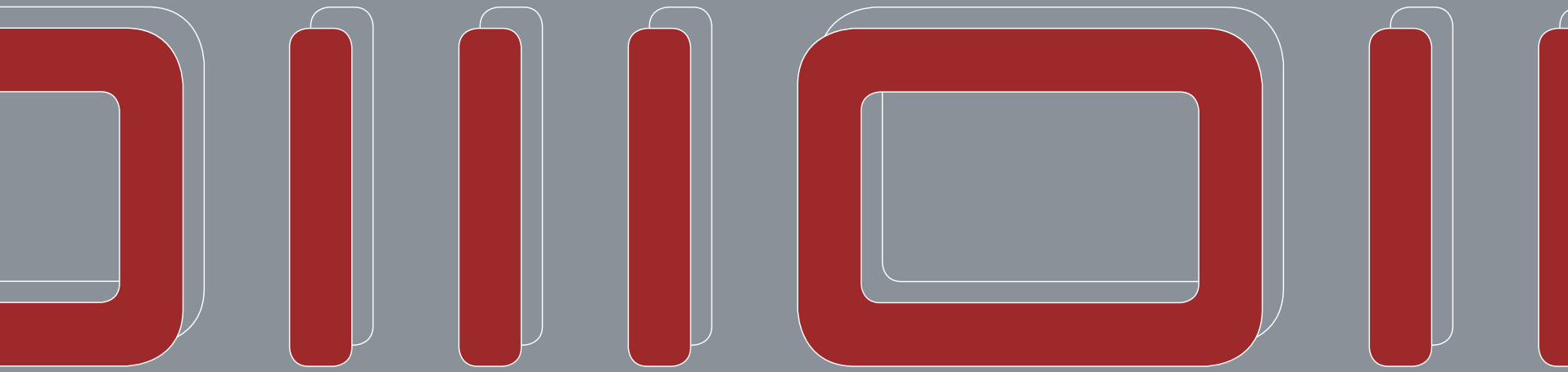


dataport

Bremen, E-Government *in medias res*, 12. Juli 2007

Internationale Standards zu Identity Management

Harald Krause

dataport

Was ist Identity-Management?

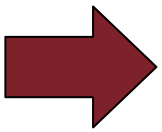
„Identity-Management in der Informationstechnologie bezeichnet die Disziplin, die sich mit der ganzheitlichen Verwaltung Digitaler Identitäten befasst.“

z.B.

- Erzeugen, Registrieren, Ändern und Löschen
- Zuordnen von Rollen, Rechten und Eigenschaften
- Bereitstellen und Verteilen
- Verwenden und Überprüfen

Warum Identity-Management?

- Das Denken bei Wirtschaft und Öffentlicher Verwaltung erfolgt zunehmend in globalen Geschäftsprozessen.
- Geschäftsprozesse überspannen daher Organisationen, Regionen und Hoheitsbereiche.
- Durch Öffnung der Netze verschwimmen die Organisationsgrenzen.
- Der Trend zur Strukturierung der IT-Unterstützung in Service-orientierte Architekturen (SOA) erfordert neue Konzepte zur Behandlung von Identitäten.



Identity-Management in moderner, service-orientierter Form wird essentieller Infrastruktur-Baustein von E-Government!

Identity-Management besitzt zwei Dimensionen

- **Authentisierung / Authentifizierung**
  - Nachweisen bzw. Überprüfen der Identität
  - Entspricht die behauptete Identität (z.B. im Login) der
  - Grundlagen sind:
    - Kenntnis eines Geheimnisses (z.B. Password, PIN)
    - Besitz (z.B. Smartcard, Token)
    - biometrische Eigenschaften (z.B. Fingerabdruck, Iris)

Technologien sind weitgehend etabliert

- **Autorisierung**
  - Einräumen von Rechten anhand der festgestellten Identität und Rolle
  - Wer darf auf welche Ressource zugreifen?
  - Grundlagen sind:
    - Identität
    - Rolle und Funktion
    - Kontext
    - Stärke der Authentisierung

Komplexität nimmt stetig zu

Autorisierung früher, heute und morgen

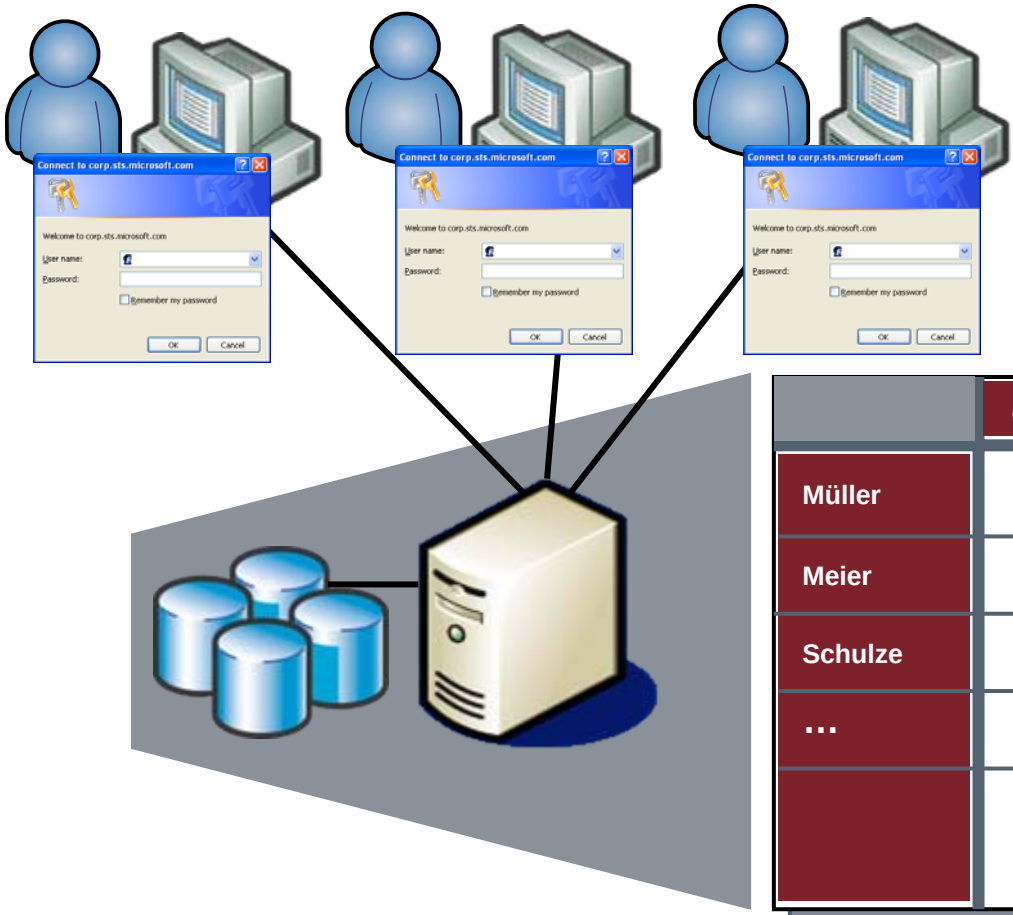
Blick zurück:

- Applikationen verwalten Nutzer und Rechte selbst.
- Jede Applikation erfordert eigene Authentisierung (Login).
- Applikationen kennen Nutzer nur innerhalb eines Kontextes.
  (keine *shared services*)
- Nutzer sind in vielen Datenbanken oder Verzeichnissen vertreten.
- Nutzerverzeichnisse sind untereinander abgeschottet („Silos“).

Klassische Autorisierung bei Client/Server

	darf dies	darf das	...
Müller	✓		✓
Meier	✓	✓	
Schulze		✓	
...	✓		

Klassische Autorisierung bei Client/Server



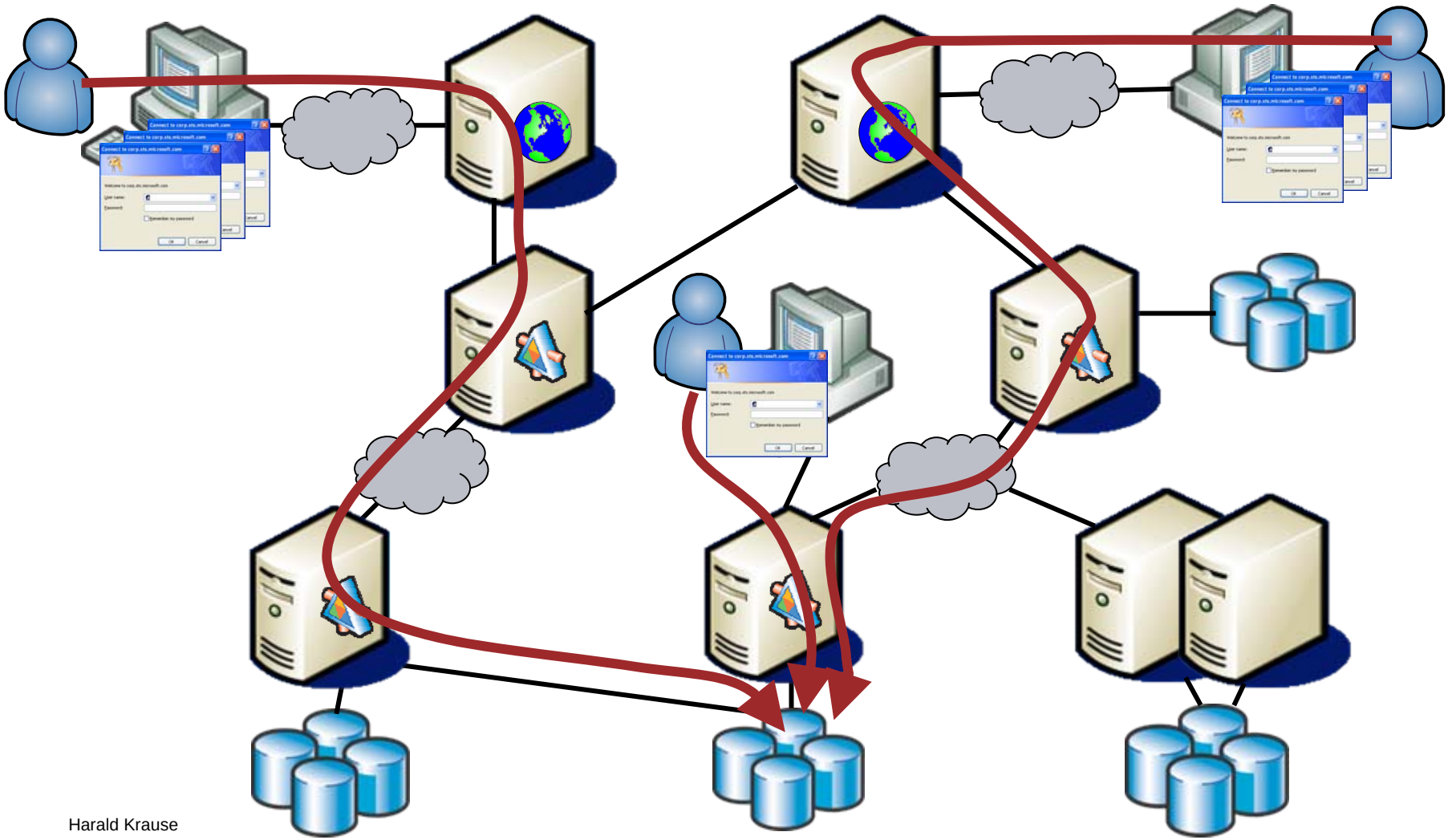
	darf dies	darf das	…
Müller	✓		✓
Meier	✓	✓	
Schulze		✓	
…	✓		

Autorisierung früher, heute und morgen

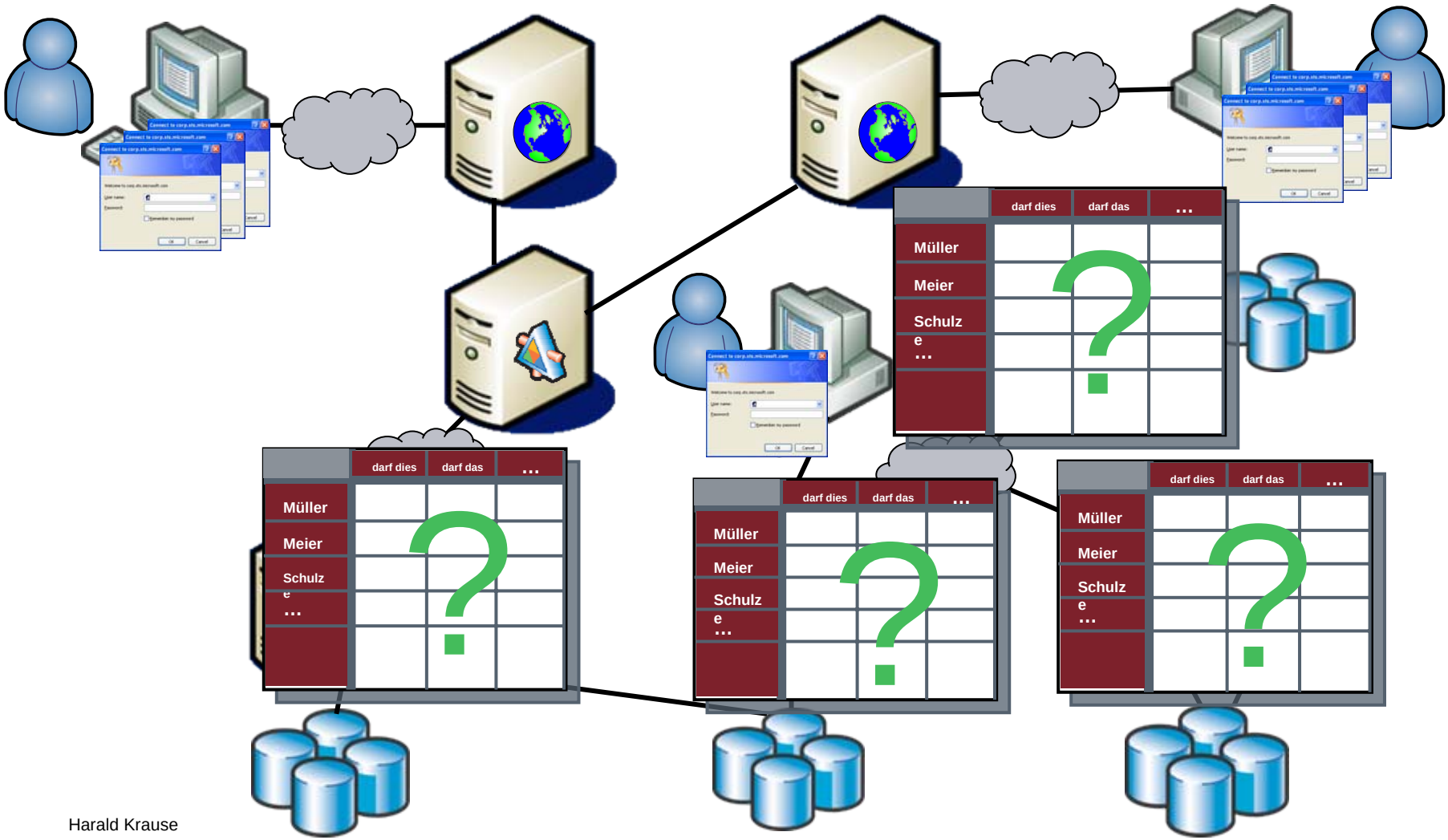
Blick nach vorn:

- Applikationen stützen sich auf virtuelle, verteilte Services.
- Ganze Prozessketten werden unterstützt.
- Nutzer können Services in unterschiedlichen Kontexten verwenden. (z.B. Sollstellung in SAP aus verschiedenen Fachverfahren)
- Autorisierungsentscheidungen können sich nicht immer auf die Identität stützen (Service kann nicht immer alle Nutzer „kennen“).

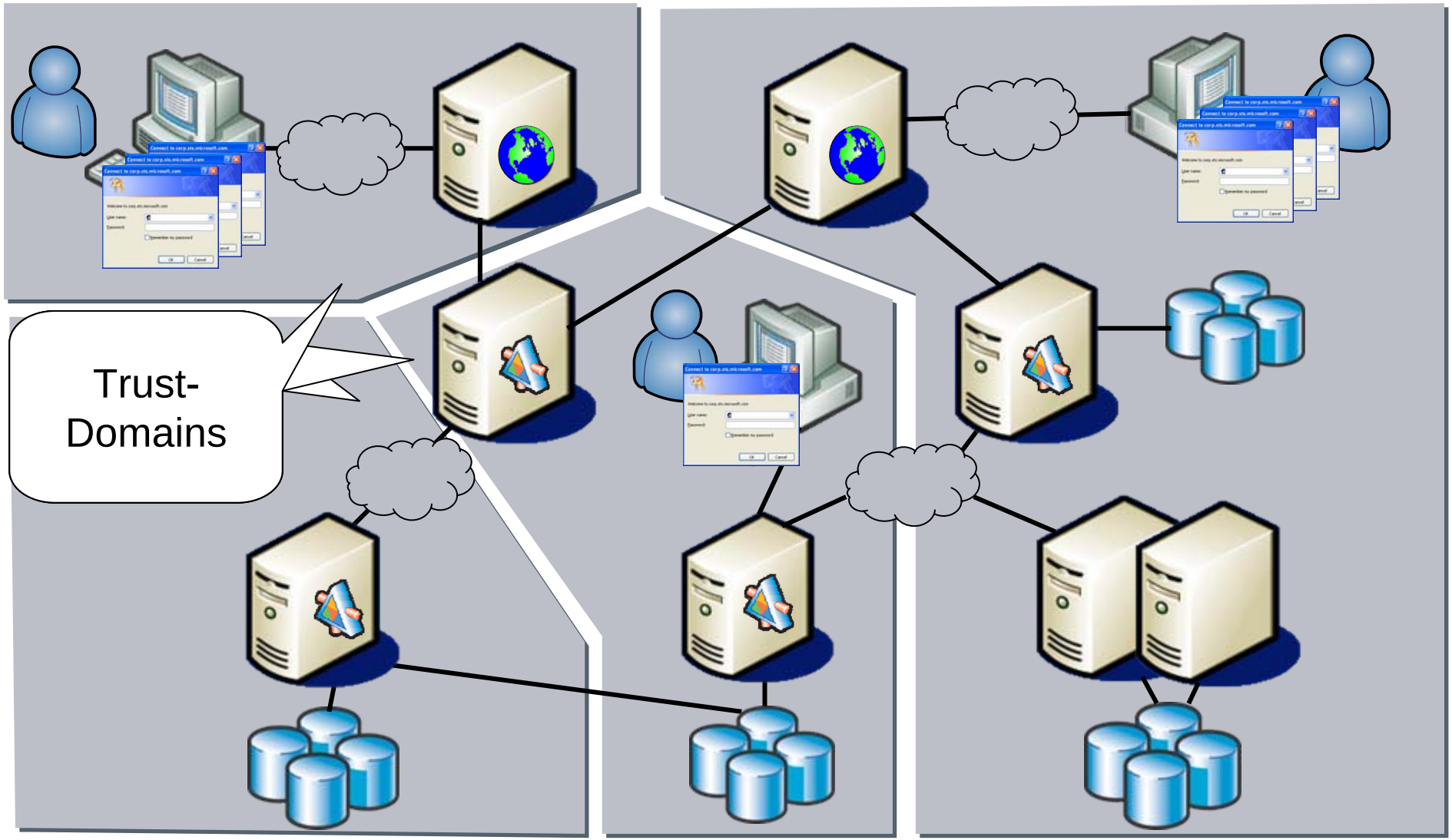
Autorisierung bei SOA (serviceorientierten Architekturen)



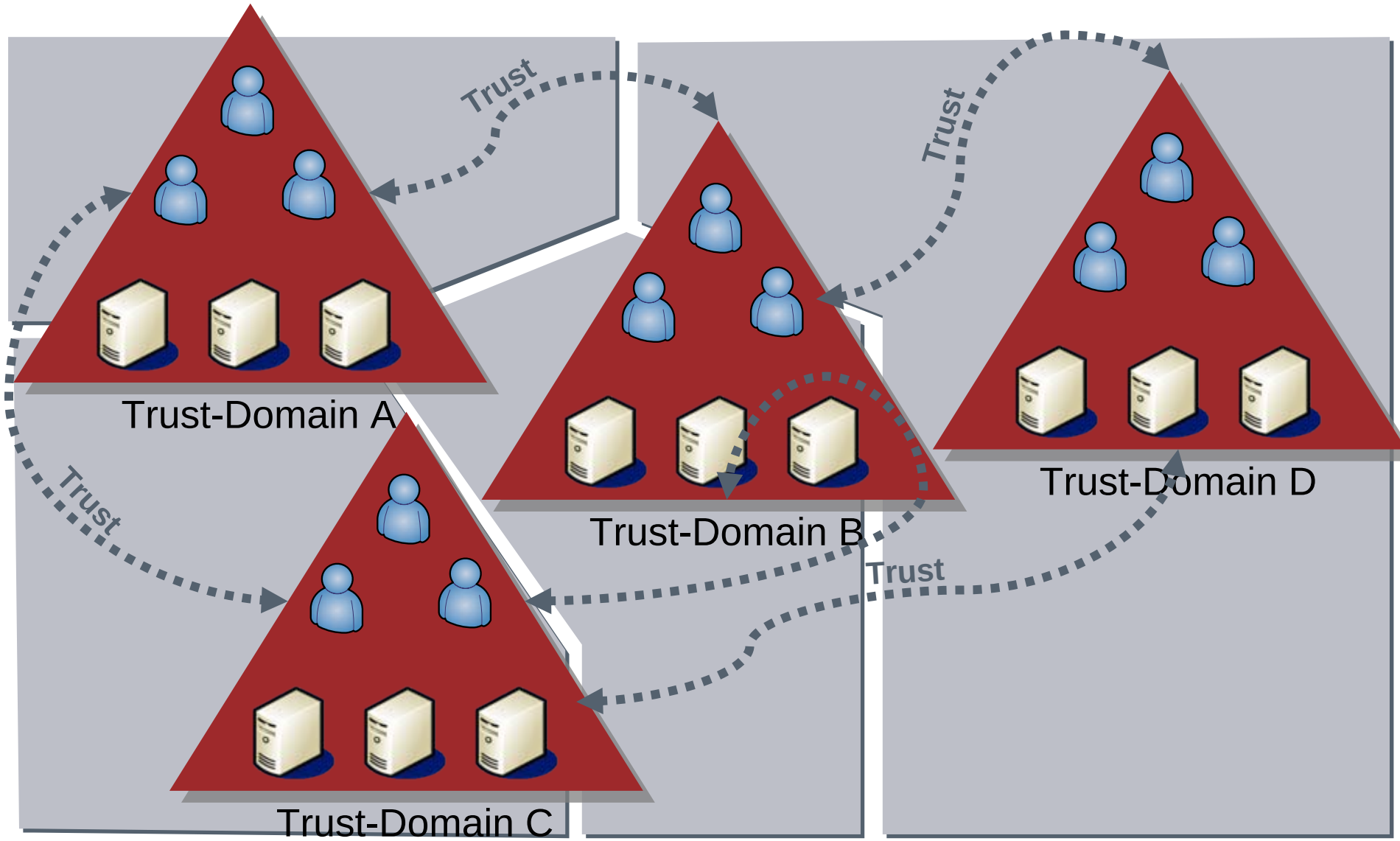
Autorisierung bei SOA (serviceorientierten Architekturen)



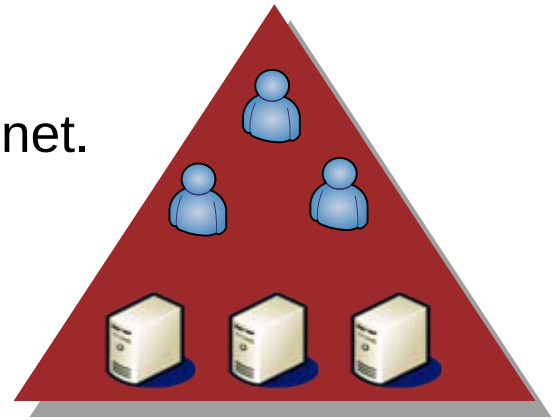
Autorisierung bei SOA (serviceorientierten Architekturen)



Lösungsansatz: Strukturierung in Trust-Domains



Trust-Domains und „Identity as a Service“



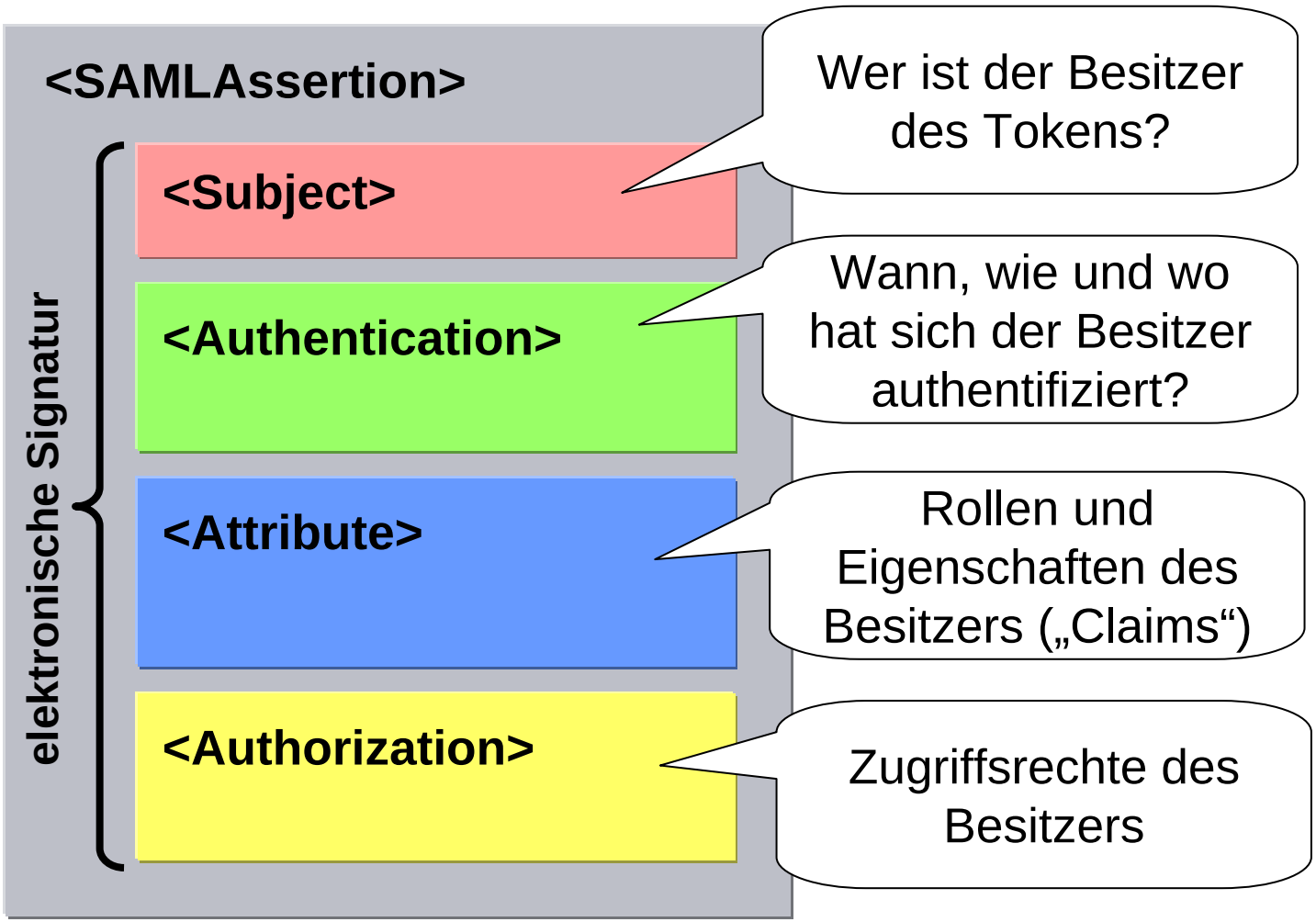
- Trust-Domains sind Nutzer und Services zugeordnet.
- Die Trust-Domain verantwortet
  - Registrierungsprozess
  - Authentifizierung
  - Zuordnung von Rollen, Rechten und Eigenschaften
- Trust-Domains können differenzierte Vertrauensbeziehungen untereinander definieren (direkt und indirekt).
- Eine Vertrauensbeziehung zwischen Services und Nutzer wird durch spezielle Services etabliert.
  (innerhalb einer Trust-Domain oder zischen Trust-Domains)

- **Wichtigster Service**: *Identity-Provider* (IdP)

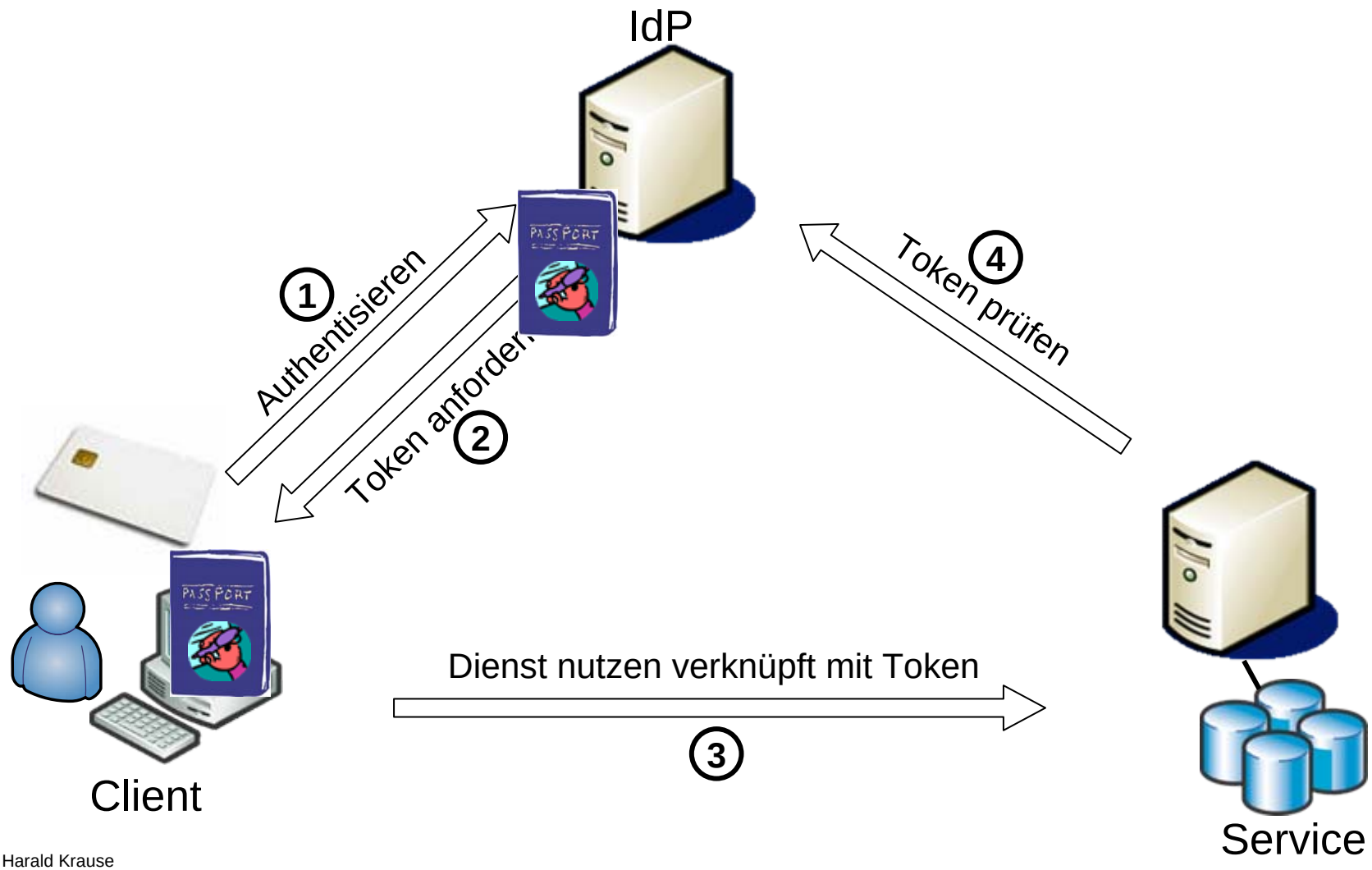
Identity as a Service: Identity-Provider (IdP)

- IdP repräsentiert Trust-Domain.
- IdP ist Instanz, die Service-Anbietern (der eigenen oder fremden Domain) folgendes in einem Token bescheinigt:
  - dass ein Nutzer sich korrekt authentifiziert hat
  - wie der Nutzer sich authentifiziert hat (Stärke)
  - welche Rollen und Eigenschaften dem Nutzer zugeordnet sind
  - welche Rechte ein Nutzer besitzt
- Diese Token sind kurzlebig, d.h. sie werden i.d.R. für nur eine Dienstnutzung ausgestellt.
- Die Token werden vom IdP elektronisch signiert.

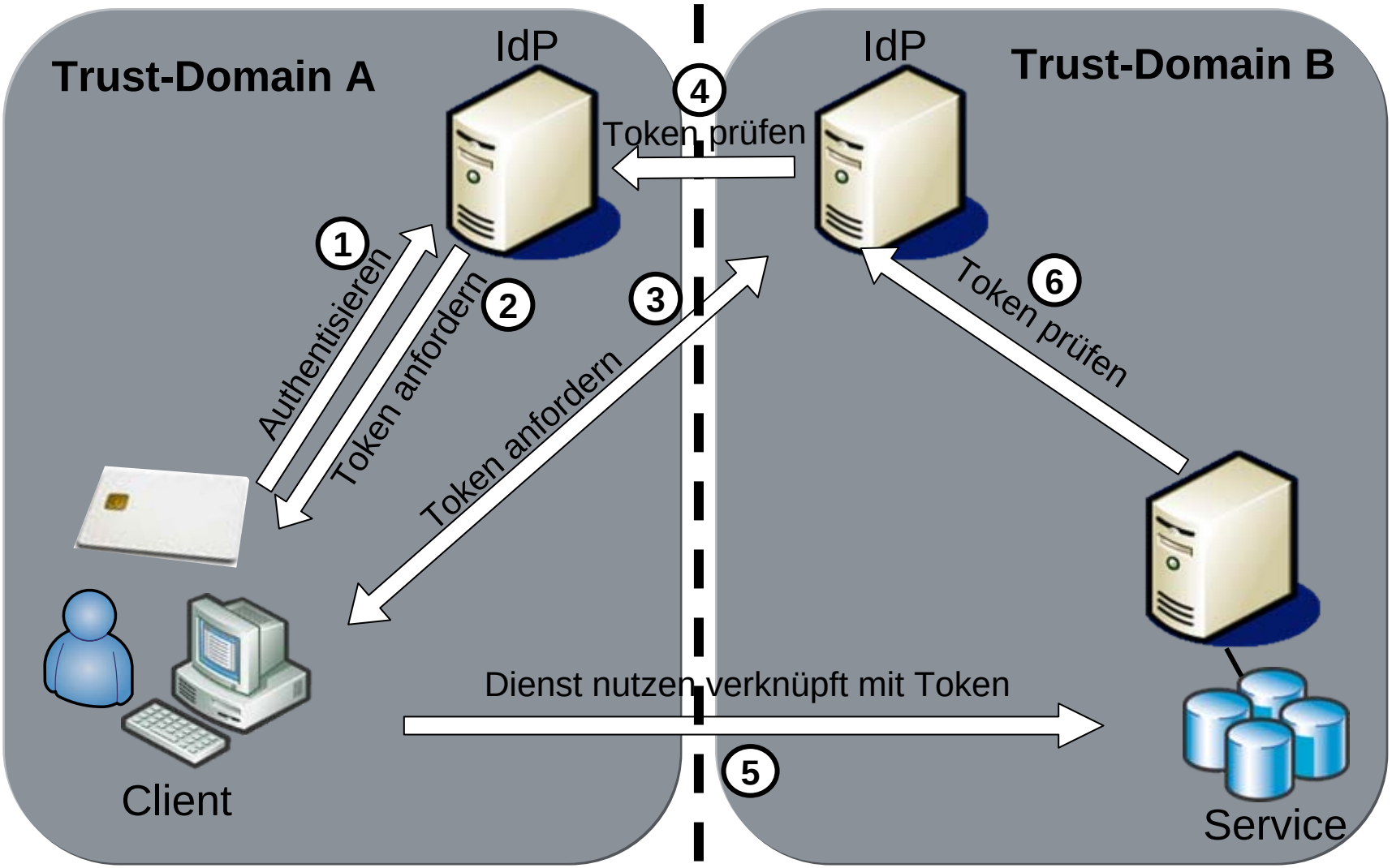
Token vom Identity-Provider (IdP)



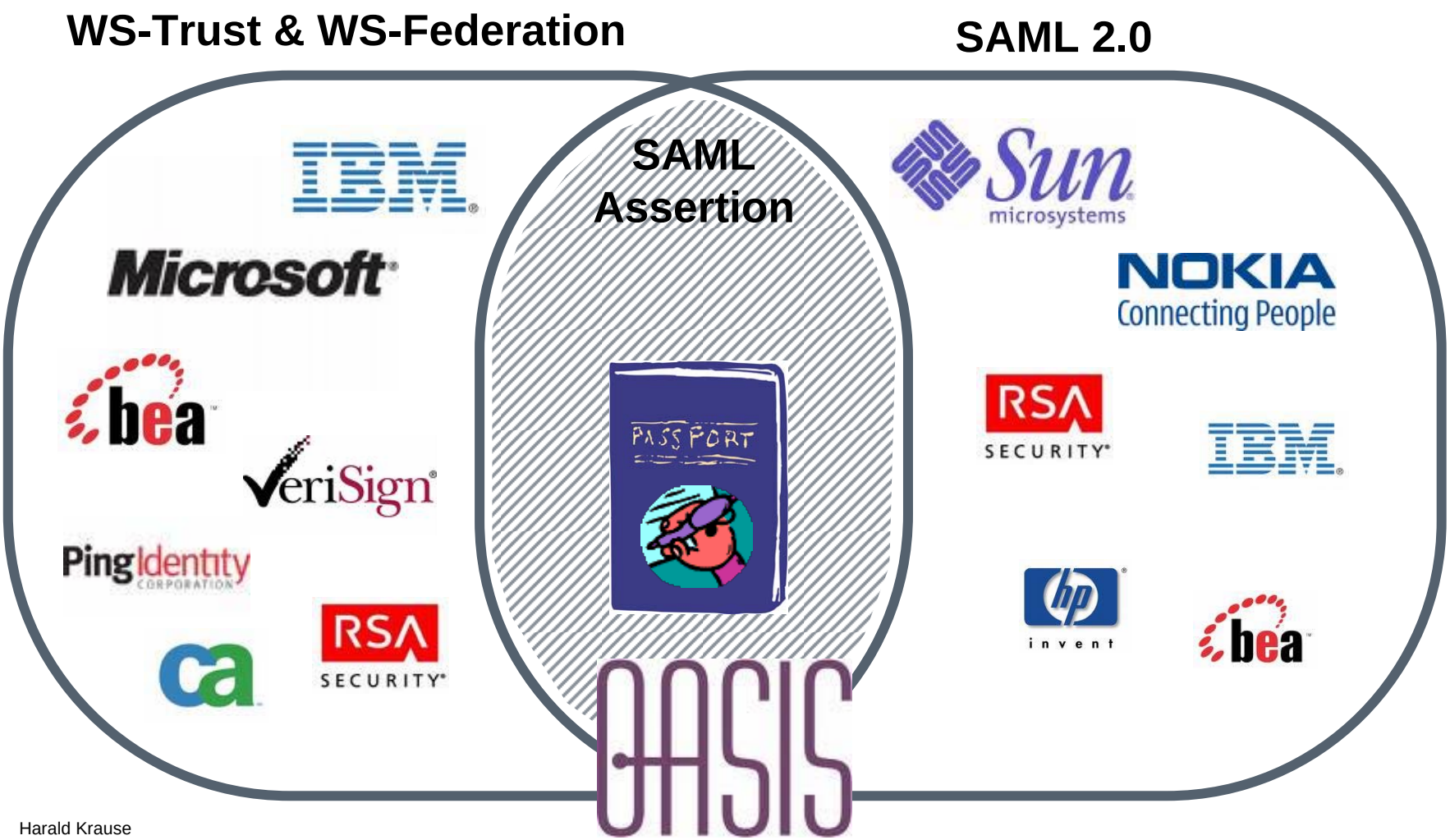
Identity as a Service: Identity-Provider (IdP)



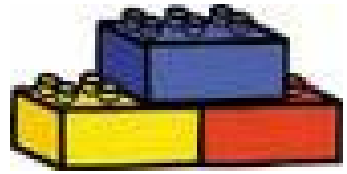
Identity Federation mittels Identity-Provider

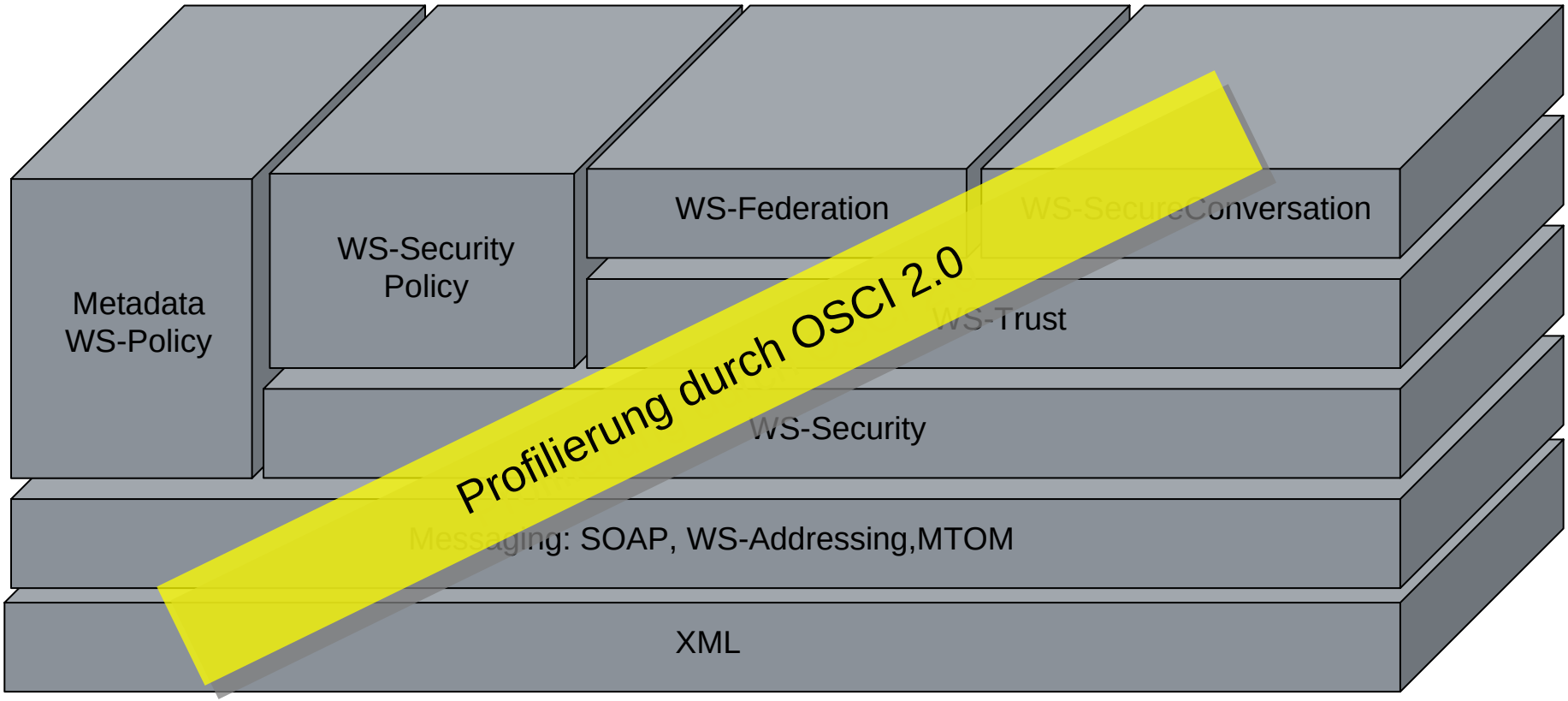


Standards zu Identity-Management



Standards zu Identity-Management





Vielen Dank für Ihre Aufmerksamkeit!

dataport