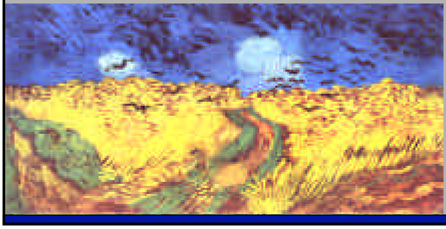
CU IT-Security
noventum consulting GmbH

Secure Messaging

Which kind of solution is the best for you?



"LKBQ EFKD FPPR OBKL QEFK DFPP ROBY RQKL QEFK DFPK LQXI TXVP PROB."

Joachim Ringelnatz

noventum
the art of business

Agenda

- Background Information
- Standard Solutions
- Virtual Post Offices
- Organizational Aspects
- Summary

LYNX
CONSULTING GROUP
We Move IT.

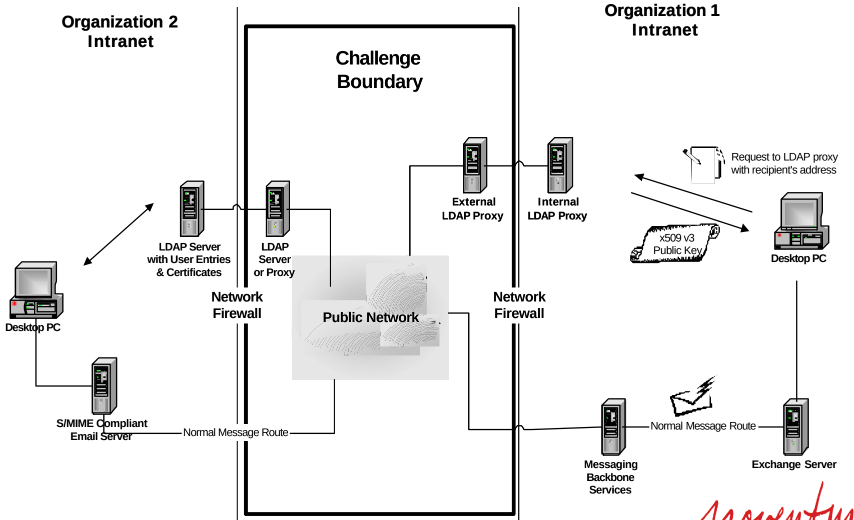
noventum
the art of business

The Secure Messaging Challenge 2001

The Challenge

Enable organizations to exchange strongly encrypted email using a standards-based, vendor neutral architecture that does not require manual key exchange.

Challenge Architecture



Organization 2 Intranet

Challenge Boundary

Organization 1 Intranet

Request to LDAP proxy with recipient's address

External LDAP Proxy

Internal LDAP Proxy

x509 v3 Public Key

Desktop PC

LDAP Server with User Entries & Certificates

LDAP Server or Proxy

Network Firewall

Public Network

Network Firewall

Desktop PC

S/MIME Compliant Email Server

Normal Message Route

Normal Message Route

Messaging Backbone Services

Exchange Server

Technical Requirements - Standards

- Use X.509 v3 CA Services
  - Self-signed or purchased commercial certificates
  - RSA algorithm with minimum 1024-bit key length
- Provide standards-based directory services accessible via the public Internet
  - Certificate stored in standard *userCertificate* attribute
- Provide S/MIME compliant messaging client capable of requesting certificates from the directory
- Provide S/MIME compliant email system
- Follow current standards regarding **S/MIME**, **X.509 v3** and **LDAP v3**

COTS or open source products only

Standard Solutions

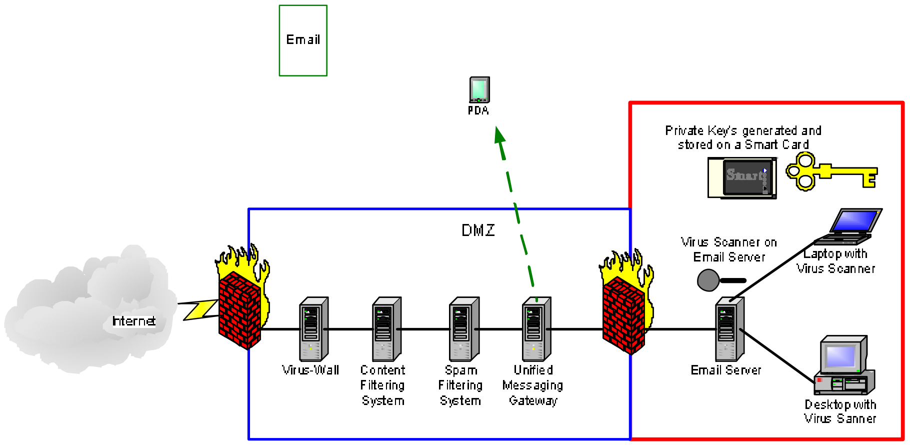
- **End/Site – to – End Security**
  - Use of Standard Clients (e.g. Outlook XX, Netscape, Lotus Notes…)
  - Message will be encoding and decoding on the Client
  - Generation of electronic Signatures on the Client
  - Every User needs one or more X.509 Certificates
  - Roll out of the participating Company CA Certificates
  - If you use no LDAP proxy or central configuration database, you have to distribute the directory configuration information of the other interested firms to all clients.

Advantage vs. Disadvantage – Standard Solution

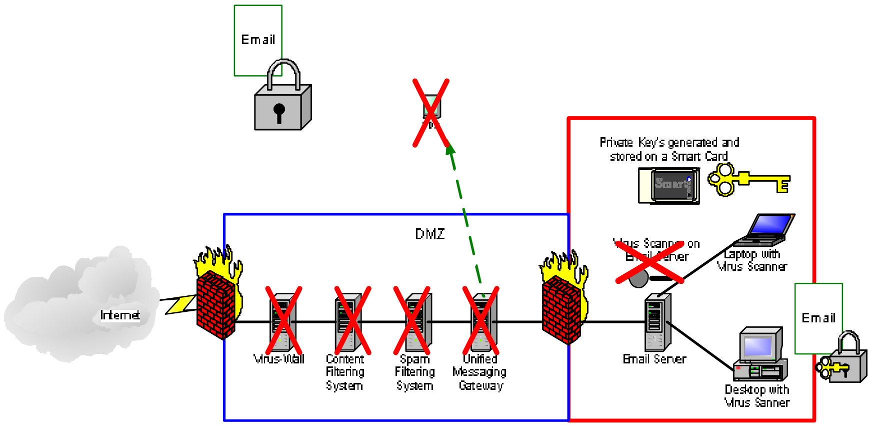
- **Advantages**
  - Economical solution, without investment in addition software
  - Fast realization possible

- **Disadvantages**
  - No central Content and Spam Filtering
  - No multi level Antivirus Scanning
  - No Unified Messaging Solution can work with encrypted emails
  - Last bastion is the desktops or notebook
  - Each user needs at least one X.509 Certificate
  - Roll out of the interested partner CA certificates necessary
  - Distribution of the directory configuration information of the other interested firms necessary

Standard Network


Email
PDA
Private Key's generated and stored on a Smart Card
Smart
DMZ
Virus Scanner on Email Server
Laptop with Virus Scanner
Internet
Virus-Wall
Content Filtering System
Spam Filtering System
Unified Messaging Gateway
Email Server
Desktop with Virus Sanner

Standard Network with Encrypted Emails



Email
DMZ
Private Key's generated and stored on a Smart Card
Virus Scanner on Email Server
Laptop with Virus Scanner
Internet
Virus-Wall
Content Filtering System
Spam Filtering System
Unified Messaging Gateway
Email Server
Desktop with Virus Sanner
Email

Virtual Post Offices

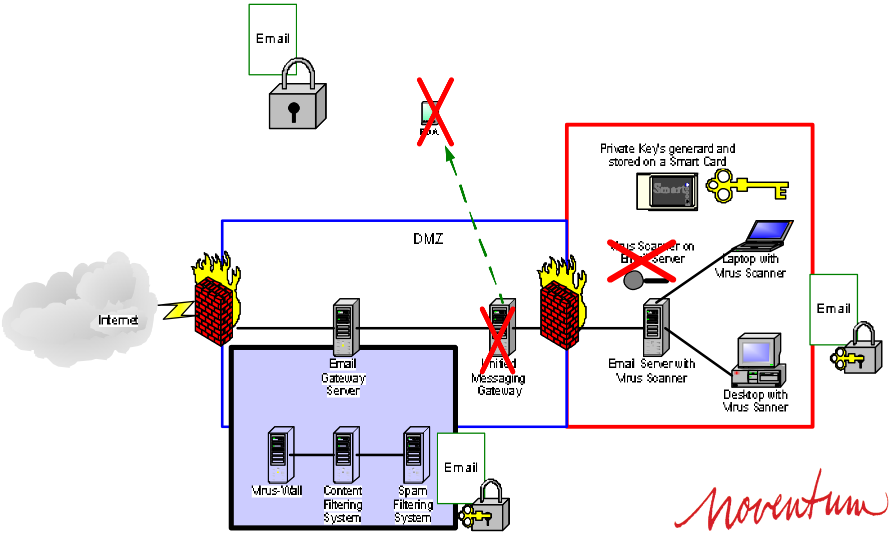
- **End/Site – to – End Security**
  - Message decoding with User interaction – Solution A
  - Message decoding without User interaction – Solution B
- **End/Site – to – Site Security**
  - Central Message decoding and Signing with a Company certificate – Solution C

Virtual Post Office – Solution A (1/3)

- **Functional method**
  - Encrypted email is stored in a special gateway
  - Gateway forwards the email header with symmetric key to Recipient
  - Recipient encrypts the symmetric key with his private key and he decrypts the symmetric key with the Gateway key (symmetric or asymmetric)
  - Gateway decrypts the symmetric key and than the Gateway decrypts the email
  - Gateway scans the email for Viruses and filters the Content in a Black box.
  - If the email is ok than the Gateway forwards the encrypted Email to the User
  - User decrypts the email on his desktop

Moventum
the art of business

Virtual Post Office – Solution A (2/3)


Email
PDA
Private Key's generard and stored on a Smart Card
Smart
DMZ
Virus Scanner on Email Server
Laptop with Virus Scanner
Internet
Email
Email Gateway Server
Unified Messaging Gateway
Email Server with Virus Scanner
Desktop with Virus Sanner
Virus-Wall
Content Filtering System
Spam Filtering System
Email

Moventum
the art of business

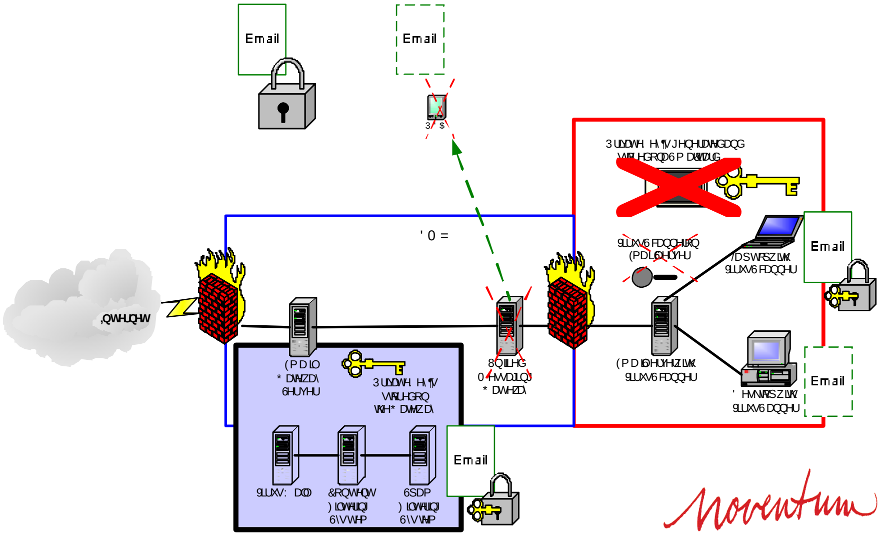
Virtual Post Office – Solution A (3/3)

- **Advantages**
  - Virus scanning and Content/Spam filtering is possible
  - Two-level virus scanning concept can be realized
- **Disadvantages**
  - No Unified Messaging Solution will be supported
  - Proprietary solution
  - Client plug in for Gateway interaction and Gateway is necessary – investment
  - Attack points are
    - gateway
    - data transmission between client and gateway
  - Each user needs at least one X.509 Certificate
  - Roll out of the interested partner CA certificates necessary
  - Distribution of the directory configuration information of the other interested firms necessary

Virtual Post Office – Solution B (1/3)

- **Functional method**
  - The private keys of the recipients are stored in a secure gateway environment.
  - Encrypted emails will decrypt at the gateway.
  - Gateway scans the email for Viruses and filters the Content in a Black box.
  - If the email is ok than the Gateway forwards the encrypted Email to the User.
  - User decrypts the email on his desktop
  - Gateway can also forward the email unencrypted to the Recipient.

Virtual Post Office – Solution B (2/3)



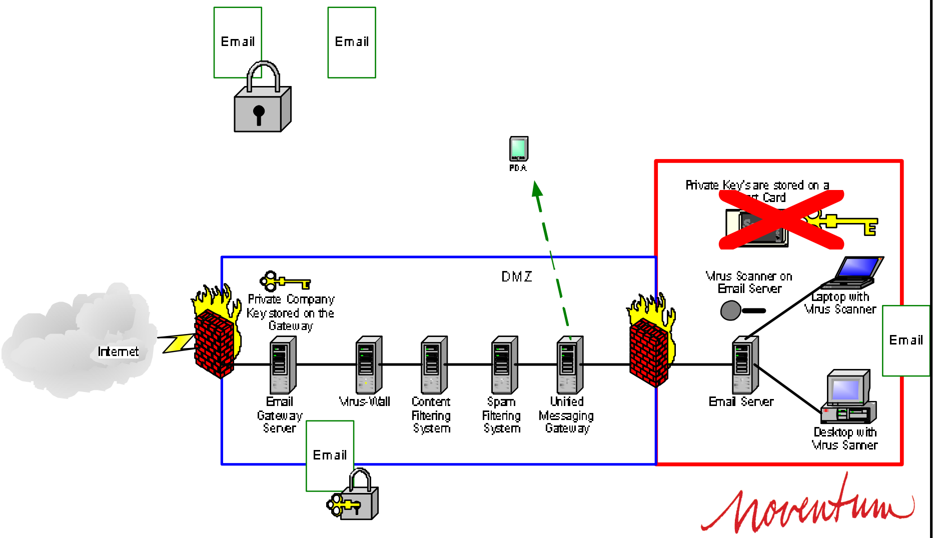
Virtual Post Office – Solution B (3/3)

- **Advantages**
  - Virus scanning and Content/Spam filtering is possible
  - Two-level virus scanning concept can be realized
  - Three-level virus scanning concept (unencrypted email forwarding) can be realized
  - Unified Messaging Solutions will be supported
  - Representative regulation can be realized.
- **Disadvantages**
  - Storage of the private keys at central point –> attack point.
  - Use of on Smart Cards / USB Token generated and stored private keys is not possible (not selection).
  - Sender and colleagues should be informed about the use of the technology.
  - Each user needs at least one X.509 Certificate
  - Roll out of the interested partner CA certificates necessary
  - Distribution of the directory configuration information of the other interested firms necessary
  - Gateway is necessary - investment

Virtual Post Office – Solution C (1/3)

- **Functional method**
  - Sender encrypts the email with a company certificate of the receiver.
  - Encrypted emails will decrypt at the gateway.
  - Than the email can be scanned for Viruses and the Content can be filtered
  - If the email is ok than the Gateway forwards the decrypted Email to the email server
  - A centralized or decentralized email encryption and/or signing is possible.
  - At the gateway can be defined an extensive control device for the email intercourse (encryption, signing, removing of signatures, validation of signatures, etc.)

Virtual Post Office – Solution C (2/3)


Email
Email
PDA
Private Key's are stored on a
rt Card
DMZ
Private Company Key stored on the Gateway
Virus Scanner on Email Server
Laptop with Virus Scanner
Internet
Email
Email Gateway Server
Virus-Wall
Content Filtering System
Spam Filtering System
Unified Messaging Gateway
Email Server
Desktop with Virus Sanner
Email

Virtual Post Office – Solution C (3/3)

- **Advantages**
  - Virus scanning and Content/Spam filtering is possible
  - Three-level virus scanning concept (unencrypted email forwarding) can be realized
  - Unified Messaging Solutions will be supported
  - Representative regulation can be realized.
  - Definition of an extensive control device is possible.
  - Only a company certificate necessarily.
  - All outgoing emails can signed with a company signature.
  - Central administration point for partner CA certificates.

- **Disadvantages**
  - Use of on Smart Cards / USB Token generated and stored private keys for email encryption is not possible.
  - Between gateway and email server and between email server and desktop all email will transmitted unencrypted.
  - Problems in the addressing of email at the receiver are well known.
  - Gateway is necessary - investment

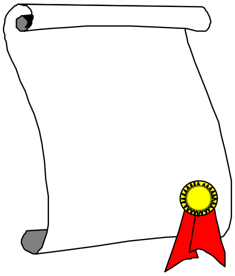
Moventum
the art of business

Common Practices

Addressing the

- **Legal,**
- **Political and**
- **Business issues**

are just as important for success as the technical solution.



Moventum
the art of business

Best Practices

- **How do we know that the public key actually belongs to the intended recipient?**

  Certificate Policies

  Certification Practice Statement

- **How do we know that the recipient will safeguard the infrastructure and their encrypted documents?**

  Relying Party Agreement

- **Many companies have thousands of trading partners -> with millions of possible combinations of bi-lateral agreements**

  Multi-lateral Agreements and acceptance of Best Practices

the art of business

Summary

- All Virtual Post Office Solutions use the Secure Messaging Challenge Standards.
  - LDAPv3
  - X.509v3
  - S/MIME
- Spam and Content filtering can be realized.
- The use of more level Virus scanning solution is possible.
- There is a solution for (almost) each business case.
- The view of the organization and the legal aspects are for the successful, durable utilization of decisive importance.

the art of business

Contact information

Address:	noventum consulting GmbH CU IT-Security Muensterstrasse 111 48155 Muenster / Germany
Contact:	Stephan Wappler
Phone:	+49 2506 93020
Mobile Phone:	+49 173 948 6631
Email:	stephan.wappler@noventum.de
Web:	www.noventum.de

"One thing is sure nothing is sure
but nothing is not always sure."

Joachim Ringelnatz

noventum
the art of business