Analyse de sécurité de la plateforme de vote Belenios
Conformité avec les recommandations 2019 de la CNIL

Date de rédaction : 2 décembre 2020
Rédacteurs : Véronique Cortier, Pierrick Gaudry, Stéphane Glondu

Belenios est un logiciel de vote en ligne. La version à laquelle se réfère ce document est la 1.11 (mai 2020). Pour être utilisé, Belenios doit être déployé sur un serveur. Plusieurs instances de Belenios existent, sur différents serveurs. L'analyse de sécurité de ce document porte uniquement sur l'instance déployée sur le serveur `https://belenios.loria.fr/admin`.

1 Contexte

1.1 Références utiles

CNIL. Les recommandations 2019 de la CNIL [1] sont disponibles au journal officiel du 21 juin 2019 (un petit rectificatif du 29 juin ajoute un nombre de mois qui manquait). Ces nouvelles recommandations font suite et remplacent les anciennes recommandations de la CNIL émises en 2010. Elles définissent 3 niveaux de sécurité suivant l'enjeu du scrutin, et les objectifs de sécurité à réaliser pour chaque niveau.

La CNIL a également mis en ligne une fiche pratique [2] qui propose une grille d'analyse permettant d'évaluer le niveau de sécurité requis, ainsi que des moyens concrets pour réaliser les objectifs de sécurité des recommandations.

Fonctionnement de Belenios.

- La spécification complète du logiciel Belenios [7] déployé sur la plateforme de vote éponyme est disponible en ligne et mise à jour régulièrement.
- Une description plus haut niveau, ainsi que quelques statistiques sur l'usage de Belenios se trouvent dans l'article [6].
- Le site web `http://www.belenios.org/` de présentation de Belenios donne également des informations haut niveau sur le fonctionnement du logiciel.
- Le code source du logiciel est disponible [3] sous licence libre et sert de référence en cas d'ambigüité dans la documentation.

Tous ces documents sont en anglais.

Analyse de Belenios. Le protocole de vote Belenios a été analysé formellement, selon les standards académiques [2].

Autres sources sur le vote électronique. Chaque pays a sa propre vision du fonctionnement des élections, et les réglementations pour le vote électronique sont très variables d'un pays à l'autre. Il est très intéressant de considérer le contexte général pour mettre en perspectives les recommandations de la CNIL, comprendre ses forces, mais aussi ses limites. Le livre de Hao et Ryan [8], écrit en 2016, couvre de nombreux aspects et pointe sur une bibliographie très riche. Pour les aspects réglementaires, le cadre mis en place par la Chancellerie suisse [1] est un exemple intéressant qu'il est instructif de mettre en parallèle du point de vue CNIL.

1. Le texte complet est disponible sur le site de Legifrance `https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038661239`.
2. Cf `https://www.cnil.fr/fr/securite-des-systemes-...-de-2010` (dernière visite du lien le 9 janvier 2020).
3. Le dépôt public de référence est `https://gitlab.inria.fr/belenios/belenios/`.

1.2 Contexte d'utilisation

La plateforme de vote est utilisée et est adaptée pour des élections à enjeux modérées (en termes de sécurité) comme des élections de conseil de laboratoire ou autres instances scientifiques, des votes au sein de comités de recrutement, des élections au sein d'associations de parents d'élèves ou des associations sportives.

Ainsi, la plateforme de vote Belenios peut être utilisée si les conditions suivantes sont remplies :

1. Le nombre d'électeurs est modéré (autour de 2000),
2. Le scrutin *peut* être reporté (ou au moins prolongé) en cas de problème majeur.
   En effet, la plateforme est hébergée par un serveur unique. Une panne informatique / électrique / de réseau est toujours possible. Une attaque par déni de service est également envisageable si l'enjeu du scrutin le justifie.
3. Il n'y a pas de risque important d'achat de vote : comme tous les systèmes de vote déployés à l'heure actuelle, il est possible de vendre ses identifiants par exemple.
4. Une attaque par infection des machines des électeurs est considérée comme hautement improbable. En effet, une machine d'électeur corrompue peut modifier le choix de l'électeur (le votant clique sur A et sa machine chiffre B).
5. Plus généralement, les risques résiduels décrits à la Section 4.8 sont considérés comme acceptables.

Nous insistons sur le fait que, à nos yeux, il n'y a pas de solution de vote qui permette actuellement d'atteindre un niveau de sécurité suffisant pour des élections à très fort enjeu (par exemple élection présidentielle, législative). Dans ce type d'élection, des élections papier à l'urne (avec une urne effectivement surveillée, de façon constante, par des personnes indépendantes) représentent le seul système proposant un niveau de sécurité acceptable (même si les élections papier, même correctement surveillées, ne sont pas parfaites non plus).

Important : *La plateforme de vote offre plusieurs choix de sécurité, notamment pour permettre une prise en main plus facile. L'analyse de sécurité de ce document correspond à une utilisation de la plateforme avec un niveau de sécurité maximal :*

- *utilisation d'un générateur de code de vote extérieur (Credential management → Manual)*
- *au moins une autorité extérieure de déchiffrement (au moins un « trustee ») dans le cas sans seuil, au moins deux autorités (extérieures) de déchiffrement dans le cas à seuil (« threshold mode »). Dans tous les cas, le serveur détient lui aussi une part de la clé : il faut l'action du serveur et des autorités pour déchiffrer.*
- *authentification par mot de passe ou authentification externe (serveur CAS)*

Les élections correspondant à ces critères sont surveillées (monitorées) automatiquement comme décrit dans le rôle « Auditeur » de la section suivante.

1.3 Modalités d'élection

La plateforme de vote Belenios permet d'organiser deux grands types d'élection appelés ici « standard » et « méthodes alternatives ».

Élection standard. Dans le mode par défaut, l'administrateur de l'élection définit pour chaque question, la liste des réponses possibles (par exemple les noms des candidats). L'électeur pourra choisir entre a et b réponses, avec a et b déterminés par l'organisateur. Il y a possibilité de voter blanc (si l'organisateur le souhaite).

- Si $a = b = 1$, l'électeur peut choisir exactement une réponse.
- Si $a = 0$ et b est le nombre total de réponses, l'électeur peut choisir librement les réponses qu'il veut.
- Toute autre combinaison est possible.

Le résultat de l'élection est le nombre total de votes reçus, pour chaque réponse possible, ainsi que le nombre de votes blancs, le cas échéant.

Méthodes alternatives de vote. Dans le mode « méthodes alternatives », l'électeur va attribuer un nombre (entre 0 et 255) à chaque réponse.

- Par exemple, l'élection peut demander à l'électeur d'attribuer 1 à son candidat favori, 2 à son deuxième choix et ainsi de suite.
- Ou alors, l'élection peut demander à l'électeur d'attribuer une note (par exemple entre 1 et 5) à chaque candidat.

Le résultat de l'élection est l'ensemble des votes reçus (chaque vote est un vecteur d'entier représentant les choix de l'électeur), présenté dans un ordre aléatoire pour éviter tout lien entre bulletin chiffré et bulletin en clair (des techniques cryptographiques de mélangeurs vérifiables sont utilisées).

C'est alors à l'organisateur de l'élection d'employer la technique de comptabilisation qu'il souhaite (Condorcet, STV, jugement majoritaire) pour calculer le résultat à partir des bulletins bruts.

2 Description succincte du fonctionnement de la plateforme Belenios

Il n'est pas possible de décrire complètement le fonctionnement dans ce document, mais nous en rappelons ici les grandes lignes, ce qui doit suffire pour comprendre l'analyse de sécurité des sections suivantes. Nous nous contentons donc ici de lister les différents acteurs qui interviennent lors d'un scrutin ainsi qu'un condensé de leur rôle. Une description plus précise et fonctionnelle de ce que doit faire chacun est donnée ici : `http://www.belenios.org/instructions-fr.html`

Administrateur de l'élection. Il met en place l'élection en définissant plusieurs paramètres. En particulier il fournit :

- le choix du mode de scrutin (standard ou alternatif) ;
- les choix de sécurité (qui détient les clés de déchiffrement, comment le matériel de vote est envoyé) ;
- le choix du libellé des questions et des réponses possibles ;
- la liste électorale (la liste des adresses mail qui recevront le matériel de vote, ainsi que l'identifiant CAS dans le cas où ce mode d'authentification est utilisé).

L'administrateur de l'élection interagit avec les autres acteurs pendant la mise en place de l'élection et son dépouillement. Il peut, à tout moment, fermer ou rouvrir une élection (avant son dépouillement). Il peut également programmer l'ouverture et la fermeture du scrutin à la date et à l'heure de son choix. Pendant l'élection, il peut demander au serveur de renvoyer le login et mot de passe à un électeur. Il n'a plus la possibilité de modifier la liste électorale ni aucun autre des paramètres listés ci-dessus.

Électeur. Avant le début de l'élection, chaque électeur reçoit :

- un code de vote (une suite de caractères) ;
- un login et un mot de passe (sauf si un mode d'authentification pré-existant, de type CAS, est utilisé).

Pour voter, il se connecte au site de l'élection, rentre son code de vote et répond aux questions comme prévu dans le scrutin. Ses choix de vote sont chiffrés sur la machine qu'il utilise (ordinateur, tablette, smartphone) puis le bulletin chiffré est envoyé au serveur, qui authentifie l'électeur avec son login et mot de passe. Une empreinte du bulletin chiffré, appelée *numéro de suivi*, est créée dès le chiffrement

du bulletin et affichée à l'électeur. Ce numéro de suivi est envoyé par mail lorsque le bulletin est bien reçu par le serveur. Grâce à ce numéro de suivi, l'électeur peut vérifier à tout moment que son bulletin est dans l'urne en consultant la page web de l'urne (accessible depuis le site de l'élection).

Jusque la fin du scrutin, un électeur peut voter de nouveau. Dans ce cas, seul son dernier vote est comptabilisé.

Une fois l'élection close et le dépouillement effectué, l'électeur peut consulter le résultat en visitant le même lien que celui qui lui a servi pour voter. Il peut (et est encouragé à) vérifier que son numéro de suivi est toujours dans l'urne. Il peut également, vérifier toutes les données d'audit disponibles, ce qui revient à jouer le rôle d'auditeur décrit ci-dessous.

Serveur de vote - plateforme de vote. Le serveur de vote reçoit les bulletins de vote chiffrés et centralise toutes les opérations. Il :

- offre un tableau de bord à l'administrateur ;
- orchestre les interactions entre les différentes parties ;
- envoie des identifiants aux électeurs ;
- authentifie les électeurs et réceptionne les bulletins chiffrés ;
- gère l'urne et la maintient publique ;
- après dépouillement, rend les résultats publics, avec toutes les données d'audit ;
- gère la base de données des élections et met en œuvre la politique d'archivage associée [5].

Autorité de déchiffrement (trustee). Les votes sont chiffrés avec la clé publique de l'élection. Les clés de déchiffrement sont partagées entre plusieurs autorités, possiblement avec un système de seuil (par exemple 3 autorités parmi 5 suffiront pour déchiffrer). Ces autorités sont des personnes choisies par la commission électorale. D'autre part, pour plus de sécurité, le serveur de vote détient également une des clés de déchiffrement.

Chaque autorité de déchiffrement génère sa clé secrète avant le début de l'élection et la stocke de façon sécurisée. Au moment du dépouillement, elle doit utiliser sa clé secrète. Tous les calculs utilisant sa clé secrète sont faits en local sur sa machine.

Générateur de codes de vote. Une autorité est en charge de créer les codes de vote, un pour chaque électeur. Elle envoie par mail un code à chaque électeur et transmet la partie publique au serveur de vote.

Pendant l'élection, le générateur de codes peut renvoyer leur code de vote aux électeurs qui l'ont perdu.

Auditeur. Un auditeur vérifie la conformité de l'élection. Plus précisément, il a accès à toutes les données publiques disponibles sur la page web de l'élection et il s'assure que :

- Le nombre de codes publics affichés correspond au nombre d'électeurs,
- La liste des questions et des réponses correspond bien à ce qui a été déterminé pour ce scrutin,
- Les bulletins chiffrés présents sur l'urne publique ne disparaissent pas. Plus précisément, l'auditeur vérifie qu'aucun bulletin ne disparait sauf s'il est remplacé par un bulletin signé par le même code de vote (revote de l'électeur).
- Chaque bulletin chiffré est signé par un code valide (permet de vérifier que les bulletins proviennent d'électeurs légitimes)
- Les données cryptographiques sont cohérentes (cohérence entre les clés publiques des autorités de déchiffrement et clé publique de l'élection par exemple).
- Après le dépouillement, il s'assure que le résultat correspond aux bulletins chiffrés de l'urne, grâce aux preuves cryptographiques fournies par les autorités de déchiffrement.

A minima, ce rôle est joué par un serveur tiers mis en place par l'équipe de développement Belenios. Cependant, plus l'urne est surveillée, mieux c'est. Les organisateurs de l'élection peuvent donc mettre en place leurs propres audits, par exemple en utilisant les fonctions offertes par l'outil ligne de commande `belenios-tool`.

3 Conformité aux recommandations 2019 de la CNIL

La plateforme de vote Belenios est conforme aux niveaux 1 et 2 définis par la CNIL, ainsi que le niveau 3, suivant la mise en œuvre choisie (voir Section 3.3). Nous argumentons comment Belenios réalise chaque objectif de sécurité demandé par la CNIL.

Il est à noter cependant que les recommandations de la CNIL ne constituent par le graal en matière de sécurité. Par exemple, les exigences de la chancellerie Suisse sont bien plus précises et bien plus poussées. Ainsi, pour la chancellerie Suisse, le résultat de l'élection doit pouvoir être vérifié sans faire confiance au prestataire de vote. Un vote ne doit pas pouvoir être modifié même si l'ordinateur du votant est corrompu. D'autre part, le fonctionnement du système de vote doit être public (spécifications détaillées publiques). Plus généralement, la communauté académique a développé et défini de nombreuses propriétés de sécurité souhaitables pour le vote électronique, qui vont bien plus loin que les recommandations de la CNIL.

3.1 Niveau 1

Les solutions de vote dont le scrutin présente un risque de niveau 1 doivent atteindre a minima l'ensemble des objectifs de sécurité suivants.

Objectif de sécurité n° 1-01 : *Mettre en œuvre une solution technique et organisationnelle de qualité ne présentant pas de faille majeure (faille publiée par l'éditeur et/ou rendue publique par des tiers).*

Comme préconisé par la CNIL, la plateforme de vote Belenios utilise les dernières versions stables et mises à jour des systèmes d'exploitation, des serveurs Web, des solutions de chiffrement et des bases de données mobilisées dans la solution. Les protocoles et algorithmes publics de chiffrement sont réputés « forts ».

Objectif de sécurité n° 1-02 : *Définir le vote d'un électeur comme une opération atomique, c'est-à-dire comme comportant de manière indivisible le choix, la validation, l'enregistrement du bulletin dans l'urne, l'émargement et la délivrance d'un récépissé.*

Le bulletin contenant le choix validé par l'électeur et signé par son code valide est préparé entièrement du côté client, y compris le chiffrement. L'opération d'enregistrement dans l'urne est effectuée par le serveur, à la condition que le bulletin soit valide (cryptographiquement), et que l'authentification de l'électeur ait réussi. Dans ce cas, et uniquement dans ce cas, la liste d'émargement est mise à jour, un mail de confirmation est envoyé à l'électeur avec un numéro de suivi faisait office de récépissé, et l'urne publique lui fournit de plus une manière de vérifier que son bulletin y est bien présent.

Objectif de sécurité n° 1-03 : *Authentifier les électeurs en s'assurant que les risques majeurs liés à une usurpation d'identité sont réduits de manière significative.*

L'électeur s'authentifie à l'aide de deux éléments, login et mot de passe d'une part, et code de vote d'autre part. Ces deux éléments sont transmis séparément, l'un par le serveur de vote, l'autre par le générateur de codes de vote.

En cas de perte ou de vol, l'électeur peut demander un nouveau mot de passe. Dans ce cas, l'ancien mot de passe est invalidé. Le code de vote peut également être ré-envoyé à l'électeur par le générateur de codes de vote (sans changement). Si entre temps le matériel de vote a été utilisé par un usurpateur, l'électeur peut revoter avec ses nouveaux identifiants, et cela annulera l'ancien vote. Par ailleurs, un vote avec usurpation d'identité va générer un envoi de récépissé automatique vers l'électeur légitime, ce qui augmente significativement la détection de la fraude.

Objectif de sécurité n° 1-04 : *Assurer la stricte confidentialité du bulletin dès sa création sur le poste du votant.*

Comme préconisé par la CNIL, le bulletin est chiffré sur le poste du votant, coté client et avant son émission, à l'aide d'un algorithme public réputé « fort ».

Objectif de sécurité n° 1-05 : *Assurer la stricte confidentialité et l'intégrité du bulletin pendant son transport.*

Le bulletin de vote est chiffré et transmis au serveur par un canal HTTPS, qui ajoute une deuxième couche de chiffrement et assure l'intégrité. D'autre part, le bulletin est authentifié grâce à une signature dérivée du code de vote, il est impossible de modifier le bulletin en gardant une signature valide. Enfin, l'intégrité du bulletin est encore une fois assurée par le fait que l'électeur peut vérifier la présence de son propre bulletin dans l'urne, avec son numéro de suivi.

Objectif de sécurité n° 1-06 : *Assurer, de manière organisationnelle et/ou technique, la stricte confidentialité et l'intégrité du bulletin pendant son traitement et son stockage dans l'urne jusqu'au dépouillement.*

La confidentialité du bulletin lors de son traitement et son stockage dans l'urne est assurée par le chiffrement utilisé. Son intégrité est assurée par une double protection. D'une part, la signature associée au bulletin devient invalide si le bulletin est modifié. Le serveur de vote ne possède aucune clé de signature, il ne peut donc pas produire de signature valide. La seule possibilité serait donc l'effacement pure et simple d'un bulletin. Or cela serait détecté puisque les électeurs peuvent vérifier la présence de leur bulletin dans l'urne et des audits extérieurs assurent que l'urne ne fait que croître.

Objectif de sécurité n° 1-07 : *Assurer l'étanchéité totale entre l'identité de votant et l'expression de son vote pendant toute la durée du traitement.*

L'étanchéité entre l'identité de votant et l'expression de son vote est assurée par deux moyens.

- Les clés nécessaires au déchiffrement sont générées et stockées sur des machines distinctes, indépendantes, administrées par des personnes ou entités différentes puisqu'il s'agit du serveur d'une part et des autorités de déchiffrement choisies par la commission électorale d'autre part. Il est même peu probable qu'elles aient tous le même système d'exploitation par exemple.
  Ainsi, même si le lien est fait entre un votant et son bulletin chiffré, il est impossible de faire le lien entre votant et expression du vote.
- Lors du dépouillement, les clés nécessaires au déchiffrement restent sur des machines distinctes, indépendantes, administrées par des personnes ou entités différentes. Les bulletins chiffrés des votants *ne sont jamais* déchiffrés. Belenios utilise deux solutions de déchiffrement suivant le mode de scrutin utilisé : dépouillement homomorphe ou mixnets vérifiables. Dans les deux cas, il est impossible de faire le lien entre expression du vote et bulletin.

Note. La CNIL préconise quant à elle l'absence d'horodatage du bulletin. Cette solution est un pis-aller pour les solutions de vote peu avancées technologiquement et qui dépouillent les bulletins chiffrés tels qu'ils sont été reçus (éventuellement après un simple mélange, ce qui laisse les bulletins toujours parfaitement identifiables). Pour ces solutions, le lien entre expression du vote et bulletin chiffré sera connu, il est donc absolument nécessaire que le lien entre un votant et son bulletin chiffré soit rompu, d'où la préconisation de la CNIL. Cette approche présente cependant deux défauts majeurs.

- Le serveur de vote doit d'une part stocker le bulletin chiffré et faire émarger le votant. Il possède donc le lien entre bulletin chiffré et identité du votant, même si ce lien n'est pas stocké et qu'il n'est que « furtif ». En d'autres termes, le serveur de vote / le prestataire a les moyens techniques pour faire le lien entre bulletin chiffré et électeur, et donc avec l'expression de son vote, pour ce type de solutions.
- Il est presque impossible d'empêcher l'horodatage d'un bulletin, même si le prestataire prend garde à stocker la liste d'émargement et les bulletins dans des espaces séparés. En effet, afin d'assurer la robustesse du système, il est crucial de prévoir de la redondance, avec de la réplication des données, il est aussi délicat de ne garder aucune trace des connexions au serveur.

Objectif de sécurité n° 1-08 : *Renforcer la confidentialité et l'intégrité des données en répartissant le secret permettant le dépouillement exclusivement au sein du bureau électoral et garantir la possibilité de dépouillement à partir d'un seuil de secret déterminé.*

Les clés permettant le déchiffrement sont construites par un nombre quelconque n de personnes de confiance (chaque personne construit une clé secrète), avec un seuil de k pour déchiffrer (il faut alors k secrets pour déchiffrer). On peut ainsi faire du « 2 parmi 3 » ou du « 3 parmi 5 », ou toute autre combinaison. D'autre part, une clé secrète additionnelle est toujours confiée au serveur de vote. La clef du serveur ne rentre pas dans le calcul du seuil : il faut l'action du serveur ET d'un certain nombre d'autorités (le seuil) pour déchiffrer. Cela augmente strictement la sécurité des clés et donc la confidentialité des votes.

À noter : à la différence de nombreuses solutions de vote, les secrets permettant de déchiffrer ne sont *jamais* présents sur une seule machine, que ce soit lors de la génération de la clé publique ou bien lors du dépouillement. De plus, chaque autorité possédant un secret peut vérifier que la clé publique de l'élection utilise bien ce secret (grâce à la partie publique de la clé secrète).

Objectif de sécurité n° 1-09 : *Définir le dépouillement comme une fonction atomique utilisable seulement après la fermeture du scrutin.*

L'option de dépouillement n'est activable qu'après la fermeture du scrutin. Chaque autorité de déchiffrement procède alors à un calcul sur sa propre machine, à l'aide de son secret. Lorsque le seuil de contributions est atteint, le résultat est proclamé. Aucun dépouillement partiel, en cours d'élection ne peut être obtenu car l'opération de dépouillement n'est activable qu'une seule fois et demande la participation active des autorités de déchiffrement.

Objectif de sécurité n° 1-10 : *Assurer l'intégrité du système, de l'urne et de la liste d'émargement.*

L'urne (c'est-à-dire la liste des bulletins chiffrés), la clé publique de l'élection, la liste des questions, la liste des parties publiques des codes de vote sont consultables publiquement (du moins par toute personne ayant l'url de l'élection). Des programmes automatiques, extérieurs au serveur de vote, surveillent régulièrement ces données (ce monitoring peut même être réalisé par des auditeurs extérieurs). La modification des données de l'élection (suppression d'un bulletin, changement de la liste des codes de vote publics, etc.) serait donc immédiatement détectée.

La liste d'émargement n'est pas publique. Elle est maintenue à jour par le serveur et mise à disposition de l'administrateur de l'élection. En cas de doute sur son intégrité, la cohérence de la liste d'émargement avec l'urne peut être vérifiée par le générateur de codes de vote qui connaît le lien entre les codes utilisés pour signer les bulletins de l'urne et les électeurs.

Objectif de sécurité n° 1-11 : *S'assurer que le dépouillement de l'urne puisse être vérifié a posteriori.*

Belenios est conçu de manière à ce que le dépouillement de l'urne puisse être vérifié a posteriori. Ainsi, après le dépouillement, la page web de l'élection contient :

- l'ensemble des bulletins chiffrés acceptés. Les électeurs peuvent toujours vérifier que leur bulletin est présent ;
- le résultat de l'élection ;
- les preuves cryptographiques permettant de s'assurer (sans aucun secret particulier) que le résultat correspond bien aux bulletins dans l'urne ;
- La liste des parties publiques des codes de vote, ce qui permet de s'assurer que seuls des bulletins provenant d'électeurs (ie signés par un code valide) sont présents dans l'urne.

3.2 Niveau 2.

Les solutions de vote dont le scrutin présente un risque de niveau 2 doivent atteindre a minima l'ensemble des objectifs de sécurité du niveau 1 ainsi que les suivants.

Objectif de sécurité n° 2-01 : *Assurer une haute disponibilité de la solution.* Belenios est hébergé par un serveur unique situé au laboratoire haute sécurité du Loria, bien dimensionné pour héberger des élections de quelques milliers d'électeurs. En cas de panne de ce serveur, il est possible, avec les données sauvegardées de façon régulières (toutes les heures) de remettre en place l'élection un autre serveur, avec les bulletins déjà reçus. Cette étape n'est pas automatique, elle demande une intervention manuelle de l'équipe Belenios.

Objectif de sécurité n° 2-02 : *Assurer un contrôle automatique de l'intégrité du système, de l'urne et de la liste d'émargement.*

L'auditeur télécharge régulièrement le contenu de l'urne et vérifie sa cohérence. Ces tests assurent qu'aucun bulletin n'a disparu et que seuls des bulletins légitimes (correctement signés) ont été ajoutés. Cet audit est fait a minima par un programme automatique mis en place par l'équipe Belenios mais peut être également assuré par des tiers. Les outils logiciels permettant ces tests sont disponibles dans le code open-source de Belenios. D'autre part, la spécification détaillée de Belenios [7] permet également de reprogrammer l'ensemble des tests à effectuer.

De plus, les électeurs peuvent vérifier, à tout moment, que leur bulletin est bien dans l'urne. Ce dernier point fait que la sécurité ne repose pas autant sur la liste d'émargement que pour un système traditionnel. Toutefois, la vérification que celle-ci est en accord avec l'urne peut être effectuée en permanence par le générateur de codes de vote.

Objectif de sécurité n° 2-03 : *Permettre le contrôle automatique par le bureau électoral de l'intégrité de la plateforme de vote pendant tout le scrutin.*

Comme expliqué ci-dessus, l'audit du système est réalisable par n'importe qui connaissant l'url de l'élection. L'outil ligne de commande `belenios-tool` accepte les instructions `verify` et `verify-diff` et prend en entrée une url à auditer. Cet outil doit être lancé de manière régulière (typiquement toutes les 2 minutes) par le bureau électoral et tous les auditeurs qui le souhaitent.

Objectif de sécurité n° 2-04 : *Authentifier les électeurs en s'assurant que les risques majeurs et mineurs liés à une usurpation d'identité sont réduits de manière significative.*

L'électeur s'authentifie à l'aide de deux éléments, login et mot de passe d'une part, et code de vote d'autre part. Ces deux éléments sont transmis séparément, l'un par le serveur de vote, l'autre par le générateur de codes de vote. Le code de vote permet de dériver une clé de signature unique, pour chaque électeur, et telle que le serveur de vote ne connait que la clé de vérification associée. Seul le générateur de codes de vote (et l'électeur) connait cette clé de signature. Si les deux éléments (login/mot de passe d'une part et code de vote d'autre part) sont transmis par des canaux séparés (adresses mail différentes, ou bien 1 envoi mail et 1 envoi postal), alors la compromission du matériel du vote devient très difficile. Selon les risques, il peut être nécessaire de faire un envoi courrier pour le code de vote.

Cet objectif de sécurité est obtenu de façon plus forte encore lorsque l'authentification a lieu par l'intermédiaire d'un service CAS existant. Pour compromettre les données d'authentification d'un électeur, il faut non seulement avoir accès à son code de vote (envoyé typiquement par mail) et son mot de passe CAS usuel (mot de passe professionnel, lié à son outil de travail).

Objectif de sécurité n° 2-05 : *Assurer un cloisonnement logique entre chaque prestation de vote de sorte qu'il soit possible de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours.*

D'un point de vue logique, toutes les élections hébergées par le serveur sont indépendantes. Le système prévoit l'arrêt total d'un scrutin sans impact sur les autres scrutins. De plus, il est possible à tout moment de suspendre, clore définitivement ou effacer les données associées à un scrutin, selon les nécessités. Les autres scrutins ne seront aucunement affectés, même si une personne est électeur à la fois dans une élection qui doit être interrompue et dans une élection qui perdure.

Objectif de sécurité n° 2-06 : *Utiliser un système d'information mettant en œuvre les mesures de sécurité physique et logique recommandées par les éditeurs et l'ANSSI.*

Le serveur de la plateforme Belenios est hébergé par le laboratoire haute sécurité du LORIA. Il bénéficie ainsi des services associés : accès physique contrôlé, monitoring des activités, compartimentage logique avec les autres services hébergés. Le système est une version stable, avec un nombre de services limité et des mise à jour régulières. La liste des personnes ayant un accès physique et logique au serveur est limitée et contrôlée.

Objectif de sécurité n° 2-07 : *Assurer la transparence de l'urne pour tous les électeurs.*

Une fois que l'électeur a saisi ses choix de vote sur son ordinateur, le bulletin de vote est chiffré et un « numéro de suivi » est affiché à l'électeur. Ce numéro de suivi est une empreinte numérique (un haché) du bulletin chiffré. Il est également envoyé par mail à l'électeur. L'électeur peut, à tout moment, vérifier que son bulletin est dans l'urne en consultant la page web des bulletins acceptés, disponible depuis la page de l'élection. Il lui suffit pour cela de vérifier que son numéro de suivi apparait bien sur cette page. Les auditeurs externes garantiront que le résultat proclamé correspond aux bulletins présents sur l'urne, grâce aux preuves de bon déchiffrement.

Belenios n'offre pas la fonctionnalité appelée cast-as-intended qui permet en particulier à l'électeur de valider que son terminal de vote n'est pas infecté par un logiciel malveillant. La solution recommandée par la CNIL dans cette direction est ce qui est appelé "Benaloh challenge". Les recherches académiques récentes montrent la difficulté de mise en œuvre pratique de cette approche y compris auprès d'un électorat averti.

3.3 Niveau 3.

Les solutions de vote dont le scrutin présente un risque de niveau 3 doivent atteindre a minima l'ensemble des objectifs de sécurité des niveaux 1 et 2, ainsi que les suivants.

Objectif de sécurité n° 3-01 : *Étudier les risques selon une méthode éprouvée afin de définir les mesures les plus adéquates au contexte de mise en œuvre.*

Cette étude est à réaliser en fonction de chaque scrutin. Elle doit permettre de déterminer en particulier quels canaux choisir pour faire parvenir les éléments d'authentification (login / mot de passe d'une part et code de vote d'autre part) et éviter les risques d'usurpation d'identité.

Objectif de sécurité n° 3-02 : *Permettre la transparence de l'urne pour tous les électeurs à partir d'outils tiers.*

Le contenu de l'urne (les bulletins chiffrés) est téléchargeable par les électeurs à l'aide de n'importe quelle machine connectée au réseau. La recherche du bulletin de l'électeur se fait à l'aide d'outils tiers : fonction « rechercher » du navigateur ou simple recherche exhaustive par l'électeur (les bulletins sont affichés, triés par ordre lexicographique du numéro de suivi).

Objectif de sécurité n° 3-03 : *Assurer une très haute disponibilité de la solution de vote en prenant en compte les risques d'avarie majeure.*

Comme expliqué en réponse à l'objectif de sécurité n° 2-01, il est possible de redéployer une élection en cours vers un nouveau serveur de vote, après une intervention manuelle de l'équipe Belenios (avec un délai). Dans le cas où une disponibilité plus haute est nécessaire, alors il faut envisager de déployer la solution Belenios sur des autres serveurs.

Objectif de sécurité n° 3-04 : *Permettre le contrôle automatique et manuel par le bureau électoral de l'intégrité de la plateforme pendant tout le scrutin.*

Le code open-source de Belenios met à disposition tous les outils nécessaires pour procéder à l'audit de l'urne, que ce soit de façon automatisée ou manuelle. Comme expliqué en réponse aux objectifs de sécurité n° 2-02 et n° 2-03, cet audit assure qu'aucun bulletin n'a disparu et que seuls des bulletins légitimes (correctement signés) ont été ajoutés. Avec ces outils, le bureau peut également vérifier que le résultat correspond aux bulletins chiffrés présents dans l'urne.

Enfin, une spécification complète de Belenios est disponible, à l'octet près [7] ce qui permet la ré-implémentation de ces outils par une entité exterieure à Belenios (prestataire ou établissement académique par exemple).

Objectif de sécurité n° 3-05 : *Assurer un cloisonnement physique entre chaque prestation de vote de sorte qu'il soit possible de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours.*

Le cloisonnement physique n'est pas nécessaire pour pouvoir stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours. Toutefois, si un scrutin est d'un enjeu suffisant pour devenir une cible, il peut être préférable de déployer un serveur spécifique autre que celui hébergé au LORIA afin d'éviter qu'une tentative d'attaque par déni de service impacte les autres scrutins en cours. Ceci est à évaluer au cas par cas en fonction du contexte.

3.4 Autres points des recommandations

En dehors des objectifs de sécurité, qui forment le point principal des recommandations 2019 de la CNIL, les recommandations abordent quelques autres points, que nous reprenons ici.

Expertise indépendante. La CNIL recommande que le système de vote soit expertisé par un expert indépendant (du prestataire de vote et de l'organisateur de l'élection). Cette expertise est pensée dans un cadre où le système de vote est fermé et confidentiel et où seul l'expert peut y accéder. Charge à lui de s'assurer que l'ensemble des objectifs sont remplis et que la solution expertisée sera celle mise en œuvre (point virtuellement impossible à réaliser).

L'esprit d'un système de vote comme Belenios est radicalement différent. Le système est entièrement ouvert. Le fonctionnement du protocole de vote a fait l'objet de publications scientifiques [3, 4, 2], expertisées par des pairs (d'autres chercheurs spécialistes du vote électronique et de la sécurité, au niveau académique international). Le code source est distribué sous licence AGPLv3 et peut être inspecté librement. D'autre part, le système est construit de manière à ce que le fonctionnement du serveur de vote puisse être surveillé à tout moment par des tiers (monitoring de l'urne). Sans même savoir si le « bon » code tourne sur le serveur (point impossible à assurer quelque soit le système à moins d'être soi-même administrateur du serveur), on peut vérifier que le serveur conserve bien tous les bulletins chiffrés reçus, puis que le résultat correspond aux bulletins de l'urne. L'ensemble des vérifications à effectuer est présenté à la section 5 de ce document.

Cela étant dit, le système Belenios n'a à ce jour *pas fait l'objet d'une expertise au sens de la CNIL*. Il est à noter qu'une expertise au sens de la CNIL doit être réalisée pour chaque scrutin pour les scrutins de niveau 3, et respectivement au minimum tous les 12 ou 24 mois pour les scrutins de niveau 2 et 1, sous réserve que le système n'ait pas été modifié entre temps. Une expertise de Belenios devrait donc être renouvelée fréquemment, pour chaque type de scrutin envisagé. Bien sûr, nous ne sommes pas opposés à une expertise CNIL (au contraire !) et nous apporterons notre soutien à l'organisateur d'une élection qui souhaiterait procéder à une telle expertise. Ce document, ainsi que tous les documents annexes, se veulent une aide et une préparation à une expertise au sens de la CNIL.

Vote blanc ou nul. Comme demandé par la CNIL, la plateforme de vote Belenios permet le vote blanc.

Si le droit de voter nul (en plus du vote blanc) est reconnu par les textes fondant l'élection organisée, c'est possible si une méthode alternative de vote est choisie (cf Section 1.3), ou bien, dans le cas d'une élection standard en ajoutant explicitement un choix « vote nul » dans la liste des réponses possibles. Toutefois, dans ce dernier cas, ceci ne fera du sens que si les règles du scrutin sont que l'électeur sélectionne un unique choix parmi les réponses possibles.

Conservation des données. Les données très sensibles comme la clé de déchiffrement du serveur ou le lien entre votant et bulletin *chiffré* sont détruites une semaine après le dépouillement de l'élection. Ensuite, l'ensemble des données permettant le contrôle a posteriori de l'élection, ainsi que la liste des emails des électeurs et la liste d'émargement sont conservés jusqu'à l'archivage de l'élection, par son administrateur, et à défaut au bout d'un an. Un document complet faisant état des données stockées sur le serveur et leur conservation est disponible en ligne [5].

4 Scénarios de menace

4.1 Compromission du serveur

En cas de piratage du serveur de vote, les possibilités d'attaque sont les suivantes, ainsi que, le cas échéant, les mesures pour les diminuer :

- Annulation de l'élection. Si l'attaquant rend brusquement le serveur inutilisable, il est possible de redémarrer un autre serveur et de continuer l'élection. Mais si la corruption est plus sournoise, on peut arriver à une situation où l'élection est définitivement perdue (par exemple, si le serveur perd volontairement sa contribution à la clef de déchiffrement).
- Envoi du mauvais Javascript aux électeurs. Ceci peut permettre à l'attaquant de rompre le secret du vote et de changer l'intention du vote dans le bulletin. Afin de réduire le risque, il est encouragé d'effectuer un monitoring du Javascript servi aux électeurs tout le long de l'élection. Le code doit correspondre à celui obtenu après compilation des sources de Belenios. Un tel monitoring est présent en permanence indépendamment des élections en cours.
- Envoi du mauvais Javascript aux autorités de déchiffrement. Ceci permet à l'attaquant de connaître la clé secrète, et met en danger le secret du vote.
- Manipulation de l'urne. Ceci permet à l'attaquant de supprimer ou modifier des bulletins. Le monitoring de l'urne, ainsi que les preuves de bonne formation avec les signatures offrent une bonne protection contre ce risque.
- Le serveur peut manipuler l'urne envoyée aux autorités de déchiffrement, par exemple en envoyant seulement le bulletin d'Alice ou bien le bulletin d'Alice accompagné de bulletins dont il connait le contenu. Ainsi, le résultat de l'élection lui révèlera le vote d'Alice. Cependant, cette attaque, sophistiquée, est détectable (le haché de l'urne déchiffrée ne correspondra pas au haché de l'urne réelle) et ne permet d'apprendre qu'un seul vote. Un risque beaucoup plus important apparait dans le cas où des mélangeurs sont utilisés (cas du vote alternatif). Dans le pire des cas, le serveur peut fournir l'urne initiale à dépouiller, au lieu de celle obtenue après mélange, ce qui lui permet de connaitre l'intégralité des contenus des bulletins et donc de savoir qui a voté quoi. À nouveau, cette attaque est détectable : sur la page finale de l'élection, après dépouillement, les autorités de déchiffrement constateront que l'empreinte de l'urne finale ne correspond pas à celle déchiffrée. Mais cette vérification intervient trop tard. Si ce risque est jugé non acceptable (élections de niveau 3 par exemple), les autorités de déchiffrement doivent utiliser l'outil en ligne de commande `belenios-tool` pour déchiffrer, qui effectue toutes les vérifications nécessaires.

4.2 Compromission de l'administrateur

Le premier risque vis-à-vis de l'administrateur est son contrôle de la liste électorale. Il appartient à la commission électorale de vérifier que cette liste est correcte grâce au rapport fourni par le serveur qui affiche le nombre d'électeurs inscrits et le haché de la liste électorale. Le générateur de codes de vote peut lui aussi détecter une liste manipulée par l'administrateur et alerter le cas échéant la commission.

D'autre part, l'administrateur a la possibilité de créer deux élections en parallèle. La « vraie » où les électeurs vont voter et où il contrôlerait les autorités de déchiffrement et de génération de codes de vote (il se nomme autorités de déchiffrement et générateur de codes de vote). D'autre part, il peut créer une

« fausse » élection (ou utiliser une autre élection moins importante) où il ferait intervenir les autorités officielles, qui n'agiraient donc pas sur la bonne élection. L'administrateur serait alors en mesure de savoir qui a voté quoi, du moins en mode threshold. En effet, en mode non threshold, le serveur détient toujours une des clés nécessaires au déchiffrement. Dans tous les cas, un tel agissement est détectable :

- en s'assurant que l'url de l'élection donnée aux autorités est bien celle donnée aux votants ;
- en contrôlant que la liste électorale est bien celle établie par la commission électorale.

4.3 Compromission des autorités de déchiffrement

En cas de perte d'une des clés de déchiffrement (ou d'un certain nombre de clés, dans le cas d'un système à seuil), alors l'élection sera annulée. Nul ne pourra déchiffrer les bulletins. Le secret du vote est préservé, mais l'élection est à refaire.

En cas de vol ou de malhonnêteté de certaines autorités de déchiffrement, le secret du vote est mis en danger. Si le nombre de clés qu'il a obtenues est suffisant, l'attaquant pourra déchiffrer les bulletins disponibles dans l'urne publique. Toutefois, il aura besoin d'une connaissance supplémentaire pour faire le lien entre un bulletin et l'électeur correspondant. Il peut, par exemple avoir une connaissance approximative du jour et de l'heure où l'électeur a voté, et si de plus il monitore l'urne avec une précision suffisante, réduire le choix à quelques bulletins.

4.4 Compromission du générateur de codes de vote

La seule compromission du générateur de codes de vote ne permet pas de mener une attaque. Si celle-ci s'accompagne de la compromission du serveur, alors on a une possibilité de bourrage d'urne. Le générateur de codes de vote dispose également du lien entre les électeurs et leur bulletin (via la signature de ceux-ci), et peut donc faire une coalition avec les autorités de déchiffrement pour mener une attaque contre le secret du vote.

4.5 Usurpation d'identité des électeurs

Le matériel de vote est envoyé à l'électeur en deux parties, par deux entités distinctes, le serveur et le générateur de codes de vote. Si ces deux entités utilisent le même canal d'envoi, typiquement la même adresse e-mail, alors on s'expose à de l'usurpation d'identité de la part d'un attaquant qui aurait accès à cette adresse e-mail.

- Si l'attaquant a accès à l'adresse e-mail d'un électeur, alors il peut voler le droit de vote correspondant. Ceci risque toutefois d'être détecté par l'électeur légitime lors de la réception de l'e-mail de confirmation.
- Si l'attaquant a accès à de nombreuses adresses e-mail d'électeurs, alors le bourrage d'urne peut devenir très significatif, mais le risque de détection est bien plus élevé.

Dans ce scénario, le secret du vote est préservé, et le droit de vote également, car un électeur dont l'identité a été usurpée peut toujours revoter, et seul le dernier vote est pris en compte.

Dans un contexte où le mode d'authentification des électeurs est CAS, il faut prendre en compte le risque que les administrateurs du service CAS soient les mêmes que ceux du service e-mail utilisé pour les électeurs. Même avec ce risque, la situation est plus solide qu'avec un envoi de tout le matériel par e-mail.

4.6 Logiciel malveillant sur le poste de l'électeur

Un attaquant qui aurait la possibilité de déployer un logiciel malveillant sur le poste de l'électeur y gagnerait les possibilités, d'une part de savoir pour qui l'électeur a voté, et d'autre part (avec un logiciel malveillant ad-hoc sophistiqué), de changer l'expression du vote : faire voter pour A alors que l'électeur veut voter B.

4.7 Électeur menacé, électeur prêt à vendre son vote

Même si les outils ne sont pas fournis clé en main, le protocole Belenios n'a pas la propriété "sans reçu", et il est en théorie possible de prouver cryptographiquement à un tiers comment on a voté. Des scénarios de vente de vote ou de menace de l'électeur pour l'inciter à voter d'une certaine manière sont donc réels, comme dans la plupart des systèmes de vote à distance.

La possibilité laissée à l'électeur de revoter est une contre-mesure contre une incitation faible, de type familiale, qui ne va pas jusqu'à une menace.

4.8 Conclusion : risques résiduels

Les risques résiduels sur le secret du vote sont :

- La compromission de suffisamment d'entités de confiance (autorités de déchiffrement et un moyen de faire le lien avec les électeurs) ;
- La présence d'un logiciel malveillant sur le poste de l'électeur ;
- La compromission du serveur qui enverrait du mauvais Javascript, sans que cela soit détecté par le monitoring.

Les risques résiduels liés à la sincérité du scrutin sont :

- La compromission simultanée du serveur et du générateur de codes de vote ;
- L'usurpation d'identité par logiciel malveillant sur le poste de l'électeur ou par attaque de l'adresse e-mail.

D'autres risques apparaissent rapidement si les procédures d'audit ne sont pas suivies.

5 Recommandations

La sécurité de Belenios repose de façon fondamentale sur la surveillance mutuelle des différents acteurs de l'élection (administrateur, serveur, autorités de déchiffrement, générateur de codes de vote, votants). Il est donc important que chaque autorité suive scrupuleusement les différentes étapes, vérifications incluses. Une description plus précise et fonctionnelle de ce que doit faire chacun est donnée ici : `http://www.belenios.org/instructions-fr.html`.

Références

[1] Ordonnance de la ChF sur le vote électronique (OVotE) du 13 décembre 2013 (État le 15 janvier 2014). Chancellerie fédérale ChF `https://www.bk.admin.ch/dam/bk/fr/dokumente/pore/Anhang_VEleS_2018.pdf.download.pdf/Annexe_OVotE_V2.0_FR.pdf`, 2013. Swiss recommendation on e-voting.

[2] Véronique Cortier, Constantin Catalin Dragan, Pierre-Yves Strub, Francois Dupressoir, and Bogdan Warinschi. Machine-checked proofs for electronic voting : privacy and verifiability for Belenios. In *31st IEEE Computer Security Foundations Symposium (CSF'18)*, pages 298–312, 2018.

[3] Véronique Cortier, David Galindo, Stéphane Glondu, and Malika Izabachene. Distributed ElGamal à la Pedersen - Application to Helios. In *Workshop on Privacy in the Electronic Society (WPES 2013)*, Berlin, Germany, 2013.

[4] Véronique Cortier, David Galindo, Stéphane Glondu, and Malika Izabachene. Election verifiability for Helios under weaker trust assumptions. In *19th European Symposium on Research in Computer Security (ESORICS'14)*, volume 8713 of *LNCS*, pages 327–344. Springer, 2014.

[5] Véronique Cortier, Pierrick Gaudry, and Stéphane Glondu. Gestion des données sur Belenios. `http://www.belenios.org/data-Belenios-fr.pdf`, 2018.

[6] Véronique Cortier, Pierrick Gaudry, and Stéphane Glondu. *Belenios : A Simple Private and Verifiable Electronic Voting System*, pages 214–238. Springer International Publishing, 2019.

[7] Stéphane Glondu. Belenios specification - Version 1.10. `http://www.belenios.org/specification.pdf`, 2019.

[8] Feng Hao and Peter Y. A. Ryan. *Real-World Electronic Voting : Design, Analysis and Deployment*. Series in Security, Privacy and Trust. Auerbach Publications ;, 2016.