

KDC LDAP Schema

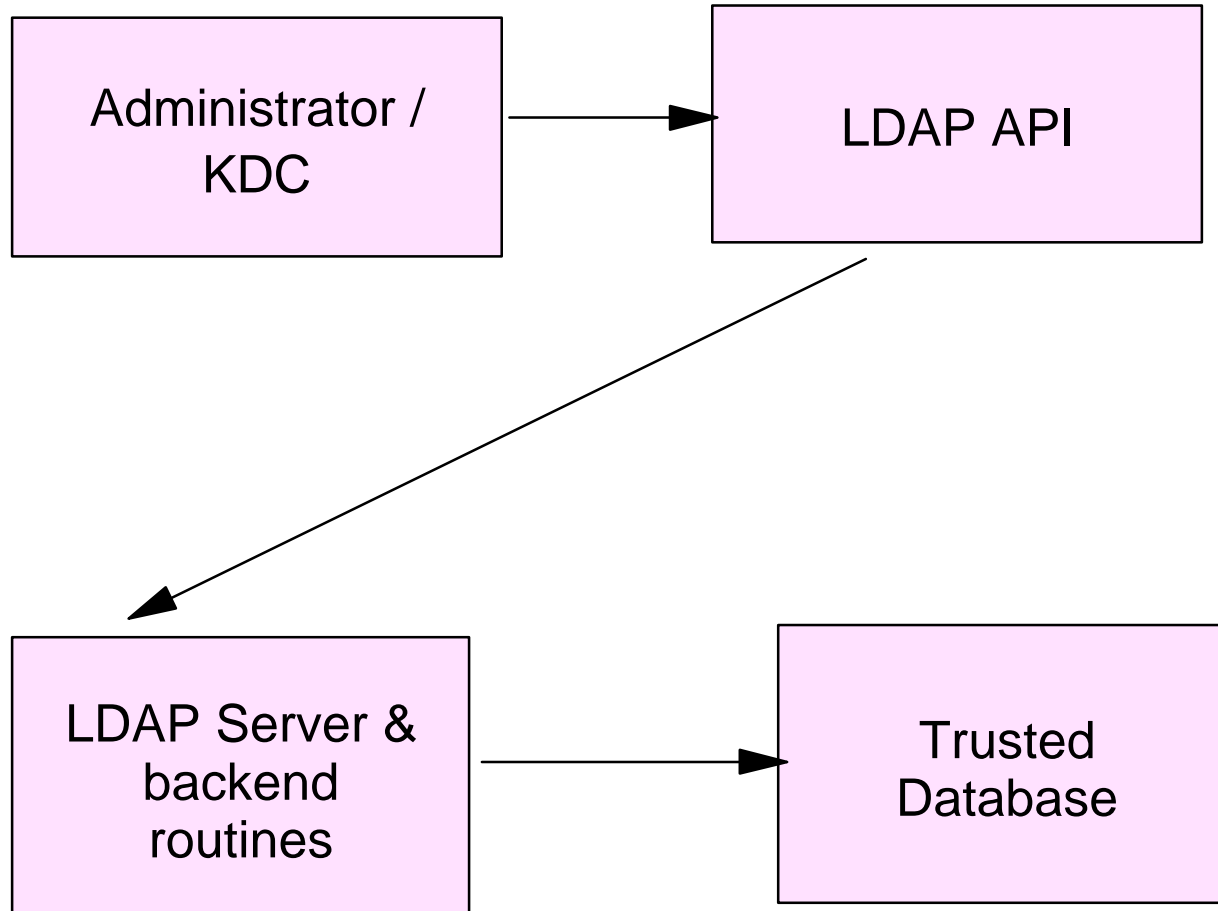
IETF 11/02

Donna Skibbie, IBM

Overview

- KDC LDAP Schema draft: Defines all KDC attributes except for those used to store key data
- Keys Extension draft: Defines attributes used to store key data

Flow of Data to LDAP



Progress

- 3/01: Version 1 of KDC LDAP schema draft submitted to IETF Kerberos working group
- 1/02: Started work on Version 2 of KDC LDAP schema draft and Keys Extension draft
- 4/02: Version 2 of KDC LDAP schema draft submitted
- 4/02: Version 1 of Keys Extension draft submitted

Major Revisions Required

- Limit scope of drafts to KDC management concerns (do not mention LDAP/DB backend)
- Define only those attributes mentioned in Kerberos Revisions

Minor Revisions Required

- Reference other drafts/RFCs for principal types and encryption types
- Define administrative error conditions
- Add section on future extensibility
- Move lastLogon to the principal entry
- Delete the log entry
- Delete LDAP authentication warning; no longer applies
- Use LDAP URL syntax for krbPrincSubtree
- Short names must be registered
- Use of compound matching

Major Open Issue

- Create a separate draft defining KDC information model?

Other Open Issues

- Should we mandate the structure of the DIT?
- Should we mandate the RDN?
- Should we define LDAP syntax definitions for certain attributes?
- Should we use multi-valued rather than bit-mask attributes?

Current Distribution List for Schema Drafts

- Tolga Acar <tacar@novell.com>
- Morteza Ansari <morteza.ansari@sun.com>
- John Griffith <john.griffith@entegrity.com>
- Timothy Hahn <hahnt@us.ibm.com>
- Paul B. Hill <pbh@mit.edu>
- Wyllys Ingersoll <wyllys.ingersoll@sun.com>
- Leif Johansson <leifj@it.su.se>
- Bob Joslin <bob_joslin@hp.com>
- Bob Morgan <rlmorgan@washington.edu>
- Ken Raeburn <raeburn@mit.edu>
- Sabu Sheffeq <sst@india.hp.com>
- Donna Skibbie <donnas@us.ibm.com>
- Jonathan Trostle <john3725@world.std.com>

For More Information

- Donna Skibbie, donnas@us.ibm.com