LEOSAC SAS



LEOSAC KEY MANAGER

Table des matières

[DOCUMENTATION UTILISATEUR 1](#__RefHeading___Toc1154_2924010706)

[LEOSAC KEY MANAGER 2](#__RefHeading___Toc1156_2924010706)

[Prérequis 2](#__RefHeading___Toc1158_2924010706)

[Logiciels 2](#__RefHeading___Toc1160_2924010706)

[Matériels 2](#__RefHeading___Toc1162_2924010706)

[Accueil 3](#__RefHeading___Toc1164_2924010706)

[Mode Sombre 4](#__RefHeading___Toc1166_2924010706)

[Log Console 4](#__RefHeading___Toc1168_2924010706)

[A propos 5](#__RefHeading___Toc1170_2924010706)

[Plan de maintenance 5](#__RefHeading___Toc1172_2924010706)

[Magasins de clés 6](#__RefHeading___Toc1174_2924010706)

[Liste des clés 7](#__RefHeading___Toc1176_2924010706)

[Recherche d’une clé 7](#__RefHeading___Toc1178_2924010706)

[Création d’une nouvelle clé 7](#__RefHeading___Toc1180_2924010706)

[Définition manuelle 7](#__RefHeading___Toc1182_2924010706)

[Import d’un cryptogramme 9](#__RefHeading___Toc1184_2924010706)

[Clés symétriques 10](#__RefHeading___Toc1186_2924010706)

[Version de la clé 10](#__RefHeading___Toc1188_2924010706)

[Somme de contrôle 10](#__RefHeading___Toc1190_2924010706)

[Génération 10](#__RefHeading___Toc1192_2924010706)

[Liaison 14](#__RefHeading___Toc1194_2924010706)

[Impression 14](#__RefHeading___Toc1196_2924010706)

[Clés asymétriques 15](#__RefHeading___Toc1198_2924010706)

[Enregistrement dans les favoris 15](#__RefHeading___Toc1200_2924010706)

[Edition du favori 16](#__RefHeading___Toc1202_2924010706)

[Fermeture du magasin de clés 16](#__RefHeading___Toc1204_2924010706)

[Types de magasins 16](#__RefHeading___Toc1206_2924010706)

[Fichiers 16](#__RefHeading___Toc1208_2924010706)

[NXP SAM AV2 17](#__RefHeading___Toc1210_2924010706)

[HSM PKCS#11 20](#__RefHeading___Toc1212_2924010706)

[Favoris 21](#__RefHeading___Toc1214_2924010706)

# LEOSAC KEY MANAGER

Leosac Key Manager est un logiciel de gestion de clés pour différents types de magasins de clés.

Il fournit une interface générique de génération, de création, d’édition et de calculs cryptographiques pour des clés symétriques et asymétriques.

## Prérequis

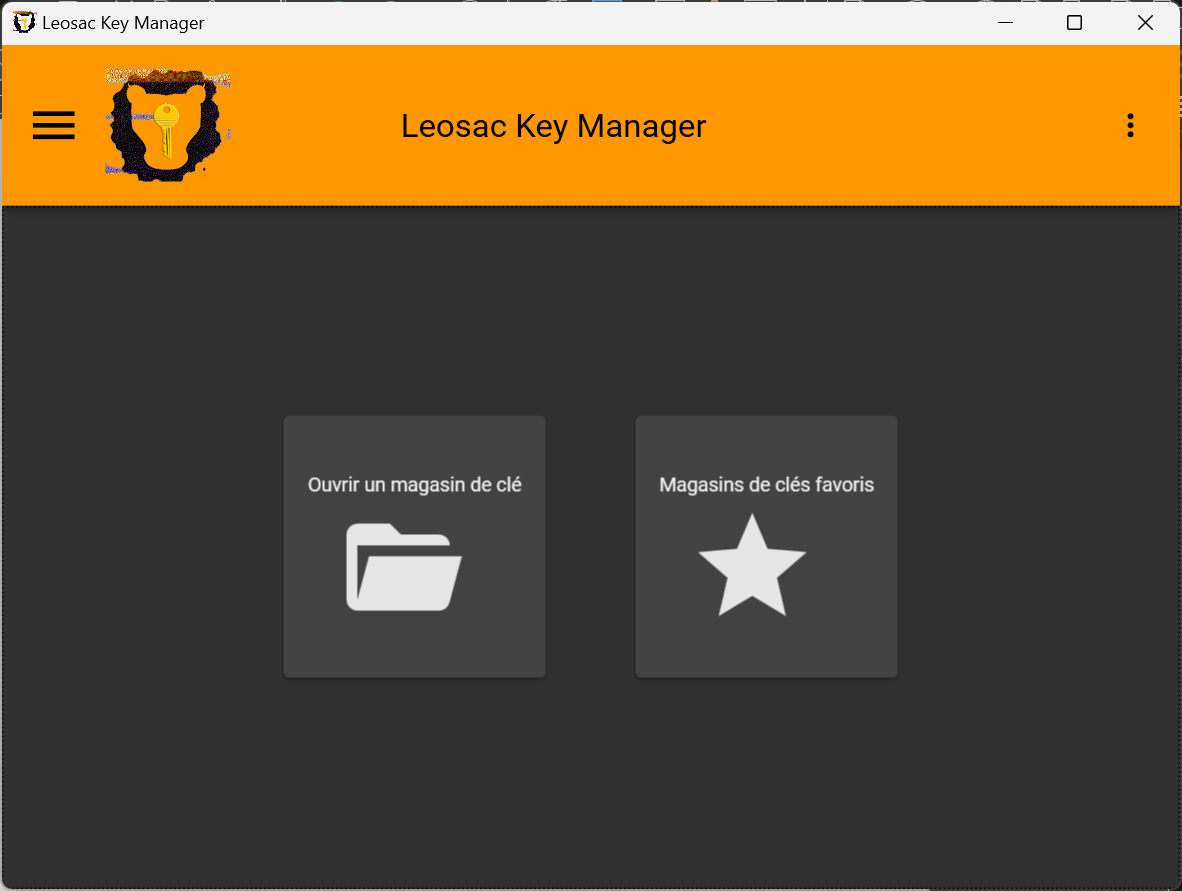
### Logiciels

* **.NET Desktop 8.0[[1]](#footnote-1)**
* **VC++** **Redistributable[[2]](#footnote-2)**

### Matériels

|  |  |
| --- | --- |
| Processeur | 2 GHz |
| RAM | 4096 MB |
| Espace Disque Minimal | 4.5 GB |

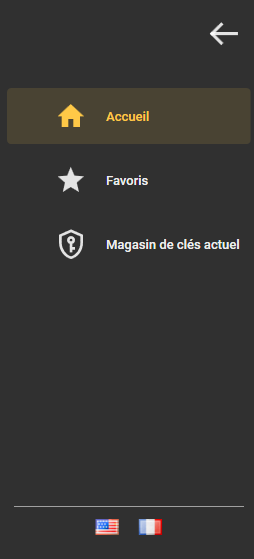
## Accueil



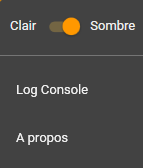
L’écran d’accueil de Leosac Key Manager vous permet d’accéder rapidement aux fonctionnalités principales du logiciel.

Des « tuiles » vous invitent à ouvrir un magasin de clés existant ou bien à lister les magasins de clés favoris.

Sur la gauche, un menu  vous permet de passer rapidement aux différentes sections.



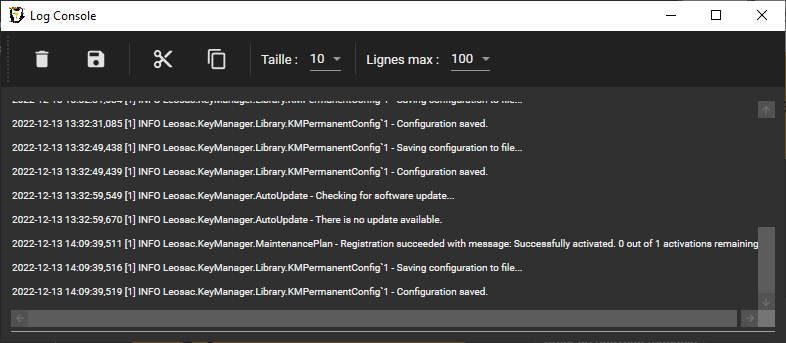
Sur la droite, un menu complémentaire  vous donne accès aux paramètres plus avancés et secondaires de l’application.



## Mode Sombre

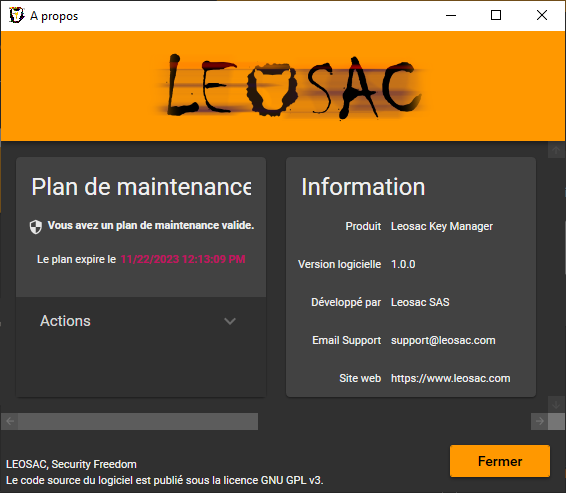
L’option  permet de basculer rapidement l’interface utilisateur d’un mode clair à un mode sombre. Ce choix est sauvegardé.

## Log Console



Le détail des opérations effectuées et leur trace est enregistré par défaut dans un fichier de logs.  
Ces logs peuvent être visualisés en temps réel directement dans l’application via la fenêtre « Log Console ».

## A propos



La fenêtre « à propos » fournit des informations complémentaires sur le programme, l’éditeur et les bibliothèques dépendantes.

C’est également à partir de cette fenêtre que la vérification des mises à jour peut être effectuée et son automatisation activée/désactivée.

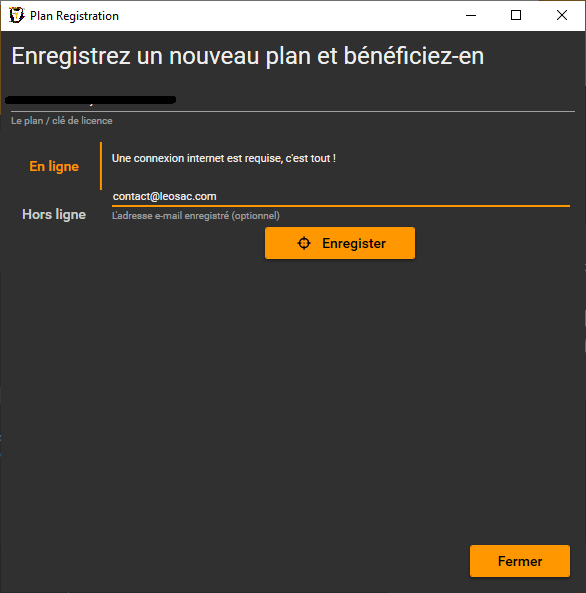
Des détails sur le plan de maintenance actuel sont par ailleurs affichés.

## Plan de maintenance

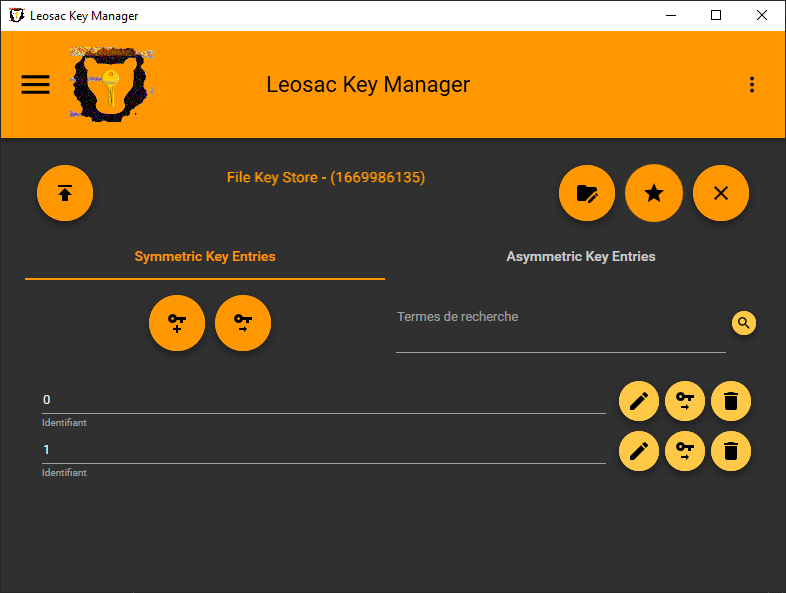
Il est fortement recommandé de souscrire à un plan de maintenance afin de garantir un support minimum de votre installation, de s’affranchir de toute limitation, de bénéficier des services annexes à l’applicatif et de contribuer financièrement au développement du logiciel.

Visitez <https://leosac.com/fr/key-manager/> ou contactez votre revendeur pour plus d’informations sur les plans.

Une fois le plan souscrit, procédez à son enregistrement directement dans l’application.



# Magasins de clés



## Liste des clés

Lors de l’ouverture du magasin de clés, la liste des clés disponibles est automatiquement affichée.

En fonction des capacités du magasin, il vous sera possible d’éditer une clé existante via , importer un cryptogramme vers une clé existante via  ou tout simplement supprimer la clé avec .

### Recherche d’une clé



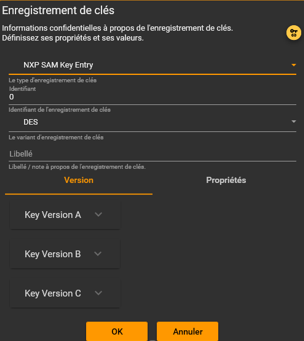
Lorsque le magasin possède un nombre significatif de clés, vous pouvez chercher rapidement une clé cible via un filtre de recherche situé au-dessus de la liste de clés.

## Création d’une nouvelle clé

### Définition manuelle

La création d’une nouvelle clé définie localement se fait facilement via le bouton .

Une nouvelle fenêtre vous invitant à définir les paramètres de la nouvelle clé s’offre à vous.



#### Type de clé

Le type de clé défini ici.

Il est recommandé de sélectionner directement un type pour la technologie cible, des incompatibilités ou un manque de granularité pouvant autrement apparaitre.

#### Identifiant de clé

Un identifiant, souvent unique, permettant de référencer la clé ultérieurement.

Certains magasins peuvent nécessiter un formatage particulier de cet identifiant.

#### Variant

Représente généralement l’algorithme cryptographique à utiliser.

#### Libellé

Ce champ est optionnel, pas toujours sauvegardé de façon permanente en fonction du magasin de clés, et permet de définir un libellé ou une note sur l’usage de la clé.

#### Versions

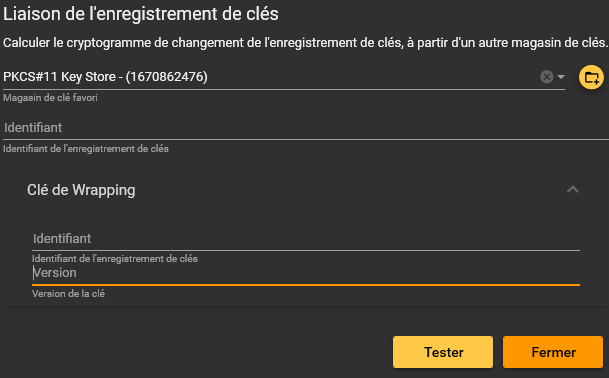
Plusieurs versions de clés peuvent co-exister pour un même enregistrement de clés en fonction de la technologie cible, chacune pouvant être configurée avec des valeurs différentes.

#### Propriétés

Les paramètres complémentaires propres à la technologie cible sont définis ici. Plus d’informations directement dans la section Types de magasins de clés.

#### Liaison

Vous pouvez effectuer une liaison de l’enregistrement de clé dans sa totalité vers un autre enregistrement de clé stocké dans un autre magasin, via le bouton .



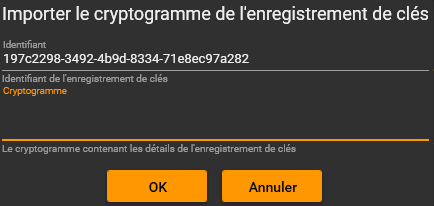
Vous devrez alors renseigner le magasin de clé favori à utiliser pour la liaison, et l’identifiant de clé dans ce magasin.

Les liaisons à ce stade sont simplement déclaratives, elles ne sont exécutées qu’au moment de la publication du magasin vers un magasin cible. Ce type d’opération est généralement effectué à partir d’un magasin de type « Fichiers », servant de modèle à la création de magasins de type « NXP SAM AV2/AV3 » ou « HSM PKCS#11 ».

De plus, il vous sera sûrement nécessaire de définir une Clé de Wrapping sécurisant le cryptogramme. Cette clé devra exister de façon conjointe dans le magasin de liaison, et dans le magasin cible au moment de la publication.

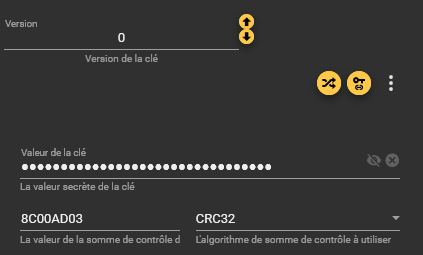
### Import d’un cryptogramme

Si vous possédez un cryptogramme qui vous a été transmis de façon déconnectée, vous pouvez l’importer directement afin de créer l’enregistrement de clé via le bouton .



Vous devrez alors définir l’identifiant de clé à utiliser, et la valeur brute du cryptogramme.

## Clés symétriques



### Version de la clé

Lorsque le magasin supporte les versions de clés, vous pouvez définir ici sa valeur.

Cette information est purement informative mais peut permettre des automatismes ultérieurs de rotation de clés.

### Somme de contrôle

Afin de s’assurer de la validité de la saisie d’une clé, vous pouvez vous référer à la somme de contrôle.

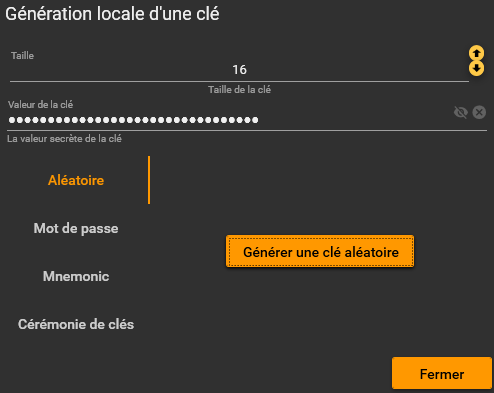
Pour les clés symétriques de type DES et AES, Il est recommandé d’utiliser l’algorithme KCV. Pour les autres, vous pouvez utiliser CRC32 ou un simple hash SHA256.

### Génération

Leosac Key Manager attache une attention particulière à la génération des clés. Ouvrez l’interface de génération locale d’une clé via le bouton .

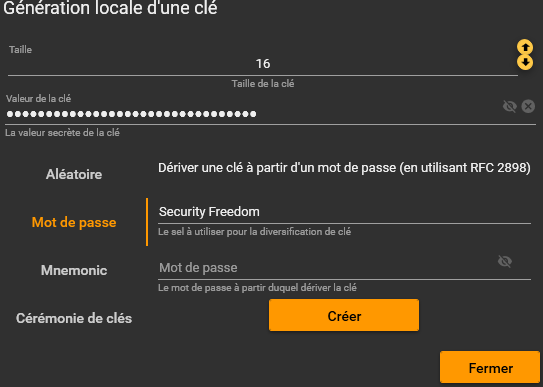
Plusieurs méthodes sont ici à votre disposition.

#### Aléatoire



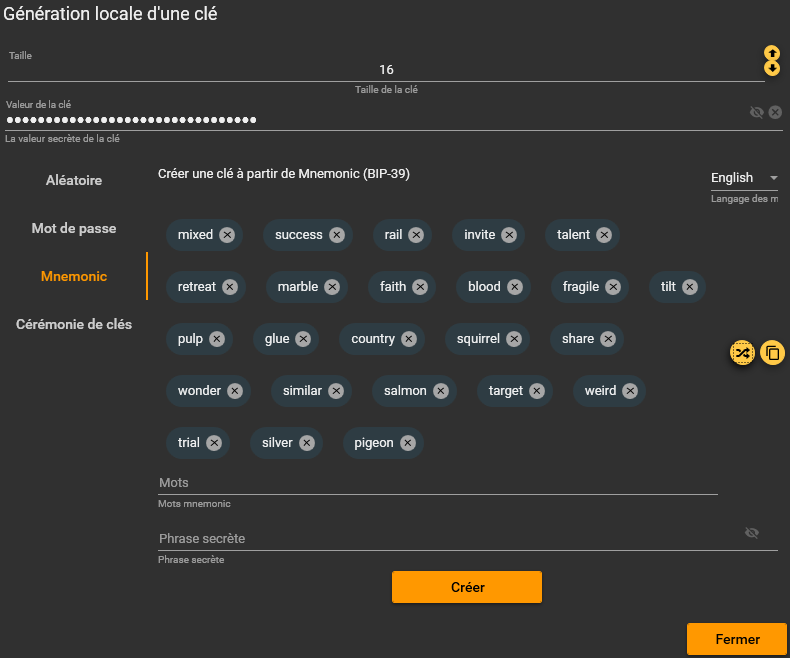
Générez une clé de façon pseudo-aléatoire via le bouton « Générer une clé aléatoire ».

#### Mot de passe



Dérivez une clé à partir d’un mot de passe, en utilisant la RFC 2898.

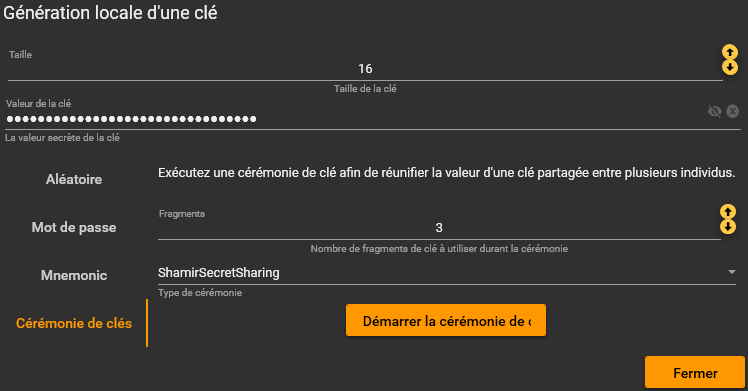
#### Mnémonic



Créez une clé à partir de mots Mnemonic (BIP-39). Il est recommandé de générer une liste de mots via le bouton  puis de définir une phrase secrète.

Ce mode de génération a surtout un intérêt pour des clés de taille importante.

#### Cérémonie de clés

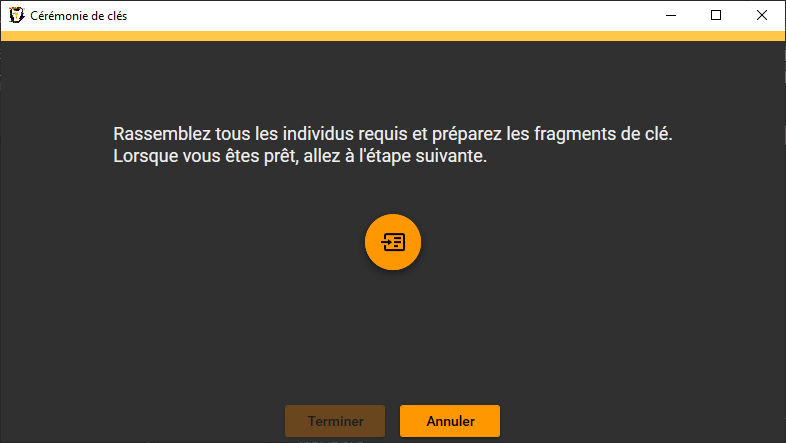


Une cérémonie de clé correspond à la réunification de plusieurs fragments partagés entre plusieurs individus, afin de retrouver la clé secrète d’origine.

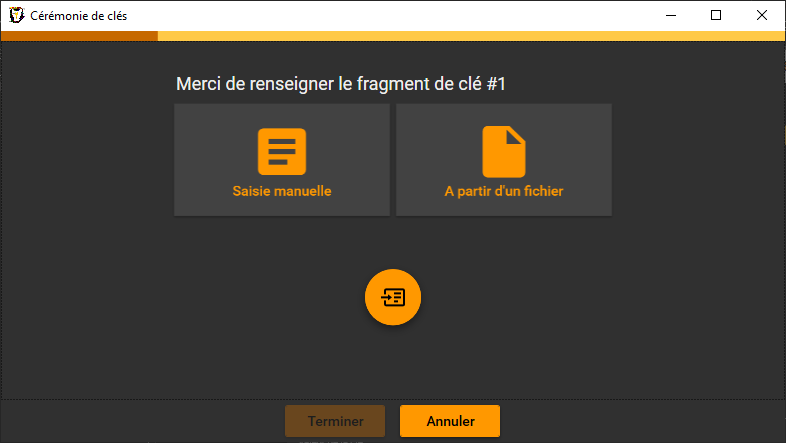
Définissez ici le nombre de fragments attendus et le type de cérémonie à effectuer.

Une cérémonie simple correspond à un XOR ou une concaténation des fragments. Il est toutefois recommandé d’utiliser une cérémonie plus fiable, fournissant de la parité en cas de perde d’un des fragments. La cérémonie de clé de type Shamir est donc ici recommandé.

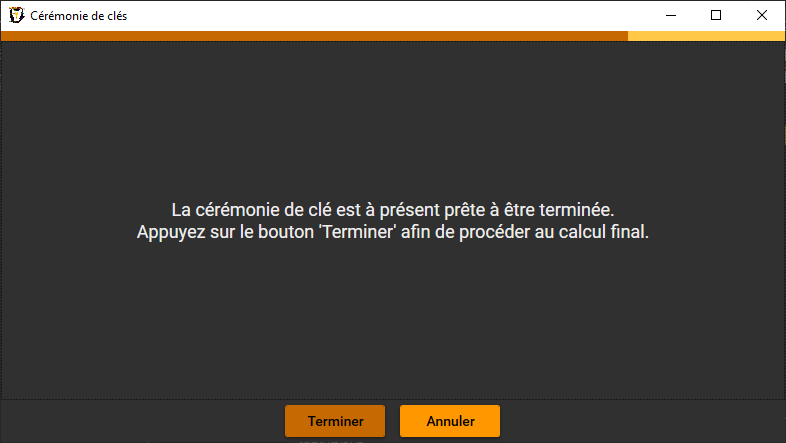
Cliquez sur « Démarrer la cérémonie de clés » afin d’ouvrir une interface utilisateur vous guidant à la réunification.



Préparez les différents individus et leurs fragments, puis démarrez la réunification via le bouton .



Renseignez chaque fragment puis passez à l’étape suivante via .

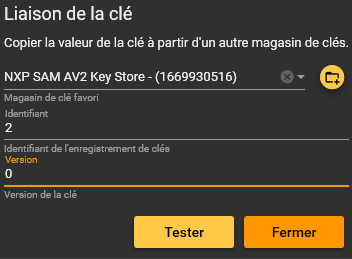


Une fois tous les fragments renseignés, terminez la cérémonie via le bouton « Terminer ».

### Liaison

Vous pouvez lier la valeur de la clé à partir d’une clé située dans un autre magasin via le bouton .

Ce type de liaison est généralement moins sécurisé qu’une liaison sur l’enregistrement de clé dans sa totalité mais correspond toutefois à un besoin. En pratique, la valeur de la clé est généralement extraite temporairement en clair du magasin de clé d’origine.

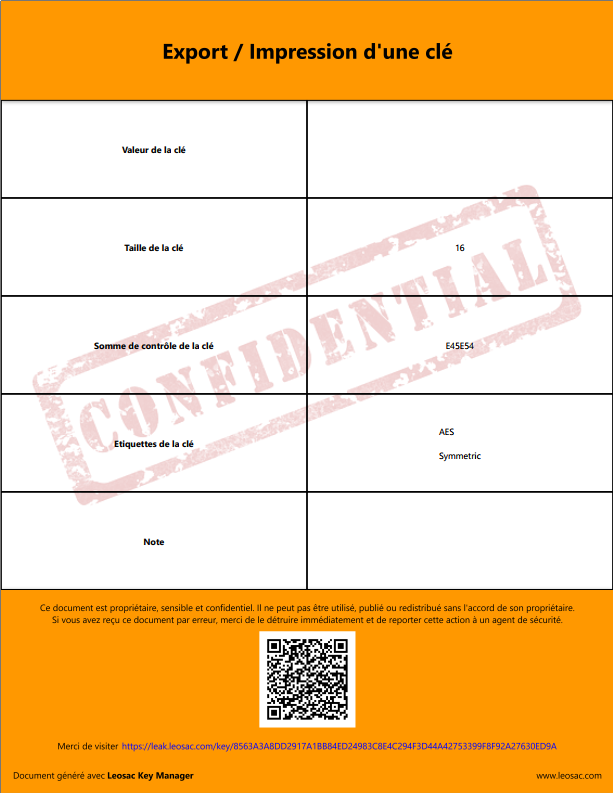


Sélectionnez le magasin de clé favori d’origine et renseignez l’identifiant de l’enregistrement de clé à utiliser ainsi que la version de clé de cet enregistrement, si nécessaire.

### Impression

La valeur d’une clé peut facilement être imprimé via le bouton .

Cette opération est considérée comme sensible, sortant du magasin de clé sa valeur, en clair, et à effectuer en connaissance de cause.



## Clés asymétriques

Le support des clés asymétriques est pour le moment rudimentaire. Il vous est possible de définir, par saisie, la valeur de la clé publique et de la clé privée, sans option de génération ou de fonctionnalité avancée. Ce sont des évolutions prévues dans les versions futures.

## Enregistrement dans les favoris

Utilisez le bouton  afin d’enregistrement dans les favoris le magasin de clés actuellement ouvert.

Si celui-ci est actuellement dans les favoris et que vous souhaitez le retirer, utiliser le bouton , ou supprimez-le de la liste des favoris via l’écran dédié.

## Edition du favori

Lorsque le magasin actuellement ouvert est un favori, vous pouvez éditer les paramètres de connexion au magasin via le bouton .

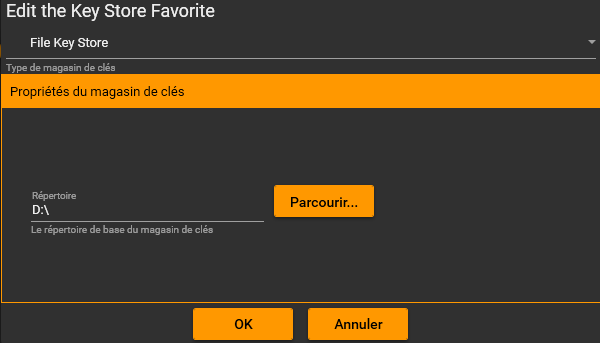
## Fermeture du magasin de clés

Il est recommandé de fermer le magasin lorsque vous ne l’utilisez plus si vous conservez l’application ouverte. Pour ce faire utilisez le bouton .

## Types de magasins

### Fichiers

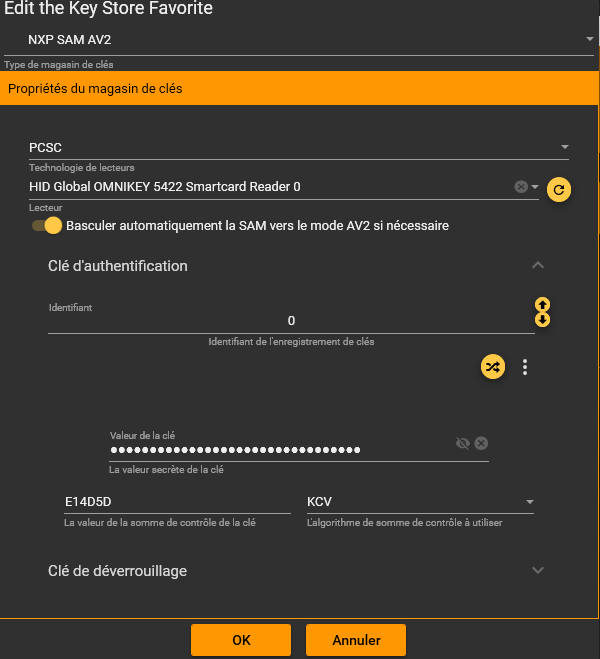
#### Propriétés du magasin de clés



#### Types de clés

### NXP SAM AV2 / AV3

#### Propriétés du magasin de clés



#### Types de clés

##### DES / 3DES / 3K3DES / AES128 / AES192 / AES256

###### Options

Les enregistrements de clés d’une SAM AVx possèdent une classification limitant leur usage.

De manière générale à l’usage, les enregistrements 0 et 1 sont de type HOST, et les clés DESFire stockées à partir de l’enregistrement 2 sont de type PICC.

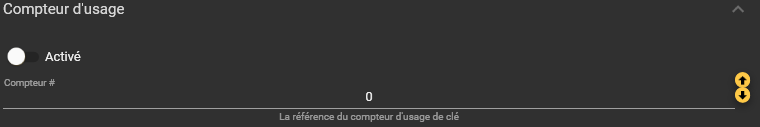
En fonction de l’applicatif cible, les clés HOST doivent avoir soit l’option « Verrouiller / Déverrouiller » ou l’option « Authentification Hôte » d’activée.

Concernant les clés PICC, les options « Activer le dump de la clé de session » et « Conserver l’IV » sont nécessaires. Si la SAM est utilisée pour encoder de nouveaux badges, l’option « Désactiver le changement de clé sur une carte » ne doit pas être cochée ; autrement il est recommandé d’activer cette option.



###### Compteur d’usage

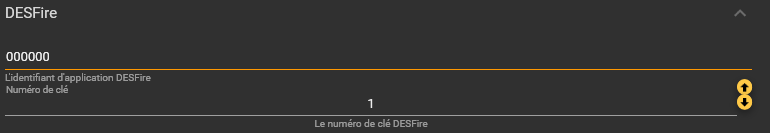
Il est possible de limiter le nombre d’usages d’une clé en assignant un compteur à celle-ci. Si activé, à chaque usage le compteur référencé est incrémenté, et ce jusqu’à sa valeur maximale. Ensuite, la clé ne peut plus être utilisée.



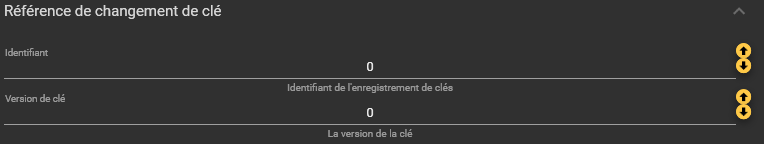
###### DESFire

Dans le cadre d’une clé de type PICC, il est possible de définir des métadonnées concernant son usage sur le badge DESFire, à savoir l’Application ID et le numéro de clé dans l’application.

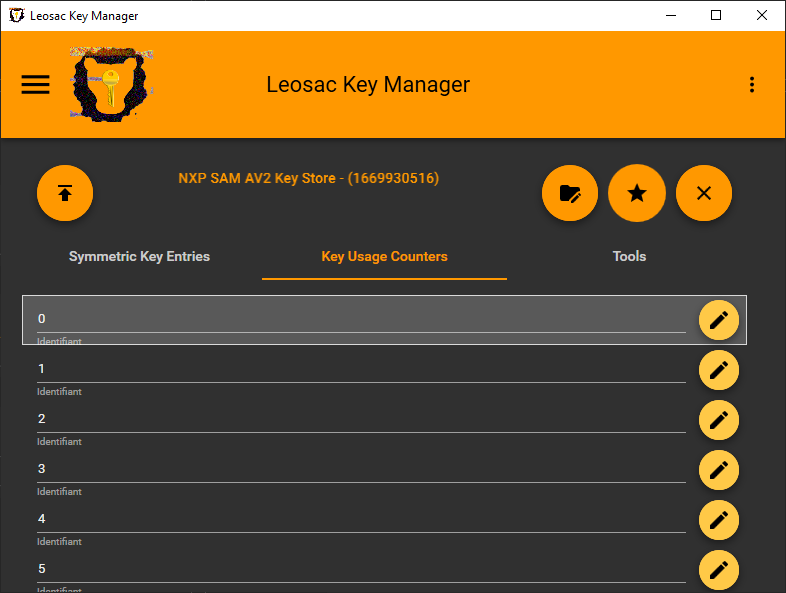
Ce paramétrage est optionnel dans le cadre de l’usage de la SAM avec les produits LEOSAC, ceux-ci accédant aux clés de la SAM directement via le numéro d’enregistrement de clé.

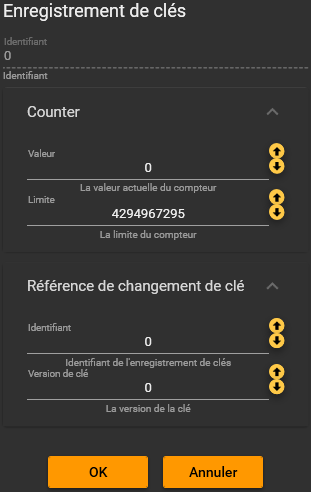


###### Référence de changement de clé

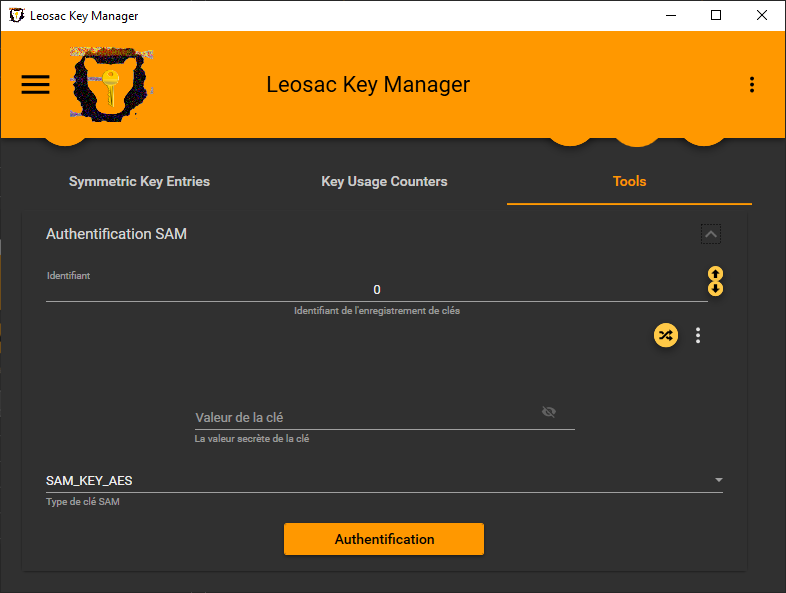


#### Compteurs



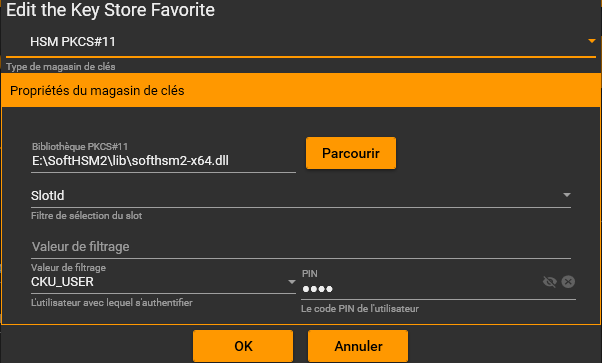


#### Outils

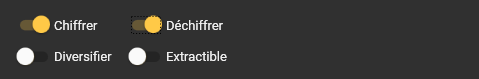


### HSM PKCS#11

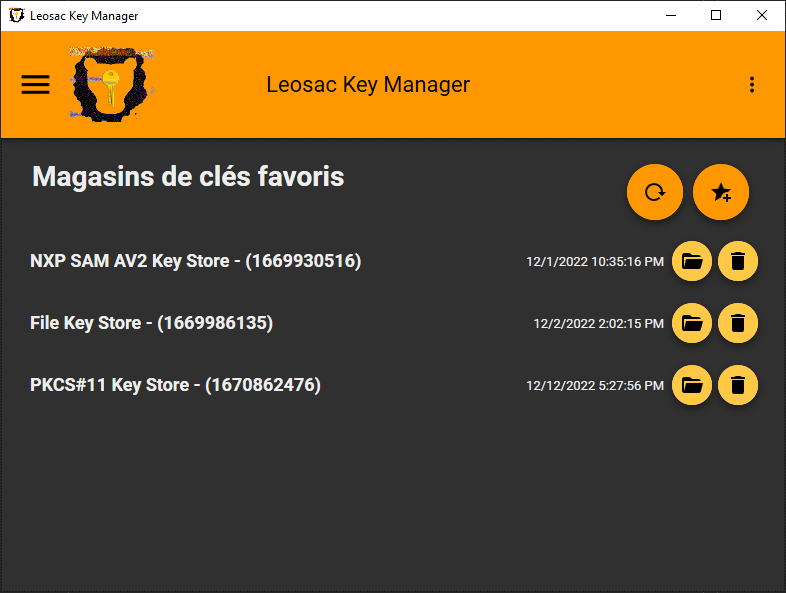
#### Propriétés du magasin de clés



#### Types de clés



# Favoris



Il est recommandé d’enregistrer dans les favoris les magasins de clés que vous utilisez fréquemment.

L’utilisation des favoris est également nécessaire pour effectuer des interactions entre différents magasins de clés (eg. publication, liaison, …).

1. <https://dotnet.microsoft.com/en-us/download/dotnet/8.0> [↑](#footnote-ref-1)
2. <https://aka.ms/vs/17/release/vc_redist.x64.exe> [↑](#footnote-ref-2)