GUIDE D'UTILISATION

RSA-DataSafe

Table des matières

1 Introduction **2**

2 Matériel Nécessaire **2**

3 Accès à l'application **2**
- 3.1 Récupérer les sources de l'application . . . 2
- 3.2 Installation des dépendances . . . 2
- 3.3 Compiler l'application . . . 2
- 3.4 Exécuter l'application . . . 3

4 Page d'accueil **3**
- 4.1 Authentification . . . 3
- 4.2 Inscription . . . 4

5 Menu d'accueil **5**

6 Chiffrement **6**

7 Déchiffrement **7**

8 Messagerie **8**
- 8.1 Menu de la messagerie . . . 8
- 8.2 Envoyer un message . . . 9
  - 8.2.1 Message . . . 10
  - 8.2.2 Signature . . . 11
- 8.3 Messages reçus . . . 11
- 8.4 Messages indésirables . . . 12

9 Paramètres **14**
- 9.1 Compte . . . 15
- 9.2 Sécurité . . . 15

10 Informations complémentaires **16**

1 Introduction

L'application "RSA-DataSafe" est une application bureau permettant aux utilisateurs, de pouvoir chiffrer/déchiffrer des données ou encore accéder à une messagerie sécurisée à l'aide du chiffrement à clé publique RSA .
L'application se veut très simple d'utilisation.Ce guide a par ailleurs été conçu afin de répondre aux moindres de vos questions et de visualiser le fonctionnement général.

2 Matériel Nécessaire

Le matériel nécessaire pour accéder à l'application est le suivant :

1. un P.C
2. L'installation de l'application (Détaillée dans la section suivante)

3 Accès à l'application

3.1 Récupérer les sources de l'application

Le lien suivant peut être utilisé afin de cloner ou télécharger l'archive contenant le code source.
https://github.com/RSA-DataSafe/RSA-DataSafe.git

1. Télécharger l'archive RSA-DataSafe.zip

   OU

2. Saisir sur l'invite de commande :
   ➤ git clone https://github.com/RSA-DataSafe/RSA-DataSafe.git

3.2 Installation des dépendances

Ouvrir un terminal et placer l'interpréteur de commandes dans le répertoire RSA-DataSafe. Saisir sur le terminal :

➤ ./configure.sh

3.3 Compiler l'application

Placer l'interpréteur de commandes dans le répertoire RSA-DataSafe. Saisir sur le terminal :

➤ make

3.4 Exécuter l'application

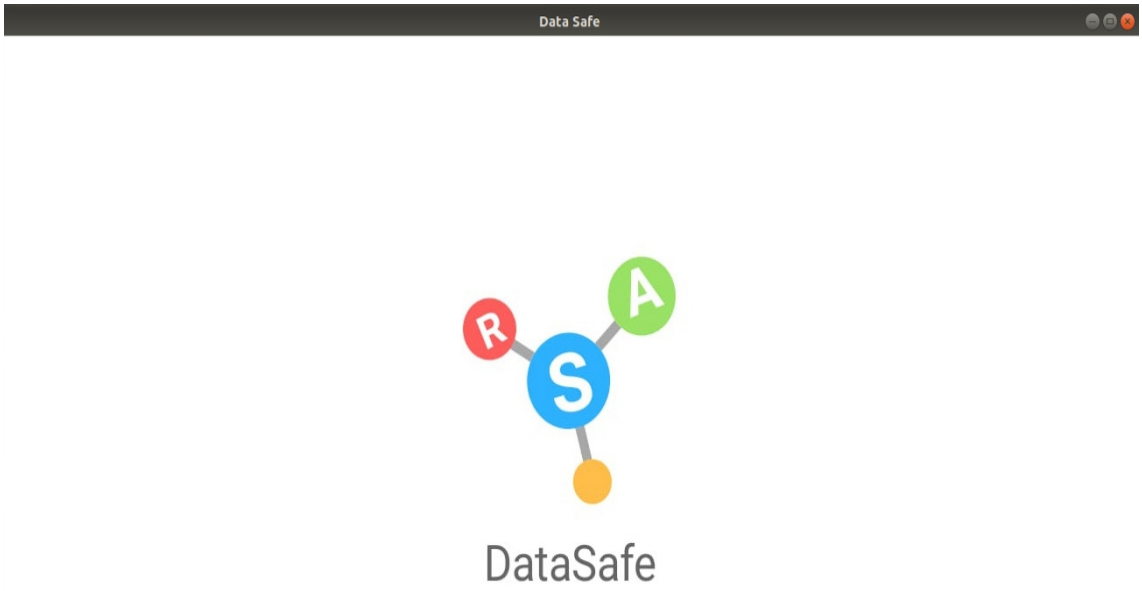
Afin d'exécuter le programme il suffit de taper sur l'invite de commande :

➤ make run

Ainsi vous pouvez poursuivre avec l'utilisation de l'application à travers l'interface graphique.

4 Page d'accueil

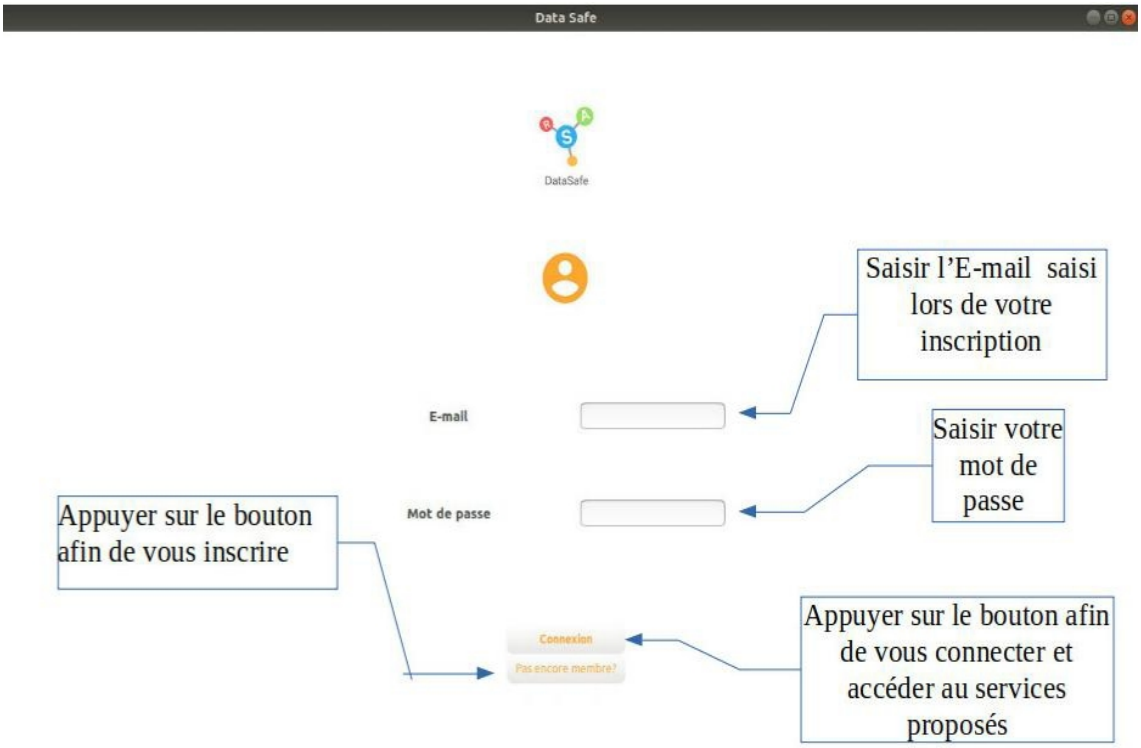
La page d'accueil s'affiche pendant un lapes de temps (4) puis s'en suis la page d'authentification.(4.1).



4.1 Authentification

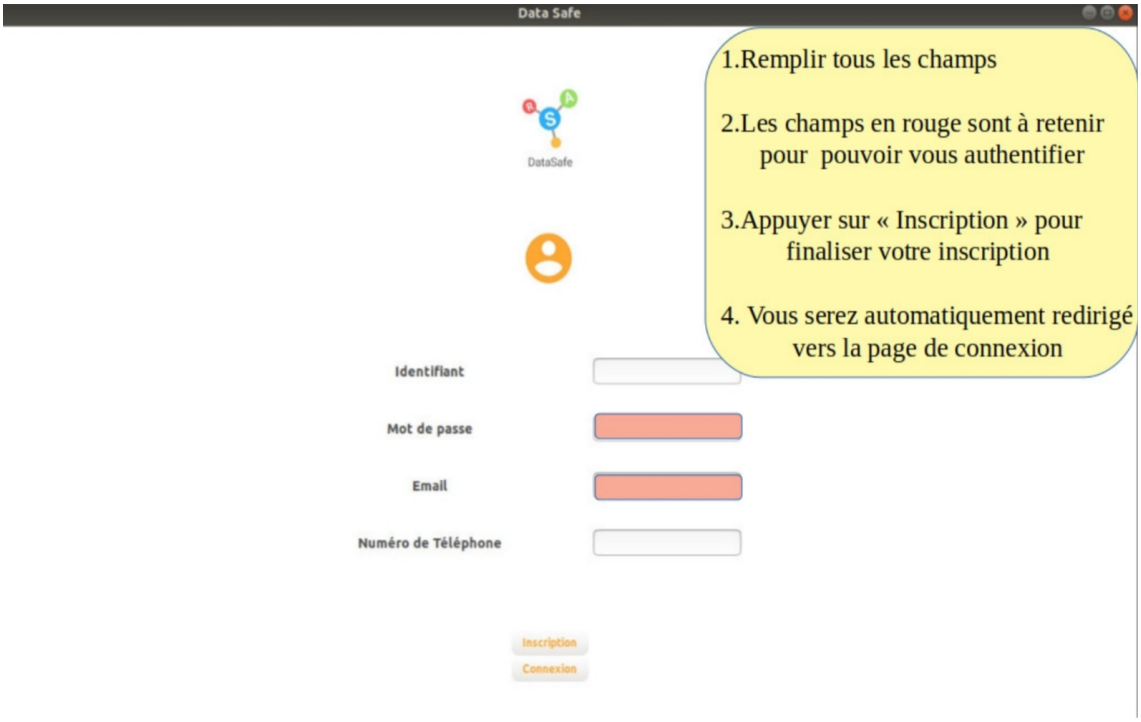
Si vous possédez des identifiants de connexion, il suffit de les saisir dans les champs correspondants puis de cliquer sur le bouton "connexion".

Si vous en êtes à votre première utilisation de l'application, il suffit de cliquer sur le bouton "Pas encore membre ?", afin de vous inscrire.Notez bien vos identifiants de connexions (E-mail , mot de passe).



4.2 Inscription

Pour permettre votre inscription dans la base de donnée, les champs contenus dans cette fenêtre devront être remplis. Une fois saisis, appuyez sur le bouton inscription pour finaliser l'inscription.
Lors de votre inscription une paire de clés est générée.

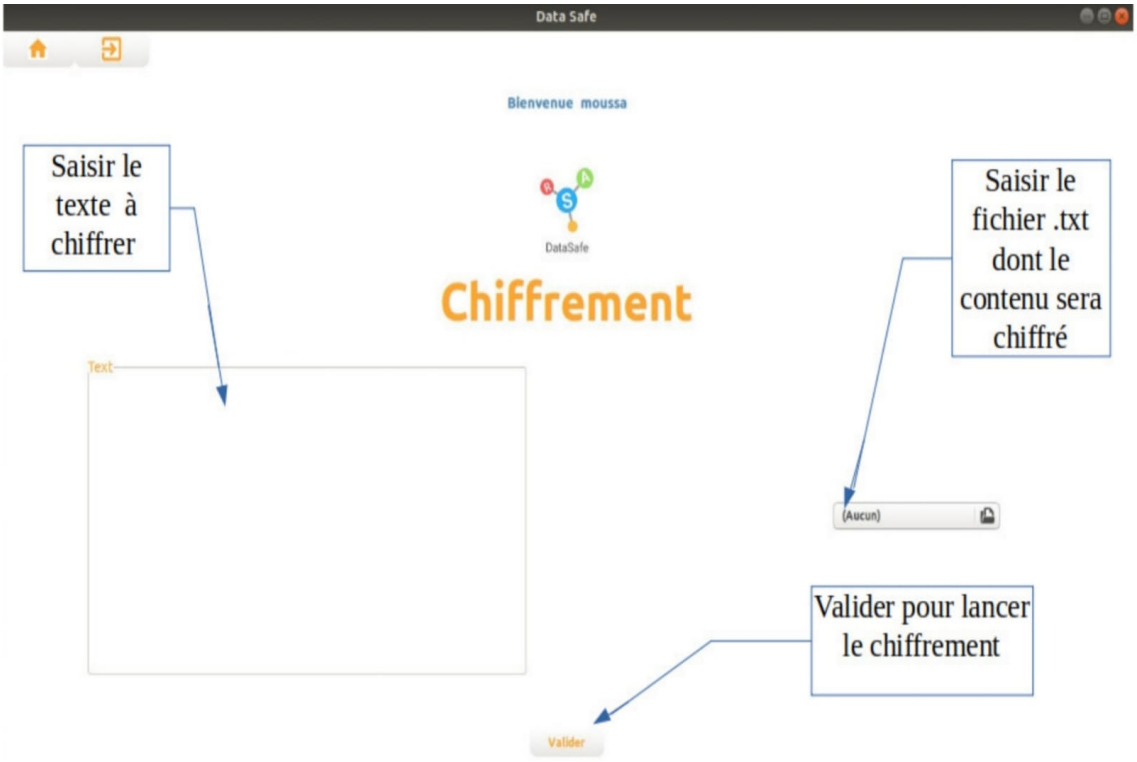


5 Menu d'accueil

Après avoir accéder à votre compte, un menu d'accueil est alors affiché afin de vous permettre de saisir la fonctionnalité souhaitée.

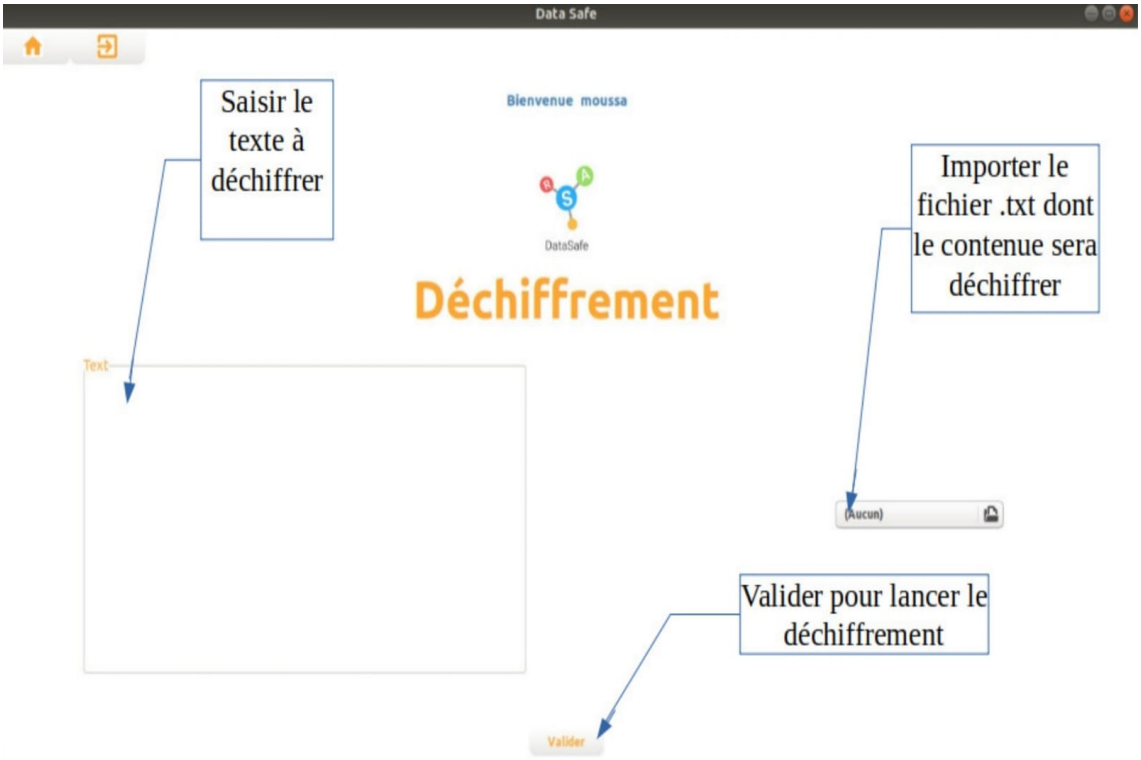
6 Chiffrement

En accédant à cette fonctionnalité, vous avez la possibilité de chiffrer vos données personnelles avec votre propre clé publique.
Vous n'avez pas à la saisir cela est traité directement par l'application.



7 Déchiffrement

Après avoir chiffré vos données personnelles, vous pouvez les déchiffrer en saisissant simplement le message chiffré.
Votre clé privée est alors utilisée afin de mener à bien le déchiffrement automatiquement.

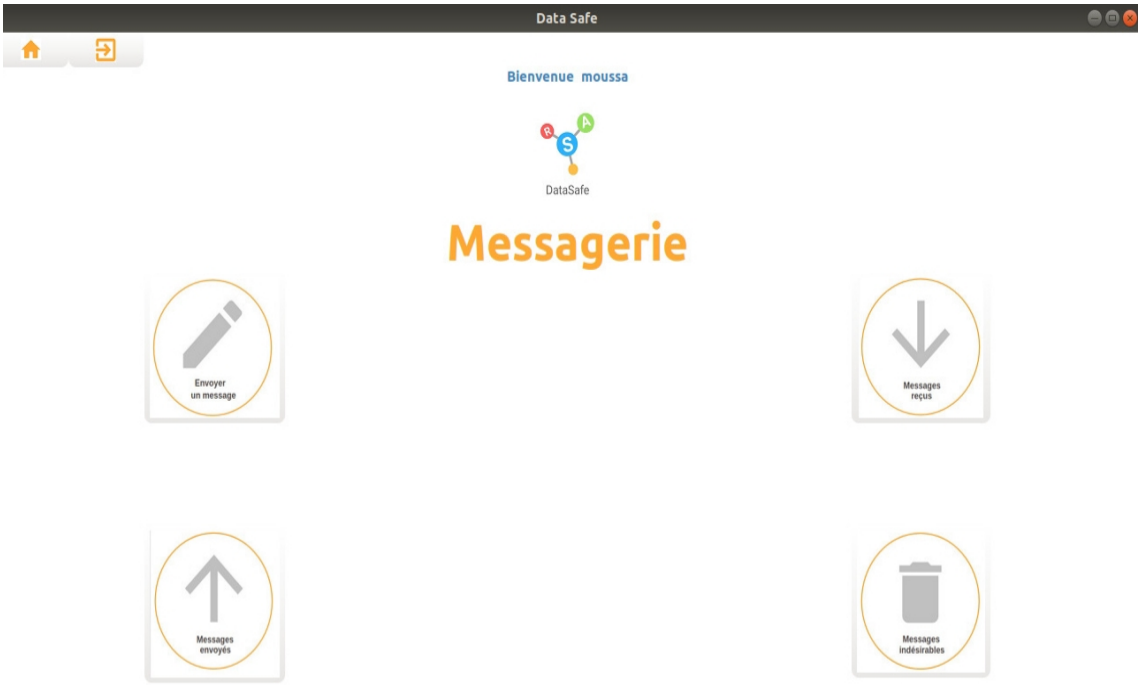


8 Messagerie

La messagerie vous permet d'envoyer des messages en toute sécurité, à n'importe quel utilisateur inscrit dans la base de donnée et d'en recevoir. Il suffit de saisir l'E-mail de votre destinataire et vous n'avez plus qu'à profiter de la messagerie cryptée.
En utilisant le chiffrement RSA, lors de chaque échange, la clé publique de chaque destinataire est récupérée afin de chiffrer les messages ; puis déchiffrés à l'aide de la clé privée.
Si le message est signé une vérification de la signature a eu lieu pour pouvoir positionner le message dans section correspondante (reçu ou indésirable).
Tout ses traitements ne sont pas visibles, vous pouvez donc directement profiter des avantages de cette messagerie sans vous en soucier.

8.1 Menu de la messagerie

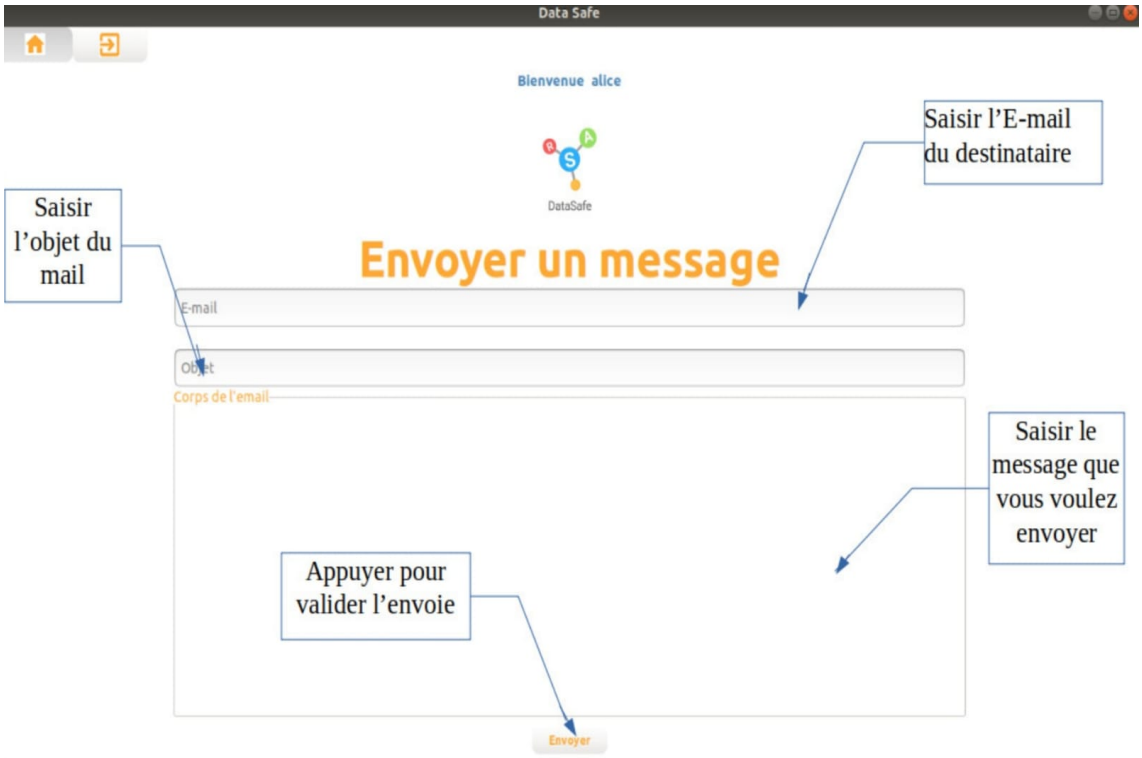
Le Menu de la messagerie vous permet de saisir les différentes actions possibles.



8.2 Envoyer un message

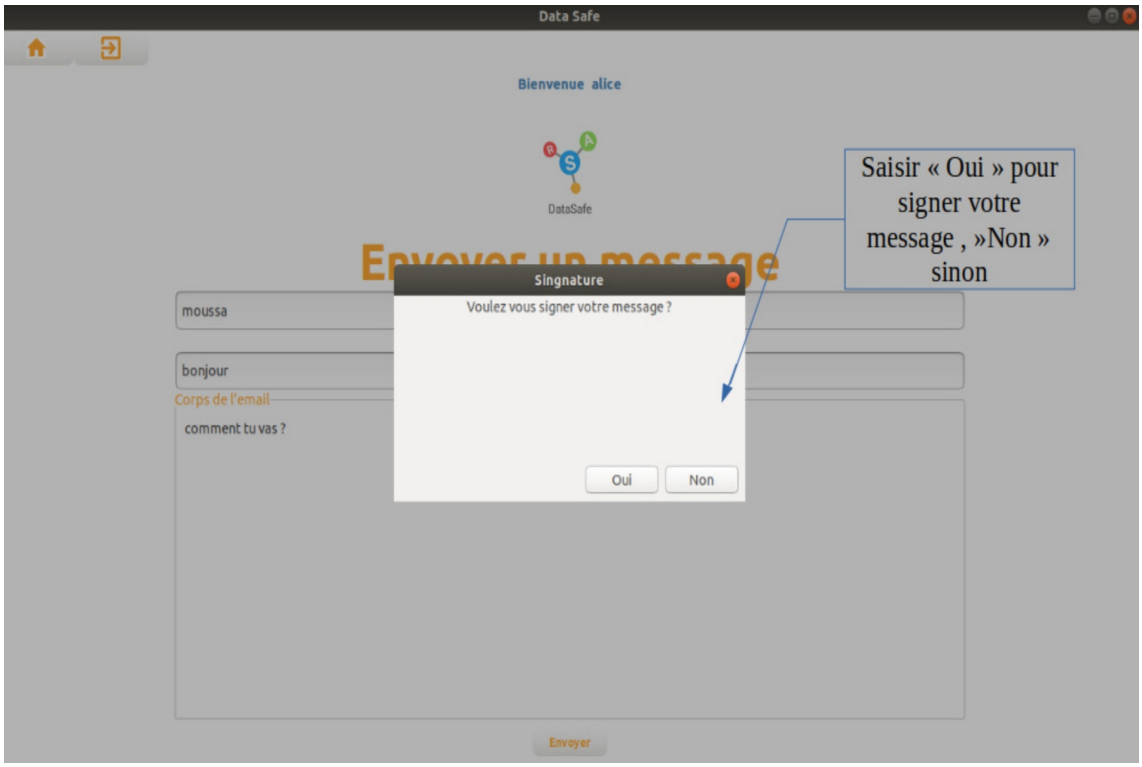
Vous pouvez envoyer un message à votre destinataire, en saisissant simplement son E-mail.

8.2.1 Message



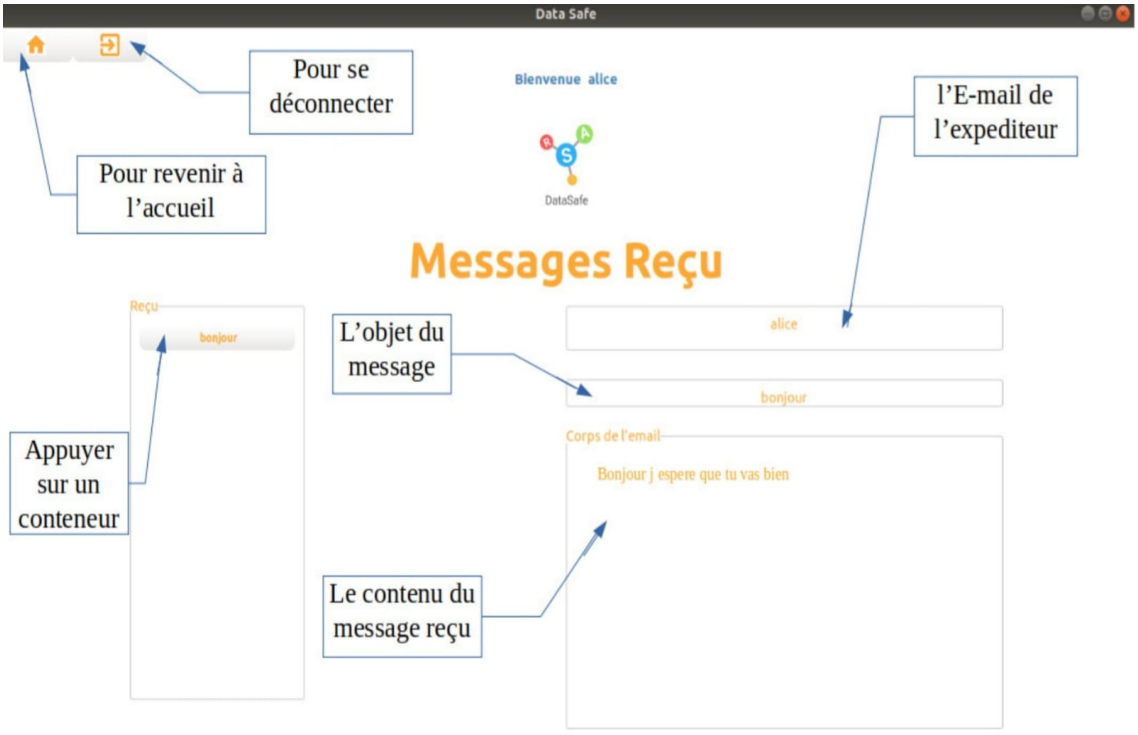
Après avoir saisi votre message une fenêtre pop-up apparaît afin que vous puissiez choisir entre signer ou non votre message.
Pour plus de sécurité nous vous recommandons de signer chaque message que vous envoyez.

8.2.2 Signature



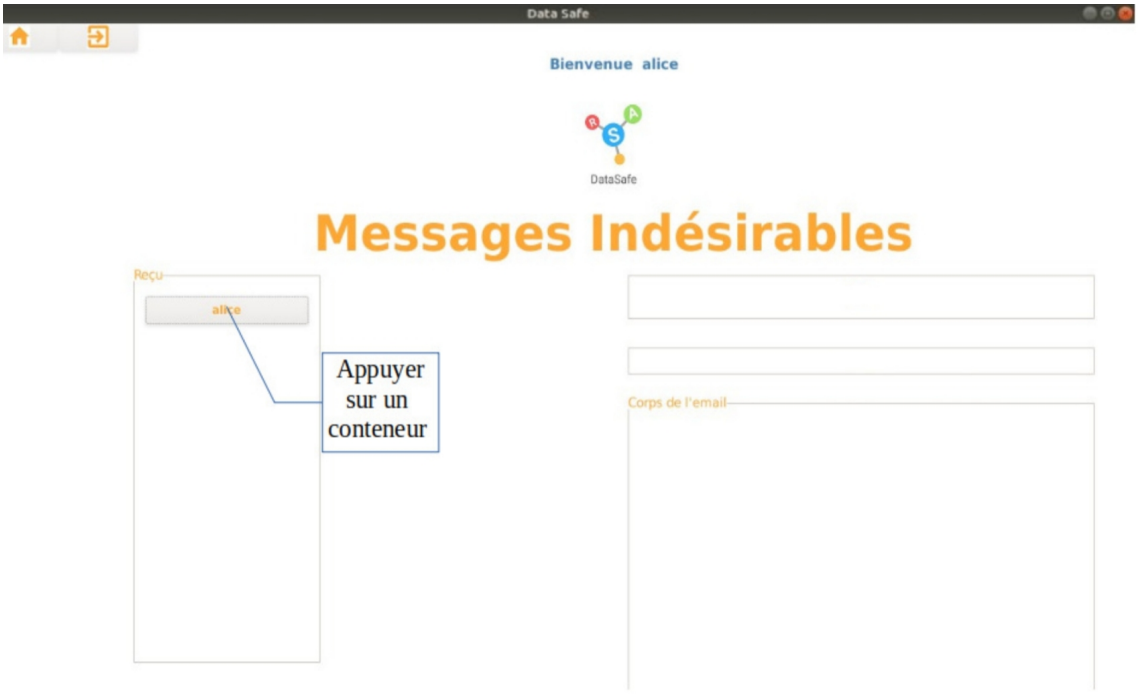
8.3 Messages reçus

Les messages affichés dans cet onglet sont uniquement ceux qui ont été signés et dont la signature a été vérifiée.



8.4 Messages indésirables

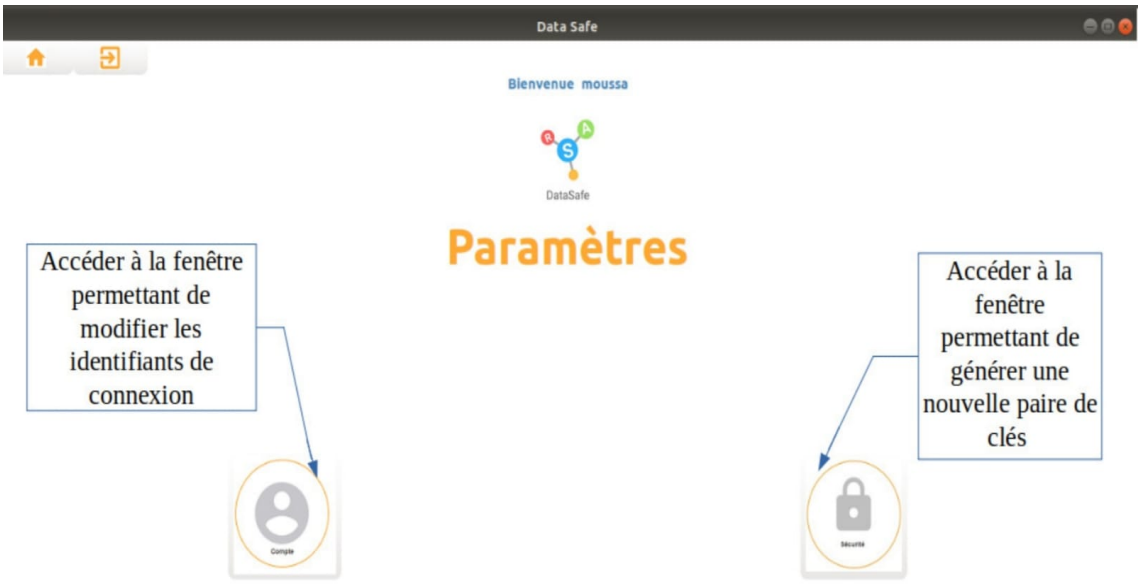
Vous trouverez donc dans cette section tous les messages non signés ou dont la signature n'est pas conforme .
Dans un premier temps avant d'accéder directement aux messages, en cliquant sur un des onglets, une fenêtre pop-up apparaît afin de savoir si vous voulez consulter ou supprimer le message indésirable.
⚠ Un message n'ayant pas de signature ou dont la signature n'est pas vérifiée n'est pas intègre et est donc non sûr.


Data Safe
Bienvenue alice
DataSafe
Messages Indésirables
Reçu
alice
Appuyer sur un conteneur
Corps de l'email

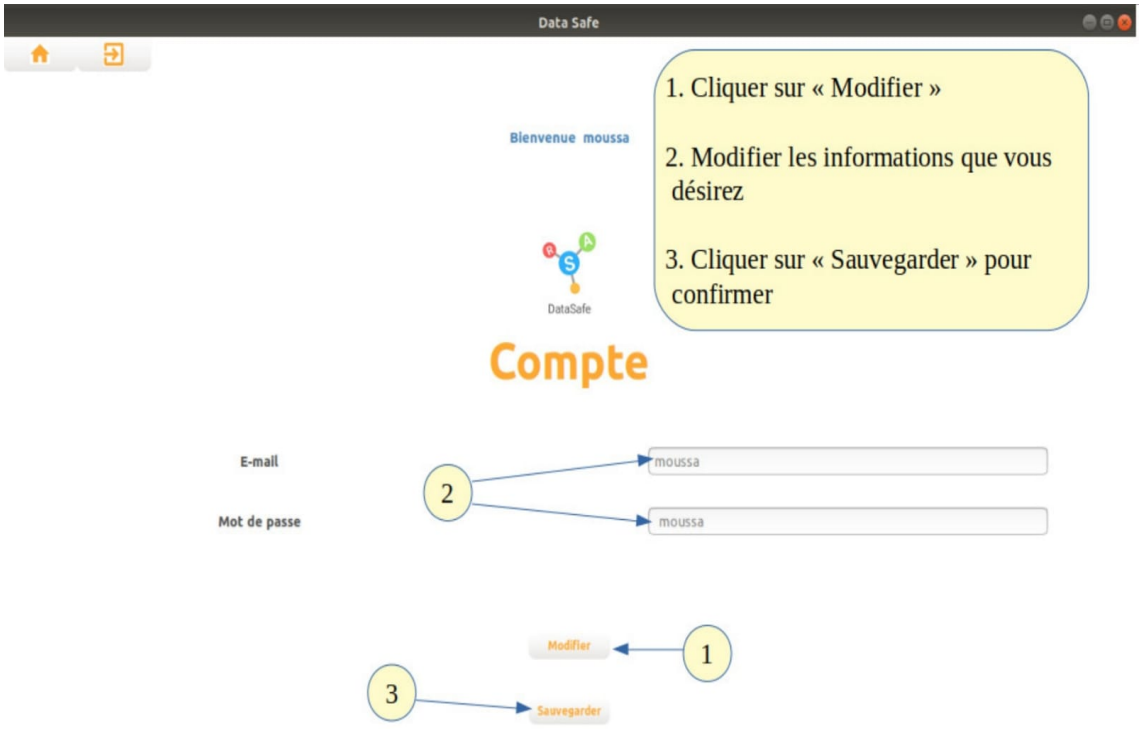

Data Safe
Bienvenue moussa
DataSafe
Data Safe
Voulez vous afficher ou supprimer ce message!
Reçu
bonjour
Saisir pour afficher le message.
Saisir pour supprimer définitivement le message.

9 Paramètres

Cette section vous permettra de modifier vos identifiants de connexion ainsi que votre paire de clés.

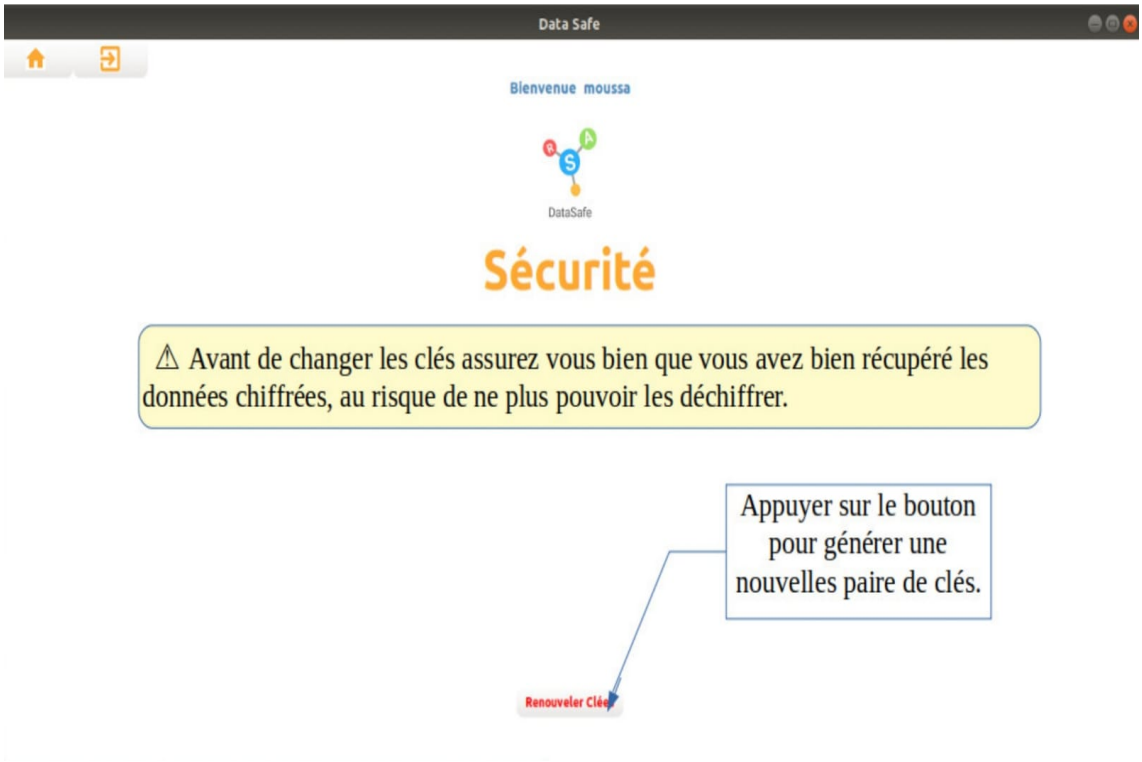


9.1 Compte



9.2 Sécurité

⚠ Une fois vos clés modifiées, les messages chiffrés avec l'ancienne paire de clés ne pourront plus être déchiffrer.



10 Informations complémentaires

Cette application a été réalisée par un groupe de huit étudiants dans un cadre pédagogique au sein de l'Université de Versailles Saint-Quentin-En-Yvelines.
Dans un souci d'amélioration continue de notre application toute proposition d'amélioration est la bienvenue.L'application sera donc régulièrement mise à jour. Vous pouvez donc accéder à la dernière version sur le lien ci-dessous :
https://github.com/RSA-DataSafe/RSA-DataSafe.git