GÉANT TrustBroker: Föderationsübergreifendes Identity Management

Daniela Pöhn, Michael Grabatin,
Stefan Metzger und Wolfgang Hommel
ZKI-Arbeitskreis Verzeichnisdienste

Heidelberg, 1./2. Oktober 2015

Agenda

- Motivation
- GÉANT TrustBroker
  - Überblick
  - Workflow und Initiierung
  - Metadaten-Registrierung
  - Konvertierungsregeln
- Aktueller Stand
  - Prototyp
  - Protokoll
  - Kleine Demo
- Zusammenfassung und Ausblick

Motivation

GN3+: Open Call Projekt (Start Okt 2013)

GN4 Phase 1: JRA3 T3

GÉANT TrustBroker (GNTB):

- Dynamischer Aufbau von technischem Vertrauen
- On demand Metadaten-Austausch
  zwischen Identity Provider (IDP) und Service Provider (SP)
- Initiiert durch den Benutzer
- Repository für Konvertierungsregeln

IETF Internet-Draft

Shibboleth-basierter Prototyp

Motivation

SP und IDP müssen in der **selben** Föderation oder Inter-Föderation sein.

→ Communities müssen in nationalen Föderationen teilnehmen oder eigene Föderationen gründen.

→ IDPs/SPs müssen teils mehreren Föderationen beitreten.

Zudem:

→ Manuelle Konfiguration durch den IDP

→ Vertrauen: IDPs müssen SPs vertrauen

- Metadaten
- Weitere Aspekte des Vertrauens
  → *SPs erhalten ggf. nicht alle benötigten Attribute*

→ Begrenzung durch Schemata

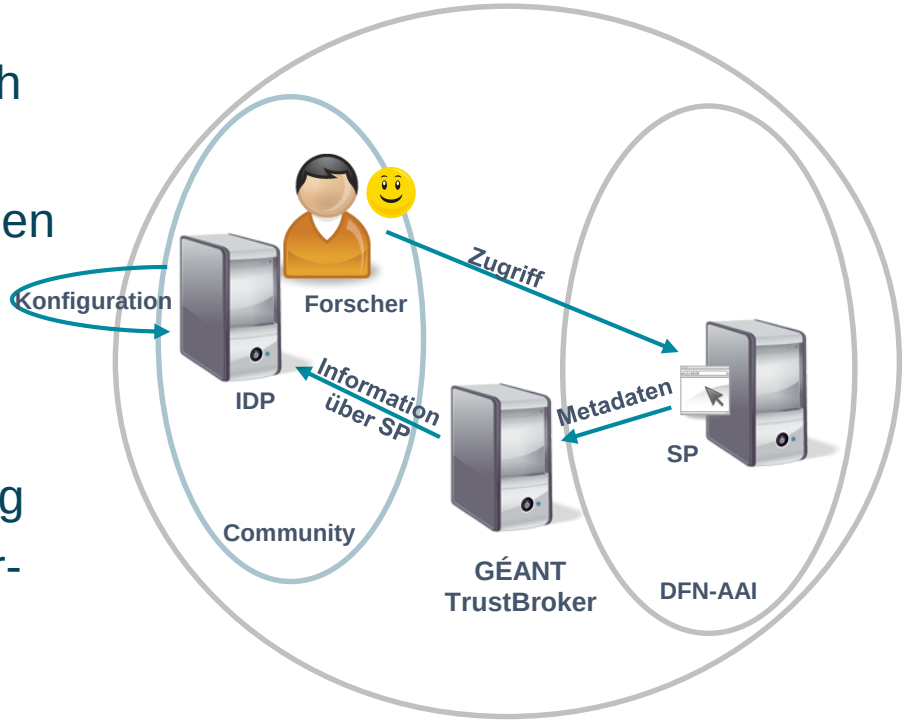
GNTB Überblick

Ziel: SPs mit den IDPs der Nutzer verbinden

- Unabhängig von Föderationen
- Dynamischer Metadatenaustausch
- Initiiert durch den Benutzer

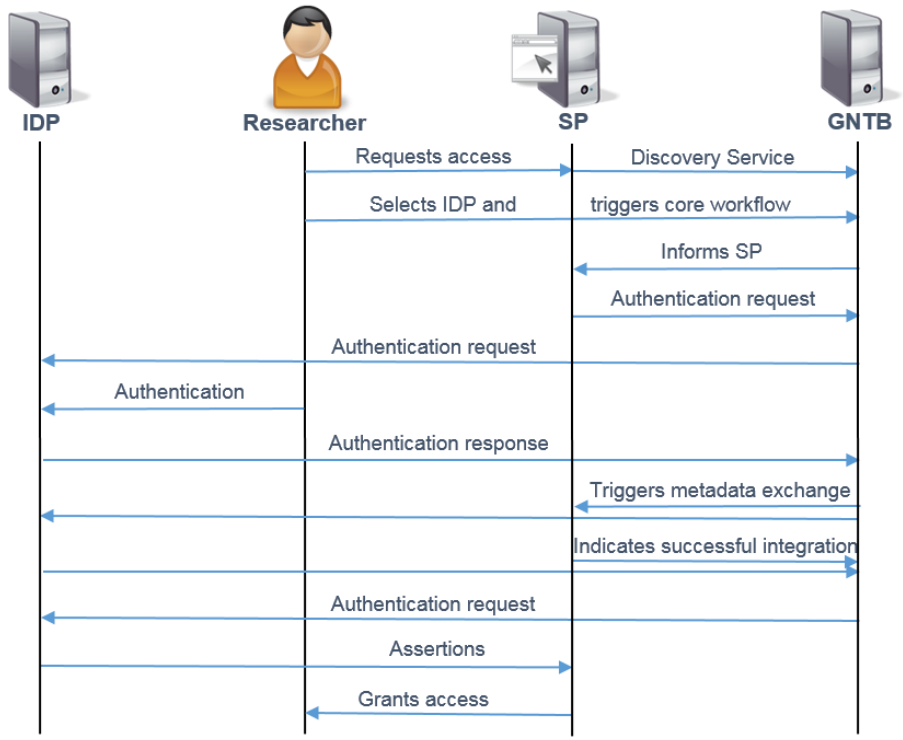
Konvertierungsregeln wiederverwenden

→ Keine manuelle Konfiguration
→ Keine Wartezeit für Benutzer
→ GNTB Registrierung + Erweiterung
→ Parallel zu Föderationen und Inter-Föderationen einsetzbar



GNTB Workflow

1. Nutzer F wählt seinen IDP bei GNTB aus (Discovery Service).
2. F initiiert technisches Setup.
3. SP sendet Authentication Request an GNTB.
4. GNTB leitet F zu seinem IDP weiter zur Authentifizierung.
5. IDP lädt sich die Metadaten des SPs herunter.
   Konfiguration wird automatisch aktualisiert.
6. Selbe gilt für den SP.
7. IDP sucht nach Konvertierungsregeln.
8. IDP sendet Assertion zum SP.
   F kann Dienst des SPs nutzen.



GNTB Metadaten-Registrierung

Vorbedingungen: Registrierung und GNTB Erweiterung installieren.

On demand Austausch von Metadaten

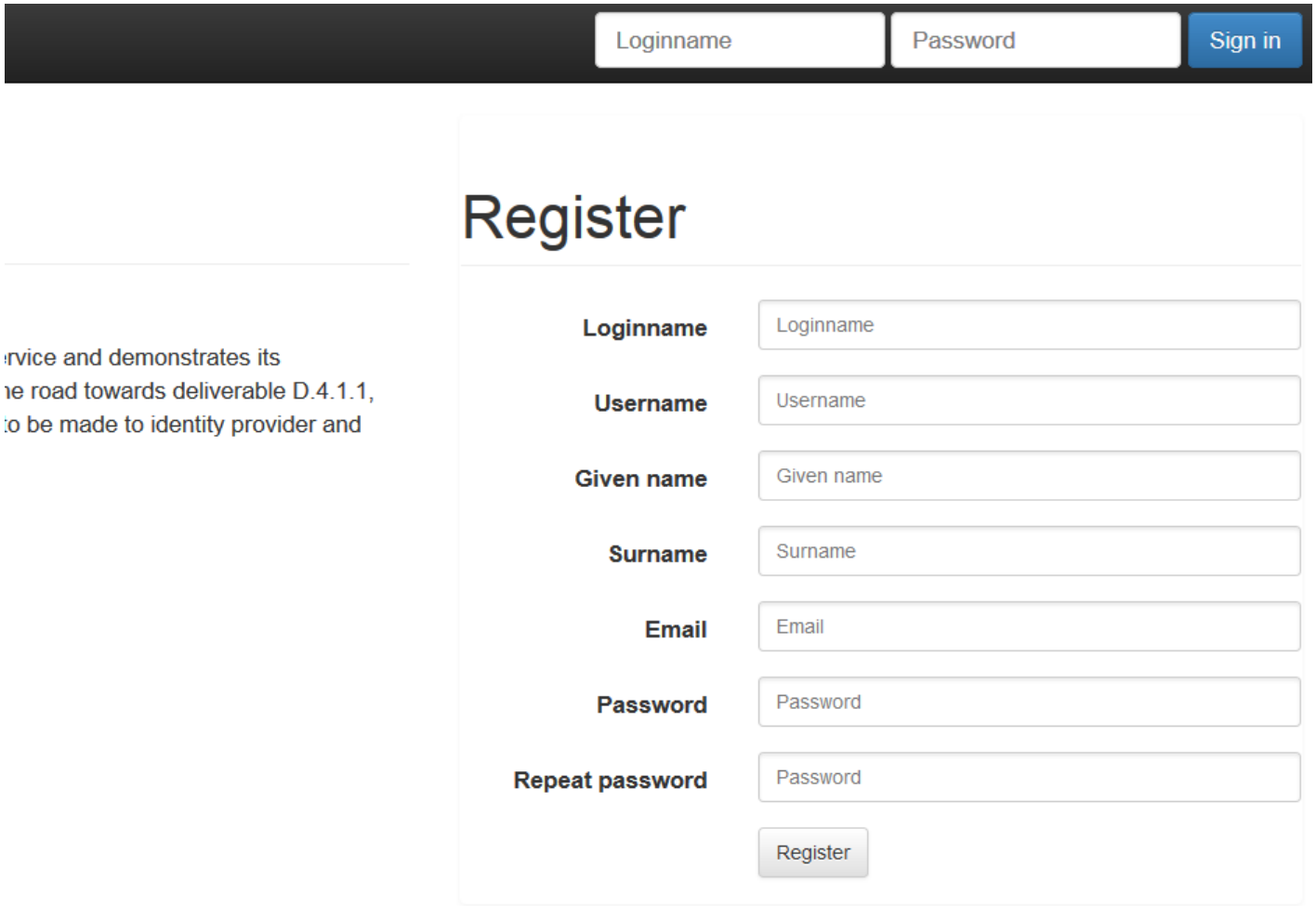
→ Automatisches Hinzufügen zur lokalen Konfiguration

→ Technisches Vertrauen

Wo ist das Vertrauen?

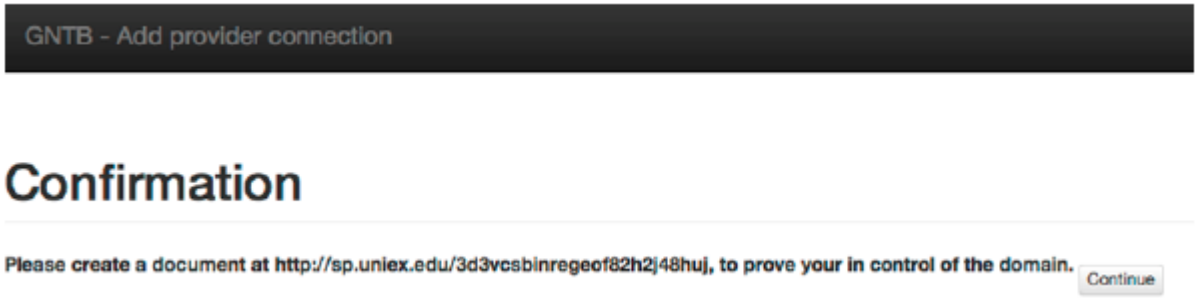
- Metadaten werden, initiiert durch den Nutzer ausgetauscht.
  - Signaturen und Technisches Vertrauen
- Validierung
  - Berechtigung von IDP und SP, beispielsweise anhand von Zertifikaten
  - Metadaten
- Zusätzliche Möglichkeiten:
  - Whitelists / Blacklists
  - Weitere Konfiguration, wie Möglichkeit der expliziten Zustimmung durch IDP/SP

GNTB Metadaten-Registrierung



http://gntb08.srv.lrz.de:8080/discovery/ttp/index.jsp

GNTB Metadaten-Registrierung



GNTB Metadaten-Registrierung

Provider https://color.ado/shibboleth

Member of organization -

Description

COLORado Service Provider

Available metadata (The currently active metadata is highlighted blue)

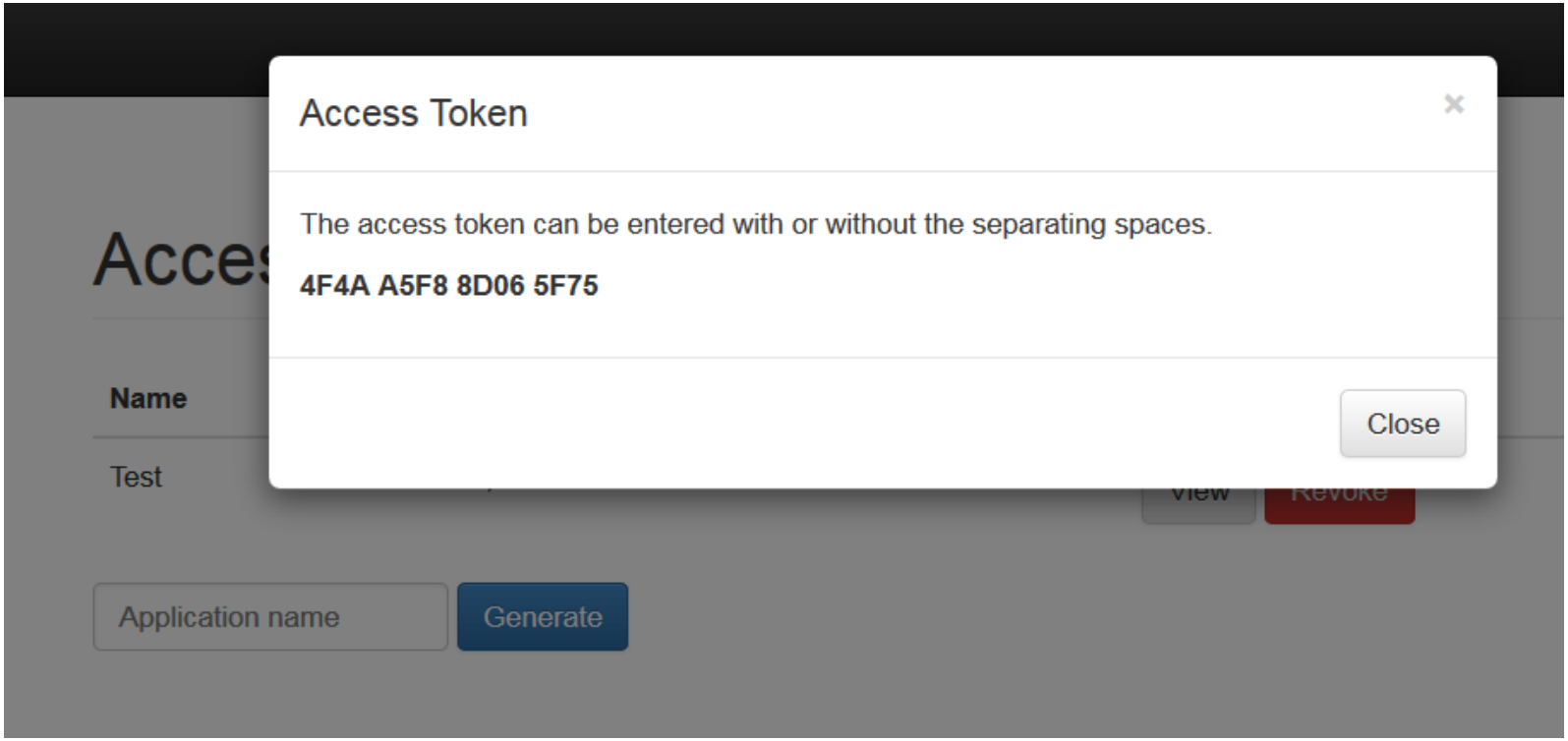
ID	ParentID	entityID	Owner	Comment
38	0	https://color.ado/shibboleth	admin	Initial metadata for the COLORado Service Provider

Blacklist

Whitelist

Attribute Release Policy

GNTB Metadaten-Registrierung



GNTB Konvertierungsregeln

Typische Konvertierungsregeln:

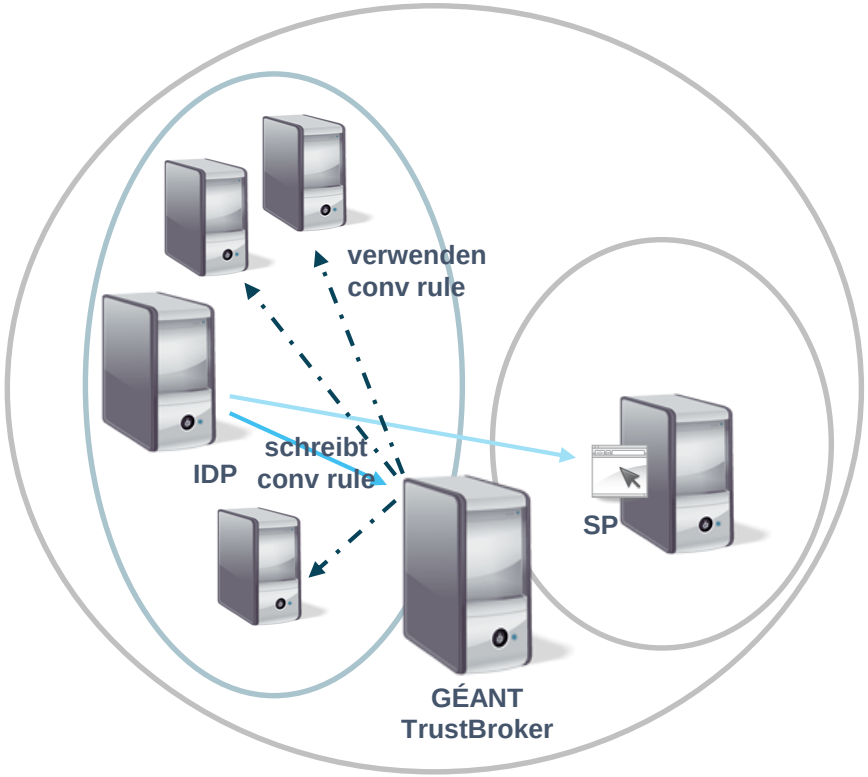
- Umbenennen
- Splitting/Merging
- Transformation

Konvertierungsregeln können gesucht und wieder verwendet werden, z.B. innerhalb einer Föderation

Regeln werden über eine Erweiterung + API geladen und integriert

→ Nur ein IDP muss Regel schreiben

→ IDPs und AAs können Regel verwenden

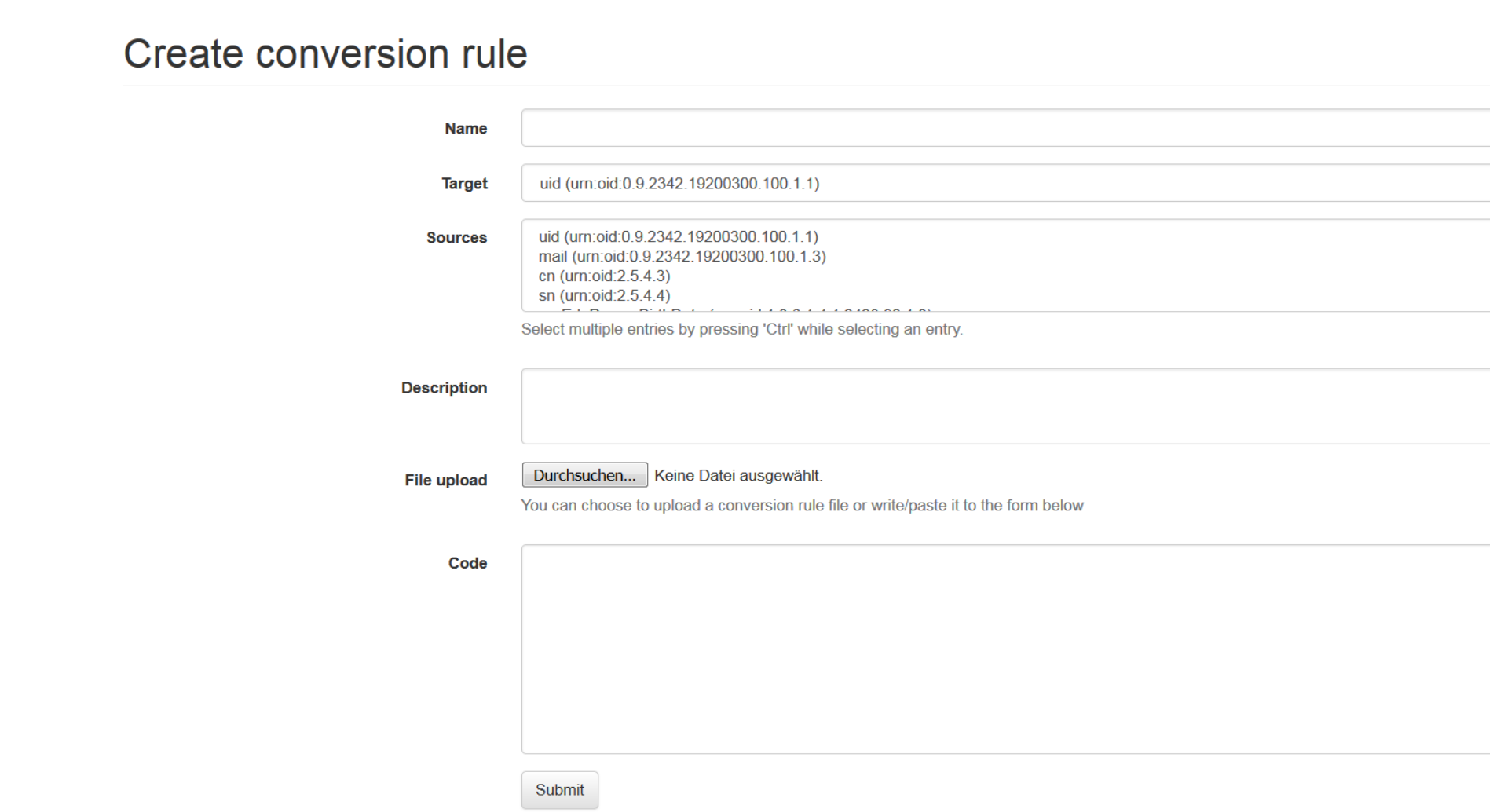


GNTB Konvertierungsregeln

Conversion Rules

ID	ParentID	Name	Sources	Target
23	0	Common name from given name and surname	• sn (urn:oid:2.5.4.4) • givenName (urn:oid:2.5.4.42)	cn (urn:oid:2.5.4.3)
24	0	Mail to eppn	• mail (urn:oid:0.9.2342.19200300.100.1.3)	eduPersonPrincipalName (urn:oid:1.3.6.1.4.1.5923.1.1.1.6)
25	0	norEduPersonBirthDate to schacDateOfBirth	• norEduPersonBirthDate (urn:oid:1.3.6.1.4.1.2428.90.1.3)	schacDateOfBirth (urn:oid:1.3.6.1.4.1.1466.115.121.1.36)
27	0	schacUserPresenceID 2 skypeID	• schacUserPresenceID (urn:oid:1.3.6.1.4.1.1466.115.121.1.15)	skypeID (urn:oid:1.3.6.1.4.1.7650.6.1)

GNTB Konvertierungsregeln



Aktueller Stand

Protokoll als Internet-Draft bei IETF

Prototyp → Pilotbetrieb?

Proof of Concept Implementierung:

- Erweiterungen für Shibboleth IdP und Shibboleth SP
- Erweiterung für Shibboleth Centralized Discovery Service

SVN-Repository mit Code:

svn.geant.net/GEANT/TrustBroker

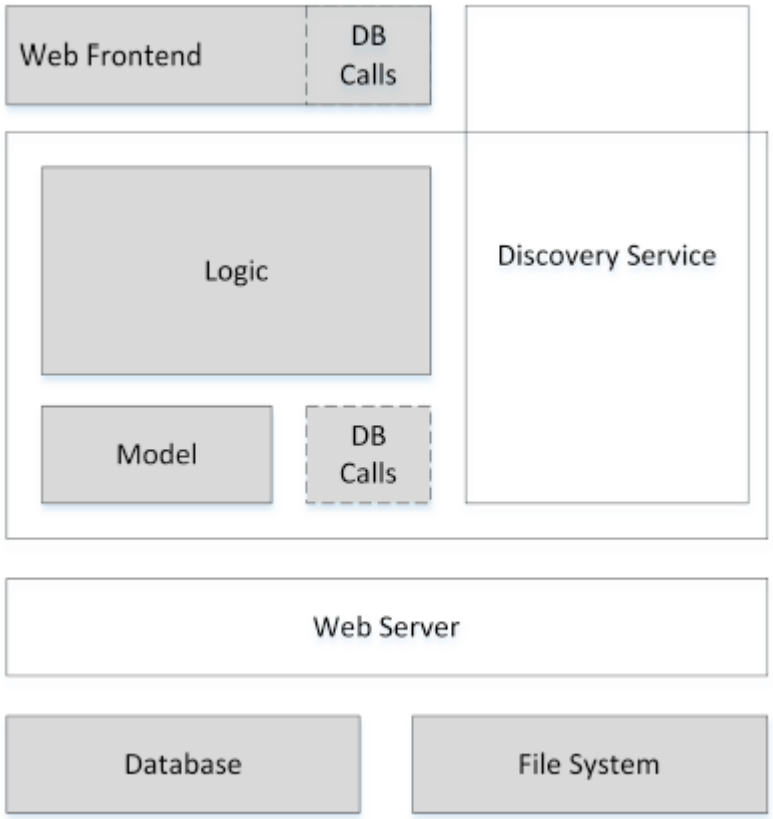
Zentraler GNTB Dienst:

http://gntb08.srv.lrz.de:8080/discovery/ttp/index.jsp

Aktueller Stand Prototyp

Erweiterung des Discovery Service:

- Implementiert als Java Servlet für Apache Tomcat
- Aktivierbar über Discovery Service (DS) Konfigurationsdatei
- Kompatibel mit Metadatenquellen, die für DS konfiguriert werden können
- Parallel als DS und GNTB einsetzbar
- Erweitert SAML-Discovery-Service-Protocol
- GNTB speichert vom SP übermittelten Auth-Request in HttpSession



Aktueller Stand Prototyp

Aktuell: Optimierung und Erweiterung der Implementation

GNTB Enhancement

- REEP/PEER
- Statistiken

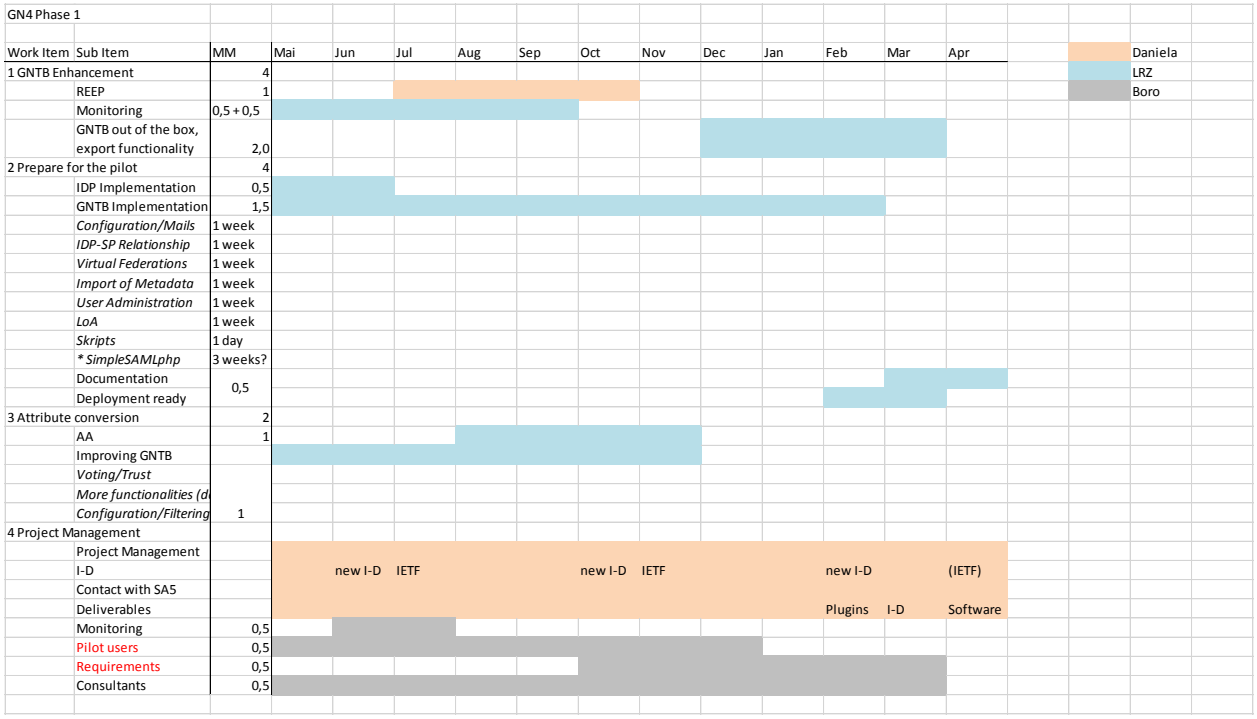
Prepare the Pilot

- Verbesserungen bei IDP/SP + Unterstützung von Shibboleth IdP 3.x
- Erweiterte Funktionalität bei GNTB
- Nice to have: SimpleSAMLphp

Attribute Konvertierung

- Verbesserter Support für AAs
- Konvertierungsregeln nicht nur für Shibboleth, sondern auch SimpleSAMLphp etc.

Aktueller Stand Prototyp



GN4 Phase 1																	
Work Item	Sub Item	MM	Mai	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr			Daniela
1 GNTB Enhancement		4															LRZ
	REEP	1															Boro
	Monitoring	0,5 + 0,5															
	GNTB out of the box, export functionality	2,0															
2 Prepare for the pilot		4															
	IDP Implementation	0,5															
	GNTB Implementation	1,5															
	Configuration/Mails	1 week															
	IDP-SP Relationship	1 week															
	Virtual Federations	1 week															
	Import of Metadata	1 week															
	User Administration	1 week															
	LoA	1 week															
	Skripts	1 day															
	** SimpleSAMLphp*	3 weeks?															
	Documentation	0,5															
	Deployment ready																
3 Attribute conversion		2															
	AA	1															
	Improving GNTB																
	Voting/Trust																
	More functionalities (d																
	Configuration/Filtering	1															
4 Project Management																	
	Project Management																
	I-D			new I-D	IETF			new I-D	IETF			new I-D		(IETF)			
	Contact with SA5																
	Deliverables											Plugins	I-D	Software			
	Monitoring	0,5															
	Pilot users	0,5															
	Requirements	0,5															
	Consultants	0,5															

Aktueller Stand Protokoll

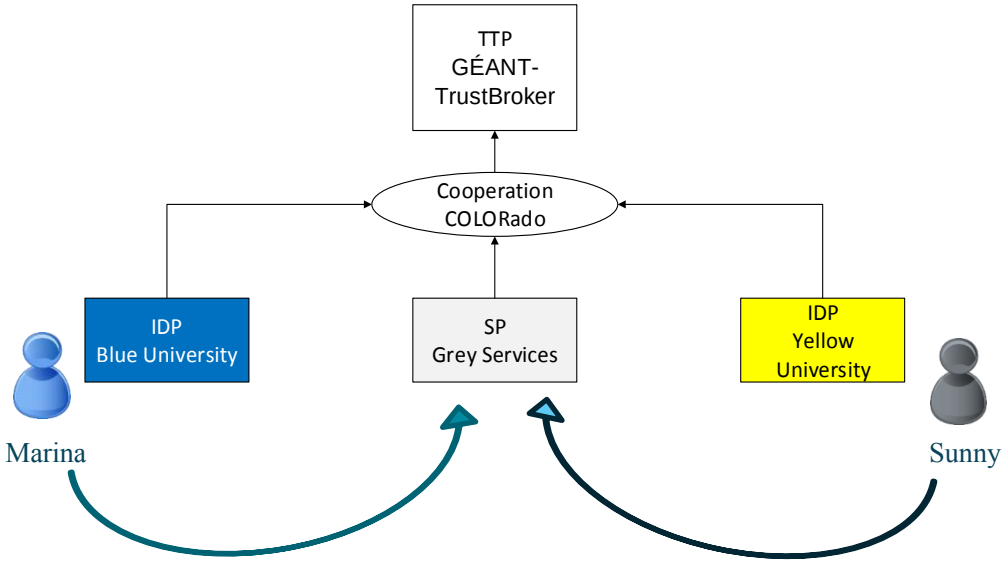
Dynamic Automated Metadata Exchange (DAME)

Kommunikation zwischen IDP, SP und GNTB
Initiierung des Metadaten-Austausches
Erweiterung von SAML 2.0 Web Browser SSO Profile
Basierend auf SAML Identity Provider Discovery Service Protocol and Profile

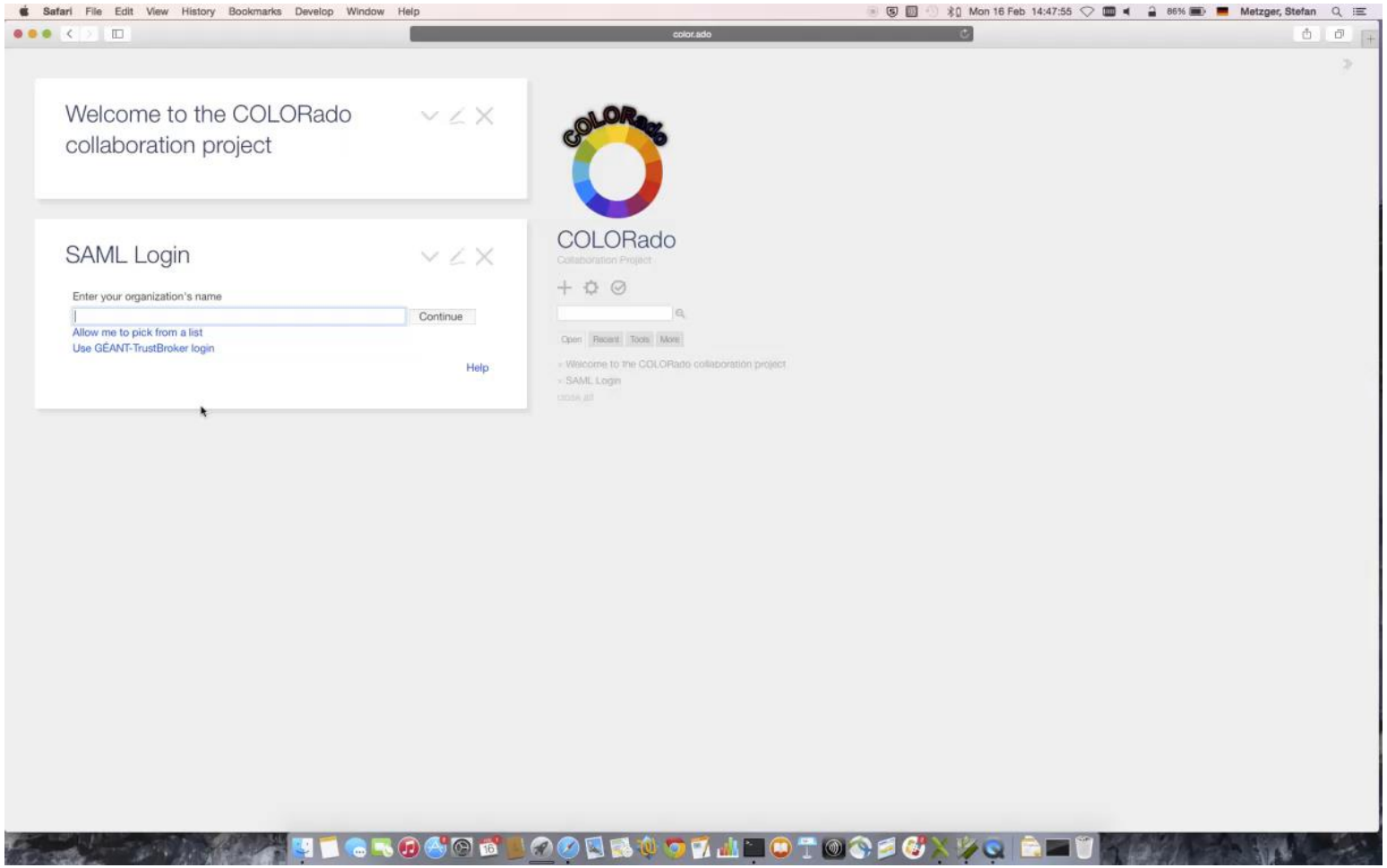
https://datatracker.ietf.org/doc/draft-poehn-dame/

Aktueller Stand Demo

Setup:



Aktueller Stand Demo



Zusammenfassung und Ausblick

Funktionalität des GNTB:

- Metadaten-Registrierung und -Austausch
  → Metadaten werden automatisch in lokale Konfiguration eingefügt
  → Reduziert Größe des benötigten Metadatensatzes
- Feature: Konvertierungsregeln
  Verwaltung und Austausch von Konvertierungsregeln

Noch fertig zu stellen:

- RFC
- Optimierung der Implementierung

Pilotbetrieb startet hoffentlich in GN4

- Testbenutzer und Feedback sind jederzeit willkommen!

→ Welche Funktionen sind interessant?

Noch was

Level of Assurance / Verlässlichkeitsklassen

- DFN-AAI: Basic und Advanced
- Für manche Nutzer möglicherweise nicht genug
- SA5T1 Work item 4: Service Aspects of Assurance

Umfrage:

http://goo.gl/forms/vprx6EpNSO

Mehr Informationen gibt es im GÉANT Wiki:
https://wiki.geant.org/pages/viewpage.action?pageId=45844180

E-Mail:
geant-trustbroker@lists.lrz.de

GÉANT

Connect | Communicate | Collaborate

www.geant.net

www.twitter.com/GEANTnews | www.facebook.com/GEANTnetwork | www.youtube.com/GEANTtv

SEVENTH FRAMEWORK PROGRAMME