RECHTLICHE ASPEKTE DER DATENHALTUNG

von Andreas Dorfer, Sabine Laubichler

Gliederung

- Definitionen
- Rechtliche Rahmenbedingungen
- C3-Framework

Servicemodelle

- Software as a Service (SaaS)
  - salesforce.com, SAP Business ByDesign, Apple iCloud
- Platform as a Service (PaaS)
  - Google App Engine, Windows Azure
- Infrastructure as a Service (IaaS)
  - Amazon EC2, Oracle Cloud

Betriebsmodelle

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

Europäische Datenschutz-Richtlinie

7 Prinzipien:

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit und Datensparsamkeit
5. Transparenz und Betroffenenrechte
6. Datensicherheit
7. Kontrolle

Rechtliche Anforderungen (1/3)

- Personenbezogene Daten

„Alle Daten, die einen Personenbezug haben."

- Auftraggeber (Cloud-Nutzer)

„Natürliche oder juristische Personen, die allein oder gemeinsam Daten verwenden, unabhängig davon, ob sie die Daten selbst verwenden oder einen Dienstleister beauftragen."

Rechtliche Anforderungen (2/3)

- Dienstleister (Cloud-Provider)

„Natürliche oder juristische Personen, die Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwenden.“

- Datei

„Strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind.“

Rechtliche Anforderungen (3/3)

- Datenanwendung

„Summe der logisch verbundenen Verwendungsschritte, die zur Erreichung eines inhaltlich bestimmten Ergebnisses geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt erfolgen."

- Verwendung von Daten

„Jede Art der Handhabung, Verarbeitung oder Übermittlung von Daten."

Auswahl des Cloud-Anbieters (1/2)

Anforderungen an den Cloud-Anbieter:

- Organisatorische und technische Maßnahmen laut §14 DSG
  - Sicherheitskonzept muss als Leistungspflicht im Vertrag geregelt sein
  - Abstrakte, pauschalierte Beschreibungen sind unzulässig
  - Nutzer ist verpflichtet das Sicherheitskonzept vor Auslagerung der Daten zu prüfen

Auswahl des Cloud-Anbieters (2/2)

- Sichere und rechtmäßige Datenverwendung (§10 DSG)

- Gütesiegel
  - z.B. Euro Cloud Austria - Gütesiegel

Dienstleistervertrag – Gegenstand des Auftrags

- Leistung muss grob umschrieben werden
- Verweise auf verlinkte Seiten, Testseiten, etc. genügen nicht

- Personenbezogene Daten müssen mit Sorgfalt behandelt werden!

Dienstleistervertrag – Auslandssachverhalte

- Im EWR-Raum: §12 Abs 1 DSG
- In Drittstaaten: §13 DSG
- Übertragung ins Ausland genehmigungsfrei, wenn
  - Daten im Inland bereits veröffentlicht
  - Indirekt personenbezogene Daten
  - Für private oder publizistische Zwecke
  - Zustimmung durch den Betroffenen

Safe-Harbor-Abkommen

- Zertifizierung für US-Unternehmen
- Prinzipien
  1. „Notice“ (Benachrichtigung)
  2. „Choice“ (Freiwilligkeit)
  3. „Onward Transfer“ (Übermittlung)
  4. „Security“ (Datensicherheit)
  5. „Data Integrity“ (Datenintegrität)
  6. „Access“ (Zugang)
  7. „Enforcement“ (Durchsetzung)

Dienstleistervertrag – Verantwortlichkeit

- Sollte eindeutig zwischen Nutzer und Anbieter geregelt sein
- Anbieter ist verpflichtet „ausschließlich nur im Rahmen des Auftrages die Daten des Nutzers zu verarbeiten oder zu übermitteln“ (§11 Abs 1 DSG)

- Wer haftet für Pannen?
- Wie ist der Nutzer zu informieren, wenn Verstöße eintreten?

Dienstleistervertrag – Nutzerkontrolle

- Nutzer kann jederzeit die Schutzmaßnahmen des Anbieters prüfen
  - Im Ausland meist durch Dritte
- Beschränkung der Kontrolle
  - Während der Geschäftszeiten
  - Unentgeltlich

Dienstleistervertrag – Laufzeit und Rückgabe von Daten

- Rückgabe ist in §11 Abs 1 Z5 DSG festgelegt
- Wenn Bestätigung über die endgültige Löschung versendet worden ist, enden die Pflichten des Anbieters

- Welches Dateiformat und welche Struktur soll übermittelt werden?

Sonderregelungen – Berufsgeheimnis

- Bestimmte Berufsgruppen sind zur Verschwiegenheit verpflichtet
  - Gesundheitswesen
  - Versicherungsmakler

- → Besonderes Augenmerk auf sensible und personenbezogene Daten

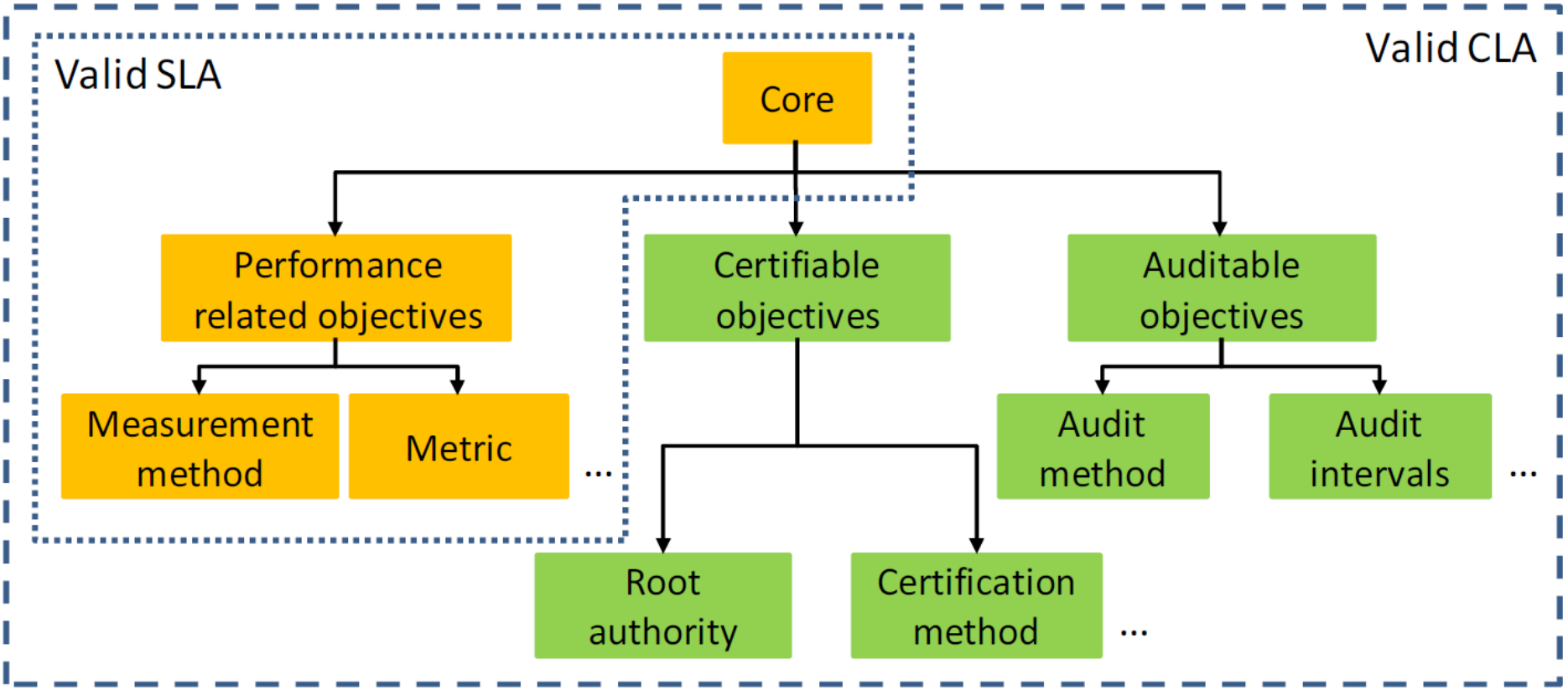
Compliant Cloud Computing (C3)

- Service Level Agreement (SLA)
  - Erreichbarkeit
  - Durchsatz
  - …
- Problem: SLAs zur Einhaltung von Rechtsvorschriften meist nicht ausreichend
- Lösung: C3-Framwork

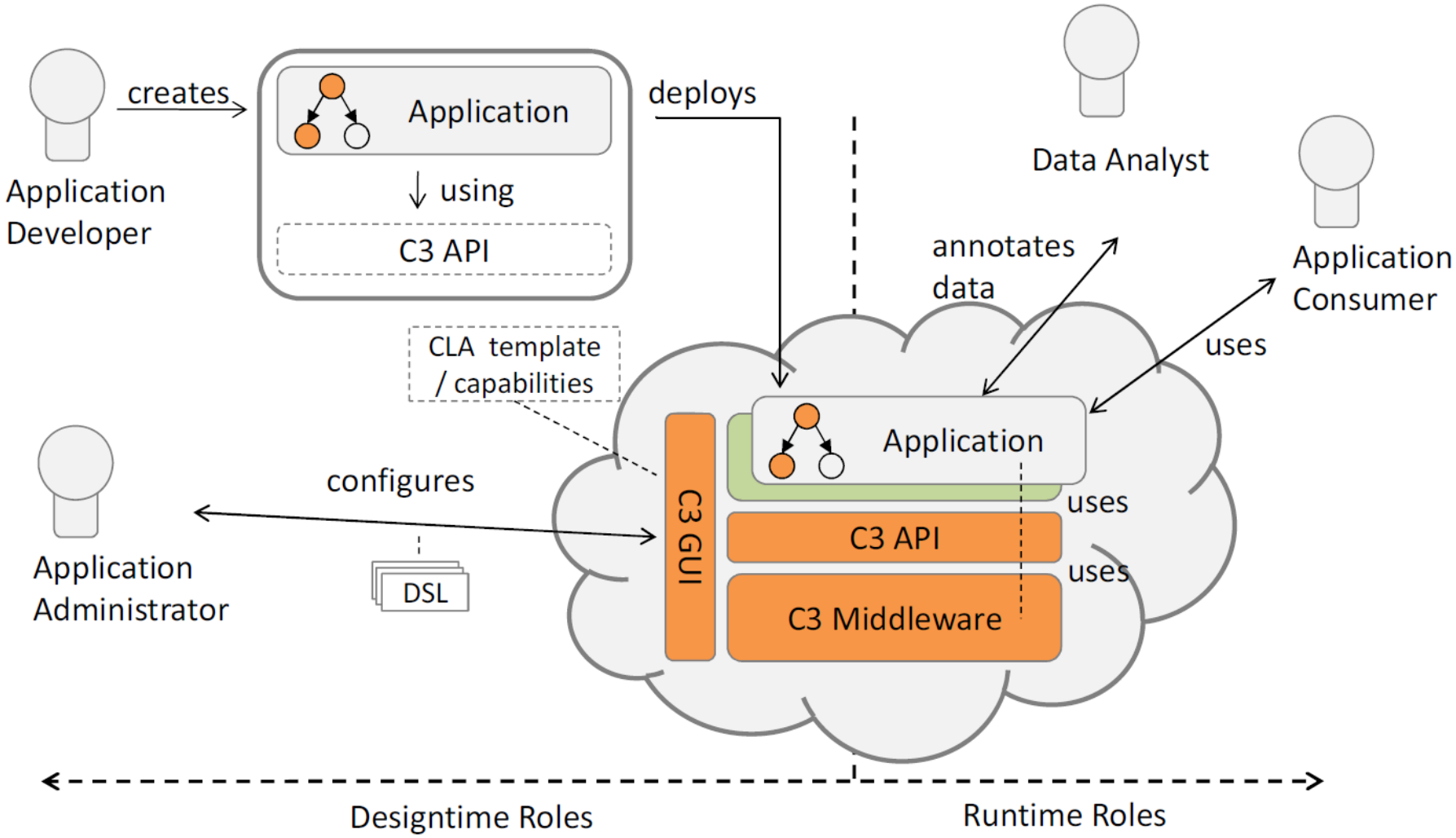
C3-Framwork

- Sprache zur Beschreibung der Anforderungen (DSL)
  - Sicherheit
  - Datenschutz
  - …
- C3-Middleware
  - Verteilung der Anwendung
  - Cloud-Provider-Auswahl
  - Überwachung und Durchsetzung der Anforderungen

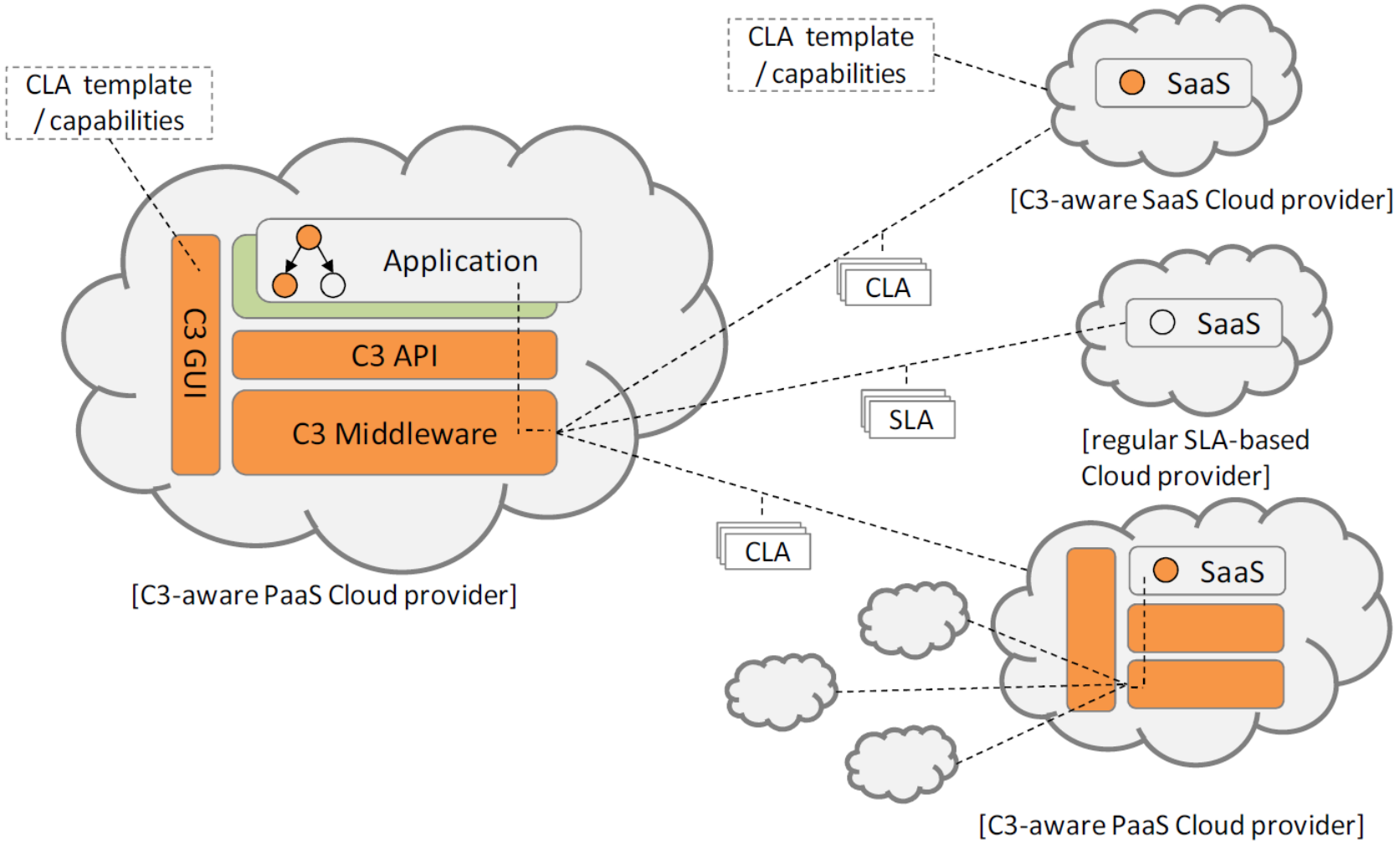
SLA vs. CLA


Valid CLA
Valid SLA
Core
Performance related objectives
Certifiable objectives
Auditable objectives
Measurement method
Metric
...
Audit method
Audit intervals
...
Root authority
Certification method
...

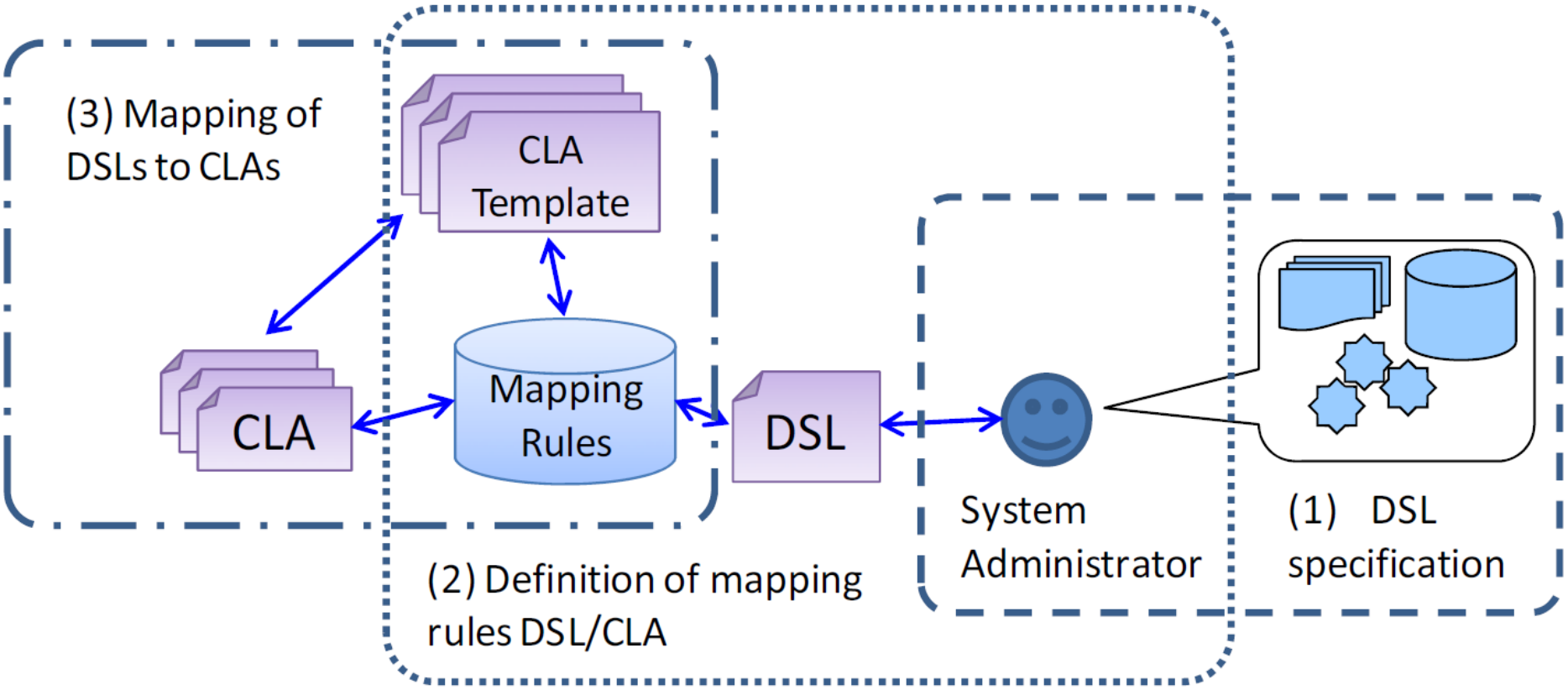
Rollen


creates
Application
Developer
Application
using
C3 API
deploys
Data Analyst
annotates
data
Application
Consumer
uses
CLA template
/ capabilities
Application
configures
C3 GUI
C3 API
uses
C3 Middleware
uses
Application
Administrator
DSL
Designtime Roles
Runtime Roles

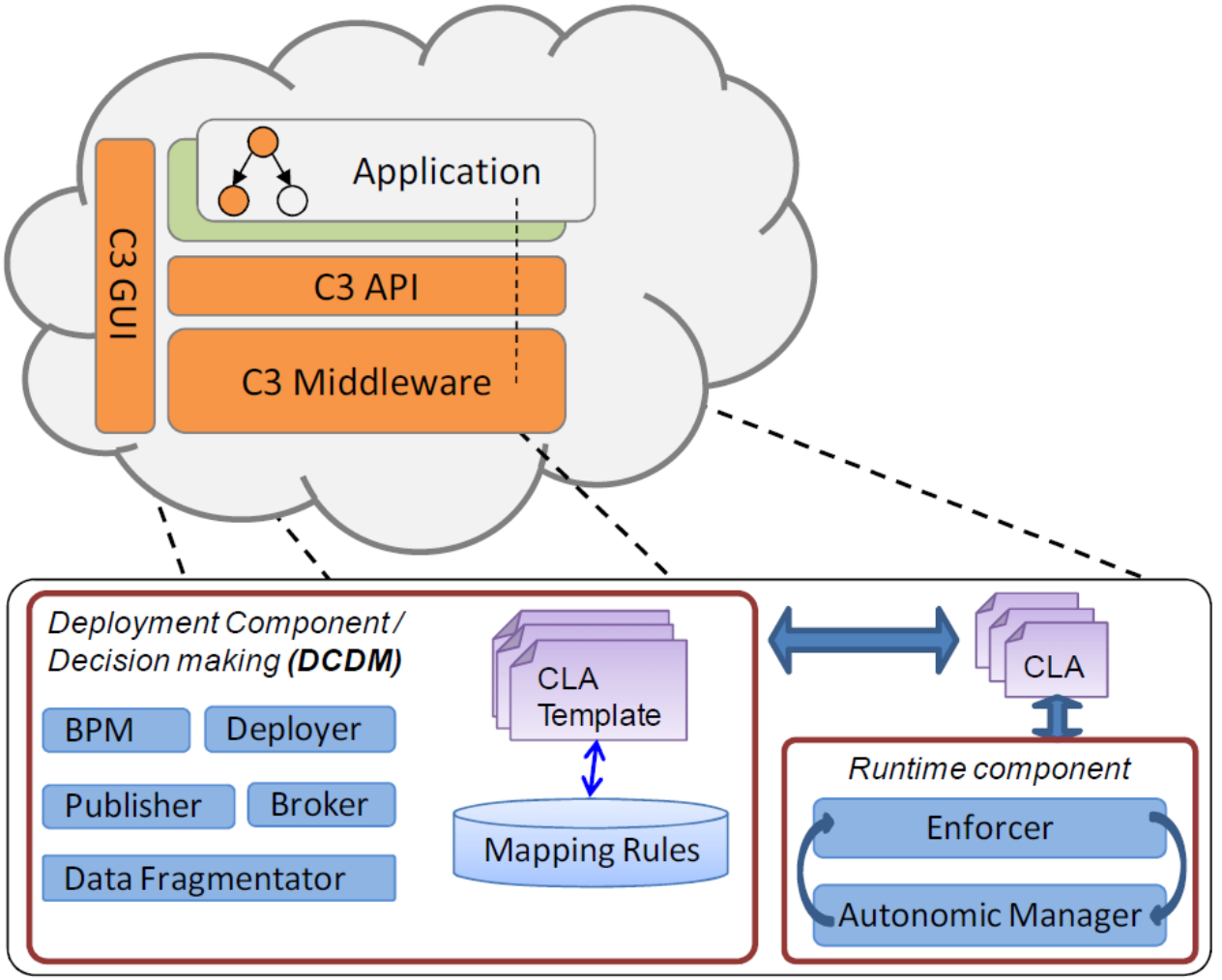
Ausführung der Anwendung



Beschreibung der Anforderungen



Middleware


Application
C3 GUI
C3 API
C3 Middleware
Deployment Component / Decision making (DCDM)
BPM
Deployer
Publisher
Broker
Data Fragmentator
CLA Template
Mapping Rules
CLA
Runtime component
Enforcer
Autonomic Manager

Quellen

- Borges/Schwenk, Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce (2012)
- Pollirer, Datenschutz und Cloud Computing (2011)
- EuroCloud Austria, Leitfaden Cloud Computing. Recht, Datenschutz & Compliance (2011)
- Bizer, Sieben goldene Regeln des Datenschutz (2007)
- Marnau/Schlehahn, Cloud Computing und Safe Harbor (2011)
- Brandic/Dustdar/Anstett/Schumm/Leymann/Konrad, Compliant Cloud Computing (C3): Architecture and Language Support for User-driven Compliance Management in Clouds (2010)
- http://www.nist.gov/itl/cloud/index.cfm
- http://www.ris.bka.gv.at/