# Annexe II : Exigences techniques

Table des matières

[Annexe II : Exigences techniques 1](#_Toc188306975)

[1 Exigences techniques générales 2](#_Toc188306976)

[1.1 L’organisation générale de la solution de vote électronique 2](#_Toc188306977)

[1.2 Les prérequis techniques 3](#_Toc188306978)

[1.3 Les prérequis de compatibilité 4](#_Toc188306979)

[1.4 Prérequis en matière d’hébergement 5](#_Toc188306980)

[1.5 Exigences mode SaaS et hébergement 6](#_Toc188306981)

[2 Fiabilité, disponibilité et performances 8](#_Toc188306982)

[2.1 Fiabilité et disponibilité du système de vote électronique 8](#_Toc188306983)

[2.2 Engagement de niveaux de service et performances 8](#_Toc188306984)

[3 L’assistance technique 11](#_Toc188306985)

[3.1 Support de niveau 2 11](#_Toc188306986)

[3.2 Cellule de support de niveau 3 du titulaire 13](#_Toc188306987)

[3.3 Traçabilité 14](#_Toc188306988)

[4 Notice d’information détaillée 16](#_Toc188306989)

[4.1 Principes 16](#_Toc188306990)

[4.2 Personnalisation de la notice 16](#_Toc188306991)

[5 Notice de vote 17](#_Toc188306992)

[5.1 Génération et conservation d’une notice de vote 17](#_Toc188306993)

[5.2 Impression, conditionnement et expédition des notices de vote 17](#_Toc188306994)

[5.2.1 La procédure d’impression et d’expédition des notices de vote “papier” 17](#_Toc188306995)

[5.2.2 Les rôles des référents notice et de la cellule de supervision technique 18](#_Toc188306996)

# Exigences techniques générales

## L’organisation générale de la solution de vote électronique

Comme il est précisé dans le corps du CCTP, le SyVE s’organise autour de trois portails dénommés « B1 », « B2 » et « B3 » qui doivent être sécurisés de sorte à garantir en tous points le respect du cadre législatif et réglementaire du vote électronique par internet pour les élections professionnelles de 2026 :

* **Le portail B1** correspond à l’espace Electeurs dédié à chaque électeur ;
* **Le portail B2** est le portail de vote dédié aux électeurs, il n’est accessible que pendant la période de vote ;
* **Le portail B3** est réservé en accès aux utilisateurs avec pouvoirs pour leur proposer les fonctionnalités indispensables pour exercer leurs compétences.

Les portails B1 et B2 sont regroupés en un seul portail dénommé « **portail Electeurs** ». Cette fusion ne remet pas en cause les fonctionnalités des deux portails qui sont conservées :

* Accès pour l’électeur en consultation des listes électorales comme des listes de candidatures constituées par les listes de candidats et leurs professions de foi (fonctionnalité B1) ;
* Accès de l’électeur en consultation à son « compte Electeur » qui contient des DACP (Données à caractère personnel) et précise ses droits de vote (fonctionnalité B1) ;
* Possibilité pour l’électeur de soumettre une requête de modification des DACP de son compte électeur (fonctionnalité B1) ;
* Accès pour l’électeur à la fonctionnalité « Vote » dès que le scrutin est ouvert (fonctionnalité B2).

Dans la semaine qui va suivre l’injection de la première version du « référentiel électeurs » dans le SyVE, les fonctionnalités B1 du portail Electeurs sont proposées aux électeurs au-moins [soixante (60)] jours calendaires avant l’ouverture de la période de vote. Les fonctionnalités B2 de vote ne peuvent être accessibles qu’après que l’électeur se soit dûment identifié puis authentifié pour accéder au portail Electeurs et doit exiger la saisie d’un secret ou code de vote pour pouvoir voter.

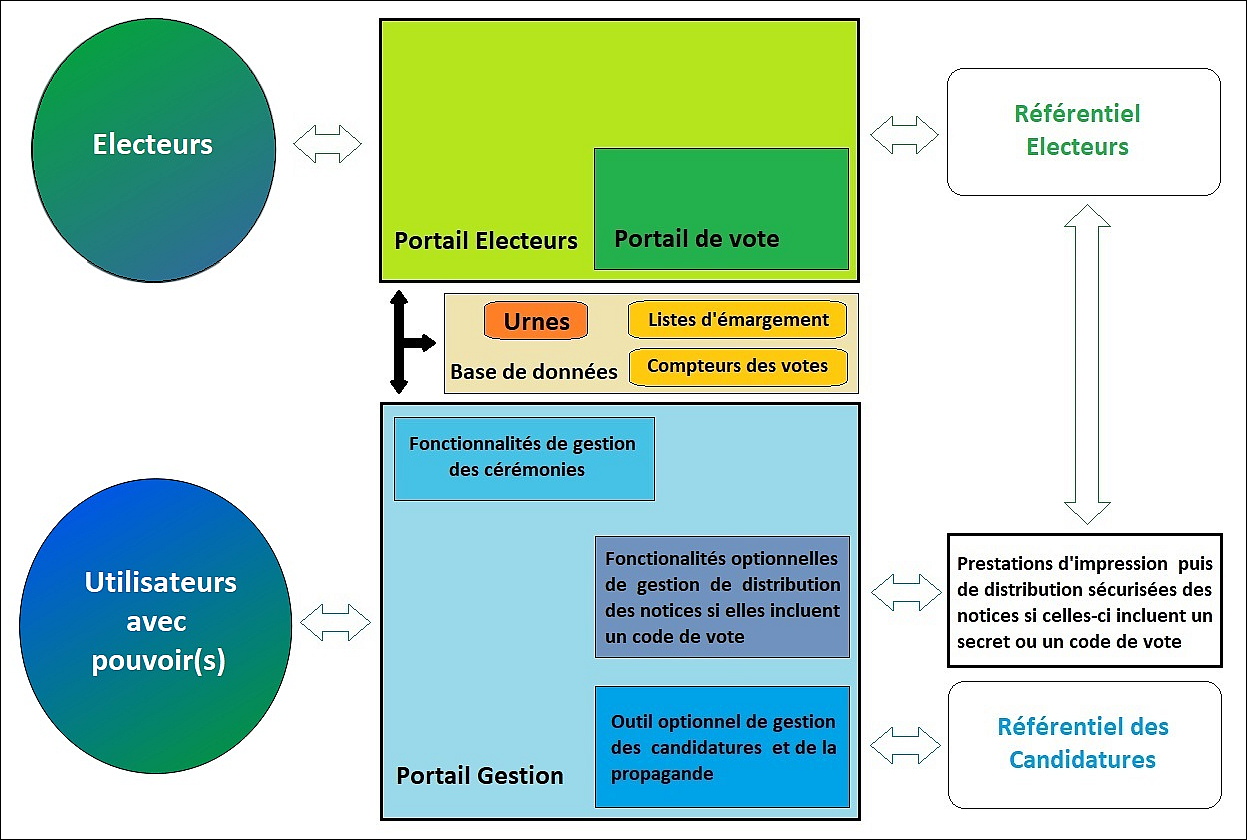
**Le portail B3** est conservé et renommé « **Portail Gestion** », il doit répondre aux objectifs suivants:

* Permettre l’accès authentifié par profil aux utilisateurs avec pouvoirs ;
* Permettre de procéder aux opérations de préparation de l’élection par validation de la configuration des scrutins ;
* Permettre de réaliser les cérémonies de création et attribution des clefs de chiffrement et déchiffrement ;
* Permettre de réaliser la cérémonie de scellement du dispositif de vote électronique ;
* Permettre aux utilisateurs avec pouvoirs d’exercer les fonctions relevant de leur domaine de compétences pendant la période de vote et le déroulement des scrutins, telles que la consultation de la liste d’émargement ;
* A l’issue de ladite période de vote, permettre aux membres des BCVE et éventuels BVE qui ne sont pas rattachés à un BCVE, de contrôler le scellement du système de vote avant dépouillement, de prononcer la clôture des scrutins puis de lancer les opérations de dépouillement ;
* Procéder à la vérification des preuves relatives à la vérifiabilité universelle du scrutin ;
* A l'issue du dépouillement, produire et enregistrer les procès-verbaux d’opérations électorales pour les BCVE et les procès-verbaux de résultat de scrutin pour les BVE.

Les portails interagissent avec l’ensemble des données relatives à l’élection qui comprennent le référentiel électeurs (les listes électorales de chaque scrutin) et le référentiel candidatures (les candidatures, profession de foi et logos pour chaque scrutin).

Il y a deux catégories d’utilisateurs de la SVE : les électeurs et les utilisateurs avec pouvoirs. Ces utilisateurs avec pouvoirs sont répartis en groupes avec divers profils :

* Les membres de BCVE (ou d’un BVE non rattaché à un BCVE) :
  + Le président ;
  + Le secrétaire, suppléant du président ;
  + Le suppléant du secrétaire ;
  + Les délégués
  + Le suppléant de chaque délégué ;
* Les membres de BVE :
  + Le président ;
  + Le secrétaire, suppléant du présentant ;
  + Les délégués de liste ;
  + Le suppléant de chaque délégué de liste ;
* Les membres de la CdST :
  + Les représentants de l’autorité organisatrice ;
  + L’expert indépendant ;
  + Les représentants du prestataire ;
* Les membres du centre d’assistance qui doit assurer la *« hot line »* de premier niveau ;
* Le cas échéant, les utilisateurs de l’outil de gestion des listes de candidats et de la propagande ;
* Si les notices d’information détaillée, ou notices de vote, sont communiquées aux électeurs sous format papier par courrier postal ou remise en main propre, et si ces notices sont utilisées pour transmettre à chaque électeur un secret ou code de vote alors les référents notice, qui doivent gérer l’opération de communication des notices, constituent un dernier groupe d’utilisateurs avec pouvoirs.



Organisation générale de la SVE

## Les prérequis techniques

Il est exigé que le SyVE présente une *« architecture Full Web »* pour que l’intégralité des fonctionnalités de la SVE soit accessible depuis un navigateur quel qu’il soit. Il est demandé que cette architecture soit une architecture « trois-tier » :

* Un premier niveau ou « couche de présentation » qui est celui du navigateur client. Ce premier « tier » traite de la partie navigable par le client ou l’utilisateur de la SVE. Dans cette couche, les exigences techniques vont porter notamment sur l’ergonomie et les performances de chargement des pages ;
* Un second niveau ou « couche de traitement » qui est celui du serveur http du SyVE. Ce second « tier » traite notamment de la partie liée aux aspects fonctionnels de la SVE. Cette couche doit prendre en charge la réception des requêtes provenant du navigateur de l’utilisateur et renvoyer ces données au serveur de base de données avant de pouvoir récupérer les traitements effectués par celui-ci pour finalement les retourner au navigateur client de l’utilisateur ;
* Un troisième et dernier niveau ou « couche d’accès aux données ». Ce dernier « tier » est celui du serveur de base de données.

La solution doit ainsi être accessible par Internet et être compatible avec la majorité des systèmes d’exploitation pour poste informatique, tablette comme smartphone comme avec les principaux navigateurs bénéficiant d’un support éditeur. La solution doit inclure, au niveau du portail Electeurs et du portail Gestion, un outil permettant de diagnostiquer la compatibilité du poste utilisateur avec les prérequis techniques. Si l’outil formule un diagnostic négatif, il doit proposer a minima une solution adéquate permettant à l’utilisateur d’accéder à la SVE et notamment :

* Un lien vers la page de téléchargement officielle des dernières versions du navigateur détecté par l’outil sur le poste utilisateur ;
* Des liens vers la page de téléchargement officielle d’autres navigateurs.

L’application « client » du SyVE doit reposer sur les langages de technologie *Web HTML5* et *JavaScript*. Les portails Electeurs comme Gestion ne doivent pas nécessiter l’emploi des composants suivants :

* Des extensions de navigateur (*plug-in*) tels qu’*Adobe Flash* ou *Acrobat* ;
* Des programmes écrits en langage *Java* (*Applets*) ;
* Des objets logiciels écrits en C++ ou *Visual Basic* (*ActiveX*) ;
* Des logiciels tiers tels qu’une suite bureautique (*MS-Office*, *LibreOffice* ou autre) ;
* Il est acceptable que les documents communiqués à l’électeur à l’issue du vote requièrent l’emploi d’une application d’affichage de fichiers PDF.

Pour rappel, l’installation sur tout poste professionnel d’application(s) tierce(s) par son utilisateur est prohibée au motif que les applications sont déployées par des administrateurs de l’autorité organisatrice à travers des mécanismes approuvés.

La SVE ne doit pas exiger une connexion Internet à haut débit pour permettre à tout utilisateur d’accéder à ses fonctionnalités.

## Les prérequis de compatibilité

L’article R. 211-559 CGFP dispose que le SyVE permette de voter à partir de tout équipement informatique permettant l’accès à Internet et répondant à des exigences de sécurité minimales. La SVE doit donc :

* Être accessible par tout poste informatique, tablette ou smartphone disposant de l’un des principaux systèmes d’exploitation de l’accord-cadre ;
* Être compatible avec la majorité des navigateurs Internet bénéficiant d’un support éditeur tels que *Chrome*, *Safari*, *Edge*, *Firefox* dans leurs versions supportées par leurs éditeurs respectifs ;
* Permettre un fonctionnement avec des navigateurs intégrant les dernières mises à niveau de sécurité.

La SVE ne doit pas contraindre l’utilisateur à revenir à une version ancienne de son navigateur, ni a fortiori à une version dudit navigateur présentant des failles de sécurité. En particulier, la SVE devra être mise à niveau pour permettre un fonctionnement avec les versions les plus récentes des navigateurs et des systèmes d’exploitation en 2026 et intégrant les dernières mises à niveau de sécurité (ci-dessous, les versions en vigueur à la date de rédaction du modèle de CCTP).

Les exigences de compatibilité pour les navigateurs des postes électeurs pour accéder au portail Electeurs sont notamment :

* *Internet Explorer* ne bénéficiant plus d’un support depuis juin 2022, il n’est pas imposé que la SVE supporte une version de ce navigateur obsolète ;
* La « version héritée » de *Microsoft Edge* ne bénéficiant plus d’un support depuis mars 2021, il n’est pas imposé que la SVE supporte une version de ce navigateur obsolète ;
* La version minimale de *Microsoft Edge « Chromium »* supportée doit être la version 108 diffusée à partir de décembre 2022 ;
* La version minimale de *Google Chrome* supportée doit être la version 108 diffusée à partir de décembre 2022 ;
* La version minimale de *Mozilla Firefox* supportée doit être la version 108 diffusée à partir de décembre 2022 ;
* La version minimale de *Opera* supportée doit être la version 72 diffusée à partir de 2022 ;
* La version minimale de *Apple Safari* supportée doit être la version 16 diffusée à partir de 2022.

Les exigences de compatibilité pour les navigateurs des postes utilisateurs pour accéder au portail Gestion sont notamment :

* *Internet Explorer* ne bénéficiant plus d’un support depuis juin 2022, il n’est pas imposé que la SVE supporte une version de ce navigateur obsolète ;
* La « version héritée » de *Microsoft Edge* ne bénéficiant plus d’un support depuis mars 2021, il n’est pas imposé que la SVE supporte une version de ce navigateur obsolète ;
* La version minimale de *Microsoft Edge « Chromium »* supportée doit être la version 121 diffusée à partir de février 2024 ;
* La version minimale de *Google Chrome* supportée doit être la version 121 diffusée à partir de janvier 2024 ;
* La version minimale de *Mozilla Firefox* supportée doit être la version 121 diffusée à partir de janvier 2024 ;
* La version minimale de *Opera* supportée doit être la version 80 diffusée à partir de janvier 2024 ;
* La version minimale de *Apple Safari* supportée doit être la version 17 diffusée à partir de 2023.

Ces deux listes de versions ne sont que des propositions. L’autorité organisatrice doit s’approprier ces deux listes pour y préciser ses exigences voire ajouter d’autres navigateurs.

Le candidat décrit dans son cadre de réponse technique (CRT) les contraintes ou restrictions applicables aux équipements utilisables par les utilisateurs de la SVE pour accéder au portail Electeurs, portail de vote et au portail Gestion.

## Prérequis en matière d’hébergement

En application des recommandations des objectifs n°2-05 et 3-05 de la délibération CNIL n° 2019-053 [à actualiser selon la délibération CNIL en vigueur], les serveurs de l’infrastructure de la SVE sont préférentiellement dédiés à l’hébergement des portails Electeurs et Gestion et aux opérations électorales objet du présent accord-cadre relatif au vote électronique. Ces serveurs de la plate-forme de production doivent être dédiés à l’autorité organisatrice pendant toute la période de fonctionnement des portails Electeurs et Gestion.

Les machines virtuelles et l’hyperviseur exécutant le SyVE doivent être dédiées aux scrutins de l’autorité organisatrice.

En cas de recours à un même SyVE pour plusieurs scrutins, chacun de ces scrutins est cloisonné de manière à pouvoir être totalement interrompu sans impact sur les autres scrutins en cours (cf. délibération CNIL en vigueur à la date de soumission de l’accord-cadre, la délibération actuellement en vigueur prévoyant le seul cloisonnement physique).

Si le candidat propose une mutualisation des serveurs ou un cloisonnement logique, il doit être en mesure d’expliquer dans son CRT ce choix et de justifier la sécurité et la disponibilité offertes par la plate-forme proposée même en cas d’incident majeur ou d’intrusion affectant une autre opération électorale se déroulant sur l’infrastructure mutualisée.

Les prestations d’hébergement et de connexion doivent comporter au moins :

* La mise à disposition d'un espace d'hébergement sécurisé conforme au PAQ et au taux de service contractuel ;
* La mise à disposition des équipements permettant une connectivité dans un contexte hautement sécurisé à savoir : routeurs, pare-feu, système d'équilibrage de charges et redondance des systèmes si nécessaire ;
* La supervision et l’anticipation face aux incidents détectés ;
* Un monitoring permanent des éléments de la SVE ;
* Une application de détection d’intrusions ;
* Un système anti-DDoS (*distributed denial of service*) ;
* L’extensibilité du dimensionnement des infrastructures d’hébergement pour permettre de s’adapter aux exigences techniques, fonctionnelles et de sécurité du projet ;
* La mise en œuvre rapide, selon l’évolution de la sollicitation du site, de serveurs d'applications et de serveur de base de données intégrant des possibilités de redondance ;
* La relance de tout ou partie de l’architecture matérielle du SyVE sur demande 7j/7 ;
* La surveillance de la connexion IP permanente avec alerte envoyée par email pour « Ping » et port serveur ;
* L’accès aux locaux d’hébergement des infrastructures principale et de secours sur demande pour l’autorité organisatrice ou tout expert désigné par elle, ainsi que pour l’expert indépendant auquel aura été confiée la mission d’expertise indépendante précisée par les articles R. 211‑518 à R. 211-53 et R. 211-21 du CGFP ;
* La mise à disposition d’un support technique de niveaux 2 et 3 ;
* L’autorité organisatrice du SyVE 24h/24 et 7j/7 ;
* La synchronisation sur une source de temps fiable de tous les équipements venant composer le SyVE. La dérive par rapport à l’heure légale de Paris ne saurait excéder une minute ;
* La mise en place et l’exploitation de statistiques ;
* L’élaboration, la documentation et l’application des procédures d’exploitation ;
* L’élaboration, la documentation et l’application des procédures d’intervention en cas d’incident ou de suspension d’un ou plusieurs scrutins, y compris les aspects d’audit en cours d’intervention et *a posteriori* ;
* L’installation de tout élément applicatif et sa configuration, que cet élément soit un composant initial du SyVE ou un composant qui aura été spécifié dans les prestations 1 à 4 du CCTP ;
* La garantie de sécurité et de confidentialité de la SVE et de l’ensemble des données du scrutin.

## Exigences mode SaaS et hébergement

Afin de permettre un contrôle effectif et, le cas échéant, l’intervention des autorités nationales compétentes, le SyVE est impérativement localisé sur le territoire métropolitain. Aucun flux d’administration ni de supervision ne doit être situé hors du territoire français. La même SVE est utilisée pour tous les scrutins, que les élections se déroulent en métropole, en outre-mer, ou à l’étranger.

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 que l’infrastructure d’hébergement repose sur un mode actif/actif de redondance.

Les centres où sont physiquement implantées les infrastructures d'hébergement principales et de secours de la SVE doivent présenter toutes les garanties de sécurité et de sûreté et notamment de construction, de mesures anti-intrusion, et de mesures anti-incendie. Les prérequis suivants sont imposés pour l’implantation de l’infrastructure d’hébergement principale :

* Centre d’hébergement :
  + Energie redondante ;
  + Générateur en cas de perte de courant ;
  + Réseau protégé (pare-feu, routeurs redondants, antivirus serveur, détection d’intrusion…) ;
  + Système d'extinction d'incendie par gaz (*FM200*, ou autre agréé) ;
  + Système de vidéosurveillance interne et externe sur l'ensemble du bâtiment avec enregistrement vidéo 24h/24 ;
  + Bâtiment entièrement sous alarme ;
  + Système de contrôle d'accès biométrique ou par badge ;
* Connectivité :
  + Connectivité Internet redondante par deux (2) fournisseurs différents ;
  + Accès par réseau Internet et bande passante redondante réservée pour le projet de vote électronique.

Pour l'implantation de l'infrastructure d'hébergement de secours, le titulaire met en œuvre les mêmes modalités et respecte les mêmes contraintes, il doit présenter le dispositif dédié permettant d’assurer le PCA et le PRA. Une conformité aux normes ISO, notamment 270010 et 50001, ou équivalentes du domaine doit être privilégiée.

Le candidat doit décrire dans son CRT l’infrastructure entièrement redondante d’hébergement en mode actif/actif de la SVE et son niveau de conformité ISO notamment 27001 et 50001, ou équivalent qu’il propose et il doit préciser le taux de disponibilité auquel il s’engage.

La qualification *SecNumCloud* de l’hébergement n'est pas exigée mais l’autorité organisatrice formule diverses exigences relatives à ce référentiel.

Si l’autorité organisatrice décide d’exiger la qualification SecNumCloud alors toute cette partie doit être reportée dans l’annexe III des exigences de sécurité au motif que ce tableau constitue alors un tableau d’exigences de sécurité.

Cette qualification n’étant pas exigée, ce tableau est un tableau d’exigences techniques en matière d’hébergement qui trouve donc sa place dans cette section 1.5 de l’annexe II.

| **Exigence du Référentiel *SecNumCloud*** | **Exigence de l’autorité organisatrice** |
| --- | --- |
| §6. Organisation de la sécurité de l’information | Conformité au référentiel ANSSI ou pratique équivalente souhaitée |
| §7. Sécurité des ressources humaines | Conformité au référentiel ANSSI ou pratique équivalente exigée |
| §8. Gestion des actifs et notamment : restitution des actifs | Conformité au référentiel ANSSI ou pratique équivalente exigée |
| §9. Contrôle d’accès et gestion des identités et notamment : gestion des droits d’accès, accès aux interfaces d’administration, restriction des accès à l’information | Conformité au référentiel ANSSI ou pratique équivalente exigée |
| §10. Cryptologie | Conformité au référentiel ANSSI exigée ou pratique équivalente exigée |
| §11. Sécurité physique et environnementale et notamment : contrôle d’accès physique, protection contre les menaces extérieures et environnementales, sécurité du câblage | Conformité au référentiel ANSSI exigée |
| §12. Sécurité liée à l’exploitation et notamment : séparation des environnements de développement, de test et d’exploitation, journalisation des événements, synchronisation des horloges, gestion des vulnérabilités techniques, administration | Conformité au référentiel ANSSI exigée |
| §13. Sécurité des communications et notamment : cloisonnement des réseaux, surveillance des réseaux | Conformité au référentiel ANSSI ou pratique équivalente exigée |
| §14. Acquisition, développement et maintenance des systèmes d’information, et notamment : politique de développement sécurisé, procédures de contrôle des changements de système, protection des données de test | Conformité au référentiel ANSSI ou pratique équivalente souhaitée |
| §15. Relations avec les tiers et notamment : la sécurité dans les accords conclus avec les tiers, engagements de confidentialité | Conformité au référentiel ANSSI ou pratique équivalente souhaitée |
| §16. Gestion des incidents liés à la sécurité de l’information | Conformité au référentiel ANSSI ou pratique équivalente souhaitée |
| §17. Continuité d’activité | Conformité au référentiel ANSSI exigé |

Le référentiel *SecNumCloud* est disponible sur le site de l'ANSSI :

<https://www.ssi.gouv.fr/administration/qualifications/prestataires-deservices-de-confiance-qualifies/referentiels-exigences/>.

# Fiabilité, disponibilité et performances

## Fiabilité et disponibilité du système de vote électronique

La fiabilité du SyVE est la probabilité que ce système ou l’un de ses composants puisse remplir ses fonctions sur une durée déterminée sans discontinuer. Il est possible de mesurer cette propriété au moyen d’une métrique classique de gestion des incidents et notamment :

* **Le MTBF (*mean time between failure* ou temps moyen entre pannes) qui est obtenu en** divisant le temps total de fonctionnement par le nombre de pannes ;
* **Le MTTR (*mean time to repair* ou durée moyenne de réparation) prend en compte la durée totale pour remettre le système ou le composant en état de fonctionner. Il est obtenu en** divisant le temps total de maintenance par le nombre total d'actions de maintenance dans une période donnée ;
* **Le FIT (*failure(s) in time* ou taux d’échec(s)) est obtenu en** divisant le nombre de défaillance(s) par le temps total en service du système ou composant.

Pour améliorer la fiabilité du SyVE, diverses actions sont envisageables et notamment :

* Disposer de procédures de mise à jour des composants logiciels du SyVE, les documenter et les appliquer ;
* Développer la redondance de l’infrastructure du SyVE pour augmenter sa disponibilité ;
* Formaliser le PCA et le PRA et vérifier leur efficacité avec un plan de tests ;
* Effectuer en pré-production, contrôles et tests de qualité lors de toute modification du SyVE, afin que les éventuels problèmes puissent être détectés et corrigés avant de passer en mode production ;
* Développer les procédures de gestion des incidents et implémenter leurs processus.

En termes informatiques, la disponibilité ou opérabilité est la propriété du SyVE susceptible de traduire la facilité avec laquelle il est possible d'accéder aux données ou aux ressources du SyVE dans un format exploitable. Cette propriété est alors associée à la rapidité avec laquelle ce 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.

La mesure de la disponibilité est une métrique à pourcentage unique. Il s'agit du temps total écoulé moins le temps d'arrêt total divisé par le temps total écoulé :

**Pourcentage de disponibilité = (temps total écoulé – temps d'arrêt) / temps total écoulé**

Comme pour la fiabilité, il existe diverses actions pour améliorer la disponibilité du SyVE et notamment :

* Implémenter des plannings de maintenance standard et proactifs pour prévenir les pannes plutôt que de devoir les constater et les traiter ;
* Développer la redondance de l’infrastructure de la SVE en l’exploitant au moyen de mécanismes de basculement de préférence automatiques (mode actif/actif) ;
* Développer et implémenter des processus de remise rapide en état opérationnel dans le cadre des procédures de gestion des incidents.

Fiabilité et disponibilité sont souvent confondues mais non seulement ces deux propriétés diffèrent, mais elles ne s'alignent pas toujours. Les métriques de fiabilité et de disponibilité du SyVE doivent être analysées séparément :

* La **fiabilité** doit mesurer si le SyVE a produit le bon résultat à une heure précise et définie. La fiabilité va surtout viser à limiter les pannes du SyVE et les temps d'arrêt de la SVE ;
* La **disponibilité** doit mesurer le temps de fonctionnement du SyVE. La disponibilité va avoir pour objectif d’optimiser le temps de fonctionnement de la SVE.

L'amélioration des deux propriétés du SyVE nécessite toutefois des approches similaires comme l’implémentation des routines de maintenance, la mise en œuvre du PCA et du PRA, le développement d’une infrastructure redondante en mode actif/actif, le développement de procédures pertinentes et efficaces de gestion des incidents.

## Engagement de niveaux de service et performances

La SVE doit offrir une qualité de service garantie en termes de disponibilité et de fiabilité mais aussi « tenir la charge » notamment pendant la période de vote. Un nombre simultané d’électeurs significatif par rapport au nombre total d’électeurs doit être accepté sans dégradation sensible des performances. Dès l’ouverture du portail Electeurs et jusqu’à la fin des opérations d’archivage prévues par les dispositions des articles R. 211‑580 à R. 211-584 du CGFP, la SVE doit offrir une disponibilité 24h/24 et 7j/7.

La solution doit donc être capable d'absorber les accès au portail Electeurs comme les votes des électeurs lors de la totalité des scrutins simultanés sur toute la période de vote, avec des pics attendus les deux premiers jours et le dernier jour de cette période de vote pendant les heures ouvrées.

En application des recommandations de l'objectif n°3-03 de la délibération CNIL n° 2019-053 [à actualiser selon la délibération CNIL en vigueur], la SVE et son infrastructure d'hébergement doivent être conçues pour garantir une très haute disponibilité et prendre en compte les risques d’avarie majeure. La SVE doit donc offrir une qualité de service garantie en termes de très haute disponibilité et de tenue de charge :

* Pendant la période d’avant-vote, seules sont admises les périodes d’interruption validées conjointement par le titulaire et la direction projet de l’autorité organisatrice qui sont nécessaires notamment :
  + Aux mises à jour requises pour prévenir des cas d’attaque malveillante ou de panne du système de vote ;
  + Aux mises à jour de l’ensemble des données relatives aux scrutins telles que pour l’injection d’une nouvelle version de référentiel Electeurs ou encore l’injection d’une nouvelle version de référentiel de candidatures ;

La garantie sur le temps de rétablissement (GTR) est de [huit (8)] heures et la durée d’indisponibilité maximale admissible (DIMA) est donc de [huit (8)] heures pendant cette période d’avant-vote exception faite de la période de saisie des listes de candidatures où le GTR passe à [quatre (4)] heures et l'indisponibilité cumulée tolérée est limitée à [quatre (4)] heures ;

* Aucune interruption de service supérieure à [une (1)] heure n’est admissible pendant toute période consacrée à une cérémonie et la durée d’indisponibilité cumulée tolérée pour l’ensemble des cérémonies est d’[une (1)] heure ;
* Aucune interruption de service supérieure à [une (1)] heure n’est admissible pendant la période de vote. La DIMA est donc d’[une (1)] heure pendant la période de vote et l'indisponibilité cumulée est au maximum de [quatre (4)] heures maximum sur la période de vote ;
* Aucune interruption de service supérieure à [quatre (4)] heures n’est admissible pendant la période post-vote et l'indisponibilité cumulée est au maximum de [huit (8)] heures maximum sur cette période de post-vote.

Cette exigence s’applique, 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) est affichée à destination des électeurs et des utilisateurs avec pouvoirs.

Les valeurs portées dans cette section sont proposées à titre d’exemple.

Toutes ces exigences doivent être définies par l’autorité organisatrice qui doit s’assurer qu’elles sont cohérentes avec celles portées au titre de la « disponibilité » dans l’annexe III d’exigences de sécurité.

Comme précisé dans la nomenclature portée en annexe V du CCTP :

* La période d’avant-vote, ou encore de « pré-vote », est la période séparant l’ouverture du portail Electeurs de la cérémonie de scellement ;
* La période de vote présente une durée d’au plus huit jours pendant laquelle les électeurs peuvent voter en accédant au portail de vote intégré au portail Electeurs. Cette période commence le lendemain de la tenue de la cérémonie de scellement ;
* La période post-vote est la période séparant la clôture du dépouillement de la remise par l’expert indépendant de son rapport d’expertise indépendante final. C’est pendant cette période post-vote que doit être constitué l’archivage *ad probationem* prévu par les dispositions des articles R. 211-580 à R. 211-584 du CGFP.

Le taux de disponibilité global de la SVE ne peut être inférieur à 99,5 %. La durée d’indisponibilité maximale admissible (DIMA) est de soixante minutes à huit (8) heures. **Aucune perte de données (PDMA) n’est admise**.

Le temps de latence du service ne peut être supérieur à 1/100ème de seconde.

Ces exigences de performances sont aussi applicables dans le contexte de l'élection test puisque le PRA sera notamment vérifié durant la prestation 4 « Organisation et tenue d’une élection test » du CCTP. A cette occasion, le titulaire doit fournir des résultats de tests de montée en charge avec différents scénarios représentatifs d’une opération de vote réelle complexe (nombre de votants simultanés répartis temporellement en pics, simultanément à de nombreuses opérations de réassortiment d’authentifiants et de codes de vote ainsi que des générations de professions de foi ou de listes de candidats différentes en quantité). Ces tests feront l’objet de vérification par d’autres tests de montée en charge par les moyens de l’autorité organisatrice.

Le jour de fin de scrutin (T1), la SVE permet le dépouillement simultané de l’ensemble des scrutins selon l’ordre défini par l’autorité organisatrice. La SVE doit nativement proposer des performances permettant de réaliser et clôturer ce dépouillement le jour de fin de la période de vote.

L’expression des objectifs de performance des fonctionnalités, que celle-ci repose sur un traitement transactionnel ou sur un traitement décalé, se fait sous la forme de temps de réponse attendus entre la soumission d’une demande à la SVE et l’obtention d’une réponse. En « sortie de l’architecture du SyVE » proposée par le titulaire en prestation 2 du CCTP, la SVE fournit des temps de réponse inférieurs ou égaux aux temps de réponse listés ci-dessous.

| **Type de fonctionnalité** | **Nombre d’accès simultanés (à adapter selon la taille de la structure organisatrice)** | **Temps de réponse maximum** |
| --- | --- | --- |
| **Authentification** | 50 000 | [Quatre (4)] secondes |
| **Affichage des pages accessibles depuis le portail Electeurs, y compris depuis le portail de vote** | 35 000 | [Deux (2)] secondes |
| **Affichage des pages accessibles depuis le portail Gestion** | 10 000 | [Huit (8)] secondes |
| **Vote** | 3 000 | [Deux (2)] secondes |

La solution doit être dimensionnée pour être capable de fournir une réponse dans un délai maximal de [trente (30)] minutes pour les demandes lancées et notamment pour l’export des résultats électoraux au format CSV.

Les performances attendues concernant les traitements par lots à la charge du titulaire sont les suivantes :

| **Type de fonctionnalité** | **Volume de données traitées (à adapter selon la taille de la structure organisatrice)** | **Temps de réponse maximum** |
| --- | --- | --- |
| **Import et contrôle des référentiels Electeurs** | 1 500 000 lignes | [Quatre (4)] heures |
| **Import et contrôle des autres référentiels électoraux** | 35 000 lignes | [Une (1)] heure |
| **Scellement** | Tous les scrutins | [Trente (30)] minutes |
| **Dépouillement** | Tous les scrutins | [Deux (2)] heures pour le scrutin présentant la plus grande liste d’électeurs |

En outre, le taux de succès minimum des traitements par lots attendu doit être de 99,50%. Ce taux constate le nombre d’activités terminées avec succès dans le délai imparti.

Le candidat doit préciser dans son CRT comment la SVE va respecter ses diverses exigences pour pouvoir présenter une qualité de service garantie en termes de disponibilité, de fiabilité et de tenue de la charge.

# L’assistance technique

Cette section 3 est consacrée aux prestations d’assistance technique du prestataire. Sa rédaction est assez proche de celle de la section 9 du document corps du CCTP consacrée à la prestation 7 d’assistance technique avec laquelle elle demeure totalement cohérente.

Si la rédaction de la section 9 du document corps est orientée vers la production du tableau des livrables de la prestation 7, la rédaction de cette section 3 est orientée vers la production du tableau des niveaux de service attendus.

Il est important de conserver ces deux sections et d’utiliser cette section 3 de l’annexe II pour permettre à chaque autorité organisatrice d’y développer ses besoins propres et les niveaux de services qu’elle veut exiger du titulaire.

En application des dispositions de l’article R. 211-527 du CGFP, l'autorité organisatrice met en place un centre d’assistance (CA) chargé d’assurer la mission d’assistance technique de niveau 1 et, à ce titre :

* D’aider les électeurs dans l’utilisation du portail Electeurs et l'accomplissement des opérations électorales ;
* De répondre aux membres des BVE, des BCVE et des organisations syndicales ayant déposé une candidature, pour toute demande d’assistance dans le cadre de l’exercice de leurs missions.

Le titulaire doit, au titre des prestations 6 d’assistance pour les cérémonies et 7 d’assistance aux utilisateurs de la SVE, mettre en place l’organisation et les intervenants permettant d’assurer le niveau 2 et de contribuer au niveau 3 du support technique aux utilisateurs de la SVE. Au titre de la prestation 5 de formation, le titulaire forme les membres du CA pour exercer leur mission et répondre aux demandes d’assistance de « niveau 1 » des utilisateurs de la SVE.

## Support de niveau 2

Le titulaire assure un support de niveau 2 technique et un support de niveau 2 fonctionnel auprès des agents de l’autorité organisatrice qui sont membres du CA. A cet effet, le titulaire met en place une « cellule d’assistance et de support technique et fonctionnel de niveau 2 » qui soit joignable par formulaire de contact, par mail et par téléphone. Ce centre d’appels est destiné à l’assistance de premier niveau des membres du CA et de la direction projet de l’autorité organisatrice.

Le titulaire met en place les outils permettant de formaliser, tracer et suivre les échanges entre les niveaux 1, 2 et 3 de support technique et fonctionnel des utilisateurs de la solution de vote électronique. Le formulaire de contact du CA est notamment associé à l’outil de type *helpdesk* de déclaration et suivi des incidents qui est validé lors de la prestation 1.

Les membres du CA ou de la direction projet de l’autorité organisatrice doivent émettre chaque demande de support de niveau 2 au moyen :

* Du formulaire dédié de demande d’assistance ;
* Ou d’un courriel ;
* Ou encore d’un appel téléphonique sur un numéro de téléphone non-surtaxé.

La demande fait l’objet d’un accusé de réception (AR) du titulaire par courrier électronique dans un délai maximum de [quinze (15)] minutes. Ce courriel d’AR précise :

* Le numéro de suivi de la demande ;
* L’identité du demandeur ;
* La date et l’heure de réception de la demande ;
* Le motif de la demande ;
* La référence aux éventuels documents ou copies d’écrans annexés à la demande.

Toutes les demandes d’assistance au niveau 2 doivent être tracées via l’outil de gestion des incidents pour permettre à l’autorité organisatrice d’avoir accès en permanence à la liste exhaustive des demandes de support de niveau 2. Chaque demande est documentée pour préciser les dates et heures :

* De soumission de la demande par l’autorité organisatrice ;
* De réponse par le titulaire à cette demande,
* D'analyse et de résolution de l'incident par le titulaire.

Les modalités et exigences relatives au support de niveau 2 fourni par le titulaire sont notamment les suivantes :

* Pendant la période d’avant-vote qui se comprend comme la période commençant avec l’ouverture du portail Electeurs et se terminant avec l’ouverture de la période de vote mais ne comprenant pas les cérémonies :
  + Assistance garantie chaque jour ouvré, de [9h00 à 18h00] ;
  + Emission d’un AR de la demande dans un délai de [quinze (15)] minutes et prise de contact téléphonique sous [quinze (15)] minutes après émission de l’AR ;
  + Le délai de résolution maximum est de [huit (8)] heures. Au terme de ce délai, l’incident doit être résolu ou une solution de contournement opérationnelle est mise en œuvre. Si la résolution est impossible alors il y a escalade vers le support de niveau 3 ;
  + Dès la clôture de l’incident, son traitement est enregistré dans l’outil de gestion des incidents et sa résolution est actée par courriel ;
* Pendant chaque cérémonie :
  + Assistance garantie chaque jour ouvré de [8h00 à 20h00] ;
  + Emission d’un AR de la demande dans un délai de [cinq (5)] minutes et prise de contact téléphonique avec le BCVE en charge de la cérémonie sous [cinq (5)] minutes après émission de l’AR ;
  + Délai de résolution maximum fixé à [une (1)] heure. Au terme de ce délai, l’incident doit être résolu ou une solution de contournement opérationnelle est mise en œuvre. Si la résolution est impossible alors il y a escalade vers le support de niveau 3 ;
  + Dès clôture de l’incident, son traitement est enregistré dans l’outil de gestion des incidents et sa résolution est actée par courriel à l’émetteur de la demande d’assistance ;
* Pendant la période de vote :
  + Assistance garantie pendant toute la durée de la période de vote en mode 24h/24 7j/7 en heure ouvrées et non ouvrées ;
  + Emission d’un AR de la demande dans un délai de [quinze (15)] minutes et prise de contact téléphonique et, le cas échéant, par courriel sous [quinze (15)] minutes en heures ouvrées et sous [trente (30)] minutes en heures non-ouvrées ;
  + Résolution de l’incident sous un délai maximum fixé à [quatre (4)] heures. Cette résolution peut être une solution de contournement ou une escalade vers le support de niveau 3 ;
  + Dès clôture de l’incident, son traitement est enregistré dans l’outil de gestion des incidents et sa résolution est actée par courriel à l’émetteur de la demande ;
* Pendant la période post-vote qui se comprend comme commençant dès après la fin de la cérémonie de dépouillement et se prolongeant jusqu’à la fin des opérations d’archivage *ad probationem* :
  + Assistance garantie chaque jour ouvré de [9h00 à 18h00] ;
  + Emission d’un AR de la demande dans un délai de [quinze (15)] minutes ;
  + Délai de résolution maximum fixé à [huit (8)] heures. Au terme de ce délai, l’incident doit être résolu ou une solution de contournement opérationnelle est mise en œuvre. Si la résolution est impossible alors il y a escalade vers le support de niveau 3 ;
  + Dès clôture de l’incident, son traitement est enregistré dans l’outil de gestion des incidents et sa résolution est actée par courriel à l’émetteur de la demande.

| Période | Objectif à atteindre | Valeur |
| --- | --- | --- |
| Avant-vote | Période de couverture | [9h00 à 18h00] jour ouvré |
| Délai maximum émission AR d’une demande | [quinze (15)] minutes |
| Délai maximum appel téléphonique à l’émetteur de la demande après émission de l’AR de la demande | [quinze (15)] minutes] |
| Délai maximum de résolution | [huit (8)] heures |
| Cérémonies | Période de couverture | [8h00 à 20h00] jour ouvré |
| Délai maximum émission AR d’une demande | [cinq (5)] minutes |
| Délai maximum appel téléphonique à l’émetteur de la demande après émission de l’AR de la demande | [cinq (5)] minutes |
| Délai maximum de résolution | [une (1)] heure |
| Vote | Période de couverture | 24h/24 7j/7 |
| Délai maximum émission AR d’une demande | [quinze (15)] minutes |
| Délai maximum appel téléphonique à l’émetteur de la demande après émission de l’AR de la demande | [quinze (15)] minutes en heure ouvrée [trente (30)] minutes en heure non-ouvrée |
| Délai maximum de résolution | [quatre (4)] heures |
| Post-vote | Période de couverture | [9h00 à 18h00] jour ouvré |
| Délai maximum émission AR d’une demande | [quinze (15)] minutes |
| Délai maximum de résolution | [huit (8)] heures |

## Cellule de support de niveau 3 du titulaire

Il est exigé du titulaire qu’il mette en œuvre deux cellules d’assistance technique :

Une première cellule d’assistance de niveau 2 (section 3.1) qui est surtout consacrée au support du centre d’assistance qui est en charge du niveau 1 d’assistance des utilisateurs ;

Une seconde cellule à qui est consacrée la section 3.2 et qui est celle de « l’expertise » car elle intervient en support de la direction projet de l’autorité organisatrice comme de la CdST (sachant que c’est bien la CdST qui est en charge du niveau 3 d’assistance aux utilisateurs).

Rien ne s’oppose à ce que le titulaire décide de fusionner ces deux cellules mais il doit être en mesure de fournir effectivement un niveau expertise pour cette assistance de niveau 3.

Le support de niveau 3 des utilisateurs de la SVE est assuré par la CdST. En complément de ses représentants qui sont membres de cette cellule, le titulaire met en place une cellule d’assistance technique et fonctionnelle de niveau 3 à l’attention de la CdST. Les modalités de fonctionnement de cette assistance à la CdST sont notamment les suivantes :

* Pendant la période d’avant-vote :
  + Assistance garantie chaque jour ouvré, de [9h00 à 18h00] ;
  + Emission d’un AR de la demande dans un délai de [cinq (5)] minutes et prise de contact téléphonique sous [dix (10)] minutes après émission de l’AR ;
  + L’assistance de la CdST pour la résolution de l’incident fait l’objet d’une obligation de moyen renforcée avec un délai de résolution maximum fixé à [quatre (4)] heures ;
  + Dès la clôture de l’incident, son traitement est enregistré dans l’outil de gestion des incidents et sa résolution est actée par courriel ;
* Pendant chaque cérémonie :
  + Assistance garantie chaque jour ouvré, de [8h00 à 20h00] ;
  + Emission d’un AR de la demande dans un délai de [cinq (5)] minutes et prise de contact téléphonique sous [cinq (5)] minutes après émission de l’AR ;
  + L’assistance de la CdST pour la résolution de l’incident fait l’objet d’une obligation de résultat avec un délai de résolution maximum fixé à [trente (30)] minutes ;
  + Dès la clôture de l’incident, son traitement est enregistré dans l’outil de gestion des incidents et sa résolution est actée par courriel ;
* Pendant la période de vote :
  + Assistance garantie pendant toute la durée de la période de vote en mode 24h/24 7j/7 en heure ouvrées et non ouvrées ;
  + Emission d’un AR de la demande dans un délai de [cinq (5)] minutes ;
  + Prise de contact téléphonique sous [cinq (5)] minutes en heures ouvrées ;
  + Prise de contact téléphonique sous [vingt (20)] minutes en heures non-ouvrées.
  + L’assistance de la CdST pour la résolution de l’incident fait l’objet d’une obligation de moyen renforcée avec un délai de résolution maximum fixé à [deux (2)] heures ;
  + Dès la clôture de l’incident, son traitement est enregistré dans l’outil de gestion des incidents et sa résolution est actée par courriel ;
* Pendant la période post-vote :
  + Assistance garantie chaque jour ouvré, de [9h00 à 18h00] ;
  + Emission d’un AR de la demande dans un délai de [cinq (5)] minutes et prise de contact téléphonique sous [quinze (15)] minutes après émission de l’AR ;
  + L’assistance de la CdST pour la résolution de l’incident fait l’objet d’une obligation de moyen renforcée avec un délai de résolution maximum fixé à [huit (8)] heures ;
  + Dès la clôture de l’incident, son traitement est enregistré dans l’outil de gestion des incidents et sa résolution est actée par courriel.

| Période | Objectif à atteindre | Valeur |
| --- | --- | --- |
| Avant-vote | Période de couverture | [9h00 à 18h00] jour ouvré |
| Délai maximum émission AR d’une demande | [cinq (5)] minutes |
| Délai maximum appel téléphonique à l’émetteur de la demande après émission de l’AR de la demande | [dix (10)] minutes |
| Délai maximum de résolution | [quatre (4)] heures |
| Cérémonies | Période de couverture | [8h00 à 20h00] jour ouvré |
| Délai maximum émission AR d’une demande | [cinq (5)] minutes |
| Délai maximum appel téléphonique à l’émetteur de la demande après émission de l’AR de la demande | [cinq (5)] minutes |
| Délai maximum de résolution | [trente (30)] minutes |
| Vote | Période de couverture | 24h/24 7j/7 |
| Délai maximum émission AR d’une demande | [cinq (5)] minutes |
| Délai maximum appel téléphonique à l’émetteur de la demande après émission de l’AR de la demande | [cinq (5)] minutes en heure ouvrée [vingt (20)] minutes en heure non-ouvrée |
| Délai maximum de résolution | [deux (2)] heures |
| Post-vote | Période de couverture | [9h00 à 18h00] jour ouvré |
| Délai maximum émission AR d’une demande | [cinq (5)] minutes |
| Délai maximum appel téléphonique à l’émetteur de la demande après émission de l’AR de la demande | [quinze (15)] minutes |
| Délai maximum de résolution | [huit (8)] heures |

Cette cellule de support technique et fonctionnel de niveau 3 du titulaire est chargée d’assister la CdST dans la vérification de l'origine de tout dysfonctionnement ou incident qui lui est escaladé, dans l’estimation de sa gravité et dans la préconisation des actions à mettre en œuvre. Les délais de résolution doivent respecter les exigences de disponibilité de la solution de vote électronique et la garantie de temps de rétablissement (GTR) qui qui sont notamment précisés dans l’annexe III.

## Traçabilité

Le titulaire assure la traçabilité de toutes les demandes d'assistance et de support de niveau 2 comme de niveau 3 avec notamment l’enregistrement dans l’outil de gestion des incidents :

* De l’identification de l’origine de la demande d’assistance ;
* Des dates et heures de soumission de la demande ;
* Des dates et heures de réponse par l’assistance technique du titulaire ;
* De l’identification de l’émetteur de la réponse avec ses coordonnées ;
* De la synthèse de l'analyse et de la résolution de l'incident.

L'autorité organisatrice doit avoir accès en permanence à la liste exhaustive des dossiers d’interventions d’assistance aux niveaux 2 comme 3. Plus globalement, la « traçabilité » est traitée dans l’annexe III consacrée aux exigences de sécurité.

Le candidat doit documenter dans son CRT les modalités d’organisation de ses cellules d’assistance technique et fonctionnelle de niveau 2 et de niveau 3. Il est attendu que le candidat précise si les coordonnées de contact par téléphone et messagerie électronique des deux cellules seront différentes ou identiques. Le candidat doit aussi préciser si une externalisation de ses prestations d’assistance est envisagée auprès d’un tiers et, le cas échéant, il doit identifier ce tiers et la nature des prestations qui vont lui être confiées.

# Notice d’information détaillée

## Principes

Pour tout le présent CCTP :

* Une « notice de vote » désigne une notice d’information détaillée dans laquelle est imprimé un secret indispensable à l’électeur pour pouvoir voter ;
* Une « notice d’information » désigne une notice d’information détaillée ne comportant aucun secret imprimé ;
* Une « notice » désigne indifféremment une notice de vote ou une notice d’information.

En application des dispositions de l’article R. 211-553 du CGFP, l'autorité organisatrice doit communiquer à chaque électeur une notice d’information détaillée sur le déroulement des opérations électorales. Chaque électeur doit recevoir cette notice au moins quinze (15) jours avant le début de la période de vote. Les modalités de transmission prévues par cet article R. 211‑553 sont :

* Le courrier postal ;
* Ou le courrier électronique ;
* Ou la remise en main propre contre signature.

Cette notice d’information détaillée doit inclure :

* Un guide synthétique d’utilisation de la SVE ;
* Les prérequis techniques pour l’accès à la SVE ;
* L’URL d’accès au portail Electeurs, avec notamment :
  + L’accès aux listes de candidats et aux professions de foi de ces candidats ;
  + L’accès au portail de vote.

La notice n’inclut ni les listes de candidats, ni les logos, ni les professions de foi, qui sont mises à disposition des électeurs via le portail Electeurs. Des manuels d’utilisation des fonctionnalités du portail Electeurs et du portail de vote peuvent être mis à disposition des électeurs sur le portail Electeurs pour compléter la notice. Cette dernière peut alors préciser aux électeurs comment consulter voire télécharger ces manuels.

## Personnalisation de la notice

Toute notice est personnalisée selon la charte graphique de l’autorité organisatrice. Le titulaire formalise cette notice et soumet son projet à la direction de projet de l’autorité organisatrice.

Si la notice d’information détaillée doit être utilisée comme canal pour transmettre un secret, qu’il s’agisse d’un authentifiant ou du code de vote, le titulaire doit accompagner la présentation de son projet de notice avec les modalités permettant d’assurer la confidentialité dudit secret une fois qu’il est intégré dans la notice qui devient une « notice de vote ».

# Notice de vote

Aucun texte n’impose que la notice d’information détaillée soit utilisée comme canal de communication d’un secret. Cependant, cette notice d’information détaillée est souvent utilisée pour transmettre à chaque électeur son « code de vote ». Si tel devait être le cas, alors la procédure d’impression comme de distribution des notices intégrant un secret doit être sécurisée pour garantir la confidentialité du secret qui est imprimé dans la notice et assurer que seul l’électeur attributaire qui réceptionne la notice aura connaissance dudit secret.

Cette procédure peut être formalisée par une PES « Impression des notices ». Si cette PES existe, le candidat doit la prendre en compte et l’appliquer pour l’ensemble des opérations de conception, édition, impression et expédition des notices.

Il est recommandé que cette impression des notices fasse l’objet d’une PES d’impression des notices susceptible d’être intégrée au CCTP sous forme d’une annexe.

## Génération et conservation d’une notice de vote

Le SyVE doit exploiter le référentiel Electeurs pour créer un fichier contenant tous les secrets qui vont devoir être imprimés dans chaque notice pour que ce secret puisse être communiqué à son électeur attributaire. Ce fichier des secrets à imprimer doit être protégé notamment par chiffrement pour en assurer l’intégrité et la confidentialité. Il est exploité pour imprimer les notices de vote sur deux étapes :

* Une première étape d’impression de chaque notice dans un format numérique de type nom\_notice.pdf où « nom\_notice » doit permettre d’identifier chaque notice. Un fichier d’enregistrement de ces notices dématérialisées doit être constitué et chiffré pour en garantir la confidentialité ;
* Une seconde étape :
  + D’impression sur papier de chaque notice de vote nom\_notice.pdf si l’autorité organisatrice commande la prestation 11 d’impression sur papier des notices de vote du CCTP ;
  + De communication de chaque notice dématérialisée nom\_notice.pdf à son électeur attributaire si l’autorité organisatrice ne commande pas la prestation 11.

Les modalités de génération, d’impression et de communication des notices de vote doivent être conçues de façon à garantir la confidentialité du secret intégré à chaque notice. Au surplus, pendant toutes les périodes d’avant-vote et de vote, l’autorité organisatrice ne peut avoir communication que de la version chiffrée du fichier d’enregistrement des notices nom\_notice.pdf et à condition que l’autorité organisatrice ne dispose pas de la clef de déchiffrement. Le titulaire conserve les clés de déchiffrement jusqu’à la fin de la période de vote.

Une fois que la clôture du dépouillement a été prononcée, ce fichier d’enregistrement des notices de vote dématérialisées est communiqué sans délai par le titulaire à l’autorité organisatrice avec les clés de chiffrement et de déchiffrement. L’autorité organisatrice conserve l’enregistrement chiffré et les clefs de chiffrement/déchiffrement au titre de l’archivage *ad probationem*.

## Impression, conditionnement et expédition des notices de vote

### La procédure d’impression et d’expédition des notices de vote “papier”

Toute cette section doit être supprimée de l’annexe II si l’autorité organisatrice décide de ne pas utiliser une notice de vote « papier » pour communiquer un secret à chaque électeur.

A noter toutefois qu’il est possible de conserver cette section pour présenter une procédure d’impression des « notices d’information détaillée papier » si l’autorité organisatrice décide d’imprimer des notices sans secret et de les mettre sous plis pour les remettre ensuite à chaque électeur.

Dans un tel cas, il n’y a plus d’exigences de sécurisation de la procédure d’impression puisque les notices « papier » ne contiennent aucun secret.

Les opérations liées à l’impression sur papier, au conditionnement (colisage) et à l’expédition des notices de vote font l’objet d’une organisation-projet spécifique qui est cadrée pendant les prestations 1 et 2 du CCTP. L’autorité organisatrice doit communiquer au titulaire un fichier formalisant l’ensemble des colis de notices de vote à produire avec confirmation de l’adresse de livraison de chaque colis. Les notices de vote doivent en effet être regroupées par colis pour un même service d’affectation administrative (SAA) des électeurs. Ces colis de notices de vote pour SAA doivent ensuite être conditionnés pour livraison sur les sites de regroupement géographiques désignés par l’autorité organisatrice.

Il est recommandé de préciser ici le nombre de site de regroupement qu’il est envisagé en commençant la phrase par « *A titre indicatif, l’autorité organisatrice envisage d’utiliser xyz sites de regroupement géographique*» et si possible les lister pour que le candidat puisse valablement déterminer les coûts de livraison sur ces sites des colis de notices.

Le titulaire procède à l’impression des notices individuelles de vote nom\_notice.pdf sur papier à partir du fichier d’enregistrement des notices de vote dématérialisées. Ce processus d’impression sur papier doit être conçu pour garantir que le secret intégré à chaque notice ne peut être compromis.

Le conditionnement individuel de chaque notice de vote « papier » et notamment son format, son pliage, et la pellicule d’occultation du secret imprimé, doivent permettre de garantir l’intégrité du caractère strictement confidentiel des données personnelles d’identification et du secret dont la notice de vote « papier » est le canal de communication.

En complément du fichier d’enregistrement des notices de vote dématérialisées, le titulaire doit procéder à une copie scan des notices de votes « papier ». Ces copies sont enregistrées dans une archive de sauvegarde dont la confidentialité doit être assurée par chiffrement. L’archive chiffrée est communiquée sans délai par le titulaire à l’autorité organisatrice. Le titulaire conserve les clés de déchiffrement jusqu’à la fin de la période de vote. Le titulaire ne doit remettre ces clés à l’autorité organisatrice qu’une fois la clôture du dépouillement prononcée. L’autorité organisatrice conserve l’archive chiffrée des copies scan des notices et les clefs de chiffrement/déchiffrement au titre de l’archivage ad probationem.

L’expédition des colis de notices de vote est réalisée sur palettes ou par conditionnement adapté en vue de leur routage. Ce conditionnement des colis doit comporter les noms et codes du site de regroupement géographique des colis de SAA constituant la destination de l’expédition. Les colis destinés au SAA doivent être étiquetés pour présenter les informations suivantes :

* Code et nom du SAA ;
* Adresse physique de livraison du SAA ;
* Nombre de notices individuelles de vote contenues dans la boite ou colis.

Chaque boîte ou colis de notices de vote « papier » contient :

* Une lettre d’introduction à l’attention du référent notice en charge de la réception de la boîte ou colis des notices ;
* Un bordereau d’attribution pré-renseigné pour la remise de chaque notice de vote de la boîte, ou colis, en main propre de son électeur attributaire ;
* Les notices individuelles de vote sous plis, voire pliées, garantissant la confidentialité du secret imprimé.

Les plis de notice de vote doivent être identifiés au moyen d’un code d’attribution permettant au référent notice d’associer le pli à son électeur attributaire du secret. Ces codes d’attribution ne doivent pas permettre d’identifier l’électeur par leur seule connaissance (principe de pseudonymisation de l’information) mais ils doivent être reportés sur le bordereau d’attribution pré‑renseigné. L’autorité organisatrice communiquera à chaque référent notice une table associant chaque code d’attribution à l’identité de l’électeur attributaire pour permettre au référent notice de remettre le bon pli à son attributaire.

La rédaction ci-dessus des exigences techniques suppose que le titulaire doit expédier les colis de notices de vote pour SAA sur un à plusieurs sites géographiques de regroupement puisque c’est l’autorité organisatrice qui va prendre en charge l’expédition des colis de notices de vote vers chaque SAA où ils seront réceptionnés par les référents notice.

L’autorité organisatrice peut toutefois décider que c’est le titulaire qui doit procéder à la livraison de tous les colis de notices à destination des SAA et supprimer le passage par l’intermédiaire de points de regroupement géographiques. Si tel est le cas, la présente annexe doit être modifiée en conséquence mais aussi la section consacrée à la prestation 12 d’impression des notices de vote du CCTP.

Si l’autorité organisatrice décide de ne pas intégrer un secret dans les notices d’information détaillées et de privilégier des canaux dématérialisés de communication des secrets de la SVE à ses utilisateurs, cette section d’impression des notices doit être supprimée de l’annexe II.

### Les rôles des référents notice et de la cellule de supervision technique

Les analyses de risques réalisées pour les processus d’impression mis en œuvre pour les élections professionnelles de 2022 ont identifié divers évènements redoutés et notamment :

* L’impossibilité de produire les référentiels indispensables pour permettre l’impression des notices ;
* L’altération des fichiers exploités par le processus d’impression et de distribution des notices de vote ;
* La compromission des fichiers et la divulgation des secrets destinés à être imprimés ;
* Le détournement des notices pour compromettre les secrets de vote qui y sont imprimés ;
* L’exploitation des secrets imprimés dans des notices de vote qui n’auraient pas pu être remise à leur électeur attributaire.

La prise en compte de ces évènements redoutés conduit l’autorité organisatrice à exiger une sécurisation du processus d’impression des notices de vote qui est précisée dans la présente annexe comme dans le document corps du CCTP. Il demeure nécessaire de compléter cette sécurisation par :

* Un contrôle efficace de la remise des notices de vote à leur électeur attributaire reposant notamment sur une traçabilité de cette remise exploitant les bordereaux d’attribution ;
* Une destruction effective de toutes les notices de vote qui n’auraient pas pu être remises à leur électeur attributaire. Cette destruction devant intervenir avant l’ouverture de la période de vote ;
* Une suppression avant scellement de la SVE de tous les secrets imprimés sur les notices qui n’auront pas pu être remises à leur électeur attributaire.

Le titulaire doit donc développer deux fonctionnalités du portail Gestion :

* Fonction de déclaration des notices de vote non-attribuées. Cette fonction est réservée aux référents notice pour lesquels elle doit afficher leurs bordereaux d’attribution en leur demandant d’y cocher les notices qui n’ont pas pu être attribuées à leur destinataire. Le SyVE doit prendre en compte la liste des notices cochées pour en identifier les secrets qui y étaient imprimés et les marquer comme devant être supprimés par la fonction de suppression ;
* Fonction de suppression des secrets imprimés dans toutes les notices de vote déclarées « non-attribuées » par les référents notice. Cette fonction est réservée aux membres qui représentent l’autorité organisatrice dans la CdST pour lesquels elle doit afficher le nombre de notices déclarées comme non-attribuées par SAA et pour l’ensemble des électeurs et proposer d’en supprimer tous les secrets imprimés. Cette suppression doit être réalisée en une seule opération et ne reposer que sur une décision globale : aucune suppression partielle ne doit pouvoir être proposée. La fonction de suppression doit demander au membre de la CdST de décider cette suppression puis de la valider avant que le SyVE ne procède à la suppression effective des secrets.

Toute utilisation de ces deux fonctions doit être tracée avec horodatage et identification de l’utilisateur avec pouvoirs comme du poste à partir duquel il accède au portail Gestion et à l’une ou l’autre de ces deux fonctions.

Le candidat doit documenter dans son CRT les modalités d’organisation des opérations d’impression, de mise sous pli sécurisé et de colisage des notices « papier » qu’il propose et comment il peut les sécuriser si les notices doivent intégrer un secret comme le code de vote.