

All New and Shiny in Domino 8.5 Administration

LSBG Vårseminar 2009
Gregory Engels

I am not
Paul Mooney



I am not
Paul Mooney

I am his twin brother
only two feet taller



About me

Gregory Engels

Born in Moscow, live in Frankfurt, Germany since 1989

Been around Lotus Notes since 1998

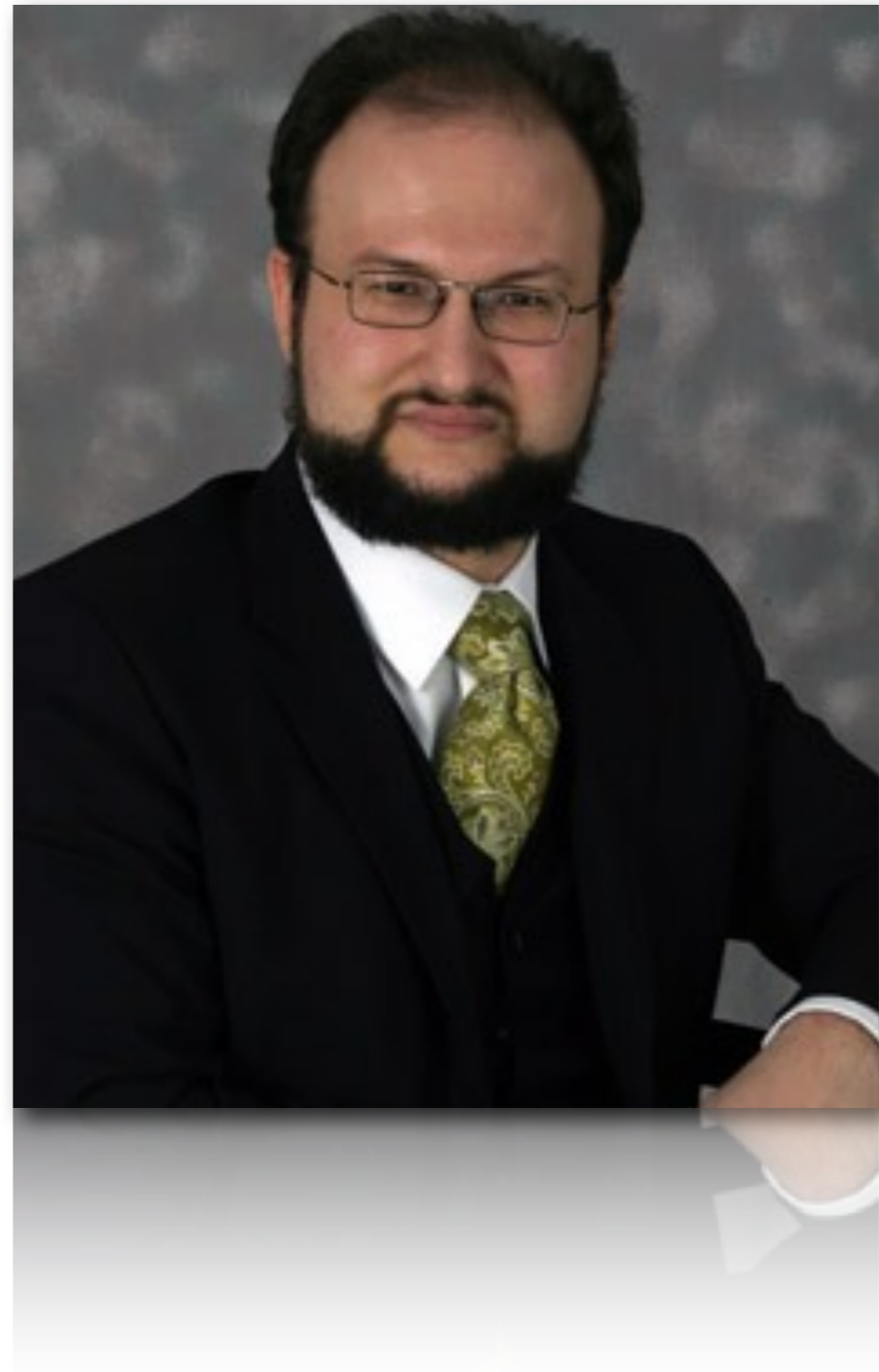
Advanced Certified Domino Developer and Admin and Security R5, R6, R7, R8

Co-Author  **Redbook** "Migrating Microsoft Exchange 2000/2003 to IBM Lotus Notes 7"

Founder Kompurity <http://www.kompurity.de>

Specialize in Hosting, Infrastructure management

- Blog: <http://inotes.de>



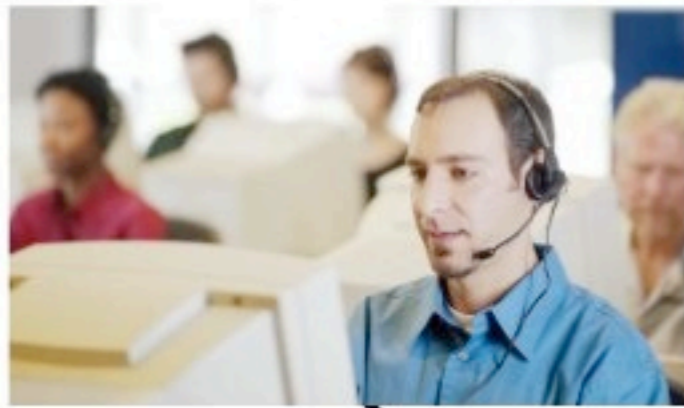
- ID Vault
- DAOS
- Questions at the end

ID Vault

What is ID-Vault

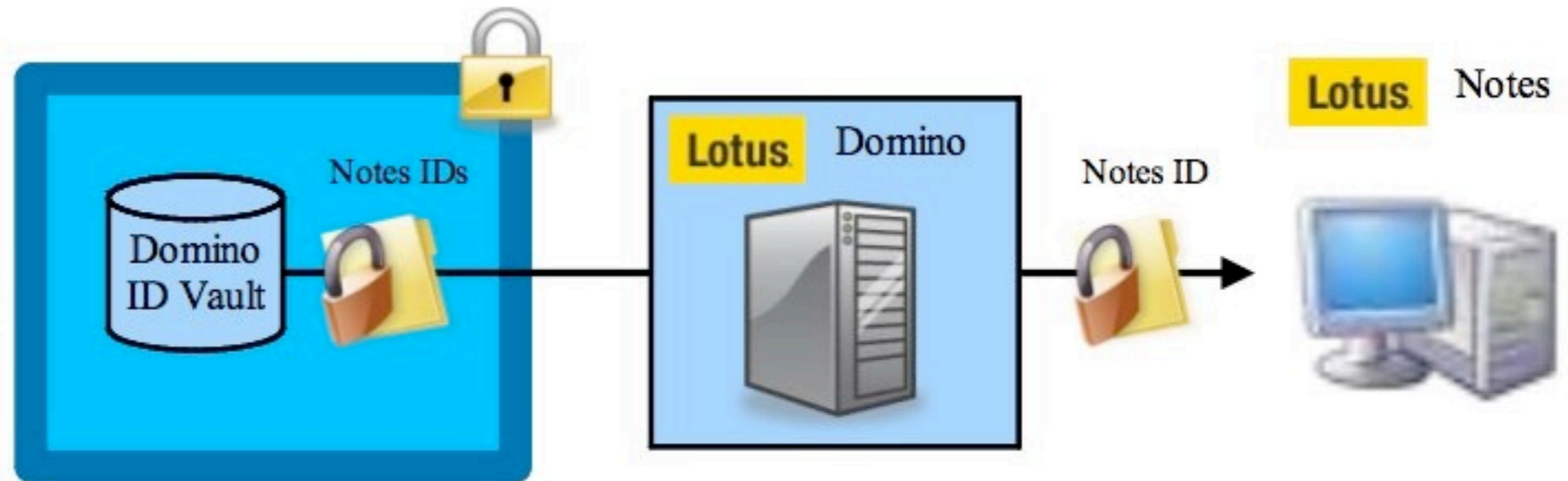
- Server based application for storing and managing protected copies of Notes ID files
- Reset forgotten passwords
- Synchronize ID files across multiple computers
- Auditor function to gain access to encrypted data

Password Reset with ID Vault



Helpdesk

Self service
password reset application



ID Vault capabilities

- Upload copies of ID files for existing users
- Register ID files to vault for new users
- Reset passwords when forgotten (Help desk, self-service app)
- Synchronize ID files across multiple computers
 - Recommended for use with new File Server Roaming

ID Vault Capabilities

- Auditor function to gain access to encrypted data
- Requires administrator access, vault admin rights, auditor role
- Can be disabled using `SECURE_DISABLE_AUDITOR=1` in `notes.ini`

How is this working?

- Vault trust certificate
 - A special cross-cert created by certifier
 - Example: O=DSKTest:VT:O=DSKTest Vault
- Vault ID file
 - Acts like a cert ID file for vault operations
 - Example: ID file for “O=DSKTest Vault”

ID Vault and Security

- Protection against the use of an unauthorized vault
- Creation of vault trust certificate requires access to certifier ID
- Protection against unauthorized:
- Downloads of IDs
- Failed password attempts restricted to 10 per day

- Option to require authorization for all downloads
- Password resets
 - Creation of password reset certificate requires access to certifier ID
- Access to vault contents
 - Attached IDs are encrypted in vault
- Access to data transmitted over network
 - ID vault transactions are encrypted

Password Reset Cert

- Special cross-certificate issued by a certifier to each entity who can change the vault auth data
- Example: O=DSKTest:PR:CN=dskadmin/O=DSKTest
- Can only reset passwords for the issuing organization
- Password reset applications need password reset certs, too
- Certs for signing ID and password reset app server

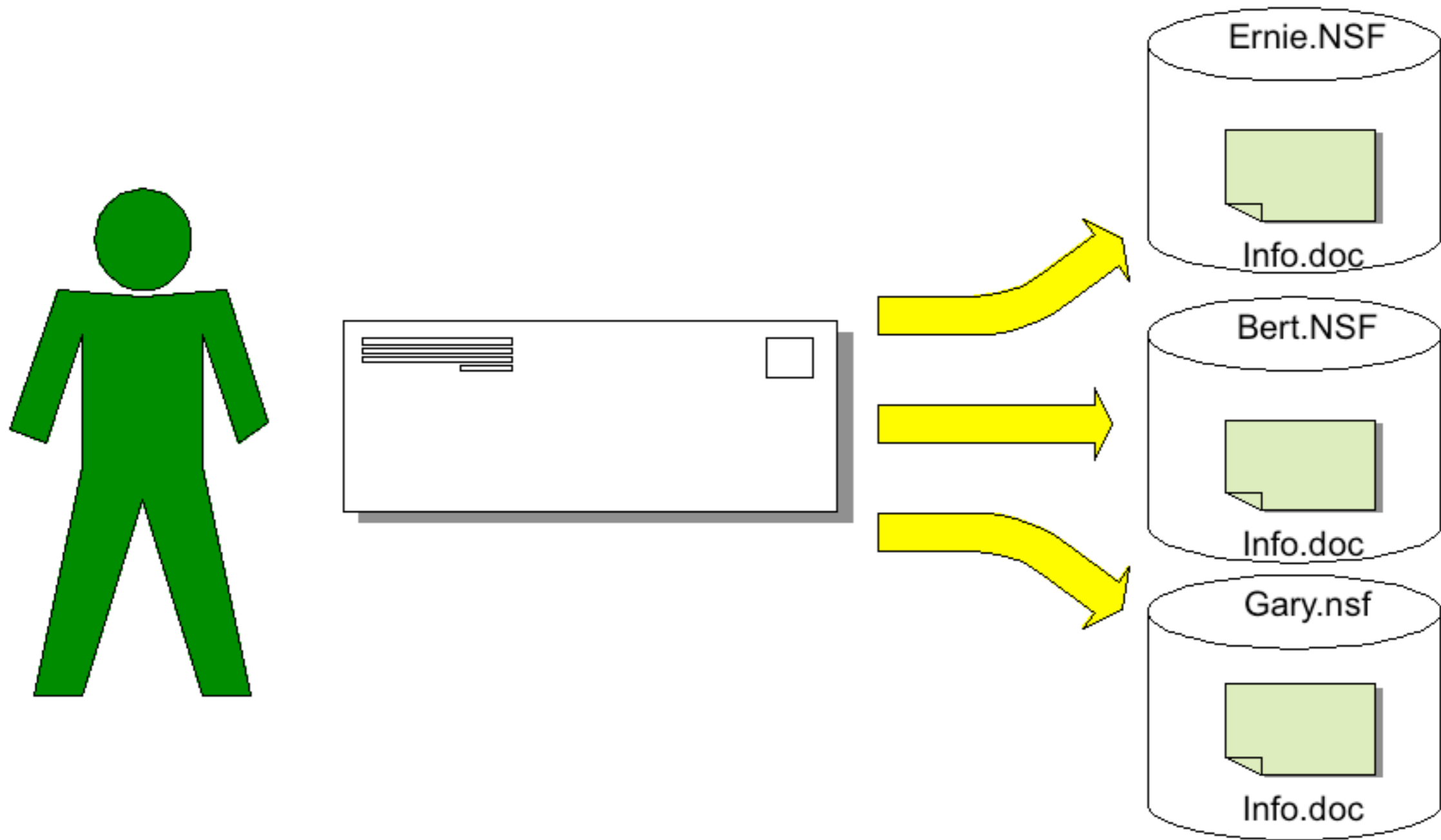
Deployment

- Issue a password reset cert to an entire “helpdesk OU”
- Renaming people to that org will grant/deny access
- Issue a single PR cert to an application, and give the help desk access to that application
- Easy to add and remove people from that ACL, can add supplemental logging and auditing

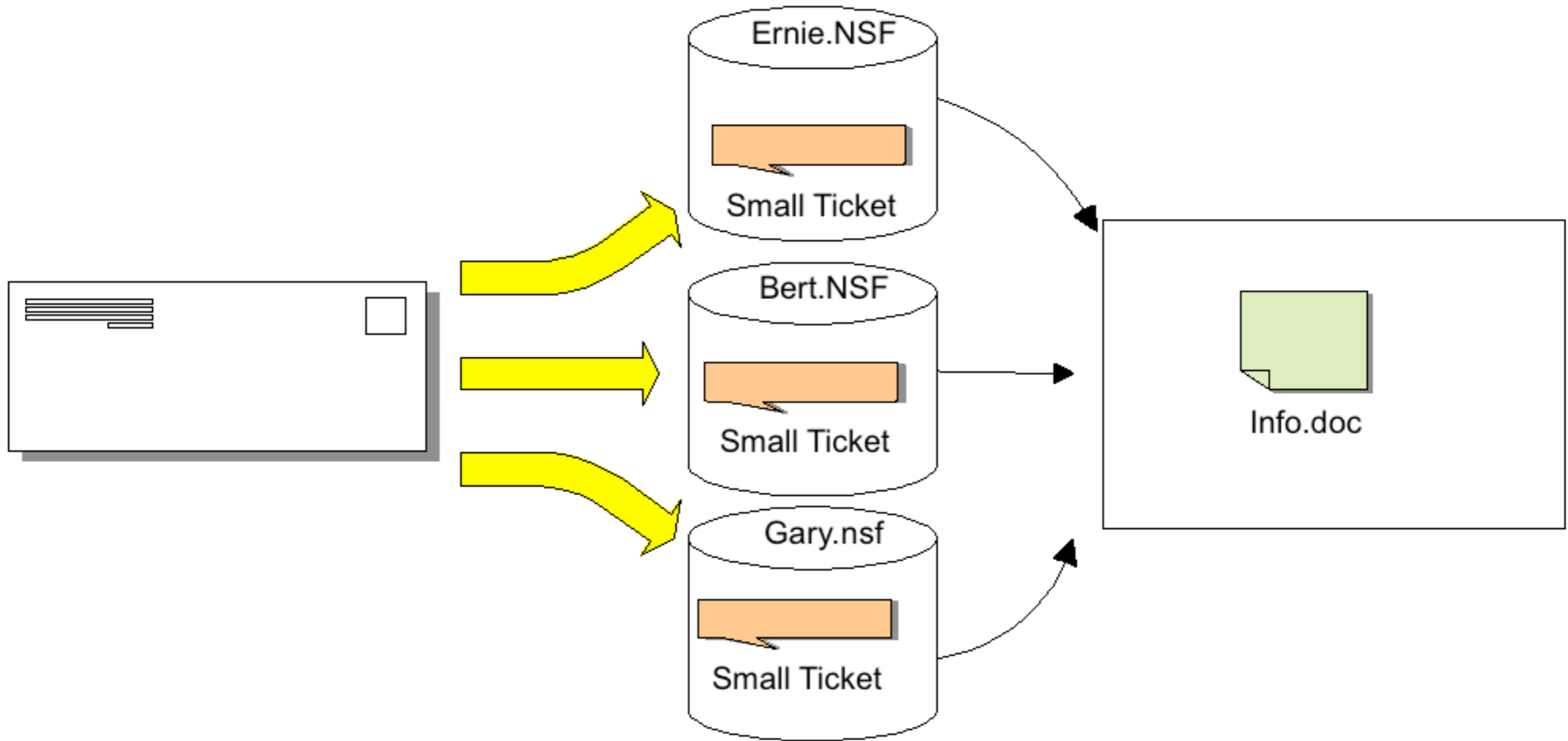
What can you expect?

- It does currently not working with CA-enabled certifiers
- Vault.id file created on Admins desktop and should be backed up and protected like a certifier id
- It does currently not working with id files stored in mail (iNotes, BES)

DAOS



Attachments without DAOS



Attachments with DAOS

Example calculation

- Samantha sends an email containing a final proposal for an flyer (5 MB) to 20 coworkers and ask for their approval.
($5 \times 20 = 100$ MB)
- Everyone “reply to all” with “I’m fine with it” ($20 \times 20 \times 5 = 2$ GB)

**With DAOS, only
5 MB storage
are needed!**

2 GB are being transferred through the wire, still.

How does it work?

- Server has to be version 8.5
- Transparent to Clients (Notes, Web, API)
- Database has to be ODS 51
- Create_R85_Databases=1 in the Notes.ini

- **Configure the Server to use DAOS in the Server Document**
- **Use a separate RAID for the .nlo files**
- **To determine the correct size for the smallest extractable Attachment use the DAOS estimator**

- Database has to be enabled to use DAOS
- load compact -C -DAOS on
enables DAOS and offload attachments in
the same step.
- or use the property box ;-)
(still need a
compact afterwards)

Things to consider

- Use DAOS Estimator

<http://www-01.ibm.com/support/docview.wss?rs=463&uid=swg24021920>

- Use Separate RAID disks or a Storage-LUN
- Needs Mail.box to be transactionally logged
- You need to Backup the .nsf's and the .nlo's
- Do not try to share .nlo disk between servers

What can you expect?

- DAOS does not solve capacity problem.
- It fastens up compact, backup, etc considerably
- You can have .nsf's with logical size bigger than 64GB (2TB has been reported)

...More Shiny and New

- DCT - Domino Configuration Tuner
- New Shared Login with Windows
- Dynamic Policies
- XPages
- Overall improvements: DDM, Compact, Update, TransLog, Router, Design and Document compression, ...

Questions?

Thank You!

- Please fill out the evaluation (so I can get back next year)
- Contact: Gregory.Engels ✖ kompurity.de
Blog <http://inotes.de>
twitter: dichter
XING, Linked-In, Facebook, Plaxo, etc...