d'**entropie**.
- 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. Des mécanismes de dérivation des secrets d'authentification sont par exemple fournis dans le *Guide de sélection d'algorithmes cryptographiques* [50].
- Le système de vote doit être protégé contre les attaques par recherche d'authentifiants (attaques par force brute, pulvérisation de mots de passe ou *password spraying*, bourrage d'authentifiants ou *credential stuffing*, etc.). Ce type de protection peut s'appuyer sur un délai d'attente incompressible et croissant après plusieurs présentations de mots de passe erronés et/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 tiers

La recommandation suivante concerne la transmission des secrets d'authentification à des tiers sous-traitants, qui vont traiter leur envoi aux électeurs (envoi postal, envoi par messagerie électronique, envoi par SMS ou envoi par messagerie instantanée). Il est nécessaire de protéger ces secrets contre la divulgation et la modification car ces attaques peuvent porter atteinte à la sincérité du scrutin, en permettant à des personnes non légitimes de voter. De nombreux tiers, en particulier ceux spécialisés dans l'envoi d'e-mail et de SMS, exposent des interfaces (API) qui peuvent être directement appelées par le système de vote.

R12 ★

Protéger la transmission des secrets d'authentification à des tiers

Lorsque le système de vote transmet des secrets d'authentification à des tiers sous-traitants pour leur envoi aux électeurs (postal, par messagerie électronique, par SMS ou par messagerie instantanée), cette transmission doit garantir leur confidentialité et leur intégrité.

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 un tiers et une fois les secrets envoyés, le sous-traitant doit supprimer toute copie de ces secrets.

Cette transmission peut être réalisée par échange de fichier ou en utilisant des API exposées par le tiers.

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

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

- Les fichiers doivent être chiffrés dès leur constitution et ne doivent être déchiffrables que par le tiers destinataire au moyen d'un algorithme de chiffrement conforme aux *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* [49].
- 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* [49].
- Les fichiers doivent être protégés avant leur transfert (la confidentialité et l'intégrité des fichiers ne doivent pas être assurées par le dispositif d'échange).

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

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

- Le sous-traitant doit suivre l'état de l'art et les bonnes pratiques pour le déploiement d'API, par exemple les recommandations du *OWASP API Security Project* [27].
- La transmission doit être protégée par TLS, conformément aux *Recommandations de sécurité relatives à TLS* [47].
- Le secret d'authentification (mot de passe ou jeton d'authentification) utilisé pour accéder aux API doit être dédié au scrutin.
- 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

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).

Par exemple, pour l'élection de représentants du personnel dans une entité qui fournit une adresse de messagerie professionnelle ainsi qu'un téléphone portable professionnel à ses employés, l'utilisation de cette messagerie, l'envoi de SMS sur le téléphone portable professionnel ou la remise de courrier en main propre favorisent l'accès aux secrets d'authentification par un administrateur

technique de la même entité que l'organisateur du scrutin. Cela implique donc un risque d'usurpation d'identité.

R13 ★

Privilégier des canaux d'envoi hors de portée de l'organisateur du scrutin

Il est recommandé que le système de vote utilise des canaux d'envoi des secrets d'authentification hors de portée de l'organisateur du scrutin.

Par exemple, pour l'élection de représentants du personnel dans une entité qui fournit une adresse de messagerie professionnelle ainsi qu'un téléphone professionnel à ses employés, le Tableau 2 fournit des canaux d'envoi acceptables :

- Courrier postal envoyé au domicile de l'électeur, dès lors que l'impression est externalisée.
- E-mail personnel ou SMS sur téléphone personnel, généralisable aux messageries instantanées. Ces canaux requièrent la collecte et l'utilisation de données personnelles (adresse e-mail, numéro de téléphone personnel). Il convient de justifier ces usages par rapport au Règlement général sur la protection des données (**RGPD**) [20] et de sécuriser ces données en conformité.

Ainsi, dans ce contexte, l'utilisation d'e-mail ou de SMS professionnels doit être complétée par un défi-réponse conforme au guide *Authentification multifacteurs et mots de passe* [58].

Canal d'envoi du secret d'authentification	**Utilisable comme canal d'envoi d'un unique secret d'authentification**
Courrier postal sur adresse personnelle	Oui
E-mail personnel	Oui
SMS personnel	Oui
E-mail professionnel	Non (compléter avec défi-réponse [58])
SMS professionnel	Non (compléter avec défi-réponse [58])
Imprimé remis en main propre	Non

TABLEAU 2 – Canaux d'envoi acceptables pour un unique secret d'authentification dans le contexte d'une entité fournissant une adresse de messagerie professionnelle ainsi qu'un téléphone professionnel à ses employés.

L'envoi par courrier postal doit assurer la confidentialité du secret d'authentification qui figure dans le courrier. A 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.

R14 ★

Assurer la confidentialité des secrets transmis par voie postale

En cas d'envoi par courrier postal d'un moyen d'authentification, le système de vote doit assurer 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 R14★ 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 imprimé de brouillage sur sa face intérieure.

Les deux premières technologies permettent en outre une détection de lecture du secret. Les deux dernières 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 dispositif 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.

R15 ★

Fournir un recouvrement de secret d'authentification ne dégradant pas la sécurité

Le système de vote doit mettre en place un recouvrement des secrets d'authentification qui ne dégrade pas le niveau de sécurité obtenu par 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 initiaux.

Dans certains cas, la réutilisation du canal d'origine 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 alors arbitrer entre une sécurité stricte et interdire la saisie d'une nouvelle adresse, limitant le

risque d'usurpation d'identité, et favoriser la participation en permettant 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.

R16 ★

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

Si l'organisateur du scrutin veut favoriser la participation en permettant la saisie d'une nouvelle adresse de messagerie ou d'un 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 appartient les électeurs, identité numérique [18], vérification d'identité à distance [29]) ou grâce à un défi-réponse conforme au guide *Authentification multifacteurs et mots de passe* [58].
- 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 une nouvelle adresse.
- Le système de vote électronique renouvelle le secret et l'envoie à la nouvelle adresse.

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 3.05 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.

Lorsque l'électeur saisit son **suffrage** sur le **client de vote**, ce dernier génère un **bulletin** contenant le suffrage chiffré. D'abord, le client de vote doit protéger le secret du suffrage. Ensuite, le client de vote peut également détecter le niveau de sécurité du dispositif de vote. Enfin, le chiffrement du suffrage doit s'appuyer sur des mécanismes cryptographiques adaptés aux besoins du vote par correspondance électronique.

Protection 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 suffrage est un enjeu majeur du système. 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 le dispositif de vote, le client de vote ne doit pas faire appel à des ressources tierces qui ne seraient pas maîtrisées, c'est à dire hébergées sur le serveur de vote et auditées par des tiers (par exemple soumise à l'expertise indépendante, au sens de la délibération de la CNIL [77]). Ainsi, le recours à un service de **CAPTCHA** d'un site Web tiers doit être proscrit.

La constitution du bulletin (le suffrage chiffré) implique l'usage d'aléa par le client de vote, dont la confidentialité doit être assurée au même niveau que 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.

R17 ★

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'algorithmes cryptographiques* [50]. En particulier, lorsque le client de vote fait appel à des librairies cryptographiques (par exemple du navigateur), les appels à ces librairies doivent être réalisés conformément aux préconisations des fournisseurs de ces librairies.
- 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 généré.

Le client de vote est communément un script JavaScript [17] intégré à la page Web présentée à l'électeur et exécuté par le navigateur du dispositif de vote. Dans ce contexte, les *Recommandations pour la mise en oeuvre d'un site Web : maîtriser les standards de sécurité côté navigateur* [51] 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.

La Section 3.2.2 souligne la nécessité d'estimer le risque de compromission du client de vote lorsque celui-ci est transmis par le serveur de vote, notamment en cas de mise en place d'analyse de flux HTTPS ou d'interception TLS [1, 44, 46]. Il est également important d'estimer le risque de compromission du suffrage ou de l'aléa utilisé pour réaliser le chiffrement du suffrage, par ce dispositif. Afin de réduire ce dernier risque, il est possible de mettre en œuvre une détection des caractéristiques techniques du dispositif de vote.

R18 ★

Détecter les caractérisques techniques du dispositif de vote

Lorsque le client de vote est un script JavaScript [17] intégré à la page Web présentée à l'électeur et exécuté par le navigateur du dispositif de vote, il est recommandé que le système de vote intégre des mécanismes de détection des caractéristiques techniques du dispositif de 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 incompatible car n'ayant pas le niveau de sécurité requis. 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 la sandbox afin de restreindre la modification ou la récupération illégitime de donnée.
- 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 permettant d'assurer une détection, basés sur la contruction d'heuristiques dédiées.

Information

Il est envisageable de considérer un client de vote de type « client lourd », installé sur le dispositif de vote de l'électeur.

Protection du suffrage par des mécanismes cryptographiques

Le mécanisme cryptographique permettant d'assurer 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).

Le chiffrement doit également être **probabiliste**. En effet, si le 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 vote car il serait possible d'identifier les électeurs ayant le même suffrage.

R19 ★

Protéger le suffrage par un mécanisme de chiffrement probabiliste

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

Dans ce cas, 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).

Pour le choix de l'algorithme, il est nécessaire de prendre en compte le parcours complet du suffrage depuis son expression par l'électeur jusqu'au dépouillement, ainsi que sa compatibilité avec des mécanismes permettant d'atteindre les niveaux supérieurs (2 et 3).

R20 ★

Utiliser un mécanisme de chiffrement renforçant la sincérité

Il est recommandé que le système de vote mette en œuvre un algorithme de chiffrement des suffrages adapté pour les mécanismes renforçant la sincérité du scrutin et la transparence :

- L'**accumulation** ou le **mélange vérifiable** des bulletins, qui permettent d'assurer l'étanchéité entre l'identité du votant et l'expression de son vote (1.07).
- Le **partage de secret à seuil vérifiable** appliqué à la clé privée de déchiffrement, permettant de renforcer le secret du vote (1.08).
- Le **déchiffrement vérifiable** des bulletins de vote, permettant de garantir la sincérité du résultat (1.11).
- De manière plus élargie, l'algorithme de chiffrement devrait être utilisé au sein d'un **protocole de vote** publié (objectif 2.08).

Actuellement les deux algorithmes les plus utilisés sont l'algorithme de chiffrement RSA [97], qui est nativement déterministe et l'algorithme de chiffrement ElGamal [73], qui est nativement probabiliste. Comme décrit dans [50], l'algorithme de chiffrement RSA peut être rendu probabiliste au moyen d'un mécanisme d'encapsulation tel que OAEP [62].

Pratique limitée à un scrutin de niveau 1

L'utilisation de l'algorithme de chiffrement RSA probabiliste pour le chiffrement du suffrage n'est pas adaptée pour l'accumulation des bulletins, l'implémentation d'un mélange vérifiable et efficace ou pour l'implémentation d'un déchiffrement vérifiable et efficace.

L'organisateur du scrutin peut donc envisager **uniquement le niveau 1** avec un système de vote basé sur l'algorithme RSA probabiliste pour le chiffrement du suffrage.

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

L'utilisation de l'algorithme de chiffrement ElGamal [73], basé sur le groupe multiplicatif d'un corps fini ou basé sur le groupe des points rationnels d'une courbe elliptique, pour le chiffrement du suffrage, est adaptée pour l'accumulation des bulletins, l'implémentation d'un mélange vérifiable et efficace, l'implémentation d'un déchiffrement vérifiable et efficace, ainsi qu'à un partage de secret à seuil vérifiable.

L'organisateur du scrutin peut donc envisager **les niveaux de scrutin 1, 2 et 3** avec un système de vote basé sur l'algorithme ElGamal pour le chiffrement du suffrage.

L'algorithme de chiffrement ElGamal est par exemple utilisé dans les protocoles de vote décrits dans [41, 65, 81, 83, 95]. Les Annexes A, D et E fournissent des exemples de mise en œuvre de cet algorithme pour la génération de clé, le chiffrement et de déchiffrement du suffrage, ainsi que des exemples de preuves à divulgation nulle de connaissance compatibles avec cet algorithme, permettant d'assurer la sincérité du scrutin.

La sécurité de l'algorithme de chiffrement ElGamal repose sur la difficulté de résolution du problème du logarithme discret. Le *Guide de sélection d'algorithmes cryptographiques* [50] 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.

Mise en œuvre du pastillage Le pastiilage consiste en une association d'attributs à un électeur, qui doivent suivre l'expression de son vote. La notion de pastillage et sa mise en œuvre sont expliquées en Annexe B. 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 reproduire en clair sur le bulletin (le chiffrement du suffrage).

Pratique limitée à un scrutin de niveau 1

Une mise en œuvre du pastillage associant les attributs au suffrage plutôt qu'au bulletin comporte un risque majeur sur le secret du vote.

L'organisateur du scrutin peut donc envisager **uniquement le niveau 1** avec un système de vote mettant en œuvre un pastillage associant les attributs au suffrage plutôt qu'au bulletin.

R21 ★

Utiliser un pastillage associant les attributs au bulletin

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

- 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.
- Le bulletin construit par le client de vote peut être unique et commun au scrutin direct et aux scrutins indirects.

- Les preuves à divulgation nulle de connaissance présentes dans les bulletins doivent permettre de détecter tout déplacement d'un bulletin d'une urne à l'autre.
- Le bulletin doit être déposé simultanément dans toutes les urnes, correspondant au scrutin direct et aux scrutins indirects, après vérification des preuves à divulgation nulle de connaissance associées.

Des exemples de preuves à divulgation nulle de connaissance permettant de réaliser la détection de déplacement d'un bulletin d'une urne à une autre sont présentées en Annexe E.

Pour aller plus loin

L'objectif 1.04 est renforcé par les objectifs 1.07 et 2.08 relatifs 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 3.08, 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.

Cet objectif concerne le transport du bulletin depuis le client de vote jusqu'à l'urne électronique hébergée par le serveur de vote. 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, ou sur le serveur Web assurant la couche de présentation d'une architecture « trois tiers »[6].

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.

R22 ★

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 au guide TLS [47]. 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 équipés de dispositifs de vote ou de navigateurs obsolètes, reposant sur des versions du protocole TLS non conformes au guide [47][7], 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 dispositifs et navigateurs obsolètes.

R23 ★

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* [47] 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).

6. 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.

7. 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 [47].

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

Les recommandations suivantes sont applicables à partir du niveau 2. Elles visent à renforcer d'une part la terminaison TLS exposée aux clients de vote et d'autre part les liaisons internes au système de vote sur le chemin jusqu'à l'urne électronique.

R24 ★★

Protéger la terminaison TLS exposée par un certificat conforme au RGS

Il est recommandé que le système de vote mette en place un certificat conforme aux préconisations du *Référentiel Général de Sécurité* [56] sur la terminaison TLS exposée aux électeurs.

R25 ★★

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 authentification du serveur **et** l'authentification du client) conformes aux *Recommandations de sécurité relatives à TLS* [47] pour l'ensemble des flux sur le chemin entre la terminaison TLS exposée aux clients de vote, jusqu'à l'urne électronique.

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.

Dans le modèle de sécurité du niveau 1, un attaquant peut transmettre des bulletins invalides qui pourraient fausser la sincérité des élections. Aussi il est important que le système de vote puisse se protéger dès ce niveau contre de telles attaques.

Vérification des suffrages exprimés

Il est nécessaire que le système de vote vérifie la validité des suffrages avant de les décompter dans le résultat de l'élection. Suivant le mécanisme utilisé pour assurer l'étanchéité entre l'identité et le suffrage (1.07, 2.08), cette vérification est différente.

En cas d'**accumulation**, la vérification ne peut être réalisée qu'*avant* celle-ci, car une fois les bulletins accumulés, les suffrages qu'ils contiennent ne peuvent plus être vérifiés. Ainsi cette vérification ne peut être réalisée que sur les bulletins (contenant les suffrages chiffrés) non accumulés. Pour cela, le système de vote vérifie les preuves à divulgation nulle de connaissance composant le bulletin qui attestent que les suffrages qu'ils contiennent sont conformes.

En cas de **mélange vérifiable**, cette vérification ne peut être réalisée avant le mélange des bulletins, car ceux-ci ne contiennent pas une preuve de la même portée que celle présente en cas d'accumulation : la preuve est une preuve de connaissance de l'aléa et pas une preuve de conformité du suffrage. Ainsi la conformité des suffrages ne peut être vérifiée que *après* mélange et déchiffrement des bulletins.

Ainsi, il est possible de vérifier les bulletins à leur réception, cependant la portée de la vérification est différente suivant que le système de vote procède à l'accumulation ou le mélange des bulletins pour répondre à l'objectif d'étanchéité entre l'identité et le suffrage.

Le système de vote doit également assurer que les bulletins ne sont pas déposés dans d'autres urnes que celles auxquelles ils sont destinés, car cela pourrait porter atteinte au secret du vote, en particulier en cas de **pastillage** (1.04).

R26 ★

Vérifier les bulletins avant de les déposer dans l'urne électronique

Le système de vote doit vérifier chaque bulletin lors de sa réception avant de le déposer dans l'urne électronique à laquelle il est destiné. En particulier, le système de vote doit vérifier les preuves à divulgation nulle de connaissance composant le bulletin.

Des exemples d'algorithmes de génération et de vérification des preuves de validité du bulletin, adaptées à l'algorithme de chiffrment ElGamal sont décrits en Annexe E. La vérification des preuves peut avoir un impact sur le dimensionnement du système de vote (2.01 et R47★★).

8. En cas d'accumulation des bulletins, il faut garantir que chacun d'eux contient un vote valide. Par exemple, que seul une des listes candidates a été choisie, et pour y porter un seul vote. Les preuves jouent ce rôle de garant, sans divulguer l'expression du vote.

Disponibilité des bulletins

Une fois que les bulletins sont déposés dans l'urne, il est nécessaire de prévenir et détecter leur perte ou leur modification jusqu'au dépouillement, consécutives 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 sites 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, quels que soient l'incident ou la panne qui touche le système de vote. Si le système de vote ne permet pas d'atteindre une PDMA nulle [9], 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.

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.

Comme mentionné dans *Les fondamentaux de l'ANSSI - Sauvegarde des systèmes d'information* [43], une PDMA nulle implique une réplication synchrone entre deux centres de données distincts car elle intègre le risque majeur de perte d'un centre de données suite à un incident majeur. Ce type de risque correspond à un scrutin de niveau 3 qui nécessite donc une réplication totale. Un scrutin de niveau 1 ou 2 ne justifie pas la mise en place de réplication : il peut suffire d'appliquer des mesures de redondances des équipements au sein d'un unique centre de données.

Intégrité des bulletins - détection basique des modifications

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

9. Lorsque le système de vote est hébergé sur deux centres de données distants de centaines de kilomètres, la réplication synchrone peut être difficile à mettre en place. La PDMA sera alors non nulle.

R28 ⋆

Restreindre les accès techniques au système de vote pendant le scrutin

Le prestataire doit restreindre ses accès 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.

R29 ⋆

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 ou un chaînage cryptographique des bulletins : une telle modification est détectable car elle rend la signature ou le chaînage invalide.

La signature des bulletins peut être réalisée par le serveur de vote après la vérification des bulletins (R26⋆). Dans ce cas, la clé privée de signature est totalement sous le contrôle du serveur de vote, aussi en cas de compromission de ce serveur, la signature des bulletins peut être falsifiée.

La signature doit être réalisée au moyen d'un algorithme de signature conforme au *Guide de sélection d'algorithmes cryptographiques* [50]. De la même manière, un chaînage des bulletins peut être réalisé par le serveur de vote après la vérification des bulletins et avant le dépôt des bulletins dans l'urne électronique (R26⋆). Si le chaînage repose sur un mécanisme de signature, la même contrainte s'applique, si le chaînage s'appuie sur une prise d'empreinte numérique (par exemple HMAC [59]), le mécanisme doit être conforme au *Guide de sélection d'algorithmes cryptographiques* [50], la clé secrète est totalement sous le contrôle du serveur de vote.

Légitimité des bulletins - détection des modifications par le serveur de vote

Attention

La propriété de **vérifiabilité de la légitimité** (tous les bulletins proviennent d'électeurs légitimes et seulement de ceux-ci), qui constitue une partie de la **vérifiabilité universelle**, ne peut *pas* être atteinte avec la Recommandation R29⋆ (le système de vote contrôle la clé privée ou la clé secrète de signature ou de chaînage des bulletins). En effet, dans ce cas, le système de vote dispose des moyens de modifier les bulletins qu'il stocke puis de générer une nouvelle signature, à l'insu des électeurs.

Si le risque de modification illégitime de bulletin par le système de vote n'est pas acceptable, il est nécessaire de renforcer la signature des bulletins : elle doit être réalisée dès leur émission sur le client de vote et cette signature ne doit pas pouvoir être réalisée par les entités qui ont les moyens techniques de modifier les bulletins (le prestataire, l'organisateur du scrutin) car ces entités contrôlent également les dispositifs de surveillance et de scellement qui pourraient détecter cette modification. Une solution consiste à faire réaliser la signature des bulletins par les électeurs, sur le client de vote, au moyen d'une clé privée de signature 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 le prestataire doit intégrer la vérification de signature dans la solution de vote.

R30 ★★ ★+

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

En fonction des conclusions de l'analyse de risque (R67★★), il est recommandé qu'une entité indépendante de l'organisateur du scrutin et du prestataire fournisse une clé individuelle privée de signature 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 au moyen de la clé publique fournie par l'entité indépendante et doit vérifier l'association des clés publiques aux identités des électeurs.

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 l'objectif 3.03 qui concerne le renforcement de la PDMA en cas de bascule vers un site de secours.

Objectif n° 1-07

Assurer l'étanchéité totale entre l'identité du votant et l'expression de son vote (le contenu déchiffré de son bulletin de vote) pendant toute la durée du traitement.

Cet objectif est central pour garantir le secret du vote : il doit être impossible de mettre en relation l'identité de l'électeur avec l'expression de son vote.

Pour attenter à ce secret, il faut réussir 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.

Protection de l'étanchéité électeur/bulletin

Pour la première association 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, et si le bulletin est également horodaté, on peut rapprocher facilement le bulletin de l'électeur à travers leur horodatage.

En apparence simple, cette mesure est en pratique difficile à assurer (et à vérifier) sur des systèmes d'informations complexes, car toute opération laisse des traces techniques : traces des échanges réseaux entre le client de vote et le serveur de vote sur divers équipements, horodatage du système de fichiers sur un disque, journaux transactionnels des bases de données, etc. S'il est souhaitable de travailler sur cet axe, cela ne peut être suffisant pour des scrutins de niveau 2 ou 3 pour lesquels les mécanismes cryptographiques d'accumulation ou de mélange vérifiable sont recommandés.

Pratique limitée à un scrutin de niveau 1

Les mesures consistant à rendre impossible ou très difficile l'association électeur/bulletin, comme celles consistant à ne pas horodater les bulletins dans l'urne ou bien à désactiver la génération de traces techniques du système de gestion de la base de données, ont un impact limité sur l'étanchéité.

L'organisateur du scrutin peut donc envisager **uniquement le niveau 1** avec un système de vote mettant en œuvre uniquement de telles mesures pour assurer l'étanchéité.

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

Les mesures consistant à rendre impossible ou très difficile l'association bulletin/suffrage, comme l'accumulation ou le mélange vérifiable, décrites à l'objectif 2.08, ont un impact positif avéré et prouvé sur l'étanchéité.

L'organisateur du scrutin peut envisager **tous les niveaux de scrutin** avec un système de vote mettant en œuvre les mesures de l'objectif 2.08 pour assurer l'étanchéité.

Receipt-freeness

L'étanchéité entre l'identité du votant 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 tiers son suffrage (l'électeur peut toujours divulguer son suffrage à un tiers, ici il s'agit de le prouver). Pour cela, l'électeur 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. De plus, des contraintes peuvent être exercées par un tiers sur l'électeur. Comme expliqué à l'Annexe C, 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** [66], issue des travaux académiques, est le niveau le 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 **cœrcition** sont difficiles à mettre en œuvre aussi elles sont de niveau supérieur au niveau 3 de la CNIL : elles sont envisageables en fonction de l'analyse de risque (3.01)

R31 ★

Assurer la propriété de receipt-freeness

Il est recommandé que le système de vote assure 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 tiers, également destinataire de ces données. L'électeur n'effectue pas de manipulation supplémentaire à celles prévues par le protocole de vote.

Pour aller plus loin

L'objectif 1.07 est renforcé par l'objectif 2.08, le déchiffrement vérifiable (1.11), l'objectif 1.08 et la vérification de l'ensemble des preuves générées lors du dépouillement ainsi que la destruction des clés à l'issue du dépouillement (3.02).

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 de déchiffrement des bulletins permet de réaliser le dépouillement mais également de porter atteinte au secret du vote si cette clé est utilisée de manière illégitime ou si elle est compromise.

Afin de réduire ces risques, il est recommandé de fragmenter cette clé et d'attribuer les fragments aux membres du bureau électoral.

Fragmentation et stockage de la clé de déchiffrement

Une collusion des attributaires des fragments de la clé de déchiffrement 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 dépouillement. Pour cela, un algorithme de partage de secret à seuil [10] doit être utilisé.

R32 ★

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

Le système de vote doit fragmenter la clé privée de déchiffrement des bulletins au moyen d'un algorithme de partage de secret à seuil. 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).

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

L'Annexe D fournit des exemples de fragmentation de clé de chiffrement adaptés à l'algorithme 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).

R33 ★

Stocker les fragments de clés de manière sécurisée

Le système de vote doit stocker les fragments de la clé de déchiffrement des bulletins en respectant les points suivants :

- La clé entière (non fragmentée) ne doit jamais être stockée.
- À chaque fragment de la clé privée de déchiffrement doit être associé un code d'activation, seulement connu de l'attributaire.

10. 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.

- 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* [58]. Cette règle doit tenir compte de l'utilisation du code dans la protection du fragment de clé (code permettant de dériver une clé symétrique de chiffrement ou bien code PIN d'activation de support matériel).
- Chaque fragment de clé 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 déchiffrement 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 et les contrôles d'intégrité ou la vérification des mécanismes d'alerte (2.02, 2.03, 2.04, 3.04). Comme exprimé à la Recommandation R1★, le prestataire doit fournir la procédure de la cérémonie adaptée au contexte de l'organisateur du scrutin, pour assurer la sécurité de la génération, et l'organisateur du scrutin doit respecter cette procédure.

Génération de la clé de déchiffrement

Le **partage de secret à seuil** de Shamir [98] est communément utilisé. Ce mécanisme de partage a l'avantage d'être compatible avec n'importe quel algorithme de chiffrement utilisé mais il impose la génération de la clé de déchiffrement (et donc son existence, même temporaire) sur une même machine.

De plus, il repose sur l'hypothèse que l'ensemble des participants impliqués (attributaires, organisateur, prestataire) va exécuter correctement les procédures de génération, 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 pour nuire à la sincérité du scrutin. En particulier, comme expliqué dans [86], le secret du vote peut être compromis.

Afin de traiter ce risque, un **partage de secret à seuil *vérifiable*** permet de s'assurer que la clé publique de chiffrement générée est bien celle qui est issue des manipulations réalisées par les attributaires, et que chacun dispose bien d'un fragment de la clé privée de déchiffrement 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 déchiffrement, ainsi qu'un fragment de clé publique de chiffrement correspondant. La clé publique de chiffrement 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** (appelée preuve de connaissance de clé secrète) attestant 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. Le partage de secret de Pedersen [92] est un exemple de partage de secret vérifiable et il est compatible avec l'algorithme de chiffrement ElGamal [64]. D'autres exemples d'algorithmes de génération et de vérification des preuves de connaissance de clé secrète, compatibles avec l'algorithme de chiffrement ElGamal, sont décrits en Annexe E.

R34 ★★

Utiliser un partage de secret à seuil vérifiable

Il est recommandé que le système de vote mette en œuvre un partage de secret à seuil vérifiable, compatible avec l'algorithme de chiffrement des bulletins.

Dans ce cas, un tiers (par exemple l'expert indépendant au sens de la délibération de la CNIL [77]) doit pouvoir vérifier les preuves à divulgation nulle de connaissance générées par le partage de secret et vérifier que la clé publique de chiffrement des bulletins, telle que déployée sur le serveur de vote, correspond aux fragments de clés publiques générés par les attributaires.

Le partage de secret à seuil vérifiable permet de détecter une erreur ou une mauvaise manipulation volontaire lors de la génération de la clé de chiffrement des bulletins. Cependant il ne couvre pas le risque d'une génération de la clé compromise par le serveur de vote lui-même, qui serait indétectable. En effet, comme exposé à l'objectif 1.10, même en cas d'expertise indépendante du code source correspondant à la génération de la clé, cette expertise repose *in fine* sur un certain niveau de confiance dans le serveur de vote. Afin de couvrir ce risque, il est nécessaire de mettre en œuvre un partage de secret à seuil distribué utilisant des dispositifs de génération non (ou difficilement) contrôlables par l'organisateur du scrutin et le prestataire (R76★★+).

Pour aller plus loin

L'objectif 1.08 est renforcé par l'objectif 3.07 qui impose de ne pas traiter la clé de déchiffrement des bulletins sur le serveur stockant les bulletins déposés par les électeurs.

Objectif n° 1-09

Définir le dépouillement comme une fonction atomique utilisable seulement sur l'ensemble des bulletins du scrutin et après sa fermeture.

Le terme *atomique* signifie qui ne peut être coupé, indivisible. Dans le contexte du dépouillement, l'opération atomique est l'opération de déchiffrement des bulletins, qui suit l'opération d'accumulation ou de mélange vérifiable (1.07, 2.08), ou bien qui est incluse dans le mélange vérifiable, suivant le type de mélange (voir Annexe A). L'atomicité signifie qu'une fois que le déchiffrement des bulletins est initié, il doit être réalisé en une seule fois et sur l'ensemble des bulletins de l'élection : soit l'opération de déchiffrement réussit sur tous les bulletins qui doivent être dépouillés, soit elle échoue, ce qui interdit les dépouillements partiels non prévus [11]. Il impose également que le dépouillement ait lieu après la fermeture du scrutin, pour la même raison.

Une pratique répandue consiste à organiser une cérémonie au cours de laquelle les fragments de la clé privée de déchiffrement sont utilisés par les attributaires pour déchiffrer les bulletins. De manière analogue à la cérémonie de génération (1.08), cette cérémonie permet de réunir le bureau électoral et peut permettre de réaliser d'autres actions comme la vérification du scellement et des contrôles d'intégrité ou la vérification des mécanismes d'alerte (2.02, 2.03, 2.04, 3.04). Comme exprimé à la recommandation R1★, le prestataire doit fournir la procédure de la cérémonie adaptée au contexte de l'organisateur du scrutin pour assurer la sécurité de la génération, et l'organisateur du scrutin doit respecter cette procédure.

S'il est possible d'effectuer le dépouillement sur des ensembles de bulletins arbitraires, une atteinte au secret du vote est réalisable [12]. 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, y compris en cas de **pastillage** (1.04).

R35 ★

Détecter tout dépouillement illégitime

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

En cas de **pastillage** (1.04), les urnes à dépouiller sont celle du scrutin direct et celles des scrutins indirects.

Comme expliqué à l'objectif 1.07, le dépouillement nécessite l'accès aux fragments de la clé privée de déchiffrement des bulletins. 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, de mélange vérifiable et de déchiffrement après la clôture du scrutin doit tenir compte des temps de traitement de chaque opération.

11. Le pastillage (1.04) implique des dépouillements qui sont bien prévus et qui ne sont pas partiels.
12. À l'extrême, un ensemble peut être constitué d'un bulletin et cela peut permettre de dévoiler le suffrage d'un électeur.

R36 ★★

Ne déchiffrer que des bulletins accumulés ou mélangés

La solution de vote doit assurer (organisationnellement ou techniquement) que seuls les bulletins vérifiés sont déchiffrés :

- En cas d'accumulation (2.08), l'accumulation ne peut être réalisée qu'après vérification individuelle des preuves composant les bulletins et le déchiffrement ne peut être réalisé que sur l'accumulation produite et pas sur les bulletins d'origine.
- En cas de mélange vérifiable incluant le déchiffrement (2.08), celui-ci ne peut être réalisé qu'après vérification individuelle des preuves composant les bulletins.
- En cas de mélange vérifiable n'incluant pas de déchiffrement, le mélange ne peut être réalisé qu'après vérification individuelle des preuves composant les bulletins et le déchiffrement ne peut être réalisé que sur les bulletins issus de l'ensemble des mélanges et après vérifications des preuves associées aux mélanges.

Il est recommandé que le prestataire adapte la mise en œuvre et les moyens attribués à ces opérations afin de faciliter l'organisation de la cérémonie de dépouillement.

Pour aller plus loin

L'objectif 1.09 est renforcé par l'objectif 2.04 et la mise en place d'alerte en cas de détection de tentative de dépouillement illégitime.

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 la sincérité du scrutin : le système de vote doit être conforme aux attentes et il ne doit pas être modifié. De plus, le résultat de l'élection ne sera sincère que si l'urne et la liste d'émargement sont vides au début du scrutin.

Idéalement, l'intégrité est assurée pour l'ensemble du système de vote, y compris son hébergement. Cependant, et en particulier pour les scrutins de niveau 1, la vérification de l'intégrité peut se concentrer sur l'application de vote et la configuration de l'élection.

Intégrité de l'application de vote

La référence du contrôle d'intégrité est produite par l'expertise indépendante exigée par la délibération CNIL [77]. Cette expertise doit assurer que l'application de vote est conforme aux objectifs de la délibération et se comporte de façon sincère, notamment grâce à une analyse du code source, des scripts et des fichiers composant l'application.

Attention

Garantir que les fichiers exécutables issus de la compilation du code source correspondent de manière équivalente à ce code source est impossible : d'une part les fonctionnalités implémentées peuvent être modifiées et d'autre part des vulnérabilités peuvent être introduites [91, 103].

De plus, le périmètre de l'expertise indépendante peut ne pas couvrir l'intégralité du code source de l'application de vote.

Il s'agit d'un compromis qui fait l'hypothèse que le périmètre de l'expertise couvre les fonctionnalités principales du système de vote, que la compilation du code source respecte ces fonctionnalités et que la compilation n'introduit pas de vulnérabilités.

Pour ensuite étendre cette assurance au système de vote entier, il faut établir un lien entre le code source et l'application effectivement déployée sur le système de vote. Cela passe par les étapes suivantes :

- Réaliser une compilation du code source en application exécutable de manière reproductible [31], au sens où le résultat de cette compilation est déterministe.
- Prendre une empreinte numérique de l'application exécutable issue de la compilation du code source expertisé.
- Vérifier 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.

Attention

Vérifier l'intégrité d'une application exécutée par un serveur sans se connecter à ce serveur en tant qu'administrateur système est impossible, aussi cette vérification est

nécessairement intrusive. Or, pendant le scrutin, il est recommandé de ne pas se connecter au système de vote en tant qu'administrateur système (R28★), car ce rôle dispose de privilèges qui pourraient eux-mêmes attenter à l'intégrité du système de vote.

Aussi, la vérification de l'intégrité de l'application de vote devra se contenter de comparer l'empreinte calculée et affichée par le serveur de vote lui-même [13] avec l'empreinte de référence.

Il s'agit d'un compromis qui fait l'hypothèse que le serveur de vote est au moins partiellement de confiance et que, si le serveur est compromis, il sera difficile pour l'attaquant de modifier l'application de vote sans déclencher une alerte (2.04).

R37 ★

Fournir une compilation reproductible

Il est recommandé que le prestataire fournisse une compilation reproductible [31] 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 [77]) 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.

R38 ★

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

Le système de vote doit permettre à un tiers (par exemple l'expert indépendant au sens de la délibération de la CNIL [77]) de contrôler que les fichiers exécutables de l'application de vote correspondent au résultat de la compilation du code source audité par le tiers.

L'intégrité de ces fichiers exécutables doit pouvoir être attestée par une prise d'empreinte numérique et une comparaison avec l'empreinte de référence calculée par un tiers qui réaliserait la compilation reproductible (R37★).

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 attestée, également par comparaison d'empreinte numérique.

Cohérence de l'urne et de l'émargement

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

13. Cette empreinte est généralement disponible sur l'interface Web du serveur de vote, au moins dans sa partie destinée au bureau électoral.

R39 ★

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

Le système de vote doit permettre au prestataire de contrôler la cohérence de l'urne et 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 (1.04), la cohérence doit être vérifiée sur l'urne du scrutin direct et les urnes des scrutins indirects.

La cohérence doit pouvoir être attestée par requêtes directes sur la base de données, 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 et la sincérité du scrutin, ou qui peuvent avoir un impact sur la sincérité du scrutin.

R40 ★

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

Il est recommandé que le prestataire mette en œuvre un dispositif de journalisation des événements, par exemple en suivant les *Recommandations de sécurité pour l'architecture d'un système de journalisation* [54].

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 ou de chaînage des bulletins (1.06).
- Les fragments de la clé de déchiffrement des bulletins 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 ainsi que 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.

R41 ★

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).

- L'envoi et le recouvrement de secret d'authentification des électeurs ; le changement de moyen d'adressage des moyens d'authentification des électeurs (1.03, R16★).
- La génération des clés privées ou des secrets de signature, (1.06, 2.02) et de la clé privée de signature des preuves de vote (2.07).
- La génération des fragments de la clé de déchiffrement (1.08).
- L'ouverture, la suspension, l'arrêt et la fermeture du scrutin (2.05).
- Le lancement du dépouillement, y compris le lancement et la clôture des opérations d'accumulation, de mélange vérifiable et de déchiffrement (1.09).
- Le scellement et toute vérification de scellement du système (2.02).
- Les alertes transmises au bureau électoral (2.04, 3.06).

R42 ★

Journaliser les événements ayant un impact sur la sincérité du scrutin

Il est recommandé que le système de vote journalise les événements ayant un impact direct ou indirect sur la sincérité du scrutin , notamment :

- Échec d'une opération de la transaction de vote (1.02).
- Dépôt d'un bulletin dans une urne sans émargement ou émargement sans dépôt de bulletin dans une urne (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.

Le dépouillement, dernière étape du scrutin, produit le décompte des suffrages et le résultat de l'élection. 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 proposées (voir par exemple [8]) : pouvoir rejouer le dépouillement à la demande du juge, ou pouvoir prouver de façon irréfutable que le décompte correspond effectivement au contenu de l'urne au moyen de preuves mathématiques.

Vérification du dépouillement par rejeu

La première solution est donc de permettre un rejeu du dépouillement. Cette solution s'impose lorsque le déchiffrement des bulletins est *non vérifiable* : le seul moyen de le vérifier est de le rejouer. Pour cela, l'organisateur de l'élection doit :

- Conserver l'urne d'origine (non mélangée, non accumulée) et de façon générale la configuration de l'élection. Cette conservation est de toute façon obligatoire (dans sa section « Conservation des données portant sur l'opération électorale », la délibération CNIL [77]) utilise la notion de **matériel de vote**).
- Conserver les fragments de la clé privée de déchiffrement.
- Obtenir la coopération d'assez d'attributaires de ces fragments pour qu'ils acceptent d'utiliser leur code d'activation lors du rejeu (et que ces attributaires se souviennent de leur code d'activation).
- Pouvoir utiliser une fonction de rejeu du scrutin dans le système de vote fourni par le prestataire (parfois des mois après le scrutin, alors que le système de vote pourrait avoir été sauvegardé puis démantelé).

La limite de cette première solution est qu'en conservant la possibilité d'un nouveau dépouillement alors que la surveillance du bureau électoral est relâchée après le scrutin, on augmente le risque d'une atteinte au secret du vote.

En effet, l'organisateur conserve le matériel de vote (dont l'urne d'origine avec les bulletins individuels) et les journaux de l'élection. Or, comme vu dans l'objectif 1.07, il est illusoire de compter sur une absence de lien électeur/bulletin. Il faut donc apporter des garanties supplémentaires, après le scrutin, qu'une collusion d'acteurs aux intérêts divergents sera nécessaire pour effectivement réaliser un nouveau dépouillement d'une part, et d'autre part que l'accès aux informations nécessaires à ce dépouillement sera tracé.

Attention

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

Cependant, ce serait une atteinte intolérable au secret du vote. L'organisateur pourrait en effet déchiffrer seul les bulletins individuels de l'urne d'origine. 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 vérifiable ou à l'accumulation de l'urne (2.08).

Cela irait enfin à l'encontre de la délibération CNIL [77] qui cite parmi les garanties minimales qu'il faut pouvoir « prouver de façon irréfutable que les clés de chiffrement/déchiffrement ne sont connues que de leurs seuls détenteurs. »

En plus de ce risque d'atteinte au secret du vote, l'utilisation d'un déchiffrement non vérifiable (c'est à dire ne produisant pas de preuves mathématiques) peut porter atteinte à l'intégrité du résultat. En effet, comme expliqué à l'Annexe D, une compromission de l'application ou du serveur de vote suffit à générer un résultat ne correspondant pas aux suffrages exprimés. Comme exposé à l'objectif 1.10, même en cas d'expertise indépendante, cette expertise repose *in fine* sur un certain niveau de confiance dans l'application de vote déployée et dans le serveur de vote, aussi le risque de production d'un résultat ne correspondant pas aux suffrages exprimés est avéré pour les scrutins de niveau 2 ou 3.

Enfin, l'organisateur s'expose aussi en pratique à un risque juridique : si le juge demande un rejeu, l'organisateur dépendra des attributaires des fragments de la clé privée, qui devront en effet pouvoir entrer le code d'activation relatif à leur fragment personnel. Le risque juridique augmente si les relations entre les attributaires sont conflictuelles, ce qui pourra être le cas si un recours a été déposé (le niveau 3 défini par la délibération de la CNIL [77] mentionne explicitement le climat conflictuel comme facteur de risque).

Pratique limitée à un scrutin de niveau 1

Le recours au rejeu du dépouillement comporte des risques qui peuvent porter atteinte au secret du vote, à l'intégrité du résultat et sur la capacité réelle à pouvoir effectuer un tel rejeu.

L'organisateur du scrutin peut donc envisager **uniquement le niveau 1** avec un système de vote mettant en œuvre uniquement la vérification du dépouillement par rejeu.

Vérification du dépouillement par des preuves mathématiques

Lors du dépouillement, le **déchiffrement vérifiable** [80] produit des preuves mathématiques attestant que le résultat du déchiffrement correspond bien au contenu des bulletins avant déchiffrement.

Information

Le déchiffrement vérifiable est la solution requise par le Code électoral [5] (article R.179-1) pour les élections politiques.

De plus, la vérification de ces preuves ne nécessite pas de rejouer le dépouillement, ni de disposer de la clé privée. Ainsi, cette vérification est possible par tout tiers disposant des informations et des compétences nécessaires, dont l'expert indépendant au sens de la délibération de la CNIL [77] ou un juge, et en toute autonomie.

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

La vérification du dépouillement par des preuves mathématiques au lieu du rejeu assure le secret du vote, l'intégrité du résultat. Cette vérification est de plus réalisable en autonomie et ne nécessite pas de clé privée.

L'organisateur du scrutin peut envisager **tous les niveaux de scrutin** avec un système de vote mettant en œuvre une vérification de dépouillement par des preuves mathématiques.

R43 ★★

Utiliser un déchiffrement vérifiable

Il est recommandé que le système de vote mette en œuvre un déchiffrement vérifiable des bulletins (soit intégré à un mélange vérifiable, soit portant sur des bulletins mélangés ou accumulés), au moyen de preuves à divulgation nulle de connaissance attestant 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 sans utilisation des fragments de la (ou les) clé(s) privée(s) de déchiffrement. Le prestataire doit fournir la procédure de déchiffrement adaptée au contexte de l'organisateur du scrutin pour assurer la validité des preuves générées, et l'organisateur du scrutin doit respecter cette procédure.

Le lien entre l'urne d'origine et le résultat est également vérifiable, par des moyens qui dépendent du mécanisme choisi pour assurer l'étanchéité entre les bulletins et les suffrages (voir R65★★) :

- En cas d'**accumulation**, le lien entre l'urne d'origine (non accumulée) et le résultat final est prouvé ainsi : l'accumulation est déterministe et peut être rejouée à l'identique à partir de l'urne d'origine pour produire une urne accumulée. Les preuves issues du déchiffrement vérifiable attestent ensuite que le résultat correspond à l'urne accumulée.
- En cas de **mélange vérifiable intégrant le déchiffrement**, les preuves produites par le mélange et le déchiffrement attestent que les bulletins issus de ces opérations contiennent les mêmes suffrages que ceux de l'urne d'origine.
- En cas de **mélange vérifiable n'intégrant pas le déchiffrement**, les premières preuves produites par le mélange attestent que les bulletins issus du mélange contiennent les mêmes suffrages que ceux de l'urne d'origine. Les secondes preuves produites par le déchiffrement vérifiable attestent ensuite que le résultat correspond aux bulletins issus du mélange.

Des exemples de preuves à divulgation nulle de connaissance adaptées à l'algorithme ElGamal sont présentés en Annexe E.

Attention

La disponibilité de preuves de déchiffrement correct rend inutile la vérification du dépouillement basé sur un rejeu. Il n'est donc plus nécessaire de conserver les clés de déchiffrement ni les codes d'activation associés, alors que cette conservation met en danger le secret du vote [14].

14. Le Code Électoral [5] mentionne explicitement que les clés de déchiffrement doivent être détruites (Article R179-1).

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

R44 ★★

Conserver les éléments nécessaires à la vérification des preuves mathématiques

L'organisateur du scrutin doit conserver l'ensemble des éléments nécessaires à la vérification des preuves mathématiques générées lors du dépouillement :

- La configuration de l'élection.
- Les preuves générées par le partage vérifiable de la clé privée de déchiffrement des bulletins.
- La clé publique de chiffrement des bulletins.
- L'urne d'origine avec les bulletins non accumulés et non mélangés, y compris les preuves associées à chaque bulletin.
- En cas de **mélange vérifiable** (2.08), le résultat de chaque mélange réalisé par chaque mélangeur et les preuves générées lors de chaque mélange.
- Les preuves générées par le déchiffrement du résultat de l'accumulation ou du mélange.
- L'ensemble des données publiques utilisées pour enrichir le contexte des preuves générées, comme expliqué à l'Annexe E.
- Les résultats de l'élection.

i

Information

Le résultat de l'accumulation de l'urne (2.09) est calculable directement à partir de l'urne non accumulée, aussi il n'est pas nécessaire de le conserver. De plus :

- En cas de **pastillage** (1.04), il y aura plusieurs urnes à accumuler ou à mélanger (une par scrutin direct ou indirect), et donc plusieurs déchiffrements. Les preuves sont conservées pour chacun de ces mélanges et déchiffrements.
- En cas de déchiffrement distribué (voir R77★★+), chaque déchiffrement partiel produit des preuves.

Ensuite, toujours pour que la vérification puisse être réalisée, il faut qu'il existe un outil de vérification des preuves. Pour le niveau 2 cet outil peut être fourni par le prestataire (à condition qu'il soit auditable et audité) et pour le niveau 3 le prestataire doit fournir une spécification publique permettant à tout tiers de le développer.

R45 ★★

Fournir un outil de vérification des preuves auditable

Le prestataire doit fournir un outil permettant au bureau électoral de vérifier les preuves générées par le système de vote. Le code de cet outil doit être auditable par un tiers (par exemple l'expert indépendant au sens de la délibération de la CNIL [77]) et fournir des résultats compréhensibles à toute personne amenée à l'utiliser.

Au final, les preuves générées doivent être vérifiées, pour le niveau 2 au moyen de l'outil fourni par le prestataire et pour le niveau 3 au moyen d'un outil tiers développé à partir des spécifications fournies par le prestataire. La vérification de ces preuves est indispensable à la sincérité du scrutin, aussi elle devrait faire partie des prestations assurées par les tiers (par exemple l'expert indépendant au sens de la délibération de la CNIL [77]).

Pratique limitée à un scrutin de niveau 1

L'absence de vérification des preuves mathématiques générées par la solution de vote porte atteinte à la sincérité du scrutin.

L'organisateur du scrutin peut donc envisager **uniquement le niveau 1** si aucun tiers indépendant (y compris l'expert indépendant au sens de la délibération de la CNIL [77]) n'intègre dans son périmètre d'intervention la vérification des preuves mathématiques.

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

La vérification des preuves mathématiques générées par la solution de vote assure la sincérité du scrutin.

L'organisateur du scrutin peut donc envisager **tous les niveaux de scrutin** si un tiers indépendant (par exemple l'expert indépendant au sens de la délibération de la CNIL [77]) intègre bien dans son périmètre d'intervention la vérification des preuves mathématiques, soit au moyen de l'outil fourni par le prestataire (**pour le niveau 2**), soit au moyen d'un outil développé indépendamment de la solution du prestataire (**pour le niveau 3**). Dans les deux cas le périmètre d'intervention du tiers doit inclure l'audit de l'outil et la vérification que celui-ci effectue correctement la vérification des preuves.

R46 ★★

Vérifier les preuves mathématiques

Il est recommandé que l'expert indépendant (au sens de la délibération de la CNIL [77]) intègre dans le périmètre de sa prestation la vérification des preuves mathématiques générées par la solution de vote.

Pour aller plus loin

Cet objectif est renforcé par l'objectif 3.02 qui impose la publication de spécifications permettant à un tiers, indépendant du prestataire, de développer un outil de vérification des preuves générées par le système de vote.

4.2 Objectifs de sécurité de niveau 2

Définition de la CNIL [77] : **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 système de vote, le prestataire et l'organisateur du scrutin peuvent porter atteinte à la sincérité du scrutin. En conséquence, les recommandations de ce niveau complètent celles du niveau 1 et visent à renforcer le secret du vote via l'utilisation de mécanismes cryptographiques adaptés, et à renforcer l'intégrité par la surveillance effective du système de vote et son durcissement. Les enjeux plus élevés des scrutins de niveau 2 justifient des moyens supplémentaires pour en assurer la disponibilité ainsi qu'une plus grande transparence avec la vérifiabilité individuelle.

2-01	Assurer une haute disponibilité de la solution.
2-02	Assurer un contrôle automatique de l'intégrité du système de vote et de la cohérence entre l'urne et la liste d'émargement pendant toute la durée du scrutin.
2-03	Permettre la surveillance par le bureau électoral de l'intégrité du système de vote et de la cohérence entre l'urne et la liste d'émargement pendant toute la durée du scrutin.
2-04	Assurer que le bureau électoral soit alerté de tout incident de sécurité survenant sur le système de vote électronique et dispose d'un accès à un journal de ces alertes.
2-05	Assurer un cloisonnement entre chaque scrutin de sorte qu'il soit possible 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 et par l'ANSSI.
2-07	Permettre aux électeurs de vérifier la présence de leur bulletin dans l'urne.
2-08	Assurer sur le plan technique l'étanchéité totale entre l'identité des électeurs et les bulletins déchiffrés lors du dépouillement.
2-09	Favoriser la transparence de la solution de vote en publiant, en amont du scrutin, les spécifications techniques du protocole de vote.

Tableau 3 – Objectifs de niveau 2

Attention

La conformité au niveau 2 ne fournit pas de protection contre un attaquant disposant de ressources importantes permettant d'usurper l'identité des électeurs, de porter atteinte à la disponibilité ou à la surveillance du système de vote, ou de remettre en cause la validité du dépouillement. Pour ce niveau d'attaquant, des mesures complémentaires doivent être envisagées.

Objectif n° 2-01

Assurer une haute disponibilité de la solution.

L'indisponibilité de la solution peut avoir un impact sur la sincérité du scrutin 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.

La disponibilité de la solution dépend du système de vote et des moyens qui lui sont attribués. Elle dépend également de la disponibilité d'autres systèmes qui peuvent ne pas être directement contrôlés par le prestataire. Il est également important de prendre en compte l'aspect géographique pour estimer la disponibilité.

R47 ★★

Dimensionner 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 (cf. 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 de 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 de candidats 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.

R48 ★★

Mettre en œuvre un système de vote redondant

Le prestataire doit fournir un système de secours susceptible de prendre le relais en cas de panne du 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 infrastructure technique redondante.

Au niveau 2, il est acceptable que les deux systèmes, principal et de secours, soient hébergés dans le même centre de données. 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.

R49 ★★

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) et l'état du réseau (volume des données échangées).

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 en 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 important de mettre en place les moyens permettant de prévenir ces attaques, et de réagir afin d'en limiter l'impact pendant la période de vote.

R50 ★★

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* [22] ainsi que les *Fiches Réflexes du CERT-FR* [12, 13].

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

Assurer un contrôle automatique de l'intégrité du système de vote et de la cohérence entre l'urne et la liste d'émargement pendant toute la durée du scrutin.

Cet objectif renforce l'objectif 1.10 : aux contrôles initiaux de l'intégrité du système et de la vacuité de l'urne et de la liste d'émargement, il ajoute l'automatisation de ces contrôles pendant toute la durée du scrutin. Cette automatisation 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 (R38★). 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.

R51 ★★ 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* [42] : 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* [49] et notamment porter sur les éléments suivants :

- Avant l'ouverture du scrutin :
  - Les données relatives à l'application de vote (R38★).
  - Les données relatives à la configuration de l'élection. La configuration inclut notamment le découpage électoral, la liste des candidats et l'ordre dans lequel ils sont présentés aux électeurs, la liste électorale, les heures d'ouverture et de fermeture du scrutin, la clé publique de chiffrement et les éventuels secrets de signature (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 et la liste d'émargement.
- À la fin des opérations sur l'ensemble du système.

R52 ★★

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, l'intégrité du système est assurée par de la supervision de l'état du système de vote (R49★★) et des accès au système de vote, déjà limités (R28★).

R53 ★★

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.

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 la surveillance par le bureau électoral de l'intégrité du système de vote et de la cohérence entre l'urne et la liste d'émargement pendant toute la durée du scrutin.

Cet objectif renforce les objectifs 1.10 et 2.02 : il requiert la mise à disposition du bureau électoral du résultat du contrôle de cohérence entre l'urne et l'émargement et des scellements, et la mise à disposition du journal des événements.

R54 ★★

Fournir au bureau électoral les résultats des contrôles d'intégrité

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

- Contrôle de l'intégrité de l'application de vote (R38★).
- Contrôle de cohérence entre l'urne et la liste d'émargement décrit (R39★).
- Contrôle des scellements (R52★★).

R55 ★★

Permettre l'analyse du journal des événements par un tiers

Le prestataire doit permettre à un tiers (par exemple l'expert indépendant au sens de la délibération de la CNIL [77]) d'analyser les journaux collectés pendant les opérations, contenant les événements relatifs au fonctionnement du système de vote (R41★) ainsi que les événements ayant un impact sur la sincérité du scrutin (R42★).

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.

Objectif n° 2-04

Assurer que le bureau électoral soit alerté de tout incident de sécurité survenant sur le système de vote électronique et dispose d'un accès à un journal de ces alertes.

Cet objectif renforce les objectifs 1.02, 1.03, 1.06, 1.09, 2.01, 2.02 et 2.07. 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 la sincérité du scrutin (cohérence urne et émargement, intégrité des bulletins) ou concernent des événements qui peuvent avoir un impact sur la sincérité du scrutin.

R56 ★★

Alerter le bureau électoral en cas d'incident ou de rupture d'intégrité

Le système de vote doit émettre des alertes à destination du bureau électoral pour tout événement ou incident relatif à la sécurité du système ou à la sincérité du scrutin.

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 dispositif d'alerte doit également générer une alerte automatique au bureau électoral.

Le prestataire doit s'assurer que les alertes à destination du bureau électoral sont suffisamment compréhensibles pour que celui-ci puisse prendre toute décision relativement à ces alertes en toute autonomie.

Le système de vote doit générer une alerte à destination du bureau électoral notamment dans les cas suivants :

- Échec d'une opération de la transaction de vote (1.02, R7★).
- Incohérence entre l'urne et l'émargement (1.02, R8★, R39★).
- Attaque par recherche d'authentifiants (1.03, R11★).
- Modification de bulletin transmis par un électeur, traité par le serveur de vote et stocké dans l'urne électronique (1.06, R29★).
- Détection d'une modification de clé privée ou de secret de signature, de chaînage ou de scellement (1.06, 2.02) ou de signature des preuves de vote (2.07).
- Détection d'une modification des données publiques intervenant dans la vérification de la sincérité du scrutin, notamment dans la constitution des preuves à divulgation nulle de connaissance générées par la solution de vote (1.04, 1.07, 1.08, 1.11), 2.08).
- Tentative de dépouillement illégitime : dépouillement avant la clôture ou dépouillement sur un ensemble de bulletins non autorisé (1.09, R35★).
- Indisponibilité, attaque en déni de service sur le système de vote (2.01, R49★★, R50★★).
- Rupture d'un scellement (2.02, R52★★).

Pour aller plus loin

Cet objectif est renforcé par l'objectif 3.06 relatif à la mise en place d'alertes en cas d'intervention de gestion et de maintenance sur le système de vote.

Objectif n° 2-05

Assurer un cloisonnement entre chaque scrutin de sorte qu'il soit possible 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 d'arrêter un scrutin sans que cela empêche d'autres scrutins de continuer. Les autres scrutins sont d'abord ceux du même organisateur, mais également ceux d'autres clients du prestataire.

Information

Seuls les scrutins *directs* peuvent être suspendus ou arrêtés. Les scrutins *indirects* liés au pastillage (1.04) dépendent de l'état du scrutin direct auquel ils sont associés.

Pour permettre de 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. 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 oeuvre 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 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 niveau de cloisonnement peut se justifier d'abord par l'ampleur du scrutin (nombre important de votants) et parfois en tant que mesure de sécurité avancée [15].

R57 ★★ 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 [16].

Le cloisonnement entre les scrutins peut être applicatif ou logique ou (optionnellement) physique.

Hébergement et mutualisation

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 [40], et en fonction du modèle de sécurité, le choix de l'offre sera adapté aux conclusions de l'analyse des risques (3.01).

15. Le cloisonnement physique va limiter les possibilités de **latéralisation** d'un attaquant d'un scrutin à l'autre. Cependant, si l'application gérant les différents scrutins est la même, et si l'exposition des différents scrutins à Internet est similaire, alors une telle mesure n'est pas pertinente : si un des systèmes est compromis, les autres peuvent probablement l'être aussi par le même moyen.

16. « autres scrutins » signifie les autres scrutins gérés par l'organisateur et les autres scrutins gérés par le prestataire (pour d'autres clients que l'organisateur).

Dans le cadre d'une offre mutualisée, voire externalisée, il convient d'intégrer ces spécificités à l'analyse de risques indiquées ci-dessus. Si l'étude conclut à la compatibilité d'une telle offre avec les objectifs de sécurité, alors elle devient acceptable pour cet usage. Et, 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 (SecNumCloud) ou un hébergement internalisé et sécurisé peuvent fournir des alternatives. Comme expliqué dans [40], les offres Cloud qualifiées SecNumCloud non commerciales (internes et communautaires) et commerciales privées permettent de disposer d'une infrastructure dédiée évitant le risque de latéralisation d'un attaquant depuis l'environnement d'un client vers un autre.

Objectif n° 2-06

Utiliser un système d'information mettant en œuvre les mesures de sécurité physique et logique recommandées par les éditeurs et l'ANSSI.

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.

Le guide *Recommandations pour la mise en œuvre d'un site Web* [51] 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 le dispositif de vote 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, le Top 10 OWASP [96] 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 permettent de renforcer la sincérité du scrutin car elles protègent le système de vote contre des attaques internes et externes.

R58 ★★

Suivre des 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* [51] de l'ANSSI et les recommandations du *TOP 10 OWASP* [96].

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, le prestataire doit suivre les bonnes pratiques applicables fournies par les éditeurs ou par des tiers.

Pour les systèmes reposant sur LINUX, le guide *Recommandations de configuration d'un système GNU/LINUX* [42] fournit 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.

R59 ★★

Suivre des 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* [42].

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 issues de la liste *National Checklist Program for IT Product* [90] ou les recommandations émises par le *Center for Internet Security* [4].

Les administrateurs du système de vote (qu'ils soient du prestataire ou de l'organisateur du scrutin) ont un rôle essentiel pour assurer la sincérité du scrutin. Le guide [52] fournit des indications pour mettre en œuvre ces accès privilégiés au système de vote.

R60 ★★

Suivre des 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* [52].

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 (R41★, R42★) et les alertes (R73★★★).

Enfin, la sécurité physique des composants techniques est essentielle pour assurer la sincérité du scrutin, car un accès physique illégitime peut permettre de lire ou modifier les données sensibles (notamment les fragments de clés, l'urne électronique, la liste d'émargement, la configuration de l'élection, l'application de vote). Le guide [48] fournit des indications pour mettre en œuvre des contrôles d'accès physique à ces composants.

R61 ★★

Suivre des 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* [48].

Objectif n° 2-07

Permettre aux électeurs de vérifier la présence de leur bulletin dans l'urne.

L'objectif correspond à la propriété appelée **recorded-as-cast** (*présence dans l'urne* du bulletin 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 contenues dans les preuves de vote. L'objectif ne concerne par contre pas la propriété appelée **cast-as-intended**, qui constitue l'autre partie de la vérifiabilité individuelle.

Le système de vote doit fournir à l'électeur une **preuve de vote** contenant une donnée calculée à partir de son bulletin. Le système de vote doit également publier l'ensemble des données permettant aux électeurs de vérifier la présence de leur bulletin dans l'urne. La preuve de vote est indépendante du **récépissé** [17]. Comme expliqué à la recommandation R9★, afin d'obtenir un premier niveau de **receipt-freeness**, la preuve de vote, associée au récépissé, ne doit pas contenir d'information permettant de compromettre le secret du vote.

R62 ★★

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 est une information 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 choix de vote.

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 non plus pas contenir de données qui, seules ou ajoutées aux informations fournies par le récépissé, permettent de compromettre le secret du vote. L'information est transmise au serveur de vote pour publication.

Il est recommandé que la preuve de vote contienne également une signature de cette information 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 de l'information 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 la transaction 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.

17. 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.

Lorsque le serveur de vote réalise la signature des bulletins (R29★), le dispositif de signature peut être utilisé pour réaliser la signature des preuves de vote.

R63 ★★

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

Le serveur de vote doit publier les informations présentes dans les preuves de vote transmises par les clients de vote sur une page Web accessible sans restriction.

Les électeurs doivent disposer d'un moyen pour contrôler que la donnée présente dans leur preuve de vote et correspondant à leur bulletin est bien présente dans la liste des données publiées par le système de vote.

Les tiers réalisant les contrôles pour la vérifiabilité individuelle (R64★★) et la vérifiabilité universelle (R68★★) doivent pouvoir s'assurer de la cohérence de cette liste avec les données dont ils disposent pour réaliser leurs vérifications.

Pour les scrutins de niveau 3, le prestataire doit publier des spécifications pour l'implémentation d'un outil de vérifiabilité individuelle par un tiers. Une recommandation similaire est faite, également au niveau 3, pour la vérifiabilité universelle.

R64 ★★

Publier les spécifications d'un outil de vérifiabilité individuelle

En amont du scrutin, le prestataire doit publier une spécification détaillant la constitution des preuves de vote et publier une spécification d'un outil permettant de les vérifier. Ces publications doivent être réalisées suffisamment en amont du scrutin et permettre à un tiers de développer un outil de vérification de l'authenticité des données publiées à destination des électeurs et de leur cohérence avec l'urne, indépendant du système de vote. Cet outil doit permettre à un tiers disposant de l'urne électronique, non accumulée ou non mélangée, de réaliser les vérifications. Le tiers réalisant le développement de l'outil peut être le tiers réalisant la vérification ou être indépendant.

Ces spécifications doivent notamment décrire :

- Le format de l'urne électronique et des bulletins.
- Le format des informations présentes sur la preuve de vote confiée à l'électeur.
- Les algorithmes cryptographiques utilisés pour générer les empreintes et signer les informations précédentes, ainsi que leurs paramètres, et le format de la signature.
- Le format de la clé publique de vérification de la signature des preuves de vote, et les modalités d'accès à cette clé.
- Le format de la page Web publiant les informations des bulletins dans l'urne (R63★★), et les modalités d'accès à cette page.

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

Pour aller plus loin

Cet objectif est complété par l'objectif 3.02 relatif à la vérifiabilité universelle, et renforcé par l'objectif 3.08 qui concerne la publication du code source du client de vote.

Objectif n° 2-08

Assurer sur le plan technique l'étanchéité totale entre l'identité des électeurs et les bulletins déchiffrés lors du dépouillement.

Cet objectif complète l'objectif 1.07 qui porte sur le même besoin central pour garantir le secret du vote : il doit être impossible de mettre en relation l'identité de l'électeur avec l'expression de son vote.

Pour attenter au secret du vote, il faut réussir 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.

Comme expliqué à l'objectif 1.07, les mesures consistant à rendre impossible ou très difficile l'association électeur/bulletin, comme celles consistant à ne pas horodater les bulletins dans l'urne ou bien à désactiver la génération de traces techniques du système de gestion de la base de données, ont un impact limité sur l'étanchéité, aussi seul un scrutin **de niveau 1** peut être envisagé avec un système de vote mettant en œuvre uniquement de telles mesures pour assurer l'étanchéité.

Les mesures consistant à rendre impossible ou très difficile l'association bulletin/suffrage, comme l'accumulation ou le mélange vérifiable, ont en revanche un impact avéré et prouvé sur l'étanchéité. L'organisateur du scrutin peut envisager **tous les niveaux de scrutin** avec un système de vote mettant en œuvre de telles mesures pour assurer l'étanchéité.

Protection de l'étanchéité bulletin/suffrage

En complément ou en remplacement de l'absence d'horodatage du bulletin, des mesures peuvent être prises pour assurer l'étanchéité entre le bulletin et le suffrage. Les premières mesures sont bien sûr l'utilisation d'un chiffrement robuste (1.04) et la protection de la clé privée de déchiffrement (1.08). Elles évitent qu'il soit possible de déchiffrer le bulletin en dehors du dépouillement légitime.

Mais ces mesures 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 vérifiable que d'éviter ce lien. Ces notions sont expliquées à l'Annexe A.

R65 ★★

Assurer l'étanchéité par accumulation ou mélange vérifiable des bulletins

Il est recommandé que le système de vote assure l'étanchéité entre l'identité du votant et l'expression de son vote par l'accumulation ou le mélange vérifiable des bulletins.

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

Par exemple, lorsque l'algorithme de chiffrement ElGamal est utilisé, composé avec des preuves à divulgation nulle de connaissance (voir les Annexes A, D et E) :

- En cas d'**accumulation**, chaque bulletin contient un ensemble de preuves de validité du bulletin, dont le contexte est éventuellement complété avec les attributs des électeurs en cas de **pastillage** (R21★). Ces preuves doivent être vérifiées avant l'accumulation et conservées.
- En cas de **mélange vérifiable**, chaque bulletin contient un ensemble de preuves 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** (R21★). Ces preuves doivent être vérifiées avant le mélange. Chaque mélangeur génère en plus une preuve à divulgation nulle de connaissance que le mélange de bulletins obtenu correspond bien au même ensemble de suffrages. Ces preuves doivent être vérifiées avant de procéder au dépouillement et conservées.

Dans certains cas, prouver la légitimité des bulletins (le fait que chaque bulletin a été généré par un électeur légitime) passera par l'officialisation du lien électeur/bulletin, par exemple par une signature électronique du bulletin par l'électeur.

Information

En fonction des conclusions de l'analyse de risque (R67★★★), si la preuve de légitimité est recherchée (voir par exemple la recommandation R30★★★+), le lien électeur/bulletin pourrait être officialisé au moyen d'une signature électronique et le secret du vote devra reposer entièrement sur l'absence de lien bulletin/suffrage. Pour ne pas reposer entièrement sur cette absence de lien, une solution à base de preuve à divulgation nulle de connaissance pourrait être envisagée [68].

Pour aller plus loin

L'objectif 2.08 est renforcé par le déchiffrement vérifiable (1.11) et la vérification de l'ensemble des preuves générées lors du dépouillement ainsi que la destruction des clés à l'issue du dépouillement (3.02).

Objectif n° 2-09

Favoriser la transparence de la solution de vote en publiant, en amont du scrutin, les spécifications techniques du protocole de vote.

Pour les scrutins de niveau 2, une première étape de transparence est demandée au prestataire qui doit rendre publique la spécification du protocole de vote utilisé ainsi que les propriétés de sécurité prétendument atteintes, ainsi que le modèle de sécurité 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.

Comme exposé à l'objectif 1.04, l'usage d'un protocole de vote non prouvé doit être évité. 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 à la sincérité du scrutin. Aussi le prestataire doit fournir les références correspondant au protocole qu'il met en œuvre. Des exemples de spécifications de protocoles de vote sont fournis dans [41, 81, 83, 95, 101].

R66 ★★

Publier les spécifications du protocole de vote

En amont du scrutin, le prestataire doit publier les spécifications du protocole de vote qu'il met en œuvre dans le système de vote. Ces spécifications doivent notamment comprendre :

- Les éventuelles références académiques sur lesquelles s'appuient 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.
- 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, les preuves à divulgation nulle de connaissance, les tests d'égalité). La description doit être aussi précise que possible pour chaque acteur.

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 [77]), sur la base des spécifications publiées. Un point de contact doit être identifié pour rendre possible la **divulgation responsable** [28] d'éventuelles faiblesses identifiées par les tiers.

4.3 Objectifs de sécurité de niveau 3

Définition de la CNIL [77] : **Niveau 3 (risques significatifs)** : *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 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, pour compromettre la sincérité du scrutin. Les recommandations de ce niveau complètent celles du niveau 2 et visent à renforcer l'intégrité du scrutin par un premier niveau de vérifiabilité universelle et le secret du vote par la gestion renforcée de la clé de déchiffrement des bulletins. La vérifiabilité individuelle, le contrôle par le bureau électoral, la disponibilité du système, l'authentification des électeurs et la transparence, initiés aux niveaux 1 et 2, sont également renforcés.

3-01	Effectuer une analyse de risque selon une méthode éprouvée afin de définir les mesures les plus adéquates au contexte spécifique de l'élection.
3-02	Assurer que le dépouillement de l'urne peut être vérifié a posteriori, y compris par un tiers. Mettre en place pour ce faire des méthodes n'impliquant pas un nouveau déchiffrement des urnes, par exemple en générant des preuves mathématiques démontrant l'exactitude du décompte des suffrages par rapport au contenu de l'urne.
3-03	Assurer une très haute disponibilité de la solution de vote en prenant en compte les risques d'avarie majeure.
3-04	Permettre le contrôle manuel par le bureau électoral de l'intégrité du système de vote pendant toute la durée du scrutin.
3-05	Authentifier les électeurs en s'assurant que la vraisemblance d'une usurpation d'identité est négligeable.
3-06	Assurer que le bureau électoral soit alerté de toute intervention de gestion et de maintenance sur le système de vote électronique et dispose d'un accès à un journal de ces alertes.
3-07	Renforcer la confidentialité des bulletins de vote en ne manipulant jamais le secret permettant leur dépouillement sur le serveur stockant les bulletins tels que déposés par les électeurs. À cette fin, le dépouillement peut par exemple être mis en œuvre sur un serveur tiers ne traitant que l'urne mélangée et le secret permettant son déchiffrement ou être mis en œuvre de manière décentralisée, sans que le secret permettant le déchiffrement des bulletins ne soit jamais rassemblé.
3-08	Favoriser la transparence de la solution de vote et la confiance des électeurs en publiant, en amont du scrutin, le code source du client de vote.

Tableau 4 – Objectifs 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.

Objectif n° 3-01

Effectuer une analyse de risque selon une méthode éprouvée afin de définir les mesures les plus adéquates au contexte spécifique de l'élection.

L'organisateur du scrutin peut réaliser une première estimation de la sensibilité de son scrutin avec la grille d'analyse fournie dans la recommandation de la CNIL [77]. 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.

R67 ★★★

Effectuer une analyse de risque selon la méthode EBIOS-RM

L'organisateur du scrutin doit effectuer une analyse de risque selon une méthode éprouvée, telle que la méthode EBIOS-RM [45], portant sur la solution de vote.

Cette analyse de risque doit notamment permettre de qualifier le risque de compromission du secret du vote et de la sincérité du scrutin à la suite d'une attaque interne au système de vote, par un attaquant disposant de ressources élevées. Les recommandations de niveau supérieur à 3 présentées dans ce guide peuvent permettre de répondre à ces risques :

- L'hébergement de la solution dans un Cloud de confiance ou dans un hébergement internalisé et sécurisé (2.05).
- La protection contre l'achat de vote et la cœrcition (Annexe C).
- La signature des bulletins avec une clé fournie à l'électeur par une entité indépendante de l'organisateur du scrutin et du prestataire (1.06, R30★★+★).
- La génération distribuée de la clé de déchiffrement des bulletins (3.07, R76★★+★, Annexe D).
- Le déchiffrement distribué des bulletins (3.07, R77★★+★, Annexe D).
- La mise en œuvre de la propriété de cast-as-intended (3.08).
- La mise en œuvre de la propriété de confidentialité persistante - *everlasting privacy* [84].
- La mise en œuvre d'algorithmes cryptographiques post-quantiques et de techniques d'hybridation [53, 55].

En fonction des risques, d'autres mesures pourront être mises en œuvre, notamment pour assurer un plus haut niveau de transparence.

Objectif n° 3-02

Assurer que le dépouillement de l'urne peut être vérifié a posteriori, y compris par un tiers. Mettre en place pour ce faire des méthodes n'impliquant pas un nouveau déchiffrement des urnes, par exemple en générant des preuves mathématiques démontrant l'exactitude du décompte des suffrages par rapport au contenu de l'urne.

Cet objectif renforce l'objectif 1.11. Il correspond à la propriété appelée **tallied-as-recorded**, qui constitue une partie de la **vérifiabilité universelle** : tout le monde doit pouvoir vérifier que le résultat proclamé correspond aux suffrages contenus dans les bulletins de l'urne.

La mise en œuvre de l'objectif repose sur :

- Les spécifications pour la vérifiabilité individuelle prévues à la recommandation R63★★ de l'objectif 2.07.
- Les spécifications du protocole de vote prévues à la recommandation R66★★ de l'objectif 2.08
- La fourniture des preuves mathématiques de bon déchiffrement évoquées aux recommandations R43★★ et R44★★ de l'objectif 1.11.
- Enfin, la **publication** de la spécification d'un outil permettant de vérifier ces preuves de bon déchiffrement (recommandation ci-dessous).

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 l'objectif 1.06.

R68 ★★★

Publier les spécifications d'un outil de vérifiabilité universelle

En amont du scrutin, le prestataire doit publier une spécification détaillant la constitution des preuves de déchiffrement 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. Cet outil doit permettre à un tiers disposant de l'urne électronique, non accumulée ou non mélangée, de réaliser les vérifications.

Le tiers réalisant le développement de l'outil peut être le tiers réalisant la vérification ou être indépendant.

Ces spécifications doivent notamment décrire :

- Les algorithmes utilisés pour chiffrer les bulletins, générer les preuves, ainsi que leurs paramètres.
- Le format de l'urne.
- Le format de la clé publique du scrutin.
- Le format des bulletins en clair et des bulletins chiffrés.
- Le format des preuves associées aux bulletins chiffrés.
- Le format du décompte (déchiffrement de l'urne).

- Le format des preuves de déchiffrement ou de mélange.
- La liste minimale des vérifications que doit effectuer un outil tiers afin de garantir la propriété de tallied-as-recorded.

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

Objectif n° 3-03

Assurer une très haute disponibilité de la solution de vote en prenant en compte les risques d'avarie majeure.

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. Pour couvrir ce risque, le système de vote peut être répliqué dans un second centre de données qui prend le relais.

R69 ★★★ 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.

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.

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

Permettre le contrôle manuel par le bureau électoral de l'intégrité du système de vote pendant toute la durée du scrutin.

Cet objectif renforce les objectifs 2.02 et 2.03. Il donne la possibilité au bureau électoral de déclencher manuellement et en autonomie un contrôle de l'intégrité sur le système de vote.

R70 ★★★

Permettre au bureau électoral de réaliser 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 2.03 :

- Contrôle de l'intégrité de l'application de vote (R38★).
- Contrôle de cohérence entre l'urne et la liste d'émargement décrit (R39★).
- Contrôle des scellements (R52★★).

Objectif n° 3-05

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

Cet objectif renforce l'objectif 1.03 en imposant un second facteur d'authentification, en plus de celui spécifique au scrutin requis par la R10★. Ce second facteur peut être lui aussi spécifique au scrutin, ou bien relever d'une solution d'authentification existante, externe à la solution de vote.

R71 ★★★

Combiner deux secrets d'authentification dont un spécifique au scrutin

Le système de vote doit combiner deux secrets d'authentification, dont un spécifique au scrutin. Les deux cas suivants sont possibles :

- Générer deux secrets spécifiques au scrutin et les envoyer par deux canaux différents.
- Authentifier l'électeur par une solution d'authentification existante et indépendante du scrutin et, en complément, utiliser un secret d'authentification spécifique au scrutin.

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

- Elle renforce la sécurité de l'authentification sans la complexifier par la manipulation d'un nouveau secret.
- Elle évite la génération et l'envoi à l'électeur d'un second 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 offrir des garanties suffisantes.

R72 ★★★

Utiliser une solution d'authentification existante présentant des garanties suffisantes

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

- Elle est disponible pour tous les électeurs. 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.

Objectif n° 3-06

Assurer que le bureau électoral soit alerté de toute intervention de gestion et de maintenance sur le système de vote électronique et dispose d'un accès à un journal de ces alertes.

Cet objectif renforce l'objectif 2.04 qui permet au bureau électoral d'être alerté en cas de détection de rupture d'intégrité ou d'incident sur le système de vote. Pour le niveau 3, le bureau électoral doit également être alerté en cas d'intervention du prestataire sur le système de vote.

R73 ★★★

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

Le prestataire doit mettre en œuvre un dispositif d'alerte 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 dispositif d'alerte doit également générer une alerte automatique vers le bureau électoral.

Objectif n° 3-07

Renforcer la confidentialité des bulletins de vote en ne manipulant jamais le secret permettant leur dépouillement sur le serveur stockant les bulletins tels que déposés par les électeurs. À cette fin, le dépouillement peut par exemple être mis en œuvre sur un serveur tiers ne traitant que l'urne mélangée et le secret permettant son déchiffrement ou être mis en œuvre de manière décentralisée, sans que le secret permettant le déchiffrement des bulletins ne soit jamais rassemblé.

Cet objectif renforce l'objectif 1.08 en séparant à tout moment les bulletins de vote (tant qu'ils sont non mélangés et non accumulés) de la clé de déchiffrement de ces bulletins. Cela offre une garantie supplémentaire pour assurer le secret du suffrage (cf. 2.08) car les bulletins non mélangés ou non accumulés ne seront pas déchiffrés illégitimement.

Pour mettre en œuvre cet objectif, la clé de déchiffrement ne doit être ni générée, ni reconstituée sur le serveur qui stocke les bulletins non mélangés et non accumulés. La génération de la clé et son utilisation pour le déchiffrement peuvent être déportées sur un poste client unique utilisé pendant les cérémonies, être distribuées sur plusieurs postes clients, ou enfin être réalisées sur un serveur indépendant, dédié à ces opérations.

R74 ★★★

Dissocier la clé privée de déchiffrement des bulletins non mélangés ou non accumulés

Le système de vote doit être conçu pour dissocier strictement les bulletins non mélangés ou non accumulés de la clé de déchiffrement de ces bulletins.

La génération de la clé de déchiffrement et l'utilisation de la clé pour déchiffrer les bulletins (une fois mélangés ou accumulés) doivent être réalisées hors du serveur 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 E, en particulier la partie relative aux preuves de déchiffrement correct).

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 devront 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 sera nécessaire de réaliser le déchiffrement sur une machine ayant les capacités de calcul d'un serveur équivalent à ceux utilisés pour le mélange.

Les sections suivantes proposent 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 pourront être mises en œuvre si l'analyse de risque (R67★★★) conclut sur le besoin de renforcer la confidentialité de la clé de déchiffrement, ou si le déport des traitements sur un navigateur n'est pas compatible avec les contraintes du scrutin.

Génération hors ligne de la clé de 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 de déchiffrement. Sa position hors ligne, déconnectée d'Internet, le rend plus difficile à compromettre par un acteur malveillant.

Cependant, cette architecture complexifie aussi la cérémonie de dépouillement, 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.

R75 ★★★+

Réaliser les opérations impliquant la clé de déchiffrement sur une machine dédiée hors ligne

En fonction des conclusions de l'analyse de risque (R67★★★), il est recommandé que le système de vote utilise une machine hors ligne dédiée aux opérations impliquant la clé de déchiffrement des bulletins, à savoir la génération des fragments de cette clé (R32★) et le déchiffrement des bulletins (R43★★).

Enfin, même si elle renforce la protection de la clé 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'expertise indépendante, cette expertise repose *in fine* sur un certain niveau de confiance dans l'application de vote et les serveurs utilisés, aussi la compromission de la clé de l'élection est toujours possible car celle-ci est calculable à partir des fragments de clés qui sont centralisés sur une même machine. Si ce risque n'est pas acceptable, la génération de clé ainsi que le déchiffrement distribués devront être envisagés.

Génération distribuée de la clé de déchiffrement

Si le risque de compromission de la clé de déchiffrement par le système de vote n'est pas acceptable, il est nécessaire de renforcer la génération de la clé et son usage pour le dépouillement. Une solution consiste à réaliser une génération de clé ainsi qu'un déchiffrement distribués, tels que décrits en Annexe D. Ces recommandations sont de niveau supérieur au niveau 3 de la délibération de la CNIL car leur mise en œuvre est difficile.

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 chiffrement des bulletins, sans avoir à regrouper les clés privées de chaque attributaire. Ainsi, les fragments de la clé privée de déchiffrement ne sont jamais regroupés sur un même dispositif, contrairement aux architectures précédentes. L'Annexe D fournit des exemples de générations de clé distribuées adaptées à l'algorithme de chiffrement ElGamal.

Des mécanismes de génération distribués de la clé de déchiffrement s'appuyant sur un partage de secret vérifiable sont décrits dans [38, 65, 69, 81]. Ces mécanismes de génération sont délicats à mettre en œuvre car, pour que les garanties de sécurité qu'ils apportent soient effectives, ils peuvent nécessiter que les dispositifs sur lesquels la génération des clés 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. L'utilisation de matériel disposant d'une enclave sécurisée peut fournir une réponse à ces contraintes [64].

R76 ★★ ★+

Générer la clé de déchiffrement de manière distribuée

En fonction des conclusions de l'analyse de risque (R67★★★), il est recommandé que le système de vote mette en œuvre une génération distribuée du bi-clé de chiffrement / déchiffrement des bulletins. Cette génération doit assurer que les fragments de la clé privée de déchiffrement ne sont jamais présentes sur le même dispositif.

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 le niveau de sécurité obtenu avec la génération de clé distribuée, le dépouillement des bulletins ne doit pas non plus s'appuyer sur une reconstitution de la clé privée de déchiffrement.

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 que le résultat du déchiffrement partiel correspond bien aux bulletins (1.11). L'ensemble des déchiffrements 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 dispositifs sur lesquels les déchiffrements partiels s'effectuent ne soient pas sous le contrôle de l'organisateur du scrutin ni du prestataire.

R77 ★★ ★+

Utiliser un déchiffrement vérifiable distribué

En fonction des conclusions de l'analyse de risque (R67★★★), 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 de déchiffrement réalisent chacun un déchiffrement partiel, assurant que la clé privée de déchiffrement n'a jamais besoin d'être explicitement reconstituée. Chaque déchiffrement partiel doit générer une preuve à divulgation nulle de connaissance que le résultat du déchiffrement correspond bien aux bulletins issus de l'urne.

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.

Objectif n° 3-08

Favoriser la transparence de la solution de vote et la confiance des électeurs en publiant, en amont du scrutin, le code source du client de vote.

Cet objectif renforce les objectifs 1.04 et 2.07. Il constitue une partie de la **vérifiabilité individuelle** : il est possible de constater que le client de vote fourni à l'électeur correspond à un client de vote dont le code non offusqué a été rendu public. Cela fournit un premier niveau d'assurance que le client de vote respecte bien l'intention de l'électeur.

La propriété idéale (et qui n'est *pas atteinte* par l'objectif 3.08) est la propriété appelée **cast-as-intended**. Cette propriété fait l'objet de recherche active : idéalement, il faudrait que l'électeur puisse se convaincre en autonomie que le bulletin généré par le client de vote respecte bien son intention. Historiquement le mécanisme appelé Challenge de Benaloh [63] a été proposé, mais sa mise en œuvre pratique est délicate [87].

R78 ★★★

Publier le code source du client de vote

En amont du scrutin, le prestataire doit publier le code source du client de vote utilisé par les électeurs. 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.

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.

Comme évoqué dans [70], la publication du code source du client de vote peut être facilitée par l'utilisation d'application monopage [35].

Liste des recommandations

Glossaire

Accumulation : mécanisme consistant à calculer le chiffrement de la somme des suffrages en additionnant (ou multipliant suivant les cas) les bulletins entre eux. Ce mécanisme nécessite l'utilisation d'un chiffrement additivement homomorphe (2.08, Annexe A).
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 (1.03).
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 [16].
Application de vote : logiciel installé sur le serveur de vote traitant les bulletins transmis par les électeurs.
Atomique : qui ne peut être coupé, indivisible (1.02).
Authentification : processus consistant à vérifier la preuve d'une identité précédemment annoncée grâce à un moyen d'authentification [7, 58]. Dans le contexte d'un scrutin, processus permettant de vérifier l'identité et la légitimité d'un électeur (1.03, 3.05).
Bulletin : donnée contenant le suffrage de l'électeur chiffré. Cette notion correspond à la notion d'enveloppe dans le vote à l'urne.
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.
Bureau électoral : entité responsable du contrôle des opérations de vote par voie électronique.
Cachet : signature numérique.
CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) : test automatisé permettant de différentier un utilisateur humain d'un ordinateur (1.03). Mesure de protection visant notamment à limiter les attaques par force brute automatisées.
Cast-as-intended (vérifiabilité de l'intention) : propriété faisant partie de vérifiabilité individuelle qui signifie que l'électeur doit pouvoir vérifier que son bulletin contient bien l'expression de son vote (3.08).
Chaînage : mécanisme cryptographique utilisant des signatures ou des empreintes numériques liant entre eux des ensembles de données et permettant de détecter leur modification (1.06).
Chiffrement : mécanisme cryptographique [49] permettant d'assurer la confidentialité d'une donnée (1.04).
Chiffrement asymétrique : chiffrement consistant à chiffrer une donnée avec une clé publique et la déchiffrer avec une clé privée (1.04).
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 (1.04).
Chiffrement probabiliste : chiffrement utilisant un aléa permettant de différentier le chiffré de deux données identiques (1.04).
Clé privée de l'élection : lorsque le chiffrement du suffrage est réalisé par un algorithme de chiffrement asymétrique, une paire de clé publique/privée est générée et la partie privée est utilisée pour réaliser le dépouillement. La clé privée est alors appelée clé privée de l'élection.
Clé publique de l'élection : lorsque le chiffrement du suffrage est réalisé par un algorithme 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.
Client de vote : partie logicielle du système de vote exécutée sur le dispositif de vote pour permettre à l'électeur d'exprimer son vote. En général, application JavaScript exécutée dans un navigateur (1.04).
Configuration de l'élection : ensemble des données caractérisant une élection (notamment : dates d'ouverture et de clôture, liste électorale, liste des candidats, découpage électoral, pastillage, données de vérification de l'authentification des électeurs, clé publique de chiffrement des suffrages).
CPU (Central Processing Unit) : processeur d'un ordinateur.
CSE : Comité Social Économique [23].
CVE (Common Vulnerabilities and Exposures) : programme d'identification, de qualification et de publication de vulnérabilités informatiques [6].
CVSS (Common Vulnerability Scoring System) : méthode permettant de qualifier le niveau de sévérité d'une vulnérabilité [39].
Dispositif de vote : équipement personnel de l'électeur que ce dernier utilise pour voter. Exemples : ordinateur personnel, téléphone multifonction, tablette.
Dépouillement : opération intervenant après l'accumulation ou le mélange vérifiable des bulletins, au cours de laquelle la clé de déchiffrement de l'élection (éventuellement fragmentée) est utilisée pour déchiffrer les bulletins et obtenir le résultat de l'élection.
Dérivation : mécanisme cryptographique [49] permettant de calculer une ou plusieurs clés à partir d'un secret maître.
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 [28].
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.
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. [45].
Élection : choix exprimé au travers d'un vote.
ElGamal : algorithme de chiffrement asymétrique [73], 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 (1.04, Annexe D).
Éligibilité (des candidats) : aptitude à être élu.
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.
Empreinte : donnée calculée au moyen d'une fonction de hachage cryptographique (1.06).
Entropie : mesure de la quantité d'aléa contenu dans un système, une application ou une information.
Enveloppe : dans le cas du vote à l'urne, les bulletins sont mis dans une enveloppe opaque, qui est déposée par l'électeur dans l'urne.
ETag : Entity Tag [10].
Everlasting Privacy : Propriété signifiant que le secret du vote 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 [84].
Expert indépendant : entité réalisant pour le compte de l'organisateur du scrutin le contrôle de la conformité de la solution de vote à la recommandation de la CNIL [77].
Fonction de hachage : mécanisme cryptographique [49] permettant de calculer une donnée unique de petite taille à partir de toute donnée, fournissant les propriétés de résistance aux collisions (1.06).
HTTP : Hyper Text Transfer Protocol.
HTTPS : Hyper Text Transfer Protocol Secure.
IND-CPA : INDistinguishability under Chosen Plaintext Attack [60].
INSEE : Institut national de la statistique et des études économiques.
JavaScript : langage de programmation permettant la mise en œuvre de mécanismes complexes dans une page Web [17].
Journalisation : collecte des journaux d'évènements [54].
Latéralisation : accès à des systèmes tiers depuis un système compromis (2.05).
Légitimité (des électeurs) : désigne le fait que les électeurs sont bien inscrits sur les listes électorales (1.03).
Liste électorale : liste des électeurs pouvant participer à un vote.
Liste d'émargement : liste des électeurs ayant participé à un vote.
Malléabilité (du chiffrement) : propriété d'un algorithme de chiffrement permettant d'effectuer des opérations sur les données chiffrées pour obtenir le chiffrement d'autres données que celles initialement chiffrées (Annexe D).
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.
Mécanisme d'authentification : moyen permettant de générer, transmettre ou vérifier les secrets d'authentification (1.03).
Mélange vérifiable : mécanisme cryptographique permettant de vérifier qu'un mélange d'un ensemble de bulletins correspond au même ensemble de suffrages (2.08, Annexe A).
Mix-Net (réseau de mélangeurs) : mécanisme cryptographique permettant de réaliser un mélange vérifiable (2.08, Annexe A).
Modèle de confiance : description des hypothèses sur lesquelles s'appuie la sécurité d'un système de vote.
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 [58] (1.03).
NM-CPA : Non-Malleability under Chosen Plaintext Attack [60, 72].
OAEP (Optimal Asymmetric Encryption Padding) : mécanisme d'encapsulation adapté à l'algorithme de chiffrement RSA [62].
Offuscation (ou obscurcissement ou *obfuscation*, en anglais) du code source : technique qui vise à rendre difficile l'interprétation d'un programme, par exemple pour protéger la propriété intellectuelle (secret industriel) associée (3.08).
OTP (One Time Password) : est un code à usage unique utilisé pour une authentification. (1.03).
Organisateur du scrutin : entité responsable de l'organisation et de la sincérité du scrutin. La recommandation de la CNIL [77] fait référence aux organisateurs de scrutin en tant que responsables de traitement.

OWASP (Open Web Application Security Project) : fondation à but non lucratif dédiée à la sécurité des applications Web (2.06).
PASSI : prestataire d'audit de la sécurité des systèmes d'information [57] (1.01).
Pastillage : association d'attributs à un électeur, qui doivent suivre l'expression de son vote (1.04, Annexe B).
PDMA : Perte de Données Maximale Admissible (1.06, 3.03).
Période de vote : période pendant laquelle les électeurs peuvent voter.
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 (1.08).
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 [61, 71, 79, 88] (Annexe E). Dans le contexte du vote par correspondance électronique, les preuves à divulgation nulle de connaissance concernent notamment le fait qu'un bulletin est bien le chiffrement d'un suffrage légitime (sans révéler ce suffrage) ou le fait qu'un déchiffrement est réalisé avec la clé privée correspondant à une clé publique de chiffrement (sans révéler la clé de déchiffrement).
Preuve de vote : information anonyme et non horodaté, généré par le client de vote, contenant une référence du bulletin de vote. La preuve de vote permet à l'électeur de vérifier la présence de son bulletin dans l'urne (2.07). Cette information est distincte de celle fournie par le récépissé de vote, qui contient l'heure de dépôt du bulletin dans l'urne.
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 (2.08).
RAM (Random Access Memory) : composant d'un ordinateur stockant les données de manière temporaire pour un accès plus rapide.
Récépissé de vote : information transmise aux électeurs à la fin de la transaction de vote, contenant l'heure de dépôt du bulletin dans l'urne (1.01). Cette information est distincte de celle fournie par la preuve de vote, anonyme et non horodatée, qui référence le bulletin (2.08).
Receipt-freeness : propriété d'un système de vote qui signifie que les données publiées par le système de vote ne permettent pas de compromettre le secret du vote.
Recorded As Cast (présence dans l'urne) : propriété faisant partie de vérifiabilité individuelle qui signifie que l'électeur doit pouvoir vérifier que son bulletin est bien présent dans l'urne (2.07).
Recouvrement (de secret d'authentification) : désigne à la fois la récupération de secret d'authentification et son masquage par un dispositif physique opaque lorsque ce secret est imprimé pour sa transmission par courrier postal (1.03).
Redondance : duplication de données et de composants techniques matériels pour en assurer la disponibilité en évitant les pannes.
Réplication : copie et stockage de données sur un système primaire et un système secondaire. La réplication est synchrone lorsque les données sont écrites sur le système secondaire en même temps que le système primaire et l'acquittement d'écriture est réalisé à la fin de l'écriture sur les deux systèmes. La réplication est asynchrone lorsque les données sont écrites sur le système secondaire à l'issue de leur écriture sur le système primaire, cette seconde écriture pouvant être planifiée pour être périodique (2.01, 3.03).
Responsable de traitement : personne morale (entreprise, commune, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser [32]. La recommandation de la CNIL [77] fait référence aux organisateurs de scrutin en tant que responsables de traitement.
REU : Répertoire électoral unique [21].

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.
RGPD : Règlement Général sur la Protection des Données [20].
RGS : Référentiel Général de Sécurité [56].
RSA (Rivest Shamir Adleman) : algorithme de chiffrement asymétrique [49, 97] dont la sécurité repose sur la difficulté de résoudre le problème de la factorisation d'entiers de grande taille (1.04).
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 (2.02).
Scrutin : ensemble des opérations constituant un vote.
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 (1.03).
Serveur de vote : partie centralisée du système de vote. Elle est au moins en partie exposée sur Internet pour recueillir les votes des électeurs.
Signature numérique : mécanisme cryptographique [49] permettant de détecter la modification d'une donnée et d'assurer son authenticité (1.06).
Sincérité du scrutin : propriété exprimant que le scrutin a respecté les principes fondamentaux du vote, à savoir que le suffrage est universel, égal et secret [19].
Solution de vote : comprend le système de vote ainsi que ses procédures d'exploitation et de sécurisation.
SQL (Structured Query Language) : langage d'interrogation et de manipulation de base de données [36].
Suffrage : expression du vote de l'électeur, c'est-à-dire le choix de cet électeur parmi les propositions soumises au vote (candidat(s), liste(s), réponse à une question, etc.). Le suffrage chiffré est contenu dans le bulletin.
Système de vote : ensemble des moyens physiques (matériels) et logiques (logiciels) utilisés pour le vote électronique.
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 (3.02).
TLS (Transport Layer Security) : protocole cryptographique [47] assurant la confidentialité et l'intégrité des données, l'authentification des participants et la protection contre le rejeu (1.05).
TPE (Élection syndicale) : élection syndicale des salariés des très petites entreprises et des employés à domicile [9].
Urne électronique : dispositif technique (i.e. base de donnée, fichier, etc.) assurant le stockage des bulletins.
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 (1.06, 3.02).
Vérifiabilité individuelle : propriété d'un système de vote signifiant que tout électeur est en mesure de vérifier que son bulletin a été décompté. Cette propriété se décline en deux propriétés : « Cast As Intended » et « Recorded As Cast » (2.07, 3.08).
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 candidat) correspond au contenu de l'urne. Cette propriété se décline en deux propriétés : « Tallied As Recorded » et « vérifiabilité de la légitimité » (3.02).
Vote par correspondance électronique : mode de scrutin dans lequel l'électeur exprime son vote au moyen de matériel de vote dématérialisé et transmet son bulletin par voie électronique.

Annexe A
Accumulation et 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 sincérité des scrutins. Elle fournit des explications sur les notions d'accumulation et de mélange vérifiable.

L'accumulation et le mélange vérifiable sont les deux mécanismes mentionnés dans ce guide pour assurer l'étanchéité entre l'identité du votant et l'expression de son vote, c'est à dire le contenu déchiffré de son bulletin de vote (1.07, 2.08). **Ces mécanismes sont requis pour les scrutins de niveau 2 et 3**.

Accumulation des bulletins

Ce mécanisme est adapté lorsque les suffrages sont chiffrés avec un algorithme de chiffrement asymétrique **additivement homomorphe**, ce qui est le cas lorsque l'algorithme de chiffrement ElGamal avec le codage exponentiel (Annexe D) est utilisé pour le chiffrement du suffrage. L'accumulation est la première opération réalisée avec l'ensemble des bulletins, c'est à dire le produit de l'ensemble des chiffrés correspondant à chaque option d'un vote.

Information

L'accumulation ne nécessite pas la clé de déchiffrement, elle peut donc être réalisée sur le serveur contenant l'urne électronique (3.07), le résultat de l'accumulation pouvant ensuite être déporté de ce serveur.

Comme les bulletins ne sont pas individuellement déchiffrés (et donc le suffrage qu'ils contiennent n'est pas individuellement vérifié), il est nécessaire de vérifier leur validité avant de les accumuler. 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. Par exemple, lorsque l'algorithme de chiffrement ElGamal à codage exponentiel est utilisé, cela signifie que pour cette option, le message chiffré est g^a, avec $a > 1$ au lieu de g^1.
- Un bulletin contenant plus (ou moins) d'options que le nombre prévu par la configuration de l'élection. Par exemple, lorsque l'algorithme de chiffrement ElGamal à codage exponentiel est utilisé, avec les notations de l'Annexe D, cela signifie que la liste des chiffrés générée par le client de vote, $(\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots, (\alpha_M, \beta_M)$, contient un nombre de chiffrés du message g^1 strictement inférieur ou strictement supérieur à celui prévu par la configuration de l'élection.

Pour éviter cela, le bulletin de vote est associé à deux types de **preuves à divulgation nulle de connaissance**, décrites en Annexe E :

- Chaque chiffré ElGamal contenu dans la liste fournie par l'électeur est associé à une preuve qu'il correspond à une option sélectionnée (g^1) ou non sélectionnée (g^0).

- Chaque liste de chiffrés ElGamal fournie par l'électeur est associée une preuve que le nombre d'options sélectionnées est correct et conforme à la configuration de l'élection.

Comme expliqué en Annexe E, la vérification de ces preuves peut être réalisée directement avec le bulletin. Des exemples de systèmes de vote mettant en œuvre le mécanisme d'accumulation basé sur l'algorithme de chiffrement ElGamal sont décrits dans [14, 65, 81].

Mélange vérifiable des bulletins

Lorsque la configuration de l'élection est complexe (typiquement lorsque le nombre d'options proposées aux électeurs est élevé, par exemple dans le cas du vote avec rature [18]), les preuves à divulgation nulle de connaissance nécessaires pour l'accumulation des bulletins peuvent être difficiles à mettre en œuvre (si par exemple le nombre de preuves à calculer est linéaire en le nombre de choix proposés à l'électeur, ce qui est le cas pour les preuves présentées en Annexe E). Dans ce cas, il est nécessaire soit d'adapter les preuves pour continuer à utiliser l'accumulation des bulletins, soit basculer sur un autre mécanisme que l'accumulation pour assurer l'étanchéité bulletin/suffrage.

Le mélange vérifiable utilise un mécanisme cryptographique appelé Mix-Net (ou réseau de mélangeurs), adapté à l'algorithme de chiffrement utilisé. Dans le cas de l'algorithme de chiffrement ElGamal, ce mécanisme peut ainsi être utilisé lorsque le chiffrement classique est utilisé pour chiffrer le suffrage, tel que présenté en Annexe D. Dans ce cas, il est recommandé de composer le chiffré ElGamal à une preuve à divulgation nulle de connaissance de l'aléa utilisé pour réaliser le chiffrement, par exemple celle que décrite en Annexe E. La vérification de cette preuve doit être effectuée avant de réaliser le mélange.

Il y a classiquement deux types de mélange, le mélange par **déchiffrement** et le mélange par **rechiffrement**. Dans le premier cas, chaque mélangeur effectue une partie du déchiffrement, qui est donc complètement réalisé à l'issue du 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.

Chaque opération réalisée au niveau d'un mélangeur est un mécanisme probabiliste qui modifie les bulletins, aussi il est nécessaire que chaque mélangeur produise une **preuve à divulgation nulle de connaissance** que l'ensemble des bulletins mélangés contient exactement le même ensemble de suffrages chiffrés 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 [85]. Enfin, la réalisation du mélange peut nécessiter des délais importants incompatibles avec leur tenue au cours d'une cérémonie publique de dépouillement dès la clôture du scrutin (1.09).

Des exemples de systèmes de vote mettant en œuvre un mélange vérifiable basé sur l'algorithme de chiffrement ElGamal sont décrits dans [38, 81, 83, 100, 101, 102].

18. Le vote avec rature est explicitement autorisé pour l'élection de la délégation du personnel au comité social économique (CSE) [23].

Annexe B
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 sincérité 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 de l'élection ou aux candidats (représentativité 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 conseiller 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 oeuvre du pastillage consiste en l'association d'attributs à un électeur, qui doivent suivre son bulletin de vote. 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 expressions de vote, mais sur un sous-ensemble des bulletins qui disposent d'un ou plusieurs d'attributs donnés, correspondant au scrutin indirect. Il est important de ne pas pouvoir générer d'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 vote.

Exemple

Dans l'exemple précédent, cela signifie qu'il doit être impossible de générer un scrutin indirect informatif donnant les résultats pour les actifs et les retraités *au niveau d'un quartier*.

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*. Les attributs ne sont pas reproduits sur le bulletin (c'est à dire le chiffrement du suffrage). Dans ce cas, il n'existe qu'une seule urne, correspondant au scrutin direct, qui est dépouillée. Le déchiffrement des bulletins doit être individualisé, il n'y a pas d'accumulation possible. Après le déchiffrement, il est possible de sélectionner l'ensemble des suffrages associées aux attributs afin d'obtenir les résultats des scrutins indirects.

Attention

Cette solution comporte un risque majeur sur le secret du vote. En effet, même si au final un seul attribut est utilisé pour produire chaque résultat partiel, chaque expression de vote est liée à une liste d'attributs et cette liaison persiste sur le suffrage quel que soit le mélange effectué sur les bulletins. Cela implique que lorsque la liste contient beaucoup d'attributs, il est possible de retrouver le lien suffrage/électeur : le secret du vote peut être compromis. Aussi cette solution doit être limitée au niveau 1.

Une seconde mise en œuvre possible du pastillage consiste à *ne pas* associer les attributs au suffrage mais à les reproduire en clair sur le bulletin (le chiffrement du suffrage). Dans ce cas il y a une urne correspondant au scrutin direct et autant d'urnes qu'il y a de scrutins indirects, pour autant il y a bien 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. Dans cette situation, le pastillage n'est *pas* un obstacle à la mise en place de l'étanchéité bulletin/suffrage via à l'accumulation des bulletins (1.07, 2.08). Le contexte des preuves à divulgation nulle de connaissance déjà existantes nécessaires pour l'accumulation peut être complété avec les attributs des électeurs, afin de lier sans ambiguïté les bulletins aux urnes des scrutins indirects. Ces preuves permettant de détecter un éventuel déplacement de bulletin qui porterait atteinte au secret du vote [70], aussi elles doivent être vérifiées avant le dépôt du bulletin dans chaque urne et avant l'accumulation de chaque urne.

Si l'accumulation des bulletins n'est pas mise en œuvre et que l'étanchéité entre l'identité du votant et l'expression de son vote est assurée par un mélange vérifiable (1.07, 2.08), le bulletin contient au minimum une preuve de connaissance de l'aléa utilisé pour chiffrer le suffrage : le contexte de la preuve peut être complété avec les attributs des électeurs. Comme dans le cas précédent, 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 (R21★).

Dans les deux cas (accumulation ou mélange vérifiable), les bulletins sont déchiffrés dans des urnes dédiées, chacune correspondant à un ensemble d'attributs définissant un scrutin indirect. Si chaque bulletin (contenant l'expression de vote chiffrée) est lié à une combinaison d'attributs, au final l'expression du vote ne sera pas liée à cette combinaison mais sera additionnée à l'ensemble des expressions du même scrutin indirect : **il est impossible d'obtenir un résultat partiel non souhaité sauf à modifier la configuration de l'élection**, aussi la présentation du pastillage à l'électeur et sa vérification par l'électeur sont essentielles.

Annexe C
Receipt-freeness, protection contre l'achat de vote et résistance à la cœrcition

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 sincérité des scrutins. Elle fournit des explications sur les notions de receipt-freeness, de protection contre l'achat de vote et de résistance à la cœrcition.

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 cœrcition sont de niveau **supérieur au niveau 3 de la CNIL** : elles sont envisageables en fonction de l'analyse de risque (3.01).

La protection contre l'achat de vote et la résistance à la cœrcition sont des domaines de recherche actifs. Une propriété minimale importante, appelée **receipt-freeness** [66] est issue des travaux académiques. Cette propriété signifie (informellement) que le système de vote ne permet pas à un électeur ne sauvegardant que les données transmises et publiées par ce système de *prouver comment il a voté* à un tiers ayant également accès aux données émises par le système de vote. Suivant le tiers, les données auxquelles il a accès peuvent être différentes.

Information

La propriété receipt-freeness ne signifie *pas* « sans reçu », c'est à dire « sans récépissé » ou « sans preuve de vote » : la propriété receipt-freeness est bien compatible avec la fourniture de récépissé et/ou de preuve de vote.

Ainsi, il est important (et possible) de mettre en œuvre cette propriété, valable pour tous les niveaux de scrutins, en s'assurant que le récépissé, la preuve de vote ainsi que les affichages réalisés par le client de vote à l'électeur ne contiennent pas de données qui *seules* permettent de compromettre le secret du vote (par exemple, ces données ne doivent pas contenir le suffrage en clair ou contenir la clé de déchiffrement des bulletins, ou bien le client de vote ne doit pas afficher à l'électeur l'aléa généré pour chiffrer le bulletin).

La protection contre l'**achat de vote** est une propriété plus forte que la propriété receipt-freeness : l'électeur est considéré capable d'effectuer des manipulations, par exemple d'extraire des données intervenant dans la constitution de son bulletin de vote et de s'en servir pour prouver son vote au moyen des données publiées par le système de vote. Ainsi, l'électeur pourrait utiliser les informations contenues dans la preuve de vote et publiées afin de réaliser la vérifiabilité individuelle

(R63★★). L'électeur qui arriverait à extraire et conserver l'aléa utilisé pour le chiffrement du bulletin pourrait utiliser la preuve de vote pour prouver son suffrage si par exemple les données publiées sont une liste des empreintes des bulletins. Pour assurer la protection contre l'achat de vote, les données publiées devraient dépendre d'un secret non connu de l'électeur, tout en assurant la propriété de vérifiabilité individuelle : l'électeur ayant conservé l'aléa ne pourrait plus l'utiliser pour prouver son suffrage. En conséquence, une protection contre l'achat de vote est de niveau supérieur au niveau 3 de la CNIL car la mise en œuvre d'une telle protection est difficile : elle est envisageable en fonction de l'analyse de risque (3.01).

Enfin, la **résistance à la cœrcition** est une propriété plus forte que la protection contre l'achat de vote : l'électeur peut être contraint pendant une partie de la procédure de vote. Cette propriété est de niveau supérieur au niveau 3 de la CNIL et est envisageable en fonction de l'analyse de risque (3.01).

Annexe D
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 sincérité des scrutins. Elle fournit des explications sur la mise en œuvre de l'algorithme de chiffrement ElGamal.

Cette annexe présente deux versions de l'algorithme ElGamal : à codage classique (adapté au mélange des bulletins), à codage exponentiel (adapté à l'accumulation des bulletins), déclinées selon les critères suivants : centralisé ou distribué, avec ou sans seuil, vérifiable ou non.

Attention

L'algorithme de chiffrement ElGamal *seul* (à codage classique ou exponentiel) n'assure *pas* le secret du suffrage car il est **malléable** : il n'atteint que la propriété **IND-CPA** [60] et cette propriété est insuffisante. Des attaques exploitant la malléabilité de l'algorithme de chiffrement ElGamal pour porter atteinte au secret du vote sont par exemple décrites dans [89] et doivent être prises en compte pour **les scrutins de tous les niveaux**.

L'algorithme de génération de clé (identique pour les codages classique ou exponentiel), peut être décliné de manière centralisé ou distribuée, avec ou sans seuil (R32★). Ce mécanisme *seul* n'assure *pas* le secret du suffrage en cas de compromission de l'application de vote (une attaque directe est par exemple décrite dans décrite dans [86]), ce qui est envisageable **pour les scrutins de niveau 2 ou 3**.

Toutes les versions (à codage classique ou exponentiel, centralisé, distribué) de l'algorithme de déchiffrement n'assurent pas *seules* que le déchiffrement des bulletins respecte le suffrage des électeurs (et donc n'assurent pas *seules* l'intégrité du résultat) en cas de compromission de l'application de vote (une attaque directe est par exemple décrite dans [86]) , ce qui est envisageable **pour les scrutins de niveau 2 ou 3**.

En conséquence, il est nécessaire d'adapter l'algorithme ElGamal aux étapes de génération de la clé, de chiffrement et de déchiffrement afin que la sincérité du scrutin soit assurée :

- Une première adaptation consiste à composer la génération de clé (centralisée ou distribuée, avec ou sans seuil) avec une preuve de connaissance de clé privée. Cette preuve permet d'attester de la sincérité de la génération de la clé et au final assure le secret du suffrage.
- Une seconde adaptation consiste à composer le chiffrement du suffrage avec une preuve de connaissance de l'aléa utilisé lors du chiffrement du suffrage. Cette association empêche d'exploiter la malléabilité et permet d'atteindre la propriété de sécurité **NM-CPA** [60, 72], qui assure le secret du suffrage.

- Une troisième adaptation consiste à composer le déchiffrement (centralisé ou distribué, avec ou sans seuil) des bulletins avec une preuve de déchiffrement correct. Cette preuve permet d'attester de la sincérité du déchiffrement et au final assure l'intégrité du résultat.

Des exemples classiques [67] de preuves compatibles avec l'algorithme ElGamal sont présentées en Annexe E.

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 $\mathbb{G}$.

Chiffrement ElGamal à codage classique

Les algorithmes 1, 2 et 3 décrivent l'algorithme ElGamal à codage classique. Ces algorithmes sont adaptés au mélange vérifiable mais pas à l'accumulation des bulletins.

Attention

Ces algorithmes ne doivent pas être utilisés seuls et doivent être composés avec une preuve de connaissance de l'aléa (pour tous les niveaux de scrutin) et avec une preuve de connaissance de la clé privée (pour les scrutins de niveau 2 et 3), par exemple celles fournies à l'Annexe E.

Algorithme 1 : Génération de clé ElGamal à codage classique

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).

Algorithme 2 : Chiffrement ElGamal à codage classique

Entrée : g, q, K, m (générateur de groupe, ordre du groupe, clé publique, message à chiffrer)
Sortie : (α, β) (chiffré)

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

Algorithme 3 : Déchiffrement ElGamal à codage classique

Entrée : k, (α, β) (clé privée, chiffré)
Sortie : m (message en clair)

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

Ainsi l'algorithme de chiffrement ElGamal à codage classique founit un homomorphisme *multiplicatif* : si l'on considère deux chiffrés ElGamal de deux messages m_1 et m_2 avec la même clé publique K, $(\alpha_1, \beta_1) = (g^{r_1}, K^{r_1}\, m_1)$ et $(\alpha_2, \beta_2) = (g^{r_2}, K^{r_2}\, m_2)$, alors le produit défini par $(\alpha, \beta) = (\alpha_1\, \alpha_2, \beta_1\, \beta_2)$ est le chiffré du message $m_1\, m_2$. Le chiffrement El Gamal classique n'est adapté que pour le mélange des bulletins.

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.

Chiffrement ElGamal à 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 : l'entier 0 est codé comme l'élément de groupe g^0, l'entier 1 est codé comme g^1, et plus généralement l'entier j est codé comme g^j. La génération de clé est identique au cas classique, seuls le chiffrement et le déchiffrement sont différents.

Les algorithmes 4, 5 décrivent le chiffrement et le déchiffrement de l'algorithme ElGamal à codage exponentiel.

Attention

Ces algorithmes ne doivent pas être utilisés seuls et doivent être composés, pour tous les niveaux de scrutin, avec une preuve de chiffrement de 0 ou 1 et une preuve de sélection d'une option ou de chiffrement d'entier dans un intervalle et pour les scrutins de niveau 2 et 3, avec une preuve de connaissance de la clé privée et une preuve de déchiffrement correct, par exemple celles fournies à l'Annexe E.

Algorithme 4 : Chiffrement ElGamal à codage exponentiel

Entrée : g, q, K, j (générateur de groupe, ordre du groupe, clé publique, message à chiffrer)
Sortie : (α, β) (chiffré)

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

Algorithme 5 : Déchiffrement ElGamal à codage exponentiel

Entrée : k, (α, β) (clé privée, chiffré)
Sortie : j (message en clair)

1 $J = \beta / \alpha^k$
2 Return $j = \log(J)$ i.e j tel que $J = g^j$

Avec le codage exponentiel, l'algorithme 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 j_1 et j_2 avec la même clé publique K, $(\alpha_1, \beta_1) = (g^{r_1}, K^{r_1}\, g^{j_1})$ et $(\alpha_2, \beta_2) = (g^{r_2}, K^{r_2}\, g^{j_2})$, alors le produit défini par $(\alpha, \beta) = (\alpha_1\, \alpha_2, \beta_1\, \beta_2)$ est le chiffré du message $g^{j_1+j_2}$, et après décodage cela fournit $j_1 + j_2$.

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 E.

Considérons une configuration d'élection avec M options, telle que chaque électeur peut en choisir C, C étant compris dans un intervalle I inclus dans $[1, \ldots, M]$. Chaque électeur va générer une liste contenant M chiffrés ElGamal qui a le même ordre pour tous les électeurs et qui correspond

à l'ordre dans lequel les options sont présentées aux électeurs : chaque élément de la liste correspond au chiffré avec codage exponentiel de l'entier 0 si l'électeur n'a pas sélectionné l'option et au chiffré avec codage exponentiel de l'entier 1 si l'électeur a sélectionné l'option. Ainsi, chaque électeur génère une liste de chiffrés $(\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots, (\alpha_M, \beta_M)$, telle que $(\alpha_i, \beta_i) = (g^{r_i}, K^{r_i}\, g^0)$ si l'option i n'a pas été sélectionnée ou $(\alpha_i, \beta_i) = (g^{r_i}, K^{r_i}\, g^1)$ si l'option i a été sélectionnée, telle que le nombre de fois qu'une option est sélectionnée est compris entre M et N. Une fois le vote clos, le nombre de fois que l'option i a été sélectionnée est calculable d'abord en effectuant le produit de l'ensemble des chiffrés correspondant à cette option, pour l'ensemble des électeurs ayant voté et ensuite en en réalisant le déchiffrement. Ainsi le décodage $j = \log(J)$ est borné par le nombre d'électeurs participant à l'élection et est donc réalisable en temps raisonnable [99]. L'annexe E fournit des exemples de preuves à divulgation nulle de connaissance adaptées à ce contexte.

Génération centralisée de clé ElGamal fragmentée

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

Ces algorithmes ne doivent pas être utilisés seuls et doivent être composés, pour les scrutins de niveau 2 et 3, avec une preuve de connaissance de la clé privée et une preuve de déchiffrement correct, par exemple celles fournies à l'Annexe E.

Algorithme 6 : Génération centralisée de clé ElGamal fragmentée

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 ElGamal centralisé à clé fragmentée, codage classique

Entrée : $(k_1, \ldots, k_N)$, (α, β) (N fragments de la clé privée, chiffré)
Sortie : m (message en clair)

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

Algorithme 8 : Déchiffrement ElGamal centralisé à clé fragmentée, codage exponentiel

Entrée : $(k_1, \ldots, k_N)$, (α, β) (N fragments de la clé privée, chiffré)
Sortie : j (message en clair)

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

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 ElGamal 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 et t désigne le seuil.

Le chiffrement (à codage classique ou exponentiel) est identique aux cas précédents, seuls la génération de clé et le déchiffrement sont différents. Les algorithmes 9, 10, 11 décrivent la génération centralisée de clé fragmentée à seuil, le déchiffrement à seuil centralisé classique et avec codage exponentiel, respectivement.

Attention

Ces algorithmes ne doivent pas être utilisés seuls et doivent être composés, pour les scrutins de niveau 2 et 3, avec une preuve de connaissance de la clé privée et une preuve de déchiffrement correct, par exemple celles fournies à l'Annexe E.

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)

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

Algorithme 10 : Déchiffrement ElGamal à seuil centralisé, codage classique

Entrée : $(k_1, \ldots, k_t)$, (α, β) (t fragments de la clé privée, chiffré)
Sortie : m (message en clair)

for i *from* 1 *to* t **do**
    $\gamma_i = \alpha^{k_i}$
$D = \prod_i \gamma_i^{a_i}$, where $a_i = \prod_{j!=i}(j)/(j-i)$ (Interpolation de Lagrange)
Return $m = \beta / D$

Algorithme 11 : Déchiffrement ElGamal à seuil centralisé - codage exponentiel

Entrée : $(k_1, \ldots, k_t)$, (α, β) (t fragments de la clé privée, chiffré)
Sortie : j (message en clair)

for i *from* 1 *to* t **do**
    $\gamma_i = \alpha^{k_i}$
$D = \prod_i \gamma_i^{a_i}$, where $a_i = \prod_{j!=i}(j)/(j-i)$ (Interpolation de Lagrange)
$J = \beta / D$
Return $j = \log(J)$ i.e j tel que $J = g^j$

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 ElGamal fragmentée

La génération de clé ainsi que le déchiffrement (à codage classique ou exponentiel) peuvent être adaptées 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 permet de réaliser 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

Ces algorithmes ne doivent pas être utilisés seuls et doivent être composés, pour les scrutins de niveau 2 et 3, avec une preuve de connaissance de la clé privée et une preuve de déchiffrement correct, par exemple celles fournies à l'Annexe E.

Algorithme 12 : Génération de fragment de clé par un attributaire

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 de la clé de chiffrement ElGamal

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 ElGamal partiel par un attributaire

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 déchiffrement partiel)

Algorithme 15 : Génération du déchiffrement ElGamal, codage classique

Entrée : $N, (\alpha, \beta)$ (nombre d'attributaires, chiffré)
Sortie : m (message en clair)

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

Algorithme 16 : Génération du déchiffrement ElGamal, codage exponentiel

Entrée : $N, (\alpha, \beta)$ (nombre d'attributaires, chiffré)
Sortie : j (message en clair)

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

Attention

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

Génération distribuée de clé ElGamal 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 t désigne le seuil.

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

La génération des fragments de clés par les attributaires nécessite l'établissement d'un canal sécurisé entre ces attributaires (instructions $\text{in}(i, *)$ et $\text{out}(j, *)$ de l'algorithme 17).

Algorithme 17 : Génération de fragment de clé à seuil par un attributaire

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)

$f_i(X) \xleftarrow{\$} \mathbb{Z}_q[X]$, tel que $deg(f_i) = t - 1$ et $f_i(0) = k_i$
$K_i := g^{k_i}$
$\text{out}(K_i)$ (publication du fragment de clé publique)
for j *from* 1 *to* N, $j \neq i$ **do**
    $k_{i,j} := f_i(j)$
    $\text{out}(j, k_{i,j})$ (transmission sur canal sécurisé aux autres attributaires)
    $\text{in}(i, k_{j,i})$ (réception sur canal sécurisé en provenance des autres attributaires)
$z_i = \sum_j k_{j,i}$ (génération du fragment de clé de déchiffrement d'attributaire)
Return (z_i, K_i).

Attention

Ces algorithmes ne doivent pas être utilisés seuls et doivent être composés, pour les scrutins de niveau 2 et 3, avec une preuve de connaissance de la clé privée et une preuve de déchiffrement correct, par exemple celles fournies à l'Annexe E.

Algorithme 18 : Génération de la clé de chiffrement ElGamal

Entrée : N (nombre d'attributaires)

Sortie : K (clé publique de chiffrement ElGamal)

for i *from* 1 *to* N **do**
    $\text{in}(K_i)$ (récupération des fragments de clé publique)
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 permet de réaliser 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 ElGamal partiel par un attributaire

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 déchiffrement partiel)

Algorithme 20 : Génération du déchiffrement ElGamal, codage classique

Entrée : $t, (\alpha, \beta)$ (seuil, chiffré)
Sortie : m (message en clair)

1 **for** i *from* 1 *to* t **do**
2 in(γ_i) (récupération des déchiffrements partiels)
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 21 : Génération du déchiffrement ElGamal, codage exponentiel

Entrée : $t, (\alpha, \beta)$ (seuil, chiffré)
Sortie : j (message en clair)

1 **for** i *from* 1 *to* t **do**
2 in(γ_i) (récupération des déchiffrements partiels)
3 $D = \prod_i \gamma_i^{a_i}$, where $a_i = \prod_{j!=i}(j)/(j-i)$ (Interpolation de Lagrange)
4 $J = \beta/D$
5 Return $j = \log(J)$, i.e j tel que $J = g^j$

Attention

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

Annexe E
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 sincérité des scrutins. Elle fournit des exemples de preuves à divulgation nulle de connaissance [61, 79].

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

- La génération de la clé de l'élection pour le chiffrement/déchiffrement ElGamal (R34★★), composée avec une preuve de connaissance de clé secrète. **Ce type de preuve est requis pour les scrutins de niveau 2 et 3**, car elle permet d'assurer le secret du vote.
- Le chiffrement du suffrage au moyen de l'algorithme de chiffrement ElGamal, composé avec une preuve de connaissance de l'aléa utilisé pour le chiffrement. **Ce type de preuve est requis dès lors que le chiffrement ElGamal est mis en œuvre, pour tous les niveaux de scrutins**, car elle permet de contrer des attaques portant atteinte au secret du vote [86].
- En cas d'accumulation des bulletins, utilisant le caractère homomorphe du chiffrement ElGamal (R65★★), le chiffrement du suffrage, composé avec deux preuves : une preuve de validité de chaque chiffré ElGamal et une preuve de conformité à la configuration de l'élection. **Ces types de preuves sont requis pour tous les niveaux de scrutins, dès lors que l'accumulation est mise en œuvre**. La preuve de validité du chiffré impliquant la connaissance de l'aléa, elle peut se substituer à la preuve précédente.
- En cas de pastillage (R21★), l'adaptatoin du contexte des preuves précédentes pour tenir compte des attributs des électeurs. **Ce type d'adaptation est requis pour tous les niveaux de scrutins, dès lors qu'un pastillage est mis en œuvre**, car cette adaptation permet d'assurer l'intégrité du scrutin et le secret du vote.
- Le déchiffrement des bulletins (R43★★), composé avec une preuve de déchiffrement correct. **Ce type de preuve est requis pour les scrutins de niveau 2 et 3** car elle permet d'assurer l'intégrité 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 ou la propriété de confidentialité persistante - *everlasting privacy*) ou bien peuvent ne pas être 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). 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 [84, 93, 94].

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.
- 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 [67], aussi il est nécessaire d'être vigilant sur sa définition suivant les cas d'usage des preuves.

Il est important de noter que les preuves expliquées dans cette annexe sont adaptées à un type de scrutin (l'électeur a la possibilité de sélectionner N options parmi M), 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 [71, 88], car elles jouent un rôle essentiel pour assurer la sincérité d'un scrutin.

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 classique ou avec le codage exponentiel (Annexe D). 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 $(\alpha, \beta) = (g^r, K^r\, m)$, avec m 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 D). 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 A, 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 $(\alpha, \beta) = (g^r, K^r\, m)$.

Algorithme 26 : Génération de la 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 la 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 D) et après la génération de preuve de chiffrement correct (de 0 ou 1). En reprenant les notations de l'Annexe D, chaque électeur génère une liste de chiffrés $(\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots, (\alpha_M, \beta_M)$, telle que $(\alpha_i, \beta_i) = (g^{r_i}, K^{r_i}\, g^0)$ si l'option i n'a pas été sélectionnée ou $(\alpha_i, \beta_i) = (g^{r_i}, K^{r_i}\, g^1)$ 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, afin de détecter les bulletins invalides avant de réaliser l'accumulation.

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 : $\mathcal{D}_{\mathsf{pub}} = \{K, (\alpha, \beta), (\alpha_1, \beta_1), \ldots, (\alpha_M, \beta_M), \mathsf{ctx}\}$, où $K \in \mathbb{G}$ est une clé publique, $(\alpha_1, \beta_1), \ldots, (\alpha_M, \beta_M)$ et (α, β) sont des chiffrés ElGamal.

Données secrètes : $\mathcal{D}_{\mathsf{sec}} = \{r\}$, où $r \in \mathbb{Z}_q$ est tel que $(\alpha, \beta) = (g^r, K^r\, g^1)$.

Algorithme 28 : Génération de preuve de sélection d'une une et une seule option

Entrée : $\mathcal{D}_{\mathsf{pub}}, \mathcal{D}_{\mathsf{sec}}$
Sortie : $\pi = (c, v)$

1 $\xi \xleftarrow{\$} \mathbb{Z}_q$
2 $A := g^{\xi}$
3 $B := K^{\xi}$
4 $c = \mathsf{hash}(\text{"zkp\_enc\_simple"}, \mathsf{ctx}, K, \alpha, \beta, \alpha_1, \beta_1, \ldots, \alpha_M, \beta_M, A, B)$
5 $v = (\xi - r\, c) \bmod q$
6 Return $\pi = (c, v)$

Algorithme 29 : Vérification de preuve de sélection d'une et une seule option

Entrée : $\mathcal{D}_{\mathsf{pub}}, \pi = (c, v)$

1 $A := g^v\, \alpha^c$
2 $B := K^v\, (\beta/g)^c$
3 $c' := \mathsf{hash}(\text{"zkp\_enc\_simple"}, \mathsf{ctx}, K, \alpha, \beta, \alpha_1, \beta_1, \ldots, \alpha_M, \beta_M, A, B) \bmod q$
4 Check $c' == c \bmod q$.

Information

L'inclusion de la liste ordonnée des chiffrés $\alpha_1, \beta_1, \ldots, \alpha_M, \beta_M$ 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 : $\mathcal{D}_{\text{pub}} = \{K, (\alpha, \beta), (\alpha_1, \beta_1), \ldots, (\alpha_M, \beta_M), \text{ctx}\}$, où $K \in \mathbb{G}$ est une clé publique, $(\alpha_1, \beta_1), \ldots, (\alpha_M, \beta_M)$ et (α, β) sont des chiffrés ElGamal.

Données secrètes : $\mathcal{D}_{\text{sec}} = \{i_{\text{choisi}}, r\}$, où $i_{\text{choisi}} \in \{i_{\text{min}}, i_{\text{min}} + 1, \ldots, i_{\text{max}}\}$ est l'entier codé par le message clair associé au chiffré, et $r \in \mathbb{Z}_q$ est tel que $(\alpha, \beta) = (g^r, K^r\, g^{i_{\text{choisi}}})$.

Algorithme 30 : Génération de preuve de chiffrement d'entier dans un intervalle

Entrée : $\mathcal{D}_{\text{pub}}, \mathcal{D}_{\text{sec}}$
Sortie : $\pi = ((c_{i_{\text{min}}}, v_{i_{\text{min}}}), (c_{i_{\text{min}}+1}, v_{i_{\text{min}}+1}), \ldots, (c_{i_{\text{max}}}, v_{i_{\text{max}}}))$

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
    $c_i \xleftarrow{\$} \mathbb{Z}_q$
    $v_i \xleftarrow{\$} \mathbb{Z}_q$
    $A_i := g^{v_i}\, \alpha^{c_i}$
    $B_i := K^{v_i}\, (\beta / g^i)^{c_i}$
$c_{i_{\text{choisi}}} = \text{hash}(\text{"zkp\_enc\_int"}, \text{ctx}, K, \alpha, \beta, \alpha_1, \beta_1, \ldots, \alpha_M, \beta_M, A_{i_{\text{min}}}, B_{i_{\text{min}}}, A_{i_{\text{min}}+1}, B_{i_{\text{min}}+1}, \ldots, A_{i_{\text{max}}}, B_{i_{\text{max}}}) - (\sum_{i \neq i_{\text{choisi}}} c_i) \bmod q$
$v_{i_{\text{choisi}}} = (\xi - r\, c_i) \bmod q$
Return $\pi = ((c_{i_{\text{min}}}, v_{i_{\text{min}}}), (c_{i_{\text{min}}+1}, v_{i_{\text{min}}+1}), \ldots, (c_{i_{\text{max}}}, v_{i_{\text{max}}}))$

Algorithme 31 : Vérification de preuve de chiffrement d'entier dans un intervalle

Entrée : $\mathcal{D}_{\text{pub}}, \pi = ((c_{i_{\text{min}}}, v_{i_{\text{min}}}), (c_{i_{\text{min}}+1}, v_{i_{\text{min}}+1}), \ldots, (c_{i_{\text{max}}}, v_{i_{\text{max}}}))$

for i *from* i_{min} *to* i_{max} **do**
  $A_i := g^{v_i}\, \alpha^{c_i}$
  $B_i := K^{v_i}\, (\beta / g^i)^{c_i}$
$c' := \text{hash}(\text{"zkp\_enc\_int"}, \text{ctx}, K, \alpha, \beta, \alpha_1, \beta_1, \ldots, \alpha_M, \beta_M, A_{i_{\text{min}}}, B_{i_{\text{min}}}, A_{i_{\text{min}}+1}, B_{i_{\text{min}}+1}, \ldots, A_{i_{\text{max}}}, B_{i_{\text{max}}}) \bmod q$
Check $c' == (\sum_i c_i) \bmod q$.

Information

L'inclusion de la liste ordonnée des chiffrés $\alpha_1, \beta_1, \ldots, \alpha_M, \beta_M$ 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 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 du votant et l'expression de son vote (1.07, 2.08), 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 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 sincérité 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 (R17★) et d'autre part en détectant les caractéristiques du dispositif de vote (R18★).

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 :

- Contrôler le cache HTTP via des entêtes : les entêtes « Cache-Control » [3], « Expires » [11] ou « Etag » [10] sont définis côté serveur et peuvent empêcher le client de placer la réponse en cache.
- Utiliser l'API Cache Web [2]. Cette API specifique au contexte des Service Workers [33] permet de supprimer une réponse du cache.
- Remplir la mémoire d'un grand nombre d'objets afin de provoquer l'exécution du Garbage Collector [25].
- Contrôler le cache CPU via l'utilisation de SharedArrayBuffer [34].

Contrôle du dispositif de vote

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 :

- 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 [15].
- Activation du mode debug : heuristique basée sur le temps d'exécution de certaines requêtes.

Pour le système d'exploitation et le navigateur : le UserAgent [26] 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.

Bibliographie

[1] *Analyse de flux https : bonnes pratiques et questions*.
https://www.cnil.fr/fr/analyse-de-flux-https-bonnes-pratiques-et-questions.

[2] *Cache*.
https://developer.mozilla.org/en-US/docs/Web/API/Cache.

[3] *Cache-Control*.
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control.

[4] *Center For Internet Security Benchmarks*.
https://www.cisecurity.org/cis-benchmarks-overview.

[5] *Code électoral*.
https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006070239/.

[6] *Common Vulnerabilities and Exposures*.
https://www.cve.org/.

[7] *CyberDico, Qu'est-ce que c'est ?*
https://cyber.gouv.fr/publications/cyberdico-quest-ce-que-cest.

[8] *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.

[9] *Élection syndicale TPE* .
https://election-tpe.travail.gouv.fr/.

[10] *ETag*.
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/ETag.

[11] *Expires*.
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Expires.

[12] *Fiche réflexe du CERT-FR. Déni de service réseau - Endiguement*.
https://www.cert.ssi.gouv.fr/fiche/CERTFR-2024-RFX-010/.

[13] *Fiche réflexe du CERT-FR. Déni de service réseau - Qualification*.
https://www.cert.ssi.gouv.fr/fiche/CERTFR-2024-RFX-009/.

[14] *Helios Voting*.
https://vote.heliosvoting.org/.

[15] *<iframe> : The Inline Frame element*.
https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe#attr-sandbox.

[16] *Interface de programmation d'application (API)*.
https://www.cnil.fr/fr/definition/interface-de-progPammation-dapplication-api.

[17] *JavaScript Tutorial*.
https://www.w3schools.com/js/.

[18] *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.

[19] *La notion de sincérité du scrutin*.
https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/la-notion-de-sincerite-du-scrutin.

[20] *Le règlement général sur la protection des données - RGPD*.
https://www.cnil.fr/fr/reglement-europeen-protection-donnees.

[21] *Le Répertoire électoral unique*.
https://www.insee.fr/fr/information/3539086.

[22] *Les Essentiels de l'ANSSI - Dénis de service distribués (DDos)*.
https://cyber.gouv.fr/publications/denis-de-service-distribues-ddos.

[23] *L'élection de la délégation du personnel au CSE*.
https://travail-emploi.gouv.fr/lelection-de-la-delegation-du-personnel-au-cse.

[24] *Machines à voter*.
https://www.interieur.gouv.fr/Elections/Comment-voter/Machines-a-voter.

[25] *Memory management*.
https://developer.mozilla.org/en-US/docs/Web/JavaScript/Memory_management.

[26] *Navigator : userAgent property*.
https://developer.mozilla.org/en-US/docs/Web/API/Navigator/userAgent.

[27] *OWASP API Security Project*.
https://owasp.org/www-project-api-security/.

[28] *OWASP Cheat Sheet Series - Vulnerability Disclosure Cheat Sheet*.
https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html.

[29] *Prestataires de vérification d'identité à distance (PVID)*.
https://cyber.gouv.fr/prestataires-de-verification-didentite-distance-pvid.

[30] *Produits et services qualifiés*.
https://cyber.gouv.fr/produits-services-qualifies.

[31] *Reproducible Builds*.
https://reproducible-builds.org/.

[32] *Responsable de traitement*.
https://www.cnil.fr/fr/definition/responsable-de-traitement.

[33] *Service Worker API*.
https://developer.mozilla.org/en-US/docs/Web/API/Service_Worker_API.

[34] *SharedArrayBuffer*.
https://developer.mozilla.org/fr/docs/Web/JavaScript/Reference/Global_Objects/SharedArrayBuffer.

[35] *SPA (Single-page application)*.
https://developer.mozilla.org/en-US/docs/Glossary/SPA.

[36] *SQL Tutorial*.
https://www.w3schools.com/sql/.

[37] *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.

[38] *Verificatum Mix-Net*.
https://www.verificatum.org/.

[39] *Vulnerability Metrics*.
https://nvd.nist.gov/vuln-metrics/cvss.

[40] *Recommandations pour l'hébergement dans le Cloud des systèmes d'information sensibles*, juillet 2024.
https://cyber.gouv.fr/publications/recommandations-pour-lhebergement-des-si-sensibles-dans-le-cloud.

[41] 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.

[42] *Recommandations de sécurité relatives à un système GNU/Linux*.
Guide ANSSI-BP-028 v2.0, ANSSI, octobre 2022.
https://cyber.gouv.fr/guide-linux.

[43] *Sauvegarde des systèmes d'information*.
Fondamentaux ANSSI-BP-100 v1.0, ANSSI, octobre 2023.
https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation.

[44] *Recommandations de securité concernant l'analyse des flux HTTPS*.
Note technique DAT-NT-019/ANSSI/SDE/NP v1.2, ANSSI, février 2016.
https://cyber.gouv.fr/guide-analyse-https.

[45] *La méthode EBIOS Risk Manager - Le Guide*.
Guide ANSSI-PA-048 v1.0, ANSSI, octobre 2018.
https://cyber.gouv.fr/ebios-rm.

[46] *Recommandations relatives à l'interconnexion d'un système d'information à Internet*.
Guide ANSSI-PA-066 v2.0, ANSSI, juin 2019.
https://cyber.gouv.fr/guide-interconnexion-si-internet.

[47] *Recommandations de sécurité relatives à TLS*.
Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020.
https://cyber.gouv.fr/guide-tls.

[48] *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.

[49] *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*.
Guide ANSSI-PG-083 v2.0, ANSSI, janvier 2020.
https://cyber.gouv.fr/publications/mecanismes-cryptographiques.

[50] *Guide de sélection d'algorithmes cryptographiques*.
Guide ANSSI-PA-079 v1.0, ANSSI, mars 2021.
https://cyber.gouv.fr/publications/mecanismes-cryptographiques.

[51] *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.

[52] *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.

[53] *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.

[54] *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.

[55] *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.

[56] *Référentiel général de sécurité (RGS)*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://cyber.gouv.fr/rgs.

[57] *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.

[58] *Authentification multifacteurs et mots de passe*.
Guide ANSSI-PG-078 v1.0, ANSSI, octobre 2021.
https://cyber.gouv.fr/guide-authentification.

[59] 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.

[60] 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.

[61] 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.

[62] Mihir Bellare and Phillip Rogaway.
Optimal Asymmetric Encryption.
In Alfredo De Santis, editor, *Advances in Cryptology – EUROCRYPT'94*, volume 950 of *Lecture Notes in Computer Science*, pages 92–111, Perugia, Italy, mai 9–12, 1995. Springer, Berlin, Heidelberg, Germany.

[63] Josh Benaloh.
Simple Verifiable Elections.
In *2006 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 06)*, Vancouver, B.C., août 2006. USENIX Association.

[64] Josh Benaloh, Michael Naehrig, and Olivier Pereira.
REACTIVE : Rethinking Effective Approaches Concerning Trustees in Verifiable Elections.
Cryptology ePrint Archive, Paper 2024/915, 2024.

[65] 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.

[66] 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.

[67] 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.

[68] 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.

[69] 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.

[70] 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.

[71] 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.

[72] 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.

[73] 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.

[74] Commission Nationale Informatique et Libertés.
Délibération 03-036 du 1 juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique.
https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000017653831/.

[75] Commission Nationale Informatique et Libertés.
Délibération n°2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000023124205/.

[76] Commission Nationale Informatique et Libertés.
Délibération n°2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038661239/.

[77] Commission Nationale Informatique et Libertés.
Délibération n°2025-xxx du xx xxx 2025 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.
https://ACORRIGER/.

[78] *Licence ouverte / Open Licence v2.0*.
Page web, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

[79] 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.

[80] Rojan Gharadaghy and Melanie Volkamer.
Verifiability in Electronic Voting - Explanations for Non Security Experts.
In *Electronic Voting 2010 (EVOTE2010), 4th international conference co-organized by Council of Europe, Gesellschaft für Informatik and E-Voting.CC, Bregenz, A, July 21-24, 2010*, volume 167 of *GI-Edition : Proceedings*, pages 151–162. Gesellschaft für Informatik (GI), 2010.

[81] Stéphane Glondu.
Belenios specification.
https://www.belenios.org/specification.pdf.

[82] Jim Gray and Andreas Reuter.
Transaction Processing : Concepts and Techniques.
Morgan Kaufmann, December 1991.

[83] Rolf Haenni, Reto E. Koenig, Philipp Locher, and Eric Dubuis.
CHVote System Specification.
Cryptology ePrint Archive, Report 2017/325, 2017.

[84] Thomas Haines, Rafieh Mosaheb, Johannes Müller, and Ivan Pryvalov.
SoK : Secure E-Voting with Everlasting Privacy.
Proc. Priv. Enhancing Technol., 2023 :279–293, 2023.

[85] 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.

[86] Feng Hao and Peter Y. A. Ryan.
Real-World Electronic Voting : Design, Analysis and Deployment.
Series in Security, Privacy and Trust. CRC Press, 2016.

[87] 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.

[88] 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.

[89] 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.

[90] National Institute of Standard and Technology.
National Checklist Program for IT Products.
https://ncp.nist.gov/repository.

[91] Marco Patrignani, Amal Ahmed, and Dave Clarke.
Formal Approaches to Secure Compilation : A Survey of Fully Abstract Compilation and Related Work.
ACM Computing Surveys, 51 :1–36, 02 2019.

[92] Torben P. Pedersen.
Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing.
In Joan Feigenbaum, editor, *Advances in Cryptology – CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 129–140, Santa Barbara, CA, USA, août 11–15, 1992. Springer, Berlin, Heidelberg, Germany.

[93] 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.

[94] David Pointcheval.
Efficient Universally-Verifiable Electronic Voting with Everlasting Privacy.
In Clemente Galdi and Duong Hieu Phan, editors, *Security and Cryptography for Networks*, pages 323–344, Cham, 2024. Springer Nature Switzerland.

[95] 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/Protocol.

[96] Open Worldwide Application Security Project.
OWASP TOP 10.
https://owasp.org/Top10/.

[97] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman.
A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.
Communications of the Association for Computing Machinery, 21(2) :120–126, février 1978.

[98] Adi Shamir.
How to Share a Secret.
Communications of the Association for Computing Machinery, 22(11) :612–613, novembre 1979.

[99] Daniel Shanks.
Class number, a theory of factorization, and genera.
Jan 1971.

[100] 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.

[101] Tomasz Truderung.
POLYAS 3.0 Verifiable E-Voting System.
https://github.com/polyas-voting/core3-verifiable-doc/.

[102] Douglas Wikström.
A Commitment-Consistent Proof of a Shuffle.
In Colin Boyd and Juan González Nieto, editors, *Information Security and Privacy*, pages 407–421, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[103] Jianhao Xu, Kangjie Lu, Zhengjie Du, Zhu Ding, Linke Li, Qiushi Wu, Mathias Payer, and Bing Mao.
Silent Bugs Matter : A Study of Compiler-Introduced Security Bugs.
In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 3655–3672, Anaheim, CA, août 2023. USENIX Association.

Version 0.1 - 2025 - Consultation Publique

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Secrétariat général de la défense et de la sécurité nationale