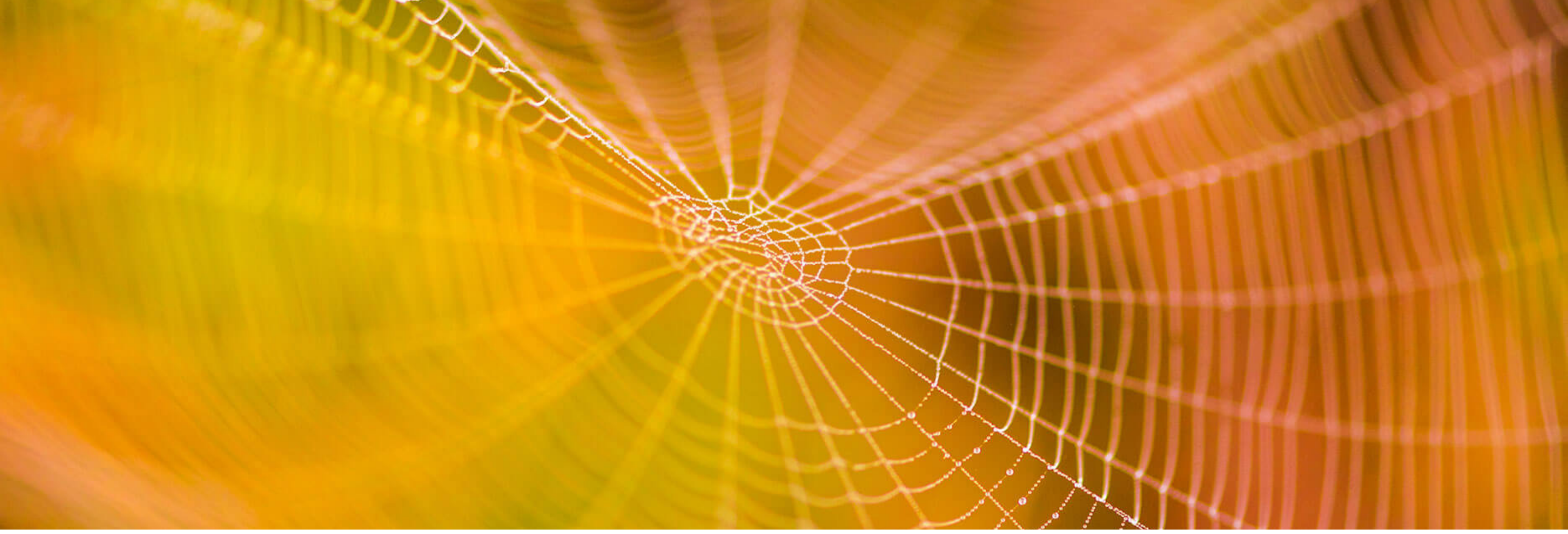

Email encryption for better security

Protect your email communication with easy centralized encryption

Encryption is a key building block of email security, though many companies fear its complexity. Yet even highly secure email encryption can be simple. iQ.Suite is a comprehensive, central encryption solution that allows you to communicate easily and securely with any recipient. No matter whether with other companies thanks to S/MIME and PGP or with recipients that do not have their own encryption solution thanks to AES-256 Bit PDF encryption.

Server-based encryption with iQ.Suite

With the server-based encryption of iQ.Suite, you protect not only your external, but also your internal email communication. This is made possible by implementing central encryption and decryption on your email server based on the industry standards S/MIME and PGP. Unlike client based methods, no installation on the end user's workstation is necessary and your employees don't have to deal with the technical aspects.

The flexible rules allow you to adjust the entire encryption process to your specific requirements and guarantee compliance with legal requirements, such as the GDPR. And thanks to integrated key and certificate management, managing these becomes effortless, even in complex environments.

PDF-based encryption with iQ.Suite

If your communication partners do not have their own encryption solution, you can still send them emails securely and easily using iQ.Suite's PDF-based encryption. Thanks to the AES-256 Bit PDF encryption standard, iQ.Suite balances between security and user-friendliness – without requiring the recipient to install keys, certificates or software.

The process is amazingly simple: The email, including all file attachments, is automatically converted into an encrypted PDF file and sent to the recipient. All file attachments remain in their original format.

In other words, the recipient only needs a PDF reader and the provided password.

Through the central password management, the sender can automatically generate a password and send it directly to the recipient. Alternatively, the sender can request to receive the password and then forward it to the recipient over the phone or SMS, for example. The recipient can then use their password and a PDF reader to open the encrypted PDF file in the mail client and on any end-device to read the message and access the attached files.

Benefits

- Holistic protection of the entire email communication – Communicate securely with external and internal recipients.

- Easy and centralized management – Easy administration of the central encryption policies. For server-based, by automatic multi-tenant management of keys and certificates, including import, export and backup functions, integration of existing PKI structures, etc. For PDF-based, by confidential email correspondence without PGP, S/MIME or PKI structures.

- Easy to use – End users don’t have to deal with encryption/decryption. No installation on end-devices or employee training are required.

- Protection from spying – Maximum security thanks to S/MIME, PGP and 256 Bit PDF encryption.

- Flexible rules & full control – Automatic encryption on the email server based on sender-recipient constellations, groups, domains or email content.

- Compliance with regulations – Server based approach guarantees continuous compliance with regulations such as the GDPR.