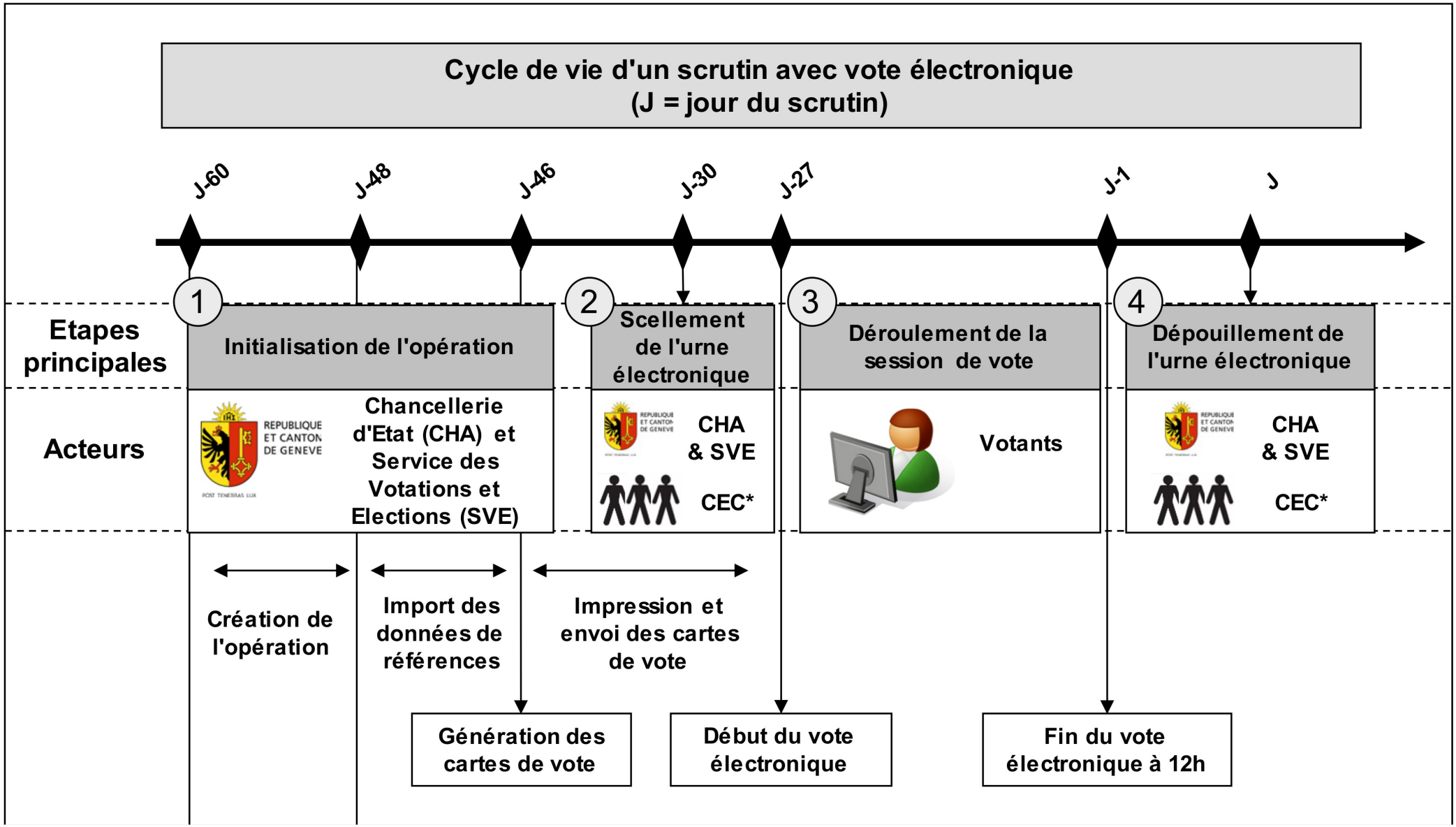
Berner Fachhochschule
Technik und Informatik

Système de vote électronique Genevois

Philémon von Bergen
12.10.2012

Cette présentation s'inspire uniquement de documents publics disponibles sur http://www.geneve.ch/evoting/

Cycle


Cycle de vie d'un scrutin avec vote électronique
(J = jour du scrutin)
J-60
J-48
J-46
J-30
J-27
J-1
J
1
2
3
4
Etapes principales
Acteurs
Initialisation de l'opération
Scellement de l'urne électronique
Déroulement de la session de vote
Dépouillement de l'urne électronique
REPUBLIQUE ET CANTON DE GENEVE
Chancellerie d'Etat (CHA) et Service des Votations et Elections (SVE)
CHA & SVE
CEC*
Votants
CHA & SVE
CEC*
Création de l'opération
Import des données de références
Impression et envoi des cartes de vote
Génération des cartes de vote
Début du vote électronique
Fin du vote électronique à 12h

Initialisation d'une opération

- Données reçues
  - Les données relatives aux objets du scrutin
  - Les données nécessaires à la production du matériel de vote : registre électoral avec nom, prénom, adresse
  - Les données nécessaires à l’authentification des électeurs sur le système de vote par internet : date de naissance et commune d’origine.

Initialisation d'une opération

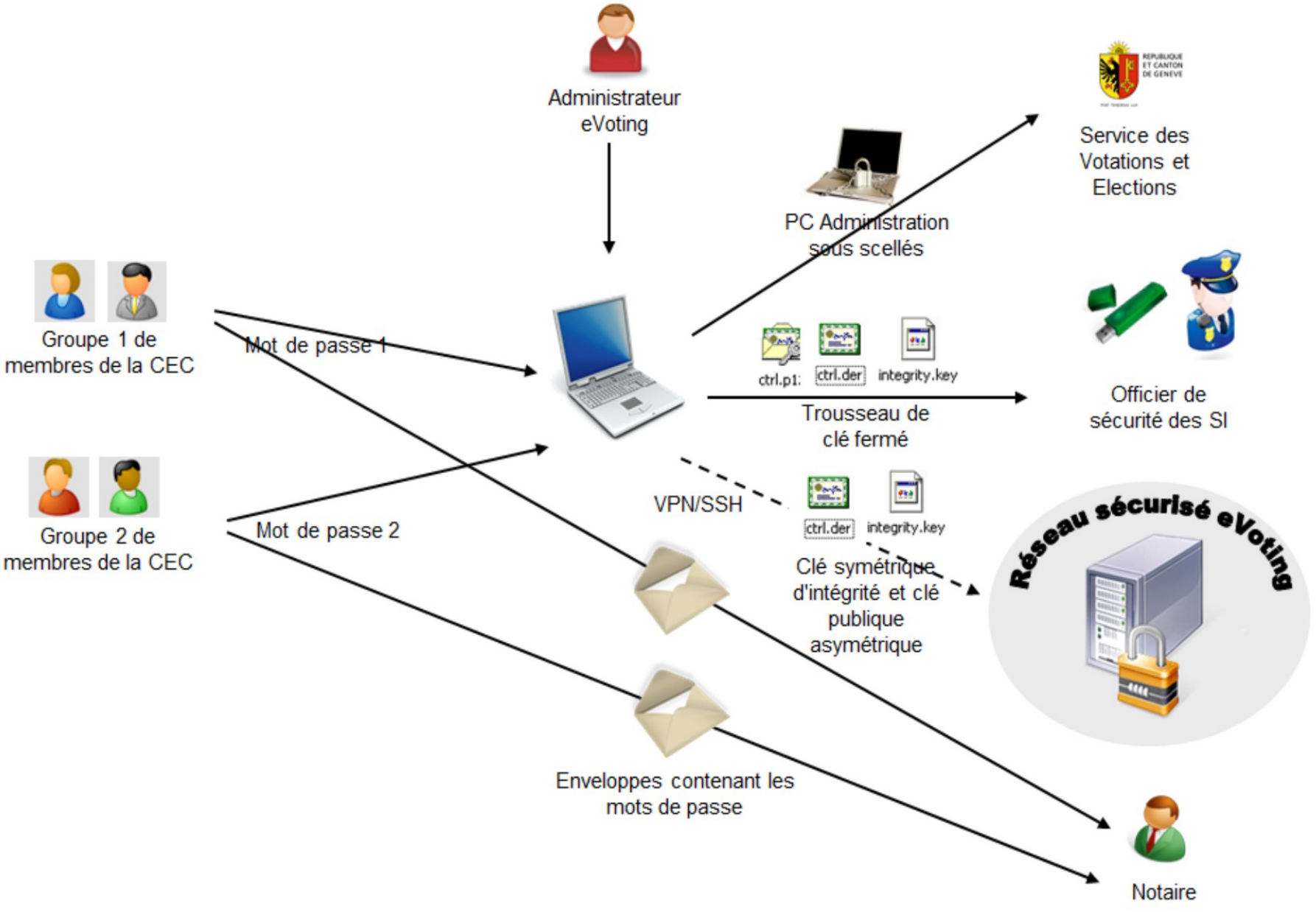
- Données générées
  - Numéro de carte de vote (NCV)
  - Mot de passe (PIN)
  - Code de contrôle du serveur

Ces données sont uniques et imprimées sur les cartes de vote.

Scellement de l'urne

- Les votes dans l'urne sont chiffrés avec une clé publique
- La clé privée est mise en lieu sûr
- Compteur d'intégrité (chiffrage symétrique)

Scellement de l'urne



Scellement de l'urne

Clés	Propriétaire	Utilisation
Clé publique de chiffrement des votes	Administrateur système	Cette clé permet de chiffrer les votes dans l'urne mais ne permet pas de les déchiffrer.
Clé privée de déchiffrement des votes	Officier sécurité police	Cette clé permet de déchiffrer les votes dans l'urne et d'obtenir le résultat du scrutin.
Clé symétrique du compteur d'intégrité	Administrateur système	Cette clé permet de chiffrer et de déchiffrer le compteur d'intégrité dans la base de données et d'assurer l'inaltérabilité de l'urne.

Tableau 1: Clés du système produites pendant l'étape de scellement de l'urne

Secret	Créateur	Support de sauvegarde
Mot de passe 1	Premier groupe de membres de la CEC	Formulaire de saisie 1
Mot de passe 2	Second groupe de membres de la CEC	Formulaire de saisie 2
Trousseau de clés protégé par mot de passe	PC Administration	CD et clé USB
Clé publique de chiffrement des votes	PC Administration	CD et clé USB
		Disques durs du système de vote par internet
Clé symétrique du compteur d'intégrité	PC Administration	CD et clé USB
		Disques durs du système de vote par internet

Tableau 2: Liste des secrets

Scellement de l'urne

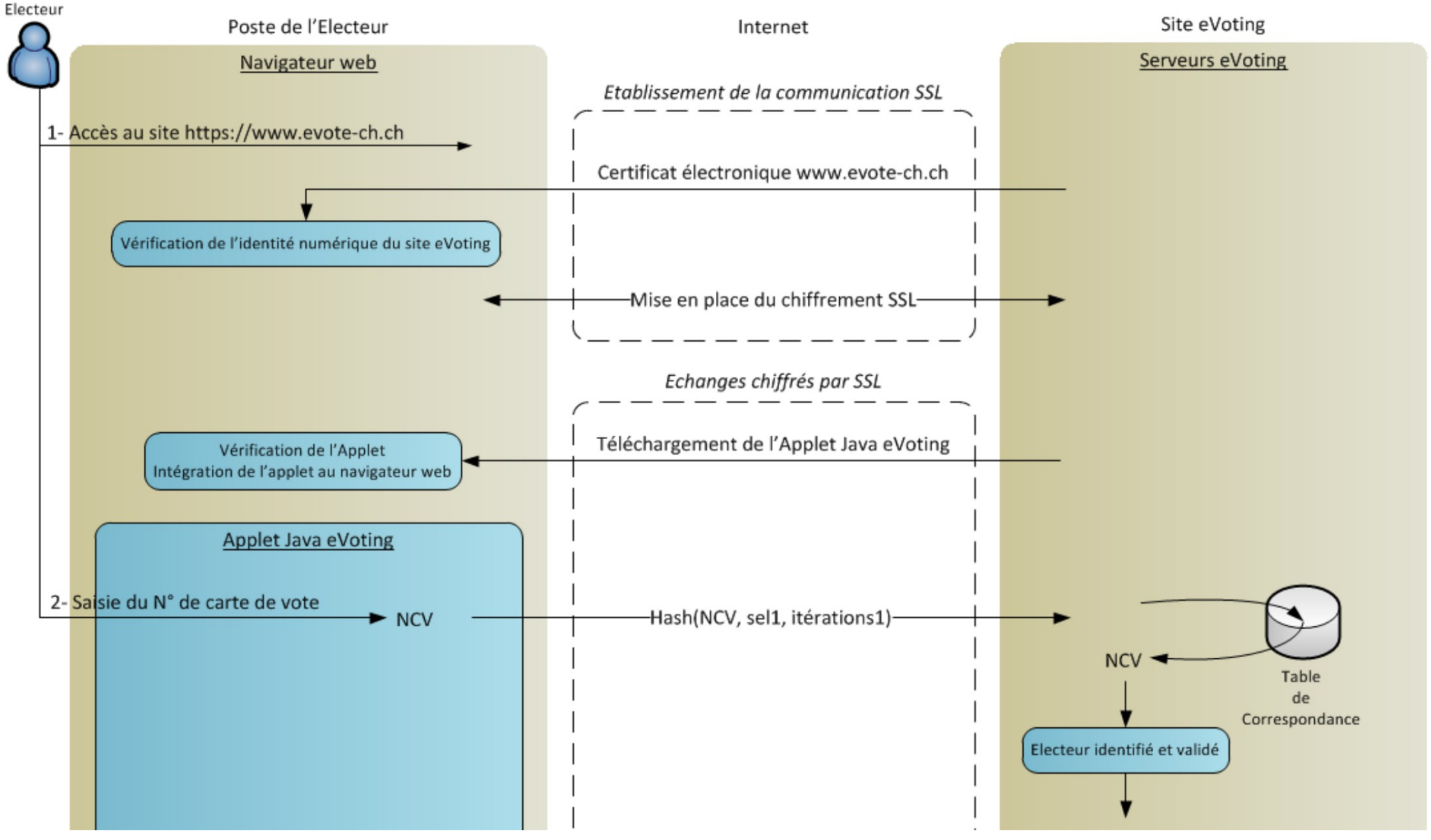
Support de sauvegarde	Mesures de protection de l'intégrité	Propriétaire pendant la durée du scrutin
PC Administration	Sac plombé	Représentant du SVE
Formulaire de saisie 1	Enveloppes scellées 1 et 2	Notaire
Formulaire de saisie 2	Enveloppes scellées 3 et 4	
CD et Clé USB	Enveloppe scellée 5	Officier de sécurité

Tableau 3: Liste des supports de sauvegarde

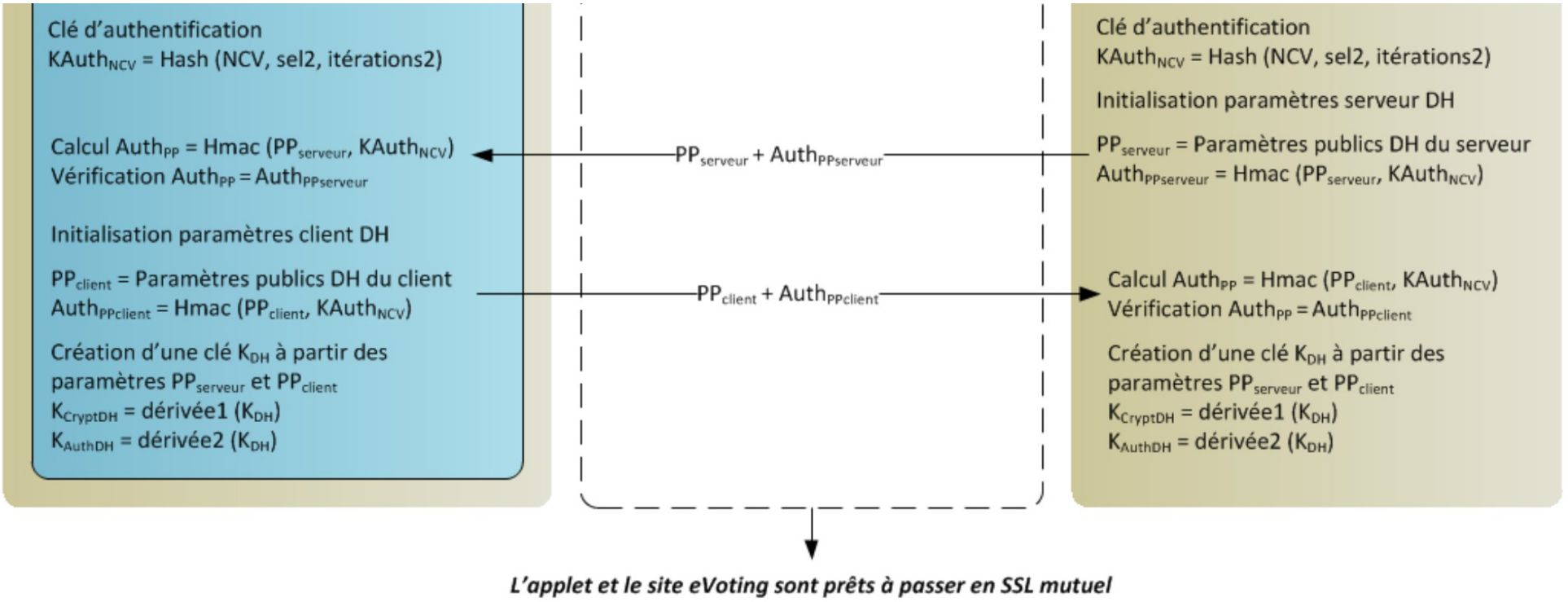
Session de vote

- Pour le votant :
  - Introduction du NCV (numéro de carte de vote)
  - Votation
  - Introduction des secrets (date de naissance, commune d'origine, PIN)
  - Contrôle du code de vérification

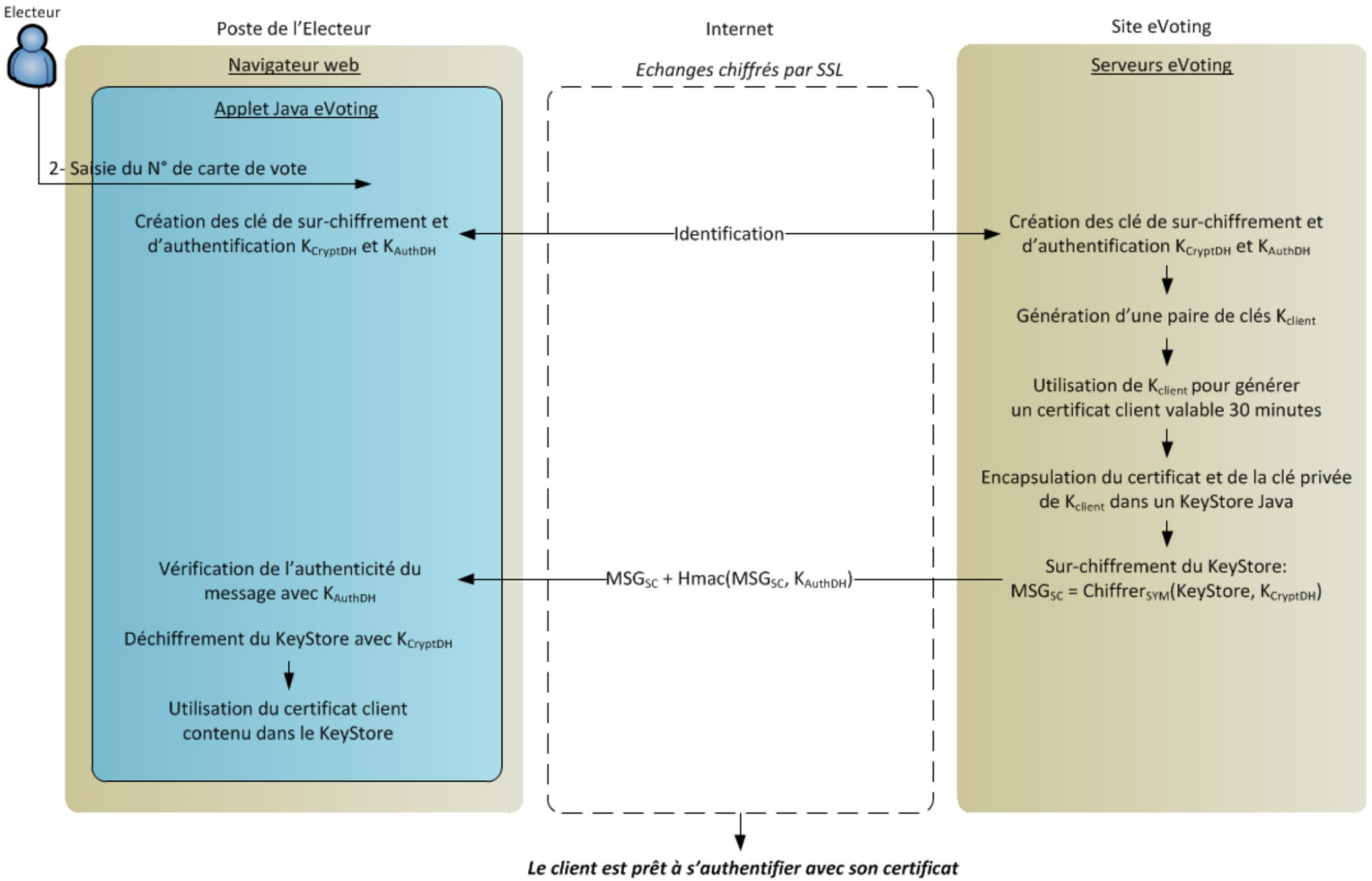
Identification du votant

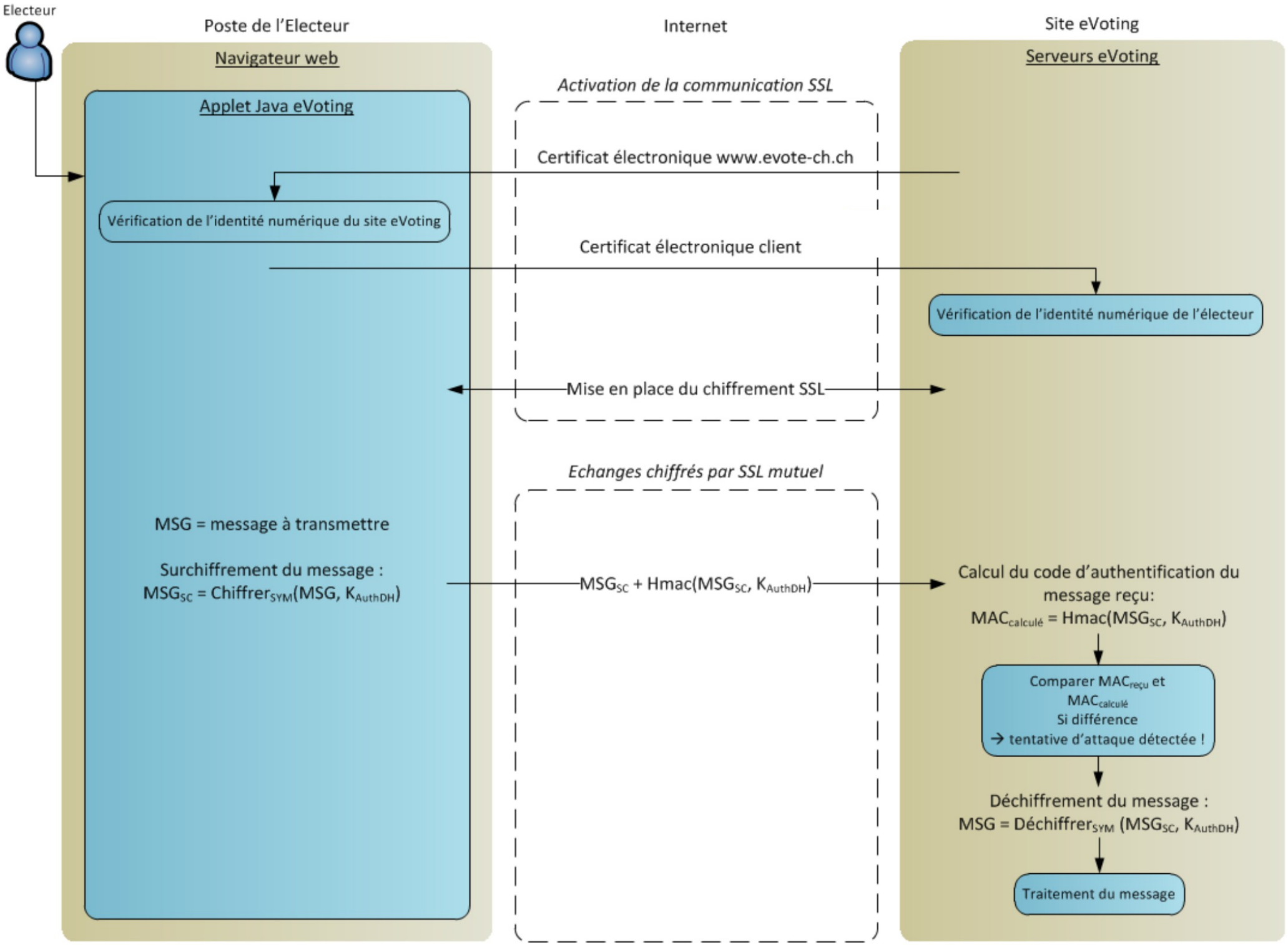


Identification du votant

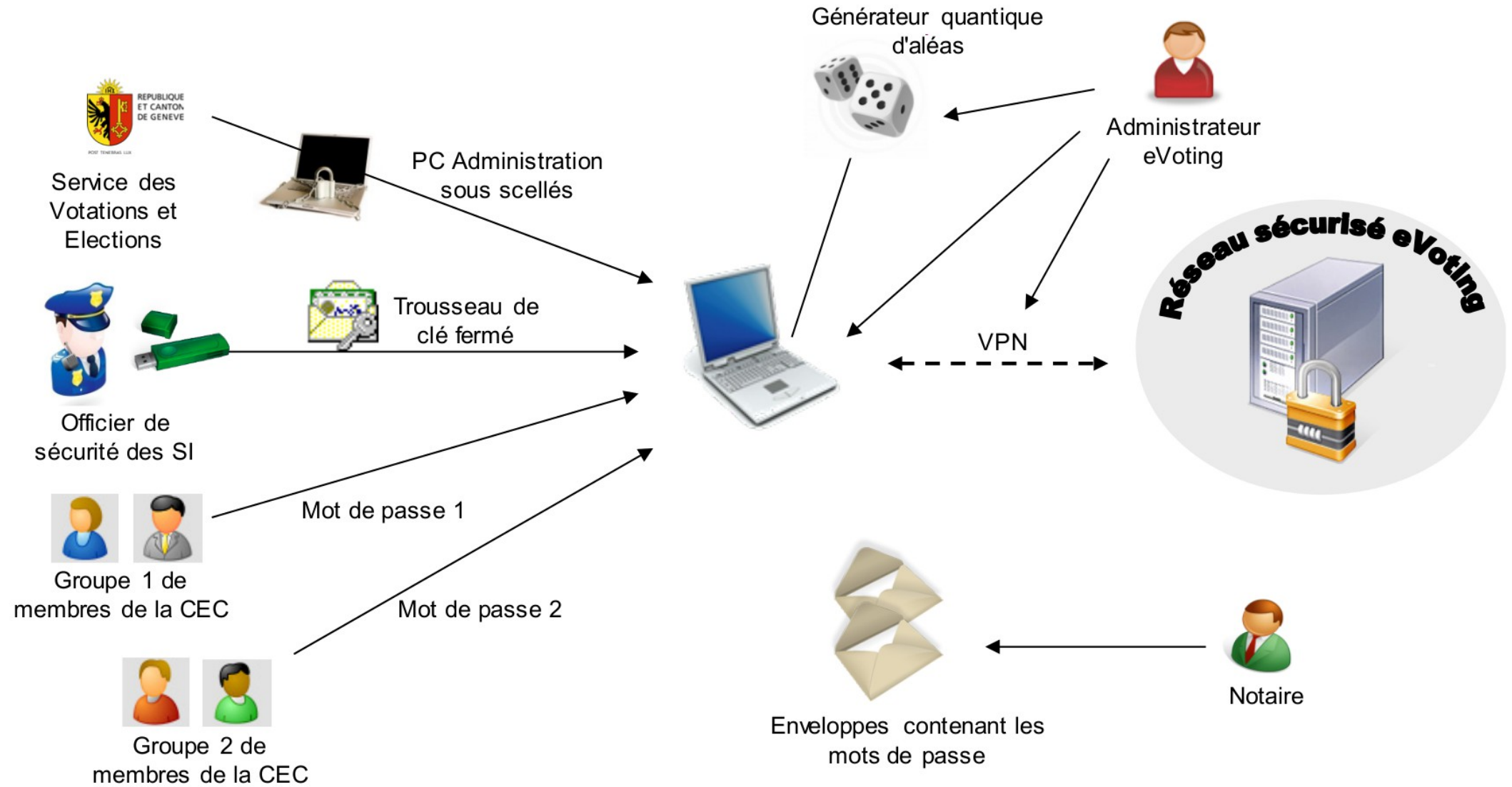


Canal sécurisé




Electeur
Poste de l'Electeur
Internet
Site eVoting
Navigateur web
Serveurs eVoting
Applet Java eVoting
Activation de la communication SSL
Certificat électronique www.evote-ch.ch
Vérification de l'identité numérique du site eVoting
Certificat électronique client
Vérification de l'identité numérique de l'électeur
Mise en place du chiffrement SSL
Echanges chiffrés par SSL mutuel
MSG = message à transmettre
Surchiffrement du message :
MSGSC = ChiffrerSYM(MSG, KAuthDH)
MSGSC + Hmac(MSGSC, KAuthDH)
Calcul du code d'authentification du message reçu:
MACcalculé = Hmac(MSGSC, KAuthDH)
Comparer MACreçu et MACcalculé
Si différence
→ tentative d'attaque détectée !
Déchiffrement du message :
MSG = DéchiffrerSYM (MSGSC, KAuthDH)
Traitement du message

Dépouillement de l'urne



Dépouillement de l'urne

- Brassage de l'urne

- Déchiffrage et comptage

Vulnérabilités

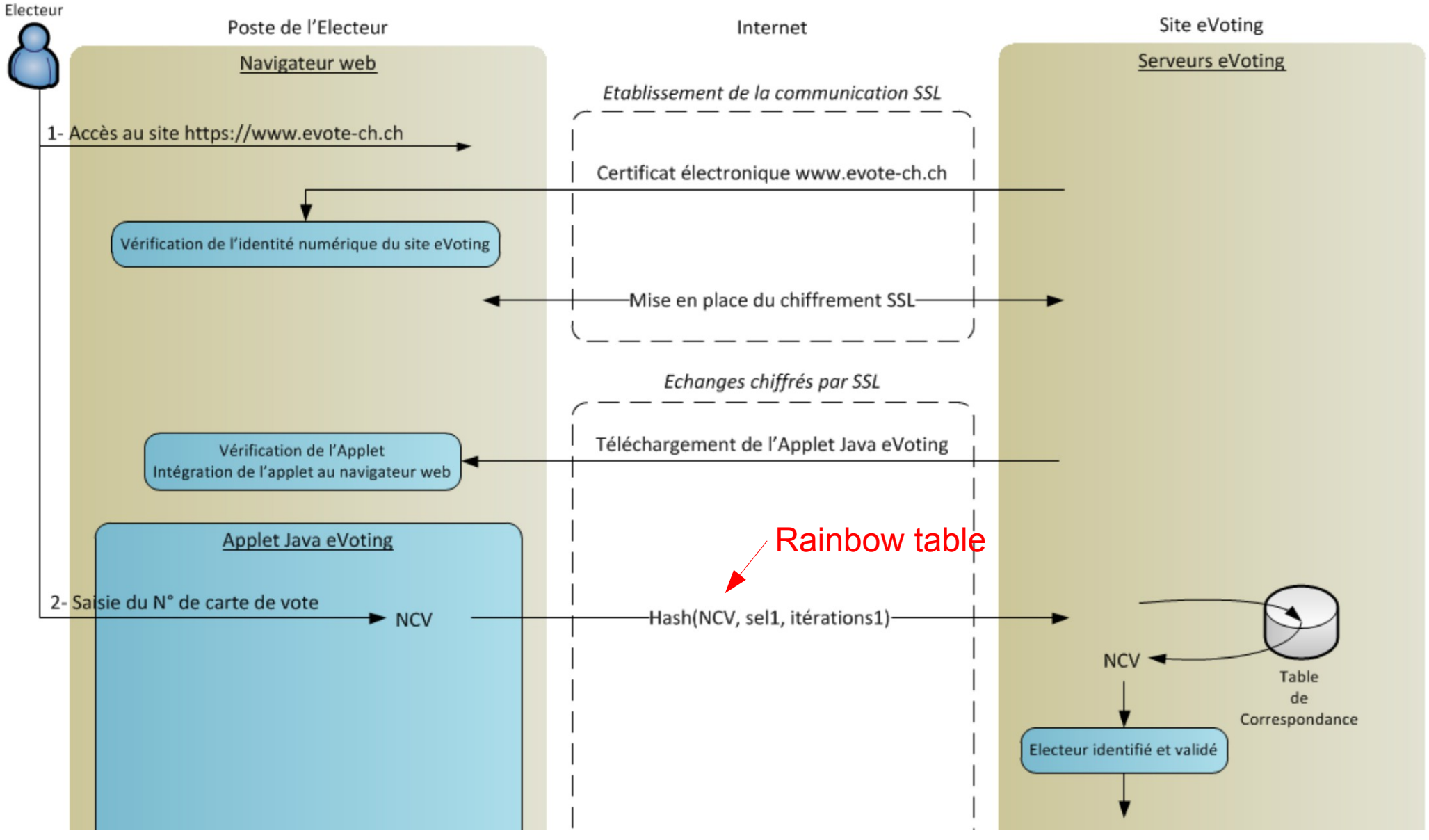
- Correspondance Nom – NCV
  - La relation entre la personne et le NCV doit être possible (vol de la carte, perte,...)

    Il est donc théoriquement possible, lors de l'entrée du vote, de retrouver le votant
- La date de naissance et la commune d'origine ne sont pas des secrets
  - Ils sont censés renforcer la sécurité du PIN

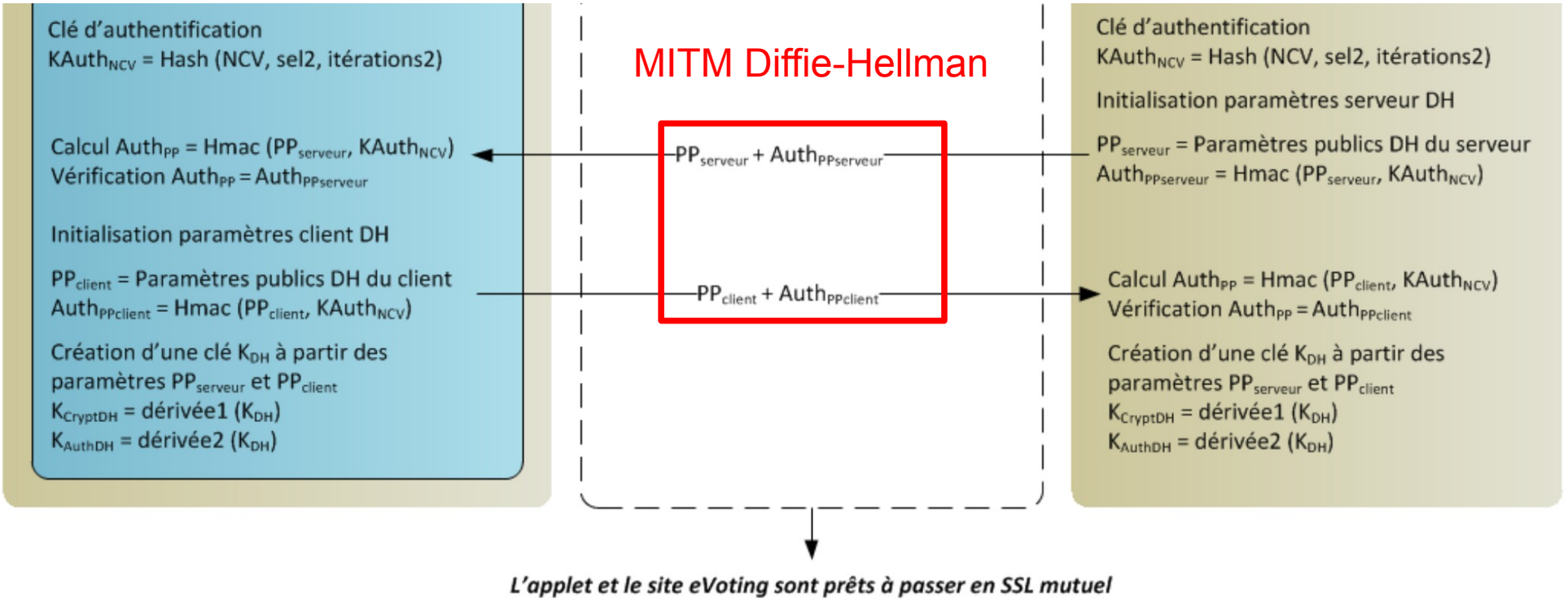
Vulnérabilités

- Entropie du NCV est de 50 bits
  - Rainbow table possible en connaissant le sel et les itération (si ceux-ci sont codés en dur dans l'applet)
  - Si on arrive à faire un Man in the Middle sur le SSL, toute la communication est contrôlée

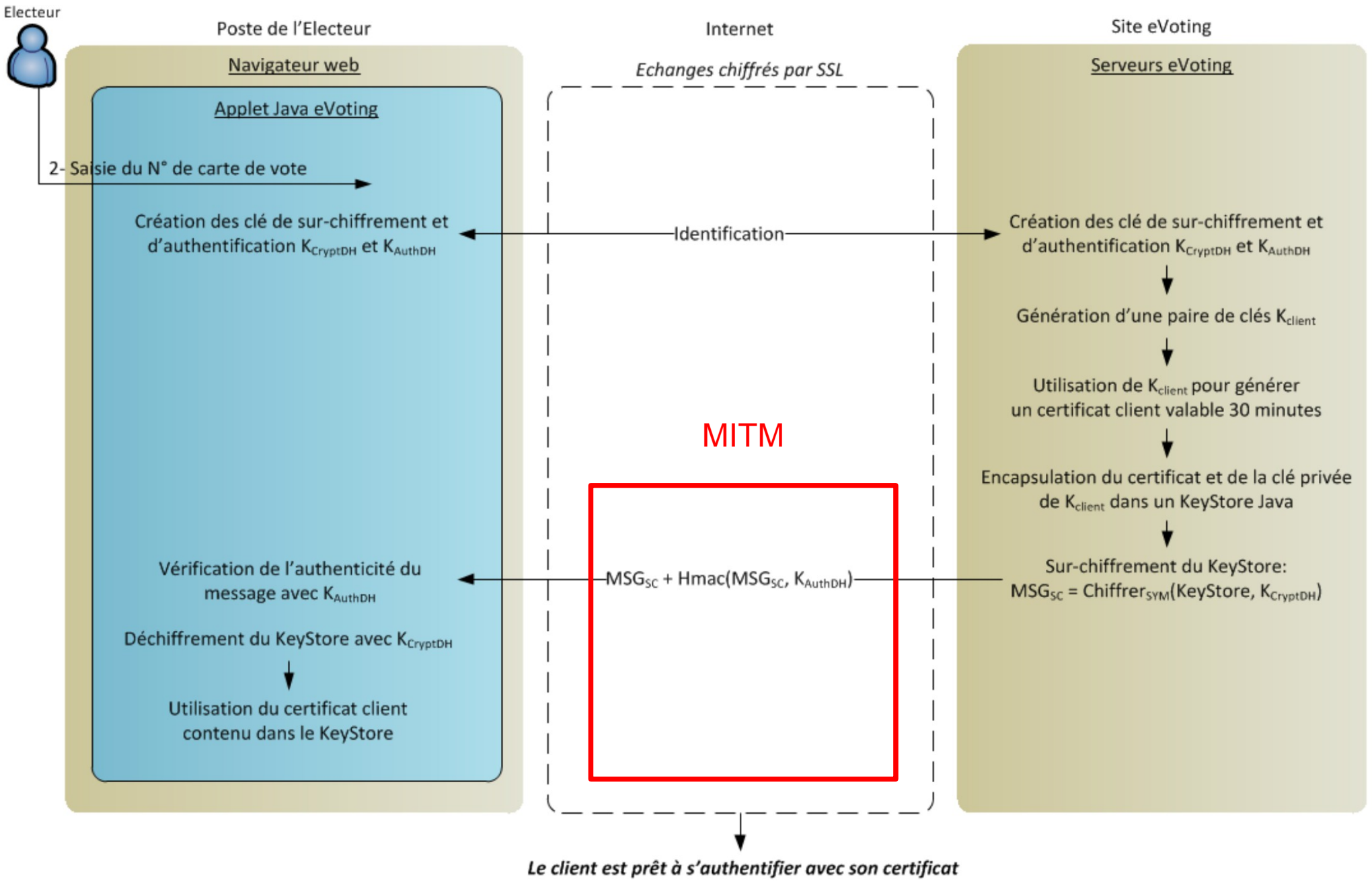
Identification du votant

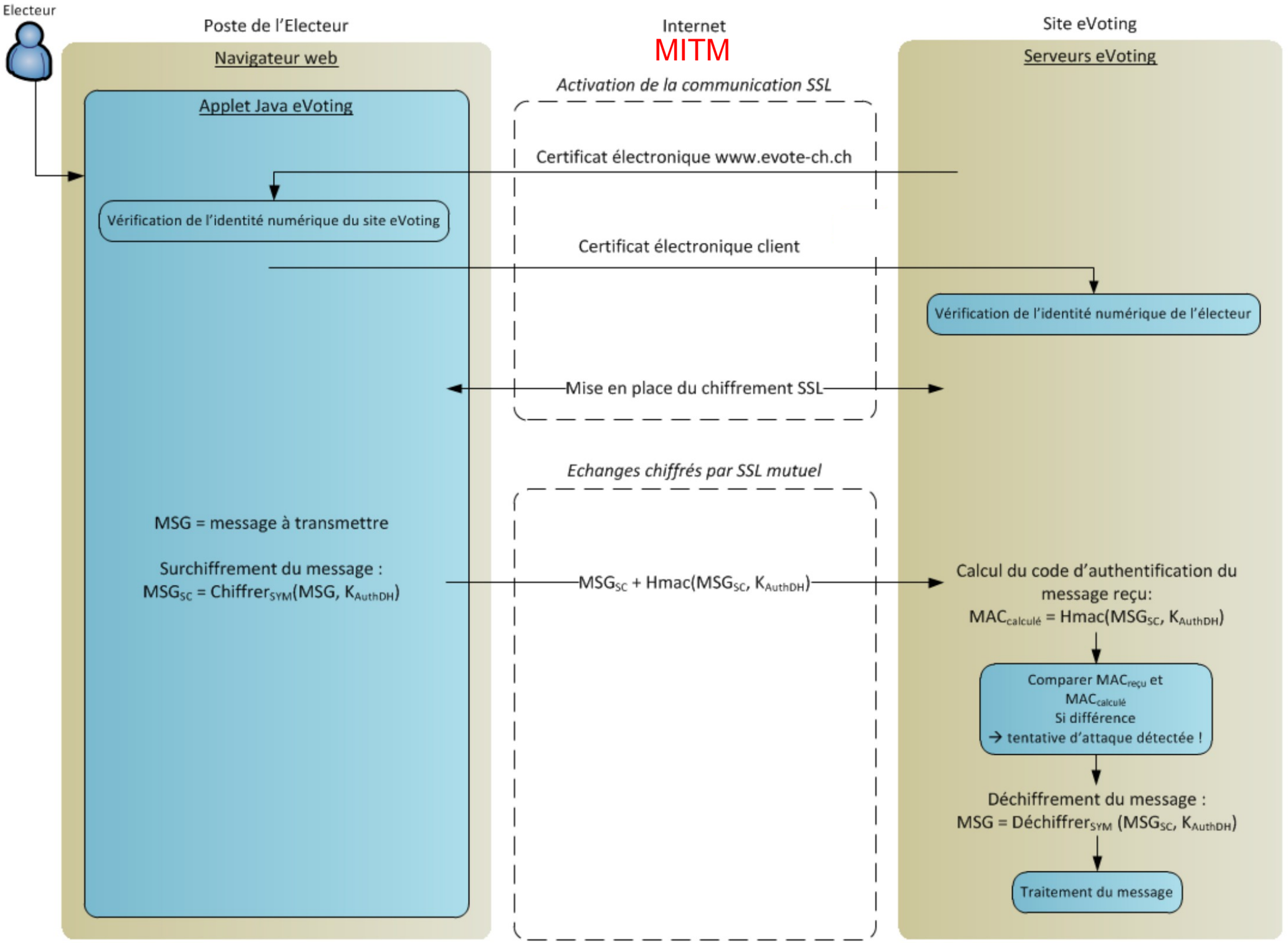


Identification du votant



Canal sécurisé

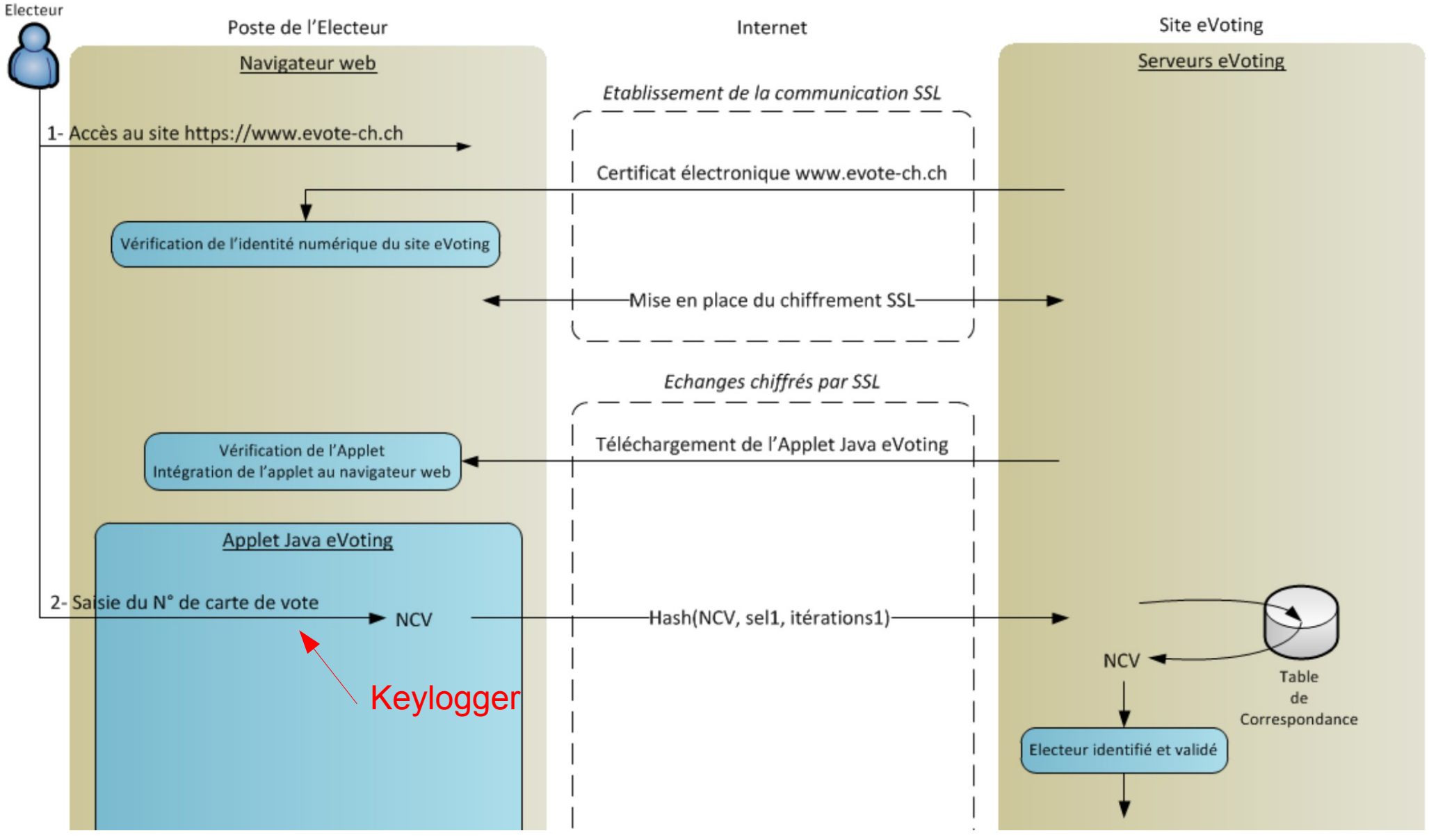



Electeur
Poste de l'Electeur
Navigateur web
Applet Java eVoting
Vérification de l'identité numérique du site eVoting
MSG = message à transmettre
Surchiffrement du message :
MSGSC = ChiffrerSYM(MSG, KAuthDH)
Internet
MITM
Activation de la communication SSL
Certificat électronique www.evote-ch.ch
Certificat électronique client
Mise en place du chiffrement SSL
Echanges chiffrés par SSL mutuel
MSGSC + Hmac(MSGSC, KAuthDH)
Site eVoting
Serveurs eVoting
Vérification de l'identité numérique de l'électeur
Calcul du code d'authentification du message reçu:
MACcalculé = Hmac(MSGSC, KAuthDH)
Comparer MACreçu et MACcalculé
Si différence
→ tentative d'attaque détectée !
Déchiffrement du message :
MSG = DéchiffrerSYM (MSGSC, KAuthDH)
Traitement du message

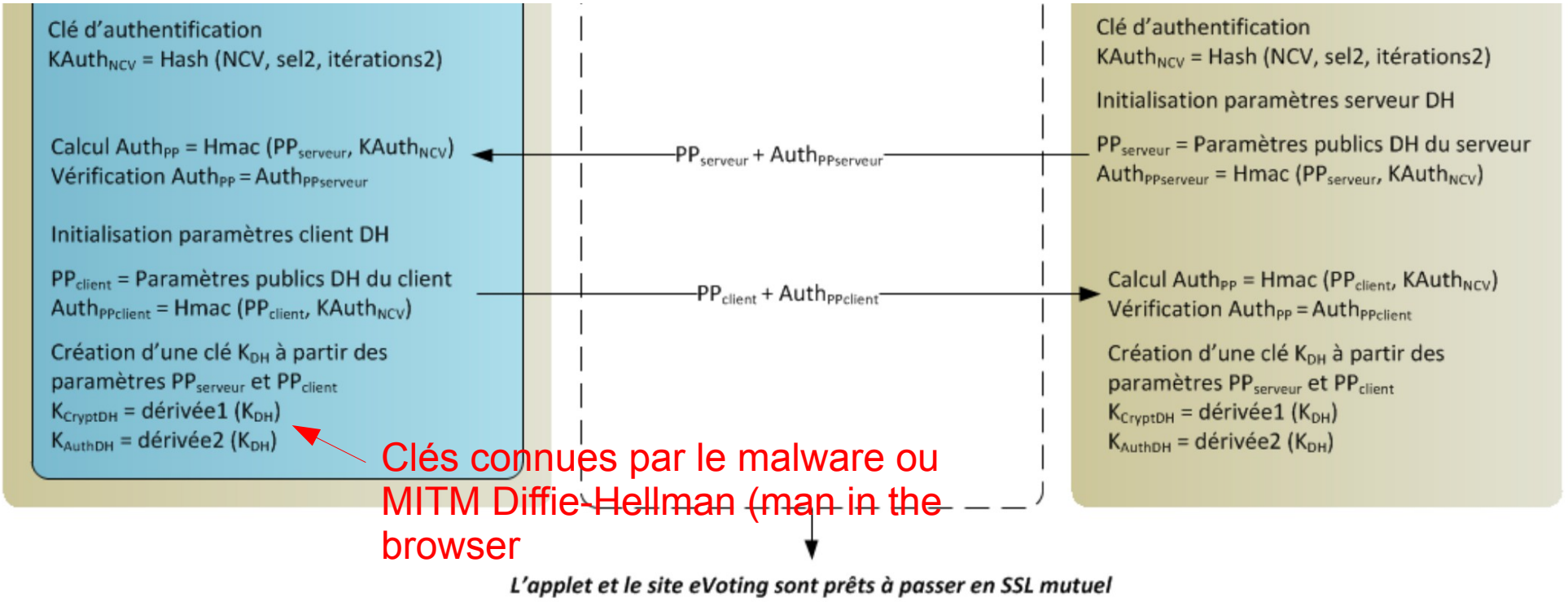
Vulnérabilités

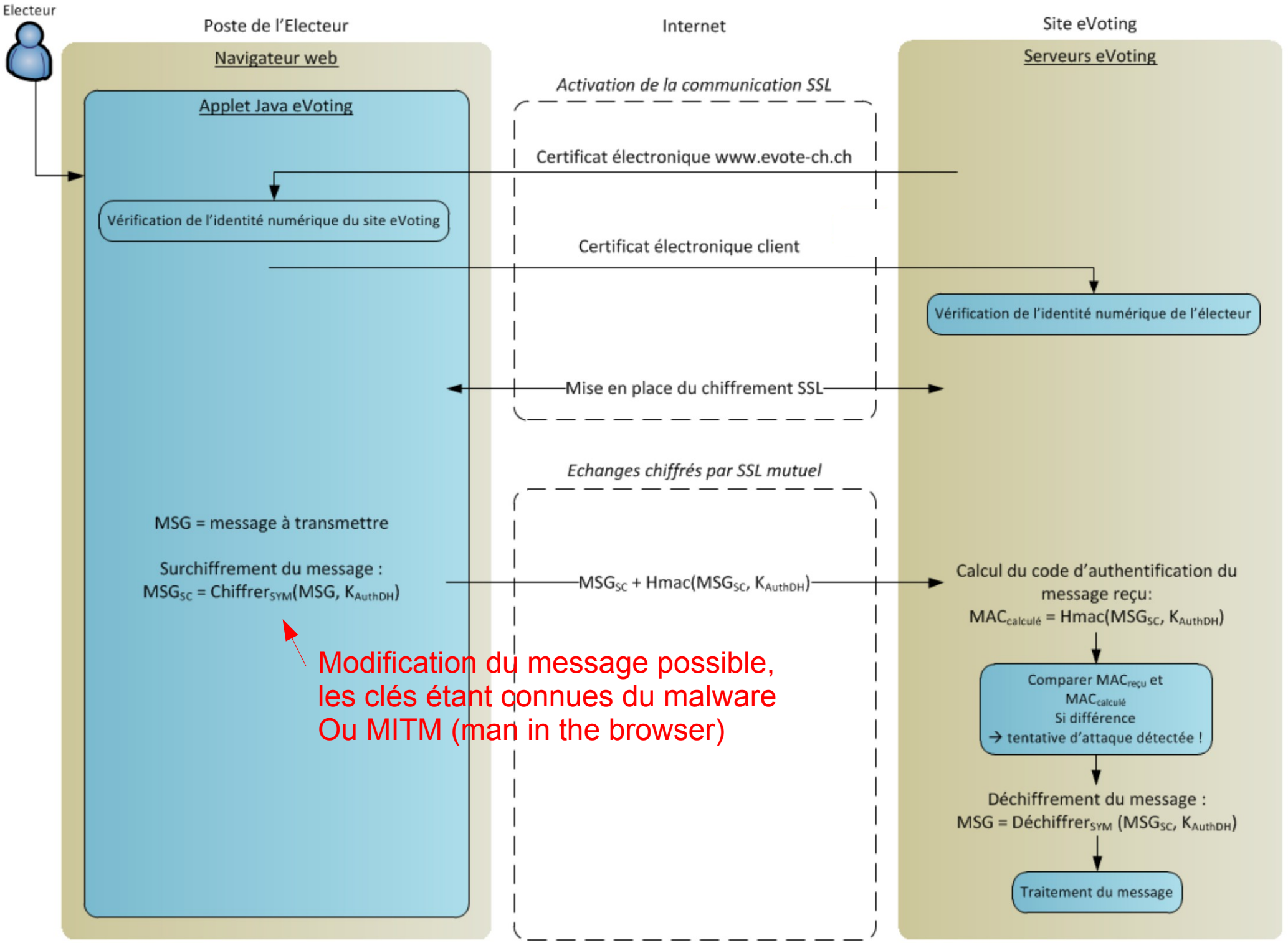
- Sensible au malware
  - Keylogger pour le NCV
  - Plus besoin de casser le SSL (man in the browser)

Identification du votant



Identification du votant




Electeur
Poste de l'Electeur
Internet
Site eVoting
Navigateur web
Serveurs eVoting
Applet Java eVoting
Activation de la communication SSL
Certificat électronique www.evote-ch.ch
Vérification de l'identité numérique du site eVoting
Certificat électronique client
Vérification de l'identité numérique de l'électeur
Mise en place du chiffrement SSL
Echanges chiffrés par SSL mutuel
MSG = message à transmettre
Surchiffrement du message :
MSGSC = ChiffrerSYM(MSG, KAuthDH)
MSGSC + Hmac(MSGSC, KAuthDH)
Calcul du code d'authentification du message reçu:
MACcalculé = Hmac(MSGSC, KAuthDH)
Comparer MACreçu et MACcalculé
Si différence
→ tentative d'attaque détectée !
Déchiffrement du message :
MSG = DéchiffrerSYM (MSGSC, KAuthDH)
Traitement du message
Modification du message possible,
les clés étant connues du malware
Ou MITM (man in the browser)

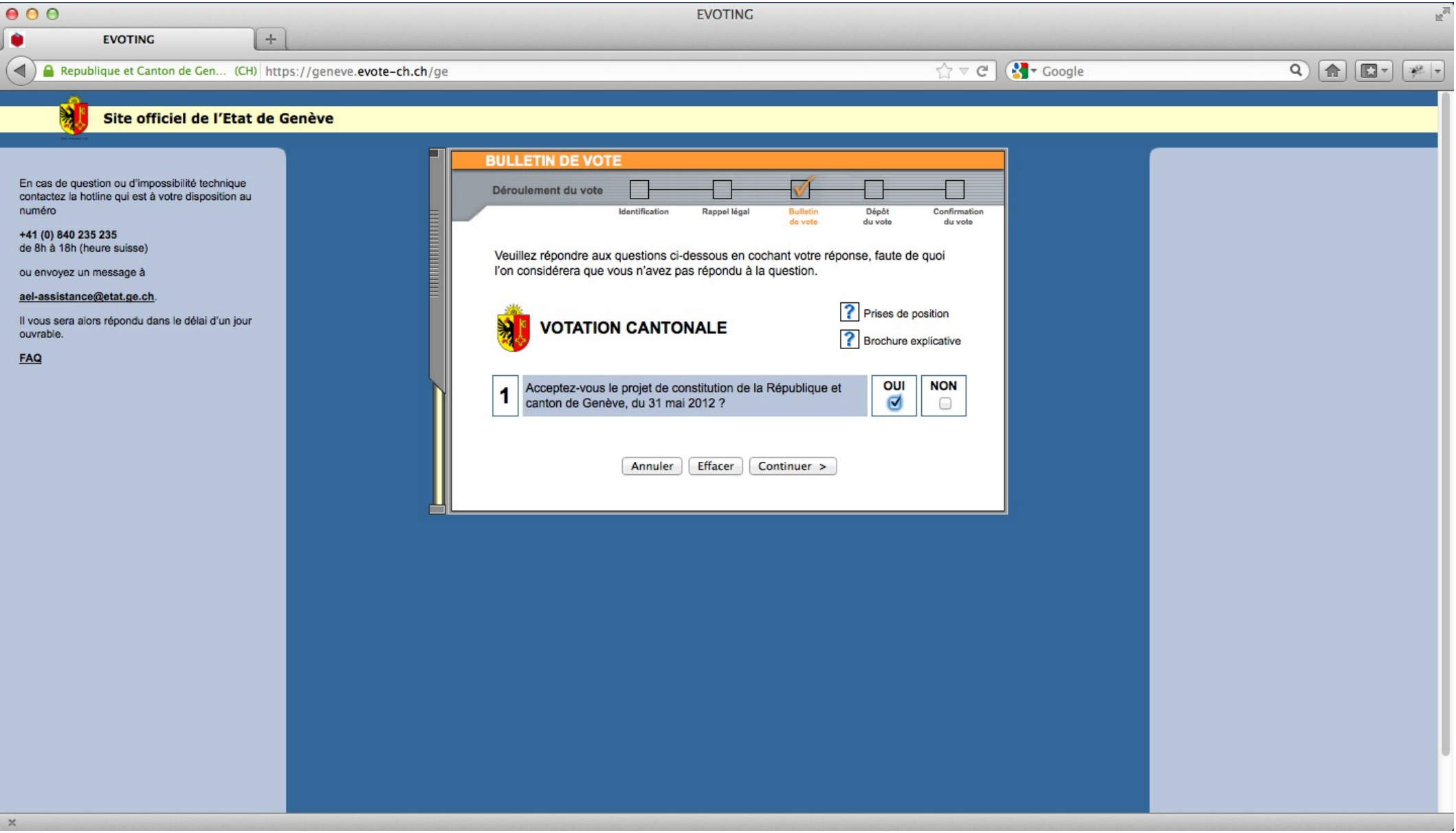
Vulnérabilités

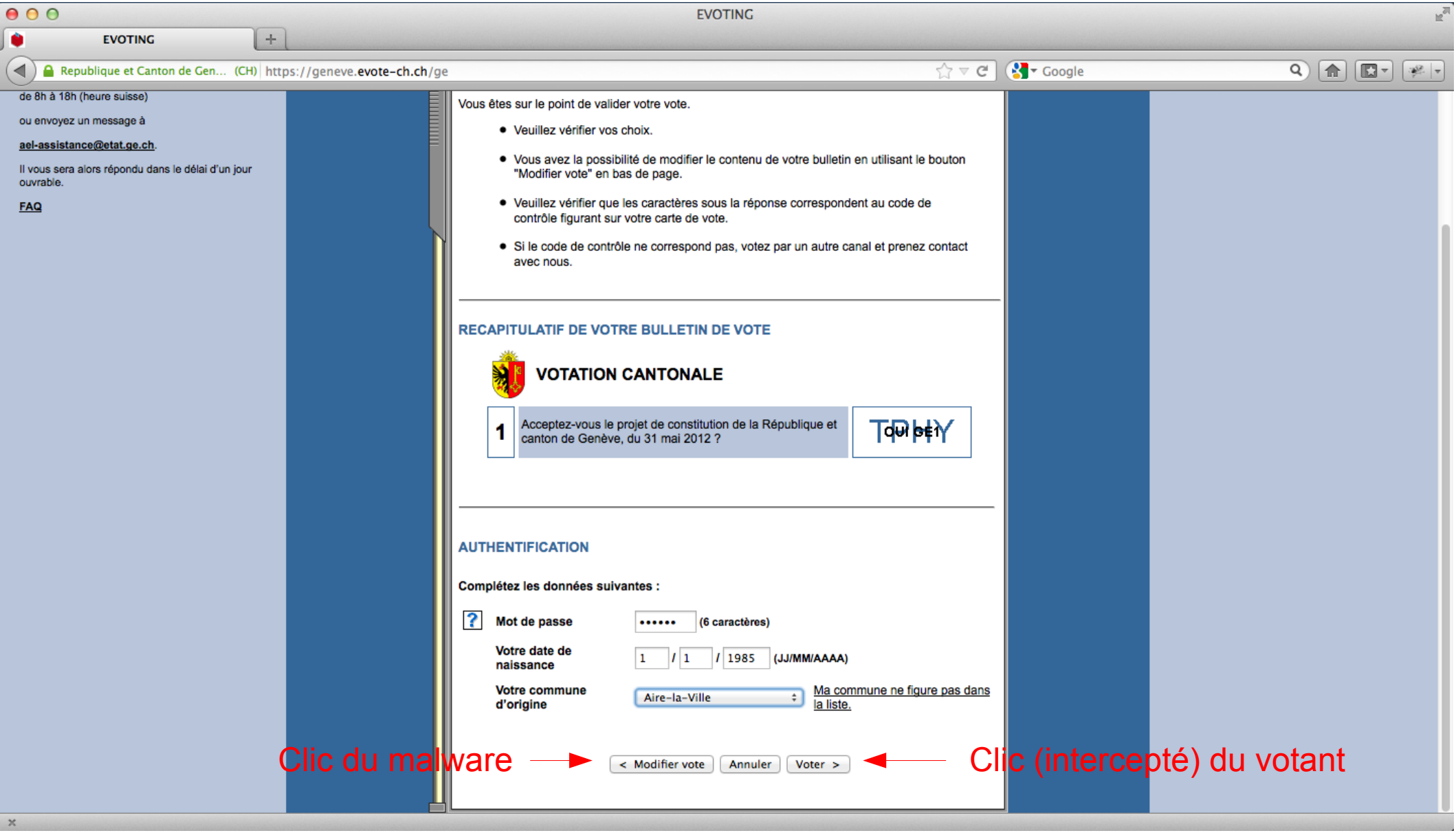
- Déchiffrage du vote pour contrôle de vote correct
  - Un malware (ou l'administrateur) sur le serveur pourrait modifier le vote, ou savoir qui a voté quoi (le vote est encore en rapport avec le NCV)

- Compteur d'intégrité
  - La clé symétrique de chiffrage du compteur d'intégrité est entre les mains de l'administrateur

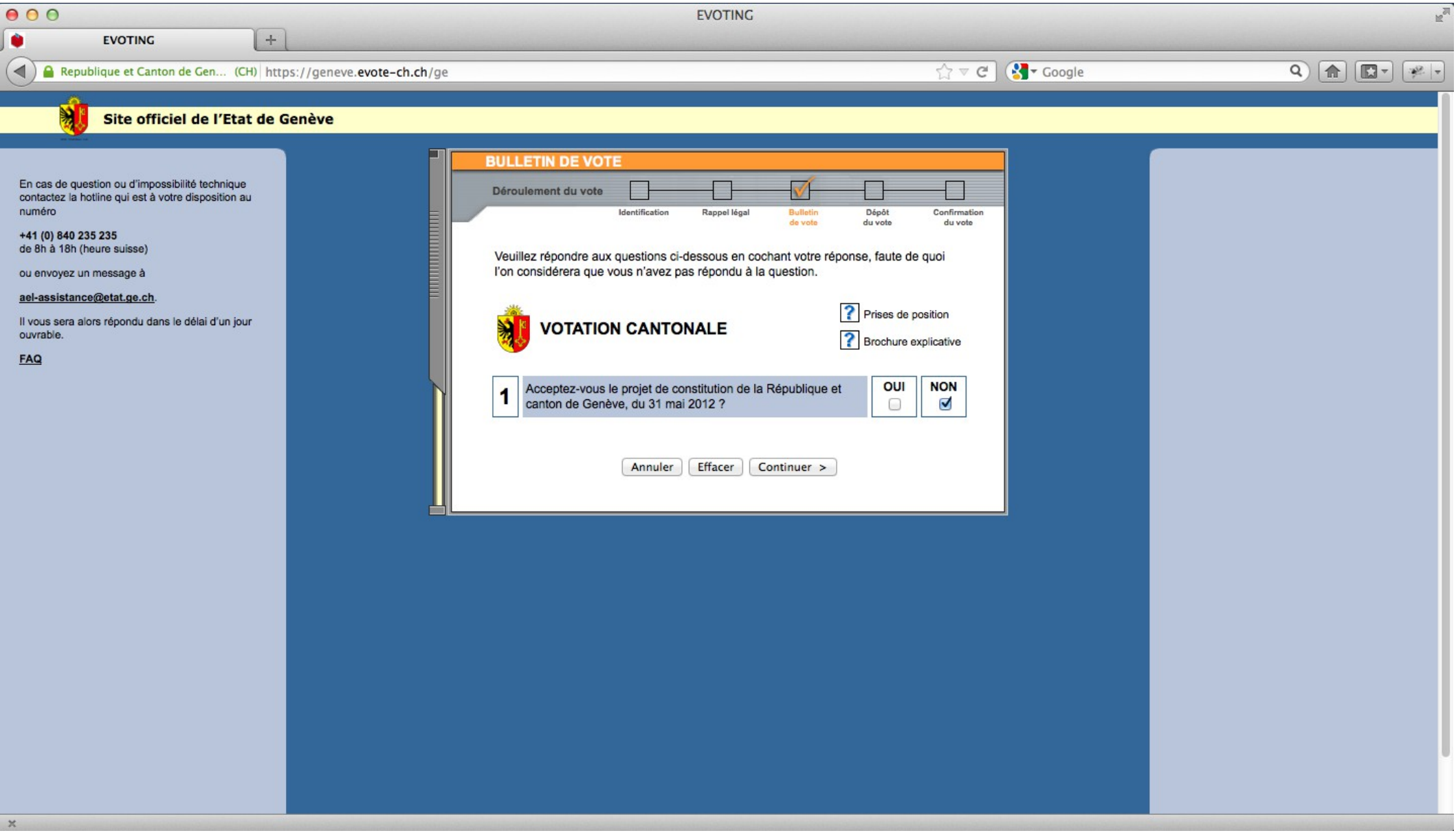
Vulnérabilités

- Le malware peut agir au niveau du GUI
  - L'utilisateur sélectionne un choix et continue vers la page suivante
  - Le code de confirmation du serveur est indiqué, ainsi que sa réponse
  - A ce moment, un malware peut figer l'écran, revenir en arrière, sélectionner un autre choix et valider ce choix
  - L'écran de confirmation final est affiché
- Variante : manipulation de l'image de contrôle

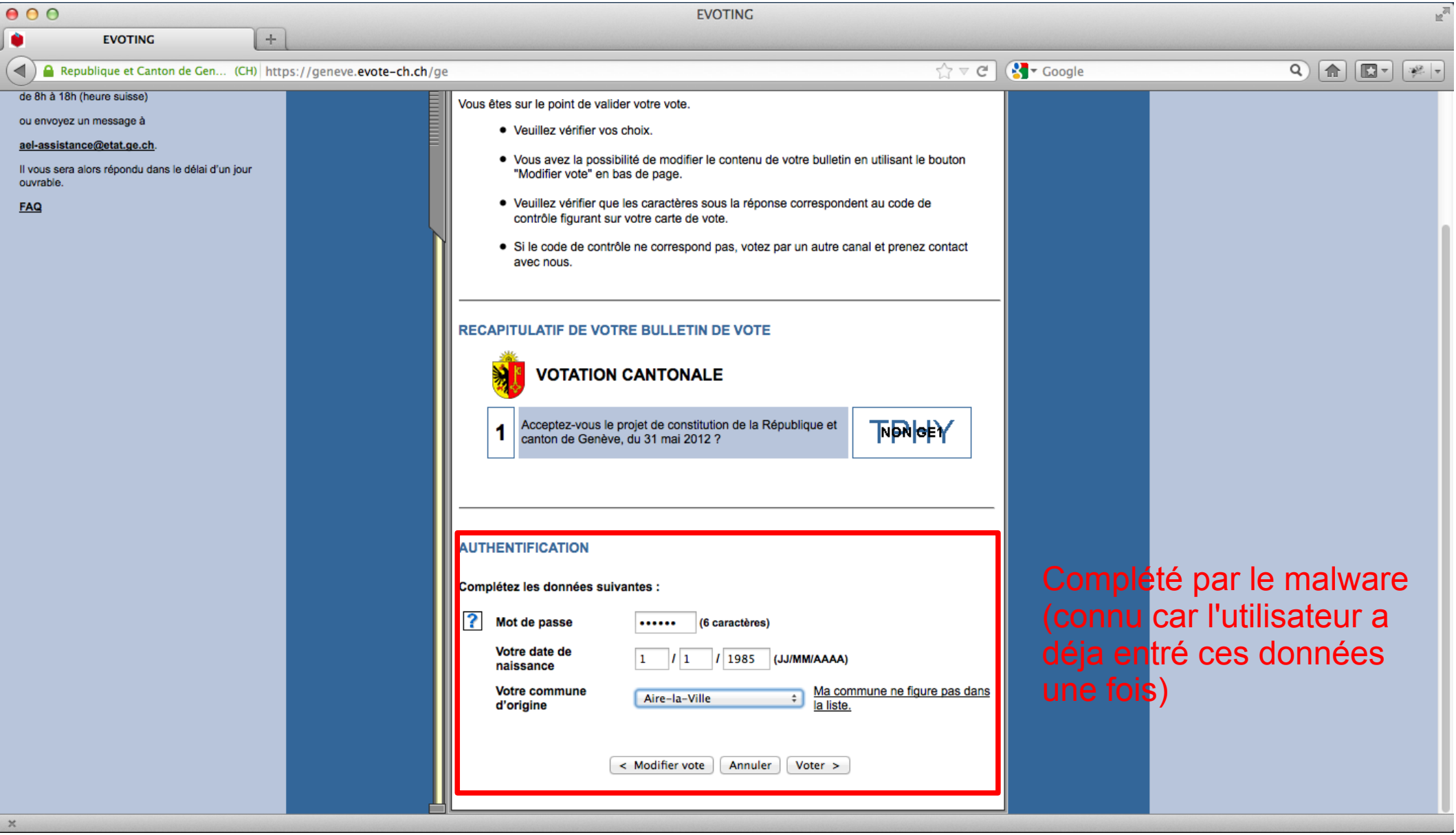

EVOTING
EVOTING
Republique et Canton de Gen... (CH) https://geneve.evote-ch.ch/ge
Google
Site officiel de l'Etat de Genève
En cas de question ou d'impossibilité technique contactez la hotline qui est à votre disposition au numéro
+41 (0) 840 235 235
de 8h à 18h (heure suisse)
ou envoyez un message à
ael-assistance@etat.ge.ch.
Il vous sera alors répondu dans le délai d'un jour ouvrable.
FAQ
BULLETIN DE VOTE
Déroulement du vote
Identification
Rappel légal
Bulletin de vote
Dépôt du vote
Confirmation du vote
Veuillez répondre aux questions ci-dessous en cochant votre réponse, faute de quoi l'on considérera que vous n'avez pas répondu à la question.
VOTATION CANTONALE
Prises de position
Brochure explicative
1
Acceptez-vous le projet de constitution de la République et canton de Genève, du 31 mai 2012 ?
OUI
NON
Annuler
Effacer
Continuer >


EVOTING
EVOTING
Republique et Canton de Gen... (CH) https://geneve.evote-ch.ch/ge
Google
de 8h à 18h (heure suisse)
ou envoyez un message à
ael-assistance@etat.ge.ch.
Il vous sera alors répondu dans le délai d'un jour ouvrable.
FAQ
Vous êtes sur le point de valider votre vote.
Veuillez vérifier vos choix.
Vous avez la possibilité de modifier le contenu de votre bulletin en utilisant le bouton "Modifier vote" en bas de page.
Veuillez vérifier que les caractères sous la réponse correspondent au code de contrôle figurant sur votre carte de vote.
Si le code de contrôle ne correspond pas, votez par un autre canal et prenez contact avec nous.
RECAPITULATIF DE VOTRE BULLETIN DE VOTE
VOTATION CANTONALE
1
Acceptez-vous le projet de constitution de la République et canton de Genève, du 31 mai 2012 ?
OUI PE1
AUTHENTIFICATION
Complétez les données suivantes :
Mot de passe
(6 caractères)
Votre date de naissance
1 / 1 / 1985 (JJ/MM/AAAA)
Votre commune d'origine
Aire-la-Ville
Ma commune ne figure pas dans la liste.
Clic du malware
< Modifier vote
Annuler
Voter >
Clic (intercepté) du votant

Ecran masqué au votant



Ecran masqué au votant



Complété par le malware (connu car l'utilisateur a déja entré ces données une fois)

Ecran de confirmation, le votant ne voit pas qu'une modification de son vote a été faite