the globus alliance
www.globus.org

Globus Toolkit: Authorization Processing

GlobusWORLD 2005

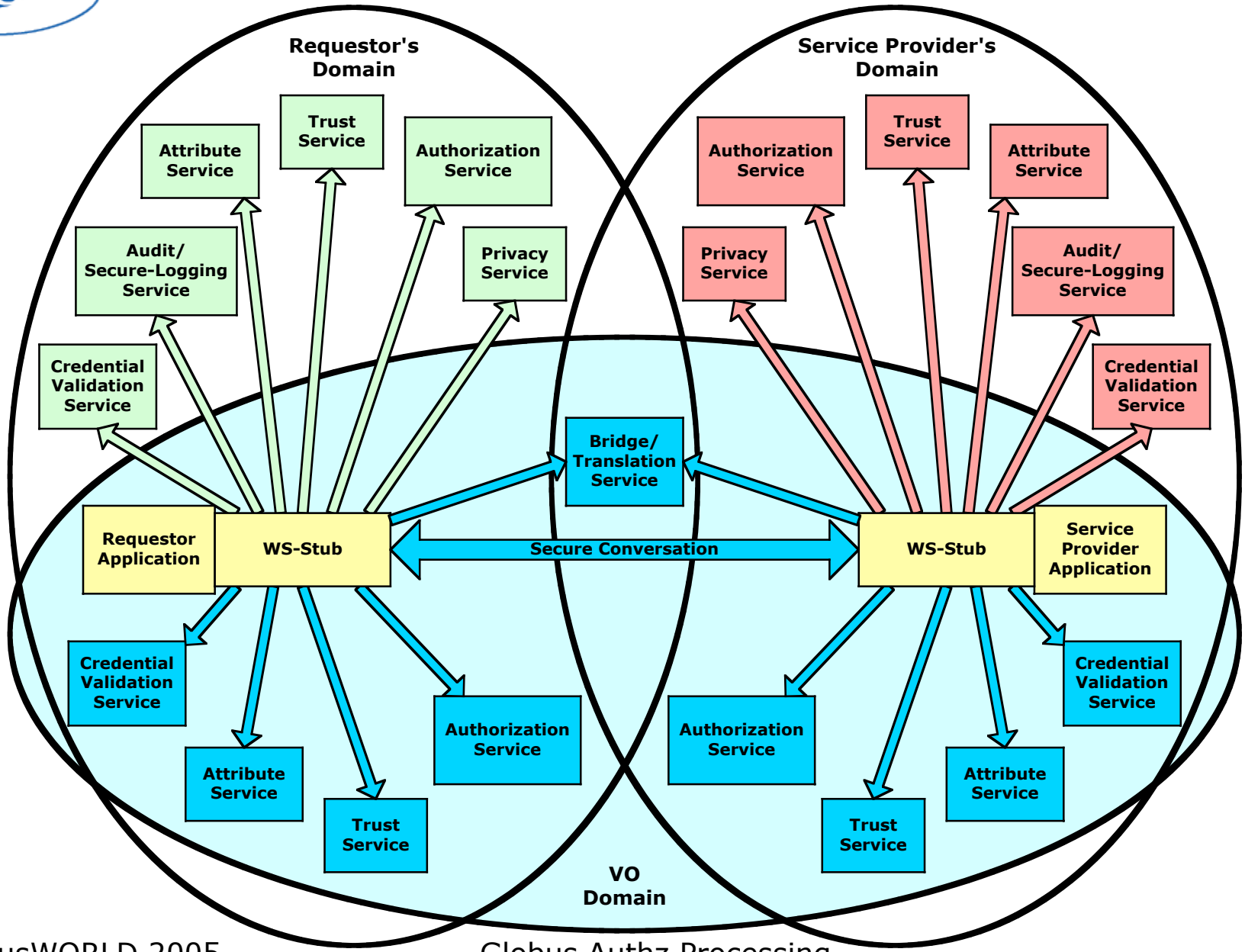
Feb 7-11, Boston, MA

Frank Siebenlist - ANL (franks@mcs.anl.gov)

Takuya Mori - NEC (mori@mcs.anl.gov)

http://www.globus.org/

OGSA Security Services



GT's GGF's Authorization Call-Out Support

- GGF's OGSA-Authz WG:
  "Use of SAML for OGSA Authorization"
  - Authorization service specification
  - Extends SAML spec for use in WS-Grid
  - Recently standardized by GGF
- Conformant call-out integrated in GT
  - Transparently called through configuration
- Permis interoperability
  - XACML coming…
- Futures…
  - SAML2.0 compliance … XACML2.0-SAML2.0 profile

GT-XACML Integration

- eXtensible Access Control Markup Language (XACML)
  - OASIS standard
  - Open source implementations
- XACML: sophisticated policy language
- Globus Toolkit will ship with XACML runtime
  - Integrated in every client and server build on GT
  - Working on integration details right now…
- GW05: "Access Control for the Grid"
  - Anne Anderson (Sun - OASIS/XACML TC)
  - Takuya Mori (NEC - visiting researcher at ANL)
  - Tue Feb 8, 10:30am, Session 1b, Back Bay A
- Demo: GT-XACML Integration plus Delegation of Rights
  - Takuya Mori in CyberCafe - Tue Feb 8, 2:30pm

GT's Assertion Processing "Problem"

- VOMS/Permis/X509/Shibboleth/SAML/Kerberos identity/attribute assertions
- XACML/SAML/CAS/XCAP/Permis/ProxyCert/SPKI authorization assertions
- Assertions can be pushed by client, pulled from service, or locally available
- Policy decision engines can be local and/or remote
- Delegation of Rights is required "feature" implemented through many different means

GT-runtime has to mix and match all policy information and decisions in a consistent manner…

"Authorization Policy Federation"

GT's Authorization Processing Model

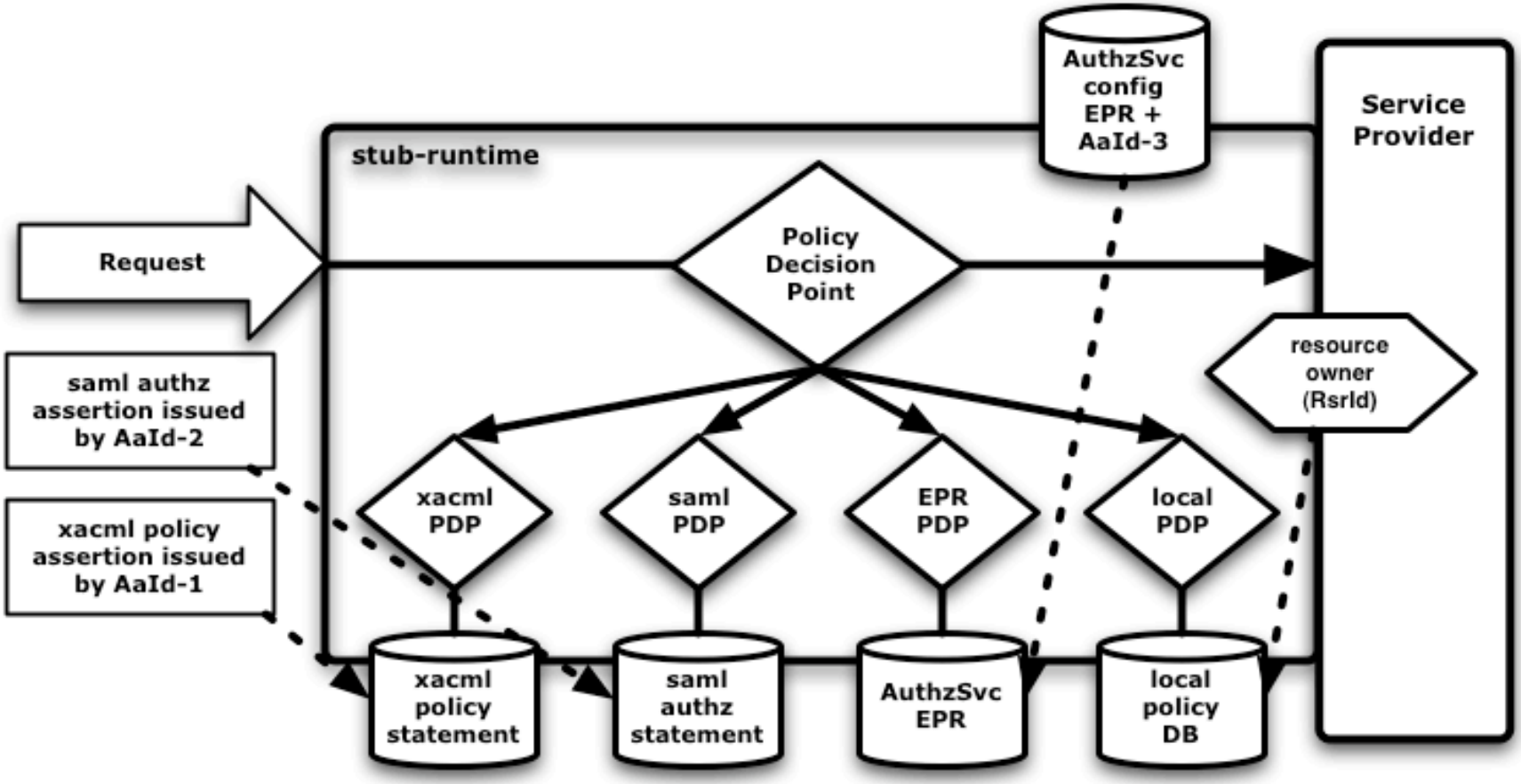
- Use of a Policy Decision Point (PDP) abstraction that conceptually resembles the one defined for XACML.
  - Normalized request context and decision format
  - Modeled PDP as black box authorization decision oracle
- After validation, map all attribute assertions to XACML Request Context Attribute format
- Create mechanism-specific PDP instances for each authorization assertion and call-out service
- The end result is a set of PDP instances where the different mechanisms are abstracted behind the common PDP interface.

GT's Authorization Processing Model (2)

- The Master-PDP orchestrates the querying of each applicable PDP instance for authorization decisions.
- Pre-defined combination rules determine how the different results from the PDP instances are to be combined to yield a single decision.
- The Master-PDP is to find delegation decision chains by asking the individual PDP instances whether the issuer has delegated administrative rights to other subjects.
- the Master-PDP can determine authorization decisions based on delegated rights without explicit support from the native policy language evaluators.

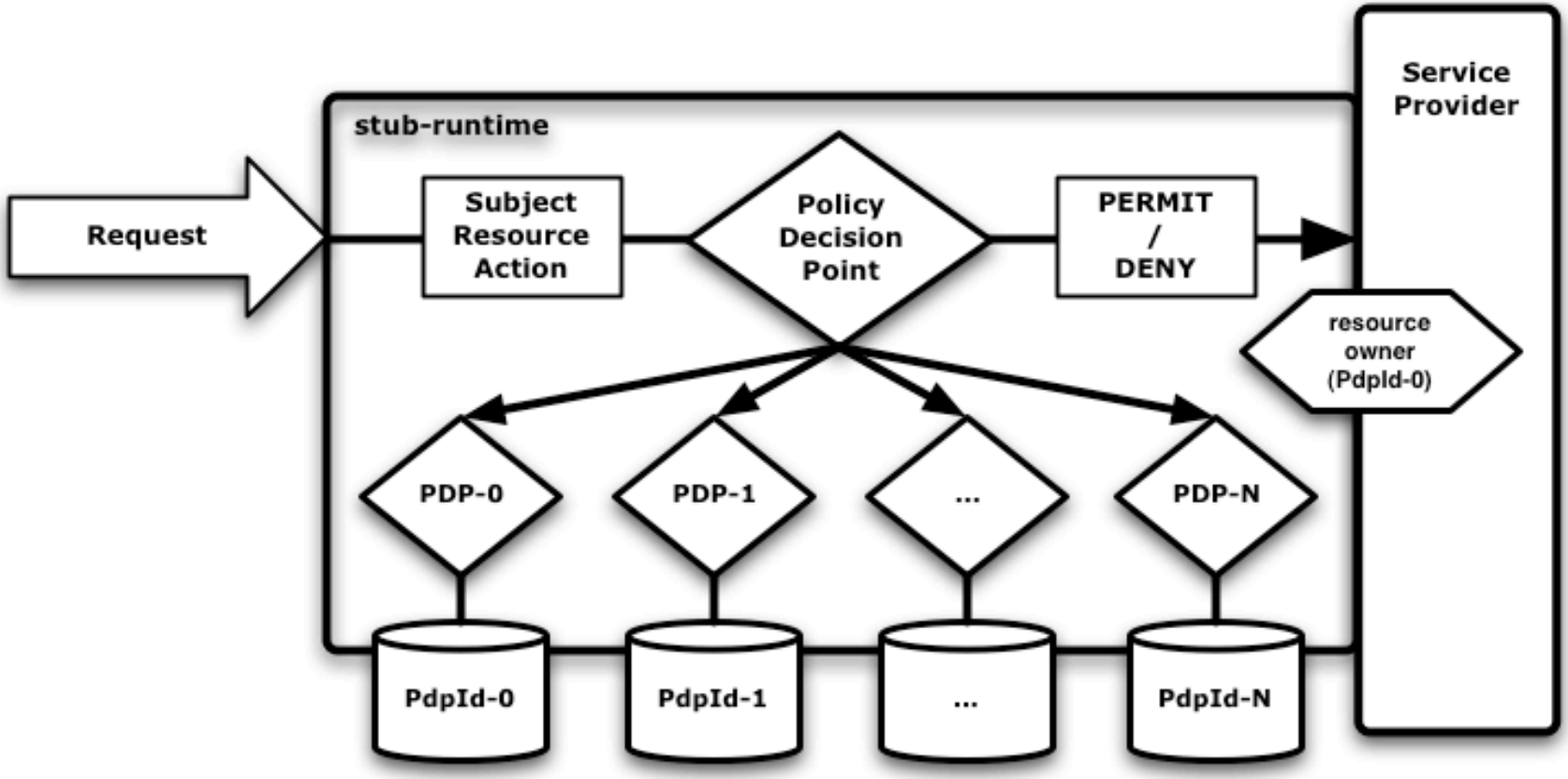
the globus alliance
www.globus.org

GT Authorization Framework (1)



the globus alliance
www.globus.org

GT Authorization Framework (2)

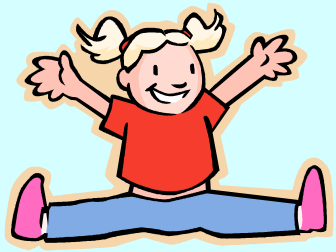


GT Authorization Framework (3)

- Work in progress
  - Not part of GT4.0
  - Planned for GT4.*…
- Note that we “have” to solve this problem… (as in “we have no choice…”)

Globus-XACML Demo (1)

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



Alice

Can I have glass of lemonade?

Sure, here is a glass

Ivan

Can I have glass of lemonade?

No way, I don't like you

Mallory

Globus-XACML Demo (2)

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

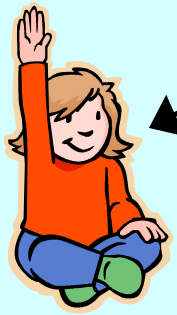
Can I have glass of lemonade?

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

Globus-XACML Demo (3)

Ivan's PermitPolicy: Subject.vo-role == "administrator"
Ivan's Attribute Assertion: Carol.vo-role = "administrator"
Ivan has no policy applicable to Bob => NotApplicable

Bob

Ivan's local XACML PDP

Request to invoke porttype/operation on ws-resource

Application Reply

Ivan

Can Bob's request context invoke porttype/operation on my ws-resource?

Carol's SAML Authz Svc EPR = Ext-PDP

Permit

Carol

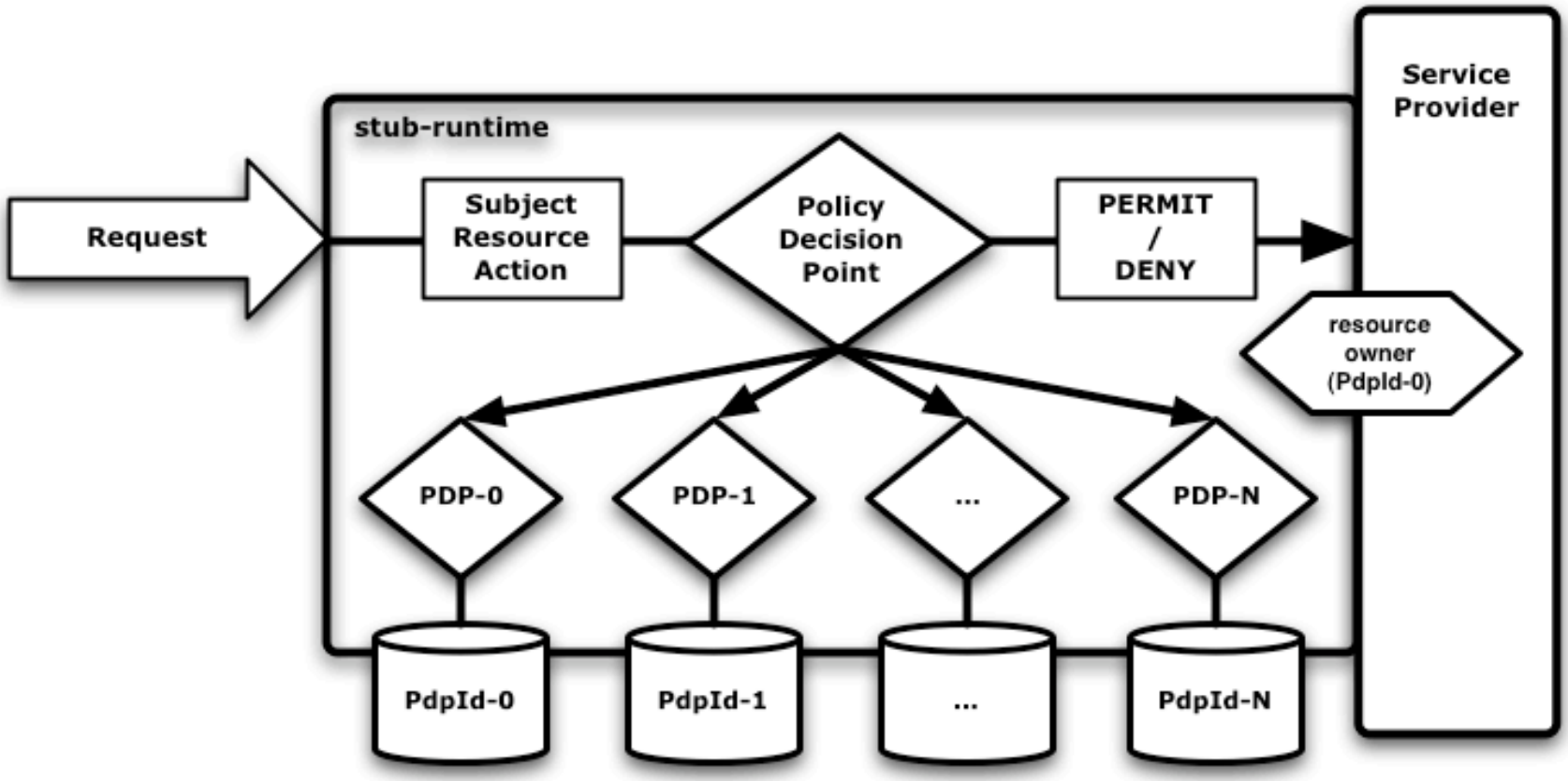
Ivan delegates the rights to administrate access to Carol

Carol's PermitPolicy:
Subject.name == "Bob"

Demo Configured Policies

- Ivan's Local XACML policies
  1. if name=="Alice" then Permit
  2. if subject.vo-role == "user" then Permit
  3. if subject.vo-role == "administrator" then Permit
- Ivan's Locally stored attribute assertions:
  1. Dave.vo-role = "user"
  2. Carol.vo-role = "administrator"
- Carol's External ACL-rules
  1. Bob - permit

GT Authorization Framework (2)



the globus alliance
www.globus.org

Demo

- Normal "real" demo disclaimers…
  - Raw, last code changes 5 min before presentation, may crash, don't try at home, not for minors, keep doors unlocked, … show kindness and forgiveness…
- 2nd chance:
  - Demo: GT-XACML Integration plus Delegation of Rights
  - Takuya Mori in CyberCafe - Tue Feb 8, 2:30pm
  - More time to ask questions and discuss implementation issues