X509 EMAIL ENCRYPTION

White paper

Introduction

Most email is sent as plain text. This means that anyone who can intercept email messages, either in transit or at rest, can read the content. Today, companies and governments realize that this is unacceptable. Email needs to be confidential, email needs to be encrypted.

Our email encryption products will secure your email and protect messages against unauthorized access, both in transit and at rest.

The X509 Secure Mail Gateway (SMG) is a standards based centrally managed email server (MTA) that encrypts and decrypts your incoming and outgoing email at the gateway level. The SMG is compatible with any existing email infrastructure like Microsoft Exchange and Lotus Notes and has support for S/MIME, OpenPGP PDF encryption as well as supporting secure webmail. The built-in Data Leak Prevention (DLP) module can be used to prevent certain information to leave the organization via email.

The SMG can be installed on most Linux and UNIX based systems. Installation packages are available for Ubuntu/Debian, Red Hat/CentOS and OpenSUSE. A ready to run virtual appliance for VMware and Hyper-V is also available.

X509 for BlackBerry® is an add-on to the X509 SMG which can be used to send and receive S/MIME digitally signed and encrypted email from a BlackBerry® smartphone.

X509 for Android is an Android application which can be used with your existing Android mail application to send and receive S/MIME digitally signed and encrypted email with an Android smartphone. X509 for Android can be used to encrypt all email on an Android smartphone.

X509 Secure Mail Gateway

The SMG is a centrally managed email server (MTA) which encrypts and decrypts your incoming and outgoing email. Because the SMG functions as a general SMTP email server, it is compatible with any existing email infrastructure and can easily be placed before or after existing email servers. The SMG is typically installed as a “store and forward” server. Email is therefore only temporarily stored until it is forwarded to its’ final destination.

“The SMG is compatible with any existing email infrastructure like Microsoft Exchange and Lotus Domino”

The SMG currently supports three encryption standards: S/MIME, OpenPGP and PDF encryption. S/MIME and OpenPGP provide authentication, message integrity and non-repudiation and protection against message interception. S/MIME and OpenPGP use public key encryption (PKI) for encryption and signing. Email that is encrypted and/or digitally signed by the SMG can be read in Outlook, Thunderbird and other mail clients, provided the user has the proper email certificates installed.

Despite the fact that products like the SMG makes S/MIME and OpenPGP fairly easy to use, some recipients might find S/MIME or PGP encryption too cumbersome. Especially when you only need to exchange secure email once, or a few times over a longer period, installing an S/MIME certificate or PGP key might be more problematic than it’s worth. To accommodate for those situations, we have included a PDF encryption module in the SMG. You can configure the SMG to automatically convert outgoing email, including all attachments, to a password encrypted PDF document using standard PDF encryption techniques.

Various password modes are supported:

a) Encrypt with a pre-defined static password;
b) Encrypt with a randomly generated password which is then sent by SMS Text to the recipient;
c) Encrypt with a randomly generated password which is then sent back to the sender by email; or
d) Encrypt with a password generated using a One Time Password (OTP) algorithm.

By using a separate channel for sending passwords, PDF encryption is almost as secure as full S/MIME or PGP encryption, provided that the password is long enough to withstand a brute force attack. PDF encryption in the SMG is intuitive and easy. There is no need to specifically instruct end-users.

The SMG is compatible with any existing CA server (like EJBCA or Microsoft CA) Authorities (CAs) like Verisign, Comodo and CACert. Alternatively, the SMG contains a basic CA server which allows you to create certificates for internal and external users. Certificates can be transported to external recipients in a password protected format. The password can be automatically generated and provided to the recipient as an SMS Text message. Installation of the certificate in the recipients' mail client is straightforward. This allows you to setup your own private PKI with external recipients.

General features

- Web based interface.
- Supports virtually unlimited number of users and certificates.
- Sender notification after email encryption.
- Settings can be specified at gateway, domain and user level.
- Automatic backup to remote shares at set intervals.
- Separate back-(encryption engine) and front-end (SOAP API).
- Java, Spring based. Services can be easily replaced and/or extended.
- AGPLv3 licensed (for closed source license or OEM please contact us).
- Packages available for Ubuntu, Debian, RedHat/Centos.
- Ready-to-run Virtual Appliance for VMware ESX/ESXi/Workstation/Player and Hyper-V available.
- TAR distribution available for other systems that support Java and Postfix.

S/MIME features

- S/MIME 3.1 (X.509, RFC 3280).
- Built-in CA which can be used to securely issue certificates for internal and external users.
- Automatic and manual certificate selection.
- Domain certificates (encryption to domains with just one certificate).
- Certificates are automatically extracted from incoming email.
- Support for multiple certificates per sender/recipient.
- Validation of signed email.
- Certificate revocation lists (CRLs) are automatically downloaded (LDAP and HTTP).
- Certificate trust lists (CTLs) can be used to black or white-list certificates.
- Compatible with existing S/MIME implementations (Outlook, Lotus Notes, Thunderbird etc.).
- S/MIME support for Blackberry BIS users with Blackberry add-on.
- Optional support for Hardware Security Modules (HSM).
- Integrates with EJBCA and Comodo EPKI.

OpenPGP features

- OpenPGP RFC 4880.
- PGP/INLINE and PGP/MIME (RFC 3156).
- Secret keys can be generated and revoked.
- Keys can be downloaded and uploaded to remote key servers (HKP).
- Domain keys (encryption to certain domains with a domain key).
- Keys can be automatically extracted from incoming email.
- Validation of signed email.
- Optional support for Hardware Security Modules (HSM).

PDF email encryption features

- Email is automatically converted to an encrypted PDF (including all attachments).
- PDF is encrypted with AES-128.
- PDF passwords can be automatically generated.
- PDF passwords can be sent by SMS, generated using a One Time Password algorithm, or sent back to sender.
- The recipient can reply using the built-in secure portal.

DLP features

- Outgoing email can be scanned on keywords and regular expressions.
- Keywords and regular expressions can be specified at gateway, domain and user level.
- Messages can be blocked or quarantined when a rule is violated.
- Email encryption can be forced when a rule matches.
- DLP managers will be notified when a rule is violated.
- DLP managers can release quarantined email.
- If allowed, users can manage their own quarantined email.
- Email bodies, attachments and nested attachments of type text, html, xml and other text-based formats are supported (support for pdf, doc, xls, zip etc. will be added to future versions of the SMG).

X509 SMG with content/virus scanner

Most organizations need to scan all incoming and outgoing email for viruses. A typical setup of an encryption gateway and a virus scanner can be seen in figure 1.

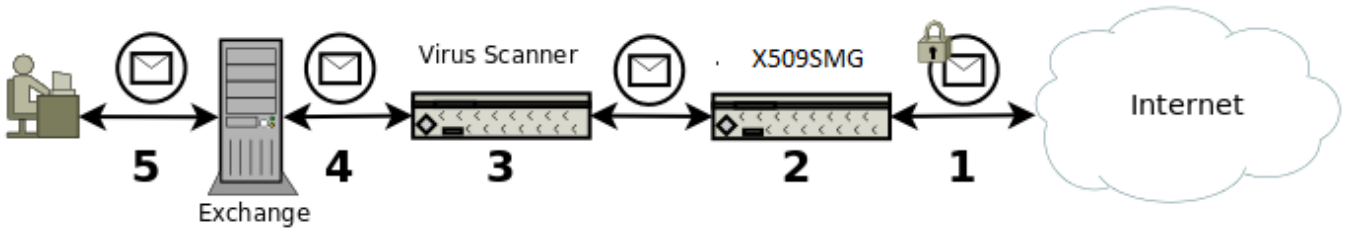

Figure 1: Virus scanning

X509 SMG with virus scanning:

1. S/MIME encrypted message is received from the Internet.
2. X509 SMG gateway decrypts the message.
3. The decrypted message is scanned for viruses.
4. After virus scanning the message is forwarded to Exchange.
5. User reads the message.

A more advanced setup is required when email must be encrypted on the desktop yet all outgoing email must be virus scanned because of corporate policies.

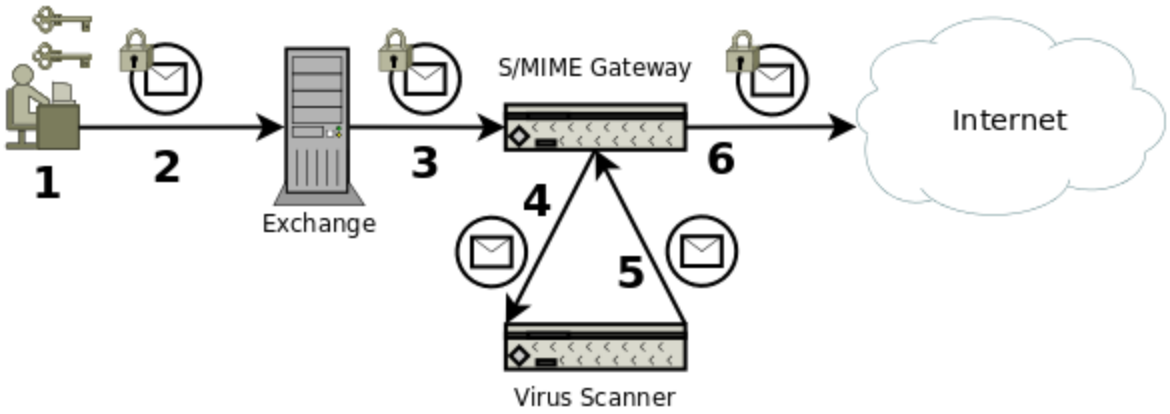

Figure 2: Virus scanning with desktop encryption

X509 SMG with desktop encryption and virus scanning:

1. User encrypts message.
2. S/MIME encrypted message is sent to Exchange.
3. Exchange sends S/MIME encrypted message to the X509 SMG.
4. The X509 SMG decrypts the message with the senders' private key (the gateway stores a copy of the key) and sends the decrypted message to the virus scanner.
5. Virus scanner scans the message and if clean it will be sent back to the SMG.
6. The SMG re-encrypts the message and sends the message to the external recipient.

S/MIME

S/MIME is based on Public Key Infrastructure (PKI) and uses X.509 certificates. Public Key Infrastructure is a technology which can be used to securely exchange information over insecure networks using public key cryptography. PKI uses X.509 certificates to bind a public key to an identity. The main advantage of PKI is that there is no need to directly trust everyone involved because trust can be inferred.

"S/MIME is supported by most email clients."

S/MIME uses a hierarchical trust model. Most email clients, like Outlook and Lotus Notes, support S/MIME out of the box. If required, the X509 SMG will automatically select the correct certificates for signing and encryption based on strict PKI rules. Only certificates that are valid (i.e., trusted, not expired, not revoked) are automatically used (see figure 3)

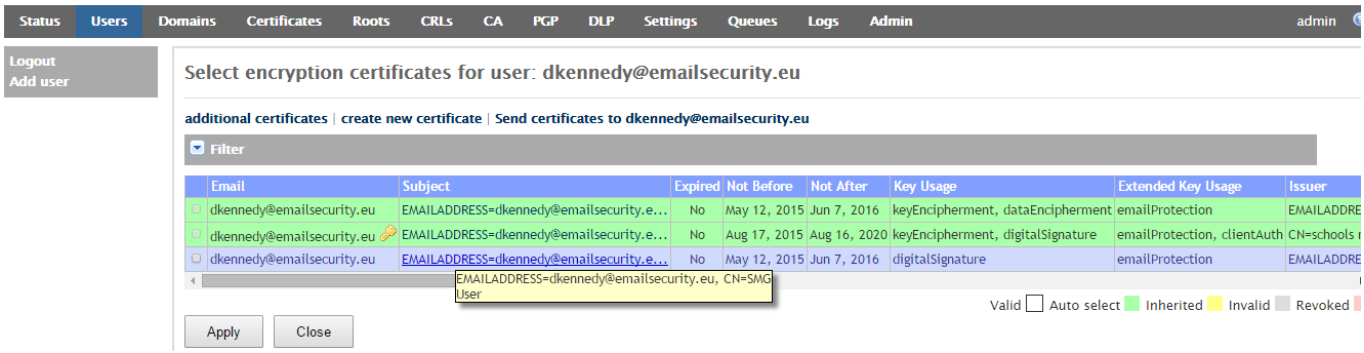

Figure 3: Select encryption certificates

PDF encryption

PDF encryption can be used as a light-weight alternative to S/MIME encryption. PDF allows you to decrypt and read encrypted PDF documents. The basic idea of the X509s' PDF email encryption is that the complete message, including all attachments, sent by a user is converted to a password encrypted PDF document (encrypted with AES-128). A standard message, with the encrypted PDF attached, is then sent to the recipient. The recipient can open the PDF by entering the password.

Various password modes are supported:

a) Encrypt with a pre-defined static password;
b) Encrypt with a randomly generated password which is then sent by SMS Text to the recipient;
c) Encrypt with a randomly generated password which is then sent back to the sender by email; or,
d) Encrypt with a password generated using a One Time Password (OTP) algorithm.

"PDF encryption in the SMG is intuitive and easy. There's no need to specifically instruct end-users."

A PDF encrypted message looks similar to figure 4. All email clients, including webmail like Gmail, Hotmail etc. are supported. The message contains a general message which is based on a configurable template. The encrypted PDF is attached to the message. The PDF can be opened with any PDF reader.

Figure 4: Message with encrypted PDF

After decryption, the PDF will be opened by the default PDF reader. The PDF will be shown as an email message. All attachments can be accessed from the attachment pane (see figure 5). The recipient can securely reply to the encrypted PDF by clicking the reply link in the PDF.

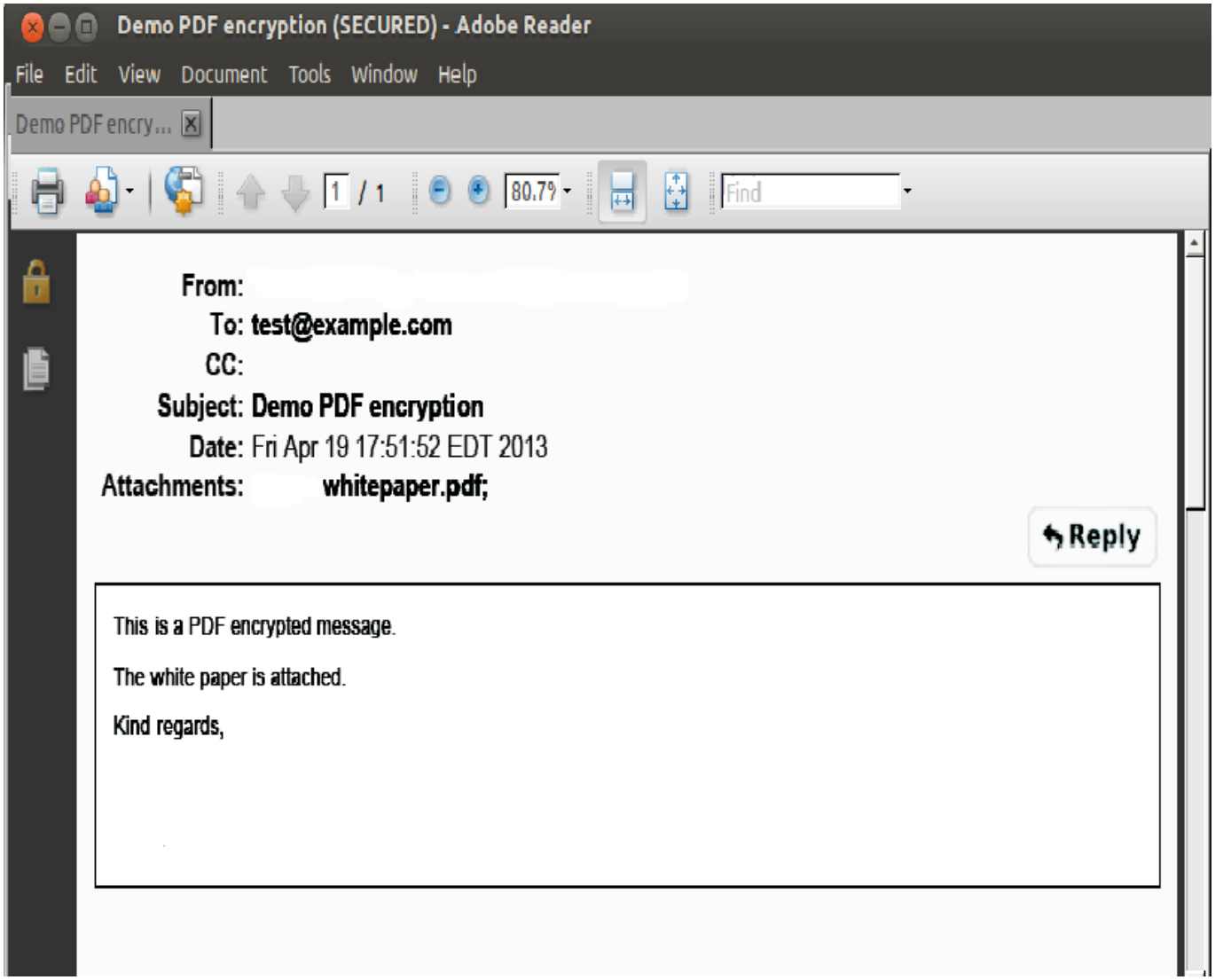

Figure 5: PDF decrypted message. Attachments can be opened from the attachment panel

Data Leak Prevention

Data Leak Prevention (DLP) is a feature that prevents certain information to leave the organisation via email. What information this is, is defined in the configuration of the DLP system. Typically, it includes credit card numbers, bank account numbers, excessive amounts of email addresses or other personal information in one email message, etc. DLP is implemented as a filter on outgoing email. DLP can be a separate system or product, or it can be integrated with another email related product or system. X509 has integrated DLP into the SMG.

DLP can monitor email at various levels:

- email body content
- email headers
- email attachments of various types
- nested attachments of various types

X509s' DLP currently filters email bodies, attachments and nested attachments of type text, html, xml and other text-based formats. Filtering attachments of type pdf, doc, xls etc. will be part of a future offering of X09s' DLP.

Configuring DLP is done via the SMG Web GUI. You can specify keywords and sentences that outgoing email messages should not contain. More elaborate filtering is achieved via regular expressions, a specification format that allows you to specify virtually any combination of characters, words or sentences that should be filtered. Sample regular expression configuration files can be downloaded from our web site.

DLP can be configured on three levels, similar to how encryption is configured: at gateway level, at domain level and at individual user level. The latter is useful in specific cases where some users can send out information via email that other users cannot.

If a policy is violated, the gateway can send a notification message to the sender of the message and/or to the DLP managers. If a message has been quarantined and the sender or one the DLP managers clicks on the link from the quarantine notification message, the quarantine email information page will be opened in the web browser (see figure 6). Depending on the authorizations of the sender, the sender can download, release or delete the quarantined message.

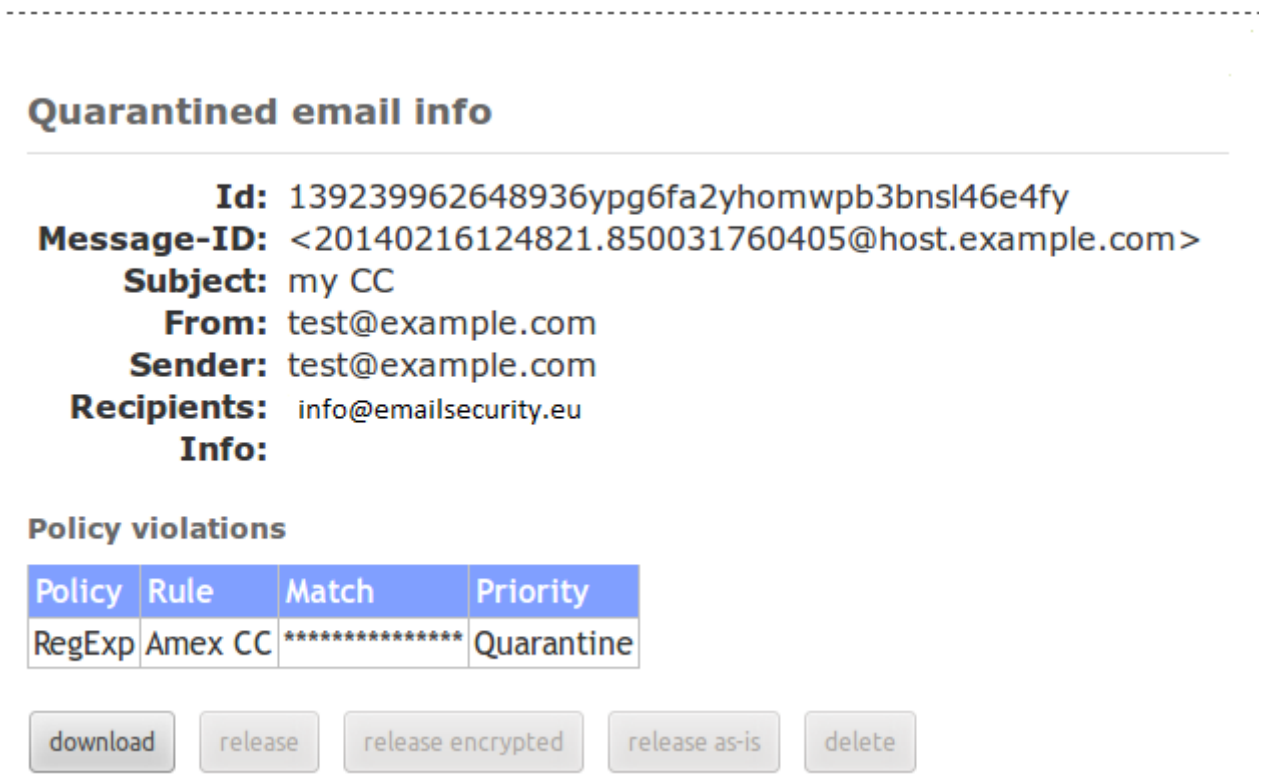

Figure 6: Quarantined email

X509 for BlackBerry

The BlackBerry® smartphone is the most secure generally available smartphone on the market. All communication between a BlackBerry Enterprise Server (BES) and a BlackBerry smartphone is encrypted with 3DES or AES.
For added security the S/MIME support package can be installed allowing email to be digitally signed and encrypted using digital certificates. BlackBerry Internet Service (BIS) users however, do not have the same level of protection that BES users have.

“With X509 for BlackBerry, all email on the BlackBerry is S/MIME encrypted.”

Even though all communication between the carriers BIS and a BlackBerry smartphone is encrypted, data from the carriers BIS to the Internet is not. Email sent to and from a BlackBerry smartphone goes without any protection and can potentially be intercepted and/or modified by any intermediate gateway. It is unfortunate that even though the BlackBerry smartphone has built-in functionality to handle S/MIME encrypted email, the S/MIME support package is not supported by BIS.

X509 for BlackBerry is an add-on to the SMG which can be used to send and receive S/MIME digitally signed and encrypted email from a BlackBerry smartphone. X09 for BlackBerry is used in combination with the X509 SMG Email X509 for BlackBerry integrates with the built-in BlackBerry mail application.

Features

- S/MIME encryption and digital signing using X.509 certificates.
- Compatible with BIS.
- Is compatible with existing S/MIME clients (like Outlook and Lotus Notes).
- Message body and attachments are encrypted.
- HTML email support.
- Uses BlackBerry encryption functionality (3DES, AES, X.509, S/MIME).
- Uses the BlackBerry built-in key and certificate store.
- Is compatible with the BlackBerry smart card reader.
- Encrypted messages sent from BlackBerry smartphone are securely relayed by the X509 SMG via an encrypted S/MIME tunnel.
- Because email is relayed by the SMG, email sent from the BlackBerry can be easily archived using any existing email archiving functionality.
- Messages are stored on the BlackBerry smartphone in encrypted form.
- Because email is relayed by the SMG, all email originates from the companies IP range. This is especially useful when the companies’ domains have SPF records setup.

X509 for Android

X509 for Android is an Android application which can be used with your existing Android mail application to send and receive S/MIME digitally signed and encrypted email with an Android smartphone. X509 for Android can be used to encrypt all email on an Android smartphone.

"X509 for Android can be used to encrypt all Gmail email."

Features: X509 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".

Contact information

info@emailsecurity.com
Enniscorthy Enterprise & Technology Centre, Milehouse Road, Enniscorthy, Co. Wexford. Ireland
T: +353 53 910 5050 **M**: +353 862 555 555