

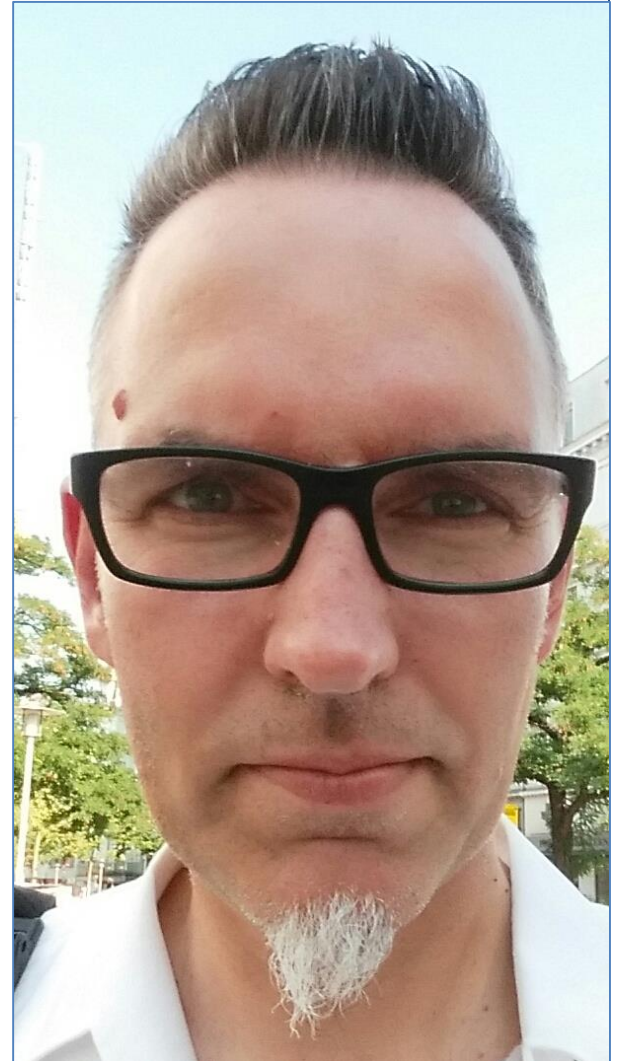


# ID Vault – jetzt aber wirklich los!

AdminCamp 2016, Ulf Duvigneau

# Über mich

- Lotus Notes Entwicklung seit 1992 mit Version 2
- Lotus Notes Administration seit 1994 mit Version 3 (OS2-Server)
- Kunden- und Entwickler-Versteher
- Senior Architekt/Administrator  
Domino, Travler, Sametime (Community)
- Arbeitet bei TimeToAct Hamburg



# Agenda

Was ist ID Vault?

ID Vault Funktionalität

ID Vault Anforderungen

ID Vault Zusammenarbeit

In 10 Schritten zum ID Vault

ID Vault in Action

ID Vault Fehlersuche

ID Vault Bemerkenswertes

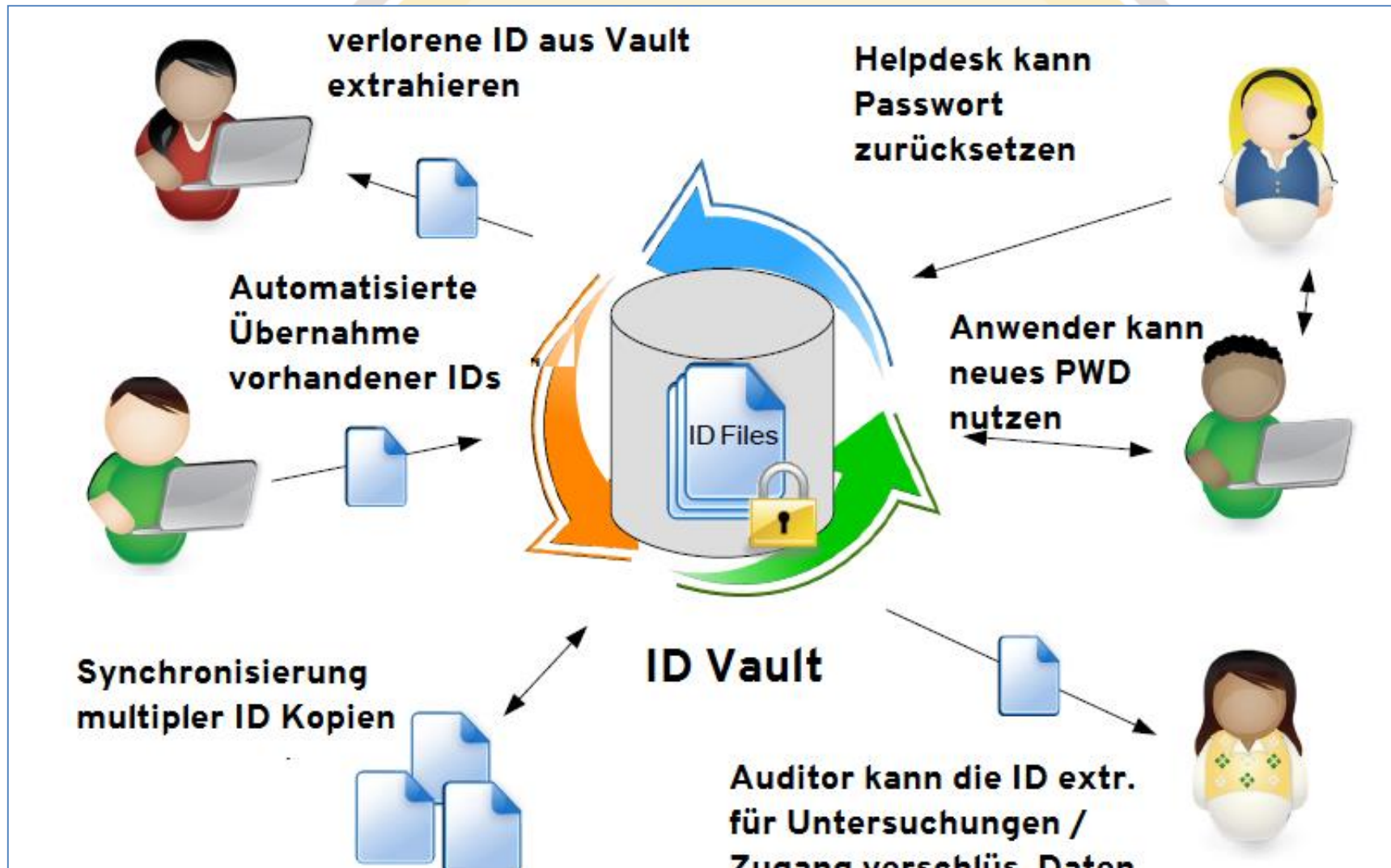
Quellen / Hilfen



# Was ist ID Vault?

- ... wurde in Domino 8.5 eingeführt
- Verschlüsseltes Speichern der User.ID Dateien an einem zentralen Ort (Vault Datenbank)
- Änderungen lokal oder am Server an der ID werden in den Vault übernommen
- Konfiguriert auf dem Server und über Security Policy an die Anwender verteilt
- Beim ersten Mail-Server Zugriff (oder Weiterleitung auf Replic)
- Alle 8 Stunden oder beim Clientstart, 3 Wiederholungen n 5 Minuten

# Was ist ID Vault?



# Wofür ist ID Vault?

- Für Notes
- iNotes
- Traveler

# ID Vault Funktionalität

- Passwortwechsel oder Reset für autorisiertes Personal wie z.B. ServiceDesk
- Offen für individuelle Applikationen dasselbe zu tun (C-APIs Funktionen Put, Get Sync)
- Leichte Wiederherstellung verlorener oder defekter IDs
- Bereits bei der ID Erstellung
  - Keine eigene Archivierung der IDs nötig
  - Kein Verteilen der Ids beim Setup eines neuen Anwenders
- Automatische Synchronisation von Ids verschiedener Maschinen auch bei Kennwortwechsel
- Umbenennung > ID Vault verteilt

# ID Vault Anforderungen

- Je höher die Version, je besser
- Domino und Notes Version 8.5 oder höher
- Directory 8.5 oder höher
- Penames 8.5 oder höher
- Sicherheits-Richtlinie, die den Vault zuweist
- Ein Vault Server, Backup ist empfohlen

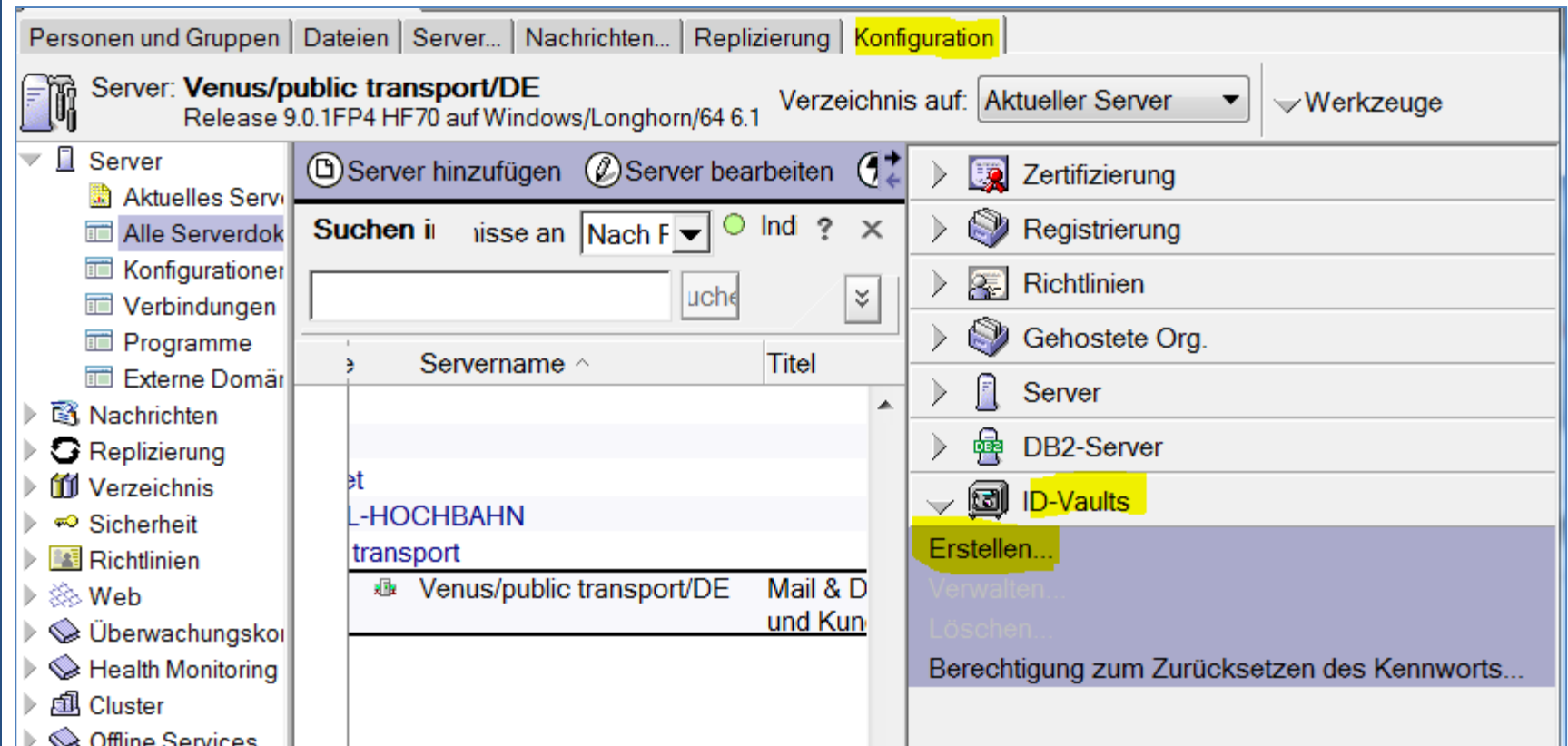


# ID Vault Zusammenarbeit

- Shared Login
- Roaming (keine ID im persönlichen Adressbuch)
- iNotes, Traveler, Blackberry (8.5.1)
- ID Recovery (parallel)  
WikiPage für Mig von Recovery > Vault
- CA Process (8.5.1)


# In 10 Schritten zum ID Vault I

Im Admin Client > Werkzeuge > ID Vault > Erstellen



# In 10 Schritten zum ID Vault II

## Notes-ID-Vault erstellen und konfigurieren



Eine Notes-ID-Vault ist ein sicherer Aufbewahrungsort für Benutzer-ID-Dateien. Sie ermöglicht das einfache Ändern von ID-Passwörtern, falls Benutzer sie vergessen haben. Die Notes-ID-Vault dient auch als Backup, von dem verlorene und beschädigte IDs leicht wiederhergestellt werden können. Wenn eine Änderung vorgenommen wird, gewährleistet die Notes-ID-Vault, dass alle Kopien von IDs von Benutzern, die Notes auf mehreren Computern ausführen, auf dem neuesten Stand gehalten werden. Klicken Sie auf '?' für weitere Informationen über ID-Vaults.

Mit diesem Werkzeug können Sie die folgenden Schritte ausführen, die erforderlich sind, um eine Notes-ID-Vault zu erstellen und in Betrieb zu nehmen:

- Notes-ID-Vault erstellen
- Vault-Server und -administratoren angeben
- Organisationen festlegen, die der ID-Vault zum Speichern von Benutzer-IDs vertrauen (Zugriff auf die Zertifizierer-ID erforderlich)
- Personen oder eine Self-Service-Anwendung autorisieren, Benutzerkennwörter zurückzusetzen (Zugriff auf Zertifizierer-ID erforderlich)
- Richtlinien konfigurieren, um Benutzer-IDs anzugeben, die in einer Vault gespeichert werden sollen

Mit diesem Werkzeug müssen Sie die ID-Vault auf dem angegebenen Server erstellen sowie mind. einen Vaultadministrator angeben. Für die weiteren Schritte kann auch 'ID-Vaults - Verwaltung' verwendet werden. Die ausgewählten Schritte werden ausgeführt, wenn Sie im letzten Schritt auf 'Vault erstellen' klicken. 'Abbrechen' speichert Ihre Auswahl.

## In 10 Schritten zum ID Vault III

- Namen (DB-Dateiname) und Beschreibung (DB-Titel) hinterlegen
- Der Vaultname beschreibt den hierarchischen Namen der Vault und sollte daher nicht einem hierarchischen Zertifizier entsprechen

### Notes-ID-Vault erstellen und konfigurieren



Geben Sie einen Namen und eine Beschreibung für die Notes-ID-Vault an.

Name der Notes-ID-Vault

ExperimentVault


Beschreibung der Notes-ID-Vault (optional - wird auch als Titel der Notes-ID-Vaultdatenbank verwendet)

ID Vault für alle ID PT Domaene

# In 10 Schritten zum ID Vault IV

- Vault Kennwort (8 Länge) vergeben
- Kennwort sollte behalten werden, um später Server zu entfernen oder hinzuzufügen oder Vault zu löschen

Notes-ID-Vault erstellen und konfigurieren

 Geben Sie ein Kennwort und einen Speicherort für die Vault-ID-Datei an.

Vault-ID-Kennwort

Kennwort:

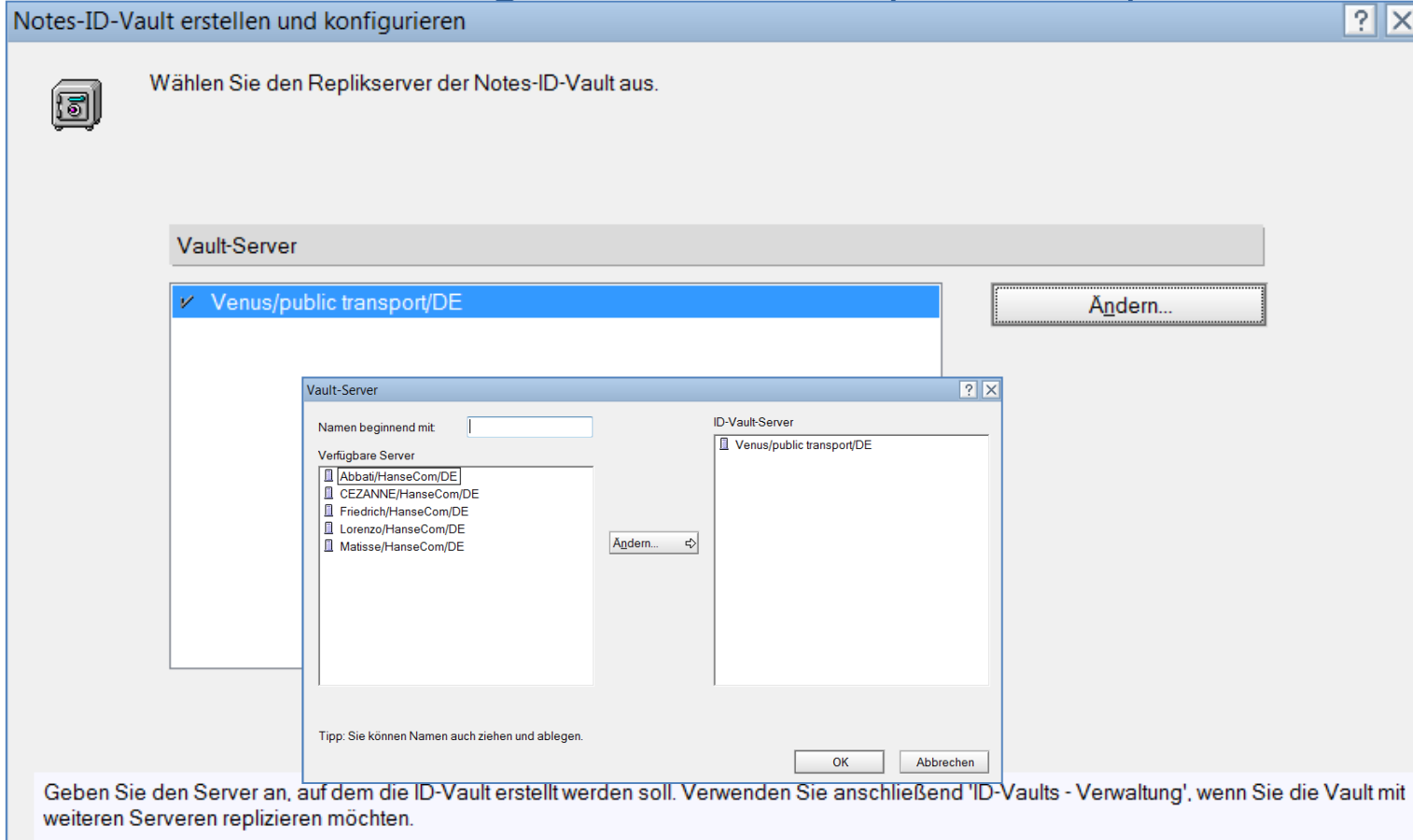
Kennwort bestätigen:

Speicherort der Vault-ID-Datei

C:\Anwender\Notes\ids\vault\experimentvault.id

# In 10 Schritten zum ID Vault V

- Vault Server bestätigen / erweitern (Domäne!)



# In 10 Schritten zum ID Vault VI

- Vault Administratoren angeben (> ACL!)
  - Vaultserver ändern
  - weitere Administratoren festlegen
  - Nur Administratoren (Personen) des Serverdokuments auswählbar

Notes-ID-Vault erstellen und konfigurieren

Wählen Sie die Notes-ID-Vaultadministratoren aus.

Die folgenden Administratoren können die Notes-ID-Vault verwalten.

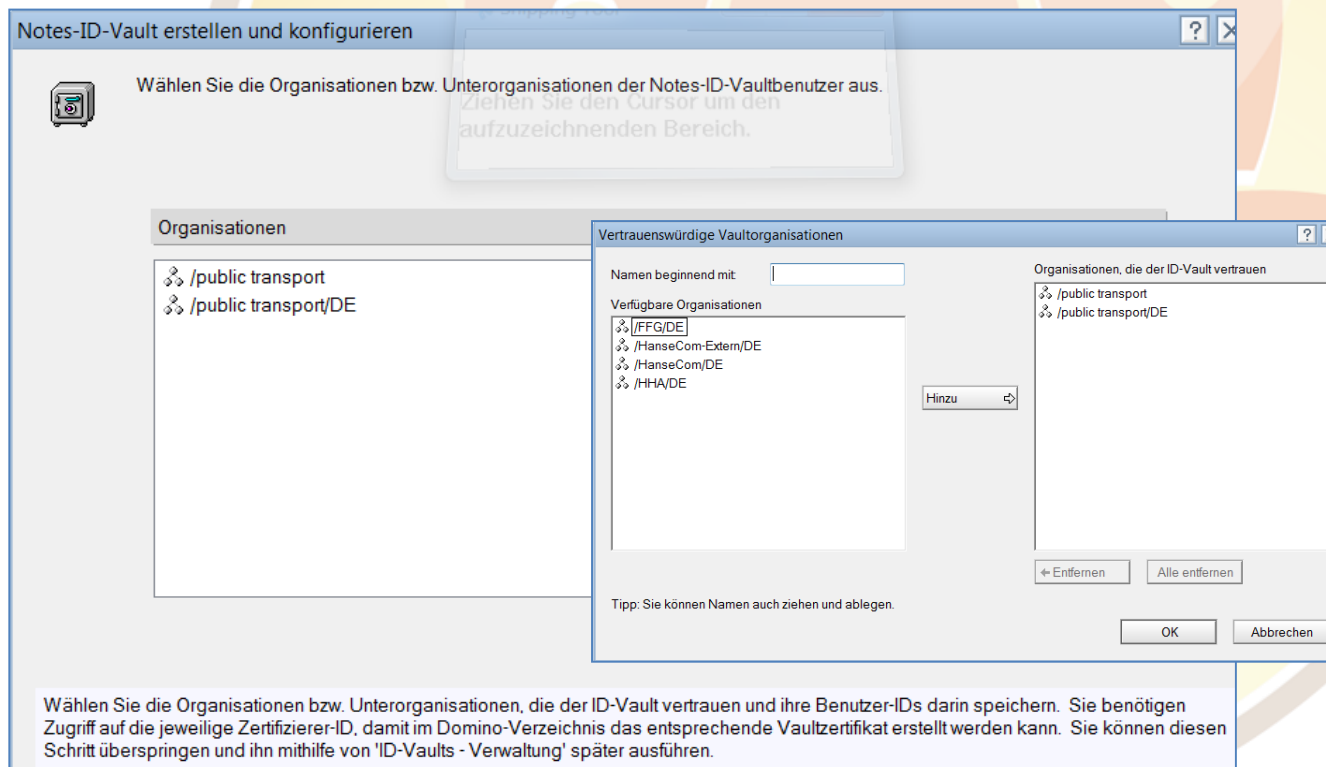
Ulf Duvigneau/HanseCom/DE

Hinzufügen/Entfernen...

Sie müssen mindestens einen Notes-ID-Vaultadministrator wählen. Sie können nur Benutzernamen wählen, keine Gruppennamen. Nur Vaultadministratoren können Vault-Server hinzufügen und entfernen, ID-Dateien aus einer Vault löschen sowie andere Vaultadministratoren hinzufügen und entfernen. Die Namen der Vaultadministratoren werden zur ACL der Vaultdatenbank und zum Vaultdokument im Domino-Verzeichnis hinzugefügt.

# In 10 Schritten zum ID Vault VII

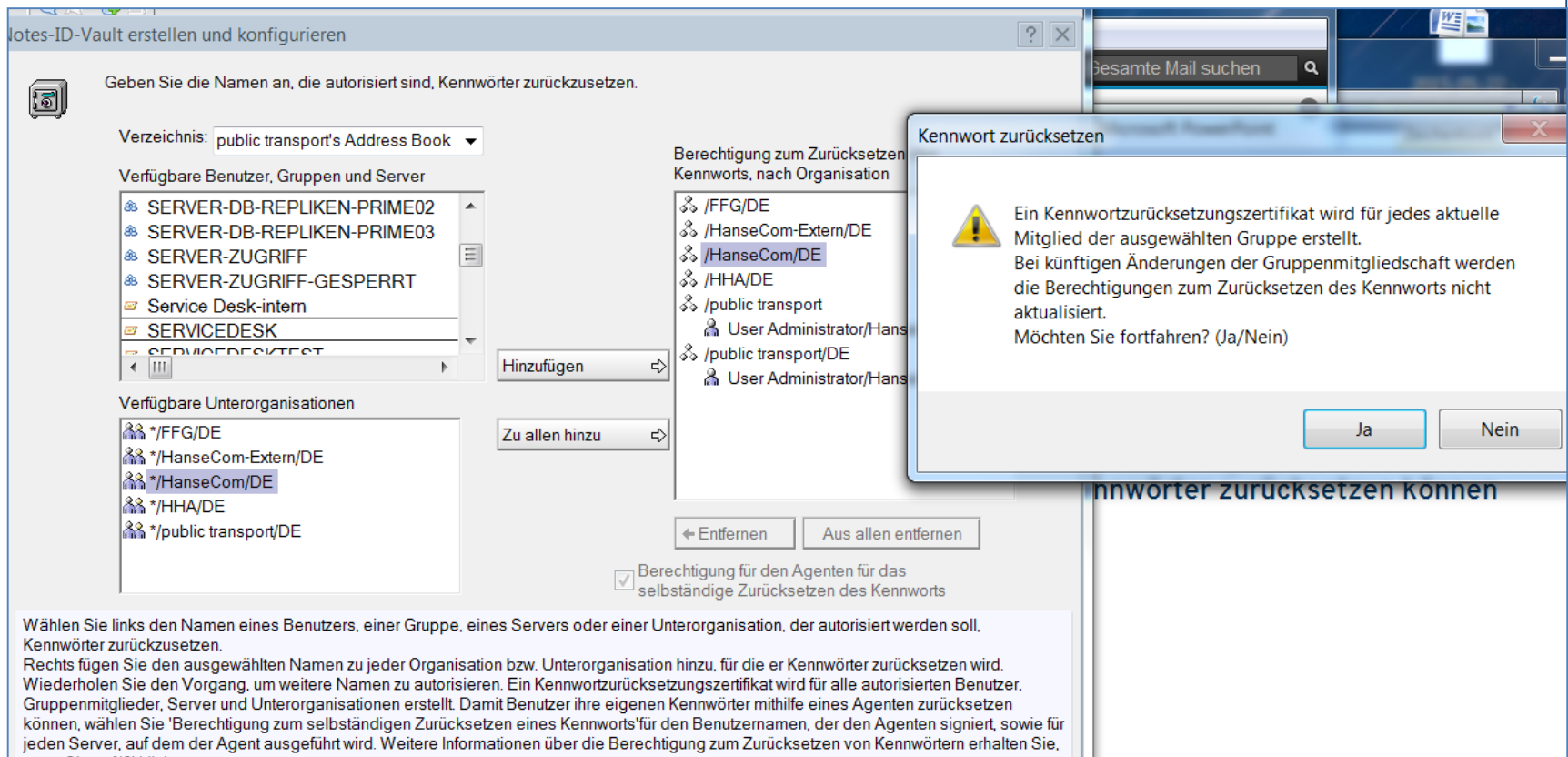
- (Unter-)Organisationen (certs) auswählen, deren IDs aufgenommen werden sollen
- VaultReplicas müssen innerhalb einer Domino Domäne sein!





# In 10 Schritten zum ID Vault VIII

- Personen, die Kennwörter zurücksetzen können



Notes-ID-Vault erstellen und konfigurieren

Geben Sie die Namen an, die autorisiert sind, Kennwörter zurückzusetzen.

Verzeichnis: public transport's Address Book

Verfügbare Benutzer, Gruppen und Server

- SERVER-DB-REPLIKEN-PRIME02
- SERVER-DB-REPLIKEN-PRIME03
- SERVER-ZUGRIFF
- SERVER-ZUGRIFF-GESPERRT
- Service Desk-intern
- SERVICEDESK
- SERVICEDESKTEST

Verfügbare Unterorganisationen

- \*/FFG/DE
- \*/HanseCom-Extern/DE
- \*/HanseCom/DE
- \*/HHA/DE
- \*/public transport/DE

Hinzufügen

Zu allen hinzu

Entfernen

Aus allen entfernen

Berechtigung zum Zurücksetzen Kennworts, nach Organisation

- /FFG/DE
- /HanseCom-Extern/DE
- /HanseCom/DE
- /HHA/DE
- /public transport
- User Administrator/HanseCom
- /public transport/DE
- User Administrator/HanseCom

☒ Berechtigung für den Agenten für das selbständige Zurücksetzen des Kennworts

Wählen Sie links den Namen eines Benutzers, einer Gruppe, eines Servers oder einer Unterorganisation, der autorisiert werden soll, Kennwörter zurückzusetzen. Rechts fügen Sie den ausgewählten Namen zu jeder Organisation bzw. Unterorganisation hinzu, für die er Kennwörter zurücksetzen wird. Wiederholen Sie den Vorgang, um weitere Namen zu autorisieren. Ein Kennwortzurücksetzungszertifikat wird für alle autorisierten Benutzer, Gruppenmitglieder, Server und Unterorganisationen erstellt. Damit Benutzer ihre eigenen Kennwörter mithilfe eines Agenten zurücksetzen können, wählen Sie 'Berechtigung zum selbständigen Zurücksetzen eines Kennworts' für den Benutzernamen, der den Agenten signiert, sowie für jeden Server, auf dem der Agent ausgeführt wird. Weitere Informationen über die Berechtigung zum Zurücksetzen von Kennwörtern erhalten Sie.

Kennwort zurücksetzen

Ein Kennwortzurücksetzungszertifikat wird für jedes aktuelle Mitglied der ausgewählten Gruppe erstellt. Bei künftigen Änderungen der Gruppenmitgliedschaft werden die Berechtigungen zum Zurücksetzen des Kennworts nicht aktualisiert. Möchten Sie fortfahren? (Ja/Nein)

Ja


Nein

- Außerhalb der Org ... Querezulassungen ins lokale NAB

# In 10 Schritten zum ID Vault IX

- Vault Richtlinien Einstellung erstellen  
Take Care! Explizite, Organisation oder später

Notes-ID-Vault erstellen und konfigurieren

 ID-Vaultrichtlinieneinstellungen erstellen oder bearbeiten.

Wie wird diese Richtlinie zugewiesen?

☐ Neue Richtlinie erstellen, die einer Organisation zugewiesen wird

☐ Neue Richtlinie erstellen, die bestimmten Personen oder Gruppen zugewiesen wird

☐ Neue Richtlinie erstellen, die einem Home-Server zugewiesen wird

☐ Vorhandene Richtlinie bearbeiten

☒ Ich werde eine Notes-ID-Vaultrichtlinie zu einem späteren Zeitpunkt angeben

# In 10 Schritten zum ID Vault X

- Wizard Einstellung überprüfen und GO oder zurück

## Notes-ID-Vault erstellen und konfigurieren



Überprüfen Sie Ihre Auswahl. Sofern alles in Ordnung ist, klicken Sie auf "GO" können ein Protokoll der ausgeführten Aufgaben in der Zwischenablage

### Bei der Erstellung anzuwendende Vaultkonfiguration

Name der Notes-ID-Vault

ExperimentVault

Beschreibung der Notes-ID-Vault

ID Vault für alle ID PT Domaene

Pfad der ID der Notes-ID-Vault

C:\Anwender\Notes\ids\vault\experimentvault.id

Primärer Server der Notes-ID-Vault

Venus/public transport/DE

Datenbankpfad der Notes-ID-Vault

\\IBM\_ID\_VAULT\ExperimentVaultnsf

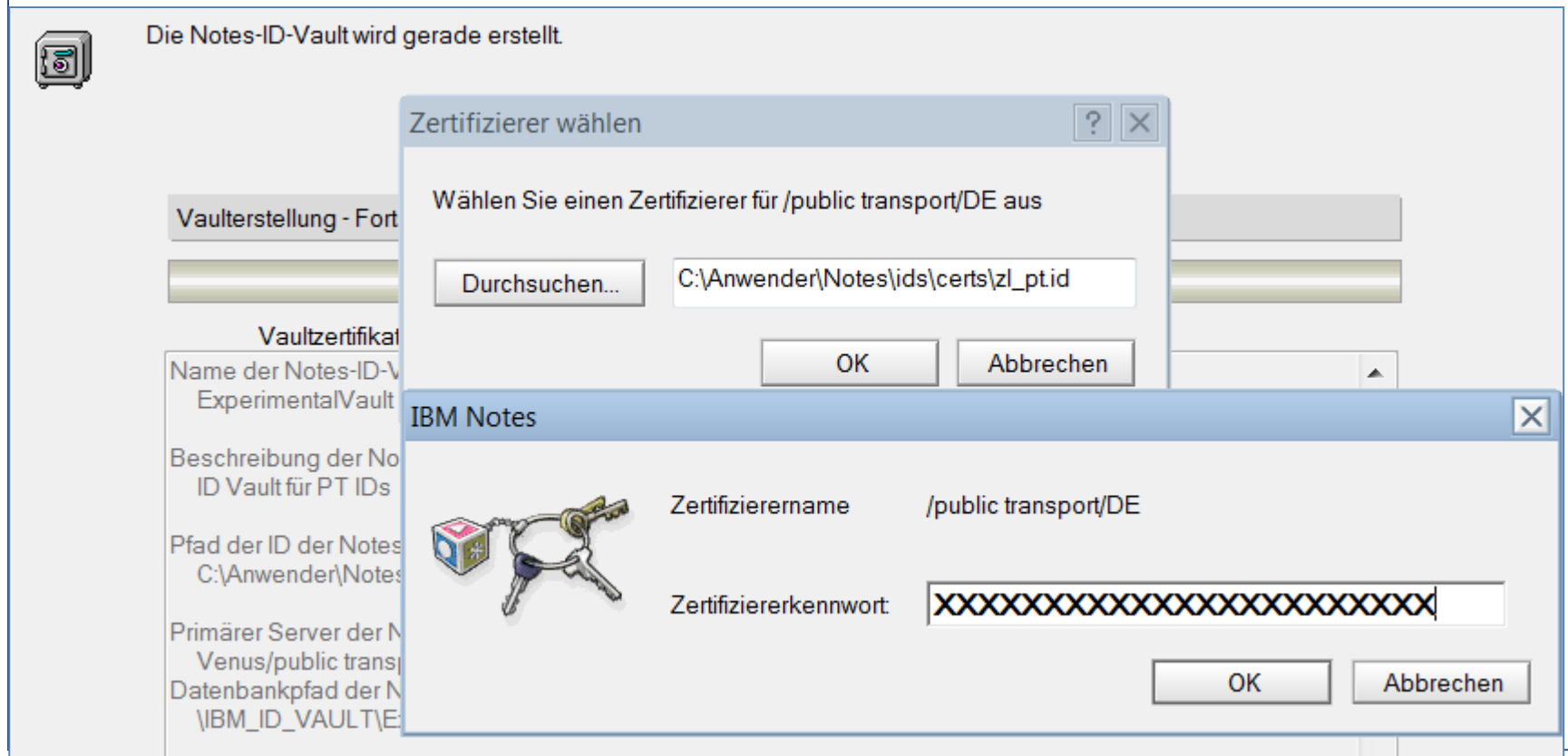
Notes-ID-Vault-Server:

Venus/public transport/DE

Notes-ID-Vault Administratoren:

## In fast 10 Schritten zum ID Vault **XI**

- Zulassung auswählen und Kennwort angeben



# ID Vault Einstellungen

- Directory > Sicherheit > ID Vaults
- Nur wenn ausgewählt, Verwalten oder Löschen möglich ( „/“ !)
- Empfehlung besser Verwalten-Tool als Bearbeiten

## ID-Vault : /ExperimentalVault

Allgemein | Administration

### Allgemein

|                       |   |
|-----------------------|---|
| Vaultname:            | /ExperimentalVault  |
| Beschreibung:         | ID Vault für PT IDs   |
| Vaultadministratoren: | Birgit Dahdouli/HanseCom/DE, Jürgen B Duvigneau/HanseCom/DE |
| Vault-Server:         | Venus/public transport/DE                                   |
| Pfad zur Vault:       | \\IBM_ID_VAULT\\ExperimentalVault.nsf                       |

Personen und Gruppen | Dateien | Server... | Nachrichten... | Replizierung | Konfiguration

Domino Designer Venus/public transport/DE  
Release 9.0.1FP4 HF70 auf Windows/Longhorn/64 6.1

Server  
Nachrichten  
Replizierung  
Verzeichnis  
Sicherheit  
Zertifikate  
**ID-Vaults**  
Richtlinien

Hilfe

Suchen in Ansicht 'gebnisse anzeigen: Nach Relevanz Indiziert

Suchen nach  Suchen

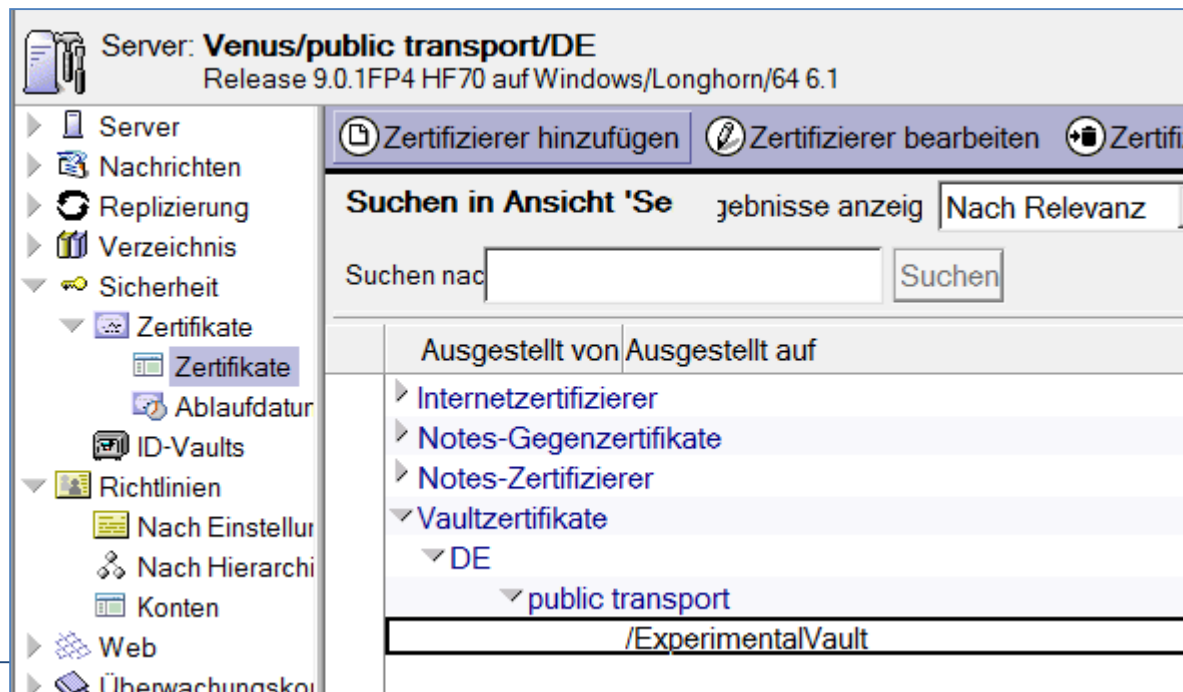
| Vaultname          | Administrationsserver     |
|--------------------|---------------------------|
| /ExperimentalVault | Venus/public transport/DE |

ID-Vaults

- Erstellen...
- Verwalten...
- Löschen...
- Berechtigung zum Z...

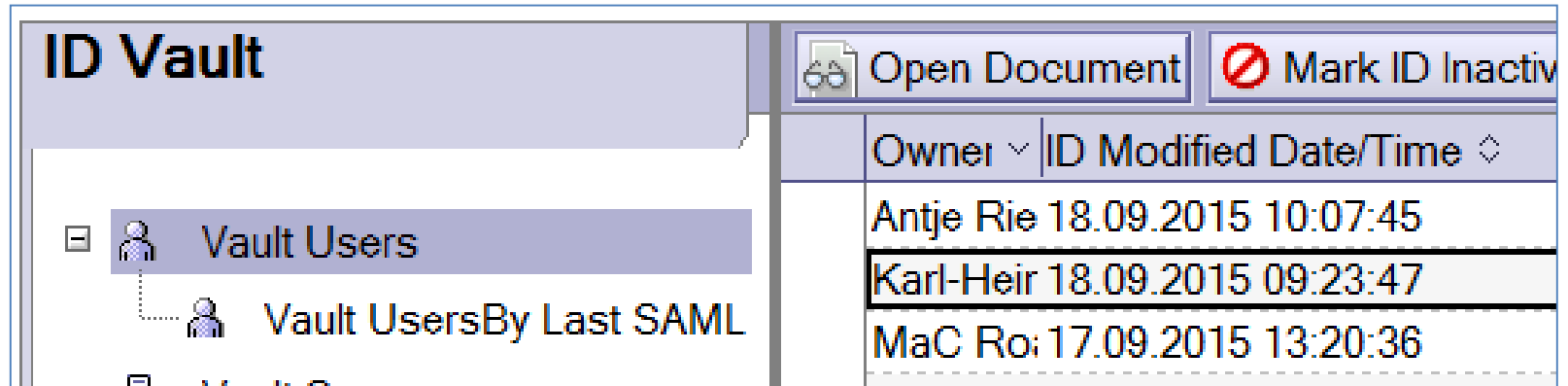
# ID Vault Zertifikate

- Vault-Zertifikat  
Cross Zertifikat, das Organisation dem Vault vertraut
- Password Reset Zertifikat



# ID Vault Database

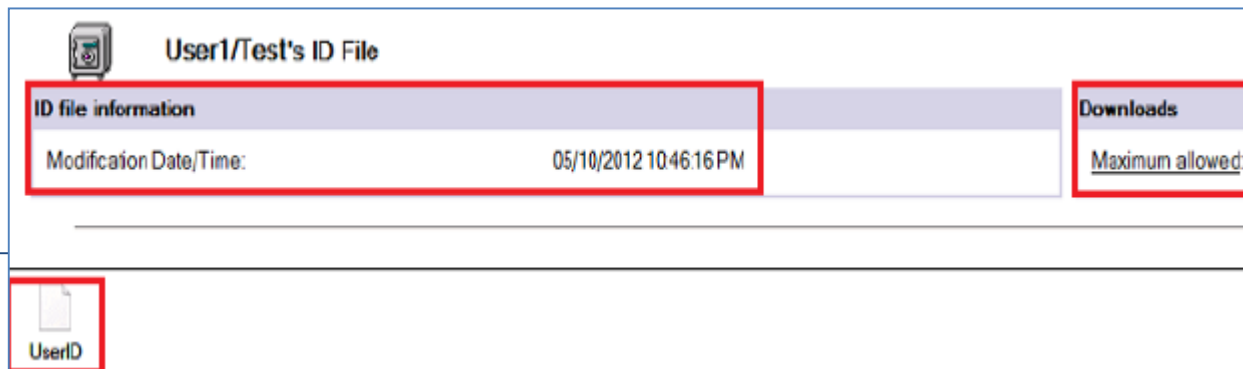
- UserID ist verschlüsselt!



The screenshot shows the ID Vault interface. On the left, there is a tree view with 'Vault Users' and 'Vault UsersBy Last SAML'. On the right, there is a table with columns 'Owner' and 'ID Modified Date/Time'. The table contains three rows of data.

| Owner     | ID Modified Date/Time |
|-----------|-----------------------|
| Antje Rie | 18.09.2015 10:07:45   |
| Karl-Heir | 18.09.2015 09:23:47   |
| MaC Ro:   | 17.09.2015 13:20:36   |

- Inactive – Gelöschte User, über „Restore ID“ back
- Download = 0, nicht mal beim Setup, Policy!



The screenshot shows the details for 'User1/Test's ID File'. It has two main sections: 'ID file information' and 'Downloads'. The 'ID file information' section shows 'Modification Date/Time: 05/10/2012 10:46:16 PM'. The 'Downloads' section shows 'Maximum allowed:'. Below these sections, there is a red box containing a document icon and the text 'UserID'.

# ID Vault Database ACL

- Rolle [Auditor] um IDs direkt aus der Vault wiederherzustellen

Zugriffskontrollliste für: ID Vault für PT IDs

**Allgemein** | Zugriffskontrollliste | Attribute

Personen, Server, Gruppen | Alle anzeigen

**Rollen** | **Protokoll** | **Erweitert**

**Attribute**

Benutzertyp: Person

Zugriff: Manager

☒ Dokumente erstellen

☒ Dokumente löschen

☒ Private Agenten erstellen

☒ Private Ordner/Ansichten erstellen

☒ Gemeins. Ordner/Ansichten erstellen

☒ LotusScript/Java-Agenten erstellen

☒ Öffentliche Dokumente lesen

☒ Öffentliche Dokumente schreiben

☒ Dokumente replizieren oder kopieren

Rollen: ☐ [Auditor]

**Personen, Server, Gruppen**

-Default-

Anonymous

Birgit Dahdouli/HanseCom/DE

Jürgen Bigdowski/HanseCom/DE

Jürgen Lehnert/HanseCom/DE

LocalDomainAdmins

LocalDomainServers

Martin Corleis/HanseCom/DE

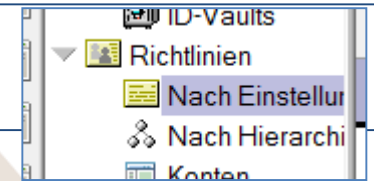
OtherDomainServers

Ulf Duvigneau/HanseCom/DE

Venus/public transport/DE



# Policy – Sicherheits-Einstellungen



- Neue Einstellungen (Wechsel und Vault für iNotes/Trav.)

## Sicherheitseinstellungen : SecSet HanseCom

Allgemein | Kennwortverwaltung | Ausführungskontrollliste (ECL) | Schlüssel und Zertifikate | Signierte Plug-ins | Portalserver | **ID-Vault** | Prox

| ID-Vaultoptionen:  |  | Wie diese Einstellung angewendet wird:        | Übernehm übergeord Richtlinie:    |
|--|--|---|-----------------------------------|
| Zugewiesene Vault:   | /Experimental/Vault  | <input type="checkbox"/> Wert nicht festlegen | <input type="checkbox"/> Übernehm |
| Hilfetext für vergessene Kennwörter:                               | Sollten Sie Ihre Kennwort vergessen haben, wenden Sie sich bitte an den Servicedesk unter der Nummer 040 / 27845 +++ | <input type="checkbox"/> Wert nicht festlegen | <input type="checkbox"/> Übernehm |
| Kennwort muss nach dem Zurücksetzen des Kennworts geändert werden: | <input checked="" type="checkbox"/> Ja   | <input type="checkbox"/> Wert nicht festlegen | <input type="checkbox"/> Übernehm |
| Notes-basierte Programme dürfen die Notes-ID-Vault verwenden:      | <input checked="" type="checkbox"/> Ja   | <input type="checkbox"/> Wert nicht festlegen | <input type="checkbox"/> Übernehm |
| Automatische ID-Downloads:   |  | Wie diese Einstellung angewendet wird:        | Übernehm übergeord Richtlinie:    |
| Automatische ID-Downloads zulassen:                                | <input checked="" type="checkbox"/> Ja   | <input type="checkbox"/> Wert nicht festlegen | <input type="checkbox"/> Übernehm |
| Zeitraum für ID-Downloads:   | 1 Tage   | <input type="checkbox"/> Wert nicht festlegen | <input type="checkbox"/> Übernehm |

# ID Vault - Check

- In den Eigenschaften der ID
- Im Notes Protokoll > Sicherheitsereignisse

17.09.2015 11:20:05 ID Vault replica 'O=FuWVault' successfully created on server 'CN=LNSV04/O=puw' by 'administrator/puw' (IP address 172.30.4.39:53232).

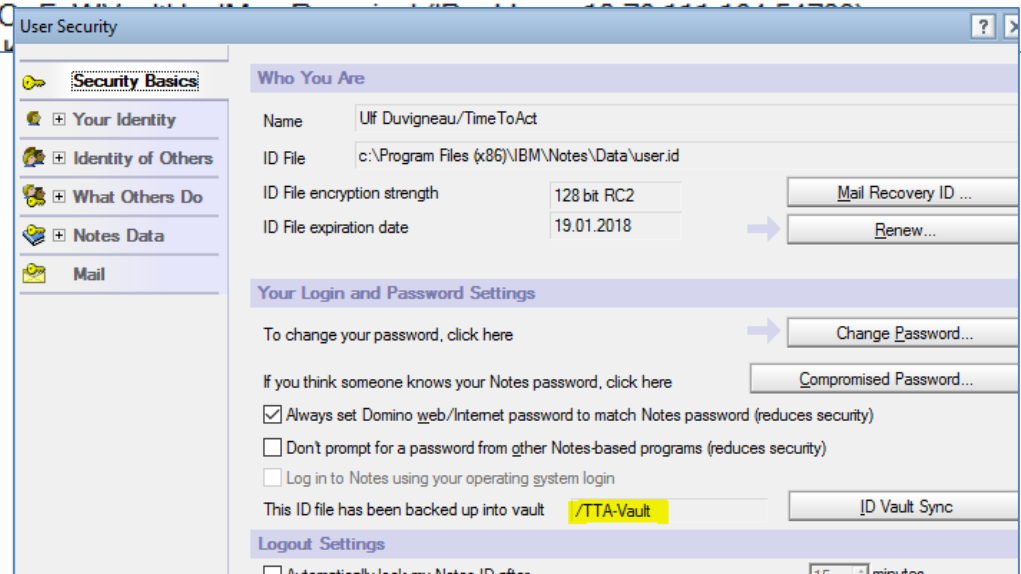
17.09.2015 13:20:29 Unable to find ID for 'MaC Roaming/puw' in vault 'O=FuWVault'. Error: Entry not found in index

17.09.2015 13:20:29 ID failed to authenticate in vault 'O=FuWVault'. 'MaC Roaming/puw' (IP address 10.76.111.166:62391) made request. Error: Entry not found in index

17.09.2015 13:20:36 ID successfully synchronized with vault 'O=FuWVault' for 'MaC Roaming/puw' (IP Address 10.76.111.166:62393).

17.09.2015 14:39:59 ID successfully downloaded from vault 'O=FuWVault' for 'MaC Roaming/puw' (IP Address 10.76.111.166:62393).

18.09.2015 00:22:44 Unable to find ID for 'Karl Heinz Eggers' in vault 'O=FuWVault'. Error: Entry not found in index



# ID Vault – Verwalten im Admin Client

- Werkzeug:

## Notes-ID-Vault verwalten



Mithilfe dieses Werkzeugs können Sie die Notes-ID-Vault '/ExperimentalVault' verwalten.

### Vaultverwaltungsaufgaben

Vaultbeschreibung bearbeiten

Vault-ID-Kennwort ändern

Vault-Replikserver verwalten

Vaultadministratoren hinzufügen bzw. entfernen

Organisationen, die der Vault vertrauen, hinzufügen bzw. entfernen

Berechtigung zum Zurücksetzen des Kennworts hinzufügen bzw. entfernen

Vaulttrichtlinieneinstellungen erstellen oder ändern



## ID Vault – in Action (21)

- Admin Client > Personen > Werkzeug ID Vault

The screenshot shows the Domino Admin Client interface. The top bar indicates the domain 'HANSECOM Domäne - Venus...' and the tool 'ID Vault für PT IDs'. The 'Personen und Gruppen' tab is selected, and the 'Werkzeuge' button is highlighted. The 'ID-Vaults' section is expanded, showing options like 'Kennwort zurücksetzen...'. A dialog box for password reset is also visible.

**Personen und Gruppen** | Dateien | Server... | Nachrichten... | Replizierung | Konfiguration

Server: **Venus/public transport/DE**  
Release 9.0.1FP4 HF70 auf Windows/Longhorn/64 6.1

**Werkzeuge**

Domino-Verzeichnisse

- public transport's Adre
  - Personen**
    - Nach Organisation
    - Gruppen
    - Mail-In-DBs und Re
    - Richtlinien
      - Dynamische Ric
        - nach Person/
        - nach Kategor

Person hinzufügen | Person bearbeiten

Sucher isse ar Nach Inc ? X

Name ^

|                        |
|------------------------|
| Administrator , User   |
| Connector , PT-COM     |
| IMB-Datenaustausch IMB |

Kennwort:

Arbeitsumgebung: Ulf NCP Home (Netzwerk)

☐ Kennwort vergessen?

Falls Sie Ihr Kennwort vergessen haben, wenden Sie sich an Ihr Support-Team.

# ID Vault – in Action (21 Min)

Helpdesk kann  
Passwort  
zurücksetzen



Werkzeug ID Vault > Kennwort zurücksetzen.

- Personen
- Gruppen
- Mail-In-DBs und

Roamer , MC2  
Roaming , MaC

**Benutzerkennwort zurücksetzen**

Mit diesem Werkzeug können Sie das Kennwort des Benutzers zurücksetzen.

Kennwort zurücksetzen

Abbrechen

Benutzername: MaC Roaming/puw

Automatisch generiertes Kennwort

Kennwort zurücksetzen und Benutzer benachrichtigen

Benachrichtigungsart: Persönlich

Neues Kennwort: ZkT4MKj6

Neues Kennwort bestätigen: ZkT4MKj6

ID-Vaults

Kennwort zurücksetzen

ID-Downloadzähler setz

ID aus Vault extrahieren.

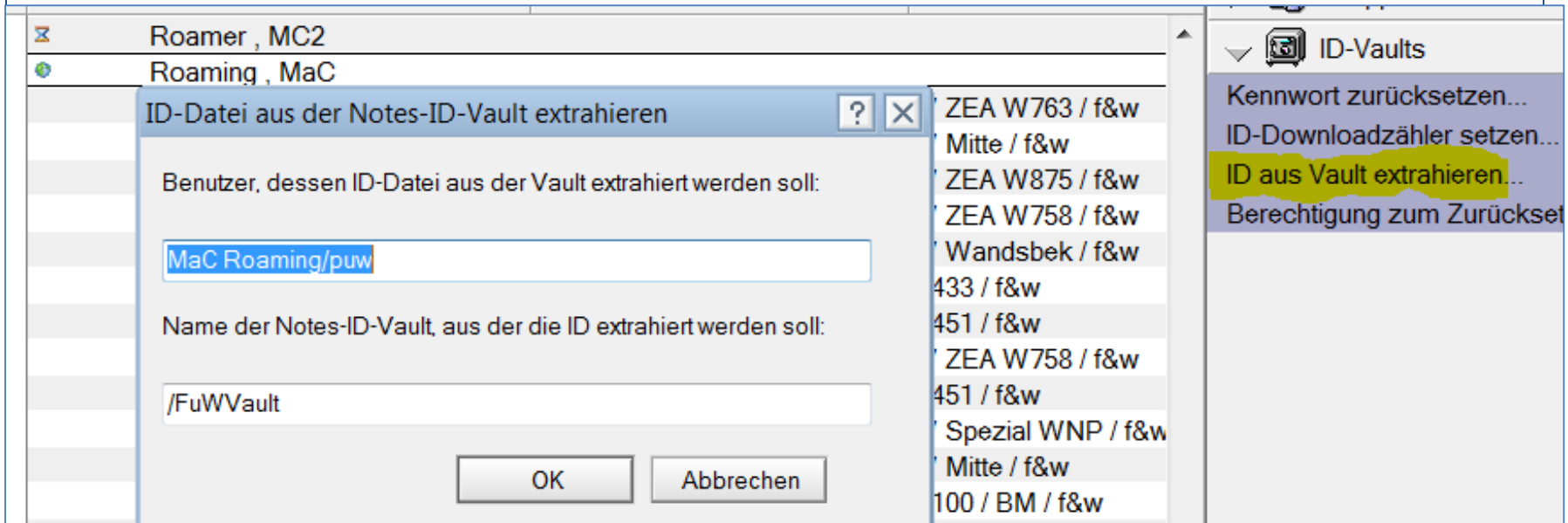
Berechtigung zum Zurück

# ID Vault – in Action

Auditor kann die ID extr.  
für Untersuchungen /  
Zugang verschlüs. Daten



- Werkzeug ID Vault > ID aus Vault extrahieren
  - Manager Recht an Vault und Rolle!
  - Neues Kennwort vergeben



# ID Vault Fehlersuche I - auf der Server Konsole

- show idvault  
Überblick ob alles Grün ist

```
ID Vault /ExperimentalVault (E:\Venus\IBM_ID_VAULT\ExperimentalVault.nsf)
Control Vault Name: /ExperimentalVault
Control Vault Servers: Venus/public transport/DE
Vault Operations Key: VO-dogb-biau/Venus/ExperimentalVault
Servers: Venus/public transport/DE
15.09.2015 08:30:19 Remote console command issued by Ulf Duvigneau/HanseCom/DE:
Vault Name: /ExperimentalVault
Description: ID Vault für PT IDs
Administrators: Birgit Dahdouli/HanseCom/DE
Administrators: Jürgen Bigdowski/HanseCom/DE
Administrators: Jürgen Lehnert/HanseCom/DE
Administrators: Martin Corleis/HanseCom/DE
Administrators: Ulf Duvigneau/HanseCom/DE
Servers: Venus/public transport/DE
Administration Server: Venus/public transport/DE
/public transport/DE trusts this vault
```

## ID Vault Fehlersuche II – Log Dateien

- Auf dem Server im Log > Security Events
- Auf dem Client

17.09.2015 11:20:05 ID Vault replica 'O=FuWVault' successfully created on server 'CN=LNSV04/O=puw' by 'administrator/puw' (IP address 172.30.4.39:53232).

17.09.2015 13:20:29 Unable to find ID for 'MaC Roaming/puw' in vault 'O=FuWVault'. Error: Entry not found in index

17.09.2015 13:20:29 ID failed to authenticate in vault 'O=FuWVault'. 'MaC Roaming/puw' (IP address 10.76.111.166:62391) made request. Error: Entry not found in index

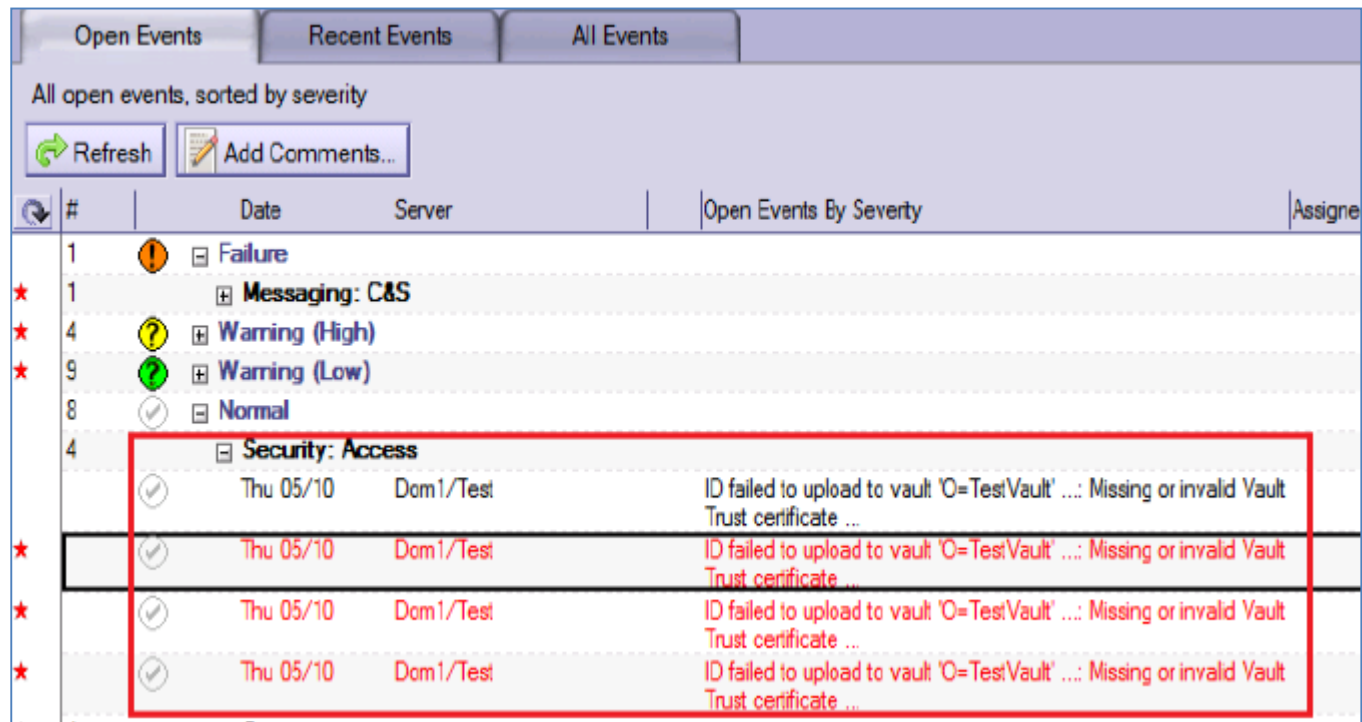
17.09.2015 13:20:36 ID successfully synchronized with vault 'O=FuWVault' for 'MaC Roaming/puw' (IP Address 10.76.111.166:62393).

17.09.2015 14:39:59 ID successfully downloaded from vault 'O=FuWVault' by 'Mac Roaming' (IP address 10.76.111.164:54783).



# ID Vault Fehlersuche III – DDM

- Domino Domain Monitoring (DDM.NSF) > Security
- Event Handler, die Mail senden wenn ID Vault Fehler



The screenshot shows the 'Open Events' tab in the Domino Domain Monitoring (DDM.NSF) interface. The events are sorted by severity. A red box highlights four 'Security: Access' events, each with a checkmark icon and the message 'ID failed to upload to vault 'O=TestVault' ...: Missing or invalid Vault Trust certificate ...'.

| # | Date      | Server    | Open Events By Severity  | Assigne |
|---|-----------|-----------|--|---------|
| 1 |           |           | Failure  |         |
| 1 |           |           | Messaging: C&S   |         |
| 4 |           |           | Warning (High)   |         |
| 9 |           |           | Warning (Low)  |         |
| 8 |           |           | Normal   |         |
| 4 |           |           | Security: Access   |         |
|   | Thu 05/10 | Dom1/Test | ID failed to upload to vault 'O=TestVault' ...: Missing or invalid Vault Trust certificate ... |         |
|   | Thu 05/10 | Dom1/Test | ID failed to upload to vault 'O=TestVault' ...: Missing or invalid Vault Trust certificate ... |         |
|   | Thu 05/10 | Dom1/Test | ID failed to upload to vault 'O=TestVault' ...: Missing or invalid Vault Trust certificate ... |         |
|   | Thu 05/10 | Dom1/Test | ID failed to upload to vault 'O=TestVault' ...: Missing or invalid Vault Trust certificate ... |         |

# ID Vault Fehlersuche IV – Log Parameter hochsetzen

- Wenn Probleme nicht lösbar mit Standard Ausgaben
  - Notes.ini Debug Paramter **Server**
    - DEBUG\_THREADID =1
    - CONSOLE\_LOG\_ENABLED = 1
    - DEBUG\_IDV\_CONNECT = 1
    - DEBUG\_IDV\_TRUSTCERT = 1
    - DEBUG\_IDV\_UPDATE = 1
  - Notes.ini Debug Paramter **Client**
    - DEBUG\_IDV\_TRACE = 1
    - DEBUG\_IDV\_TRUSTCERT = 1
    - DEBUG\_IDVAULT\_SERVER\_SELECTION = 1
    - DEBUG\_THREADID =1
    - CONSOLE\_LOG\_ENABLED = 1

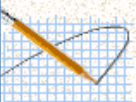


# ID Vault Einschränkungen

- „works as designed – in most cases!“
- CA Prozess kann nicht in der initialen ID Vault ID Erstellung benutzt werden (weil Certifier ID + Kennwort benötigt werden)
- Nicht Cross-Domain! Vault Repliken immer innerhalb einer Domäne sein. (Home-Mail-Server)
- Dieselbe ID mit unterschiedlichen Kennwörtern – erster Sync gewinnt (noch offen SPR MBOK8L44CS?)
- ~~Nicht supportet: offenem Schlüsselaustauschverfahren mit IDs – erst danach ID Vault aktivieren.~~
- IDs sollten lokale abgespeichert werden (Probleme mit SMB2 Netzwerk Verzeichnissen)

# ID Vault - Event

- Event Warnung, wenn keine Policy eingerichtet

|  |            |   |
|--|------------|---|
| <br><b>Venus/public<br/>transport/DE@PUBLIC TRANSPORT</b><br><br>14.09.2015 20:27 | An         | Auftrag-BK@Hansecom   |
|  | Kopie      |   |
|  | Blindkopie |   |
|  | Thema      | Integrity check failed for ID Vault O=ExperimentalVault: No Policy Setting found that use vault /ExperimentalVault: Invalid or nonexistent document |

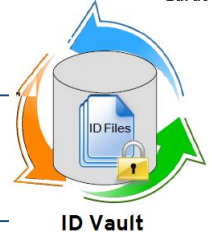
**Originating Server:** Venus/public transport/DE  
**Event Severity:** Failure  
**Event Type:** Network  
**Event Time:** 14.09.2015 20:27:02

## Lotus Entries

### Probable Cause:

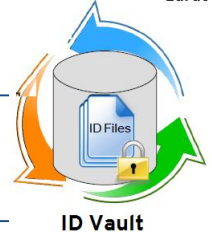
1. This message could appear for several reasons: 1. The PC Based Service has not been set up. 2. The Notes server name does not match the item part of the StreetTalk PC Based Service Name. 3. The PC Based Service Name does not reside in group@org of the Banyan username logged in at the Notes server. 4. The Banyan server where the PC based service resides is unavailable.

# ID Vault Bemerkenswertes I



- Roaming aktiv und ID im pnab, was tun? > Script, das es rausholt (client-side IBM tool called DetachID that can be used to remove the ID from the Personal Address Book)
- SETUP und ID Vault > ID wird aus dem Vault geholt
- Notes.ini Setting für Fehlversuche ID Kennwort gegen Vault & Vault resetting user
- Default user.id, andere ID Namen bleiben erhalten (ini Einstellung)
- ID Files mit multiplen Kennwörtern werden nicht gevaultet
- Notes Single Login (Dienst) ist nicht supportet, Notes Shared Login nutzen (SAML?)
- ID Vault Server über Notes Passthru Server ist nicht supportet.

# ID Vault Bemerkenswertes II

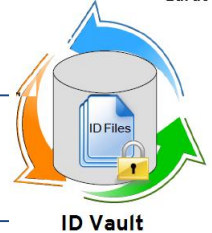


- Vault DBs nicht über den normalen Replik-Erstellen Prozess, sondern über das Manage Replica Tool
- 9er Admin Client nötig, wenn 9er ID Vault Server
- Key Paar Erneuerung nicht mehr vom Client aus, sondern nur noch über Policy
- Vault DB muss in Manage Vaults entfernt und manuell vom Server gelöscht werden
- Kennwortwiederhersteller, die nicht im Directory als Personendok. stehen (andere Zulassung) sollten hinein kopiert werden
- Vault-Manager brauchen Vault-ID und –Kennwort!

A screenshot of a Windows File Explorer window. The address bar shows the path: "lokaler Datenträger (C:) > Anwender > Notes > ids > vault". The main area displays a list of files and folders. The table below represents the data shown in the screenshot.

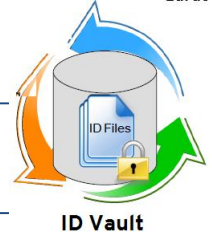
| Name                 | Änderungsdatum   | Typ   |
|----------------------|------------------|-------|
| experimentalvault.id | 14.09.2015 19:58 | ID-Da |
| experimentvault.id   | 14.09.2015 19:54 | ID-Da |
| fuwvault.id          | 17.09.2015 11:07 | ID-Da |

## ID Vault Bemerkenswertes III



- Vault IDs so behandeln wie Zertifizierer
- Die Schlüssel alter Server IDs sollten auf 2048-Bit aktualisiert werden, da diese benutzt werden, die Vault Schlüssel zu verschlüsseln.
- Server-ID mit Kennwort schützen.
- Fehlerhaftes ID-Herunterladen auf 10/Tag begrenzt
- IDs im Vault sind verschlüsselt
- ID Vault Transaktionen sind verschlüsselt
- ID Recovery und ID Vault laufen parallel
- Konfig-Datei für die Vereinfachung der Erstanmeldung bei Multiuser Installation (mit ID Vault) in Default Notes.ini:  
ConfigFile=c:\program files\notes\...\config.txt

## ID Vault Bemerkenswertes IV

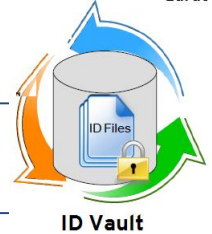


- **User Key Roll Over**

„The ID vault server takes care of the User key rollover process. For all vaulted users, the option for users to create new public keys from a Notes client is disabled. User key rollover is automatically triggered as configured via policy when needed, and is also automatically completed of by the ID vault. An advantage of this is that users will never receive dialogs related to User key rollover. Also, User key rollover will always only be initiated once on the ID vault server. Users should not attempt rolling over keys using pre-Notes 8.5 clients themselves, as this could lead to discrepancies between the user's local ID file and the vaulted ID file.”



# ID Vault Bemerkenswertes V



- **Anwender Umbenennung**  
„Renames are done on IDs in the vault and resynchronized to the user's local ID file. An administrator specifies a new name for a user and this user's Person Document is updated by the Administration Process with the new name information. The next time the user's ID file is resynchronized with the server, the new user name is transparently and automatically transferred to the user's local ID file. “

# Life Demo



# Fazit & Fragen?



Tausend Dank!



# Quellen / Hilfen

- [Domino Wiki](#)
- Lotus Knows: Colin Murray: nsl, WebSSO, Notes ID Vault
- [Admin Client Hilfe](#)
- [Open Mic Webcast: ID Vault across multiple ICS](#)
- Lotus Notes ID Vault, 19 Mai 2011, Open Mic
- ID Vault Best Practices, Open Mic 19 Dez 2012
- ID Vault in Notes Domino, Open Mic, 16 Mai 2012
- [ID vault interoperability FAQ](#), 8. Apr 2013
- [Transitioning to the ID vault and disabling ID Recovery, 20. Okt 2010](#)  
Empfehlung: Q&A hören und sich der indischen Akzente erfreuen
- IBM Support: [“How to set up a Notes client without user intervention using a scriptable setup”](#)