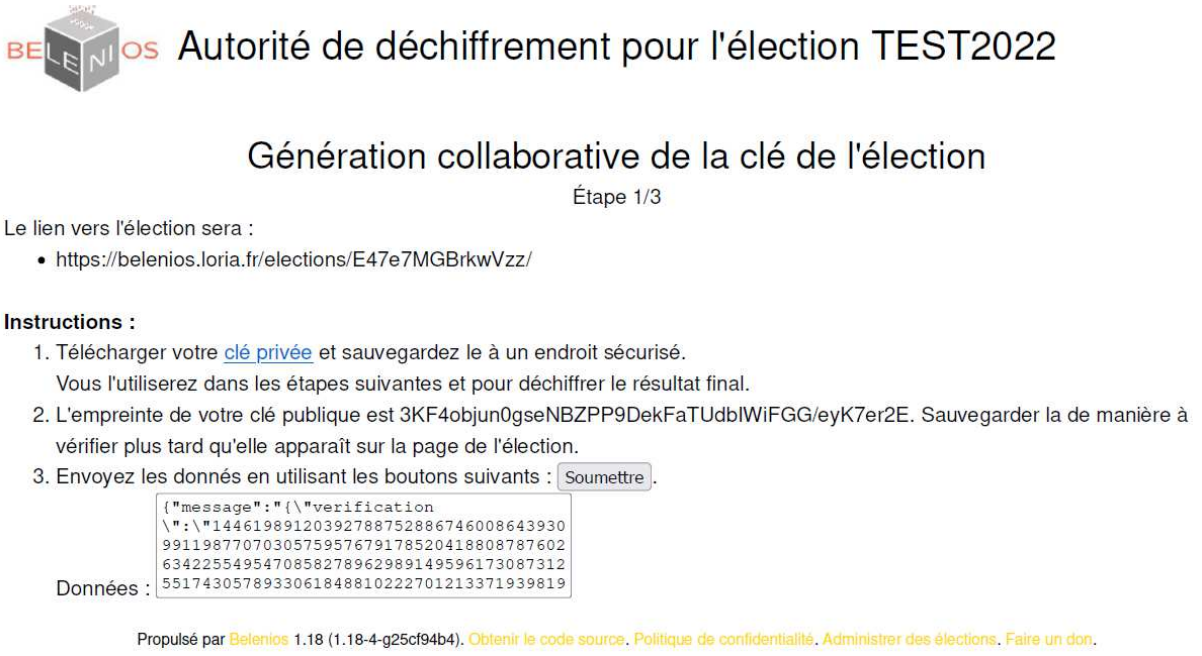
Procédure de cryptographie d'urne pour autorité de chiffrement

ETAPE 1

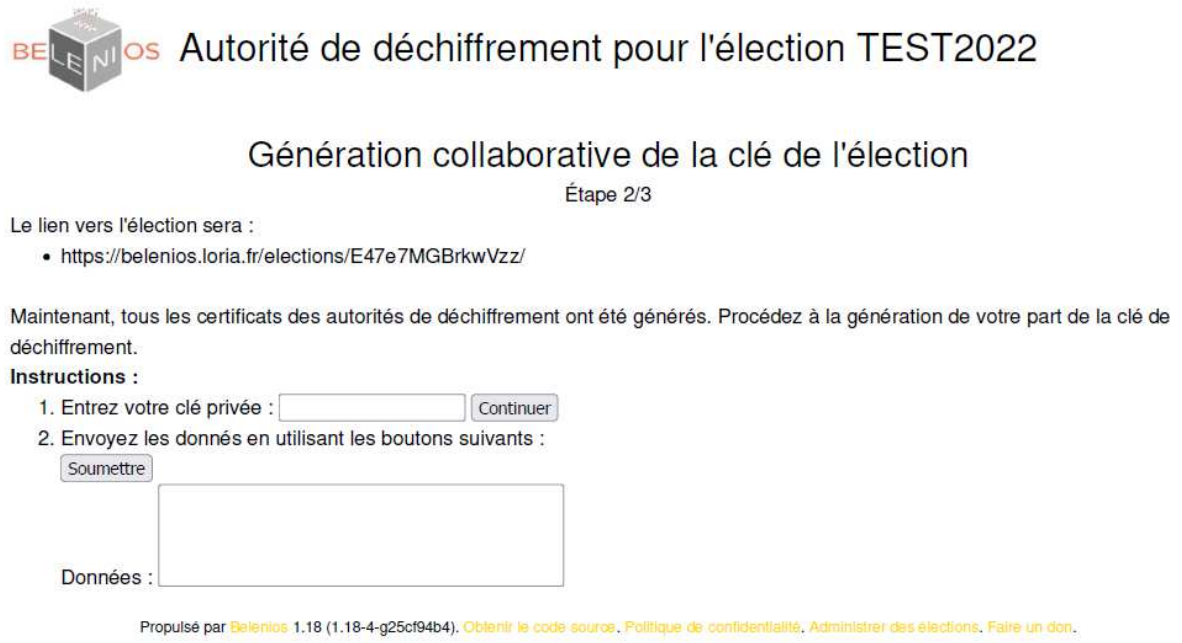
1. cliquer sur le lien reçu par courriel de la forme
https://belenios.loria.fr/draft/trustee?token=xXxXxXxXx&uuid=yYyYyYyYyY

2. IMPORTANT : cliquer sur « clé privée » pour télécharger le fichier « private_key.txt » qui contient une ligne avec le mot de passe de l'autorité de chiffremment
3. clique sur « Soumettre »

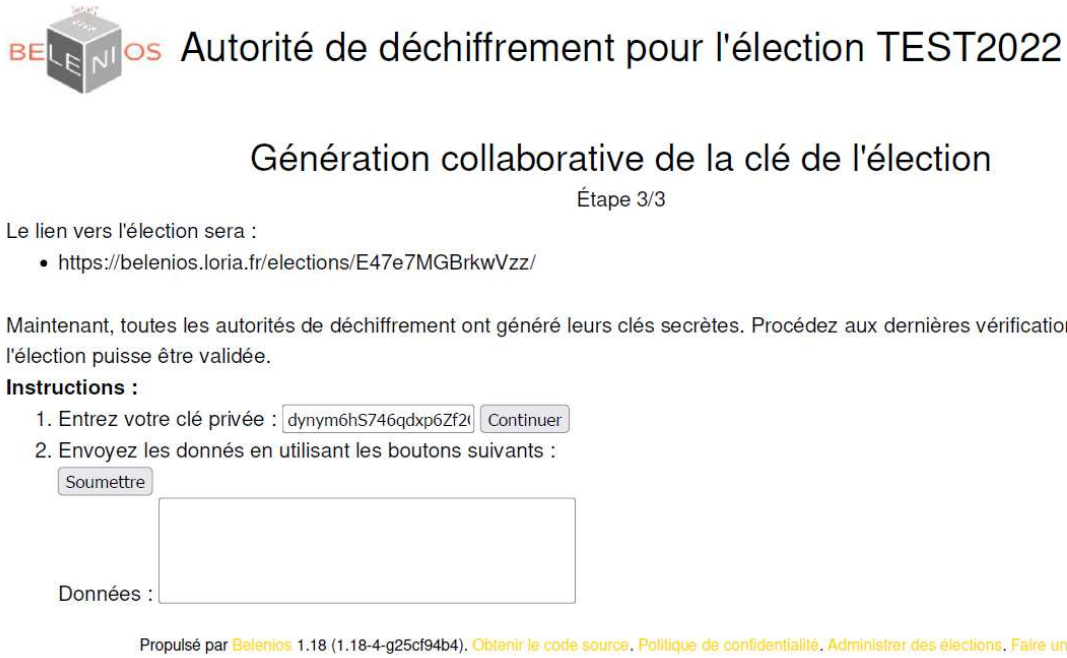


Propulsé par Belenios 1.18 (1.18-4-g25cf94b4). Obtenir le code source. Politique de confidentialité. Administrer des élections. Faire un don.

Etape 2
Entrez votre clé privée (contenue dans le fichier private_key.txt obtenue à l'étape 1)
cliquer sur « Continuer »
cliquer sur « Soumettre »



Etape 3
Entrez votre clé privée (contenue dans le fichier private_key.txt obtenue à l'étape 1)
cliquer sur « Continuer »
cliquer sur « Soumettre »



Fin de chiffrement

Autorité de déchiffrement pour l'élection TEST2022

Génération collaborative de la clé de l'élection

Étape 3/3

Le lien vers l'élection sera :

- https://belenios.loria.fr/elections/E47e7MGBrkwVzz/

Votre travail dans le protocole d'établissement des clés est terminé ! L'empreinte de votre clé de vérification est I76uXqvcRnPryQY1AOcPVZpDQtnpZvEmum4ST6m41nI. Vérifiez qu'elle est publiée par le serveur lorsque l'élection sera ouverte. Votre clé privée sera nécessaire pour décrypter le résultat de l'élection.

Instructions

1. Sauvegardez l'empreinte ci-dessus.
2. Une fois que l'élection est ouverte, vous devez vérifier qu'elle est présente dans la liste des clés de vérification publiées par le serveur.
3. Souvenez-vous que vous devez également vérifier la présence de votre clé publique.
4. N'oubliez pas de sauvegarder votre clé privée de manière sécurisée.

Le panneau de l'administrateur affiche :

Connecté en tant que *arc-occitanie*.
Déconnexion.

Autorités de déchiffrement pour l'élection ELECTION TEST

Sur cette page, vous pouvez configurer un groupe d'autorités de déchiffrement tel que seulement un sous-ensemble d'entre elles sera nécessaire pour effectuer le déchiffrement.

2 parmi 4 autorités de déchiffrement seront nécessaires pour déchiffrer le résultat.

AUTORITÉ DE DÉCHIFFREMENT	NOM PUBLIC	COURRIEL	LIEN	ÉTAT
trustee01@arcoccitanie.fr	trustee01@arcoccitanie.fr	Courriel	Lien	done
trustee02@arcoccitanie.fr	trustee02@arcoccitanie.fr	Courriel	Lien	done
trustee03@arcoccitanie.fr	trustee03@arcoccitanie.fr	Courriel	Lien	done
trustee04@arcoccitanie.fr	trustee04@arcoccitanie.fr	Courriel	Lien	done

Signification des états :

- initialisation : l'administrateur doit définir le seuil
- 1a : action requise de la part de l'autorité : générer la clé privée
- 2a, 3a : action requise de l'autorité : entrer la clé privée
- 1b, 2b, 3b : en attente des autres autorités
- Terminé : le protocole d'établissement de clé est terminé

Il y a un lien par autorité. Envoyez à chaque autorité son lien.

Réinitialiser le seuil

Retourner à la mise en place de l'élection