ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

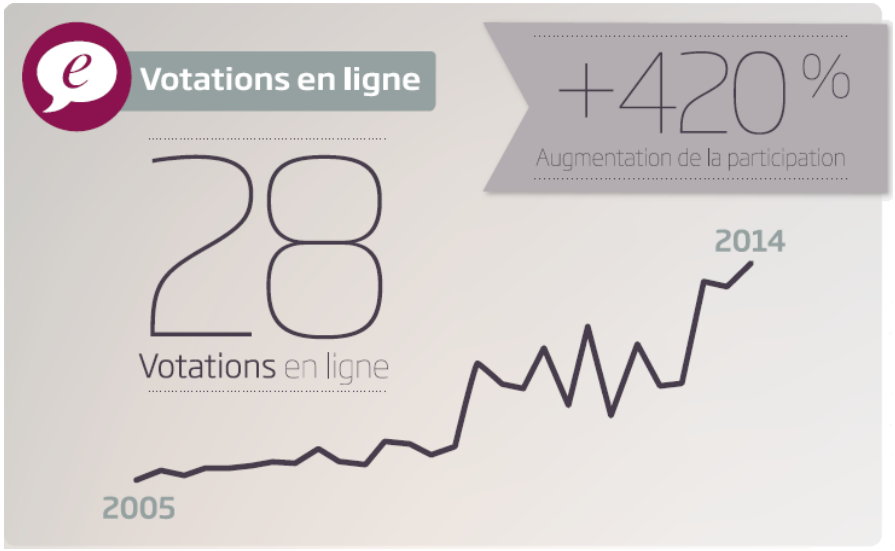
Swiss E-Voting Workshop 2014

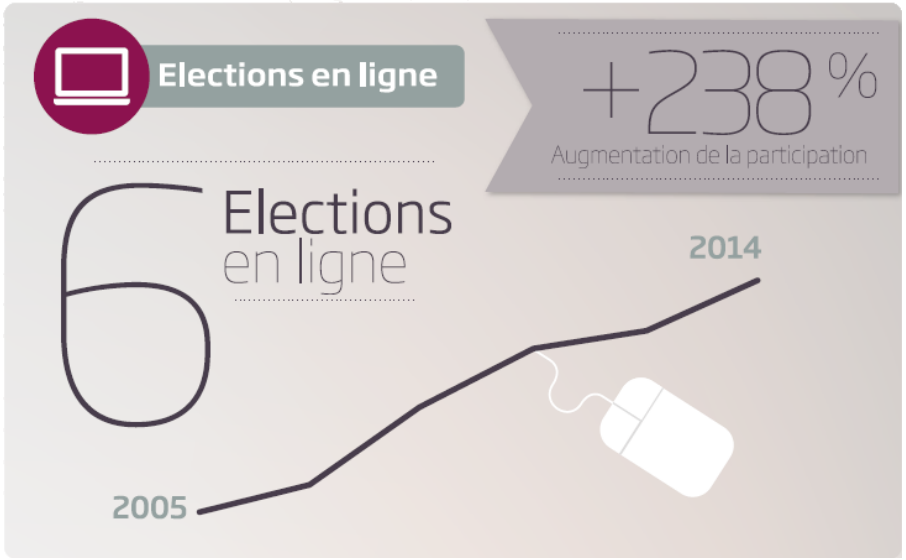
L'évolution de la solution de Neuchâtel vers la conformité complète aux normes définies par la Chancellerie fédérale

Aarau, le 5 septembre 2014

Neuchâtel eVoting – Quelques chiffres

Le vote en ligne neuchâtelois en chiffres





Feuille de route de la sécurité du vote électronique neuchâtelois

2005....2013

Intégration Guichet Unique:

- **Liste des électeurs autorisés**
- **Génération des cartes de vote avec identifiant et mot de passe**
- **Authentification et autorisation des électeurs pendant le scrutin**
- **Sécurité de l'interface de vote (applet Java fournie par Scytl)**

Plateforme de Vote Pnyx.core avec client Java

- **Cryptographie de type RSA**
- **Chiffrage de bout en bout avec un applet Java**

o Protège le secret du vote des acteurs externes et internes, inclus les administrateurs des serveurs

- **La clef de déchiffrage de l'élection est partitionnée entre les membres de la commission électorale**

o Seuls les membres de la commission électorale ensemble peuvent reconstituer la clef qui permet de déchiffrer l'urne lors de la cérémonie de clôture

- **Le processus de déchiffrage casse la corrélation entre les votes déchiffré et l'identité des électeurs**

Vérifiabilité individuelle

- **Reçu de vote qui garantit que le bulletin de l'électeur a bien été placé dans l'urne digitale et qu'il a bien été pris en compte dans le déchiffrage**

2014

A toutes les caractéristiques précédentes s'ajoutent:

Intégration Guichet Unique:

- **Sécurité de l'interface de vote (librairies Javascrip fournies par Scytl)**

Plateforme de Vote Pnyx.core avec client Javascript

- **Chiffrage de bout en bout Javascript**

o Compatibilité étendue à la majorité des navigateurs sans besoin d'installation de logiciels supplémentaires

o Possibilité de voter depuis un téléphone mobile ou une tablette

o Réduction drastique des appels au centre d'assistance

2015...

A toutes les caractéristiques précédentes s'ajoutent :

Plateforme de Vote de Nouvelle Génération avec client Javascript

- **Adhérence aux spécifications de la Chancellerie fédérale**

- **Cryptographie vérifiable de type Elgamal**
- **Vérifiabilité individuelle**

o S'ajoute un mécanisme de codes de retour qui garantit l'intégrité des choix de l'électeur

o S'ajoute une garantie de présence dans l'urne pendant le scrutin

o Vérifiabilité garantie par des preuves mathématiques

- **Vérifiabilité universelle**

o Le processus de déchiffrage garantit que le résultat publié est identique au contenu de l'urne chiffrée

o Vérifiabilité garantie par des preuves mathématiques

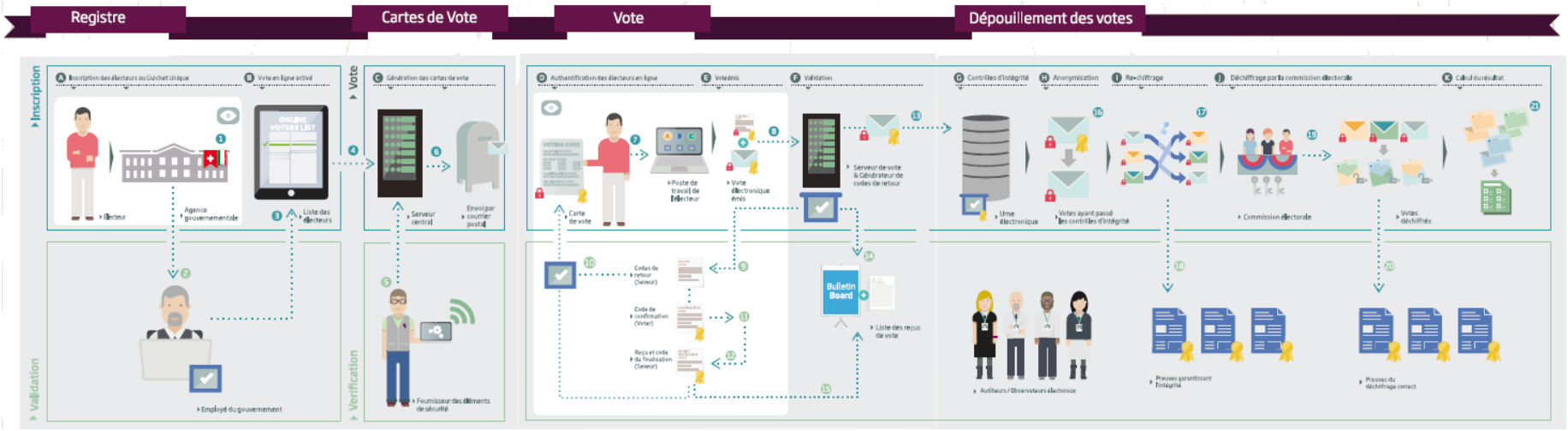
- **Preuves de connaissance nulle**

o Possibilité de vérifier mathématiquement l'intégrité de bulletins individuels et de l'urne chiffrée, sans avoir connaissance de leur contenu (propriétés mathématiques d'El Gamal)

- **Publication du code source**

Neuchâtel eVoting – 2ème génération

Plateforme neuchâteloise de vote en ligne de 2ème génération



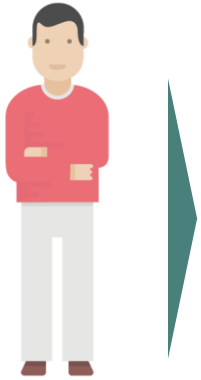
ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

Neuchâtel eVoting – Guichet unique

A Inscription des électeurs au Guichet unique

B Vote en ligne activé

Inscription



Électeur

Agence gouvernementale

4a

3 Liste des électeurs

Validation

2

Employé du gouvernement

1 Inscription au Guichet unique (en personne)

2 Validation du gouvernement

3 Génération de la liste des électeurs pour le vote en ligne

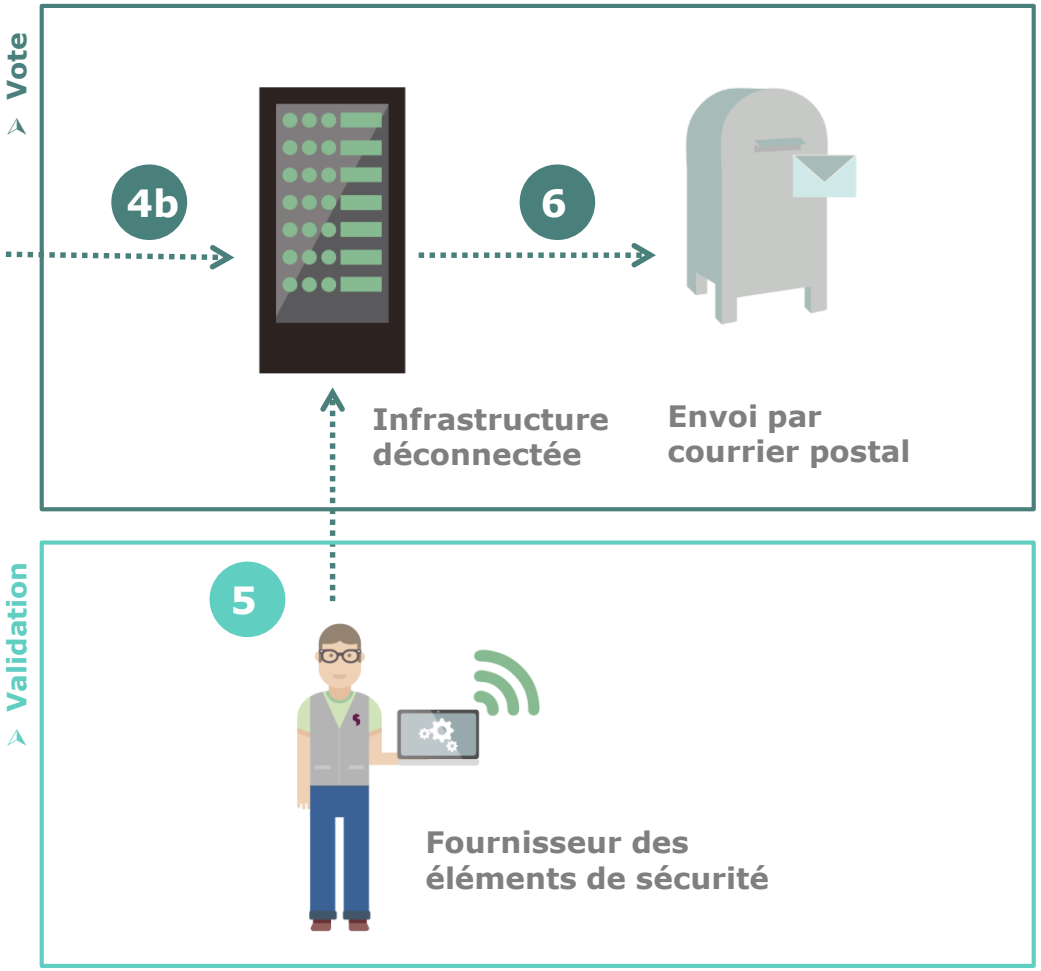
4a Transmission de la liste au serveur central

DÉPARTEMENT DES FINANCES ET DE LA SANTÉ

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

Neuchâtel eVoting – Cartes de vote

C Génération des cartes de vote



4b Transmission de la liste à l'infrastructure déconnectée

5 Génération des codes de sécurité et livraison dans l'infrastructure déconnectée

6 Impression et envoi des cartes de vote aux électeurs

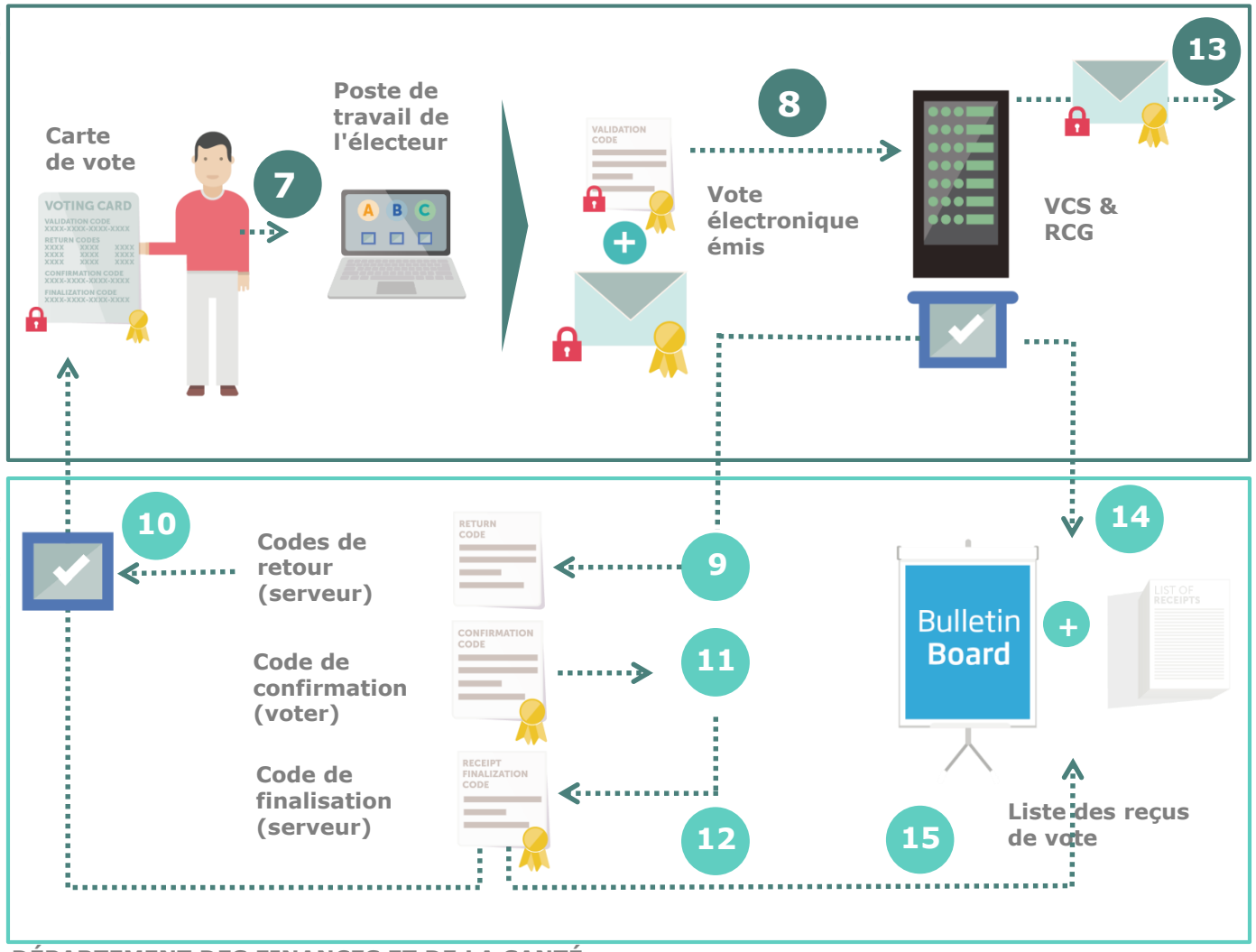
ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

Neuchâtel eVoting - Vote

D Authentification des électeurs en ligne

E Vote émis

F Validation



7 Vote émis par le dispositif de vote de l'électeur

8 Code de validation (assigné à l'électeur)

9 Codes de retour

10 L'électeur vérifie les codes de retour

11 Code de confirmation

12 Reçu et code finalisation

13 Vote chiffré et signé enregistré dans l'urne numérique

14 Chaque reçu est publié

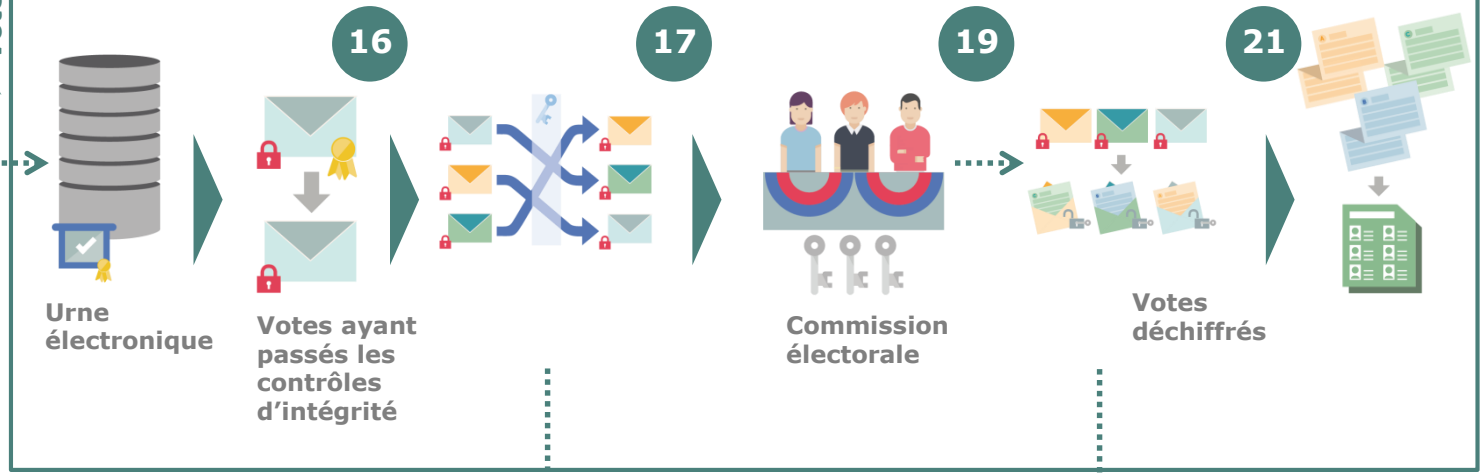
15 L'électeur vérifie que son reçu est bien présent

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

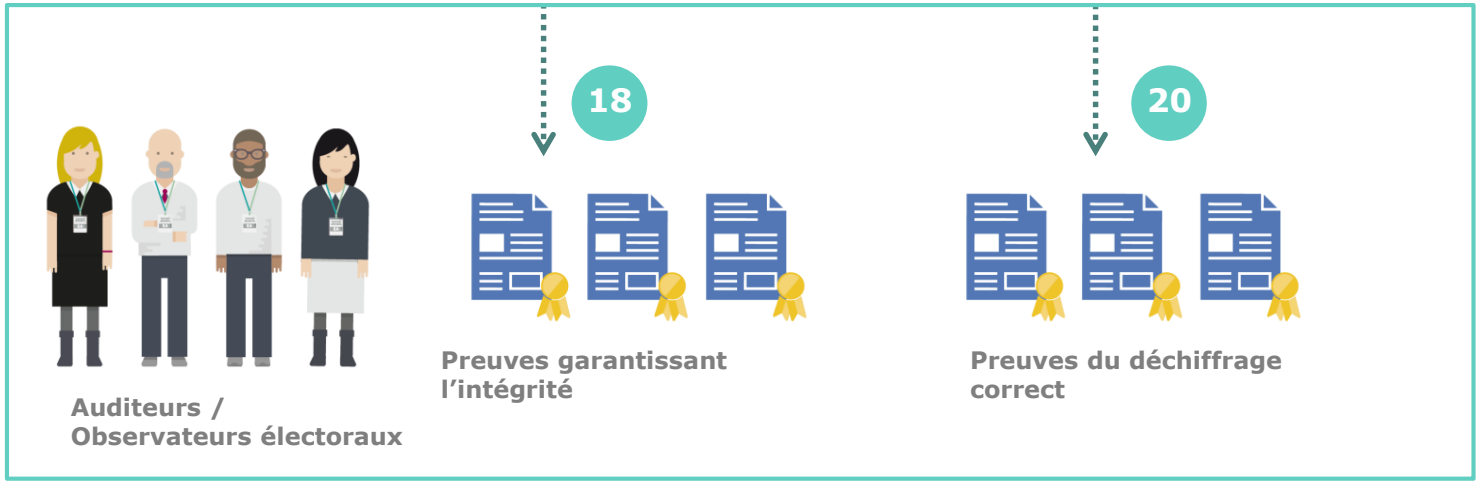
Neuchâtel eVoting - Dépouillement

G Contrôles d'intégrité
H Anony-misation
I Re-chiffrage
J Déchiffrage par la commission électorale
K Calcul des résultats

Voter



Validation



16 Processus de séparation de la signature digitale

17 Anonymisation par re-chiffrage et mixing

18 Preuves mathématiques garantissant l'intégrité de l'urne électronique

19 Déchiffrage des votes

20 Preuves mathématiques garantissant l'intégrité du résultat de l'élection

21 Processus de comptage des votes

Travaux en cours

- Gros travail d'évolution de la solution actuelle
- Capitalisation de 10 ans de travaux et d'expériences
- 7 cas d'utilisation adaptés ou créés
- Nouvelle infrastructure technique (PC et serveurs)
- Nouvelle organisation pour la configuration d'un scrutin
- Communication aux électrices et électeurs
- Audits ➔ 2015 / 2016
- **Objectif ➔ votation fédérale du 8 mars 2015**

Neuchâtel eVoting – Carte de vote

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

Madame
Catherine Aeschlimann
Route de la Jonchère 14
2300 La Chaux-de-Fonds

VOLET DE TRANSMISSION

(ne doit pas être renvoyé)

A PRIORITY PRIORITAIRE

P.P.
2300 La Chaux-de-Fonds
Poste CH SA

Les envois non distribués sont à envoyer à :
Commune de La Chaux-de-Fonds

◄◄◄ A détacher ici ◄◄◄

CARTE DE VOTE

Madame
Catherine Aeschlimann

No scrutin : 0137
Référence : 126286
No contrôle : 42

Scrutin du 8 mars 2015

Commune de La Chaux-de-Fonds

Droits de vote : **CH - NE**

Vote par correspondance ou au bureau électoral

A remplir obligatoirement pour voter

Date de naissance : ___ / ___ / _____

Signature : _____

Vote électronique

- Voir instructions au verso.

Vote par correspondance

- Après avoir rempli le ou les bulletins de vote, les introduire dans l'enveloppe de vote.
- Mettre cette dernière collée dans l'enveloppe de transmission.
- Inscrire sur la carte de vote votre date de naissance et apposer votre signature.
- **Attention ! Sans ces deux mentions, votre vote ne sera pas pris ne sera pas pris en compte.**
- Insérer la carte de vote dans l'enveloppe de transmission de manière que l'adresse de votre administration communale apparaisse dans la fenêtre.
- En cas d'envoi par la poste, affranchir l'enveloppe.
- Poster suffisamment tôt votre vote, soit :
  - Avant le mardi à 18 heures en courrier B
  - Avant le vendredi à 18 heures en courrier A.
- **Il est aussi possible de déposer votre vote sans l'affranchir auprès de votre administration communale ou dans sa boîte aux lettres.** Votre enveloppe de transmission doit parvenir à l'administration communale au plus tard le dimanche du scrutin à 10 heures.

Vote au bureau électoral

- Prendre le carte de vote et le matériel officiel avec vous.
- Vous ne pourrez voter que contre remise de votre carte de vote complétée et signée.
- Dans toutes les communes, les bureaux électoraux sont ouverts le dimanche matin du scrutin, de 10 à 12 heures.

Attention ! Se présenter personnellement au bureau électoral car le vote par procuration est interdit.

Vote électronique

Adresse : https://www.GuichetUnique.ch

Empreinte numérique : 89 67 ag h7 12 75 ku hg mn zu tr 6t 76 uz re ws 47 nb vf gh lp

Clôture du vote électronique (heure suisse) à 12h00 le samedi 7 mars 2015.

A saisir à la fin de la sélection des choix.	A saisir après la vérification des codes de retour.	A contrôler après la génération de l'accusé de réception.
Code de validation :	**Code de confirmation :**	**Code de finalisation :**
99jh – 6gww – b8fi – 9at7	6785 – 7901	3459 – 0654

Votation du 8 mars 2015 – Codes de retour

N°	Objets fédéraux	Oui	Non	Blanc	Initiative	Contre-projet
1	Initiative populaire "Pour la protection de salaires équitables (Initiative sur les salaires minimums)"	6789	6789	6789		
2	Initiative populaire "Pour la protection de salaires équitables (Initiative sur les salaires minimums)"	6789	6789	6789		
3a	Initiative populaire "Pour la protection de salaires équitables (Initiative sur les salaires minimums)"	6789	6789	6789		
3b	Initiative populaire "Pour la protection de salaires équitables (Initiative sur les salaires minimums)"	6789	6789	6789		
3c	Initiative populaire "Pour la protection de salaires équitables (Initiative sur les salaires minimums)"			6789	6789	6789
N°	**Objets cantonaux**	**Oui**	**Non**	**Blanc**		
1	Initiative populaire "Pour la protection de salaires équitables (Initiative sur les salaires minimums)"	6789	6789	6789		
2	Initiative populaire "Pour la protection de salaires équitables (Initiative sur les salaires minimums)"	6789	6789	6789		
3	Initiative populaire "Pour la protection de salaires équitables (Initiative sur les salaires minimums)"	6789	6789	6789		
N°	**Objets communaux – Commune de La Chaux-de-Fonds**	**Oui**	**Non**	**Blanc**		
1	Initiative populaire "Pour la protection de salaires équitables (Initiative sur les salaires minimums)"	6789	6789	6789		
2	Initiative populaire "Pour la protection de salaires équitables (Initiative sur les salaires minimums)"	6789	6789	6789		

Administration communale
Contrôle des habitants
Tour Espacité
Case postale
2301 La Chaux-de-Fonds

Conclusion

- Intégration avec l'infrastructure existante de Neuchâtel
- Système protégé des attaques externes et internes
- Preuves d'intégrité des bulletins reçus, de leurs existences dans l'urne et de leurs intégrations dans les résultats publiés, accessibles par les citoyens
- Preuves mathématiques d'intégrité des bulletins individuels et de toute l'élection, jusqu'aux résultats publiés, vérifiable par des experts tiers

Questions

Questions / Réponses

Stand à disposition

Merci pour votre attention

Danilo Rota
danilo.rota@ne.ch

DÉPARTEMENT DES FINANCES ET DE LA SANTÉ