



Kevin Cooper
Principal Consultant
Systems Evolution, Inc.

Digital ID World Virtual Directory Panel

May 10, 2005



Pre-Existing Directory/Identity Environment

- Global (parent) corporation hosting two Active Directory implementations:
 - User profile directory
 - contains contact info, public certificates, corporate user ID (numeric)
 - can be searched, but not used for authentication
 - Domain users
 - exposes authentication services for users across all corporate Windows domains
 - can **not** be searched ... but, information resident within the user profile directory can be used to synthesize the DN's for this directory, so programmatically we can locate these records and bind against them.



Pre-Existing Directory/Identity Environment

- **Plus**, my client (a subsidiary of this corporation) maintains its own user base:
 - Oracle database
 - Java API exists that applies business logic for password management and auditing to satisfy regulatory and S-Ox requirements



Integration solutions before Virtual Directory

- Mostly used in custom development only
 - Home-grown applications (Java, PHP, PL/SQL)
 - Customizations to off-the-shelf software
- Due to the “non-standard” directory configuration, using the LDAP connectors available with packaged software was impossible.

Example custom pseudo-code:

```
$userAttrs = ldap_search("(uid=12345)");  
$bindDN = 'cn = ' + $userAttrs['msUser'] +  
          ',dc=' + $userAttrs['msDomain'];  
$result = ldap_bind($bindDN, 'myPassword123');
```



Why Virtual Directory?

- Predetermined enterprise directory structure is unchangeable, thus unusable for most packaged software
- Need for incremental changes to support new applications as new requirements are discovered
- Need to merge LDAP directories and proprietary data sources and API's into a single, logical directory



Why not Meta-Directory?

- Design and construction overhead would be cost-prohibitive to smaller business application projects. Directory architecture concerns are generally considered “out of scope” for tactical implementations.
- Changes to the corporate directory structure (managed outside our IT group entirely) could result in significant (and immediate) effort to repair and regression test a meta-directory solution.
- Network bandwidth and processing power on source LDAP servers is plentiful, thus it is not necessary to leverage a meta-directory to improve performance.







Our Deployment

Virtual Directory Product: OctetString VDE

- LDAP connectors to our two corporate AD's
- Joiner API – allowed us to customize the “join” rules for the two AD's (moves the logic shown earlier from the client app to the middle tier)
- Adapter API – facilitated a custom “backend” to talk to our proprietary (operating company) Java API to access our local user store
- Plugin API – allowed us to insert additional, read-only attributes to user records as entry data is returned to the client. (This “extra” data is maintained within a separate Oracle database)
- All data above accessible to applications from a single point of entry



-  VDE integration points
-  Database table
-  active Directory
-  Custom API + data store

