S/MIME Compatibility

Assessing the compatibility and best practices of using S/MIME encryption

GLOBALSIGN WHITE PAPER

Ben Lightowler, Security Analyst
GMO GlobalSign Ltd

www.globalsign.com

Contents

INTRODUCTION

Many organizations, both large and small, face difficult choices when considering secure data transfer between stakeholder groups. Virtual teams made up of internal colleagues, outside partners and even potential clients find a need to collaborate effectively and securely, requiring cost effective ways to authenticate the integrity of data they receive but also the need to maintain confidentiality. This is especially true with data transmission systems using the open Internet to relay e-mail and storage being so freely available in the "cloud" to collaborate (Google Docs, Dropbox etc). Now more than ever, data protection is one of the biggest concerns for CISOs and heads of security with solutions needed to cover the encryption of data either at rest or during transmission to other parties. Within this white paper we will be highlighting the use of S/MIME certificates as a solution; providing a way to maintain confidentiality, as well as proving the integrity and origin of emails and their authors.

Although there has never been a want or a desire for sensitive information to be exposed many organizations risk exposure by using insecure channels to transmit data. Password protecting ZIP files still requires the secure transfer of the password and the ever-present problem of accidentally forgetting to protect a ZIP file prior to transmission. In recent times the need to encrypt sensitive information including the e-mail text content itself has grown in prominence. As the world moves data storage and communications to the 'cloud' and assets become available 'remotely' extra dimensions are added to the threat model. However, this new added convenience need not require a compromise in security. Provided that the correct standard of encryption has been implemented, even if data has been intercepted, it cannot be exposed modified or manipulated.

S/MIME or Secure/Multipurpose Internet Mail Extensions is the industry standard for public key encryption for MIME based data. S/MIME Encryption provides Message integrity, authentication, privacy via data encryption and non-repudiation via digital signatures. S/MIME is a standard tracked by IETF and now defined by several RFC's 3851, 3850, 3370, and 3369. S/MIME works by using a data envelope to surround the data entity which is inserted into a PKCS7 MIME Entity (when encrypting).

WHY S/MIME CERTIFICATES?

- **Prevent tampering of email content**
- **Prove message origin**
- **Prevent exposure of email content**
- **Flexible & secure communication**

S/MIME COMPATIBILITY

The S/MIME protocol occupies an ever-evolving space in the communications spectrum. Over time it has proven to be robust enough to cope with an array of different environment preferences and requirements. It is for this reason that browser based web client implementations as well as desktop and server implementations must be able to work with each other in this regard. This is where; to a certain extent the system can develop a few pitfalls as it's not always possible to meet future needs and past desires with the same settings.

Due to the timeframes involved in product development and mismatched release cycles between different vendors, there appears to be no universal standard; Best practice at the time often moves the goal posts with increased security sometimes being achieved at the expense of maximum compatibility. Algorithms used for digital signatures, for example hashing, have moved forward in recent years (from MD5 to SHA1 and now onwards towards adoption of the SHA2 family). In much the same way the RSA asymmetric key length necessary for signing has moved from 1024 to 2048 bit. Encryption too has now moved away from triple DES (3DES) to various strengths of AES (The Advanced Encryption Standard). Unfortunately in the case of unmodified email clients of different ages this can cause frustration where authors and recipients are unable to decrypt messages.

A comprehensive summary into these issues can be seen in the Fig 1 at the end of this paper with conclusions offering a choice.

One concern is that the value of email encryption seems to have been greatly underestimated, especially with so many recent high profile attacks against e-mail service providers. Personal users with concerns over privacy and

corporate users with concerns over confidentiality need to realise that using the Internet as the transport mechanism for e-mail is equivalent to sending a postcard by snail mail. In the case of the postcard anyone involved in the delivery chain is able to intercept and read the content – at the sorting office and right up to the letterbox itself. Given that it's obvious never to send a postcard with confidential details in plain text, why should an email be any different? Malicious users can monitor e-mails quite freely and the authors are none the wiser.

Best Practices

Research into the strengths and weakness of S/MIME compatible email clients has yielded certain recommendations of best practices when using certain applications.

Encryption Strength vs. Compatibility

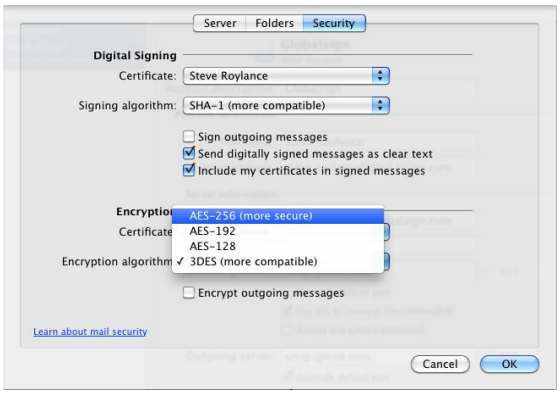
For almost all Mail Clients users have the option to set both the signing algorithm and the encryption algorithm. When selecting signing algorithms it can be temptation to utilise the strongest algorithm available at the time. In the case of Outlook 2010 this would be SHA-256 up to SHA-512. Whilst this might be reassuring, the negative implications on compatibility can greatly outweigh the benefits of the stronger encryption as highlighted in fig 1. Whilst options of algorithms are more limited in legacy versions, this does mean they are insecure. The signing algorithm SHA-1 (recommended below) is currently striking the best balance between ubiquitous compatibility and hash algorithm strength.

The other option available to most mail client users is the encrypting algorithm. In this case it is the recommendation of this author to use the strongest where possible. It was during the research that produced that table below, see fig 1, that the strongest encryption possible was almost always used; 3DES in the case of legacy clients and AES-256 for more modern mail clients. This is not to say that the encryption algorithms available to older mail clients is sub-standard, users should not feel paranoid or insecure when utilising the 3DES algorithm as their strongest encryption algorithm option. This option is just as viable in a situation where certain compatibility is called for.

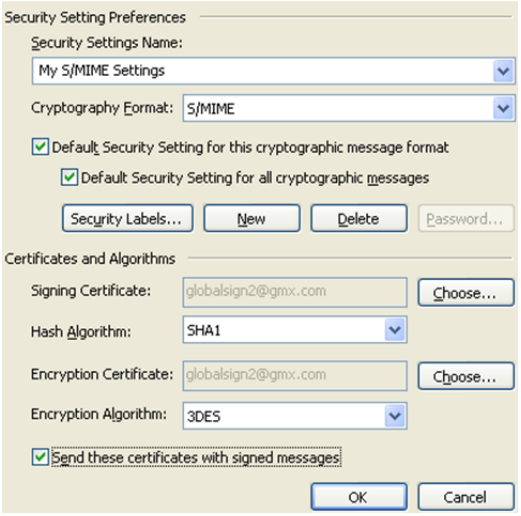
In simple terms, the choice is down to the user's specific needs. If the requirement is maximum security over a long period of time, selecting the strongest and most robust algorithm available is the sensible choice. If the requirement of the user is based in the short term and the primary concern is clear authentication, then the older and more proven algorithms would be more suitable.

Setting Algorithms and Recommendations

For optimal compatibility settings, Outlook 2011 for Mac OS X users should set their email security settings to SHA-1 signing algorithm and 3DES encrypting algorithm for compatibility or AES-256 for greater security. These settings can be located through Outlook-> Preferences-> Accounts-> Advanced-> Security tab.

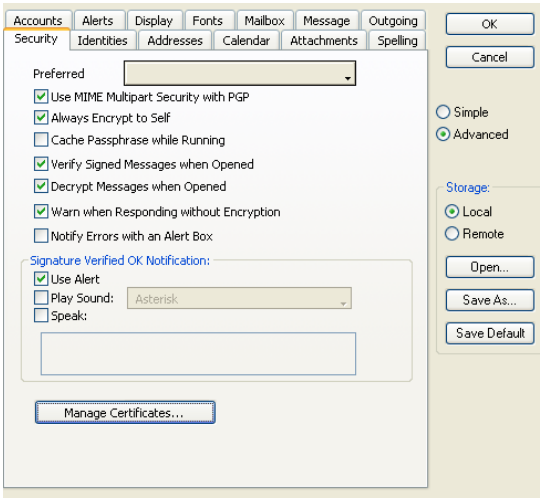


Outlook 2007 users can locate their email security settings through Tools-> Trust Center-> E-mail Security Tab-> Settings. As with Outlook for Mac the recommended settings are SHA-1 signing algorithm and 3DES encrypting algorithm as shown below.

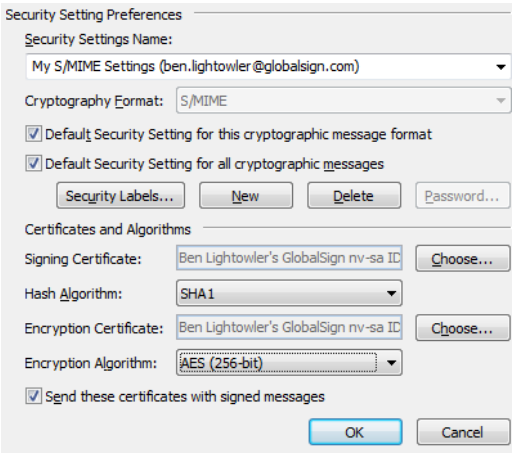


Thunderbird users will find that their email security settings are limited to the point where the option to change the signing and encrypting algorithms is not available.

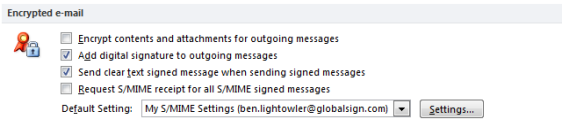
Mulberry Mail users can find the email security settings through File-> Preferences-> Advanced Radio button-> Security Tab. For the highest level of compatibility available make sure the 'Use MIME Multipart Security with PGP' is ticked and for ease of use make sure the automatically verify and decrypt messages when opened options are ticked.



The next section is aimed at Outlook 2010 users. To check your hashing and encrypting algorithms, locate the security settings through in Outlook via File -> options-> Trust Center Settings-> Email Security Tab-> Settings. Ideally the Hash algorithm should be set to SHA-1 and the encrypting algorithm AES (256-bit).



The following are a couple of points to avoid a few common issues. The first point is to avoid an encryption flagging error, ensure that the 'send clear text messages' is ticked. This option can be located in Outlook via File -> options-> Trust Center Settings-> Email Security Tab as shown below.



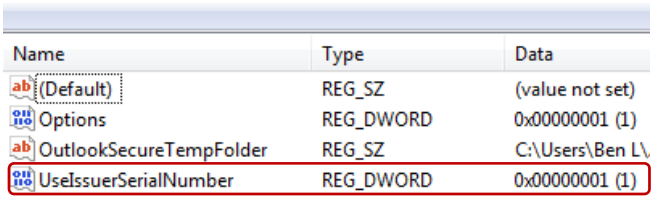
Trouble Shooting

Outlook 2010 users might find that the recipients of their encrypted emails unable to decrypt them. The following is a fix that Microsoft has released to address this problem.

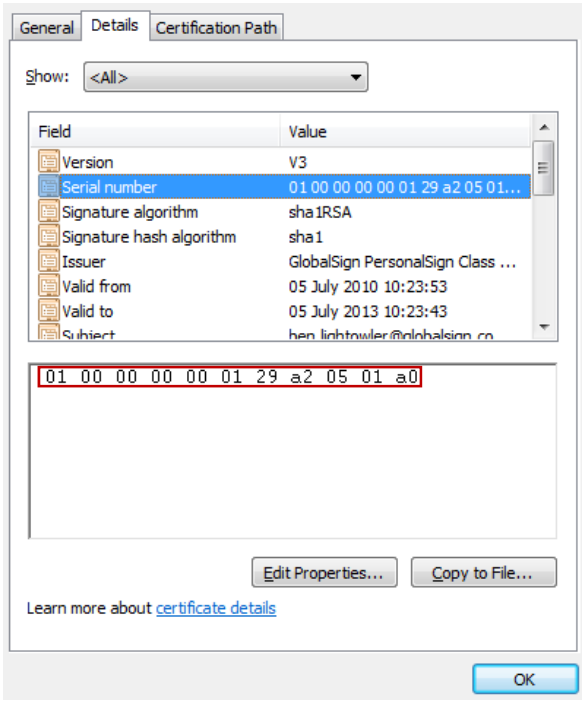
1. Start Registry Editor: Start -> search -> regedit
2. Locate and then click to select the following registry
   subkey: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Security
3. Note Create the \Security registry subkey if it does not exist.
4. Right click -> new -> DWORD(32bitValue)

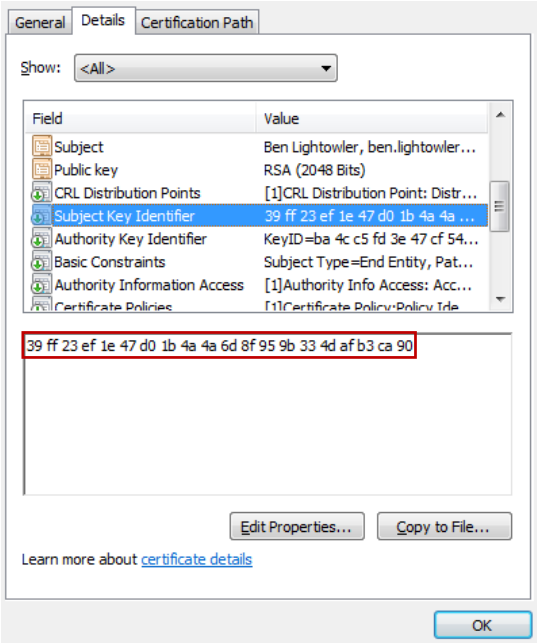
5. Add the following registry data to the this key: Value name: UseIssuerSerialNumber Value data: 1 (0x00000001 (1))

6. Close regedit and Restart Outlook.



This quick fix simply changes the method by which emails are encrypted. Rather than using the newer Subject Key Identifier (SKI) method for encryption, Outlook will revert to using the Serial Number (S/N) of the certificate. Whilst SKI offers an advantage in that multiple 're-issued' certificates could all have the same SKI (SKI is a SHA-1 hash of the public key) rather than being tied to a unique S/N, it is not yet widely used by other email clients and operating systems. This is described in RFC 5652 and implemented in the Cryptographic Message Syntax (CMS).

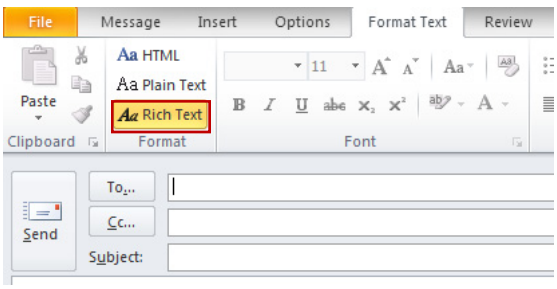




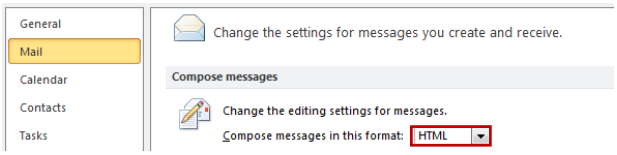
For more info please visit Microsoft Knowledgebase article - *http://support.microsoft.com/kb/2142236*

Another Issue potentially affecting Outlook 2010 users is an attachment error. It could be the case that MAC OSX users (even those using Outlook for MAC) receive winmail.dat attachments as shown below.

This issue is caused by the sender (An Outlook 2010 user), using an email format known as 'Rich Text'. To temporarily change this option on a message by message basis the option is available under the Format Text tab when composing a new message.



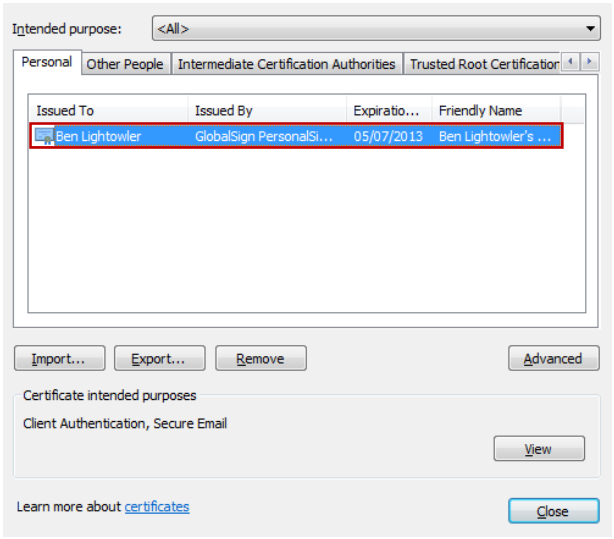
Or to change this option on a permant basis the option can be located through File-> Options-> Mail-> Compose Messages heading-> Compose messages in the this format.



It is recommomeded to have this option se to either Plain Text or HTML.

Backing Up

It is highly recommend that when using any Digital certificate and Public key, that you make a backup of your certificate and private key. Windows users may create a back up in the form of a PKCS#12 (.pfx) password protected file. To do this, Open Internet Explorer in administrator mode (this provides the necessary permissions for private key exporting) and for all versions previous to IE 9 locate the trust store through Tools-> Internet Options-> Content-> Certificates. Open IE 9, again in administrator mode and locate the certificate store through the cog icon in the top right hand corner of your browser then -> Internet Options-> Content-> Certificates.



Next select your certificate from the Personal tab and click the 'export' option. Select the 'make private key exportable radio button and follow the export wizard. Once you have backed up the certificate, the issuing certificate and have the PKCS12 file available to you, place it on a removable media device of your choice and store it in a secure location.

FIG 1: S/MIME EMAIL CLIENT COMPATIBILITY TABLE

Sender \ Recipient	Outlook 2010		Outlook 07		Thunderbird 3.1		OSX 10.6.7 iMail		Outlook 2011 OSX		Mulberry Mail		Lotus Notes 8.5.2	
	Signed	Signed & Encrypted	Signed	Signed & Encrypted	Signed	Signed & Encrypted	Signed	Signed & Encrypted	Signed	Signed & Encrypted	Signed	Signed & Encrypted	Signed	Signed & Encrypted
Outlook 2010 (Rich Text)	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✗	✓	?
Outlook 2010 (Plain Text)	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✗	✓	?
Outlook 2010 (HTML)	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✗	✓	?
Outlook 2010 (Rich Text) with attachment	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✗	✓	?
Outlook 2010 (Plain Text) with attachment	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✗	✓	?
Outlook 2010 (HTML) with attachment	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✗	✓	?
Outlook 2010 (Plain Text) with attachment SHA 256	✓		✗		✓		✓		✓		✗		✓	
Outlook 2010 (Rich Text) with attachment SHA 256	✓		✗		✓		✓		✓		✗		✓	
Outlook 2010 (HTML) with attachment SHA 256	✓		✗		✓		✓		✓		✗		✓	
Outlook 2010 Registryfix*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?	?
Thunder Bird 3.1 Plain Text	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?
Thunder Bird 3.1 Rich Text	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?
Thunder Bird 3.1 Plain and Rich Text	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?
Outlook 07 (Rich Text) with attachment	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?
Outlook 07 (Plain Text) with attachment	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?
Outlook 07 (HTML) with attachment	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?
Lotus Notes (Plain Text) with attachment	?	?	?	?	?	?	?	?	?	?	?	?	✓	✓
Lotus Notes (HTML) with attachment	?	?	?	?	?	?	?	?	?	?	?	?	✓	✓
Lotus Notes (Rich Text) with attachment	?	?	?	?	?	?	?	?	?	?	?	?	✓	✓
Gmail with Penandgo S/MIME Plugin FireFox 4	✓	?	✓	?	✓	?	✓	?	✓	?	✓	?	✓	?

INQUIRE ABOUT SECURE EMAIL SOLUTIONS

To learn more about GlobalSign S/MIME solutions, please visit https://www.globalsign.com/secure-email/ or contact us for further information. We would be happy to discuss your specific requirements.

ABOUT GLOBALSIGN

GlobalSign was one of the first Certification Authorities and has been providing digital credentialing services since 1996. It operates multi-lingual sales and technical support offices in London, Brussels, Boston, Tokyo and Shanghai.

GlobalSign has a rich history of investors, including ING Bank and Vodafone. Now part of a GMO Internet Inc group company - a public company quoted on the prestigious Tokyo Stock Exchange (TSE: 9449) whose shareholders include Yahoo! Japan, Morgan Stanley and Credit Suisse First Boston.

As a leader in public trust services, GlobalSign Certificates include SSL, Code Signing, Adobe CDS Digital IDs, Email & Authentication, Enterprise Digital Solutions, internal PKI & Microsoft Certificate Service root signing. Its trusted root CA Certificates are recognized by all operating systems, all major web browsers, web servers, email clients and Internet applications; as well as all mobile devices.

Accredited to the highest standards

As a WebTrust accredited public Certificate Authority, our core solutions allow our thousands of enterprise customers to conduct secure online transactions and data submission, and provide tamper-proof distributable code as well as being able to bind identities to Digital Certificates for S/MIME email encryption and remote two factor authentication, such as SSL VPNs.

GlobalSign Americas
Tel: 1-877-775-4562
www.globalsign.com
sales-us@globalsign.com

GlobalSign EU
Tel: +32 16 891900
www.globalsign.eu
sales@globalsign.com

GlobalSign UK
Tel: +44 1622 766766
www.globalsign.co.uk
sales@globalsign.com

GlobalSign FR
Tel: +33 1 82 88 01 24
www.globalsign.fr
ventes@globalsign.com

GlobalSign DE
Tel: +49 30 8878 9310
www.globalsign.de
verkauf@globalsign.com

GlobalSign NL
Tel: +31 20 8908021
www.globalsign.nl
verkoop@globalsign.com