S/MIME on Good for Enterprise Client for Android

Release Notes

Updated: April 20, 2012

These notes apply to the use of S/MIME with Good for Enterprise Android Client 1.8.2.

The Client is available for download from Get.good.com/smime. It is not available on the Android Market.

Note: Upgrades from previous Client versions are not supported. Users must delete any previous Client from the device before installing this version.

Good software versions supported:

- Good Mobile Messaging (GMM Exchange) 6.4.0 and above
- Good Mobile Control (GMC) 1.3.5 and above
- Good Android Client 1.8.2

Requirements:

- Good Mobile Messaging Servers: Microsoft Exchange 2003, 2007, 2010
- Tested with Outlook 2003, 2007, 2010, together with Thunderbird client
- Certificate Authorities Supported: Entrust, Dogtag, GlobalSign, CyberTrust, Microsoft, and Verisign
- Digital Certificate Formats Supported: PKCS 12 (.p12 and .pfx)
- OCSP Responders Supported: Microsoft OCSP Responder
- Tested for soft token

Features not support in this release:

- Searching personal contacts for Recipient's public certificate
- Html support for reading S/MIME messages
- Support for reading attachments from signed email on a device that is not enabled for SMIME
- Support for mismatch of email address on certificate (e.g., certificate has John@visto.com and Outlook has John@good.com)

Usage Notes

To set up S/MIME use, do the following:

1. Go to the Settings tab and select Secure Messaging (S/MIME).

   Select the LDAP or GAL radio button to specify where the user certificates are located. If you select LDAP, fill in the location of the LDAP Certificate Authorities Directory URL, the User Certificate Directory URL, and the OCSP Responder URL. If you select GAL, enter the OCSP Responder.

2. Enable an S/MIME policy for the desired devices using Good Mobile Control Console (GMC):
   a. Log in to GMC and navigate to the policy to be used, or create a new policy.
   b. Select "Handheld Authentication" and enable SMIME by selecting radio button "S/MIME with password-protected lock screen or CAC PIN (Enables S/MIME)" in "Handheld Authentication Type"

c. From the S/MIME options displayed when the radio button is selected, choose “Authenticate with password” (the default).

d. Set the Digitally sign and Encrypt options as desired.

e. Save the policy.

3. Assign users to the S/MIME policy.
4. Add “Upload S/MIME certificate” responsibility to the Self Service role; assign the users the Self Service role in GMC. Instruct the users to log into GMC Self Service and upload (from GMC to device) one or two S/MIME certificates for signing and encryption.

   Going forward, new users added to the policy will need to upload a certificate via Self Service.

Open Issues for GFE Android Client

Note: Issues that have been resolved in this release are indicated by strikethrough text.

Issue	Tracker
If a non-SMIME client receives a signed email, the files in any zip attachment <8k in size cannot be listed and downloaded.	89142
Cannot send encrypted email without certificate installed.	95693
Sent SMIME emails cannot be verified or decrypted in Sent Items folder.	96129
App hangs when trying to forward a signed email containing attachments, without downloading the attachments first.	96408
Cannot forward normal email as SMIME after removing non-downloaded attachments	96548
The Client does not respond when the user tries to reply to or forward a signed email without downloading the entire message first (verifying the email on the device).	