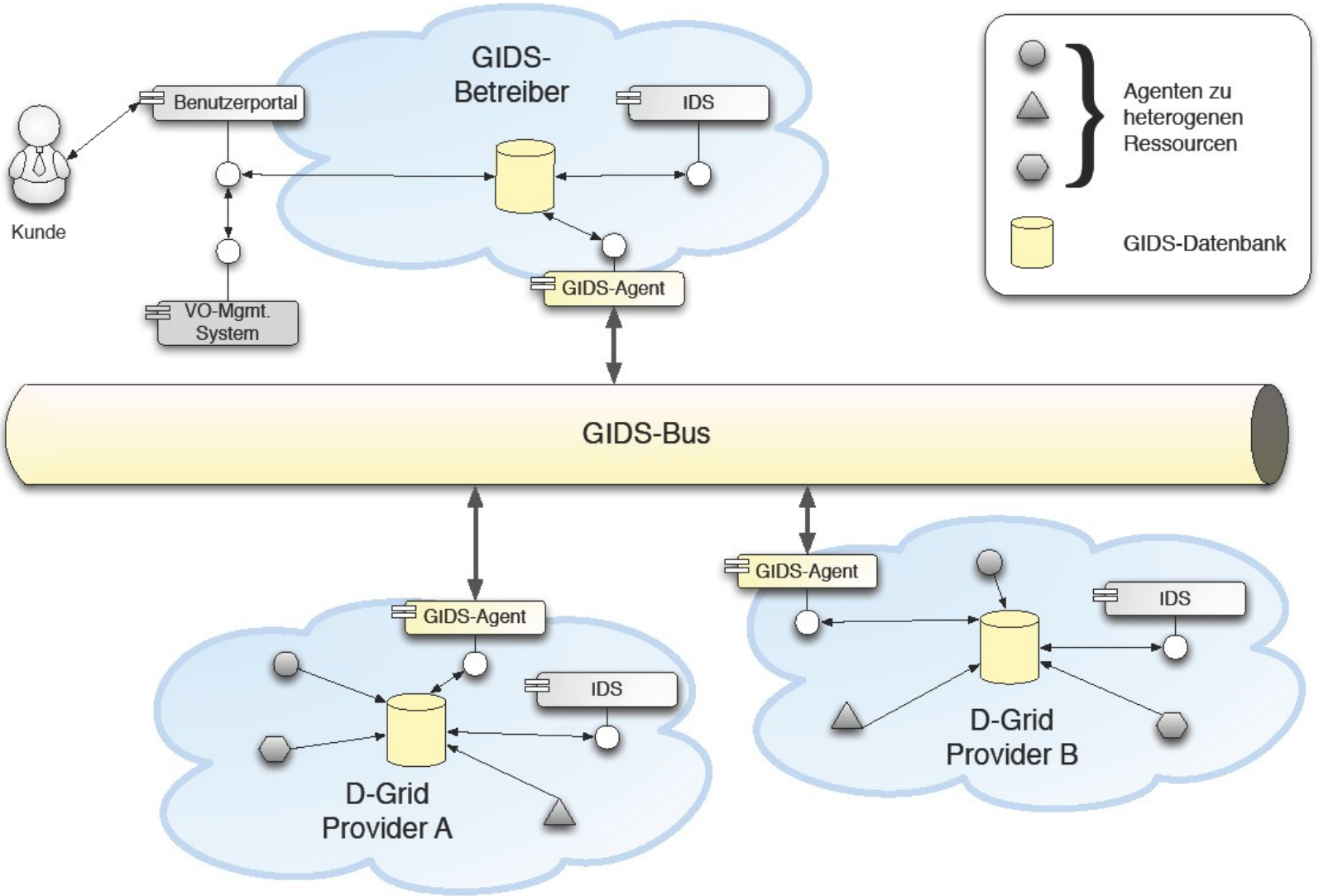
Datenschutzkonzept des GIDS-Projektes

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

Datenschutzkonzept

- Grundlage für Erhebung, Transport, Verwendung und Speicherung der Sensor- und Betriebs-Daten
- Sicherheit der Daten:
  - Vertraulichkeit und Integrität beim Transport und Speicherung
  - Weitergabe
  - Rechte des Zugriffs
- Basis:
  - Anforderungen der Rollen im GIDS
  - Rechtliche Grundlagen
  - Least-Privilege Prinzip

Architekturüberblick

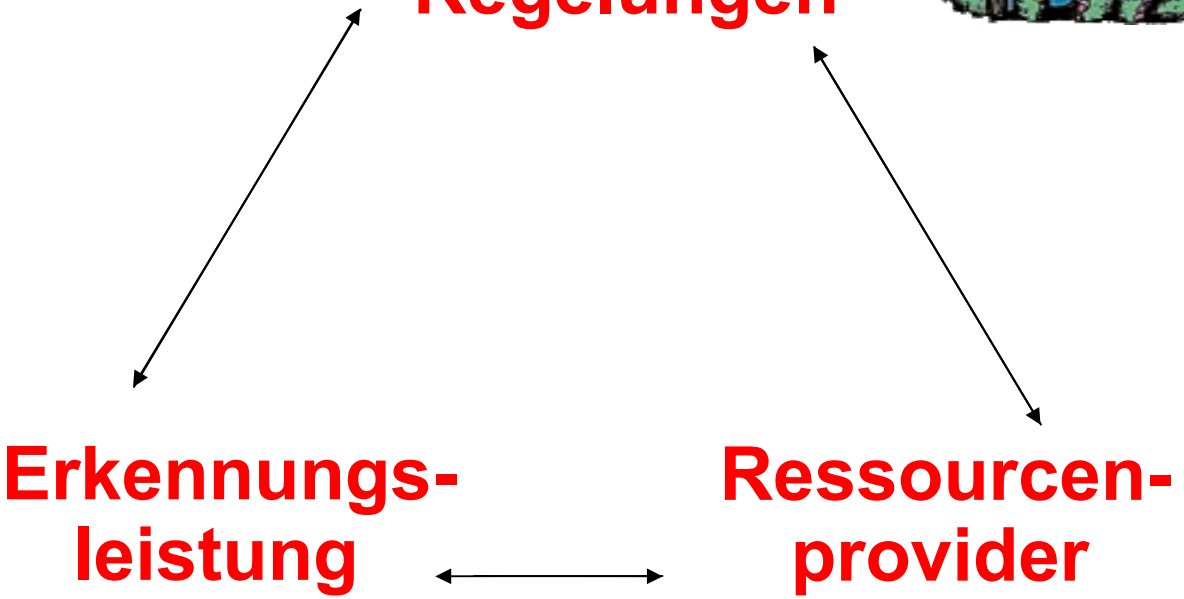


Anforderungen

- **GIDS-Betreiber und Kunden:**
  - Effektive Erkennung durch Korrelation der Daten
  - Offene Architektur
  - Verwertbarkeit der Ergebnisse
- **Ressourcenprovider:**
  - Vertraulichkeit der Daten
  - Autonomie beim Betrieb
- **Rechtliche Anforderungen:** Einhaltung des Datenschutzes
  - Rechtlich eingeschränkte Verwendung personen-gebundener Daten
  - Zweckgebundenheit
  - Sind IP-Adressen betroffen?

Herausforderung

- **Widersprüchliche Anforderungen:**



Lösung

- Kryptographische Maßnahmen
  - Pseudonymisierung und Anonymisierung personenbezogener Daten:
    - IP-Adressen (Crypto-PAn)
    - Account-/Benutzernamen
    - Pfadangaben
- Flexibilität als Design-Merkmal
  - Schnelle Reaktion auf gewachsene Anforderungen
  - Reaktion auf gesetzliche Regelungen

Lösung II

- Fokussierung auf zentrales Datenaustausch-format IDMEF
- IDMEF hat festgelegte Syntax und Semantik
- A-priori Informationen über potentiellen Personenbezug in Datenfeldern:
  - IP-Adressen
  - Account-Namen
  - Prozess- und Verzeichnisnamen
- Datenschutz ist nicht vom IDS-Sensor abhängig
- IDMEF ist Basis für das GIDS-Datenformat

Orginale IDMEF-Meldung

```
<?xml version="1.0"?>
<idmef:IDMEF-Message>
  <idmef:Alert>
    <idmef:Analyzer name="syslogd"/>
    <idmef:Classification text="SSH login attempt"/>
    <idmef:Source spoofed="unknown">
      <idmef:Node>
        <idmef:Address category="ipv4-addr">
          <idmef:address>192.168.11.12</idmef:address>
        </idmef:Address>
      </idmef:Node>
      <idmef:Service ip_version="4">
        <idmef:port>22</idmef:port>
        <idmef:protocol>TCP</idmef:protocol>
      </idmef:Service>
    </idmef:Source>
    <idmef:Target> ... </idmef:Target>
    ...
  </idmef:Alert>
</idmef:IDMEF-Message>
```

Abgeleitete GIDS-Meldung

```
<?xml version="1.0"?>
<idmef:IDMEF-Message>
  <idmef:Alert>
    <idmef:Analyzer name="syslogd"/>
    <idmef:Classification text="SSH login attempt"/>
    <idmef:Source spoofed="pseudonymized">
      <idmef:Node>
        <idmef:Address category="ipv4-addr">
          <idmef:address>1.2.3.4</idmef:address>
        </idmef:Address>
      </idmef:Node>
      <idmef:Service ip_version="4">
        <idmef:port>22</idmef:port>
        <idmef:protocol>TCP</idmef:protocol>
      </idmef:Service>
    </idmef:Source>
    <idmef:Target> ... </idmef:Target>
    ...
  </idmef:Alert>
</idmef:IDMEF-Message>
```

Fragen?

- Projekt-Homepage:
  http://www.grid-ids.de
- Kontakt:
  Jan Kohlrausch, kohlrausch@dfn-cert.de