

Tutoriel

Organiser une élection avec

Belenios



Auteurs :

Hassan QAMAR & Hery RAKOTOARISOA

Université de Versailles Saint-Quentin-en-Yvelines – DSIN

Version de ce document 0.8.1 (Mai 2020) pour la version de Belenios 1.10

Sommaire

| | |
|---|-----------|
| Introduction | 1 |
| 1. Gestion automatique confiée entièrement au serveur | 6 |
| 1.1. Préparation d'une élection par l'organisateur | 6 |
| 1.1.2. Préparation de l'élection : Création d'une nouvelle élection..... | 6 |
| 1.1.3. Préparation de l'élection : Choix du mode d'organisation | 6 |
| 1.1.4.1. Préparation de l'élection : Page principale de configuration | 7 |
| 1.1.4.2. Préparation de l'élection : Edition des questions posées aux votant dans l'élection | 8 |
| 1.1.4.3. Préparation de l'élection : Prévisualisation des questions et leur présentation | 9 |
| 1.1.4.4. Préparation de l'élection : Prévisualisation des questions -> Saisie du code de vote | 9 |
| 1.1.4.5. Préparation de l'élection : Prévisualisation des questions -> Réponse aux questions..... | 10 |
| 1.1.4.6. Préparation de l'élection : Prévisualisation des questions -> Récapitulatif et chiffrement..... | 11 |
| 1.1.5.1. Préparation de l'élection : Saisie de la liste électorale (liste des mails des votants) | 12 |
| 1.1.5.2. Préparation de l'élection : Saisie de la liste des mails des votants -> Ajout/Suppression d'adresses mail de votants... | 13 |
| 1.1.6.1. Préparation de l'élection : Génération des codes de vote et envoi par mails aux votants..... | 14 |
| 1.1.6.2. Préparation de l'élection : Téléchargement pour sauvegarde des codes de vote privés (Download private credentials) | 15 |
| 1.1.7.1. Préparation de l'élection : Génération des codes d'authentification et envoi aux votants..... | 16 |
| 1.1.8.1. Préparation de l'élection : Gestion des autorités de déchiffrement (Trustee)..... | 17 |
| 1.1.8.2. Préparation de l'élection : Exemple de modèle de mail envoyé aux autorités de chiffrement..... | 19 |
| 1.1.9.1. Préparation de l'élection : Création de l'élection..... | 20 |
| 1.1.10.1. Administration de l'élection : Nouvelle page d'accueil après la création de l'élection | 21 |
| 1.1.10.2. Administration de l'élection : Régénérer et renvoyer un mot de passe à un votant, et informations diverses | 22 |
| 1.1.11.1. Administration de l'élection : Lancer le comptage des votes..... | 23 |
| 1.1.11.2. Administration de l'élection : Lancer le dépouillement des votes | 24 |
| 1.1.11.2. Administration de l'élection : Visualisation des résultats des votes..... | 25 |
| 1.1.11.3. Administration de l'élection : Publication ou report de publication des résultats des votes..... | 26 |
| 1.1.11.4. Administration de l'élection : Archiver une élection – Supprimer une élection..... | 27 |
| 1.2. Les actions des autorités de déchiffrement (Trustees) | 28 |
| 1.2.1. Avant la création d'élection : réception du lien (mail envoyé par l'organisateur), génération des clés..... | 28 |
| 1.2.2. Dépouillement de l'élection : saisie de la clé privée et la partie de clé globale du déchiffrement propre à chaque autorité | 30 |

| | |
|---|-----------|
| 1.3. Les actions du votant | 33 |
| 1.3.1. Votant : Réception du mail du vote (contenant le lien de l'élection et le code de vote) | 33 |
| 1.3.2. Votant : Cliquer sur le lien de l'élection et commencer la procédure en saisissant le code de vote | 34 |
| 1.3.3. Votant : Voter en répondant aux questions | 35 |
| 1.3.4. Votant : Récapitulatif des votes avant de continuer | 36 |
| 1.3.5. Votant : Connexion avec les codes envoyés par mail (login & mot de passe) | 36 |
| 1.3.6. Votant : Confirmation et dépôt du bulletin dans l'urne | 37 |
| 2. Gestion automatique (serveur) et authentification CAS..... | 39 |
| 3. Gestion manuelle déléguée à une tierce personne et authentification serveur | 40 |
| 4. Gestion manuelle déléguée à une tierce personne et authentification CAS | 1 |

■

Introduction

Objectif de Belenios :

Belenios est une plateforme disponible en ligne qui **vis** à **fournir un système de vote facile à utiliser, garantissant une sécurité à l'état de l'art**, à savoir la **confidentialité** (chiffrement des votes) **et la vérifiabilité des votes** (transparence de l'urne, vérifiabilité et visibilité des bulletins déposés, mais pas leurs contenus chiffrés).

Cette plateforme peut être utilisée dans de nombreux types d'élections : conseils scientifiques, conseils d'administration, référendums, élections locales...

Pour plus d'information : <http://www.belenios.org>

Avertissements :

- ✓ La [plateforme Belenios](http://www.belenios.org) est libre et gratuite. Il s'agit d'une plateforme issue de travaux de recherche et développée par un petit groupe de [chercheurs](#) du centre Inria de Nancy (Loria).
- ✓ Elle est disponible « en l'état » sans aucune garantie de continuité de service et de support car le serveur peut être en maintenance ou victime d'une coupure électrique...
- ✓ Il est fortement recommandé de **bien vous familiariser avec la plateforme et d'organiser des votes tests avant de lancer la « vraie » élection**. Faites une répétition générale (une élection test) avec les personnes concernées (autorités de déchiffrement, générateur de codes de vote) quelques jours avant l'élection.
- ✓ Cette plateforme de vote permet d'organiser des élections avec au plus 1000 électeurs. Au-delà, il est préférable d'installer votre propre serveur en local.
- ✓ Voir le site de Belenios pour son niveau de conformité aux recommandations de la CNIL et au RGPD.

Principe de fonctionnement :

- ✓ **L'organisateur** choisit le mode d'organisation de l'élection et les différents acteurs nécessaires à l'exécution du scrutin (voir ci-dessous). Il crée et paramètre l'élection sur le serveur Belenios selon ces choix et en échanges avec les acteurs concernés pour les différentes étapes, de la création de l'élection jusqu'à sa clôture et la publication des résultats.
- ✓ Pour voter, **un électeur** a besoin d'un **identifiant** et d'un **mot de passe** lui permettant d'être authentifié auprès du serveur. Selon le mode d'organisation choisi (voir ci-dessous), soit c'est le serveur Belenios qui les lui transmet par mail, soit il utilise son identifiant et son mot de passe du système CAS de son établissement.

INTRODUCTION

- ✓ Il a également besoin d'un **code de vote personnel** lui permettant d'exprimer son vote **pour une élection bien précise**. Selon le mode d'organisation choisi, soit c'est le serveur Belenios que le lui transmet, soit une tierce personne autorité de gestion de ces codes.
- ✓ L'électeur reçoit également le **code de l'élection** concernée et **les liens web nécessaires pour voter**.
- ✓ Pour plus de détails, voir sur <http://www.belenios.org/setup.html> (en anglais) et <http://www.belenios.org/organiser-une-election.html> (en français).

Objectif de ce document :

- ✓ Ce document est écrit pour la version en ligne en mai 2020 : **Belenios version 1.10**
- ✓ **Ce document, de version 0.8.1, n'est pas achevé, sa rédaction est en cours.** Cette version 0.8.1 ne traite pour le moment que le cas où les codes de votes (credential) et les codes d'authentification (identifiants et mots de passe) sont générés et envoyés par le serveur Belenios.
- ✓ Nous ne rentrons pas ici les dans détails de Belenios qui sont largement expliqués sur le site web ci-dessus. En revanche, **nous détaillons ici, pas à pas (écran par écran), les différentes étapes de création et de gestion d'une élection sur la plateforme Belenios** pour aider à la prise en main pouvant sembler difficile au premier abord.
- ✓ Ce tutoriel représente notre expérience de simple utilisateur de l'outil Belenios.

Quatre modes d'organisation d'élections possibles :

Les 4 modes suivants constituent les 4 parties de ce document :

1. Gestion automatique totalement confiée au serveur Belenios (**mode par défaut, seul cas traité dans ce document pour le moment**) : La génération et l'envoi des codes de vote (credential) et des codes d'authentification (identifiant et mot de passe) est assuré par le serveur Belenios pour la liste des électeurs déclarés (Credential automatic : authentication Password).
2. Confier la génération et l'envoi des codes de vote (credential) au serveur Belenios, et l'authentification au serveur CAS de l'Université (Credential automatic : authentication-CAS).
3. Confier la génération et l'envoi des codes de vote (credential) à une tierce personne autorité de gestion de ces codes, mais confier au serveur Belenios la génération et l'envoi des codes d'authentification (identifiant et mot de passe) (Credential manual : authentication Password).
4. Confier la génération et l'envoi des codes de vote (credential) à une tierce personne autorité de gestion de ces codes, et l'authentification au serveur CAS de l'Université (Credential manual : authentication CAS).

Nous allons détailler dans ce document ces différents modes d'organisation d'élection pour guider à la fois l'organisateur, le votant et les autorités de déchiffrements.

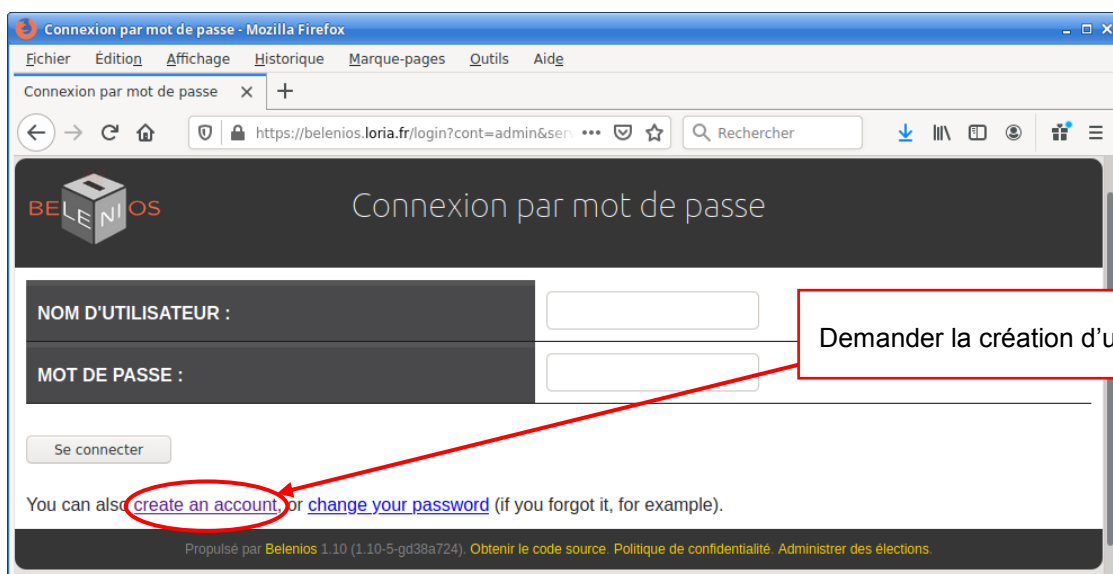
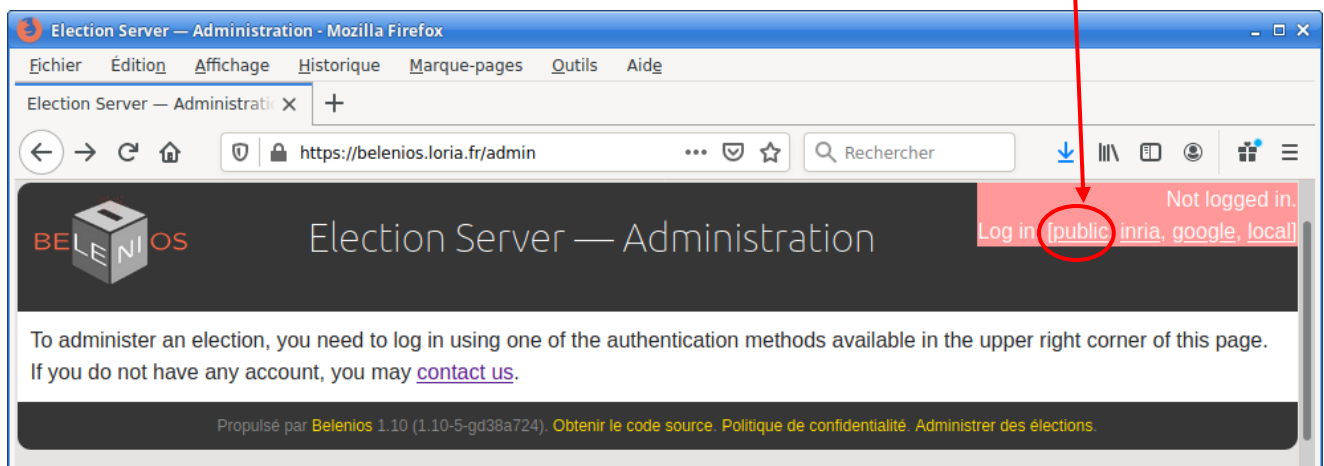
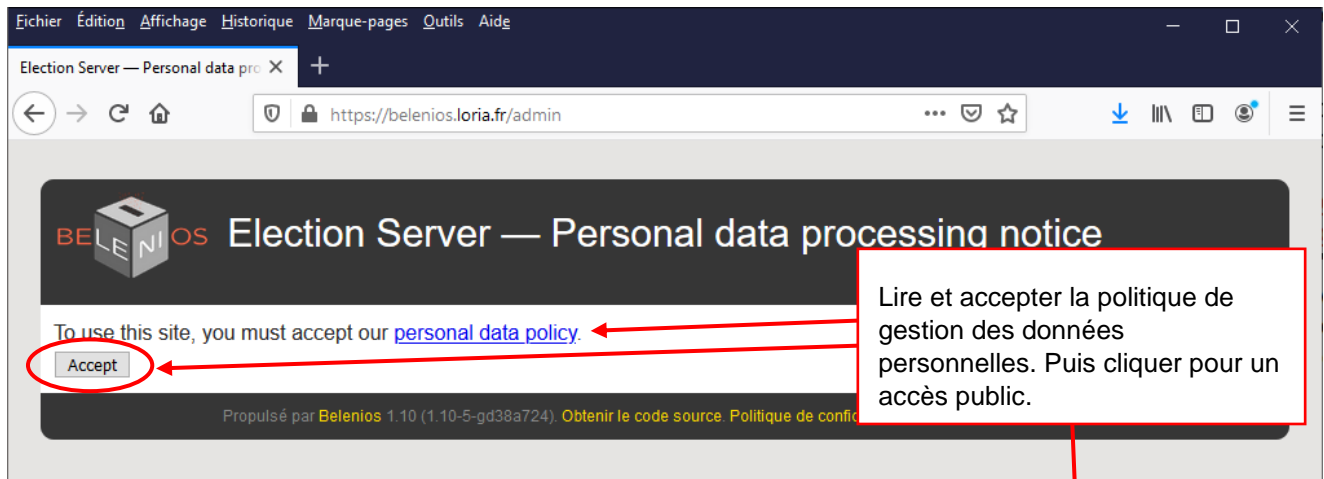
Les acteurs de l'élection :

- ✓ **L'organisateur** de l'élection qui est de fait l'administrateur principal de cette élection sur la plateforme *Belenios*. Cette personne a un ensemble de tâches de préparation, de suivi, de validation, de clôture des votes, de dépouillement... et enfin de publication des résultats. C'est l'organisateur qui **saisit la liste électorale lors de la création de l'élection sur le serveur**.
- ✓ **L'autorité de gestion des codes de votes** quand cette fonction est déléguée par l'organisateur à une tierce personne. Cette autorité est chargée de générer, en dehors du serveur *Belenios*, les codes de vote. Elle est également en charge de l'envoi (et du renvoi si besoin) de ces codes aux électeurs. Cette autorité a de fait un **rôle de contrôle de la liste électorale** saisie par l'organisateur dans le serveur.
- ✓ **Les autorités de déchiffrement** (3 autorités dont le serveur est un bon compromis) préalablement désignées qui vont permettre avec l'organisateur le lancement de l'élection, et à la fin du scrutin, le déchiffrement de l'urne pour faire le dépouillement et publier les résultats de l'élection. Chaque autorité détient une partie de la clé globale de déchiffrement du scrutin. Il faut donc la présence et l'action de chacune et de toutes les autorités pour que le scrutin puisse être dépouillé. Par défaut, le serveur est seul autorité de déchiffrement.
- ✓ **Les votants**.

INTRODUCTION

Pour commencer, l'organisateur doit se créer un compte personnel sur la plateforme pour pouvoir organiser une élection.

Aller sur Belenios : <https://belenios.loria.fr/admin>



INTRODUCTION

The screenshot shows the 'Create an account' page of the Belenios system. The browser address bar shows <https://belenios.loria.fr/signup/?service=public>. The page has a dark header with the Belenios logo and the title 'Create an account'. Below the header, there is a form with two input fields: 'E-mail address' (containing 'hassan.qamar@uvsq.fr') and 'Please enter [captcha] in the following box:' (containing '638647'). A 'Submit' button is at the bottom of the form. Red arrows point from the email field and the captcha box to a text box on the right that says 'Donner votre adresse mail, retaper le code anti-robot affiché.' and 'Envoyer la demande.' Another red arrow points from the 'Submit' button to the same text box. Below the form, there is a footer with the text 'Propulsé par Belenios 1.10 (1.10-5-gd38a724). Obtenir le code source. Politique de confidentialité. Administrer des élections.'

Donner votre adresse mail, retaper le code anti-robot affiché.

Envoyer la demande.

Your e-mail address has been used to create an account on our Belenios server. To confirm this creation, please click on the following link:

<https://belenios.loria.fr/signup/login?token=mrHzdKJGpHt8fBtM9ow3>

or copy and paste it in a web browser.

Warning: this link is valid for 1 day, and previous links sent to this address are no longer valid.

Best regards,

--
Belenios Server

Please choose a username: and a password: .

Type the password again:

Submit

Propulsé par Belenios 1.10 (1.10-5-gd38a724). Obtenir le code source. Politique de confidentialité. Administrer des élections.

Cliquer sur le lien dans le mail envoyé par le serveur pour confirmer la demande.

Entrer un identifiant et un mot de passe de votre choix. Le même mot de passe dans les deux champs et valider.

Le serveur confirme à l'écran la création de votre compte, vous pouvez dorénavant vous connecter :

The screenshot shows the 'Connexion par mot de passe' page of the Belenios system. The browser address bar shows <https://belenios.loria.fr/login?cont=admin&servi...>. The page has a dark header with the Belenios logo and the title 'Connexion par mot de passe'. Below the header, there is a form with two input fields: 'NOM D'UTILISATEUR :' (containing 'votre-identifiant-ici') and 'MOT DE PASSE :' (containing '••••••••'). A 'Se connecter' button is at the bottom of the form. Red arrows point from the username field and the password field to a text box on the right that says 'Taper votre identifiant, votre mot de passe, et vous connecter'. Another red arrow points from the 'Se connecter' button to the same text box. Below the form, there is a footer with the text 'Propulsé par Belenios 1.10 (1.10-5-gd38a724). Obtenir le code source. Politique de confidentialité. Administrer des élections.'

Taper votre identifiant, votre mot de passe, et vous connecter

1

Se connecter

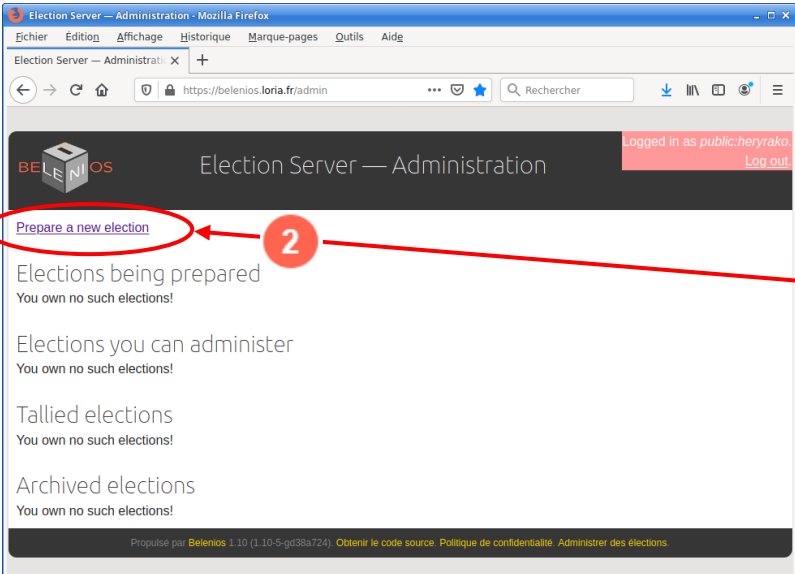
You can also [create an account](#), or [change your password](#) (if you forgot it, for example).

Propulsé par Belenios 1.10 (1.10-5-gd38a724). Obtenir le code source. Politique de confidentialité. Administrer des élections.

1. Gestion automatique confiée entièrement au serveur

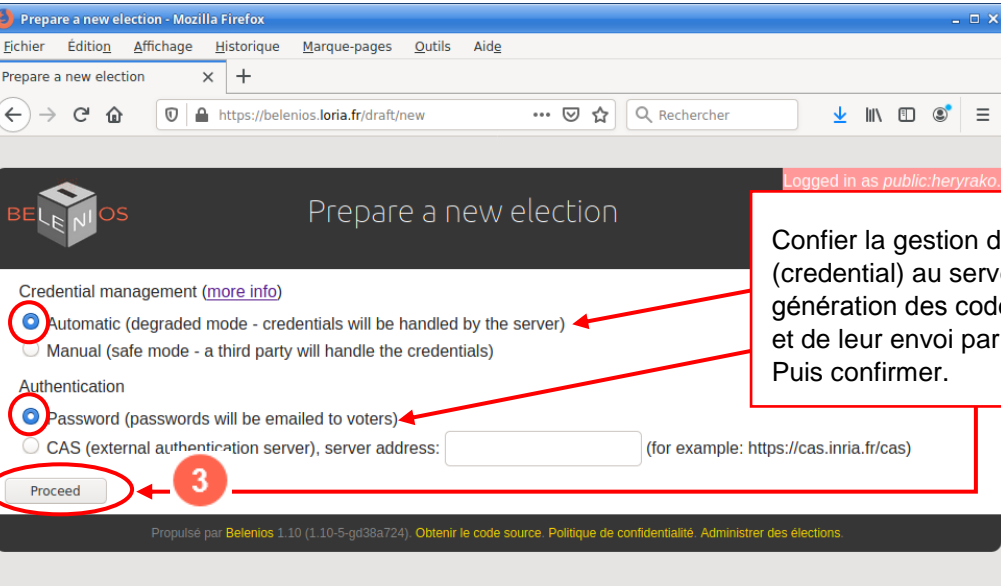
1.1. Préparation d'une élection par l'organisateur

1.1.2. Préparation de l'élection : Création d'une nouvelle élection



Créer une nouvelle élection en cliquant sur « Prepare a new election ».

1.1.3. Préparation de l'élection : Choix du mode d'organisation



Confier la gestion des codes de vote (credential) au serveur, ainsi que la génération des codes d'authentification et de leur envoi par mail aux votants. Puis confirmer.

1.1.4.1. Préparation de l'élection : Page principale de configuration

The screenshot shows the 'Preparation of election Election test 1' page in a Mozilla Firefox browser. The page is divided into several sections, each with a 'Save changes' button. Red callouts with numbers 1 through 7 point to specific elements, and text boxes provide instructions for each step.

- 1. Name and description of the election:** Fields for 'Name of the election' (Election test 1) and 'Description of the election' (Election test 1 (Credential=Automatic Authentication=Password)).
- 2. Languages:** A dropdown menu showing 'fr en' (Available languages: en fr de ro it).
- 3. Contact:** A text field for 'Contact' (ici-mail-organisateur@dd.pp).
- 4. Edit questions:** A link to edit the election questions.
- 5. Edit voters:** A link to edit the list of voters.
- 6. Credentials:** A section with a warning 'Warning: this will freeze the voter list!' and a 'Generate on server' button.
- 7. Authentication:** A section with 'Authentication scheme: password' and a 'Generate and mail missing passwords' button.

Additional callouts and text boxes provide further instructions:

- Compéter le nom et la description de votre élection. Puis les enregistrer.** (Points to the Name and description section)
- Choisir la (ou les) langue(s) souhaitée(s), dans l'ordre, pour les messages envoyés aux votants. Dans cet exemple : français et anglais dans cet ordre. Enregistrer.** (Points to the Languages section)
- Saisir l'adresse mail de l'organisateur, contact indiqué aux votants dans les messages qu'ils reçoivent. Enregistrer.** (Points to the Contact section)
- Éditer les questions de l'élection (Voir la suite paragraphe 1.1.4.2.). « Copier » ce code, vous aurez besoin de le « Coller » pour la prévisualisation des questions.** (Points to the Edit questions link and the credential code HsqB3C3y62Ekq4D)
- Saisir les adresses mail des votants (Voir la suite paragraphe 1.1.5.1.).** (Points to the Edit voters link)
- Faire générer par le serveur les codes de vote et les faire envoyer par mail aux votants (Voir la suite parag. 1.1.6.1). Si déjà fait, télécharger les paires Mail/Code des votants (Voir la suite parag. 1.1.6.2.).** (Points to the Generate on server button and the Download private credentials link)
- Faire générer par le serveur les codes d'authentification et les faire envoyer par mail aux votants, par le serveur (Voir la suite parag. 1.1.7.1.).** (Points to the Generate and mail missing passwords button)

1. GESTION AUTOMATIQUE CONFIEE ENTIEREMENT AU SERVEUR

1.1.4.2. Préparation de l'élection : Edition des questions posées aux votant dans l'élection

Écrans après le clic **4** Renseignez les champs du formulaire de création/suppression de questions. Il est assez simple. Nous mentionnons sur cette capture uniquement les points différents :

Questions for election Election test 1
Credential=Automatic Authentication=Password

Logged in as *public:heryako*. [Log out](#)

Alternative voting methods (warning, still experimental):
You may wish voters to rank candidates or give each candidate a score (e.g. Condorcet, STV, majority judgement).
Note that:
1. the after-the-vote procedure will require more steps;
2. you will be given the raw results (shuffled list of ballots) and you will need to apply your counting method yourself.
☐ Tick the box to activate this mode.

Question: D'accord avec le compte-rendu de la dernière réunion ? Remove Insert

The voter has to choose between 1 and 1 answers.

☒ Blank vote is allowed

Answer: Oui Remove Insert

Answer: Non Remove Insert

Add an answer

Question: Quelles couleurs pour la couverture ? (3 choix possibles maximum) Remove Insert

The voter has to choose between 1 and 3 answers.

☐ Blank vote is allowed

Answer: Blanc Remove Insert

Answer: Jaune Remove Insert

Answer: Rouge Remove Insert

Answer: Vert Remove Insert

Answer: Bleu Remove Insert

Answer: Noir Remove Insert

Add an answer

Add a question

Save changes

[Preview booth](#) you can use any credential such as HsqB3C3y62Ekq4D.

Propulsé par Belenios 1.10 (1.10-5-gd38a724). [Obtenir le code source](#). [Politique de confidentialité](#). [Administrer des élections](#).

Saisir la question, le nombre de réponses autorisées (ici : une seule, choix exclusif), et autoriser ou non le vote blanc (ici oui).

Supprimer cette question, ou en insérer une autre juste avant.

Saisir les réponses à choisir.
Supprimer cette réponse ou en insérer une autre avant.

En rajouter autre une après.

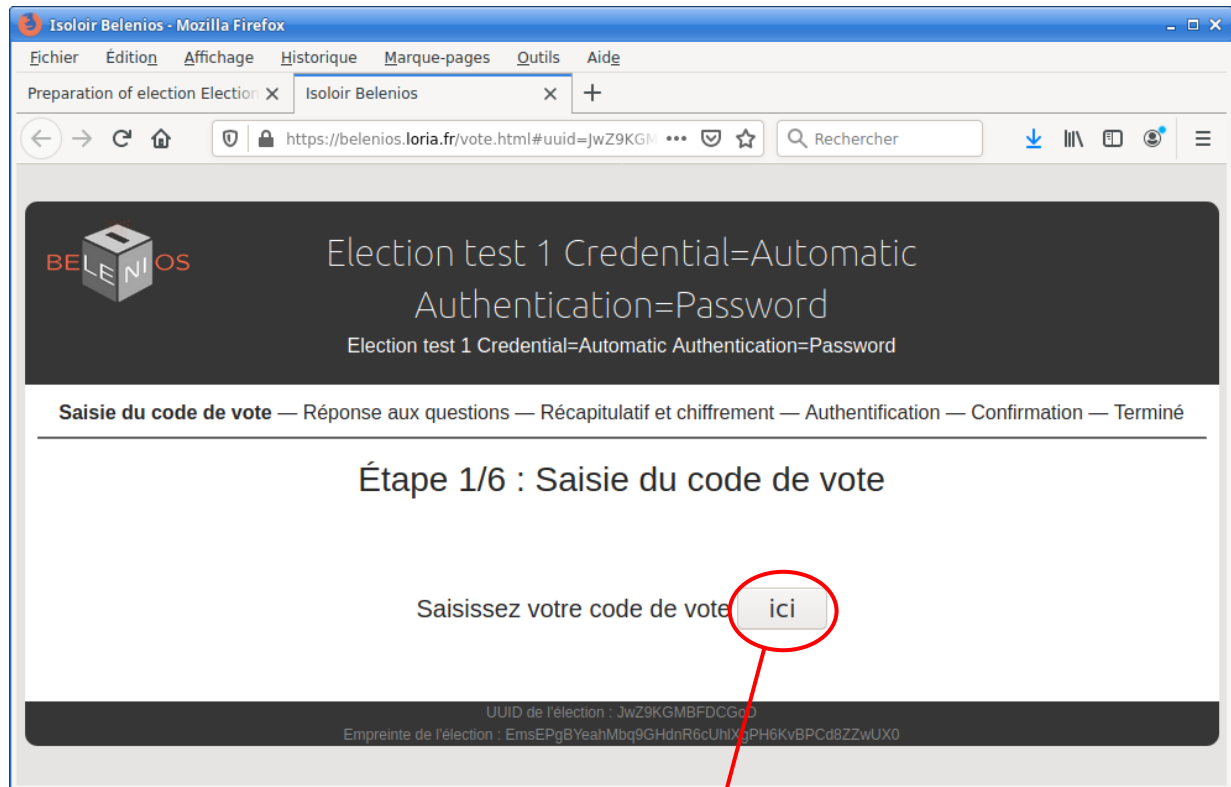
Pour cet exemple, question à choix multiple : de 1 à 3 réponses autorisées. Vote blanc non autorisé.

« Copier » ce code, à « Coller » pour la prévisualisation (voir le paragraphe [1.1.4.3.](#))

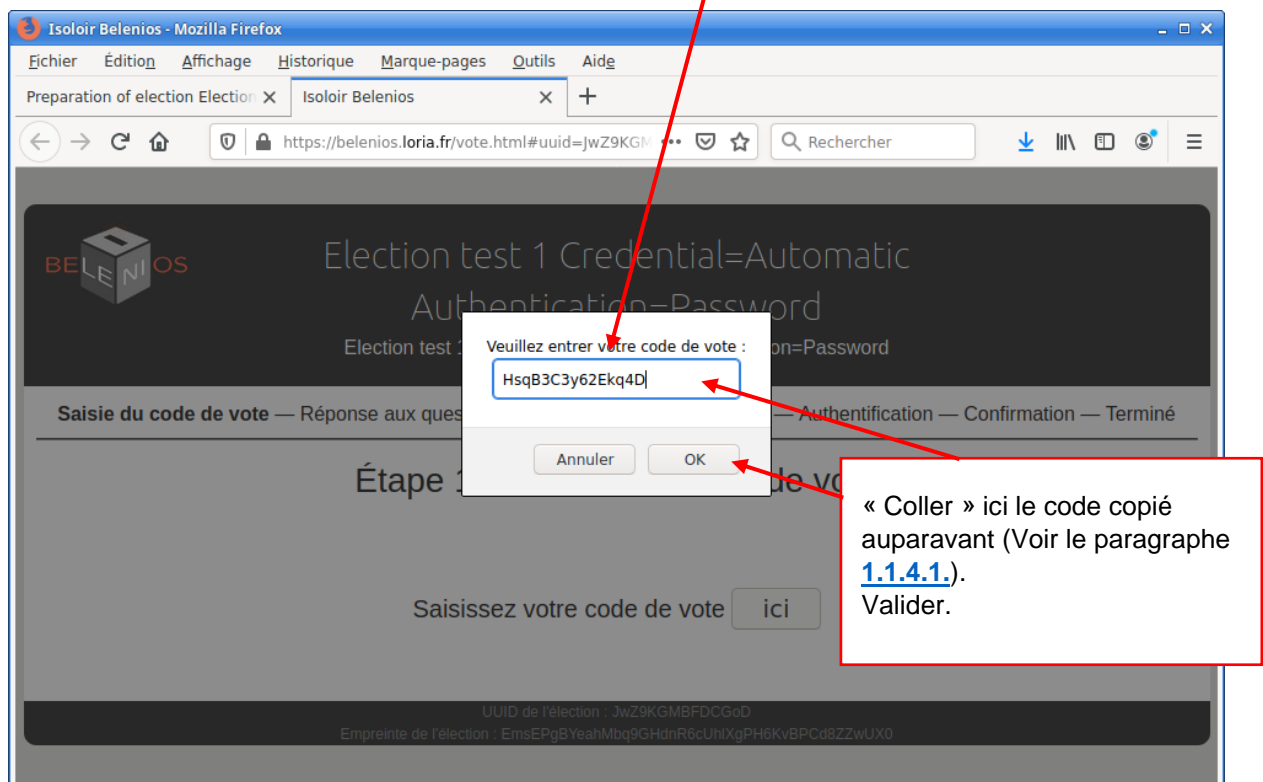
Prévisualiser les questions et leur présentation aux votants

1. GESTION AUTOMATIQUE CONFIEE ENTIEREMENT AU SERVEUR

1.1.4.3. Préparation de l'élection : Prévisualisation des questions et leur présentation



1.1.4.4. Préparation de l'élection : Prévisualisation des questions -> Saisie du code de vote



1.1.4.5. Préparation de l'élection : Prévisualisation des questions -> Réponse aux questions

The screenshot shows the Belenios web interface in a Mozilla Firefox browser. The page title is 'Election test 1 Credential=Automatic Authentication=Password'. The navigation bar includes 'Saisie du code de vote', 'Réponse aux questions' (highlighted), 'Récapitulatif et chiffrement', 'Authentification', 'Confirmation', and 'Terminé'. The main heading is 'Étape 2/6 : Réponse aux questions'. The question is 'D'accord avec le compte-rendu de la dernière réunion ?'. Below it, 'Question 1/2 — sélectionnez entre 1 et 1 réponse(s)'. The options are 'Oui' (checked), 'Non', and 'Vote blanc'. A red circle highlights the 'Suivant' button. At the bottom, the UUID and Empreinte de l'élection are displayed.

The screenshot shows the Belenios web interface in a Mozilla Firefox browser. The page title is 'Election test 1 Credential=Automatic Authentication=Password'. The navigation bar includes 'Saisie du code de vote', 'Réponse aux questions' (highlighted), 'Récapitulatif et chiffrement', 'Authentification', 'Confirmation', and 'Terminé'. The main heading is 'Étape 2/6 : Réponse aux questions'. The question is 'Quelles couleurs pour la couverture ? (3 choix possibles maximum)'. Below it, 'Question 2/2 — sélectionnez entre 1 et 3 réponse(s)'. The options are 'Blanc' (checked), 'Jaune', 'Rouge', 'Vert' (checked), 'Bleu' (checked), and 'Noir'. A red circle highlights the 'Suivant' button. At the bottom, the UUID and Empreinte de l'élection are displayed.

1.1.4.6. Préparation de l'élection : Prévisualisation des questions -> Récapitulatif et chiffrement

The screenshot shows the Belenios web interface in a Mozilla Firefox browser. The page title is 'Election test 1 Credential=Automatic Authentication=Password'. The URL is 'https://belenios.loria.fr/vote.html#uuid=JwZ9KGM'. The page is divided into several sections:

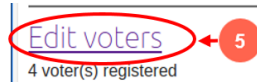
- Navigation bar:** Saisie du code de vote — Réponse aux questions — **Récapitulatif et chiffrement** — Authentification — Confirmation — Terminé
- Section Header:** Étape 3/6 : Récapitulatif et chiffrement
- Questions:**
 - D'accord avec le compte-rendu de la dernière réunion ?
 - Oui
 - Quelles couleurs pour la couverture ? (3 choix possibles maximum)
 - Blanc
 - Vert
 - Bleu
- Confirmation:**

Votre bulletin a été chiffré avec succès, **mais n'a pas encore été déposé dans l'urne !**
Votre numéro de suivi est **QslysCD3ME8yY1C3cB89EUPSJFUaNBriPEFvHlwUF8**
Nous vous invitons à le sauvegarder afin de vérifier ultérieurement que votre vote est bien pris en compte
- Buttons:** A 'Continuer' button is highlighted with a red oval, and a 'Recommencer' button is below it.
- Footer:** UUID de l'élection : JwZ9KGMBCFDCGoD
Empreinte de l'élection : EmsEPgBYeahMbq9GHdnR6cUhlXgPH6KvBPCd8ZZwUX0

Fin de la prévisualisation.■

1.1.5.1. Préparation de l'élection : Saisie de la liste électorale (liste des mails des votants)

Écrans après avoir cliqué sur le lien



Voters for election Election test 1
Credential=Automatic Authentication=Password

Logged in as *public:heryako.* [Log out.](#)

[Return to draft page](#)
[Import voters from another election](#)

No voters
Please enter the identities of voters to add, one per line (max 2000).
Warning: you have to make sure that these email addresses are valid. You won't be able to change the email addresses once the election is set up. Voters with invalid email addresses won't be able to vote.

adresse.mail01@uvsq.fr
adresse.mail02@uvsq.fr
une.autre@gmail.com
another.adress@gmail.com

[Add](#)

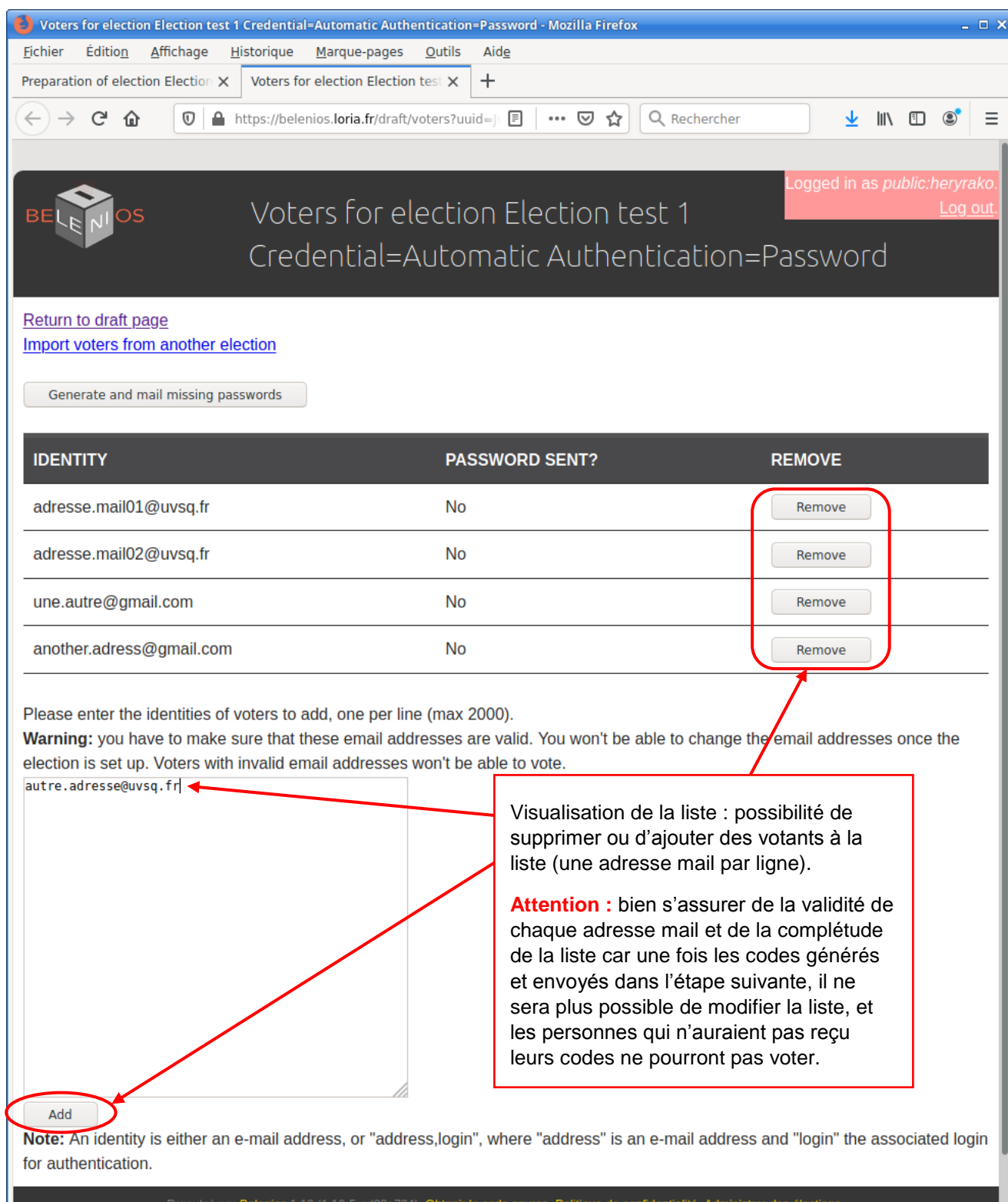
Note: An identity is either an e-mail address, or "address,login", where "address" is an e-mail address and "login" the associated login for authentication.

Propulsé par **Belenios 1.10** (1.10-5-gd38a724). [Obtenir le code source](#). [Politique de confidentialité](#). [Administrer des élections](#).

Vous pouvez importer une liste électorale (liste de mails) depuis une autre élection organisée auparavant ...

... et/ou saisir manuellement une liste d'adresses mail, une adresse par ligne. Et les ajouter à la liste électorale.

1.1.5.2. Préparation de l'élection : Saisie de la liste des mails des votants -> Ajout/Suppression d'adresses mail de votants



Voters for election Election test 1 Credential=Automatic Authentication=Password

Logged in as *public:heryako.* [Log out.](#)

[Return to draft page](#)
[Import voters from another election](#)

[Generate and mail missing passwords](#)

| IDENTITY | PASSWORD SENT? | REMOVE |
|--------------------------|----------------|------------------------|
| adresse.mail01@uvsq.fr | No | Remove |
| adresse.mail02@uvsq.fr | No | Remove |
| une.autre@gmail.com | No | Remove |
| another.adress@gmail.com | No | Remove |

Please enter the identities of voters to add, one per line (max 2000).
Warning: you have to make sure that these email addresses are valid. You won't be able to change the email addresses once the election is set up. Voters with invalid email addresses won't be able to vote.

autre.adresse@uvsq.fr

[Add](#)

Attention : bien s'assurer de la validité de chaque adresse mail et de la complétude de la liste car une fois les codes générés et envoyés dans l'étape suivante, il ne sera plus possible de modifier la liste, et les personnes qui n'auraient pas reçu leurs codes ne pourront pas voter.

Note: An identity is either an e-mail address, or "address,login", where "address" is an e-mail address and "login" the associated login for authentication.

1. GESTION AUTOMATIQUE CONFIEE ENTIEREMENT AU SERVEUR

1.1.6.1. Préparation de l'élection : Génération des codes de vote et envoi par mails aux votants

Écrans après avoir cliqué sur le bouton

Credentials

Warning: this will freeze the voter list

Generate on server

6

Voters for election Election test 1 - Mozilla Firefox

https://belenios.loria.fr/draft/voters?uuid=j

Logged in as public:heryako. Log out.

Return to draft page

Import voters from another election

Generate and mail missing passwords

6

| IDENTITY | PASSWORD SENT? | REMOVE |
|--------------------------|----------------|--------|
| adresse.mail01@uvsq.fr | No | Remove |
| une.autre@gmail.com | No | Remove |
| another.adress@gmail.com | No | Remove |
| autre.adresse@uvsq.fr | No | Remove |

Please enter the identities of voters to add, one per line (max 2000).

Warning: you have to make sure that these email addresses are valid. You won't be able to change the email addresses once the election is set up. Voters with invalid email addresses won't be able to vote.

Add

Note: An identity is either for authentication.

Faire générer les codes de votes, et les faire envoyer par le serveur par mails aux votants.

Success - Mozilla Firefox

https://belenios.loria.fr/draft/election?uuid=j

Success

Credentials have been generated and mailed! You should download private credentials (and store them securely), in case someone loses his/her credential.

Proceed

C'est fait avec succès, continuer.

1.1.6.2. Préparation de l'élection : Téléchargement pour sauvegarde des codes de vote privés (Download private credentials)

De l'écran principal de l'élection :

Preparation of election Election test 1 - Mozilla Firefox

Logged in as public:heryrako. Log out.

Name and description of the election

Name of the election: Election test 1

Description of the election: Election test 1 (Credential=Automatic Authentication=Password)

Save changes

Languages

Languages: fr en (Available languages: en fr de ro it)

This is a space-separated list of languages that will be used in emails sent by the server.

Save changes

Contact

Contact: ici-mail-organisateur@dd.pp

This contact will be added to emails sent to the voters.

Save changes

[Edit questions](#)

[Preview booth](#) (you can use any credential such as HsqB3C3y62Ekq4D).

[Edit voters](#)

4 voter(s) registered

Credentials

Credentials have already been generated!

[Download private credentials](#)

Authentication

Authentication scheme: password

Generate and mail missing passwords

Trustees

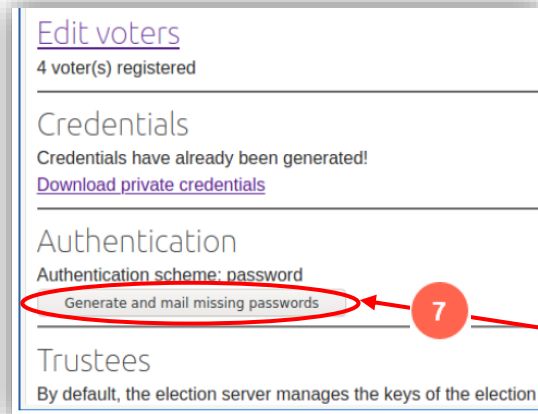
By default, the election server manages the keys of the election (degraded privacy mode). For real elections, the key must be shared

Cliquer pour obtenir les paires Mail/Code-de-vote, à sauvegarder en local sur l'ordinateur de l'organisateur de l'élection. Cela peut servir dans le cas où un votant perd son code de vote afin de le lui renvoyer à nouveau.

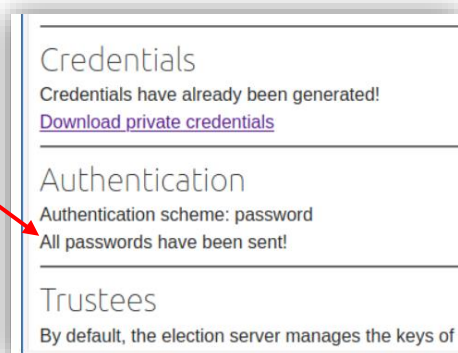
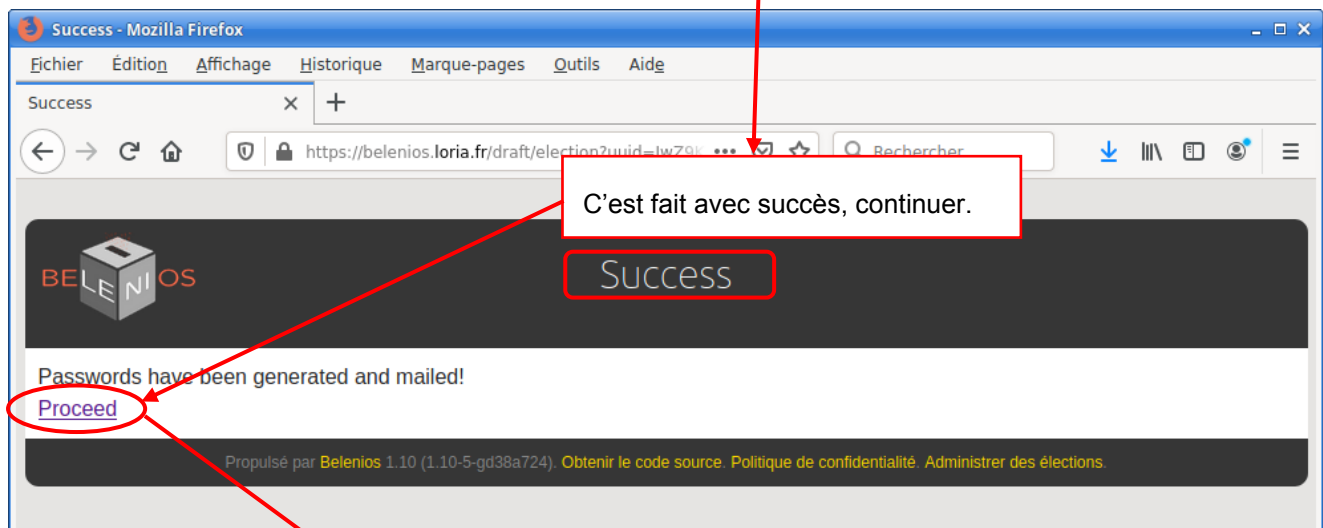
| | |
|--------------------------|-----------------|
| adresse.mail01@uvsq.fr | qUh8fkAZ4gtSHLR |
| une.autre@gmail.com | 8EQ25uRKpMBmvPW |
| another.adress@gmail.com | c8TAD658LDtNQqh |
| autre.adresse@uvsq.fr | L7PLSgZsFRK9PbS |

1.1.7.1. Préparation de l'élection : Génération des codes d'authentification et envoi aux votants

De l'écran principal de l'élection :



Faire générer les codes d'authentification et les faire envoyer par le serveur par mails aux votants.



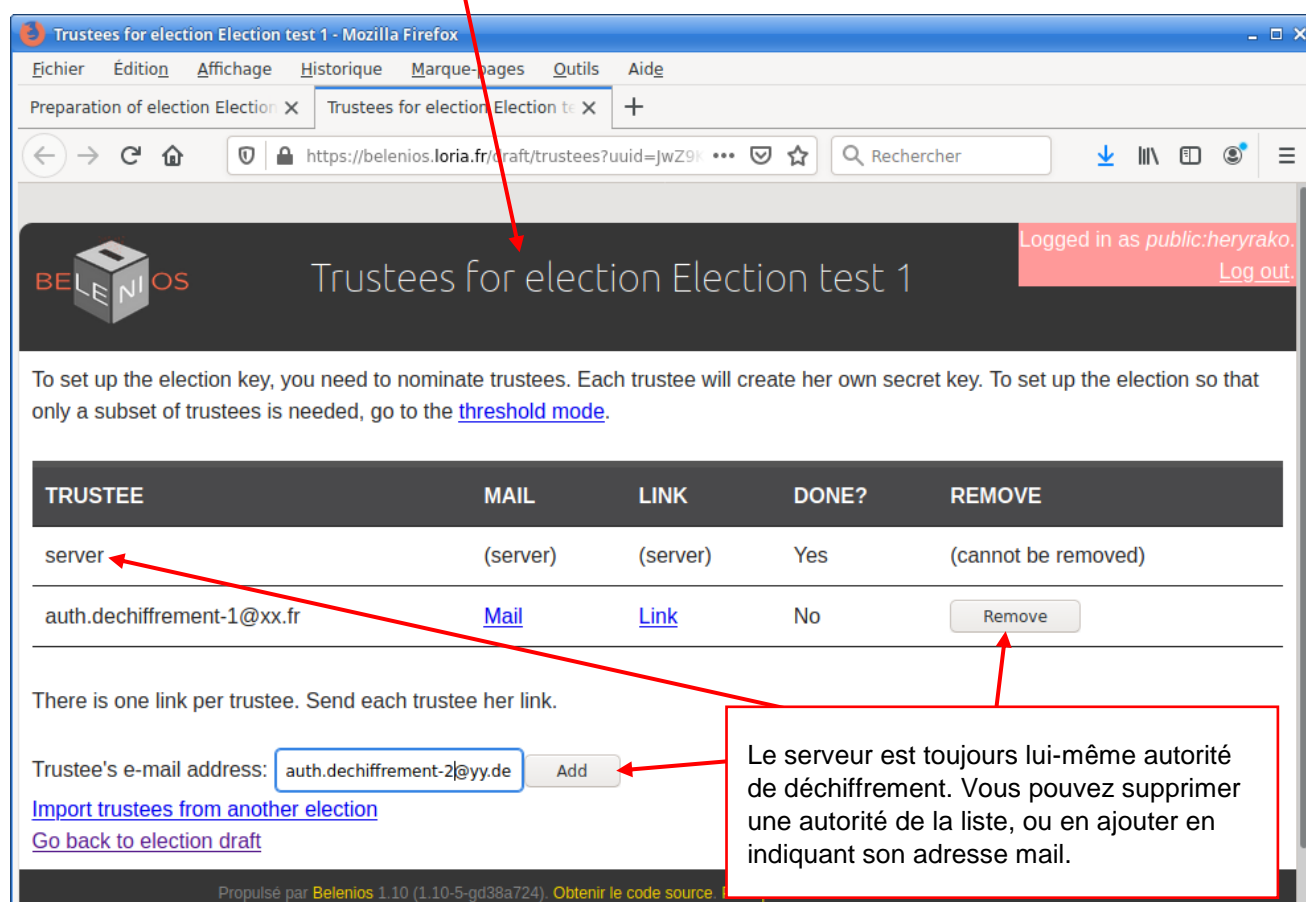
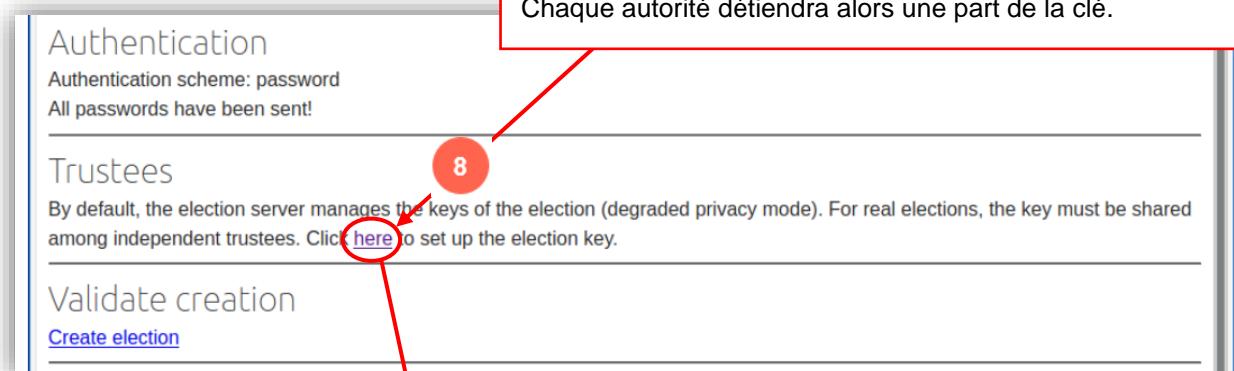
Retour sur écran principal de l'élection :

1.1.8.1. Préparation de l'élection : Gestion des autorités de déchiffrement (Trustee)

On parle ici d'autorités de déchiffrement, mais ce sont bien sûr les mêmes autorités détenant les clés qui seront aussi les autorités de dépouillement de l'élection.

De l'écran principal de l'élection :

Par défaut, la seule autorité de déchiffrement est le serveur qui détient donc seul la clé de déchiffrement. Pour ajouter d'autres autorités, cliquer ici. Chaque autorité détiendra alors une part de la clé.



1. GESTION AUTOMATIQUE CONFIEE ENTIEREMENT AU SERVEUR

Trustees for election Election test 1 - Mozilla Firefox

Preparation of election Election test 1 x Trustees for election Election test 1 x +

https://belenios.loria.fr/draft/trustee?token=oxdzK7F8Rv3PZz&uuid=JwZ9KGMBFDCGoD

Logged in as public:heryako. Log out.

Trustees for election Election test 1

To set up the election key, you need to nominate trustees. Each trustee will create her own secret key. To set up the election so that only a subset of trustees is needed, go to the [threshold mode](#).

| TRUSTEE | MAIL | LINK | DONE? | REMOVE |
|---|----------------------|---------------------------|-------|-------------------------|
| server | (server) | (server) | Yes | (cannot be removed) |
| auth.dechiffrement-1@xx.fr | Mail | Hide link | No | <button>Remove</button> |
| The link that must be sent to trustee auth.dechiffrement-1@xx.fr is: https://belenios.loria.fr/draft/trustee?token=oxdzK7F8Rv3PZz&uuid=JwZ9KGMBFDCGoD | | | | |
| auth.dechiffrement-2@yy.de | Mail | Link | NO | <button>Remove</button> |

There is one link per trustee. Send each trustee her link.

Trustee's e-mail address: Add

[Import trustees from another election](#)
[Go back to election draft](#)

Propulsé par Belenios 1.10 (1.10-5-gd38a724). Obtenir le

Cacher ou afficher le lien web à transmettre à chaque autorité.

Lien web à transmettre par mail par l'organisateur de l'élection à l'autorité (auth.dechiffrement-1@xx.fr sur cet exemple) pour qu'elle puisse générer elle-même, garder secret et mettre en sécurité sa part privée de la clé de chiffrement de l'élection.

En cliquant sur « Mail », une fenêtre de rédaction d'un nouveau mail de votre logiciel de courrier électronique par défaut s'ouvre, pré-remplie avec une proposition de texte (en anglais, voir ci-dessous) contenant le lien web à transmettre à l'autorité correspondante. Ce mail doit donner à l'autorité toutes les instructions pour générer sa part de la clé privée et transmettre au serveur la clé publique correspondante utilisée pour le chiffrement de l'élection.

Vous pouvez bien sûr modifier le contenu de ce mail (le traduire en français par exemple) avant de l'envoyer à l'autorité, mais il doit contenir le lien web et toutes les instructions nécessaires. S'assurer par la suite auprès de l'autorité qu'elle a bien reçu ce mail.

Tant que chacune des autorités de déchiffrement n'a pas accompli entièrement la procédure qui lui est demandée dans ce mail (aboutissant à l'envoi de sa clé publique au serveur), l'élection ne pourra pas être créée par l'organisateur.

1.1.8.2. Préparation de l'élection : Exemple de modèle de mail envoyé aux autorités de chiffrement

Nom : Organisateur Election test1 Adresse : ici-mail-organisateur@dd.pp

Répondre à : ici-mail-organisateur@dd.pp

À : auth.dechiffrement-1@xx.fr

Cc : ici-mail-organisateur@dd.pp

Cci :

Objet : Link to generate the decryption key

Texte simple Normal

Dear trustee,

You will find below the link to generate your private decryption key, used to tally the election.

<https://belenios.loria.fr/draft/trustee?token=oxdzK7F8Rv3PZz&uuid=JwZ9KGMBFDCGoD>

Here's the instructions:

1. click on the link
2. click on "generate a new key pair"
3. your private key will appear in another window or tab. Make sure you SAVE IT properly otherwise it will not possible to tally and the election will be canceled.
4. in the first window, click on "submit" to send the public part of your key, used encrypt the votes. For verification purposes, you should save this part (that starts with {"pok":{"challenge":}) , for example sending yourself an email.

Regarding your private key, it is crucial you save it (otherwise the election will be canceled) and store it securely (if your private key is known together with the private keys of the other trustees, then vote privacy is no longer guaranteed). We suggest two options:

1. you may store the key on a USB stick and store it in a safe.
2. Or you may simply print it and store it in a safe.

Of course, more cryptographic solutions are welcome as well.

Thank you for your help,

--
The election administrator.
--

L'autorité de chiffrement devra cliquer sur ce lien et suivre la procédure décrite dans ce mail afin que l'organisateur puisse procéder à la création de l'élection.

Sinon l'élection ne pourra être créée (voir ci-dessous clic 9).

On aura « Missing » sur la page de création finale de l'élection si l'une des autorités de déchiffrement n'a pas accompli la procédure correctement :

BELENIOS Election Election test 1 — Validate creation

Logged in as public:heryrako Log out

[Return to draft page](#)

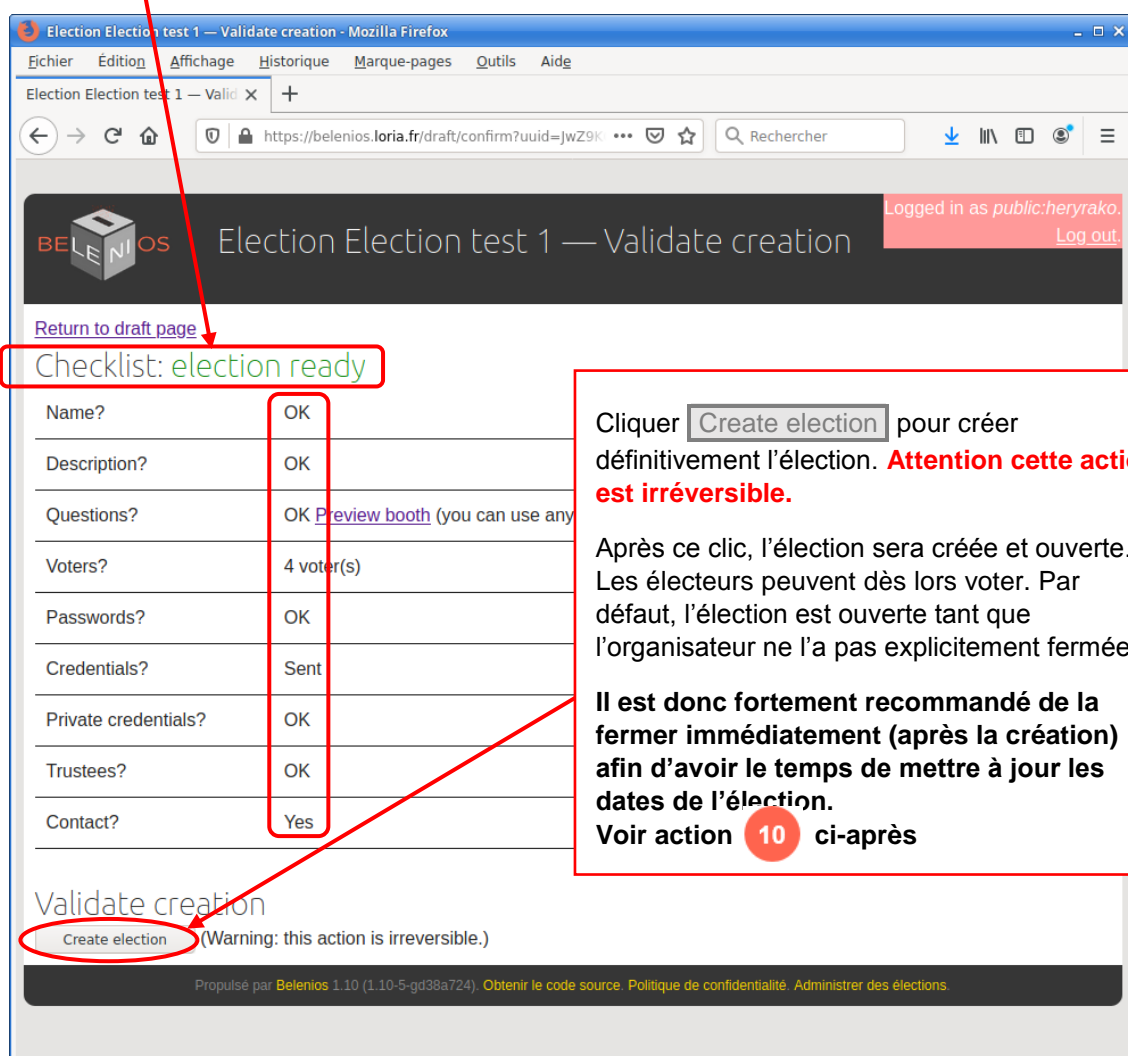
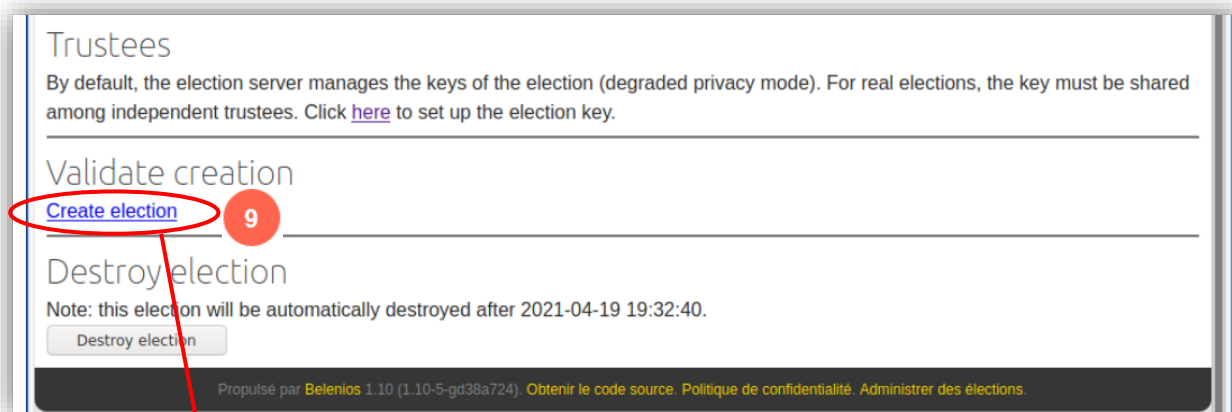
Checklist: election not ready

| | |
|----------------------|--|
| Name? | OK |
| Description? | OK |
| Questions? | OK Preview booth (you can use any credential such as HsqB3C3y62Ekq4D). |
| Voters? | 4 voter(s) |
| Passwords? | OK |
| Credentials? | Sent |
| Private credentials? | OK |
| Trustees? | Missing |
| Contact? | Yes |

Proposé par Belenios 1.10 (d.10-5-gd38e724). Obtenir le code source. Politique de confidentialité. Administrateur des élections.

1.1.9.1. Préparation de l'élection : Création de l'élection

Une fois les autorités de déchiffrement ont accompli leur procédure et que toutes les autres conditions sont remplies (OK), l'organisateur peut enfin valider et créer l'élection de la page principale de l'élection :



1.1.10.1. Administration de l'élection : Nouvelle page d'accueil après la création de l'élection

The screenshot shows the 'Election test 1 — Administration' page in a Mozilla Firefox browser. The page is logged in as 'public:heryako'. The main content area shows the election status as 'The election is open. Voters can vote.' A red circle with the number '10' highlights the 'Close election' button. Below this, there are fields for 'Automatically open the election at:' and 'Automatically close the election at:', both with date and time pickers. A red box highlights the format 'YYYY-MM-DD HH:MM:SS' in the instructions. At the bottom, there are buttons for 'Archive election' and 'Delete election', both with warning messages.

10 Fermer l'élection pour saisir d'abord ses dates et heures d'ouverture et de fermeture automatiques au format indiqué. Laisser vide si vous ne souhaitez pas mettre de dates.

Attention les dates et heures à saisir ici doivent être en UTC. Le serveur indique pour information sur la ligne « **Note** » l'heure locale pour lui. Si vous êtes en France métropolitaine, en heure d'été, mettre l'heure de Paris moins 2 heures. En heure d'hiver, mettre l'heure de Paris moins 1 heure.

Valider les dates et heures une fois saisies.

The screenshot shows the 'Election test 1 — Administration' page in a Mozilla Firefox browser. The page is logged in as 'public:heryako'. The main content area shows the election status as 'The election is closed. No one can vote.' A red circle highlights the 'Open election' button. Below this, there are fields for 'Automatically open the election at:' and 'Automatically close the election at:', both with date and time pickers. A red box highlights the format 'YYYY-MM-DD HH:MM:SS' in the instructions. At the bottom, there is a button for 'Change automatic dates'.

Puis rouvrir l'élection.

Dans cet exemple, l'élection a été ouverte du 22 avril 2020 à 23h00m01s au 23 avril 2020 à 23h59m59s heures de Paris (pour nous ☺).

1. GESTION AUTOMATIQUE CONFIEE ENTIEREMENT AU SERVEUR

1.1.10.2. Administration de l'élection : Régénérer et renvoyer un mot de passe à un votant, et informations diverses

The screenshot shows the 'Election test 1 — Administration' page in a Mozilla Firefox browser. The page is logged in as 'public:heryako'. The main navigation menu includes links for 'Election home', 'Voter list', 'Voting records', 'Missing voters', and 'Regenerate and mail a password'. A red box highlights the 'Regenerate and mail a password' link. A red arrow points from this link to a second screenshot below. A red box also highlights the 'Voter list', 'Voting records', and 'Missing voters' links, with a text box explaining they show the voter list, those who have voted, and those who haven't, respectively. Another red box highlights the 'The election is closed. No one can vote.' message, with a text box explaining that when the election is closed manually or automatically, this button appears and voting is no longer possible. A third red box highlights the 'Proceed to vote counting' button, with a text box explaining that this action is irreversible and definitively closes the election.

Afficher respectivement : la liste électorale, la liste de celles/ceux ayant déjà voté (avec les dates et heures du vote), et la liste de celles/ceux n'ayant pas encore voté.

The election is closed. No one can vote.

Lorsque l'élection est fermée, manuellement par l'organisateur ou automatiquement par la date de fermeture fixée, ce bouton apparaît et le comptage devient donc possible. Voir action ci-dessous.

Proceed to vote counting Warning: this action is irreversible; the election will be definitively closed.

The screenshot shows the 'Regenerate and mail password' page in a Mozilla Firefox browser. The page is logged in as 'public:heryako'. The main heading is 'Regenerate and mail password'. There is a form with a 'Username:' label and a text input field. Below the input field is a 'Submit' button. A red box highlights the 'Submit' button, with a text box explaining that in case of need, the password can be regenerated and sent to the voter by entering their email and clicking the button.

En cas de besoin, vous pouvez régénérer et renvoyer le mot de passe d'un votant en tapant son mail et en validant.

1. GESTION AUTOMATIQUE CONFIEE ENTIEREMENT AU SERVEUR

1.1.11.1. Administration de l'élection : Lancer le comptage des votes

Proceed to vote counting

Warning: this action is irreversible and will definitively close the election.

11

Procéder au comptage. Attention cette action est irréversible et fermera définitivement les votes.

Election test 1 — Administration - Mozilla Firefox

Logged in as public:heryrako

Election test 1 — Administration

View the encrypted tally

The encrypted tally has been computed. Its hash is ua2S4Yftadvwaf4q7jCFO7k+lguzbKI2hAyVaTlaJac. We are now waiting for trustees...

TRUSTEE

server

nom1.prénom1@uvsq.fr

nom2.prénom2@uvsq.fr

Compute the result

Archive election

Warning: this action is irreversible. A definitively closed (no vote submission, no vote counting).

This election will be automatically deleted after 2021-04-19

Delete election

Warning: this action is irreversible.

Propulsé par Belenios 1.10 (1.10-5-gd38a724). Ob

En-têtes

En-têtes de réponse

Accept-Ranges bytes

Connection keep-alive

Content-Length 11306

Content-Type application/json

Date Sun, 19 Apr 2020 22:34:34 GMT

ETag "2c2a-22d87-1587335519.979829"

Last-Modified Sun, 19 Apr 2020 22:31:59 GMT

Server nginx/1.14.2

X-Elion-Set-Process-Cookies [0]

En-têtes de requête

Accept text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Encoding gzip, deflate, br

Accept-Language fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3

Connection keep-alive

DNT 1

Host belenios.loria.fr

If-Modified-Since Sun, 19 Apr 2020 22:31:59 GMT

If-None-Match "2c2a-22d87-1587335519.979829"

Referer https://belenios.loria.fr/election/admin?uuid=JwZ9KGMBCGoD

Upgrade-Insecure-Requests 1

User-Agent Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0

1. GESTION AUTOMATIQUE CONFIEE ENTIEREMENT AU SERVEUR

1.1.11.2. Administration de l'élection : Lancer le dépouillement des votes

The screenshot shows the 'Election test 1 — Administration' page in a Mozilla Firefox browser. The page header includes the Belenios logo and the title 'Election test 1 — Administration'. A red box highlights the login status: 'Logged in as public:heryrako' with a 'Log out' link.

Navigation links on the left include: Election home, Voter list, Voting records, Missing voters, and Regenerate and mail a password.

A message states: 'The encrypted tally has been computed. Its hash is ua2S4Yftadvwaf4q7jCFO7k+lguzbKI2hAyVaTlaJac. We are now waiting for trustees...'.

A table lists trustees with columns: TRUSTEE, MAIL, LINK, and DONE?. The first row shows 'server' with '(server)' in the MAIL and LINK columns and 'Yes' in the DONE? column. The second row shows 'nom1.prénom1@uvsq.fr' with a 'Mail' link. The third row shows 'nom2.prénom2@uvsq.fr' with a 'Mail' link.

A red box highlights the 'Compute the result' button. Another red box highlights the URL: 'https://belenios.loria.fr/election/trustees?token=2&uuid=JwZ9KGMBFDCGoD'.

At the bottom, there are buttons for 'Archive election' and 'Delete election', both with warning messages. A footer bar contains the text: 'Propulsé par Belenios 1.10 (10-5-gd38a724) Obtenir le code source Politique de confidentialité Administrer des élections'.

Annotations in red boxes provide instructions:

- En attente de l'action de déchiffrement par l'ensemble des autorités de déchiffrement avec leurs clés.
- En cliquant sur « Mail », même remarque que dans le paragraphe 1.1.8.1., pour l'envoi du lien par mail à faire pour chaque autorité (deux pour cet exemple).
- Lien à envoyer à l'autorité de déchiffrement (dans cet exemple : nom1.prénom1@uvsq.fr) afin qu'elle accomplisse sa procédure de déchiffrement avec sa clé pour lancer le dépouillement et publier les résultats.
- Cliquer [Compute the result] pour effectuer le comptage, après déchiffrement par les autorités. Dès lors les résultats sont publiés. Voir la page suivante pour la visualisation des résultats.

1.1.11.2. Administration de l'élection : Visualisation des résultats des votes

The screenshot displays the Belenios 1.10 web interface for "Election test 1". The main content area shows the results of the election, which has been counted. The interface includes a navigation bar with "Fichier", "Edition", "Affichage", "Historique", "Marque-pages", "Outils", and "Aide". The URL bar shows "https://belenios.loria.fr/elections/jwZ9KGMBFDCr...".

The election results are displayed in two sections:

- D'accord avec le compte-rendu de la dernière réunion ? (3 choix possibles maximum)**

| | |
|------------|---|
| Oui | 2 |
| Non | 1 |
| Vote blanc | 1 |
- Quelles couleurs pour la couverture ? (3 choix possibles maximum)**

| | |
|-------|---|
| Blanc | 3 |
| Jaune | 3 |
| Rouge | 1 |
| Vert | 3 |
| Bleu | 1 |
| Noir | 1 |

Below the results, it states: "Nombre de bulletins acceptés : 4. Vous pouvez également télécharger le [résultat avec les preuves cryptographiques](#)." A red circle highlights this link, and another red circle highlights the link "Voir les bulletins acceptés".

The bottom section shows the "Bulletins acceptés" page, which lists 4 accepted ballots. The first ballot is highlighted:

- 4ruglEulbpeMY6th2PsWl6YXiYFextupXwQs5FDo1va
- QlARldZNSRNdX3obMmVvg9VW06BdNI3SfosLzuL+8
- XlokcQ+YwVokUXYYPgEeJBw0wzRjIG8LCGYJfz5VB4
- XVGOrcFPSsM5MzS0egQ499GRKja0FhebWhXkQz6YHe

The right side of the image shows a JSON file containing the cryptographic proofs for the accepted ballots. The JSON structure includes "non_tallied", "encrypted_tally", and "partial_decryptions".

1.1.11.3. Administration de l'élection : Publication ou report de publication des résultats des votes

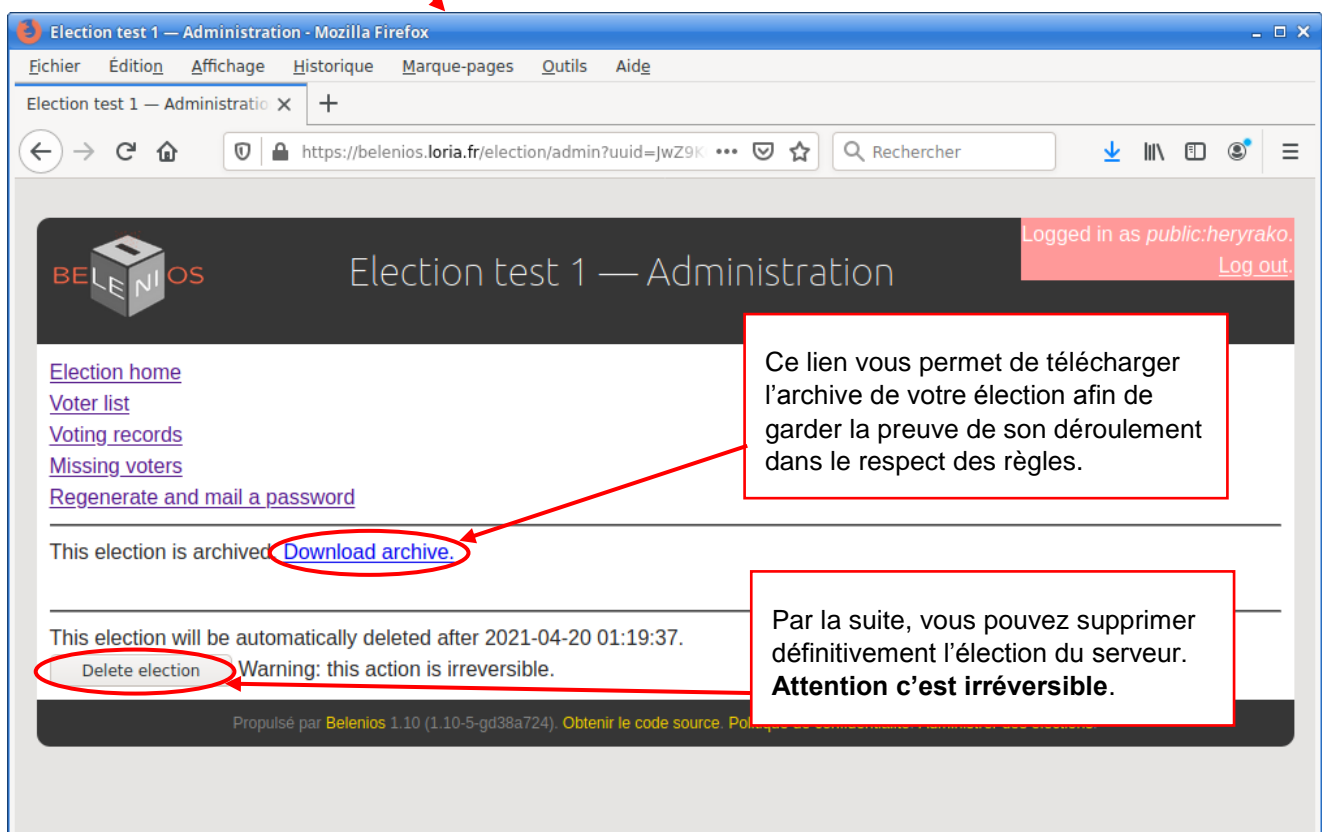
The screenshot shows the 'Election test 1 — Administration' page in a Mozilla Firefox browser. The page is logged in as 'public:heryako'. The main content area displays the election status and options for publication. A red box highlights the 'Postpone publication until' button and the date input field '2020-04-19 23:16:00'. A red arrow points from this box to a text box on the right. Another red box highlights the 'Publish the result now' button, with a red arrow pointing from a text box on the left.

Les résultats sont déjà publiés depuis le clic sur **Compute the result** (Voir parag. [1.1.11.2.](#)). Il est possible de refermer la publication et de la différer à une date ultérieure (au maximum 7 jours plus tard). Saisir la date ici, et cliquer **Postpone publication until**.

Attention, même remarque que pour les dates vues plus haut pour leur valeur et leur format (UTC). (Voir parag. [1.1.10.1.](#)).

La publication est alors reportée à la date fixée. Il est ensuite possible de la rouvrir avant cette date en cliquant **Publish the result now**

1.1.11.4. Administration de l'élection : Archiver une élection – Supprimer une élection



1.2. Les actions des autorités de déchiffrement (Trustees)

1.2.1. Avant la création d'élection : réception du lien (mail envoyé par l'organisateur), génération des clés

Pour pouvoir créer l'élection, l'organisateur doit attendre que toutes les autorités de déchiffrement aient généré chacune sa part de la clé privée de déchiffrement et transmis au serveur sa part de la clé publique correspondante. Pour faire cette opération, chaque autorité doit cliquer sur le lien et suivre la procédure contenues dans le mail transmis par l'organisateur. Pour rappel ci-dessous notre exemple pris au paragraphe [1.1.8.1](#) :

Nom : Organisateur Election test1 Adresse : ici-mail-organisateur@dd.pp

Répondre à : ici-mail-organisateur@dd.pp

À : auth.dechiffrement-1@xx.fr

Cc : ici-mail-organisateur@dd.pp

Cci :

Objet : Link to generate the decryption key

Texte simple Normal

Dear trustee,

You will find below the link to generate your private decryption key, used to tally the election.

<https://belenios.loria.fr/draft/trustee?token=oxdzK7F8Rv3PZz&uuid=JwZ9KGMBFDCGoD>

Here's the instructions:

1. click on the link
2. click on "generate a new key pair"
3. your private key will appear in another window or tab. Make sure you SAVE IT properly otherwise it will not possible to tally and the election will be canceled.
4. in the first window, click on "submit" to send the public part of your key, used encrypt the votes. For verification purposes, you should save this part (that starts with {"pok":{"challenge":}}), for example sending yourself an email.

Regarding your private key, it is crucial you save it (otherwise the election will be canceled) and store it securely (if your private key is known together with the private keys of the other trustees, then vote privacy is no longer guaranteed). We suggest two options:

1. you may store the key on a USB stick and store it in a safe.
2. Or you may simply print it and store it in a safe.

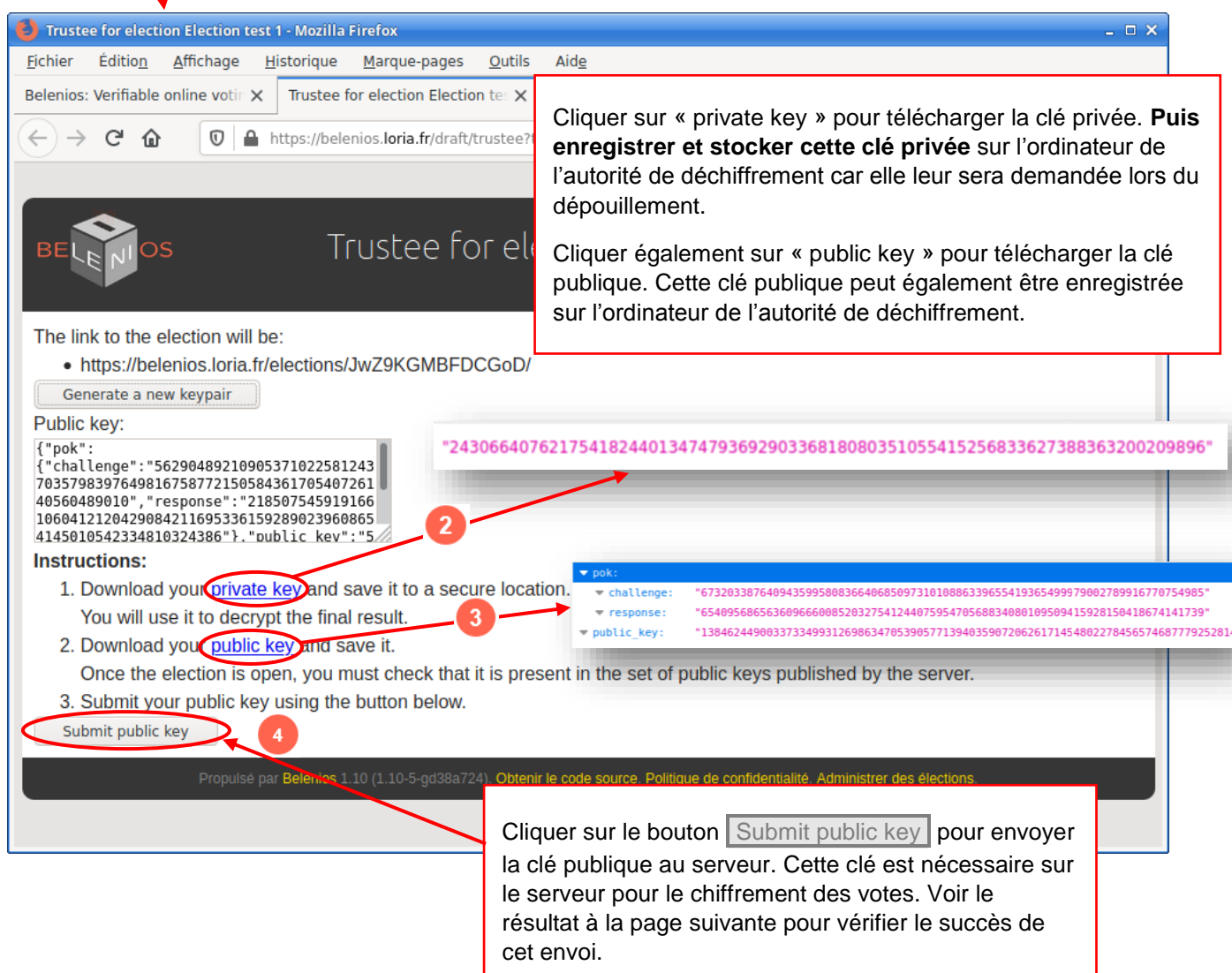
Of course, more cryptographic solutions are welcome as well.

Thank you for your help,

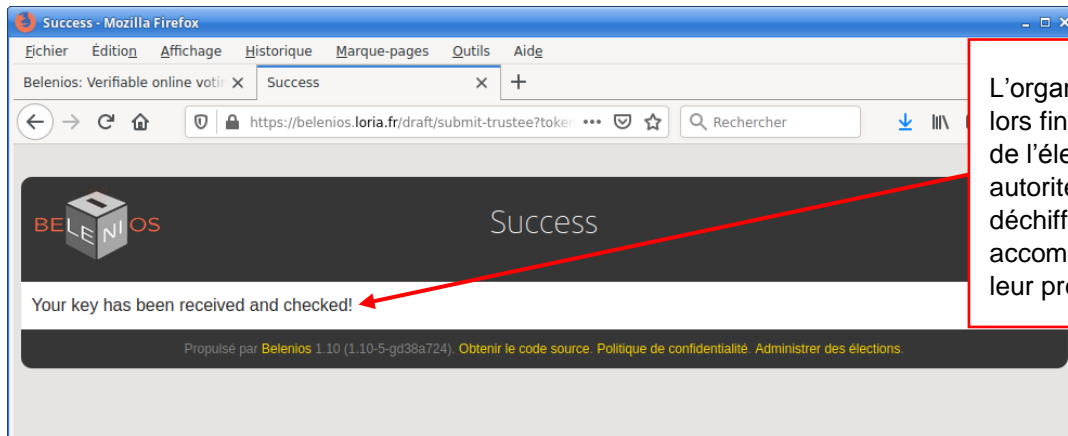
--
The election administrator.
--

Cliquer le lien pour accéder à la procédure à suivre donnée dans ce message.

1. GESTION AUTOMATIQUE CONFIEE ENTIEREMENT AU SERVEUR



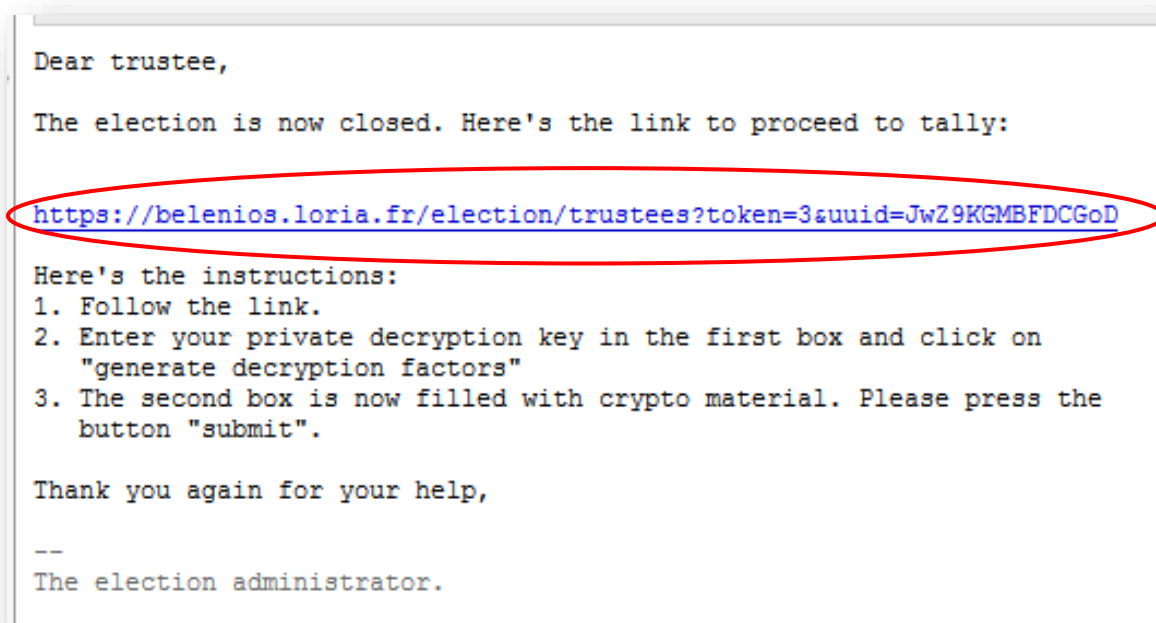
1. GESTION AUTOMATIQUE CONFIEE ENTIEREMENT AU SERVEUR



L'organisateur peut dès lors finaliser la création de l'élection si toutes les autorités de déchiffrement ont accompli avec succès leur procédures.

1.2.2. Dépouillement de l'élection : saisie de la clé privée et la partie de clé globale du déchiffrement propre à chaque autorité

Lors du dépouillement, l'organisateur fait envoyer par le serveur le mail ci-dessous de demande de dépouillement aux autorités de déchiffrement. Chaque autorité doit cliquer sur ce lien et suivre la procédure indiquée pour envoyer sa partie de la clé de dépouillement globale.



1. GESTION AUTOMATIQUE CONFIEE ENTIEREMENT AU SERVEUR

Election test 1 — Partial decryption #2 - Mozilla Firefox

Belenios: Verifiable online voting | Election test 1 — Partial decryption #2

https://belenios.loria.fr/election/trustees?token=...

Election test 1 — Partial decryption #2

It is now time to compute your partial decryption factors.
The hash of the encrypted tally is **ua2S4Yftadvwaf4q7jCFO7k+lguzbKI2hAyVaTlaJac**.

Instructions:

1. Please enter your private key:
- Or load it from a file:
 Aucun fichier sélectionné.
2.
3. your contribution to decryption.

Data:

Propulsé par Belenios 1.10 (1.10-5-gd38a724)

Chaque autorité de déchiffrement doit saisir sa clé privée stockée précédemment après sa génération, **ou** la charger à partir d'un fichier en cliquant sur le bouton **Parcourir...**.

Lancer le calcul de la clé à transmettre en cliquant sur **Compute decryption factors**.

Election test 1 — Partial decryption #2

It is now time to compute your partial decryption factors.
The hash of the encrypted tally is **ua2S4Yftadvwaf4q7jCFO7k+lguzbKI2hAyVaTlaJac**.

Instructions:

1. Please enter your private key:
- Or load it from a file:
 Aucun fichier sélectionné.
2.
3. your contribution to decryption.

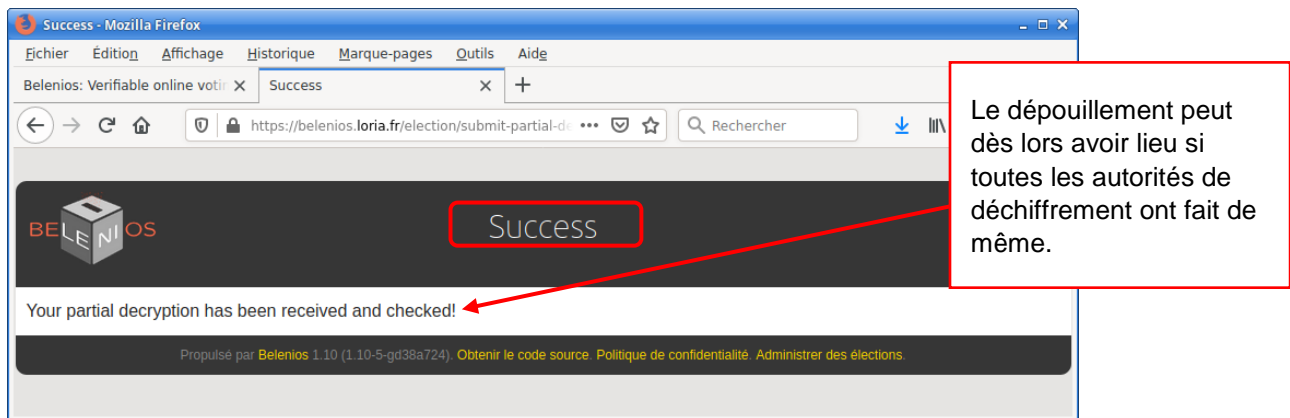
Data:

```
{
  "decryption_factors": [
    [
      "1471423174869347479963516281089577009",
      "8864832118625339869866324144243296169386",
      "6899249578799545346020904391330302661331",
      "8717363466662647362630011027226402264771",
      "5052423048914142139027797600138474754200"
    ]
  ]
}
```

Propulsé par Belenios 1.10 (1.10-5-gd38a724). [Obtenir le code source](#) [Politique de confidentialité](#) [Administrer cette élection](#)

La clé est calculée et présentée dans le champ Data. Cliquer sur **Submit** pour la transmettre au serveur. Voir le résultat à la page suivante pour vérifier le succès de cet envoi.

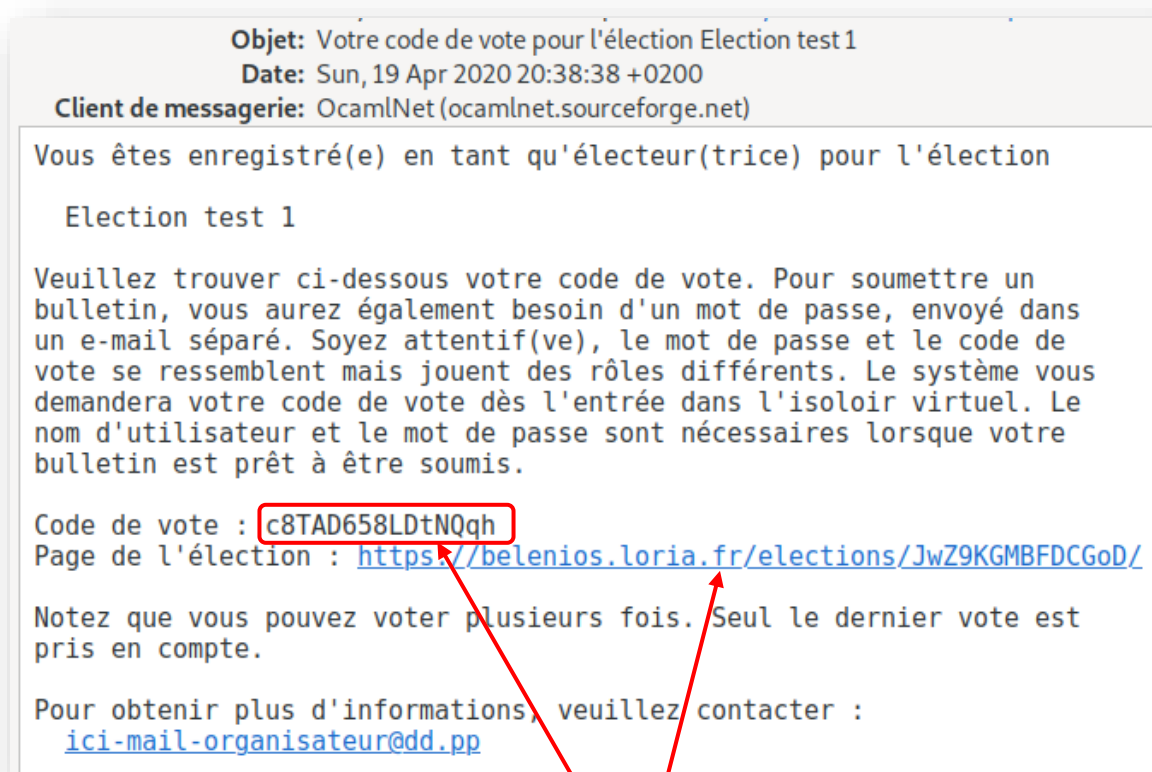
1. GESTION AUTOMATIQUE CONFIEE ENTIEREMENT AU SERVEUR



1.3. Les actions du votant

1.3.1. Votant : Réception du mail du vote (contenant le lien de l'élection et le code de vote)

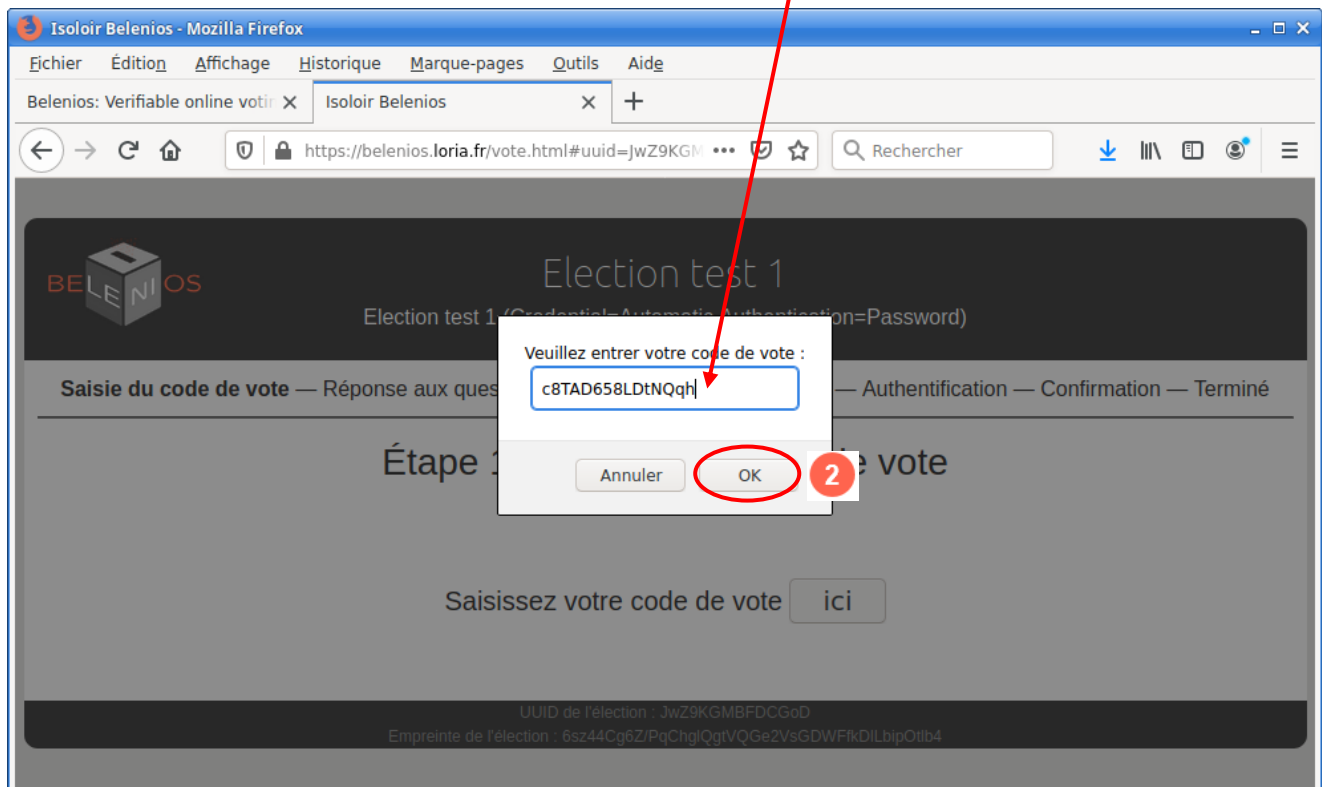
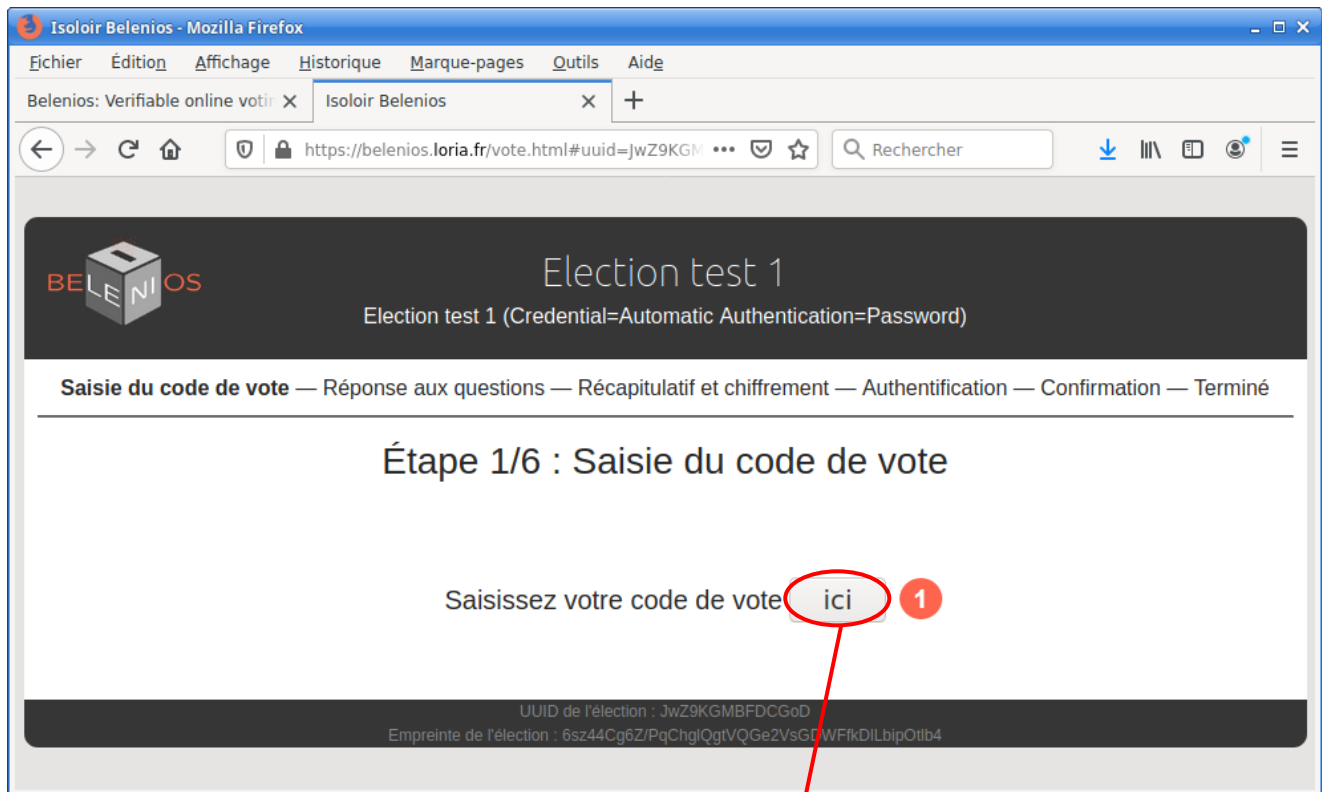
Chaque votant reçoit le mail l'invitant à aller sur la page de l'élection pour voter comme dans l'exemple suivant :



« Copier » le code de vote car vous en aurez besoin après avoir cliqué sur le lien pour voter. (Voir la page suivante)

1. GESTION AUTOMATIQUE CONFIEE ENTIEREMENT AU SERVEUR

1.3.2. Votant : Cliquer sur le lien de l'élection et commencer la procédure en saisissant le code de vote



1.3.3. Votant : Voter en répondant aux questions

Isoloir Belenios - Mozilla Firefox

Belenios: Verifiable online voting x Isoloir Belenios x +

https://belenios.loria.fr/vote.html#uuid=JwZ9KGM...

BELENIOS Election test 1
Election test 1 (Credential=Automatic Authentication=Password)

Saisie du code de vote — **Réponse aux questions** — Récapitulatif et chiffrement — Authentification — Confirmation — Terminé

Étape 2/6 : Réponse aux questions

D'accord avec le compte-rendu de la dernière réunion ?

Question 1/2 — sélectionnez entre 1 et 1 réponse(s)

☒ Oui
☐ Non
☐ Vote blanc

Suivant

UUID de l'élection : JwZ9KGM8BFDGCoD
Empreinte de l'élection : 6sz44Cg6Z/PqChglQgtVQGe2VsGDWfKdILbipOtlb4

Isoloir Belenios - Mozilla Firefox

Belenios: Verifiable online voting x Isoloir Belenios x +

https://belenios.loria.fr/vote.html#uuid=JwZ9KGM...

BELENIOS Election test 1
Election test 1 (Credential=Automatic Authentication=Password)

Saisie du code de vote — **Réponse aux questions** — Récapitulatif et chiffrement — Authentification — Confirmation — Terminé

Étape 2/6 : Réponse aux questions

Quelles couleurs pour la couverture ? (3 choix possibles maximum)

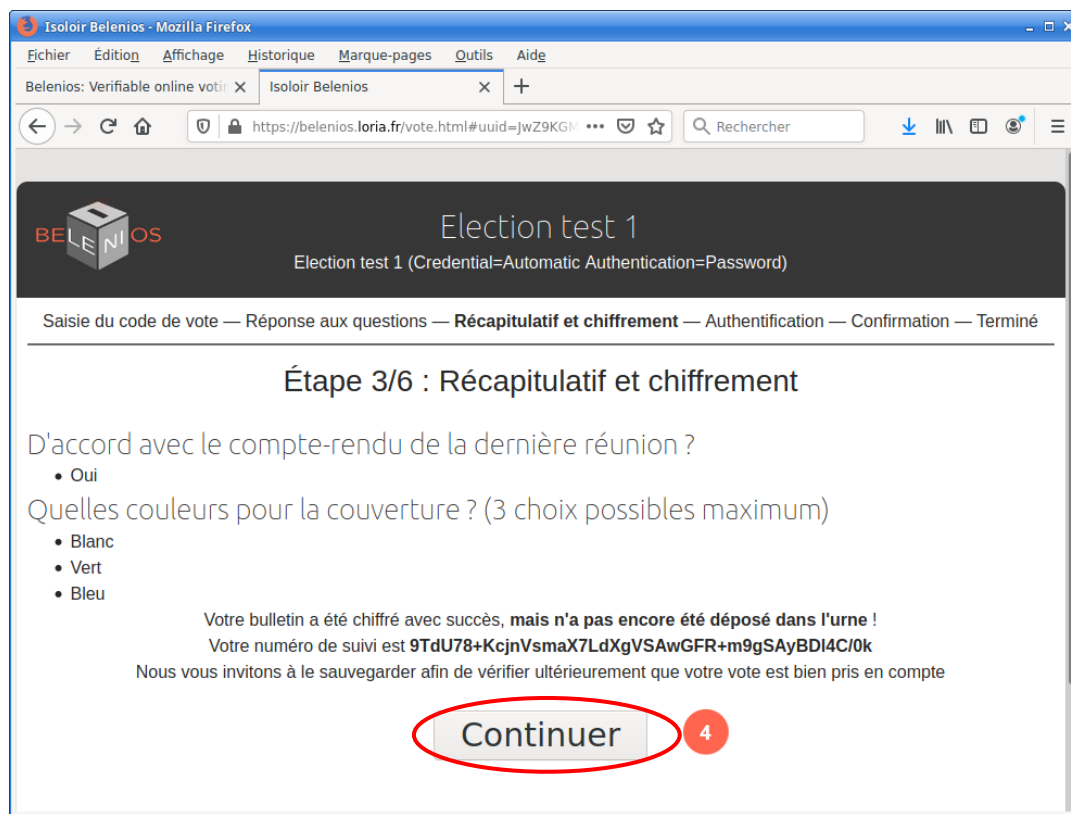
Question 2/2 — sélectionnez entre 1 et 3 réponse(s)

☒ Blanc
☐ Jaune
☐ Rouge
☒ Vert
☒ Bleu
☐ Noir

Précédent **Suivant** 3

UUID de l'élection : JwZ9KGM8BFDGCoD
Empreinte de l'élection : 6sz44Cg6Z/PqChglQgtVQGe2VsGDWfKdILbipOtlb4

1.3.4. Votant : Récapitulatif des votes avant de continuer



1.3.5. Votant : Connexion avec les codes envoyés par mail (login & mot de passe)

Vous êtes enregistré(e) en tant qu'électeur(trice) pour l'élection

Election test 1

Veuillez trouver ci-dessous votre nom d'utilisateur et votre mot de passe. Pour soumettre un bulletin, vous aurez également besoin d'un code de vote, envoyé dans un e-mail séparé. Soyez attentif(yg), le mot de passe et le code de vote se ressemblent mais jouent des rôles différents. Le système vous demandera votre code de vote dès l'entrée dans l'isoloir virtuel. Le nom d'utilisateur et le mot de passe sont nécessaires lorsque votre bulletin est prêt à être soumis.

Nom d'utilisateur : adresse.mail01@uvsq.fr

Mot de passe : vKBQXJFv9XHcdo

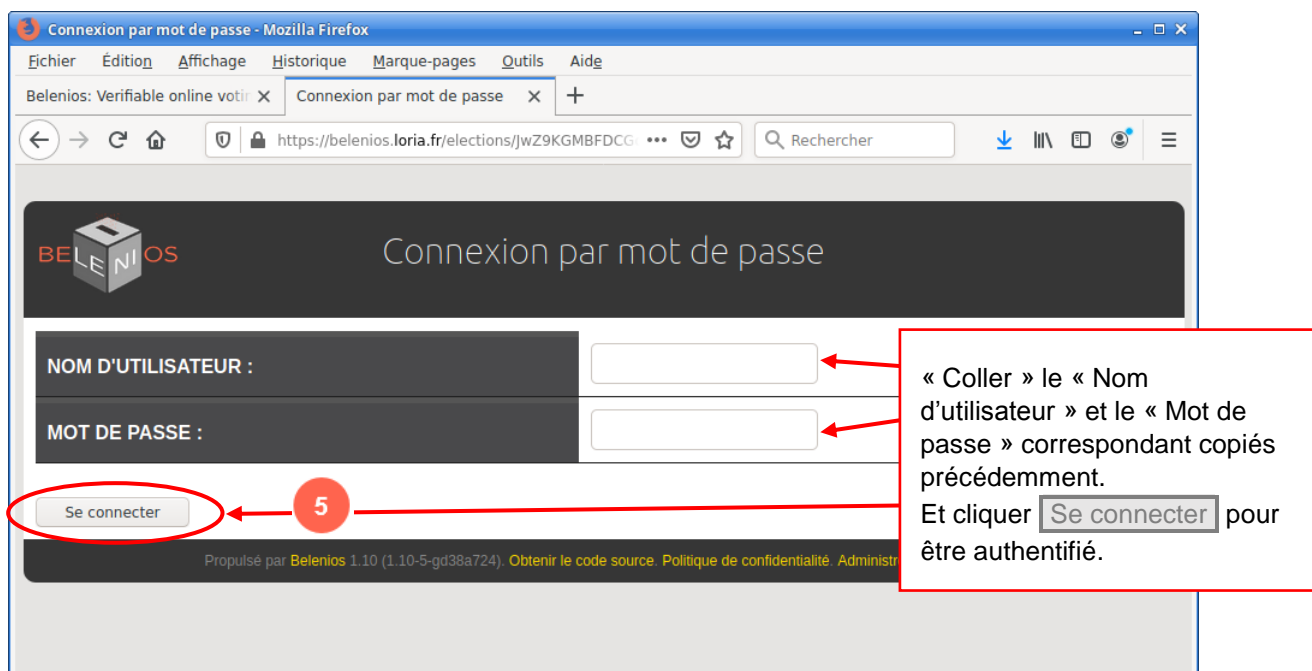
Page de l'élection : <https://belenios.loria.fr/elections/JwZ9KGMBFDCGoD/>

Notez que vous pouvez voter plusieurs fois. Seul le dernier vote est pris en compte.

Pour obtenir plus d'informations, veuillez contacter :
ici-mail-organisateur@dd.pp

Le mail reçu contenant le
 « Nom d'utilisateur » et le
 « Mot de passe »
 correspondant. Informations à
 « Copier » pour les « Coller »
 ci-après dans l'étape suivante.

1. GESTION AUTOMATIQUE CONFIEE ENTIEREMENT AU SERVEUR



Connexion par mot de passe - Mozilla Firefox

Belenios: Verifiable online voting x Connexion par mot de passe x +

https://belenios.loria.fr/elections/jwZ9KGMBFDCG

BELENIOS Connexion par mot de passe

NOM D'UTILISATEUR :

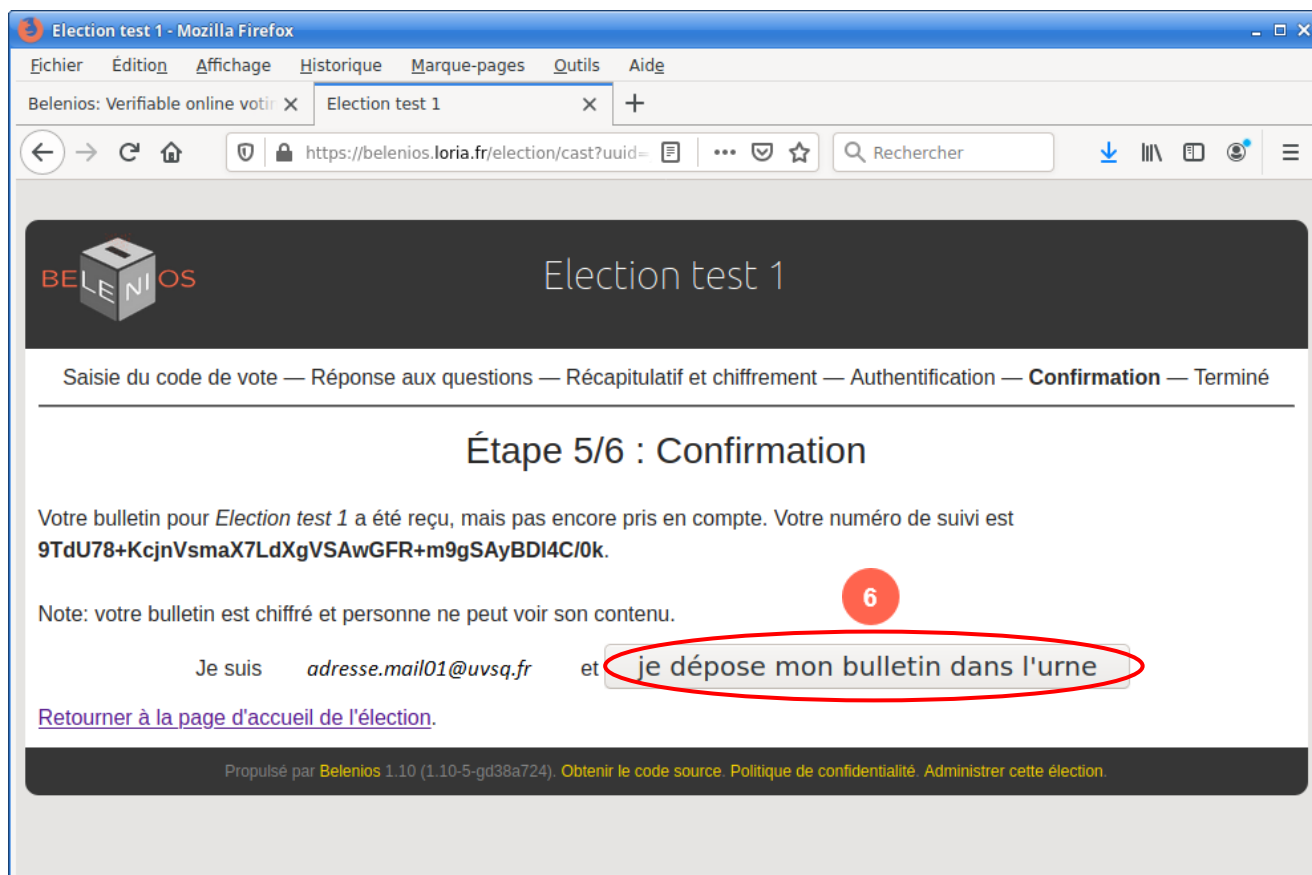
MOT DE PASSE :

Se connecter

Propulsé par Belenios 1.10 (1.10-5-gd38a724). [Obtenir le code source](#). [Politique de confidentialité](#). [Administrer](#)

« Coller » le « Nom d'utilisateur » et le « Mot de passe » correspondant copiés précédemment.
Et cliquer **Se connecter** pour être authentifié.

1.3.6. Votant : Confirmation et dépôt du bulletin dans l'urne



Election test 1 - Mozilla Firefox

Belenios: Verifiable online voting x Election test 1 x +

https://belenios.loria.fr/election/cast?uuid=

BELENIOS Election test 1

Saisie du code de vote — Réponse aux questions — Récapitulatif et chiffrement — Authentification — **Confirmation** — Terminé

Étape 5/6 : Confirmation

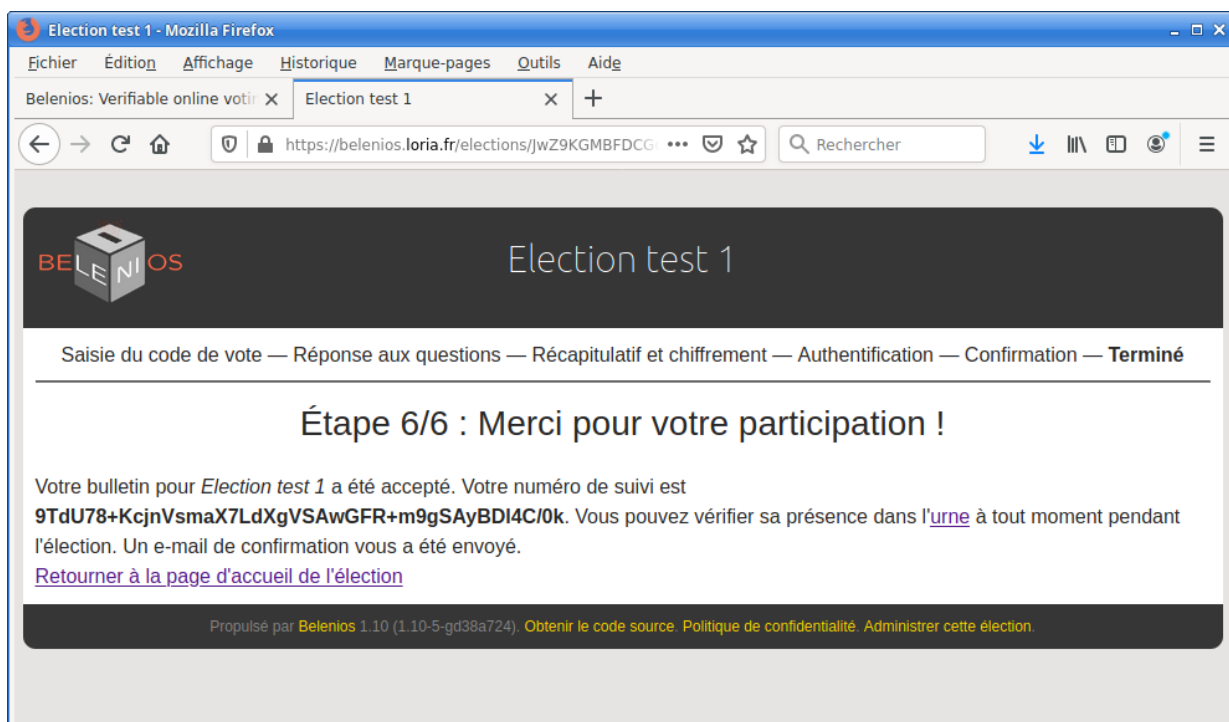
Votre bulletin pour *Election test 1* a été reçu, mais pas encore pris en compte. Votre numéro de suivi est **9TdU78+KcjinVsmaX7LdXgVSAwGFR+m9gSAyBDI4C/0k**.

Note: votre bulletin est chiffré et personne ne peut voir son contenu.

Je suis *adresse.mail01@uvsq.fr* et **je dépose mon bulletin dans l'urne**

[Retourner à la page d'accueil de l'élection.](#)

Propulsé par Belenios 1.10 (1.10-5-gd38a724). [Obtenir le code source](#). [Politique de confidentialité](#). [Administrer cette élection](#).



Le serveur envoie alors au votant le mail suivant de confirmation en lui indiquant son numéro de suivi visible dans l'urne, le lien pour visualiser l'urne, et le lien où seront publiés les résultats :

```
Votre vote pour l'élection

Election test 1

a été enregistré. Votre numéro de suivi est

9TdU78+KcjnVsmaX7LdXgVSAwGFR+m9gSAyBD14C/0k

Vous pouvez vérifier sa présence dans l'urne, accessible au
https://belenios.loria.fr/elections/JwZ9KGMBFDCGoD/ballots

Les résultats seront publiés sur la page de l'élection
https://belenios.loria.fr/elections/JwZ9KGMBFDCGoD/

Pour obtenir plus d'informations, veuillez contacter :
ici-mail-organisateur@dd.pp

--
Belenios
```

2. Gestion automatique (serveur) et authentification CAS

Cette section est en cours de rédaction...

3. Gestion manuelle déléguée à une tierce personne et authentification serveur

Cette section est en cours de rédaction...

4. Gestion manuelle déléguée à une tierce personne et authentification CAS

Cette section est en cours de rédaction...

