Aktuelle Entwicklungen zu GridShib

Ralf Gröper und Christian Grimm, RRZN
Reimer Karlsen-Masur, DFN

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

2. D-Grid Security Workshop
27. März 2007

Agenda

Das IVOM-Projekt

Übersicht GridShib: Komponenten und Aufbau

Aktuelle GridShib Versionen: Was geht schon und was kommt noch

SLCs und SLCS mit GridShib☐

Offene Fragen

IVOM: Eckdaten

IVOM

- Interoperabilität und Integration der VO-Management Technologien im D-Grid

Laufzeit

- 1. Oktober 2006 – 31. März 2008 (18 Monate)

Partner

- Alfred Wegener Institut
- DAASI International GmbH
- DFN-Verein (assoziiert)
- FhG SCAI
- Forschungszentrum Jülich (assoziiert)
- LRZ München
- RRZN und Forschungszentrum L3S
- SUN Microsystems GmbH (assoziiert)
- Universität Göttingen (assoziiert)

Grundsätzliche Ausrichtung

- Hauptarbeiten beziehen sich auf Einsatzmöglichkeiten von Shibboleth im D-Grid

Motivation: zunehmende Nutzung des „klassischen“ Shibboleth

- Verschiedene vorrangig Web-basierte Anwendungsbereiche
- Bibliotheken, Zugang zu Campus-Netzen und -Diensten, eLearning
  - andere Beispiele s. DFN-AAI
- Start einer Shibboleth-basierten DFN-AAI Anfang 2007

Das IVOM-Projekt

Ziele: Verbesserung des VO-Managements durch Shibboleth-Technologien

- Einführung von Shibboleth-basiertem VO-Management
- Konzeption einer D-Grid-weit gültigen Autorisierung auf Grid-Ressourcen
- Umfassende Nutzung von Attributen unabhängig von Grid Middleware
  - Attribute werden – wie die Informationen zur Authentifizierung – dezentral verwaltet
  - Implementierung bisher mit GridShib für Globus Toolkit 4 verfügbar

Einbindung von Globus, gLite und UNICORE

- Globus Toolkit: GridShib und VOMS-PDP werden z. Z. entwickelt
- gLite: Anbindung an Shibboleth-Attribute wird in IVOM realisiert
- UNICORE: Integration von VOMS- und Shibboleth-Attributen wird in IVOM realisiert

Interoperabilität mit den VO-Management Technologien der D-Grid Communities

Grundlagen GridShib

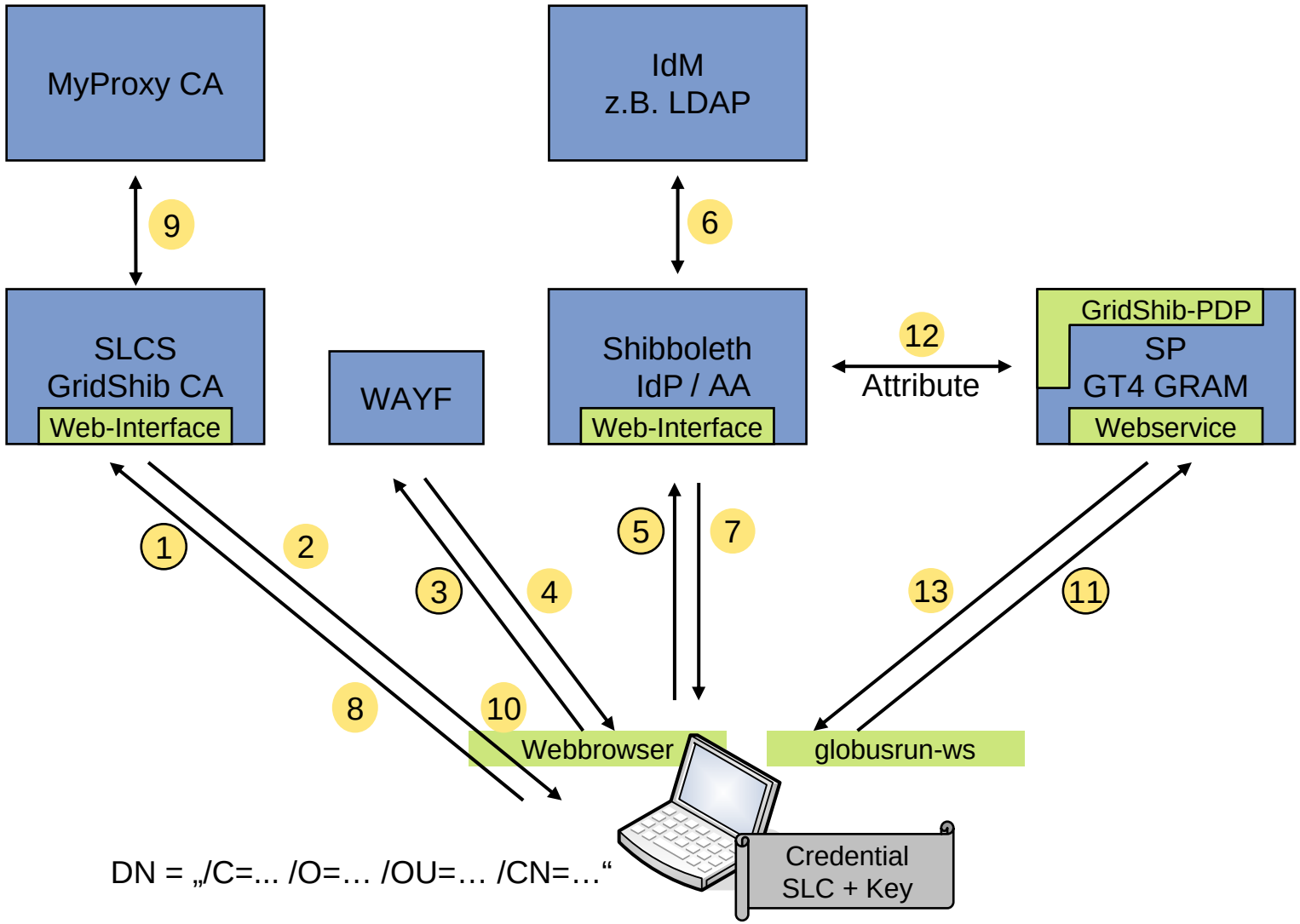
Ziele von GridShib im Globus Toolkit 4:

- GT4 + Shibboleth-Mechanismen = GridShib
- Föderierter Ansatz zum Identitätsmanagement
- Weitestgehende Beibehaltung der X.509-Proxy-Zertifikatsbasierten GSI
- Bereitstellung von IdP-verwalteten Attributen auf Grid Ressourcen

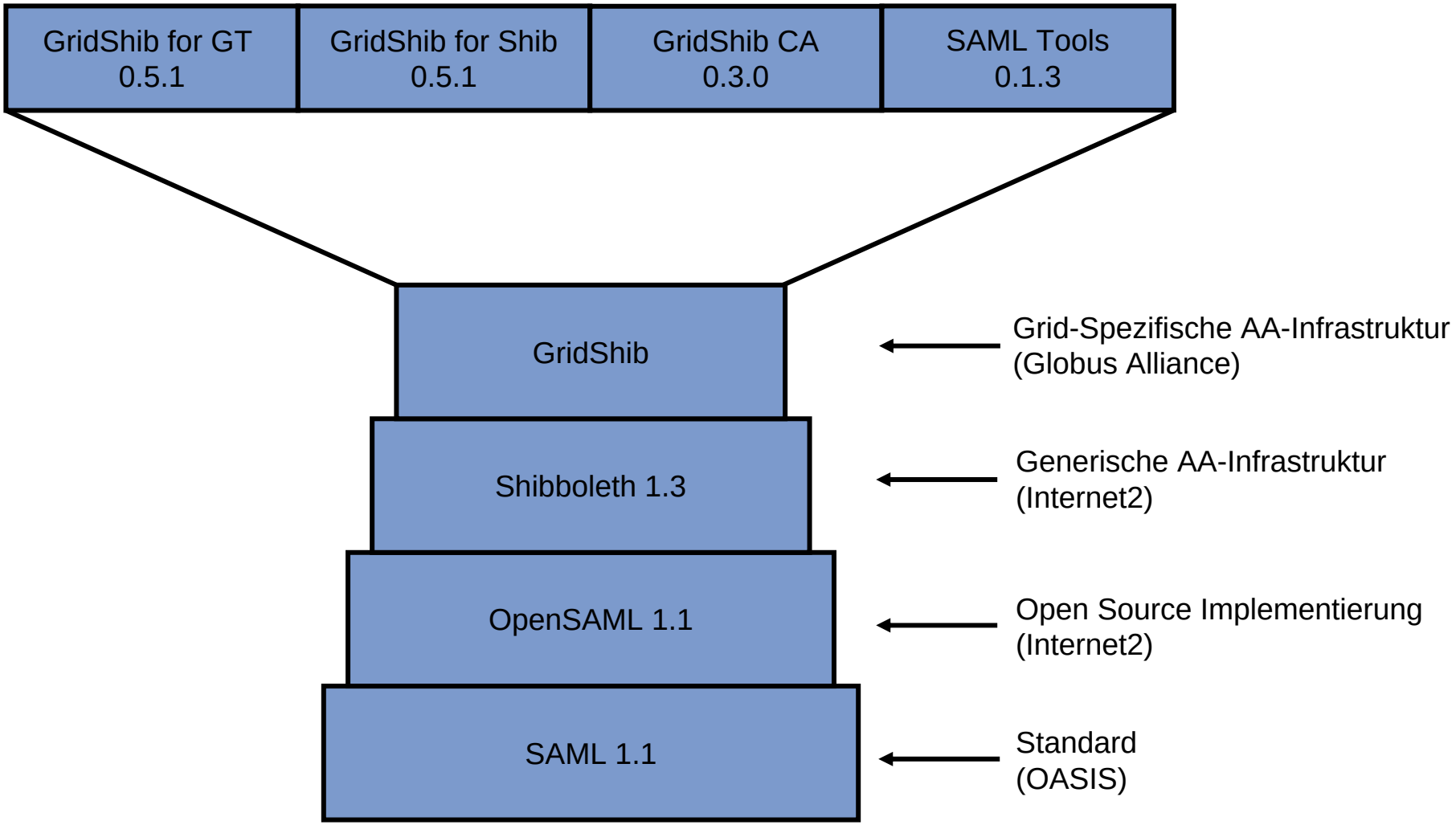
Ansatz:

- Ausstellung eines kurzlebigen X.509 Zertifikates durch Online-CA
  - SLC: Short Lived Credential - max. 1Mio Sekunden (~11 Tage) gültiges X.509 Zertifikat
  - SLCS: Short Lived Credential Service - die Online-CA
- Authentifizierung und Autorisierung bei Online-CA durch Shibboleth-Mechanismen
  - Daten für das SLC u.a. aus Attributen vom Identitiy Provider (IdP)
- Verwaltung von Attributen durch IdP in der Heimateinrichtung
  - Attribute werden per Push oder Pull zum Service Provider (SP, Bsp. SLCS, GT4 GRAM) übertragen

GridShib: Aufbau mit Online CA



GridShib Komponenten



Zukünftige GridShib Versionen

GridShib for GT

- Version 0.5.1 (beta): verfügbar
- Version 0.6: Ende März 2007
  - Einfacher SAML PIP für Attribut-push

GridShib for Shibboleth

- Version 0.5.1 (beta): verfügbar
- Version 0.6.0: Kein geplantes Releasedatum
  - Certificate Registry wird eigene GridShib Komponente
  - SAML IdP Tester wird Bestandteil der SAML Tools

GridShib CA

- Version 0.3.0 (beta): verfügbar
- Version 0.4: März 2007
  - Von IdP ausgestellte Attribute-Assertion an SLC binden
  - DN aus Attributen zusammensetzen

SAML Tools

- Version 0.1.3 (beta): verfügbar
- Version 0.2: Ende Februar 2007
  - Komplexeres Attributhandling
  - Logging und Debugging verbessern
  - Java API

Kontakt zu führenden GridShib-Entwicklern ist hergestellt

- Großes Interesse an unseren Anforderungen & Use-Cases
- Realistische Chance auf Umsetzung unserer Anforderungen

SLCs und SLCS mit GridShib

EUGridPMA akkreditiert Short Lived Credential Services (SLCS)

- Basierend auf dem *Short-lived Credential Services Profile* der TAGPMA

DFN-Verein betreibt durch die DFN-PCA einen DFN-SLCS im Pilotbetrieb

- Stellt SLCs mit max. Laufzeit von 1 Mio. Sekunden (ca. 11 Tage) aus
- Verwendung der GridShib CA mit OpenSSL (Online CA)
- Als Shibboleth Service Provider Mitglied der
  - DFN-AAI Test Föderation
  - und der Vascoda Föderation
- Nach Beendigung der Pilotphase und Etablierung der DFN-AAI Policys (Qualitätsregeln für IdPs/IDMS) wird eine Akkreditierung des DFN-SCLS bei der EUGridPMA angestrebt

Im IVOM-Projekt werden bereits IdPs und GridShib Online CAs getestet

- Mitglied der Vascoda Test-Föderation
- Umzug in die DFN-AAI geplant (sobald möglich)
- Enge Zusammenarbeit mit der DFN-PCA

Offene Fragen I

Zwei Attribute Authorities für Grid AAI

- 1. Grid-unabhängige Attribute vom Shibboleth IdP
- 2. VO-Attribute von VO-AA, beispielsweise VOMS
- Wie kann man effizient und praktikabel Attribute aus beiden Quellen auf Ressourcen verfügbar machen? → IVOM

Generierung des DN

- Beispiel DN:
  - „C=DE/O=GridGermany/OU=Leibniz Universitaet Hannover/OU=RRZN/CN=groeper@idp.uni-hannover.de“
- Bisher in GridShib Online-CA:
  - C, O und OU vom SLCS, CN vom IdP
- Besser (Ausbau des Piloten):
  - Eindeutige Zugehörigkeit des DNs zu genau einer Identität muss immer gewährleistet sein
  - C und O vom SLCS
  - OU(s) und CN vom IdP

Bildung einer Föderation mit verbindlicher Policy: DFN-AAI

- Zwischen SPs und IdPs
  - Ein einzelner unsicherer IdP kompromittiert alle über die Föderation zugänglichen Ressourcen
  - Ggf. bilaterale Vereinbarungen zwischen SLCS-SP und IdPs nötig, um strengere IDMS Kriterien der EUGridPMA zu erfüllen

Offene Fragen II

Authentifizierung beim IdP

- Username/Password
  - Momentan eingesetztes Verfahren
- Nutzerzertifikat
  - Ebenfalls möglich
  - Wird im Kontext der Akkreditierung bei der EUGridPMA als qualitativ hochwertiger angesehen
    - Zwei-Faktor Authentisierung: Nutzer hat das Zertifikat, Nutzer weiß das Passwort
  - Gefahr, dass das Passwort wie bei anderen Logins des Nutzers ggf. auch ungeschützt übertragen wird, ist kleiner
  - Zertifikat auf Hardware-Token ist möglich

GridShib mit gLite

- Mit VOMS direkt kombinierbar
- IVOM und EGEE-2/SWITCH arbeiten an Integration

GridShib mit UNICORE

- IVOM arbeitet an Integration

Zusammenfassung

Das IVOM Projekt

Übersicht GridShib: Komponenten und Aufbau

- 4 Komponenten: GS for Shib, GS for GT, Online CA und SAML Tools

Aktuelle GridShib Versionen: Was geht schon und was kommt noch

- Was geht?
  - Online-CA
  - PDP auf GT4 Ressourcen mit Attribute Pull
- Was kommt noch?
  - Attribute Push über Zertifikate
  - Viele Detailverbesserungen

SLC und SLCS mit GridShib Online-CA

- SLCS-Pilotbetrieb durch DFN-Verein
- IVOM arbeitet an AAI- und VO-Management Konzept

Offene Fragen

- Kombination von zwei AAs

Attributsbasierte Autorisierung

- GT4 heute: ausschließlich Identitätsbasiert (grid-mapfile)
- GridShib ermöglicht attributsbasierte Autorisierung
- VOMS-PDP ermöglicht attributsbasierte Autorisierung

Zukünftig eher Attribute Push als wie bisher Attribute Pull

- Attribute werden als SAML-Assertion formuliert
- Attribute werden als X.509v3 Zertifikatserweiterung in Zertifikate eingebunden
- Vorteile:
  - IdP Discovery kein Problem mehr
  - Vereinfachte Firewall-Konfiguration (wenn ausschließlich Push verwendet wird)
- Nachteil:
  - SP Discovery Problem: Welcher Service Provider benötigt welches Attribut?
  - Lösung:
    - Entweder alle Nutzerattribute an alle SPs schicken (Datenschutz?)
    - Oder Minimalsatz von Attributen definieren, der an SPs per push übertragen wird

GridShib Use Cases

„Existing Grid-User“

- Hat X.509 Nutzerzertifikat
- Hat ggf. keine Attribute
  - Attribute werden auf IdP verwaltet → IdP Discovery Problem

„New Grid-User“

- Hat kein Nutzerzertifikat
- Bekommt SLC von SLCS ausgestellt
- Attribute werden auf IdP verwaltet und sind bereits in SLC enthalten
  - D.h. Attribut-Push und kein IdP Discovery Problem

„Portal User“

- Nutzer authentifiziert sich am Portal über Shibboleth-Mechanismen
- Jobs werden mit „Community Credential“ des Portals gestartet
  - Verbindung zum Nutzer ausschließlich über Attribute in diesem Community Credential