

IBM®



ENVISION

LotuspHERE® 2005

DECISIONS





Lotusphere[®] 2005



ENVISION

DECISIONS

**BP115
Best Practices for Secure
Messaging with S/MIME**

**Marc Luescher
IBM Technical Support Switzerland
Daniel Nashed
Nash!Com Germany**



Please come meet and talk with us in the labs....

- Performance and TCO lab – Dolphin Europe 5&6
- Application Dev Lab – Dolphin Asia 3
- Meet the Developers Lab – Dolphin Asia 1&2
- Certification Prep Lab – Swan Peacock 1&2
- Certification Test Lab – Swan Lark 1&2
- Innovation Lab – Dolphin Europe 3&4
- Mobile Computing Lab – Dolphin Europe 7

Index

- Notes Secure Mail Backgrounder
- Secure E-Mail Landscape
- Notes/Domino CA Features and S/MIME Functions
- Some Important Domino X509 and S/MIME Processes
- Demo
- Other important PKI Vendors
- S/MIME Plug-ins and Gateways
- Lessons Learned



ENVISION

DECISIONS

Index

- **Notes Secure Mail Backgrounder**
- Secure E-Mail Landscape
- Notes/Domino CA Features and S/MIME Functions
- Some Important Domino X509 and S/MIME Processes
- Demo
- Other important PKI Vendors
- S/MIME Plug-ins and Gateways
- Lessons Learned

Secure e-mail (Notes / Standards)

- At about the same time SMTP was defined, PKI was developed. *PKI (Public Key Infrastructure)* is a secure system for a trusted third party (known as a Certificate Authority or CA) to provide digital identities to users and servers and to publish those identities using X.509 V3 digital certificates.
 - ◆ The identity consists of an asymmetrical key pair: a Public Key that anyone can use (thus the name) and a unique Private Key known only to the user.
 - ◆ This digital identity can then be used to exchange text securely by encryption using the key pair.

Internals of Lotus Notes Secure e-mail

- Notes uses a public and private key set to encrypt and decrypt data, as well as to validate digital signatures.
- The public and private key in a set are mathematically related to each other and are unique to your User ID.
 - ◆ Your public key is stored in your Notes certificate. Your certificate is stored in your User ID and the Domino Directory. Your private key is stored only in your User ID.
 - ◆ People can encrypt data they send you by using the public key from your certificate located in the Domino Directory. When you receive encrypted data, your private key in your User ID decrypts the data.

Secure e-mail between Notes and Internet (Encrypted mail)

- Notes to Notes
 - ◆ Easy
 - Send a message from Joe to Mike
 - ❖ Public/Private Key system
 - Native Notes PKI
- Notes to non-Notes
 - ◆ Not as easy
 - Send a message from Bubba to Mike
 - ❖ Again Public/Private system
 - Standards based PKI

Index

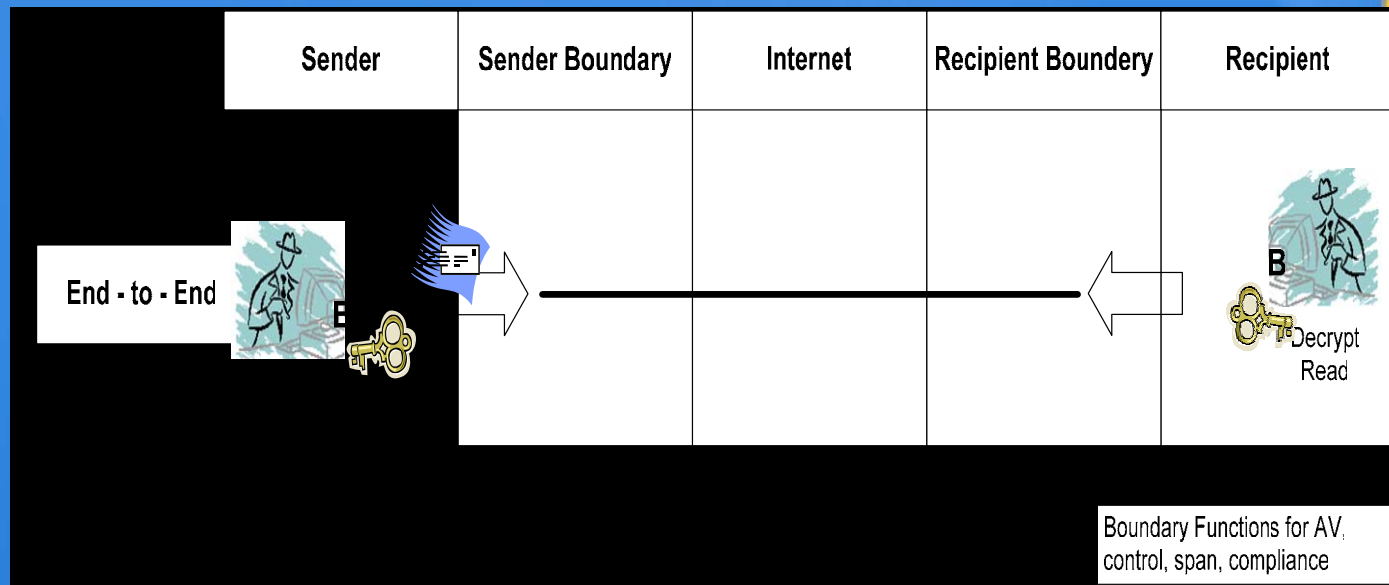
- Notes Secure Mail Backgrounder
- **Secure E-Mail Landscape**
- Notes/Domino CA Features and S/MIME Functions
- Some Important Domino X509 and S/MIME Processes
- Demo
- Other important PKI Vendors
- S/MIME Plug-ins and Gateways
- Lessons Learned

Secure E-Mail Landscape

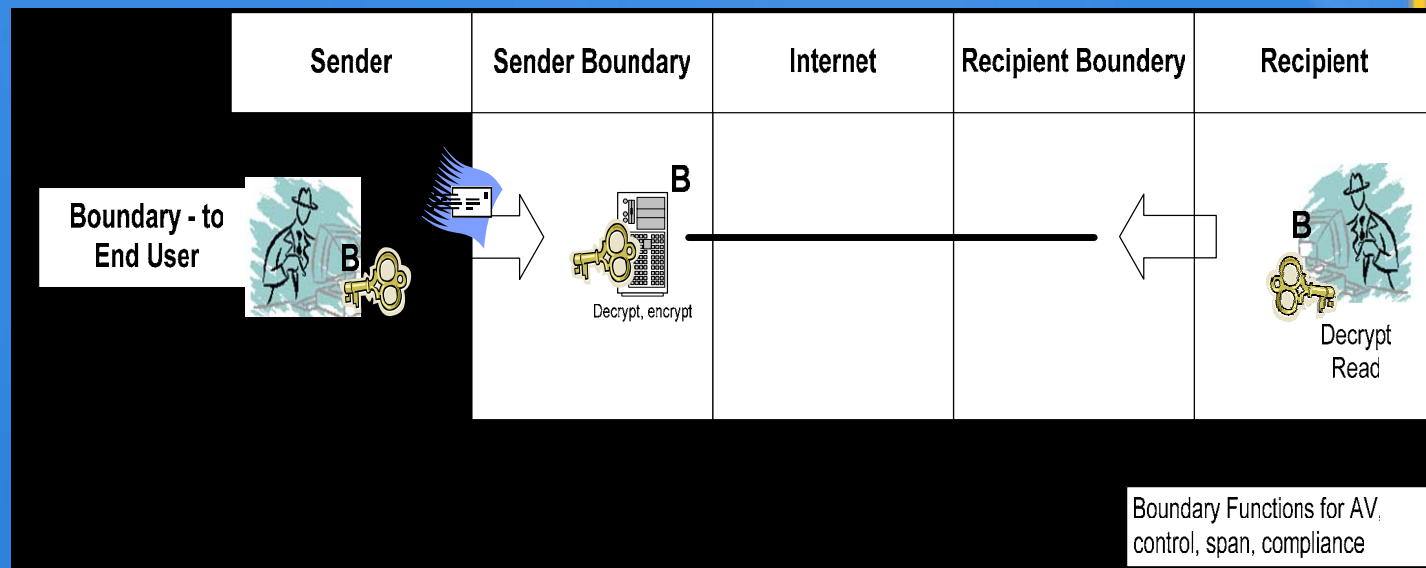
- Adoption rate of S/MIME for Internal Mails is currently only about 5%-10%
- Business requirements for secure mail are confirmed for many B2B and B2C S/MIME scenarios
- PKI adoption rate is still far behind market expectations and therefore use of S/MIME for B2C is restricted
- S/MIME based secure email is still not as easy to use as it could be
- Many news vendors are trying with innovative new solutions to make it easier and accessible to end users
- Only a few companies have deployed S/MIME based security solutions with customers and business partners. Most of them are still using either PGP or WINZIP encrypted file attachments instead to transfer secure informations.



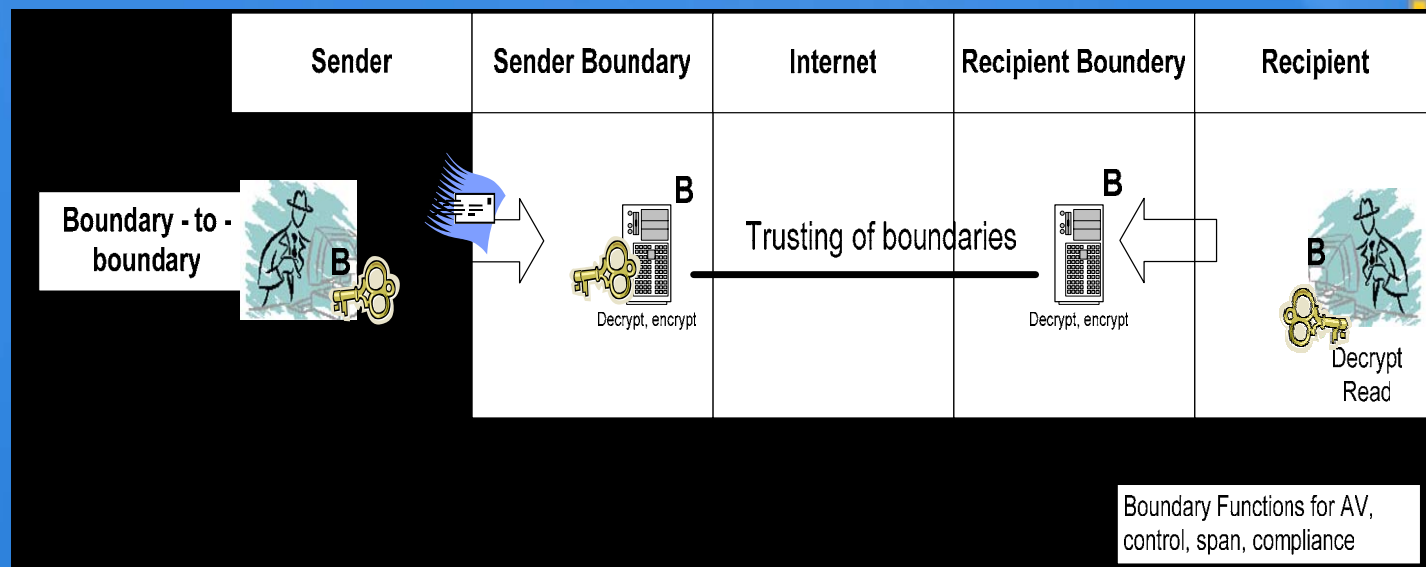
End-to-End Scenario



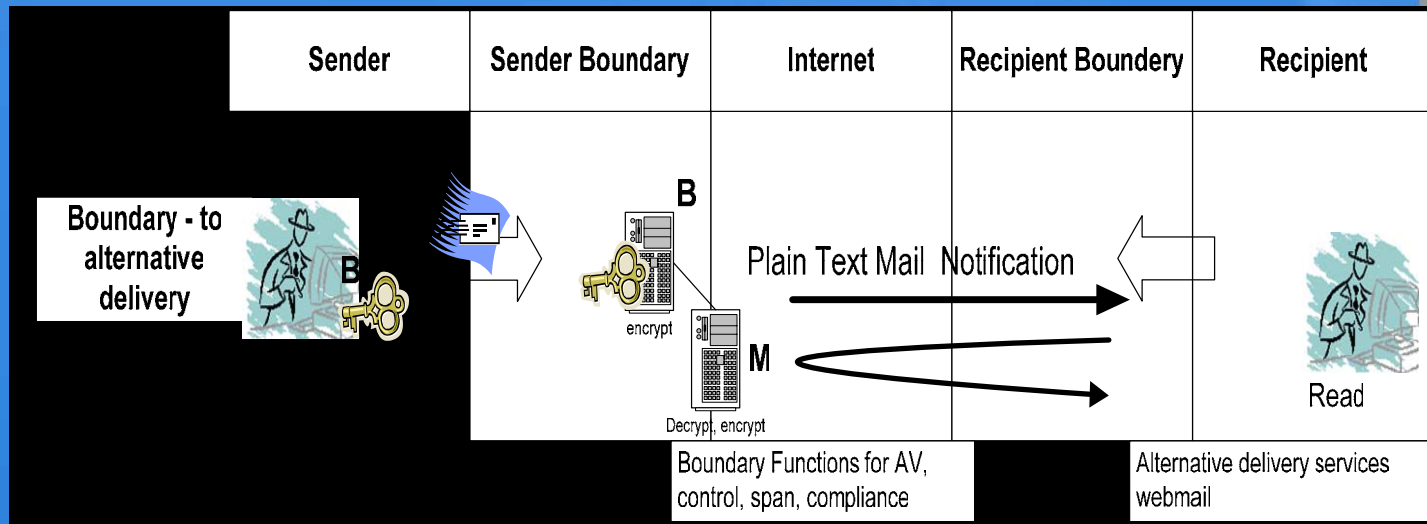
Boundary-to-End-User Scenario



Boundary-to-Boundary Scenario

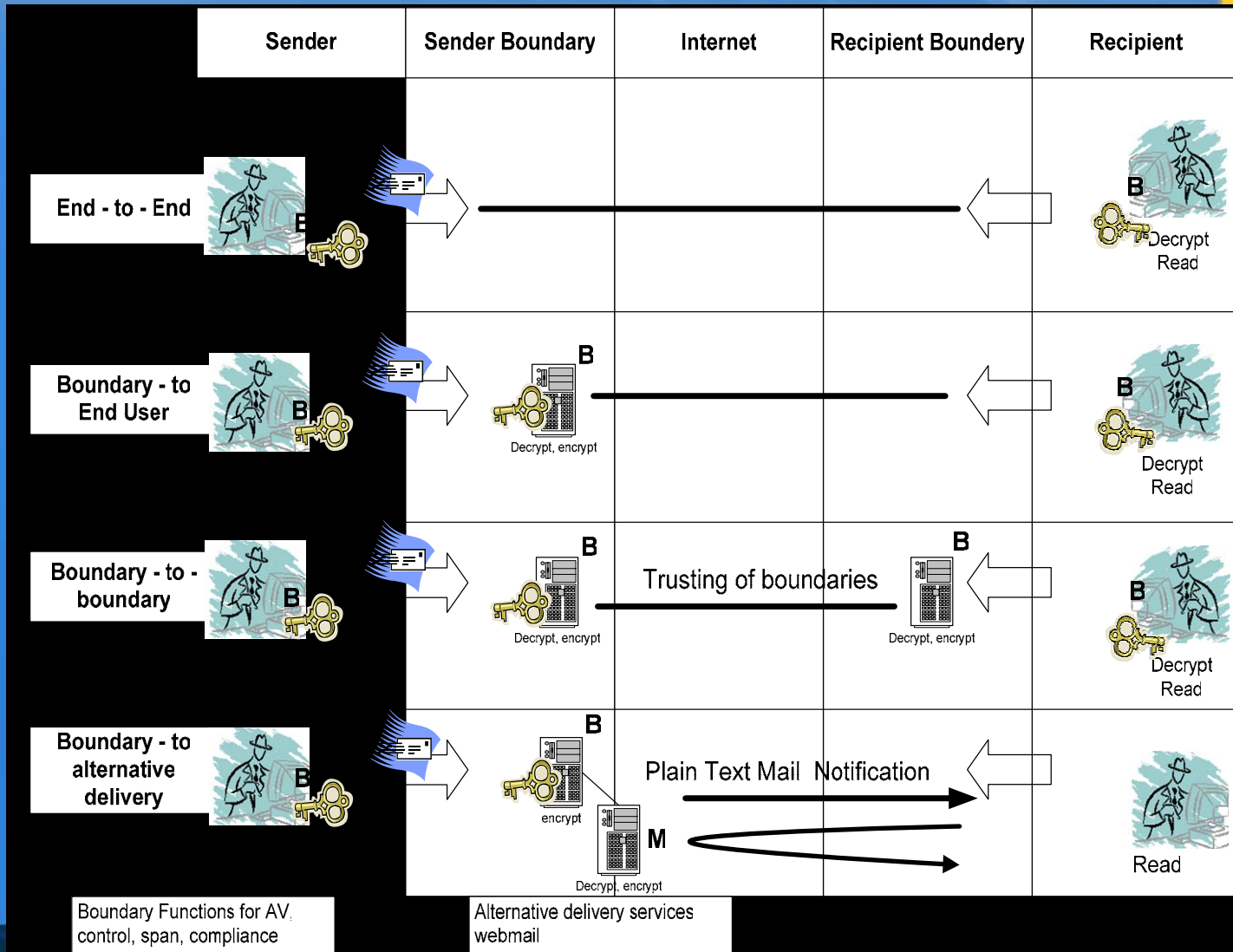


Boundary-to-Alternate Delivery Scenario



E-Mail Landscape

ENVISION



Index

- Notes Secure Mail Backgrounder
- Secure E-Mail Landscape
- **Notes/Domino CA Features and Processes**
- Some Important Domino X509 and S/MIME Processes
- Demo
- Other important PKI Vendors
- S/MIME Plug-ins and Gateways
- Lessons Learned

Domino CA

- Server based Certificate Authority
 - ◆ Implemented as server task
 - ◆ Signs certificates via Admin4
- Enhanced Security
 - ◆ Admins don't need access to certifier IDs & passwords
 - ◆ Certifiers can be password protected individually or as a group
 - ◆ Tamper-resistant auditing of all activity
- Manages list of administrators who can approve certificate requests (RAs)
- Manages both Notes and X.509 certificates
- Publishes CRLs, supports CDP
- Supports x.509 extensions

Domino CA - Processes

- Admin4.nsf(Administration Requests)
 - ◆ New Admin Process Requests
 - ◆ Create Domino CA
 - ◆ Configure Certificate Authority Publication
 - ◆ Store CA Policy Info in Domino Directory
 - ◆ Modify CA Configuration in Domino Directory
 - ◆ Recertify CA in Domino Directory
 - ◆ Store Certificate in Domino or LDAP Directory
 - ◆ Store CRL in Domino or LDAP Directory

Domino CA - Tasks

- Certificate Authority (CA) Task
 - ◆ Manages Certificates
 - ◆ Certifies
 - Users
 - Servers
 - Certificates

Domino CA – Cert by Mail Process

- Internet Certificates can be requested thru email.
 - ◆ This is to ensure interoperability with Lotus for Workplace (LWP2.0)
- Setup:
 - ◆ Make certreq.nsfdatabase a mail-in database
 - ◆ Email request must be in a specific format
 - ◆ Email request must be processed by an administrator in the certreq.nsfdatabase, this will convert the email request into a certificate request
 - ◆ Certificate request will follow certificate process in previous slide
 - ◆ Certificate (with the root certificate) will be sent back to the sender

DWA and Domino 7

- S/MIME encryption and decryption available through web browser
- Users can verify an S/MIME signature on a received message. Users who have an X.509 certificate in their mailfile-based Notes ID can decrypt received S/MIME messages as well as S/MIME sign messages they send.
- Outgoing messages can be S/MIME encrypted for recipients who have an X.509 certificate in the Domino Directory or DWA contacts.
 - ◆ Note that for an X.509 certificate to be used by DWA, an Internet cross-certificate must be issued from the user's organizational certifier to the certificate authority that issued the X.509 certificate.
 - ◆ This Internet cross-certificate must be present in the Domino Directory.
- Programmatic interfaces for manipulating secure email
 - ◆ 3rd party vendors can hook into API

Index

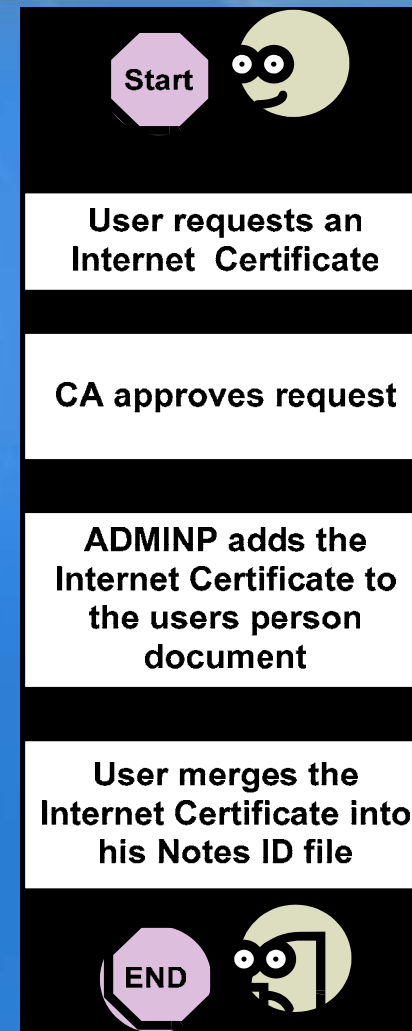
- Notes Secure Mail Backgrounder
- Secure E-Mail Landscape
- Notes/Domino CA Features and Processes
- **Some Important Domino X509 and S/MIME Processes**
- Demo
- Other important PKI Vendors
- S/MIME Plug-ins and Gateways
- Lessons Learned

Other Important X509 Processes

- The following steps and processes will be explained on the next slides:
 - ◆ Requesting X509 certificate for Notes client
 - ◆ Requesting browser Internet Certificate
 - ◆ Automated x509 issuance of S/MIME certificates
 - ◆ Set up Notes Client for S/MIME
 - ◆ Prepare Notes Client with certificates for S/MIME
 - ◆ Issue Cross-certificate for encrypted S/MIME messages
 - ◆ Importing Internet certificates
 - ◆ Exporting Internet certificates
 - ◆ Adding user X509 certificates to the Domino Directory

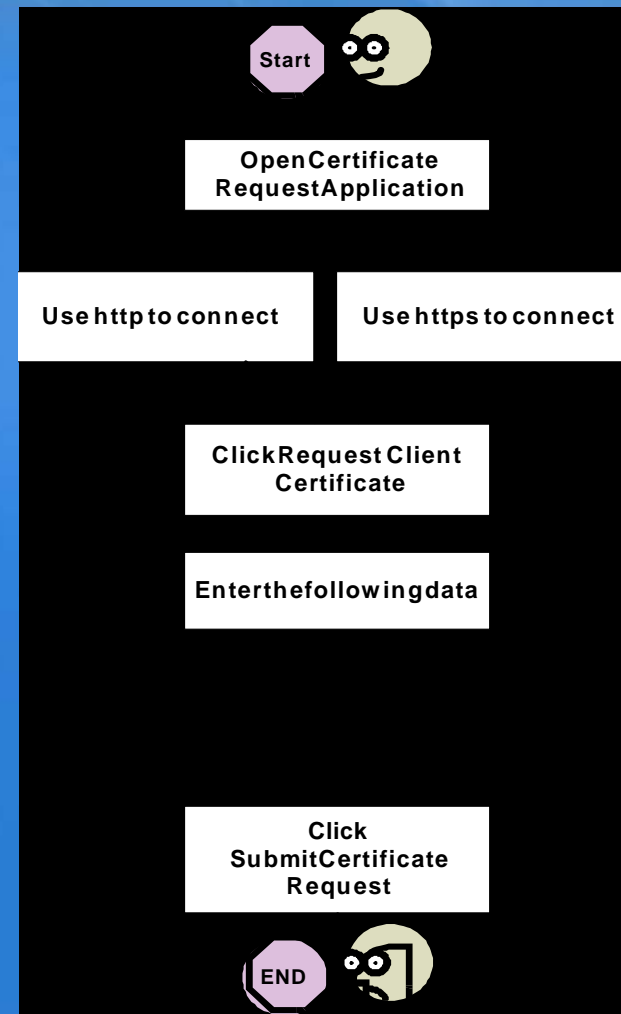
Requesting X509 certificate for Notes client

- To obtain an Internet Certificate for your Notes client follow the chart on the right side.



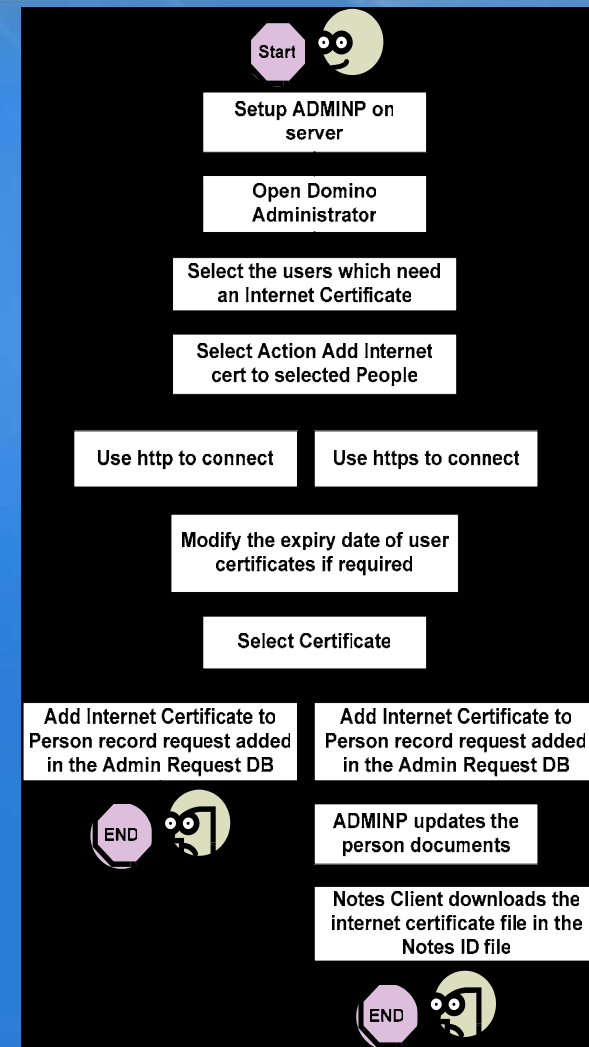
Requesting browser X509 certificate

- To obtain a browser Internet Certificate follow the chart on the right side.



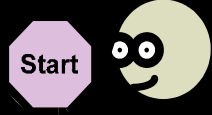
Requesting multiple X509 certificates

- To issue multiple X509 user certificates at once follow the process as described on the right side.



Setting of Notes client for S/MIME use

- To enable a Notes client to use S/MIME proceed as follows:




Recipient Internet certificate needs to be available

Cross certificate for either recipient or recipients CA must be available in personal address book

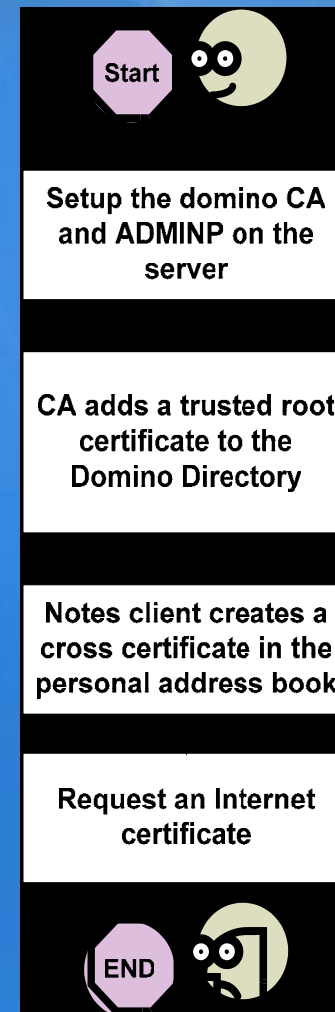
Internet certificate must be available in ID file of the „sender“

Client settings need to be correct (mail settings and location document)



Actions on Notes client for S/MIME use

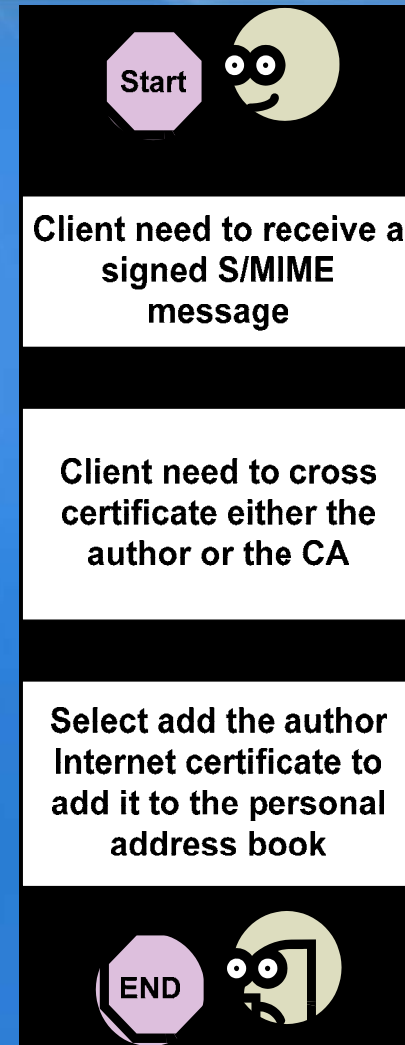
- To prepare a Notes client to be able to do S/MIME with external parties:





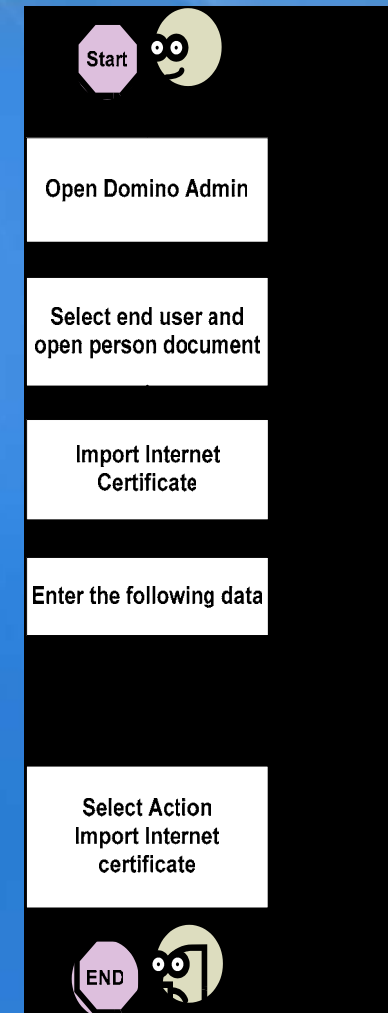
Issue X-Certificate for S/MIME use

- To add an Internet certificate and cross certificate for S/MIME use:



Importing X509 certificates

- To import certificates using the admin client:

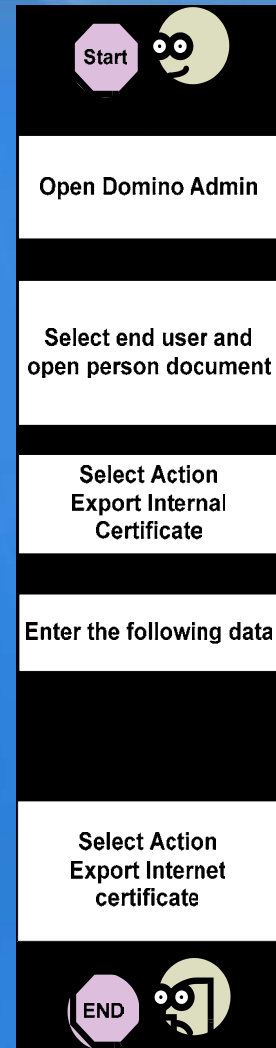


Exporting Internet certificates

ENVISION

Exporting X509 certificates

- To export Internet Certificates using the Admin client :



DECISIONS

Adding X509 certificates to the Domino directory

- To add Certificates to the Domino directory proceed as follows:

Start

Open Domino Administrator Client

Open the Domino request application

Submit all unprocessed request if there are on

Approve or clear requests in ADMIN4.nsf database

Transfer all requests out of Admin Requests DB

Notify the user who requested that

GO

Index

- Notes Secure Mail Backgrounder
- Secure E-Mail Landscape
- Notes/Domino CA Features and Processes
- Some Important Domino X509 and S/MIME Processes
- **Demo**
- Other important PKI Vendors
- S/MIME Plug-ins and Gateways
- Lessons Learned

S/MIME Demonstration

- Import of own certificate
- Sending of signed mail
- Receiving and validation of signed mail, import of certificate
- Sending of encrypted mail
- Local (client side) certificate management

Index

- Notes Secure Mail Backgrounder
- Secure E-Mail Landscape
- Notes/Domino CA Features and Processes
- Some Important Domino X509 and S/MIME Processes
- Demo
- **Other important PKI Vendors**
- S/MIME Plug-ins and Gateways
- Lessons Learned

Other important PKI vendors

- Microsoft (MS Windows PKI and Certification Services)
- IBM (Domino, Tivoli, Host)
- Entrust
- RSA (KEON Product Line)
- Baltimore (no longer visible on market)
- ID2 (no longer visible on market)

Index

- Notes Secure Mail Backgrounder
- Secure E-Mail Landscape
- Notes/Domino CA Features and Processes
- Some Important Domino X509 and S/MIME Processes
- Demo
- Other important PKI Vendors
- **S/MIME Plug-ins and Gateways**
- Lessons Learned

Why using S/MIME Plugins or Gateways

- No S/MIME support available in R4 clients
- S/MIME-Support of R5 not always good enough for all cases (interoperability)
- SMIMEv3 not available before R6
- Easier to support because of central administration
- Better PKI Vendor integration
- Might allow alternate encryption eg PGP for some cases
- Better usability to end users

S/MIME Plugins

- Integration of additional menu items and functionalities
- Adaptation of the mail template and personal address book templates
- Administration of certificates and often lifecycle management
- Uses standard Notes/Domino mail routing

Alternative : Gateways and Boundaries

- Trusting the security of the Lotus Notes system as long as mails are inside of Lotus Notes world
- Does not require X509 client certificates in the Notes ID file
- Does not require 3rd party plugins
- Does sometimes require mail template changes and acts like a new Security MTA or gateway with central administration
- Allows central archiving, compliance checking and antivirus checking
- New on the market e.g. Entrust EMS

Some additional products

- AssureMail, Entergrity (Proxy)
- Entrust/Express, Entrust
- Entrust EMS Gateway, Entrust
- Mailsecure, Baltimore
- Mailprotect, BCC / IBM Deutschland
- Multisec Mail, CoConet
- SafeGuard Sign&Crypt, Utimaco
- TrustedMIME, SSE
- Tumbleweed Messaging

Index

- Notes Secure Mail Backgrounder
- Secure E-Mail Landscape
- Notes/Domino CA Features and Processes
- Some Important Domino X509 and S/MIME Processes
- Demo
- Other important PKI Vendors
- S/MIME Plug-ins and Gateways
- **Lessons Learned**

Key Technical Issues with S/MIME

- **Boundary functions (antivirus, content scanning, spam, compliance watch and policy enforcement)**
- **Current features of email clients are limited in regards to secure mail support (S/MIME v2/v3, PGP, multiple Certificates and usability)**
- **Certificate import and life cycle Management in email clients (Key history, Certificate extensions)**
- **Integration with other PKI products**
- **Interoperability**

Key Organisational Issues with S/MIME

- User acceptance and education of email clients with secure mail
- Delegation of secure emails not possible
- Deployment and support of 3rd party security plug-ins
- Certificate and client software distribution for external users and customers
- Certificate Lifecycle Management

Summary

- Avoid deployment of 3rd party client plug-ins unless you really need them as version management and software distribution is very difficult.
- Trust your internal email system security as far as you can e.g. Notes PKI until mail leaves the Notes world
- Consider the use of existing and upcoming boundary solutions for external secure email (B2B and B2C) to ease and speedup deployment
- Consider the use of „proxy certificates“ instead of full blown certificates for the use with secure email clients. A proxy cert can only be sued for the purpose of secure email and can be hosted by a gateway. This would also allow easy key escrow for archiving and scanning of secure email.

Thanks

- Special Thanks To :
 - ◆ Katherine Spanbauer, Charlie Kaufmann, Kevin Lynch, Mary ellen Zurko for all their help and support now and in the past
 - ◆ Tim Speed for interesting discussion and reusing 3 slides
 - ◆ Dr Freddo aka Frederic Dahm for tips and tricks and for the support with the first security redbook

References

- Secure Messaging
 - ◆ <http://www-106.ibm.com/developerworks/lotus/library/securemessaging/#IDABJFQB>
- Lotus Security Redbook
 - ◆ <http://www.redbooks.ibm.com/abstracts/sg247017.html?Open>
- Policy-based system administration
 - ◆ <http://www-10.lotus.com/ldd/today.nsf/Lookup/policy>
- Domino CA & CPS
 - ◆ <http://www-10.lotus.com/ldd/today.nsf/0/d3646dc17fbea0b200256c410049d8d5?OpenDocument>
 - ◆ <http://www-106.ibm.com/developerworks/lotus/library/article/domino-cps/>

Please come meet and talk with us in the labs....

- Performance and TCO lab – Dolphin Europe 5&6
- Application Dev Lab – Dolphin Asia 3
- Meet the Developers Lab – Dolphin Asia 1&2
- Certification Prep Lab – Swan Peacock 1&2
- Certification Test Lab – Swan Lark 1&2
- Innovation Lab – Dolphin Europe 3&4
- Mobile Computing Lab – Dolphin Europe 7

Other FUN Sessions

- **ID103 Upgrading to IBM Lotus Notes and Domino 7.0 (R1)**
 - ◆ Dolphin Southern IV-V 413
 - Monday 1:00 – 2:00 pm
- **ID103 Upgrading to IBM Lotus Notes and Domino 7.0 (R2)**
 - ◆ Dolphin Northern A-C 782
 - Wednesday 4:15 – 5:15 pm
- **ID118 Secure Internet Mail with Notes/Domino 7 via S/MIME**
 - ◆ Dolphin Southern II 410
 - Tuesday 4:15 – 5:15 pm

LotuspHERE[®] 2005

ENVISION

DECISIONS

