Absicherung von Grid Services

Transparenter Application Level Gateway

Thijs Metsch (DLR Simulations- und Softwaretechnik)

Göttingen, 27.03.2007, 2. D-Grid Security Workshop

Überblick
Gliederung des Vortrages

Überblick	ALG	Ausblick
Einführung Sicherheitskonzepte Risiken	Design ALG Technische Umsetzung Demonstration	GridFTP Einordnung des ALGs Fazit

Einführung
Aktuelle Situation

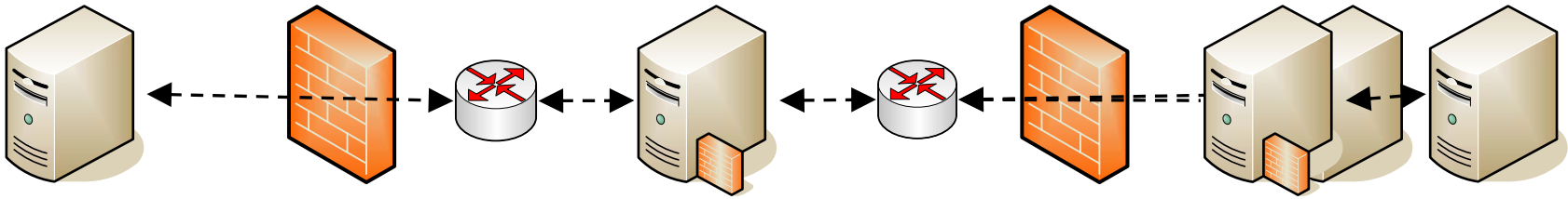
- Realisierung von Grids über aktive Firewalls hinweg ist nahezu unmöglich

- Mögliche Optionen
  - „Verbiegen“ der Firewall Richtlinien
  - Grid Ressourcen in der DMZ platzieren
  - Gatekeeper in der DMZ platzieren

- Nachteile
  - Mögliche Unverträglichkeit mit der Sicherheitsstrategie des Unternehmens
  - Komplexe Applikationen können damit nicht abgebildet werden

Sicherheitskonzept
Ideen und Strategien

- Bundesamt für Sicherheit in der Informationstechnik (BSI) schlägt als Grundstruktur *Paketfilter – Application-Level-Gateway (ALG) – Paketfilter (PAP)* vor
- Ein ALG unterbricht den direkten Datenstrom, nimmt Anfragen entgegen und leitet diese weiter
- Mögliche Steuerung der Richtung des Datenstroms



Sicherheitskonzept (2)
Aufgaben der Komponenten

- Aufgaben der Paketfilter

  Traffic Management **Lastverteilung** **Erster Filter**

- Aufgaben des Application Level Gateways / Proxies

  Validation von Anfragen **Accounting** **Logging**

  Unterstützung von Non blocking buffered I/O

- Vorteile dieses Konzeptes
  - Grundlage zur Erzeugung eines hohen Schutzfaktors
  - Einfache Erweiterbarkeit (z.B. durch Virenscanner, IDS)
  - Ausnutzung von Sicherheitslöchern im Server kann unterbunden werden

Sicherheitsrisiken

Und die Gegenmaßnahmen

Risiken

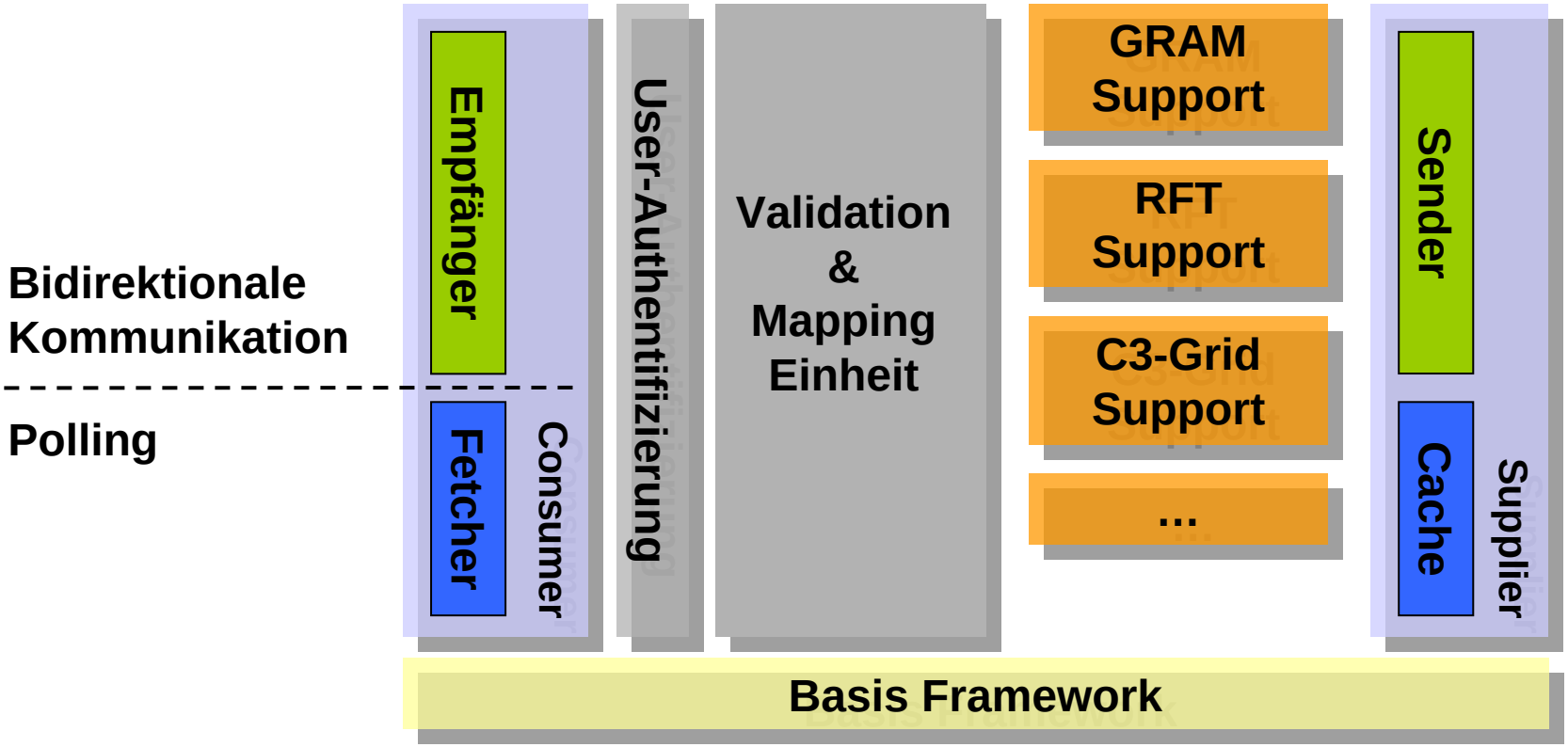
- Verschleiern der Identität ✓
- Daten-Manipulation ✓
- Unkontrollierter Zugriff ✓
- DoS-Angriffe ✓
- Abhören von Daten ✓
- Privilegien-Manipulation ✓

Gegenmaßnahmen

- Authentifizierung von Nutzern.
- Validierung des Traffic
- Abbilden von Nutzern
- Erkennung von DoS-Angriffen
- Daten-Verschlüsselung
- Daten liegen im Intranet

Application Level Gateway

Design für ein Web Service Proxy

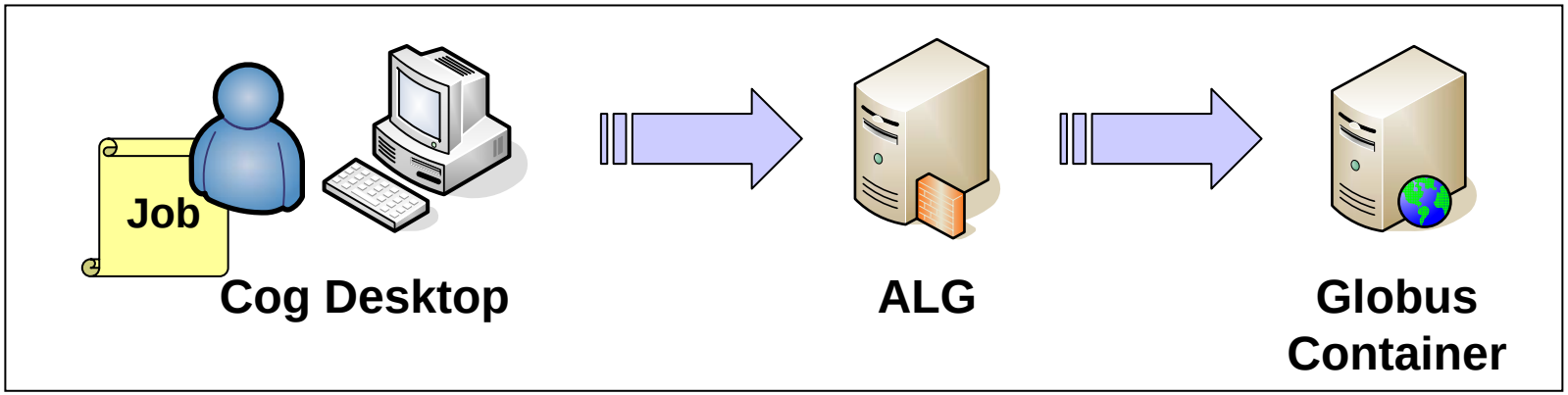


Technische Umsetzung
Vorteile des Plug-In-Designs

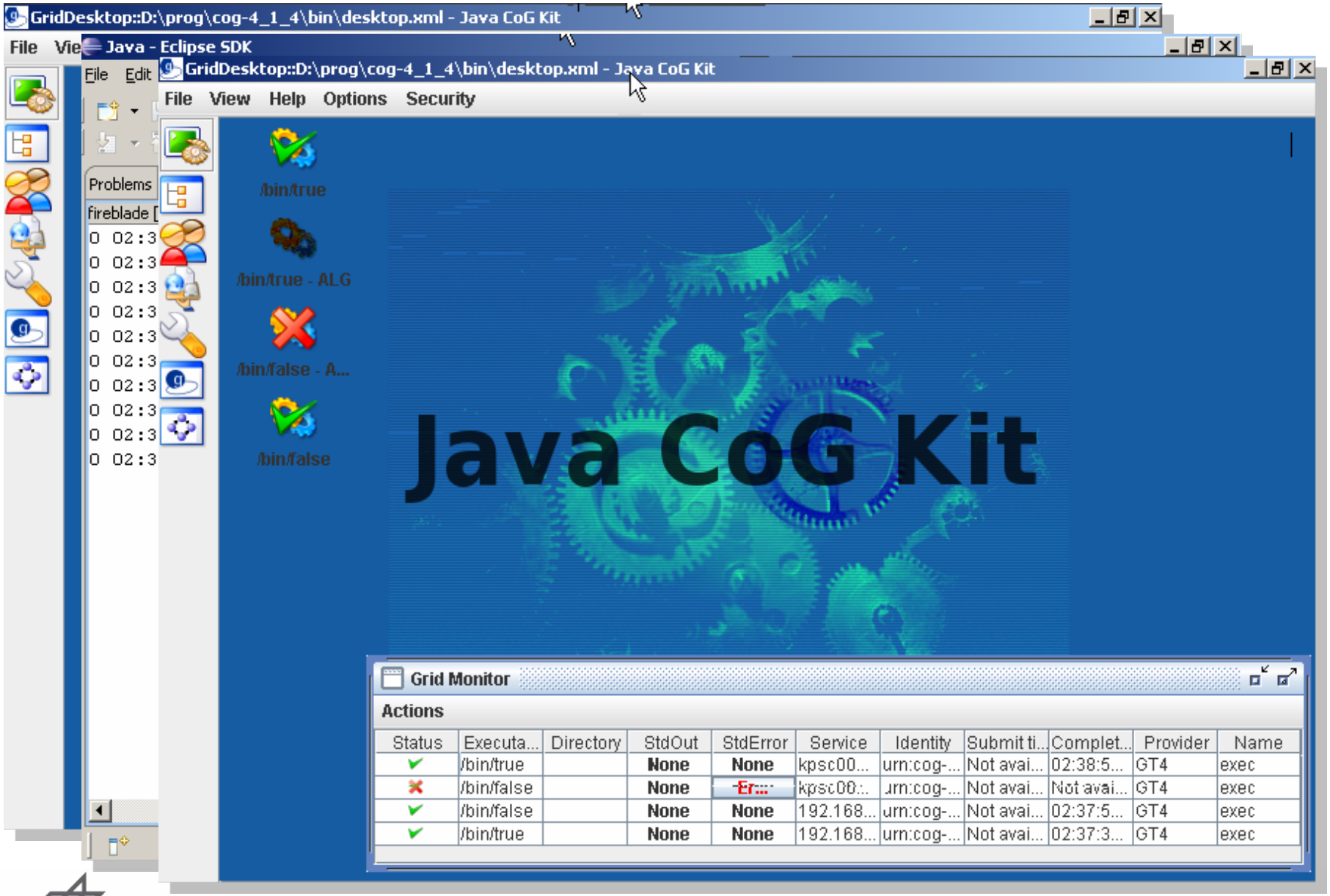
- Technische Umsetzung
  - Entscheidung Aufgrund von Information in SOAP-Meldungen
  - Detaillierte Prüfung in einzelnen Plug-Ins (z.B. über Schemata)
  - Lastverteilung kann durch Kopplung von ALGs realisiert werden

- Vorteile des Plug-In-Designs
  - Einfache Erweiterbarkeit des ALG
  - Einfache Integration von weiteren Features (z.B. Transport Protokolle)
  - Unterstützung von eigenentwickelten In-House-Services

Demo
ALG in use



Demo


GridDesktop::D:\prog\cog-4_1_4\bin\desktop.xml - Java CoG Kit
File Vie
Java - Eclipse SDK
File Edit
GridDesktop::D:\prog\cog-4_1_4\bin\desktop.xml - Java CoG Kit
File View Help Options Security
Problems
fireblade [
0 02:3
/bin/true
/bin/true - ALG
/bin/false - A...
/bin/false
Java CoG Kit
Grid Monitor
Actions
Status Executa... Directory StdOut StdError Service Identity Submit ti... Complet... Provider Name
/bin/true None None kpsc00... urn:cog-... Not avai... 02:38:5... GT4 exec
/bin/false None Er... kpsc00... urn:cog-... Not avai... Not avai... GT4 exec
/bin/false None None 192.168... urn:cog-... Not avai... 02:37:5... GT4 exec
/bin/true None None 192.168... urn:cog-... Not avai... 02:37:3... GT4 exec

Einsatz des ALGs

Lösung für verschiedene Strategien

- Nutzung als einfacher Sicherheits-Proxy
  - Authentifizierung des Nutzer mittels GSI
  - Kein wissen über die vorgehenden Aktionen des Nutzers
- Überprüfung der Aktionen im Grid
  - Wissen über alle Operationen kann erlangt werden (Accounting, Logging)
  - Gegebenenfalls Erhöhung der Latenzzeit
- Einsatz als “Firewall-Opener”
  - Realisierung schneller Verbindungen möglich (GridFTP)
  - Eher schwierig zu realisieren

Einsatz je nach gewünschtem Sicherheitslevel

Einordnung des ALGs

Vor- und Nachteile durch den Einsatz von Proxies

- Vorteile von Proxies
  - Geringere Anzahl von Programmierfehlern im ALG als in den geschützten Services
  - Filterung/Löschung von Inhalten
  - Erzwingung einer starken Authentifizierung
  - Protokollierung
  - Abwehr von Angriffen (z.B. Integration eines IDS)
  - Keine Modifikation der Applikationen nötig
- Nachteile von Proxies
  - Komplexität der Entwicklung und Konfiguration
  - Verringerung des maximalen Durchsatzes
  - Größere Antwortzeiten (Latenzzeiten) beim Abruf von Information (nicht unbedingt bei Daten-Transfers)

Aber ein ALG ist auch nur ein Teil eines Sicherheitskonzeptes

Fazit und Ausblick
Planung und Implementierung

- Bewährtes Konzept (z.B. in IBM Websphere Web Service Gateway, Xtradyne WS-DBC, Visonys Airlock)
- Einsatz von modernen Technologien
  - Java und Axis (auch im Globus Toolkit eingesetzt)
  - Geeignet für OGSA/WSRF-basierende Grids
- Prototyp wurde in Rahmen einer Diplomarbeit erstellt und beim OGF präsentiert
- Zukünftige Entwicklungen
  - Weiterentwicklung am Argonne National Lab zur besseren Integration mit dem Globus Toolkit
  - Kopplung mit Firewalls (z.B. für den Einsatz von GridFTP)
  - Entwicklung von verschiedener Plug-Ins

Fragen und Anregungen?
Referenzen auf weitere Arbeiten

„Globus Toolkit Version 4: Software for Service-Orientated Systems“,
Ian Foster

„Globus Firewall Requirements“,
Von Welch

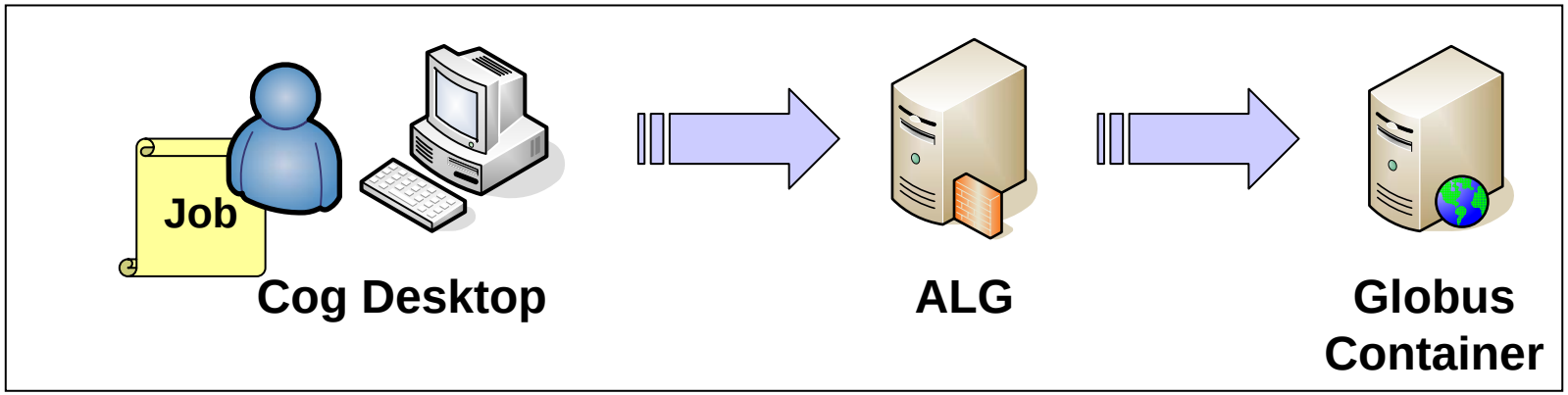
„Firewall Issues Overview“,
Open Grid Forum

„Konzeption von Sicherheitsgateways“,
Bundesamt für Sicherheit in der Informationstechnik

“Simple Object Access Protocol”,
W3 Konsortium

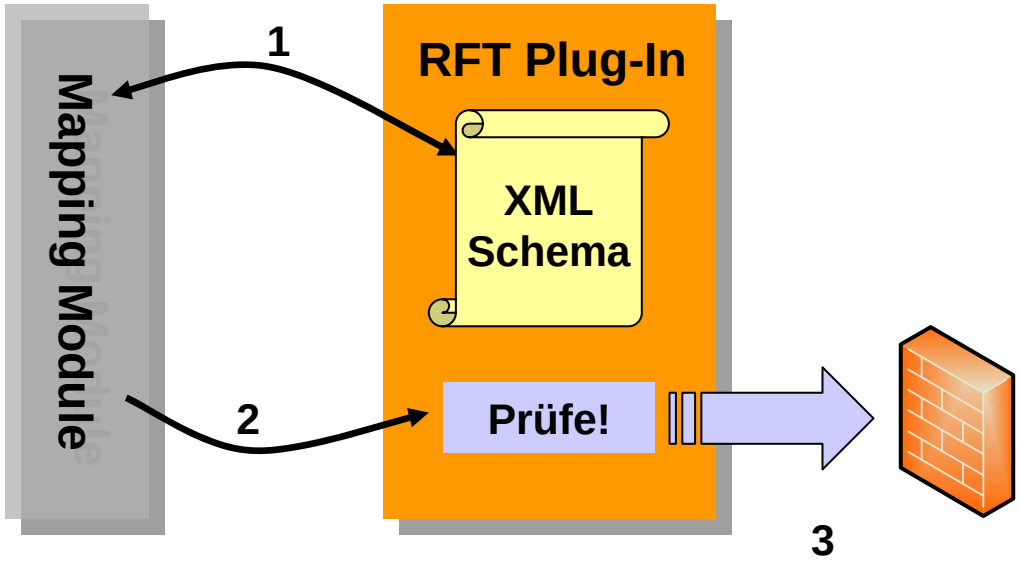
Backup Slides

Demonstration
ALG im Einsatz



Demo

Unterstützung von RFT (Reliable File Transfer)
ALG als Garagen-Tor-Öffner



1. Bestimmung des Anfragetyps mittels eines XML Schemas
2. Übergabe an Plug-In und weitere Prüfungen der Anfrage (z.B. durch Virenscanner)
3. Öffnen des benötigten Port(-range) bei der Firewall für die Partner