

SwissiVi: PoC for a Novel E-Voting Platform

**Informatique / Directeurs de thèse: Prof. Dr. Eric Dubuis, Prof. Dr. Rolf Haenni, Prof. Reto Koenig
Expert: Dr. Andreas Spichiger**

Bien qu'il existe aujourd'hui plusieurs protocoles cryptographiques qui satisfont de nombreuses exigences suggérées pour des systèmes de vote électronique, une interface sûre et facile à utiliser entre le votant et la cryptographie sur un PC ou smartphone potentiellement vulnérable manque toujours à l'appel. Le Research Institute for Security in the Information Society de la HESB a mis en place un nouveau concept de vote électronique résolvant ce problème. Le but de ce travail de bachelor est de réaliser une démonstration de faisabilité (Proof of Concept, POC) de ce concept.

Le concept de la HESB en bref

La plateforme sécurisée est un problème récurrent dans le domaine de l'e-voting. Si le support utilisé pour afficher la plateforme est infecté par un malware, la confidentialité ainsi que l'intégrité du vote ne peuvent pas être garanties.

Pour éviter ce problème, la HESB a développé un concept mettant en jeu un petit appareil permettant de confirmer le vote. Cet appareil n'a pas de moyen de communication direct avec l'ordinateur ou avec internet, et ne peut donc pas être infecté par un malware.

Par conséquent, un support infecté affichant la plateforme peut toujours modifier le vote, mais cela sera détecté par l'utilisateur lorsqu'il devra confirmer son choix sur l'appareil de vote.

Trois acteurs principaux interviennent dans ce concept: une plateforme de vote, l'appareil de vote mentionné plus haut et une carte de vote personnelle.

La plateforme de vote permet à l'utilisateur de consulter les objets à voter. Les résultats pouvant être choisis par le votant sont représentés sous forme de codes-barres bidimensionnels.

A l'aide de l'appareil de vote, l'utilisateur peut lire ces codes-barres dont le contenu apparaît sur l'écran. Il doit alors confirmer son choix.

La carte de vote permet de vérifier la légitimation de vote, ainsi que de récupérer le vote créé par l'appareil de vote afin de l'envoyer à l'urne électronique.

Réalisation

Le travail consiste en deux parties principales. Pour la première, il s'agit de simuler l'appareil et la carte de vote avec des smartphones. La seconde partie est la réalisation de la plateforme de vote. Celle-ci doit supporter les types de votes suisses (vote, initiative et élections) pour le niveau fédéral, le

niveau cantonal et le niveau communal.

La simulation de l'appareil et de la carte de vote a été réalisée sur Android. L'appareil de vote permet de scanner un code-barres de la plateforme de vote, décode le contenu du code-barres et l'affiche sur l'écran. L'utilisateur confirme le vote, puis celui-ci est envoyé au smartphone simulant la carte.

Le fichier enregistré sur la carte de vote peut être récupéré sur un ordinateur en y connectant le smartphone. Le vote peut finalement être chargé dans l'urne électronique.

La plateforme propose une page d'accueil où l'utilisateur peut choisir son canton de résidence. Il doit ensuite indiquer sa commune et voit apparaître une vue d'ensemble de tous les objets pour lesquels il peut voter. Une page lui permet alors d'afficher les codes-barres pour les différents objets. Si des élections sont disponibles, une interface lui permet de choisir une liste, de la modifier ou de composer sa propre liste.

Pour utiliser de manière optimale la surface disponible à l'écran, les différents objets sont groupés par niveau (fédéral, cantonal, communal), puis répartis en différents onglets.

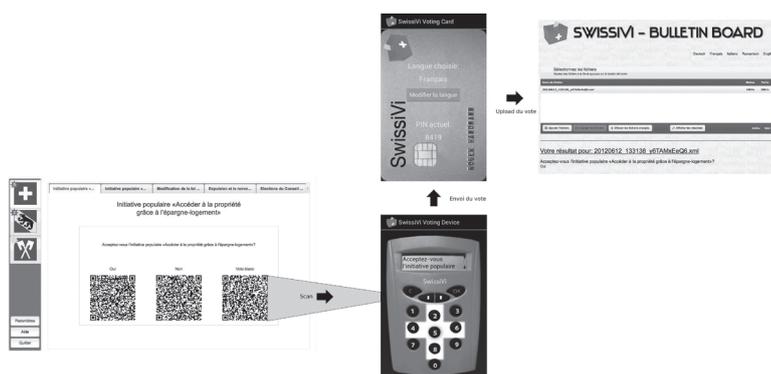
Le résultat obtenu dans ce travail propose une implémentation possible de ce concept et peut être utilisé pour le présenter aux personnes intéressées.



Andrea Pellegrini



Philémon von Bergen



Aperçu du déroulement d'un vote