



Communication without certificate

If your recipient / communication partner neither disposes of a key system nor of an encryption solution JULIA MailOffice offers you various alternatives to send encrypted emails to this recipient and to receive such emails from your partner.

Alternative 1: The JULIA MailOffice Webmailer Component

JULIA MailOffice provides a webmailer component and enables you to communicate via encrypted emails because the Webmailer component is an independent JULIA application that will be installed on a separate webserver. According to your demands concerning automation and security level different operation modes are available:

A: Webmailer with "single-use password"

Your communication partner without certificate receives a standard email from you including a https link to your Webmailer. Additionally you inform your partner about an individual login and send the corresponding password separately (we recommend not to use the same communication channel for both). You also can send the password with a second email to your recipient. The desired procedure can be determined in the JULIA MailOffice configurations.

B: Webmailer with personalized inbox

The difference between this operation mode and type A (described left) is that only one password for every email will be generated here. The user can/has to change the password after having opened the inbox specifically created for him for the first time. All further emails will be stored in this inbox and can be edited there. Emails having exceeded a preset storage time can be deleted automatically.

„Password Self Service“

In order to reduce the interaction between sender and recipient of an email the following procedure was implemented enabling entire communication via Webmailer without password exchange between sender and recipient:

1. Using the policy "forced encryption" and due to a missing public key for the recipient the email will be forwarded to the Webmailer.
2. The recipient gets an email with a link and after clicking on this link a password for the recipient will be generated. This password will be sent to the recipient by email immediately.
3. With this password the recipient can log on to the Webmailer and is requested to change the password.
4. If the recipient has forgotten the password he can generate a new one which will be sent to him by email.

Adapting your corporate identity

The look&feel of the Webmailer's user interface can completely be adapted to the corporate identity of your company.

Alternative 2: Smart PKI Solution

Within the JULIA MailOffice system you have the option to create certificates. You tell your communication partner how to proceed with the certificate and where to find the private key. After having sent and installed the certificate you can communicate using the created pair of keys.

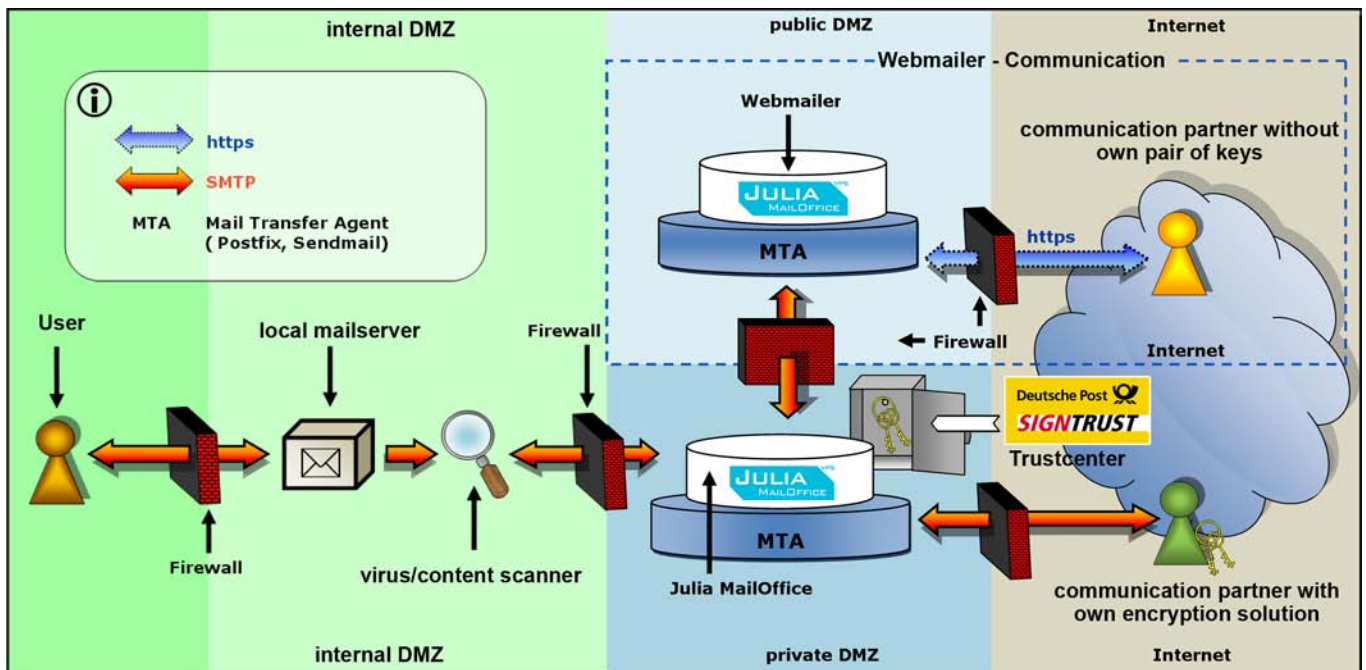
For sending the new generated certificates to your communication partner you also can use the Webmailer as mentioned above. After successful authentication your communication partner can download the new certificate you have created from the Webmailer. In this case the Webmailer will only be used for the first steps. Your further communication conveniently runs only with the use of the new generated pair of keys via email.

Alternative 3: Encrypted PDF mailing / Security forced automatically (Sfa)

If your communication partner uses neither S/MIME nor PGP besides Webmailer and the smart PKI solution you also can use following variation to send confidential documents via email to the user:

Before sending an email including the attachments will be transformed into a PDF file. This PDF file will be encrypted and sent as attachment via email to the specific recipient. With help of the password the recipient got he can now open the PDF file and import it to the his email client.

EXAMPLE ENVIRONMENT



Workflow of outgoing emails

The user sends an email and the inbound mail server forwards this email via a virus or content scanner to JULIA MailOffice.

By means of defined rules the system decides if the message shall be signed and/or encrypted. Then the message will be sent to the recipient.

If no key or certificate of the recipient is available according to the policy the message is stored on the Webmailer of JULIA MailOffice.

The recipient gets a notification email and can check his message on the Webmailer using a login and password mechanism and a secure internet connection (HTTPS). Finally the user can answer with an encrypted email via the Webmailer.

Compatibility

- S/MIME
- PGP
- compatible with all common email clients (SPHINX interoperability test)
- implementation of SMTP standard applications
 - virus scanners
 - content checkers
 - email archivers
 - document management systems (DMS)
- download of keys from directory services (LDAP)

Workflow of incoming emails

JULIA MailOffice verifies the validity of the signature of an incoming signed and/or encrypted email and decrypts this email.

If required at this point the email can be forwarded to an archiving system for storing the original email.

Subsequently JULIA MailOffice sends the email for further processing (e.g.: virus or content scanner) to the internal email infrastructure.

If required the internal recipient can get an attachment containing a report of the signature or decryption process of JULIA MailOffice.

Compatibility (continuance)

- creates certificates according to RFC (from trust center via „managed PKI“)



Technical requirements

- Intel Pentium III processor or SUN Sparc
- 512 MB RAM or more
- Linux operation system on Intel; Solaris 9 and 10 on Sparc
- 20 GB hard disk space or more

References on:

<http://www.iccsec.com> -> company -> references