Android で S/MIME を使う

菊谷誠

2023 年 9 月 6 日 Revision 1.0

PC では Thunderbird などで S/MIME を使うのは比較的容易ですし、iPhone ではデフォルトのメーラーが S/MIME をサポートしているようですが、Android で S/MIME を使うのは簡単ではありません。ここでは CipherMail というアプリを使う方法を説明します。

前提

- CipherMail 自身が作る証明書(いわゆる「オレオレ証明書」)を使う場合と、すでに Thunderbird などで使う S/MIME 証明書を Actalis 等から入手している場合の二通りについて説明します。
- CipherMail はメールを読む機能はないので、BlueMail などの Android 用メールアプリを入れておいてください。なお、Gmail アプリでは相手の証明書を入手するのが難しいので BlueMail がお勧めです。

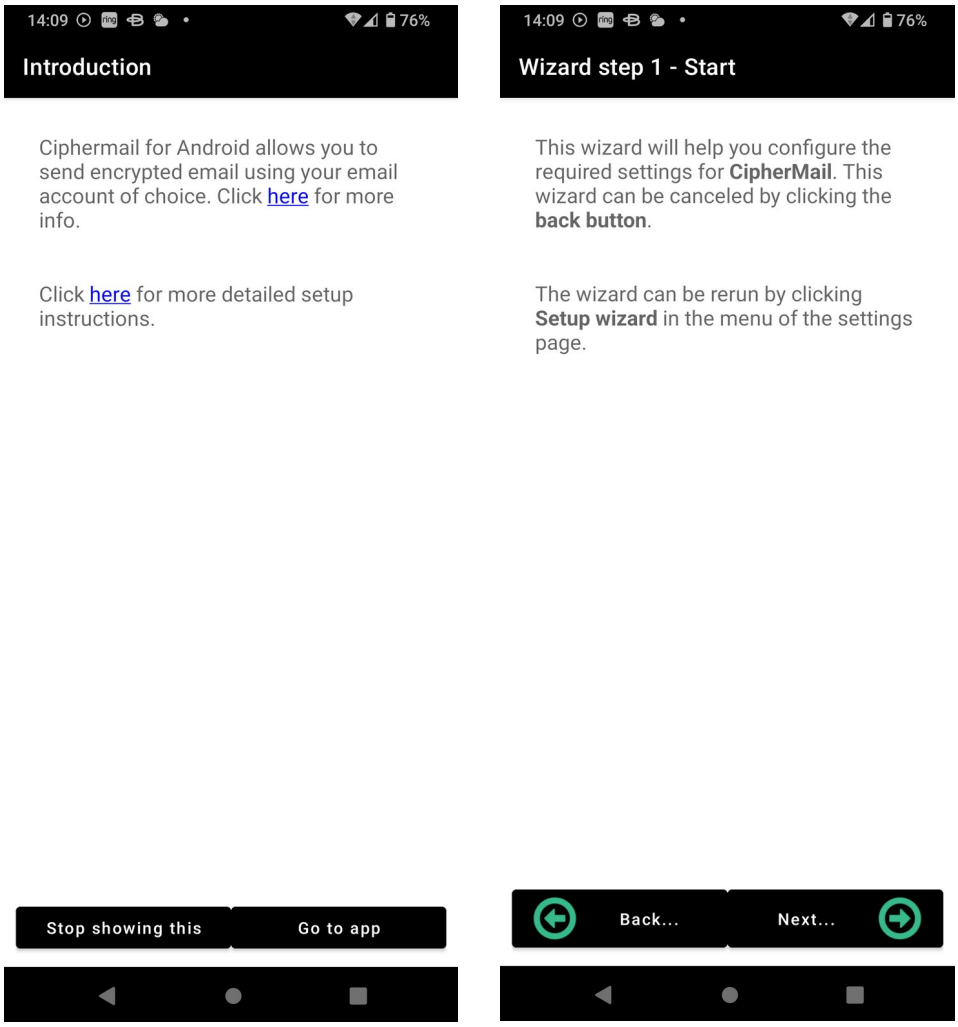
シナリオ

1. foo@gmail.com から bar@me.com へ署名したメッセージを CipherMail で送る
2. PC で bar@me.com から foo@gmail.com へ署名して返信する
3. foo@gmail.com から bar@me.com へ暗号化したメッセージを CipherMail で送る
4. PC で bar@me.com から foo@gmail.com へ暗号化したメッセージを送る
5. foo@gmail.com は CipherMail を使ってその暗号化されたメッセージを読む

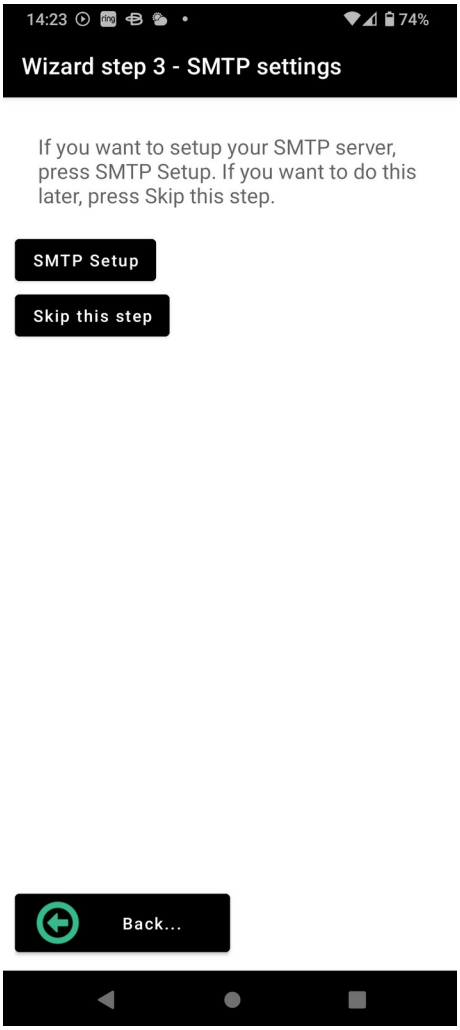
アプリのインストール

まず Play ストアから CipherMail を入れます。

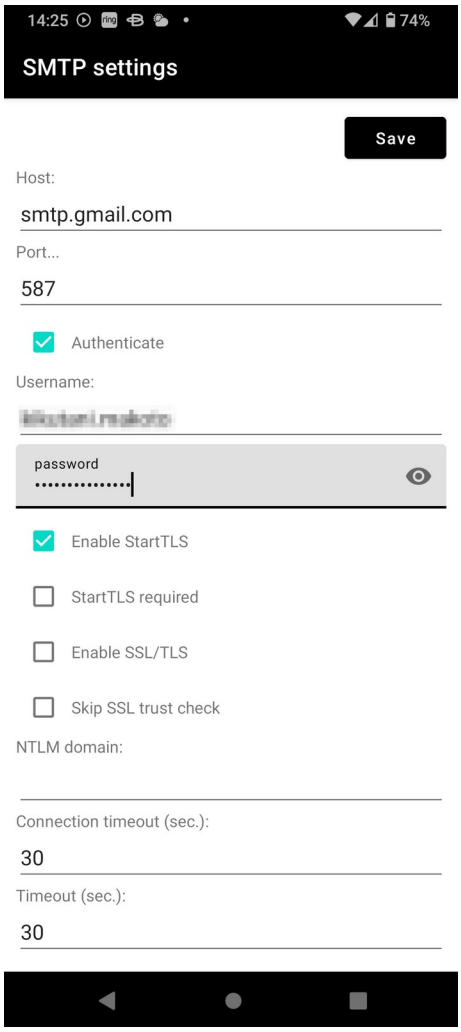
開くとこうなります。「Stop showing this」を押してもこの画面が出続けますけど、今は「Go to app」を押して進みます。次の step 1 ではそのまま Next を押して進みます。

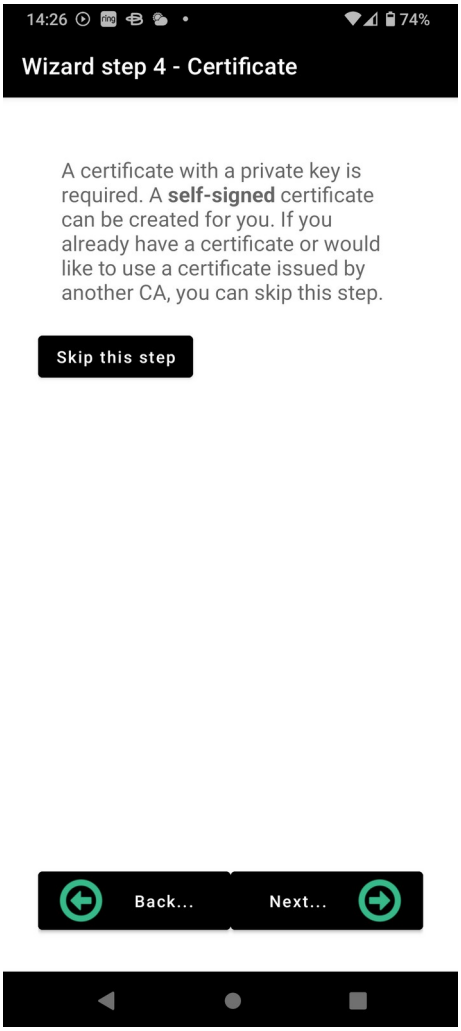


step 2 では使うメールアドレスを入れます。step 3 で「SMTP Setup」を押して SMTP の設定を行います。



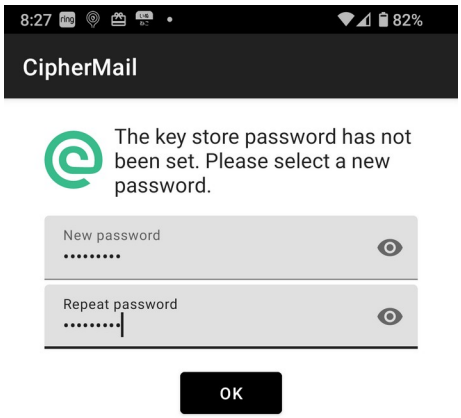
この例では Gmail の場合ですが、お使いのメールに合わせて SMTP を設定してください。なお、Google で二段階認証にしている場合はアプリ用のパスワードを生成してここで入れます。step 4 から証明書の設定です。今回は self signed certificate、つまり「オレオレ証明書」を作るので Next を押します。すでに Actalis 等の証明書を持っている場合は Skip this step を押します(「既存証明書編」で説明)。

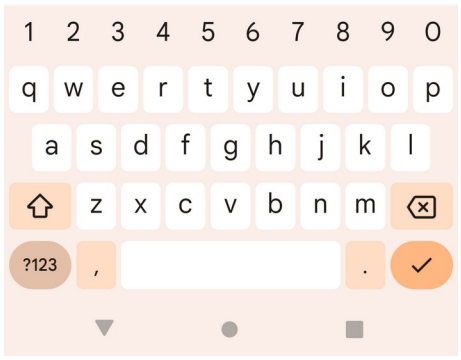




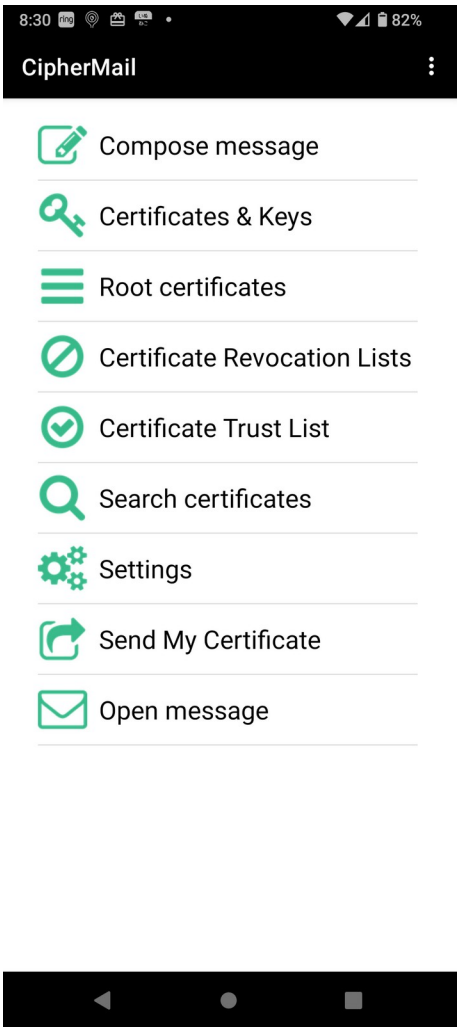
オレオレ証明書編

ここでオレオレ証明書を作り、パスワードを設定します。署名付きのメールや暗号化メールを送るたびに、あるいは暗号化されたメッセージを読むたびにパスワードを入力させられるので短めのほうがいいでしょう。

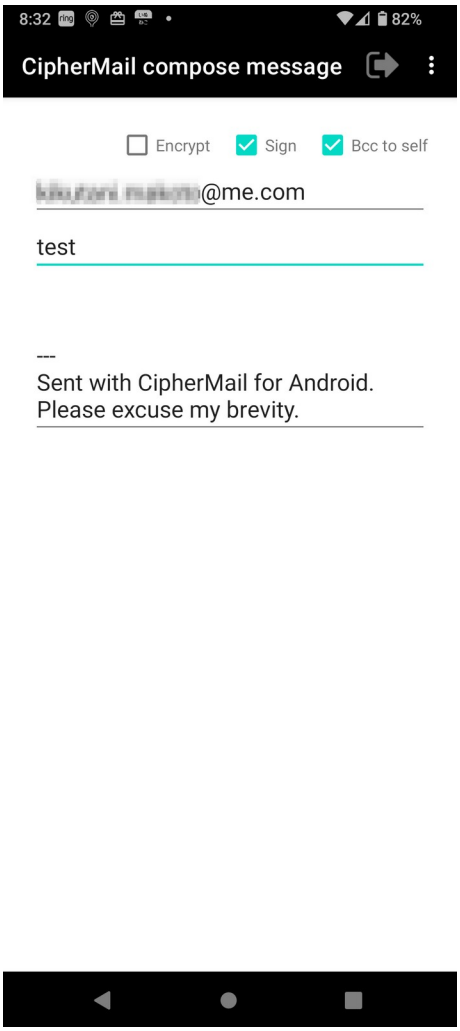




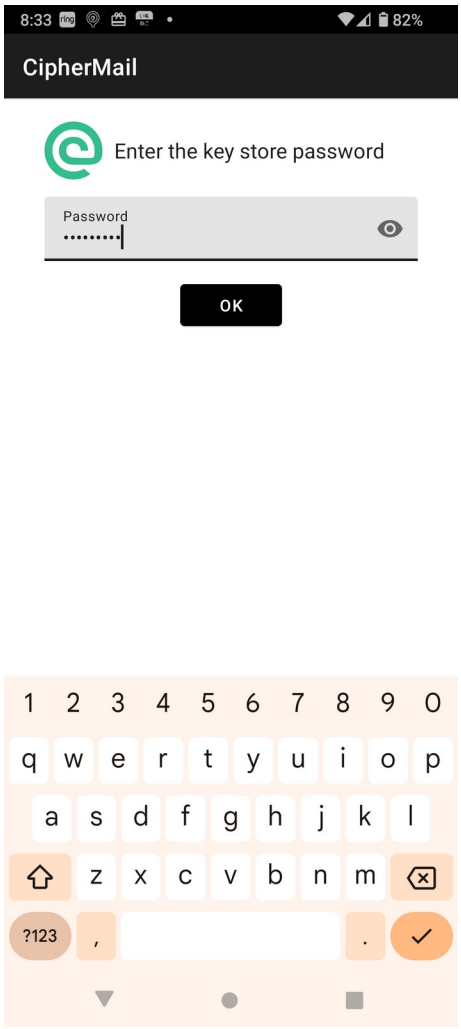
ここでいったんウィザードは終了するのでメインメニューになります。ここで Certificates & Keys を選択します。



作られたオレオレ証明書が見えます。次にメインメニューの Compose messag を選択してテストメールを @me.com 宛に送ることにします。今回は署名だけで暗号化はしません。本文は省略してます。



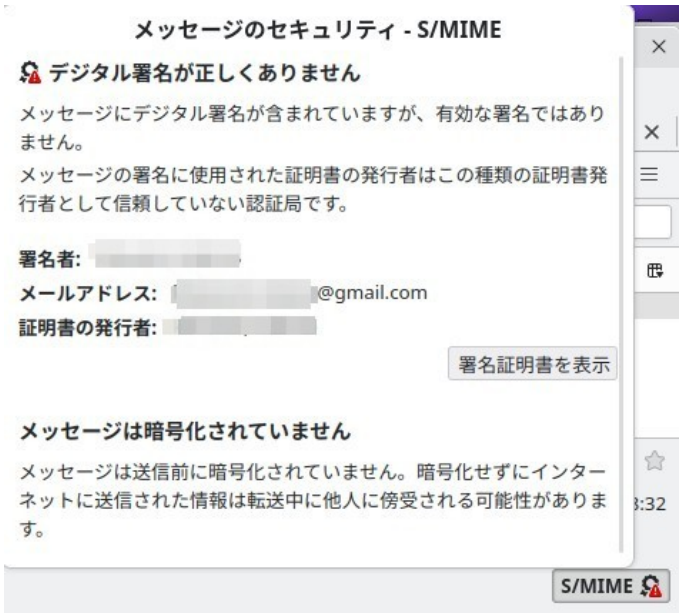
証明書を作ったときに設定したパスワードを入れると送信できます。



送られた @me.com 側は Thunderbird で読むとこうなります。S/MIME のマークに赤い警告が付いてることに注意です。

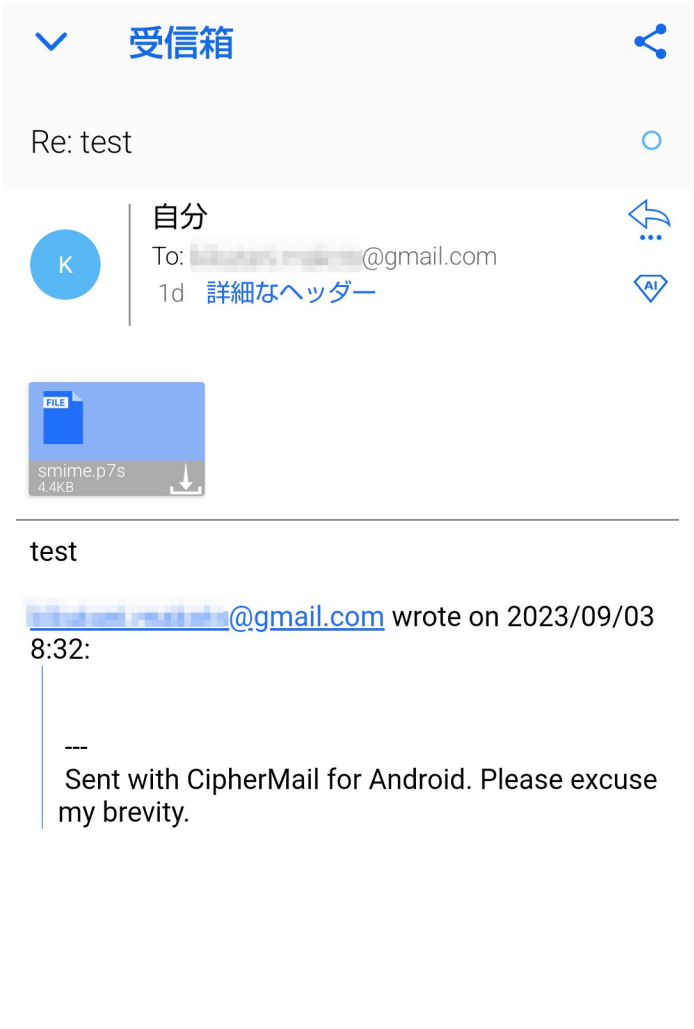

```
---
Sent with CipherMail for Android. Please excuse my brevity.
```

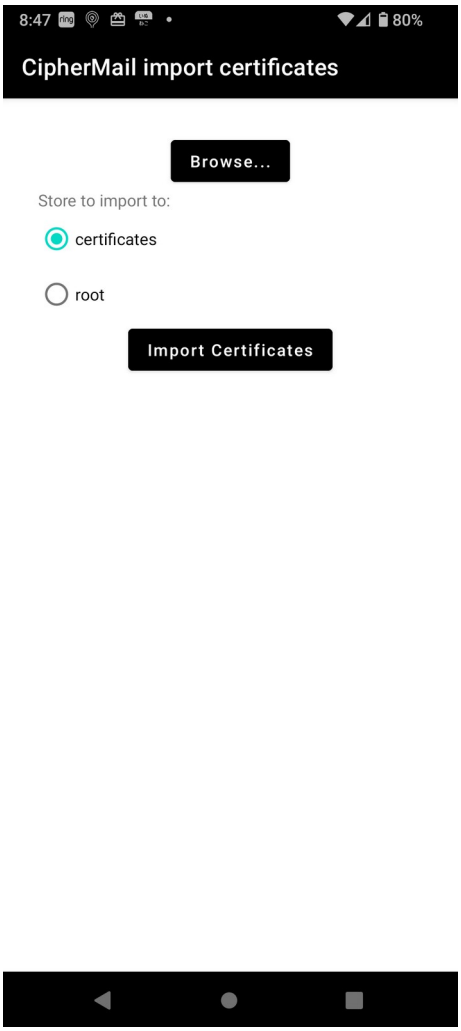
S/MIME のマークをクリックするとこうなってオレオレ証明書であることがわかります。



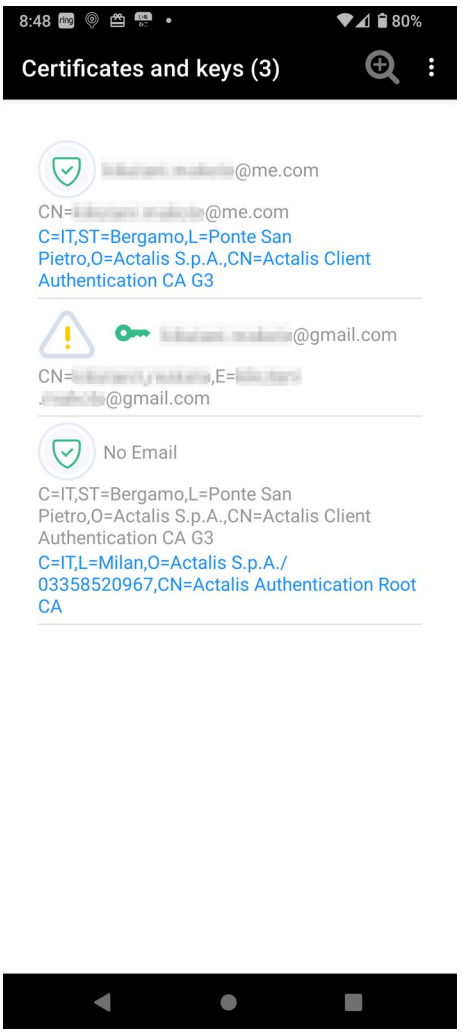
@me.com 側ではこのメッセージに S/MIME 署名して返信します。こちらの証明書を送るためです。

Android 側では@me.com から送られた返信を BlueMail で読むとこう見えます。smime.p7s という添付ファイルが S/MIME 署名された証明書なので、これをクリックすると CipherMail が開くので、Import Certificates を押します。

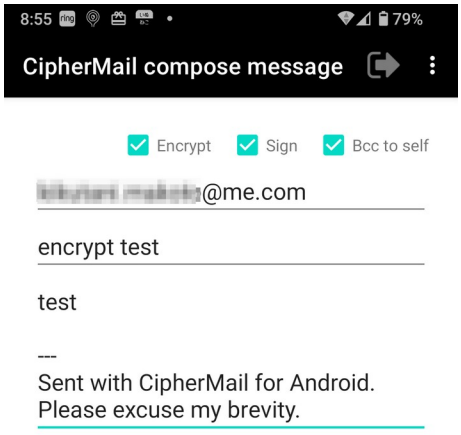




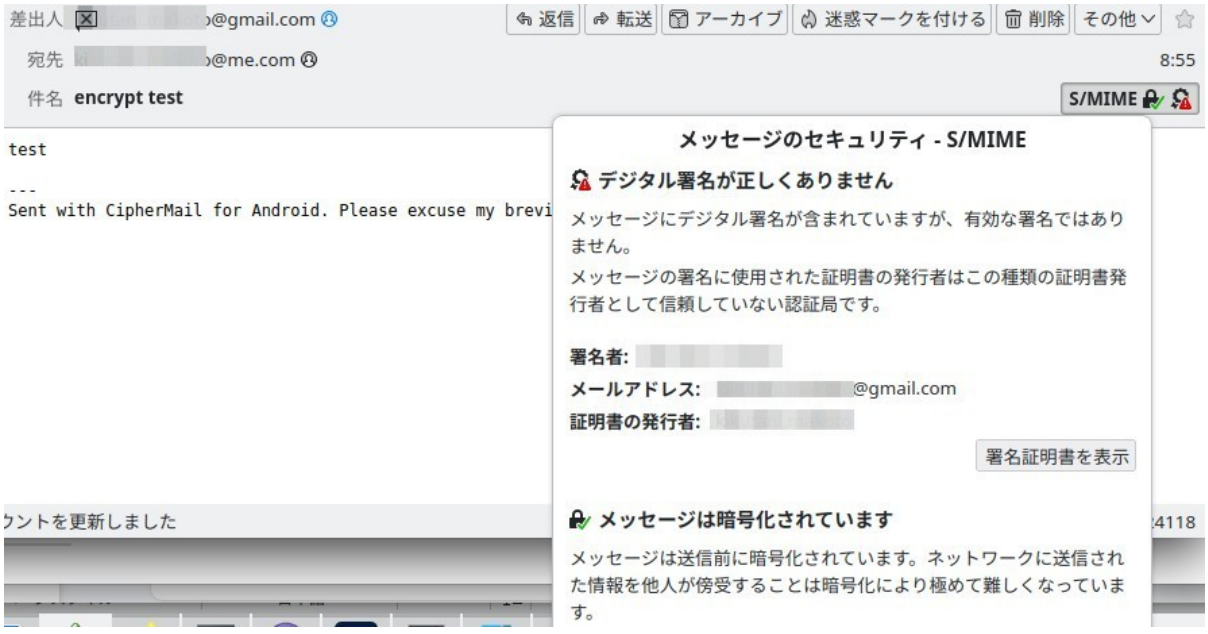
2 certificates were imported と出ます。CipherMail の Certificates & Keys 画面で見ると右のように見えて、@me.com 側の Actalis で作られた証明書がインポートされていることがわかります。



@me.com 側の証明書を持ったので、今度は CipherMail で暗号化したメッセージを送れます。署名だけのときと同様、パスワードの入力が求められます。



@me.com 側で Thunderbird で読むと以下のように、ちゃんと暗号を復号できて読めます。



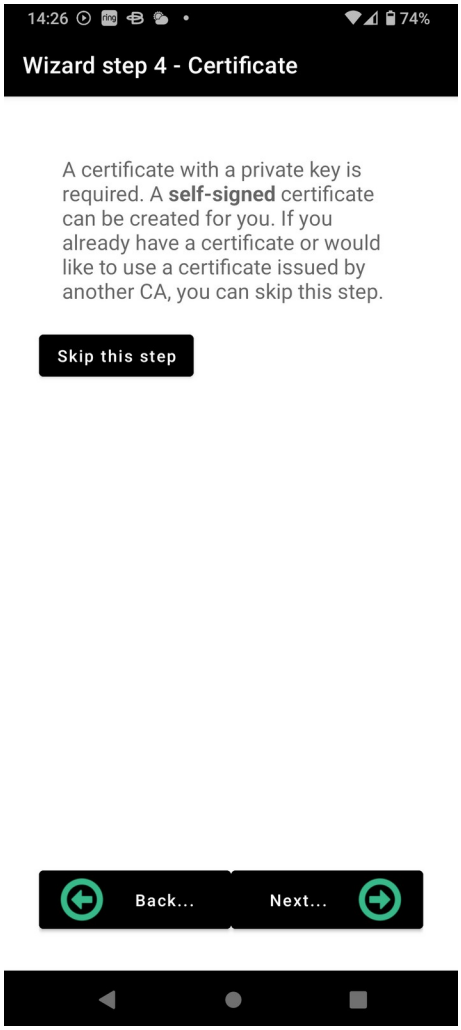
このあと、以下のシナリオをやりたいところですが、

- PC で bar@me.com から foo@gmail.com へ暗号化したメッセージを送る
- CipherMail を使ってその暗号化されたメッセージを読む

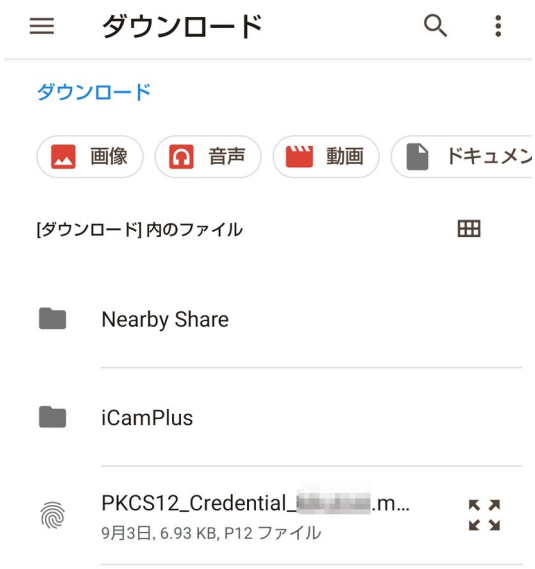
どうもオレオレ証明書では Thunderbird が自動でインポートしてくれないのか、うまく行かなかったので、この部分は次の「既存証明書編」でやります。

既存証明書編

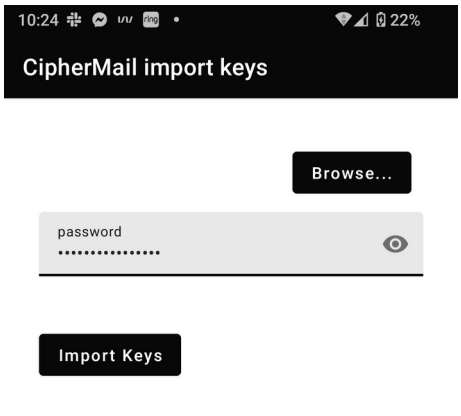
Wizard の step 4 でオレオレ証明書を作らず Skip this step を押し、メインメニューから Certificates & Keys を選択し、右上のメニューから Import keys を選択します。

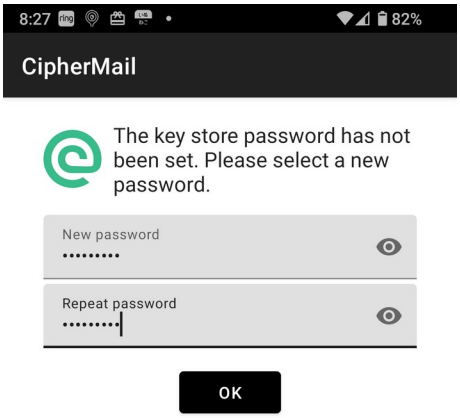


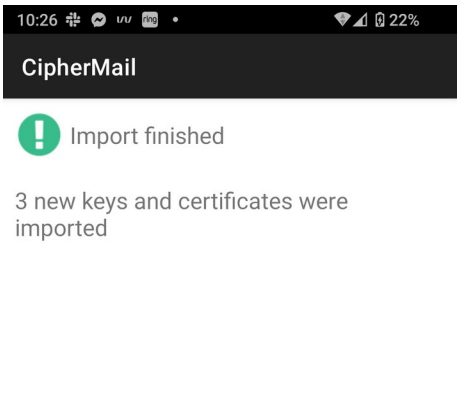
この例では Actalis の証明書をインポートする例を示しますが、
PKCS12_Credential_foo@gmail.com.pfx を何らかの方法で Android のダウンロード・フォルダに持ってきます。Google Drive を経由して持ってくるなどが考えられます。

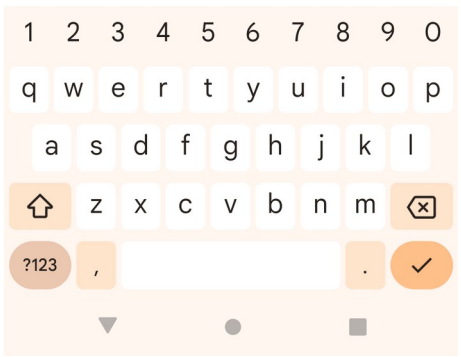


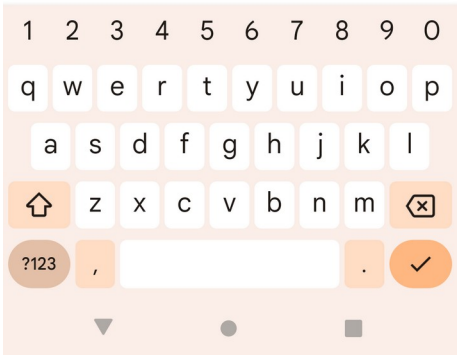
Actalis で証明書を作ったときのパスワードを使ってインポートします。また、証明書を使うときのパスワードも設定します。



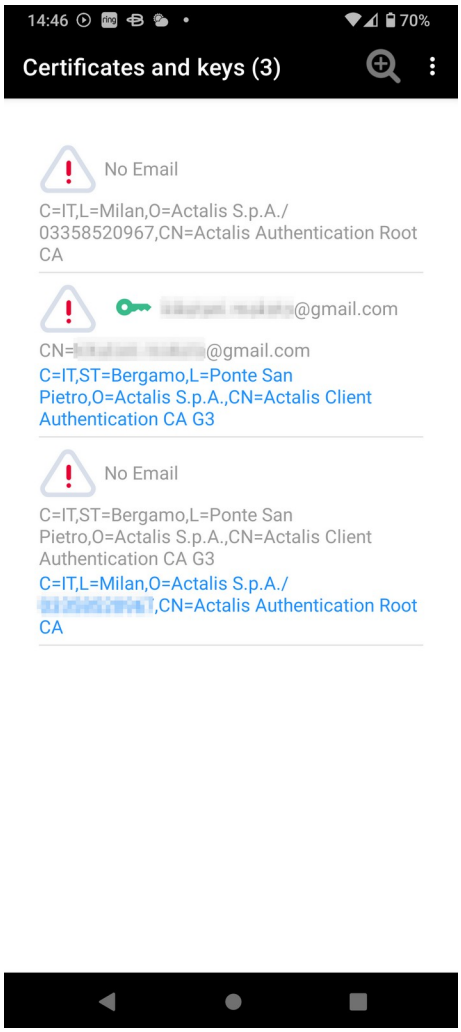


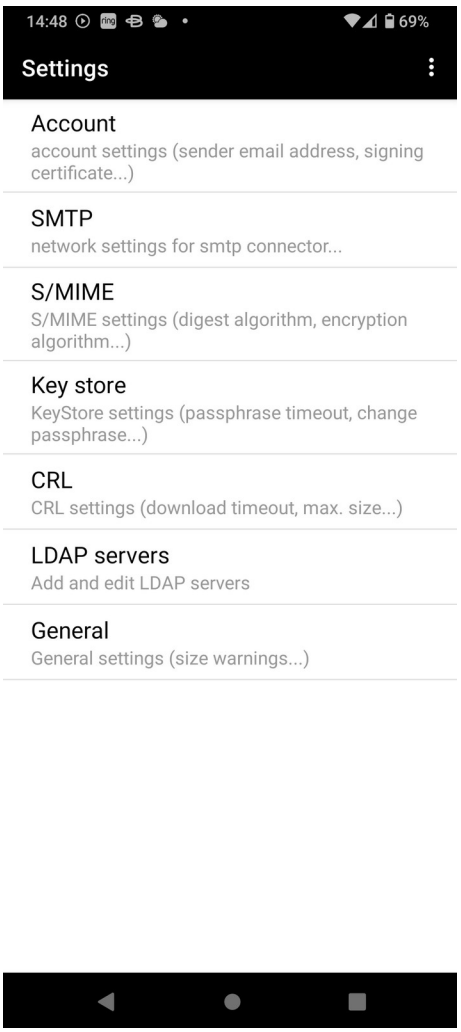




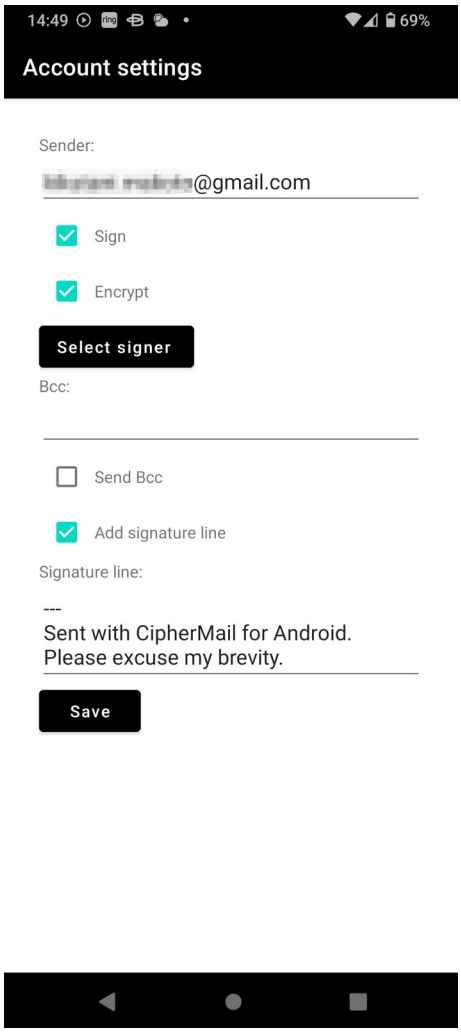


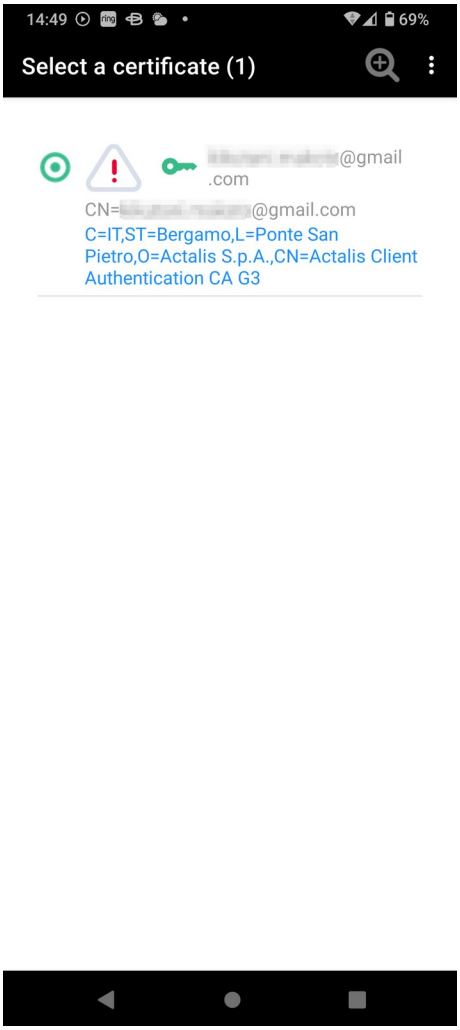
以下のように三つのキーがインポートされていることがわかります。オレオレ証明書のときと違って、インポートした証明書がどのアカウントのものかを教えてやる必要があります。メインメニューから Settings を選び、さらに Account に行きます。



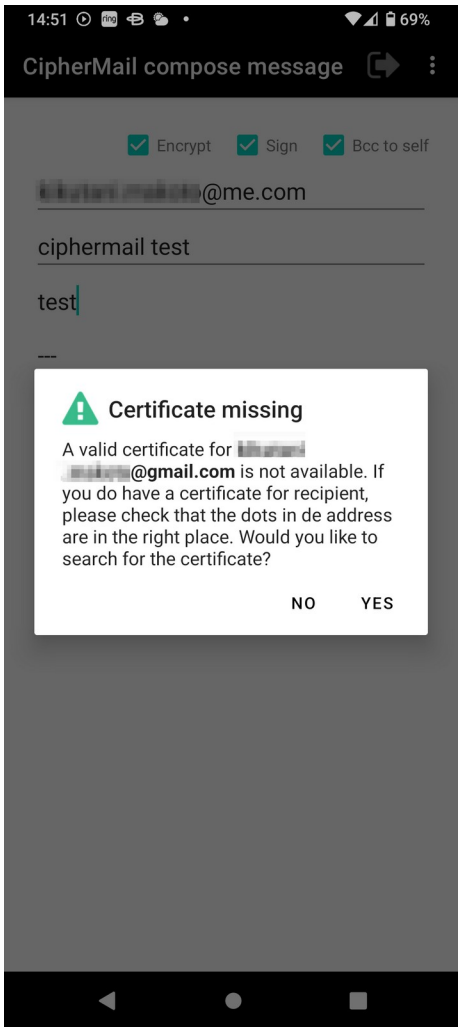


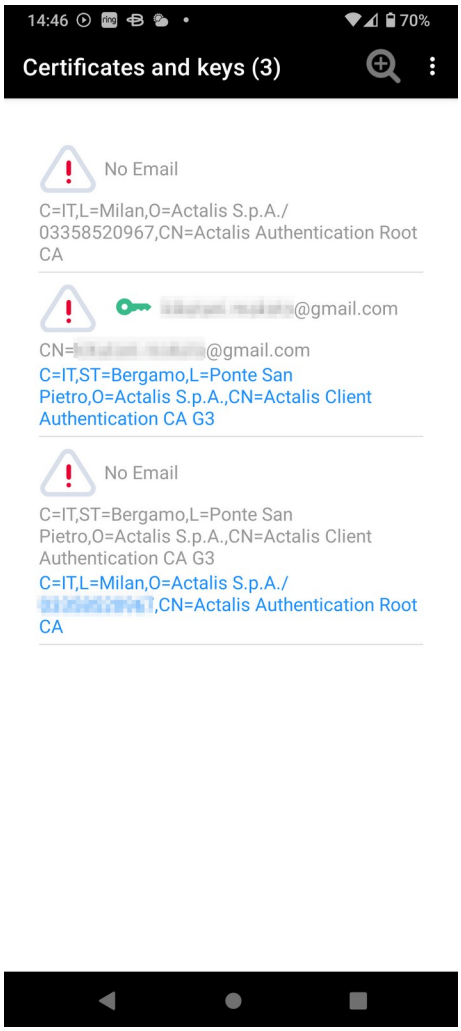
Select signer を押して、@gmail.com の証明書を選びます。



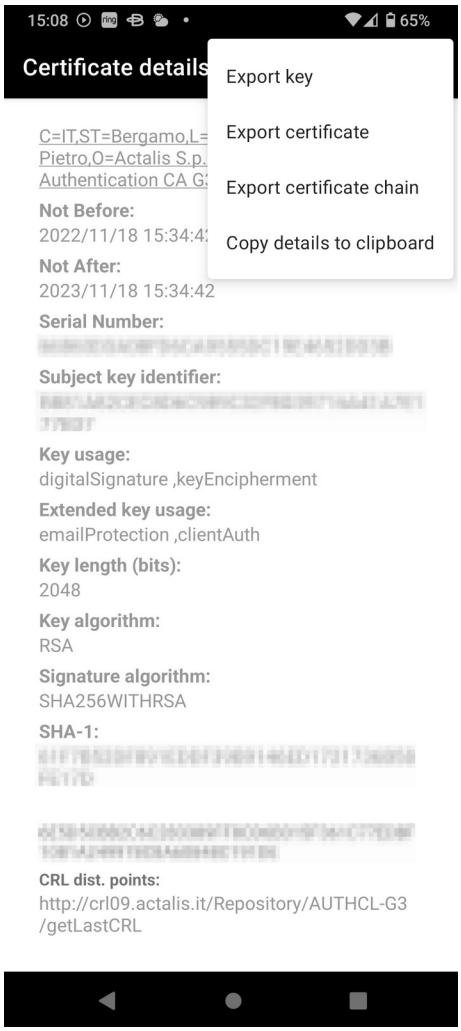


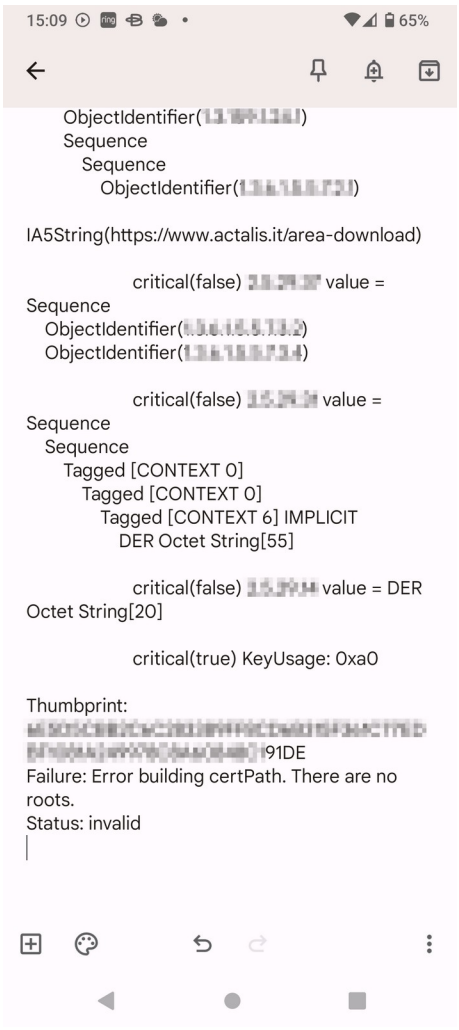
しかし、テストメールを送ろうとしても、アカウントに証明書を紐付けたのに Certificate missing になってしまいます。証明書の search に進んでもみつかりません。この解決はかなりめんどうです。証明書を Certificate Trust List というものに加える必要があるのですが、そのためには証明書の thumbprint を知る必要があります。Certificte and keys 画面から 2 番目を選びます。



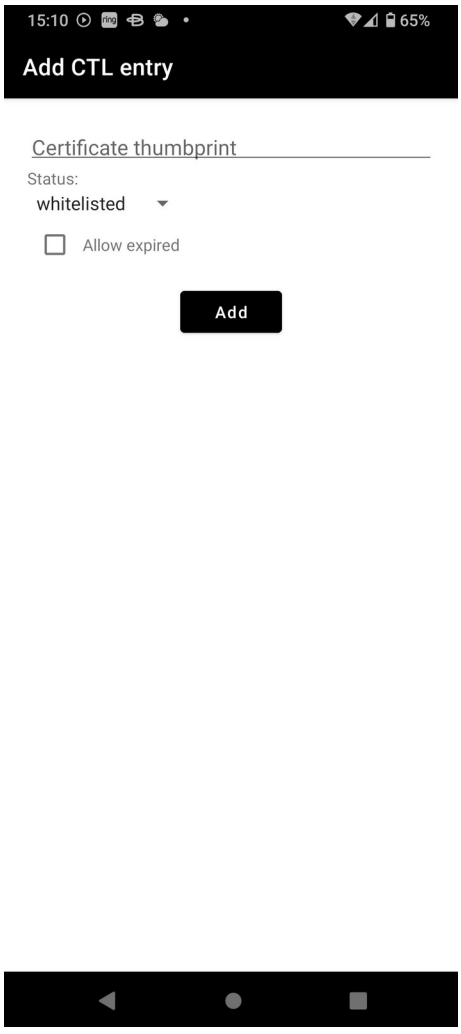


右上のメニューから Copy details to clipboard を選択し、適当なところでペーストし、一番下のところにある Thumbprint の内容をコピーしておきます。





メインメニューから Certificate Trust List を選び、右上のメニューから Add CTL entry を選びます。
先程コピーしておいた thumbprint をペーストして Add を押します。

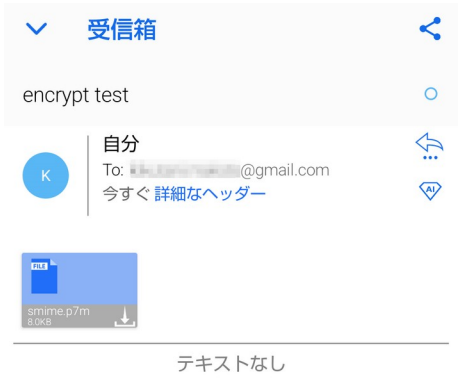


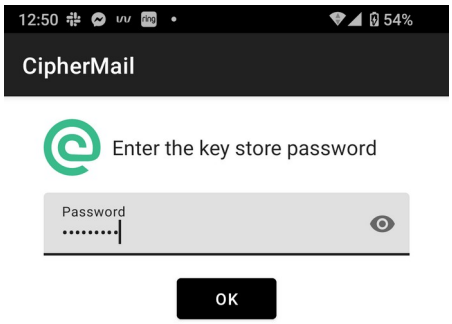
このように whitelisted となって追加されました。あとはオレオレ証明書のときと同様にテストメールを送れます。

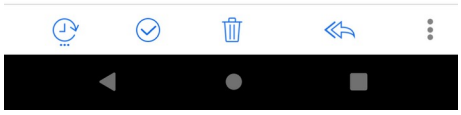
オレオレ証明書のときはできなかった以下をやります。

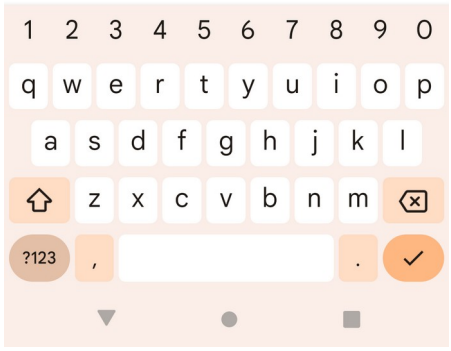
- PC で bar@me.com から foo@gmail.com へ暗号化したメッセージを送る
- CipherMail を使ってその暗号化されたメッセージを読む

BlueMail で暗号化されてきたメッセージを開くと左のように見えます。暗号化されているので本文は BlueMail では読めません。smime.p7m という名の添付ファイルをクリックすると CipherMail が開き、証明書をインポートしたときに設定したパスワードを入力します。









本文が復号され読むことができます。

以上