

DJIGZO EMAIL ENCRYPTION

DJIGZO for Android Reference Guide



March 11, 2012, Rev: 5460

Contents

1	Introduction	3
2	Start page	3
3	Certificates & Keys	5
3.1	Certificate details	5
3.2	Import keys	6
3.3	Import certificates	7
4	Root certificates	8
5	CRLs	8
5.1	CRL details	9
6	CTLs	9
7	Search certificates	10
7.1	Import certificates	12
7.2	LDAP servers	12
7.2.1	Adding LDAP server	12
8	Composing email	14
8.1	Signing the message	15
8.2	Encrypting the message	15
8.3	Bcc to self	16
8.4	Attachments	17
8.5	Drafts & Templates	18
8.6	Attach my certificate	18
9	Opening email	18
9.1	S/MIME layers	18
9.2	Menu options	20
9.3	Importing certificates from email	22
9.4	Importing certificates from signatures	22
9.5	Importing .pfx files from email	23
10	Settings	24
10.1	Account	24
10.2	SMTP	26
10.3	S/MIME	27
10.4	Key Store	28
10.5	CRL	29
10.6	LDAP servers	30
10.7	General	30

1 Introduction

This reference guide explains in detail all the features and settings of DJIGZO for Android. This guide assumes that DJIGZO for Android has already been installed and that the setup wizard has already been run. See the *DJIGZO for Android Quick Install Guide* for installation instructions.

Features: DJIGZO for Android has the following features:

- Encryption and digital signing with S/MIME 3.1 (X.509, RFC 3280).
- Can be used with the Android Gmail application.
- Compatible with existing S/MIME clients (like Outlook, Lotus Notes, Thunderbird etc.)
- Message body and attachments are encrypted.
- HTML email support.
- Certificates are automatically extracted from incoming email.
- Certificate revocation lists (CRLs) are automatically downloaded (LDAP and HTTP).
- Certificate trust lists (CTLs) can be used to black or white-list certificates.
- External LDAP servers can be queried for new certificates.
- Can generate self-signed certificates for a “private-PKI”.

2 Start page

The DJIGZO start page contains the following items (see figure 1):

- Compose message
- Certificates & Keys
- Root certificates
- CRLs
- CTLs
- Search certificates
- Settings

The main menu of the start page (which will be viewed when the menu button is pressed) contains some extra functionality (see figure 2). The next chapters will explain in detail all the relevant functionality.

Note the chapters are not necessarily in the same order as the main page menu items.

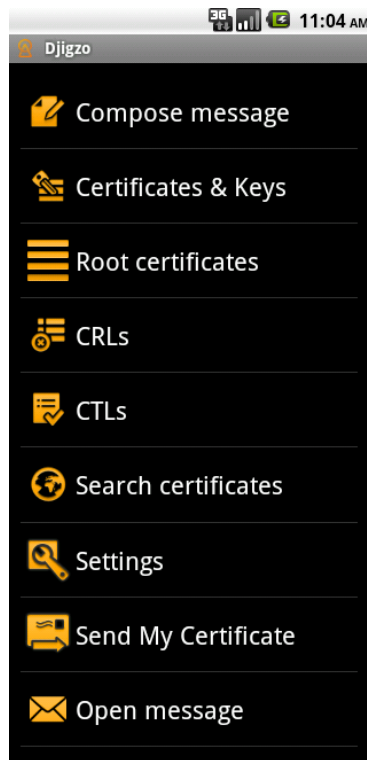


Figure 1: Start page

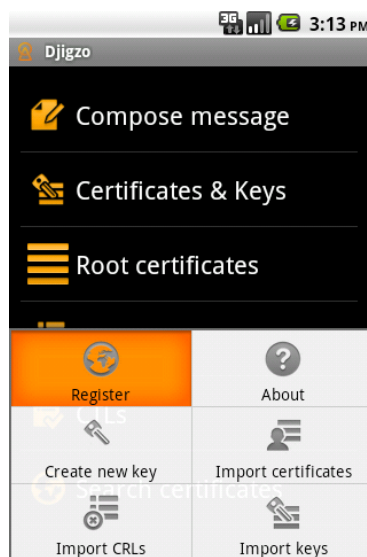


Figure 2: Start page - menu

3 Certificates & Keys

All the end-user and intermediate certificates and their associated private keys are stored in the *Certificate & Keys* store (see figure 3). When the *Certificate & Keys* page is opened, all the visible certificates in the store are PKI validated, i.e., the certificates are checked to see whether they are valid, not revoked, not expired etc. The different certificate status types can be seen in figure 12. If a certificate has an associated private key, a *key* icon is visible for the certificate entry.

The email addresses for which the certificate is issued, the subject of the certificate and the issuer of the certificate are shown. The certificate details page, for example to get more information why a certificate is not valid, can be opened by clicking the certificate entry or by opening the context menu (using a *long click*) and then select *Details* from the context menu.

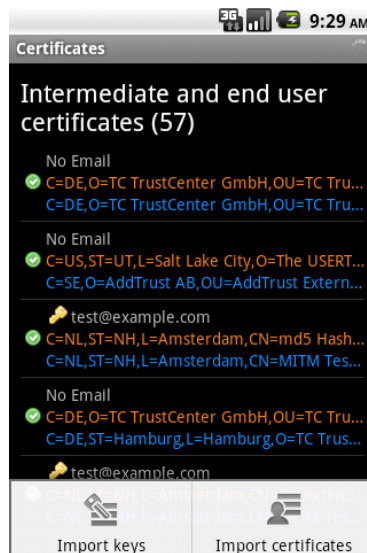


Figure 3: Certificates & Keys



Figure 4: Certificate status types

3.1 Certificate details

The certificate details page shows more information about the certificate (see figure 5). If a certificate is valid, for example the certificate is not issued by a trusted root, the certificate details page provides information why the certificate is not valid. The menu options contain the following menu items: a) Export

key; b) Export certificate; c) Export certificate chain; and d) Copy details to clipboard.

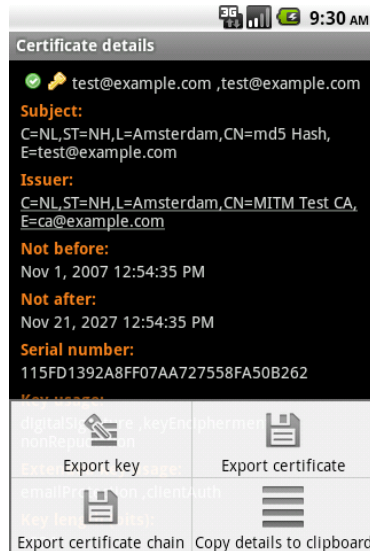


Figure 5: Certificates & Keys

Export key With the *Export key* option, the certificate and private key can be exported to a password protected *.pfx* file. The *Export key* option is only enabled if the certificate entry has an associated private key.

Export certificate With the *Export certificate* option, a certificate can be exported to a *.cer* file.

Export certificate chain With the *Export certificate chain*, the complete certificate chain, i.e., the end-user and all certificate up to the root, can be exported to a *.p7b* file. The *Export certificate chain* option is only enabled if the certificate chain is available.

Copy details to clipboard With the *Copy details to clipboard*, all the certificate details will be copied to the clipboard. This can be helpful for example when the certificate details need to be emailed.

3.2 Import keys

With the *Import keys* menu option, certificates and their associated private keys can be imported into the *Certificates & Keys* store (see figure 6). With the *Browse* button, a password protected *.pfx* file can be selected for import. Since a *.pfx* file can contain multiple certificates and keys, a progress dialog is shown while importing the *.pfx* file (see figure 6).

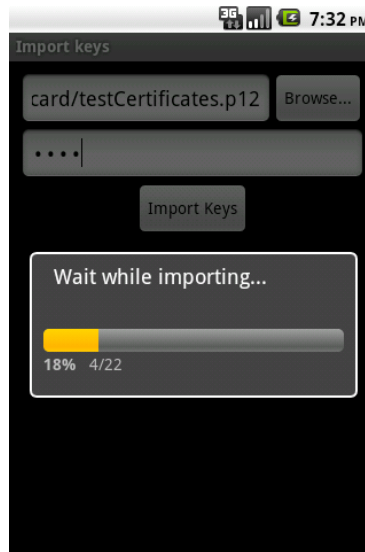


Figure 6: Import keys

3.3 Import certificates

With the *Import certificates* menu option, certificates can be imported into the *Certificates & Keys* store (see figure 7). The store to import to is set to *certificates* if the import was started from the *Certificates & Keys* store and cannot be changed. If the import was started from the *Root certificates* store, root will be selected.

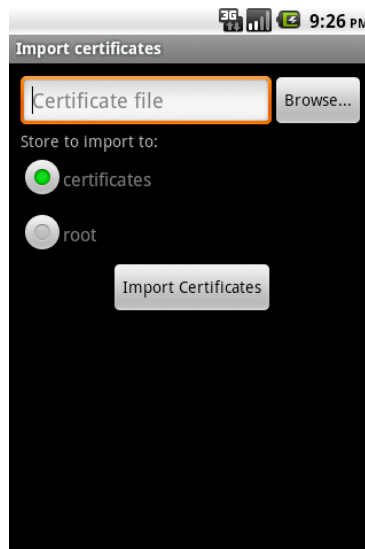


Figure 7: Import certificates

4 Root certificates

The *Root certificates* store contains the trusted certificate authorities (CAs). Only certificates can be imported into the root store.

5 CRLs

The *CRLs* store contains all the downloaded and imported *Certificate Revocation Lists (CRLs)* (see figure 8). CRL details can be viewed by clicking the CRL entry. The context menu (activated with a long click) allows you to delete the CRL entry.

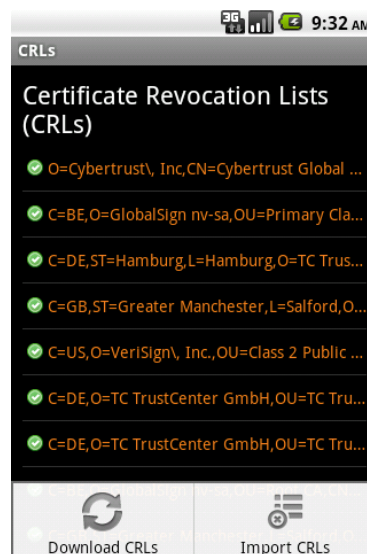


Figure 8: CRLs

Download CRLs Certificates sometimes contain URLs from which a CRL can be downloaded (the so called *CRL distribution points*). When the *Download CRLs* menu option is clicked (see figure 8), all the certificates from the certificate and root store are scanned for any *CRL distribution points* and the CRLs are downloaded. Sometimes CRLs can be very large in size, often too large to be handled by an Android application. If a CRL is larger than the max CRL size, default set at 1MB (see CRL settings), the CRL is skipped.

Note: Downloading a large number of CRLs can consume a lot of bandwidth. It's therefore advised to only download CRLs via WIFI.

Import CRLs CRLs can be manually imported via the *Import CRLs* page. This allows you to use a CRL when the certificate does not contain a *CRL distribution point* or when the *CRL distribution point* cannot be accessed from the Android device.

5.1 CRL details

The CRL details (see figure 9) can be viewed by single clicking the CRL entry, or by selecting *Details* from the context menu.

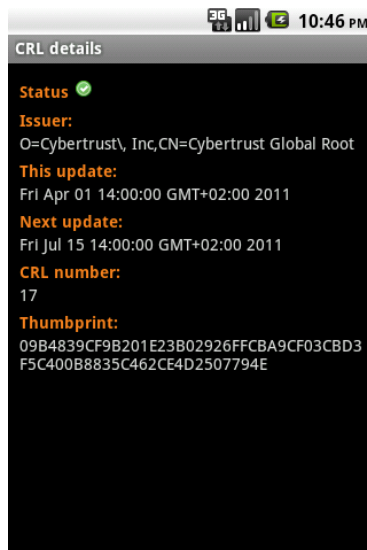


Figure 9: CRL details

6 CTLs

A Certificate Trust List (CTL) is a list of certificates (to be precise, a list of certificate thumbprints) which are explicitly trusted (*white listed*) or explicitly distrusted (*black listed*). The administrator can manually add or remove certificates to the Certificate Trust List. In most cases PKI is sufficient for deciding whether or not a certificate is valid. Sometimes however, the administrator needs more control over this automatic process. Some examples when a CTL can be helpful:

- a)** A certificate should no longer be used because it was compromised but the certificate issuer does not have a CRL. In this case the user can *black list* the certificate.
- b)** A certificate is not valid because the root is missing. The user however knows that the certificate is valid (for example the thumbprint has been checked over the phone). After *white listing* the certificate, the certificate is trusted and can therefore be used.
- c)** A certificate is not valid because the certificate has expired. However, the user is 100% certain that the certificate is still 'valid'. By *white listing* the certificate and checking the *Allow expired* checkbox the certificate is trusted and can therefore be used.

Note: The CTL should only be used as a “last resort” mechanism when a full PKI approach is not sufficient.

A certificate can be placed on the CTL by selecting the *Add to CTL* from the certificate context menu (see figure 10). Alternatively, a CTL entry can be added by clicking the *Add CTL entry* menu item from the CTL page (see figure 11). A *whitelisted* entry is shown with the whitelisted icon (figure 12-a) and a *blacklisted* entry is shown with the blacklisted icon (figure 12-b).

If a CTL entry is underlined (the first entry in figure 11 is underlined, the second is not) it means that there is a certificate available in the *Certificates & Keys* store associated with the CTL entry. Clicking the underlined CTL entry open the certificate details page of the certificate. If the CTL entry is not underlined, there is no associated certificate available. A CTL entry can be removed by opening the context menu for the CTL and then select *Delete* from the context menu.

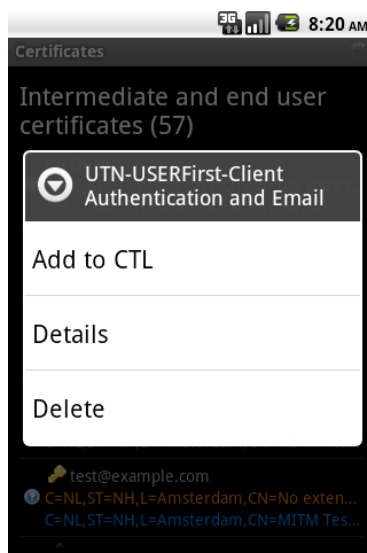


Figure 10: Add to CTL

7 Search certificates

The *Search certificates* functionality can be used to query external LDAP servers for certificates (see figure 13). By default two public accessible LDAP servers are searched: Trustcenter and Verisign.

Certificates can be queried based on *name*, *email* or *company*. The following matching rules can be selected: a) Equality; b) Approximate; and c) Sub-string.

Equality With *Equality* matching, LDAP entries only match if the fields of the entry are equal to the search fields.

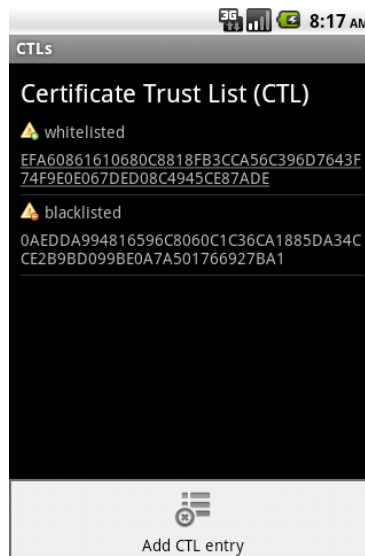


Figure 11: CTL



Figure 12: CTL status icons

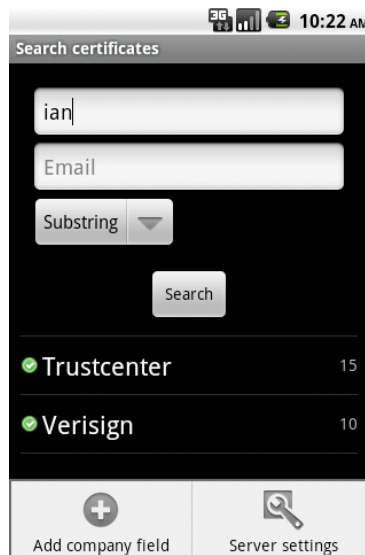


Figure 13: Search certificates

Approximate With *Approximate* matching, LDAP entries match if they are approximately equal to the search fields. The algorithm used for approximate matching depends on the LDAP server and on the field type.

Substring With *Substring* matching, LDAP entries only match if the search fields are a substring of the LDAP entries.

7.1 Import certificates

Newly found certificates can be viewed by clicking the LDAP server entry. Certificates can be added to the *Certificates & Keys* store by opening the context menu for the certificate and select *Add to certificate & key store* (see figure 14).

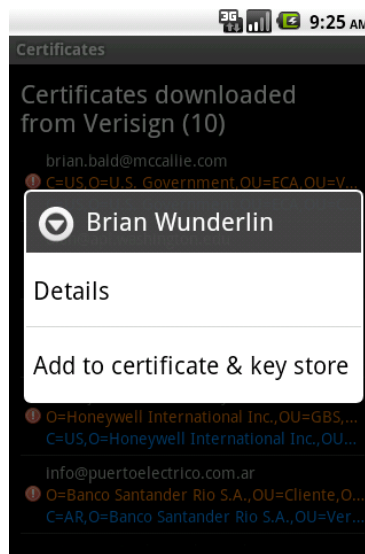


Figure 14: Add found certificate

7.2 LDAP servers

The list of registered LDAP servers can be viewed by selecting *Server settings* from the search certificates page (see figure 13). The LDAP servers page shows all the LDAP servers that will be queried (see figure 15).

7.2.1 Adding LDAP server

New LDAP servers can be added by selecting *Add LDAP server* from the menu (see figure 15). On the LDAP server settings page, the new LDAP settings can be set (see figure 16). The most relevant LDAP server settings will briefly be discussed.

Name Every LDAP server must have a unique name. The name is only used to identify the LDAP server.

Enabled If set, the LDAP server will be queried when searching for certificates.

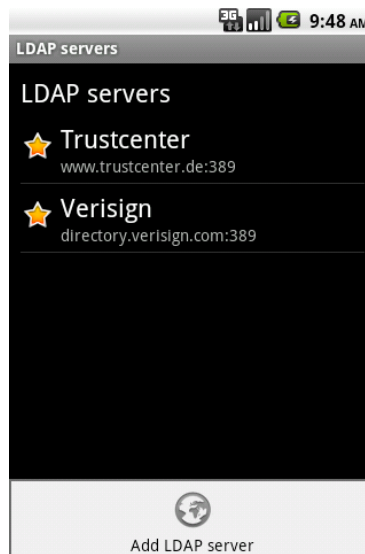


Figure 15: LDAP servers

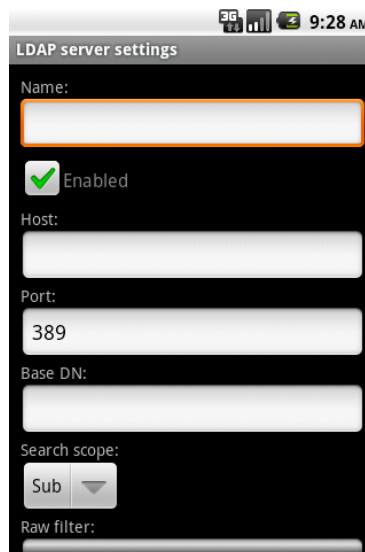


Figure 16: LDAP server settings

Host The hostname of the LDAP server. This should be a fully qualified domain name.

Port The port the LDAP server accepts connection on. The default LDAP port is 389 (for SSL/TLS it's 636).

Base DN The *Base DN* is the top level of the LDAP directory tree. The *Base DN* is different for every LDAP server. For example the *Base DN* for Trustcenter

is “dc=trustcenter,dc=de” and the *Base DN* for Verisign is “” (i.e. an empty value).

Search scope The search scope determines how the LDAP server will be searched. The required value depends on the LDAP server.

Raw filter The default LDAP query used to search for certificates is build-up as follows: cn=NAME,mail=EMAIL,o=ORGANIZATION (where *NAME*, *EMAIL* and *ORGANIZATION* are replaced with the actual value). This is suitable for most LDAP servers. Sometimes however a different LDAP query is required. A user configurable LDAP query can be specified with the *Raw filter* setting. The Name, Email and Organization parameters are provided as positional parameters.

Example The following LDAP query searches for LDAP entries with name equal to the given name: (&(givenName=%1\$s)

Use SSL If set, the LDAP query will be done via SSL/TLS.

Enable StartTLS If set, the LDAP query will support StartTLS.

Trust all certificates If the LDAP connection is established with SSL/TLS, the server certificate is checked and if the server certificate is not trusted, the connection is closed. To skip checking the server certificate, select *Trust all certificates*. This can for example be helpful when the LDAP server is using a self-signed certificate and the user is 100% certain that the LDAP server connection can be trusted.

Timeouts The *Time limit*, *Connect timeout* and *Response timeout* set the maximum times the LDAP server can take while handling the query.

Max message size The *Max message size* setting is a protective measure to protect DJIGZO for Android against very large LDAP server responses. If the LDAP server returns more data than the *Max message size*, the data is dropped.

8 Composing email

With the *Compose message* page, a new message can be created and sent. Before a message can be created, the following prerequisites are required:

- Account must be set.
- The SMTP host must be set
- The signing certificate must be set.

Note: If one of these requirements is not fulfilled, a warning will be shown.

On the *Compose message* page a message can be created and attachments added (see figure 17). The message can be saved as a draft or as a template (encrypted with your personal certificate) using the *Save draft* and *Save as template* menu items.

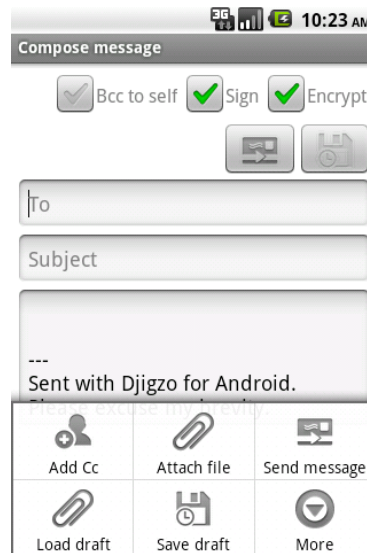


Figure 17: Compose message

8.1 Signing the message

When the *Sign* checkbox is checked, the message will be digitally signed with your signing certificate when the message is sent. Because signing a message requires access to a private key, the key store password must be provided when the password is not cached (see figure 18).

8.2 Encrypting the message

When the *Encrypt* checkbox is checked, the message will be encrypted with the certificates of the recipients. Only valid certificates with a matching email address (i.e., the certificate email address matches the recipients address), are used. The message will be encrypted with the users personal certificate (i.e., your signing certificate) to make sure the user is able to open the encrypted message.

If a certificate for a recipient cannot be found in the *Certificates & Keys* store, a warning message will be shown asking whether the LDAP servers should be searched for any certificates (see figure 19). If *Yes* is selected, the *Search certificates* page (see section 7) will be shown with a preconfigured email address.

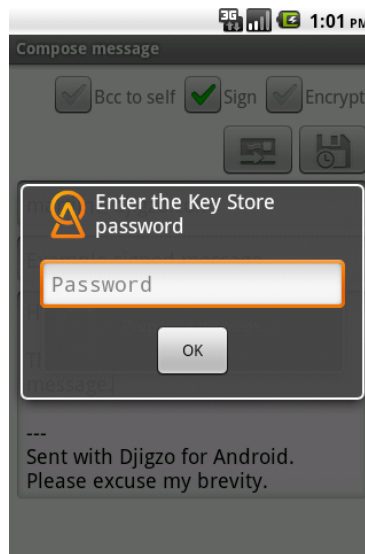


Figure 18: Key store password

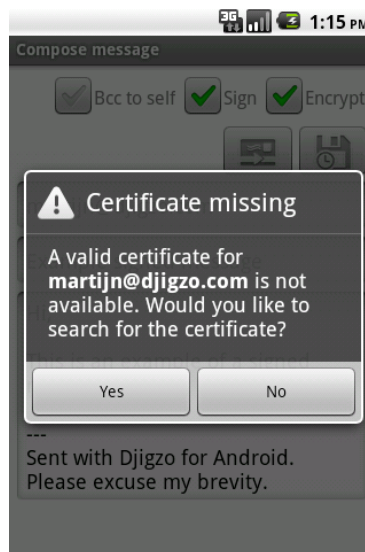


Figure 19: Missing certificate

8.3 Bcc to self

If the *Bcc to self* checkbox is checked, a blind copy (bcc) of the email will also be sent to the bcc email address (see Account settings for the Bcc email address).

Note: If DJIGZO for Android is used with Gmail and outgoing email is relayed via the Gmail SMTP servers, there is no need in sending a *Bcc to self* since Gmail stores all sent email in the *Sent* folder.

8.4 Attachments

Attachments can be added by selecting *Attach file*. A *File chooser* activity allows a file to be selected (see figure 20). The attachment can be removed or opened (see figure 21). When an attachment is opened, the available system handler for the attachment will be opened to view the attachment.

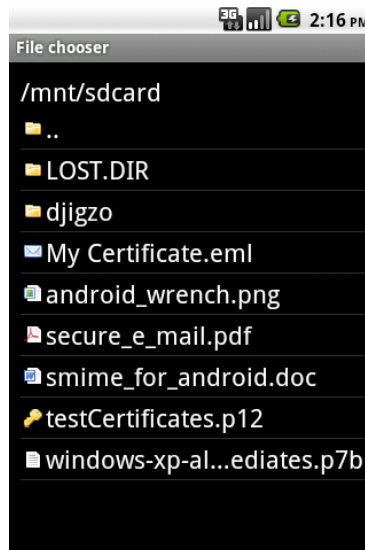


Figure 20: File chooser

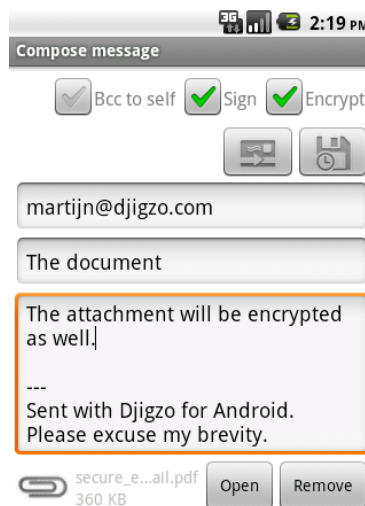


Figure 21: Attachment

8.5 Drafts & Templates

When a message is created but not yet finished, the message can be saved as a draft message and later be reopened using the *Load draft* menu option (see figure 17). When a draft message is reopened, the compose message fields are filled with the drafts's content and the draft message is removed from "disk".

If a message is saved as a template, the template can be reused again and again as the basis of an email message. A message can be saved as a template with the *Save as template* menu option and loaded with the *Load template* menu option.

8.6 Attach my certificate

With the *Attach my certificate* menu option, the personal certificate of the user will be attached to the message. This can be helpful when an external sender requires the certificate of the user for sending an encrypted email.

Note: A signed message will include the signing certificate. A signed message can be used as an alternative way of sending the personal certificate.

9 Opening email

DJIGZO for Android should be used in combination with an existing Android email client like for example the Google Gmail App or K9 email client since DJIGZO for Android does not contain a module that can retrieve email.

An S/MIME encrypted email in Gmail will be shown as a normal email with an *smime.p7m* attachment (see figure 22). The *smime.p7m* attachment contains the encrypted message. The encrypted message can be opened by clicking the *Preview* button. The encrypted message will be opened by DJIGZO and will be decrypted (see figure 23).

The headers of the message and meta information about the security properties of the message are shown at the top part of the message view (see figure 23). This message for example is encrypted with *3DES* and digitally signed with a valid and trusted signing certificate issued to the email address *test@example.com*.

If a message is signed but the signature is invalid, more detail why the signature is not valid is provided. For example the signature of the message shown in figure 24 is invalid because the message was signed with a certificate which was not authorized by the issuer to sign messages with.

9.1 S/MIME layers

An S/MIME protected message can be protected with multiple levels of protection. A message can be compressed, then signed, then encrypted and then signed again. The S/MIME layers view provides the details of every individual layer.

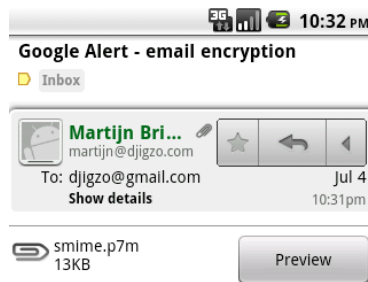


Figure 22: Encrypted email

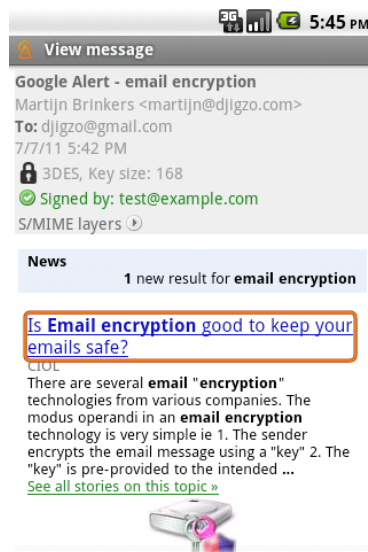


Figure 23: Decrypted email

Using a *long click* more detailed information about the layer can be viewed. By *long clicking* the signature layer, all signing certificates of the layer can be viewed and by *long clicking* the encryption layer, information about the encryption recipients (i.e., with which certificates the layer was encrypted) can be viewed (see figure 25).

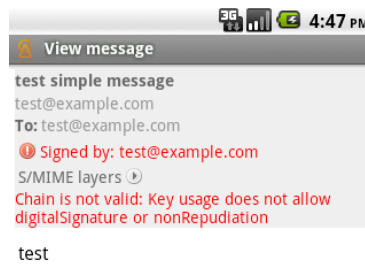


Figure 24: Invalid signature

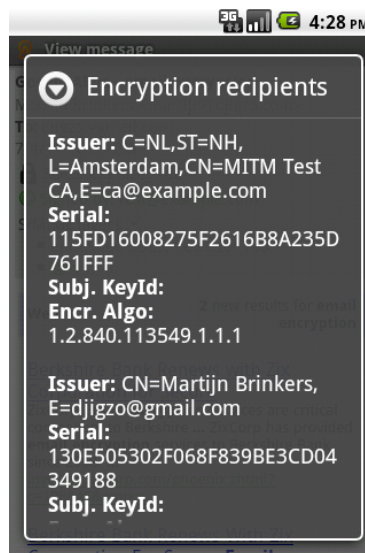


Figure 25: Encryption recipients

9.2 Menu options

The *View message* page contains options for replying, forwarding, switching between HTML and text etc. (see figure 26). Some of these menu options will be briefly discussed.

Toggle text/HTML Sometimes a message contains a text part and an alternative HTML part. By default the HTML part will be shown. With the *Toggle text/HTML* option, the user can switch between the text part and the HTML part.

Load external images If the message contains the HTML part and the HTML part is shown, the HTML might contain references to external images. By de-

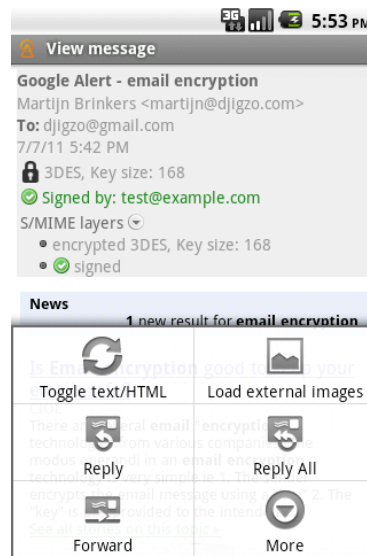


Figure 26: View message menu options

fault external images are not loaded. By clicking *Load external images*, the HTML is reloaded and if there are any external images, the external images are loaded and shown.

Warning: You should be warned that loading external images can expose your *IP* and email address since the external server can detect that an image has been downloaded. Also note that external images are not part of the signed content and it's therefore unclear what part of the message is signed and what part is not after external images have been downloaded.

Reply & Reply All With *Reply* and *Reply All* the *Compose message* page is opened with all the relevant fields preconfigured and the original text of the message added to the reply message.

Note: The original text of the message is only added if the message contains a text part.

Forward When a message is forwarded, the *Compose message* page is opened and the original message is attached as an RFC822 (also known as *eml*) attachment.

Toggle headers Sometimes the message contains hidden headers. By clicking *Toggle headers* all the available headers will be shown.

Note: Instead of clicking *Toggle headers*, the user can also click on the top part of the header section.

9.3 Importing certificates from email

Certificates attached to an email can be directly imported into the *Certificates & Keys* store. For example figure 27 shows a Gmail message containing a single certificate.

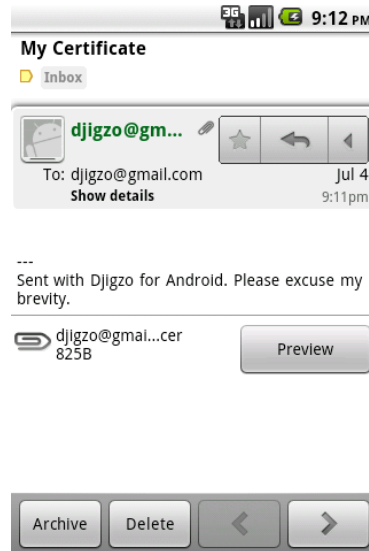


Figure 27: Attached certificate

By clicking the *Preview* button, the certificate can be directly imported into DJIGZO¹. If the imported certificate contains only a single certificate, the certificate import page will be opened (see figure 28). If the attachment contains multiple certificates (for example the attachment is a *.p7b* file) the general certificates import page will be opened (see figure 7).

9.4 Importing certificates from signatures

Due to technical reasons, DJIGZO cannot open the complete message if a message is *clear text* signed (for an example of a clear signed message see figure 29). The signature can therefore not be validated².

To be able to encrypt a message for a recipient, the certificate of the recipient is required. Since a digitally signed message contains the certificate of the signer, it might be helpful to import the certificates from the signature. The certificates from the digital signature can be imported by clicking the *Preview* button of the *smime.p7s* attachment. This will open the general certificates import page (see figure 7) with which the certificates can be extracted from the digital signature and imported.

¹The certificate will only be imported if the content-type of the certificate attachment is either *application/x-x509-ca-cert* or *application/x-x509-user-cert*

²the only workaround is to download the message source and open the message with the *Open message* option

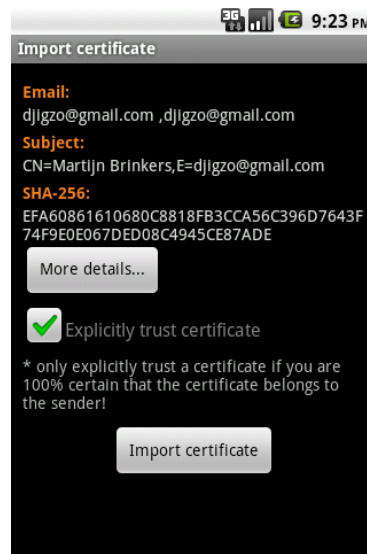


Figure 28: Certificate import

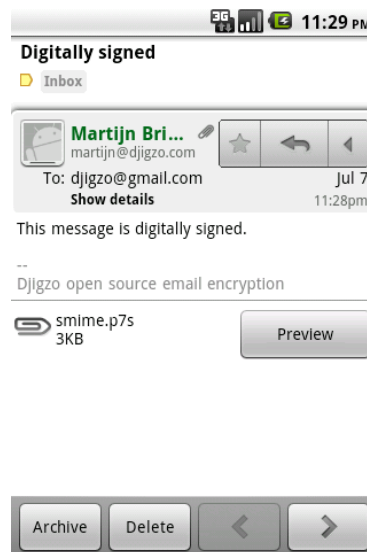


Figure 29: Clear signed message

9.5 Importing .pfx files from email

When a password protected .pfx file (containing private keys) is attached to a message, the .pfx file can be imported into DJIGZO by clicking *Preview* of the .pfx attachment. The *Import keys* page (see figure 6) can be used to import the .pfx file.

10 Settings

The settings page contains links to specific setting pages (see figure 30). All the individual settings pages will be discussed.



Figure 30: Settings

10.1 Account

The *Account settings* page specifies all the settings for the sender (see figure 31).

Sender The sender email address (i.e., the *From* of the message). This should be a valid email address.

Sign The default value of the *Sign* checkbox of the *Compose message* page. If checked, the *Sign* checkbox will be checked by default when the *Compose message* page is opened.

Encrypt The default value of the *Encrypt* checkbox of the *Compose message* page. If checked, the *Encrypt* checkbox will be checked by default when the *Compose message* page is opened.

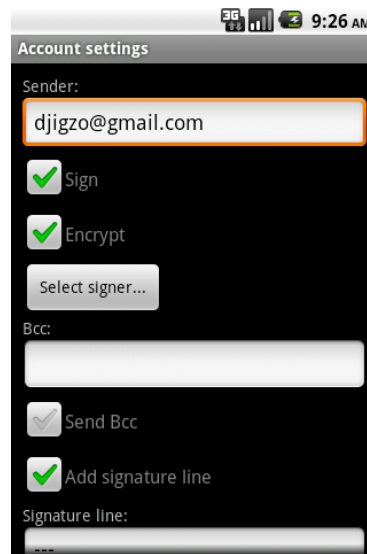


Figure 31: Account settings

Select signer... The *Select signer...* button opens the page on which you can select the signing certificate. The currently selected signing certificate is shown with a selected radio button on the right hand side of the page (see figure 32). In most cases there will only be one signing certificate.

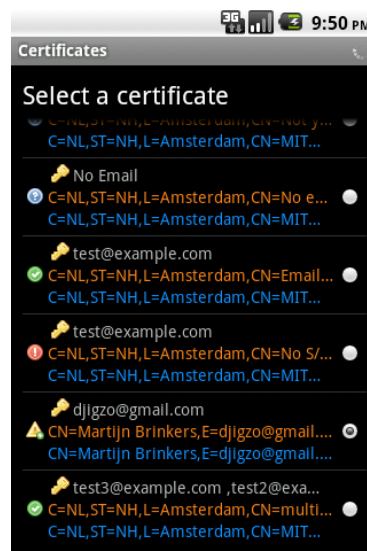


Figure 32: Signing certificate selection

Note: It is important that the selected signing certificate is a valid certificate.

Send Bcc The default value of the *Bcc to self* checkbox of the *Compose message* page. If checked, the *Bcc to self* checkbox will be checked by default when the *Compose message* page is opened.

Add signature line If checked, the signature will be added to the message when composing a new message.

10.2 SMTP

The *SMTP settings* are used to setup the outgoing SMTP connection settings (see figure 33).

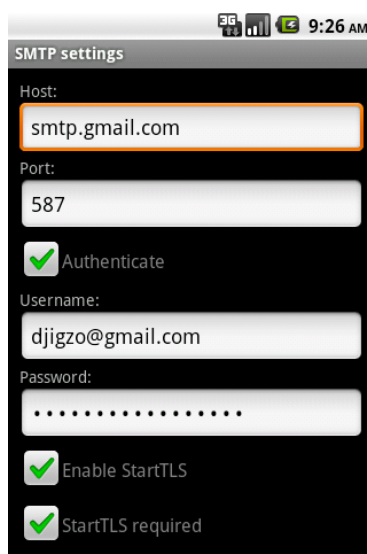


Figure 33: SMTP settings

Host The outgoing SMTP server host. This should be a fully qualified domain name.

Port The outgoing SMTP server port. This should be a number between 1 and 65535.

Authenticate If checked, the outgoing connection will use authentication.

Username The username to use for authentication.

Password The password to use for authentication.

Enable StartTLS If checked, StartTLS will be issued if the SMTP server supports it.

StartTLS required If checked, the SMTP connection will only be established if the SMTP server supports StartTLS.

Enable SSL/TLS if checked, the SMTP connection will be setup with SSL/TLS.

Skip SSL trust check If checked, the SMTP server certificate will not be checked, i.e., all server certificates will be accepted.

Note: Only enable *Skip SSL trust check* if it's impossible to create a trusted SSL/TLS connection and if you are 100% certain the the SMTP connection can be trusted.

10.3 S/MIME

The S/MIME algorithms and key strengths for digital signing and encryption can be set on the *S/MIME settings* page (see figure 34).

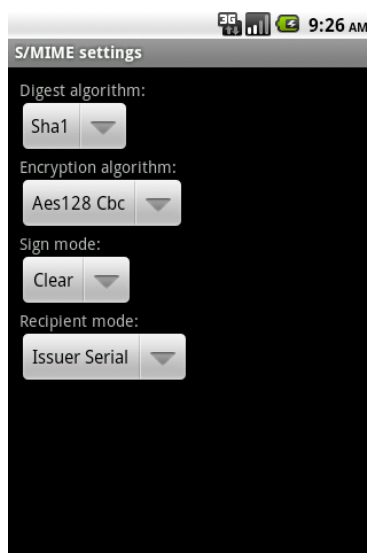


Figure 34: S/MIME settings

Digest algorithm The *Digest algorithm* specifies which hashing algorithm should be used for digital signing of messages.

Encryption algorithm The *Encryption algorithm* specifies which encryption algorithm and key strength should be used for encryption.

Sign mode A message can be *clear text* signed and *opaque* signed. With *clear text* signing, the message can be read even when the recipient does not use an S/MIME capable email client. With *opaque* signing, the signed message is encoded. The recipient therefore requires an email client capable of reading S/MIME email. It's advised to use *clear text* signing.

Recipient mode The recipient mode determines what method should be used to identify the encryption recipient. It's advised to use *Issuer serial* mode.

10.4 Key Store

The *Key Store* settings are shown in figure 35.

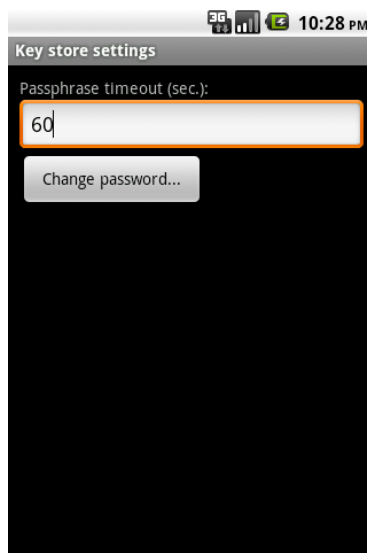


Figure 35: Key Store settings

Passphrase timeout The number of seconds the key store password is cached. If the *Passphrase timeout* is changed by the user, the key store password must be entered before the timeout will be changed.

Change password... The key store password can be changed by clicking *Change password...*. When setting a new password, the old password must be provided (see figure 36).

Note: The private keys are protected with a secure randomly generated password. This randomly generated password is encrypted with the Key Store password. Changing the Key Store password only changes the password with which the randomly generated password is encrypted.

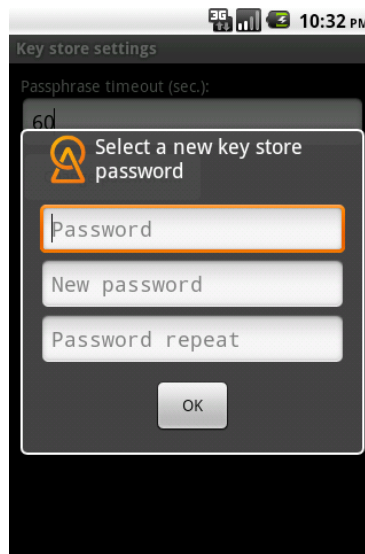


Figure 36: Change Key Store password

10.5 CRL

The *CRL* settings are shown in figure 37.

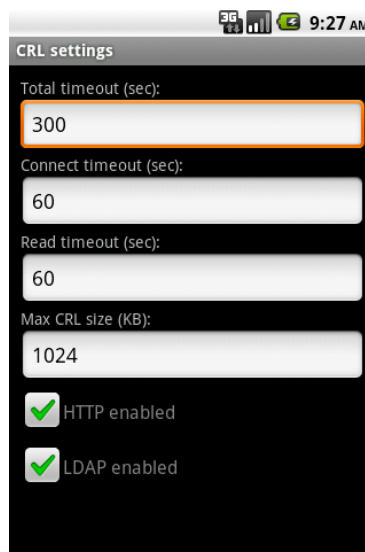


Figure 37: CRL settings

Timeouts The *Timeout* settings set a limit on the maximum time a CRL download may take.

Max CRL size Sometimes CRLs can be very large in size, often too large to be handled by an Android application. If a CRL is larger than the max CRL size, the CRL is skipped.

HTTP enabled If checked, the CRL downloader will support downloading CRLs via HTTP(S).

LDAP enabled If checked, the CRL downloader will support downloading CRLs via LDAP(S).

10.6 LDAP servers

The settings for the registered LDAP servers. See section 7.2 for more information.

10.7 General

The *General settings* are shown in figure 38.

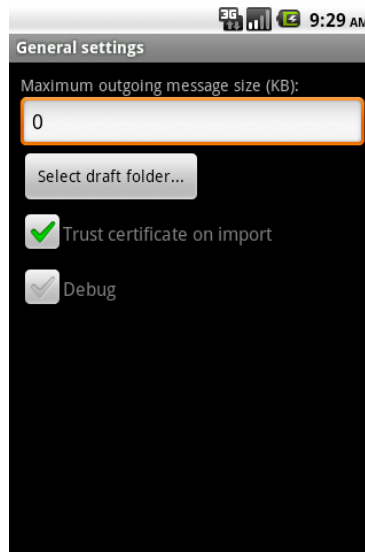


Figure 38: General settings

Maximum outgoing message size If an outgoing message exceeds the *Maximum outgoing message size* setting (in KB), the message will not be sent. The default value 0 means that there is no limit.

Select draft folder... The default folder in which drafts and templates will be stored can be set by clicking *Select draft folder...*

Trust certificate in import When a single certificate is imported, the import activity can automatically trust the certificate. The certificate should only be explicitly trusted if the receiver knows with 100% certainty that the certificate belongs to the sender. Whether or not the *Explicitly trust certificate* is checked by default is determined by the setting *Trust certificate on import*. To make it less likely that the user explicitly trusts the certificate on import, uncheck the *Trust certificate on import* setting.

Debug If checked, detailed debugging information will be written to the Android log file.