

S/MIME on Good for Enterprise Client for iOS

Release Notes

Updated: March 29, 2012

Usage Notes	1
Open Issues for GFE iOS Client	2

These notes apply to the use of S/MIME with Good for Enterprise iOS Client 1.9.8 and above.

Good software versions supported:

- Good Mobile Messaging (GMM) 6.3.1 and above
- Good Mobile Control (GMC) 1.3.1 and above
- Good iOS Client 1.9.8 and above

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, and Verisign
- Digital Certificate Formats Supported: PKCS 12 (.p12 and .pfx)
- OCSP Responders Supported: Microsoft OCSP Responder
- Tested with iOS 4.0 and higher, iPad and iPhone
- Tested for soft token

Usage Notes

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

1. 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.
2. 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.
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 iOS Client

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

Issue	Tracker
Reading emails in HTML format is not supported in this release.	
If S/MIME is not enabled on the device, any attachments on signed emails will not be delivered.	
If the user excludes public certificates in signing messages, Verify Signature on HH will fail and the user will not be able to reply or forward the messages.	90875
Attachments added to a forwarded S/MIME HTML email from the iOS Client will not appear in the attachment list when received by the iOS Client on another device. The user can view the attachments on Outlook or any desktop email client.	94514