

Heimdal

Love Hörnquist Åstrand
Stockholm University

Who are we

- Love Hörnquist Åstrand
- Johan Danielson
- Luke Howard
- Assar Westerlund
- Jacques Vidrine

10 years

- Heimdal turned 10 years this spring

Heimdal features

- PK-INIT support
- Great AFS integration
- Clean code-base that easy to modify
- Up to date documentation

Changes going into 0.8

- Many new regression tests on the Kerberos API
- Documentation of all Heimdals file formats: database dump file, keytab, etc
- Plenty of documentation updates

Changes going into 0.8

- Fixes reported from IBM Checker BEAM (Samba) and Coverity (NetBSD)
- Password expiration message
- Extended the database to support extensions

Changes going into 0.8

- New ASN.1 compile supporting CHOICE, SET OF, and SEQUENCE OF. Supports, PK-INIT, LDAP, X.509, PKCS-12 and more
- Use MIT style ticket flags in file credential caches (reversed bit order)
- Always compile in Kerberos 4 support into the KDC, default disabled

Changes going into 0.8

- Make the KDC log more verbose information about all requests.
- Regression suite for KDC and dumping/loading the database.

Changes going into 0.8

- Merged HDB back end changes from Samba 4
- Split the KDC into two parts, the front end talking the the network and libkdc.
- Add support to list iterate over credential caches (klist -l)

Changes going into 0.8

- PK-INIT support
- Tested with Microsoft Vista beta
- New X.509 code-base
- Supports PKCS-11, PKCS-12, PEM, and raw DER files

Changes going into 0.8

- Self contained crypto
- no more libidos, its now called libhcrypto
- no longer contains any Eric Young code
- include bigness, RSA, and DH (but slow)

Before 0.8

- GSS-API mechanism glue
- GSS-API SPNEGO - RFC 4178
- Encryption type negotiation - RFC 4537

Past 0.8

- ssh client and ssh server
- Better pre-authentication mechanism
- Better SASL and GSS-API support

Related software

- HTTP Negotiate support for
 - ruby client
 - python client
 - apache commons http patch
 - JBOSS/tomcat value
 - tomcat filter
 - apache 1.3 SPENGO module

Related software

- software pkcs-11 module