Hochschule RheinMain

NAMEN UND VERZEICHNISDIENSTE

Verteilte Systeme

Prof. Dr. Georg Hinkel
21.06.2024

GLIEDERUNG

Hochschule RheinMain

Datum	Vorlesung	Übungsblatt	Abgabe
19.04.2024	Einführung	HamsterLib	06.05.2024
26.04.2024	Netzwerkprogrammierung	Theorie	
03.05.2024	World Wide Web	HamsterRPC 1	20.05.2024
10.05.2024	Remote Procedure Calls	Theorie	
17.05.2024	Webservices	HamsterRPC 2	03.06.2024
24.05.2024	Fehlertolerante Systeme	Theorie	
31.05.2024	Transportsicherheit	HamsterREST	17.06.2024
07.06.2024	Architekturen für Verteilte Systeme	Theorie	
14.06.2024	Internet der Dinge	HamsterIoT	01.07.2024
21.06.2024	Namen- und Verzeichnisdienste	Theorie	
28.06.2024	Authentifikation im Web	HamsterAuth	15.07.2024
05.07.2024	Infrastruktur für Verteilte Systeme	Theorie	
12.07.2024	Wrap-Up	HamsterCluster (Bonus)	16.08.2024

AGENDA UND LERNZIELE

Hochschule RheinMain

Agenda

- Namen und Adressen
- Namens-/Verzeichnisdienste
- Zeroconf
- LDAP Verzeichnisdienst
- OPC UA

Lernziele

- Begrifflichkeiten erklären können
- Zeroconf erklären können
- LDAP erklären können
- Verwendung von OPC UA erklären können

EINFÜHRUNG

Hochschule RheinMain

- Numerische Identifier und Adressen sind für Menschen schwer zu merken (e.g. IP-Adressen)
- Adressen können sich ändern
  - Migration von Servern
  - DHCP
- Grundsätzliche Frage: Wie kommt man von einem Namen zu einer Adresse?

NAMEN

Hochschule RheinMain

- Namen werden genutzt, um Objekte zu identifizieren
  - Ressource
  - Objekt
  - Dienst
- Name ist Bitstring oder Zeichenfolge
- Binding: Prozess, der Namen an Objekt bindet
- Eigenschaften von Namen
  - *unique*: Name ist eindeutig
  - *pure*/*rein*: Name ist nur Bitmuster, enthält keine weiteren Informationen
  - *impure*/*unrein*: Name impliziert zusätzliche Informationen über Objekt

BEISPIELE

Hochschule RheinMain

- unique
  - „Erika Mustermann“ ist im Allgemeinen nicht unique
    - In Deutschland zählen erst Name, Geburtstag und Geburtsort als eindeutig
  - UUID (Universally Unique Identifier) sind unique
    - Auch als Global Unique Identifier (GUID) bezeichnet
    - 128 Bit-Zahl
    - Spezifiziert in RFC 4122 / ISO/IEC 9834-8:2005
    - Beispiel: 123e4567-e89b-12d3-a456-426614174000
- pure
  - UUIDs als Namen (bspw. von DCOM-Objekten) sind *pure*
- impure
  - Domain-Namen implizieren oft zusätzliche Funktionalität
    - z.B. mail.hs-rm.de

NAMENSRÄUME

Hochschule RheinMain

- Bedeutung eines Namens abhängig vom Kontext

- Strukturierung von Namen in Namensräumen
  - Geben Struktur der Namen vor
  - Meist hierarchischer Aufbau
  - Beispiele: Namespaces in C++/C#, DNS, ISBN, …

ADRESSEN

Hochschule RheinMain

- Adressen sind Attribute von Objekten, die genutzt werden können, um mit dem Objekt zu interagieren
  - Straße, Hausnr., Ort
  - Telefonnummer
  - IP-Adresse, Port
  - Speicheradresse

  } Adresse eines Objekts i.d.R. nicht eindeutig aber oft ausreichend, um Objekt zu identifizieren

- Vorteile bei der Nutzung von Namen
  - Ortsunabhängig
  - Leichter zu merken
  - Eindeutig(er)
  - Abstraktion von Protokollart und –details

- Grenze zwischen Namen und Adressen ist fließend
  - Ist https://www.hs-rm.de Name oder Adresse?

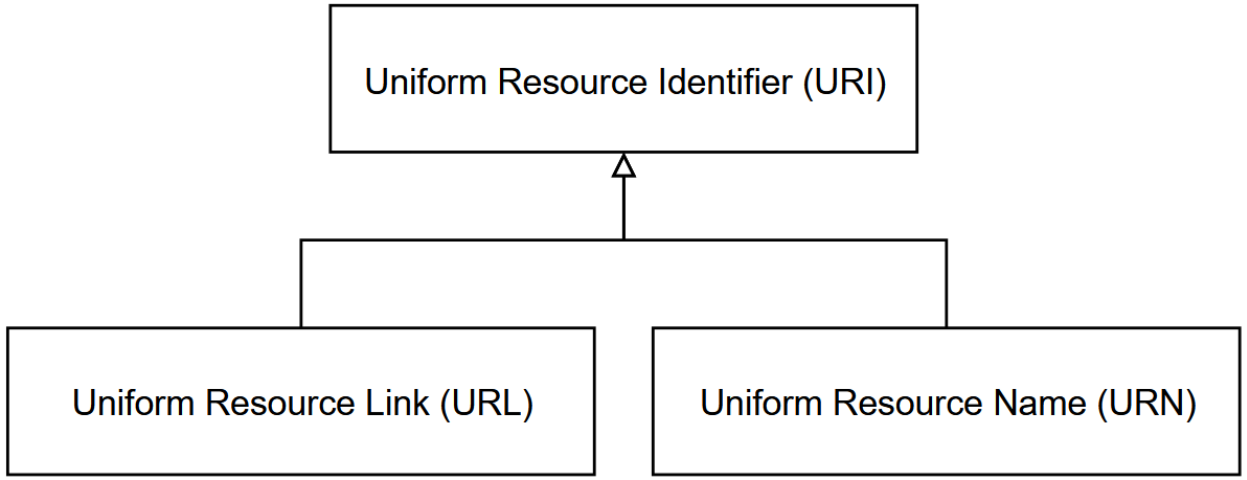
UNIFORM RESOURCE IDENTIFIER (URI)

Hochschule RheinMain

- Zeichenkette, die eine Ressource einheitlich darstellt
  - Nur ASCII-Zeichen, keine Leerzeichen, keine Kontrollzeichen

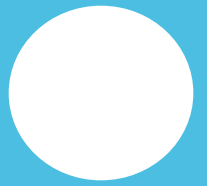
- <schema>:<Aufbau von Schema vorgegeben>
  - https://www.hs-rm.de
  - file:///d/lehre/verteilte%20systeme/
  - about:blank
  - urn:isbn:978-1543057386

- URL ➔ Schema definiert Zugriff
- URN ➔ Eindeutiger Name



Hochschule RheinMain

SIND URIS UNIQUE?



URI-SCHEMATA SIND NAMENSRÄUME

Hochschule RheinMain

- URI-Schema kann frei gewählt werden
  - Definiert Namensraum
  - Definiert Reinheit der Namen (oder ob als Adresse nutzbar)
  - Syntaxregeln für Namen werden durch URI-Schema vorgegeben
  - Erlaubt URI-Schema für spezifische Anwendung

- Betriebssysteme verwalten Standardanwendungen pro URI-Schema
  - HTTP, HTTPS: Browser
  - Mailto: E-Mail Client
  - …

  ➔ Nutzung von URIs zur Kommunikation zwischen Anwendungen auf einem System

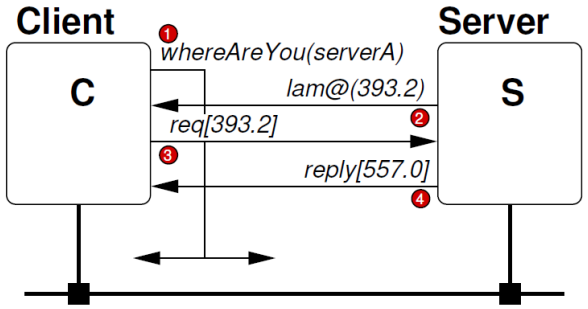
VERZEICHNISDIENSTE

Hochschule RheinMain

- Suche Objekte anhand bestimmter Eigenschaften
  - Analogie: Gelbe Seiten
  - Namensdienste: Suche Adressen anhand von Namen (Namensauflösung) ➔ Telefonbuch

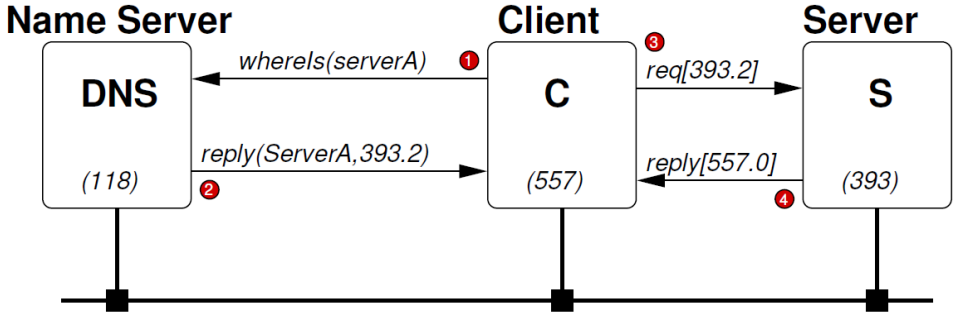
Suche durch Broadcast

- Anfrage wird an alle Einheiten geschickt; nur betreffende Einheit antwortet
- Keine Konfiguration notwendig
- Skaliert schlecht
- Beispiel: Multicast-DNS (Zeroconf)



Dedizierter Server

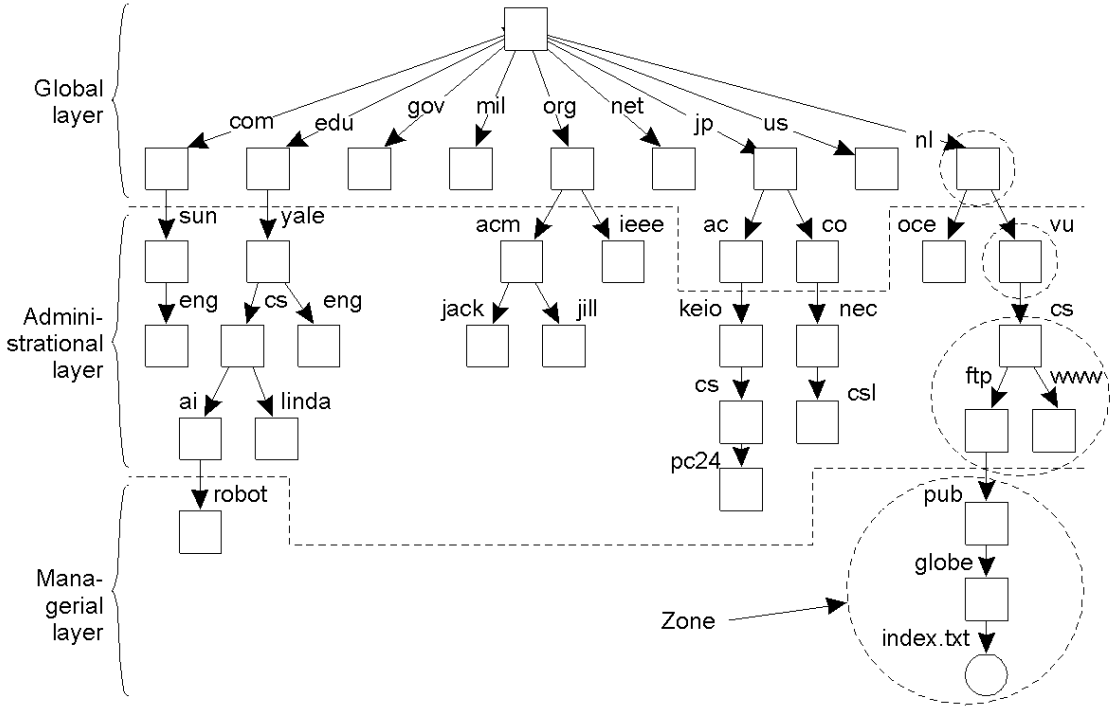
- Dedizierter Server hält Zuordnung von Eigenschaften
  - Namensdienst ➔ Name Server
- Benötigt Wissen über Adresse des Servers
- Beispiel: DNS, LDAP



DOMAIN NAME SERVICE (DNS)

Wiederholung aus Rechnernetze

Hochschule RheinMain



[Bild: Tanenbaum, van Steen: Verteilte Systeme]

- Dedizierte Name-Server lösen Domain-Namen zu IP-Adressen auf
- Hierarchischer Namensraum, aufgeteilt in verschiedene Schichten
  - Global Layer: Einstiegspunkt, verwaltet von IANA und beauftragten Gesellschaften
  - Administrational Layer: Verwaltet von einzelnen Organisationen
  - Managerial Layer: Individuell verwaltet

ZERO-CONFIGURATION (ZEROCONF)
Überblick

Hochschule RheinMain

- Problem: Konfiguration von Kommunikationspartnern in kaum/nicht administrierten Netzwerken (e.g. Heimnetzwerke)
  - IP-Adressen typischerweise dynamisch per DHCP vergeben
- IETF Arbeitsgruppe 1999-2004 (ergebnislos beendet mangels Konsens)
  - Aber verbreitete Implementierungen: Apple Bonjeur, Avahi
  - Heute trotzdem weite Verbreitung
- Multicast-DNS (mDNS): Regeln für DNS-Aufruf im lokalen Netzwerk
  - Top-Level-Domain .local ist link-lokal
  - Andere Namensteile sind pro Anwendung frei wählbar
  - Versand der Pakete per UDP Multicast (Broadcast)
- DNS Service Discovery (DNS-SD): Registrierung der Services

ZERO-CONFIGURATION (ZEROCONF)
Ablauf

Hochschule RheinMain

1. Client schickt Anfrage mit Service-Typ an alle Parteien im Netzwerk
   - Service-Typen wurden von IANA verwaltet, jedoch nicht weiter gepflegt
   - Service-Typen können Zusatzinformationen oder Adressangaben implizieren
   - Beispiel: _ipp._tcp (Internet Printing Protocol über Bonjeur)

2. Server antwortet mit Beschreibung

PTR	Namen des Service (verpflichtend)
SRV	Port (falls nicht per Protokoll definiert oder abweichend)
A	IPv4-Adresse
AAAA	IPv6-Adresse
TXT	Zusatzinformationen als Key-Value-Paare (bspw. Druckermodell)

3. Client kann weitere Adressinformationen anfordern (optional)

4. Client nimmt Verbindung über eigentliches Protokoll auf, Adresse jetzt bekannt

ZERO-CONFIGURATION (ZEROCONF)
Beispiele

Hochschule RheinMain

- Netzwerkdrucker
- Apple-Produkte (Safari, iChat, Messages, …)
- Laborgeräte (SiLA2)

LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

Hochschule RheinMain

- Entstanden aus X.500 Standard basierend auf Directory Access Protocol
  - zu komplex, keine Implementierung
  - LDAP ist Vereinfachung, aktuell Version 3 (RFC 4511)

- Hierarchischer Namensraum: Directory Information Tree (DIT)
  - Einträge sind beliebige Objekte
  - Objekte sind Menge von <Attribut,Wert>-Paaren, gehören zu mindestens einer Klasse
  - Klassen definieren Attributmengen und Wertmengen, Vererbung möglich
  - Vordefinierte Klassen (e.g. für Person, Organisation)
  - Anwendungsspezifisch erweiterbar

- Verwendung typischerweise um auf unternehmensinterne Nutzerverwaltung zuzugreifen
  - Identifikation des Servers mit dem Protokoll ➔ LDAP-Server

Hochschule RheinMain

WAS HAT EIN VERZEICHNISDIENST WIE X.500 MIT X.509-ZERTIFIKATEN ZU TUN?

LDAP
Bezeichnung der Objekte

Hochschule RheinMain

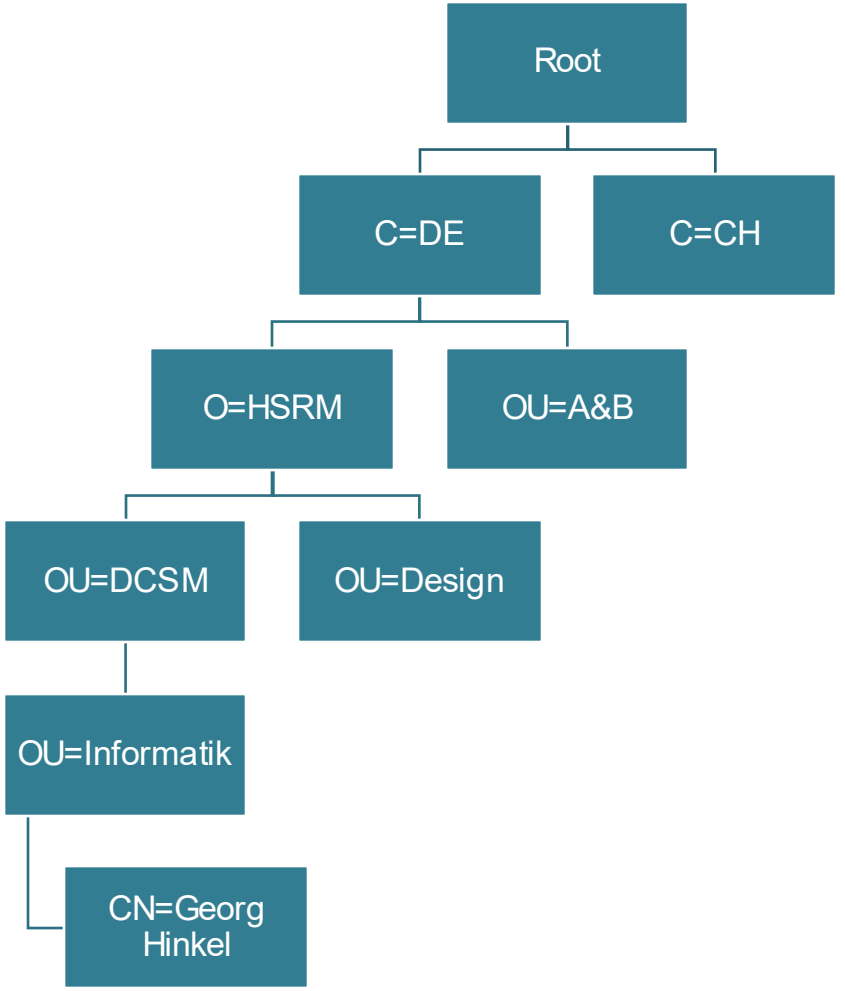
- Bezeichnung von Objekten durch relative und absolute Namen im DIT
- Repräsentieren Organsisationsstruktur

Attribut	Kürzel	Beispiel-Wert
Country	C	DE
Locality	L	Wiesbaden
Organization	O	HSRM
OrganizationalUnit	OU	DCSM
OrganizationalUnit	OU	Informatik
CommonName	CN	Georg Hinkel

LDAP
DN vs. RDN

Hochschule RheinMain

- Wurzelknoten des DIT heißt Root
- Jeder Knoten hat auf seiner Ebene eindeutigen Namen
  - Relative Distinguished Name (RDN)
- Zusammensetzung der RDNs ergibt kompletten Namen
  - Distinguished Name (DN)



LDAP
Beispiele

Hochschule RheinMain

- Typische Informationen, die unternehmensweit „im LDAP“ stehen
  - Name
  - Email-Adresse
  - Abteilung
  - Zugewiesene Rollen
  - Vorgesetzte(r)
  - Login-Informationen
  - …
- Manche Attributmengen standardisiert
  - Bspw. RFC 2798 inetOrgPerson

LDAP
Anfragen

Hochschule RheinMain

- Nutzung als Namensdienst
  - Finde Objekt bei gegebenem Namen
  - Z.B. read(/C=DE/O=HSRM/OU=DCSM/OU=Informatik/CN=Georg Hinkel)
- Nutzung für Passwortvalidierung
  - Prüfe Passwort für Nutzer mit vollständigem Namen
  - Z.B. bind(/C=DE/O=HSRM/OU=DCSM/OU=Informatik/CN=Georg Hinkel, Password=******)
- Suche von Objekten mit bestimmten Attributwerten
  - Anfragen können mehrere Ergebnisse liefern
  - Wildcards, Logische Ausdrücke in ungarischer Notation
  - Z.B. &(C=DE)(CN=*Hinkel)
- Weitere Operationen zum Hinzufügen, Ändern, Entfernen, Umbenennen von Einträgen

LDAP
Typische Anwendung: Authentifikation

Hochschule RheinMain

- Problem: Nutzende sollen sich mit Unternehmens-Account anmelden können

- Lösung: LDAP-Integration
  1. UI-Fenster für Nutzername/Email-Adresse/Mitarbeiternummer
  2. Authentifikation mit Service-Account
  3. Suche nach DN des Nutzenden
     - z.B. &(C=DE)(|(CN=<user>)(email=<user>))
  4. Authentifikation mit Account des Nutzers

LDAP
Replikation

Hochschule RheinMain

- Problem: Verzeichnisse können sehr groß werden
  - Replikation aus Gründen der Fehlertoleranz und Performance
  - Replikation kann Stunden dauern
  - Master-Slave Konfigurationen
    - Änderungen nur auf Master
    - Propagation an Slaves
- Nächstes Problem: Update-Zeiten bei Änderungen
  - Updates nicht sofort global sichtbar

LDAP
Produkte

Hochschule **RheinMain**

- OpenLDAP (Open Source)
- NetIQ eDirectory
- Microsoft Active Directory
- Atos DirX
- Oracle Directory Server
- …

OPC UNIFIED ARCHITECTURE (UA)
Einführung

Hochschule RheinMain

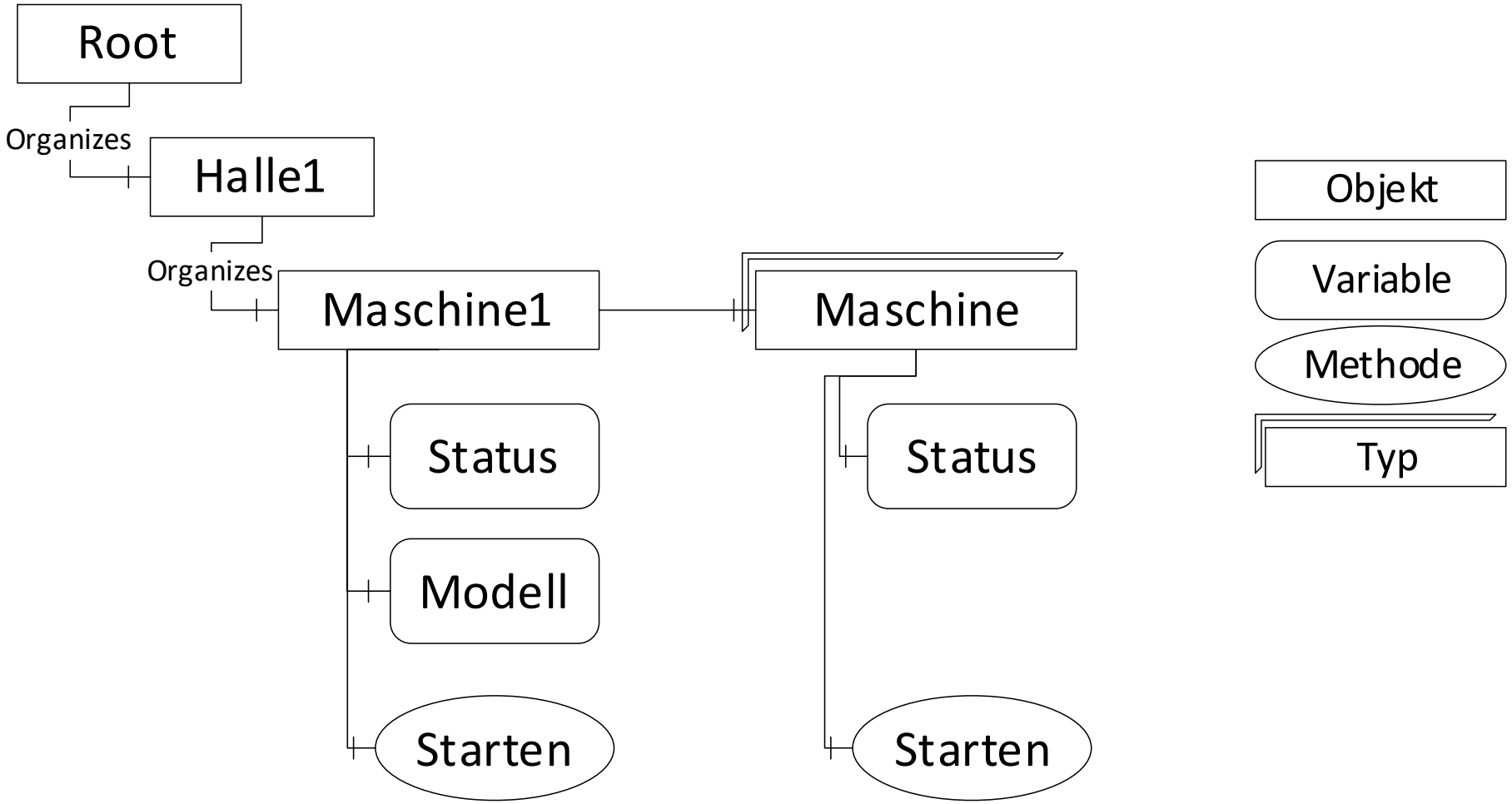
- Probleme
  - Welche Geräte/Sensoren/… existieren in einer Fabrik?

- Lösung: OPC UA (Open Platform Communications, 2006)
  - Server bestehen aus Knoten, die Ressourcen repräsentieren
  - Informationsmodell basierend auf Ontologien
    - Vom Server repräsentierte Geräte werden als Objekt-Knoten bezeichnet
    - Referenzen auf Variablen-Knoten, Methoden-Knoten, Event-Knoten (optional, können zwischen Objekten geteilt werden)
    - Typisierung durch Typ-Knoten (optional): Definiert welche anderen Knotentypen im Objekt vorhanden sein müssen
  - Transportprotokoll zum Zugriff auf Informationsmodell (binär/TCP oder Webservice)
    - Variable setzen
    - Variable abrufen
    - Methode ausführen
    - Objekt erzeugen
    - …

OPC UNIFIED ARCHITECTURE (UA)

Beispiel

Hochschule RheinMain



OPC UNIFIED ARCHITECTURE (UA)
Einsatzgebiete

Hochschule RheinMain

- Verzeichnisse von >1000 smarten Geräten (e.g. in der Produktion)
  - „Industrie 4.0“

ZUSAMMENFASSUNG

Hochschule RheinMain

- Namen als Mittel, um Ortstransparenz zu erreichen
- Namens-/Verzeichnisdienste

Verbindung	Namensdienst	Verzeichnisdienst
Broadcast	Zero-configuration networking (zeroconf)	
Zentraler Server	Domain Name System (DNS)	Lightweight Directory Access Protocol (LDAP), OPC UA

MÖGLICHE PRÜFUNGSAUFGABEN

Hochschule RheinMain

- Sind HTTP-Adressen pure? Sind sie unique?
- Bringen Sie die Abkürzungen URI, URL und URN in Zusammenhang!
- Wofür wird Zeroconf verwendet? Ist es ein Namens- oder Verzeichnisdienst?
- Welche Adresse muss ein Dienst haben, um über Zeroconf gefunden werden zu können?
- Welche Technologien könnte man für einen Verzeichnisdienst unter gegebenen Anforderungen verwenden?
- Was ist ein RDN in LDAP?
- Wie ist der grundsätzliche Aufbau, um in einer verteilten Anwendung eine Authentifikation über LDAP zu realisieren?
- Ein Unternehmen unterhält einen LDAP-Server, in dem Daten über die Mitarbeiter:innen verwaltet werden. Nun wird eine „Lisa Müller“ eingestellt, obwohl bereits eine Mitarbeiterin dieses Namens im Unternehmen arbeitet. Ist das für den LDAP-Server ein Problem? Warum nicht?