

LEOSAC SAS



LEOSAC KEY MANAGER

VERSION 1.0

14/12/2022

DOCUMENTATION UTILISATEUR

AUTEUR

LEOSAC SAS

www.leosac.com

Table des matières

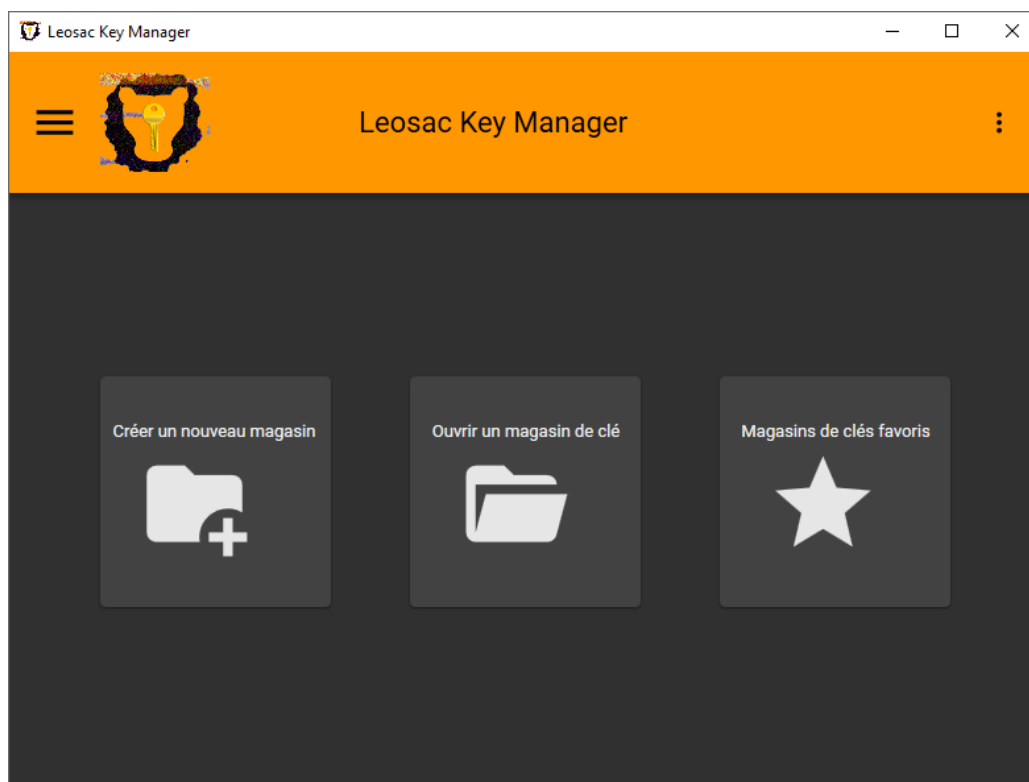
| | |
|--------------------------------------|----|
| LEOSAC KEY MANAGER..... | 2 |
| Accueil..... | 2 |
| Mode Sombre..... | 3 |
| Log Console..... | 3 |
| A propos..... | 4 |
| Plan de maintenance..... | 4 |
| Magasins de clés..... | 5 |
| Liste des clés..... | 6 |
| Recherche d'une clé..... | 6 |
| Création d'une nouvelle clé..... | 6 |
| Définition manuelle..... | 6 |
| Import d'un cryptogramme..... | 8 |
| Clés symétriques..... | 9 |
| Version de la clé..... | 9 |
| Somme de contrôle..... | 9 |
| Génération..... | 9 |
| Liaison..... | 13 |
| Impression..... | 13 |
| Clés asymétriques..... | 14 |
| Enregistrement dans les favoris..... | 14 |
| Edition du favori..... | 15 |
| Fermeture du magasin de clés..... | 15 |
| Types de magasins..... | 15 |
| Fichiers..... | 15 |
| NXP SAM AV2..... | 16 |
| HSM PKCS#11..... | 19 |
| Favoris..... | 20 |

LEOSAC KEY MANAGER

Leosac Key Manager est un logiciel de gestion 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.

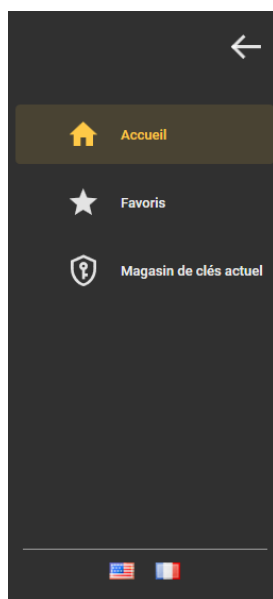
Accueil




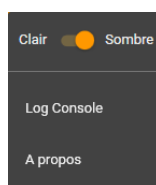
L'écran principal de Leosac Key Manager vous permet d'accéder rapidement aux fonctionnalités principales du logiciel.

Des « tuiles » vous invitent à créer un nouveau magasin de clés, 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.



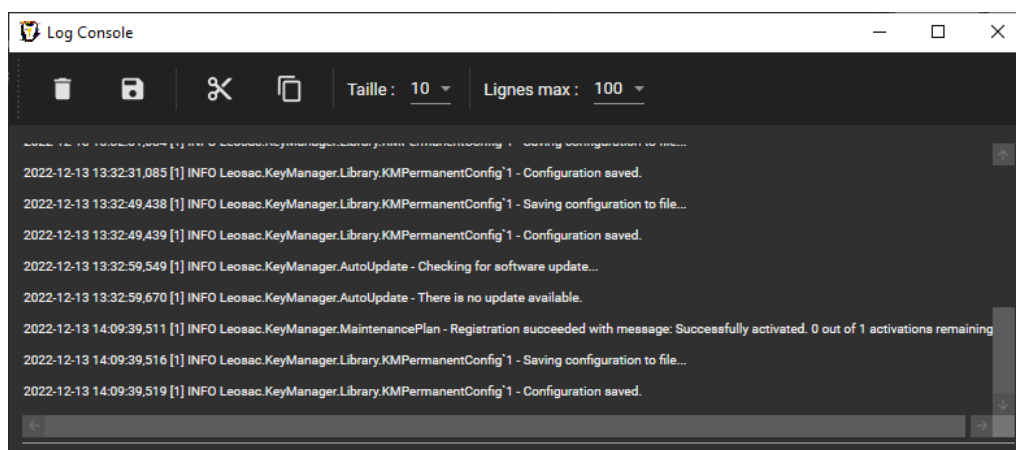
Sur la droite, un menu complémentaire  vous donne accès aux paramètres plus avancés et secondaires de l'application.



Mode Sombre

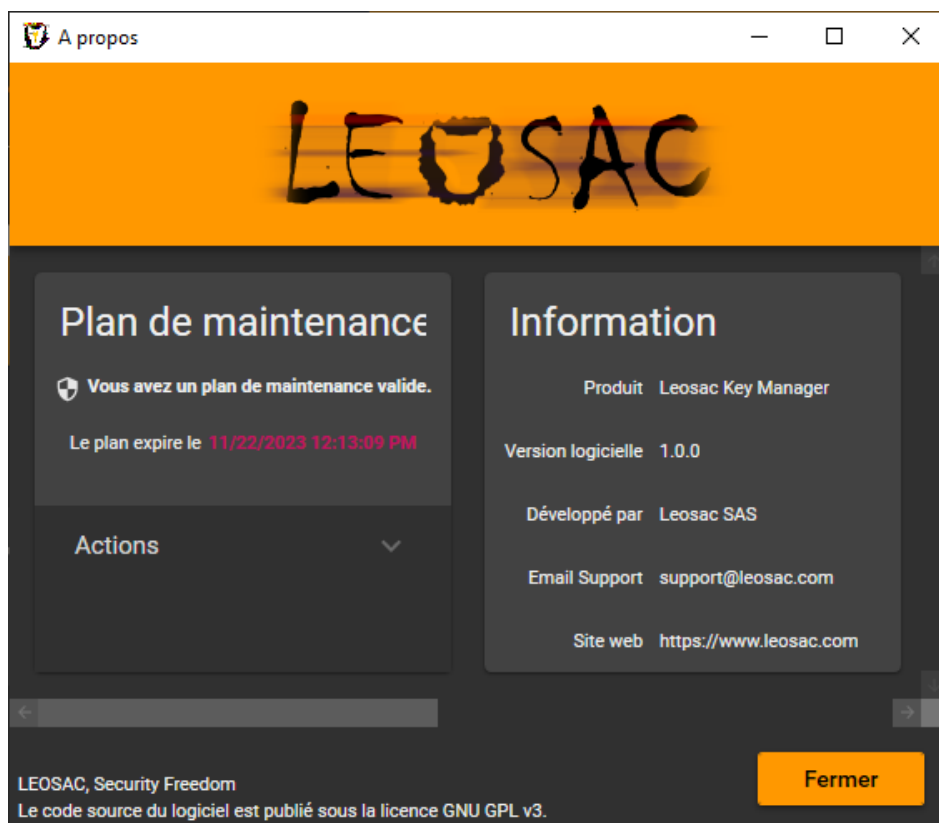
L'option  permet de basculer rapidement l'interface utilisateur d'un mode clair à un mode sombre. Ce choix est sauvegardé.

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.

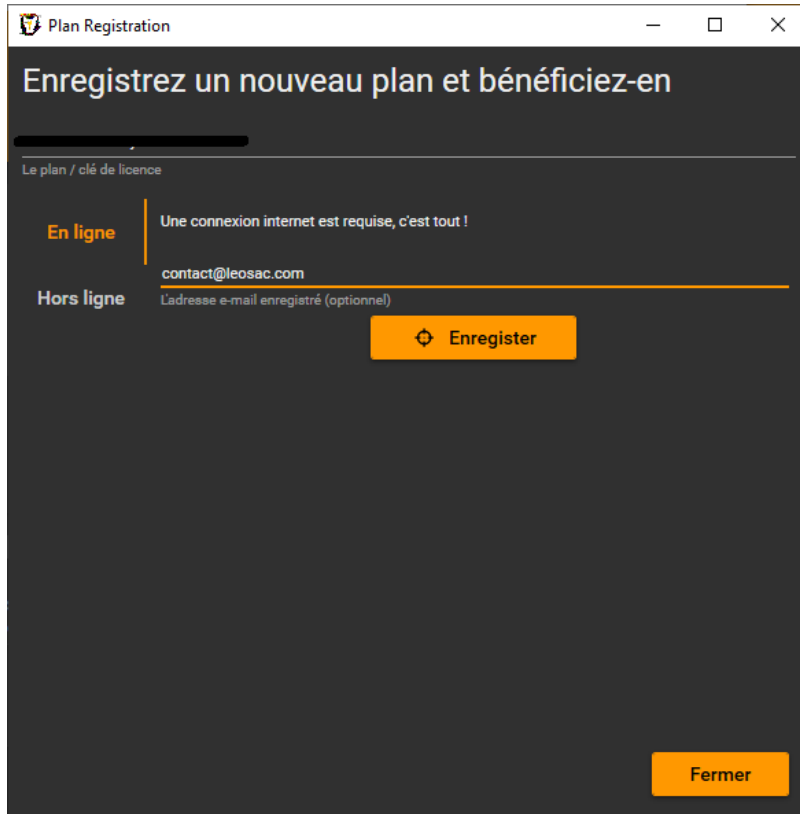
Des détails sur le plan de maintenance actuel sont par ailleurs affichés.

Plan de maintenance

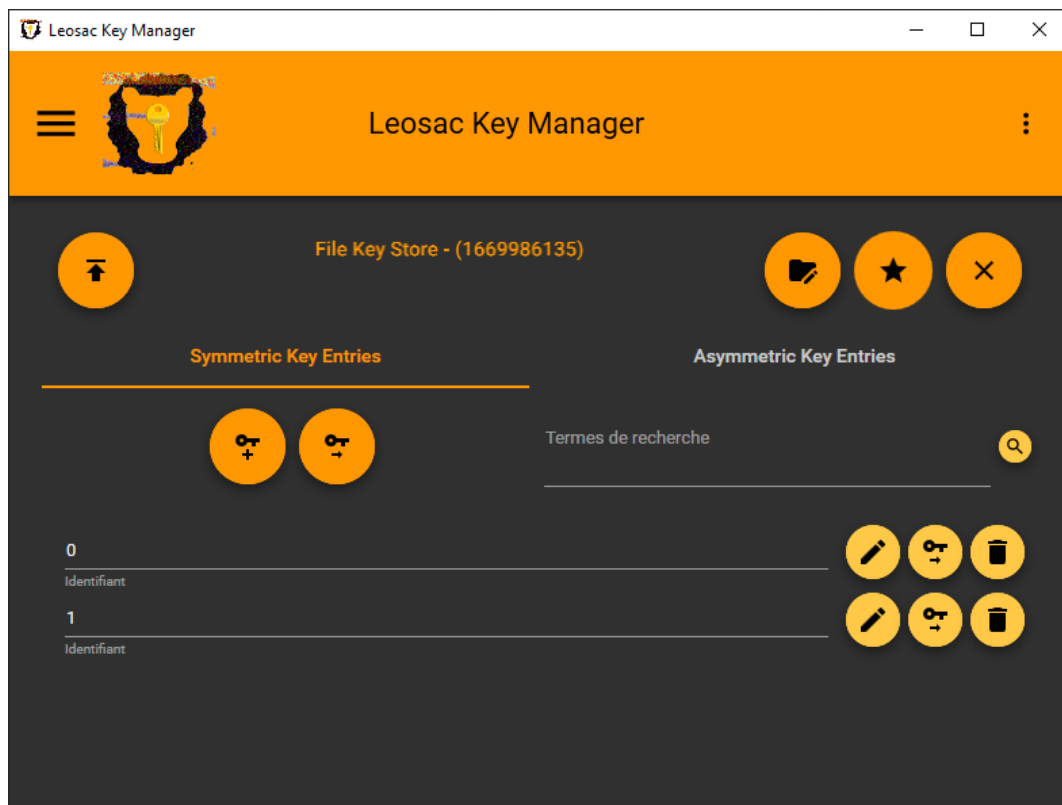
Il est fortement recommandé de souscrire à un plan de maintenance afin de garantir un support minimum de votre installation, de s'affranchir de toute limitation, de bénéficier des services annexes à l'applicatif et de contribuer financièrement au développement du logiciel.

Visitez <https://leosac.com/fr/key-manager/> 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 apparaître.

Identifiant de clé

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

Certains magasins peuvent nécessiter un formatage particulier de cet identifiant.

Variante

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

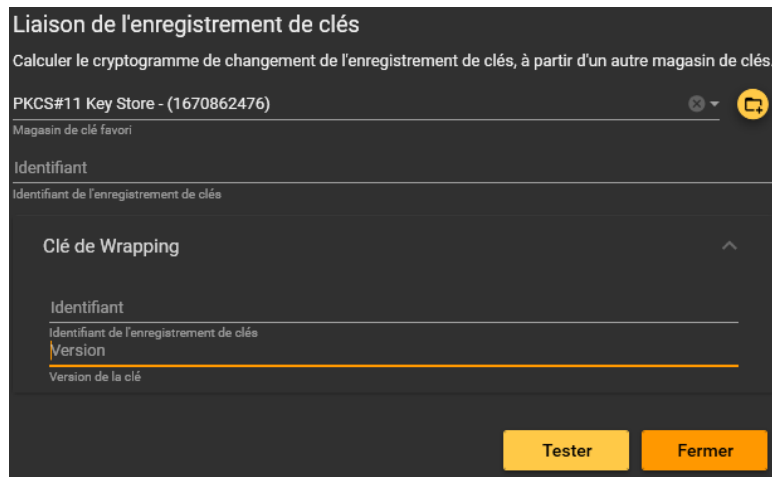
Plusieurs versions de clés peuvent co-exister pour un même enregistrement de clés en fonction de la technologie cible, chacune pouvant être configurée avec des valeurs différentes.

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.

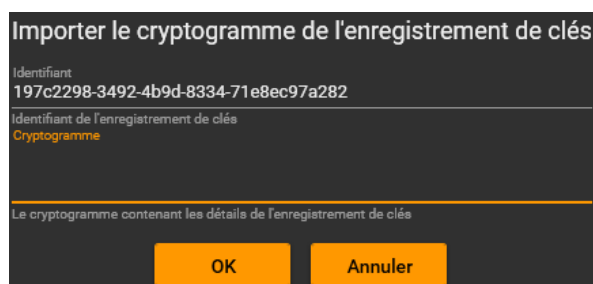
Les liaisons à ce stade sont simplement déclaratives, elles ne sont exécutées qu'au moment de la publication du magasin vers un magasin cible. Ce type d'opération est généralement effectué à partir d'un magasin de type « Fichiers », servant de modèle à la création de magasins de type « NXP SAM AV2/AV3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

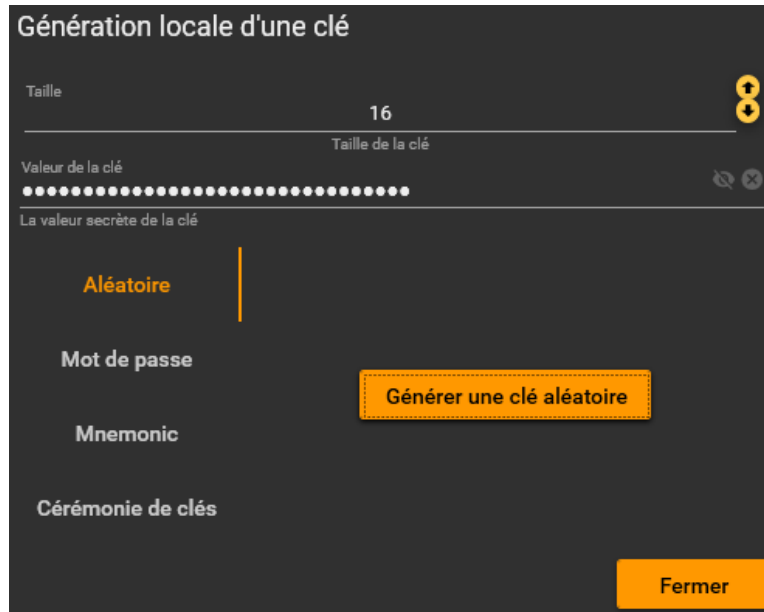
Pour les clés symétriques de type DES et AES, Il est recommandé d'utiliser l'algorithme KCV. Pour les autres, vous pouvez utiliser CRC32 ou un simple hash SHA256.

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 .

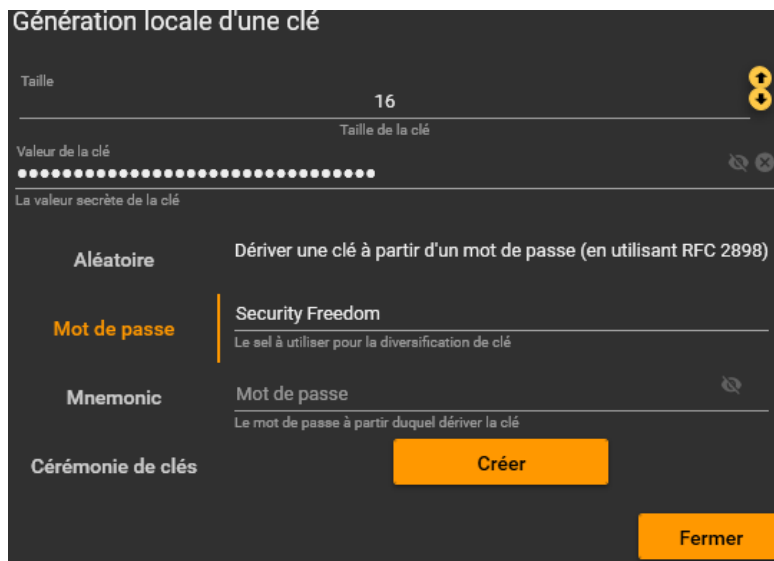
Plusieurs méthodes sont ici à votre disposition.

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.

Mnemonic

The screenshot shows the 'Génération locale d'une clé' (Local key generation) interface. At the top, the key size is set to 16. Below this, there are fields for 'Valeur de la clé' and 'La valeur secrète de la clé'. The main section is titled 'Créer une clé à partir de Mnemonic (BIP-39)'. It features three tabs: 'Aléatoire', 'Mnemonic' (which is selected), and 'Cérémonie de clés'. Under the 'Mnemonic' tab, there are two rows of word buttons. The first row contains: mixed, success, rail, invite, talent. The second row contains: retreat, marble, faith, blood, fragile, tilt. Below these are two rows of word buttons for the 'Cérémonie de clés' mode: pulp, glue, country, squirrel, share; wonder, similar, salmon, target, weird; trial, silver, pigeon. At the bottom, there are fields for 'Mots' and 'Mots mnemonic', a 'Phrase secrète' field, and a 'Créer' button. A 'Fermer' button is located at the bottom right.

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

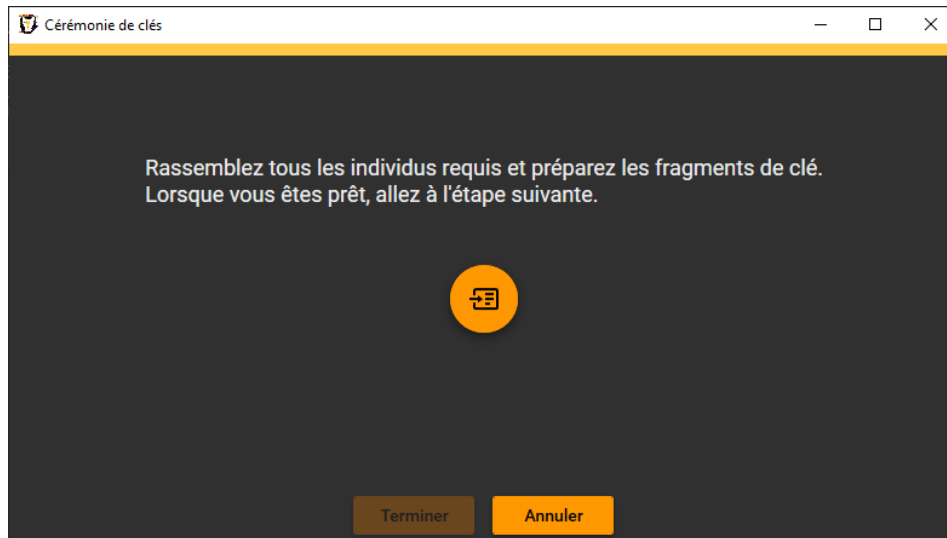
The screenshot shows the 'Génération locale d'une clé' (Local key generation) interface. At the top, the key size is set to 16. Below this, there are fields for 'Valeur de la clé' and 'La valeur secrète de la clé'. The main section is titled 'Exécutez une cérémonie de clé afin de réunifier la valeur d'une clé partagée entre plusieurs individus.'. It features three tabs: 'Aléatoire', 'Mot de passe', and 'Mnemonic'. Under the 'Mnemonic' tab, there are two rows of word buttons: pulp, glue, country, squirrel, share; wonder, similar, salmon, target, weird; trial, silver, pigeon. Below these are two rows of word buttons for the 'Cérémonie de clés' mode: pulp, glue, country, squirrel, share; wonder, similar, salmon, target, weird; trial, silver, pigeon. At the bottom, there are fields for 'Mots' and 'Mots mnemonic', a 'Phrase secrète' field, and a 'Créer' button. A 'Fermer' button is located at the bottom right.

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

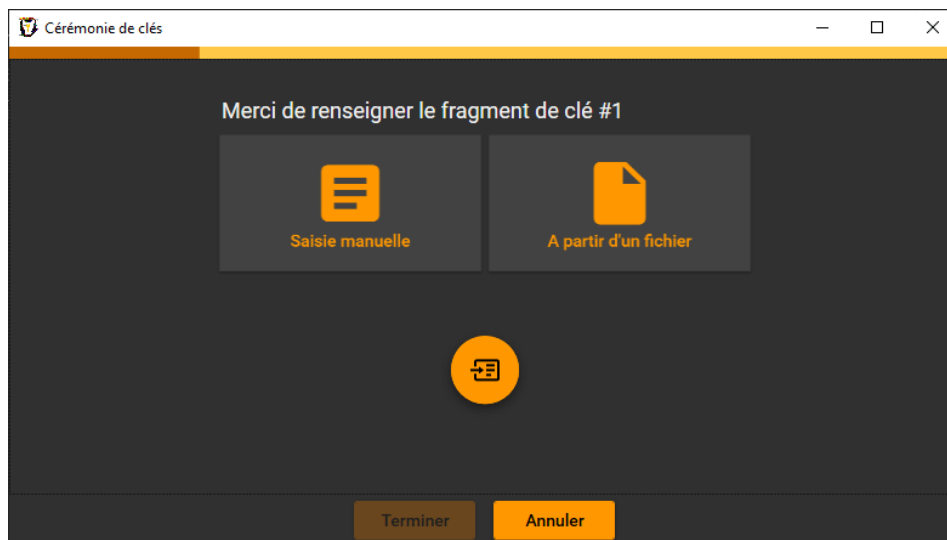
Définissez ici le nombre de fragments attendus et le type de cérémonie à effectuer.


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 perte d'un des fragments. La cérémonie de clé de type Shamir est donc ici recommandée.

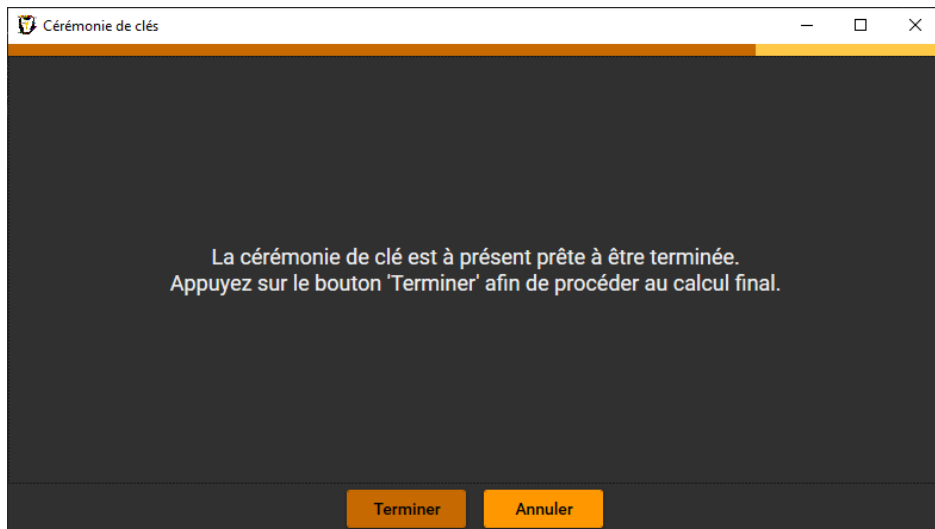
Cliquez sur « Démarrer la cérémonie de clés » afin d'ouvrir une interface utilisateur vous guidant à la réunification.



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



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



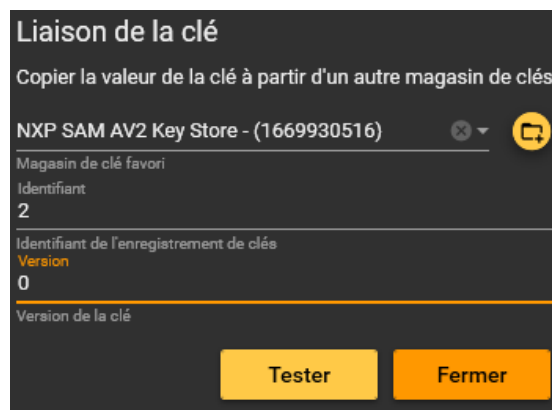
Une fois tous les fragments renseignés, terminez la cérémonie via le bouton « Terminer ».

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.

Export / Impression d'une clé

| | |
|-----------------------------|------------------|
| Valeur de la clé | |
| Taille de la clé | 16 |
| Somme de contrôle de la clé | E45E54 |
| Etiquettes de la clé | AES Symmetric |
| Note | |

Ce document est propriétaire, sensible et confidentiel. Il ne peut pas être utilisé, publié ou redistribué sans l'accord de son propriétaire.
Si vous avez reçu ce document par erreur, merci de le détruire immédiatement et de reporter cette action à un agent de sécurité.



Merci de visiter <https://leak.leosac.com/key/8563A3A8DD2917A18B84ED24983C8E4C294F3D44A42753399F8F92A27630ED9A>


Document généré avec **Leosac Key Manager** www.leosac.com

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

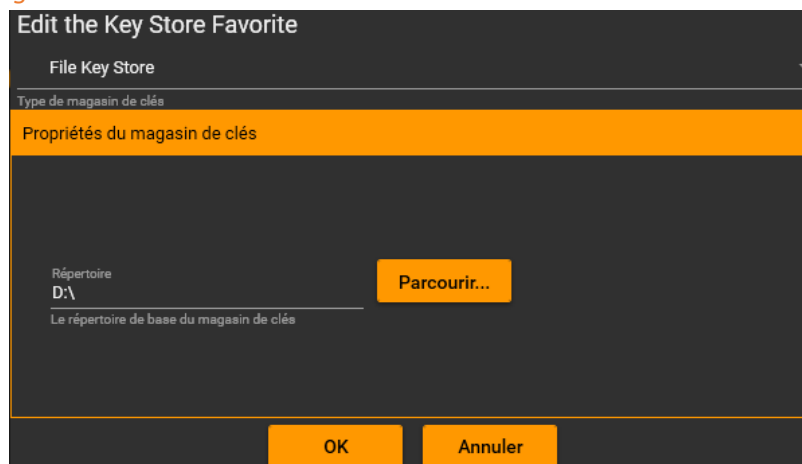
l'application ouverte. Pour ce faire utilisez le bouton



Types de magasins

Fichiers

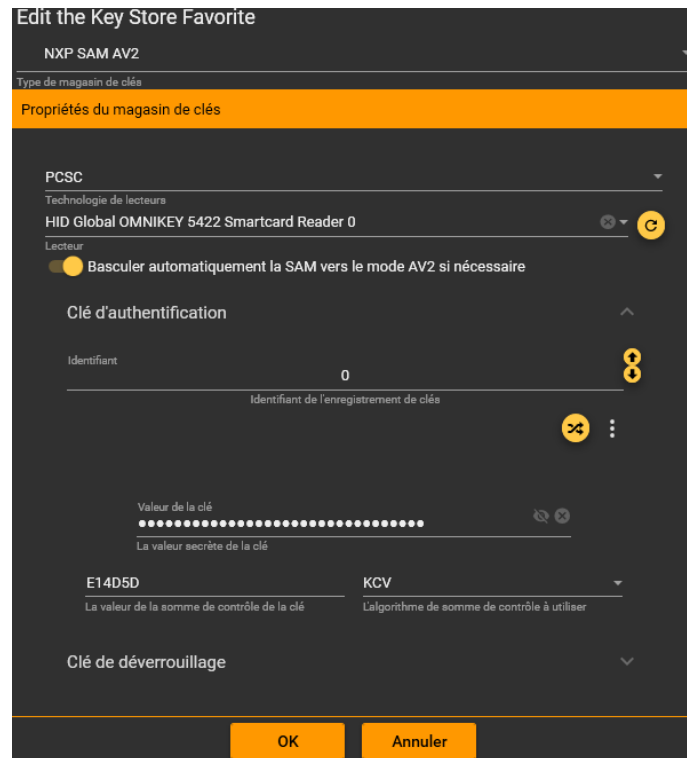
Propriétés du magasin de clés



Types de clés

NXP SAM AV2

Propriétés du magasin de clés



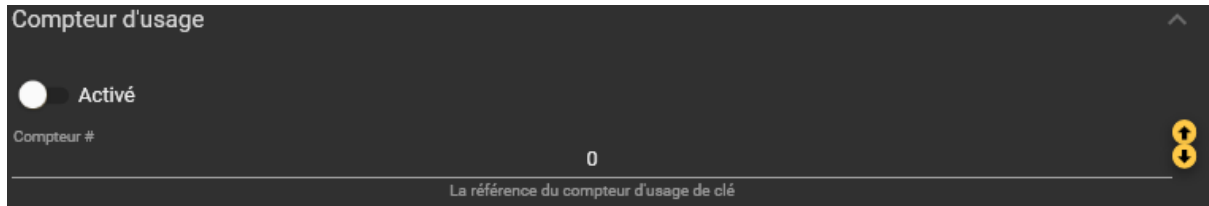
Types de clés

DES / 3DES / 3K3DES / AES128

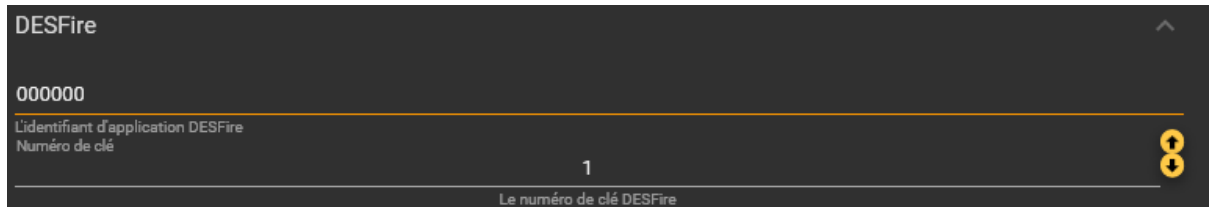
Options



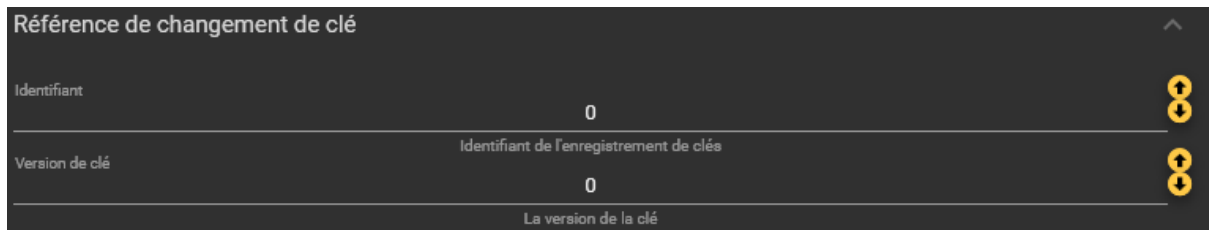
Compteur d'usage



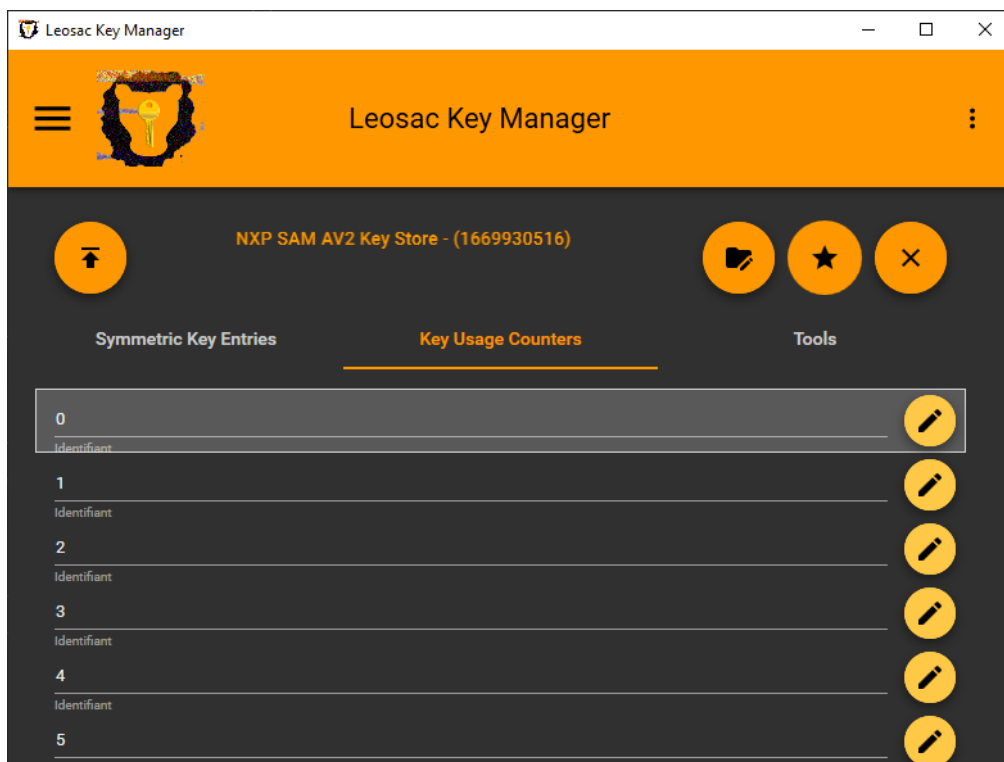
DESFire



Référence de changement de clé



Compteurs





Enregistrement de clés



Identifiant
0

Identifiant

Counter



Valeur 0  

La valeur actuelle du compteur



Limite 4294967295  

La limite du compteur

Référence de changement de clé

Identifiant 0  

Identifiant de l'enregistrement de clés

Version de clé 0  

La version de la clé

OK **Annuler**



Outils

Leosac Key Manager



Leosac Key Manager


- Symmetric Key Entries
- Key Usage Counters
- Tools**

Authentication SAM

Identifiant 0  

Identifiant de l'enregistrement de clés

Valeur de la clé 

La valeur secrète de la clé

SAM_KEY_AES

Type de clé SAM

Authentication

HSM PKCS#11

Propriétés du magasin de clés

Edit the Key Store Favorite

HSM PKCS#11

Type de magasin de clés

Propriétés du magasin de clés

Bibliothèque PKCS#11
E:\SoftHSM2\lib\softhsm2-x64.dll **Parcourir**

SlotId
Filtre de sélection du slot

Valeur de filtrage
Valeur de filtrage
CKU_USER PIN
L'utilisateur avec lequel s'authentifier Le code PIN de l'utilisateur

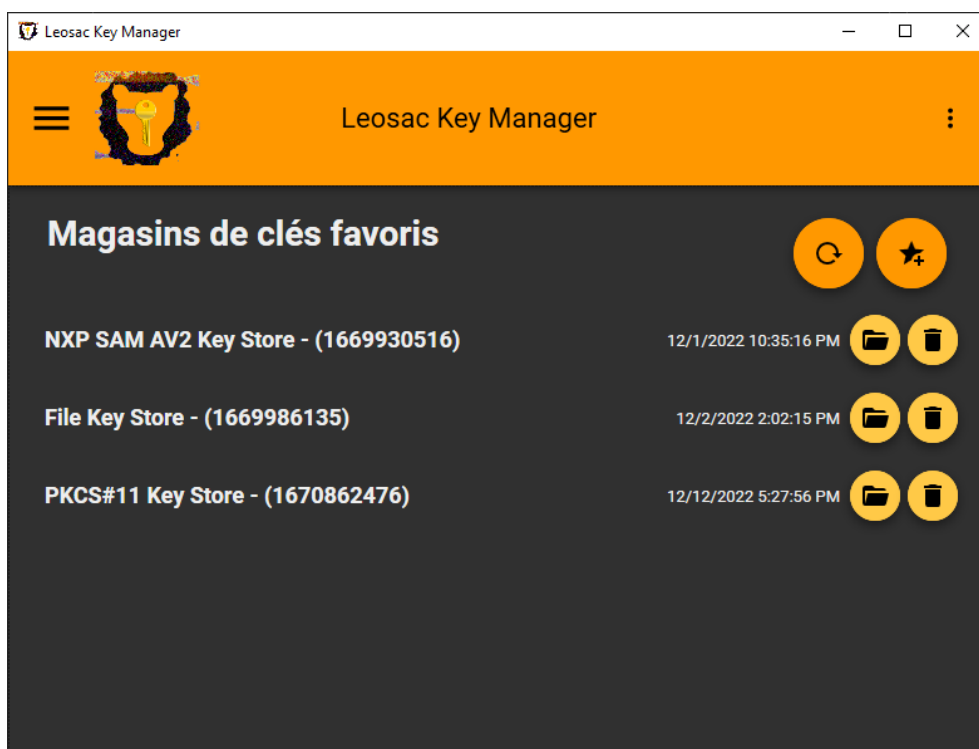
OK **Annuler**

Types de clés

Chiffrer Déchiffrer

Diversifier Extractible

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, ...).