



# Import de certificats sur les applications mobiles

Version 1

## Document

Auteur	Franck MEIGNEN	Date de diffusion	08/11/16
Chef de projet	Adrien BRICCHI	N° de version	1

## Évolution du document

Version	Auteur	Nature des changements	Date
1.0		Création du document	

## Licence

Ce document n'est pas libre de droits.

Ce manuel est publié sous la licence Creative Commons avec les particularités "Paternité – Partage à l'identique" (également connue sous l'acronyme CC BY-SA).

Détails de cette licence : <http://creativecommons.org/licenses/by-sa/2.0/fr/>



## Table des matières

---

<b>1 GÉNÉRAL</b>	<b>4</b>
1.1 Valeur légale	4
1.2 URL-Scheme	4
<b>2 ANDROID</b>	<b>5</b>
2.1 Créer un Keystore BKS	5
2.2 Importer le Keystore	5
<b>3 IOS</b>	<b>6</b>
3.1 Importer le Keystore	6

# 1. GÉNÉRAL

## 1.1. Valeur légale

Seuls les certificats dématérialisés sont compatibles avec les applications iParapheur mobiles.

Ne traitez pas de documents nécessitant une signature en RGS (avec une clef physique). La signature apposée aux documents officiels n'aurait certainement pas une valeur suffisante.

## 1.2. URL-Scheme

La version iPad 1.4.09 et Android 1.5.03 du parapheur peuvent importer des certificat depuis un simple lien. Nous utilisons une URL-scheme pour tablettes : `iparapheur://importCertificate?liste_des_arguments`

Les paramètres passés en scheme ont été encodé selon la norme URL, et les caractères spéciaux échappés selon le standard : [http://www.w3schools.com/tags/ref\_urlencode.asp]

- `iOsUrl = https%3A%2F%2Fcurl%2Fcertif.p12` (nécessaire pour iOS)
- `iOsPwd = pwd` (facultatif)
- `AndroidUrl = https%3A%2F%2Fcurl%2Fcertif.bks` (nécessaire pour Android)
- `AndroidPassword = pwd` (facultatif)

Un exemple de lien complet pouvant être intégré dans un mail : `<a href="iparapheur://importCertificate?iOsUrl=https%3A%2F%2Fcurl.adullact.org%2FsUSyh%2Fbma.p12&iOsPwd=bma&AndroidUrl=https%3A%2F%2Fcurl.adullact.org%2FsUSyh%2Fbma.p12&iOsPwd=bma">Importer le certificat</a>`

Un simple clic sur le lien, l'app se lancera, et la tablette téléchargera le certificat. Si le MdP du keystore été renseigné, il sera importé automatiquement. Dans le cas contraire, la pop-up de demande de MdP sera présentée à l'ouverture de l'application.

Il n'y a pas d'ordre à respecter dans les arguments du lien, et l'on peut supprimer l'un des deux systèmes sans soucis, si l'on sait que le parc de tablettes cible ne l'utilisera pas. Évidemment, le lien de téléchargement de l'URL devra-t-être accessible depuis les tablettes.

L'import du MdP dans le lien n'est conseillé que si le mail reste confiné à un réseau interne. Pour toute autre configuration, nous conseillons d'envoyer certificat et MdP par deux canaux différents. ""

## 2. ANDROID

### 2.1. Créer un Keystore BKS

Le système Android est écrit en Java, et n'est compatible qu'avec un keystore de type BKS. La structure d'un BKS est sensiblement la même qu'un certificat JKS (Java KeyStore) standard, mais s'affranchit des licences propriétaires d'Oracle/Sun.

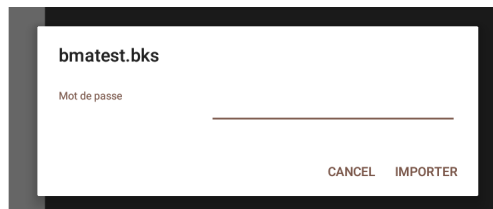
On peut convertir un certificat JKS en BKS avec PorteClef :

- Télécharger l'utilitaire depuis <http://sourceforge.net/projects/portecle/>
- File > Open Keystore File... > Saisir le Mot de passe du certificat.
- Tools > Change Keystore Type > BKS
- File > Save Keystore As...

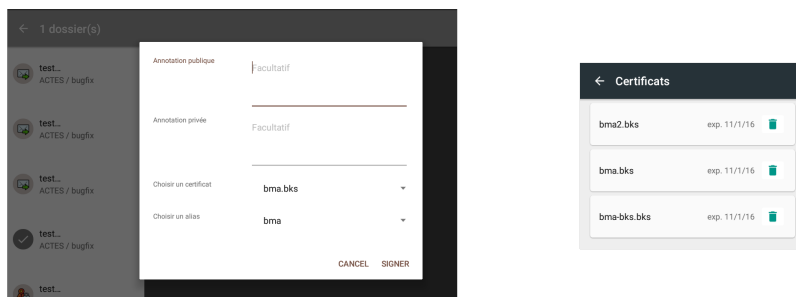
### 2.2. Importer le Keystore

Au démarrage de l'application Android, l'app vérifiera la présence d'un fichier BKS dans le dossier de téléchargement de la tablette.

Il suffit donc de s'envoyer le certificat par mail, Curl, DropBox, ou n'importe quel autre moyen, et de le télécharger normalement. Au redémarrage de l'application, une pop-up demandera le mot de passe défini, pour permettre l'import du certificat dans la mémoire interne.



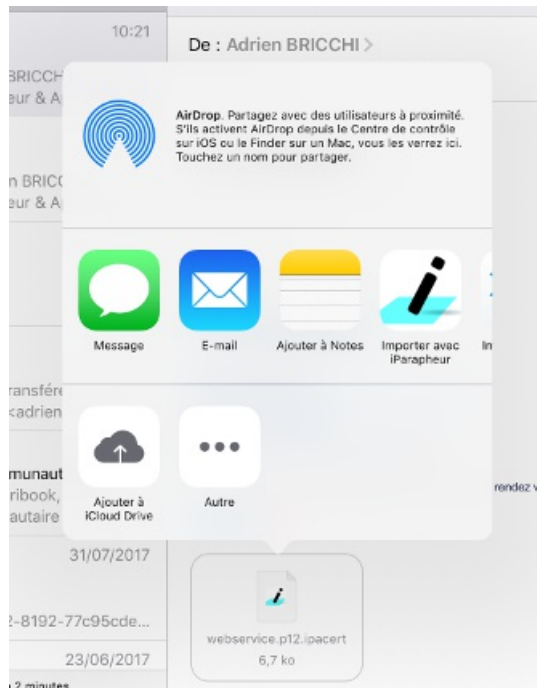
Le certificat sera ensuite disponible lors d'une signature. Les préférences permettent de vérifier et supprimer les certificats importés.



## 3. IOS

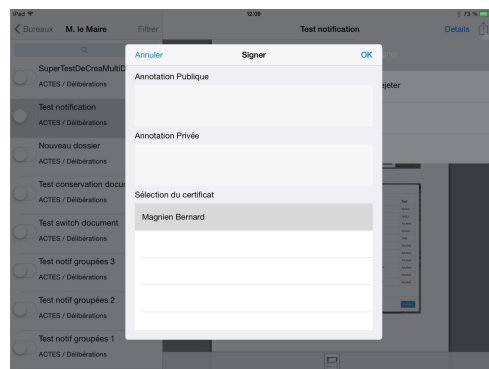
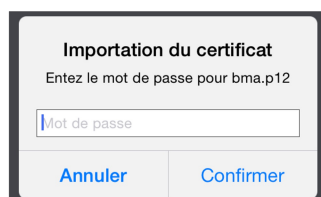
### 3.1. Importer le Keystore

- Zipper le fichier p12
- Renommer le fichier `(mon_certificat).p12.zip` en `(mon_certificat).p12.ipacert`
- S'envoyer le fichier `(mon_certificat).p12.ipacert` par mail, et l'ouvrir depuis l'iPad
- Sélectionner le fichier, et choisir **Importer avec iParapheur**



- L'application se lancera, et présentera une popup au démarrage, demandant le mot de passe du certificat.

Une fois l'import effectué, ce certificat sera disponible dans la pop-up de signature.



Le système iOS capture et garde jalousement les fichiers `p12` ou `zip`. C'est pourquoi nous créons ici un nouveau nom de fichier, pour pouvoir l'ouvrir depuis l'application iParapheur, sans ingérence du système iOS.