System 5 now supports **"E-Mail Encryption"** and **"Digital Signatures" (S/Mime).**

By default, a standard e-mail is sent without any encryption and the recipient of such an e-mail cannot be 100 % sure, whether that e-mail really came from the displayed sender, or whether someone altered it during transmission.

System 5 already offers many security features like "Black- / White List", "Spam Journal", "Faked Sender Warning" and "DKIM-Check".

To complete the list of security enhancements, we have implemented the technique of "Digital Signing and Encryption" within System 5.

How does it work? All you need are "Digital Certificates", one for each of your own e-mail addresses. Digital Certificates are available from about € 30.00 p.a. and can be obtained from trusted organisations like "Comodo", "GlobalSign" or "VeriSign".

By using such a certificate, System 5 can add a digital signature to your outgoing e-mail. The recipient can use this signature to verify the sender, to check whether someone else has changed the message, and to encrypt new e-mails, which he addressed to you.

It also works the other way around. If someone sends you an e-mail together with her/his digital signature, System 5 runs the same checks (genuine origin and contents) and lets you encrypt your e-mails addressed to this person.

What sounds a bit complicated (and can be quite cumbersome with "off-the-shelf" solutions) is a simple task with System 5, which now comes with a fully automated and server based certificate-handling solution. There is no need to install and maintain any certificates on workstations or servers. Digital signatures of your clients and partners are collected and saved automatically when received by e-mail.

Within System 5, the user simply ticks a checkbox for "digitally signing" and another checkbox, if the message shall be encrypted. Decryption is handled fully automatically in the background, and does not require any user action at all.