

by The Messaging Forum
of The Open Group

toolkit

Secure Messaging Toolkit

- Practical real-world advice
- Step-by-step “How-to” guide
- Sample agreements and scripts
- Commercial off-the-shelf and Open Source products

THE *Open* GROUP



*Boundaryless
Information Flow*

*Boundaryless Information Flow™
achieved through global interoperability
in a secure, reliable and timely manner*

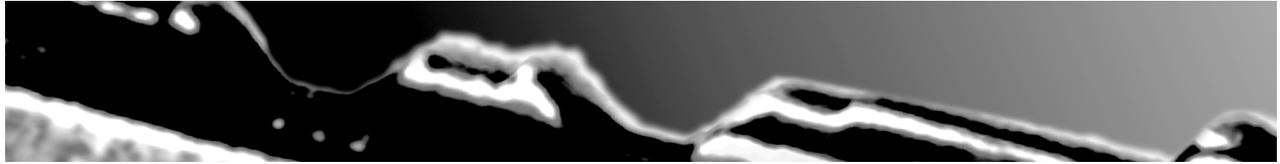
vision



The Messaging Forum

The Messaging Forum promotes Boundaryless Information Flow with standards-based electronic messaging. The forum operates in such areas as Secure Messaging, Instant Messaging, Anti-Spam and Anti-Virus best practices, Unified Communications and VPIM (voice profile for internet messaging). It is focused on creating a broad awareness of electronic messaging issues using educational and technological tools.

The Messaging Forum works with other forums on mutual work areas of interest in Boundaryless Information Flow such as Identity Management, Access Control and PKI Guidelines and Manageability which are also relevant to the Directory Interoperability, Mobile Management and Security Forums.



Secure Messaging Toolkit

by The Messaging Forum
of The Open Group

THE *Open* GROUP

Copyright © 2002, The Open Group

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owners.

Secure Messaging Toolkit

ISBN: 1-931624-14-3

Document No.: G260

Published by The Open Group, September 2002.

Any comments relating to the material contained in this document may be submitted to:

The Open Group
44 Montgomery St. #960
San Francisco, CA 94104

or by Electronic Mail to:

ogpubs@opengroup.org

Contents

Acknowledgements	vi
Secure Messaging Challenge 2001.....	v
<i>This Toolkit.....</i>	<i>v</i>
<i>The Challenge.....</i>	<i>v</i>
<i>Challenge Technical Requirements.....</i>	<i>v</i>
<i>Public Key Infrastructure Requirements.....</i>	<i>v</i>
<i>Feedback and Comments</i>	<i>v</i>
PKI Tutorial	1
<i>Encryption.....</i>	<i>1</i>
<i>Public Key Cryptography.....</i>	<i>1</i>
<i>Digital Signatures.....</i>	<i>1</i>
<i>Certificates.....</i>	<i>2</i>
<i>Policies.....</i>	<i>2</i>
<i>Key Management—PKI.....</i>	<i>2</i>
<i>Certificate Authority.....</i>	<i>2</i>
<i>Registration Authority (RA)</i>	<i>3</i>
<i>Directory Service.....</i>	<i>3</i>
<i>Timestamp Service</i>	<i>3</i>
Technical Implementation Details	5
<i>Components and Software Packages Used in the Challenge Testing.....</i>	<i>5</i>
<i>Certificate Servers</i>	<i>5</i>
<i>LDAP Servers.....</i>	<i>5</i>
<i>Messaging Servers.....</i>	<i>5</i>
<i>Messaging Clients.....</i>	<i>5</i>
<i>General Test and Implementation Considerations.....</i>	<i>6</i>
<i>Preparing for Test and Implementation.....</i>	<i>6</i>
<i>Public Key Infrastructure Requirements</i>	<i>6</i>
<i>Directory System Requirements</i>	<i>7</i>
<i>Messaging Server Requirements.....</i>	<i>7</i>
<i>Messaging Client Requirements.....</i>	<i>7</i>
<i>Components and Software Packages Used in the Challenge Testing.....</i>	<i>7</i>
<i>Certificate Servers</i>	<i>7</i>
<i>LDAP Servers.....</i>	<i>7</i>
<i>Messaging Servers.....</i>	<i>8</i>
<i>Messaging Clients.....</i>	<i>8</i>
<i>Challenge Test Environment.....</i>	<i>8</i>
<i>Boeing Test Environment</i>	<i>8</i>
<i>SMTPTSTBED.COM Test Environment.....</i>	<i>9</i>

<i>Relying Party Agreements</i>	90
<i>Technical Procedures</i>	91
<i>Certificate Exchange</i>	91
<i>Certificate Maintenance</i>	92
<i>Physical Security</i>	94
Appendix 1. Sample Challenge PKI Disclosure Statement (Version 1)	95
Appendix 2. Sample Relying Party Agreement	97
Appendix 3. MaXware Virtual Directory	99
<i>Introduction</i>	99
<i>Description</i>	99
<i>Specifications</i>	99
<i>MaXware Virtual Directory Referenced Lookup Examples</i>	99

Acknowledgements

Considerable effort went into the design, planning, and successful public demonstration of the Secure Messaging Challenge. Experts from around the world, both customers and suppliers, joined to define, create, and demonstrate the exchange of encrypted email among multiple companies using many existing standards-based applications. The Open Group and the Challenge Team would like to extend its gratitude to this dedicated group of individuals and their sponsoring companies:

Management Architect	<i>Dean Sepstrup</i> , The Boeing Company
Test Management	<i>Wen Fang</i> , The Boeing Company
Marketing Director	<i>Paul Van Avery</i> , FTT Consultants, Inc.
Technical Coordinator	<i>Dean Richardson</i> , The Boeing Company
Test Coordinators	<i>Russ Chung</i> , American Eagle Group
	<i>Kermit Russell</i> , NASA
	<i>Stephan Wappler</i> , Lynx Consulting Group
	<i>Kim Warford</i> , The Boeing Company
Demonstration Coordinators	<i>Wen Fang</i> , The Boeing Company
	<i>Stephan Wappler</i> , Lynx Consulting Group
Test Validators	<i>Fred Berlack</i> , Ferris Research
	<i>Paul Evans</i> , Booz Allen Hamilton
	<i>David Ferris</i> , Ferris Research
	<i>Roger Mizumori</i> , Waterforest Consulting Services
	<i>Jonathan Penn</i> , Giga Group
Summary Report Author	<i>Dean Richardson</i> , The Boeing Company
Summary Report Reviewer	<i>Dan Blum</i> , The Burton Group
Messaging Forum Director	<i>Teresa Schauer</i> , The Open Group
Messaging Forum Chair	<i>Dean Richardson</i> , The Boeing Company

The following people made major contributions to this document:

<i>Renée Barnow</i> , McKinley Marketing Partners	<i>Wen Fang</i> , The Boeing Company
<i>Russ Chung</i> , American Eagle Group	<i>Stephan Wappler</i> , Lynx Consulting Group

The Challenge Team would also like to recognize several individuals whose special contributions to the Challenge helped make it a success:

<i>Renée Barnow</i> , McKinley Marketing Partners	<i>Andreas Roscher</i> , Lynx Consulting Group
<i>Alexis Bor</i> , DirectoryWorks	<i>Michèle Rubenstein</i> , solutions4networks
<i>Brian Dilley</i> , Booz Allen Hamilton	<i>Bill Stroeing</i> , The Boeing Company
<i>Dr. Frank Gutberlet</i> , Lynx Consulting Group	<i>Dennis Taylor</i> , NASA—Goddard Space Flight Center
<i>Franz Mülkens</i> , Lynx Consulting Group	<i>Brad Wright</i> , The Boeing Company

The following companies participated in the Secure Messaging Challenge:

American Eagle Group	MaXware
The Boeing Company	Microsoft
Directory Works	NASA (Goddard Space Flight Center)
FTT Consultants	solutions4networks
Lynx Consulting Group	

Secure Messaging Challenge 2001

This Toolkit

The purpose of this Secure Messaging Challenge 2001 Toolkit is to document the “lessons learned” during the Challenge planning, implementation, and testing. By using the Toolkit, companies interested in secure messaging can adopt one of the methods the Challenge tested.

The Challenge

The 2001 Challenge was to enable organizations to exchange strongly encrypted email using a standards-based, vendor neutral architecture that does not require manual key exchange.

Challenge Technical Requirements

- Use X.509 v.3 Certificate Authority (CA) Services
 - Self-signed or purchased commercial certificates
- Use Rivest, Shamir, & Adleman (RSA) algorithm with minimum 1024-bit key length
- Provide standards-based directory services accessible via the public Internet
 - Certificate stored in standard *userCertificate* attribute
- Use S/MIME compliant messaging clients capable of requesting certificates from the directory
- Provide S/MIME compliant email system
- Follow current standards regarding S/MIME, X.509 v.3 and LDAP v.3
- Use commercial, off-the-shelf (COTS) or open source products only

Public Key Infrastructure Requirements

The intent of this Challenge was to plan, implement, and test only those components of a Public Key Infrastructure (PKI) that are needed to support a secure messaging system. The Challenge never intended to implement and test all aspects of PKI.

Feedback and Comments

We welcome your feedback, your comments or details of your experience in using this toolkit. Email us at challenge-questions@opengroup.org.

PKI Tutorial

Encryption

Encryption is the process of transforming the contents of a message using a secret key so that the message cannot be read. Decryption is the process of transforming the message back into a readable form. Message encryption and decryption is the foundation upon which a secure messaging system is built.

The problems with establishing and managing a secure messaging system are to ensure that—

- Encryption techniques and secret keys are sufficiently complex so that unauthorized people cannot decrypt messages
- Keys are accessible to people who are authorized to use them, and kept away from people who are not authorized to use them

Public Key Cryptography

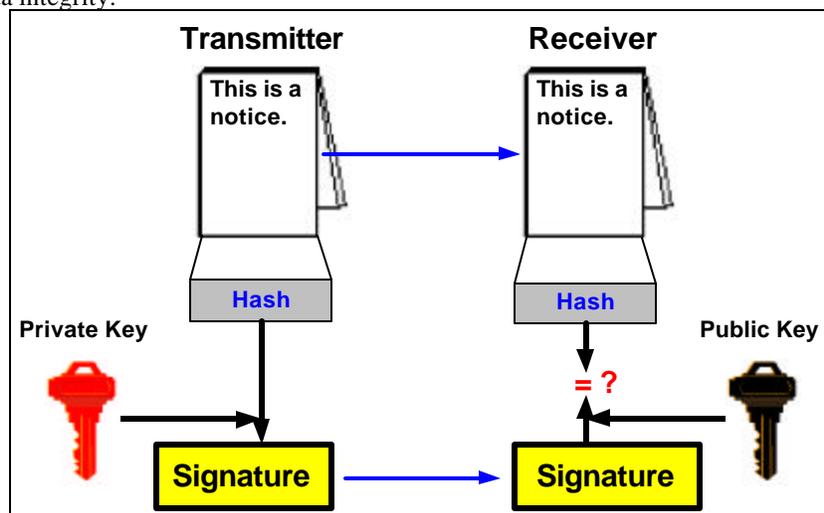
One assumes that encryption techniques have been used for as long as written languages have existed. Traditionally (until about 30 years ago), the secret key used to encrypt a message was the same key used to decrypt a message. This technique is known as *symmetrical key* or *secret key cryptography*. This technology is thought to be sufficiently strong that it would be almost impossible to decrypt a message without the secret key. The problem with symmetrical key encryption is key distribution: ensuring that the keys to the message senders and recipients do not get into the hands of unauthorized persons. As the number of users of the secure messaging system increases, the problem of generating, distributing, safeguarding, and accounting for the secret keys increases at a geometric rate.

In the 1970s, cryptographers introduced the concept of *asymmetrical key* or *public key cryptography*. Public key cryptography uses two keys that are mathematically linked; one key can be used only to encrypt a message, and the other key can be used only to decrypt the message. The key that is used to encrypt a message can be freely distributed (or placed in an accessible directory), and the recipient keeps the key used to decrypt the message.

Digital Signatures

Generally speaking, electronic signatures are data attached to other data for authentication purposes. The term not only refers to digital signatures (see below), but also to PINs and faxed signatures.

Digital signatures are electronic signatures linked to the signed data in a way that tampering is noticed and that the sender can be identified unequivocally. Other forms of electronic signatures, such as PINs, do not protect the data integrity.



To create a digital signature, the signing transmitter creates a Manipulation Detection Code (hash) of the message and then uses an exclusively transmitter-owned private key to encrypt the hash. This is the digital signature and it is attached to the real message (message expanding).

The private key has a matching public key that the receiver can use to verify the signature. The receiver uses the same hash function to create a hash of the real message, and then takes the public key to the transmitter, decrypts the digital signature, and compares hashes.

A trustworthy institution (i.e., a Trust Center or a Certificate Authority) assigns this pair of keys to a particular person.

The following factors form the basis for using digital signatures:

- Secure software, which supports digital signature functionality (e.g., email-clients or plug ins)
- Secure infrastructure, which supports key exchange (PKI—a Trust Center is a special PKI with more security)
- Choice of hash functions and public key algorithms

Certificates

Digital certificates are virtual fingerprints that authenticate absolutely the identity of a person or thing. The certificate itself is simply a collection of information to which a digital signature is attached. A third-party authority that the community of certificate users trusts attaches the digital signature.

Policies

A Certificate Policy is a set of rules that indicates the applicability of a certificate.

A Certification Practice Statement (CPS) is a statement of the practices that a PKI uses to manage the certificates that it issues. The Operating Authority (usually an individual within the IT unit) is responsible for preparing and maintaining the CPS. The CPS describes how the Certificate Policy is interpreted in the context of the system architecture and operating procedures of the organization.

While a Certificate Policy is defined independently of the specific details of the operating environment of the PKI, the corresponding CPS is tailored to the organizational structure, operating procedures, facilities, and computing environment of the Operating Authority. The use of a standard structure for Certificate Policy and CPS documents is recommended to ensure completeness and simplify users' and other Certificate Authorities' assessment of the corresponding degree of assurance. See Section 4.1 of this Toolkit for the recommended structure for Certificate Policy and CPS documents.

Key Management—PKI

The use of PKI enables a secure exchange of digital signatures, encrypted documents, authentication and authorization, and other functions in open networks where many communication partners are involved.

PKI has four parts:

- Certificate Authority (CA)
- Registry Authority (RA) or Local Registry Authorities (LRA)
- Directory Service
- Time Stamping (as an additional service)

Certificate Authority

The Certificate Authority (CA) is the entity responsible for issuing and administering the digital certificates. The CA acts as the agent of trust in the PKI.

A CA performs the following main functions:

- Issues users with keys/Password Exchanges (PSEs) (though sometimes users may generate their own key pair)

- Certifies users' public keys
- Publishes users' certificates
- Issues certificate revocation lists (CRLs)

The foundation upon which a PKI is built is trust—in other words the user community must trust the CA to distribute, revoke, and manage keys and certificates in such a way as to prevent any security breaches. As long as users trust the CA and its business processes, they can trust certificates the CA issues.

The CA's signature in a certificate ensures that any changes to its contents will be detected. Such certificates can be distributed publicly and users retrieving a public key from a certificate can be assured of the validity that the key:

- Belongs to the entity specified in the certificate
- Can be used safely in the manner for which the CA certified it

Users need to be able to determine the degree of assurance or trust that can be placed in the authenticity and integrity of the public keys contained in certificates the CA issues. The information upon which such determinations can be made is documented in the Certificate Policy and the Certification Practice Statement of the CA.

A CA has the following tasks:

- Generate the certificate based on a public key. Typically a Trust Center generates the pair of keys on a smart card or a USB token.
- Guarantees the uniqueness of the pair of keys and links the certificate to a particular user
- Manages published certificates
- Is part of cross certification with other CAs

Registration Authority (RA)

The Registration Authority (RA) is responsible for recording and verifying all information the CA needs. In particular, the RA must check the user's identity to initiate issuing the certificate at the CA. This functionality is neither a network entity nor is it acting online. The RAs will be where users must go to apply for a certificate. Verification of the user identity will be done for example by checking the user's identity card.

A RA has two main functions:

- Verify the identity and the statements of the claimant
- Issue and handle the certificate for the claimant

Directory Service

The directory service has two main functions:

- Publish certificates
- Publish a Certificate Revocation List or to make an online certificate available via the Online Certificate Status Protocol (OCSP)

Timestamp Service

Timestamping is a special service. Timestamping confirms the receipt of digital documents at a specific point in time. The service is used for contracts or other important documents for which a receipt needs to be confirmed.

Technical Implementation Details

The following section contains some of the detailed “lessons learned” in setting up the products used for the Challenge. This does not imply that these are the only products that can be used for secure messaging.

Components and Software Packages Used in the Challenge Testing

Certificate Servers

- Microsoft Windows 2000 CA server as self-signed root certificate authority
- Microsoft Windows 2000 CA server as stand-alone subordinate certificate authority with a Microsoft Exchange 5.5 Key Management Service
- iPlanet CMS 4.0 as self-sign root certificate authority
- Open SSL as self-signed root certificate authority
- Purchase certificate from VeriSign

LDAP Servers

- MaXware Virtual Directory
- Windows 2000 Active Directory
- OpenLDAP
- directory.verisign.com
- Lotus Domino R5.0.8
- iPlanet LDAP 5.0

Messaging Servers

- Lotus Domino R5.0.8
- Microsoft Exchange 5.5/2000
- SendMail 8.11.0

Messaging Clients

- Microsoft Outlook 2000 SR1 (International + Security Patch)
- Microsoft Outlook 2000 SP2
- Lotus Notes R5.0.8

A comment about Microsoft Outlook Express

Because of the popularity of Microsoft Outlook Express and Outlook Express (International) among users, the Challenge intended to include those messaging clients to test interoperability. However, when using a digital certificate obtained or confirmed from an LDAP directory, Microsoft Outlook Express uses 40-bit encryption to send an encrypted email message rather than 128-bit encryption. According to Microsoft Tech Note Q262003, RC2 40-bit encryption is the default by design because Outlook Express cannot determine if the recipient is able to accept 128-bit encryption. Challenge testers confirmed this default behavior, and because 128-bit encryption was a Challenge requirement, Microsoft Outlook Express was not used during interoperability testing.

General Test and Implementation Considerations

- PKI infrastructure and Certificate Practice Statement to create certificate trust relationship between challenge participants
- X.509 v.3 certificate to escrow user's public key for strong encryption
- Certificate issued will be published in standard LDAP v.3 directory server for query
- Any invalid certificate will be removed from the directory
- Real-time query directory for email recipient's certificate to encrypt message (and, DO NOT store certificate in personal address book)
- S/MIME compliant email system and client to send and receive strongly encrypted email messages

Preparing for Test and Implementation

Public Key Infrastructure Requirements

CA and RA

- Self-signed
 - Self-sign Root CA and establish certificate hierarchy structure based on the industry's best practice and X.509 standard
 - CA server with off-the-shelf product like Windows 2000 CA Service, iPlanet CMS or other X.509 compliant software to issue X.509 v.3 certificate
 - Certification Practice Statement
 - Exchange Public Root CA certificates between companies to establish trust
- or*
- Purchase service from trusted vendor (RSA, VeriSign, Entrust...)
 - Vendor provided CA & RA services to issue certificates
- or*
- Become a subordinate to vendor's CA to issue certificates with off-the-shelf product
 - Certificate Practice Statement
 - Certificates can be traced to trusted commercial Root CA

Key Management (preferred, but not required)

- RSA Key Transfer (RFC 1421, 1423)
- or*
- Diffie-Hellman agreement (PKCS#3)
- or*
- ISO/IEC 9798-3, US FIPS PUB 196

Certificate

- X.509 v.3 compliant
- RSA Algorithm
- 1024-bit or higher key length
- Binary encoding (LDAP v.3)

Certificate Issuing

- Automated process (preferred) to publish certificate issued to the user's entry in the LDAP directory
- Automated process (preferred) to remove revoked, compromised, or expired certificate from the directory
- User's email address listed in the directory must be identical to the email address attribute in the certificate

Directory System Requirements

Example

Microsoft Windows 2000 Active Directory, iPlanet LDAP Directory, and others

- Answers LDAP v.3 query
- Contains user information
 - Common name
 - Email address
 - X.509 v.3 certificate
- Common directory Schema/Attribute design and naming are not required—Boeing LDAP proxy service will perform “schema attribute translation” on the fly

Messaging Server Requirements

- S/MIME compliant

Messaging Client Requirements

- S/MIME compliant
- Cipher strength of 128-bit and above (may be related to the operating system cipher strength)
- Ability to perform LDAP query for certificate to encrypt message
- Should not require key storage for message encryption
- Optional off-line mode for message encryption

Components and Software Packages Used in the Challenge Testing

Certificate Servers

- Microsoft Windows 2000 CA server as self-signed root certificate authority
- Microsoft Windows 2000 CA server as stand-alone subordinate certificate authority with a Microsoft Exchange 5.5 Key Management Service
- iPlanet CMS 4.0 as self-sign root certificate authority
- Open SSL as self-signed root certificate authority
- Purchase certificate from VeriSign

LDAP Servers

- MaXware Virtual Directory
- Windows 2000 Active Directory
- OpenLDAP
- directory.verisign.com
- Lotus Domino R5.0.8
- iPlanet LDAP 5.0

Messaging Servers

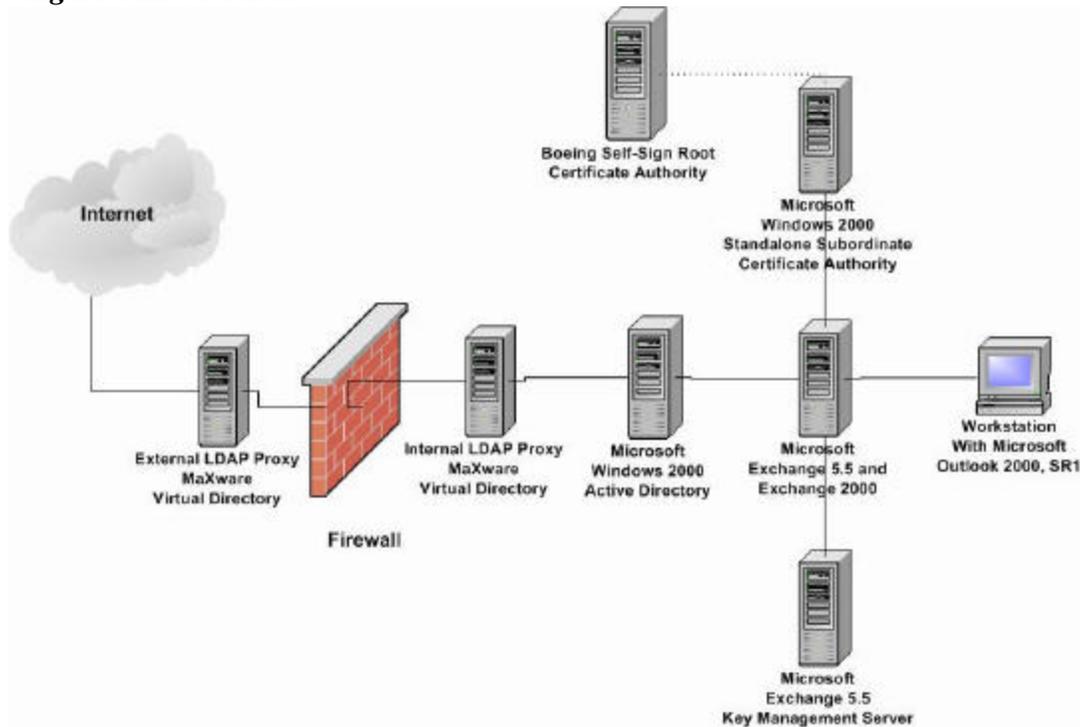
- Lotus Domino R5.0.8
- Microsoft Exchange 5.5/2000
- SendMail 8.11.0

Messaging Clients

- Microsoft Outlook Express
- Microsoft Outlook Express (International)
- Microsoft Outlook 2000 SR1 (International + Security Patch)
- Microsoft Outlook 2000 SP2
- Lotus Notes R5.0.8

Challenge Test Environment

Boeing Test Environment



Certificate Servers

- Root CA—iPlanet CMS 4.1 on Sun Solaris 8 system as the Boeing test self-sign root CA
- Subordinate CA—Microsoft Windows 2000 server with Certificate Service, which is based on the Microsoft Exchange Key Management Server's technical requirement (this Windows 2000 CA server is configured as a stand-alone subordinate server)
- Microsoft Exchange 5.5 SP3 Key Management Server configured for X.509 v.3 certificates

Directory Servers

- Microsoft Windows 2000 Active Directory, answers LDAP query on standard TCP port 389
- MaXware Virtual Directory serves as an LDAP proxy

Messaging Servers

Two different deployment sites:

- Microsoft Exchange 2000 Server deployed in one site
- Microsoft Exchange 5.5 SP3 Key Management Server deployed in one site

Messaging Client

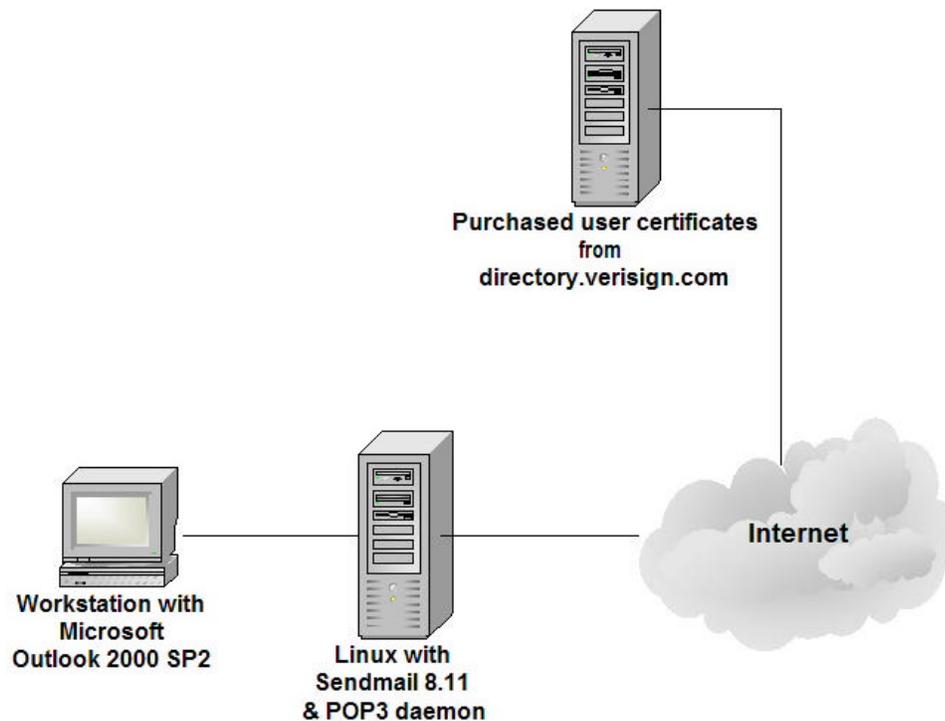
- Microsoft Outlook 2000 SP2

Internal and External LDAP Presence

A pair of LDAP proxies is deployed as the internal and external LDAP presence on Microsoft Windows NT 4.0 SP6 with the MaXware Virtual Directory. The LDAP proxy is script driven for multiple functions.

- *Incoming LDAP query*—External LDAP proxy only accepts and forwards queries with valid Boeing email address to the internal LDAP proxy. The internal LDAP proxy retrieves LDAP entry and limits query results to only three attributes, common name (cn), user's email address, and user's certificate. The query results will be sent back via the external LDAP proxy.
- *Outgoing LDAP query*—The Boeing user connects to the internal LDAP proxy to query for non-Boeing email recipient's certificate. The query gets forwarded to the external LDAP proxy for lookup. The external LDAP proxy stores a list of email domains, their corresponding directory server, and the required search parameters. The external LDAP proxy will determine where to get the certificate based on the email domain of recipient.

SMTPTTESTBED.COM Test Environment



Certificate Server

- No in-house certificate server. All certificates used in this testing are the class 1 certificates purchased from VeriSign's Web site <<http://www.verisign.com>>

Directory Server

- No in-house directory server. All certificate purchased from VeriSign are published and available for query from VeriSign's directory server at directory.verisign.com.

Messaging Server

- SendMail 8.11.0 running on Red Hat Linux 7.0. The SendMail is configured for a single domain—smtptestbed.com—email purpose.

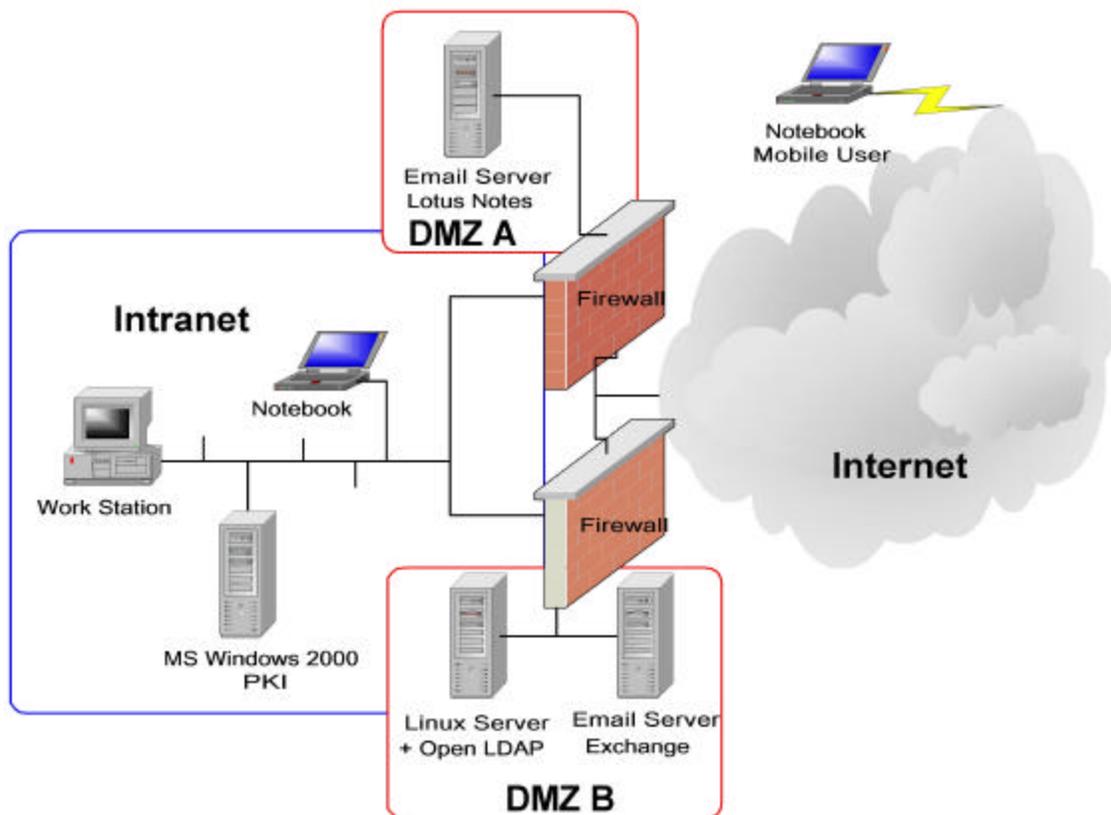
Messaging Client

- Microsoft Outlook 2000 SP2

Lynx Consulting Group Test Environment

The following documentation describes configuration, administration and usage of the secure email systems installed by Lynx-ctr GmbH as part of the Secure Messaging Challenge. The information serves as an implementation guide and to improve the understanding of the technology and systems.

Lynx-ctr GmbH system architecture is pictured below.

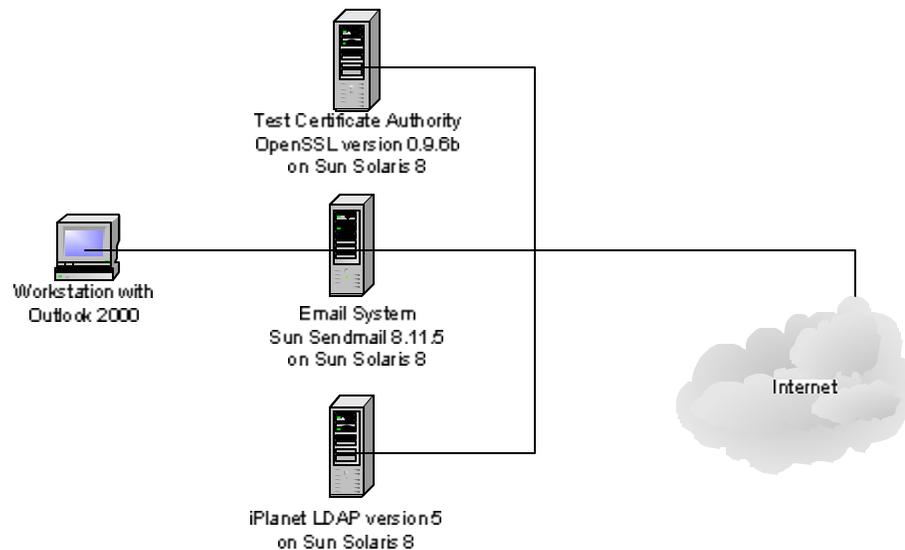


The systems consist of the following components:

- Microsoft Windows 2000 Certificate Server
- Microsoft Exchange 2000 Messaging Server
- Open LDAP Directory Server
- Lotus Domino 5.0.8 Application Server
- Microsoft Outlook 2000 Clients
- Lotus Notes 5.0.8 Clients

SEWP.NASA.GOV Test Environment

SEWP.NASA.GOV Test Environment



Certificate Server

- Self-signed test certificate authority system with OpenSSL 0.9.6b on Sun Solaris 8

Directory Server

- LDAP directory system with iPlanet LDAP version 5 on Sun Solaris 8

Messaging Server

- Email server with Sun Solaris 8.11.5 on Sun Solaris 8

Messaging Client

- Microsoft Outlook 2000

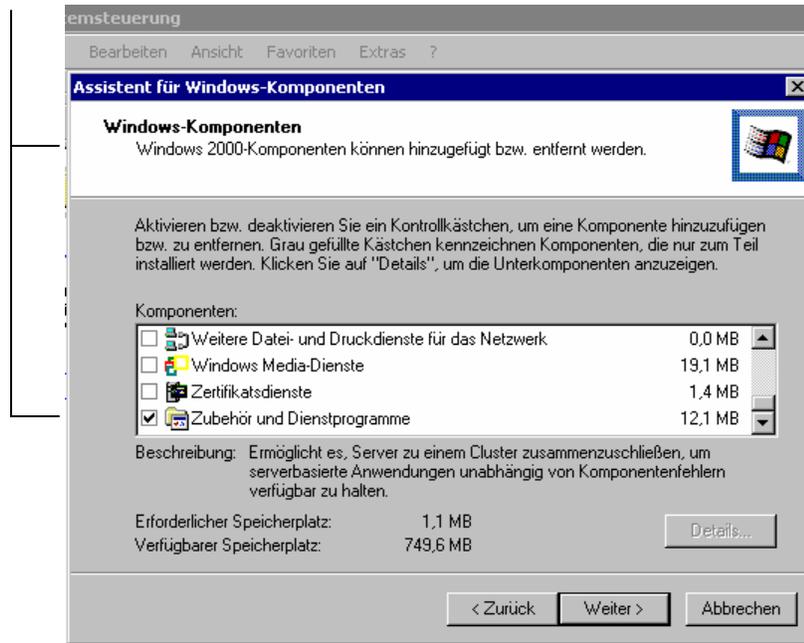
Configuration of the Microsoft Windows 2000 PKI

This part of the document describes the installation and configuration of a Microsoft Windows 2000 PKI. The PKI is contained in the program package of the W2K Advanced server. The PKI was used in an environment without Active Directory. If one were to use this PKI with Active Directory, only the display of the certificates changes. In an Active Directory environment the certificate would be issued automatically by the request for the certificate. Logging in automatically authenticates the user into the domain. If one would like to use the PKI outside an Active Directory environment, the administrator can decide to issue the certificate manually or automatically.

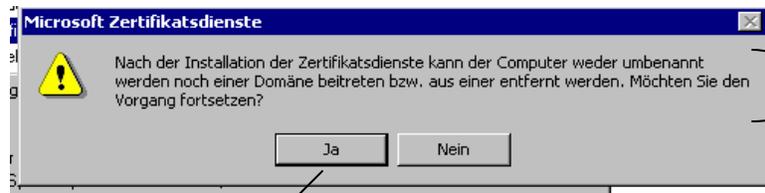
Installing ++PKI

For the CA server to issue a certificate meeting the minimum key length requirement of the Challenge (1024 bits), the CA server certificate must have that or longer key length.

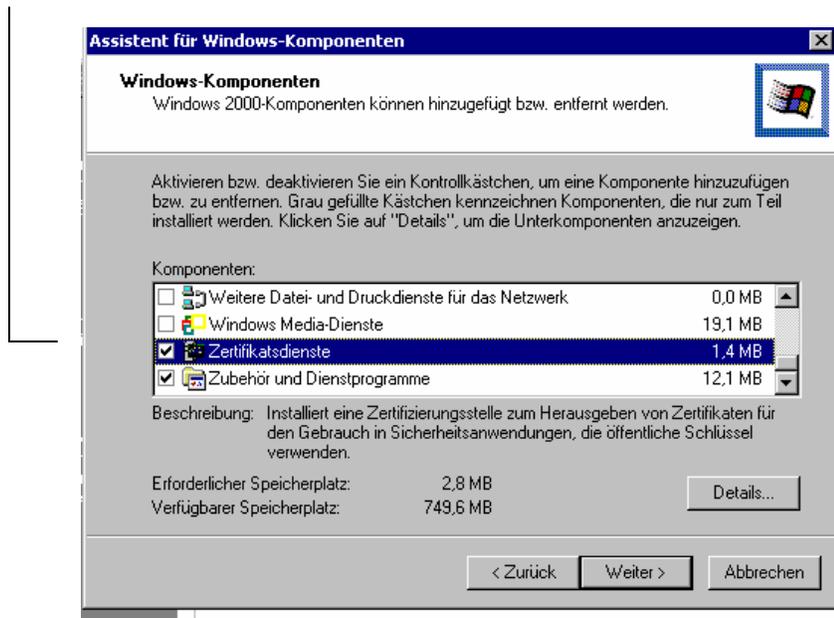
After installing and configuring the Windows 2000 Advanced server, an administrator can add a CA:
Step 1 Select **System control -> Software -> Add/ Remove Windows components**



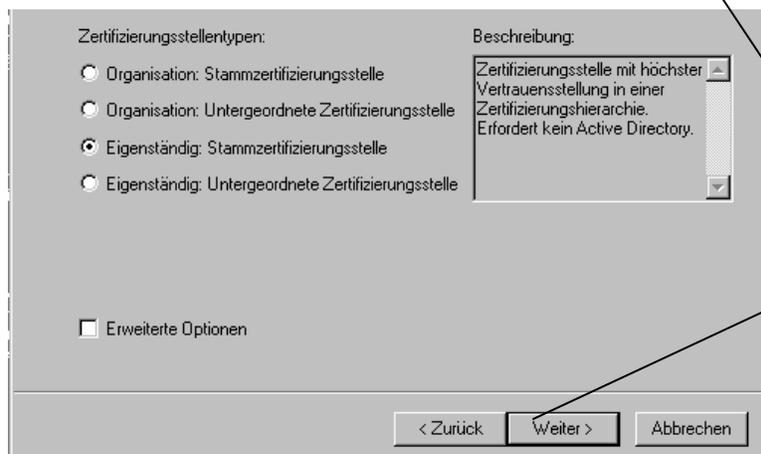
The administrator selects the certificate services and gets the following message:
“After installing the certificate services the computer cannot be renamed nor can a domain be joined or removed. Would like you to continue the occurrence?”



This message is confirmed with **yes** and the administrator sees a checkmark in the Certificate Authority box.



To install the certificate services, the administrator clicks on **Next**.

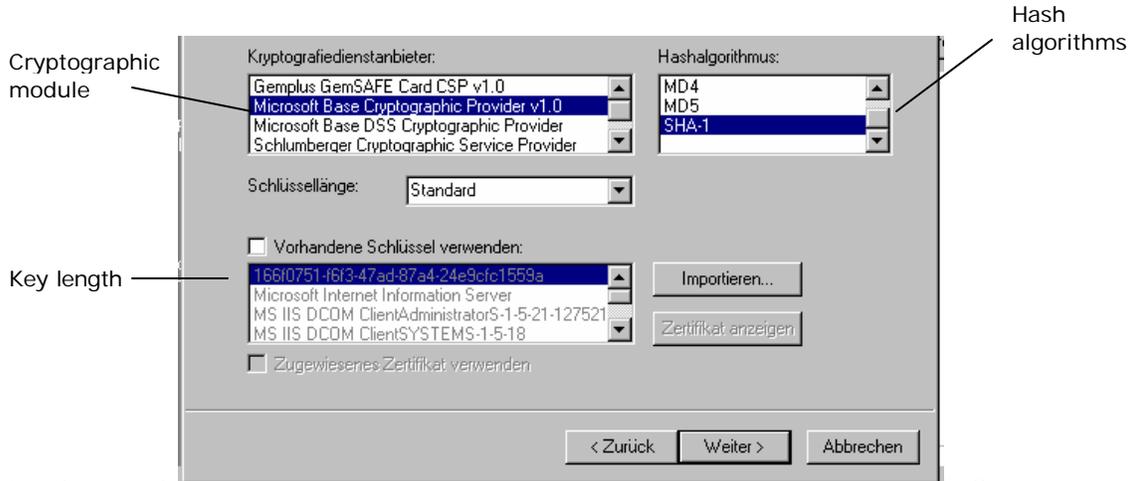


On the next screen, the administrator can select the features of a CA to install:

- Root Certificate Authority
- Subordinated Certificate Authority

At this screen, one can also select to operate the CA within an organization, under use of Active Directory, or as an independent CA.

Before proceeding further, one should click on the expanded option button. There one can select the **Cryptographic module**, the **Hash algorithms** for the certificate of the CA and most important the **key length**. Also one has the possibility to bind to an already available certificate (of a trusted organization).



After choosing the key length and the algorithm, a page comes up on which one can specify CA more closely.



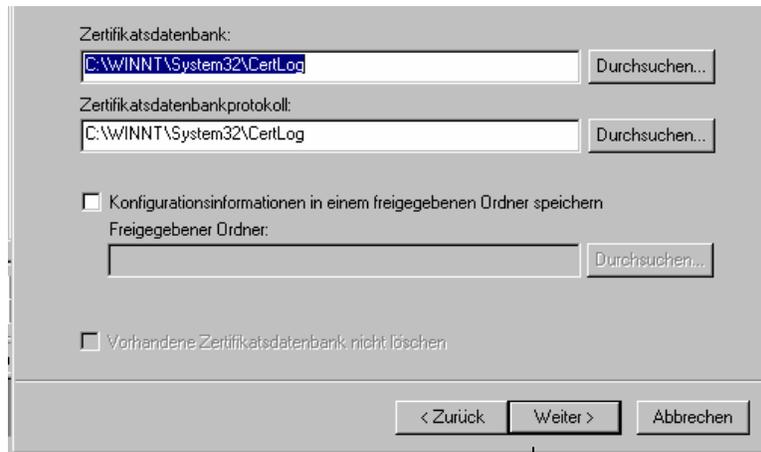
On that page one enters the following information:

- CA name
- Name of the organization responsible for the CA
- City, state and the country of the organization
- email address of the CA

In addition, one can indicate a short description of the Certificate Authority. If constructing a root CA, one must indicate expiration or the validity duration of the CA certificates. In constructing a subordinated CA, the root CA determines the validity of the subordinate CA certificates.

- Step 1** Confirm requests by expanding the window
- Step 2** Determine the storage location of the certificates in the next window

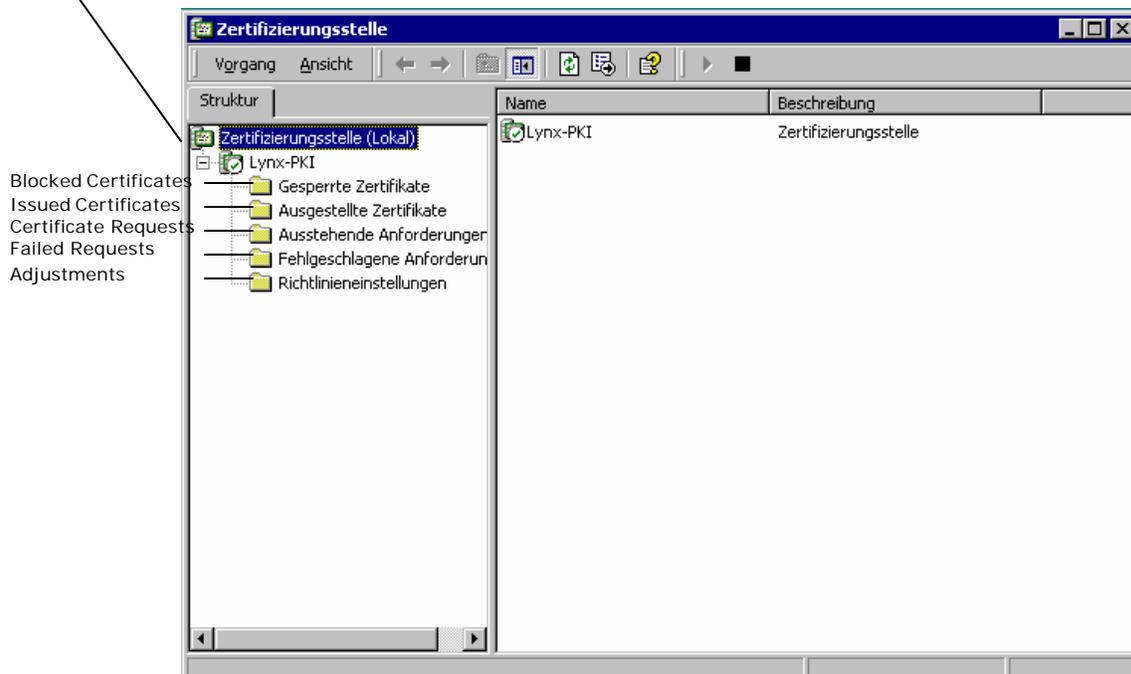
One can use the default certificate storage Microsoft provides or specify a certificate database at another storage location.



With the final click on **Next**, one configures the Certificate Authority, generates the accompanying certificate, and stores it in the certificate storage indicated previously.

Configuration of the Certificate Authority

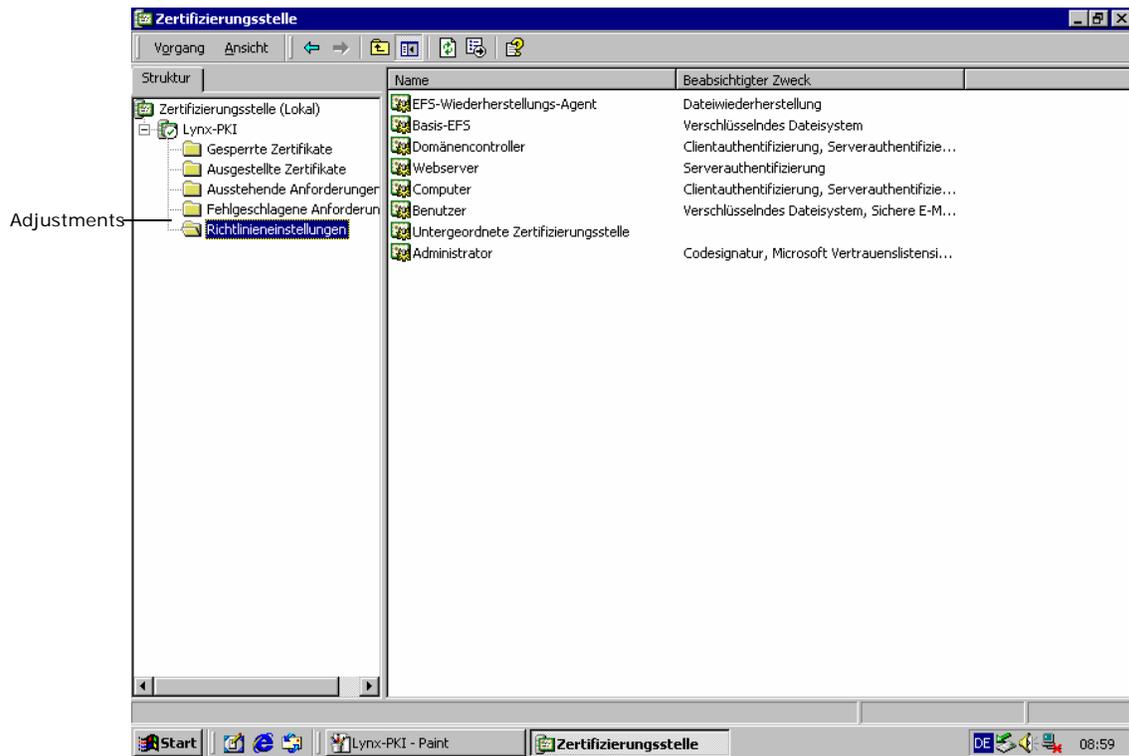
Once one has installed the Certificate Authority, one can start it under **Start -> Programs -> Administration -> Certificate Authority**.



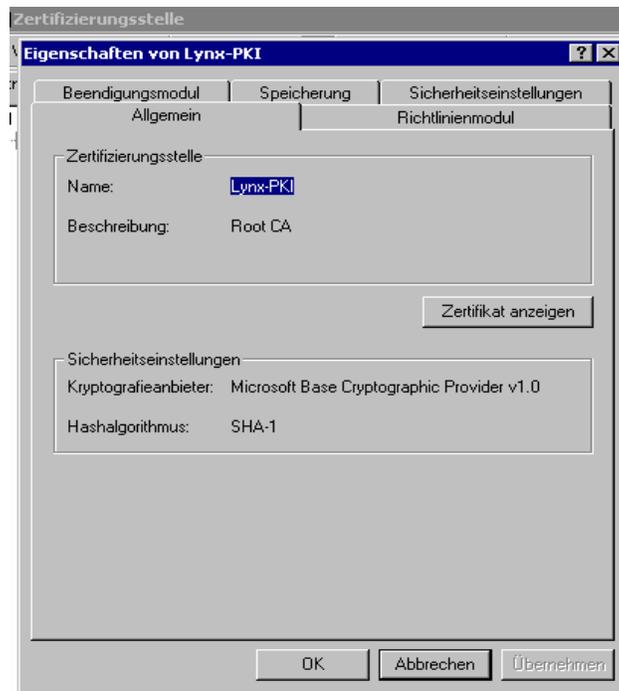
At this screen, one has different selection possibilities:

- “Blocked Certificates” folder—Blocked Certificates with the reason for the block (if a reason is indicated)
- “Issued Certificates” folder—Certificates the CA issues
- “Certificate Requests” folder—If a CA is configured without Active Directory, the CA administrator must issue the certificates
- “Failed Requests” folder—Requests that were rejected for any reason
- “Adjustments” folder—Guidelines for adjusting the CA

Mark the adjustments on the Certificate Authority folder and then right click.



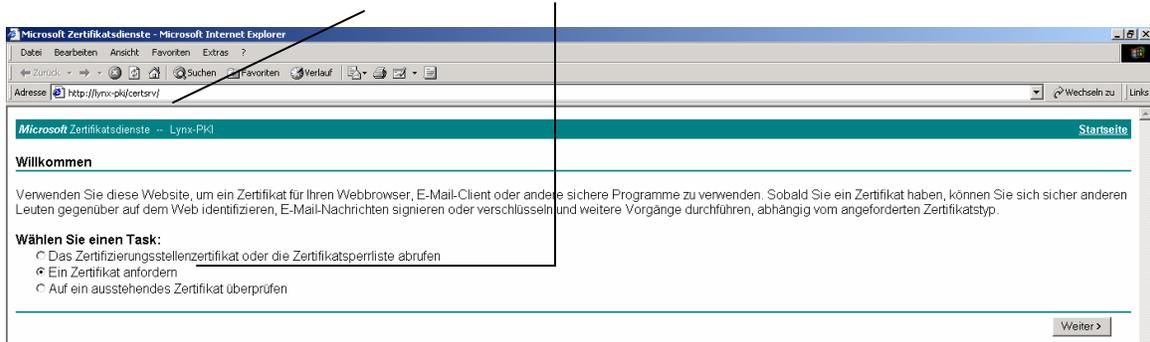
A new window will open where you can choose the desired adjustments of the PKI.



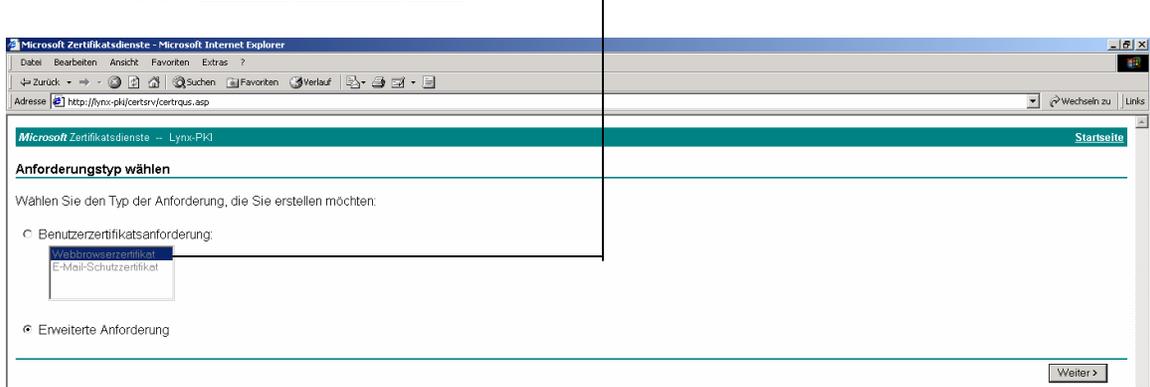
Certificate Request

The request of a certificate takes place via Web browser by opening the URL <http://lynx-pki/certsrv>.

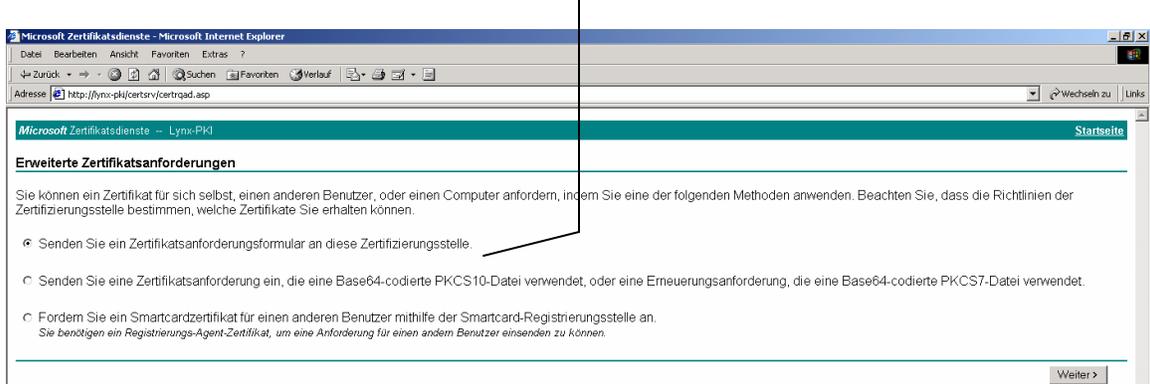
When the window is open, **select request** a new certificate.



On the next page, **select expanded requests**.



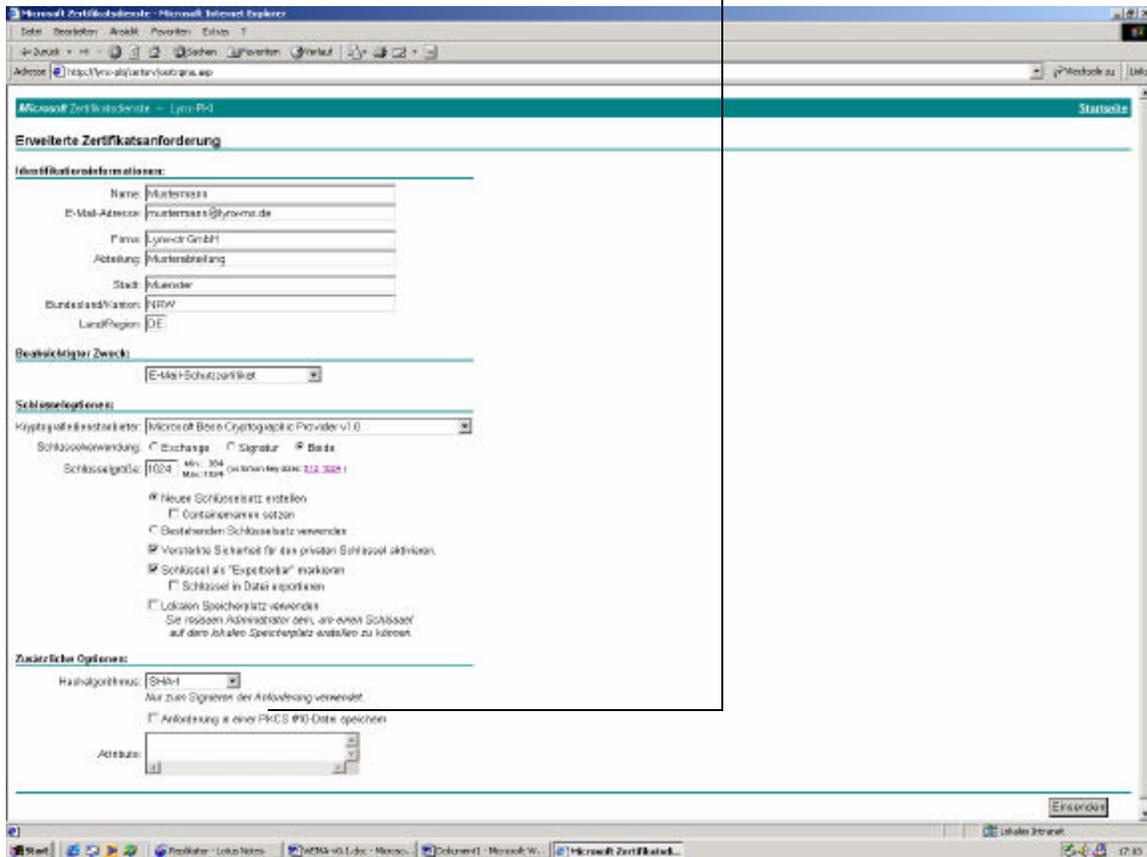
After that **click "Send a Certificate Request"** to this Certificate Authority.



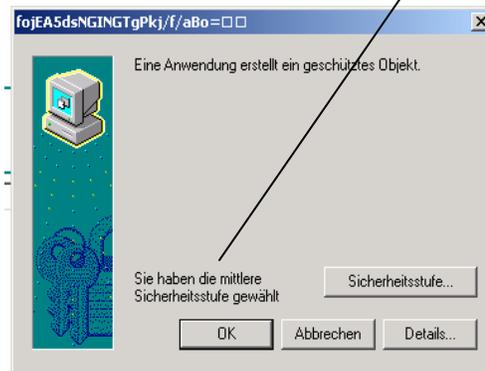
On the next page:

- Step 1** Input the user's data—Purpose for the certificate is an email protection certificate
- Step 2** Select the key options—OK to select the default key provider
- Step 3** Set the key length on 1024-bit to enable the tightest security
- Step 4** Generate a new key pair that activates the enhanced security and is marked “for export”

Note: The key is not exported into a file, but rather stored in the certificate. Lotus Notes can bind to this. In the additional options, SHA-1 must be adjusted as a Hash algorithm before submitting the request.

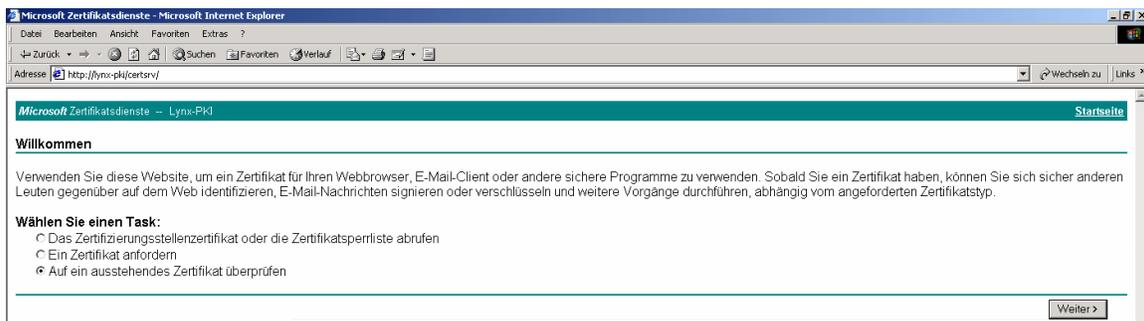


After pushing the Send Button, a message appears that the middle security step was selected.



ren.

Set the security step on high. After sending the request to the server, the extensive security examinations (see also CP and CPS) are fulfilled and the certificate is issued to the certificate requester. To pick up the issued certificate, go to <http://lynx-pki/certsrv/>, where the outstanding certificate is marked.



- Step 1** Select Next—User sees all the requested certificates that have been issued
- Step 2** Select the appropriate certificate
- Step 3** Go to “install this certificate”—Installs automatically in the certificate storage of Microsoft Windows 2000

Microsoft Outlook 2000

Configuration of Microsoft Outlook 2000 for Email Encryption and Digital Signature

The information in this section refers to Microsoft Outlook 2000 with the Security Patch for 128-bit encryption.



Microsoft Outlook client configuration is divided into two steps:

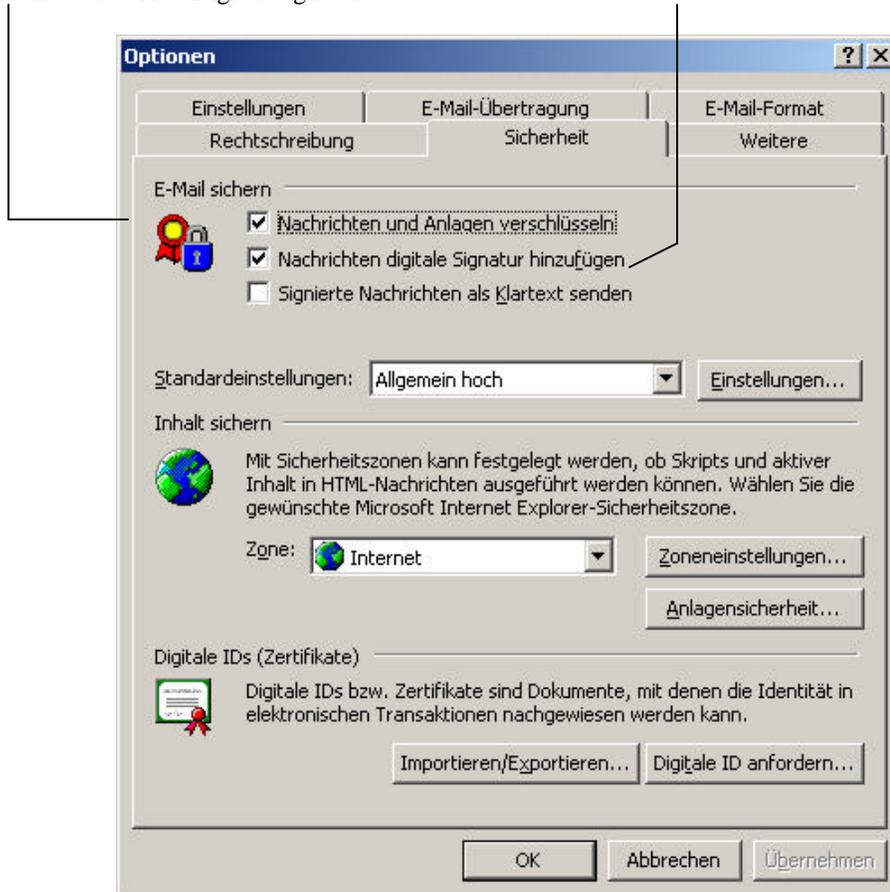
- Configuration of the optional settings
- Configuration of the directory services

This section does NOT deal with the configuration of the email account, since no changes were made from the standard configuration.

Configuration of the Optional Settings

To be able to make the fundamental settings for the email encryption and/or digital signature, from the Outlook 2000 menu the user must select “Extras” and then “Options.” Subsequently, the following window opens, where the “Security” tab is chosen.

If one wants to encrypt and sign email messages, then click on the check boxes “Encrypt content and attachments” and “Add Digital Signatures.”

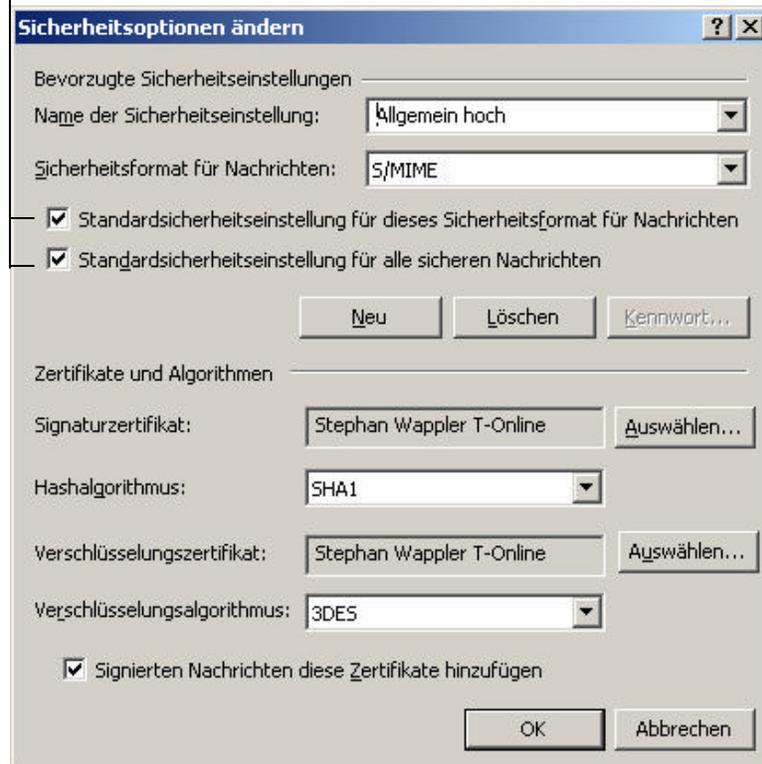


Subsequently, one selects “Settings,” which opens a new window. In this window one specifies the preferred security attributes.

- Step 1** Assign another name and, thus, administer several different settings
- Step 2** Specify the security format for the messages S/MIME must be selected

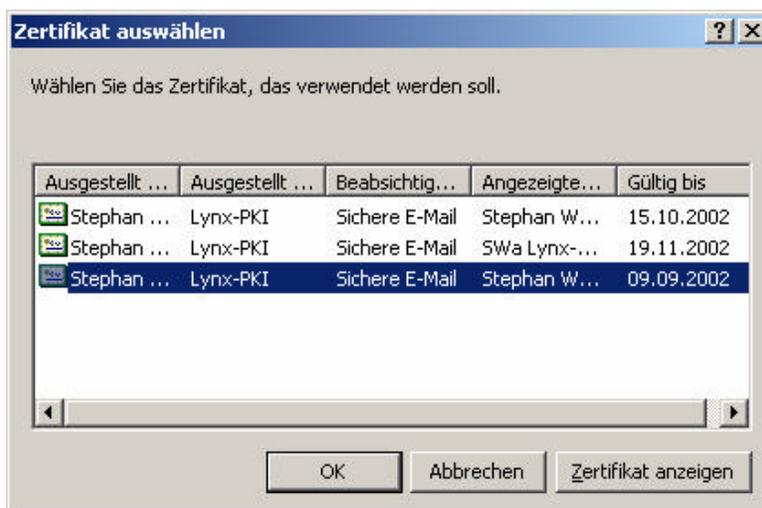
Step 3

Click the next two check boxes if this will be the standard attribute for all future email messages



The selection of the certificates and algorithms is very important. One must proceed carefully, because it is possible to enter conflicting or inconsistent settings.

First, the signature certificate is selected. The selection is made from the Microsoft certificate database and it becomes the personal certificate of the user whenever the user is indicated to have possession of the private key (i.e., whenever the user signs a message).

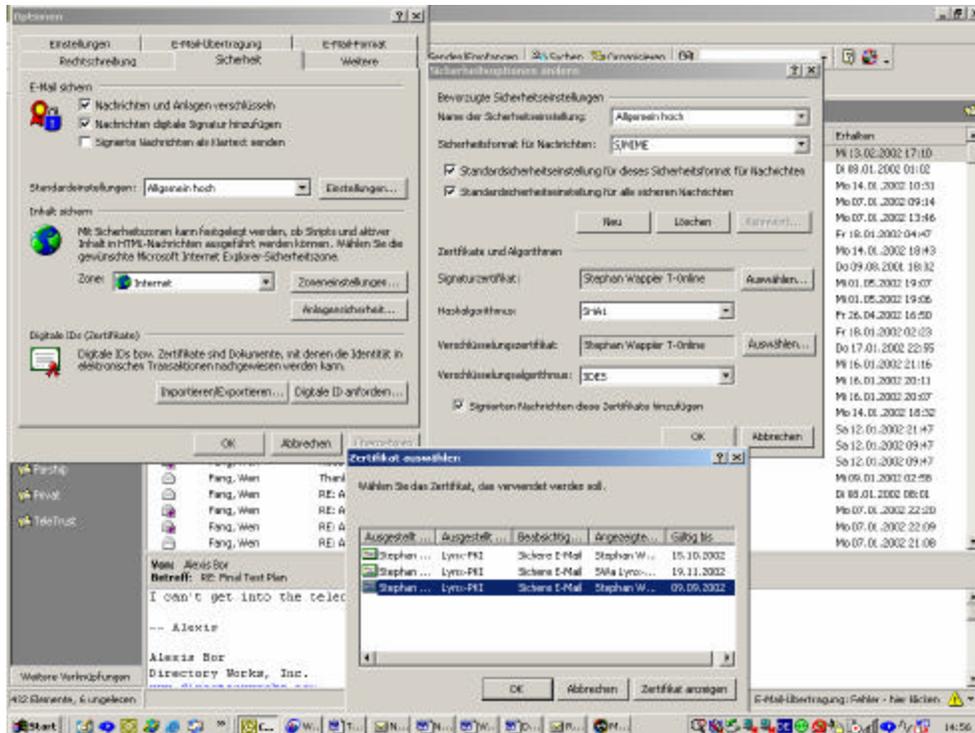


If you have a choice between different certificates for the basis of key division for different applications, then you should look at the corresponding certificate and the intended purpose one more time, before making the final selection.



Subsequently, the hash algorithm is specified. Selecting the SHA-1 algorithm and not the MD5 is recommended. After making these settings, each outgoing email could be signed digitally.

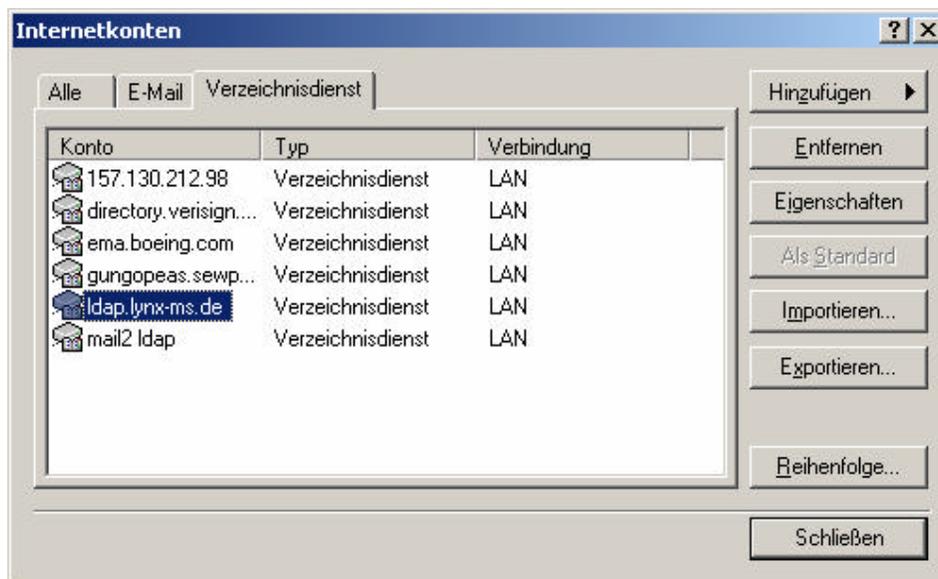
Next the user can select the encryption certificate. This is important even if the last check box “Add these certificates to signed email” is clicked. The advantage with this approach lies in the fact that the email recipient, who may not have access to the LDAP system or may have other difficulties (see Lotus Notes Work Around), can send encrypted email because this is the form in which they come into the encryption certificate. Encryption certificate selection corresponds to signature certificate selection.



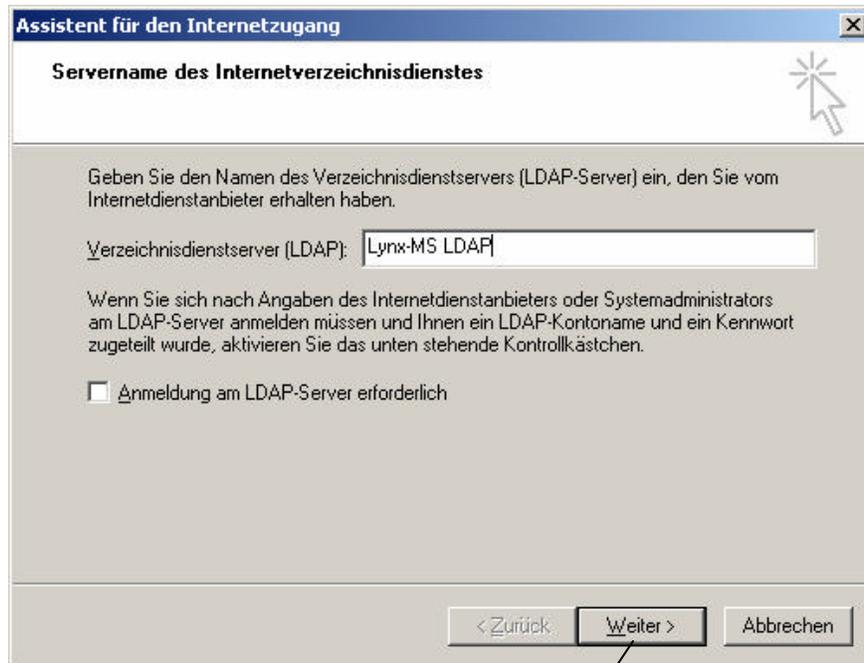
The final and important point of selection is defining the symmetric encryption algorithm. Here the 3DES algorithm should be selected to ensure interoperability with other email systems.

Configuration of the Directory Services

To be able to retrieve the message recipient's current certificates from the directory server, the directory services must be configured in the Client. To make this configuration, select "Extras" and then "Accounts" from the menu, which opens a new window with the name "Internet Accounts."



One selects the "Add" button and points to "Directory service." Subsequently, an assistant is started, which opens a new window, as the name of the directory service must be entered.

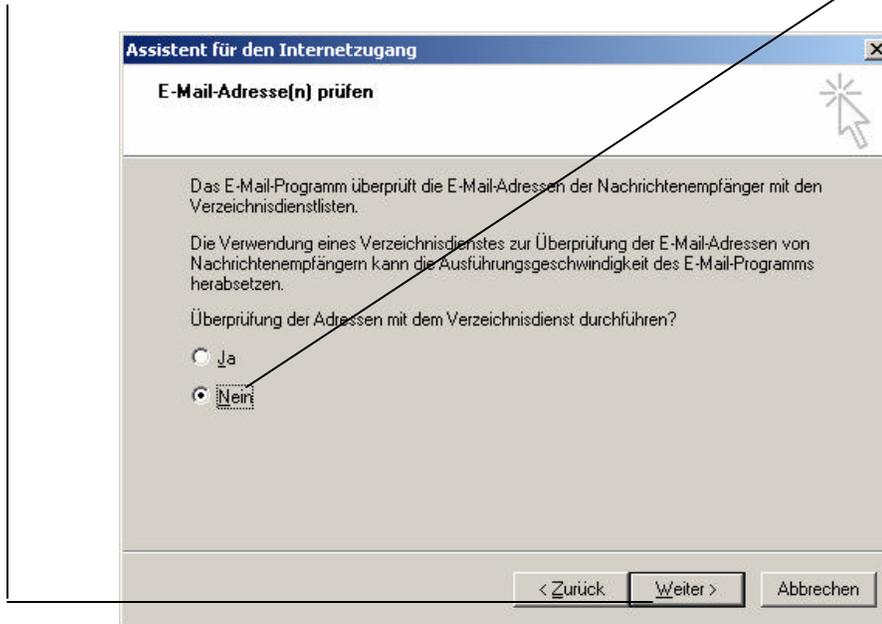


After registering the name, one selects the “Next >.”

As seen in the screen, an error message may appear indicating that the name does not correspond to the Internet conventions. Because reconfiguring the listing data is necessary anyway, one can confirm the selected name.



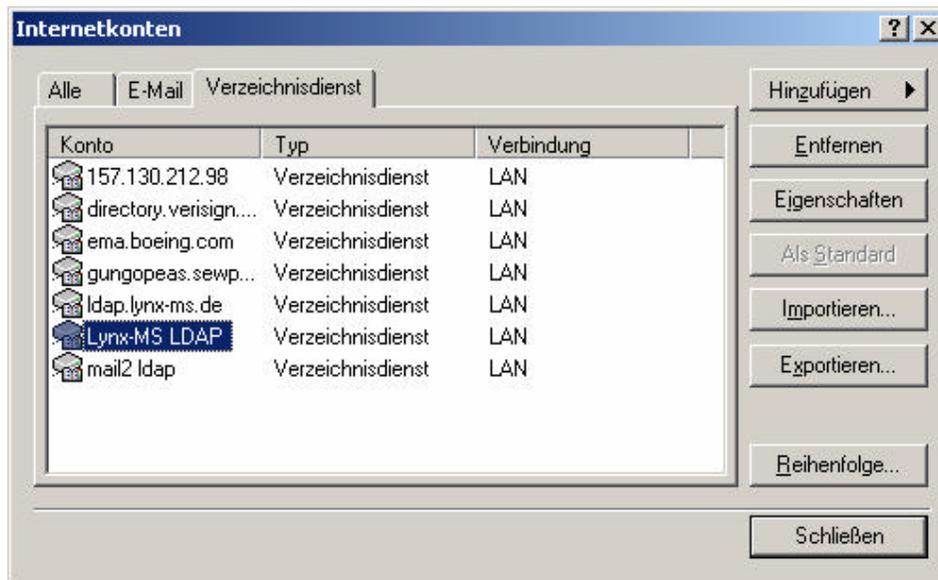
Then a new window opens, as an examination of the email addresses entered by hand can be selected over the directory service. Because the email address is selected from the directory, select “No” and then press “Next.”



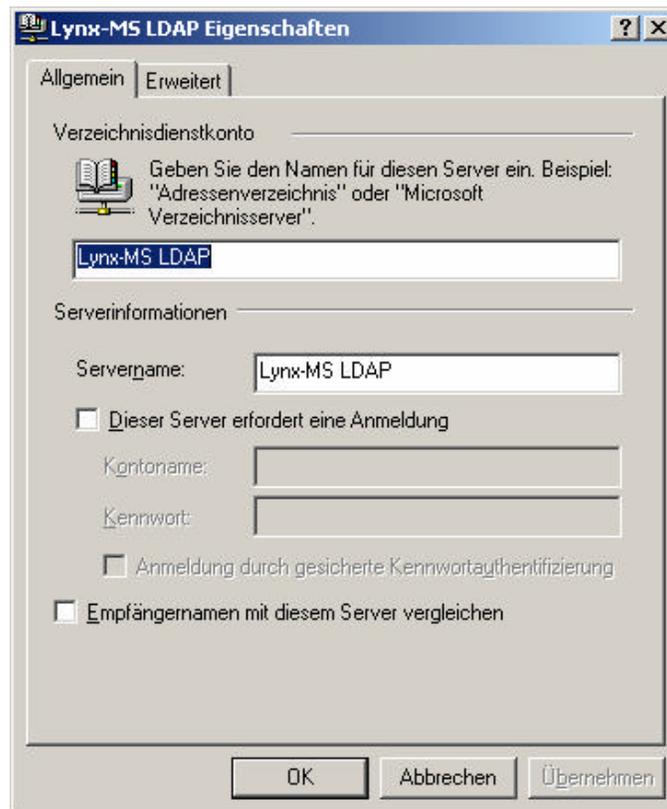
Thus, all inputs are made with the help of the assistant. To save the data, press “Save.”



Unfortunately, the assistant does not query all data, making a manual reconfiguration of the listing service configuration data necessary. Select the just saved entry, and double click to open the window “Internet Accounts.”



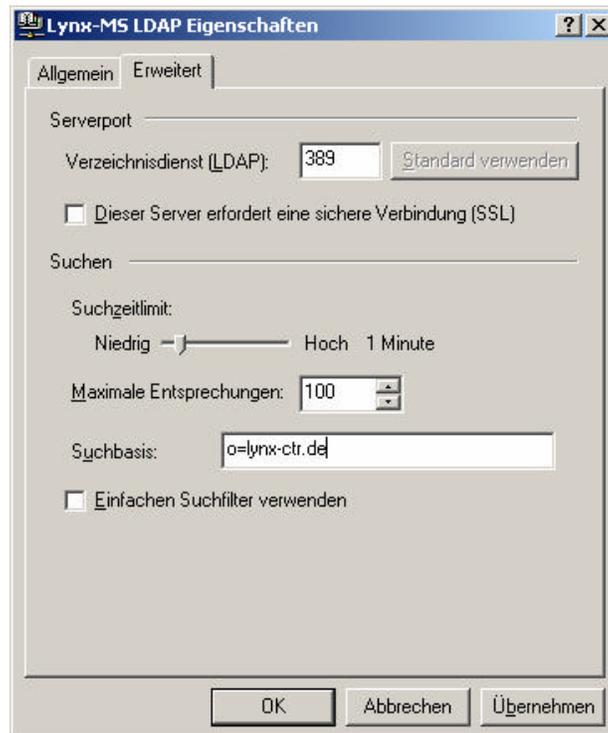
First, one must change the server name.



There are two possibilities for the server name entry. Either one may enter the Domain Name Service (DNS) name or the IP address.

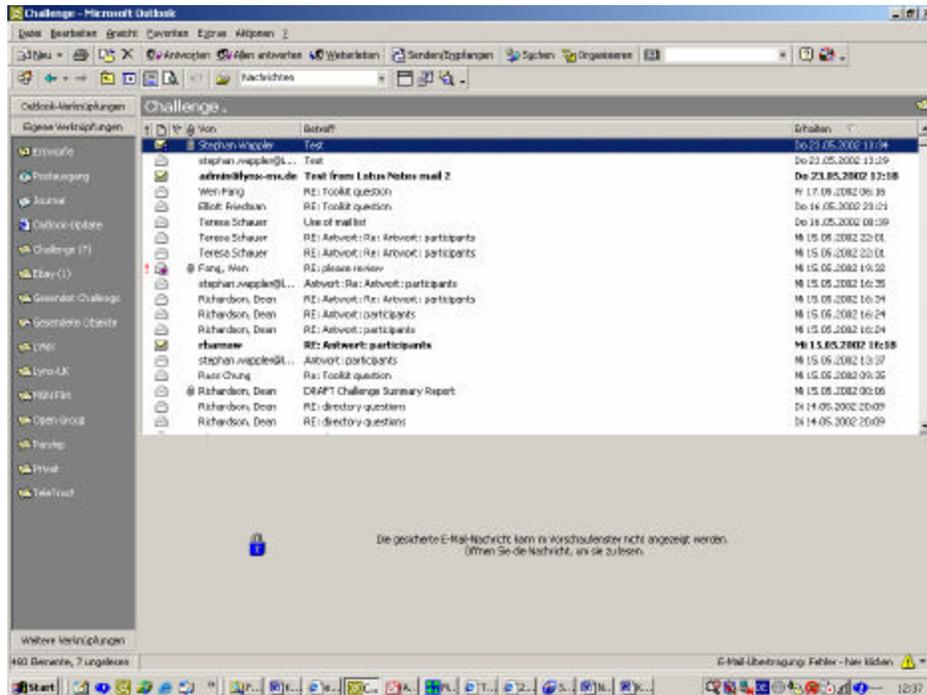


Subsequently, one selects the “Extended” tab to specify the port and the search root. If all entries were implemented correctly, click OK and the window can be closed and the data are stored. The directory service is now available for use.

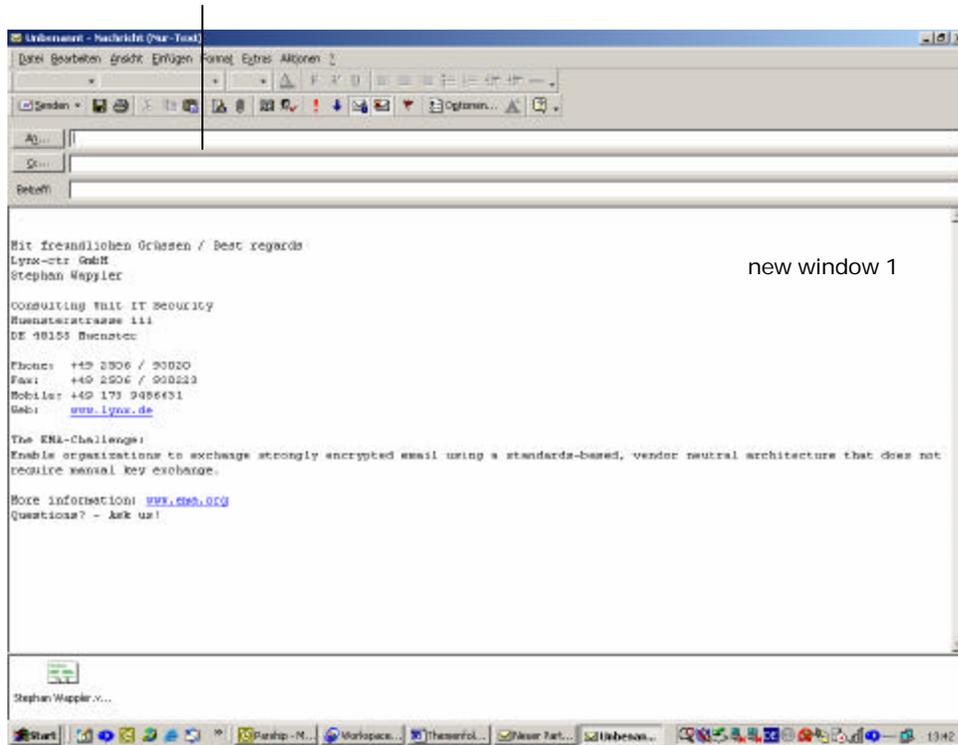


Sending an Encrypted and Signed Email

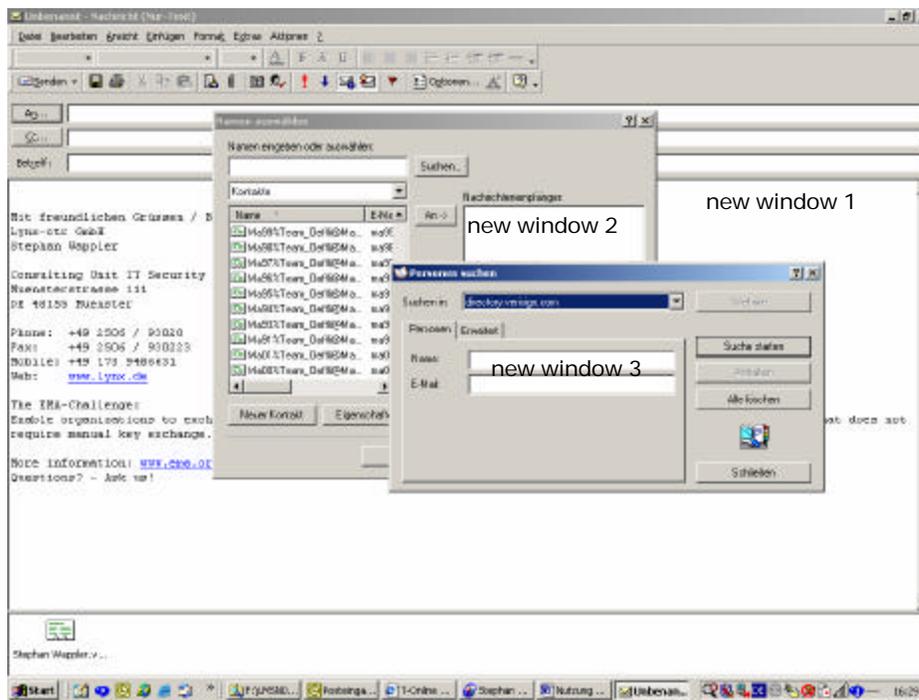
After a new email has been selected in MS Outlook, a new window opens in which the email can be written.



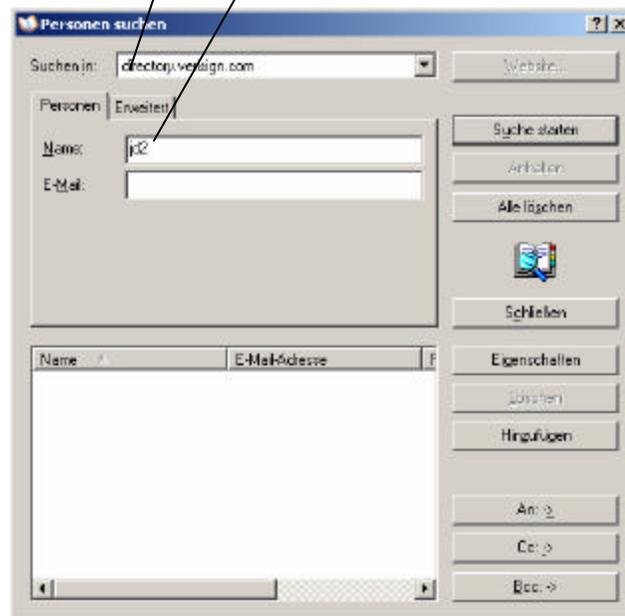
In this new window “to” is selected.

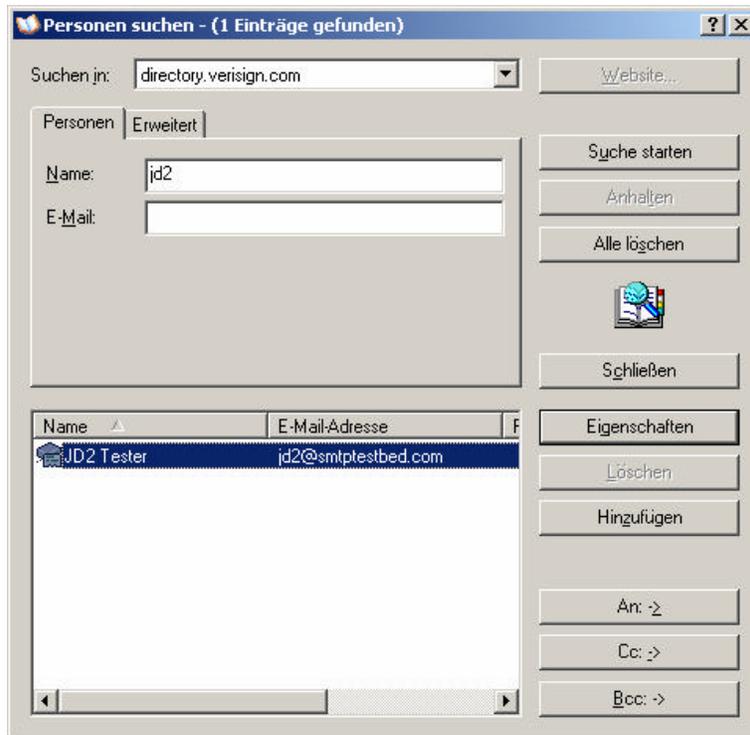


Afterward a new window opens again (new window 2), and the names can be selected from “Contacts.” However, in “new window 2” the choice of directory services also exists. Moreover when a person is selected, another new window (new window 3) opens.

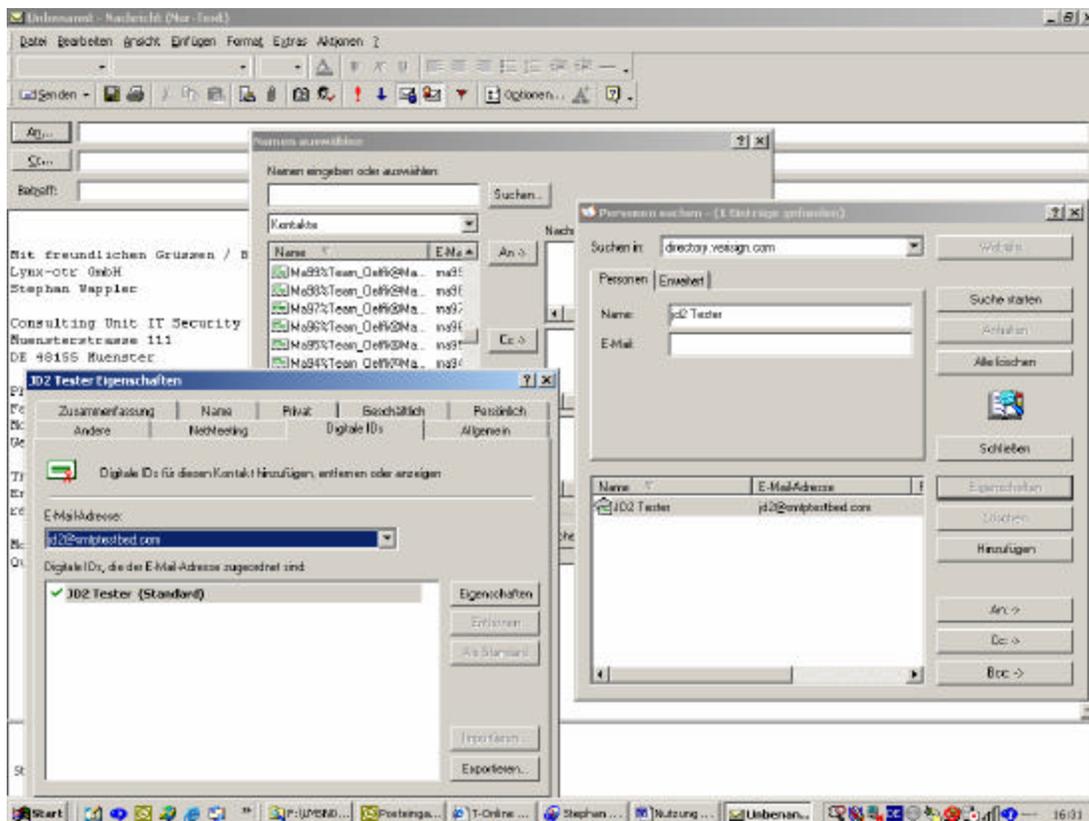


In “new window 3” the directory to search is selected. In the example, the directory directory.verisign.com was selected and was searched for the name jd2.

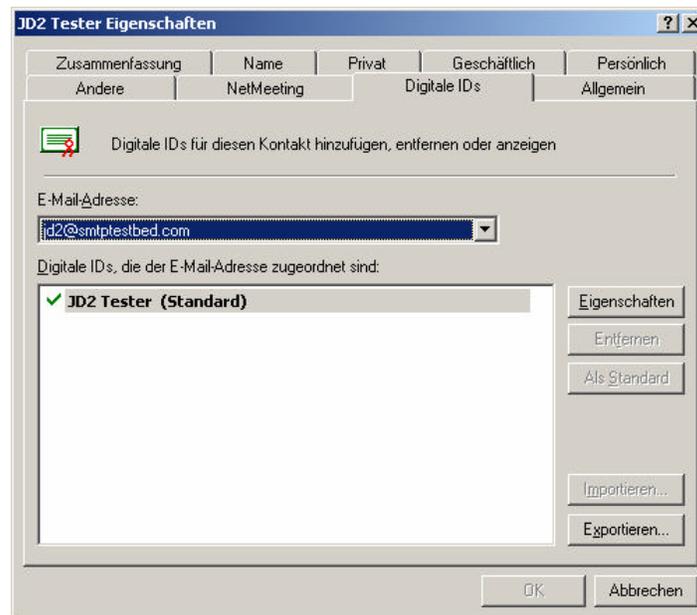




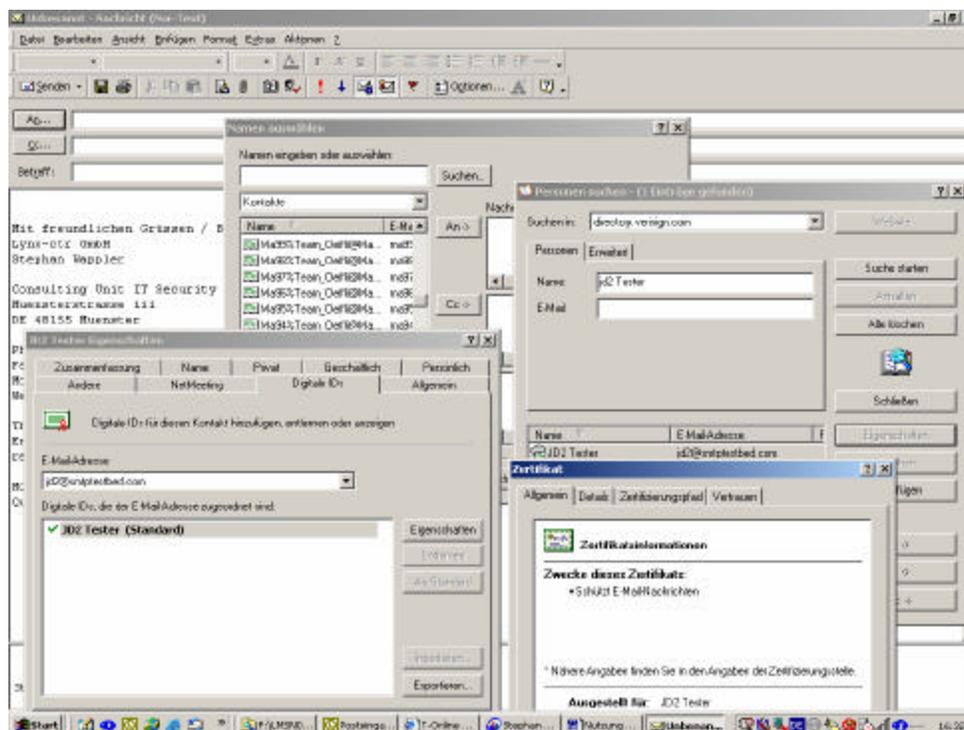
All found entries are indicated. Here one can look at the properties for each entry and check the digital ID.



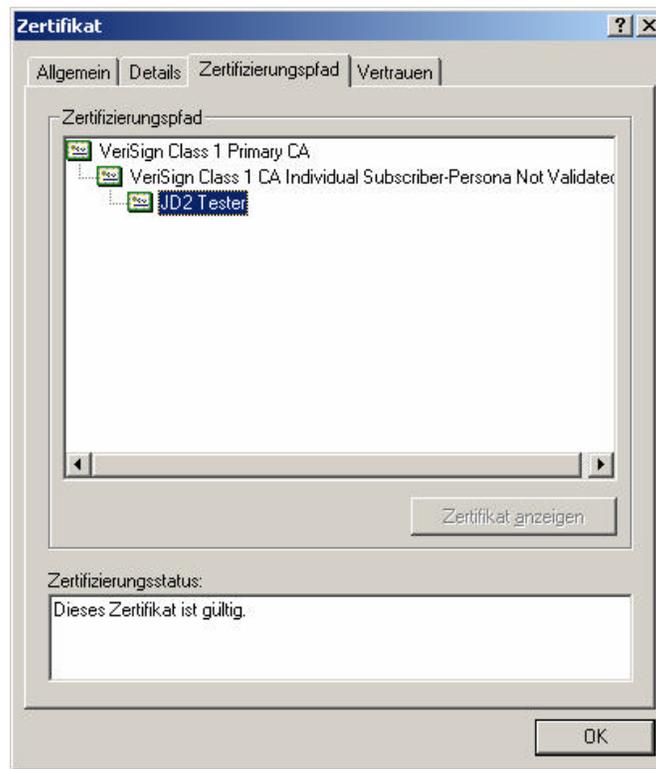
The following picture shows the email address and the associated digital ID in more detail.



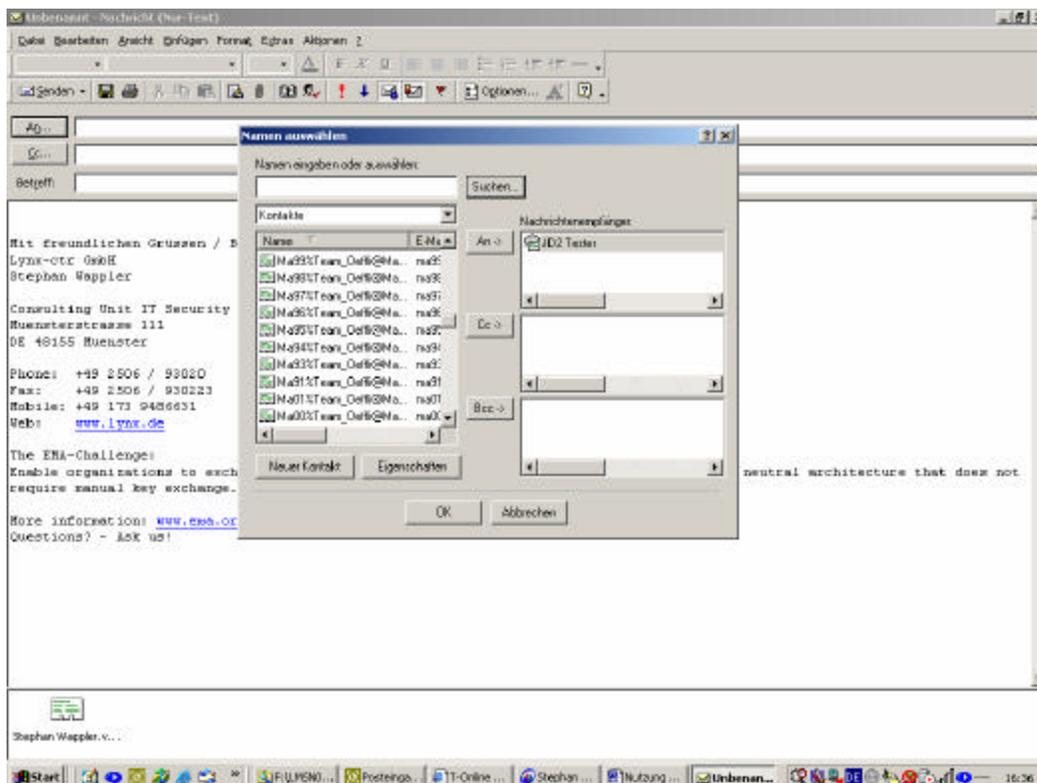
- Step 1** Select the digital ID
- Step 2** Push the badge properties
- Step 3** Examine the certificate to see
- If the root certificate of the issuing authority on the client is installed
 - If this certificate has a trust connection with the root certificate
 - If the certificate is indicated as valid



The following picture shows the trust path in more detail.

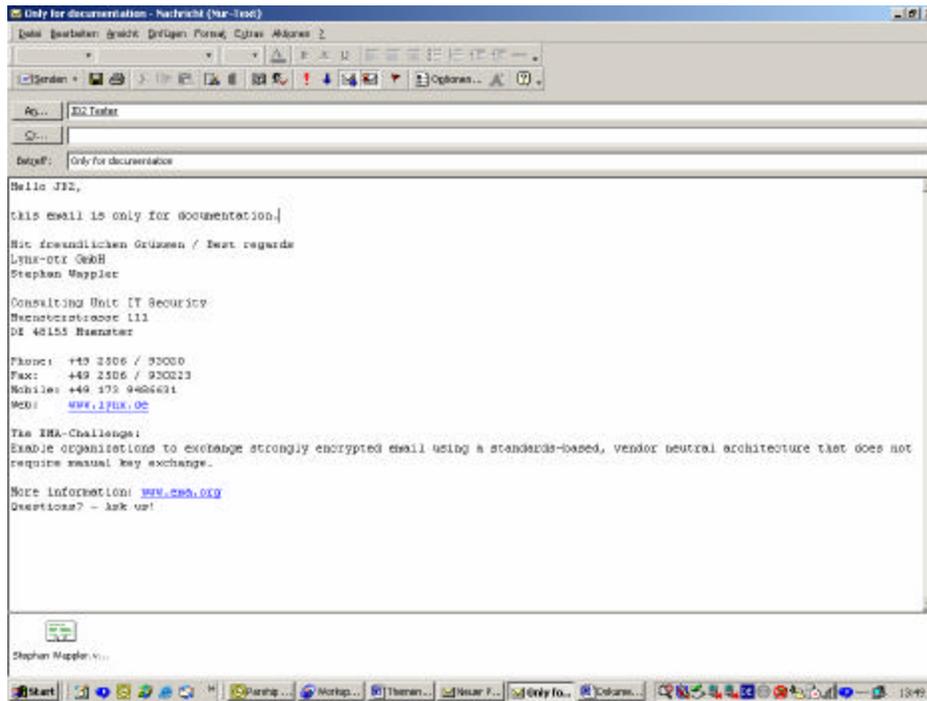


After the windows to the certificate properties and LDAP entries have been closed, one can take over the corresponding address or addresses as a new receiver.

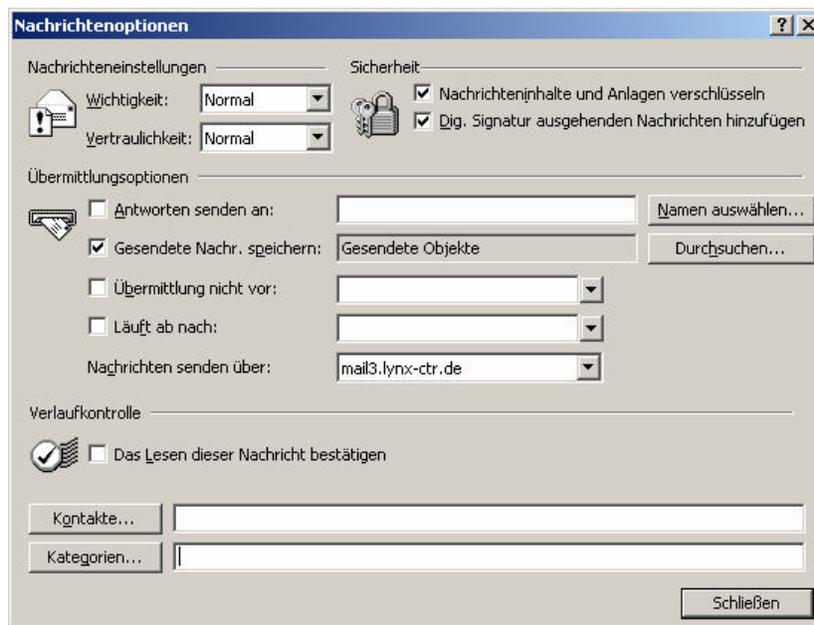


Then one can write the email in the same way as done previously.

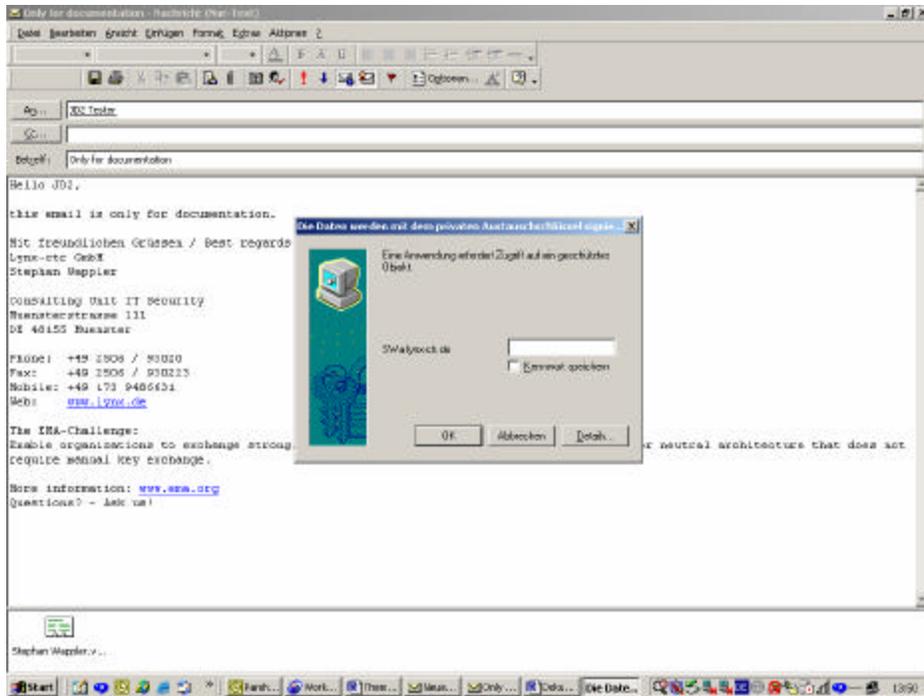
Text of
email
message



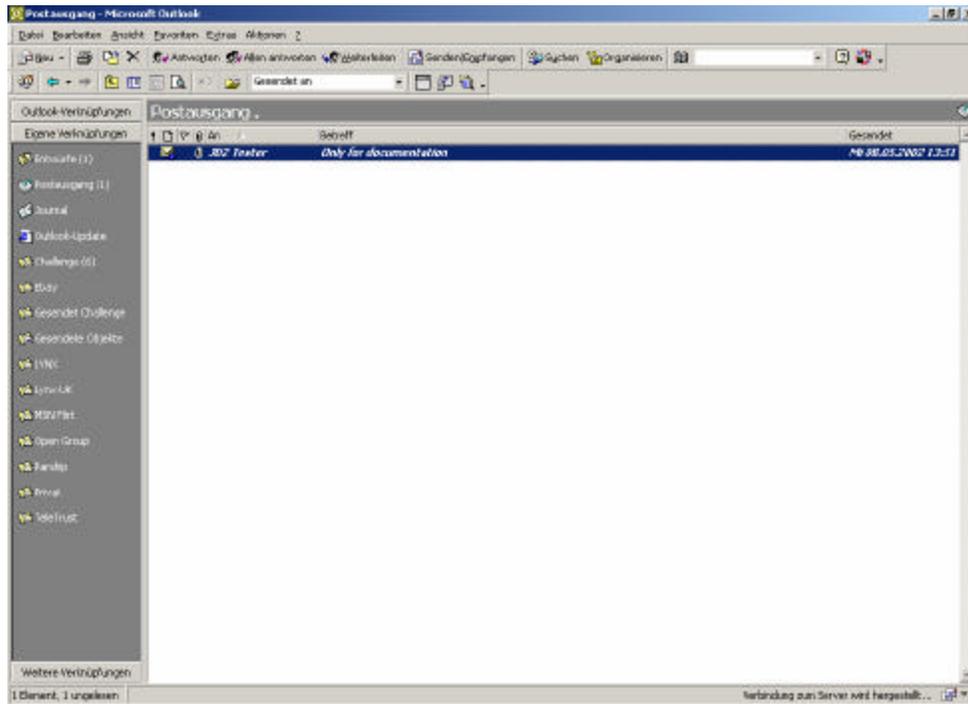
Before sending the email, the email options should be checked one more time or be adapted. The content and attachment encryption must be marked, as must the option to add a digital signature to the email.



If you have selected to add a signature and your private signature key is protected with a password, then you will be requested to input the password before you can send the email.



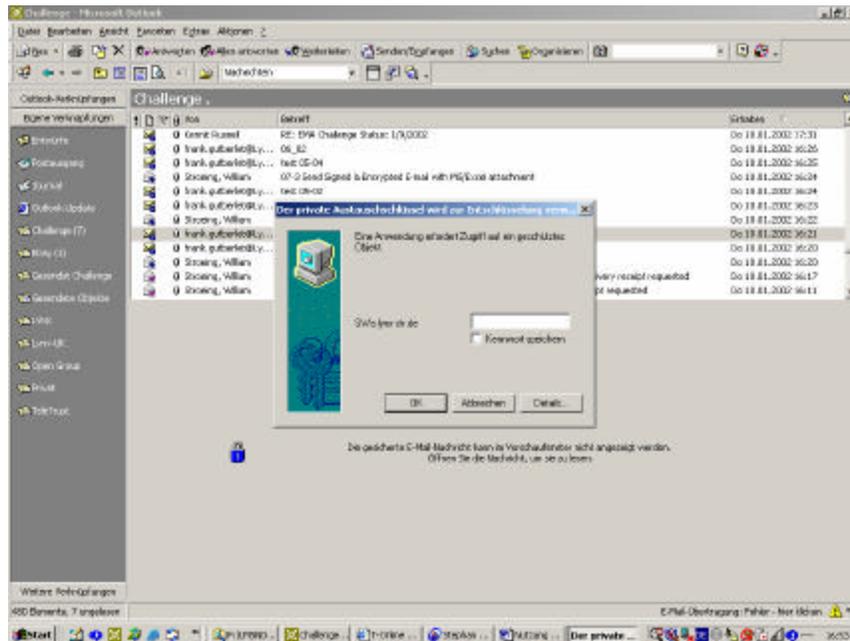
Then only with a correct input, the email is also encrypted and sent signed. In the outgoing mail an envelope with a blue castle represents an encoded email.



Opening and Reading an Encrypted and Signed Email

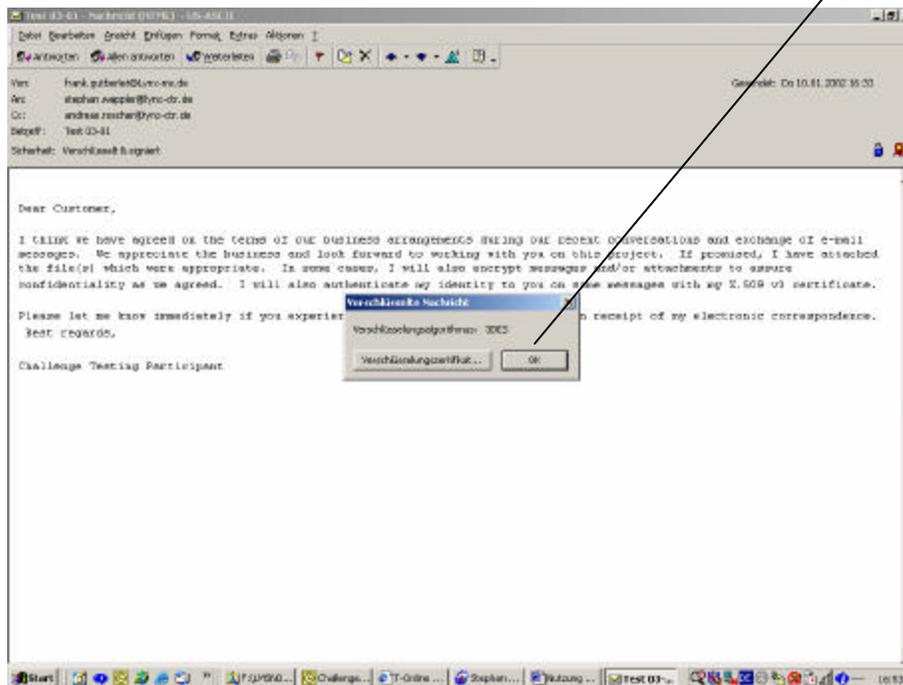
You can recognize an encrypted email by the fact that MS Outlook is not able to represent the email in the preview window.

- Step 1** Double click to open the email
- Step 2** Provide the password selected to protect your private key

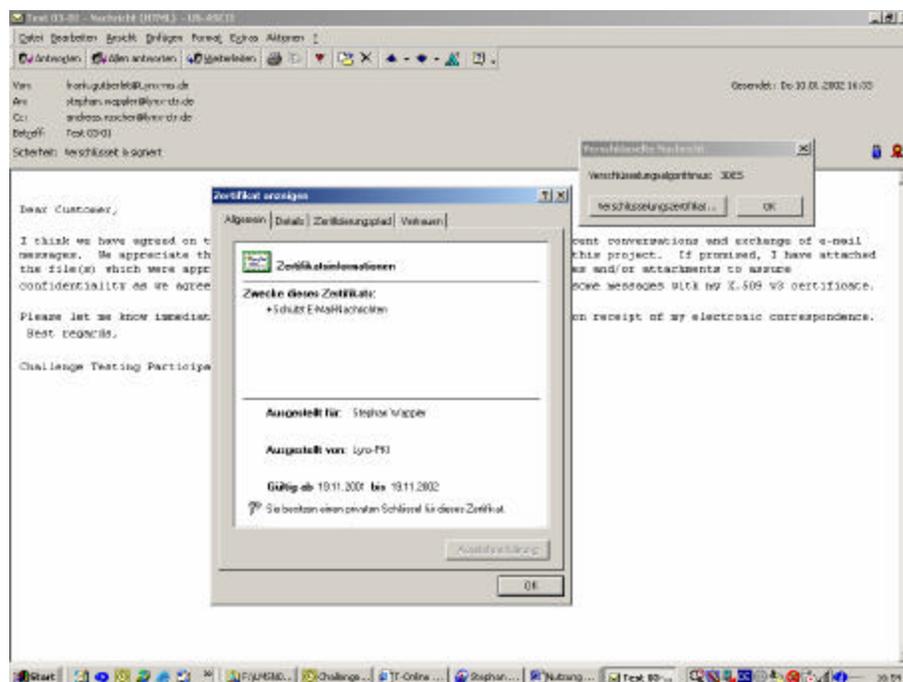


- Step 3** Click OK to confirm
- The email is opened in a new window
- Two small icons (red ribbon and blue lock) indicate that the email was sent.
- The red ribbon indicates that the sender has signed digital
 - The blue lock indicates the encrypted transmission

If you press on the blue lock, then you can see the encryption algorithm in the example 3DES.



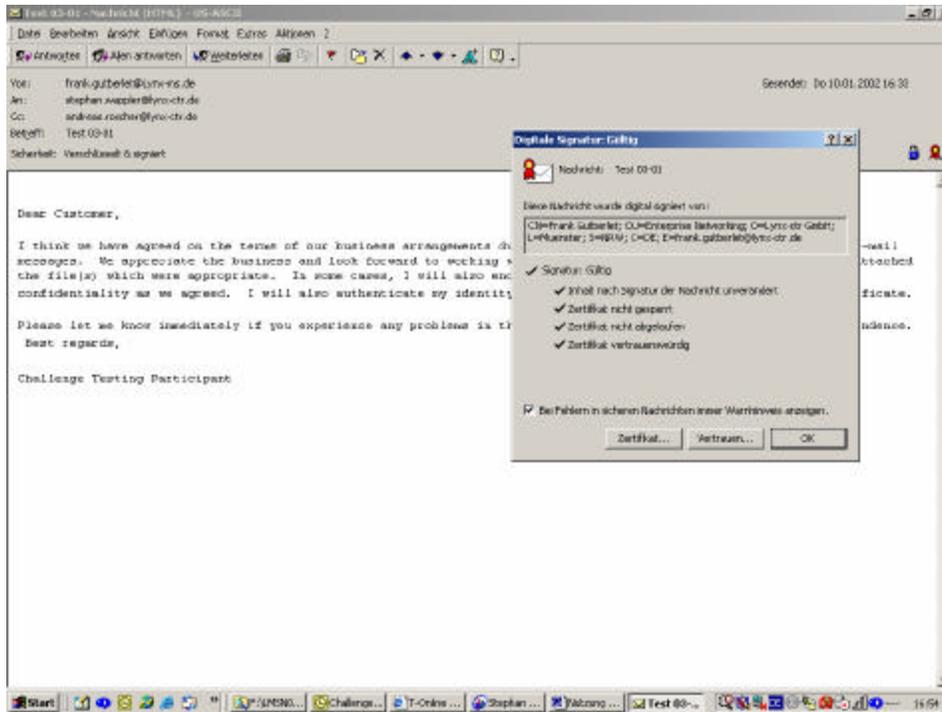
You can also look at the applied encryption certificate and its details.



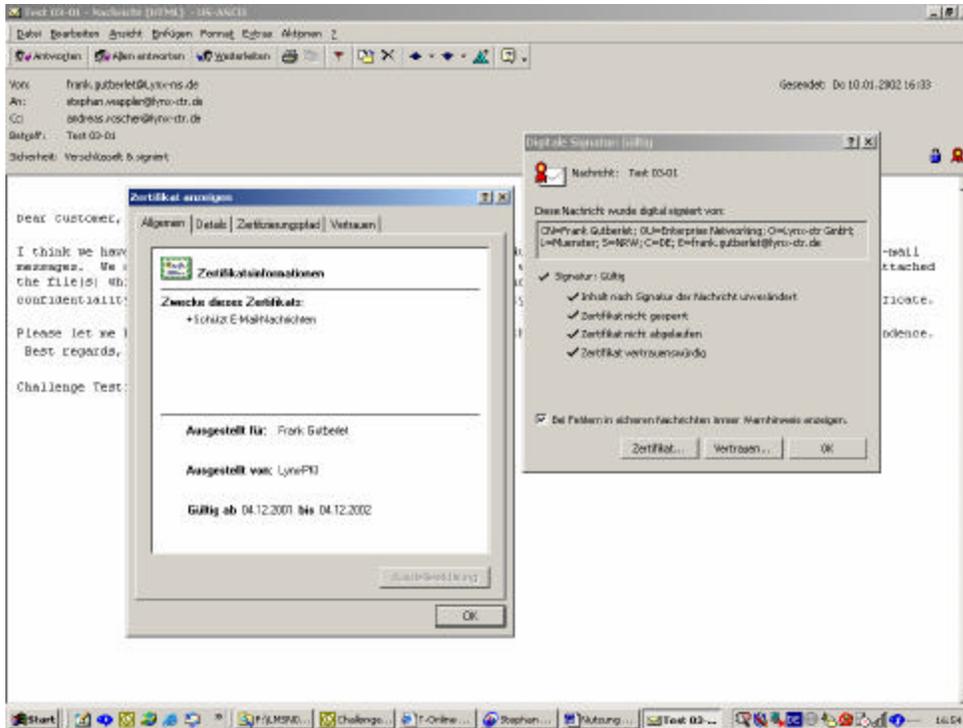
Press on the red ribbon to see information about the digital signature:

- Who has issued the digital signature
- When the digital signature was issued

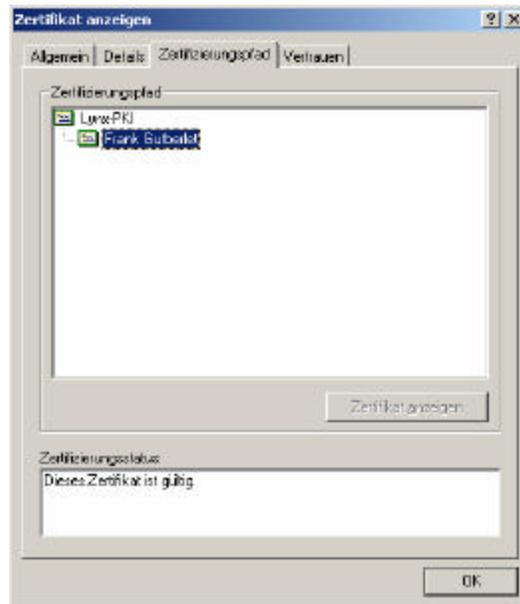
Additional information about the validity of the certificate is also provided.



In the example you can see that the certificate may be applied only for email safety and who owns the private key.



The last screen indicates the certification path and that the certificate is valid.



Lotus Domino R5.0.8 Server

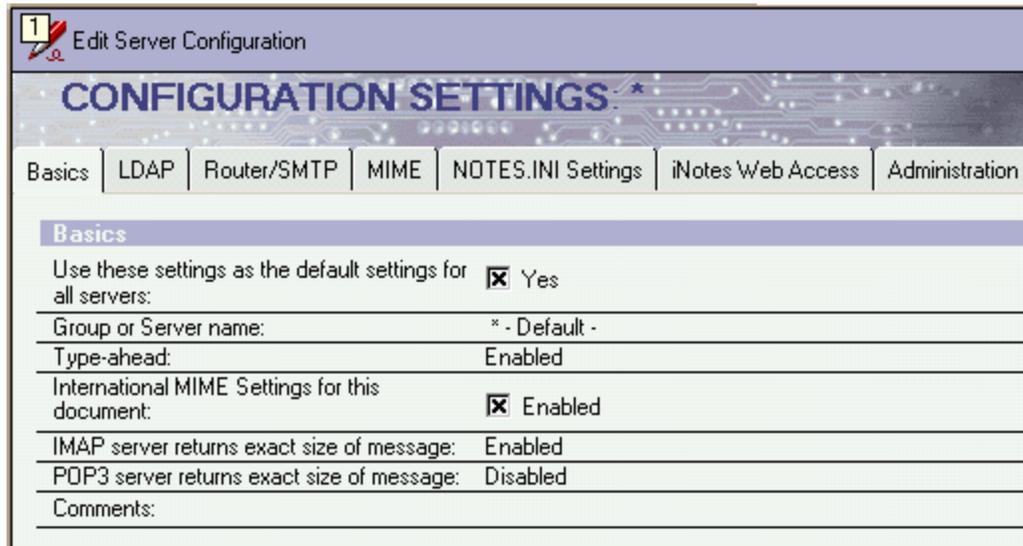
The following section describes the necessary configuration and administration of Lotus Notes as an email and LDAP server. All statements made refer to Lotus Notes 5.0.8.

Configuration of the Lotus Domino Email Servers

No changes in the default configuration of the email server tasks are necessary; a detailed description is forgone and administrators are referred to the installation handbook. Only the LDAP service configuration follows.

Configuration of the LDAP Service on the Lotus Domino Server

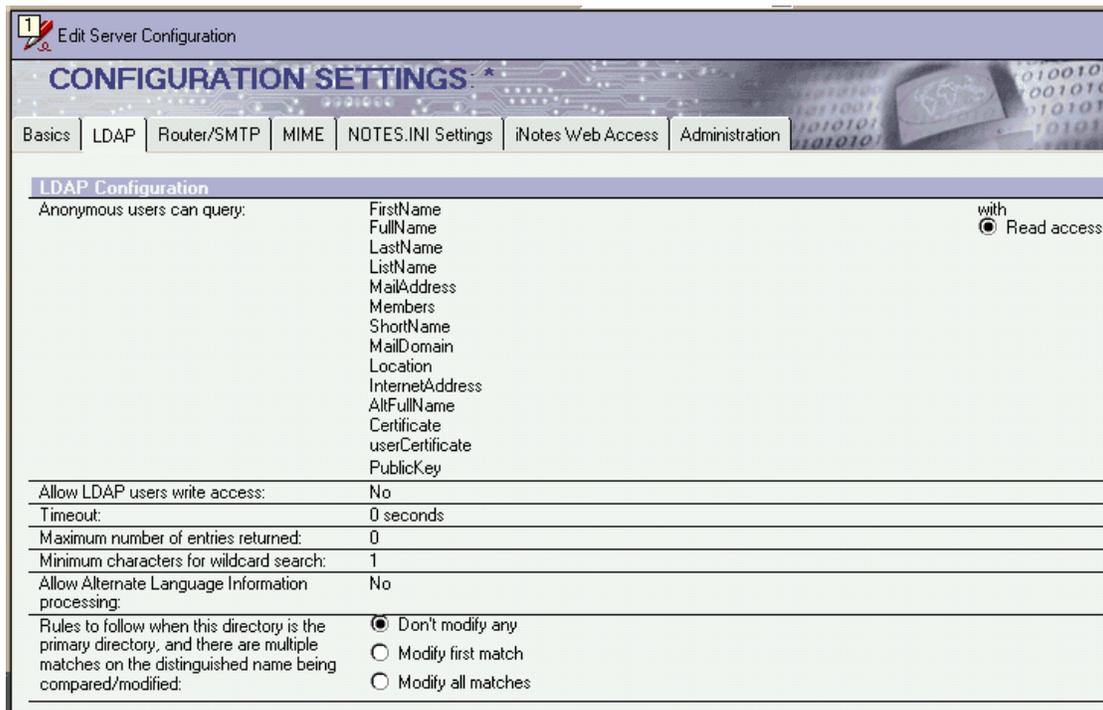
After selecting the server configuration document, set the mode on enabled.



The screenshot shows the 'Edit Server Configuration' dialog box with the 'CONFIGURATION SETTINGS' tab selected. The 'Basics' sub-tab is active, displaying several configuration options:

Use these settings as the default settings for all servers:	<input checked="" type="checkbox"/> Yes
Group or Server name:	* - Default -
Type-ahead:	Enabled
International MIME Settings for this document:	<input checked="" type="checkbox"/> Enabled
IMAP server returns exact size of message:	Enabled
POP3 server returns exact size of message:	Disabled
Comments:	

The check box for the default settings for all servers must be activated to be able to configure the LDAP service.



The screenshot shows the 'Edit Server Configuration' dialog box with the 'CONFIGURATION SETTINGS' tab selected. The 'LDAP' sub-tab is active, displaying the 'LDAP Configuration' section:

Anonymous users can query:	FirstName FullName LastName ListName MailAddress Members ShortName MailDomain Location InternetAddress AltFullName Certificate userCertificate PublicKey	with <input checked="" type="radio"/> Read access
Allow LDAP users write access:	No	
Timeout:	0 seconds	
Maximum number of entries returned:	0	
Minimum characters for wildcard search:	1	
Allow Alternate Language Information processing:	No	
Rules to follow when this directory is the primary directory, and there are multiple matches on the distinguished name being compared/modified:	<input checked="" type="radio"/> Don't modify any <input type="radio"/> Modify first match <input type="radio"/> Modify all matches	

This setting under the LDAP tab determines which entries can be read anonymously.

After enabling the configuration document for the LDAP access, Directory Assistance is activated by specifying the name of the Directory Assistance database (DA-Lynx-RC.nsf.)

The screenshot shows the Exchange Server configuration console. At the top, there are two tabs: '1 Edit Server' and '2 Web...'. Below the tabs, the server name 'SERVER: mail2/Lynx-ms/DE' is displayed. A navigation bar contains the following tabs: Basics, Security, Ports, Server Tasks, Internet Protocols, MTAs, Miscellaneous, Transactional Logging, and Administration. The 'Basics' tab is selected and highlighted. The configuration fields are as follows:

Server name:	mail2/Lynx-ms/DE
Server title:	Challenge
Domain name:	Lynx-ms
Fully qualified Internet host name:	mail2.lynx-ms.de
Cluster name:	
Directory Assistance database name:	DA-Lynx-RC.nsf
Directory Catalog database name on this server:	
Optimize HTTP performance based on the following primary activity:	Advanced (Custom Settings)

At the bottom of the 'Basics' tab, there is a section for 'Server Location Information' which is currently collapsed.

To configure the LDAP-service:

Step 1 Select "Ports"

Step 2 Select "Internet Ports"—SSL, port number and authentication options are defined

1 Edit Server 2 Web...

SERVER: mail2/Lynx-ms/DE

Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous | Transactional Logging | Administration

Notes Network Ports | Internet Ports | Proxies

SSL settings

SSL key file name: keyfile.kyr

SSL protocol version (for use Negotiated with all protocols except HTTP):

Accept SSL site certificates: Yes No

Accept expired SSL certificates: Yes No

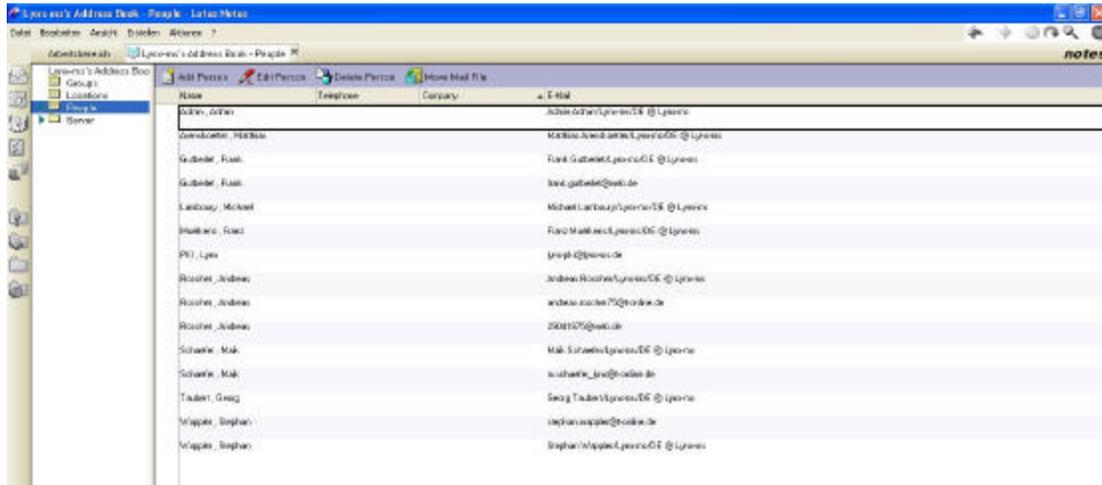
Web | Directory | News | Mail | IIOP

Directory (LDAP)

TCP/IP port number:	10389
TCP/IP port status:	Enabled
Authentication options:	
Name & password:	Yes
Anonymous:	Yes
SSL port number:	636
SSL port status:	Disabled
Authentication options:	
Client certificate:	No
Name & password:	No
Anonymous:	Yes

Linking Root Certificate in the Lotus Notes Directory

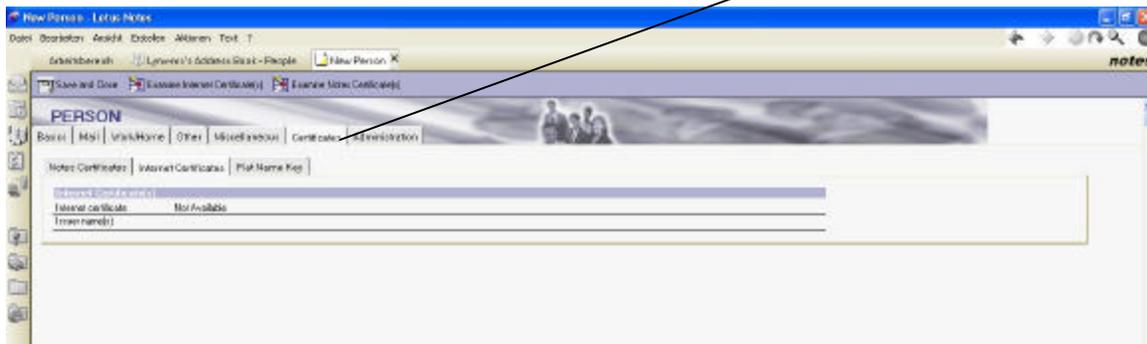
Only the administrator can bind the root certificate on the server.



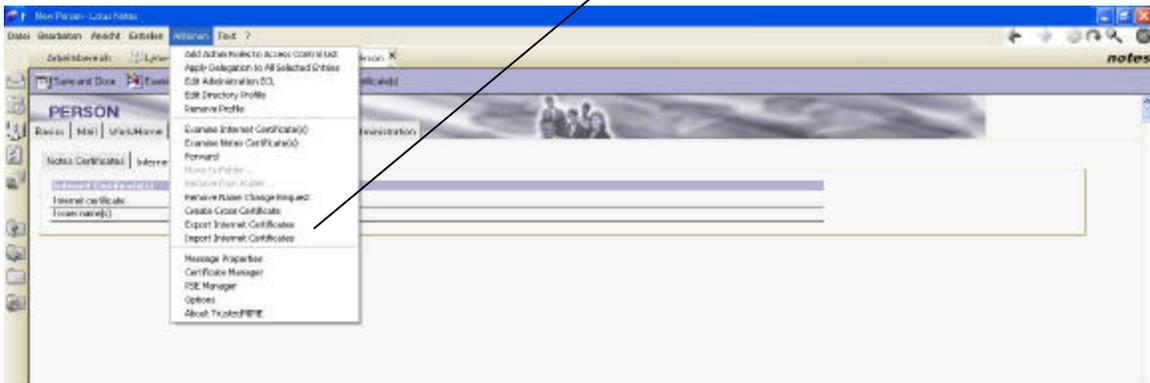
Step 1 Add someone to the directory and register that person at "New Person"



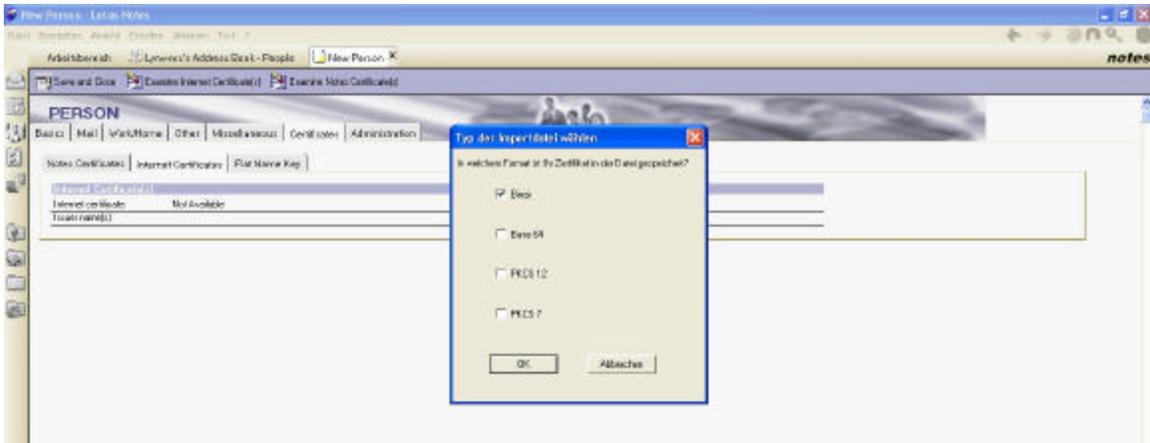
Step 2 Enter further information about the CA at the Certificates tab



Step 3 Select Actions -> Import Internet Certificate

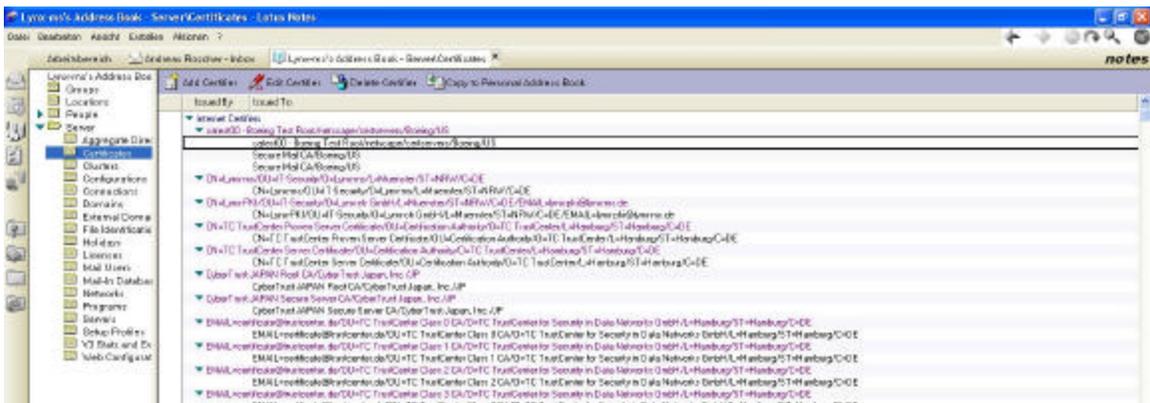


Step 4 Select the format of the certificate and the where the certificate is located



Step 5 Click OK

The certificate is automatically imported into the directory and appears in the Internet Certificates view of the directory.



Lotus Notes R5.0.8 Client

The following describes the configuration and administration of the client and the procedure for sending encrypted emails with the Lotus Notes client 5.0.8.

Configuration and Administration of Lotus Notes Clients 5.0.8

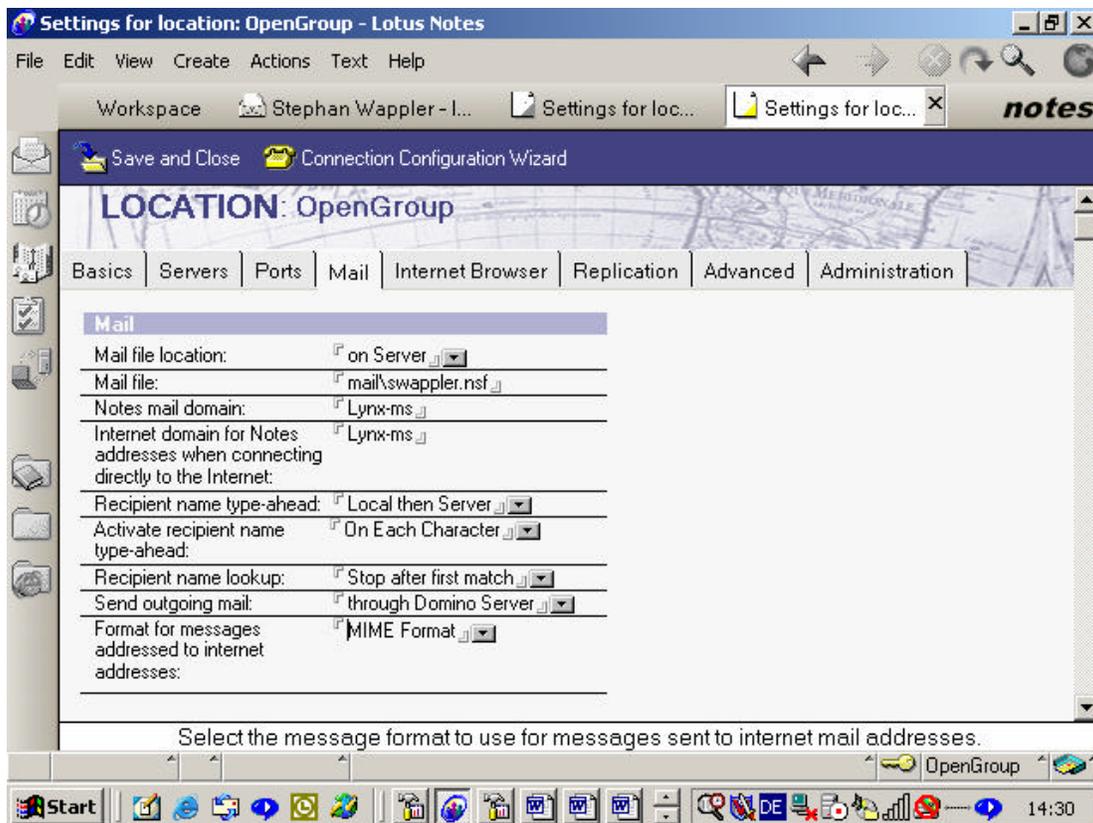
The configurations and administration described here refer to the Lotus Notes client 5.0.8. The user must change the following settings:

- Lotus Notes email format
- Linking the private key and the Internet certificate under notes
- Registering the LDAP server as an index server

Lotus Notes Email Format

By default, notes text format passed supports to Lotus Notes. This setting must be changed to MIME format, as follows:

- Step 1** Select **File** then **Mobile**
- Step 2** Select **Edit Current Location**
- Step 3** Select the **Mail** tab
- Step 4** Set the field “Format for messages addressed to Internet addresses” to “MIME format”
- Step 5** Select **Save** and **Close** to store the change

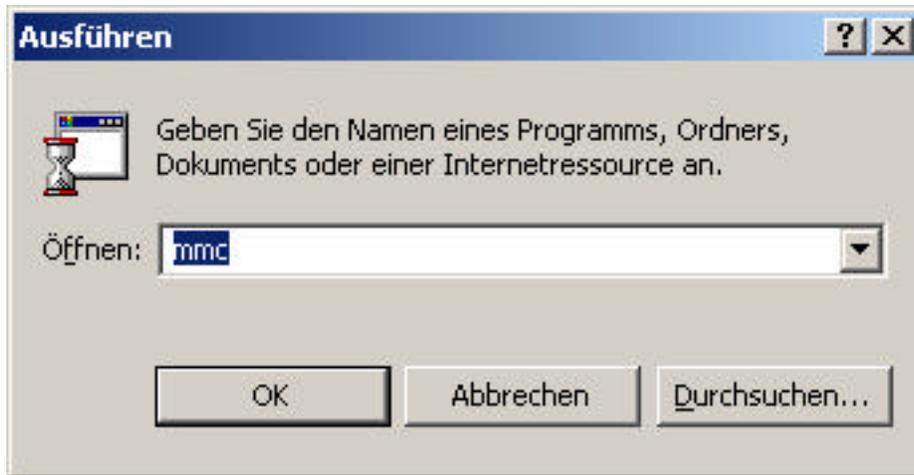


Import the Private Key and Root Certificate

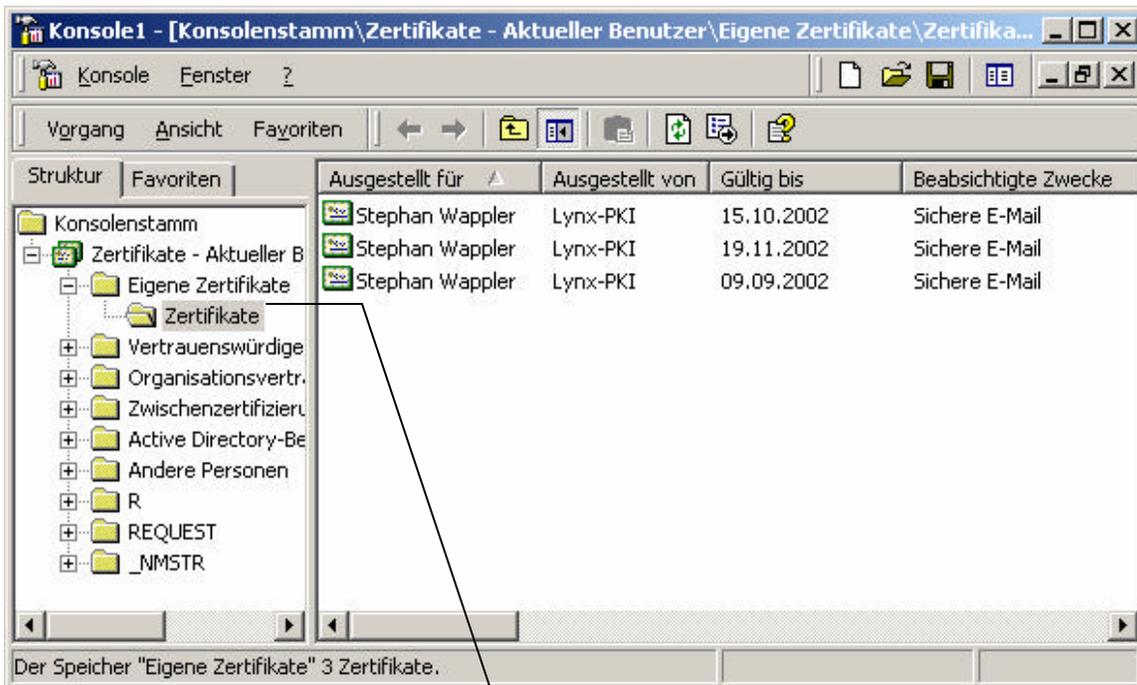
The private key and the certificate must first be exported from the Windows certificate storage as a PKCS#12 file.

Export the Private Key from Windows Certificate Storage

- Step 1** Press the **Start** button
- Step 2** Select **Run**
- Step 3** Enter the command MMC
- Step 4** Press **OK**



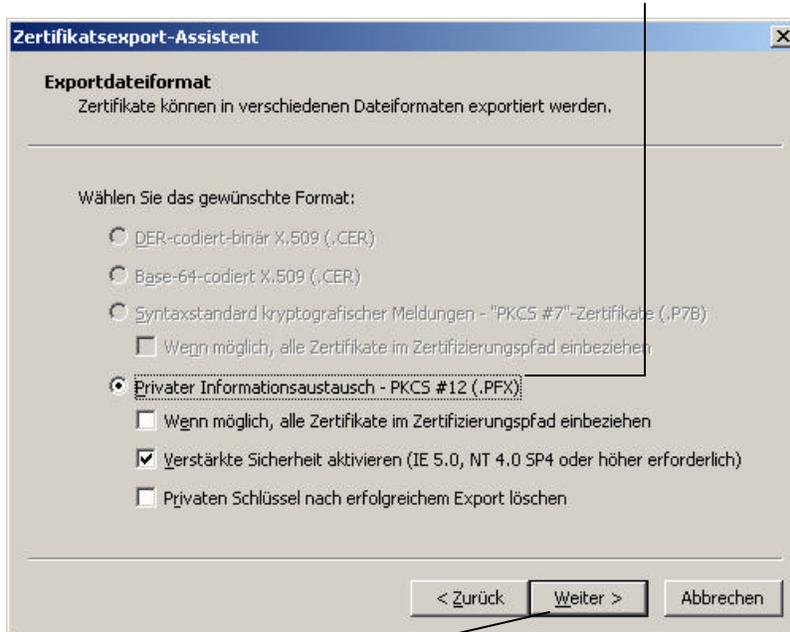
Step 5 Expand the Console, Issued Certificates, and Certificates folders



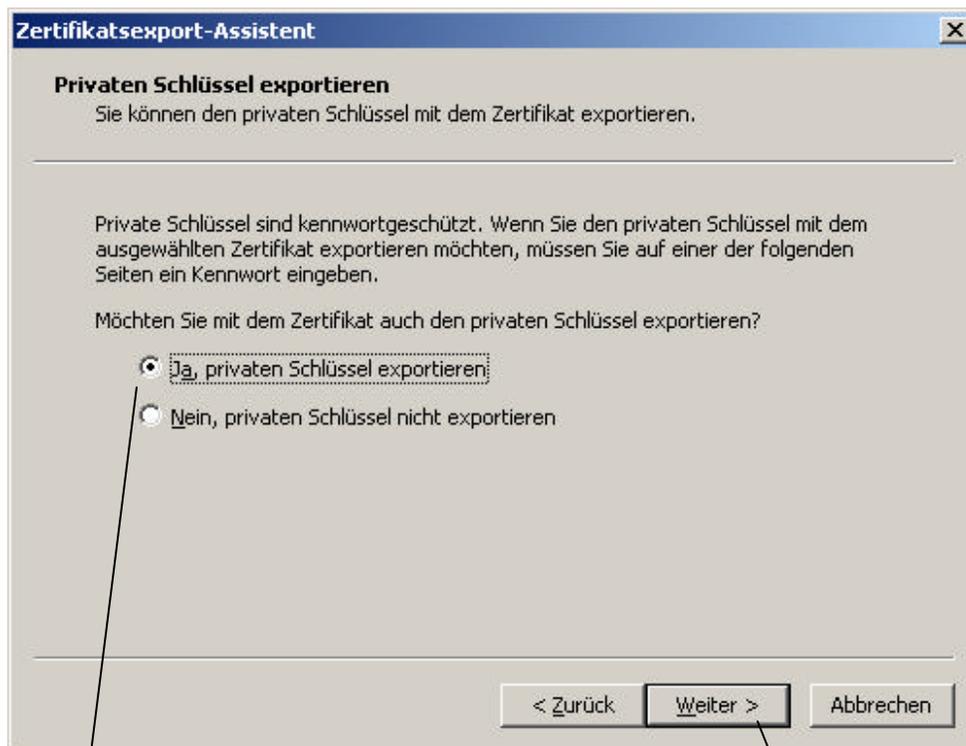
- Step 6** Select the corresponding certificate
- Step 7** Open with a double click
- Step 8** Select the details tab
- Step 9** Copy the Button into the details
- Step 10** Click Next and select export of the private key
- Step 11** Click Next



Step 11 Select the format exchange of information private—PKCS#12 and reinforced security



Step 12 Click Next

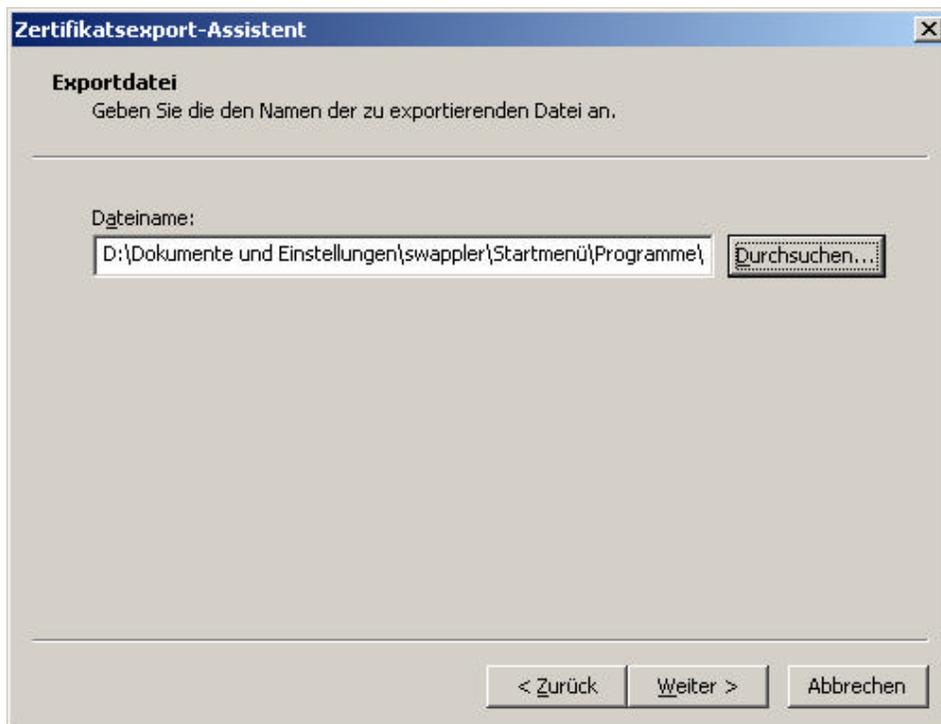


Step 13 Enter a password for protection of the private key

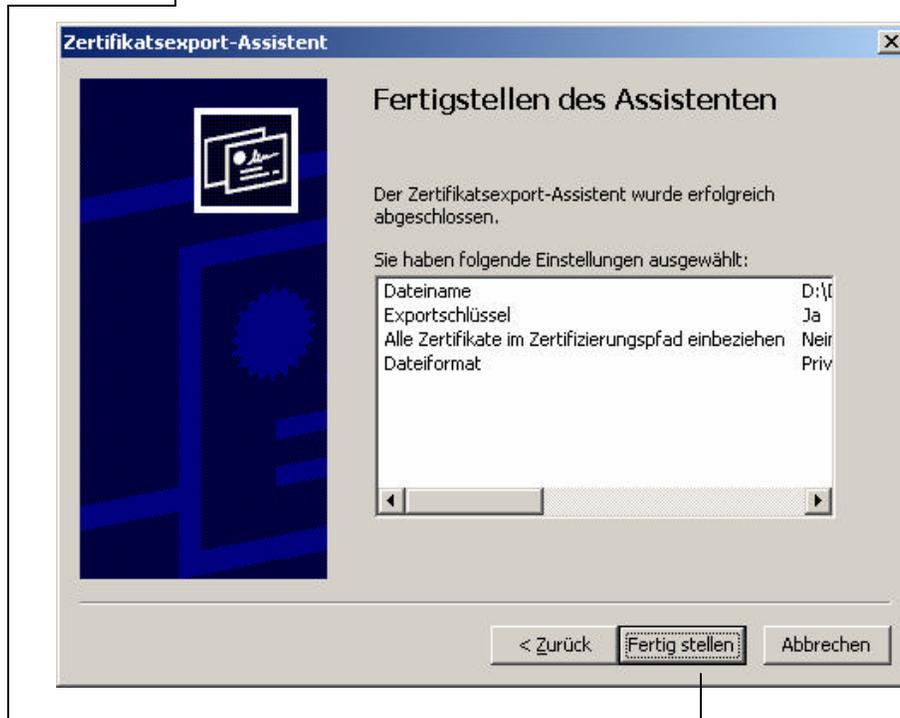
Step 14 Confirm and click Next



- Step 15 Select a path and make a note of it
- Step 16 Click Next



Step 17 Click **Finish** to complete export of the private key and certificate

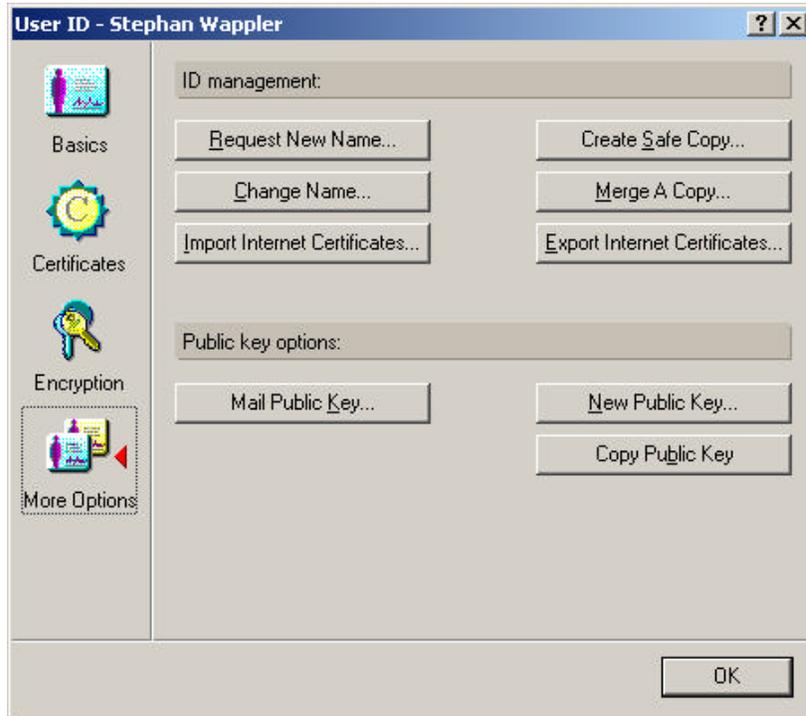


Import the Private Key and the Certificate into Lotus Notes

The private key and the root certificate of the issuing Certificate Authority must be imported before emails can be signed or before encrypted emails can be decrypted.

Step 1 Select File -> Tools -> User ID

Step 2 Enter the password



Step 3 Click the More Options icon

Step 4 Click Import Internet Certificates

Step 5 Enter the path to the Internet Certificate

Step 6 Select the corresponding file

Step 7 Click Open under File -> Tools menu

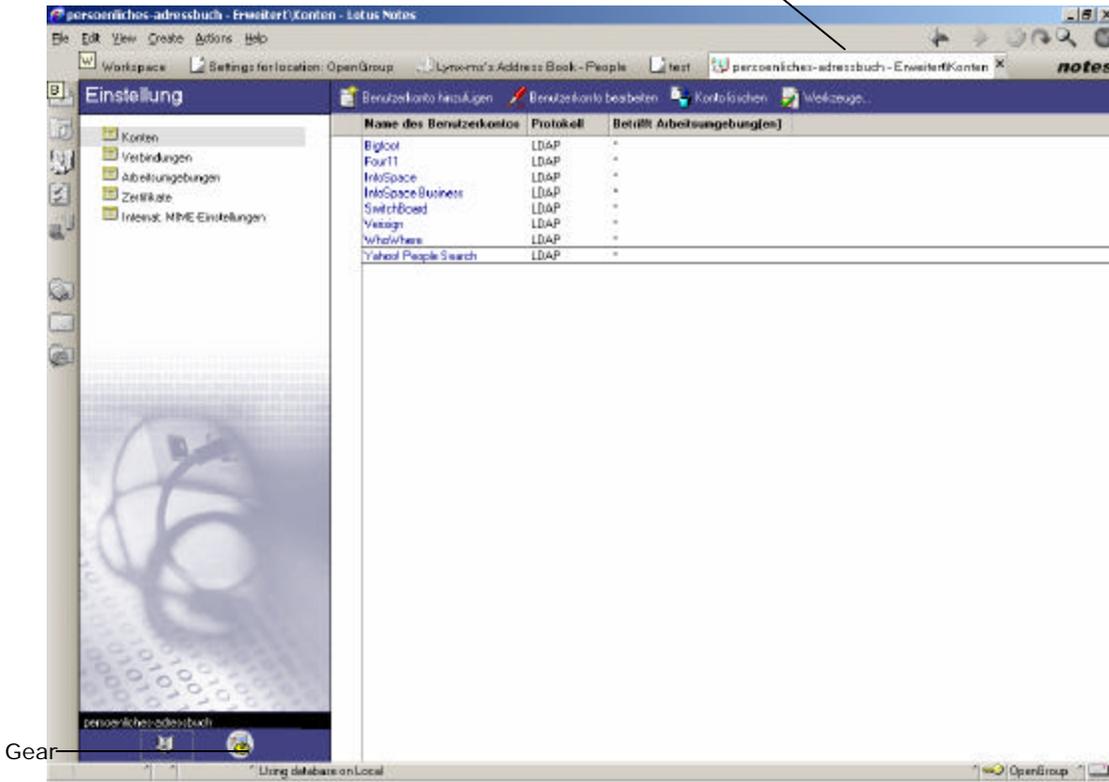
Step 8 Enter the password to release the private key

If successful, a pop up window with the message “Import was successful” will appear.

Register the LDAP Server as a Directory Server

The LDAP servers must be added to the Accounts in the user's Personal Address Book.

- Step 1 **Open** the user's Personal Address Book
- Step 2 **Click** Gear in the lower left frame
- Step 3 **Select** the Accounts View
- Step 4 **Click** "Add User Account"



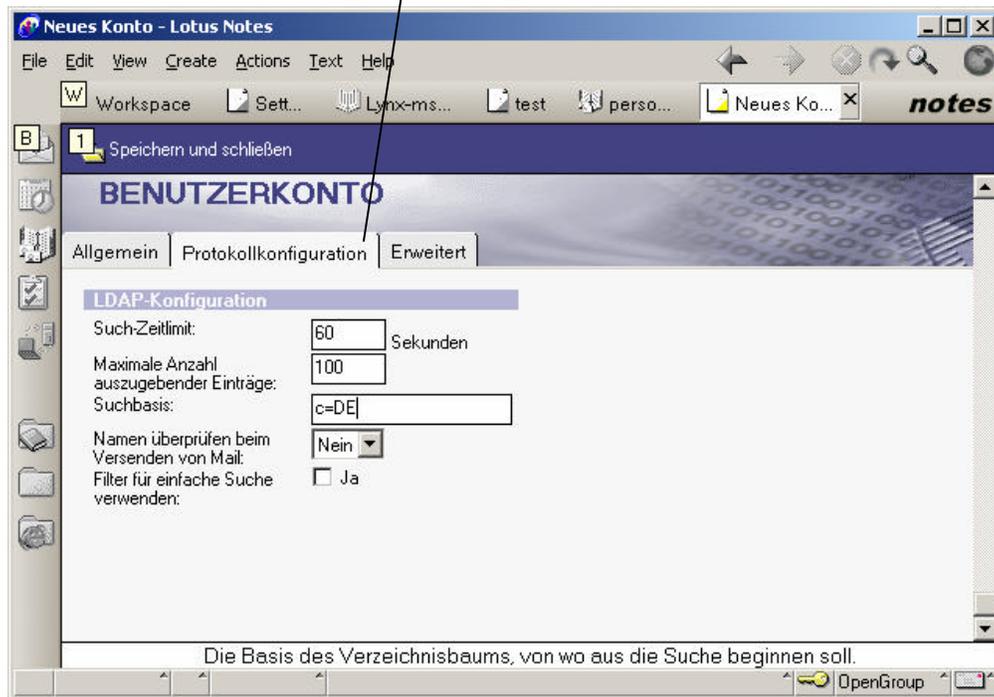
- Step 5 **Enter** a name for the account and an address for the server

Example

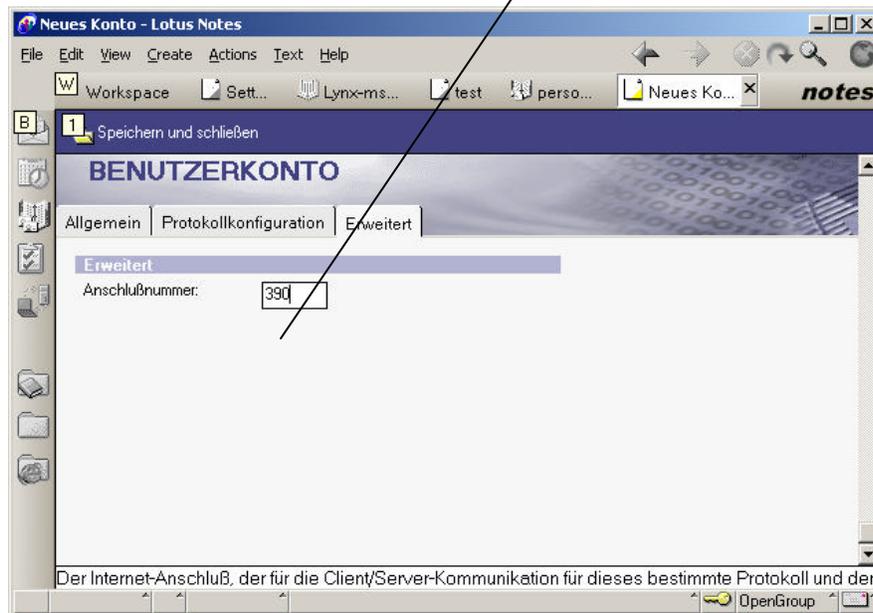
Name—Notes Lynx LDAP

Server—mail2.lynx-ms.de or the IP address 195.202.41.94

Step 6 Select the tab “Protocol Configurations” and enter the information.
Example
c=DE



Step 7 Select the next tab and input the connection number/Port
Example
390



Step 8 Save and Close—LDAP server now available as a directory service

Sending an Encrypted Email

Before an encrypted email with the Lotus Note client R5.0.8 can be sent, some further important steps are necessary. Because Lotus Notes version 5.0.8 does not support the standard Internet procedure for retrieving a X.509 v.3 certificate from an LDAP directory, the following work around solution must be used.

Work Around

Although a Notes user can see the certificate details in the LDAP directory, the Notes 5.0.8 client cannot retrieve the certificate from the LDAP directory.

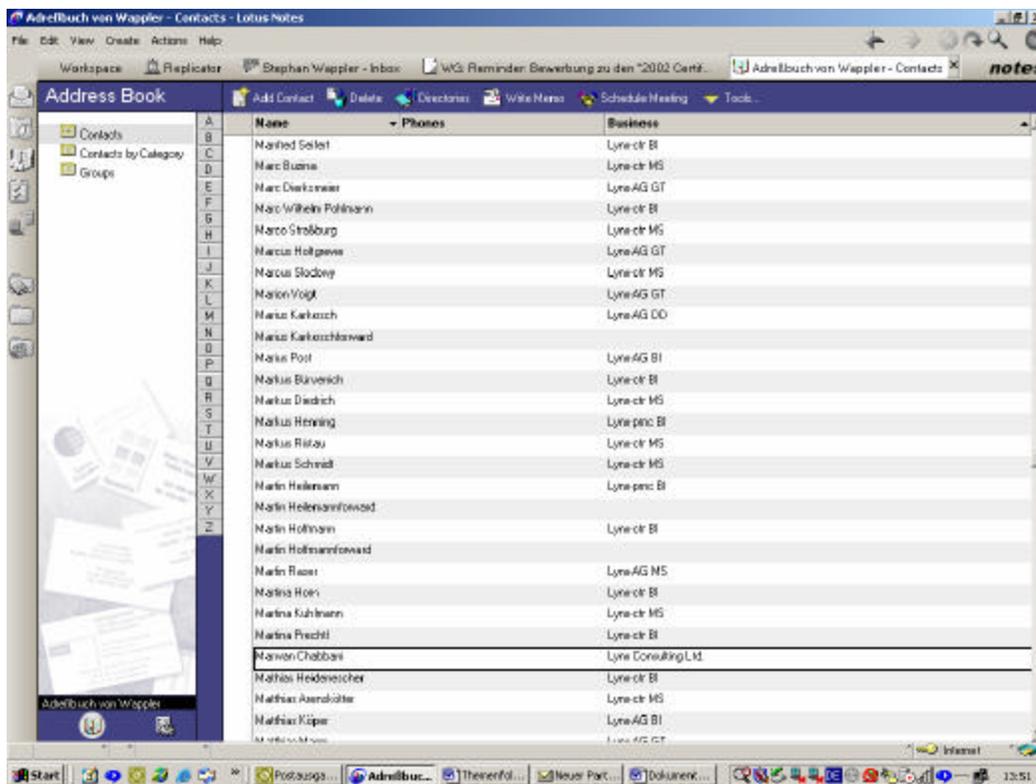
There are two possible work arounds:

One—Intended recipient must first send a signed email message via Internet mail to the Notes user. Upon opening the message, if the Notes user does not have a cross certificate for the intended recipient's Internet certificate, the user will be prompted to cross certify the Internet certificate. The Notes user must also add the user's certificate to his Personal Address Book:

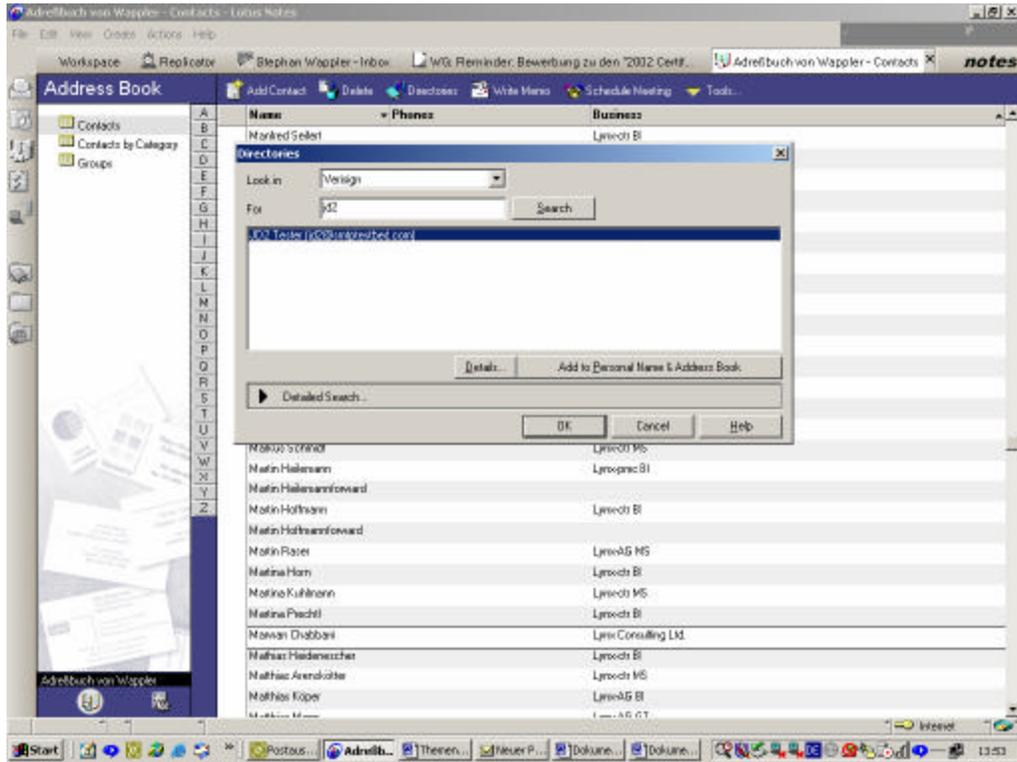
- Select the signed message
- Select Tools From the Actions menu
- Add Sender to Address Book
- Verify that the correct First and Last names are entered In the "Add Sender" window and click on the Advanced tab
- Verify that "Include X.509 certificates" is checked.

Once these steps are accomplished, the Notes user may send encrypted Internet email messages to the recipient.

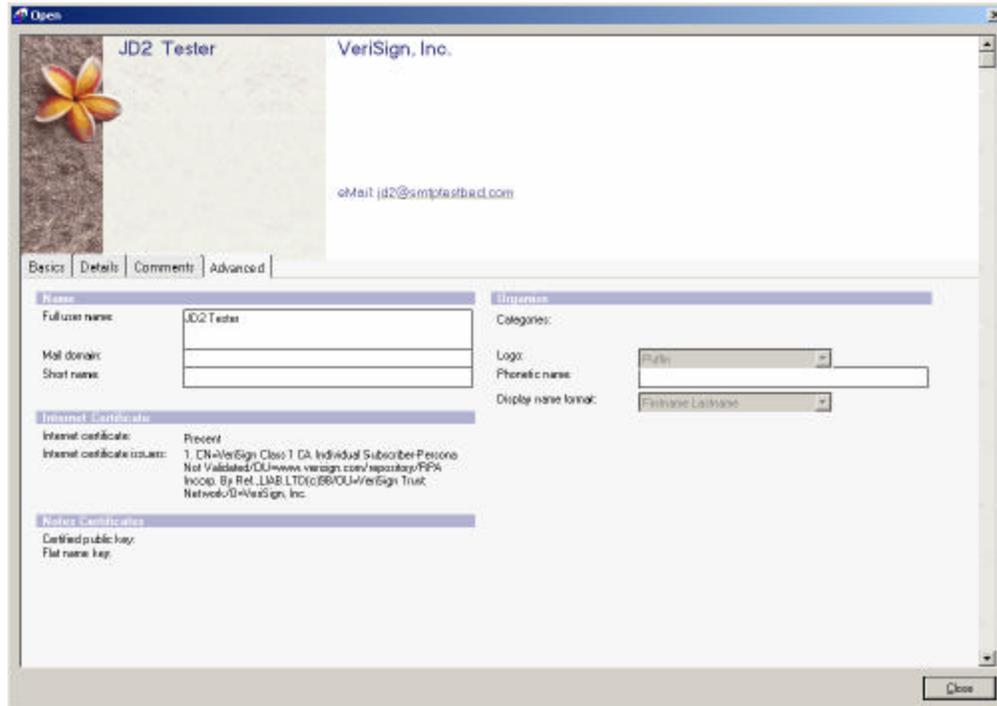
Two—The Notes user must cross-certify the recipient in the sender's Notes Personal Address Book. The Notes user can implement this without requiring the Internet user to send a signed email. The Notes user opens the Notes Personal Address Book and selects the "Directories" Action button



Then the Notes user selects the directory service in which the certificate of the recipient is stored and enters the search word (name or email address) of the recipient and starts the search.

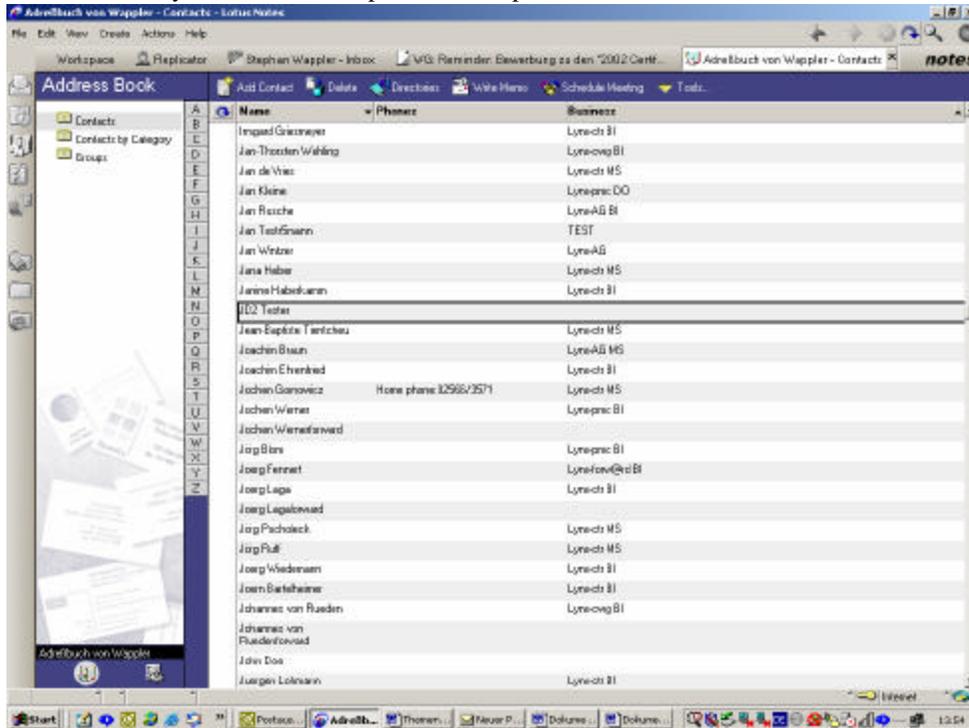


If the search is successful, one or more email addresses are indicated. The Notes user should open each possible entry and examine it for the presence of an Internet mail certificate.

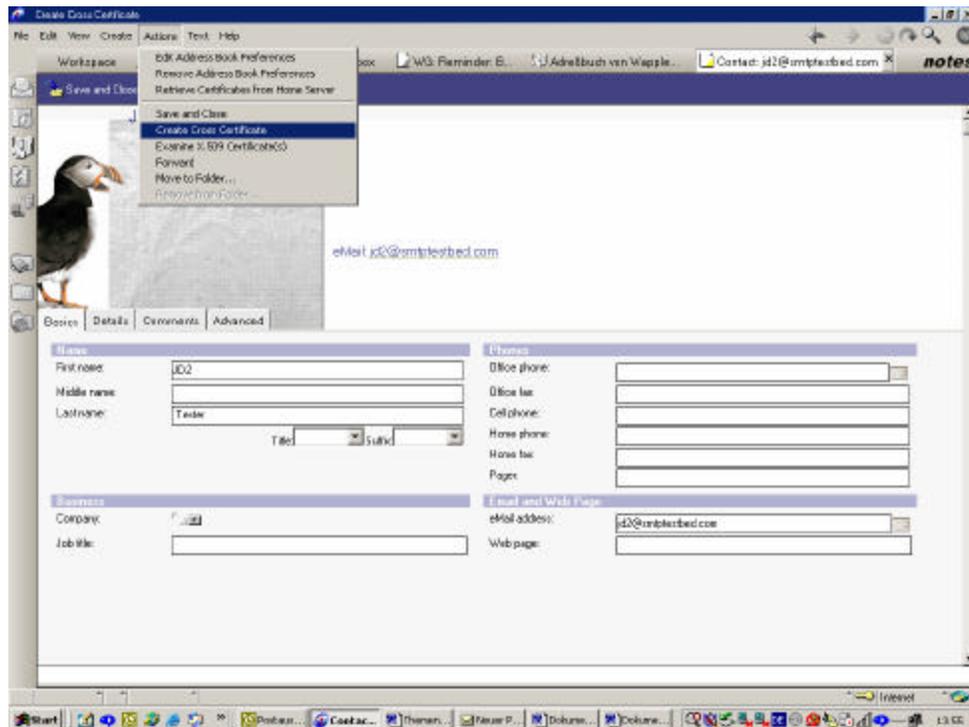


- Step 1 **Select** “Add to Personal Address Book” if a certificate is found in the directory entry (a short report appears indicating the entry was added)
- Step 2 **Select** and **open** the new entry

Note that some data may still need to be updated or adapted.



- Step 3 **Select** **Create Cross Certificate** from the Actions option



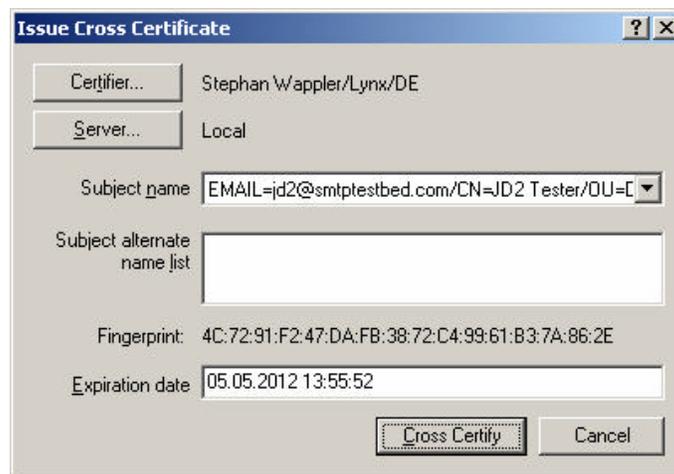
A new window and the data of the certificates belonging to the entry are indicated.

Step 4 Click **OK** if the appropriate certificates were selected



In a new window the data for the Cross Certificate is indicated. Also provided is information about who accomplished the cross certifying.

Step 5 Click **Cross Certify**



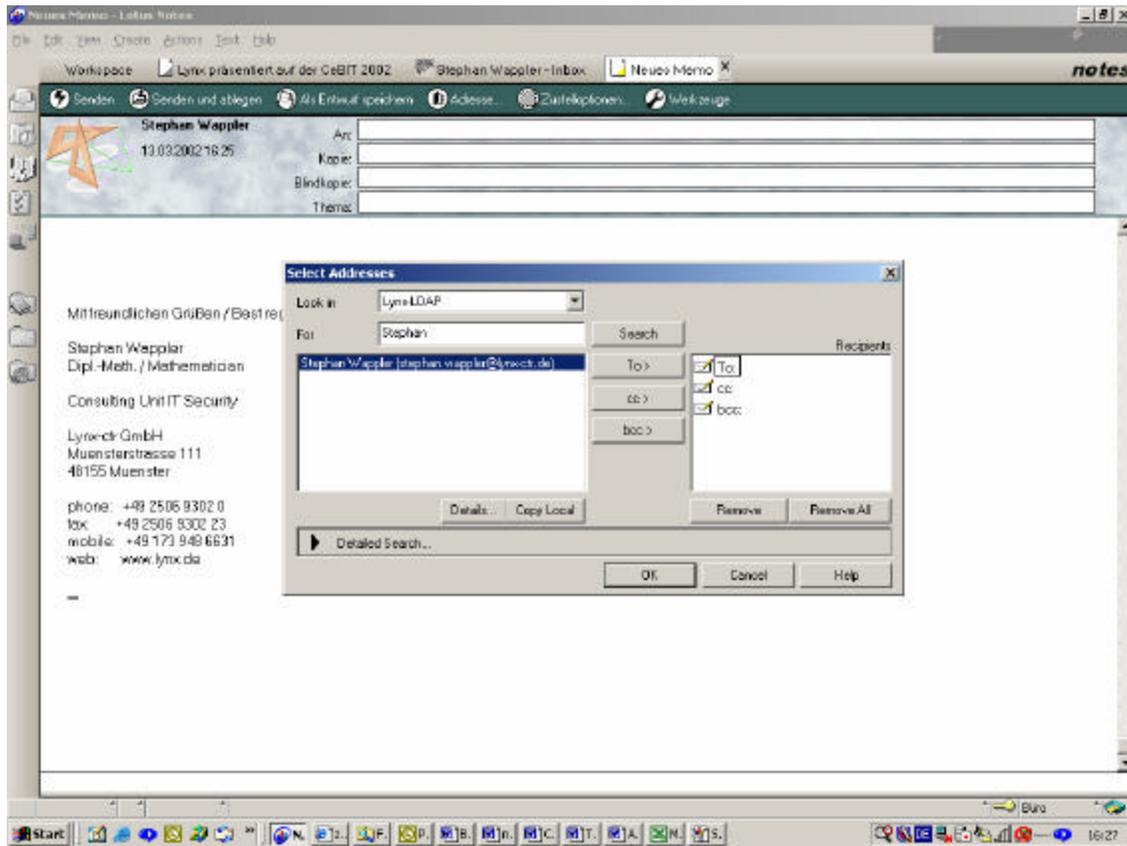
One receives still another short information whether the cross certifying was successful. If successful, encrypted emails can be dispatched to the receiver immediately.

Note: Both work arounds need a clear policy, how long these entries may remain stored in the private directory because there is no examination for validity (i.e., available on the LDAP at use). Here large organizational and administrative measures are necessary.

Challenge Standard Procedure

- Step 1** Start the Lotus Notes 5.0.8 client
- Step 2** Select “Create a new Memo”
- Step 3** Click the “Address” button
- Step 4** Select the corresponding LDAP server from the list of directories and address books
- Step 5** Enter the recipient’s name and click the Search button

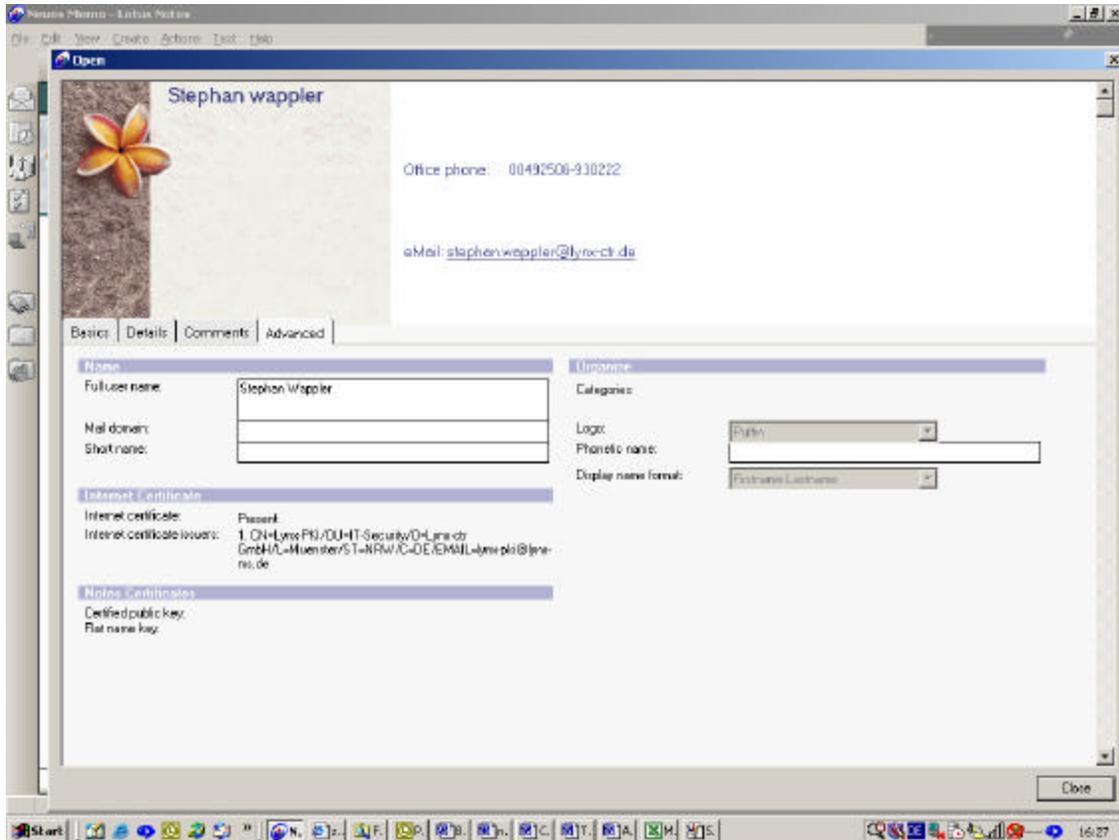
If the search is successful, the recipient’s entry will be indicated.



- Step 6** Click the details button to see the certificate information
- Step 7** Click the “To” button
- Step 8** Click OK to insert the selected recipient in the “To” field of the memo

- Step 9** Click the delivery options button at the top of the memo
- Step 10** Check the box to “encrypt” the message.

Continue to prepare and send the message as usual.



Linux with OpenLDAP

The LDAP configuration settings and an example configuration file follow.

The ldap.conf File

```
# $OpenLDAP: pkg/ldap/libraries/libldap/ldap.conf,v 1.4.8.6 2000/09/05 17:54:38 kurt Exp $
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writeable.
BASE    o=lynx-ctr.de
#URI    ldap://ldap.example.com ldap://ldap-master.example.com:666
#SIZELIMIT    12
#TIMELIMIT    15
#DEREF       never
```

The slapd.conf File

```
# $OpenLDAP: pkg/ldap/servers/slapd/slapd.conf,v 1.8.8.4 2000/08/26 17:06:18 kurt Exp $
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include      /etc/openldap/schema/core.schema
include      /etc/openldap/schema/corba.schema
# Define global ACLs to disable default read access.
schemacheck  off
# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
# referral    ldap://root.openldap.org
pidfile      /var/run/slapd.pid
argsfile     /var/run/slapd.args
# Load dynamic backend modules:
# modulepath  /usr/lib/openldap/openldap
# moduleload  back_ldap.la
# moduleload  back_ldbm.la
# moduleload  back_passwd.la
# moduleload  back_shell.la
#####
# ldbm database definitions
#####
databasesldb
suffix       "o=lynx-ctr.de"
rootdn       "cn=Admin, o=lynx-ctr.de"
# Cleartext passwords, especially for the rootdn, should
# be avoid. See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw       dasistgeheim
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory    /var/lib/ldap
# Indices to maintain
index        objectClass      eq
defaultaccess read
```

Example File Lynx-ctr.ldif

The total structure of the firm can be designed as an *.ldif file and can then be imported into the LDAP database. Here is an example of the ldif file for the Lynx-ctr.de domain

```
dn: o=lynx-ctr.de
objectClass: top
objectClass: organization
o: lynx-ctr.de
dn: ou=Enterprise Networking, o=lynx-ctr.de
ou: Enterprise Network
objectClass: top
objectClass: organizationalUnit
description: BUD Frank Gutberlet und Frank Petersen
dn: ou=Enterprise Development, o=lynxctr.de
ou: Enterprise Development
objectClass: top
objectClass: organizationalUnit
```

description: BUD Uwe Rotermund und Bernd Huener
dn: ou=Enterprise Intelligence,o=lynx-ctr.de
ou: Enterprise Intelligence
objectClass: top
objectClass: organizationalUnit
description: BUD Joerg Ruff und Wolfgang Plemper
dn: ou=Data Warehousing,ou=Enterprise Intelligence,o=lynx-ctr.de
ou: Data Warehousing
objectClass: top
objectClass: organizationalUnit
description: CUM Christoph Daeschner
dn: ou=IT-Security,ou=Enterprise Networking,o=lynx-ctr.de
ou: IT-Security
objectClass: top
objectClass: organizationalUnit
dn: ou=Network Design,ou=Enterprise Networking,o=lynx-ctr.de
ou: Network Design
objectClass: top
objectClass: organizationalUnit
dn: ou=Groupware,ou=Enterprise Development,o=lynx-ctr.de
ou: Groupware
objectClass: top
objectClass: organizationalUnit
description: CUM Hartmut Ossowitzki
dn: cn=Stephan Wappler,ou=IT-Security,ou=Enterprise Networking,o=lynx-ctr.de
givenName: Stephan
sn: wappler
telephoneNumber: 00492506-930222
ou: IT-Security
mail: stephan.wappler@lynx-ctr.de
userCertificate;binary:: MIIFEDCCBHmgAwIBAgIKB1FXJAAAAAAAAAHDANBgkqhkiG9w0BAQUF
ADCBkzEiMCAGCSqGSIb3DQEJARYTbHlueC1wa2lAbHlueC1tcy5kZTELMakGA1UEBhMCREUxD
DAK
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: swappler
cn: Stephan Wappler
description: Security
dn: cn=Andreas Roscher,ou=IT-Security,ou=Enterprise Networking,o=lynx-ctr.de
givenName: Andreas
sn: Roscher
telephoneNumber: 00492506-930222
ou: IT-Security
mail: andreas.roscher@lynx-ctr.de
userCertificate;binary:: MIIFEDCCBHmgAwIBAgIKCvfaZAAAAAAAAAHZANBgkqhkiG9w0BAQUF
ADCBkzEiMCAGCSqGSIb3DQEJARYTbHlueC1wa2lAbHlueC1tcy5kZTELMakGA1UEBhMCREUxD
DAK
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: aroscher
cn: Andreas Roscher
dn: cn=Franz Muelkens,ou=Network Design,ou=Enterprise Networking,o=lynx-ctr.

de
telephoneNumber: 02506-930222
mail: fmuellkens@Lynx-ctr.de
userCertificate;binary:: MIIFFDCCBHWgAwIBAgIKC3mmBAAAAAIDANBgkqhkiG9w0BAQUF
ADCBkzEiMCAGCSqGSIs3DQEJARYTbHlueC1wa2lAbHlueC1tcy5kZTELMakGA1UEBhMCREUxD
DAK
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
givenName: Franz
sn: Muelkens
cn: Franz Muelkens
dn: cn=Frank Gutberlet,ou=Enterprise Networking, o=lynx-ctr.de
telephoneNumber: 02506-930221
mail: frank.gutberlet@Lynx-ctr.de
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
givenName: Frank
sn: Gutberlet
cn: Frank Gutberlet

Administration of Open LDAP Server

Start LDAP Server

The files first must become ldap.conf and slapd.conf files. In the ldap.conf, the IP address or name of the server must be registered. As an example “ldap.lynx-m. de” is used. In the slapd.conf, the rootdn, the suffix, and the passport word must be edited. The server then becomes over/etc/init.d/ldap start.

Insert Additional Records

After installing the OPENLDAP2 server and configuring the files and < slapd.conf >, the databank can be furnished with data.

Command:

```
ldapadd -x -D “cn=Admin, o=lynx-ms.de” -w passwd < record.ldif
```

At the same time—

- The -x switch defines the SASL Authentication of OpenSSL, -D “Distinguished name”
- The -w switch provides the administrations password
- In the file record.ldif, the information is added to the database

The data of the file record is important. ldif in the UNIX-format is available. If this file was produced under a DOS or Windows system, it must be converted into the UNIX format.

In addition—

- dos2unix -n record-dos.ldif record-unix.ldif
or
- cat dosdaten.ldif | /usr/bin/tr -d '\r' > unixdaten.ldif

If a distant PC carries out the update, the host statement should be added.

Example

- ldapadd -x -h ldap.lynx-ms.de -D “cn=Admin, o=lynx-ms.de” -w *passwd* < record.ldif

LDAP Records Modify

A file produced that contains the corresponding LDAP record modifications.

Example

- /tmp/change
dn: uid=fmuelkens, ou=Enterprise Network, o=lynx-ms.de
changetype: modify
replace: mail
mail: modme@OpenLDAP.org
-
add: title
title: Grand Poobah
-
add: jpegPhoto
jpegPhoto:< file://tmp/modme.jpeg
add: usercertificate
userCertificate;binary:: MIIE8DCCA9igAwIBAgIBAjANBgkqhkiG9w0BAQQFADCBwTELM
AkGA1UEBhMCQ0gxEDAObgNVBAGTB1p1ZXJpY2gxZzARBgNVBAcTClpbnRlcuRodXlXJzA
delete: description
-

Formatting the Certificates

To add databank certificates, the certificate file must be in the DER encoding format. To guarantee this, execute the following formatting.

ldif -b “usercertificate;binary” < outcert.der > cert.ldif

or at the moment uses

ldif -b “usercertificate;binary” < outcert.cer > cert.ldif

Then, add dn to this file.

Example

- dn: cn=user,ou=people,dc=yourorg,dc=com
changetype: modify
add: usercertificate
userCertificate;binary:: MIIC2TCCAKKgAwIBAgIBADANBgkqhkiG9w0BAQQFADBGMQswCQYD
VQQGEwJJVDENMAsgA1UEChMESU5GTjESMBAGA1UECXMJQXV0aG9y
aXR5MRQwEgYDVQQDEwtJTkZO

Alternatively, it is also possible to have access to the file system key.

Example

```
userCertificate;binary:< file:///path/to/cert.der
```

According to Internet Explorer, the certificate can be exported in the following formats:

- Base-64-coded X509 *.cer
- DER-coded-binär X509 *.cer

Access to the OpenLDAP Server via Client GUI

Access to the LDAP server can be obtained most simply with kldap under X-Windows observes and can be edited. Under WinX, the java tool can observe “LDAP editor” and can be edited.

Additional entries can be imported over the menu point ldif. In addition the file import ldif was produced and imported.

Example

Import.ldif:

```
dn: ou=IT-Security, ou=Enterprise Network, o=lynx-ms.de
objectclass: top
objectclass: organizationalUnit
ou: IT-Security
dn: ou=Groupware, ou=Enterprise Development, o=lynx-ms.de
objectclass: top
objectclass: organizationalUnit
ou: Groupware
description: CUM Hartmut Ossowitzki
dn: uid=tpforr, ou=Groupware, ou=Enterprise Development, o=lynx-ms.de
uid: tpforr
cn: Thomas Pforr
sn: Pforr
givenname: Thomas
objectclass: Person
objectclass: organizationalPerson
ou: Groupware
mail: tpforr@lynx.de <mailto:tpforr@lynx.de>
```

LDAPSearch

Ldapsearch -x -h 10.35.1.7 -b 'o=lynx-ms.de' 'objectclass=*

This syntax (' ') is considered special to Linux. The syntax for Lotus Notes can differ.

As alternative to the objectclass, the following syntax can be inserted: 'cn = Georg Taubert' or 'cn = Georg*'

Instructions for Using OpenSSL Toolkit in a Certificate Environment

The OpenSSL toolkit is an open source SSL encryption implementation that provides SSL encryption using selectable encryption algorithms and provides the capabilities to manage the server and user (X.509) certificate mechanism required for SSL encryption. Certificate management provides for establishing a root CA, generating CSRs and signing those CSRs to generate the actual certificate. OpenSSL certificate management also provides for CRLs.

OpenSSL information can be found at: <http://www.openssl.org>. All instructions listed below are for Sun Solaris 8 operating environment.

Use OpenSSL to Create the Root CA

You must first create your root CA to generate X.509 Certificates from user requests.

Create the Master CA Key Using a Random Data Source (randfiles or random-bits)

```
randsource="/var/log/messages:/var/adm/messages:/var/log/system.log:/var/wtmp:/kernel:\
/kernel/genunix:/vmunix:/\
vmlinuz:/mach:/etc/hosts:/etc/group:\
/etc/resolv.conf:/bin/ls"
```

or

```
randsource="./random-bits"
openssl genrsa -des3 -out ca.key 1024 -rand $randsource
```

Note: The PassPhrase used to encrypt the CA key will be required in subsequent certificate signing operations.

Generate CA Configuration Information and Store it in a Temporary File

You will be prompted for the most pertinent CA information during the next step.

```
CA_CONFIG="./root-ca.conf"
```

```
cat >$CA_CONFIG <<EOT
```

```
[ req ]
default_bits                = 1024
default_keyfile              = ca.key
distinguished_name          = req_distinguished_name
x509_extensions              = v3_ca
string_mask                  = nombstr
req_extensions               = v3_req
[ req_distinguished_name ]
countryName                  = Country Name (2 letter code)
countryName_default          = MY
countryName_min              = 2
countryName_max              = 2
stateOrProvinceName         = State or Province Name (full name)
stateOrProvinceName_default = Perak
localityName                 = Locality Name (e.g., city)
localityName_default         = Sitiawan
0.organizationName           = Organization Name (e.g., company)
0.organizationName_default   = My Directory Sdn Bhd
organizationalUnitName       = Organizational Unit Name (e.g., section)
```

```

organizationalUnitName_default = Certification Services Division
commonName                    = Common Name (e.g., MD Root CA)
commonName_max                 = 64
emailAddress                   = Email Address
emailAddress_max               = 40
[ v3_ca ]
basicConstraints               = critical,CA:true
subjectKeyIdentifier           = hash
[ v3_req ]
nsCertType                    = objsign,email,server
EOT

```

Self Sign the Root CA Certificate

```
openssl req -new -x509 -days 3650 -config $CA_CONFIG -key ca.key -out ca.crt
```

This will create several CA objects in the current working directory:

- ca.crt
- ca.db.certs
- ca.db.index
- root-ca.conf
- ca.db.serial

Remove the CA Configuration Temporary File (Optional)

```
rm -f $CA_CONFIG
```

You are now ready to sign CSRs using the PassPhrase that encrypted your root CA key.

Use OpenSSL to Create the User Cert Request (Optional)

The user must generate a CSR, which is then used to generate the X.509 certificate. The client browser will generally have the capability to generate the CSR and locally store the private key.

Generate User Certificate Key

```
openssl genrsa -out <"username">.key 1024
```

Complete Necessary Certificate Data and Store in a Temporary File

```
USER_CSR_CONFIG="user-cert.conf"
cat >${USER_CSR_CONFIG} <<EOT
  [ req ]
  default_bits                = 1024
  default_keyfile              = user.key
  distinguished_name           = req_distinguished_name
  string_mask                  = nombstr
  req_extensions               = v3_req
  [ req_distinguished_name ]
  commonName                   = Common Name (eg, John Doe)
  commonName_max               = 64
  emailAddress                 = Email Address
  emailAddress_max             = 40
  [ v3_req ]
  nsCertType                   = client,email
  basicConstraints              = critical,CA:false
EOT
```

Generate User Certificate Request

```
openssl req -new -config $USER_CSR_CONFIG -key <"username">.key -out <"username">.csr
```

Use OpenSSL to Sign User Cert Request Using the Root CA

The root CA is used to sign the user CSR and produces the X.509 certificate.

Create Temporary CA Configuration in the CA Directory to Sign the User Certificate

```
cat >./ca.config <<EOT
  [ ca ]
  default_ca                   = default_CA
  [ default_CA ]
  dir                           = .
  certs                         = \${dir}
  new_certs_dir                 = \${dir}/ca.db.certs
  database                      = \${dir}/ca.db.index
  serial                       = \${dir}/random.bits
  certificate                   = \${dir}/ca.crt
  private_key                   = \${dir}/ca.key
  default_days                  = 365
  default_crl_days              = 30
  default_md                    = md5
  preserve                      = yes
  x509_extensions               = user_cert
  policy = policy_anything
  [ policy_anything ]
  commonName                    = supplied
  emailAddress                   = supplied
  [ user_cert ]
  #SXNetID                      = 3:yeak
  subjectAltName                 = email:copy
  basicConstraints               = critical,CA:false
  authorityKeyIdentifier         = keyid:always
  extendedKeyUsage               = clientAuth,emailProtection
EOT
```

EOT

Sign the X.509 User CSR and Generate the Certificate into <“username”>.cert and Verify the Certificate File Against the CA

You will need to supply the PassPhrase for the root CA key file.

```
openssl ca -config ca.config -out <“username”>.cert -infile <“username”>.csr
openssl verify -CAfile ca.crt <“username”>.cert
```

Print out certificate data (Optional).

```
openssl x509 -in <“username”>.cert -noout -text
```

iPlanet Directory Server Import

The Sun supplied “ldapmodify” command can be used to update and add entries in an LDAP directory server. Typically the change commands are placed in a temporary file and ldapmodify is called with the “-f <filename>” option. If the “filename” option is not used then ldapmodify reads commands from STDIN. The ldapmodify command cannot be used with LDAP servers that require SSL-LDAP connections.

Usage:

```
/usr/bin/ldapmodify -h <ldaphost> -p <ldapport> -D “<BindDN>” -w “<password>” \
    -b -r -f “<temp file>”
```

Example

The format of the content of file (or standard input if no -f option is specified) is illustrated in the examples below.

The file /tmp/entrymods contains the following modification instructions:

```
dn: cn=Modify Me, o=XYZ, c=US
changetype: modify
replace: mail
mail: modme@atlanta.xyz.com
-
add: title
title: System Manager
-
add: jpegPhoto
jpegPhoto: /tmp/modme.jpeg
-
delete: description
-
```

The command:

example% ldapmodify -b -r -f /tmp/entrymods modifies the “Modify Me” entry as follows:

- The current value of the mail attribute is replaced with the value “modme@atlanta.xyz.com”
- A title attribute with the value “System Manager” is added
- A jpegPhoto attribute is added, using the contents of the file /tmp/modme.jpeg as the attribute value
- The description attribute is removed

Contributed Open Source Certificate Management Tools

A contributed suite of shell scripts that use the OpenSSL toolkit utilities to manage a CA and SSL certificates is available at

<http://www.openssl.org/contrib/ssl.ca-0.1.tar.gz>

MaXware Virtual Directory Configuration

A set of internal and external LDAP proxy servers was used in Boeing's challenge testing environment to provide the functions of LDAP query security checkpoint and dynamic directory lookup based on the email domain. The purpose of this section is to explain how the MaXware Virtual Directory (MVD) was configured as the LDAP proxy on Boeing's network firewall.

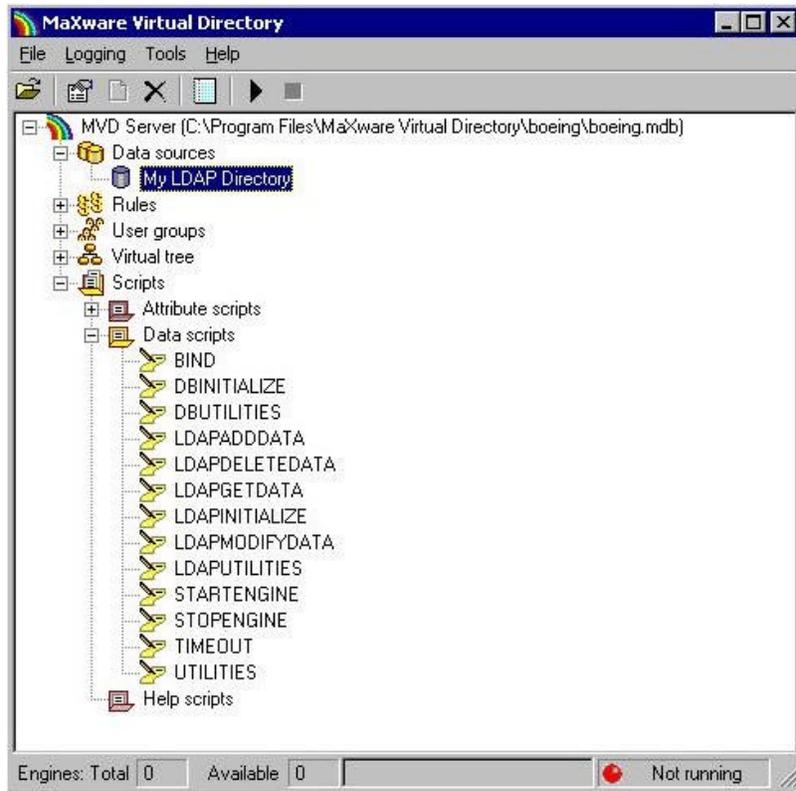
Scripts control all LDAP functions in MVD. The scripting language can be either VB script or Java script. In this testing, all scripts are written in VB script. All scripts and server settings are stored in a Microsoft Access database file. The product also supports other database formats (e.g., Microsoft SQL, Oracle or other data sources accessible through Open Data Base Connectivity— ODBC drivers).

Testing involved two Microsoft Access database files:

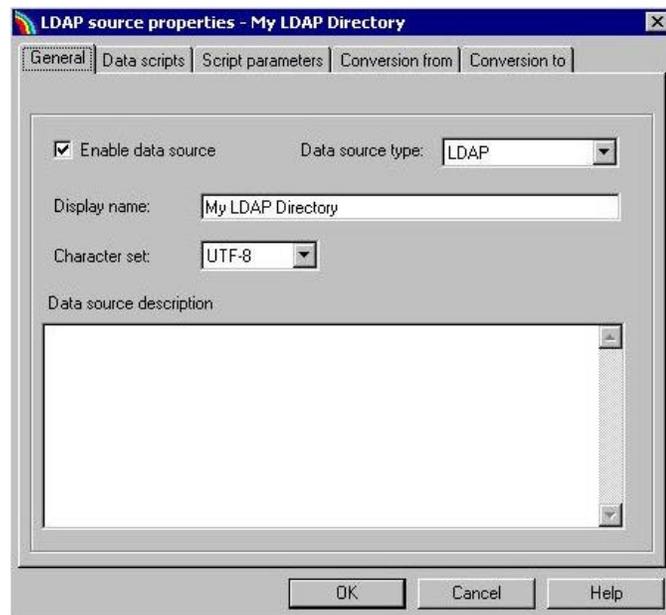
- "boeing.mdb"—store all the scripts and server settings
- "domain.mdb"—provide the mapping of email domain to the LDAP server and search base for querying for user's certificate

MaXware Virtual Directory Configuration Basics

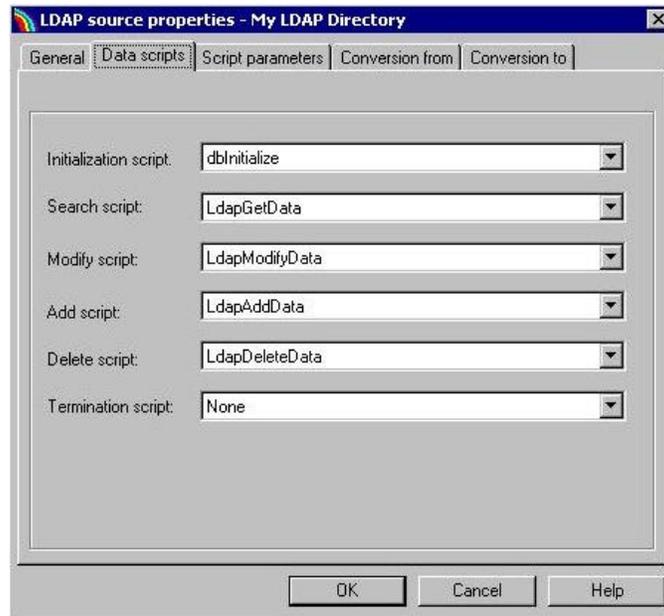
The MVD was installed on Microsoft Windows NT 4 SP6 server. This application interface opens the “boeing.mdb” for server setting and scripting controls.



See “My LDAP Directory” under “Datasource” for more settings.

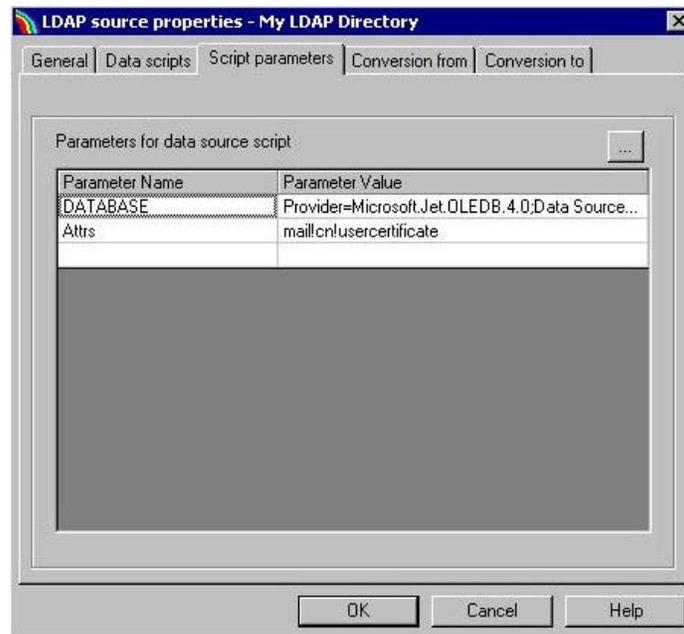


Step 1 Specify the data script names for various LDAP functions



Step 2 Specify script parameters

- “Database” parameter is to specify the “domain.mdb” for email domain and LDAP server mapping lookup
- “Attr” parameter is to limit the LDAP attributes that will be included in the query results



LDAPGETDATA Script

All LDAP function scripts and server configuration settings are stored in the boeing.mdb file. To configure the MVD as the proxy server for LDAP query, we customized the “LDAPGETDATA” script to accommodate the desired functions for external and internal proxies.

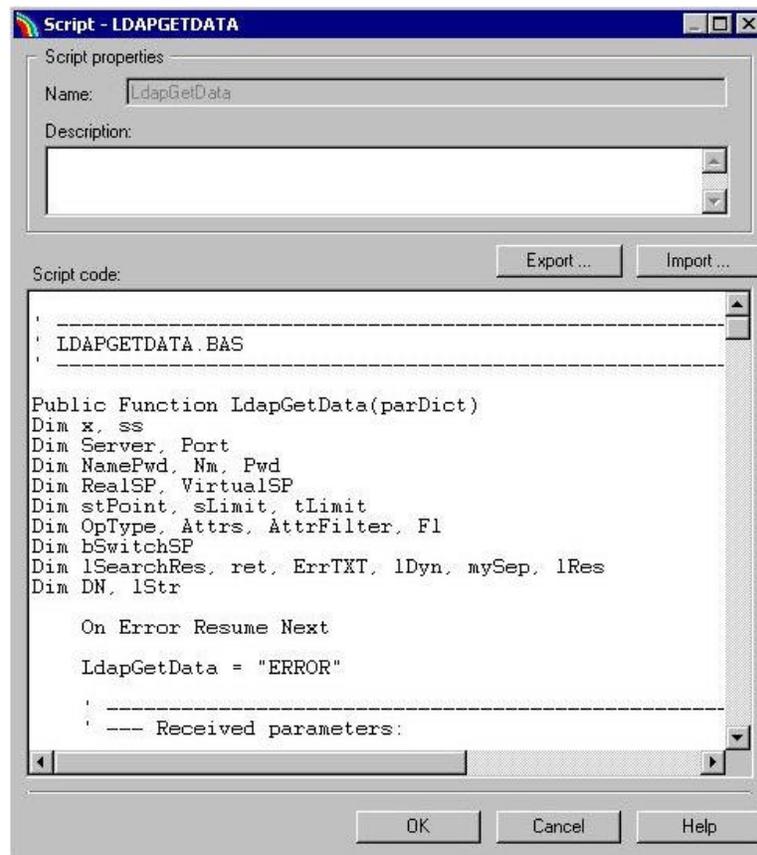
The only valid parameter for querying Boeing user’s certificate is the Boeing user’s email address.

- External LDAP proxy will check the validity of the email address in the LDAP query. Once the email address is deemed valid, the query will be forwarded to the internal LDAP proxy.
- Internal LDAP proxy will look up the Boeing email address from the internal domain.mdb file and decide where to retrieve the user’s X.509 certificate.

If the certificate exists, the internal LDAP proxy will return the query result to the external LDAP proxy, which will then return it to the person who initiated the query. The query result will contain only the Boeing user’s email address, which must be identical to the email address used to query the user, the user’s common name, and the user’s X.509 certificate. All other information stored in the Boeing’s directory will be filtered out.

The Boeing user directs all queries for non-Boeing certificates to the internal LDAP proxy. This arrangement eliminates the need to configure the user’s email client for every possible non-Boeing LDAP server for the non-Boeing certificate. When the internal LDAP proxy receives the query for a certificate of a non-Boeing person, it forwards the query to the external LDAP proxy. The external LDAP proxy will use the non-Boeing email address to look up the LDAP server name and search base from the domain.mdb file. If the email domain and LDAP server entry is found, the external LDAP proxy will query for certificate on behalf of the user and return the result. A unique error message will be returned to the Boeing user if the email domain and LDAP server entry are not found.

The window where one modifies the “LDAPGETDATA” script follows.



“LDAPGETDATA” script for external and internal LDAP proxy:

```

Public Function LdapAddData (param)
Dim stPoint
Dim lSearchRes, ret, ErrTXT, lDyn, mySep, lRes
Dim DN
Dim lStr
Dim exAddDict
    LdapAddData = "ERROR"
    On Error Resume Next
    '-----
    ' --- Received parameters:
    ' --- Scripting parameters + LDAP request parameters (search)
    ' --- DS_<Various data source parameters>
    ' --- NODE_<various node parameters>
    ' --- LDAP_StartingPoint
    ' --- LDAP_Dict
    '-----
    '-----
    ' --- List ALL received parameters, if desired
    '-----
    if False then
    Call ListAllParameterst (parDict)
    end if
    Server = FetchAttr (parDict, "DS", "SERVER")
    Port = MyCLng (FetchAttr (parDict, "DS", "PORT"))

```

```

NamePwd = FetchAttr (parDict, "DS", "NAMEPWD")
If Len(NamePwd) > 0 Then
    ss = Split(NamePwd, "|")
    Nm = ss(0)
    Pwd = ss(1)
Else
    Nm = ""
    Pwd = ""
End If
' -----
' --- if we connect to the LDAP server with the SAME starting point
' --- as the LDAP's servers starting point, the following fields
' --- should be empty. Otherwise, we HAVE to switch between the real and
' --- virtual starting point of the server
' -----
RealSP = FetchAttr(parDict, "NODE", "REALSP")
VirtualSP = FetchAttr(parDict, "NODE", "VIRTUALSP")
' -----
' --- Fetch rest of the LDAP parameters
' -----
stPoint = Trim(FetchAttr(parDict, "LDAP", "STARTINGPOINT"))
Set exAddDict = FetchAttr(parDict, "LDAP", "DICT")
' -----
' --- See the content of the dictionary !
' -----
Call Func.ListDict("mySep", exModifyDict)
' -----
' --- ACTION: ADD DATA !!!!
' -----
'DebugOut ("Server: " & Server)
'DebugOut ("Port: " & Cstr(Port))
' --- demonstrate possible exit
'LdapAddData = "ERROR:ID-234:misas error"
'Exit Function
' -----
' --- Switch starting points if necessary
' -----
bSwitchSP = SwitchSP(stPoint, VirtualSP, RealSP)
LdapAddData = Func.LdapAdd(Server,Port,Nm,Pwd,sLimit,tLimit,stPoint,exAddDict)
End Function

```

Domain.mdb—Email Domain to LDAP Server Mapping

The LDAP proxy uses the domain.mdb to lookup the LDAP server and the required search base to query for certificates based on the email domain. The database contains one table named "Directories" that has the following fields.

Field name	Description
maildomain	email domain name
StartPoint	Search base or the location in the LDAP schema that contains the user's certificate
Host	LDAP server host name
Port	TCP port number the LDAP server will answer the LDAP query. This can be either the standard LDAP port 389 or other custom port number.
Uname	User name for LDAP binding
Pword	User's password for LDAP binding

There is only one entry for each email domain of the Challenge participant in this database table. If there is duplicate entry for the same email domain in this table, the LDAP proxy will use the first one from sequential search and ignore the later one.

Public Key Infrastructure Framework

Policy Framework

When Alice sends an encrypted message to Bob, she must be certain that the public key she uses to encrypt the message is actually Bob's public key and not the public key of someone who is impersonating Bob. As stated in the PKI Tutorial chapter of this Toolkit, a digital certificate is used to prove that a public key actually belongs to a particular person or thing (the "subject" of the certificate). A CA issues the digital certificate. The degree to which a certificate user (i.e., Alice) can trust the certificate issued to the subject (i.e., Bob) depends upon the "Certificate Policies" and "Certification Practices" the CA uses to verify the subject's identity when issuing the certificate.

To meet the needs of users, CAs may provide a range of digital certificates that vary according to "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements."¹ These rules are found in a Certificate Policy ("CP") and may be used by a certificate user to determine if a certificate "is sufficiently trustworthy for a particular purpose."² A Certification Practice Statement ("CPS") is a detailed description of the practices followed by a CA in issuing and managing certificates.

While a CP is typically eight to 10 pages and a CPS is typically 40 to 80 pages, an average end user does not care about the detailed cryptographic methods or security procedures that are used. The user's primary concern is the validity of the certificate and his or her liability (or exposure) for relying on the certificate. A PKI Disclosure Statement ("PDS") is a simplified document that is designed to assist users in making informed trust decisions.

A Relying Party Agreement is a contract between a Certificate Authority and a "Relying Party" who uses a certificate and is analogous to a software license. A typical Relying Party Agreement is one or two pages. Lawyers point out that there is little or no case law to establish the validity and enforceability of such agreements.

Certificate Policy

The following section is copied from RFC 2527, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," March 1999

When a certification authority issues a certificate, it is providing a statement to a certificate user (i.e., a relying party) that a particular public key is bound to a particular entity (the certificate subject). However, the extent to which the certificate user should rely on that statement by the CA needs to be assessed by the certificate user. Different certificates are issued following different practices and procedures, and may be suitable for different applications and/or purposes.

The X.509 standard defines a certificate policy as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements"³. An X.509 Version 3 certificate may contain an indication of certificate policy, which may be used by a certificate user to decide whether or not to trust a certificate for a particular purpose.

¹ ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information Technology—Open Systems Interconnection: The Directory: Authentication Framework," 1997 edition.

² Chokhani, S. and W. Ford, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," RFC 2527, March 1999

³ ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information Technology—Open Systems Interconnection: The Directory: Authentication Framework," 1997 edition.

A certificate policy, which needs to be recognized by both the issuer and user of a certificate, is represented in a certificate by a unique, registered Object Identifier. The registration process follows the procedures specified in ISO/IEC and ITU standards. The party that registers the Object Identifier also publishes a textual specification of the certificate policy, for examination by certificate users. Any one certificate will typically declare a single certificate policy or, possibly, be issued consistent with a small number of different policies.

Certificate policies also constitute a basis for accreditation of CAs. Each CA is accredited against one or more certificate policies which it is recognized as implementing. When one CA issues a CA-certificate for another CA, the issuing CA must assess the set of certificate policies for which it trusts the subject CA (such assessment may be based upon accreditation with respect to the certificate policies involved). The assessed set of certificate policies is then indicated by the issuing CA in the CA-certificate. The X.509 certification path processing logic employs these certificate policy indications in its well-defined trust model.

CERTIFICATE POLICY EXAMPLES

For example purposes, suppose that the International Air Transport Association (IATA) undertakes to define some certificate policies for use throughout the airline industry, in a public-key infrastructure operated by IATA in combination with public-key infrastructures operated by individual airlines. Two certificate policies are defined—the IATA General-Purpose policy, and the IATA Commercial-Grade policy.

The IATA General-Purpose policy is intended for use by industry personnel for protecting routine information (e.g., casual electronic mail) and for authenticating connections from World Wide Web browsers to servers for general information retrieval purposes. The key pairs may be generated, stored, and managed using low-cost, software-based systems, such as commercial browsers. Under this policy, a certificate may be automatically issued to anybody listed as an employee in the corporate directory of IATA or any member airline who submits a signed certificate request form to a network administrator in his or her organization.

The IATA Commercial-Grade policy is used to protect financial transactions or binding contractual exchanges between airlines. Under this policy, IATA requires that certified key pairs be generated and stored in approved cryptographic hardware tokens. Certificates and tokens are provided to airline employees with disbursement authority. These authorized individuals are required to present themselves to the corporate security office, show a valid identification badge, and sign an undertaking to protect the token and use it only for authorized purposes, before a token and a certificate are issued.

X.509 CERTIFICATE FIELDS

The following extension fields in an X.509 certificate are used to support certificate policies:

Certificate Policies extension;
Policy Mappings extension; and
Policy Constraints extension

Certificate Policies Extension

The Certificate Policies extension has two variants—one with the field flagged non-critical and one with the field flagged critical. The purpose of the field is different in the two cases.

A non-critical Certificate Policies field lists certificate policies that the certification authority declares are applicable. However, use of the certificate is not restricted to the purposes indicated by the applicable policies. Using the example of the IATA General-Purpose and Commercial-Grade policies defined in Section 3.2, the certificates issued to regular airline employees will contain the object identifier for certificate policy for the General-Purpose policy. The certificates issued to the employees with disbursement authority will contain the object identifiers for both the

General-Purpose policy and the Commercial-Grade policy. The Certificate Policies field may also optionally convey qualifier values for each identified policy; use of qualifiers is discussed in Section 3.4.

The non-critical Certificate Policies field is designed to be used by applications as follows. Each application is pre-configured to know what policy it requires. Using the example in Section 3.2, electronic mail applications and Web servers will be configured to require the General-Purpose policy. However, an airline's financial applications will be configured to require the Commercial-Grade policy for validating financial transactions over a certain dollar value.

When processing a certification path, a certificate policy that is acceptable to the certificate-using application must be present in every certificate in the path (i.e., in CA-certificates as well as end entity certificates).

If the Certificate Policies field is flagged critical, it serves the same purpose as described above but also has an additional role. It indicates that the use of the certificate is restricted to one of the identified policies (i.e., the certification authority is declaring that the certificate must only be used in accordance with the provisions of one of the listed certificate policies). This field is intended to protect the certification authority against damage claims by a relying party who has used the certificate for an inappropriate purpose or in an inappropriate manner, as stipulated in the applicable certificate policy definition.

For example, the Internal Revenue Service might issue certificates to taxpayers for the purpose of protecting tax filings. The Internal Revenue Service understands and can accommodate the risks of accidentally issuing a bad certificate (e.g., to a wrongly-authenticated person). However, suppose someone used an Internal Revenue Service tax-filing certificate as the basis for encrypting multi-million-dollar-value proprietary secrets which subsequently fell into the wrong hands because of an error in issuing the Internal Revenue Service certificate. The Internal Revenue Service may want to protect itself against claims for damages in such circumstances. The critical-flagged Certificate Policies extension is intended to mitigate the risk to the certificate issuer in such situations.

Policy Mappings Extension

The Policy Mappings extension may only be used in CA-certificates. This field allows a certification authority to indicate that certain policies in its own domain can be considered equivalent to certain other policies in the subject certification authority's domain.

For example, suppose the ACE Corporation establishes an agreement with the ABC Corporation to cross-certify each other's public-key infrastructures for the purposes of mutually protecting electronic data interchange (EDI). Further, suppose that both companies have pre-existing financial transaction protection policies called ace-e-commerce and abc-e-commerce, respectively. One can see that simply generating cross certificates between the two domains will not provide the necessary interoperability, as the two companies' applications are configured with and employee certificates are populated with their respective certificate policies. One possible solution is to reconfigure all of the financial applications to require either policy and to reissue all the certificates with both policies. Another solution, which may be easier to administer, uses the Policy Mapping field. If this field is included in a cross-certificate for the ABC Corporation certification authority issued by the ACE Corporation certification authority, it can provide a statement that the ABC's financial transaction protection policy (i.e., abc-e-commerce) can be considered equivalent to that of the ACE Corporation (i.e., ace-e-commerce).

Policy Constraints Extension

The Policy Constraints extension supports two optional features. The first is the ability for a certification authority to require that explicit certificate policy indications be present in all subsequent certificates in a certification path. Certificates at the start of a certification path may be considered by a certificate user to be part of a trusted domain (i.e., certification authorities are

trusted for all purposes so no particular certificate policy is needed in the Certificate Policies extension). Such certificates need not contain explicit indications of certificate policy. However, when a certification authority in the trusted domain certifies outside the domain, it can activate the requirement for explicit certificate policy in subsequent certificates in the certification path.

The other optional feature in the Policy Constraints field is the ability for a certification authority to disable policy mapping by subsequent certification authorities in a certification path. It may be prudent to disable policy mapping when certifying outside the domain. This can assist in controlling risks due to transitive trust (e.g., a domain A trusts domain B, domain B trusts domain C, but domain A does not want to be forced to trust domain C).

RFC 2527 also sets forth an outline for a Certificate Policy or Certification Practice Statement. The use of a standard outline is not mandatory, but is encouraged in order to facilitate comparison of an organization's policies with other organizations. Nearly all Certificate Policies and Certification Practice Statements issued since 1999 have observed this standard outline.

1. OUTLINE OF A SET OF PROVISIONS

- 1.1 Overview
- 1.2 Identification
- 1.3 Community and Applicability
 - 1.3.1 Certification authorities
 - 1.3.2 Registration authorities
 - 1.3.3 End entities
 - 1.3.4 Applicability
- 1.4 Contact Details
 - 1.4.1 Specification administration organization
 - 1.4.2 Contact person
 - 1.4.3 Person determining CPS suitability for the policy

2. GENERAL PROVISIONS

- 2.1 Obligations
 - 2.1.1 CA obligations
 - 2.1.2 RA obligations
 - 2.1.3 Subscriber obligations
 - 2.1.4 Relying party obligations
 - 2.1.5 Repository obligations
- 2.2 Liability
 - 2.2.1 CA liability
 - 2.2.2 RA liability
- 2.3 Financial responsibility
 - 2.3.1 Indemnification by relying parties
 - 2.3.2 Fiduciary relationships
 - 2.3.3 Administrative processes
- 2.4 Interpretation and Enforcement
 - 2.4.1 Governing law
 - 2.4.2 Severability, survival, merger, notice
 - 2.4.3 Dispute resolution procedures
- 2.5 Fees
 - 2.5.1 Certificate issuance or renewal fees
 - 2.5.2 Certificate access fees
 - 2.5.3 Revocation or status information access fees
 - 2.5.4 Fees for other services such as policy information
 - 2.5.5 Refund policy
- 2.6 Publication and Repository
 - 2.6.1 Publication of CA information
 - 2.6.2 Frequency of publication

- 2.6.3 Access controls
- 2.6.4 Repositories
- 2.7 Compliance audit
 - 2.7.1 Frequency of entity compliance audit
 - 2.7.2 Identity/qualifications of auditor
 - 2.7.3 Auditor's relationship to audited party
 - 2.7.4 Topics covered by audit
 - 2.7.5 Actions taken as a result of deficiency
 - 2.7.6 Communication of results
- 2.8 Confidentiality
 - 2.8.1 Types of information to be kept confidential
 - 2.8.2 Types of information not considered confidential
 - 2.8.3 Disclosure of certificate revocation/suspension information
 - 2.8.4 Release to law enforcement officials
 - 2.8.5 Release as part of civil discovery
 - 2.8.6 Disclosure upon owner's request
 - 2.8.7 Other information release circumstances
- 2.9 Intellectual Property Rights

3. IDENTIFICATION AND AUTHENTICATION⁴

- 3.1 Initial Registration
 - 3.1.1 Types of names
 - 3.1.2 Need for names to be meaningful
 - 3.1.3 Rules for interpreting various name forms
 - 3.1.4 Uniqueness of names
 - 3.1.5 Name claim dispute resolution procedure
 - 3.1.6 Recognition, authentication and role of trademarks
 - 3.1.7 Method to prove possession of private key
 - 3.1.8 Authentication of organization identity
 - 3.1.9 Authentication of individual identity
- 3.2 Routine Rekey
- 3.3 Rekey after Revocation
- 3.4 Revocation Request

4. OPERATIONAL REQUIREMENTS⁵

- 4.1 Certificate Application
- 4.2 Certificate Issuance
- 4.3 Certificate Acceptance
- 4.4 Certificate Suspension and Revocation
 - 4.4.1 Circumstances for revocation
 - 4.4.2 Who can request revocation
 - 4.4.3 Procedure for revocation request
 - 4.4.4 Revocation request grace period
 - 4.4.5 Circumstances for suspension
 - 4.4.6 Who can request suspension
 - 4.4.7 Procedure for suspension request
 - 4.4.8 Limits on suspension period
 - 4.4.9 CRL issuance frequency (if applicable)
 - 4.4.10 CRL checking requirements

⁴All or some of the following items may be different for the various types of entities, i.e., CA, RA, and end entities.

⁵All or some of the following items may be different for the various types of entities, i.e., CA, RA, and end entities.

- 4.4.11 On-line revocation/status checking availability
- 4.4.12 On-line revocation checking requirements
- 4.4.13 Other forms of revocation advertisements available
- 4.4.14 Checking requirements for other forms of revocation advertisements
- 4.4.15 Special requirements re key compromise
- 4.5 Security Audit Procedures
 - 4.5.1 Types of event recorded
 - 4.5.2 Frequency of processing log
 - 4.5.3 Retention period for audit log
 - 4.5.4 Protection of audit log
 - 4.5.5 Audit log backup procedures
 - 4.5.6 Audit collection system (internal vs external)
 - 4.5.7 Notification to event-causing subject
 - 4.5.8 Vulnerability assessments
- 4.6 Records Archival
 - 4.6.1 Types of event recorded
 - 4.6.2 Retention period for archive
 - 4.6.3 Protection of archive
 - 4.6.4 Archive backup procedures
 - 4.6.5 Requirements for time-stamping of records
 - 4.6.6 Archive collection system (internal or external)
 - 4.6.7 Procedures to obtain and verify archive information
- 4.7 Key changeover
- 4.8 Compromise and Disaster Recovery
 - 4.8.1 Computing resources, software, and/or data are corrupted
 - 4.8.2 Entity public key is revoked
 - 4.8.3 Entity key is compromised
 - 4.8.4 Secure facility after a natural or other type of disaster
- 4.9 CA Termination

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS⁶

- 5.1 Physical Controls
 - 5.1.1 Site location and construction
 - 5.1.2 Physical access
 - 5.1.3 Power and air conditioning
 - 5.1.4 Water exposures
 - 5.1.5 Fire prevention and protection
 - 5.1.6 Media storage
 - 5.1.7 Waste disposal
 - 5.1.8 Off-site backup
- 5.2 Procedural Controls
 - 5.2.1 Trusted roles
 - 5.2.2 Number of persons required per task
 - 5.2.3 Identification and authentication for each role
- 5.3 Personnel Controls
 - 5.3.1 Background, qualifications, experience, and clearance requirements
 - 5.3.2 Background check procedures
 - 5.3.3 Training requirements
 - 5.3.4 Retraining frequency and requirements
 - 5.3.5 Job rotation frequency and sequence
 - 5.3.6 Sanctions for unauthorized actions

⁶All or some of the following items may be different for the various types of entities, i.e., CA, RA, and end entities.

- 5.3.7 Contracting personnel requirements
- 5.3.8 Documentation supplied to personnel

6. TECHNICAL SECURITY CONTROLS⁷

- 6.1 Key Pair Generation and Installation
 - 6.1.1 Key pair generation
 - 6.1.2 Private key delivery to entity
 - 6.1.3 Public key delivery to certificate issuer
 - 6.1.4 CA public key delivery to users
 - 6.1.5 Key sizes
 - 6.1.6 Public key parameters generation
 - 6.1.7 Parameter quality checking
 - 6.1.8 Hardware/software key generation
 - 6.1.9 Key usage purposes (as per X.509 v3 key usage field)
- 6.2 Private Key Protection
 - 6.2.1 Standards for cryptographic module
 - 6.2.2 Private key (n out of m) multi-person control
 - 6.2.3 Private key escrow
 - 6.2.4 Private key backup
 - 6.2.5 Private key archival
 - 6.2.6 Private key entry into cryptographic module
 - 6.2.7 Method of activating private key
 - 6.2.8 Method of deactivating private key
 - 6.2.9 Method of destroying private key
- 6.3 Other Aspects of Key Pair Management
 - 6.3.1 Public key archival
 - 6.3.2 Usage periods for the public and private keys
- 6.4 Activation Data
 - 6.4.1 Activation data generation and installation
 - 6.4.2 Activation data protection
 - 6.4.3 Other aspects of activation data
- 6.5 Computer Security Controls
 - 6.5.1 Specific computer security technical requirements
 - 6.5.2 Computer security rating
- 6.6 Life Cycle Technical Controls
 - 6.6.1 System development controls
 - 6.6.2 Security management controls
 - 6.6.3 Life cycle security ratings
- 6.7 Network Security Controls
- 6.8 Cryptographic Module Engineering Controls

7. CERTIFICATE AND CRL PROFILES

- 7.1 Certificate Profile
 - 7.1.1 Version number(s)
 - 7.1.2 Certificate extensions
 - 7.1.3 Algorithm object identifiers
 - 7.1.4 Name forms
 - 7.1.5 Name constraints
 - 7.1.6 Certificate policy Object Identifier
 - 7.1.7 Usage of Policy Constraints extension
 - 7.1.8 Policy qualifiers syntax and semantics

⁷All or some of the following items may be different for the various types of entities (i.e., CA, RA, and end entities).

- 7.1.9 Processing semantics for the critical certificate policy extension
- 7.2 CRL Profile
 - 7.2.1 Version number(s)
 - 7.2.2 CRL and CRL entry extensions

8. SPECIFICATION ADMINISTRATION

- 8.1 Specification change procedures
- 8.2 Publication and notification policies
- 8.3 CPS approval procedures

Certification Practice Statement

The following section is copied from RFC 2527, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," March 1999

The term certification practice statement (CPS) is defined by the ABA Guidelines as: "A statement of the practices which a certification authority employs in issuing certificates." In the 1995 draft of the ABA guidelines, the ABA expands this definition with the following comments:

A certification practice statement may take the form of a declaration by the certification authority of the details of its trustworthy system and the practices it employs in its operations and in support of issuance of a certificate, or it may be a statute or regulation applicable to the certification authority and covering similar subject matter. It may also be part of the contract between the certification authority and the subscriber. A certification practice statement may also be comprised of multiple documents, a combination of public law, private contract, and/or declaration.

Certain forms for legally implementing certification practice statements lend themselves to particular relationships. For example, when the legal relationship between a certification authority and subscriber is consensual, a contract would ordinarily be the means of giving effect to a certification practice statement. The certification authority's duties to a relying person are generally based on the certification authority's representations, which may include a certification practice statement.

Whether a certification practice statement is binding on a relying person depends on whether the relying person has knowledge or notice of the certification practice statement. A relying person has knowledge or at least notice of the contents of the certificate used by the relying person to verify a digital signature, including documents incorporated into the certificate by reference. It is therefore advisable to incorporate a certification practice statement into a certificate by reference.

As much as possible, a certification practice statement should indicate any of the widely recognized standards to which the certification authority's practices conform. Reference to widely recognized standards may indicate concisely the suitability of the certification authority's practices for another person's purposes, as well as the potential technological compatibility of the certificates issued by the certification authority with repositories and other systems.⁸

RELATIONSHIP BETWEEN CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT

The concepts of certificate policy and CPS come from different sources and were developed for different reasons. However, their interrelationship is important.

A certification practice statement is a detailed statement by a certification authority as to its practices that potentially needs to be understood and consulted by subscribers and certificate users

⁸American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Electronic Commerce, 1995.

(relying parties). Although the level of detail may vary among CPSs, they will generally be more detailed than certificate policy definitions. Indeed, CPSs may be quite comprehensive, robust documents providing a description of the precise service offerings, detailed procedures of the life-cycle management of certificates, and more—a level of detail which weds the CPS to a particular (proprietary) implementation of a service offering.

Although such detail may be indispensable to adequately disclose, and to make a full assessment of trustworthiness in the absence of accreditation or other recognized quality metrics, a detailed CPS does not form a suitable basis for interoperability between CAs operated by different organizations. Rather, certificate policies best serve as the vehicle on which to base common interoperability standards and common assurance criteria on an industry-wide (or possibly more global) basis. A CA with a single CPS may support multiple certificate policies (used for different application purposes and/or by different certificate user communities). Also, multiple different CAs, with non-identical certification practice statements, may support the same certificate policy.

For example, the Federal Government might define a government-wide certificate policy for handling confidential human resources information. The certificate policy definition will be a broad statement of the general characteristics of that certificate policy, and an indication of the types of applications for which it is suitable for use. Different departments or agencies that operate certification authorities with different certification practice statements might support this certificate policy. At the same time, such certification authorities may support other certificate policies.

The main difference between certificate policy and CPS can therefore be summarized as follows:

- (a) Most organizations that operate public or inter-organizational certification authorities will document their own practices in CPSs or similar statements. The CPS is one of the organization's means of protecting itself and positioning its business relationships with subscribers and other entities.
- (b) There is strong incentive, on the other hand, for a certificate policy to apply more broadly than to just a single organization. If a particular certificate policy is widely recognized and imitated, it has great potential as the basis of automated certificate acceptance in many systems, including unmanned systems and systems that are manned by people not independently empowered to determine the acceptability of different presented certificates.

In addition to populating the certificate policies field with the certificate policy identifier, a certification authority may include, in certificates it issues, a reference to its certification practice statement. A standard way to do this, using a certificate policy qualifier, is described [above]

Note: The above sections on Certificate Policy and Certification Practice Statements are copied from RFC 2527.

Full Copyright Statement for RFC 2527.

Copyright (C) The Internet Society (1999). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an “AS IS” basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

PKI Disclosure Statement

The PKI Disclosure Statement (PDS), a relative newcomer to PKI policy, is slowly gaining acceptance as a viable alternative to conventional policy heavyweights. The PDS began its life as an Internet Engineering Task Force Internet draft that subsequently expired. Since then, the American Bar Association has picked it up as an appendix to its PKI Evaluation Guidelines (PEG), as has the European Telecommunications Standards Institute (ETSI) Security Technical Committee.

While a CP is typically eight to 10 pages and a CPS is 40 to 80 pages, a PDS should be no more than two pages. The PDS still covers the critical items, such as the warranties, limitations, and obligations that legally bind each party. However, a PDS bears more likeness to an End User License Agreement (EULA) or cardholder agreement than a conventional policy document.

The average user doesn't care what cryptographic methods are used, or what specific security measures are taken. The user's primary concern is his or her liability under different scenarios. For example, the fact that a CA uses a hardware token to back up its private keys is likely to be important only to the CA. On the other hand, stating clearly that the relying party is responsible for ensuring the validity of all certificates prior to a transaction is noteworthy for all parties.

A PDS is a simple checklist to ensure that two organizations have generally equivalent security practices before entering a trusted relationship. The document should target PKI end users and those individuals looking to cross-certify with the organization. A PDS also limits liability. For example, a company may issue a PDS that stipulates that company-issued certificates are to be used for business purposes only. If a corporate user then uses his certificate to buy DVDs over the Internet, the user wouldn't be covered by the organization's policies.

A CPS typically involves issuers who follow documented policies and if there is a problem, resolve it by themselves. The goal of a PDS is to clearly identify where responsibilities lie. As such, a PDS is more than a document designed to protect the issuer; a PDS defines the relationship between all involved parties.

Commercial operations that have embraced the PDS generally make their CPS available; however, the signed contract is in the form of a PDS. Entrust's Entrust.NET is a good example of this arrangement. For those organizations that want to move to a more lightweight policy process, a PDS can be retrofitted without significant difficulty, so long as it conforms to current practices. Those starting with a clean slate will likely want to develop their PDS, build their CPS based on it and finish off with technical procedures based on their CPS.

A common problem within large organizations is effectively managing multiple cross-certifications. For instance, if you cross-certify with a government agency, you must meet all its security policy requirements. If later you want to cross-certify with a large financial organization, that organization's requirements will likely conflict with the government policies you've already matched. In other words, to conform to one, you must break compliance with the other. The bulk and detail of a CP/CPS generally cause incompatibilities that are difficult, but by no means impossible, to reconcile. Because a PDS is designed to use business rather than technical terms, there's a greater chance of meeting success with such a scenario.

Similar to most policy measures, a PDS isn't a cookie-cutter solution. Nor is it right for everyone. Governments and large businesses likely will find more value in the added detail a CP/CPS offers. Other organizations may want to use a PDS, but develop a CP/CPS for internal audits.

The following is excerpted from Appendix 6 of the American Bar Association Information Security Committee's *PKI Assessment Guidelines*.

Certificate policies (CPs) and certification practice statements (CPSs) are generally very detailed documents containing complex legal and technical information. Although such a large amount of complex terms and expressions may be essential to ensure the proper operation, legal certainty and full disclosure within a public key infrastructure (PKI), many PKI users, especially consumers, are likely to find these documents difficult to read, let alone comprehend. Consequently, there is often a need for a supplemental and simplified instrument to assist PKI users in making informed trust decisions. In response, members of the International Chamber of Commerce (ICC), in an informal cooperative effort with the Information Security Committee of the American Bar Association and other groups, developed a draft PKI Disclosure Statement (PDS). A PDS is a supplementary document that provides a concise, "clear and conspicuous" framework to disclose and emphasize critical information about the policies and practices of a Certificate Authority, or a PKI, that is normally addressed in much greater detail by an associated CP or CPS.⁹

A PDS is not meant to substitute for a fully detailed CP, although, strictly speaking, a PDS may satisfy the strict X.509 requirements to qualify as a certificate policy.¹⁰ As such, a PDS may function as a substitute for a larger CP in some limited situations, for example, when a relying party needs to decide quickly if it will rely on a previously unfamiliar CA's certificates, or when a CA wishes to conform simultaneously with more than one CP (i.e., when a CA wishes to participate in more than one "community of interest" by having its certificates accepted by the relying parties of one or more other CAs, and the CAs have not previously coordinated their CPs, and the CA in question does not necessarily want to (or cannot) amend its larger CP to resolve minor differences with the other CA's CPs).

The following table represents the PDS categories, listing a section for each defined *statement type* (category) and a corresponding *descriptive statement* that may include hyperlinks or computer references to the relevant CP or CPS sections.

Statement Types	Statement Descriptions
CA contact information	Name, location and relevant contact information for the CA.
Certificate type, validation procedures and usage	Description ¹¹ of each class/type of certificate issued by the CA ¹² , corresponding validation procedures ¹³ , and any restrictions on certificate usage ¹⁴ .
Reliance limits	Reliance limits, if any.

⁹The PDS has also been included as a formal annex to Policy Requirements for Certification Authorities Issuing Qualified Certificates 38-39, European Telecommunications Standards Institute (ETSI TS 101456 v.1.1.1 Dec. 2000)

¹⁰X.509 defines a certificate policy as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements."

¹¹Including the corresponding certificate policy object identifier that must also be included in the certificates.

¹²Alternatively, there can be separate PDSs for each type or class of certificate.

¹³May simply reference the X.509 certificate processing rules.

¹⁴Including the requirements to qualify as a subscriber or relying party and any restrictions on the applications for which the certificates are approved to be used.

Statement Types	Statement Descriptions
Obligations of subscribers	Description of, or reference to, the critical subscriber obligations ¹⁵ .
Certificate status checking obligations of relying parties	Extent to which relying parties are obligated to check certificate status, and references to further explanation ¹⁶ .
Limited warranty and disclaimer/Limitation of liability	Summary of the warranty ¹⁷ , disclaimers, limitations of liability and any applicable warranty or insurance programs.
Applicable agreements, Certification Practice Statement, Certificate Policy	Identification and references to applicable agreements, CPS, CP ¹⁸ .
Privacy policy	Description of and reference to the applicable privacy policy, if any.
Refund policy	Description of and reference to the applicable refund policy, if any.
Applicable law and dispute resolution	Statement of the choice of law and dispute resolution mechanism.
CA and repository licenses, trust marks, and audit	Summary of any governmental licenses, seal programs and a description of the audit process ¹⁹ and, if applicable, the audit firm.

Relying Party Agreements

A Relying Party Agreement is an agreement between a Certificate Authority and a party who uses a certificate. The purpose of the Relying Party Agreement is to define the duties, responsibilities, and terms between the Certificate Authority and the user who relies on the certificate. For example, a Relying Party Agreement may require the user to check that a certificate has not been revoked. However, there is little or no case law to establish the validity and enforceability of a Relying Party Agreement. The Information Security Committee of the American Bar Association has said that

The relationship between a certification authority and subscriber may be primarily contractual, whereby a subscriber and certification authority will agree to reinforce and enhance the subscriber's digital signature capability in exchange for a fee or other consideration. The duties of a certification authority to a third party relying on a certificate are rooted mainly in legal proscriptions against fraud and negligent misrepresentation. The duties of a subscriber to a person who relies upon the subscriber's certificate and digital signatures verified using that certificate, rest upon principles of both contract and tort.²⁰

For more discussion of the legal aspects of Relying Party Agreements, refer to the American Bar Association's Information Security Committee web site: <http://www.abanet.org/scitech/ec/isc/home.html>

Provisions that may commonly be found in a Relying Party Agreement may include:

- The permitted uses of the certificate. This involves the nature of certificate use (signing or encryption, or both), specific applications or business functions where the use of the certificate is specifically approved and specifically prohibited. For example, "certificates may be used for the

¹⁵Including the requirement to protect the confidentiality of the subscriber's private key and report actual or suspected compromise or change of material circumstances.

¹⁶Including the requirement to protect the integrity of the CA's public key, and, optionally, including instructions for retrieving certificates the CA issues.

¹⁷Including whether the CA warrants the accuracy of the information contained in the certificate.

¹⁸Particularly if the PDS is simply an extract from the CP.

¹⁹Including a reference to the current specific audit report.

²⁰Information Security Committee of the American Bar Association. Digital Signature Guidelines, Legal Infrastructure for Certification Authorities and Secure Electronic Commerce. 1996. p24.

following types of applications: information publishing, forms submission, correspondence, application workflow, electronic commerce.” “Certificates may be used only with applications that meet the following requirements: correctly establish, transfer and use the public and private keys, are capable of performing the appropriate certificate validity checking, report appropriate information and warnings to the user.”

- The identity of the permitted individuals or organizations that may be relying parties. For example, a self-signed certificate that is issued by a company may be restricted to employees and customers of that company.
- A requirement to perform cryptographic operations properly, using hardware and software that is appropriate for the assurance level.
- Limitations upon liability and indemnities.
- Applicable law.

Technical Procedures

Certificate Exchange

Out-of-Band Root Certificate Delivery Method

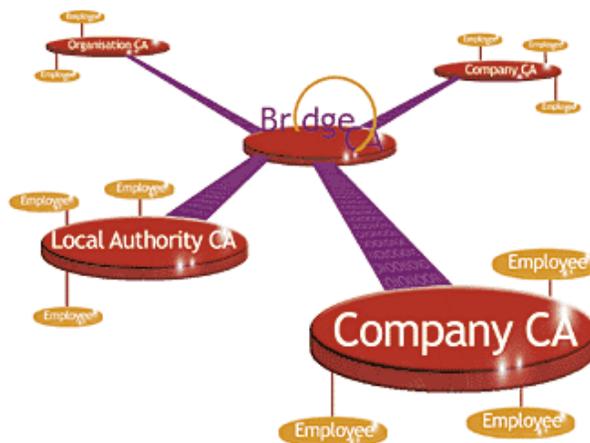
The root certificate shall be stored on unalterable media such as a CD-ROM or hardware token. Floppies and magnetic tape shall not be used for root certificate storage. Root certificates for use in the Secure Messaging Challenge must be delivered by a service that confirms delivery electronically or in writing. Examples are United States Postal Service certified or registered mail, FedEx, UPS, or Airborne.

Bridge-CA Solution

Another possibility for exchanging CA certificates of enterprises, organizations, or governments is to use a Bridge-CA solution.

As an example, the European Bridge-CA (www.bridge-ca.org) is an existing solution and is operated by the non-profit organization for The Promotion of Trusted Information and Communication Technology TeleTrust Germany Organization (www.teletrust.de) as an independent provider.

The European Bridge-CA takes the over role of the central contracting partner for trustworthy regulations on the whole network without questioning the trustworthiness and validity of PKIs or challenging their authority.



A prospective user who would like to participate in the Bridge-CA applies for admission to participate in the solution. Afterward a representative of the Bridge-CA checks the technical (e.g., interoperability) and organizational presuppositions for PKI integration in the Bridge-CA. After all tests are concluded and the participants' contracts are signed, the new participants take their CA certificates to a central point at which

participants must identify themselves. There the CA certificate will be registered and will be stored in the Bridge-CA according to the following sequence:

- The CA certificate will be stored in the centrally administrated list of the CA certificates of the other qualified participants
- The Bridge-CA signs the list and guarantees the trustworthiness of the list
- The signed list is offered to the participants (e.g., by email or downloaded)

Using this approach guarantees that every participant can trust that interoperability exists between the PKIs. Participants of the Bridge-CA can decide for themselves whether they recognize all or only some of the supplied CA certificates as reliable. This means that every participant decides for himself which CA certificates he imports in the certificate store of his email systems.

In the future the collection of the CA certificates is planned not only at a central point, but the project team also works on the arrangement at local collection places.²¹

Certificate Maintenance

Certificate Renewal

When a Certificate Authority issues a certificate, the certificate is given an expiration date. There are two main reasons a certificate is given an expiration date.

- The renewal of an expiring certificate gives the CA an opportunity to revalidate the identity and eligibility of the person or object of the certificate and automatically purges the system of certificates of terminated or deceased employees.
- Given a sufficient number of encrypted texts, sufficient time, and sufficient computing power, an attacker could compromise a private key. A renewal of a certificate provides a schedule for rekeying (i.e., changing the key pairs), if the certificate policies specify such a scheduled change.

The validity period of a certificate is specified in the Certificate Policy or Certification Practice Statement. In setting the validity period of a certificate, one should consider the following factors:

- Length of keys (longer keys are more resistant to cryptanalysis)
- Strength of the cryptographic algorithm
- Keys' usages (certificates used for critical applications should have shorter validity periods)

In some cases, there may be statutory limits placed on the validity of a certificate. For example, the Federal Republic of Germany places a five-year limit on the validity period of a certificate.²²

Certificate renewal is the process by which a new certificate is issued to replace an expired (or expiring) certificate. Certificate renewal may or may not also involve rekeying (see below), depending upon the required level of assurance and the certificate policies. The procedure by which a subscriber obtains a renewed certificate varies by CA, and is usually specified in the CA's operational procedures.

Certificate Rekeying

Rekeying involves generating a new key pair and issuing a certificate for the new public key. Messages that have been encrypted with the old public key cannot be decrypted with the new private key, so users must make some provision to convert old encrypted messages. The digital signatures of messages that have been signed with the old key pair contain the old public key, so the digital hash can still be deciphered. However, the legal standing of a signed document once the certificate has expired is questionable (a work around is the use of a time-stamping service that provides a verifiable statement that a document was digitally signed while the signing certificate was valid).

Distributing Renewed/Rekeyed Certificates

²¹Many thanks to Mr Peter Steiert, Project Manager European Bridge-CA by TeleTrust Germany Organization for the support and information for this section.

²²See *Digital Signature Ordinance (Signaturverordnung-SigV)*, F.R.G. 1997, available at <<http://www.iid.de/iukdg/gesetz/sigve.html>>

The procedure for distributing renewed/rekeyed certificates will depend on whether the certificate is a subscriber certificate or the CA's root certificate, and whether the key pair has changed.

A renewal of a subscriber certificate without rekeying can be handled by signed email or via a secure web site because the transaction can be signed and encrypted while the old certificate is still valid. Some programs, such as Lotus Notes, are capable of automatically "pushing" a renewed certificate when the user connects to the server (now this automation only applies to renewal of Notes certificates; X.509 v.3 certificate renewals still require user participation)

Rekeying CA certificates as their expiration date approaches raises the issue of how the new CA certificates resulting from the rekeying process can be distributed in an authenticated fashion. The same out-of-band procedures used to convey the original certificate may be used to transmit the renewed root certificate. The following paragraph is taken from the American Bar Association's *PKI Assessment Guidelines*.²³

A PKI, however, may also implement additional controls to demonstrate the transition from the old CA certificate to the new CA certificate. For instance, signing the new key with the old key before its expiration or compromise can authenticate a CA rekey.

PKIX protocols require the issuance of three certificates that are posted to the repository:

- New CA public key signed with the old CA private key,
- Old CA public key signed with the new CA private key, and
- New CA public key signed with the new CA private key.

Another common technique is to include a cryptographic hash of the next CA key in the current CA self-signed certificate. This hash can then be used to authenticate the new key when it is used in a self-signed certificate.

The rekeying of a subscriber certificate cannot make use of the old certificate for signing and encryption. Therefore, procedures must be specified for out-of-band certificate exchange to prevent tampering with the certificate and to ensure the security of a subscriber's private key while in transit. Organizations with a large number of mobile or remote users must take into consideration the logistics of distributing the renewed/rekeyed certificates in a way that prevents compromise of the certificates and key pairs.

Certificate Revocation

Certificates must be revoked if a key is compromised or if compromise is suspected. Another typical reason for revoking a certificate is that the subject of the certificate is deceased, changes business affiliation, or changes employment status.

Certificate Revocation List (CRL) A Certificate Revocation List (CRL) is a digitally signed list of revoked certificates that is generally issued by the Certificate Authority. This list is updated on a scheduled basis and distributed to relying parties.

Online Certificate Status Protocol (OCSP) Due to the latency involved in publishing a CRL, a relying party may not receive notification of a revoked certificate in a timely manner. On-line mechanisms may be used to communicate the current (real-time or near real-time) status of a certificate. A widely used standard for determining the on-line status of a certificate is the IETF *Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)*, RFC 2560.

In the ideal world, users must check each time they use a certificate to ensure that the certificate has not expired or been revoked. However the Challenge did not make use of CRL or OCSP. Instead, removing a certificate from the directory revoked it. Any certificate that was found in the directory was accepted for the purpose of sending encrypted email.

²³American Bar Association, *PKI Assessment Guidelines, v0.30Public Draft for Comment*. June 18, 2001. p.218

Name Change

In cases of a subject's name change or status change, a new certificate must be issued so that the certificate matches the new name. Some situations that may require a new certificate include:

- Legal name change due to marriage, divorce, or court action
- Change in business affiliation, such as corporate merger or acquisition
- Change in location
- Change in email address
- Change in any extended attribute in a certificate

To ensure continuity for the subscriber, the old certificate should not be revoked until the subscriber has accepted the new certificate.

Physical Security

In current and future environments, cyber and physical infrastructures are and will be interdependent. Even though the Challenge focused on PKI security applications for email messages, organizations planning to implement one of the methods the Challenge used must also remember to follow best practices for physical security of the facilities themselves as well as workstations, servers, and other equipment. A fundamental practice is to have regularly scheduled backups.

As for corporate documents, companies may well want to secure (keep confidential) their Policies and Procedures as well as proprietary and financial information.

Companies determine the level of physical security required to protect their assets, including clients and data, often basing the amount spent on the value of what is being protected. Other issues need to be considered when planning for and maintaining physical security for data.

For more information on security, see the *Manager's Guide to Information Security* by Eliot Solomon and The Open Group Security Forum²⁴.

²⁴ Document number 205, ISBN 1-931-62406-2, also available on the web at www.opengroup.org.

Appendix 1. Sample Challenge PKI Disclosure Statement (Version 1)

1. **CA contact information:** The Open Group Challenge Management Team (referred to hereafter as the “CMT”).
2. **Certificate type, validation procedures and usages:** The Open Group EMA Forum* is issuing Class 1 certificates in a controlled public demonstration of secure email using public key technologies.
3. **Reliance limits:** The Open Group EMA Forum* and the participants in this demonstration (hereafter referred to as the “Challenge”) do not set reliance limits for certificates for the purposes of this demonstration. Reliance limits may be set by applicable law or by agreement when and if this project goes into production. See *Limitation of Liability*, below.
4. **Obligations of subscribers:** Subscribers must provide accurate information on their certificate applications, review the certificate to establish its accuracy before using it, reasonably protect their private keys from theft and unauthorized use by or disclosure to others, and notify the CMT upon suspected private key compromise.
5. **Certificate status checking obligations of relying parties:** A participant in the Challenge (the relying party) may justifiably rely upon a certificate only after confirming that the certificate has not been revoked or expired at <<http://insert URL here>> and determining that such certificate provides adequate assurances for its intended use.
6. **Limited warranty & disclaimer/Limitation of liability:** For purposes of this public demonstration and the advance testing for this demonstration, The Open Group and all participants in the Challenge neither accept nor imply a warranty of merchantability or fitness for any particular purpose. No liability is granted in the use of certificates for the purposes of the Challenge.
7. **Applicable agreements, Certification Practice Statement (CPS), Certificate Policy: (CP)** Each participant in this Challenge (“Subscriber”) must have in place a corporate CPS and CP in place. All participant CPSs in place for purposes of this Challenge shall be made viewable by any other Challenge participant or the CMT solely for purposes of the Challenge. This shall ensure that participant certificates are used in a manner consistent with and compliant with intra-participant exchange of certificates. Each participant must reserve the right to withdraw from the Challenge if, upon viewing another participant’s CPS, the participant finds something in the content of the document which is against their business practices.
8. **Privacy policy:** Personal data is not shared without subscriber consent. The Challenge privacy policy is posted at <<http://insert URL here>>.
9. **Refund policy:** There is no refund policy.
10. **Applicable law and dispute resolution:** **We need advice on what law(s) we shall make this subject to.**
11. **CA and repository licenses, trust marks, and audit:** Participants in the Challenge shall provide their own certificates and publicly make the public keys available in some easily accessible repository in the Internet. Some participants not wishing to stand up their own CA can purchase certificates from a trusted third party such as VeriSign or Thawte so long as public keys are available on the Internet.

Note: This Open Group EMA Forum Challenge PKI Disclosure Statement is applicable to certificates issued solely for the Challenge.

* Effective April 2002, the EMA Forum is called the Messaging Forum.

Appendix 2. Sample Relying Party Agreement

BOEING RELYING PARTY AGREEMENT

This Subscriber Agreement (“Agreement”), between you and Boeing, will become effective on the date you submit the certificate application to _____. By submitting this Agreement (and corresponding certificate application) you are requesting that Boeing Certificate Authority issue a digital certificate to you for use in the _____ EMA Encryption Challenge 2001 and are expressing your agreement to the terms of this Subscriber Agreement.

Boeing S/MIME services for the _____ are governed by Boeing’s _____ Certification Practice Statement (the “CPS”) as amended from time to time, which is incorporated by reference into this Subscriber Agreement. The CPS is published on the Internet at <https://www.boeing.com>_____ and is available via E-mail from: _____. Amendments to the CPS are also posted in Boeing’s repository at _____.

Capitalized terms not defined by reference in this Agreement shall have the meaning given to them in the CPS.

The laws of the United States and the State of Washington shall govern the enforceability and interpretation of this Agreement, irrespective of choice of law provisions. You agree to be subject to the jurisdiction of the courts of the State of Washington. To the extent that you are not otherwise subject to the service of process in the State of Washington, service of process may be made on you by pre-paid certified mail with a proof of mailing receipt. Before invoking any dispute resolution mechanism (including litigation or arbitration) with respect to a dispute involving any aspect of your certificate, Boeing services, this Agreement, or the CPS, you agree to follow the procedures for dispute resolution set forth in the CPS.

I. Subscriber Obligations.

As a subscriber to the Boeing S/MIME encryption services for the _____, you agree to:

- Provide information regarding your certificate, identification, and authentication to the Remote Registration Agent that is accurate and complete to the best of your knowledge and belief.
- Promptly notify the Remote Registration Agent of any changes to the information you provide to Boeing, a Boeing Certificate Authority, or a Remote Registration Agent.
- Use your digital certificate exclusively for authorized and legal purposes and in accordance with the provisions of Boeing Inc. CPS.
- Protect your private key(s) at all times, in accordance with the Boeing, Inc. CPS, and in accordance with this Subscriber Agreement.
- Promptly notify and request the Remote Registration Agent to revoke your digital certificate if you have reason to believe or suspect the compromise or loss of control of your private key(s). Your notification must be made in the following way: _____ within [time frame].
- Abide by all the terms, conditions, and restrictions levied upon the use of your private key(s) and certificate(s). **[THESE NEED TO BE SPELLED OUT]**

II. Protection of your private key.

You acknowledge and agree

- that the Boeing Certificate Authority does not archive, keep, maintain, or otherwise store your private key.
- that you are ultimately responsible for the protection in all instances of your private key.
- to use industry standard security procedures to protect your private key from loss of control or compromise, including those procedures set forth in the CPS.

III. Warranties/Limitation of Liability.

[INCLUDE RELEVANT PORTIONS OF THE CORRESPONDING CPS ON WARRANTIES AND LIMITATIONS OF LIABILITY.]

THE BOEING CERTIFICATE AUTHORITY PROVIDES NO WARRANTIES AND DISCLAIMS ALL OTHER WARRANTIES, INCLUDING _____.

THE BOEING CERTIFICATE AUTHORITY LIMITS LIABILITY, AND EXCLUDES ALL LIABILITY FOR INCIDENTAL, CONSEQUENTIAL, AND PUNITIVE DAMAGES AS STATED IN THE CPS. THE LIABILITY CAPS ARE AS FOLLOWS:

CLASS II CERTIFICATES	\$0.
-----------------------	------

SEE THE CPS FOR IMPORTANT DETAILS.

IV. Confidentiality.

You acknowledge and agree that the existence of your digital certificate, information contained in your digital certificate, and all information in the public domain shall not be considered confidential. By applying for a digital certificate, you consent to Boeing's disclosure of the information contained in your certificate.

Boeing shall disclose, use, and share your name or other identifying information only in accordance with the CPS, and the Boeing privacy policy. The Boeing privacy policy can be found at www.boeing.com/repository.

You demonstrate your knowledge and acceptance of the terms and conditions of this Subscriber Agreement by clicking on the "I Accept" button below.

Appendix 3. MaXware Virtual Directory

Introduction

Over time, organizations will typically deploy a large number of data repositories storing many elements of business critical information. The complexity involved in accessing these data sources makes application integration, development and client configuration expensive for owner organizations.

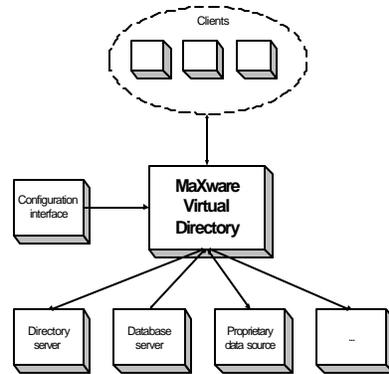
Meta Directory products have become a popular way of solving this problem by gathering information from multiple existing data sources into a common directory or database (Metastore). This provides a single entry point to the data, but the data is a copy of the original datastores. Changes to the source repositories and/or Metastore must be synchronized periodically.

Description

The Virtual Directory uses a different approach and provides real-time access to the original datastores. This means that through the Virtual Directory, clients are accessing the original data repositories directly so that any changes in the source repositories are instantly visible for the client (i.e., client does not experience update replicate delay from the source repositories to the metastore). Virtual directories also avoid some of the political fights over data ownership by keeping it where it originally resides.

The MaXware Virtual Directory can logically represent information from any number of disparate directories, databases, and other data repositories in a hierarchical directory tree. Users and applications can access the information from different views, based on their access rights and rules and filters that are customizable in the product.

Features like namespace conversions, schema adaptations and access control provide customers with a flexible solution that can continually grow and change to support various demands from current and future applications and for security and privacy without any changes to the underlying architecture and design of the existing data stores.



Specifications

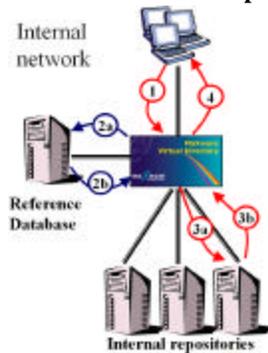
OS	User Interface: MS NT4/W2K Runtime engine: Java 2 VM (UNIX), MS NT/W2K	Supported Data Sources	JDBC, JNDI, LDAP and any source that can be programmatically accessed using Java API.
Protocols	LDAP version 3 SSL TLS	Expansion	MVD is fully customizable to meet the current and future requirements of the user organization.

MaXware Virtual Directory Referenced Lookup Examples

The referenced lookup solution is ideal when an organization has multiple internal and external repositories containing information on entries in separated domains and a reference database that contains a list of the domains and information on the host of the domains. Using this solution a client can search for information in several domains from a single entry point.

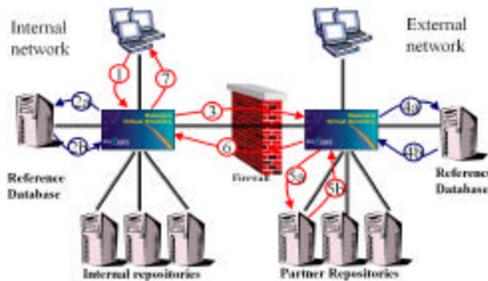
These scenarios show an organization that needs a single entry point for certificate lookups in many internal and external partner datastores. This allows secure message exchange without the need to synchronize certificates across the networks!

Internal user looks up internal entry



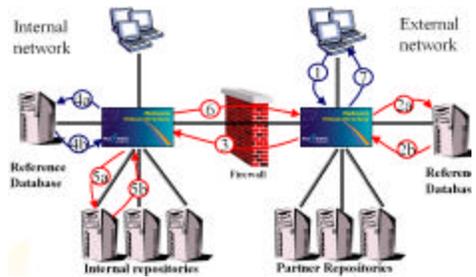
1. A search for information about “user@maxware.com” is issued
2. Virtual Directory looks for “maxware.com” in the reference database and returns a pointer to the correct repository
3. Virtual Directory searches the appropriate repository
4. The Virtual Directory reformats the results (if necessary) and returns it to the client

Internal user looks up external entry



1. A search for information about “user@partner.com” is issued
2. Virtual Directory looks for “partner.com” in the reference database and returns a pointer to the external Virtual Directory
3. Request is forwarded to the external Virtual Directory
4. The external Virtual Directory looks for connection details on “partner.com” in its reference database
5. Virtual Directory searches the defined repository
6. Results are sent back to the internal Virtual Directory
7. The internal Virtual Directory reformats the results (if necessary) and returns it to the client

External user looks up internal entry



1. A search for information about “user@maxware.com” is issued
2. The external Virtual Directory looks for “maxware.com” in the reference database and is directed to the internal Virtual Directory
3. Request is forwarded to the internal Virtual Directory
4. The internal Virtual Directory looks for data on “maxware.com” in its reference database and returns a pointer to the target repository
5. Virtual Directory searches the appropriate repository
6. Results are sent back to the external Virtual Directory
7. The internal Virtual Directory reformats the results (if necessary) and returns it to the client



*Boundaryless
Information Flow*

*Boundaryless Information Flow™
achieved through global interoperability
in a secure, reliable and timely manner*

vision



The Messaging Forum

The Messaging Forum promotes Boundaryless Information Flow with standards-based electronic messaging. The forum operates in such areas as Secure Messaging, Instant Messaging, Anti-Spam and Anti-Virus best practices, Unified Communications and VPIM (voice profile for internet messaging). It is focused on creating a broad awareness of electronic messaging issues using educational and technological tools.

The Messaging Forum works with other forums on mutual work areas of interest in Boundaryless Information Flow such as Identity Management, Access Control and PKI Guidelines and Manageability which are also relevant to the Directory Interoperability, Mobile Management and Security Forums.

Secure Messaging Toolkit

The Challenge

The Secure Messaging Challenge 2001 purpose was to enable organizations to exchange strongly encrypted email using a standards-based, vendor neutral architecture that does not require manual key exchange. The purpose of this Secure Messaging Toolkit is to document the lessons learned during the challenge planning, implementation, and testing.

Challenge Technical Requirements

- Use X.509 v.3 Certificate Authority (CA) Services; self-signed or purchased commercial certificates
- Use Rivest, Shamir, & Adleman (RSA) algorithm with minimum 1024-bit key length
- Provide standards-based directory services accessible via the public Internet; certificate stored in standard *userCertificate* attribute
- Use S/MIME compliant messaging clients capable of requesting certificates from the directory
- Provide S/MIME compliant email system
- Follow current standards regarding S/MIME, X.509 v.3 and LDAP v.3
- Use commercial, off-the-shelf (COTS) or open source products only

THE *Open* GROUP

- 44 Montgomery St., Suite 960
San Francisco, CA 94104 USA
Tel +1.415.374.8280
Fax +1.415.374.8293
(USA Sales Only)
1.800.916.OPEN (6736)
- 29B Montvale Avenue
Woburn, MA 01801
Tel +1.781.376.8200
Fax +1.781.376.9358
- Apex Plaza, Forbury Road
Reading, Berkshire RG1 1AX, UK
UK Free Phone
(0)800.072.9490
Tel +44 (0)118.950.8311
Fax +44 (0)118.950.0110

US \$69.90

G260

