Cryptography and authentication (TLS and SMTP AUTH) when sending messages

Encrypted and authenticated access to the mail service

Cryptography: As of February 22, 2002, the TLS (SSL) is supported in our mail servers (post.uv.es), in any of the protocols for accessing mailboxes (POP3, IMAP) and in the sending of messages (SMTP). Likewise, TLS access to the mail access service is supported via the WWW.

Authentication: Additionally, the servers support user authentication for sending messages via the SMTP protocol (AUTH). An authenticated user can use SMTP to send messages outside the university, even if it is connected from an external computer ("relay" permission).

MSA: All the mail servers of the university and its firewalls support the authenticated access to the MSA SMTP 587 gate for sending mail.

Straight to the point

For those who are not interested in explanations and just want to configure their email client:

- Whenever a mail client program is configured (this does not affect the web access interfaces to mail) it is recommended to use either VPN (if it is outside the UV network), or to configure the mail delivery for Use TLS (cryptography), SMTP_AUTH (authentication) and SMTP gate 587 (not gate 25) (avoid firewall).

Cryptography: the problem

As is well known, the confidentiality of data transmissions over the Internet cannot be guaranteed, as it is very easy to intercept a communication in any of the points through which it transits. This is particularly serious when an access password is included in the information transmitted, since in most cases (current client programs) it is transmitted in clear (without any type of coding).

The solution usually adopted is to encrypt the password or, more generally, all communication.

To encrypt communications on the Internet, the SSL protocol (now renamed TLS) is usually used. This protocol also allows to ensure the identity of the server, the client program and the user through a set of "certificates"; in the current services of the university only one type of certificate will be used, the server certificate. The others are still not used too much because of the complex problem of validating a certificate (who certifies the certificate?).

The TLS in the mail service

For several years prior to 2002, our mail servers post.uv.es and postal.uv.es supported, experimentally, IMAP, POP and SMTP connections encrypted via TLS. However, the low standardization of such support in the usual mail clients (starting with NS-Mail and MS-Outlook Express) and in the server programs had prevented it from being considered as an advisable option in general. Even some of the standards changed in those years, invalidating all the clients that until then had TLS support in SMTP.

The situation evolved and the mail servers of the university officially began to support the TLS as of March 2002. This allowed solving the increasingly pressing problem of securely connecting to the mail service, mainly when it comes to computers located outside the university.

- The access service via WWW to the mail also supports TLS access using the secure WWW server, accessible at the URL https://correo.uv.es (observe the "s" of "https").

The set of these facilities allows to guarantee the confidentiality of the transmission of the data from the user's PC to the server and vice versa. Therefore, except for improper access to the server, confidentiality is guaranteed between accounts of the same server (and between those of the two servers, post and post). Likewise, passwords are protected. However, it is important to note that the messages are transmitted in clear between most Internet servers, so nothing can be assured about the confidentiality of the messages that leave our servers to the outside.

How to use TLS?

Use the mail or, if you want to configure your own mail client, there is a help to configure the mail programs with SMTP AUTH and TLS / SSL.

(The SMTP AUTH and the TLS / SSL are usually configured simultaneously: the SMTP AUTH is an insecure protocol that sends the password almost in clear, so it is convenient to encrypt the connection with the TLS / SSL).

Authentication: the problem
Neither the problem (the relay permission) nor the solution of this one (the SMTP AUTH) affect those who use the WWW interface to access the mail.

The "spam" and the permission of relay

The biggest problem with the mail service on the Internet today is its abusive use for the mass sending of unsolicited messages, often unwanted propaganda of various kinds.

This abuse, always existing and baptized in English as "SPAM", is growing increasingly and has led to the message sending servers (SMTP) are increasingly shielded against it, adopting restrictive measures (and mandatory compliance to be in the network) before accepting a message.

The first and foremost of these measures is to deny the relay of messages that come from unknown computers and destined to accounts that are not their own.

This measure is essential to prevent outsiders from using the SMTP server to massively disseminate unsolicited mail. However, it has as undesirable consequence that the SMTP server of an institution denies the forwarding of messages to anyone who connects from a foreign computer, even if that "anyone" is a person of the institution. The typical case is that of a person from the university who wishes to send messages from his home connected to the network through an access provider: the SMTP server of the university will deny it.

Possible solutions

The logical solution for these cases is simply to use the SMTP server of the Internet access provider. The only drawback that this has is that the user will have to use a different configuration (a different SMTP server) depending on the site (provider) used to connect to the network. The provider's SMTP server should have no problem redirecting messages from its own network.

The above solution is perfectly applicable in the case, less common, in which the institution itself is also the provider of Internet access: just connect to the network using exclusively the institution as an access provider. Unfortunately, this is not generalizable and is usually possible only in certain specific cases. At the Universitat de València, this can only be used by those users who are university staff (not students), who want to connect from the metropolitan area of Valencia and have requested and obtained access via modem.

A more practical solution is to connect virtually to the network of the institution, after having physically connected to the Internet via the access provider. This is possible using the "virtual private network" (VPN) facilities that are supported by most current computers. Connecting via VPN to the network of the University of Valencia is perfectly possible for any network user of the same, simply authenticating with your username and password.

The first of the solutions (SMTP of the provider) is the simplest and most commonly adopted. Unfortunately, it happens more and more often that it is not possible to use it because the Internet access providers are also choosing to prohibit their SMTP servers from being used with origin (return) addresses that are not from their own network. This measure invalidates the possibility of using said SMTP servers to send mail from any institution.

In this context, the SMTP AUTH appears as an equally simple solution and allows you to always use the same configuration (the same SMTP server) for the mail program, regardless of the place where the connection is made.

What is SMTP AUTH?

The main problem with SMTP servers when deciding whether or not to forward a mail message is the identification of the originator of the message.

The original SMTP protocol, designed in a "more confident" world, does not include any type of identification. However, recent additions to the protocol, known as SMTP AUTH, have been adopted in an increasing number of client programs and servers, which makes its use possible at present.

The SMTP AUTH is an extension to the SMTP protocol that allows the person who wishes to send an email message through an SMTP server to identify himself / herself to it. The identification mechanism, similar to the one used to authorize the reading of messages, usually consists of requesting a user + password pair.

In this way, a user can always use the server of his institution as SMTP server, since this will always allow him to send messages anywhere in the network, regardless of the situation of the computer he uses to connect.

Other SMTP applications AUTH

In general, the fact of identifying the one who sends a message goes beyond the simple authorization of the "relay" permission. An authenticated user may have more privileges or specific privileges, such as permission to send to certain restricted addresses, etc ...

How to use SMTP AUTH?
Since March 2002, the university’s mail servers officially support SMTP AUTH.

The user and password to use are the same as for access to mail reading.

The SMTP AUTH and the TLS / SSL are usually configured simultaneously: the SMTP AUTH is an insecure protocol that sends the password almost in clear, so it is convenient to encrypt the connection with the TLS / SSL. There is a help to configure mail programs with SMTP AUTH and TLS / SSL.

**Note:** It is highly recommended when configuring SMTP AUTH to also specify that SMTP gate 587 (instead of 25) be used. See the explanation below.

### The firewall: the problem

Neither the problem (access to our server through a firewall) nor the solution of it (the SMTP MSA at gate 587) affect those who use the WWW access interface to the mail [https://correo.uv.es](https://correo.uv.es).

### Closing the door SMTP 25

More and more often spammers (unwanted propaganda broadcasters) "rent" the services of computer virus manufacturers to get them networks of infected PCs in which programs to send propaganda mail have been introduced.

The huge number of computers (eg, residential) infected has forced most providers to **close door 25** on the way out; that is, to prevent users' PCs from sending mail directly to external servers without going through a server of the provider (which "knows" their PCs and is the one that can take the necessary measures to avoid abuse).

Obviously, this measure prevents a user who is outside from using the mail server of their institution, since it can not connect to any server external to the provider, when door 25 is closed in the provider's firewall.

### Possible solutions

The first and most obvious solution is, once again, to use a connection to the **VPN virtual private network of the University of Valencia** and to configure the mail client as if it were inside the same university.

But, in the most general case, this is not always possible (there are providers that even block the VPN). For this reason a special gateway has been defined in the mail standard for the programs that deliver authenticated mail: the **MSA (Mail Submission Agent) 587 gate**. This gateway **must** be open in all the providers to allow the authenticated connection to the mail servers external.

### How to use the MSA 587 door?

To use door 587 for mail delivery, you just have to configure your mail program to use gate 587 with the SMTP protocol (mail delivery). **Attention!** to use the 587 gate, **authentication must also be used** (SMTP AUTH).