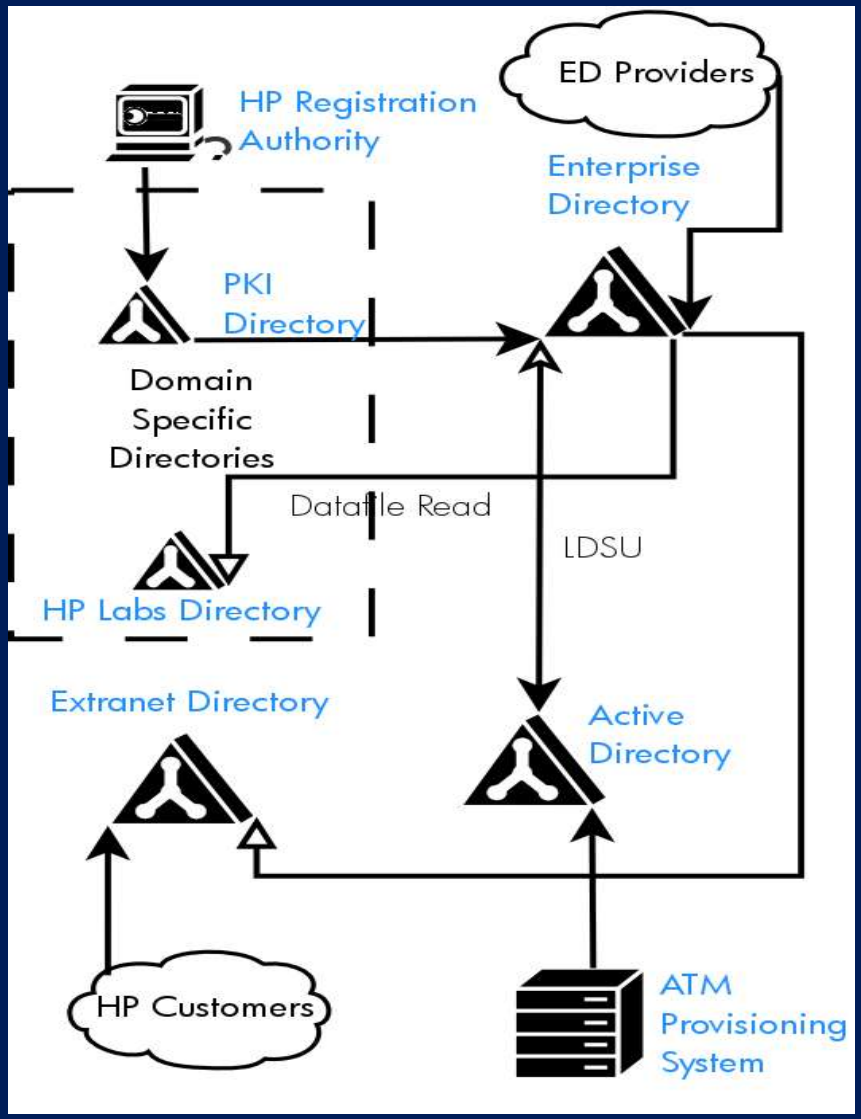
Enterprise Directory requirements for OpenLDAP

Neil Dunbar (neil.dunbar@hp.com)
Kartik Subbarao (kartik.subbarao@hp.com)
Directories Team, HP Services

HP Directories Structures

- Main Directories
  - ED (generic LDAP aware apps)
  - AD (Windows 2K NOS functions)
  - XD (customer data for managed services)
  - synced by LDSU
- Domain Specific
  - HP business units which maintain their own "view" of the directory space with added attributes



HP Directory Services (cont'd)

- Enterprise Directory (ED)
  - Sun ONE
- Active Directory (AD)
  - Microsoft Active Directory
- Extranet Directory (XD)
  - OpenLDAP (actually still Sun ONE – cutover date is Friday, 13th August)
- Domain Specific Directories
  - OpenLDAP mainly, some Sun ONE
- "OpenLDAP" is the Symas Connexitor branded version.
- General policy is "Smart Directory, Dumb Application"
- OpenLDAP is the system of choice for XD and ED within 18-month timeframe

Challenges for OpenLDAP - General

- General enterprise grade robustness
  - Solid Berkeley DB support
    - LDBM would never cut it
    - Generic relational DB too slow and resource greedy
  - Reliable replication strategy
    - robust, scalable, restartable and modifiable
  - Audit capability
    - all DIT operations must be verifiable and searchable
  - Flexible ACI policy
  - Reconfiguring must be available on-the-fly as much as possible
    - Restarting a directory server is a last resort.

Challenges to OpenLDAP – Password Policy

- Password Policy is needed in XD
  - Must be able to specify password constraints and have directory enforce them
  - One size does not fit all
    - different groups of users need different control policies
- HP prototyped the code in December 2003
- Symas rewrote the code into an overlay module in February 2004
- More flexible than Sun ONE implementation
  - tracking the draft documentation more closely

OpenLDAP needs – Data Constraints

- Consistent with "Smart Directory, Dumb Application"
  - Attribute constraints
    - Restricts attributes to particular regular expressions
    - Written by HP in May 2004
  - Attribute value uniqueness
    - Ensures an (attribute, value) tuple cannot be replicated within a backend
      - Written by Symas in March 2004
  - Referential integrity
    - Ensures that a dn-valued attribute changes its value automatically if the referenced DN changes
      - Written by Symas in March 2004

OpenLDAP needs – Group Policy

- Groups can be constrained in several ways
  - Ownership of groups
    - Minimum, maximum number of owners
    - Owners constrained to certain filters (eg, must be permanent employees, not contingent workers)
  - Similarly for members
    - enforcement of "flat" groups (eg, Unix groups), so members of the group must not be other groups
  - Policies can specify remedial action within their entries
    - Prohibit the violating action
    - Notify the group owners of pending violation
    - Delete the group
  - Module still under development in HP

OpenLDAP needs - translucency

- Want to be rid of domain specific directories copying huge chunks of information
  - Need a modified metadirectory approach
  - OpenLDAP server presents munged view of the main directory (ED, AD, XD)
  - OpenLDAP overlays domain specific attributes and values onto the “main” entries
    - No more sync'ing data
    - No more changing schema for 1-2% of customers
- Written by Symas in June 2004
  - HP still testing

OpenLDAP needs - ACIs

- ACI expressions in OpenLDAP are sufficiently expressive
  - if not documented well enough!
- Cannot be changed without server restart
  - Symas working on this right now
  - Eventually, we would like ACIs to be stored in the DIT itself (like IBM Directory Server, or Sun ONE)
  - Huber, Blakley, et al, ACI syntax seems overly complex
  - Sun ONE syntax simple, but semantically unpleasant
  - Possibility for plugin to implement in-DIT ACIs
- Long term future – HP is undecided
  - immediate problem is to use existing OpenLDAP syntax ACIs but be able to change running profile without server restart.

Summary

- OpenLDAP codebase is not in itself enough for HP's Enterprise Directory
  - SLAPI and overlay support make it possible to add functionality to give us feature-for-feature capabilities
  - Cost advantages massively outweigh the competition for our needs
  - Source availability means we can run debugger on running code and see where things go wrong
    - reduces support costs
- Look forward to being an OpenLDAP shop in 2005

Fin

Illustration of Group Policy