Lotus knows.
Smarter software for a Smarter Planet.

Lotus Domino Security
NSL, Web SSO, Notes ID vault

Collin Murray | Program Director, Lotus Domino Product Management
Challenge: Reduce Cost of Ownership

- IBM® Lotus® Notes® and Domino® have been providing a secure Public Key Infrastructure (PKI) for years
- There is a cost associated with managing ID files
  ➔ Significantly lower this cost without compromising security
Agenda

- Lotus Notes ID vault
- Lotus Notes Shared Login
- Windows single sign-on for web clients in Domino 8.5.1
Agenda

- Lotus Notes ID vault
  - Overview
  - User experience
  - Administration
  - Password resetting
  - Integration with other products
  - ID vault Security
  - Best practices
  - Planning a vault deployment

- Lotus Notes Shared Login

- Windows single sign-on for web clients in Lotus Domino 8.5.1
What is the Lotus Notes ID Vault?

Secure, centralized, server-based repository for storing and managing Lotus Notes ID files

- Streamlines process for resetting forgotten passwords, significantly reducing costly user downtime and help desk costs
- Simplifies provisioning of Lotus Notes IDs
- Automatically uploads ID files to vault for existing users
- Manages changes across multiple copies of Lotus Notes ID files
- Provides “Auditor” function to extract ID files for legal discovery/access to encrypted data
ID Files

Lotus knows.
Smarter software for a Smarter Planet.

Automatic harvests existing ID files
Provisions ID file to new user or user who has lost ID file
Help desk can reset passwords
User can use new password
Auditor can download ID file for legal discovery/access to encrypted data

Help desk can reset passwords
User can use new password

ID vault

Provisions ID file to new user or user who has lost ID file
Help desk can reset passwords
User can use new password
Auditor can download ID file for legal discovery/access to encrypted data

Synchronizes multiple copies of ID file

lotusknows.com
Simple ID Vault Environment

- **Password resetter**
- **User**
- **Vault Administrator**

**ID Vault**

**ID Files**
User Experience

ID Vault

Password resetter

User

Vault Administrator

ID Files
I forgot my password!
I accidentally deleted my ID file!
Provisioning and Updating
The User Experience

- This slide intentionally left blank
Synchronizing ID Files

- Changes made in one copy of the ID file will resync immediately with the ID in the vault
- Other clients will periodically check to see if the ID in the vault is different from their ID and they need to resync with the vault

Vault server:
ID, hash

Laptop
Client: ID, hash

Desktop
Client: ID, hash

Home
Client: ID, hash
Password Changes
Change your password once, use it everywhere!

- Password is not stored on the server or ever sent to the server
- Password changes while off-line may take time to arrive at the vault
- Password changes made on pre-8.5 clients will not synchronize with the vault

Vault server:
ID, Auth data

Laptop Client:
ID w/ pwd

Desktop Client:
ID w/ pwd

Home Client:
ID w/ pwd
User Key Rollover in the ID Vault

- New keys will be generated on the Lotus Notes ID vault server and distributed from there to all “client” copies of the ID
  - No additional configuration
  - No confusing dialogs presented to the end user
Renames and Org Moves

- Renaming vaulted users and moving vaulted users to new organizations will automatically be performed in the vault by the 8.5 admin client
  - No additional configuration required
Vault Administrator

ID Vault

ID Files

Password resetter

User

Vault Administrator

lotusknows.com
Configuring the Lotus Notes ID Vault

- Use Admin Client to create and manage ID vaults
  - Create Vault Trust Certificates
  - Create Password Reset Certificates
- Create/edit security policy to map Lotus Notes users to vaults
- Running in a mixed environment
  - Admin server, vault server, at least one mail server per cluster must be upgraded to Lotus Domino 8.5
  - Lotus Notes 8.5 required
    - ID file is backward compatible
    - Vault policies can be put in place before client upgrade and as clients are upgraded, policy will go into effect
Password Resetting

Password resetter

User

Vault Administrator

ID vault

ID Files
Password Reset
Using the Admin Client

Lotus knows.
Smarter software for a Smarter Planet.
Password Reset Options

- **Help Desk**
  - Issue password reset certificates to a small number of highly trusted individuals
  - Issue a password reset certificate to a “helpdesk” OU
    - Renaming people to that org will grant/deny access
    - Issue special IDs for resetting passwords
  - Issue a password reset certificate 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

- **Self Service application**
  - Authenticate to another system first
  - Password sync with other systems
  - Provide answers to “security” questions

- **Sample web agent in PwdResetSample database**
Password Reset with the ID Vault

Helpdesk

Self service password reset application

Domino ID Vault

Notes IDs

Lotus Domino

Notes ID

Lotus Notes

lotusknows.com
Integration with other products

- 8.51: Lotus Notes ID vault integration with iNotes, BES, and Traveler
  - Decrypt incoming mail messages without manually importing Lotus Notes ID files into their mail databases
  - Get password reset in the ID vault
  - Use the new passwords automatically to perform secure mail operations
  - Automatically synchronizes ID files in both the mail database and the ID vault when necessary as soon as a user provides a password to perform a secure mail operation.
Integration with other products

- **8.5.x**: New SDK C-APIs allow you to integrate the ID vault with your program.
  - **SECidfPut**
    - Put an ID file into the vault (used when an ID isn’t found in the vault)
  - **SECidfGet**
    - Get an ID file from the vault (used when an ID file isn’t found locally, but is in the vault)
  - **SECidfSync**
    - Sync an ID with the copy in the vault

- If you already have an application for backing up files, use these APIs to load the ID vault.
Notes ID Vault SDK APIs

- SECAttachFileToDB
- SECExtractIDFileFromDB

- Enabled in the ID Vault tab in a security policy, and the security policy is assigned to users

- SECAttachFileToDB
  - Read the user name from the ID file to be attached
  - Query the policy record of this user for ID Vault integration enablement
    - If the user is not enabled, just attach the ID file as before
    - If the user is enabled, contact an ID Vault server, perform an upload or sync with the ID Vault, then attach the file to the DB
Notes ID Vault SDK APIs

- **SECExtractIDFileFromDB**
  - Extract the ID file from the named profile
  - If successful, the user name is extracted from the ID file
  - Query the policy of this user for ID Vault integration enablement
    - If user is not enabled, return results of the extract
    - If user is enabled, contact an ID vault server, perform an upload or sync with the ID Vault
  - Attach the updated ID file to the DB
  - If there is no ID file found on the database during extract then the user name is looked for in the pReserved parameter (new use of pReserved for 8.5.1)
  - If user name is not found in pReserved, return an error
  - If user name is found in pReserved
    - Query the policy of the user for ID Vault integration enablement
    - If user is not enabled, return an error
    - If user is enabled, download the ID file and return to the caller
    - ID file is attached to the database
Lotus Notes ID Vault Security
Protection Against Unauthorized Access to Vault Contents

- ID files are encrypted and unusable if detached.
- Each ID file -> different 256 bit AES Storage Encryption key -> 2048 bit RSA Vault Operations key -> Server ID file
- You should limit access to vault through ACL.
Protecting Data Transmitted Over the Network

- All information transmitted to and from the vault is encrypted.
- A new 256 bit AES Transport Encryption key is used for each transaction.
- A different Initialization Vector (IV) is used each time the TE key is used.
Protection Against Unauthorized Downloads

- Only the server can verify password guesses, not the client. Vault server logs every failed password attempt.
- Max 10 “strikes” failed password attempts per ID file per day, configurable.
- Option to require authorization for all downloads.
Protection Against Unauthorized Password Resets

- Any server or person involved with password reset must have a password reset certificate.

- Password reset applications must be signed by a person and reside on a server who have been issued password reset certificates.

- Creation of password reset certificate requires access to certifier ID.
Protection Against an Unauthorized Vault

- A parent certifier of the user ID must have issued a Vault Trust Certificate to the vault before ID file upload.

- Creation of vault trust certificate requires access to certifier ID
ID Vault Best Practices

- Plan deployment carefully
- Protect vault ID files like O-level certifiers
- Upgrade server ID keys to 2048-bit
  - Used to encrypt the vault keys
- Password protect server ID
Planning Lotus Notes ID Vault Deployment

- **Lotus Domino domains**
  - Cross domain vaults not currently supported
  - Create one or more vaults per domain
  - Create multiple replicas for failover/load balancing

- **Certificate hierarchies**
  - Determine at which OU/Org levels to establish trust with vault and for password reset authorities

- **Replication topology**
  - Load on replicas balanced evenly
  - May need to configure regional vaults to optimize network access

- **Organizational/political requirements**
  - Are there local laws or policies to consider in a global environment?

- **Determine password resetting scheme(s)**
  - Help desk
  - Self service application
Notes ID Vault Security Summary

- 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
What about R5 “ID File and Password Recovery”?

- Still supported, but no enhancements planned
- Expect that more customers will use Notes ID vault
- IDs configured for “password recovery” can also be vaulted
- Unless recovery information is removed, backups will continue to be sent to the recovery database
- Edit recovery information from Admin client to remove recovery information
Transitioning from ID Recovery

- The ID vault can be deployed at any time.
  - Both the ID vault and ID Recovery can be used together.
  - ID Recovery can be disabled later.
  - ID file backups for ID vault users may not be automatically triggered to ID Recovery database.

- Disabling ID Recovery not recommended until servers/clients have been upgraded to 8.5.1.
Agenda

- Lotus Notes ID vault
- **Lotus Notes Shared Login**
  - Overview
  - How Notes shared login works
  - User and admin experience
  - Best practices
  - Deployment considerations
  - Using NSL with the ID vault
- Windows single sign-on for web clients in Lotus Domino 8.5.1
Why Deploy Lotus Notes Shared Login?

- Reduce number of passwords users need to remember
- Eliminate Lotus Notes password prompt ("single sign on")
  - Rely on operating system login credentials
  - Microsoft® Windows® only in 8.5
- Eliminate need to manage Lotus Notes ID passwords
  - No need to change Lotus Notes ID password
  - No need to recover from forgotten Lotus Notes passwords
  - No need to synchronize Lotus Notes password with other passwords
- Management of Lotus Notes Shared Login is made simple
How Lotus Notes Shared Login works in 8.5

- Function of Lotus Notes ID remains unchanged
  - Client authenticates to Lotus Domino server using client/server authentication
  - ID continues to hold and manages Internet certificates
  - ID continues to hold and manage secret keys
- Windows credentials used to lock and unlock the Notes ID file
- Password management is controlled by Windows mechanisms and policies
User Experience for Enabling NSL

- User enters Lotus Notes password once to authenticate before feature is enabled
- Lotus Notes will no longer prompt user to enter Lotus Notes password when launching Lotus Notes client
- When accessing User Security settings or attempting to unlock Notes after being timed out, user prompted for operating system password
How NSL is enabled on the client

1. User logs into Windows
2. At Lotus Notes startup, policy / configuration detect that NSL should be enabled
3. Notes generates a new long complex untappable secret
4. Lotus Notes calls the Microsoft DPAPI to encrypt the secret based on the user's current Windows identity and the current machine, and additional application specific entropy.
5. Lotus Notes stores the encrypted secret on the client machine in the user's profile directory
6. Lotus Notes encrypts the ID file with a bulk key derived from the new secret

Windows Identity

Entropy

Random Secret

ID File

Notes Encryption

Encrypted ID File
How NSL is used on the client

1. User logs into Windows
2. User starts the Notes client
3. The ID file indicates that it is NSL enabled.
4. The Lotus Notes client locates the encrypted secret on the desktop and calls the Microsoft DPAPI to decrypt the secret using the current user's identity on this machine.
   - Note that the DPAPI will work across Windows password changes whether they are made on the client or the Domain Controller!
5. The Lotus Notes client uses the secret to decrypt the ID file
6. Lotus Notes is running without a password prompt!
Administration

- Configured using security policy:
  - Can NSL be enabled?
  - Is it initially enabled or disabled?
  - Can the user enable or disable it themselves?
- Disabled by default; must be enabled by an admin
- Customizable end user messages when enabled/disabled
- Eliminate need to manage Lotus Notes password policies/expiration
## Lotus Notes Shared Login Security Policy

### Security Settings

<table>
<thead>
<tr>
<th>Basics</th>
<th>Password Management</th>
<th>Execution Control List</th>
<th>Keys and Certificates</th>
<th>Signed Plug-ins</th>
<th>Portal Server</th>
<th>ID Vault</th>
<th>Comments</th>
<th>Administration</th>
</tr>
</thead>
</table>

### Password Management Basics | Notes Shared Login

#### Notes Shared Login

<table>
<thead>
<tr>
<th>Setting</th>
<th>Option</th>
<th>How to apply this setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Notes shared login with operating system:</td>
<td>Yes</td>
<td>Set initial value</td>
</tr>
<tr>
<td>Allow User Changes?</td>
<td>Yes/No</td>
<td>Don't setvalue</td>
</tr>
</tbody>
</table>

#### Activation Notification

<table>
<thead>
<tr>
<th>Setting</th>
<th>Option</th>
<th>How to apply this setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to notify users when enabled:</td>
<td>System dialog</td>
<td>Don't setvalue</td>
</tr>
<tr>
<td>Custom message text:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Deactivation Notification

<table>
<thead>
<tr>
<th>Setting</th>
<th>Option</th>
<th>How to apply this setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to notify users when disabled:</td>
<td>System dialog</td>
<td>Don't setvalue</td>
</tr>
<tr>
<td>Custom message text:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
NSL Best Practices

• Access to Lotus Notes/Domino is managed by Windows identity
  – Use best practices for Windows passwords, such as minimum password strength rules and regular mandatory password changes
  – Use best practices for physical security, such as requiring the locking of the workstation when unattended
  – Note that Windows password is required to open User Security dialog and export password protected copy of ID file

• ID Backup system in place
  – Lotus Notes ID vault
  – ID recovery database
  – 3rd party or customer system (backup the password protected copy)

• Disable Lotus Notes server based password checking on pre-8.5 servers

• Do not install optional “Client Single Logon” component

• Review deployment considerations for applicability in your environment
Using NSL with the ID Vault

- Designed to work together!
- Allows for provisioning of ID files and to recover lost/damaged ID files
  - Use password reset to download new copy
  - User enters password once
  - ID then enabled again for NSL
- If ID vault is not used, another backup system is strongly recommended for recovery purposes
How Notes Single Logon works today (Notes 6+)

- Allows user to launch Notes without entering Notes password
- Notes Single Logon service is an optional install component
  - Uses network provider and Windows service to capture entered password
  - Requires synchronization of Windows password and Notes ID file password
- Must be enabled by the user via User Security dialog
- Common problems
  - Password policies for Windows and Notes may not line up well
  - Only synchronizes passwords changed on the local machine
- Notes Single Logon will continue to be supported with Notes 8.5 for backwards compatibility (with no changes)
NSL Deployment Considerations

- Lotus Notes to Internet password synchronization cannot be used with NSL enabled ID files
  - NSL ID files have no password – there is nothing to synchronize
  - New procedures may be needed to synchronize Windows passwords with Notes Internet passwords
- Because the secret that locks the NSL enabled ID file is specific to each client machine:
  - NSL enabled ID files cannot be imported into mail file for iNotes/Blackberry access
    - Not a problem if a password protected copy is made
  - NSL enabled ID files cannot be directly copied to another client machine
    - Not a problem if ID vault is used to keep all copies synchronized
    - Not a problem if a password protected copy is made
NSL is not supported for IDs that are:

- Used on Mac or Linux clients
- Protected by smartcards
- Protected by multiple passwords
- Used by roaming users whose ID files roam in the personal address book
- Used with Notes on a USB drive
- Used in a Citrix environment
- With Windows mandatory profiles
- Stored on network shares
- Enabled for password checking/expiration (unless all servers are 8.5+)
- Used with Notes to Internet password synchronization
- NSL enabled ID cannot be imported into mail file for DWA/Blackberry access (create password protected copy to import)
Slightly More Obscure Considerations for NSL

- The following configurations are not supported with NSL
  - Using Windows Roaming Profiles and logging into an Active Directory Domain from more than one system at the same time (this is a limitation with MS DPAPI)
  - Using Windows Roaming Profiles and logging into an Active Directory Domain from both Windows XP/Windows 2003 systems and Windows 2000 systems (this is a limitation with MS DPAPI)
  - Using Windows NT 4.0 Domains
  - Using Windows XP in a Windows Workgroup environment and resetting the user’s Windows password
- Joining or leaving a Windows Domain after enabling NSL
Agenda

- Lotus Notes ID vault
- Lotus Notes Shared Login
- Windows single sign-on for web clients in Lotus Domino 8.5.1

Overview
Windows Kerberos
SPNEGO
How it works
8.5.1 Windows single sign-on for Web clients

- Providing SSO for Web user on Windows desktop
  - Sometimes called by these other names:
    - SPNEGO
    - “Integrated Windows Authentication” for the Windows Intranet
  - Browse to URLs without being challenged for user name and password.
Bare Minimum Deployment

- **Lotus Domino 8.5.1 server on Windows**
- **Windows 2003 or 2008 server**
- **Intranet Windows client**
  - **Browser:**
    - Mozilla Firefox®
    - Internet Explorer®
Overview Leveraging Windows Kerberos Security

- User logs into Windows
- Windows domain controller verifies user's password.
  - password NEVER travels over the wire!
- Applications can learn who the user is, leveraging the user's Windows Kerberos credentials
About Windows Kerberos Security

• Kerberos security is built into Windows
  • Active Directory contains the user information
  • Kerberos KDC (key distribution center)
• Kerberos standard is specified in IETF RFC 1510
• Windows single sign-on for Web clients requires Windows server 2003 or greater
  • Windows 2000 backwards compatible modes not supported
About SPNEGO protocol used by browsers

- SPNEGO protocol used to authenticate the user to the HTTP server
  - SPNEGO: Simple and Protected gss-api NEGOtiation
  - Microsoft specifications published in RFCs 4559, 4178

- SPNEGO is only for the Intranet
- SPNEGO security mechanisms
  - Kerberos
  - Legacy NTLM (not supported by Domino)
Browser and Domino participate in SPNEGO authentication

1. SPNEGO/Kerberos used to authenticate the logged in Windows user to Domino.
LTPA token facilitates SSO

1. SPNEGO/Kerberos used to authenticate the user to Domino.

2. Domino returns an LTPA token for the authenticated user.

3. LTPA token used thereafter to authenticate the user to other SSO servers.
Links

- Troubleshooting technote for Windows single sign-on for Web Clients
- OpenNTF project for Windows single sign-on for Web Clients on non-Windows platforms
- Lotus Security Homepage – bulletins, articles, redbooks, doc
- Lotus Notes and Domino Wiki
- Redpaper: Security Considerations in Notes and Domino 7
- Lotus Security Redbook
Questions?
Creating an ID Vault
Creating Lotus Notes ID Vault

- “Tools > ID Vaults > Create” from Configuration tab
- Specify a name for the vault – used for
  - Hierarchical name of vault
  - Database file name
  - Vault ID file (used when adding or removing vault replicas)
- Specify password for vault ID
- Select server on which to deploy vault
Creating Lotus Notes ID Vault, cont

- Select at least one vault administrator
  - Add / remove vault servers
  - Delete ID files from the vault
  - Add / remove other administrators
- Select organizations or organizational units whose IDs will be stored
  - Need access to certifier IDs
  - Vault Trust certificates are created for each certifier and stored in Domino Directory
  - Only IDs registered with these certifiers can be uploaded to the vault
- Select user names that are authorized to reset passwords
  - Password Reset certificate is created for each user
  - Include IDs associated with any self-service password reset application
Creating Lotus Notes ID Vault, cont

- Create ID vault policy
  - Create new
  - Edit existing
  - Skip and create later

- Create Vault
  - Locate certifier IDs
Lotus Notes ID Vault Creation Complete

- **Vault ID**
  - On vault creators desktop
  - Should be secured like a certifier ID
  - Needed to create vault replicas

- **Vault Trust Certificate**
  - Lotus Notes Cross-Certificates stored in Lotus Domino Directory
  - One for each registered certifier

- **Password Reset Certificates**
  - Lotus Notes Cross-Certificates stored in Lotus Domino directory
  - One for each user or application authorized to reset passwords

- **ID Vault application**
  - Stored on hosting Lotus Domino server
  - Encrypted with hosting Lotus Domino server ID

- **Policy Settings**
  - If selected during Vault install
  - In new or existing policy document
Lotus Notes ID Vault Configuration

- Security Settings > ID Vault tab
  - Hierarchical name of vault
  - Forgotten password help text
  - Enforce password change
  - Automatic ID downloads
    - Time limit
    - Failure message
- Person document > ID Vaults
  - Number of downloads

![Security Settings: RENVaultVaultSetting](image)

![Set User's ID Download Count](image)
Initial ID file Distribution
Vault Trust Certificate

- **Vault Trust Certificate**
  - Special cross-certificate created by a certifier
  - Example: O=DSKTest:VT:O=DSKTest Vault

- **Vault ID file**
  - Acts like a certifier ID file for vault operations
  - Example: ID file for “O=DSKTest Vault”

```
Certifier ID
O=DSKTest

Vault Trust Cert
O=DSKTest:VT:O=DSKTest Vault

Vault ID
O=DSKTest Vault
```
Vault Trust (continued)

**Certifier ID**
O=DSKTest

**Vault ID**
O=DSKTest Vault

**Vault Trust Cert**
(in Domino directory)

**Server ID**
lich/DSKTest

**SVCert**
(in Vault Servers doc)

**Vault Servers**

**Vault Operations (VO) Key**

**Vault Trust Certifier ID**

**Vault ID**
O=DSKTest Vault

**Certifies**

**Server ID**
lich/DSKTest

**Encrypt**

**Vault Operations (VO) Key**

**Document**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Data Type</th>
<th>Data Length</th>
<th>Seq Num.</th>
<th>Dup Item ID</th>
<th>Field Flags</th>
<th>Names Protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Name</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>SUMMIT</td>
<td>N/A</td>
</tr>
<tr>
<td>$Owner</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$Cert</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$VOKey</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$VOName</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Document**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Data Type</th>
<th>Data Length</th>
<th>Seq Num.</th>
<th>Dup Item ID</th>
<th>Field Flags</th>
<th>Names Protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Name</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>SUMMIT</td>
<td>N/A</td>
</tr>
<tr>
<td>$Owner</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$Cert</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$VOKey</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$VOName</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Document**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Data Type</th>
<th>Data Length</th>
<th>Seq Num.</th>
<th>Dup Item ID</th>
<th>Field Flags</th>
<th>Names Protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Name</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>SUMMIT</td>
<td>N/A</td>
</tr>
<tr>
<td>$Owner</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$Cert</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$VOKey</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$VOName</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Document**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Data Type</th>
<th>Data Length</th>
<th>Seq Num.</th>
<th>Dup Item ID</th>
<th>Field Flags</th>
<th>Names Protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Name</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>SUMMIT</td>
<td>N/A</td>
</tr>
<tr>
<td>$Owner</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$Cert</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$VOKey</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>$VOName</td>
<td>Text</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Password Reset Certificates

- 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

```
Certifier ID
O=DSKTest

Password Reset Cert
O=DSKTest:PR:CN=dskadmin/O=DSKTest

dskadmin/DSKTest
```