

JULIA MAILOFFICE

VPS

BRIEF OVERVIEW

JULIA MailOffice is an extension of your email infrastructure for signature and encryption of your outgoing emails as well as for signature checking and decryption of incoming emails from a central point. JULIA MailOffice is embedded as an SMTP mail server in your network environment.

The basic component of JULIA MailOffice

- signature and signature check from a central point
- encryption and decryption from a central point

JULIA MailOffice is your virtual post office. Incoming emails are checked for signature and encrypted emails are delivered to the recipient in readable form. For outgoing emails you define policies that are embedded in JULIA MailOffice. According to these central policies your emails are signed or encrypted electronically.

Business critical

- re-encryption
- internal encryption
- multi client feature
- cluster feature (load balancing and high availability)
- own load balancer
- linear scalability

Three basic risks persist:

- loss of availability (costs of replacement)
- loss of confidentiality (costs of liability)
- loss of integrity (costs of re-establishment)

These are forcing and business critical facts and their risks have to be minimized for outbound as well as for inbound communication. Both inbound and outbound emails require a high security level. However, the needed applications (certificates, public and private keys) can be implemented with help of your system-own functions, no additional costs involved.

Integration

- automated download of certificates („managed PKI“) from a trust center like:



- integration of Microsoft PKI
- smart PKI solution of JULIA MailOffice
- integration of communication partners without certificates (Webmailer, SFA)
- integration of email archiving (DMS systems)

JULIA MailOffice can smoothly be integrated in your existent email infrastructure. You can create yourself certificates (internal communication), download certificates automatically (from a trust center via “managed PKI“) or if your communication partner do not dispose of this appropriate infrastructure (communication partners without certificates) you can use the Webmailer in accordance with law and security demands.

Conveniences

- parametrisable in very small units
- independent of clients
- password self service
- Security Forced Automatically (SFA) emails are sent as forced encrypted PDF files
- Corporate Identity can be adapted entirely (Gateway / Webmailer)
- multi level security convenience (infrastructure resists to disasters, respects secrecy demands)
- real software solution (platform independent / available as appliance)

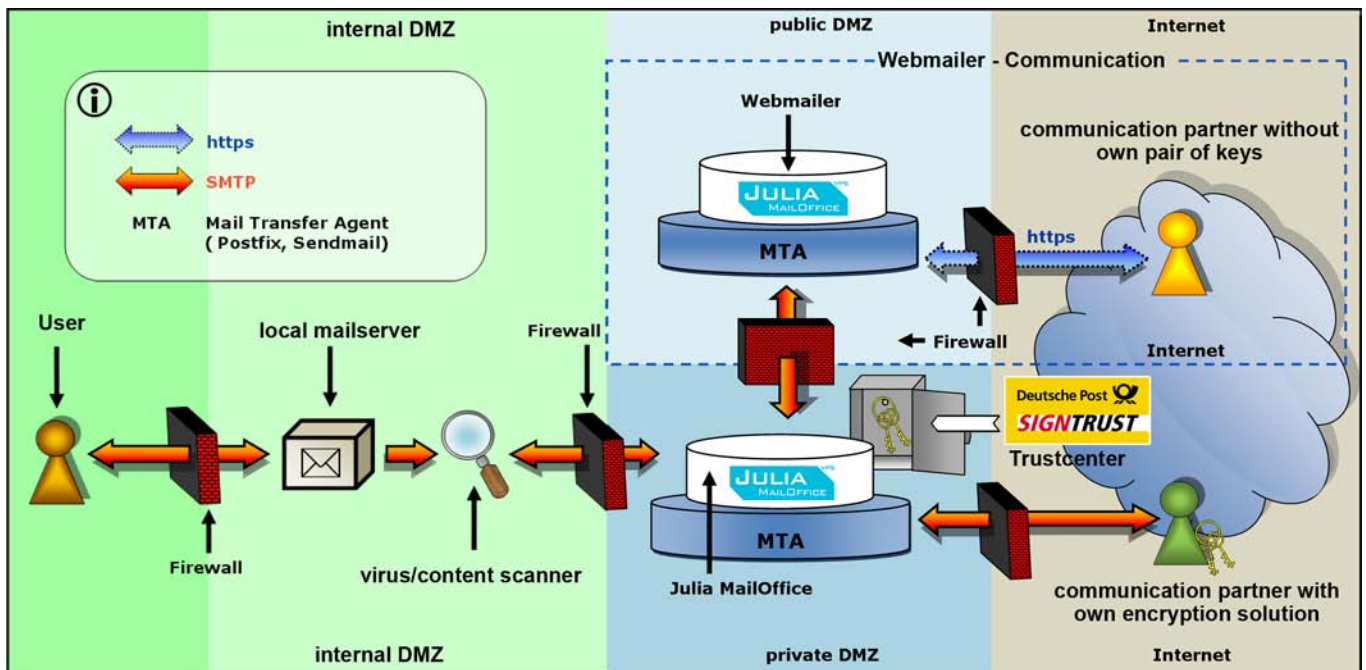
Conformity to standards, high compatibility level and customisability to your own demands are the attributes that will prevent future charges. Convenient features like password self service and client-independence reduce the use of manpower and the need of trainings in your company.

JULIA MailOffice is the email gateway of the virtual post office (VPS) of the project called BundOnline 2005.

For further information on VPS please refer to the link: <http://www.bsi.bund.de/fachthem/vps/>



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 Webmailers of JULIA MailOffice.

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

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