Users Guide

Version 4.0.5-246-g427649bc

Lybero developement team

2019-10-31

Version : 4.0.5-246-g427649bc

Summary

1 Introduction

1.1 Sécurité

CryptnDrive de Lybero.net est un logiciel serveur web permettant le stockage, le partage et le transfert de fichiers et de textes de manière chiffrée sans aucune installation de logiciels sur les machines des utilisateurs.

Il est utilisable de plusieurs manières : en s'enregistrant sur notre instance de démonstration https://drive.lybero.net où nous ne garantissons le stockage de l'information que pendant 1 mois, via une instance que Lybero.net installe et administre pour votre compte, ou bien via une instance installée par une autre organisation (la votre par exemple).

L'ensemble des chiffrements est fait de bout en bout, via un chiffrement fait en javascript dans le navigateur pour les informations. Les informations sont stockées dans une base de données mongodb. Le serveur web central est extrèmement passif, il reçoit des informations et les stocke, assure la synchronisation des informations avec les navigateurs des clients et l'envoie des notifications. Il n'a aucune fonction de traitement des informations.

1.2 Sécurité

L'authentification est faite de manière flexible, ou bien de manière autonome ou bien via oauth2 (Google, . . .). Les clés publiques sont stockées sur le serveur de fichiers, les clés privées sont stockées chiffrées avec la phrase de passe des utilisateurs et ne sont déchiffrées que dans les navigateurs.

Chaque dépôt de fichiers est chiffré avec une clé AES256 spécifique. La clé AES est elle-même chiffrée avec la clé publique de chaque utilisateur ayant accès au partage.

Le partage d'un dépôt de fichiers donc son transfert peuvent se faire entre des personnes enregistrées dans le système, ou pas encore enregistrée, ou bien avec un groupe de recouvrement que nous appelons groupe à quorum.

Lorsqu'un partage d'un dépôt de fichiers est fait avec un groupe à quorum, les membres du groupe à quorum ne peuvent pas accéder au dépôt de fichiers. Par contre, ils peuvent inviter des tiers (enregistrés ou pas). Si un tiers invité accepte l'invitation et si un quorum (par exemple 3 sur 5) accepte son accès, l'invité pourra accéder au dépôt de fichiers. Il y a donc séparation stricte (cryptographique) entre l'autorisation d'accès et l'accès à l'information. A aucun moment, un membre du quorum (que nous appelons administrateur de secrets) ne peut accéder à l'information déchiffrée, et tant que le quorum ne l'a pas accepté, le demandeur ne peut pas non plus accéder à l'information (elle reste chiffrée). Ce mécanisme offre à la fois sécurité par le nombre et flexibilité pour

les organisations. Il permet de reproduire cryptographiquement les procédures fonctionnelles d'accès à l'information.

Ce manuel est décomposé en 3 parties principales :

- Le manuel utilisateur
- Le manuel d'installation
- Des éléments sur les algorithmes utilisés.

2 Termes utilises

2.1 Définitions

Terme	Définition
Dépôt de fichiers	On peut aussi parler de coffre-fort. L'unité de partage de fichiers. Un dépôt de fichiers contient un ensemble de fichiers et de répertoires. Ils sont partagés entre un ensemble de personnes. Seules ces personnes ont accès au contenu du dépôt de fichiers.
Invité ou "guest"	Une personne n'ayant pas encore de compte dans le drive et qui est invitée à rejoindre l'application afin d'avoir accès à un contenu chiffré.

3 Utilisation

3.1 Comment s'enregistrer sur le service

Allez sur https://drive.lybero.net. Vous arrivez alors sur l'écran de login :

Vous cliquez alors sur le lien « Création d'un compte ? » pour procéder à votre enregistrement. Vous arrivez alors sur 'écran suivant :

Vous devez alors entrer votre email et un mot de passe (à retenir ou stocker dans son logiciel de gestion de mot de passe préféré tel que keepass par exemple).

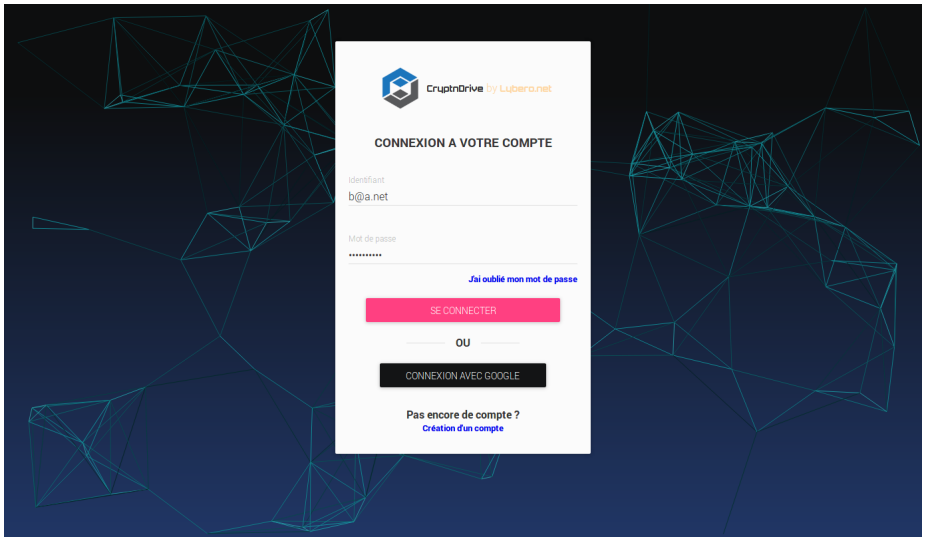


Figure 1: Écran de login

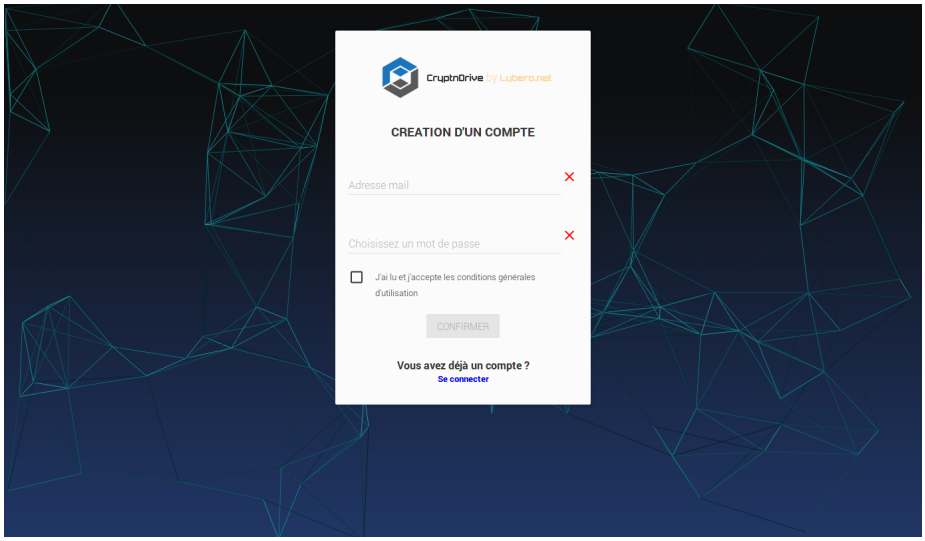


Figure 2: Formulaire d'inscription

Le mot de passe ne sera accepté que s'il a une complexité raisonnable (mélange de miniscules, majuscules, numéro et ponctuation idéalement, éviter les caractères accentués). Vous recevrez alors un mail sur l'adresse mail indiqué. En cliquant sur le lien indiqué dans le message reçu vous finaliserez la procédure d'enregistrement dans https://drive.lybero.net .

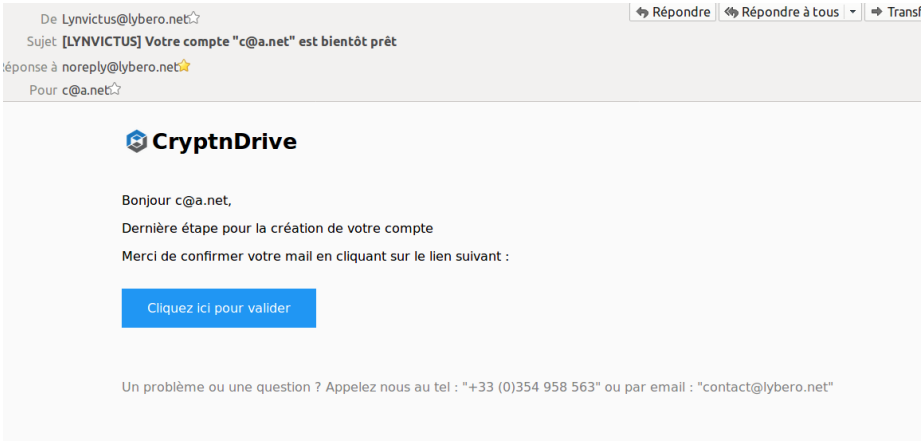


Figure 3: Mail de confirmation d'enregistrement

Lorsque vous cliquerez sur le lien de confirmation, vous arriverez sur l'écran suivant et pourrait accéder à l'écran de login avec votre adresse email pré-remplie. Vous n'aurez plus qu'à entrer votre mot de passe pour vous connecter.

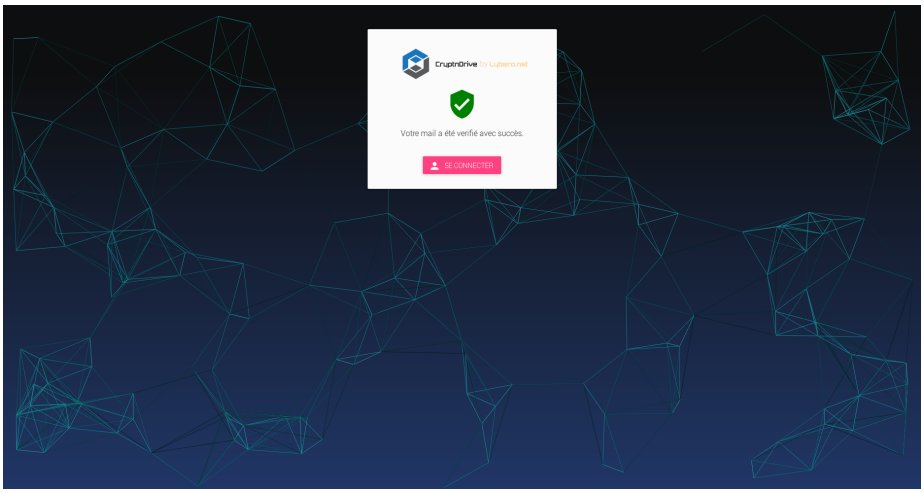


Figure 4: Finalisation de l'inscription

3.2 L'écran d'accueil

Après vous être connecté, vous arriverez sur l'écran d'accueil (cf figure *Page d'accueil*) :

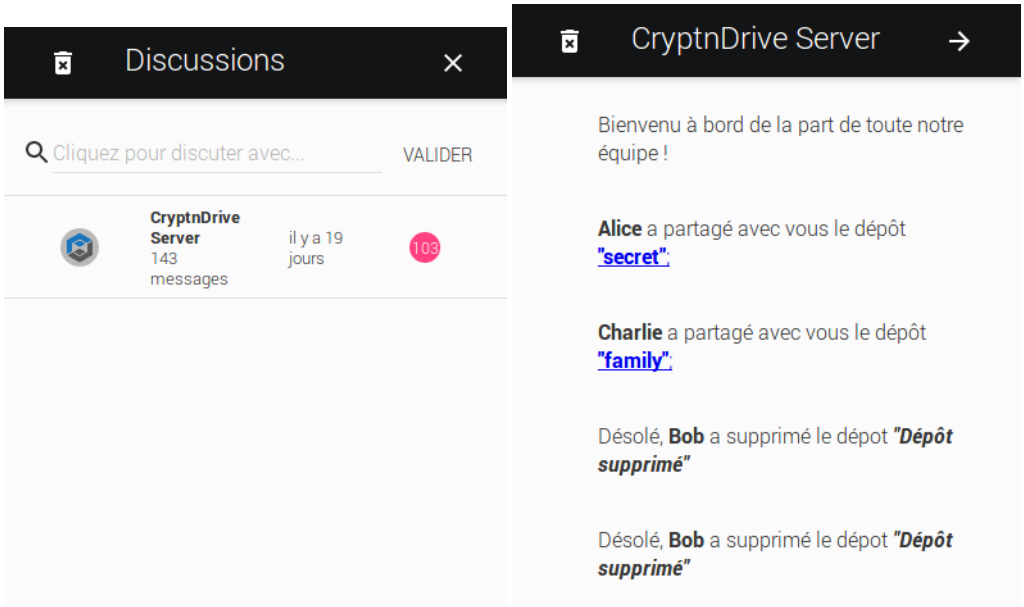
Figure 5: Page d'accueil

Cet écran d'accueil vous permet :

- de voir l'ensemble de vos dépôts de fichiers, mais vous n'en avez encore aucun,
- de créer un nouveau dépôt de fichiers (New dataroom ou),
- de créer une URL de dépôt de fichiers pour un tiers (new URL),
- de voir la liste des urls que vous avez précédemment générées (URLs),
- de changer vos réglages par défaut ou de vous déconnecter (menu en haut à droite),
- de voir les notifications (messages et événements) vous attendant ( ).

Le menu « Accueil » permet de revenir à l'écran d'accueil.

Les notifications sont l'ensemble des messages que l'application vous adresse (création de dépôt, proposition de partage, . . .). Vous y accédez en cliquant sur l'icone , puis en choisissant l'origine des notifications.



L'ensemble des notifications systèmes (information de partage de dépôt, de demande d'accès, . . .) proviennent du serveur CryptNDrive .

3.3 Création d'un nouveau dépôt de fichiers

Nous allons maintenant créer un nouveau dépôt de fichiers. Pour cela, nous utilisons le bouton + en bas à droite de l'écran d'accueil. Après la création, on arrive sur la page de modification du dépôt de fichiers.

Suivant que l'on est sur un écran large ou pas, l'affichage n'est pas tout à fait le même.

L'écran est organisé en 4 sections. La section **Fichiers** contenant les fichiers, la section **Commentaires**, la section **Utilisateurs** et la section **Propriétés**.

Le nom du dépôt chiffré est modifiable dans la section ** Propriétés**, en tapant dans l'entrée de texte "Nom". Le titre du dépôt chiffré n'est pas chiffré dans la base de données.

Vous pouvez ajouter des fichiers à tout moment en les « glissant – déposant » sur la page depuis votre gestionnaire de fichiers ou bien en cliquant sur le bouton .

Une fois un fichier ajouté, vous verrez alors l'écran suivant :

Pour ajouter un commentaire, il suffit de le taper dans la zone de saisie sous

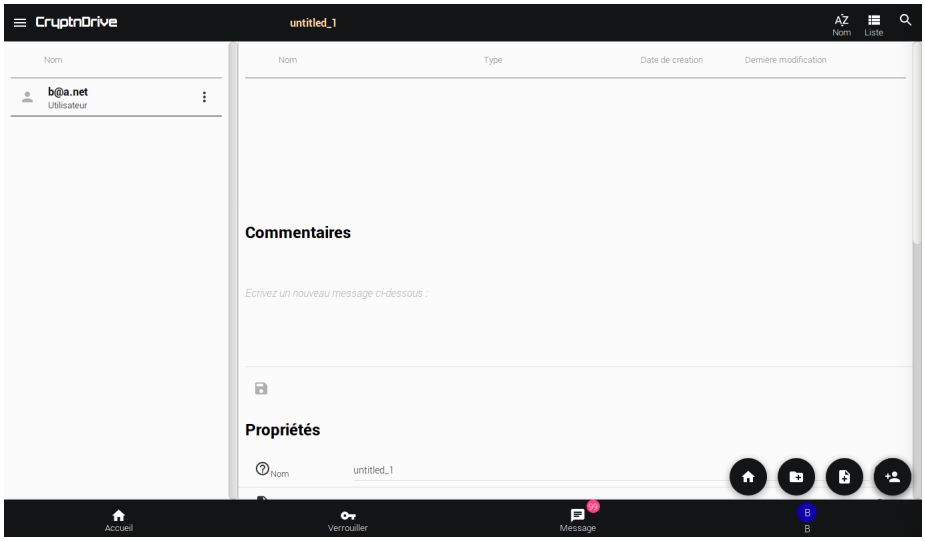


Figure 6: Nouveau dépôt de fichiers - écran large

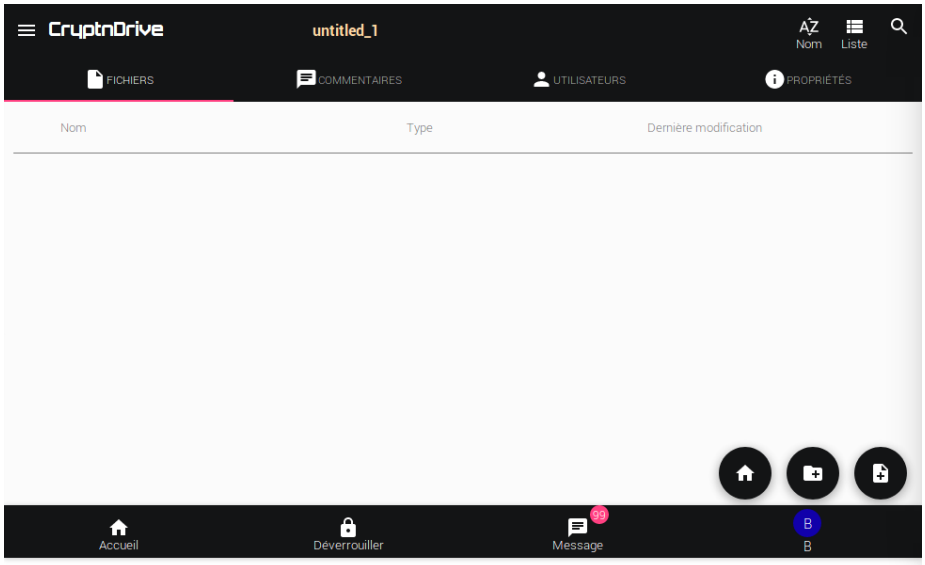


Figure 7: Nouveau dépôt de fichiers - écran type tablette

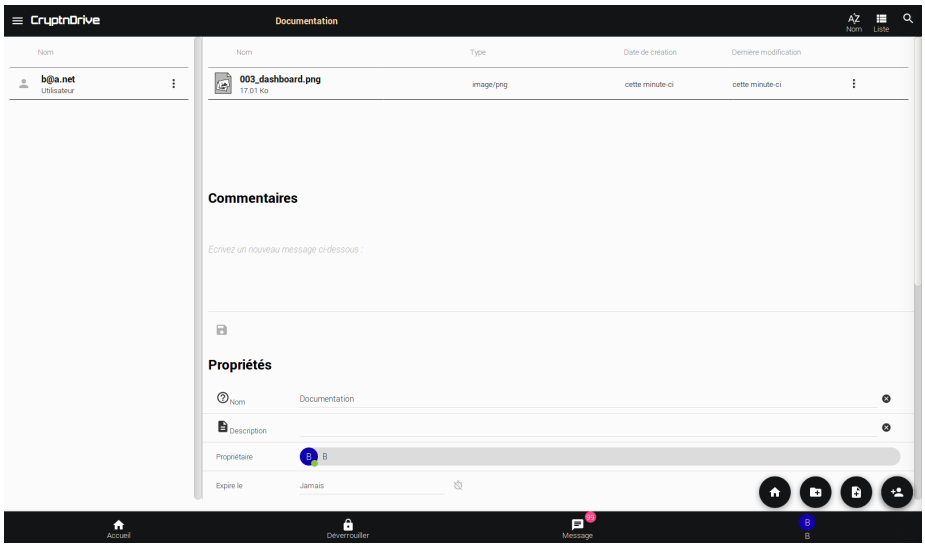


Figure 8: Un dépôt de fichiers version desktop

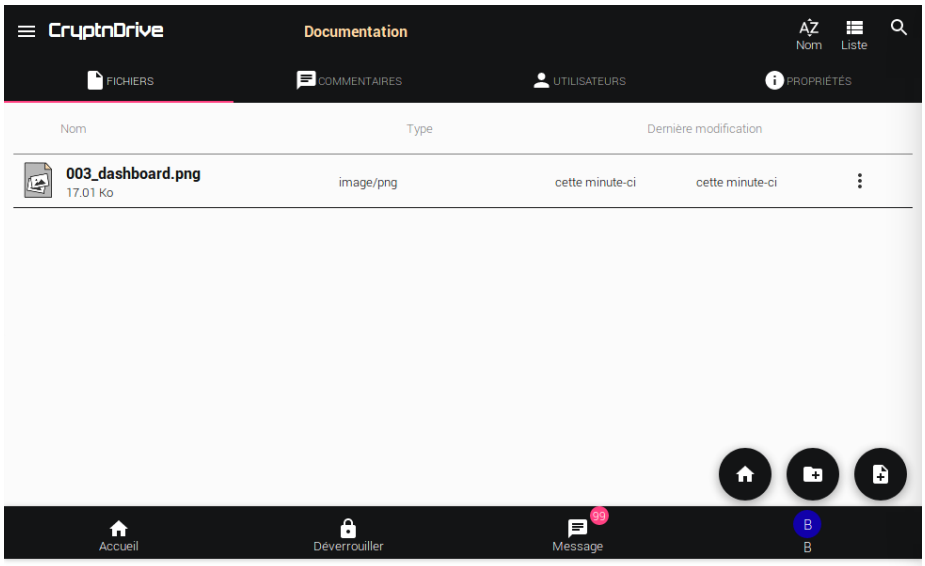


Figure 9: Un dépôt de fichiers version tablette

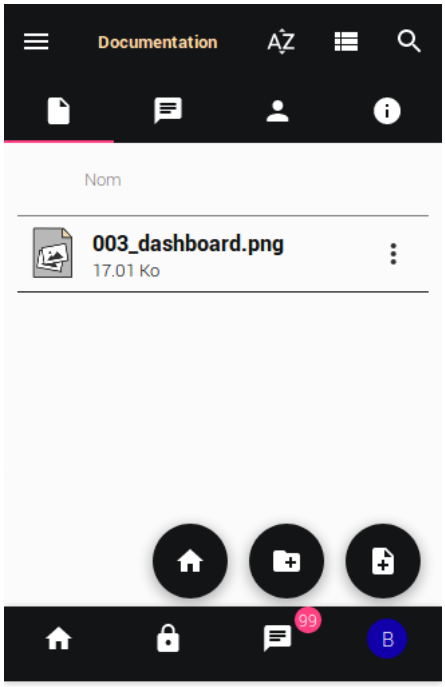


Figure 10: Un dépôt de fichiers version téléphone

Commentaires « Secret text ». Pour sauvegarder le commentaire, vous pouvez cliquer sur l'icone ou cliquer ailleurs sur la fenêtre.

A chaque action (ajout d'un fichier, d'un commentaire, modification du nom du dépôt de fichiers), le dépôt de fichiers est chiffré dans le navigateur et sauvegardé sur le serveur central. Le nombre de fichiers, le nom des fichiers, le contenu des fichiers et des textes sont chiffrés. Ils ne peuvent être déchiffrés que par le créateur du dépôt ou par une personne avec qui le dépôt est partagé.

Après la sauvegarde, vous revenez directement sur votre page où vous verrez votre nouveau dépôt chiffré :

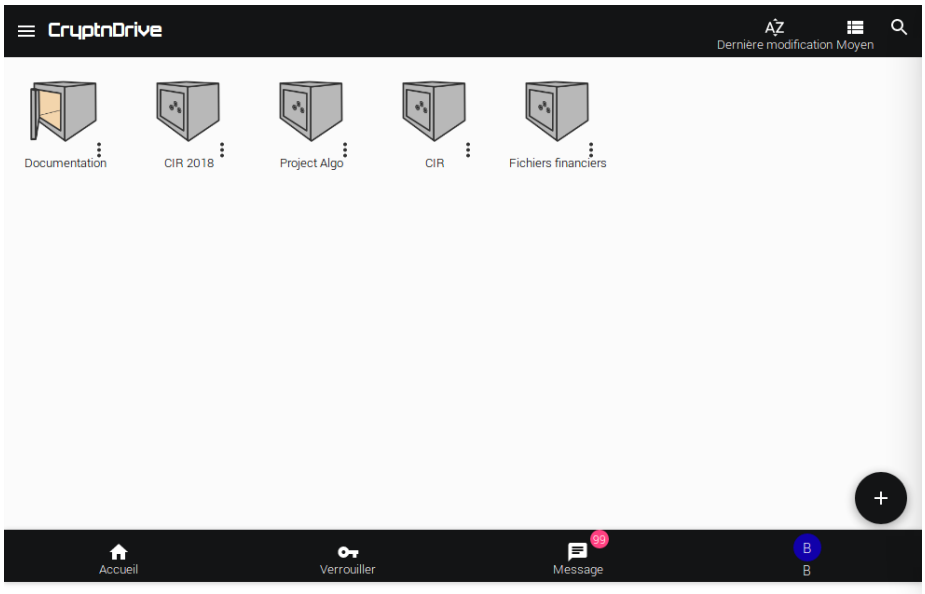


Figure 11: Écran d'accueil avec un dépôt de fichiers

3.3.1 Les logs associés

A l'usage, une des caractéristiques précieuses de CryptNDrive est la présence de logs détaillés. Ils permettent de savoir quand un dépôt est déchiffré, un fichier chargé, . . .

On accède aux logs en allant dans la section **Propriétés** après les informations de base concernant le dépôt de fichiers, on trouve un tableau avec tous les logs.

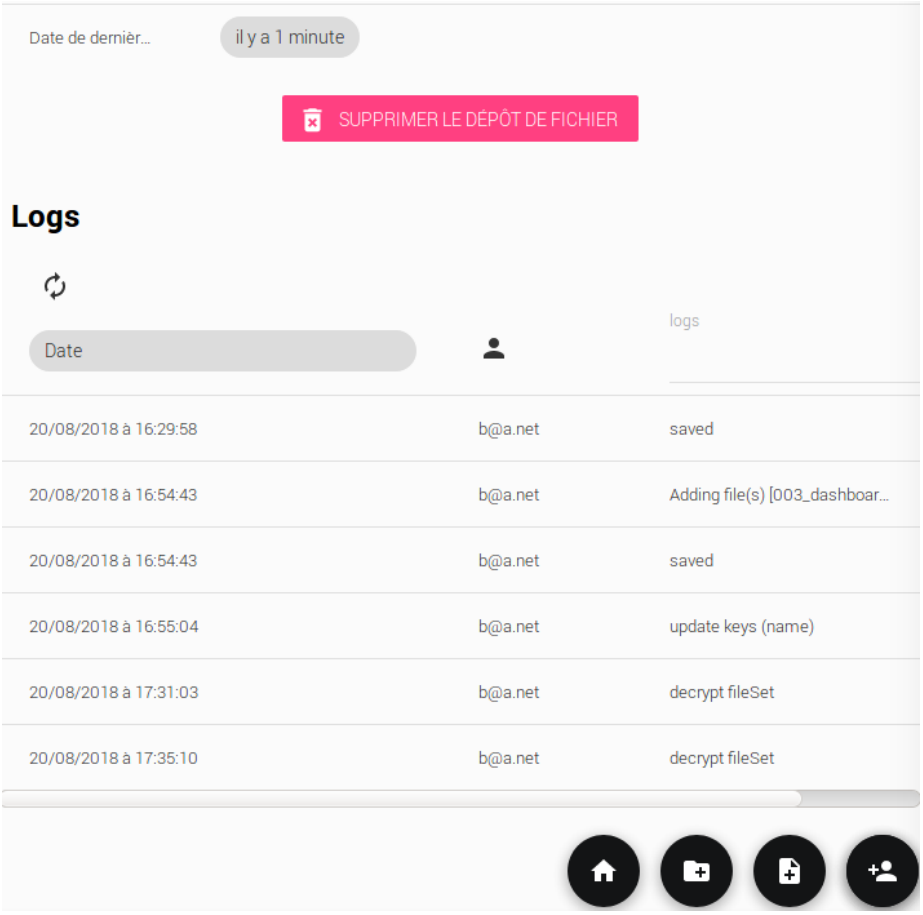


Figure 12: Page de logs

3.3.2 Qu'y a-t-il dans un dépôt chiffré

Un dépôt de fichiers chiffré est composé des informations suivantes : * Les fichiers et les textes du dépôt. Ils sont stockés sous forme d'un fichier unique chiffré. Quand le dépôt est chiffré on ne connait pas la liste des fichiers ou des textes. Il peut y en avoir 1 ou 100. * La liste des personnes avec qui le dépôt est partagé, dont le créateur du dépôt de fichiers. Attention, cette liste n'est pas chiffrée. * Une clé AES 256 de chiffrement du dépôt. Lors de la création du dépôt, cette clé est générée. Elle est toujours stockée chiffrée par les clés publiques (ElGamal 2048) des personnes ou des groupes qui partagent le dépôt de fichiers. * Les logs associés au dépôt. Certaines entrées de log sont chiffrées, d'autres non suivant leur nature.

3.4 Partage d'un dépôt de fichiers avec un tiers

3.4.1 Avec un tiers avec qui l'on a déjà partagé

Nous allons maintenant partager un dépôt de fichiers avec une personne tierce qui n'a pas de compte dans le système.

Ceci pose une difficulté particulière. Une personne non inscrite dans le système ne dispose pas de clés de chiffrement. Un dépôt de fichiers ne peut pas être chiffré avec sa clé publique qui n'existe pas encore ! Nous allons l'inviter à s'enregistrer dans le système.

Tout d'abord nous ouvrons un dépôt de fichiers. On voit sur la gauche (ou sous l'onglet utilisateur) une colonne avec l'ensemble des personnes avec qui ce dépôt de fichiers est partagé.

Il faut cliquer sur le bouton d'ajout d'utilisateurs  . Ceci permet d'avoir la boite de dialogue suivante où l'on va ou taper une adresse mail ou sélectionner des utilisateurs déjà présent dans le système.

Un partage direct avec l'envoi d'un message standard peut alors être fait en appuyant sur 

ou bien les droits associés à la personne ou aux personnes avec qui on met en partage peuvent être choisis puis le message associé peut être personnalisé (bouton SUIVANT)

On arrive alors sur la page suivante permettant de gérer les droits d'accès de la ou des personnes avec qui on partage :

Les droits sont les suivants : on peut autoriser la personne avec qui on partage à télécharger (ou seulement voir), ajouter ou modifier les fichiers (ou pas), modifier le texte chiffré, re-partager avec un tiers. Enfin, on peut donner tous ces droits en une fois avec le droit « Tous ». En cliquant sur « Suivant », on arrive sur l'écran permettant la rédaction d'un message :

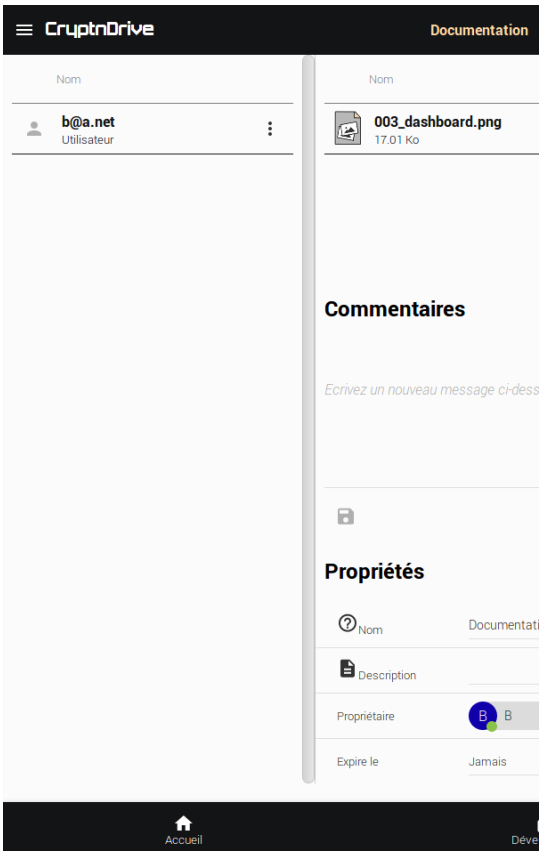


Figure 13: La colonne de gauche d'un dêpot de fichiers

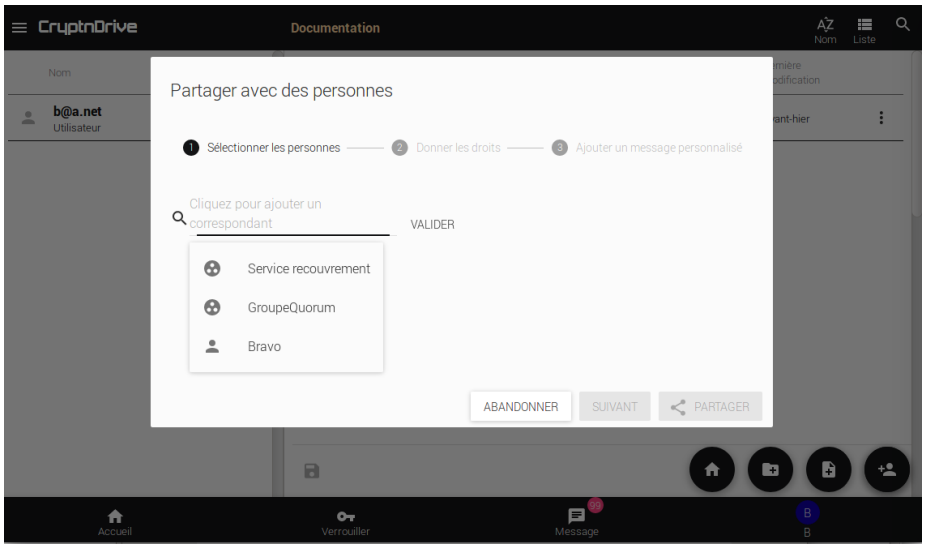


Figure 14: Ajout d'utilisateur à un dépôt de fichiers

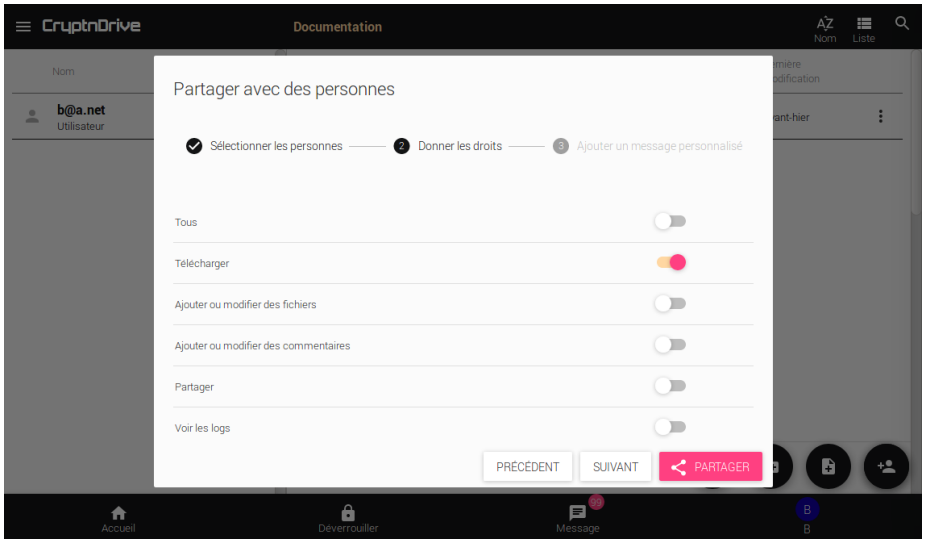


Figure 15: Gestion des droits d'un utilisateur en partage

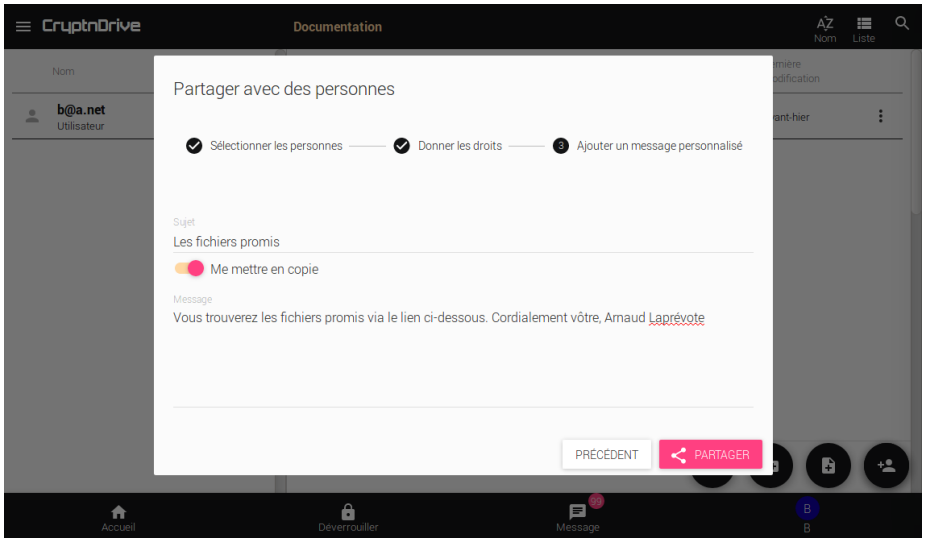


Figure 16: Rédaction d'un message de partage

Vous pouvez y remplir le sujet du message électronique envoyé, le message lui-même et demander une copie vers votre messagerie. Après appui sur PARTAGER, le message est envoyé en html, avec un lien cliquable pour la personne le recevant.

Après avoir cliqué sur PARTAGER le dépôt est sauvegardé et les personnes avec qui le dépôt est partagé apparaissent dans la liste correspondante.

Comme vous le voyez sur le côté, il y a 2 types d'icones représentant les personnes : représente les personnes ayant déjà un compte dans le système, représente les personnes invitées et qui n'ont pas encore de compte (et donc de clés de chiffrement).

c@a.net va recevoir le message suivant :

Une copie sera aussi envoyée à l'expéditeur.

En cliquant sur le lien, le destinataire va entrer dans la procédure d'inscription décrite plus haut.

Une fois le destinataire enregistré, il va arriver sur l'écran montrant le dépôt de fichier chiffré avec une indication comme quoi une demande de confirmation est en cours (« Request in progress » sous b@a.net) :

b@a.net doit confirmer le partage en cliquant sur l'icone de notification en haut à droite :

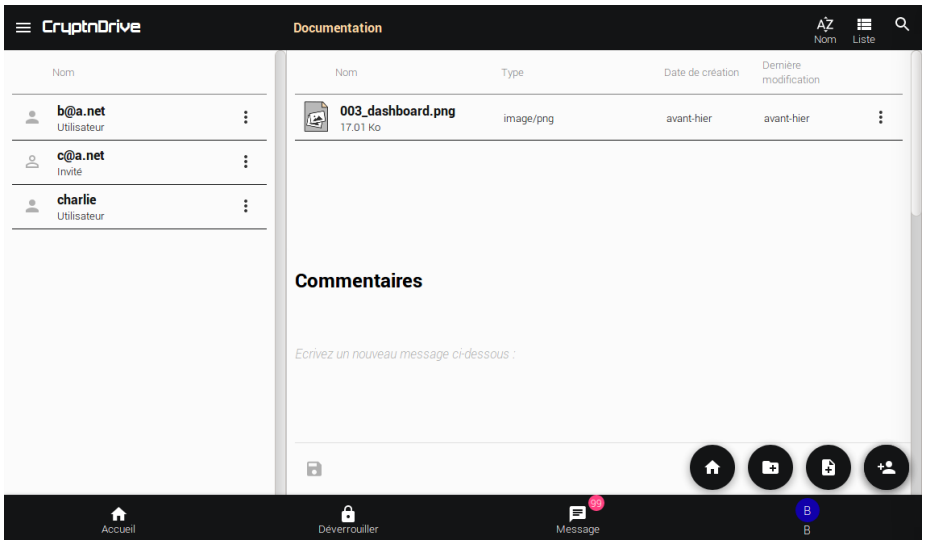


Figure 17: Personnes en partage

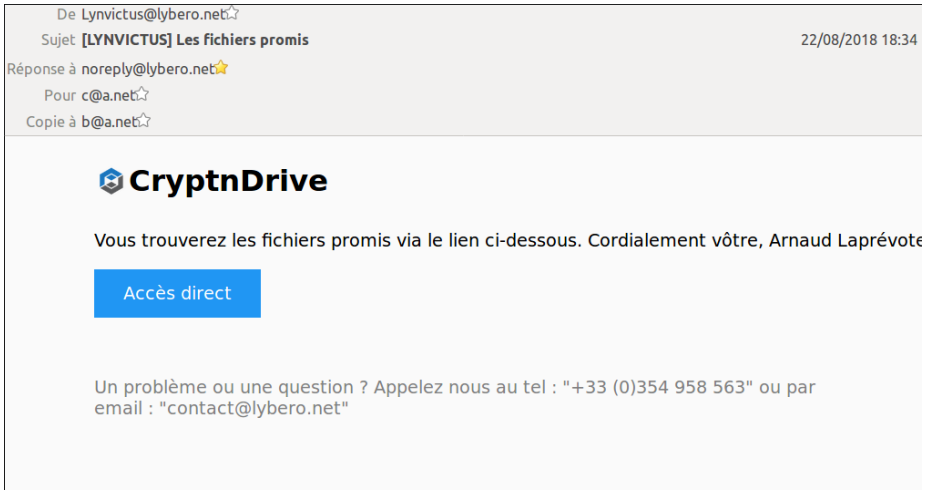


Figure 18: Mail pour inviter une personne

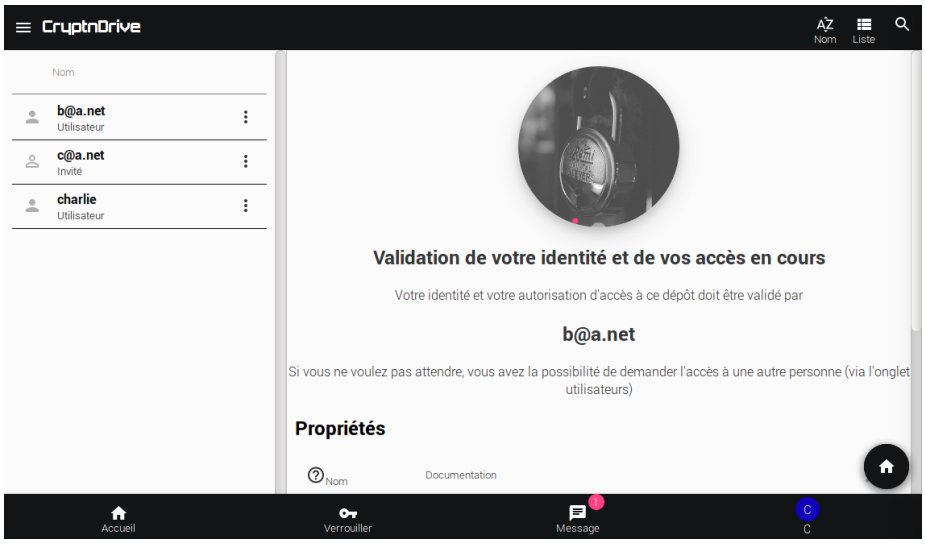


Figure 19: Attente de confirmation

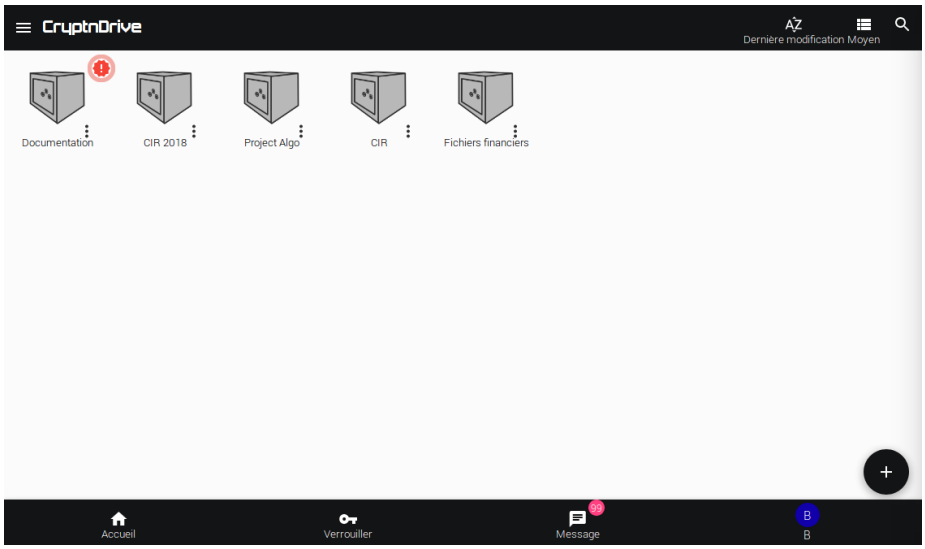


Figure 20: Notification de demande d'accès

On arrive alors sur le message d'acceptation :

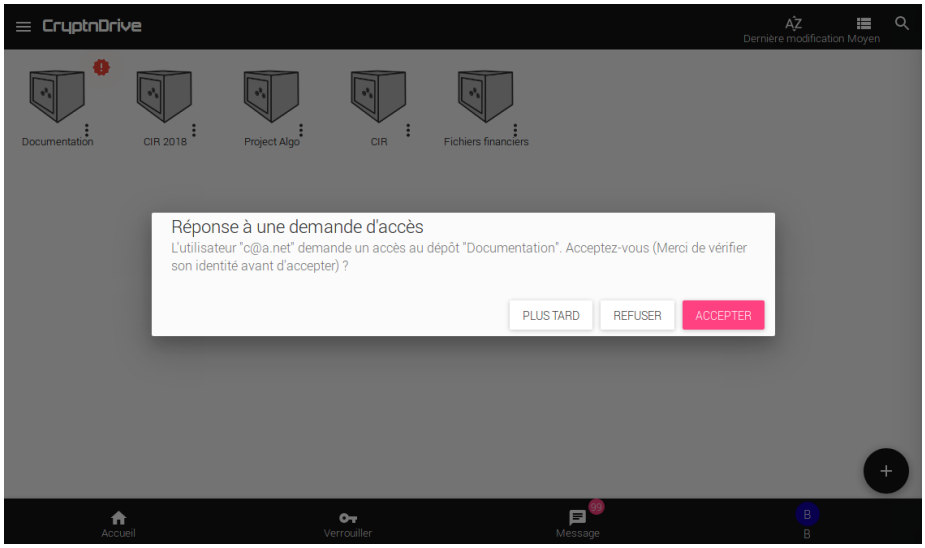


Figure 21: Demande d'accès

Après l'acceptation de b@a.net, le destinataire peut accéder au dépôt de fichiers chiffré (l'icone de déchiffrement passe de grisée à noir).

Il peut arriver que la clé privée soit de nouveau verrouillée (plus de 5 minutes après le dernier accès à la clé). Dans ce cas, il faut retaper sa passphrase pour redéchiffrer la clé privée.

E peut maintenant déchiffrer le dépôt de fichiers :

Ces allers-retours peuvent paraître lourd mais ils sont nécessaires pour 2 raisons : toutes les opérations de chiffrement / déchiffrement sont faites dans les navigateurs. Il faut donc que l'expéditeur puisse chiffrer le dépôt de fichiers avec la clé publique du destinataire. Cette clé doit donc exister. La seconde raison est que le destinataire n'est pas encore dans le système, si le mail est intercepté un tiers pourrait se faire passer pour le destinataire. Lors de l'acceptation finale, l'expéditeur a l'occasion de vérifier (par téléphone par exemple) que le destinataire s'est bien connecté.

Pour les utilisateurs déjà dans le système, cette précaution n'est pas nécessaire, puisque leur clé publique est disponible.

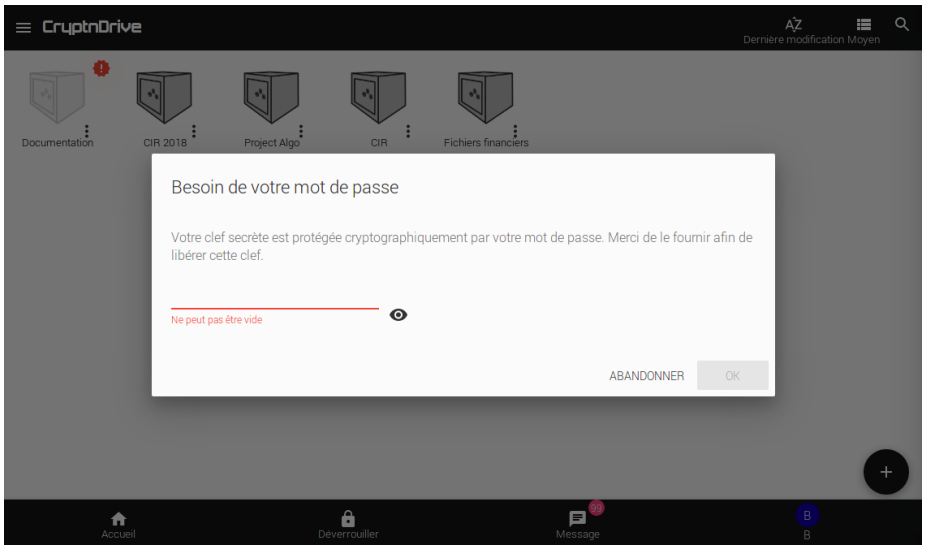


Figure 22: Demande de mot de passe

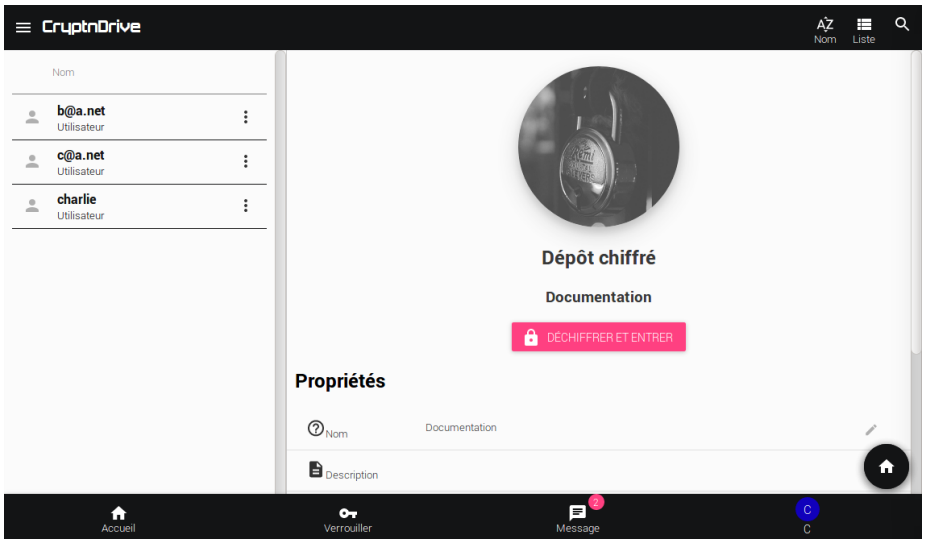


Figure 23: Le dépôt de fichiers est maintenant déchiffrable

3.5 Inviter un tiers à me déposer des fichiers

3.5.1 En utilisant votre client de messagerie

Il est possible pour un utilisateur non inscrit (le *fournisseur*) dans le système d'envoyer de manière chiffrée des fichiers et du texte à une personne inscrite (le *destinataire*). Pour ce faire, le *destinataire* va fournir au *fournisseur* une url typiquement via un mail ou tout autre moyen.

Pour générer l'url, l'on entre dans la page de gestion des urls via l'entrée de menu «URL » : URLs puis on ajoute une nouvelle url avec le bouton : + .

On obtient alors la fenêtre suivante permettant de créer une url en choisissant un destinataire (ce n'est pas obligatoire mais aide à identifier qui a envoyé le dépôt) et le nombre de fois où cette url pourra être utilisée pour créer un dépôt. Le nom du *destinataire* sera explicitement indiqué dans l'url.

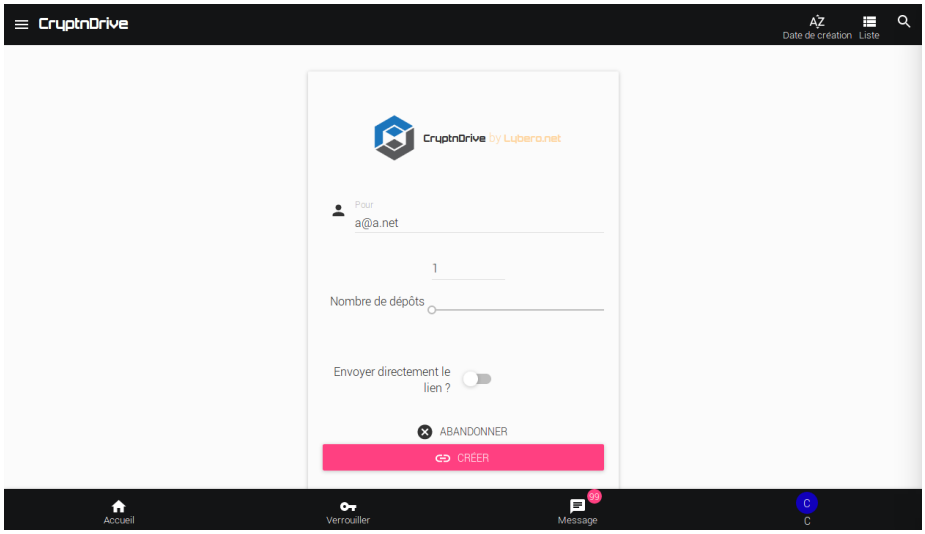


Figure 24: Création d'une url d'invitation à déposer

Il ne reste plus ensuite qu'à cliquer sur le bouton CRÉER . Une url est alors créée :

Il suffit de cliquer sur le bouton au bout de l'url pour la copier.

On peut coller l'url dans un mail pour l'envoyer au destinataire de son choix :

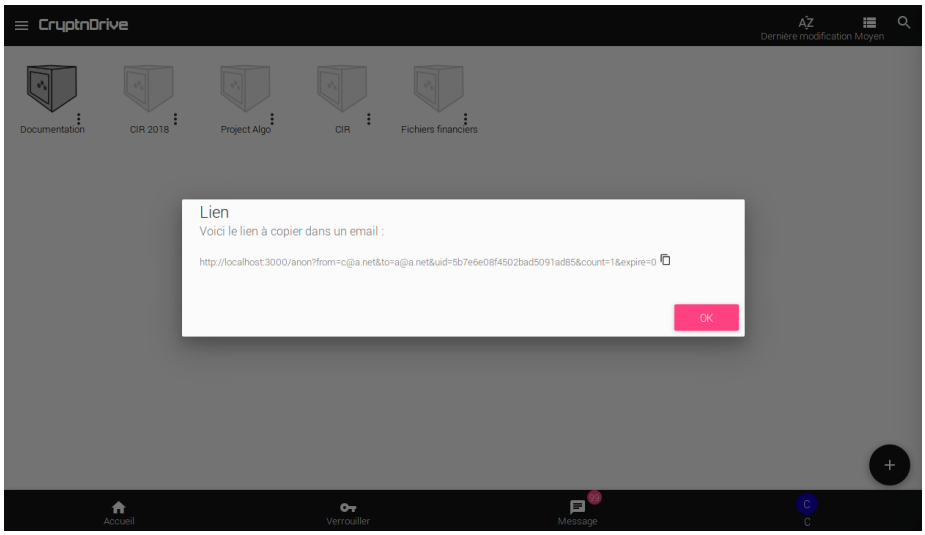


Figure 25: Création d'un lien

Figure 26: Message avec une url

3.6 En envoyant directement un message depuis l'interface

Une autre solution est de directement générer le message et de l'envoyer depuis l'interface. Pour cela on active l'option « Envoyer directement le lien ? ». L'interface change de la manière suivante :

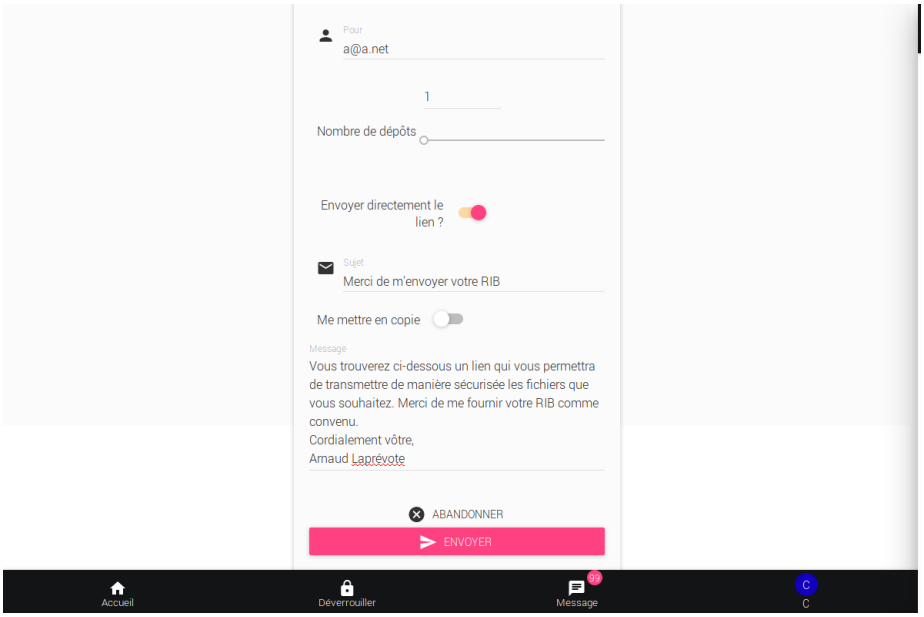


Figure 27: Envoi d'un lien depuis l'interface web

Vous pouvez indiquer un sujet, un message, et le lien sera automatiquement collé sous ce message qui est envoyé depuis l'adresse lynvictus@lybero.net au *fournisseur* de fichier. Il suffit de cliquer sur le bouton ENVOYER pour que le message parte.

3.6.1 Après réception du message pour le fournisseur

En cliquant sur le lien, le *fournisseur* arrive sur la page web permettant le dépôt de fichiers et l'écriture d'un message. Il faut ensuite cliquer sur le bouton « ENVOYER » qui va procéder au chiffrement dans le navigateur et à l'envoi. Le titre du dépôt (la première entrée de texte) n'est pas chiffré, le reste des éléments l'est. La clé de chiffrement utilisée est la clé publique du *destinataire*. Le *destinataire* est donc le seul à pouvoir accéder à ces éléments :

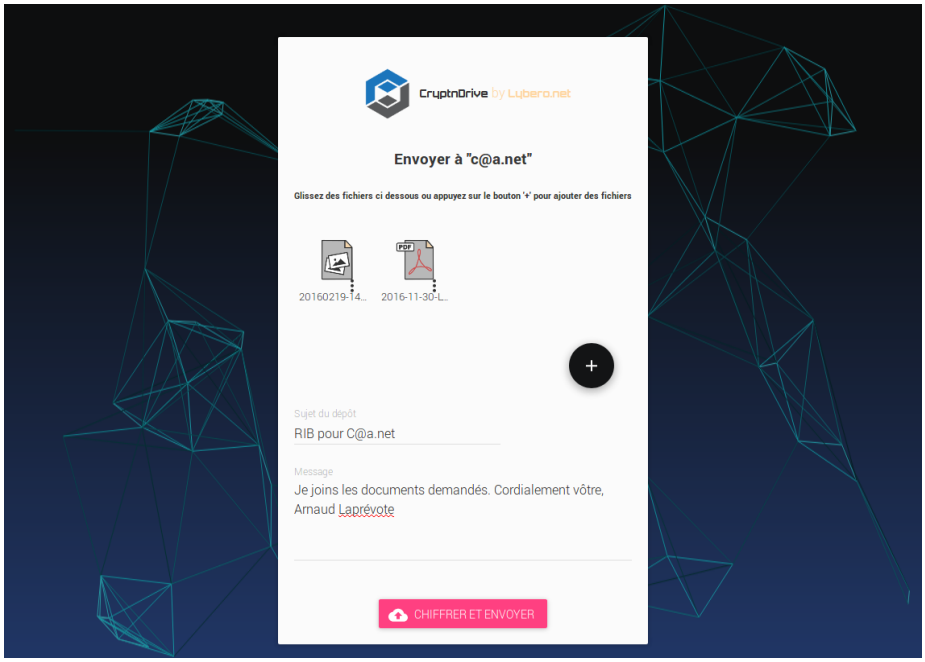


Figure 28: Page de dépôt de fichiers

Après envoi, une page web indiquant le chiffrement et l'envoi des fichiers est affichée pour le *fournisseur*.

Un nouveau dépôt de fichier apparaît sur la page d'accueil du *destinataire*. En passant en mode liste sur la page d'accueil, il voit donc l'écran suivant :

Le destinataire peut maintenant déchiffrer et entrer dans le dépôt de fichiers et il voit les éléments envoyés.

L'utilisateur qui a envoyé les documents est automatiquement intégré comme invité pour ce dépôt de fichiers. Cela signifie que s'il crée un compte plus tard, une demande d'accès au dépôt sera faite au destinataire. Il sera donc très simple à l'expéditeur de retrouver tous les fichiers qu'il a fourni à divers moments aux différents utilisateurs du système.

3.7 Gestion des droits

Nous allons ajouter en partage c@a.net à ce dépôt de fichiers, mais sans lui donner aucun droit, il pourra alors accéder au dépôt et verra les éléments suivants :

Il ne peut charger aucun fichier, mais peut les visualiser. S'il ouvre le pdf attaché

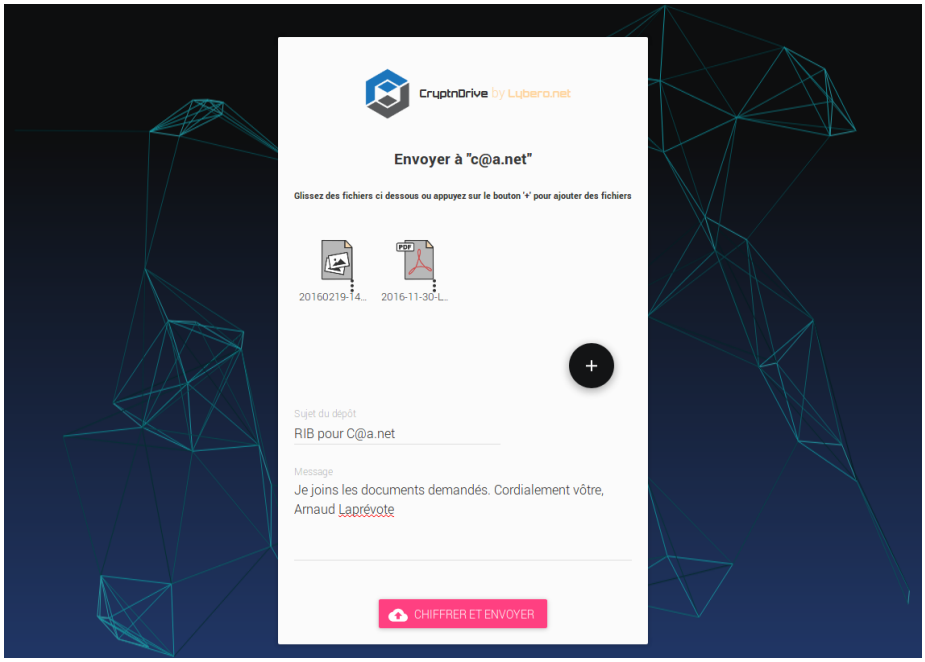


Figure 29: Page de dépôt de fichiers

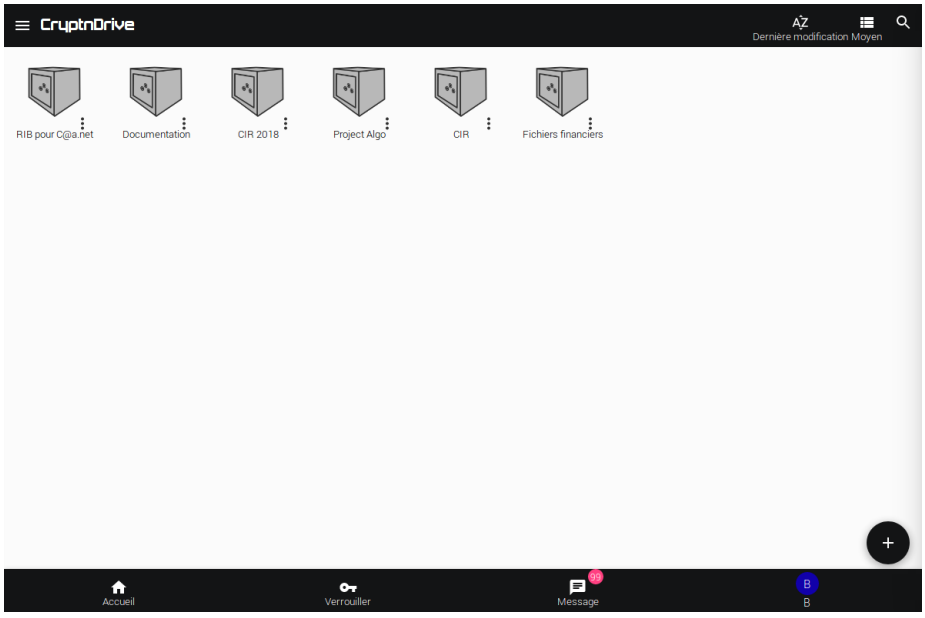


Figure 30: Un nouveau dépôt dans la page d'accueil

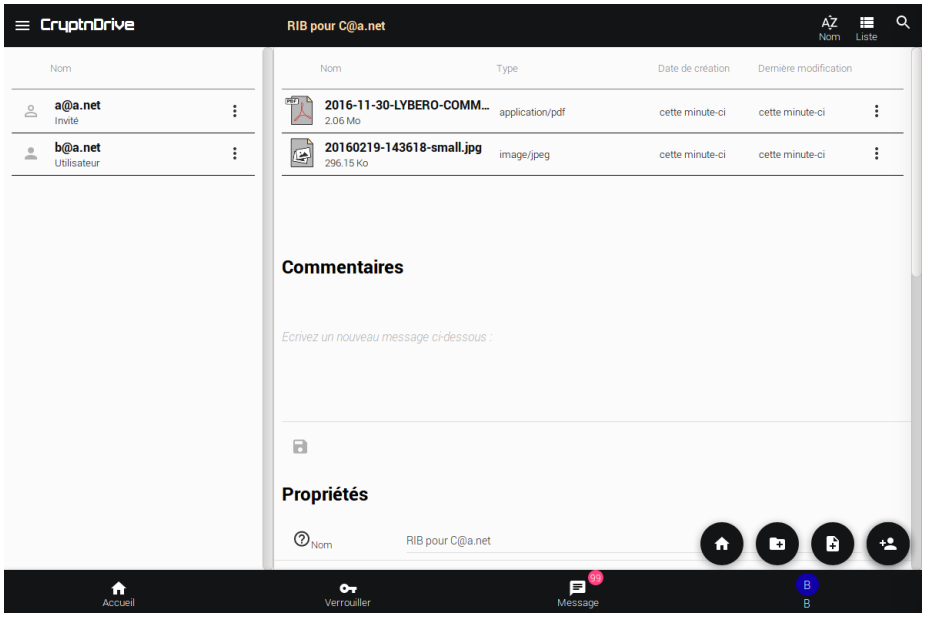


Figure 31: Les fichiers du nouveau dépôt

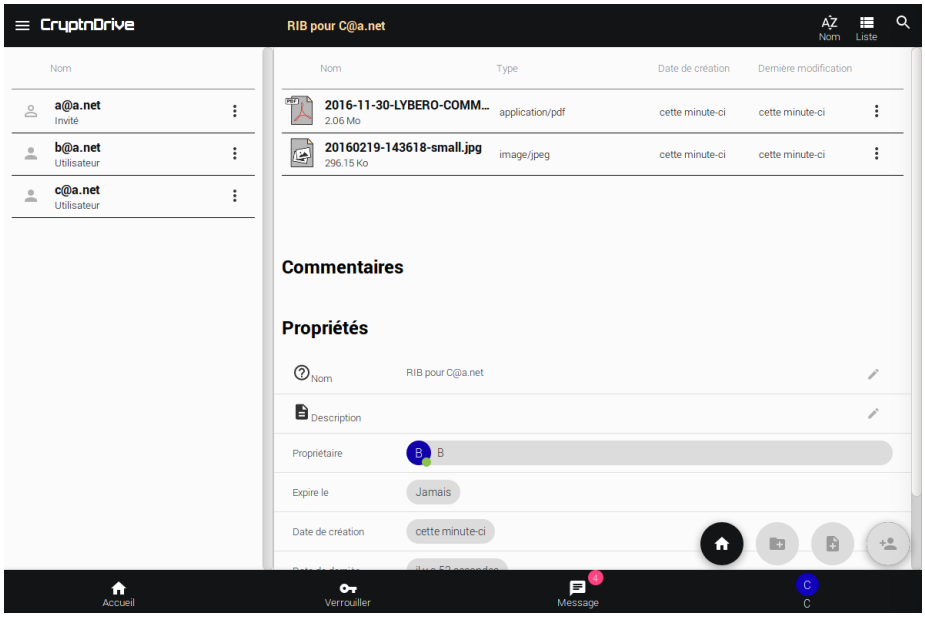


Figure 32: Dépôt en lecture seule

il verra :

Figure 33: Visualiseur de pdf

d@a.net a donc la possibilité de voir le contenu du fichier mais sans le sauvegarder. Attention cependant, il peut évidemment prendre une copie d'écran ou même en manipulant finement son navigateur extraire le fichier malgré tout.

Dans ce cas, nous avons montré un fichier pdf chiffré à un tiers, sans qu'il ne dispose d'aucun autre logiciel que son navigateur web.

Il est possible de modifier les droits associés à un utilisateur pour un dépôt de fichier en utilisant le sous-menu de gestion des permissions associé :

On arrive alors sur l'écran de modification des droits pour l'utilisateur :

Autant, l'accès à un fichier est protégé par des droits **cryptographiques** autant dans ce cas, c'est une protection **logique** des droits, susceptible d'être détournée par un expert. Bref, les règles habituelles s'appliquent : si je peux le voir, je peux le photographier ou en faire une vidéo, si je peux l'entendre, je peux l'enregistrer.

3.8 Recouvrement à quorum

Nous allons maintenant utiliser un groupe d'administrateurs de secrets à quorum pour opérer un recouvrement par un tiers.

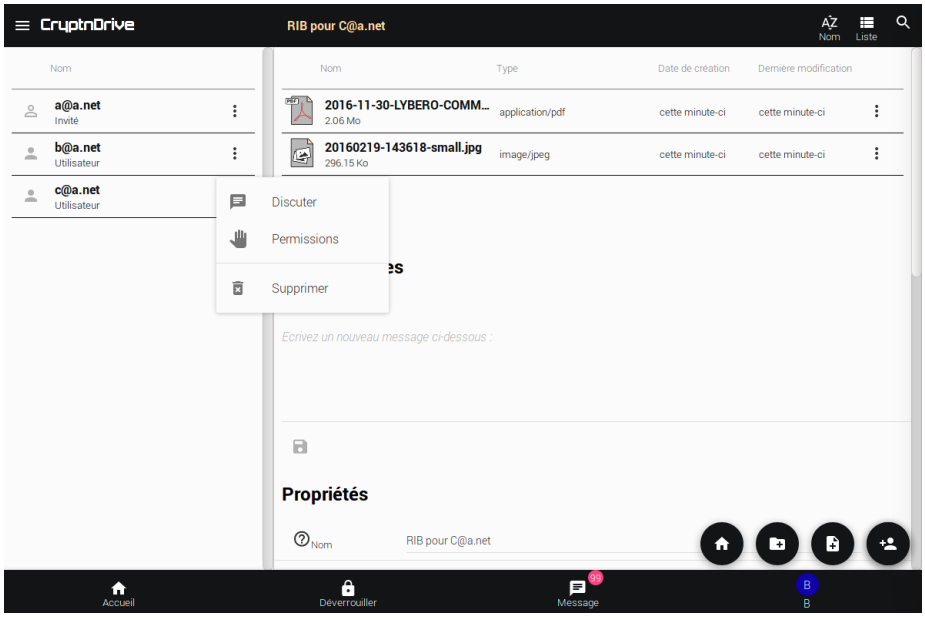


Figure 34: Menu de modification des droits

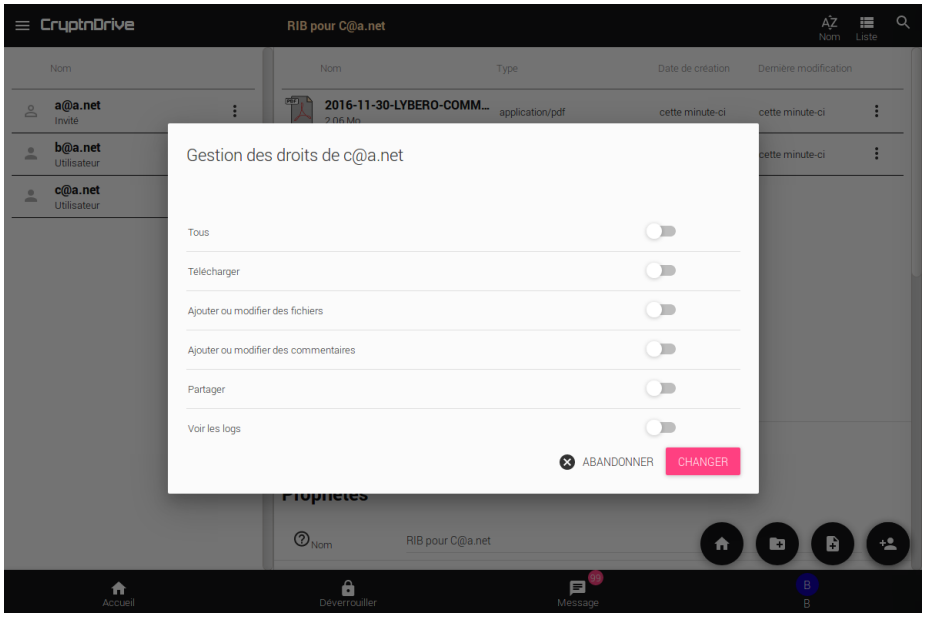


Figure 35: Écran de modification des droits

3.8.1 Configuration d'un Quorum

Tout d'abord, nous ajoutons un groupe à quorum en partage sur un dépôt de fichiers. Pour cela, l'administrateur doit ajouter le groupe à quorum via le menu d'administration (Administration > Quorums).

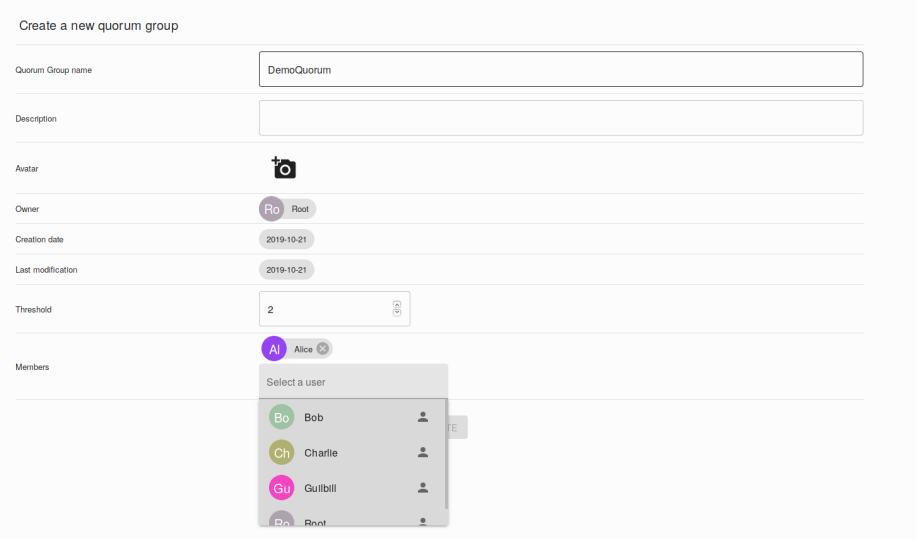


Figure 36: Ajout d'un groupe à Quorum

L'administrateur doit indiquer le nom du groupe, éventuellement une description, le seuil du quorum, et les membres du quorum. Pour finaliser le groupe à quorum il faut que chaque membre du groupe se connecte 2 fois. Dans notre cas, nous ajoutons Alice, Bob et Charlie dans un groupe à quorum avec un seuil de 2.

Une fois le groupe à quorum créé, il faut indiquer dans la configuration du répertoire de coffres concerné que l'on veut utiliser ce quorum. Pour cela, dans les paramètres du répertoire de coffres (root par exemple), ajouter au groupe souhaité (All groups par exemple) le groupe à quorum comme Service de recouvrement.

Une fois cette configuration faites, tous les coffres qui seront créés dans le répertoire de coffre root ou ses sous répertoires de coffres bénéficieront du mécanisme de recouvrement par quorum.

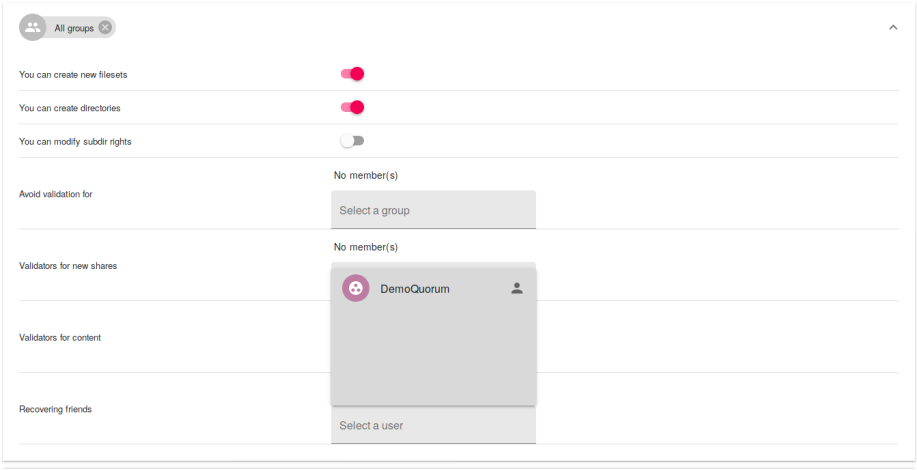


Figure 37: Configuration du groupe à quorum

3.8.2 *Création d'un coffre avec mécanisme de recouvrement par Quorum*

Maintenant que nous avons configuré le recouvrement par le groupe à Quorum composé d'Alice, Bob et Charlie, un utilisateur lambda peut créer un coffre qui bénéficiera du recouvrement pas quorum. L'utilisateur Delta créé un coffre et y dépose un fichier. Dans les partages du dépôt, nous pouvons voir le groupe à quorum.

Figure 38: Le quorum est présent dans les partages

Notons que les membres du Quorum, si on ne leur a pas partagé le coffre, peuvent le voir en grisé sur leur interface, mais ne peuvent pas le déchiffrer.

3.8.3 *Procédure de recouvrement*

Un membre du quorum peut inviter un utilisateur à accéder au coffre. Pour cela elle peut accéder au partages du coffre en question (elle ne peut toujours pas le déchiffrer), et ajouter l'utilistateur de son choix.

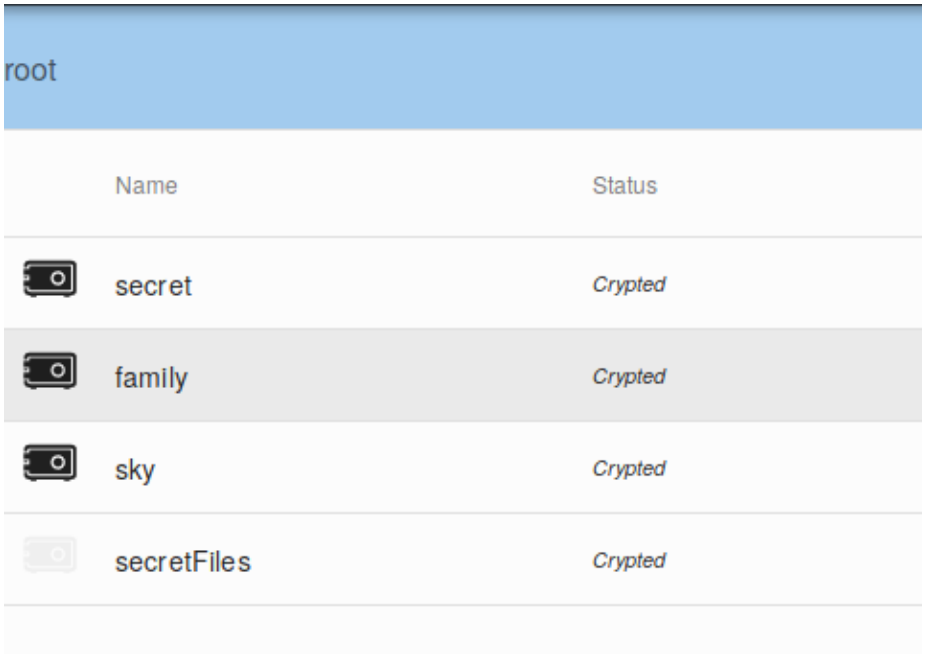


Figure 39: Vue du coffre par le quorum

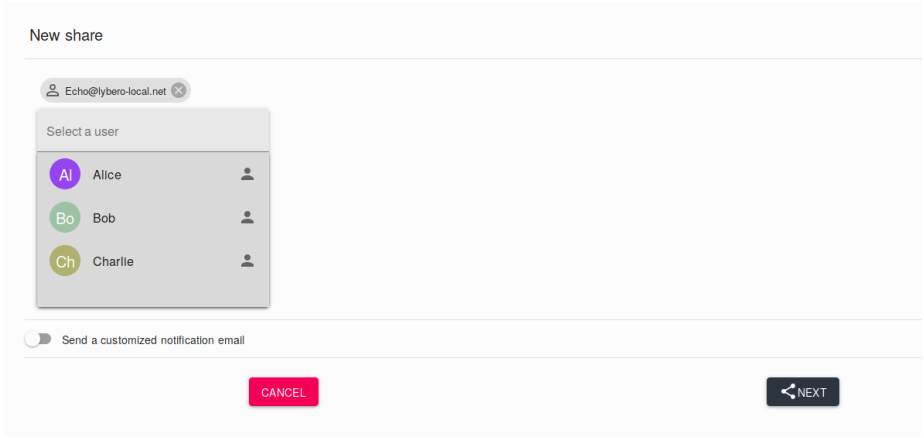


Figure 40: Partage du coffre

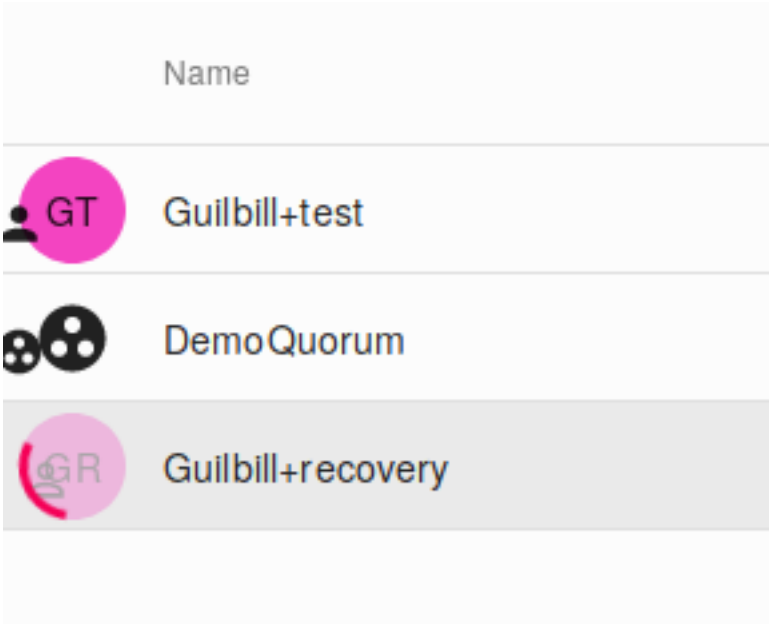


Figure 41: Recouvrement en attente

Une notification indique alors aux membres du quorum qu'une demande de recouvrement a été faite.

Ils peuvent alors accepter ou refuser. Lorsque le nombre de membres du quorum ayant accepté le recouvrement est supérieur ou égal au seuil du quorum, alors, le recouvrement est effectif et l'utilistateur a accés au coffre.

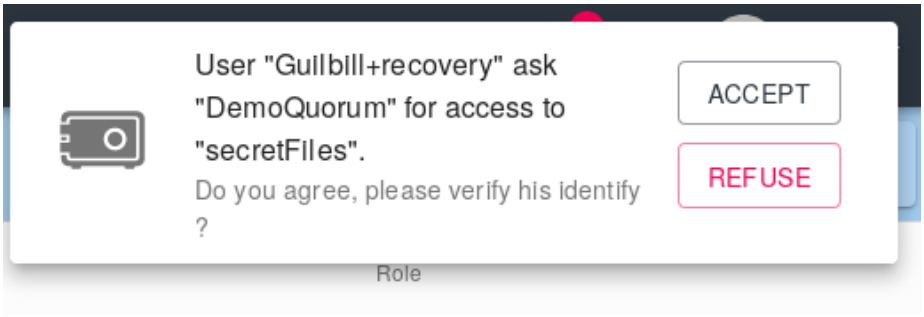


Figure 42: Demande d'accès à un dépôt

Il faut bien comprendre que ce mécanisme est cryptographique. Le groupe à quorum a une clé publique, mais pas de clé privée. Lorsque c@a.net a demandé à accéder au dépôt de fichiers, la clé AES256 du dépôt chiffrée par

la clé publique du groupe à quorum a été sur-chiffrée par la clé publique de c@a.net.

Au dernier déchiffrement partiel du membre du quorum, la clé AES256 du dépôt est restée chiffrée par la clé publique de c@a.net. c@a.net a récupéré cette valeur puis l'a déchiffrée avec sa clé privée. Il a alors eu accès à la clé AES256 du dépôt et donc au dépôt.

La séparation entre l'autorisation d'accès par le groupe à quorum et l'accès au dépôt est cryptographique. C'est une propriété très précieuse de notre système. Elle permet à un groupe de personnes non expertes de mener les opérations de recouvrement qui sont habituellement confiées à des experts techniques, qui fonctionnellement ne sont pas forcément les mieux à mêmes de mener ces opérations.

4 Conclusion

4.1 conclusion

CryptnDrive de Lybero.net permet à la fois la sécurité des données et des transferts dans une organisation avec une facilité d'utilisation maximale et en même temps une capacité pour l'organisation de maitriser totalement le système (mise à disposition des codes sources, gestion des serveurs utilisés, utilisation de groupe à quorum pour les recouvrements).

Si vous avez des suggestions de tous ordres sur le logiciel ou sur cette documentation, n'hésitez pas à nous en faire part à contact@lybero.net .