# Heimdal

AFS & Kerberos Best Practices Workshop 2007

Love Hörnquist Åstrand
Stockholm University

# Heimdal features

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

# Heimdal 0.8

- PK-INIT support
- HDB extensions support, used by PK-INIT
- New ASN.1 compiler
- GSS-API mechglue from FreeBSD
- Updated SPNEGO to support RFC4178
- Support for Cryptosystem Negotiation Extension (RFC 4537)

# Heimdal 0.8 cont

- A new X.509 library (hx509) and related crypto functions.
- A new ntlm library (heimntlm) and related crypto functions.
- Updated the built-in crypto library with bignum support using
- imath, support for RSA and DH and renamed it to libhcrypto.

# Heimdal 0.8 cont

- Subsystem in the KDC, digest, that will perform the digest
- operation in the KDC, currently supports: CHAP, MS-CHAP-V2, SASL
- DIGEST-MD5 NTLMv1 and NTLMv2.

# Heimdal 0.8 cont

- KDC will return the "response too big" error to force TCP retries for large UDP replies, common for PK-INIT requests
- Libkafs defaults to use 2b tokens
- Default to use the API cache on Mac OS X

# Heimdal 0.8 cont

- kca service, CA in KDC
- krb5_kuserok() also checks ~/.k5login.d directory for acl files
- Many, many, other update to code and info manual and manual pages.
- Bug fixes

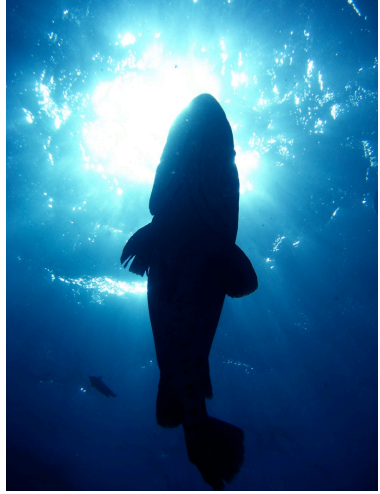
# Samba integration

- ETYPE-NEG
- NTLM support
- Windows referrals support
- Merged a rather long diff for 1.5 years
- PAC support, both in KDC and server
- GSS-API DCE-STYLE messages
- Updated SPNEGO, RFC 4178

# Past 0.8

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

# Future



- Complete referrals support, tgs-req missing
- SSPI support, EncryptMessage and friends
- Support different crypto back-ends (nss, evp)
- Test AES in Samba
- More integration with Samba4

# Related software

- Software PKCS-11 module