Policy-driven Negotiation for Authorization in the Grid

Ionut Constandache — Duke University

Daniel Olmedilla — L3S Research Center

Frank SiebenList — Argonne National Laboratory

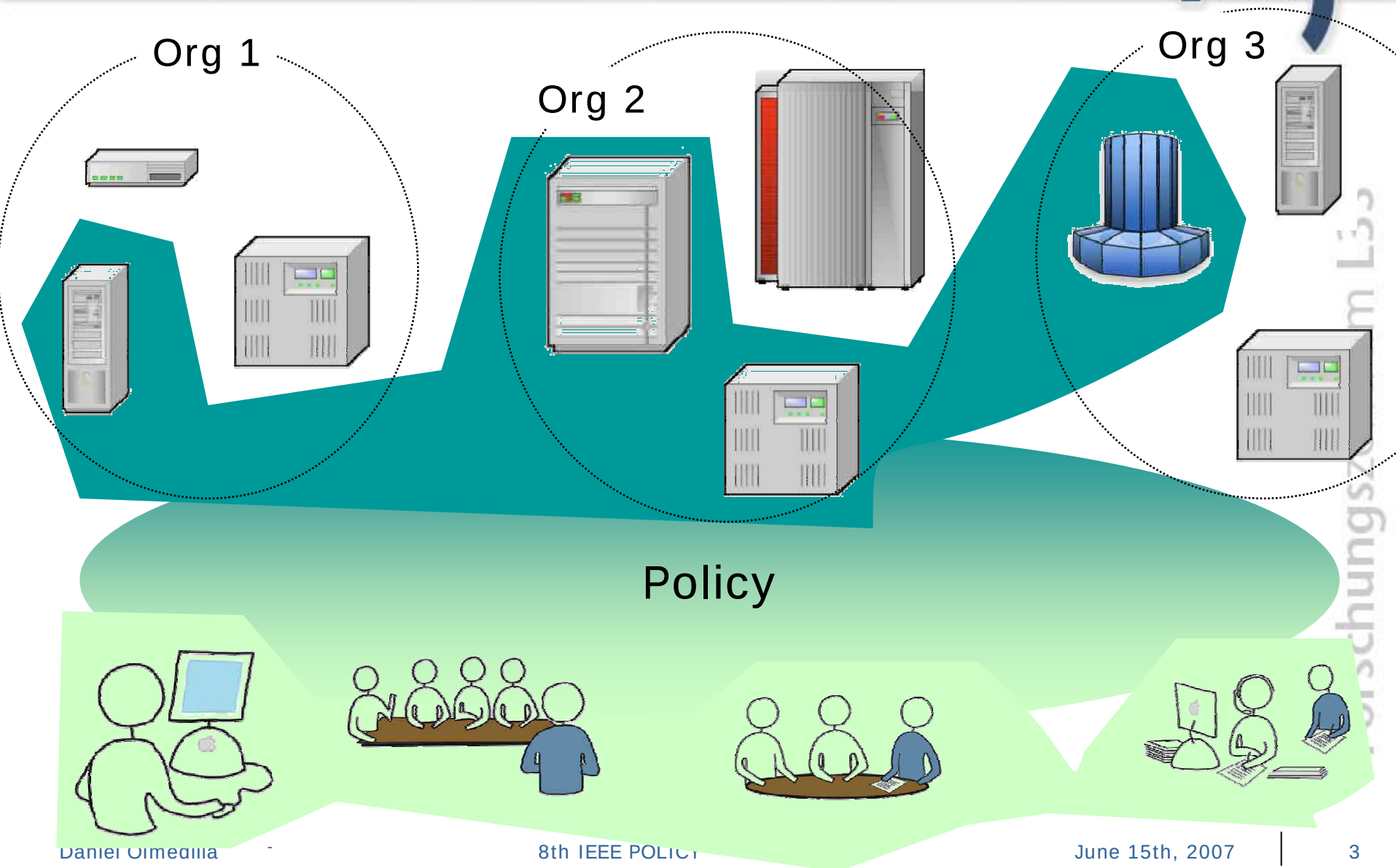
8th IEEE POLICY
Bologna, Italy, 15th June 2007

Outline

- Introduction
- Motivation
- Policy-driven Negotiations
- Negotiations in the Grid
- Implementation
- Conclusions and Further Work

Forschungszentrum L3S

Introduction
Virtual Organization



Introduction
Why Grid Security is Hard?

Resources being used may be valuable & the problems being solved sensitive

- Both users and resources need to be careful

Dynamic formation and management of virtual organizations (VOs)

- Large, dynamic, unpredictable...

VO Resources and users are often located in distinct administrative domains

- Can't assume cross-organizational trust agreements
- Different mechanisms & credentials

Interactions are not just client/server, but service-to-service on behalf of the user

- Requires delegation of rights by user to service
- Services may be dynamically instantiated

Motivation
Local Administrative Domain

Ivan's policy:
Alice is my friend and I'll share my lemonade with her
Mallory is not my friend and he can go #$%^&

Alice

Can I have glass of lemonade?

Sure, here is a glass

Ivan

Resource Owner decides!
(ultimate source of authority for access)

Mallory

No way, I don't

Motivation
Distinct Administrative Domains

Ivan's policy:
Carol is my friend and I'll share my lemonade with her
I'll share my lemonade with any friend of Carol
I don't know any Bob...(?)

Bob

Can I have glass of lemonade?

?

Ivan

Motivation
Distinct Administrative Domains – Pull (I)

Ivan's policy:
Carol is my friend and I'll share my lemonade with her
I'll share my lemonade with any friend of Carol
I don't know any Bob…(?)

Bob

Can I have glass of lemonade?

Sure, here is a glass

Ivan

Can Bob have glass of lemonade?

Sure, Bob is my friend

Carol

Carol's policy:
Bob is my friend and I'll share my lemonade with him

Motivation

Distinct Administrative Domains: Full (& II)

Neighbor's policy:
Let's party!

Aunt's policy:
Sharing is good

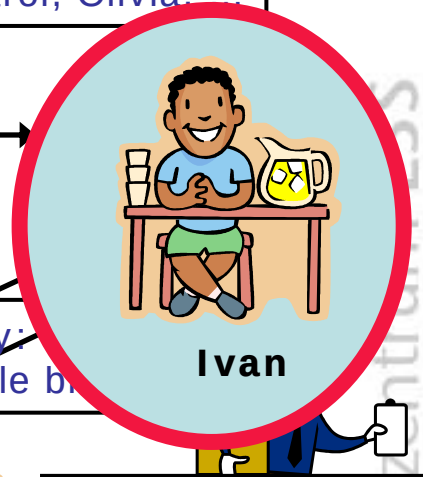
Frosty's policy:
Only share lemonade with ice

Bill's policy:
Lemonade is bad for you

Ivan's poli
I don't know any Bob...(?)
I do know John, Mary, Carol, Olivia...

Laura's policy:
Share if he pays!

s of lemon



Ivan

Bob

Jogger's policy:
I'd like

Ca

Mary's policy:
I like Bob a little bi

Ivan: HELP

John's policy:
I don't like girls

Olivia's policy:
If Carol likes Bob, I hate him!

Accountant's policy:
Only if he signs here

ure, Bob is my fri

Emma's policy:
Only on his birthday

Ann's policy:
I like Ivan very much!

Carol

Lucy's policy:
I sometimes like Carol

rol's policy:
'll share my lemona

David's policy:
Ask Laura

Motivation
Distinct Administrative Domains – Push approach

Ivan's policy:
Carol is my friend and I'll share my lemonade with her
I'll share my lemonade with any friend of Carol
I don't know any Bob...(?)

Bob

Can I have glass of lemonade?

And BTW, Carol is my friend

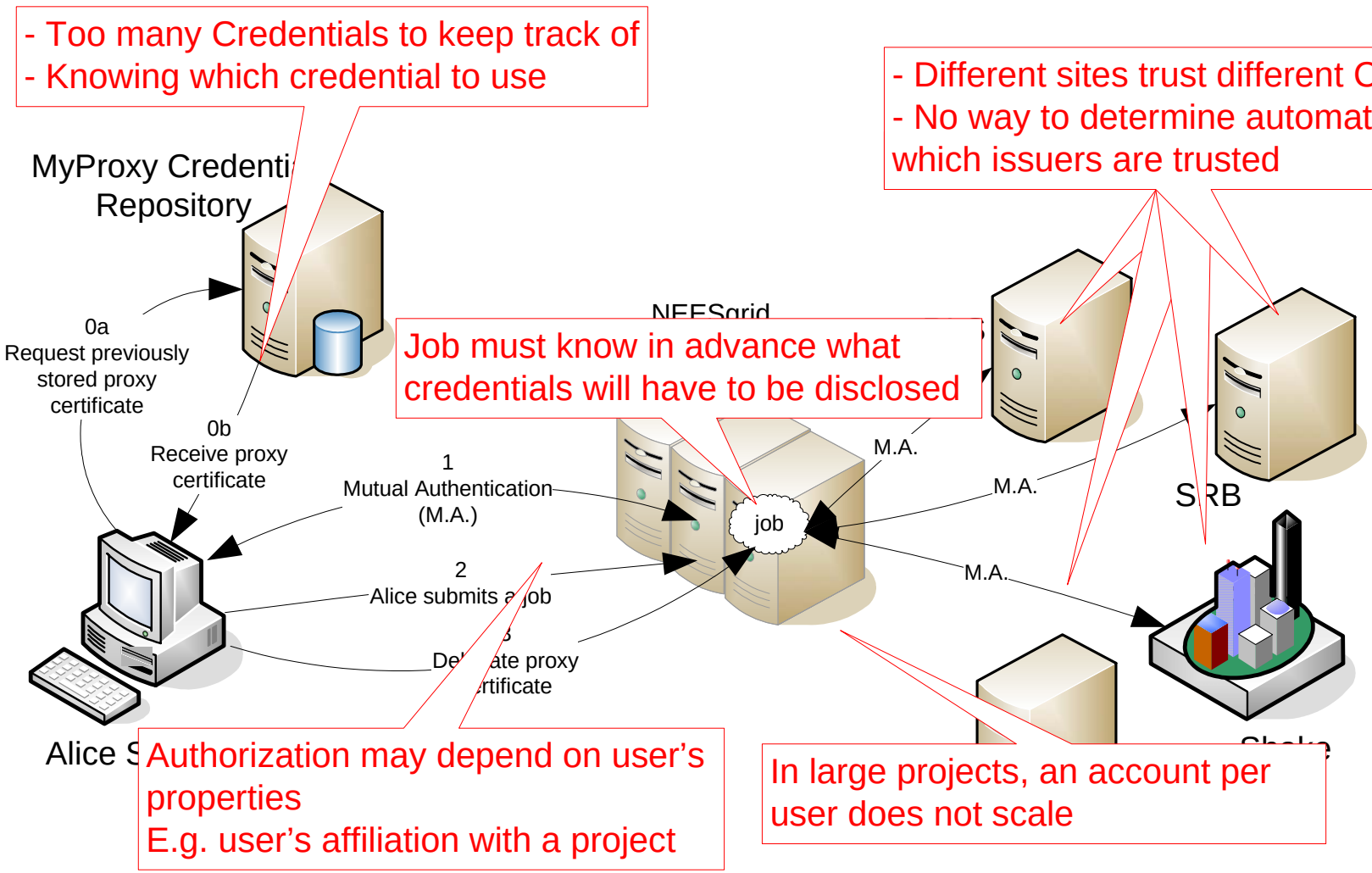
Sure, here is a glass

Ivan

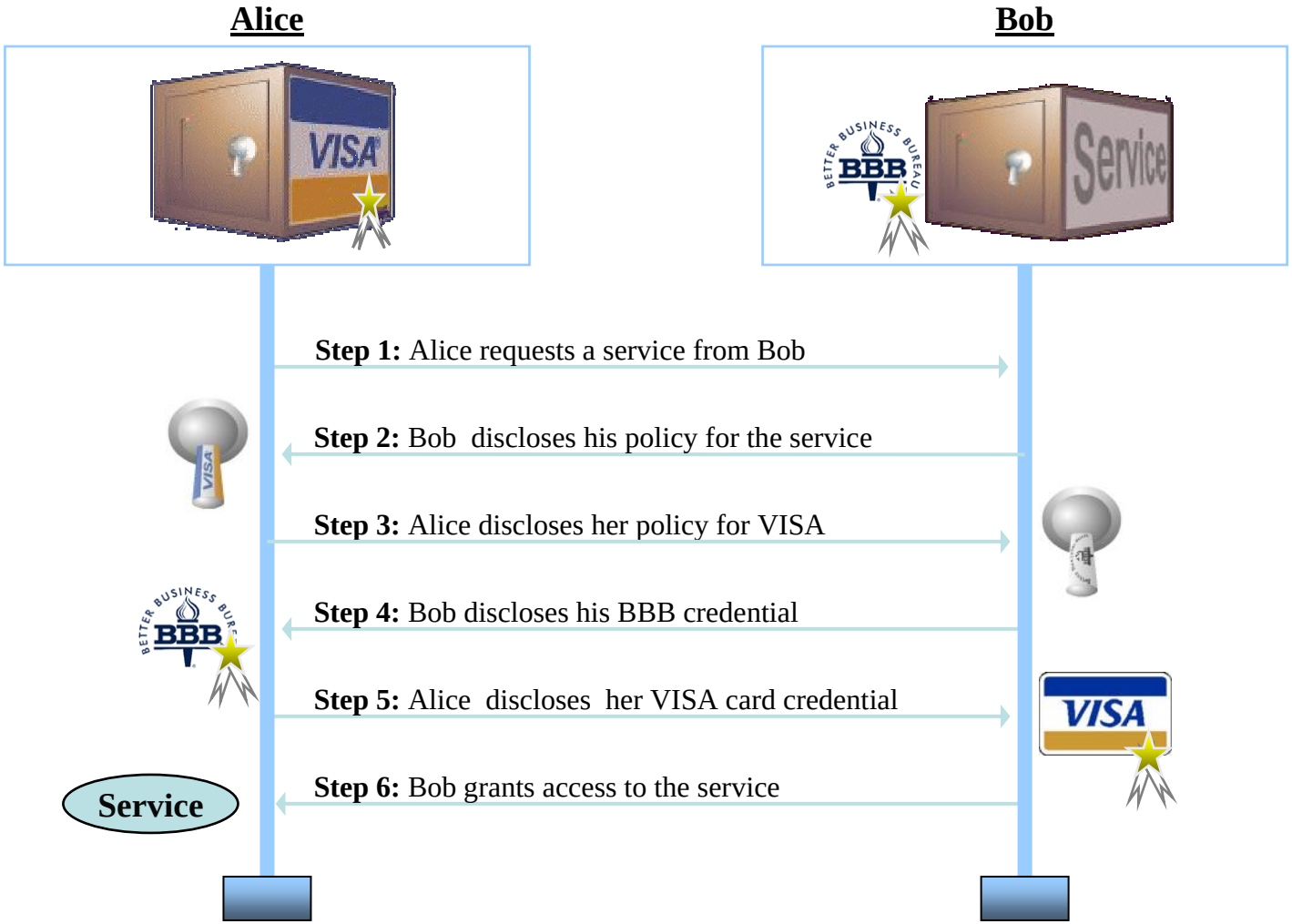
- either Bob provides a list of all his friends or
  - Privacy problems, superfluous disclosure
- Bob knows in advance the friends from Ivan
  - static
  - service instances to be used may be selected at run-time

Motivation

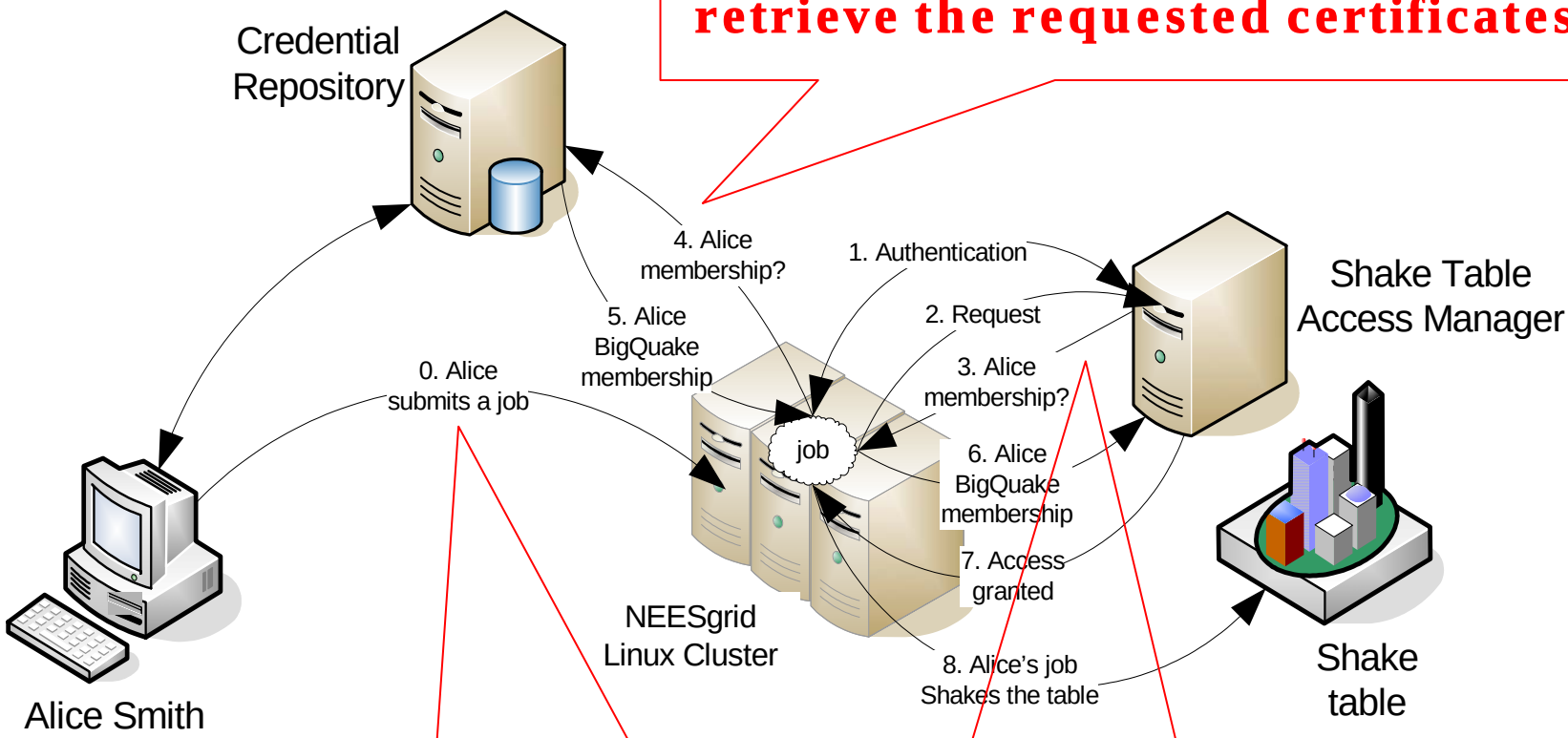
Example Scenario – Grid Limitations



Policy-Driven Negotiations
Example: Security & Privacy



Negotiations in the Grid
Revisiting the example scenario



Policy-Driven Negotiations
Characteristics

Both client and servers are semantically annotated with policies

Annotations

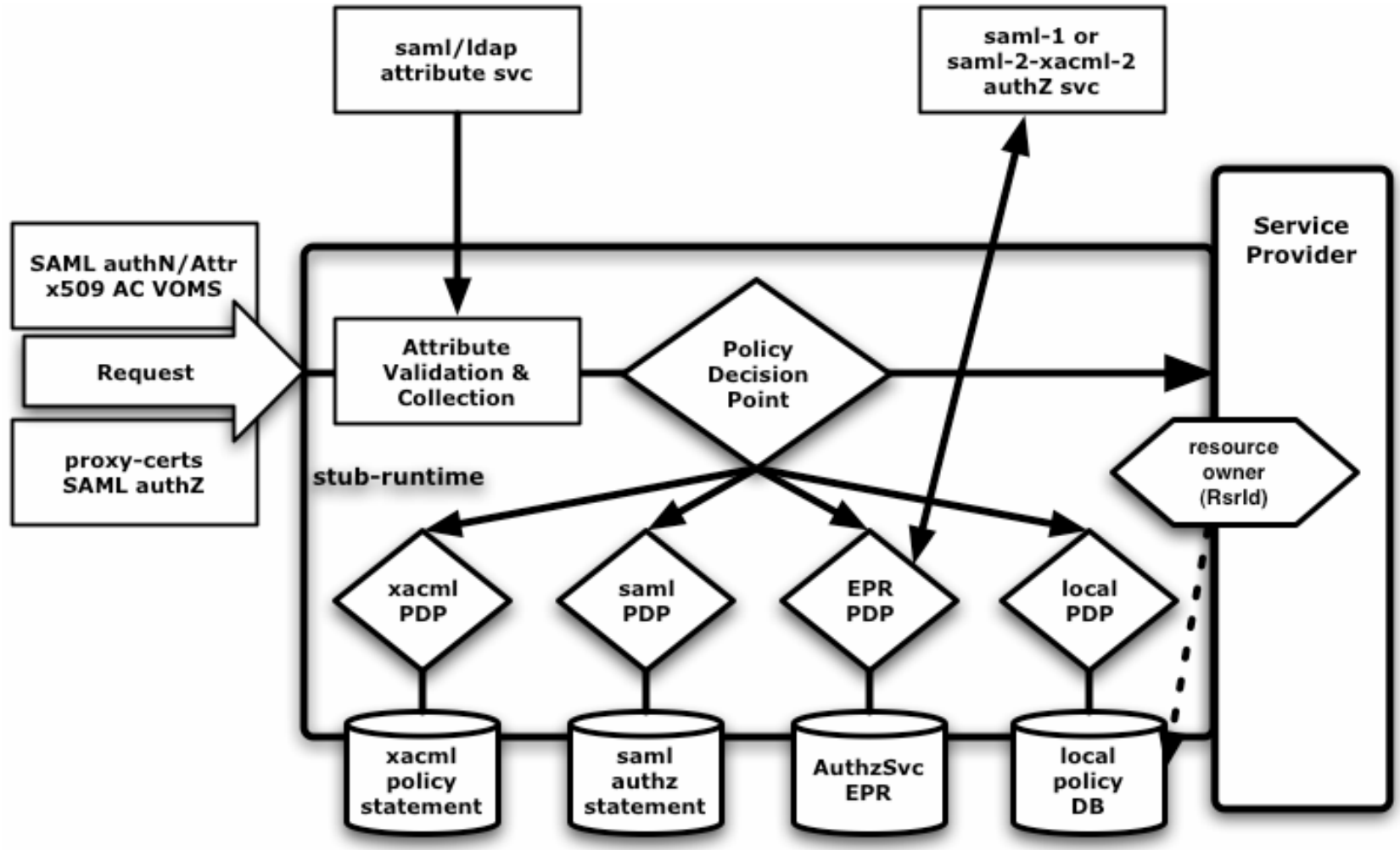
- specify constraints and capabilities – access control requirements
  - which certificates must be presented to gain access to it
  - who is responsible for obtaining and presenting these certificates
- are used during a negotiation
  - to reason about and to communicate the requirements
  - to determine whether credentials can be obtained and revealed.

User involvement is drastically reduced – automated interactions

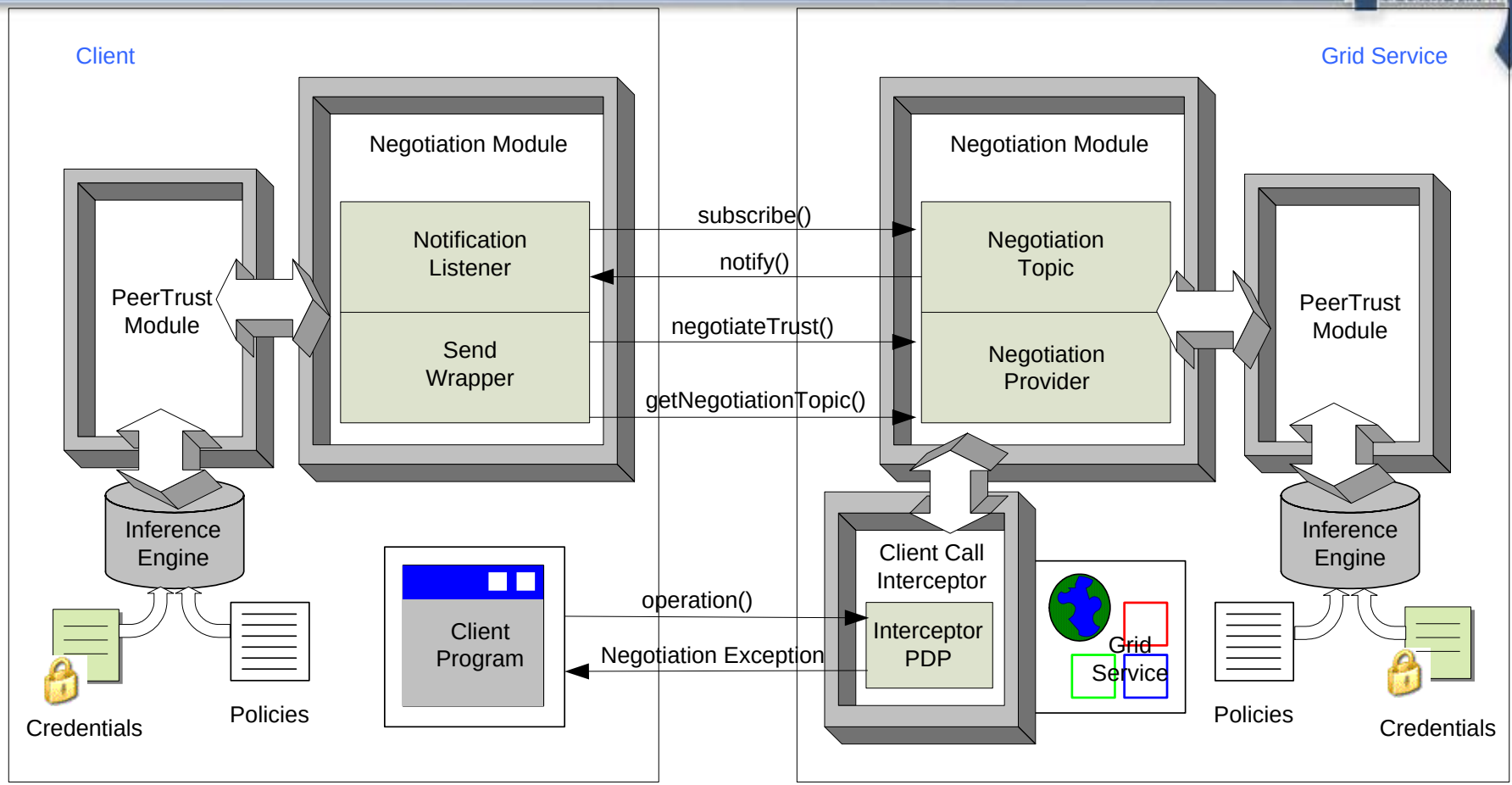
If required, for sensitive resources, negotiation can be longer

- To obtain (access to) a certificate, I must satisfy its access control policy, which specifies ... --and so on, recursively—

Implementation
Current GT4's new authZ framework



Implementation
Architecture



Service wsdl file

<wsdl:import namespace="http://linux.egov.pub.ro/ionut/TrustNegotiationwsdl" location="TrustNegotiationwsdl"/>

Service Deployment Descriptor

<parameter name="providers" value="SubscribeProvider GetCurrentMessageProvider g4mfs.impl.gridpeertrust.net.server.TrustNegotiationProvider"/>

<parameter name="securityDescriptor" value="share/schema/gt4ide/MathService/mysec.xml"/>

Forschungszentrum L3S

Implementation
Integration on Globus Toolkit 4.0

- Directed integrated with the grid services paradigm
- Extension to GSI pluggable to any GT4.0 compliant grid service or client
- Only requirement: Java based grid services

- We use:
  - Custom PDP as part of the Client Call Interceptor
    - Redirects to a negotiation if required
  - Asynchronous negotiations are achieved through WS-Base Notification and WS-Topics

- CAS integration into negotiations
- API for easy integration within client code

Forschungszentrum L3S

Conclusions & Future Work
Conclusions

Main Features

- **Self-describing resources for access requirements**
  - **Based on properties**
- **Negotiation for service authorization**
- **Dynamic credential fetching**
  - Now possible to use discovery and scheduling services to locate the best available resources
  - Otherwise, impossible to predict before hand what exact service instances would be used and which certificates required
- **Monitoring and explanation of authorization decision**

Implementation in Java

- **Extension of GSI in GT4.0**
- **Backwards compatible**

Conclusions & Future Work
Further Work

- **Study performance impact of negotiations**
- **And approaches to minimize the extra load**
  - **Limit number of iterations**
    - **E.g. 2 steps negotiations**
  - **Advertise policies before the service is invoked**
- **Investigate the use of XACML**
  - **Delegation not yet supported but planned**

Forschungszentrum L3S

Thanks!

Questions?

olmedilla@L3S.de - http://www.L3S.de/~olmedilla/

Forschungszentrum L3S