

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>



Autorité de déchiffrement pour l'élection TEST2022

Génération collaborative de la clé de l'élection

Étape 1/3

Le lien vers l'élection sera :

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

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

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 chiffrement

3. clique sur « Soumettre »



Autorité de déchiffrement pour l'élection TEST2022

Génération collaborative de la clé de l'élection

Étape 1/3

Le lien vers l'élection sera :

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

Instructions :

1. Télécharger votre [clé privée](#) et sauvegardez le à un endroit sécurisé.
Vous l'utiliserez dans les étapes suivantes et pour déchiffrer le résultat final.
2. L'empreinte de votre clé publique est 3KF4objun0gseNBZPP9DekFaTUdbWiFGG/eyK7er2E. Sauvegarder la de manière à vérifier plus tard qu'elle apparaît sur la page de l'élection.
3. Envoyez les données en utilisant les boutons suivants : .

Données :

```
{ "message": "{\nverification\n": "\n14461989120392788752886746008643930\n9911987707030575957679178520418808787602\n6342255495470858278962989149596173087312\n5517430578933061848810222701213371939819\n"
```

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

Étape 2

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



Autorité de déchiffrement pour l'élection TEST2022

Génération collaborative de la clé de l'élection

Étape 2/3

Le lien vers l'élection sera :

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

Maintenant, tous les certificats des autorités de déchiffrement ont été générés. Procédez à la génération de votre part de la clé de déchiffrement.

Instructions :

1. Entrez votre clé privée :
2. Envoyez les données en utilisant les boutons suivants :

Données :

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

Étape 3

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



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/>

Maintenant, toutes les autorités de déchiffrement ont généré leurs clés secrètes. Procédez aux dernières vérifications afin que l'élection puisse être validée.

Instructions :

1. Entrez votre clé privée :
2. Envoyez les données en utilisant les boutons suivants :

Données :

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

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.

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

Le panneau de l'administrateur affiche :



Autorités de déchiffrement pour l'élection ELECTION TEST

Connecté en tant que [arc-occitanie](#).
[Déconnexion](#).

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](#)

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