GDI NRW Testbed II

AAA-Services in GDI

Dipl. Wirt.-Inform. Rüdiger Gartmann
Fraunhofer-Institut für
Software- und Systemtechnik ISST
Dortmund

16. Dezember 2002

Fraunhofer Institut
Software- und
Systemtechnik

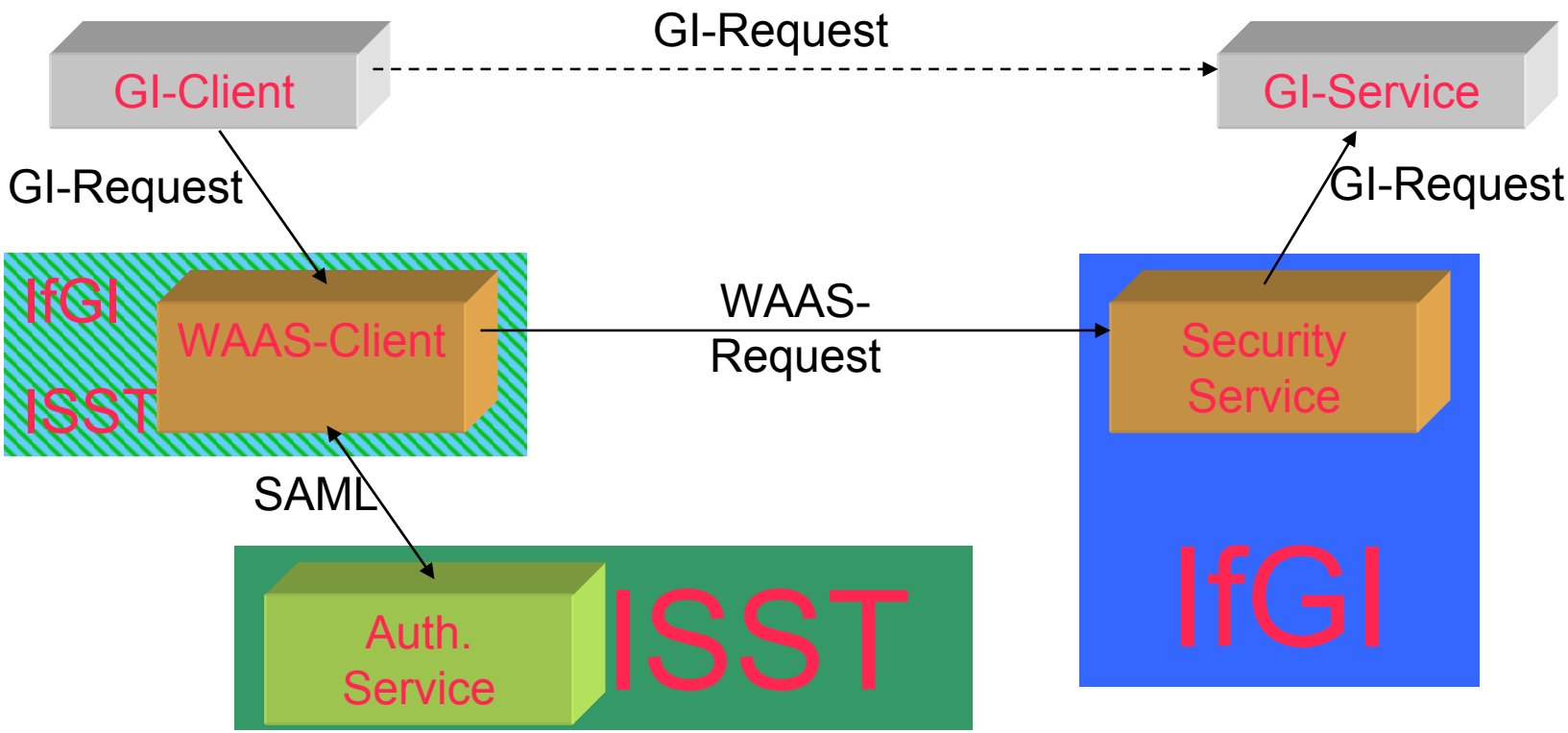
Anforderungen an einen Authentisierungsdienst in GDI

- Authentisierungsdienst soll sich möglichst homogen in das bestehende OGC- / GDI-Umfeld einfügen
- Vorhandene GI-Dienste sollten nicht geändert werden müssen
- Für Authentisierungsdienste soll ein dezentraler, verteilter Ansatz verfolgt werden
- Alle GI-Dienste (Web Services) sollen einen Authentisierungsdienst nutzen können
- Clients sollen mit unbekannten Diensten sicher kommunizieren können
- Kaskadierungen sollen unterstützt werden

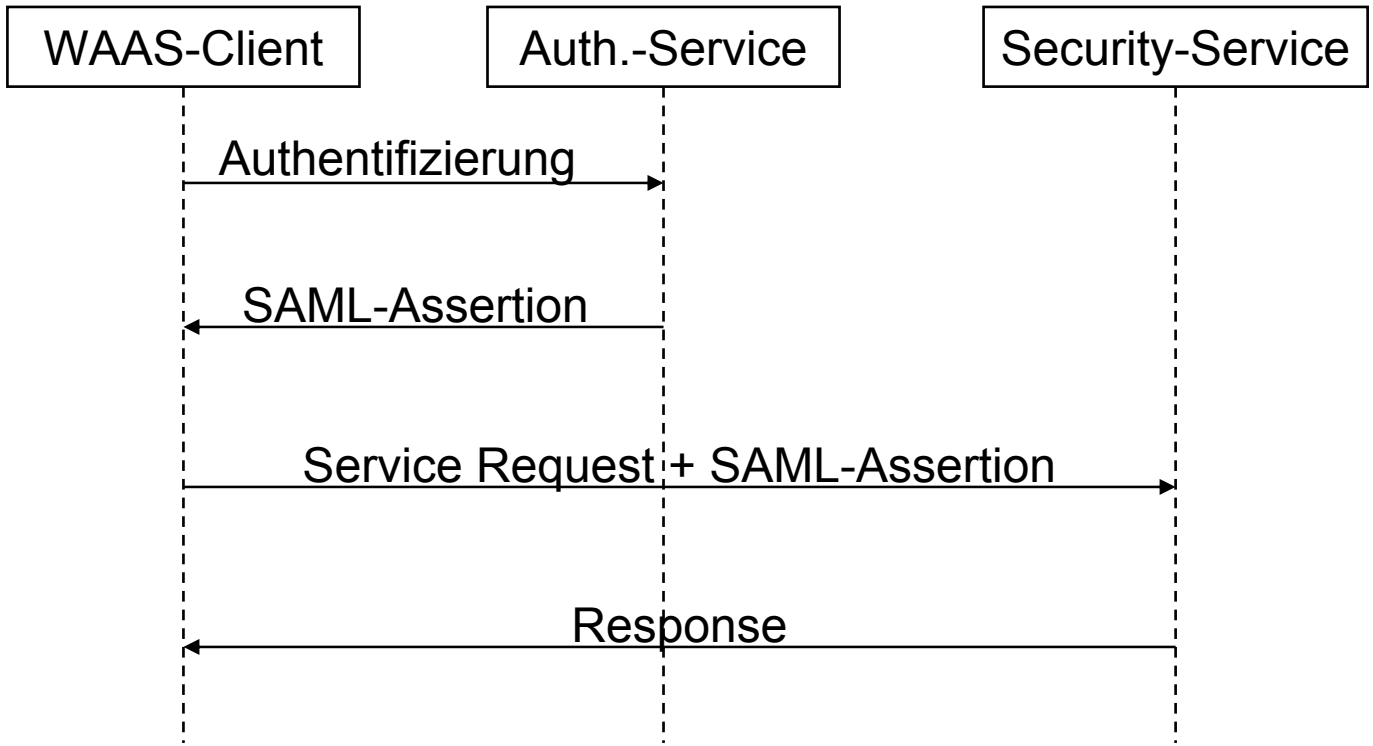
Ansatz im Testbed II

- Spezifizierung und Implementierung eines Authentisierungsdienstes
- Spezifizierung und Implementierung eines Autorisierungsdienstes
- Verwendung des OASIS-Standards SAML (Security Assertion Markup Language)
- Verwendung von XML-Signature
- Verfolgung des mit dem WPOS eingeführten Protokollschichtungsansatzes

Architektur



SAML-Protokoll (HTTP-POST)



SAML Protokoll

Request

VERSION=1.0.0
REQUEST=Authenticate
METHOD=urn:oasis:names:tc:SAML:1.0:am:password
TARGET=http://geonetz.uni-muenster.de/wms
CREDENTIALS=meinLogin;meinPasswort

Response

Recipient=http://geonetz.uni-muenster.de/wms
StatusCode Value="samlp:Success"
AssertionID="639ca10f-f0f3-442a-9f27-494c17a3f7b9"
Conditions NotBefore="2002-12-16T10:49:10Z"
NotOnOrAfter="2002-12-16T10:54:10Z"

Fraunhofer Institut
Software- und
Systemtechnik

Stand der Dinge

Implementierung	Authentisierungs- und Autorisierungsservice fertiggestellt
	-> Workflow funktioniert
Noch zu tun	Kommunikation über SSL
	Digitale Signatur der SAML-Kommunikation
	Spezifikation
	Capabilities
Offene Fragen	Eintrag in Registry