

Matériel et infrastructure

Vote Électronique Neuchâtel

Auteur	Direction du vote électronique
Date	09.06.2026
Version	1.0
Classification	Aucune

Contrôle des modifications

Version	Date	Description	Nom
0.9	16.12.2025	Version pour les auditeurs	Direction du vote électronique
0.99	17.04.2026	Modifications formelles	Direction du vote électronique
1.0	09.06.2026	Modifications apportées aux points 4.2, 5 et 7 / Modifications formelles	Direction du vote électronique

Autorités de contrôle/de validation

Contrôle	Validation	Date
Vice-chancelière	Vice-chancelière	05.06.2026

Documents référencés

N°	Document	Version
[1]	Concept de vote électronique	Version actuelle
[2]	Ordonnance de la ChF du 25 mai 2022 sur le vote électronique (OVotE, RS 161.116)	Version du 1 ^{er} juillet 2022
[3]	Basic installation and Hardening	Version actuelle
[4]	Recommandations SDM Hardening de la Poste Suisse https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/Operations/Recommendation_Safety_Measures_Cantonal_Infrastructure.md	Version actuelle sur GitLab
[5]	Directive sur la sécurité de l'information	Version actuelle
[6]	Glossaire	Version actuelle

Table des matières

1	But du document	4
2	Aperçu des composants et délimitation	4
3	Responsabilités	5
4	Aperçu du matériel informatique	6
4.1	Ordinateurs	6
4.2	Supports de données.....	7
4.3	Matériel informatique supplémentaire	8
5	Installation des ordinateurs.....	8
5.1	Définition de l'image pour chaque scrutin	9
5.1.1	Système d'exploitation.....	10
5.1.2	Logiciels supplémentaires	10
5.1.3	Renforcement	10
5.2	Vérification de l'installation et du renforcement.....	11
5.3	Comptes utilisateurs	11
5.4	Installation des logiciels de vote électronique	11
6	Locaux et mesures de protection	12
7	Stockage	13
8	Sécurité de la communication.....	13
9	Liste des illustrations.....	14
10	Liste des tableaux.....	14

1 But du document

Le présent document décrit la préparation et l'utilisation du matériel et de l'infrastructure nécessaires au déroulement d'un scrutin. Il expose également les modalités de conservation des différents moyens techniques ainsi que la marche à suivre après l'expiration du délai de conservation.

2 Aperçu des composants et délimitation

Le système de vote électronique productif est composé des éléments présentés sous l'illustration 1 (voir *point 4.1*).



Illustration 1 : Composants du vote électronique

Le présent document concerne uniquement le matériel informatique utilisé par le canton pour le vote électronique et l'organisation d'un scrutin.

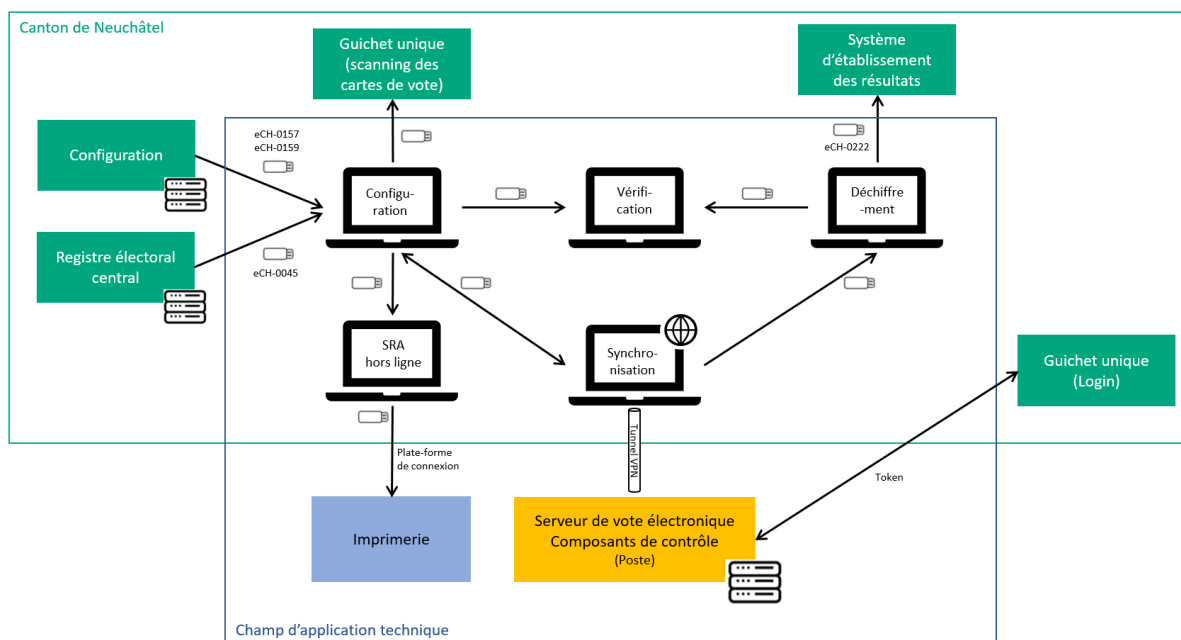


Illustration 2 : Délimitation du champ d'application

Le matériel ainsi que les composants de l'imprimerie et les systèmes périphériques du canton (en vert dans le graphique) n'entrent pas dans le champ d'application du présent document.

3 Responsabilités

La direction du vote électronique est responsable de :

- L'acquisition des ordinateurs,
- L'installation de base et la mise en œuvre des mesures de sécurité techniques et organisationnelles recommandées (renforcement),
- L'installation du logiciel de vote électronique nécessaire à l'organisation d'un scrutin sur les différents ordinateurs conformément aux instructions de la Poste,
- La conservation du matériel informatique,
- La suppression sécurisée des données.

Pour certaines tâches (mise en œuvre de l'image pour l'installation des ordinateurs), le canton fait appel des partenaires externes (voir le document de référence [1]). Diverses tâches sont effectuées par les membres de la commission administratives.

4 Aperçu du matériel informatique

Les ordinateurs et les supports de données utilisés pour le vote électronique sont décrits ci-après. Conformément au ch. 3.20 de l'ordonnance de la ChF sur le vote électronique (OVotE, voir le *document de référence [2]*), tout accès et toute utilisation d'un composant fiable ou d'un support de données sont consignés dans un procès-verbal.

4.1 Ordinateurs

Pour le vote électronique, le canton de Neuchâtel utilise les ordinateurs suivants :

- 5 ordinateurs déployés en production : 1 ordinateur en ligne, 3 ordinateurs hors ligne, 1 ordinateur hors ligne dédié à l'établissement des cartes de vote (SRA).
- 2 ordinateurs pour les tests et de remplacement : 1 ordinateur en ligne et 1 ordinateur hors ligne.

Les ordinateurs hors ligne ne sont jamais connectés au réseau cantonal ou à Internet. Tous les ordinateurs sont identifiés de manière visible.

Désignation	Environnement	But	Logiciel
Ordinateur de synchronisation (en ligne)	Production	Administration du vote électronique (par ex. transfert de la configuration du vote et du registre des électrices et électeurs anonymisé vers le portail de vote ; téléchargement de l'urne électronique avec les votes chiffrés).	• Secure Data Manager
Ordinateur de configuration (hors ligne)	Production	Configuration du scrutin, génération des codes pour les cartes de vote et mise à disposition des urnes par la commission électorale.	• Data Integration Service • Secure Data Manager • Direct Trust Tool
Ordinateur de déchiffrement (hors ligne)	Production	Mélange des votes, déchiffrement des votes par la commission électorale et traitement des résultats.	• Secure Data Manager
Ordinateur de vérification (hors ligne)	Production	Vérification du scrutin.	• Verifier
Ordinateur dédié aux cartes de vote (SRA) (hors ligne)	Production	Établissement des cartes de vote.	• VCPS • Voting Card Register
Ordinateur de test et remplacement (en ligne)	Test / éventuellement production (remplacement)	Ordinateur de remplacement en cas de panne de l'ordinateur en ligne.	• Comme pour l'ordinateur en ligne

Désignation	Environnement	But	Logiciel
Ordinateur de test et de remplacement (hors ligne)	Test / éventuellement production (remplacement)	Ordinateur de remplacement en cas de panne d'un ordinateur hors ligne déployé en production et pour le processus du Dispute Resolver.	- Comme pour les ordinateurs hors ligne - Dispute Resolver (ordinateur de remplacement hors ligne)

Tableau 1 : Ordinateurs

4.2 Supports de données

Le canton de Neuchâtel utilise divers supports de données pour chaque scrutin, conformément aux directives de la Poste et aux prescriptions cantonales. Le principe consiste à utiliser un support de données dédié à chaque opération ou étape de processus. Dans certains cas, des clés USB protégées par un code PIN avec chiffrement matériel des données sont utilisées¹. Le canton tient un inventaire des supports de données.

Les données sont supprimées après l'expiration du délai de conservation ou lors de la préparation du scrutin suivant selon le principe du double contrôle. Les exceptions à cette règle sont énumérées ci-après. La suppression des supports de données est effectuée avec sDelete. Les supports de données sont ensuite reformatés. Ces opérations sont effectuées sur un appareil hors ligne.

Matériel informatique	But
Clés USB	- Supports de données dédiés aux processus. - Utilisés pour le processus principal (transfert de données entre les ordinateurs, par ex. de l'ordinateur de configuration vers l'ordinateur de synchronisation et inversement). - Supports de données dédiés aux transferts. - Utilisés pour transférer des données sur les ordinateurs cantonaux ou les systèmes périphériques (par ex. transfert de données vers le système d'établissement des résultats). - Utilisés pour transférer les données d'impression de l'ordinateur SRA sur l'ordinateur cantonal pour le transfert à l'imprimerie (via un site SharePoint du canton dédié). - Supports de données dédiés au Verifier. - Utilisés pour transférer les données sur l'ordinateur de vérification. - Supports de données dédiés à l'image. - Utilisés pour installer l'image. - Supports de données dédiés à l'installation. - Utilisés pour installer le logiciel de vote électronique.

¹ Actuellement : clés USB Kingston Keypad 200c 64 Gb USB-C, chiffrement matériel XTS-AES 256 bits certifié à la norme FIPS 140-3 niveau 3 ([lien](#))

Matériel informatique	But
Clés USB protégées par un code PIN	• Supports de données dédiés aux sauvegardes ○ Différentes sauvegardes sont effectuées pendant le scrutin. Pour ce faire, un support de données séparé est utilisé pour chaque ordinateur (ordinateur de synchronisation, ordinateur de configuration, ordinateur de déchiffrement et ordinateur de vérification). ○ Les données de sauvegarde d'un scrutin sont effacées après l'arrêt de validation du scrutin au moyen du principe du double contrôle. • Supports de données dédiés à l'impression. ○ Utilisés pour transférer les données de cartes de vote de l'ordinateur de configuration vers l'ordinateur SRA. ○ Les données sont effacées après le transfert au moyen du principe du double contrôle. • Supports de données dédiés à la configuration. ○ Les conteneurs contiennent des mots de passe et des certificats pour l'exécution du vote électronique (Direct-Trust et SSL). • Supports de données dédiés au mot de passe du scrutin. ○ Les mots de passe du scrutin (un mot de passe pour la commission administrative et un mot de passe pour la commission électorale) sont enregistrés sur des supports de données séparés (sauvegarde incluse ; les clés de sécurité du scrutin sont générées à partir de ces deux mots de passe lors de l'étape D2 pour le chiffrement et le déchiffrement des votes). La répartition des supports de données entre différentes personnes permet de s'assurer que les mots de passe ne sont réunis qu'au moment du déchiffrement.

Tableau 2 : Supports de données

4.3 Matériel informatique supplémentaire

Le tableau suivant décrit le matériel supplémentaire utilisé.

Matériel informatique	But
Vidéoprojecteur + écran	Permet de projeter les écrans des ordinateurs.

Tableau 3 : Matériel informatique supplémentaire

5 Installation des ordinateurs

Il n'est pas possible d'intégrer les ordinateurs dans un domaine ni de les gérer de manière centralisée. Les ordinateurs hors ligne ne sont jamais connectés au réseau cantonal ou à Internet. De même, l'installation et les mises à jour sont effectuées hors ligne.

Pour l'installation et la configuration, il convient d'utiliser un support contenant le logiciel à installer et les fichiers de configuration. L'installation est divisée en plusieurs étapes :

1. Création d'une image/d'un support d'installation pour chaque scrutin :
Une image contenant les mises à jour et les nouvelles versions logicielles avant le scrutin est créée pour les ordinateurs. Elle doit contenir les éléments nécessaires à l'installation du système (système d'exploitation, pilotes, mises à jour de sécurité, etc.), les logiciels supplémentaires requis ainsi que les scripts pour le renforcement. La valeur de hachage ou la signature est vérifiée pour tous les composants. L'image est structurée de manière à ce que la composition soit facile à suivre. Un prestataire externe élabore l'image de manière centralisée sur mandat des cantons et conformément à ses instructions, puis la lui distribue.
2. Installation de l'image (avec droits d'administrateur locaux) :
L'image est sauvegardée par le canton sur un support de données (clé USB). Les ordinateurs sont sortis du coffre-fort et entièrement reconfigurés avec la nouvelle image (installation Zero-Touch). Tous les ordinateurs sont installés avec la même image selon le principe du double contrôle.
3. Vérification de l'installation et du renforcement :
Le canton vérifie l'installation et le renforcement selon le principe du double contrôle.
4. Installation du logiciel de vote électronique selon les instructions de la Poste (sans droits d'administrateur) :
Le canton vérifie et installe les logiciels fournis par la Poste (SDM, DIS, Verifier, etc.) conformément aux instructions, selon le principe du double contrôle. Aucun droit d'administrateur n'est nécessaire.

Les ordinateurs ne sont jamais mis à jour directement, mais sont réinstallés avec une image actualisée.

5.1 Définition de l'image pour chaque scrutin

Le canton commande la création de l'image au prestataire externe entre onze et douze semaines avant le scrutin. Pour créer l'image, le prestataire met en place un appareil (qui n'est pas un ordinateur de vote électronique) avec l'image du scrutin précédent (voir *le document de référence [3]*). L'ordinateur est connecté à Internet afin de rechercher des mises à jour sur les serveurs de Microsoft : documentation des numéros de mise à jour, téléchargement des mises à jour correspondantes à partir du catalogue Microsoft et réintégration dans l'image. L'ordinateur est ensuite redémarré avec l'image actualisée. Le processus est répété jusqu'à épuisement des mises à jour. Si des mises à jour d'applications sont nécessaires, elles sont téléchargées et intégrées dans le répertoire logiciel de l'image. Les mises à jour des pilotes pour les modèles d'ordinateur et la définition de l'antivirus sont également intégrées dans l'image.

Tout logiciel installé doit être obtenu auprès du fournisseur officiel ou, exceptionnellement, auprès de la Poste (voir *point 5.1.2*). Il convient d'utiliser la dernière version disponible ou la version recommandée par la Poste. Si la dernière version disponible n'est pas utilisée, cela doit être justifié.

Les valeurs de hachage ou les signatures sont vérifiées pour tous les fichiers d'installation. Tous les fichiers sont en outre contrôlés par un scanner antivirus.

5.1.1 Système d'exploitation

Il convient d'utiliser le système d'exploitation Windows 10 LTSC 2021 (image Windows non modifiée de Microsoft). Il est interdit d'utiliser un compte Microsoft ou d'installer un autre logiciel ou une autre application.

5.1.2 Logiciels supplémentaires

Les logiciels suivants sont intégrés dans l'image conformément aux instructions de la Poste :

- Notepad++ : permet d'éditer des fichiers XML.
- KeePass : permet de gérer les certificats et les mots de passe requis pour la réalisation d'un scrutin (génération des mots de passe du scrutin incluse).
- WMGJ « Verificatum Multiplicative Groups Library for Java » (fourni par la Poste) : est utilisé par le SDM.
- KeyStoreExplorer : est nécessaire pour le contrôle du contenu des fichiers Keystore.

Autres logiciels également installés :

- sDelete : permet d'effacer les données de manière sécurisée.
- OpenSSL : permet de signer des fichiers ou de contrôler des signatures.
- HP Hotkey Manager : permet de configurer des raccourcis clavier pour les appareils HP.
- 7-zip : permet de créer et de décompresser des fichiers d'archive de différents formats.
- TotalCommander : permet de gérer des fichiers à deux colonnes pour Windows.
- PowerShell 7 : nécessaire à l'exécution de scripts.
- .NET : permet d'exécuter des applications de bureau Windows existantes.

Aucun autre logiciel n'est installé.

5.1.3 Renforcement

Le renforcement répond aux objectifs suivants :

- Seuls les utilisateurs absolument nécessaires sont à disposition.
- Seuls les programmes impérativement nécessaires sont installés.
- Les recommandations de la Poste en matière de renforcement sont mises en œuvre dans la mesure où cela est possible pour les ordinateurs de vote électronique.
- Les « Microsoft-recommended security configuration baselines for Windows and other Microsoft products » sont mises en œuvre dans la mesure où cela est possible pour les

ordinateurs de vote électronique (<https://www.microsoft.com/en-us/download/details.aspx?id=55319>).

- Tous les adaptateurs réseau sont désactivés à l'exception de l'adaptateur réseau de l'ordinateur de synchronisation (en ligne), qui est obligatoire pour communiquer avec les serveurs de La Poste.

Les recommandations de la Poste en matière de renforcement peuvent être consultées sur GitLab (voir *le document de référence [4]*). Le script de renforcement est publié.

5.2 Vérification de l'installation et du renforcement

Après l'installation de l'image, le canton vérifie l'installation et le renforcement à l'aide d'une liste de contrôle, selon le principe du double contrôle.

5.3 Comptes utilisateurs

Chaque ordinateur dispose de deux comptes : (1) compte administrateur utilisé pour installer l'image, le canton étant le seul à le connaître et à pouvoir le définir ; (2) compte utilisateur pour le scrutin. Des mots de passe différents et sécurisés sont définis pour les deux comptes, conformément à la directive sur la sécurité de l'information (voir *le document de référence [5]*).

5.4 Installation des logiciels de vote électronique

Les logiciels fournis par la Poste sont installés conformément à ses instructions en matière de mises à jour. Les valeurs de hachage des logiciels fournis par la Poste sont contrôlées à l'aide des résultats de la compilation réalisée selon le protocole d'acceptation de Trusted Build et des notes de version. La liste ci-après répertorie les logiciels qu'il convient d'installer sur les différents ordinateurs (appareils).

Logiciel	Type	Description	Installé sur				
			C	S	D	V	SRA
Secure Data Manager (SDM)	Application	Programme principal permettant de configurer un scrutin. Les opérations sont effectuées à l'aide du Secure Data Manager sur les différents ordinateurs afin de garantir la sécurité des données. Le Secure Data Manager permet de synchroniser les données traitées sur l'un des ordinateurs avec les autres ordinateurs, et de synchroniser les données de l'ordinateur en ligne avec les serveurs de vote électronique de la Poste.	X	X	X		
Direct Trust Tool	Application	Outil avec lequel les certificats Direct Trust sont générés.	X				
Data Integration Service (DIS)	Application	Cet outil convertit les données de base du scrutin (fichiers eCH par ex.) pour le Secure Data Manager.	X				

Logiciel	Type	Description	Installé sur				
			C	S	D	V	SRA
Verifier	Application	Le logiciel Verifier permet de vérifier le scrutin.				X	
Voting Card Register (VCR)	Application	Le VCR établit une liste de toutes les ID de cartes de vote avec la circonscription électorale, le nom des électrices et électeurs et les statuts. Il est nécessaire pour le contrôle du double vote.					X
Voting Card Manager (VCM)	Application web	Le VCM permet de procéder à des blocages de cartes de vote pendant le scrutin (dans le cadre du contrôle du double vote). Pour cela, les communes utilisent une prestation du Guichet unique, qui fait appel à un web service du VCM.					
Voting Card Print Service (VCPS)	Application	Ce logiciel permet de créer des cartes de vote prêtes pour impression.					X
Dispute Resolver	Application	Ce logiciel intervient dans des cas exceptionnels, lorsque les données des composants de contrôle (liste des votes confirmés) sont en conflit.	Ordinateur de remplacement hors ligne				

Tableau 4 : Logiciels de vote électronique

Dans le tableau ci-dessus, les abréviations suivantes ont été utilisées pour désigner les ordinateurs :

C = ordinateur de configuration, S = ordinateur de synchronisation, D = ordinateur de déchiffrement, V = ordinateur de vérification, SRA = ordinateur de cartes de vote

6 Locaux et mesures de protection

Le matériel informatique est conservé uniquement dans les locaux du service informatique de l'Entité neuchâteloise, dotés d'un accès sécurisé. Seuls les collaborateurs du canton munis d'un badge ou les visiteurs accompagnés peuvent y accéder. L'accès aux bureaux n'est possible qu'avec une clé. De plus amples informations sur le stockage sont exposées au chapitre 7.

Pendant un scrutin, le matériel informatique est extrait du coffre-fort, puis installé et préparé pour son utilisation dans la salle prévue à cet effet. Le matériel utilisé ne doit jamais être accessible sans surveillance et doit donc être surveillé en permanence.

Si le matériel informatique (ordinateurs, supports de données) n'est pas utilisé pendant une période prolongée, il doit être placé dans le coffre-fort conformément au chapitre 7. Les accessoires comme les câbles d'alimentation électrique, les stations d'accueil, vidéoprojecteurs, etc. n'ont pas besoin d'être démontés.

Toutes les opérations (sorties et mises au coffre-fort, etc.) doivent être consignées par deux personnes dans un procès-verbal.

7 Stockage

Le matériel informatique (ordinateurs, supports de données) est stocké dans un coffre-fort situé au service informatique de l'Entité neuchâteloise, dotés d'un accès sécurisé. Le coffre-fort se trouve dans un bureau fermé à clé et est accessible au moyen d'un code PIN à 16 chiffres.

Pour des raisons de sécurité, le code PIN à 16 chiffres est divisé entre deux groupes de personnes disposant chacun de 8 chiffres. L'accès au coffre-fort nécessite la présence d'une personne de chaque groupe.

Pour les supports de données dédiés au mot de passe du scrutin pour la commission électorale, un coffre-fort supplémentaire est situé dans le même local, avec les mêmes règles de sécurité. Le canton s'assure que l'accès à ce second coffre-fort n'est possible que par d'autres personnes. Ces dernières ne peuvent pas accéder au premier coffre-fort.

8 Sécurité de la communication

Pour les ordinateurs qui doivent être connectés au système de vote électronique de la Poste dans le cadre d'un scrutin, il est possible établir une connexion via un segment de réseau configuré séparément pour le vote électronique. Cette opération est mise en œuvre par une règle dans le renforcement. Une connexion WLAN n'est pas possible, car cette fonction est désactivée lors du renforcement.

La connexion au serveur de vote électronique de la Poste se fait via un chiffrement SSL.

9 Liste des illustrations

Illustration 1 : Composants du vote électronique	4
Illustration 2 : Délimitation du champ d'application	5

10 Liste des tableaux

Tableau 1 : Ordinateurs	7
Tableau 2 : Supports de données	8
Tableau 3 : Matériel informatique supplémentaire	8
Tableau 4 : Logiciels de vote électronique	12