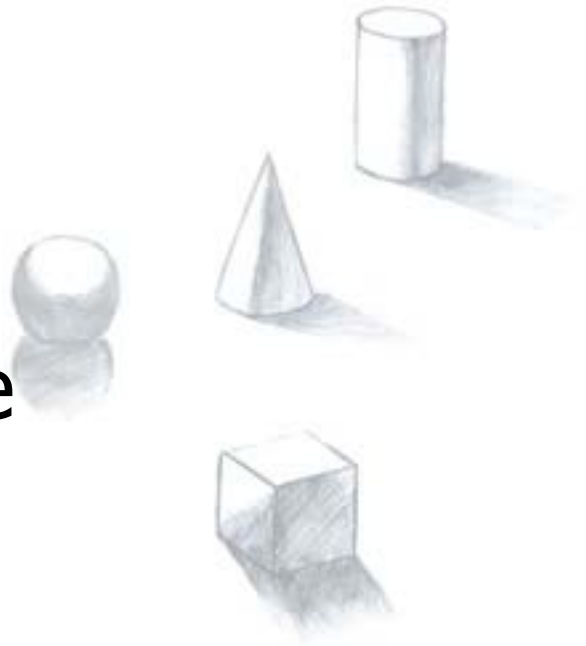
Database authentication and authorisation in LCG

Kuba Zajączkowski

Kuba.Zajaczkowski@cern.ch

Presentation Outline

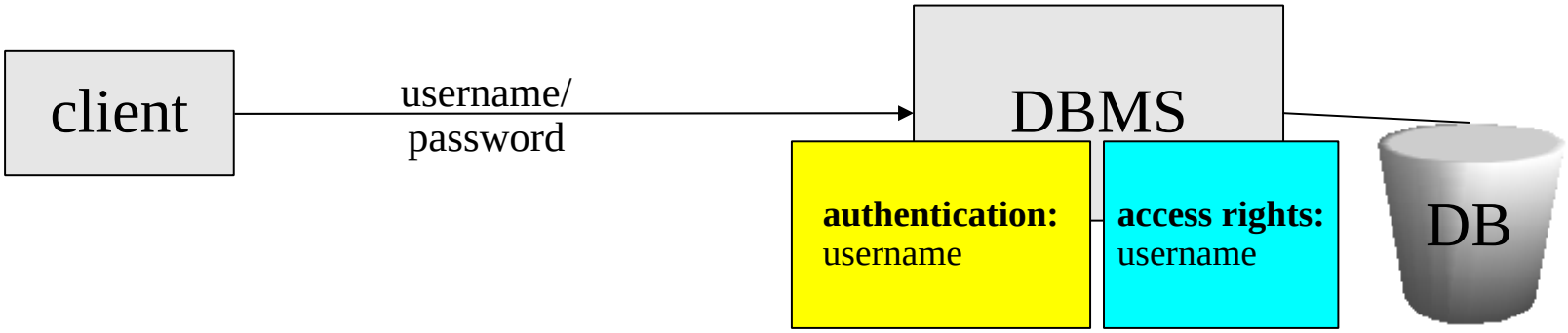
- Introduction
- Grid authentication mechanisms
- Oracle authentication mechanisms
- Current Status
- ANL-PIOCON Project
- Authentication with middleware
- Summary



Authorisation and Authentication

- LCG uses different authentication mechanisms (proxy certificates) than usual means implemented in RDBMS (user password pair, PKI certificates, etc.)
- LCG supplies it's own access control mechanism based on idea of virtual organisations (Virtual Organization Membership Service – VOMS)
- Traditional means of authorization will become either unusable or will pose a major security risk in grid environment.
- A safe and secure solution is needed.

Traditional Database Access

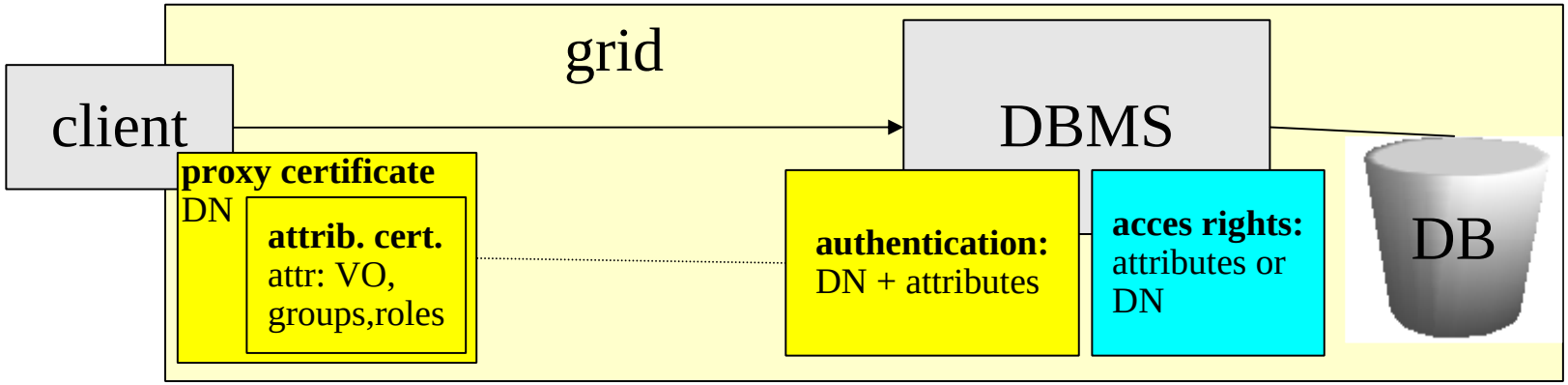


- client authenticates himself with username and password (or certificate)
- table or object access rights are granted to a username
  GRANT ... ON table TO 'joesmith'
- ***client has access to a table***
  SELECT ... FROM table WHERE ...

LCG Access Mechanisms

- identification is based on X.509 certificates, usually in connection with secure transport layer
- proxy certificates (RFC 3820) are used for regular operations
  example DN: C=CH/O=CERN/OU=LCG/CN=Jan Nowak/CN=proxy
- additional authorisation attributes are enclosed in attribute certificate (RFC 3281) connected to the proxy certificate
  VO (Virtual Organisation): /aliceCalibration
  role: /aliceCalibration/Role=Operator
- user identifier, DN and user privileges are granted and digitally signed by managing organisations of CA and VO

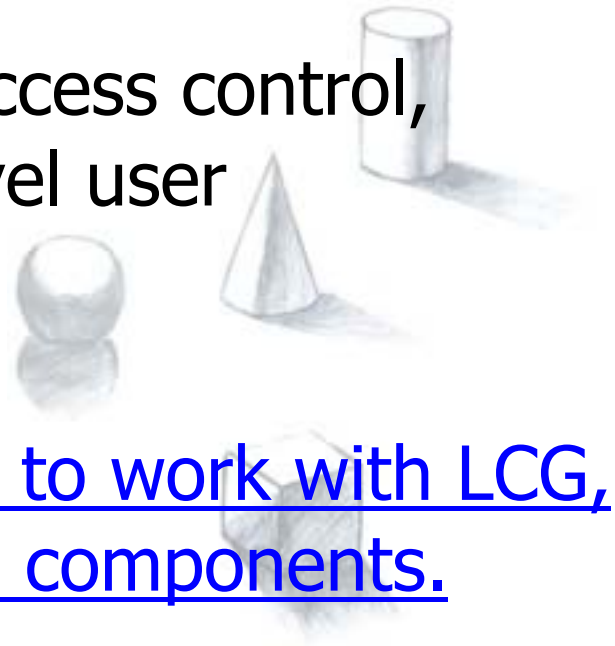
DB access with LCG authentication



- client authenticates himself with proxy certificate
- authentication: certificates validity, users DN and also VOMS signature (for attributes) are checked
- table or object access rights are granted based on DN or attributes.
  GRANT ... ON table TO 'C=CH/O=CERN/OU=LCG/CN=Jan Nowak'
  GRANT ... ON table TO 'VO=/aliceCalibration/Role=Operator'
- ***client has access to a table***
  SELECT ... FROM table WHERE ...

Authorisation Issues

- LCG Virtual Organisations and proxy certificates – fine grained access control system short term partial authorisation mechanism
- Oracle Enterprise User Security – certificate based user authentication, shared schemas, enterprise roles, user – schema and user – role mappings
- Open Source Databases – traditional access control, certificate authentication, no higher level user management, source code availability.



OpenSource databases can be adapted to work with LCG, Oracle requires the use of existing components.

Oracle Access Mechanisms

Authentication

- Username/password
- Radius
- Kerberos
- SSL (traditional, lack of official support for proxy certificates)
- proxy authentication(eg. through application server)

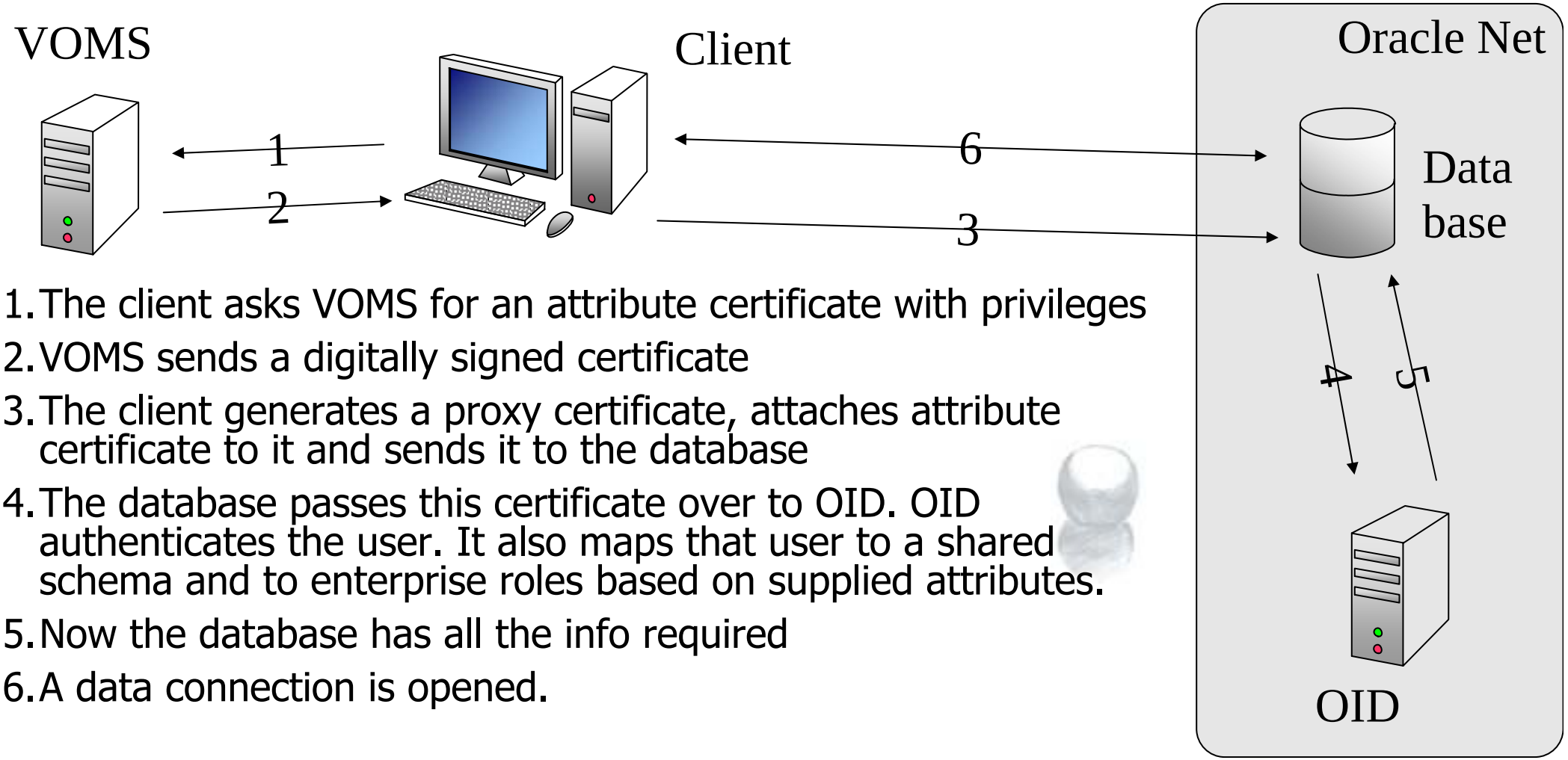
Authorisation

- Oracle Enterprise User Security
- Shared schema
- Enterprise roles
- Oracle Internet Directory + OracleContext
- has no support for attribute certificates

There is neither support for user management outside of Oracle Context nor there is support for proxy or attribute certificates.

Oracle + LCG authorisation

If Oracle will support proxy and attribute certificates



1. The client asks VOMS for an attribute certificate with privileges
2. VOMS sends a digitally signed certificate
3. The client generates a proxy certificate, attaches attribute certificate to it and sends it to the database
4. The database passes this certificate over to OID. OID authenticates the user. It also maps that user to a shared schema and to enterprise roles based on supplied attributes.
5. Now the database has all the info required
6. A data connection is opened.

Current Progress

- We've set up a test environment – Oracle database using Oracle Enterprise User Security with SSL certificates, test Virtual Organisation and a test Certificate Authority plus an example worker node for generation of proxy certificates.
- We've run a number of connection test against it.
- While access using regular SSL certificates works fine, we can't get past the Oracle's SSL layer when using proxy certificates.
- We have filed a TAR at Oracle with enhancement request to support proxy certificates. We will follow up on that closely.

Possible Scenarios

- We could send user certificates (wallets) along with the jobs and use them for authorisation. This however is not acceptable because of LCG security means. It would mean a long lasting open access to someone who could intercept that wallet.
- If we could get past the SSL layer we could use an OID module to extract user's base DN from a proxy DN and use this for authentification.
- With no attribute support a simple tool would be needed to periodically synchronise and map VOMS roles and privileges to Oracle Context. The number of entries in the OID would be signifigant – one or more for each user.
- If Oracle would choose to support attribute certificates as well, all we need is a way for OID modules to access attribute data in the same manner as it can read the DN trom the certificate. Mapping of VOMS to Oracle privileges would be only a matter of writing a simple OID module and supplying that map.

Mid-term Proposal

For the next 6 months or until proxy certificate handling is resolved we propose:

- read-only accounts for Tier 1 and 2 protected with traditional passwords
- write accounts only at Tier 0

- compatible with 3D startup model
  – write @ T0, read @ T1/2
- has been discussed with CERN and LCG security
  – seems acceptable as a stop-gap

MySQL + Grid auth Project

High-performance Database Access Technologies for Computational Grids – a project by Argonne National Laboratory and Piocon Technologies

In our proof-of-concept prototype we implemented Globus grid proxy certificate authorization technologies for MySQL database access control. By localizing Globus security concerns in our software aspect we achieved a clean separation of Globus Grid Security Infrastructure libraries dependencies from the MySQL server code.

Alexander Vaniachine, ANL

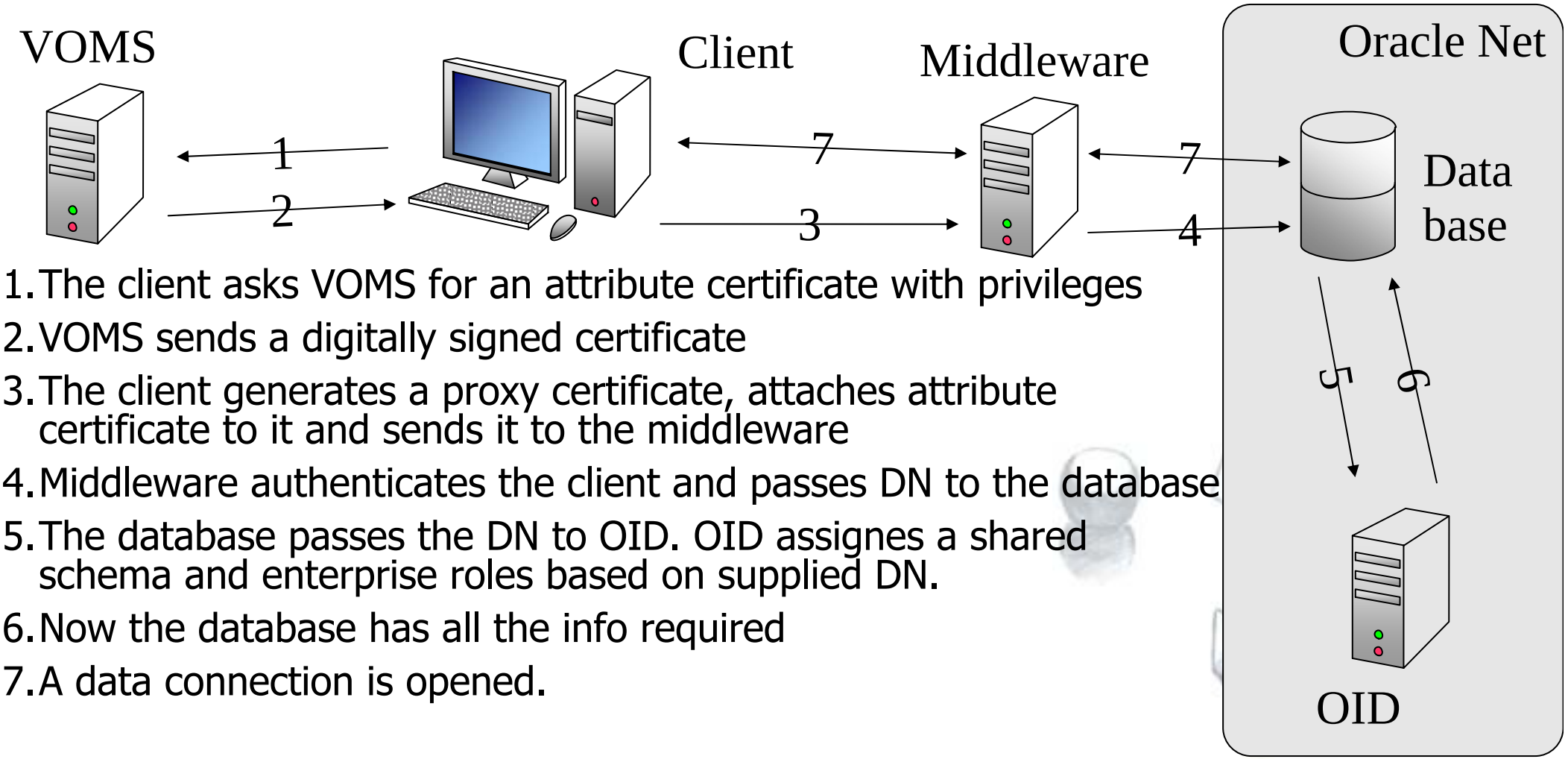
Current Status

- working prototype with Globus grid proxy certificate
- VOMS attribute certificate support planned in the future
- Open Science Grid is the main priority

You can find more info about this project at http://www.piocon.com/ANL_SBIR.php

Middleware authorisation

If middleware is required to interoperate



1. The client asks VOMS for an attribute certificate with privileges
2. VOMS sends a digitally signed certificate
3. The client generates a proxy certificate, attaches attribute certificate to it and sends it to the middleware
4. Middleware authenticates the client and passes DN to the database
5. The database passes the DN to OID. OID assignes a shared schema and enterprise roles based on supplied DN.
6. Now the database has all the info required
7. A data connection is opened.

Existing middleware projects

- OGSA-DAI: SOAP/XML + XML binary extensions
- Spitfire (EDG WP2): SOAP/XML text-only data transport
- Perl DBI database proxy (*ALICE*): SQL data transport

Why you might NOT want to use OGSA-DAI

- You want very fast data access
- OGSA-DAI is slower than direct connection methods e.g. JDBC
- But remember OGSA-DAI provides functionality "over and above" these methods – e.g. data delivery and transformation
- You need scalability
- Depends on your intended usade of e.g. delivery mechanisms, number of clients, etc.

Neil P Chue Hong, *OGSA-DAI Status Summary,* Third OGSA-DAI Users Group Meeting, 6/1/2005

Comparison

Without middleware

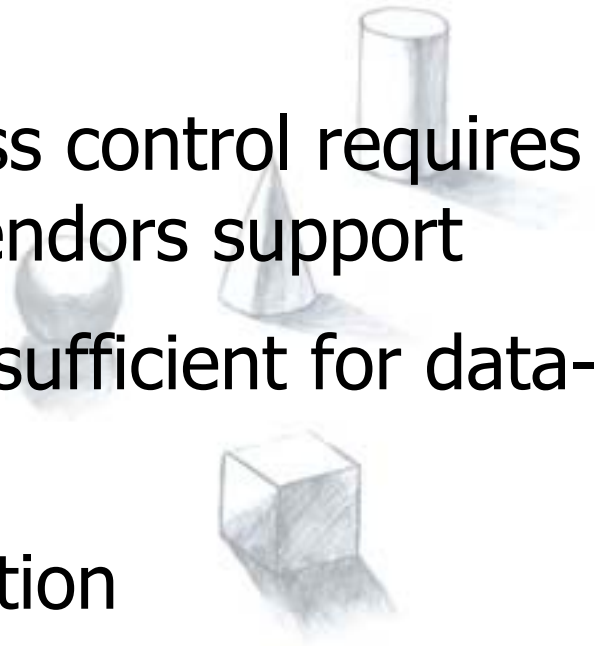
- No message-level security overhead
- Only minor changes required on the client side; normal use of database drivers (jdbc, odbc, oci, etc.)
- Vendor-specific advantages, eg. binary data transport, distributed XA transactions
- Without Oracle's support, proxy cetificate based security will remain theoretical, MySQL solution available
- Libraries available for most programming languages
- Still in developement

With middleware

- Additional overhead – possible bottleneck
- Major client-side changes nedded, existing solutions are not interchangable
- Limited support for vendor-specific capabilitities, some additional posibilites like data transformation
- Existing solutions claim to support a wide range of database engines.
- Limited support for client programming languages
- Still in developement

Summary

- Authentication and Authorisation is a major issue to be solved before production phase
- Direct access mechanisms only partially supported (MySQL), but with DB vendors help, means to utilise proxy certificates certainly exist
- Direct support for VOMS-based access control requires more developement and again DB vendors support
- Middleware solutions are probably insufficient for data-intensive access
- There is an acceptable stop-gap solution



Questions

Thank You!

In case of any questions feel free to contact me:

Kuba Zajączkowski
<Kuba.Zajaczkowski@cern.ch>