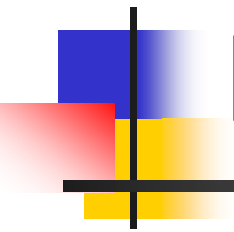
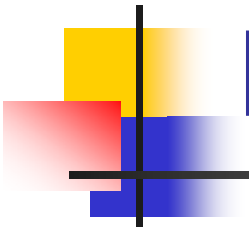


Kerberos and PKI Cooperation

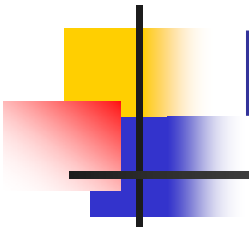
Daniel Kouřil, Luděk Matyska, Michal Procházka
Masaryk University

AFS & Kerberos Best Practices Workshop 2006



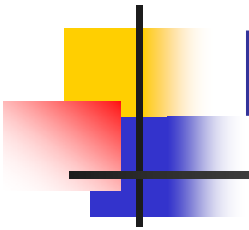
METACentre Project

- Czech nation-wide Grid activity
- Infrastructure for distributed and high performance computing
- Major computing centres in the country
- Security architecture based on Kerberos
  - (Co)-Authored a few Kerberos solutions (SSH, Web authN)
- Partner of international Grid projects (EGEE2)



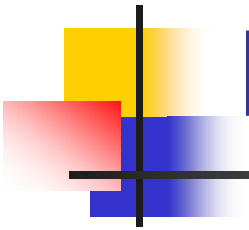
PKI Overview

- Asymmetric cryptography
- Each user has a key-pair consisting of a public and private key
- Private key kept secred, public key spread among other users
- Digital signatures
  - Private key used to generate digital signatures
  - Public key used to verify the signature
- Similarly encryption



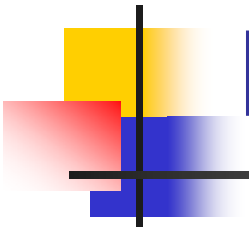
PKI - CAs

- How to get a correct public key?
- Independent identity providers – Certification authorities
- Digital certificates (X.509)
  - Public key, key owner identity, validity, other auxiliary information
  - signed by the CA key
- Only the CA key is distributed across the comunity
- Certificate revocation
- Building a trusted CA is a political and organizational problem not a technical issue



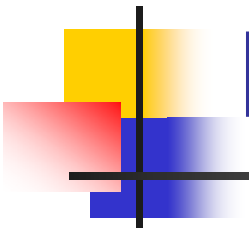
Kerberos vs. PKI

- Symmetric vs. asymmetric cryptography
  - Performace
- Tickets vs. Certificates
  - Similar concept
  - Issued by identity providers
- Online KDC vs. offline CA
  - Think of revocations (OCSP)
- Password vs. Private key
  - Long-term private keys must be stored on disk, are maintaned by the user
  - In real-word deployment many weakness in key management
- Revocation mechanism
  - Not needed for Kerberos, can be source of troubles for PKI
- Scalability
  - KDC must register every user
- Long-term digital signatures
  - Email signing, encrypting is very common using PKI
  - Message level security



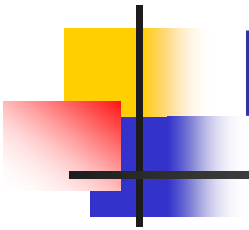
Kerberos and PKI

- Combining PKI and Kerberos
  - PKI is requested by large Grid projects
  - We have never wanted to abandon Kerberos
- Credential conversions
  - PKI to Kerberos
  - Kerberos to PKI



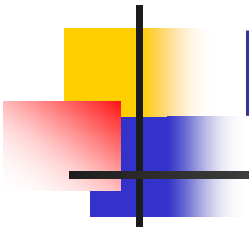
PK-INIT

- IETF specification (draft)
- Adding public key based authentication to the AS_REQ/AS_REP messages
  - Using pre-authentication mechanism
- PK-INIT only affects the initial authN step
  - rest of the protocol is untouched (and transparent for the end services).



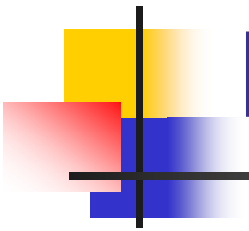
PK-INIT Protocol

- Client sends a public key (certificate) and signature
- KDC verifies the certificate (public key) and signature and check the request
  - Public key must be bound to the client principal
- The KDC reply isn't encrypted with a principal key from the DB but with a new symmetric key
  - The symmetric key is encrypted using the public key (or DH)
- The client verifies the reply, gets the key, decrypts the reply
- From this moment on the client proceeds as usual
  - TGT can be used to ask other tickets



PK-INIT Implementation

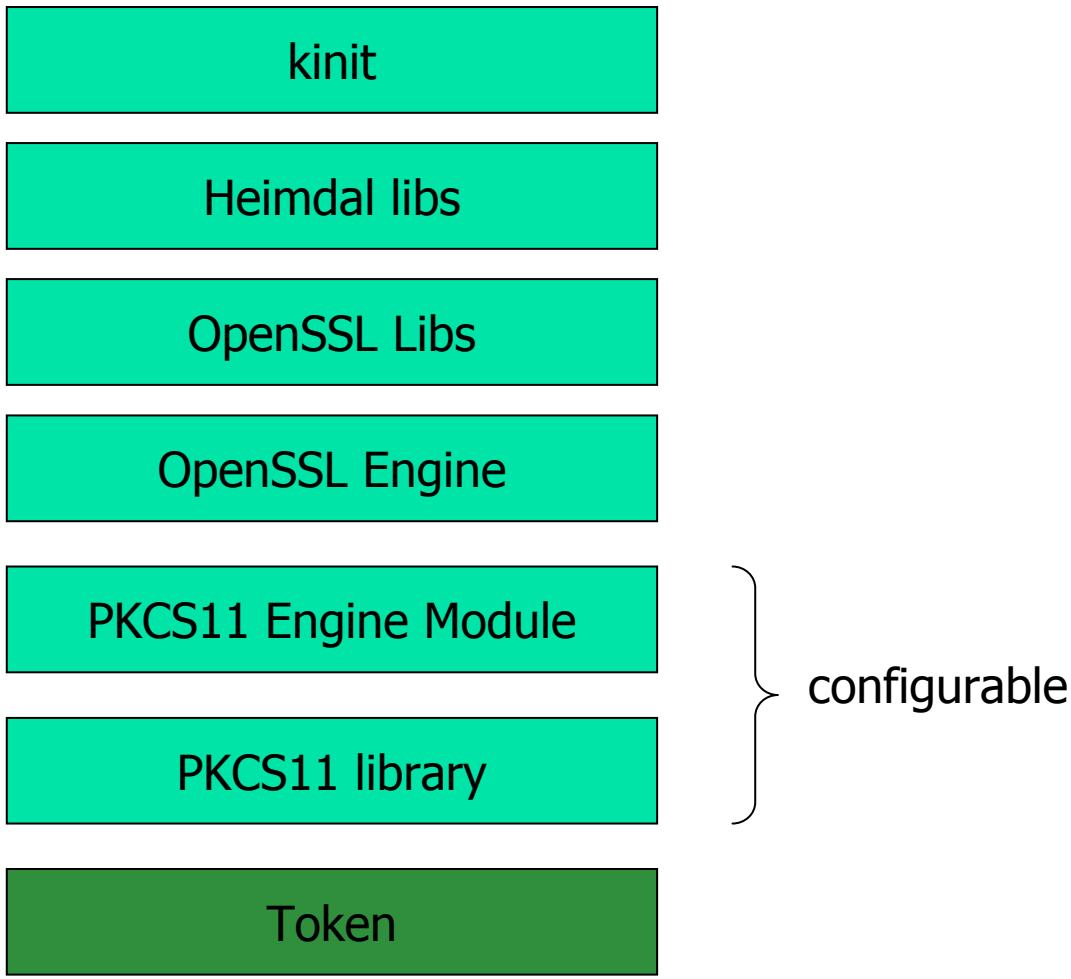
- We implemented a first version the PK-INIT specs for Heimdal
- Accepted by Heimdal
- In production use in METACentre
  - Support for Grid proxy certificates
  - Integration with the user management system

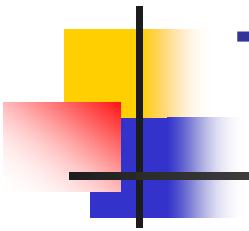


PK-INIT and Smart Cards

- OpenSSL Engine
  - Allows to use devices through #PKCS11
- OpenSC framework
- iKey3000 USB token
  - Combination of smart card and reader
  - Currently distributing among users
- Works both on Unix and Windows

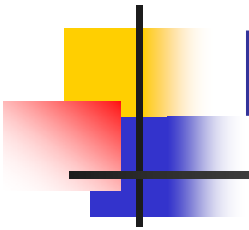
Smart Card Access





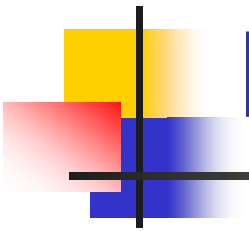
Travelkits

- Unix
  - Standard krb5 tools from the distribution
  - PK-INIT enabled kinit command and auxiliary files (CA certificates) - rpm, deb
- MS Windows
  - Standard Kerberos for Windows
  - PK-INIT enabled kinit command etc.
    - Part of Heimdal ported to Windows
  - Kerberos enabled Putty and WinSCP clients



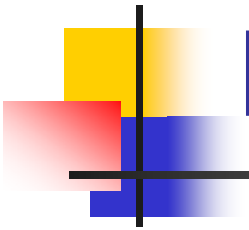
Kerberos to PKI

- Given a Kerberos ticket create a certificate and private key
- Easy access to the Grid, or other PKI based services (www)
- CA
  - Creating certificates for Kerberos tickets
  - Operating online
  - Short-time certificates
    - Private key can be unencrypted



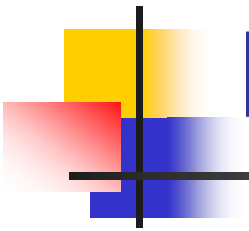
Kerberos CA

- kCA
  - Used in the Grid community (Fermilab)
  - kx509, kpkcs11
- MyProxy
  - Very common service in Grid world
  - On-line credential repository
  - Latest versions support also CA mode



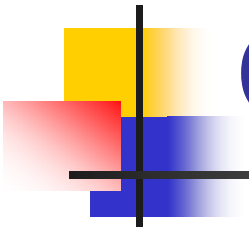
MyProxy

1. Client generates a new key-pair
2. Sends a CSR to the MyProxy server
   - Connection secured by Kerberos
3. MyProxy server returns a signed certificate
   - Using LDAP to map Kerberos principal to subject name
   - Lifetime is copied from the ticket
4. Client stores credential on disk
   - Generated private key and received certificate



PKI to Kerberos

- Credentials are stored in „Grid“ format
  - Can be used by standard grid commands
- Other applications must be configured
  - kpkcs11 library for PKCS11 aware apps
  - Using the Windows certificate repository
- Conversions can be run transparently
  - Login script on UI machines



Conclusions

- PKI and Kerberos can cooperate
- Multi-mechanim SSO possible