

Annexe III au CCTP : exigences de sécurité

Table des matières

1.	RESPECT DES PRINCIPES APPLICABLES AUX OPERATIONS ELECTORALES	3
2.	AUTHENTIFICATION	3
2.1.	<i>Principes généraux</i>	3
2.2.	<i>Authentification des électeurs</i>	4
2.3.	<i>Authentification des utilisateurs avec pouvoirs</i>	6
2.4.	<i>Authentification des candidats</i>	7
2.5.	<i>Protection des authentifications contre les attaques</i>	8
2.6.	<i>Durée des sessions</i>	8
2.7.	<i>Séparation des privilèges</i>	8
3.	TRAÇABILITE ET INTEGRITE	9
3.1.	<i>Traçabilité fonctionnelle</i>	9
3.2.	<i>Interventions et traçabilité techniques</i>	9
3.3.	<i>Scellement du système de vote électronique</i>	10
3.4.	<i>Alertes</i>	11
3.5.	<i>Intégrité de l'urne et de l'émargement</i>	11
3.6.	<i>Archivage ad probationem et conservation</i>	11
4.	TRANSPARENCE DE L'URNE	12
4.1.	<i>Vérifiabilité individuelle et preuve de vote</i>	12
4.2.	<i>Vérifiabilité universelle</i>	14
4.3.	<i>Publication du protocole de vote</i>	15
4.4.	<i>Publication du code source du client de vote</i>	15
4.5.	<i>Information des électeurs relative à la sécurité et à la fiabilité</i>	16
5.	DISPONIBILITE	16
5.1.	<i>Engagement de disponibilité</i>	16
5.2.	<i>Mise en œuvre de la disponibilité</i>	17
5.3.	<i>Perte de données maximale acceptable</i>	17
5.4.	<i>Indépendance des scrutins</i>	18
6.	CONFIDENTIALITE.....	18
6.1.	<i>Protection de la confidentialité sur le poste de l'électeur</i>	18
6.2.	<i>Chiffrement du bulletin de vote</i>	18
6.3.	<i>Chiffrement des communications réseau</i>	18
6.4.	<i>Clés de l'élection</i>	19
6.5.	<i>Anonymat du vote</i>	20
6.6.	<i>Pastillage et anonymat du vote</i>	20

6.7.	<i>Accès aux données</i>	21
6.8.	<i>Echanges sécurisés de données</i>	21
6.9.	<i>Données à caractère personnel</i>	21
7.	SECURITE PHYSIQUE ET LOGIQUE DU SYSTEME DE VOTE ELECTRONIQUE	22
7.1.	<i>Sécurité physique des locaux de développement et d'hébergement</i>	22
7.2.	<i>Développement sécurisé</i>	22
7.3.	<i>Exposition du système de vote électronique sur Internet</i>	22
7.4.	<i>Maintien en condition de sécurité et suivi des vulnérabilités</i>	22
7.5.	<i>Exploitation et autorité organisatrice technique</i>	22
7.6.	<i>Autorité organisatrice fonctionnelle</i>	23
8.	MECANISMES CRYPTOGRAPHIQUES	23
8.1.	<i>Mécanismes recommandés pour le chiffrement des bulletins de vote</i>	23
8.2.	<i>Mécanismes acceptables pour le chiffrement des bulletins de vote</i>	23
8.3.	<i>Gestion et partage de la clé privée de déchiffrement</i>	24
8.4.	<i>Mise en œuvre du pastillage</i>	25
8.5.	<i>Mécanismes de hachage pour le calcul des empreintes</i>	26
8.6.	<i>Générateur d'aléa</i>	26
8.7.	<i>Stockage des secrets d'authentification</i>	26
8.8.	<i>Evolutions</i>	26

Cette annexe a été rédigée notamment en collaboration avec l'agence nationale pour la sécurité des systèmes d'information (ANSSI), autorité nationale de cybersécurité. En cas de question relative à la sécurité les autorités organisatrices sont susceptibles de contacter conseil.technique@ssi.gouv.fr.

1. Respect des principes applicables aux opérations électorales

Le recours au vote électronique est organisé dans le respect des principes fondamentaux qui commandent les opérations électorales. Ces principes sont la sincérité des opérations électorales, l'accès au vote de tous les électeurs, le secret du scrutin, le caractère personnel, libre et anonyme du vote, l'intégrité des suffrages exprimés, la surveillance effective du scrutin par le BVE et les représentants des OS et le contrôle par le juge de l'élection (article R. 211-508 du CGFP).

A ces principes s'ajoute le respect des données à caractère personnel traitées par le SyVE.

Afin de garantir le respect de ces principes, le titulaire s'engage à :

- Garantir la sincérité du scrutin, c'est-à-dire notamment l'authentification des électeurs (voir section 2), la traçabilité et l'intégrité du SyVE (voir section 3) ;
- Contribuer à la transparence avec la vérifiabilité du scrutin, individuelle pour chaque électeur et universelle (voir section 4) ;
- Assurer la disponibilité des fonctionnalités du SyVE au regard du calendrier impératif des opérations électorales (voir section 5) ;
- Assurer l'accessibilité du SyVE pour tous les électeurs ;
- Garantir le secret du vote (anonymat et confidentialité) et empêcher la publication anticipée des résultats partiels (voir section 6) ;
- Assurer la supervision de sécurité du SyVE et l'alerte du BVE et des représentants des OS (voir section 3) ;
- Permettre la conservation des données du scrutin à l'issue du dépouillement au bénéfice par l'autorité organisatrice et, le cas échéant, le rejeu du décompte en cas de contentieux (voir section 3) ;
- Garantir la protection des données personnelles des électeurs, des agents de l'autorité organisatrice et des membres du BVE (voir section 6.9).

2. Authentification

2.1. Principes généraux

La SVE distingue deux catégories d'utilisateurs : les électeurs et les utilisateurs avec pouvoirs. Chaque utilisateur se voit affecté un identifiant utilisateur et un à deux secrets ou authentifiants qui sont utilisés dans les procédures d'identification et d'authentification. Ces procédures permettent aux utilisateurs d'accéder aux portails de la SVE comme à ses fonctionnalités.

Le SyVE met en œuvre une politique de génération des moyens d'authentification paramétrable pour chaque moyen d'authentification et chaque population d'utilisateurs. Ces paramètres peuvent notamment être le jeu de caractères ou symboles utilisés pour constituer un mot de passe ou encore la longueur d'un mot de passe. Le générateur d'aléa utilisé est conforme aux exigences de la section 8.

Le SyVE génère pour chaque utilisateur un mot de passe en tant que moyen d'authentification. La conservation du mot de passe par le SyVE est conforme aux exigences de la section 8.

La longueur d'un mot de passe et la variété de jeu de caractères qui le compose définissent sa robustesse. Dans le cadre d'un scrutin, la durée de vie du mot de passe est limitée, et la présente annexe exige des mécanismes de protection des mots de passe (génération aléatoire, protection contre les attaques). Ce contexte particulier permet d'adapter le niveau de robustesse attendu, pour simplifier le parcours de vote de l'électeur et favoriser la participation.

Ainsi, pour le code de vote généré aléatoirement, l'ANSSI suggère une longueur de 12 caractères avec un alphabet simple (tel que les 26 majuscules, 10 chiffres sans 4 caractères « ambigus » (o/O, 1/l)). En revanche, pour les mots de passe choisis par les électeurs (moyen d'authentification au portail Electeurs), ou ceux des utilisateurs avec pouvoirs, la politique devra exiger une plus grande variété dans le jeu de symboles (majuscules, minuscules, chiffres, caractères spéciaux...). Il est notamment possible de prévoir de recourir à une aide à la saisie

des authentifiants et notamment que le SyVE exploite des masques de saisie des mots de passe ou un clavier virtuel composé du jeu des symboles utilisés pour la création des mots de passe.

Ces politiques pourront être adaptées en cours de marché par le GC-MTEA autorité organisatrice **conformément à son analyse de risques et aux recommandations de l'expert indépendant, en s'appuyant sur le guide « Recommandations relatives à l'authentification multifacteur et aux mots de passe » de l'ANSSI.**

2.2. Authentification des électeurs

Le SyVE requiert l'identification et l'authentification des électeurs pour se connecter au portail Electeurs (portail B1) et au portail de vote (portail B2). Comme détaillé dans l'annexe I relative aux exigences fonctionnelles, cette authentification repose sur :

- Un **identifiant** déjà connu de l'électeur, qui n'est donc pas un secret (adresse mail professionnelle comme choisie par le présent CCTP ou un autre moyen, tel que le couple constitué par son matricule et sa date de naissance) ;
- Un **moyen d'authentification**, typiquement un mot de passe, qui diffère selon le type d'espace auquel l'électeur veut accéder. Ce mot de passe est un secret connu uniquement de l'électeur.

2.2.1. Moyen d'authentification au portail Electeurs

Le moyen d'authentification au portail Electeurs est un mot de passe choisi par l'électeur lors de sa première connexion au portail. Cette première connexion est permise par un lien (ou un mot de passe) à usage unique, généré par le SyVE et envoyé à l'électeur par courrier électronique sur son adresse email de contact connue du seul SyVE. Le générateur d'aléa pour le lien à usage unique est conforme aux exigences de la section 8. Le mot de passe choisi par l'électeur est conforme à la politique paramétrable des moyens d'authentification des électeurs (longueur minimale, jeu de caractères utilisés).

Le moyen d'authentification au portail Electeurs peut être modifié par l'électeur, soit à travers ce portail Electeur après une authentification réussie, soit par une procédure de réassortiment (mot de passe oublié) s'appuyant sur l'envoi d'un nouveau lien à usage unique, généré par le SyVE et envoyé à l'électeur par courrier électronique sur son adresse email de contact, pour limiter le risque d'usurpation d'identité.

La conservation de ce mot de passe par le SyVE est conforme aux exigences de la section 8.

2.2.2. Moyen d'authentification au portail de vote

Le SyVE génère pour chaque électeur un mot de passe, en tant que code de vote donnant accès au portail de vote pendant la période d'ouverture du scrutin.

Le titulaire fait envoyer le mot de passe à chaque électeur par courrier sur l'ENSAP, ou à défaut, en cascade, par SMS ou courrier électronique ou envoi postal ou remise en main propre.. Les échanges de données relatifs aux envois sont protégés en intégrité et en confidentialité.

2.2.3. Evaluation du niveau de sécurité selon les canaux d'envois des moyens d'authentification

Cette section décrit les enjeux et propriétés de sécurité des différents canaux d'envois des moyens d'authentification.

- **Courrier postal envoyé au domicile de l'électeur** : coûteux mais sécurisé, car l'envoi et la distribution sont généralement hors de portée de l'autorité organisatrice de scrutins et des autres parties intéressées du scrutin, dès lors que l'impression est externalisée. Plusieurs niveaux de protection sont disponibles pour ce type d'envoi ; ils seront choisis en fonction de l'analyse de risque.
- **Email personnel ou SMS sur téléphone personnel** : a priori hors de portée de l'autorité organisatrice et des autres parties. Cas généralisable aux messages instantanées type *Tchap*, *WhatsApp* ou *Signal* mais avec des contraintes plus fortes d'adoption par l'ensemble des utilisateurs. Ces canaux requièrent la collecte et l'utilisation de données personnelles (adresse email, numéro de téléphone personnel) dont il convient de sécuriser les données.

- **ENSAP** (Espace Numérique Sécurisé de l'Agent Public, dont la politique de mots de passe requiert 8 caractères dont au moins 3 parmi une majuscule, une minuscule, un chiffre et caractère spécial) : cette solution est privilégiée en première instance, offrant un cadre sécurisé, car l'envoi et le stockage sont en général hors de portée de l'autorité organisatrice du scrutin et des autres parties. La politique de mots de passe de l'ENSAP est cependant faible et apporte peu de garanties. A noter : il est possible de s'authentifier à l'ENSAP avec FranceConnect, et ainsi, combiner un secret d'authentification envoyé dans l'ENSAP avec une authentification par FranceConnect (en tant que SSO ou *Single sign-on*), ce qui n'apporte pas plus de sécurité.
- **Email professionnel ou SMS sur téléphone professionnel** : il existe un risque qu'un administrateur de l'autorité organisatrice du scrutin puisse accéder à ces informations, au profit de l'autorité organisatrice ou d'une autre partie du scrutin. Donc cette solution est moins confidentielle qu'un envoi sur un email personnel ou un SMS sur un numéro personnel.
- **Courrier remis en main propre** : ce processus semble difficile à sécuriser afin de s'assurer que le secret n'est pas lisible sans ouvrir le pli, s'assurer que le secret n'est remis qu'à l'électeur, s'assurer que les secrets non remis ne sont pas utilisés, etc. Seules des garanties fortes sur les procédures associées permettraient d'en relever le niveau de sécurité.

Le candidat doit, en les motivant, identifier dans son mémoire technique ses propositions de canaux de communication des identifiants et des moyens d'authentification qui seraient créés par le SyVE pour les diverses catégories d'utilisateurs. Il doit préciser les procédures sécurisées de communication qu'il met en œuvre pour utiliser ces canaux.

2.2.4. Sécurité des envois par courrier papier

L'objectif de sécurité de l'envoi par courrier postal (envoi postal ou remise en main propre) est d'assurer la confidentialité du secret d'authentification qui figure sur le courrier. A défaut de garantir cette confidentialité, il est important de pouvoir détecter les atteintes à cette confidentialité pour que l'électeur puisse demander le renouvellement d'un secret qui aurait pu être compromis.

Pour assurer la confidentialité en empêchant la lecture du secret sans ouverture de l'enveloppe, il est nécessaire de procéder :

- Au masquage du secret sous une couche opaque à gratter ;
- Au masquage du secret sous une languette opaque à décoller ;
- Au masquage du secret par un carré opaque situé ailleurs sur le courrier mais au-dessus lors du pliage ;
- A l'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.

Il peut être également pertinent de 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. Les enveloppements de sécurité combinent en général un caractère indéchirable et opaque avec un témoin d'ouverture.

Autres considérations :

- Dans certains cas, l'identité et l'adresse des agents doivent être protégées et l'impression doit répondre à des contraintes supplémentaires.
- L'étape d'impression elle-même peut présenter des risques : absence de confidentialité lors de l'envoi des secrets à l'imprimeur, collusion de l'imprimeur avec une des parties du scrutin, ou encore erreurs lors de l'impression conduisant à envoyer un ou plusieurs secrets au mauvais destinataire. Ces risques peuvent être considérés pendant l'analyse de risques et des solutions recherchées avec l'imprimeur.
- Il existe des papiers dits « sécurisés » qui rendent plus difficile la copie de certains documents (billets de banque, pièces d'identité, diplômes, etc.). Leur utilisation pour l'envoi de secrets d'authentification n'est pas pertinente, car une fois lu, le secret peut être copié (manuellement ou par photographie) et conserver sa valeur. La protection du courrier contre la copie ne présente donc pas d'enjeu.

2.2.5. Réassortiment des moyens d'authentification

En cas de non-réception ou de perte d'un moyen d'authentification, un électeur peut demander son renouvellement. En application de l'article R. 211-555 du CGFP, le mécanisme de réassortiment doit garantir un niveau de sécurité au moins équivalent à celui requis pour la transmission initiale de ce moyen d'authentification.

Par exemple :

- La procédure pour renouveler le mot de passe du portail Electeurs est la même que pour l'envoi initial (un lien à usage unique envoyé par email). C'est donc le même niveau de sécurité.
- S'il y a deux moyens d'authentification spécifiques au scrutin, il sera nécessaire de fournir celui qui a été reçu pour obtenir l'autre *par son canal d'origine*. Exemple : s'authentifier au portail Electeurs avant de pouvoir demander un nouveau code de vote, possibilité de « réassortiment en présentiel » en faisant appel à un utilisateur avec pouvoirs local. Cet utilisateur avec pouvoirs peut confirmer l'identité de l'électeur qui se présente physiquement à lui puis faire renouveler le moyen d'authentification manquant ;
- Possibilité d'utiliser la procédure d'enrôlement pour demander à l'utilisateur de choisir une question/défi parmi un certain nombre, puis d'enregistrer sa réponse personnelle. Donner la bonne réponse au défi permet d'initier légitimement la procédure de réassortiment.

Le renvoi d'un secret doit, si possible, passer par le canal d'envoi d'origine de ce secret, et utiliser la même « adresse » (adresse postale, adresse email, numéro de téléphone, etc.).

Dans certains cas, le renvoi par le canal d'origine peut s'avérer impossible : soit pour des contraintes temporelles (exemple : premier envoi par courrier postal), soit parce que l'adresse n'est pas ou plus valable (l'électeur n'a plus accès à cette boîte aux lettres, en raison d'une mobilité professionnelle, ou a changé de numéro de téléphone).

L'autorité organisatrice du scrutin doit alors arbitrer entre une sécurité stricte et interdire la saisie d'une nouvelle adresse, limitant ainsi le risque d'usurpation d'identité, et favoriser la participation en permettant la saisie d'une nouvelle adresse. Si cette seconde option est choisie :

- Il est recommandé que le SyVE authentifie l'électeur de façon renforcée, par exemple en utilisant un défi (information connue par l'électeur et par l'autorité organisatrice, mais non publique ou facilement devinable) ou une authentification tierce (SSO de l'entité, identité numérique, vérification d'identité à distance).
- Si l'authentification renforcée réussit ou si l'absence d'authentification renforcée ou de défi est jugée acceptable par l'autorité organisatrice du scrutin, le SyVE permet à l'électeur de saisir une nouvelle adresse.
- Le SyVE renouvelle le secret et l'envoie à la nouvelle adresse.
- Le SyVE notifie l'électeur du renouvellement de son secret d'authentification par tous les autres canaux disponibles. Cette étape permet à l'électeur d'être informé d'une éventuelle usurpation d'identité et d'une demande illégitime faite en son nom.
- Le SyVE journalise le renouvellement du secret et la nouvelle adresse.

Le candidat doit décrire dans son mémoire technique les modalités de réassortiment, qu'il propose pour chaque catégorie d'utilisateurs de la SVE ainsi que pour chaque identifiant et chaque moyen d'authentification attribués à ces utilisateurs. Il doit identifier les canaux de communication utilisés par chaque fonction de réassortiment et préciser les procédures sécurisées de communication qu'il associe à l'utilisation de ces canaux en insistant sur la méthode proposée pour s'assurer de l'identité de l'émetteur de la demande de réassortiment.

2.3. Authentification des utilisateurs avec pouvoirs

Pour chaque autorité organisatrice de scrutins, le SyVE requiert l'authentification des utilisateurs avec pouvoirs (membres des BCVE, des BVE, de la CST et du CA, gestionnaires candidatures et notices, c'est à dire tous les utilisateurs à l'exception des électeurs, avec un cas particulier pour les candidats, voir section 2.4) pour se connecter au portail Gestion.

Le GC-MTEA autorité organisatrice pourra opter pour l'une des deux options présentées ci-dessous lorsqu'un utilisateur avec pouvoirs doit jouer plusieurs rôles : un identifiant/compte par rôle, ou bien un identifiant/compte unique qui rassemble tous ses rôles.

Cette authentification repose sur :

- Soit un identifiant créé par le SyVE attribué à chaque profil dont dispose chaque utilisateur avec pouvoirs, un même identifiant ne pouvant être attribué à deux utilisateurs ou deux profils différents. Un agent qui est membre d'un BCVE et membre d'un BVE va donc disposer de deux identifiants (et donc de deux comptes) d'utilisateur avec pouvoirs : un en qualité de membre du BCVE et un autre, différent du précédent, en qualité de membre du BVE.
- Soit un identifiant unique (et donc un compte unique), éventuellement déjà connu de l'utilisateur adresse mail, à défaut matricule) qui lui permet de se connecter aux différents portails selon le rôle qui est le sien. Dans ce cas, il n'existe qu'un compte par utilisateur avec pouvoirs et c'est le SyVE qui gère ses droits d'accès en fonction de ses différents rôles. Un agent qui est membre d'un BCVE et membre d'un BVE va donc disposer d'un seul identifiant d'utilisateur avec pouvoirs : et il pourra ensuite accéder à toutes les fonctions associées à sa qualité de membre du BCVE et à sa qualité de membre du BVE. Dans tous les cas, un même identifiant ne peut être attribué à deux utilisateurs différents.
- Un mot de passe fort, secret uniquement connu de l'utilisateur.

Le SyVE génère pour chaque utilisateur un lien de connexion à usage unique, lien qui lui est envoyé par courriel. En utilisant ce lien, l'utilisateur active son compte et définit son mot de passe à sa première connexion.

La politique relative aux mots de passe pour les utilisateurs avec pouvoirs est paramétrable : longueur, jeu de caractères utilisés.

L'analyse de risques peut conduire à décider que pour tout ou partie des utilisateurs avec pouvoirs, le SyVE requiert l'usage d'un second facteur d'authentification qui peut soit être créé par le SyVE soit faire l'objet d'une procédure d'enrôlement qui est réalisée lors de la première connexion.

L'utilisateur avec pouvoirs dispose d'une fonction « mot de passe oublié » (réassortiment) qui renvoie un lien à usage unique pour réinitialiser son mot de passe.

L'ensemble des procédures relatives aux exigences de cette section sont regroupées dans une PES « Identification et authentification ». Cette PES est rédigée par l'autorité organisatrice.

2.4. Authentification des candidats

L'outil de gestion des candidatures et de la propagande, objet de la prestation 9, possède deux populations d'utilisateurs :

- Les membres de l'équipe de gestion du référentiel des candidatures. Représentants de l'autorité organisatrice de scrutins, leurs comptes sont gérés comme des comptes d'utilisateurs avec pouvoirs (section 2.3) ;
- Les candidats qui déposent une liste de candidatures.

Les comptes des candidats sont gérés de la façon suivante :

- La création d'un compte est en libre-service. Le candidat fournit une adresse email qui lui servira d'identifiant, et choisit un mot de passe.
- Le mot de passe choisi par le candidat est conforme à la politique paramétrable des moyens d'authentification des candidats (longueur minimale, jeu de caractères utilisés).
- La conservation de ce mot de passe par le SyVE est conforme aux exigences de la section 8.
- Le candidat peut utiliser une fonction « mot de passe oublié » qui renvoie un lien à usage unique pour réinitialiser son mot de passe.

2.5. Protection des authentifications contre les attaques

Le SyVE comporte un mécanisme pour le protéger contre les attaques par recherche d'authentifiants telles que notamment :

- L'attaque par force brute qui, selon la CNIL, consiste à tester, l'une après l'autre, chaque combinaison possible d'un mot de passe ou d'une clé pour un identifiant donné afin se connecter au service ciblé ;
- L'attaque par pulvérisation de mots de passe ou « *password spraying* ». C'est un type d'attaque par force brute où l'attaquant utilise la même combinaison sur plusieurs comptes utilisateurs avant d'en essayer une autre. L'efficacité de cette attaque repose sur le constat que de nombreux utilisateurs utilisent des authentifiants simples et faciles à deviner. La pulvérisation de mots de passe se distingue par le fait qu'elle peut cibler de très nombreux comptes utilisateurs différents simultanément plutôt qu'un seul compte ;
- Les attaques par bourrage d'authentifiants ou « *credential stuffing* ». Selon la CNIL, elle consiste à réaliser des tentatives d'authentification massives en exploitant des listes de couples [identifiants/mots de passe] qui sont disponibles notamment à la suite d'une fuite de données. Cette attaque ne semble pas adaptée pour cibler un compte utilisateur en particulier et elle suppose que le SyVE exploite des identifiants utilisateurs de conception identique à ceux proposés dans les listes disponibles sur le *dark web*. Toutefois, si cette dernière condition est remplie, l'automatisation de l'attaque permet d'espérer trouver dans chaque liste exploitée un voire plusieurs couples [identifiant/authentifiant] qui vont être validés par le SyVE pour ensuite conduire à autoriser un accès illégitime.

Un mécanisme de protection des secrets contre de telles attaques peut s'appuyer sur un nombre limité d'échecs dans les tentatives d'authentification avant que le compte de l'utilisateur ne soit verrouillé et qu'un délai d'attente incompressible et croissant soit appliqué pour permettre une nouvelle tentative d'authentification. Il est aussi recommandé de recourir à des l'utilisation de « captcha » pour s'assurer que l'utilisateur formulant sa demande d'accès au SyVE est bien une personne physique.

Ces mécanismes de protection sont appliqués pour toutes les populations d'utilisateurs de la SVE.

Rappel : le candidat doit décrire dans son mémoire technique les mécanismes de protection des fonctions d'identification et d'authentification qu'il propose pour chaque catégorie d'utilisateurs de la SVE, ainsi que les formalisations qu'il propose pour chaque identifiant et chaque secret attribués à ces utilisateurs.

2.6. Durée des sessions

Le SyVE impose une déconnexion automatique de l'électeur (portails B1 et B2) ou de l'utilisateur (portail B3) après un certain délai d'inactivité. Ces délais ou durées d'inactivité sont paramétrables indépendamment pour chaque population.

Une session d'électeur est déconnectée après dix (10) minutes d'inactivité par défaut, et l'électeur en est tenu informé en temps réel.

Conformément aux dispositions de l'article R. 211-563 du CGFP, le SyVE permet à l'électeur qui s'est connecté avant l'heure limite de terminer son ou ses votes dans les trente (30) minutes qui suivent tant qu'il ne se déconnecte pas. Un message d'alerte informe l'électeur du temps qui lui reste pour voter.

Une session d'utilisateur avec pouvoirs (portail B3) est déconnectée après trente (30) minutes d'inactivité par défaut.

2.7. Séparation des privilèges

Pour les utilisateurs avec pouvoirs, les privilèges associés à chaque profil d'utilisateurs doivent correspondre à la matrice présentée dans l'annexe I relative aux exigences fonctionnelles, section « Matrice des profils ».

Toute usurpation de privilèges par un utilisateur (activation illégitime d'une fonction), ou toute tentative d'usurpation, est détectée, tracée et signalée sans délai à l'autorité organisatrice.

Rappel : le candidat doit préciser dans son mémoire technique quels sont les mécanismes qu'il propose de mettre en œuvre pour protéger les droits et privilèges de chaque utilisateur contre notamment les attaques en usurpation.

3. Traçabilité et intégrité

3.1. Traçabilité fonctionnelle

Le SyVE trace les événements effectués avant, pendant et après l'élection dans une table d'audit.

Les événements relatifs à la configuration, aux étapes de l'élection et à la sécurité du SyVE sont tracés, et notamment :

- Les connexions et déconnexions d'un électeur et d'un utilisateur avec pouvoirs ;
- L'accès en lecture ou modification aux informations relatives à la configuration et à la tenue des scrutins : les informations concernées, l'action effectuée, la valeur avant et après ;
- Les modifications des privilèges associés à un profil ou à un compte d'utilisateur avec pouvoirs ;
- Les traitements du SyVE (opération, comptes rendus de traitement, flux entrants et sortants du SyVE).

Chaque entrée de la table d'audit inclut un horodatage et lorsque ces informations sont pertinentes : le scrutin, le type d'événement, l'identification de l'électeur ou de l'utilisateur avec pouvoirs concerné et l'adresse IP d'origine.

Le contenu de la table d'audit est consultable et exportable depuis le portail B3. Une fonction de recherche du contenu permet de filtrer les entrées par date, scrutin, type d'événement, identification de l'électeur ou de l'utilisateur avec pouvoirs concerné, et d'y rechercher une chaîne de textes.

Le titulaire fournit en début de projet un lexique des types d'événements permettant leur interprétation.

Note : le contenu de la table d'audit ne permet pas d'établir un lien entre l'électeur et l'expression de son vote, comme décrit dans la section 6.5.

3.2. Interventions et traçabilité techniques

Les exigences de cette section s'appliquent pendant la période d'avant-vote et pendant la période de vote, jusqu'à la réalisation de l'archivage prévu à la section 3.6

Les interventions sur le SyVE sont réservées aux seules personnes chargées de la gestion et de la maintenance de ce système et ne peuvent avoir lieu qu'en cas de risque d'altération de la sécurité de la SVE ou des données. Toutes ces interventions sont tracées et documentées.

L'article R. 211-571 du CGFP précise que les bureaux de centralisation du vote électronique, les bureaux de vote électronique et la cellule de supervision technique sont immédiatement tenus informés des interventions techniques sur le SyVE ainsi que des mesures prises pour remédier au dysfonctionnement ayant motivé l'intervention.

En accord avec les procédures d'exploitation dont le PCA et le PRA, le titulaire informe préalablement de tout besoin d'intervention technique l'autorité organisatrice de scrutins et la CST. L'autorité organisatrice de scrutins ou la cellule autorisent ou pas l'intervention (article R. 211-551 du CGFP).

Cette information est complétée par un mécanisme d'alerte automatique (voir la section 3.4).

Le SyVE conserve la trace horodatée de tous les accès et tentatives d'accès au système et de toute intervention.

Par ailleurs, les traces techniques correspondant au fonctionnement du SyVE sont également conservées à des fins d'audit. Cela concerne les événements techniques, tels que notamment les arrêts et redémarrages de tout ou partie du SyVE, les installations de correctifs et de mises à jour, les incidents réseaux.

Rappel : le candidat précise dans son mémoire technique les traces techniques relatives à l'hébergement qui sont disponibles.

Les traces du SyVE sont protégées en intégrité, contre toute modification non autorisée, et en confidentialité, c'est-à-dire un accès restreint en application du « besoin d'en connaître ».

Note : les traces techniques ne doivent pas permettre d'établir un lien entre l'électeur et l'expression de son vote, comme décrit dans la section 6.5.

L'ensemble des éléments physiques utilisés pour l'hébergement du SyVE demeure intact pendant toute la période de vote, et jusqu'à l'expiration du délai de recours contentieux après proclamation des résultats.

Pendant le scrutin et jusqu'à l'archivage (section 3.6), les traces techniques sont communiquées à la CST du scrutin sur simple demande et dans un format analysable.

3.3. Scellement du système de vote électronique

L'intégrité du système et des données du vote est contrôlée en permanence grâce à des scelllements. Un scellement consiste à apposer un cachet (signature numérique vérifiable) ou à prendre une empreinte numérique d'un contenu numérique et permettant de contrôler l'intégrité de ce contenu numérique en en détectant toute modification ultérieure.

L'article R. 211-541 du CGFP précise que le SyVE dispose de mécanismes de vérification de son intégrité couvrant :

- Les applications de vote (serveur et client) dont les programmes exécutables, les scripts et les ressources associées ;
- Le schéma de la base de données ;
- La configuration et le paramétrage du SyVE dont ensemble des données relatives aux scrutins : liste des candidats, liste des électeurs, heures d'ouverture et de fermeture du scrutin, clé publique de chiffrement (article R. 211-541 du CGFP).

La vérification de l'intégrité du SyVE permet de confirmer sa correspondance avec le système audité et expertisé par l'affichage d'empreintes de référence comparables avec celles données par l'expert indépendant (article R. 211-541 du CGFP).

En conformité avec les exigences de la CNIL, le SyVE permet de procéder à des opérations de scellement successives sous la responsabilité de l'autorité organisatrice de scrutins :

- Avant l'ouverture de la période de vote : scellement des programmes de la solution, du schéma de la base de données, de la configuration et du paramétrage de solution dont la liste des candidats et la liste des électeurs ;
- A la clôture de la période de vote, après expiration du délai de grâce : scellement de l'urne, de la liste d'émargement et du compteur de votes (article R. 211-572 du CGFP) ;
- Après le dépouillement : le SyVE est scellé après la décision de clôture du dépouillement prise par le président du bureau de centralisation du vote électronique. Le scellement interdit toute reprise ou modification des résultats. Toutefois, dans le cas où le système de vote ne produit pas les preuves de bon déchiffrement (voir section 4.2), la procédure de décompte des votes doit pouvoir être exécutée de nouveau (article R. 211-575 du CGFP).

La vérification des scelllements est effectuée automatiquement de manière périodique incluant une part d'aléa afin de rendre les contrôles non prévisibles. La fréquence des contrôles est suffisante pour dissuader une tentative d'intervention non autorisée sur le SyVE, et pour assurer une détection rapide de toute altération.

La vérification des scelllements peut aussi se faire à tout moment, y compris durant la période de vote, à l'initiative des membres des BCVE, des BVE, et de la CST (article R. 211-542 du CGFP). Ces membres doivent disposer d'outils dont l'utilisation ne requiert pas l'intervention du titulaire pour procéder à la vérification des scelllements, dans le portail B3.

Toute rupture d'intégrité déclenche une alerte immédiate et automatique à la CST de l'autorité organisatrice de scrutins.

Les scelllements du SyVE s'appuient sur des algorithmes conformes aux exigences de la section 8.

Rappel : le candidat présente dans son mémoire technique les mécanismes de scellement mis en œuvre par sa SVE et documente les outils intégrés au SyVE pour contrôler automatiquement comme manuellement l'intégrité du scellement.

3.4. Alertes

A compter du scellement, le système envoie automatiquement et immédiatement des alertes par des canaux qui auront été validés par l'autorité organisatrice (notamment courriel ou SMS) aux membres de la CST dans les cas suivants :

- Détection d'une rupture de scellement ;
- Accès ou tentative d'accès à certains types de compte avec pouvoir sur le portail B3. La liste des types de comptes à superviser sera fournie par l'autorité organisatrice ;
- Création, modification ou suppression de profils ou de comptes d'utilisateur avec pouvoir ;
- Accès ou tentative d'accès à l'infrastructure technique.

Le système d'alerte ne peut pas être désactivé. La liste des destinataires comme le système sont protégés pour en garantir l'intégrité.

La prise en compte de l'objectif de sécurité n° 2-03 de la CNIL, comme des dispositions du CGFP conduit l'autorité organisatrice de scrutins à compléter les mécanismes de journalisation par la mise en œuvre d'un outil d'analyse temps réel tel qu'un SIEM. Le titulaire est tenu d'apporter son concours à l'autorité organisatrice pour la mise en conformité de l'ensemble des journaux, traces et logs du SyVE et pour leur envoi vers tout outil de traitement temps réel qui sera retenu par l'autorité organisatrice.

3.5. Intégrité de l'urne et de l'émargement

Les données relatives aux électeurs ayant voté d'une part et les données relatives à l'expression de votes (bulletins chiffrés) d'autre part font l'objet de traitements informatiques distincts et dédiés, respectivement dénommés « liste d'émargement » et « urne électronique » (article R. 211-512 du CGFP). Le compteur de votes indique le nombre de votes ayant été validés. Ces traitements sont spécifiques à chaque scrutin (article R. 211-509 du CGFP).

Durant la période de vote, l'intégrité de l'urne électronique, ainsi que celles du compteur de votes et de la liste d'émargement de chaque scrutin est garantie. L'urne et le compteur de votes, d'une part, et la liste d'émargement, d'autre part, ne peuvent ainsi être modifiés respectivement que par l'ajout d'un bulletin de vote et par l'ajout d'un émargement (article R. 211-569 du CGFP) :

- La validation du vote entraîne l'ajout d'une entrée horodatée dans la liste d'émargement (article R. 211-568 du CGFP) ;
- La validation du vote entraîne l'ajout du bulletin dans l'urne. Cet ajout ne comporte pas d'horodatage, pour éviter tout rapprochement avec la liste d'émargement ;
- Les ajouts de l'entrée horodatée à la liste d'émargement et du bulletin dans l'urne sont réalisés comme une opération atomique ;
- La validation rend définitif le vote et interdit toute modification ou suppression du bulletin de vote déposé dans l'urne (article R. 211-566 du CGFP).

Le SyVE interdit à quiconque de voter de nouveau pour le même scrutin avec le même identifiant d'électeur (article R. 211-562 du CGFP).

La liste d'émargement et le compteur de votes ne sont accessibles qu'aux membres des BCVE et BVE responsables du scrutin visé et aux membres de la CST, aux seules fins de contrôle du déroulement du scrutin (article R. 211-570 du CGFP), et des outils de recherche sont prévus (filtres).

Rappel : le candidat présente dans son mémoire technique les fonctionnalités du portail Gestion proposées aux membres des BCVE, des BVE et de la CST pour leur permettre de contrôler le déroulement du scrutin.

3.6. Archivage *ad probationem* et conservation

A la fin des opérations électorales, le titulaire transfère à l'autorité organisatrice de scrutins une copie des informations suivantes pour archivage (article R. 211-580 du CGFP) :

- Les fichiers supports comprenant notamment la copie des programmes sources et des programmes exécutables constituant le SyVE ;

- Les clés publiques de chiffrement ;
- Les fichiers relatifs aux référentiels des candidatures, déclarations de candidatures et des professions de foi ;
- Les fichiers relatifs aux opérations de vote pour chaque scrutin : la liste des électeurs, la liste d'émargement, le compteur des votes et l'urne dans leurs états avant et après dépouillement ;
- Les fichiers et procès-verbaux des opérations électorales ;
- Le cas échéant, les preuves mathématiques produites lors du dépouillement par des mécanismes de vérifiabilité universelle, attestant de la validité du décompte des suffrages par rapport au contenu de l'urne électronique ;
- Le cas échéant, si la possibilité d'un rejeu est souhaitée (en particulier en l'absence des preuves mathématiques), les fragments de chaque clé privée de déchiffrement et les codes d'activation, dans des conditions qui en garantissent la confidentialité, y compris contre les attaques par force brute des codes d'activation ;
- Les fichiers de sauvegarde ;
- L'export de la table d'audit retraçant les événements relatifs à la configuration, aux étapes de l'élection et à la sécurité du SyVE (voir 3.1), dans leurs états avant et après dépouillement ;
- Les fichiers retraçant les interventions techniques du titulaire sur le SyVE et les traces techniques (voir 3.2).

Ces informations sont accompagnées d'empreintes de référence et de procédures permettant d'en vérifier l'intégrité.

Ces informations sont accessibles aux membres habilités de l'autorité organisatrice de scrutins pendant toute la période de leur conservation légale, de façon autonome vis-à-vis du titulaire (article R. 211-581 du CGFP).

Rappel : le candidat doit préciser dans son mémoire technique quelles sont les modalités qu'il propose pour constituer cet archivage *ad probationem* et le transmettre à l'autorité organisatrice. Il apporte une attention particulière à la documentation de la transmission des copies non-chiffrées des programmes sources et exécutables du SyVE, ainsi qu'à la présentation des procédures permettant à l'autorité organisatrice de contrôler l'intégrité des données transmises.

L'article R. 211-575 du CGFP précise que, dans le cas où le SyVE ne produit pas la preuve mathématique mentionnée en section 4.2, la procédure de décompte des votes doit pouvoir être exécutée de nouveau (rejeu). Il est demandé au candidat de spécifier et documenter une procédure de rejeu de décompte dans son mémoire technique, en précisant si l'autorité organisatrice pourra effectuer ce rejeu en autonomie.

4. Transparence de l'urne

4.1. Vérifiabilité individuelle et preuve de vote

L'article R. 211-568 du CGFP prévoit que le vote et l'émargement font l'objet d'un accusé de réception que l'électeur doit pouvoir conserver. L'électeur doit également pouvoir vérifier que son vote a bien été pris en compte. La validation du vote par le serveur de vote entraîne donc la délivrance à l'électeur de deux éléments bien distincts : un accusé de réception et une preuve de vote :

- L'accusé de réception ne contient aucune information sur le bulletin de vote déposé dans l'urne. Il identifie l'électeur et le scrutin auquel il a voté. Il est horodaté et porter la même information d'horodatage que la liste d'émargement ;
- La preuve de vote est distincte de l'accusé de réception. Elle est délivrée à l'électeur en conséquence de la validation de son vote, elle ne peut pas être récupérée ou régénérée plus tard et elle n'est pas conservée par le serveur de vote.

La preuve de vote ne doit pas pouvoir compromettre de quelque manière que ce soit le secret du vote. Elle est donc anonyme et ne doit pas comporter d'information permettant d'établir un lien avec l'électeur. Elle ne doit en aucun cas être horodatée afin de ne pas pouvoir être utilisée pour faire un rapprochement entre le bulletin chiffré déposé dans l'urne et la liste d'émargement. La preuve de vote, seule ou avec les données de l'accusé de réception, ne permet pas à l'électeur de prouver son choix (intention) de vote à un tiers.

Chaque preuve de vote contient une référence cryptographiquement liée au bulletin (par exemple une empreinte numérique du bulletin ou bien une preuve à divulgation nulle de connaissance), qui est calculée au moment où le votant valide son choix de vote. Cette référence est calculée par le client de vote. Le client de vote garantit que la référence figurant sur la preuve de vote correspond au bulletin chiffré que le client de vote a généré pendant le vote de l'électeur et transmis au serveur de vote pour être déposé dans l'urne du scrutin.

Les informations pertinentes de la preuve de vote sont signées cryptographiquement par le serveur de vote pour garantir leur authenticité, avec un algorithme conforme aux exigences de la section 8. La clé publique de signature est mise à disposition de tiers pour permettre la vérification de la signature.

Le serveur de vote publie les références présentes dans les preuves de vote (par exemple, la liste des empreintes) sur une page Web accessible sans restriction et mise à jour en temps réel pendant le scrutin.

Chaque électeur doit pouvoir, sans avoir à s'authentifier :

- Contrôler que la référence présente dans sa preuve de vote et correspondant à son bulletin est bien présente dans la liste des références publiée par le SyVE ;
- Pendant la période de vote, utiliser cette preuve de vote pour vérifier la présence de son bulletin chiffré dans l'urne ;
- Après le dépouillement et jusqu'à l'extinction du délai de cinq (5) jours de contestation des opérations électorales, utiliser cette preuve de vote pour vérifier que son bulletin chiffré était dans l'urne qui a été dépouillée ;
- Pendant la période de vote, après le dépouillement et jusqu'à l'extinction du délai de cinq (5) jours après la proclamation des résultats, vérifier la validité de la signature présente sur la preuve de vote.

Les paragraphes suivants décrivent des recommandations de l'ANSSI applicables aux scrutins de niveau 3 (au sens de la CNIL).

Pour les scrutins de niveau 3, le titulaire publie des spécifications pour l'implémentation d'un outil de vérifiabilité individuelle par un tiers. En amont du scrutin, le titulaire publie une spécification détaillant la constitution des preuves de vote et une spécification d'un outil permettant de les vérifier.

Ces spécifications permettent 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, indépendamment du SyVE. Cet outil permet à un tiers disposant de l'urne électronique, non accumulée ou non mélangée, de réaliser les vérifications. Ces spécifications décrivent notamment :

- 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, et les modalités d'accès à cette page.

Le titulaire fournit également des jeux de données de tests permettant à un tiers de valider son implémentation.

Rappel : le candidat décrit dans son mémoire technique quels mécanismes de vérifiabilité individuelle il propose et quelles garanties ces mécanismes apportent à l'électeur, aux BVE et à l'autorité organisatrice de scrutins. Il doit préciser la forme et le contenu de l'accusé de réception et de la preuve de vote que la SVE délivre à chaque électeur une fois que son vote a été validé.

4.2. Vérifiabilité universelle

Le sujet de la vérifiabilité universelle, traité dans cette section, apparaît au niveau 3 de la délibération CNIL de 2019. Cependant, les preuves mathématiques qui permettent cette vérifiabilité servent également à remplir l'objectif de niveau 1 « S'assurer que le dépouillement de l'urne puisse être vérifié a posteriori » sans recourir au rejeu.

La vérifiabilité universelle résulte de la capacité de prouver mathématiquement que le résultat d'un décompte correspond au contenu d'une urne (ensemble des bulletins chiffrés). La vérifiabilité universelle apporte des garanties sur la sincérité du scrutin.

De plus, du point de vue du contrôle de l'élection par le juge, elle est une alternative au rejeu du décompte, qui requiert la conservation des fragments de la clé privée de déchiffrement et qui peut porter atteinte au secret du vote.

La vérifiabilité universelle dépend des mécanismes de chiffrement et déchiffrement des bulletins et de leurs modalités de mise en œuvre par la SVE. Sans constituer une exigence de choix pour l'algorithme de chiffrement, l'apport à la vérifiabilité universelle de trois solutions de chiffrement sont ci-après décrits.

Dans le cas où le chiffrement des bulletins est réalisé avec un chiffrement *ElGamal* en réalisant une accumulation (voir section 8.1) :

- Le bulletin de vote contient des preuves à divulgation nulle de connaissance attestant que le bulletin est bien formé et qu'il contient un vote unique et valide (éventuellement blanc) ;
- Le processus de déchiffrement de l'accumulation de l'urne produit, en plus du décompte, des preuves à divulgation nulle de connaissance attestant que le déchiffrement, ou les déchiffrements partiels, de l'accumulation ont été correctement réalisés ;
- La combinaison de deux types de preuves atteste que le décompte correspond à l'urne avant accumulation et que les bulletins étaient bien formés ;
- Les preuves associées aux bulletins et les preuves de bon déchiffrement peuvent être vérifiées par une fonction du portail Gestion, dans un temps court compatible avec une exécution devant le BCVE, ou le BVE s'il n'est pas rattaché à un BCVE, pendant la cérémonie de dépouillement ;
- Ces preuves, ainsi que toutes les autres données nécessaires à leur vérification dont l'urne, sont conservées dans le cadre de la procédure d'archivage prévue par la section 3.6.

Dans le cas où le chiffrement des bulletins est réalisé avec un chiffrement *ElGamal* sans réaliser d'accumulation (voir section 8.2) :

- Le bulletin de vote contient des preuves à divulgation nulle de connaissance de l'aléa utilisé pour réaliser le chiffrement ;
- Le processus de mélange par rechiffrement produit des preuves de bon mélange ;
- Le processus de déchiffrement produit, en plus du décompte, des preuves à divulgation nulle de connaissance attestant que le déchiffrement, ou les déchiffrements partiels, des bulletins ont été correctement réalisés ;
- La combinaison des trois types de preuve atteste que le décompte correspond à l'urne avant mélange ;
- Les preuves de bon mélange et de bon déchiffrement peuvent être vérifiées par une fonction du portail Gestion, dans un temps court compatible avec une exécution devant le BCVE, ou le BVE s'il n'est pas rattaché à un BCVE, pendant la cérémonie de dépouillement ;
- Ces preuves, ainsi que toutes les autres données nécessaires à leur vérification dont l'urne, sont conservées dans le cadre de la procédure d'archivage prévue par la section 3.6.

Dans le cas où le chiffrement des bulletins est réalisé avec *RSA*, le candidat décrit dans son mémoire technique quelles preuves (mélange, déchiffrement) sont générées par le SyVE.

Le titulaire publie des spécifications pour l'implémentation d'un outil de vérifiabilité universelle par un tiers. En amont du scrutin, le titulaire publie une spécification détaillant la constitution des preuves de déchiffrement ainsi que la spécification d'un outil permettant de vérifier ces preuves. Ces publications permettent à un tiers de développer un outil de vérification des preuves, indépendamment du SyVE.

Cet outil permet à un tiers disposant de l'urne électronique, non accumulée ou non mélangée, de réaliser les vérifications. 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 titulaire fournit également des jeux de données de tests permettant à un tiers de valider son implémentation.

Rappel : le candidat décrit dans son mémoire technique quels mécanismes de vérifiabilité universelle (preuves de bon déchiffrement, preuves de bon mélange, outils de vérification) il propose et quelles garanties ces mécanismes apportent à l'électeur, aux BVE et à l'autorité organisatrice de scrutins.

4.3. Publication du protocole de vote

En amont du scrutin, le titulaire publie les spécifications du protocole de vote qu'il met en œuvre dans le SyVE.

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.

Les spécifications du protocole de vote 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, BVCE ou BVE) ;
- La description des cérémonies actées par l'autorité organisatrice du scrutin, notamment celles faisant intervenir le BCVE ;
- 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), sur la base des spécifications publiées. Un point de contact doit être identifié pour rendre possible la divulgation responsable d'éventuelles faiblesses identifiées par les tiers.

4.4. Publication du code source du client de vote

En amont du scrutin, le titulaire publie 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'obfuscation et doit correspondre à celui transmis aux électeurs par le serveur de vote.

La publication par le titulaire du code source en libre accès sur Internet permet sa revue par des tiers sans inscription préalable, sans préjudice de la propriété intellectuelle du Titulaire sur ce code source.

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.

4.5. Information des électeurs relative à la sécurité et à la fiabilité

L'article R. 211-553 du CGFP précise que le cas échéant, le prestataire de la SVE doit rédiger un document décrivant les principales modalités permettant de garantir la sécurité et la fiabilité de sa SVE. Ce document doit être communiqué aux électeurs au plus tard quinze (15) jours avant l'ouverture de la période de vote.

Le titulaire fournit ce document à chaque autorité organisatrice de scrutins, accompagné d'une notice d'information détaillée sur le déroulement des opérations électorales (voir section 1).

Ce document est rédigé en termes simples. Il permet à l'électeur de saisir les principaux enjeux relatifs au vote par Internet (voir section 1) et comment le SyVE répond à ces enjeux.

5. Disponibilité

5.1. Engagement de disponibilité

Ces développements relatifs aux engagements de disponibilité sont complémentaires à l'annexe II relative aux exigences techniques, section « Objectifs de disponibilité et de performance ».

La disponibilité du modèle de sécurité DICT (disponibilité, intégrité, confidentialité, traçabilité) peut être définie comme la « *propriété d'une information ou d'un traitement d'être exploitable dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, par une entité* ». Le terme « entité » est défini comme étant tout élément d'un système d'information susceptible d'être considéré individuellement, ce qui inclut notamment les personnes, processus et composant matériels comme logiciels.

Mais la disponibilité ou opérabilité est aussi une propriété d'un système d'information susceptible de traduire la facilité avec laquelle il est possible d'accéder aux données ou aux ressources du système dans un format exploitable. Cette propriété est alors associée à la rapidité avec laquelle le système d'information peut se rétablir lorsqu'un incident se produit ou lorsqu'une partie de ce système devient indisponible quelle qu'en soit la raison.

Des métriques associées à cette propriété de disponibilité du SyVE sont donc déjà développées dans le document corps du CCTP consacré à la prestation 7 d'assistance aux utilisateurs et dans l'annexe II des exigences techniques :

Période	Métrique	Valeur
Avant-vote et hors période de saisie des candidatures	GTR	huit (8) heures
	DIMA	huit (8) heures
Saisie des candidatures	GTR	quatre (4) heures
	DIMA	quatre (4) heures
Cérémonies	GTI	cinq (5) minutes
	GTR	une (1) heure
	DIMA	une (1) heure
	Durée d'indisponibilité cumulée tolérée pour l'ensemble des cérémonies	une (1) heure
Vote	GTR	une (1) heure
	DIMA	une (1) heure
	Durée d'indisponibilité cumulée tolérée pour toute la période	quatre (4) heures
Post-vote	GTR	quatre (4) heures
	DIMA	huit (8) heures

Période	Métrique	Valeur
Ensemble des périodes de vote sauf cérémonies	GTI	quinze (15) minutes
Ensemble des périodes	PDMA	Aucune
	Taux de disponibilité SVE	Au moins 99.5%

Ces exigences s’appliquent quelle que soit la nature de l’incident (incident relatif à la sécurité, aux performances, à l’exploitation du SyVE ou à ses fonctionnalités). Le cas échéant, une page d’information (indiquant la coupure de service) doit être affichée à destination des électeurs et des utilisateurs avec pouvoirs.

Pendant la période d’avant-vote, seules sont admises les interruptions de service qui sont validées conjointement par le titulaire et la direction projet du GC-MTEA autorité organisatrice et à condition que ces interruptions soient nécessaires notamment :

- Aux mises à jour requises pour prévenir des cas d’attaque malveillante ou de panne du SyVE ;
- Aux mises à jour du patrimoine informationnel telles que pour l’injection d’une nouvelle version de référentiel Electeurs ou encore l’injection d’une nouvelle version de référentiel de candidatures.

5.2. Mise en œuvre de la disponibilité

Le titulaire fournit un SyVE qui permet d’exécuter des prestations relatives à la disponibilité. Ces prestations comportent à minima :

- La sauvegarde des environnements et des données ;
- La formalisation d’un PCA et d’un PRA incluant notamment les procédures de restauration des environnements et des données à partir des sauvegardes.

Dans ce contexte, le titulaire décrit et met en place une organisation, des procédures et des moyens matériels (dont des hébergements dans des centres de données) et logiciels permettant de détecter rapidement la survenance des incidents et d’assurer la continuité d’activité et si possible, de procéder au retour à un fonctionnement nominal dans le respect des obligations de GTI et GTR.

L’article R. 211-514 du CGFP précise que pendant toutes les périodes de fonctionnement du SyVE, celui-ci peut basculer du dispositif principal vers un dispositif de secours offrant les mêmes garanties et les mêmes caractéristiques que ce dispositif principal. Le dispositif de secours prend automatiquement et sans délai le relais en cas de panne ou d’incident technique n’entraînant pas d’altération des données. Il est donc exigé en annexe II que l’infrastructure d’hébergement repose sur un mode actif/actif de redondance.

5.3. Perte de données maximale acceptable

Comme indiqué dans l’annexe II relative aux exigences techniques, la perte de données maximale acceptable (PDMA) demandée est de 0 minute. Cela signifie qu’aucune donnée ne doit être perdue, quel que soit l’incident ou la panne qui touche le SyVE.

Si le SyVE ne permet pas d’atteindre une PDMA nulle, alors des votes peuvent être perdus lors d’un incident et d’une bascule vers le dispositif de secours. Dans ce cas, il sera nécessaire de communiquer vers les électeurs dont le ou les votes sont susceptibles d’avoir été perdus pour les inviter à voter à nouveau.

Rappel : le candidat explicite dans son mémoire technique les mesures prises pour répondre à l’exigence d’une PDMA nulle. S’il ne propose pas de PDMA nulle, il doit décrire dans son mémoire technique la procédure qui permet d’identifier et d’informer les électeurs dont le ou les votes pourraient avoir été perdus lors d’un incident et comment il peut garantir que cette procédure est en mesure d’identifier sans erreur ces votes susceptibles d’avoir été perdus.

5.4. Indépendance des scrutins

L'article R. 211-513 du CGFP précise que si un même SyVE vient à être utilisé pour plusieurs scrutins, chacun de ces scrutins doit être cloisonné de manière à pouvoir être interrompu sans conséquence sur les autres scrutins en cours.

La délibération CNIL n° 2019-053 (objectif de sécurité n°3-05) en vigueur à la date de l'élaboration du CCTP n'autorise que le cloisonnement physique.

Le type de cloisonnement à mettre en œuvre, physique ou virtuel, est à déterminer selon la délibération CNIL en vigueur.

En effet, ce cloisonnement peut être assuré logiquement au sein de l'application (un seul SyVE gérant plusieurs scrutins indépendants), logiquement au niveau système (par exemple un SyVE virtuel par scrutin) ou physiquement (un SyVE physique par scrutin).

Rappel : le candidat explicite dans son mémoire technique les mesures de cloisonnement et d'indépendance des scrutins qu'il met en œuvre.

6. Confidentialité

6.1. Protection de la confidentialité sur le poste de l'électeur

Le titulaire met en œuvre toutes les mesures de l'état de l'art permettant l'intégrité et à la confidentialité du vote de l'électeur sur le poste informatique à partir duquel ce dernier a accès au portail Electeur, tant que ce poste et le navigateur de l'électeur sont intègres. Ces mesures incluent :

- Les bonnes pratiques décrites dans le guide « Recommandations pour la mise en œuvre d'un site Web : maîtriser les standards de sécurité côté navigateur » de l'ANSSI ;
- Des mesures empêchant quelqu'un qui accèderait au poste après le chiffrement du vote d'un électeur, d'obtenir des informations sur ce vote, directement à l'écran, via la fonction « Retour » du navigateur, via les cookies, via le cache du navigateur, via aucun autre canal ou via tout autre mécanisme. Aucune trace de participation d'un électeur à un scrutin ne doit pouvoir subsister sur la machine utilisée une fois l'électeur déconnecté de la plateforme de vote.

6.2. Chiffrement du bulletin de vote

L'article R. 211-567 du CGFP prévoit que le bulletin de vote de l'électeur est chiffré dès son émission sur le poste de l'électeur et stocké dans l'urne jusqu'au dépouillement, sans que ce chiffrement n'ait été à aucun moment interrompu.

Le bulletin de vote est chiffré par la clé publique associée au scrutin pour lequel ce bulletin est émis (voir section 6.4).

Le bulletin de vote est chiffré grâce à un algorithme conforme aux exigences de la section 8.

Rappel : le candidat décrit dans son mémoire technique le mécanisme utilisé pour le chiffrement des bulletins, ainsi que ses paramètres (taille de clé, courbe...).

6.3. Chiffrement des communications réseau

L'accès des utilisateurs (électeurs et utilisateurs avec pouvoirs) aux portails Electeurs et Gestion du SyVE s'effectue exclusivement avec le protocole HTTPS. Le SYVE met en œuvre le protocole TLS en conformité avec le guide de l'ANSSI « Recommandations de sécurité relatives à TLS ».

De plus, tous les échanges de données par lien réseau au sein du SyVE sont chiffrés en utilisant le protocole TLS ou un équivalent à l'état de l'art. Ces échanges incluent les communications entre les composants du SyVE que sont notamment les pare-feux applicatifs, les serveurs Web, les serveurs applicatifs, les bases de données.

6.4. Clés de l'élection

Une paire associant une clé publique de chiffrement des bulletins de vote et une clé privée de déchiffrement est générée (établie) pour chaque ensemble de scrutins dont un BCVE est responsable. Si un BVE n'est pas rattaché à un BCVE, une paire est générée pour le scrutin dont le BVE est responsable.

La clé privée de déchiffrement est générée et fragmentée grâce à un algorithme conforme aux exigences de la section 8.

L'article R. 211-545 du CGFP précise que les fragments de la clé privée de déchiffrement sont attribués aux membres des BCVE (ou, en l'absence de BCVE, aux membres du BVE) dans les conditions suivantes :

- Au moins un fragment de la clé privée de déchiffrement, associée à la clé publique de chiffrement, est attribué au président du BCVE (ou BVE si ce dernier n'est pas rattaché à un BCVE), ainsi qu'au secrétaire de ce bureau ;
- Au moins deux fragments de la clé privée de déchiffrement sont attribués à des délégués du BCVE (ou du BVE si ce dernier n'est pas rattaché à un BCVE) ;
- Au moins deux tiers des fragments de la clé privée de déchiffrement sont attribués aux délégués et à leurs suppléants ;
- Un même membre de BCVE (ou de BVE si ce dernier n'est pas rattaché à un BCVE) ne peut pas être attributaire de plus de deux fragments de la clé privée de déchiffrement ;
- Lorsqu'un délégué est attributaire d'un ou de deux fragments de la clé privée de déchiffrement, son suppléant est attributaire du même nombre de fragments de la clé de déchiffrement ;
- A chaque fragment de la clé privée de déchiffrement est associé un code d'activation. La procédure d'attribution des fragments de la clé privée de déchiffrement garantit à chaque attributaire qu'il a, seul, connaissance du code d'activation associé au fragment qui lui est personnellement attribué.

Chaque fragment de clé est enregistré individuellement en étant chiffré, en conformité avec les exigences de la section 8. Cet enregistrement peut être réalisé dans le SyVE, 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 lu ou utilisé qu'en connaissant le code d'activation.

Les codes d'activation ne sont pas enregistrés par le SyVE. Une empreinte de chaque code d'activation peut cependant être enregistrée par le SyVE.

L'article R. 211-573 du CGFP prévoit que la présence du président, ou du secrétaire en cas d'empêchement, du BCVE (ou du BVE si ce dernier n'est pas rattaché à un BCVE) et d'au moins deux délégués attributaires de fragments de la clé privée de déchiffrement doit être constatée pour procéder aux opérations de dépouillement. Leurs fragments de clé privée sont nécessaires pour procéder au dépouillement.

L'algorithme de fragmentation de la clé privée de l'élection et le mécanisme de dépouillement garantissent que les conditions de quorum prévues sont respectées :

- Que le fragment attribué au président, ou au secrétaire si le président est empêché, soit utilisé ;
- Que soit utilisé chaque fragment attribué à au moins deux délégués attributaires dont la présence physique pour la cérémonie de dépouillement a dûment été constatée ;
- Que les fragments attribués aux suppléants ne soient utilisables qu'en cas de remplacement du délégué par son suppléant, et à l'exclusion de l'utilisation du fragment du délégué qui est suppléé.

Une fois ces conditions remplies, le BCVE (ou le BVE si ce dernier n'est pas rattaché à un BCVE) peut décider d'utiliser les autres fragments de membres attributaires qui en feraient la demande.

Du point de vue organisationnel, le procès-verbal des opérations électorales fourni par le SyVE doit confirmer que ces conditions ont bien été remplies. Il doit notamment confirmer que le fragment de l'autorité organisatrice de scrutins utilisé est celui du membre de l'autorité organisatrice de scrutins qui préside la cérémonie de dépouillement ; et qu'au moins deux tiers des fragments utilisés ont été attribués à des délégués ou à leurs suppléants.

6.5. Anonymat du vote

L'article R. 211-567 du CGFP prévoit que le vote exprimé est anonyme. Il doit donc être impossible d'établir un lien entre un électeur et l'expression de son vote. Cette impossibilité s'applique à tous, et en particulier à l'autorité organisatrice de scrutins, au titulaire, aux membres des BCVE, des BVE et de la CST. Elle s'applique également à l'électeur lui-même pour éviter qu'il puisse se réclamer de son vote auprès d'un éventuel acheteur dudit vote.

Pour garantir l'anonymat, le SyVE est conforme aux exigences suivantes :

- Les traces des différents éléments intervenant dans la chaîne technique (pare-feux réseau et applicatif, répartiteurs de charge, serveurs Web, serveurs applicatifs) ne peuvent pas être recoupées et interprétées pour reconstituer un lien entre l'électeur et son bulletin chiffré ;
- Les bulletins de vote sont chiffrés grâce à un algorithme conforme aux exigences de la section 8, garantissant que seul le BCVE, ou le BVE s'il n'est pas rattaché à un BCVE, peut légitimement déchiffrer les bulletins ou l'accumulation des bulletins dans le cadre de la procédure de dépouillement.
- Avant le dépouillement, les bulletins chiffrés présents dans l'urne sont accumulés ou mélangés, pour éviter tout lien entre un bulletin chiffré et un bulletin déchiffré.
- La preuve de vote fournie à l'électeur (section 4.1), seule ou avec les données de l'accusé de réception, ne permet pas à l'électeur de prouver son choix (intention) de vote à un tiers.
- Les bulletins chiffrés dans l'urne ne sont pas horodatés afin de ne pas permettre un rapprochement entre le contenu de l'urne et la liste d'émargement.

Rappel : le candidat explicite dans son mémoire technique les mesures prises pour répondre à ces exigences.

6.6. Pastillage et anonymat du vote

Le pastillage consiste à rendre possible des extractions d'informations sur 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 de l'autorité organisatrice de scrutins ou des organisations syndicales. Les organisations syndicales sont particulièrement attentives au pastillage, qui constitue pour elles une utile source d'information et de vérification de la prise en compte de leur représentativité dans des instances où elles siègent sans élection directe. On parle alors de scrutin indirect *informatif*.

Le pastillage associe à un bulletin émis pour un scrutin *direct*, dans le respect du secret et de l'anonymat du vote, des attributs ou informations relatives à l'électeur (département d'affectation, appartenance à tel corps de fonctionnaires, etc.). Ces informations permettent, au moment du dépouillement, de fournir des résultats complémentaires ou indirects. Un scrutin indirect est ainsi défini comme le décompte de bulletins ayant un attribut particulier ou une combinaison particulière d'attributs.

La responsabilité de définir les scrutins indirects revient à l'autorité organisatrice de scrutins (cartographie de l'élection professionnelle dans son périmètre). Celle-ci tiendra notamment compte du nombre d'électeurs pour chaque scrutin indirect et du nombre potentiel de votants pour éviter tout dépouillement sur un nombre trop restreint de bulletins, conduisant à une atteinte à l'anonymat du vote.

Afin de respecter l'anonymat du vote, le SyVE, lors du dépouillement :

- Emet une alerte pour les scrutins indirects *constitutifs* pour lesquels le nombre de votants est inférieur à un seuil fixé par l'autorité organisatrice de scrutins ;
- Ne réalise pas de décompte pour les scrutins indirects *informatifs* pour lesquels le nombre de votants est inférieur à un seuil fixé par l'autorité organisatrice de scrutins.

Le seuil est fixé pour l'ensemble des scrutins. Il est identique pour les deux cas ci-dessus.

Par ailleurs, la mise en œuvre du pastillage est conforme aux exigences de la section 8.4.

Rappel : le candidat explicite dans son mémoire technique les modalités qu'il propose pour prendre en compte les besoins des autorités organisatrices de scrutins en termes de pastillage et notamment s'il existe une limite pour le nombre de pastilles susceptibles d'être affectées à chaque scrutin.

6.7. Accès aux données

L'article R. 211-570 du CGFP prévoit que durant la période de vote :

- Les fichiers comportant les éléments d'authentification des électeurs et le contenu de l'urne sont inaccessibles ;
- La liste d'émargement et le compteur de votes de chaque scrutin ne sont accessibles qu'aux membres du BVE du scrutin, et le cas échéant aux membres du BCVE auquel est rattaché le BVE, et uniquement à des fins de contrôle du déroulement du scrutin (sans aucune information nominative).
- Les listes d'émargement et les compteurs de votes de tous les scrutins sont accessibles aux membres de la CST à des fins de contrôle du déroulement du scrutin (sans aucune information nominative) ;
- Il ne peut être procédé à aucun décompte partiel en cours de scrutin.

La protection contre les accès illégitimes à certaines données peut s'appuyer sur du chiffrement. Le chiffrement est conforme aux exigences de la section 8. Le titulaire prévoit également des procédures détaillant les accès légitimes à ces données, notamment lors des actions d'autorité organisatrice technique.

Le titulaire s'engage à respecter ces dispositions par la signature, lors de l'attribution du marché, d'une annexe de sécurité valant clause de confidentialité et de sécurité (transmise dans le cadre de la prestation 1). Tous les co-traitants et sous-traitants sont également soumis à cette clause.

Le titulaire s'engage à restituer les fichiers restant en sa possession à l'issue des opérations électorales et à détruire toutes les copies totales ou partielles qu'il aurait été amené à effectuer sur quelque support que ce soit.;

6.8. Echanges sécurisés de données

Les fichiers constitués en vue de l'organisation et du déroulement de l'élection et contenant des informations confidentielles telles que notamment des données à caractère personnel, des données d'organisation, ou des secrets, font systématiquement l'objet d'une protection par chiffrement pour leur transmission et leur conservation.

Les mécanismes de chiffrement sont conformes aux exigences de la section 8.

Le cas échéant, une autorité organisatrice pourra décider d'utiliser un espace d'échange sécurisé existant, tel qu'OSMOSE.

Le titulaire met à la disposition du GC-MTEA et de chaque autorité organisatrice de scrutins et des autres acteurs du projet un espace d'échanges sécurisé permettant :

- L'authentification des acteurs ;
- La gestion des droits d'accès à des espaces correspondant au besoin d'en connaître de chacun ;
- La transmission des fichiers via un canal sécurisé ;
- La conservation des fichiers échangés sous forme chiffrée ;
- La garantie d'intégrité des fichiers lors de leur transport et de leur stockage ;
- La traçabilité des accès, consultations, dépôts et téléchargements ;
- La destruction sécurisée des éléments en fin de projet.

Il fournit à chaque utilisateur les codes d'accès permettant de s'authentifier. Si l'authentification s'appuie sur un mot de passe, l'utilisateur change son mot de passe à la première connexion.

6.9. Données à caractère personnel

L'article R. 211-583 du CGFP précise que les données personnelles des électeurs, des candidats, des délégués des organisations syndicales et des délégués de liste sont conservées de façon sécurisée pendant la durée nécessaire à la mise en place des instances ayant fait l'objet des scrutins en question.

Rappel : le candidat explicite dans son mémoire technique les procédures qu'il propose pour prendre en compte cette obligation pendant toute la durée du projet et communique sa déclaration de conformité au RGPD.

7. Sécurité physique et logique du système de vote électronique

7.1. Sécurité physique des locaux de développement et d'hébergement

Le titulaire s'engage à assurer une sécurité physique raisonnable des locaux où sont effectués les développements et des locaux où se déroulent les qualifications et les tests, interdisant l'accès d'un tiers non autorisé et permettant de protéger tout document sensible dans une armoire fermée à clé.

Les personnes habilitées à intervenir dans les locaux hébergeant le SyVE doivent faire l'objet d'une détermination préalable de leur besoin d'intervention sur le site et d'un contrôle d'accès strict.

Le titulaire doit remettre la liste de ses intervenants au GC-MTEA autorité organisatrice préalablement au commencement d'exécution de la prestation 1 de l'accord-cadre. Toute modification de cette liste venant à intervenir en cours d'exécution du marché doit être communiquée sans délai au GC-MTEA autorité organisatrice.

7.2. Développement sécurisé

Le titulaire s'engage à mettre en œuvre les bonnes pratiques de la profession en matière de développement sécurisé lors de la conception du SyVE.

Au titre de ces bonnes pratiques, le titulaire s'engage notamment à prendre en compte les prescriptions des documents techniques de l'ANSSI ainsi que certaines sources internationales telles que l'OWASP (*Open Web Application Security Project*) pour les interfaces Web.

Le titulaire fait valider par le GC-MTEA autorité organisatrice les éventuelles pratiques de développement externalisé qu'il envisagerait pour le SyVE et dans ce cas, il fait appliquer à ses sous-traitants préalablement acceptés par le GC-MTEA autorité organisatrice, les mêmes règles que celles qu'il applique aux développements internes.

Rappel : le candidat prend en compte la sécurité tout le long du cycle de vie du produit. Il montre qu'il a pris en compte les risques associés au SyVE en décrivant dans le mémoire technique comment il satisfait l'ensemble des prérequis de sécurité associés.

7.3. Exposition du système de vote électronique sur Internet

Le SyVE proposé inclut toutes les mesures de sécurisation logiques conformes à l'état de l'art telles que notamment le filtrage et le cloisonnement des flux réseau par des pare-feux, le contrôle d'accès aux applicatifs et aux interfaces d'autorité organisatrice, la détection et la protection contre les attaques, les intrusions et les dénis de service distribués (DDoS).

7.4. Maintien en condition de sécurité et suivi des vulnérabilités

Le titulaire est responsable du maintien en condition de sécurité du SyVE.

Le titulaire s'engage à mettre en œuvre une démarche qualité et des procédures et dispositifs techniques ayant pour objectif de détecter puis d'éliminer les vulnérabilités du SyVE, et notamment :

- Les erreurs de programmation ou les traitements erronés en s'appuyant sur des tests et des audits permettant leur identification puis le déploiement rapide de correctifs ;
- Les vulnérabilités connues dans les matériels, logiciels et composants logiciels tiers utilisés par le SyVE, par une veille sur la publication de ces vulnérabilités et le déploiement rapide de leurs correctifs.

7.5. Exploitation et autorité organisatrice technique

Les interfaces d'autorité organisatrice technique du SyVE ne sont pas exposées sur Internet, et ne sont accessibles qu'à travers un réseau privé virtuel (VPN) associé à une authentification multifacteur (MFA). Ces interfaces incluent notamment les ports d'autorité organisatrice des équipements physiques, des hyperviseurs, des systèmes d'exploitation, des bases de données et progiciels (tels que notamment les serveurs Web et les serveurs applicatifs).

Seuls des protocoles sécurisés tels que SSH, RDP ou HTTPS, sont utilisés pour réaliser les actions d'autorité organisatrice.

Le titulaire trace également les opérations d'autorité organisatrice technique de manière avec pouvoir gérer au niveau individuel l'imputabilité des actions d'autorité organisatrice.

La télémaintenance des matériels et logiciels est réalisée conformément aux exigences de la section 3.2.

7.6. Autorité organisatrice fonctionnelle

L'autorité organisatrice fonctionnelle via le portail Gestion (configuration et suivi du scrutin) est faite entièrement au travers d'une interface Web en HTTPS, à l'exclusion de tout autre protocole.

Les serveurs Web et applicatifs hébergeant respectivement les portails Electeurs, incluant le portail de vote destiné aux électeurs d'une part, et le portail Gestion destiné aux utilisateurs avec pouvoirs d'autre part, sont logiquement distincts.

8. Mécanismes cryptographiques

Cette section liste les mécanismes cryptographiques applicables au SyVE.

Lorsqu'un sujet n'est pas abordé dans la présente section, le SyVE doit suivre les règles du « Guide des mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » de l'ANSSI.

Le titulaire suit également les recommandations du « Guide de sélection d'algorithmes cryptographiques » de l'ANSSI.

Nota Bene : le candidat doit justifier tout écart à ces recommandations dans son mémoire technique.

8.1. Mécanismes recommandés pour le chiffrement des bulletins de vote

Il est fortement recommandé que le chiffrement des bulletins par le SyVE s'appuie sur les mécanismes présentés dans la présente section, qui apportent des garanties de sécurité significativement plus élevées que ceux de la section 8.2.

Il est recommandé que le SyVE chiffre les bulletins de vote avec un chiffrement asymétrique additivement homomorphe. En particulier, il est recommandé d'utiliser l'algorithme *ElGamal*.

Grâce à la propriété d'homomorphisme, le décompte s'effectue en accumulant les bulletins chiffrés (somme pour l'algorithme *ElGamal* sur courbe elliptique, ou produit pour l'algorithme *ElGamal* sur corps fini) puis en déchiffrant l'accumulation obtenue. Cette procédure apporte de fortes garanties sur la préservation de l'anonymat du vote.

Lorsque l'accumulation est réalisée, les bulletins doivent contenir des preuves à divulgation nulle de connaissance (*Zero Knowledge Proofs*) garantissant que le contenu de chaque bulletin chiffré est valide (par exemple, le bulletin ne contient qu'un seul vote) sans dévoiler l'expression du vote. Une preuve de bon déchiffrement de l'accumulation est également fournie.

8.2. Mécanismes acceptables pour le chiffrement des bulletins de vote

A défaut de s'appuyer sur les mécanismes décrits dans la section 8.1, le SyVE peut recourir aux mécanismes cryptographiques décrits dans la présente section.

Ces mécanismes sont plus complexes à mettre en œuvre (*ElGamal* avec *MixNet*) ou apportent des garanties moindres concernant la sécurité des élections (*RSA*).

Nota Bene : le cas échéant, le candidat justifiera dans son mémoire technique son choix de recourir à ces mécanismes.

Le SyVE peut utiliser un algorithme de chiffrement asymétrique, homomorphe ou non, pour chiffrer les bulletins. Les algorithmes de chiffrement *ElGamal* (sans réalisation d'accumulation) ou *RSA* sont les seuls algorithmes acceptables.

Dans cette configuration, il est nécessaire d'effectuer un mélange des bulletins chiffrés avant le dépouillement pour garantir l'anonymat du vote. Le SyVE utilise un réseau de mélangeurs des bulletins chiffrés (dit *MixNet*) réparti sur au moins deux serveurs distincts. Des preuves de bon mélange sont générées par chaque mélangeur garantissant que les modifications des bulletins réalisées par les mélangeurs ne modifient pas les suffrages contenus dans les bulletins. Enfin, une preuve de bon déchiffrement est générée afin d'atteindre le même objectif.

Lorsqu'il n'est pas réalisé d'accumulation et que le dépouillement n'est pas précédé d'une étape de mélange répondant aux conditions ci-dessus, alors les garanties pour le secret du vote sont considérées comme faibles.

Mécanisme	Conditions d'emploi	Commentaires
Chiffrement des bulletins avec <i>ElGamal</i> non accumulé	Les bulletins sont mélangés par un réseau de mélangeurs (<i>MixNet</i>) composé d'au moins deux serveurs distincts. Le mélange est réalisé par rechiffrements successifs. Des preuves de bon mélange sont produites et vérifiables.	L'absence d'accumulation oblige à déchiffrer les bulletins individuels. En conséquence, les bulletins doivent être mélangés d'une façon cryptographiquement sûre et vérifiable avant le dépouillement.
Chiffrement des bulletins avec <i>RSA</i> avec mélange	Les bulletins sont mélangés par un réseau de mélangeurs (<i>MixNet</i>) composé d'au moins deux serveurs distincts. Le mélange est réalisé par déchiffrements successifs. Des preuves de bon mélange sont produites et vérifiables.	L'absence d'homomorphisme oblige à déchiffrer les bulletins individuels. En conséquence, les bulletins doivent être mélangés d'une façon cryptographique sûre et vérifiable avant le dépouillement.
Chiffrement des bulletins avec <i>RSA</i> sans mélange	Il n'y a pas de mélange (<i>MixNet</i>), ou bien le mélange est réalisé sur un seul serveur, ou bien le mélange n'est pas vérifiable.	Les garanties pour le secret du vote sont faibles. Le lien entre le bulletin chiffré et le bulletin déchiffré est direct.

Le candidat doit décrire dans son mémoire technique comment les preuves de bon mélange sont générées et vérifiables.

8.3. Gestion et partage de la clé privée de déchiffrement

La clé privée de déchiffrement de l'élection est fragmentée grâce à un algorithme de partage de clé secrète à seuil. Cette exigence s'applique dans tous les cas, que le chiffrement du bulletin s'appuie sur *ElGamal* ou sur *RSA*.

Il est recommandé que :

- Les fragments de la clé privée de déchiffrement soient générés non pas sur les serveurs du SyVE, mais dans le navigateur (ou les navigateurs en cas de génération distribuée, ou dans un client lourd dédié) utilisé par les membres du BCVE, ou du BVE s'il n'est pas rattaché à un BCVE, lors de la cérémonie de génération et d'attribution de la clé ;
- La clé privée ne soit jamais envoyée aux serveurs du SyVE, ni stockée durablement sur le ou les postes ayant servi à sa génération, ni sur aucun autre support ;
- Les fragments de la clé privée non chiffrés ne soient pas envoyés aux serveurs du SyVE, ni stockés durablement sur le ou les postes ayant servi à leur génération.

L'article R. 211-549 du CGFP prévoit qu'à chaque fragment de la clé privée est associé un code d'activation, choisi par l'attributaire du fragment et connu de lui seul. La procédure encadrant le choix du code d'activation par l'attributaire prévoit des modalités garantissant que les codes d'activation résistent à une attaque par force brute.

Chaque fragment de la clé privée est enregistré individuellement en étant chiffré par une clé dérivée du code d'activation à l'aide d'un algorithme de dérivation conforme aux recommandations du guide « Sélection d'algorithmes cryptographiques » de l'ANSSI.

Les codes d'activation ne doivent pas être enregistrés « en clair » par le SyVE. Une empreinte de chaque code d'activation peut cependant être enregistrée par le SyVE.

Si l'algorithme de chiffrement des bulletins le permet (par exemple, *ElGamal*), il est recommandé que le déchiffrement ne s'appuie pas sur une reconstitution de la clé privée en mémoire, mais s'appuie sur des déchiffrements partiels successifs.

Le cas échéant, le candidat justifiera dans son mémoire technique son choix de ne pas suivre ces recommandations.

8.4. Mise en œuvre du pastillage

Rappel : le pastillage est défini par la section 6.6.

Lorsque le SyVE réalise des accumulations avant le décompte, il est recommandé que le mécanisme de pastillage soit conforme aux points suivants :

- Les attributs associés à l'électeur et servant à définir le scrutin indirect sont associés en clair au bulletin chiffré ;
- Le bulletin chiffré est unique et commun au scrutin direct et aux scrutins indirects. Sa référence, elle aussi unique, figure sur la preuve de vote ;
- Le serveur du SyVE vérifie à la réception du bulletin que les attributs associés au bulletin par le client de vote correspondent à ceux déclarés dans la liste électorale pour cet électeur ;
- Les ajouts du bulletin dans l'urne du scrutin direct et dans la ou les urnes des scrutins indirects auxquels participe l'électeur sont réalisés comme une opération atomique ;
- Les preuves à divulgation nulles de connaissance contenues dans chaque bulletin incluent dans leur contexte les attributs associés au bulletin, afin de détecter le déplacement du bulletin d'une urne à une autre ;
- Il y a une accumulation puis un décompte par scrutin indirect ;
- Pendant le décompte, une preuve de bon déchiffrement de chaque accumulation est produite, pour les scrutins directs comme pour les scrutins indirects.

Lorsque le SyVE ne réalise pas d'accumulations avant le décompte, il est recommandé que le mécanisme de pastillage soit conforme aux points suivants :

- Les attributs associés à l'électeur et servant à définir le scrutin indirect sont associés en clair au bulletin chiffré ;
- Le bulletin chiffré est unique et commun au scrutin direct et aux scrutins indirects. Sa référence, elle aussi unique, figure sur la preuve de vote ;
- Les ajouts du bulletin dans l'urne du scrutin direct et dans la ou les urnes des scrutins indirects auxquels participe l'électeur sont réalisés comme une opération atomique ;
- Les preuves à divulgation nulles de connaissance contenues dans chaque bulletin incluent dans leur contexte les attributs associés au bulletin, afin de détecter le déplacement du bulletin d'une urne à une autre ;
- Il y a un mélange puis un décompte par scrutin indirect ;
- Le serveur du SyVE vérifie lors du décompte que les attributs intégrés dans le bulletin déchiffré correspondent à l'urne en cours de décompte.

Le cas échéant, le candidat justifiera dans son mémoire technique son choix de ne pas suivre ces recommandations.

8.5. Mécanismes de hachage pour le calcul des empreintes

Le SyVE calcule les empreintes cryptographiques à l'aide des fonctions de hachage *SHA-2* (par exemple *SHA-256*) ou *SHA-3*.

Cette exigence s'applique notamment aux empreintes relatives à la vérification d'intégrité du SyVE (section 3.3) et aux empreintes des bulletins de vote dans les preuves de vote (section 4.1).

8.6. Générateur d'aléa

Tout générateur d'aléa utilisé par le SyVE est conforme aux règles applicables données par le guide « Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » de l'ANSSI.

8.7. Stockage des secrets d'authentification

Le stockage des secrets d'authentification est conforme aux recommandations de la section « Stockage des mots de passe » du guide « Recommandations relatives à l'authentification multi-facteurs et aux mots de passe » de l'ANSSI. Les secrets d'authentification n'existent donc jamais en clair sur le SyVE.

8.8. Evolutions

Le titulaire assure les évolutions des mécanismes cryptographiques du SyVE ou utilisés lors des échanges de données conformément à l'état de l'art en prenant en compte la découverte de vulnérabilités de ces mécanismes, ou encore l'évolution des techniques de cryptanalyse.