UMEÅ UNIVERSITET

Ladok
ENHETEN

Smart card authentication in the Ladok system

Mikael Berglund

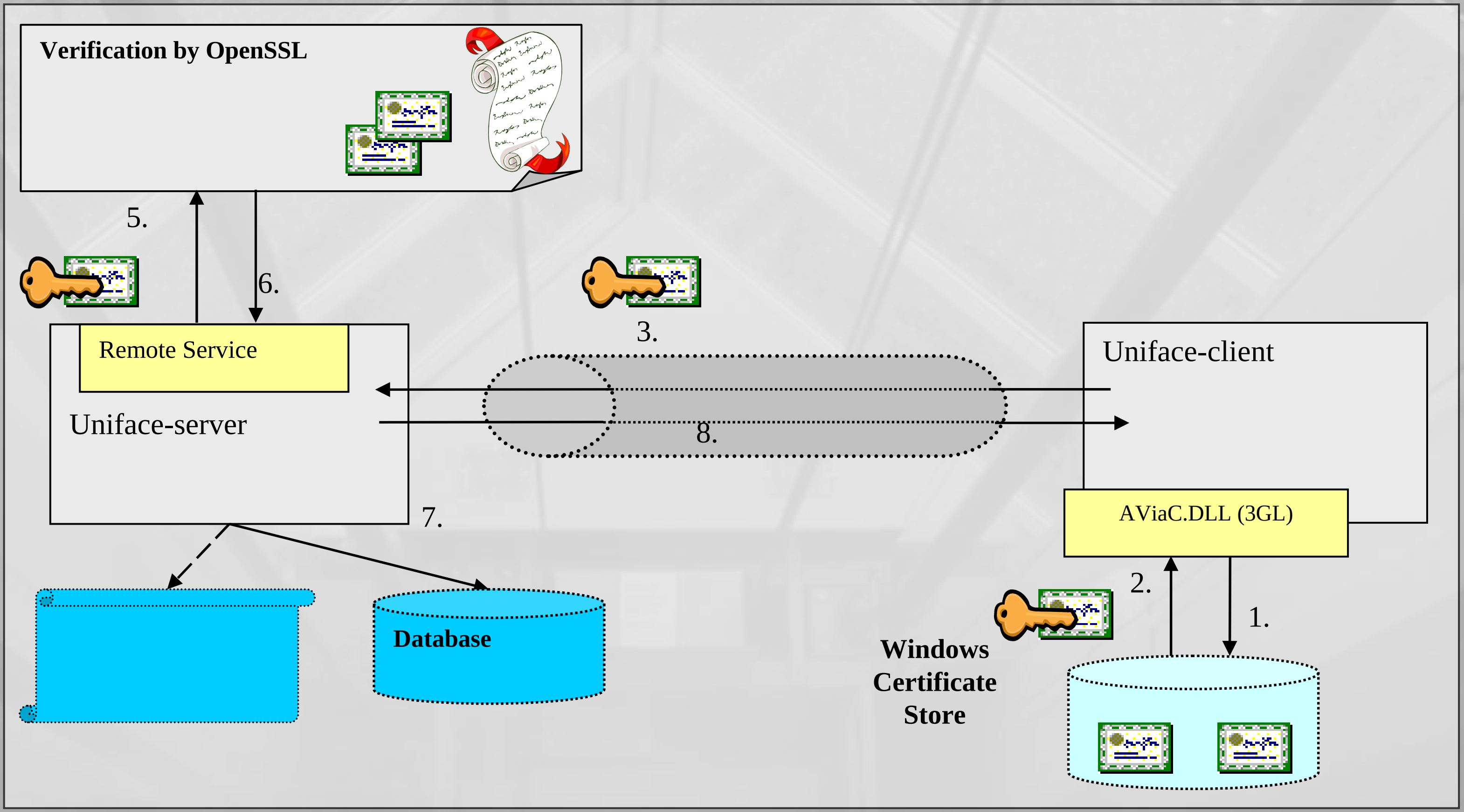
2006-10-09

The Ladok Division

- Student admission and documentation system for higher education in Sweden.
- Admission, student rectords, degrees and international studies.
- Ladok Nouveau – $ 100M
- Ladok on Web – SOAP Interface. 25+ services
- Ladok Ping – Distributed searches between all institutions
- NyA system – New Swedish Admission system

2006-10-09

Authentication in Nouveau by certificate



2006-10-09

Usage of server and client certificate

- The client certificate is retrieved from the Windows Certificate Store. The client certificate is used for signing and the server certificate is used for encryption
- Client certificate: used to sign a ticket
- Server certificate: used to encrypt the signed ticket
- Server then verifies that the signature is generated from the client certificate

2006-10-09

Certificates

- Soft certificate or smart card
- A CA could be used
- PKCS15 certificates used in prototype
- Certificates installed on client certificate store or on smart card

2006-10-09

Certificates ctd.

- Any type of certificate can be used, as long as OpenSSL and Windows Certificate Store can handle them
- Limitations in our trial:
  - PKCS12 required for smart card type
  - Only one private key can be used on each card

2006-10-09

Stunnel

- SSL/TLS tunnel
- No change in existing application

2006-10-09

Remote Service

- Used to make calls on the server side from the client
- Security checks done here together with CRL lookup
- Database connection

2006-10-09

OpenSSL

- Verification of certificate
- Handling of Certificate Revocation List
- Used as CA in our tests
- Validation of signed tickets

2006-10-09

UMEÅ UNIVERSITET
Ladok
ENHETEN

Advantages

- No local administration of users, can be centralized
- Can handle both soft and hard certificates
- Encrypted communication
- Single Sign-On possible
- Open standards – Stunnel, OpenSSL, S/MIME and CryptoAPI (Windows Server SDK)

2006-10-09

Disadvatages

- Soft certificates are locked to the client computer
- Only one private key per smart card
- Extra software required on the client – OpenSSL and smart card application

2006-10-09

Further work

- Real implementation
- Online CA

2006-10-09