# 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。

14:09 🕑 📾 🖨 🛸 🔸	<b>♥⊿ 🗎</b> 76%	14:09 🕑 🛅 🖨 🐞 🔹	♥⊿ 🗎 76%
Introduction		Wizard step 1 - Star	rt
Ciphermail for Android allov send encrypted email using account of choice. Click <u>her</u> info.	vs you to your email <mark>e</mark> for more	This wizard will help required settings for wizard can be cance <b>back button</b> .	you configure the CipherMail. This led by clicking the
Click <u>here</u> for more detailed instructions.	setup	The wizard can be re <b>Setup wizard</b> in the r page.	erun by clicking menu of the settings



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。

Skip this step





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)。

SMTP settings		Wizard step 4 - Certificat	e
	Save		
Host: smtp.gmail.com Port 587		A certificate with a priva required. A <b>self-signed</b> can be created for you. I already have a certificate like to use a certificate is another CA, you can skip	te key is certificate f you e or would ssued by o this step.
Authenticate Username:		Skip this step	
password	Ο		
Enable StartTLS			
StartTLS required			
Enable SSL/TLS			
Skip SSL trust check			
NTLM domain:			
Connection timeout (sec.):			
30			
nmeout (sec.):		Back No	ext 🕞
<u> </u>			
•		◀ ●	

# 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。

8:26 🔤 🖗 🗳 🐖 🔹	♥⊿ 🕯 82%	8:27 📖 🤅		▼⊿ 🕯 82%
Wizard step 4 - Generat	e certificate	Cipher	Mail	
A valid <b>email address</b> a required for the certific	and <b>name</b> is vate.	e	The key store pa been set. Please password.	ssword has not select a new
Email: @gmail.	com	New	password	0
Name:		Repe	eat password	O
			ок	



1	2	3	4	5	6	7	8	9	0
q	w	е	r	t	у	u	i	0	р
а	S	6 (	t b	Ę	g ł	ו j	k		I
仑	z	z ;	k d		/ k	o r	n m	1	$\overline{\times}$
?123									~
	,			•					

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。

14:27 ⊙ 🔤 🔁 💁 • 💎 🖈 🛊 74%	8:30 🔤 🍥 🗳 🛄 🔸	▶⊿ 🕯 82%
Wizard step 6 - Finish	CipherMail	•
The wizard has finished. The wizard can be rerun by clicking <b>Setup wizard</b> in the	📝 Compose message	
menu of the settings page.	🝳 Certificates & Keys	
	Root certificates	
	O Certificate Revocation	1 Lists
	📀 Certificate Trust List	
	<b>Q</b> Search certificates	
	🔅 Settings	
	🕝 Send My Certificate	
	Open message	



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。

8:29 🔤 🍥 🛱 📟 🔹	▼⊿ 🕯 82%	8:32 🔤 🖗 🛱 🛄 🔹 🔍 🗣 🖍 🛊 82%
Certificates and keys (1)	<b>(</b> :	CipherMail compose message 🚺 :
CN= ,E= . @gmail.com	gmail.com	Encrypt Sign Bcc to self
		 Sent with CipherMail for Android. Please excuse my brevity.



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。

メッセージのセキュリティ - S/MIME	×
🔒 デジタル署名が正しくありません	^
メッセージにデジタル署名が含まれていますが、有効な署名ではあり ません。	×
メッセージの署名に使用された証明書の発行者はこの種類の証明書発 行者として信頼していない認証局です。	
署名者:	œ,
メールアドレス: @gmail.com 証明書の発行者:	
署名証明書を表示	
メッセージは暗号化されていません	
メッセージは送信前に暗号化されていません。暗号化せずにインター ネットに送信された情報は転送中に他人に傍受される可能性がありま す。	合 3:32
S/MIM	ie 🔉

@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。

◇ 受信箱	<	8:47 📾 💿 🖴 💀 • CipherMail import certific	▼⊿ ≌ 80% cates
Re: test	0	Browse	
к 自分 To: @gmail.com 1d 詳細なヘッダー	₹ <u>,</u>	Store to import to: <ul> <li>certificates</li> <li>root</li> </ul> Import Certification	tes
smime.p7s 4.4KB			

**2023/09/03** 8:32:

----

Sent with CipherMail for Android. Please excuse my brevity.



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。

8:47 🚾 🍥 🛱 🌄 🔹 💎 🔷 🗣 🔊	8:48 🔤 🍥 🛱 🛤 🔹 • 🔍 🗣 🖍 🕯 80%
CipherMail	Certificates and keys (3)
Import finished	
2 certificates were imported	@me.com CN= @me.com C=IT,ST=Bergamo,L=Ponte San Pietro,O=Actalis S.p.A.,CN=Actalis Client Authentication CA G3
	CN= 
	C=IT,ST=Bergamo,L=Ponte San Pietro,O=Actalis S.p.A.,CN=Actalis Client Authentication CA G3 C=IT,L=Milan,O=Actalis S.p.A./ 03358520967,CN=Actalis Authentication Root
	CA



@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。

8:55 🔤 💿 🛱 🛄 🔹	
CipherMail compose message 🚺 :	
🗸 Encrypt 🔽 Sign 🔽 Bcc to self	
@me.com	
encrypt test	
test	
 Sent with CipherMail for Android. Please excuse my brevity.	



@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。

差出人 区 b@gmail.com <sup>®</sup> 宛先 b@me.com <sup>®</sup>	昼信 ◎ 転送 留 アーカイブ ◎ 迷惑マークを付ける 節 削除 その他 ~ 合     8:55
件名 encrypt test	S/MIME 🔐 💫
test  Sent with CipherMail for Android. Please excuse my brev	メッセージのセキュリティ - S/MIME ☆ デジタル署名が正しくありません メッセージにデジタル署名が含まれていますが、有効な署名ではあり ません。 メッセージの署名に使用された証明書の発行者はこの種類の証明書発 行者として信頼していない認証局です。 署名者: メールアドレス: @gmail.com 証明書の発行者: 署名証明書を表示

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、

<u>PKCS12 Credential foo@gmail.com.pfx</u> 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。

≡	ダウンロード	Q	:
ダウン	レロード		
	画像   百音   斷 動画     1	ドキ	כאב
[ダウン	/ロード] 内のファイル	⊞	1
	Nearby Share		
	iCamPlus		
Ĩ	PKCS12_Credentialm 9月3日, 6.93 KB, P12 ファイル	Ř	K.

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。

10:24 🧩 🗭 🗤 💼 🔹	🎔 🖌 🕃 22%	8:27 🔤 🖗 🛱 🐖 🔸	▼⊿ 🕯 82%	10:26 <b>‡ 🗭</b> 🗤 📠 🔹	♥⊿ 🖟 22%
CipherMail import keys		CipherMail		CipherMail	
	Browse	The key store pass been set. Please se password.	word has not elect a new	Import finished 3 new keys and certifica	ites were
password	Ø	New password	Ø	imported	
Import Keys		Repeat password	•		



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。

# 14:46 ○ ■ ● ● ● •

No Email C=IT,L=Milan,O=Actalis S.p.A./ 03358520967,CN=Actalis Authentication Root CA

gmail.com

CN= @gmail.com C=IT,ST=Bergamo,L=Ponte San Pietro,O=Actalis S.p.A.,CN=Actalis Client Authentication CA G3

No Email

C=IT,ST=Bergamo,L=Ponte San Pietro,O=Actalis S.p.A.,CN=Actalis Client Authentication CA G3 C=IT,L=Milan,O=Actalis S.p.A./ CA

### 14:48 ⊙ ⊕ ≌ • ♥⊿ ≌ 69% Settings

#### Account

account settings (sender email address, signing certificate...)

#### SMTP

network settings for smtp connector...

#### S/MIME

S/MIME settings (digest algorithm, encryption algorithm...)

#### Key store

KeyStore settings (passphrase timeout, change passphrase...)

#### CRL

CRL settings (download timeout, max. size...)

#### LDAP servers

Add and edit LDAP servers

#### General

General settings (size warnings...)



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

14:49 🕑 🔤 🖨 🖀 🔹	▼⊿ 🕯 69%	14:49	• 🖶 🗗 🌘	6 🖬 🗣	9%
Account settings		Selec	ct a certificate (1)	Ð	••
Sender: Sign Encrypt		0	CN= @gmail C=IT,ST=Bergamo,L=Ponte S Pietro,O=Actalis S.p.A.,CN=, Authentication CA G3	@gmail .com San Actalis Clien	t
Select signer					
Send Bcc  Add signature line					
Sent with CipherMail for Andro Please excuse my brevity.	bid.				

•	•		•		

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。

15:08 🕑 🔤 🖨 🐞 🔹	▼⊿ 🕯 65%	15:09 🕑 🔤 🖶 🍗 🔹
Certificate details	Export key	<del>~</del>
<u>C=IT,ST=Bergamo,L=</u> <u>Pietro,O=Actalis SAP</u>	Export certificate	ObjectIdentifier Sequence Sequence
Not Refere:	Export certificate chain	Objectiden
2022/11/18 15:34:4:	Copy details to clipboard	IA5String(https://ww
Not After: 2023/11/18 15:34:42		critical
Serial Number:	0850-019046820-008	ObjectIdentifier(1 ObjectIdentifier(1
Subject key identifier		critical
BBS/AS2CEC8DBC/H 37821	NCIOPELINTIALITAN(1	Sequence Sequence
<b>Key usage:</b> digitalSignature ,keyE	ncipherment	Tagged [CONTE Tagged [CON
Extended key usage: emailProtection ,clien	tAuth	Tagged [C0 DER Octe
Key length (bits): 2048		critical
<b>Key algorithm:</b> RSA		critical
Signature algorithm: SHA256WITHRSA		Thumbprint:
SHA-1:		46505CER2CVC283
61F79630F894CD0F	20091464077711336058	Failure: Error buildin
6238-52680042350089 TOBAD-RETEXABLE	TRONIDOHS/DAVICT/EDBC ICTIVIDE	Status: invalid
CRL dist. points:		
http://crI09.actalis.it/ /getLastCRL	Repository/AUTHCL-G3	E ©



÷	д	Ð	₩
Object/dentifier(	II) R.R.P.2	)	
IA5String(https://www.actalis.it/	area-d	ownloa	ıd)
critical(false)	)  )  )	lue =	
critical(false) 15.2 Sequence Tagged [CONTEXT 0] Tagged [CONTEXT 0] Tagged [CONTEXT 6] I DER Octet String[55]	MPLIC	ue = IT	
critical(false)	va va	ue = D	ER
critical(true) KeyUs	sage: C	)xaO	
Thumbprint: 91E Failure: Error building certPath. roots. Status: invalid	DE There	are no	ED
E 🖓 5 d			•••
۰ ا			

▼⊿ 🕯 65%

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。

15:09 🕑 🔤 🖨 🖀 🔹	♥⊿ 🗎 65%	15:10 🕑 🔤 🖨 🛸 🔹	♥⊿ 🖬 65%
Certificate Trust Lis	Add CTL entry	Add CTL entry	
		Certificate thumbprint Status:	
		Allow expired	
		Add	



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。

◇ 受信箱	<	12:50 🍀 🔗 🗤 📾 🔹	<b>♥⊿</b> 🛿 54%
		CipherMail	
encrypt test	0		
K 自分 To: @gmail.com	€	Enter the key store	e password
	v	Password	o
smime p7m		ок	
テキストなし			



本文が復号され読むことができます。

## CipherMail view message : AES128, Key size: 128 Signed by: @me.com S/MIME layers ►

暗号化したメッセージ

