

Modus™ Encryption

Introduction

Email is increasingly transactional in nature; it is used to communicate with employees, customers and partners. That being said, a considerable amount of sensitive information is sent over the Internet in clear text format, without any protection. Various laws and acts in the United States, Europe and in the rest of the world specify that some data **MUST** be secured. This is especially true for public companies (Sarbanes-Oxley) and the Health sector (HIPAA).

The Modus™ solutions support native secure e-mail facilities for secure Client access, secure Web access (WebMail & WebQuarantine) and secure communications between mail servers (incl. modusMail), mail relays (incl. modusGate) and back-end authentication servers.

Technology Overview

Modus™ can now ensure that the mail transmission connections are protected against sniffers and unauthorized access – messages cannot be stolen in transit and decrypted by unauthorized people.

Vircom's Modus™ technology supports encryption between email clients, email gateways, email servers using TLS/SSL (128-Bit) encryption which effectively prevents eavesdropping and message interception. Modus™ can actually manage TLS/SSL encryption requests and the related certificates and initiate TLS/SSL encryption requests (managed by other servers).

Modus™ can be configured to accept encrypted sessions from:

- Mail Clients (enabling SMTP, POP3 or IMAP4 encryption as required),
- Web Clients (enabling HTTPS encryption towards the WebMail or WebQuarantine servers),
- Mail Servers or Relays (enabling SMTP encryption)

By default, Modus™ will initiate encrypted sessions to:

- Authentication Servers (using TLS over SMTP, POP3 or Secure LDAP),
- Other Mail Servers or Relays (using TLS over SMTP)

Modus™ will try a secured connection first and if it fails it will use a non-secure connection:

- The type of connection will be saved so that the next time Modus™ will not try the secured connection if the destination server doesn't support it,
- The system will detect and correct locked situations.

Even when encryption has been enabled, Modus™ will still accept non-encrypted sessions. Modus™ can force encryption (either for incoming or outgoing connections) for a list of IP addresses. A connection made from or to an IP address in the list of "Force incoming and outgoing encryption for these IP addresses" will be rejected if the client doesn't ask for an encrypted connection. You must be aware that if you force encryption for SMTP, there may be interoperability problems if the outside server does not use the same sort of encryption protocols.

You can also encrypt specific IP addresses with different certificates, essentially using different encryptions for domains or IPs.

Performance issues

Be aware that enabling SSL/TLS is requiring a lot of CPU cycles on the server. A server will process 10 times less SSL/TLS connections. Retrieving a message will require more CPU because of the data encryption. Note that when using SSL/TLS, another service called LSASS.EXE may take some CPU. This service called "Local Security Authority Service" is in charge of checking the certificate and its validity.

modusGate Environment

Overview

The picture below highlights the different encrypted connections that will be supported.

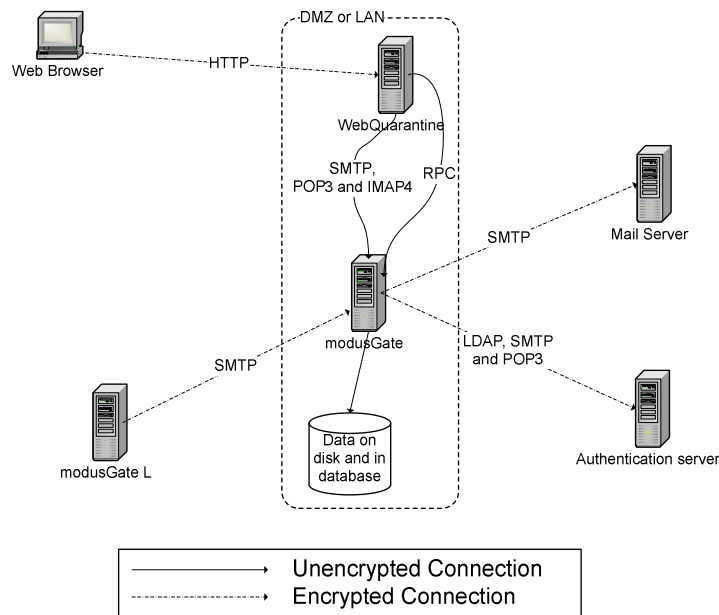


Figure-1: Encrypted Connections with modusGate

Mail client (Outlook, Eudora...) relays to modusGate

A mail client can send all its outgoing traffic towards the modusGate relay (e.g.: for outbound e-mail security) and require a Secured SMTP connection (port 25) connection.

Web Browser

The web browser can request a secured WebQuarantine HTTPS session to the modusGate WebServer.

e-Mail VPNs & Extranets

All communications between the company modusGate's (e.g. for large corporations) can be encrypted, allowing the modusGate to benefit from local internet access providers.

Companies could also extend their secured email environment towards their partners. If their partners' mail servers or relay do not support encryption, a modusGate L (starts at 395,00 €) can be installed as secured relay within their partner's email infrastructure.

Implementation

ModusGate Certificate Configuration

A new "Encryption & Certificates" tab has been added to the "Security" menu in the Modus console. By default encryption is disabled.

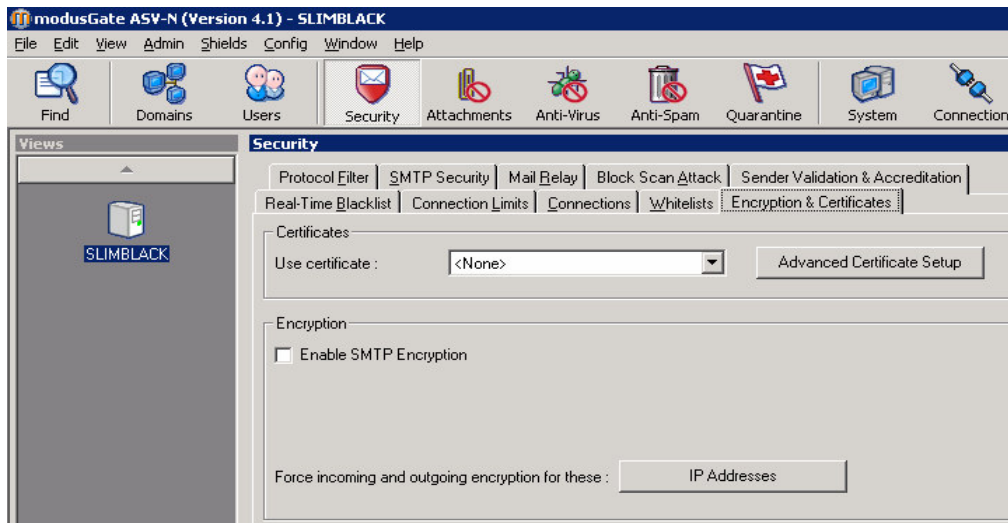


Figure-2: Encryption & Certificate Setup

To enable encryption one need to enter a selected certificate to be purchased from a certification authority¹.

The “Advanced Certificate Setup” screen allows the customer to select a different certificate for each IP address on the modusMail server. This will help ISPs to setup certificates for a particular set of domains.

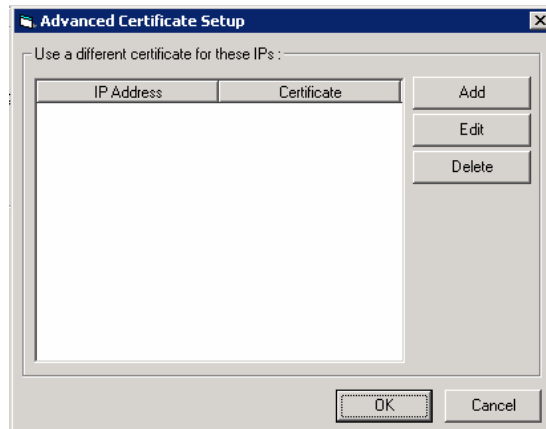


Figure-3: Advanced Certification Setup

Enabling SMTP encryption allows:

- Handling STARTTLS requests from mail clients using the modusGate as relay (for outgoing traffic),
- Handling STARTTLS requests from another modusGate (or relay) within an e-mail VPN scenario,
- Initiating STARTTLS requests towards other mail servers to which the modusGate needs to relay e-mails (this though does not require a Certificate to be defined)

Encryption can be forced for incoming our outgoing traffic, to or from a list of specific IP addresses.

¹ Purchasing and importing certificates his further detailed in Annex.

e-Mail VPN scenario

The e-mail VPN scenario is mostly used in multi-office companies. This allows a company to use its regional internet access provider, yet insuring all corporate traffic is encrypted over the Internet.

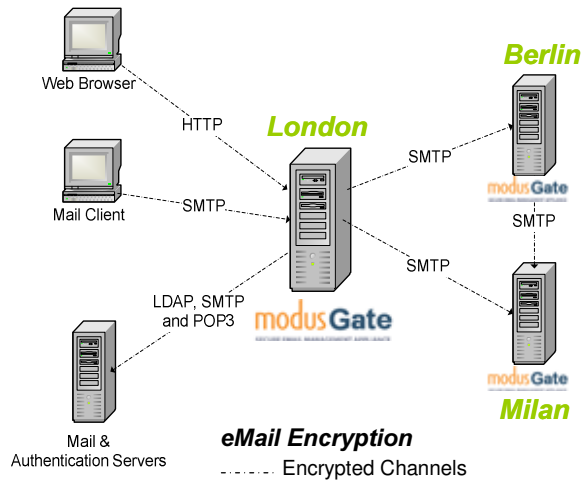


Figure-4: e-Mail VPN

To achieve this:

- Have a valid certificate on each modusGate server
- Enable SMTP Encryption on each modusGate server
- Force encryption on each modusGate for all incoming traffic from all other modusGate's IP addresses.

Mail Clients

The used method depends on the mail client capabilities:

Outlook Express

The only thing to do is to check the **SSL** checkbox in the "Advanced" section of the account. The port number can also be changed.

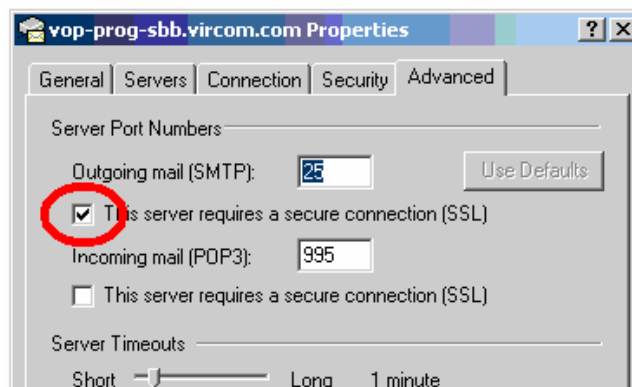


Figure-5: SMTPS client set-up with Outlook Express

Outlook 2000/XP

The only thing to do in the “**More Settings**” section is clicking on “**Advanced**” tab and checking the **SSL** checkbox. The port number can also be changed.

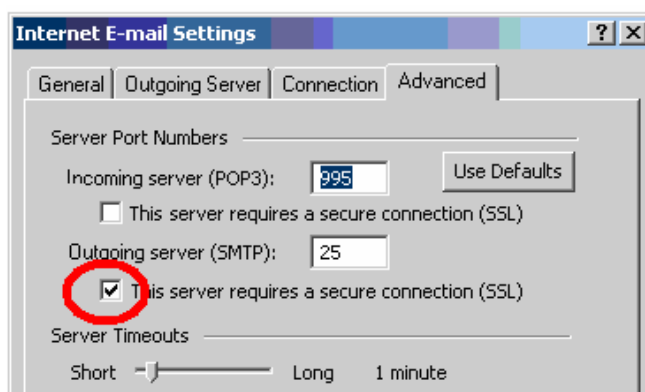


Figure-5: SMTPS client set-up with Outlook 2000 & XP

WebQuarantine/WebAdmin Clients

WebQuarantine/WebAdmin clients can access the modusGate via the secure HTTPS protocol. For this, configure encryption on the modusGate WebServer as follows:

- Make sure your WebServer machine's certificate(s) are installed in the local computer's account default directory.
- In the Internet Information Services (IIS) manager, select the default website (or select the specific website for which you want to configure encryption) and right-click to open Properties
- Select the Directory Security tab
- Click Edit
- Select the strength of the encryption you want to use:
- Require Secure Channel (SSL) forces users to use a secure connection (HTTPS) when connecting to the Modus web application
- Require 128-bit encryption forces users to use a stronger encryption method
- In the Client Certificates section, make sure that “Ignore client certificates” (which is the default option) is selected.
- Click OK to return to the IIS main view.

Encrypted Authentication

In the “Connection” menu address validation (“Automatically populate user list”) and authentication sessions can be encrypted as well. As highlighted in Figure-6, you can select your authentication method (per domain) and enable encryption for that particular session. This makes it very versatile and flexible.

Note that encryption is handled by the related authentication server. For a session to be encrypted the authentication server must have a valid certificate installed.

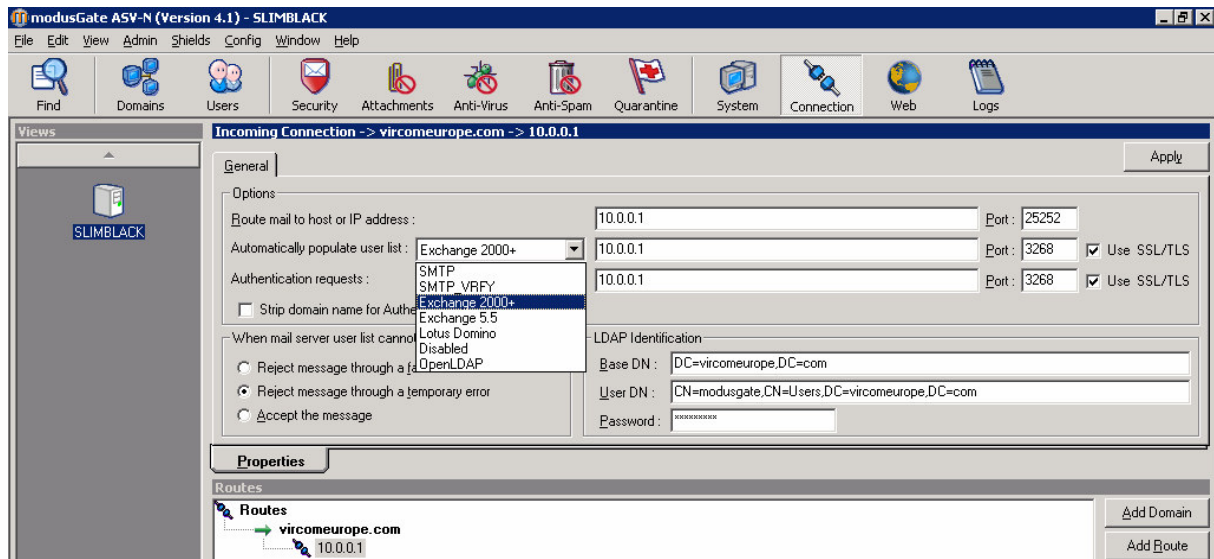


Figure-6: Encrypted Authentication Setup

modusMail Environment

Overview

The figure here below highlights the different encrypted connections that will be supported with modusMail.

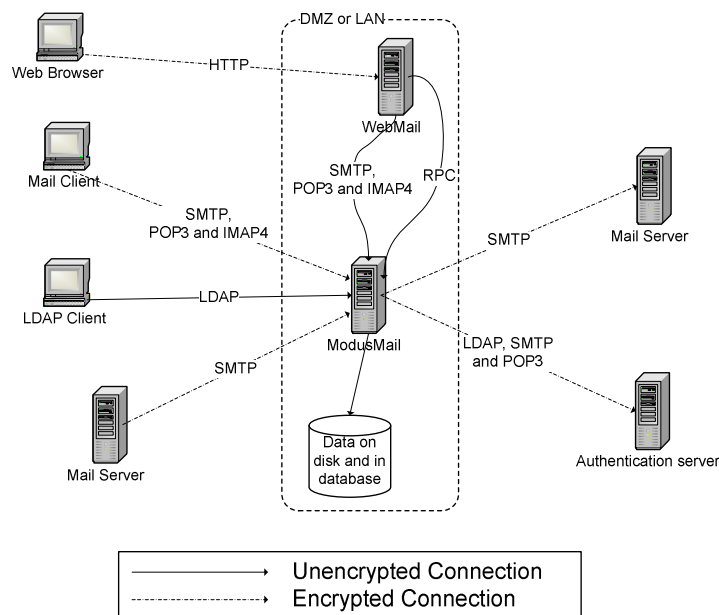


Figure-7: Encrypted Connections with modusMail

Mail client (Outlook, Eudora...)

In this case a mail client will request a secured connection. The mail client will be configured to run in secured mode, usually by requiring a Secured SSL SMTP connection (port 25) and Secured SSL POP3 (usually Port 995) connection.

Web Browser

The web browser can request a secured WebMail HTTPS session to the modusMail WebServer.

e-Mail VPN

The communication between all company mail servers (e.g. for large corporations) can be encrypted, as long as each mail server can manage and initiate a TLS/SSL Encryption Request.

Remote ETRN Request to modusMail

In this case, a remote mail server (e.g.: from a Corporate) will contact the modusMail (e.g.: at an ISP) to download all the emails related to its domains. The remote server ETRN request will not be encrypted. However, the SMTP mail transfer from the modusMail to the remote mail server can be encrypted as long as the remote mail server supports it.

Implementation

ModusMail Configuration

A new “Encryption & Certificates” tab has been added to the “Security” menu in the Modus console. By default encryption is disabled.

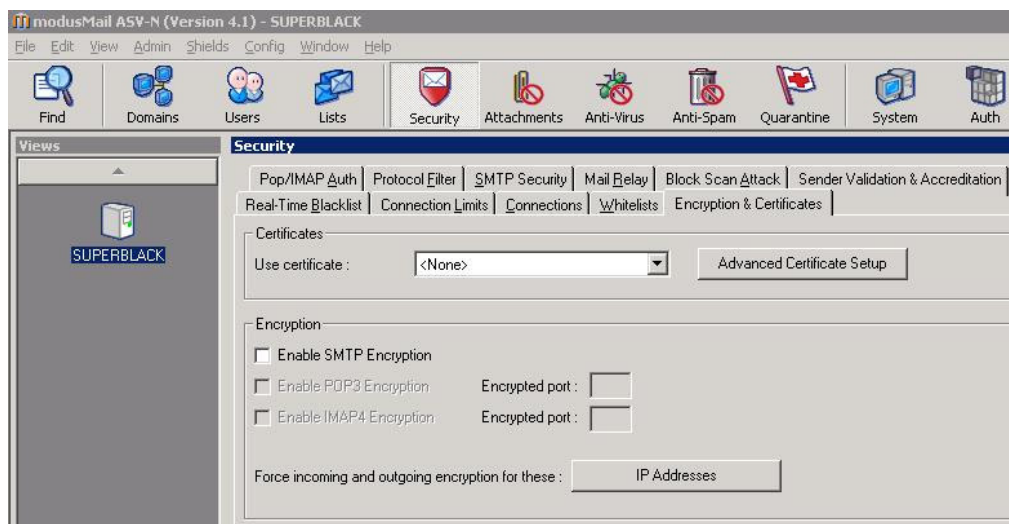


Figure-8: Encryption & Certificate Setup

To enable the encryption one need to enter a selected certificate.

As with modusGate (cfr. Figure-3), the “Advanced Certificate Setup” screen allows the customer to select a different certificate for each IP address on the modusMail server. This will help ISPs to setup certificates for a particular set of domains.

Enabling SMTP encryption, will allow you to:

- Handle STARTTLS requests from mail relays (incl. modusGate) or mail clients using the mail server as relay (for outgoing traffic),

- Initiate STARTTLS requests towards other mail servers to whom the modusMail wants to relay the e-mails (this however does not require a Certificate to be defined)

Enabling POP3 encryption will allow the modusMail to handle POP3S requests from mail clients. Enabling POP3 encryption will allow the modusMail to handle IMAP4S requests from mail clients.

You can force encryption for incoming or outgoing traffic to or from a list of specific IP addresses.

Mail Clients

For incoming e-mails, there are 2 ways to establish a secured POP3 connection:

1. Using port **995**: This port is used for secured connections only. Once a client is connected to this port, the connection is secured and then data can be exchanged confidentially.
2. Using the regular port **110**: The connection is established in clear text. Before the login part, the client issues a STLS command and the server tries to secure the connection. If successful, the data is transmitted confidentially.

The used method depends on the mail client capabilities.

Outlook Express:

For a secure POP3 connection, check the **SSL** checkbox in the “**Advanced**” section of the account. The port number can also be changed.

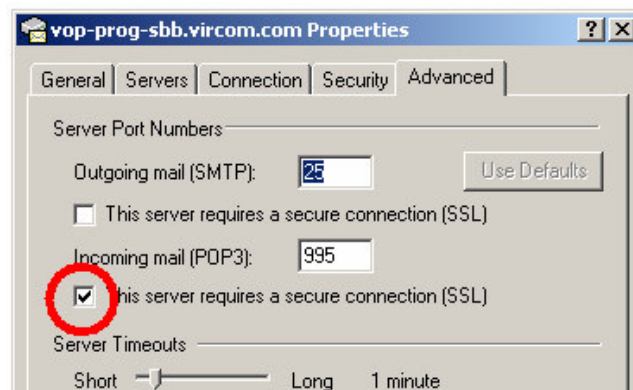


Figure-9: POP3S client set-up with Outlook Express

Outlook 2000/XP:

The only thing to do in the “**More Settings**” section is clicking on “**Advanced**” tab and checking the **SSL** checkbox. The port number can also be changed.

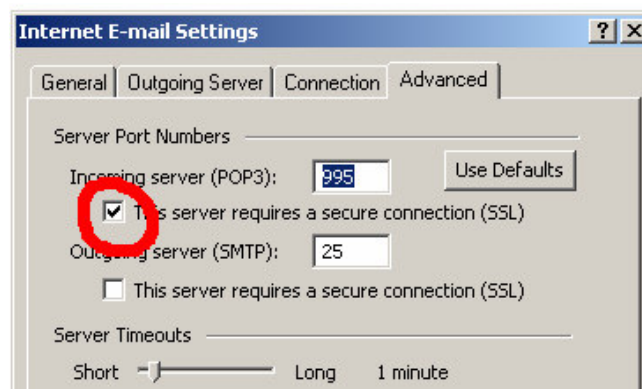


Figure-10: POP3S client set-up with Outlook 2000 & XP

Qualcomm Eudora:

Qualcomm Eudora mail client supports both ways to use SSL/TLS. Depending on the server setup, choose the appropriate way in the **“Incoming mail”** section.

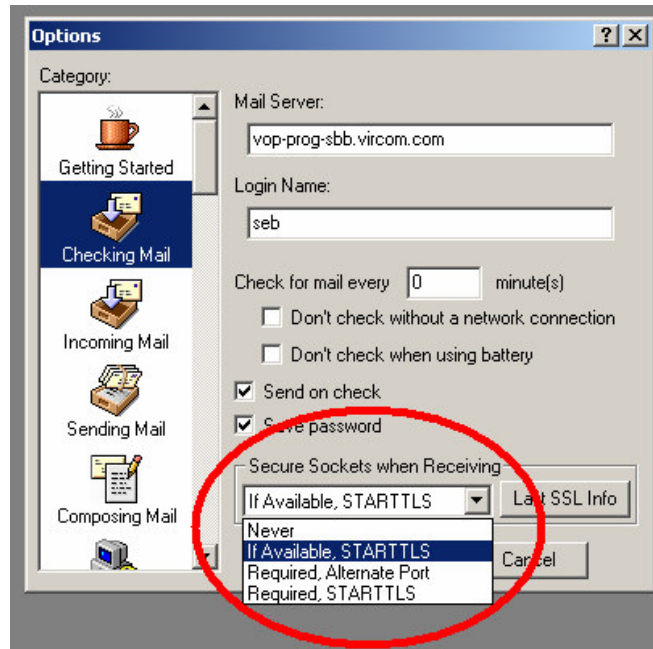


Figure-11: POP3 client set-up with Eudora

For outgoing e-mails, please refer to the SMTPS encryption details given in the modusGate section of this document.

WebMail/WebAdmin Clients

WebMail and WebAdmin clients can access the modusMail via HTTPS. For this, configure encryption on the modusMail WebServer as described in the modusGate section of this document (WebQuarantine/WebAdmin Clients).

Conclusion

Through Vircom's Modus™ technology, all email communications can now be secured:

- Communication from mail clients or web clients,
- Communications between mail servers, mail gateways or both,
- Communications with back-end authentication servers.

Annex

What are SSL and TLS?

SSL/TLS has been designed to:

- Secure the data between 2 network endpoints with encryption.
- Ensure the authenticity of the 2 endpoints with authentication.
- Ensure the integrity of the data.

SSL/TLS is mostly used to access to secured website (Bank for example) with the HTTPS protocol. But it can be used to secured any kind of connection (mail, news, custom traffic)

SSL/TLS History

SSL (Secured Socket Layer) has been invented in 1994 by Netscape and the current version is v3.

TLS (Transport Layer Security) is the standardized version of SSL. The standard has been finalized in 1999 by the IETF (Internet Engineering Task Force). Technically, TLS is compatible with SSL.

Principles and requirements to use SSL/TLS

SSL/TLS is a way to encrypt data to prevent transmission in clear text.

SSL/TLS use certificates to ensure communication is secured and authenticated. Certificates can be purchased from various companies like Thawte or Verisign². They are called Certification Authority. The certificate is a piece of data that needs to be installed on the server.

From the client point of view, certificates are not always required. Special mail client configuration is only required.

Installing the certificate

In order to handle encryption requests (STARTTLS) from mail clients or other servers, you first need to purchase and install a certificate (one per server).

A certificate request needs to be sent to a Certification Authority. In the request, we say who we are, what we want to do with this certificate (in our case, we want to do server authentication). When requesting the certificate, a name has to be given for the certificate, it's called the **Common Name** (or CN), and this name has to be the DNS name of the server, for example: pop.mycompany.com. If the certificate name does not fit with DNS naming, the certificate won't work.

When the request is accepted, the Certification Authority provides the certificate.

The certificate installation requires multiple steps:

1. The certificate has to be installed on the server in the default local computer account (certificates MUST be installed there or Modus can't use them). To do so, use the Microsoft Management Console (mmc.exe) and use the **Certificates** snap-in. Select "Computer Account" to view all certificates. And import the certificate received from the Certification Authority.
2. Check that the certificate is complete and contains the private key (one part of the certificate).

² A more detailed list of such companies can be find at <http://www.qmw.ac.uk/~tl6345/ca.htm>

This is described in Figure-10 here below:

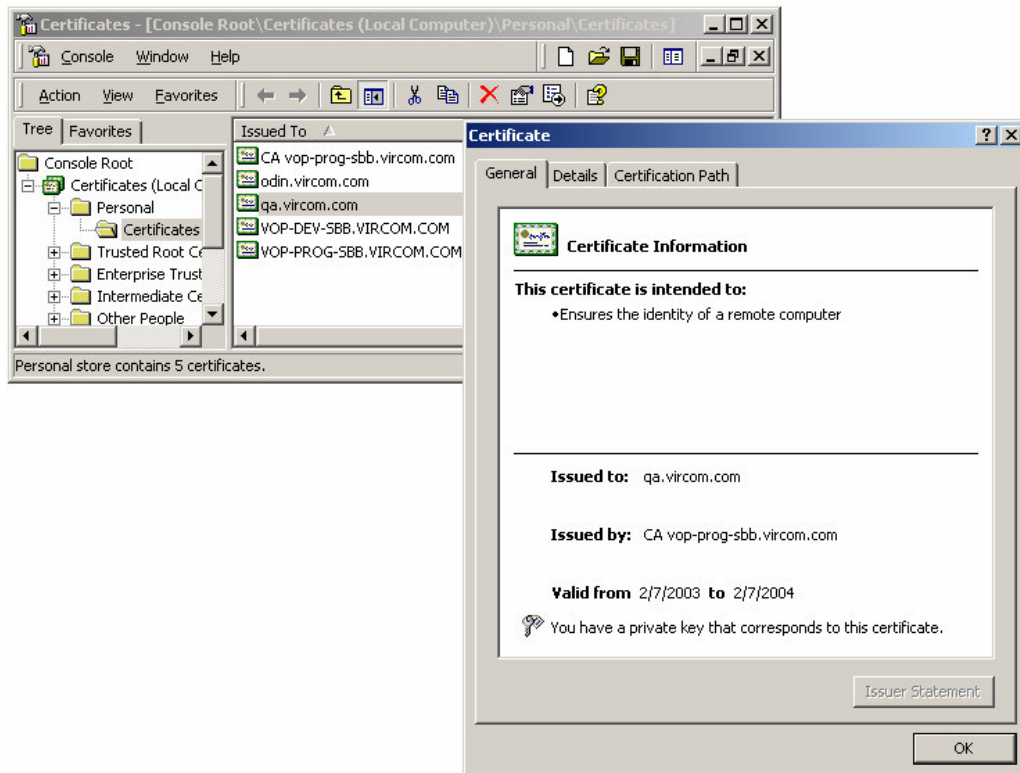


Figure-12: Certification Set-up

Other information

Ports used for encrypted connections

Take note that when using secure channels for POP3, IMAP4, LDAP or Active Directory's Global Catalog connections, the port numbers used by these services will change, and you will have to ensure they're open in your firewall. The new port numbers are:

- POP3S: 995
- IMAP4S: 993
- LDAPS: 636
- Global Catalog: 3269
- SMTPS: continues to use port 25, the only difference being that we use the STARTTLS command at the beginning of the connection. If the other server acknowledges the command, the connection is encrypted.

Disable Email Scanning in Desktop Anti-Virus Programs

If you're using any type of desktop anti-virus program on the ModusMail or ModusGate server, we are reminding you to disable the email scanning feature. This function will block messages sent through an encrypted connection because the AV engine isn't capable of parsing the message body; it also causes interference with Moduscan's ability to scan and process messages.