GIDS: Architekturvorschlag und Implementierungsüberblick

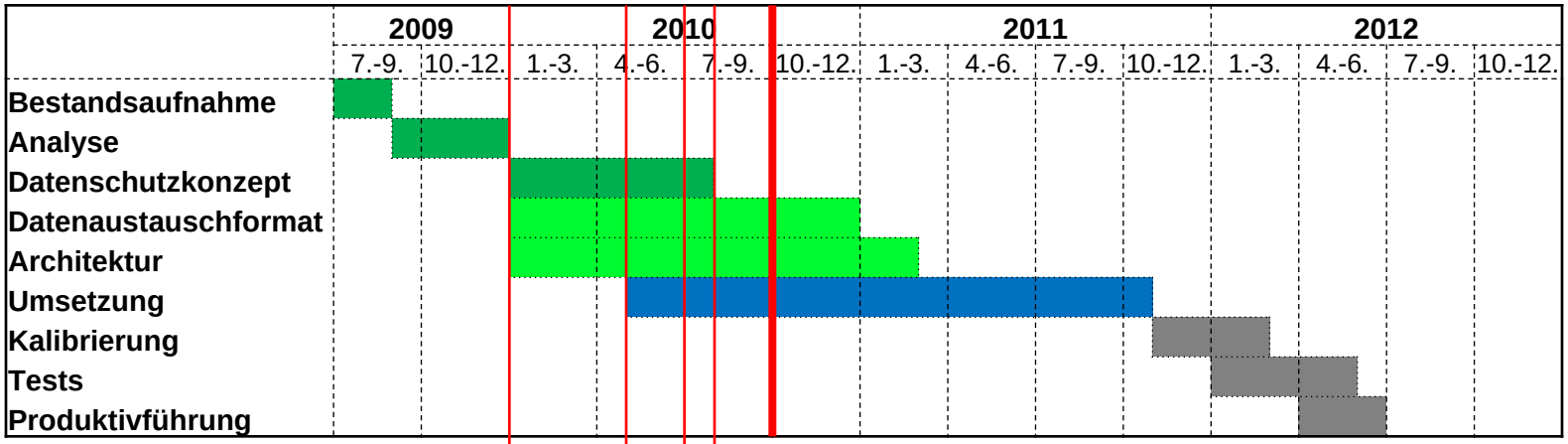
Dr. Wolfgang Hommel
Dr. Nils gentschen Felde
Felix von Eye
Jan Kohlrausch
Christian Szongott

Überblick

- **Partner:**

- **Assoziierte Partner:** STONESOFT FUJITSU
- **Motivation:**
  - Bisher IDS nur für autonome Systeme
  - Keine Grid-globale Ereigniskorrelation
- **Ziel:**
  - Konzept und Implementierung eines Grid-IDS
  - Nachhaltiger Betrieb des GIDS als Dienst im D-Grid

Projektverlauf



heute

MS13: Datenschutzkonzept

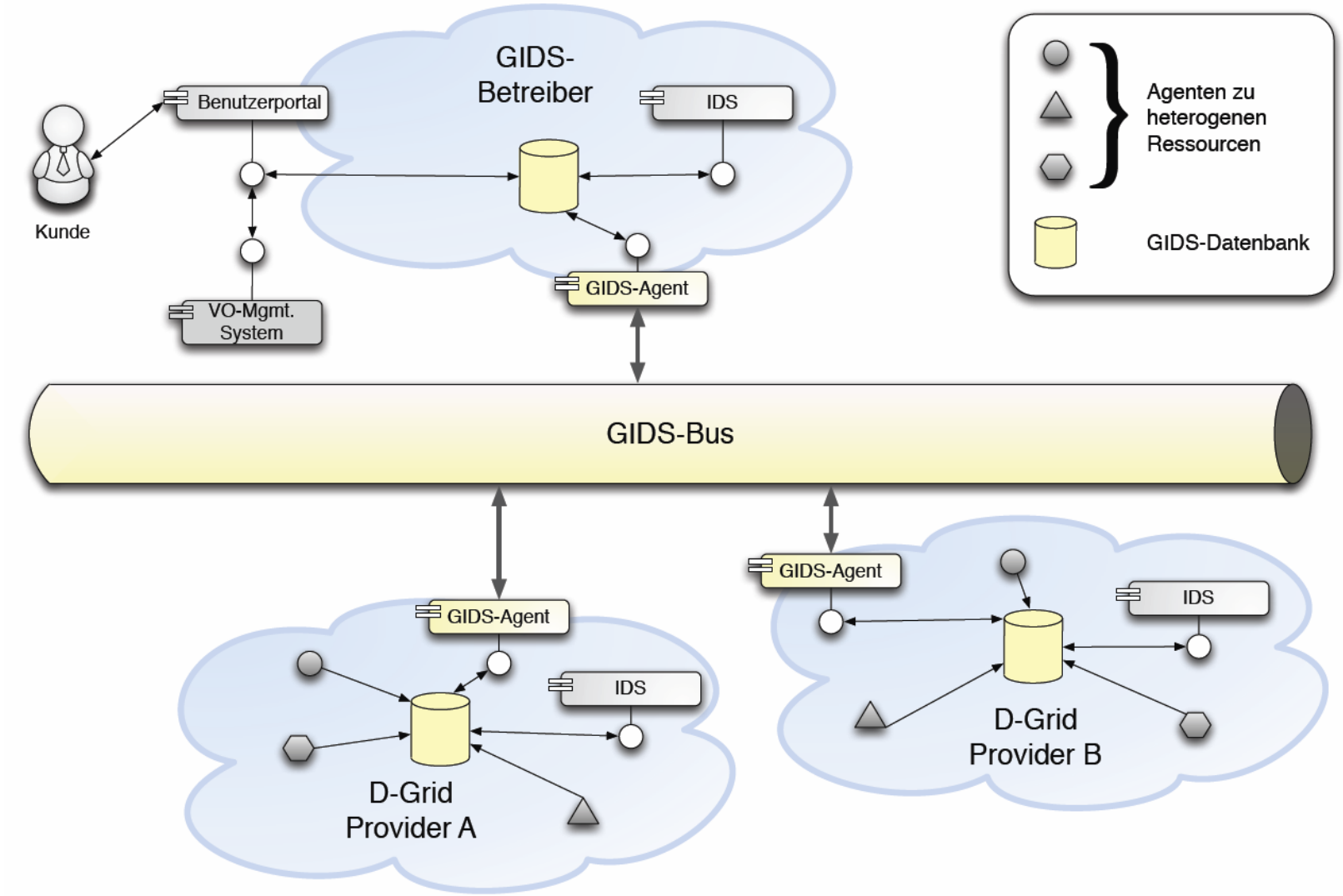
MS12: Informationsmodell und Datenaustauschformat

MS10: Architektur (Grobkonzept)

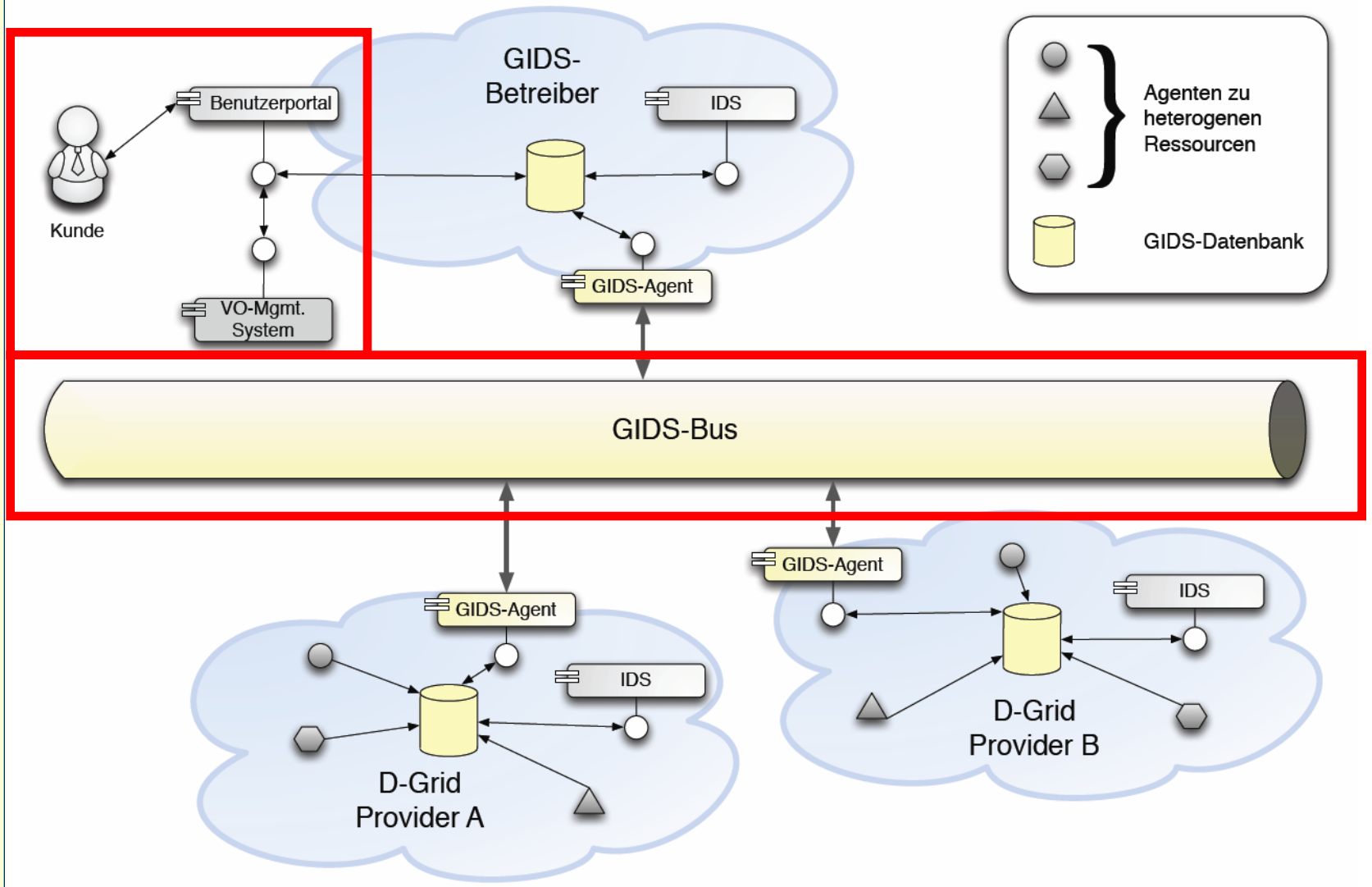
MS6: Anforderungs- und Kriterienkatalog

Alle Dokumente sind auf www.grid-ids.de zu finden

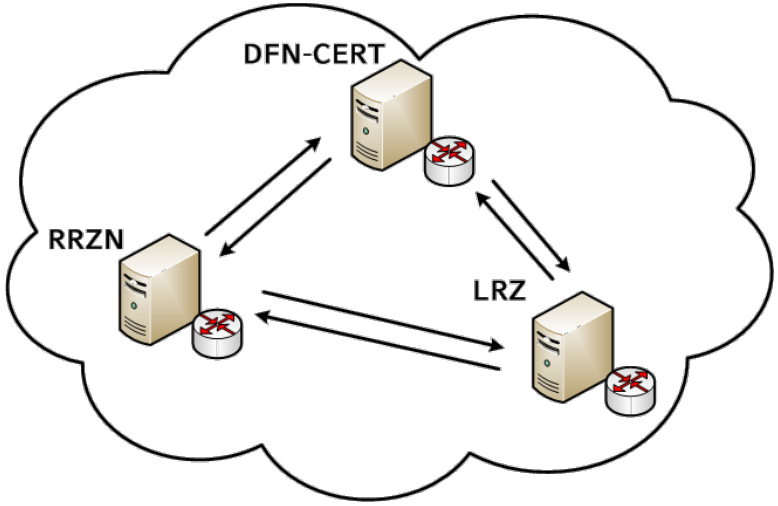
Architekturüberblick



Zugriff auf Informationen



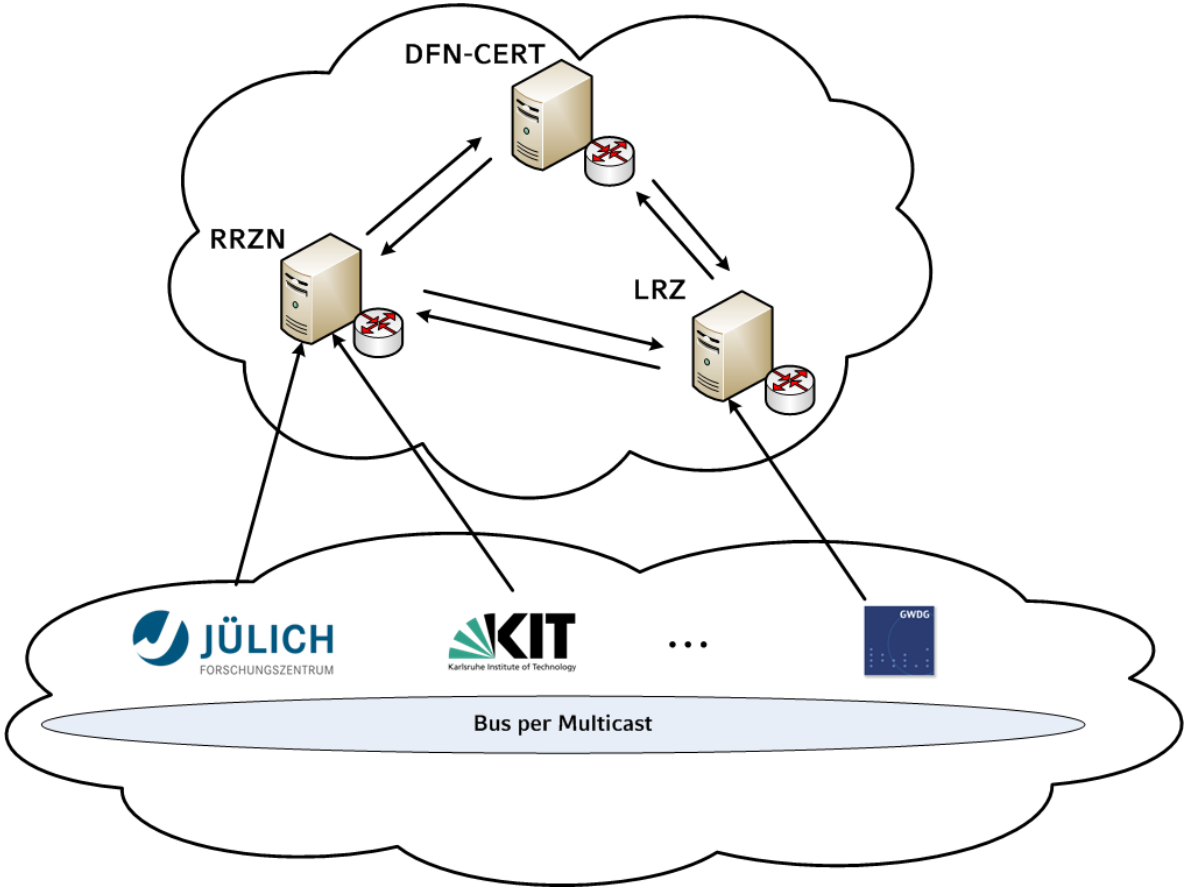
Kommunikationsinfrastruktur



Server

- VPN-Technologie: Layer-2 Tunnel
- Vollvermaschtes Backend (Spanning Tree Protocol!)
- -> EINE Broadcast-Domäne
- -> Redundanz / Ausfallsicherheit

Kommunikationsinfrastruktur

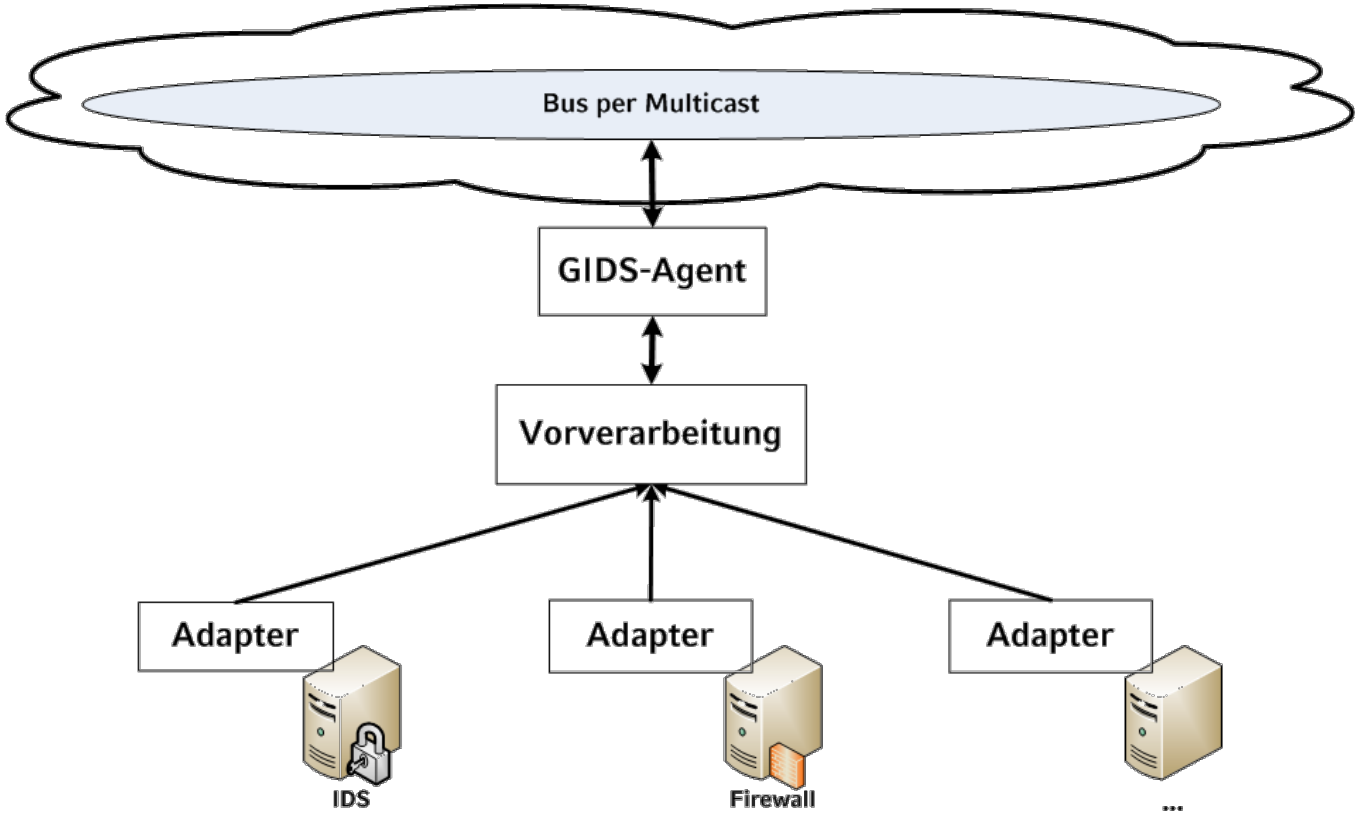


Server

Clients

- Clients kennen Server (Zugangspunkte zu GIDS-Bus)
- Keepalive-Nachrichten
- Bei Ausfall automatisches Neuverbinden mit anderem Server
- Problematisch: Theoretische Netz-Separation

Integrationsaspekte



- Provider können vorhandene Sicherheitskomponenten weiterverwenden
- Adapter übernehmen Datensammlung
  (syntaktische und semantische Nachrichtenaufbereitung)
- Vorverarbeitung: Aggregation, Korrelation, Datenschutz
- GIDS-Agent kommuniziert über Bus mit allen anderen Beteiligten

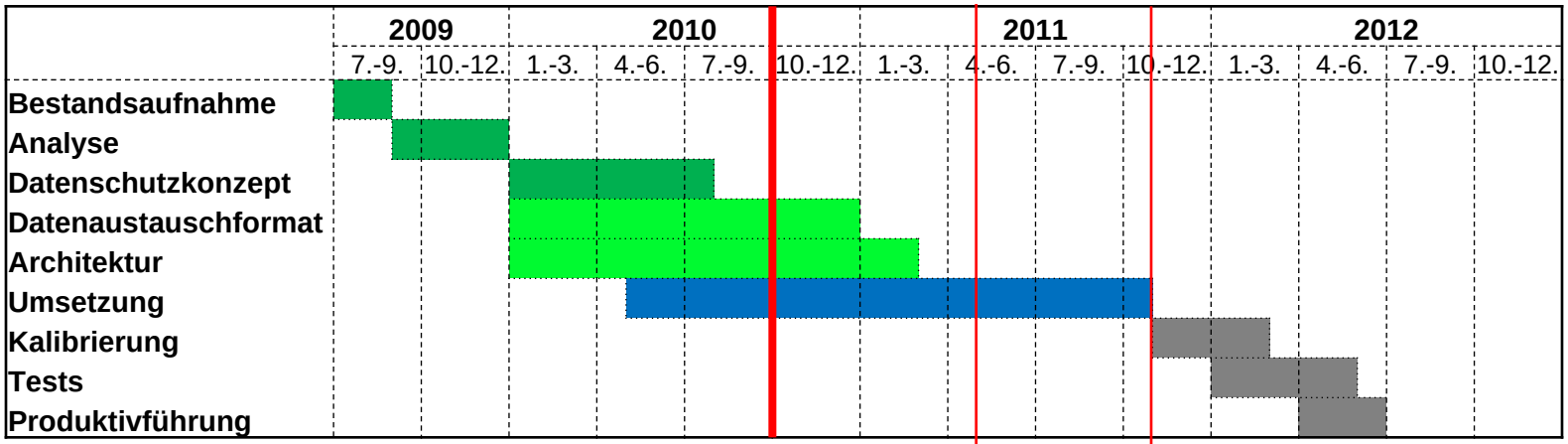
Aber: Alle Informationen preisgeben?

```
<?xml version="1.0"?>
<idmef:IDMEF-Message>
  <idmef:Alert>
    <idmef:Analyzer name="syslogd"/>
    <idmef:Classification text="SSH login attempt"/>
    <idmef:Target>
      <idmef:Node>
        <idmef:Address category="ipv4-addr">
          <idmef:address>172.16.112.20</idmef:address>
        </idmef:Address>
...
```

Datenformat: IDMEF (RFC4765)

Nächster Vortrag: Datenschutzkonzept

Upcoming Events



MS28: Prototyp des Gesamtsystems

MS22: Prototyp der GUI

Fragen?

Projektdetails:

www.grid-ids.de

Kontakt:

GIDS-Team
<gids@d-grid.de>