

■ ■ ■ Security Services versus Secure Infrastructure



Daniel Liebhart
Dozent für Informatik an der
Hochschule für Technik
Zürich, Mitglied des SOA-
Expertenrats

trivadis
makes IT easier. ■ ■ ■

12.3.2008 SOA & IT Security
AK SOA-Technologies & KB Sicherheit

Agenda

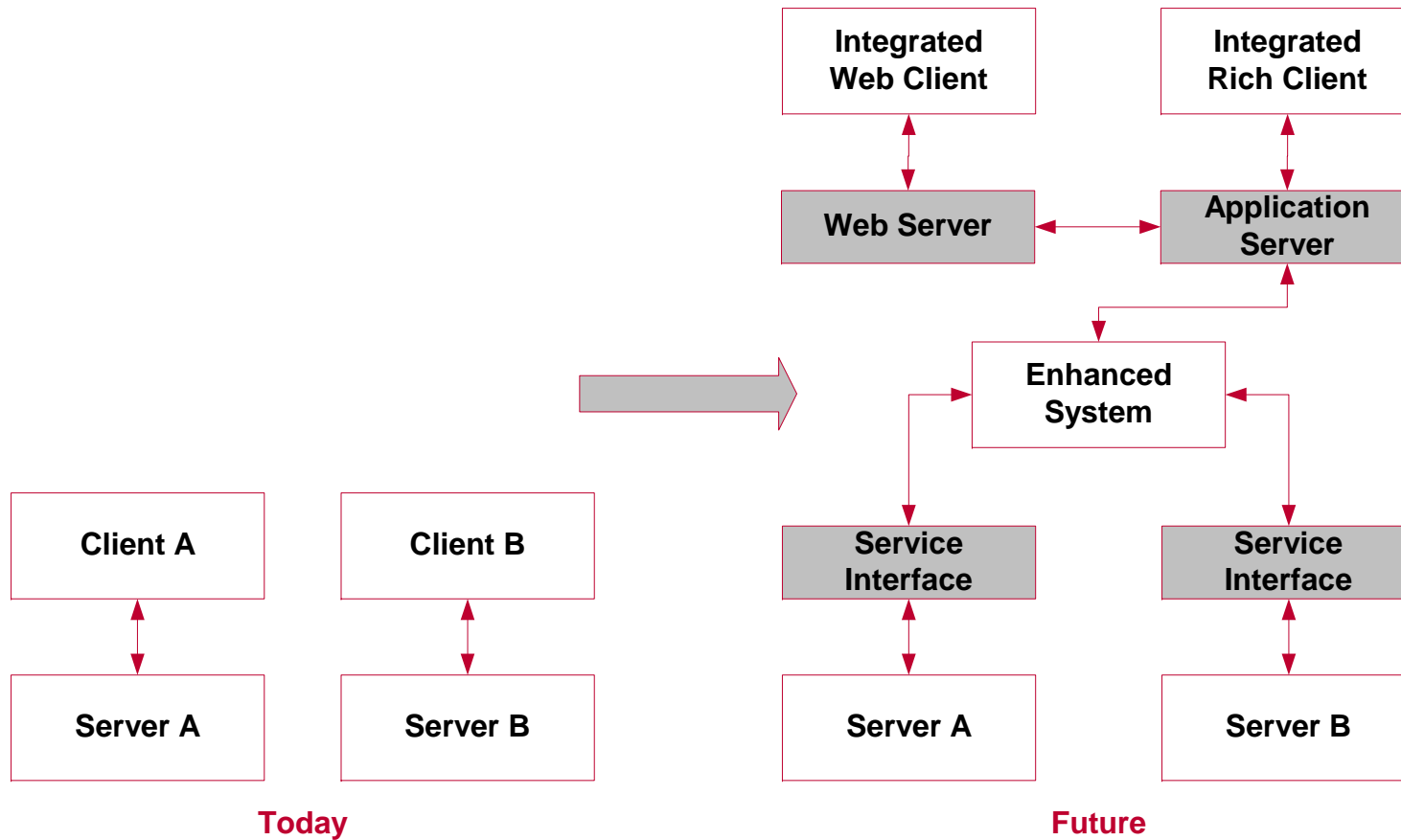


SOA

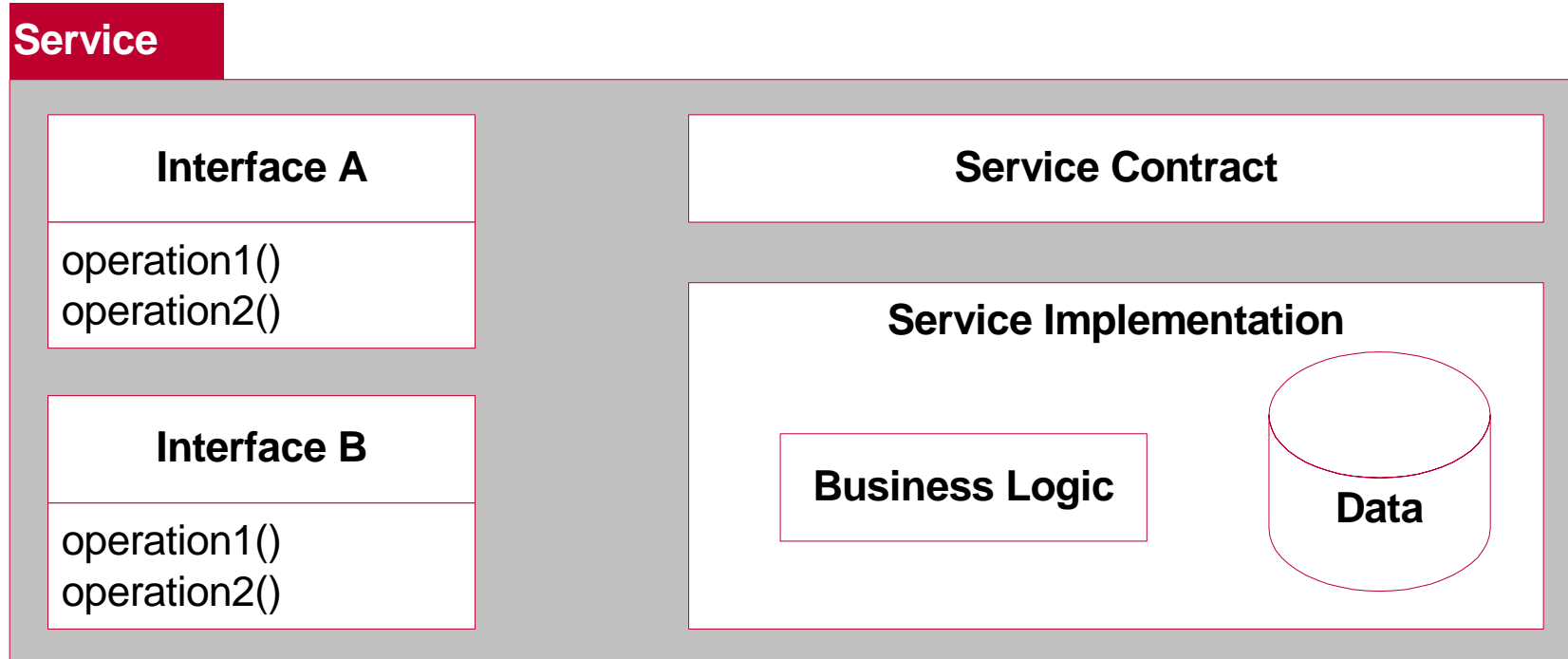
Playing the game

- SOA Intro & SOA als Standard-Architektur
- Lösungen für Security & SOA
- SOA Security Standards
- Security Services
- Security as Infrastructure
- Fazit

Intro SOA: Dienste statt Applikationen



Intro SOA: Der Dienst als Basis

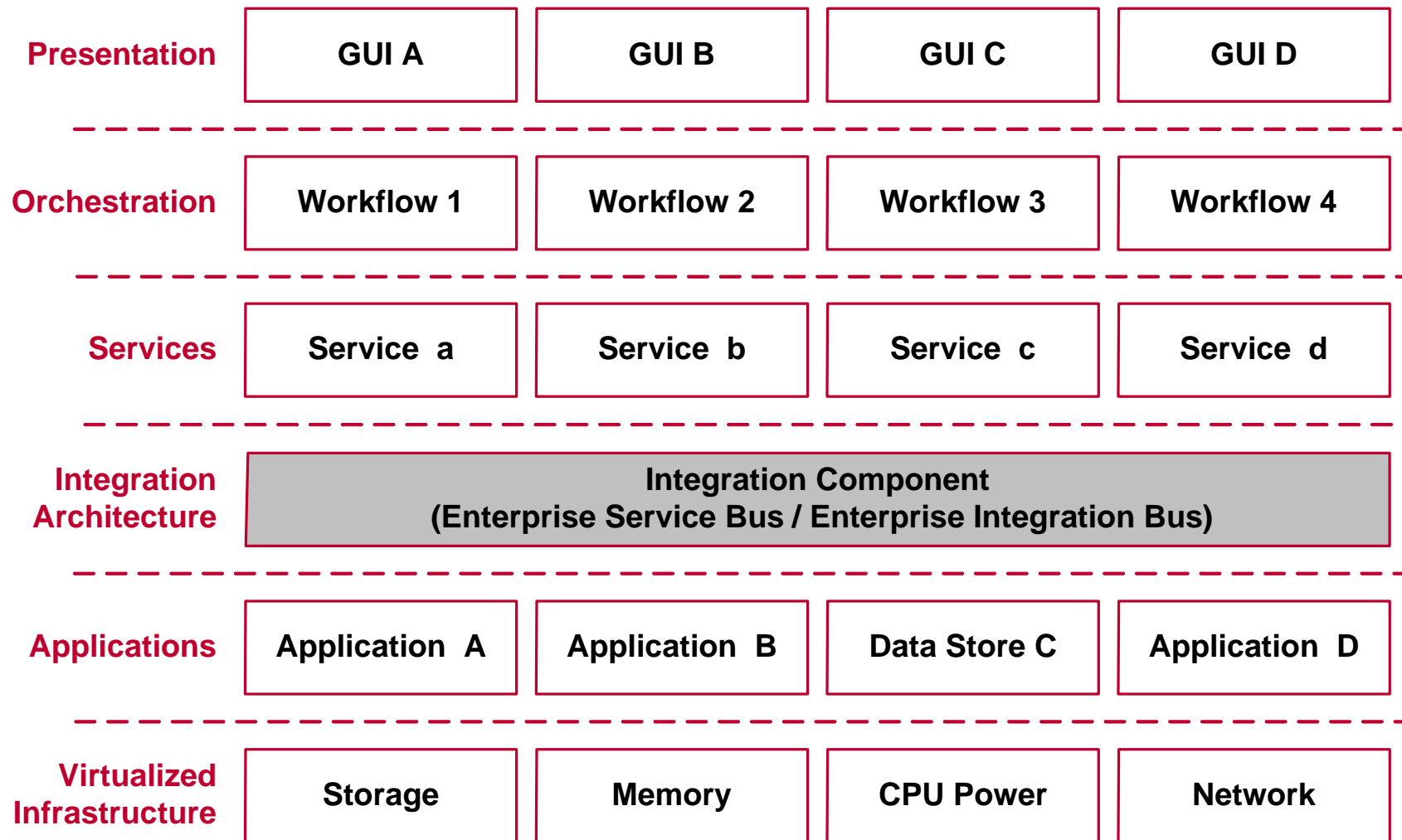


SOA Intro: Der Dienst als Basis



- Service Oriented Computing (SOC) ist ein Paradigma, welches Services (Dienste) als fundamentales Element für die Erstellung von Applikationen verwendet.
- Dieses fundamentale Element besteht aus einem Basisdienst, seiner Beschreibung sowie einer Reihe von Basisoperationen (Publication, Discovery, Selection und Binding).
- Wichtiger Vorteil der Service Abstraktion ist die Möglichkeit verschiedenste Dienstarten auf ein und dieselbe Art und Weise zuzugreifen.

SOA als Standard-Architektur: Das Architekturmodell



SOA als Standard-Architektur: Das Architekturmodell



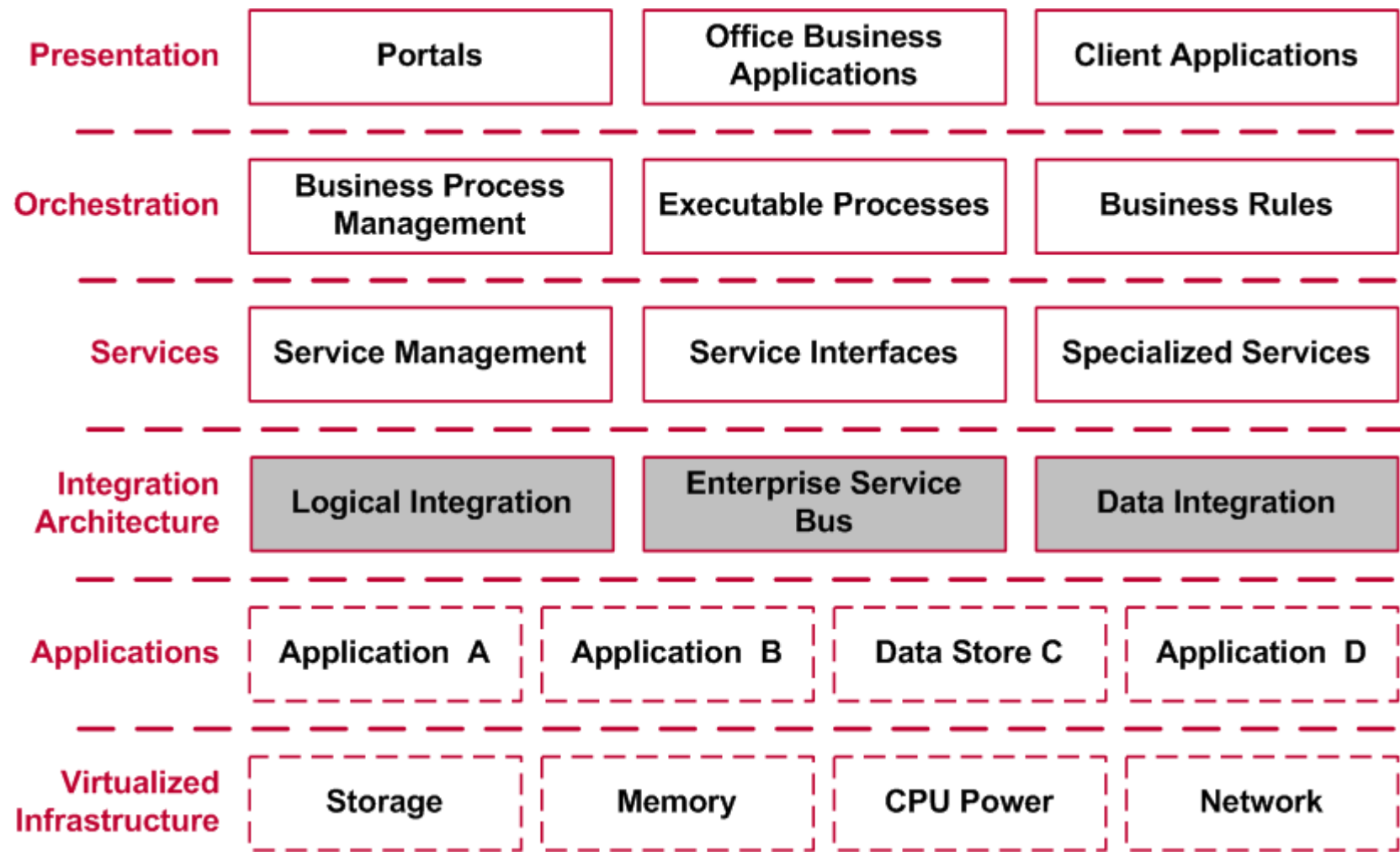
- *Presentation*: Das User Interface
- *Orchestration*: Der Ablauf einer Applikation wird als Workflows festgelegt.
- *Services*: In dieser Schicht sind sämtliche Dienste enthalten.
- *Integration Architecture*: Infrastruktur zur Verbindung der diversen Dienste und zur Verbindung von Diensten mit bestehenden Applikationen/Systemen oder Datenbanken
- *Applications*: Bestehende & neue Anwendungen sowie die Datenbanken/Datenquellen eines Unternehmens.
- *Virtualized Infrastructure*: Zum Betrieb aller Komponenten notwendigen Ressourcen

SOA als Standard-Architektur: Wichtigste Vorteile



- SOA bedeutet Standardisierung, Kostenersparnis, und Flexibilität
- 1. Die „Weiterverwendung“ bestehender Anwendungen durch standardisierte Schnittstellen
- 2. Die Flexibilisierung eines Systems durch Trennung der Logik in statische (Funktionalität) und dynamische Bereiche (Prozesse)
- 3. Die Tatsache, dass alle grossen Hersteller (IBM, Microsoft, Oracle, SAP) von ein und demselben Architekturmodell für SOA ausgehen.

SOA als Standard-Architektur: SOA Bestandteile



SOA als Standard-Architektur: SOA Bestandteile



- *Presentation*: Als Portal, Office Application oder als Client Application
- *Orchestration*: Geschäftsprozesse (als BPEL Workflows) und Geschäftsregeln (als Business Rules) – mit BPM realisiert
- *Services*: Services Management, Service Interfaces und Specialized Services
- *Integration Architecture*: Logische Infrastruktur, Enterprise Service Bus oder Mechanismen zur Datenintegration (EII)

SOA als Standard-Architektur: Was nicht dazugehört



- Monitoring, Activity Management, Deployment, IT Service Management, IT Governance Management etc.
- Sind zwar bei Herstellern zu finden
- **Aber:**
- Überladen eine mögliche Einführung
- Sind für fast jedes andere Architekturmodell genauso notwendig

- SOA löst nicht jedes Problem, das wir in der IT haben!

SOA als Standard-Architektur: Was ist anders



- Die Trennung von statischer Funktionalität und Dynamik für die Entwicklung ungewohnt
- Ein System wird nicht mehr als Ganzes modelliert
- Prozessmodellierung, respektive die Modellierung ausführbarer Prozesse
- Regelmodellierung
- Service Engineering
- Auswahl der Produkte intensiv (grosses Angebot vorhanden – Hersteller und Open Source Gemeinde)

Was wird besser mit SOA realisiert?



- Legacy Integration (Weiterverwendung bestehender Systeme)
- Legacy Migration (Schrittweise Ablösung)
- Landscape Consolidation (Konsolidierung verschiedener Anwendungen)
- Interface Processing (Schnittstellenbau mit SOA)
- Master Data Management
- Spezialisierte Services (Security, Printing Services, etc.)

Lösungen für Security & SOA: Basis



- Auf SOA basierende Lösung = verteiltes System
- Es gelten alle Sicherheitsaspekte, die auch für ein solches System gelten:
 - Identifikation
 - Authentisierung
 - Autorisierung
 - Integrität
 - Vertraulichkeit

Lösungen für Security & SOA: Varianten

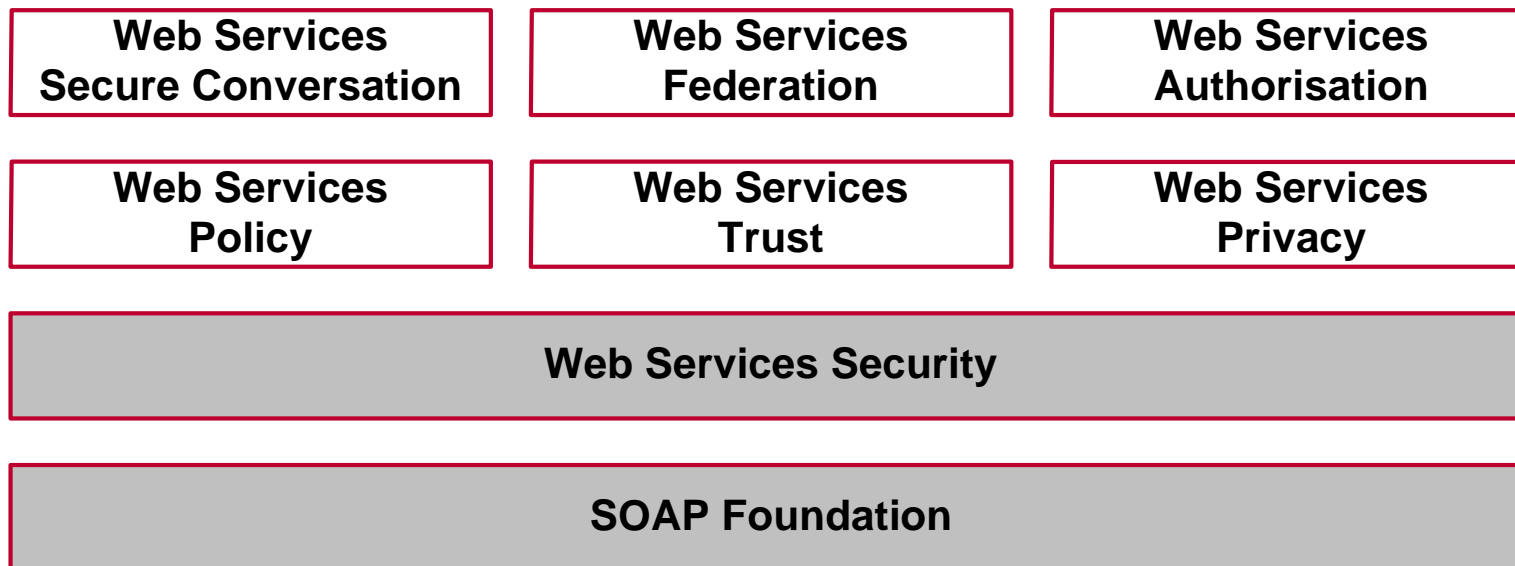


- **Security Standards:** Realisierung der Sicherheitsaspekte auf Ebene der Service Implementationen, respektive auf Ebene des Datenaustausches zwischen den verschiedenen Diensten.
- **Security Services:** Die zentrale Bereitstellung von Sicherheitsmechanismen in einer SOA als Services, die von allen anderen Komponenten einer SOA genutzt werden können.
- **Security as Infrastructure:** Security as Infrastructure realisiert die sicherheitsrelevanten Aspekte einer SOA als Teil der Infrastruktur.

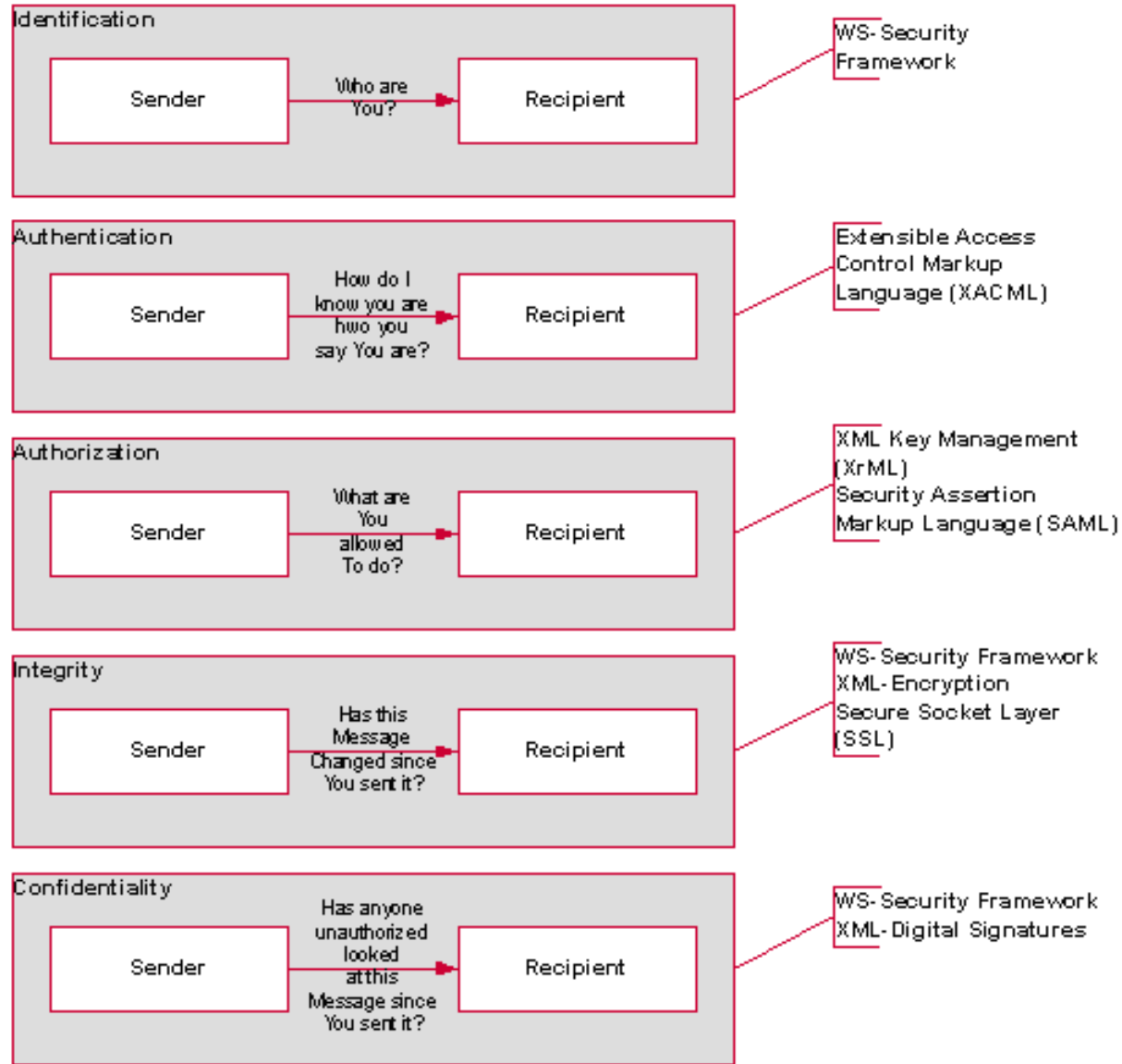
SOA Security Standards: Grundidee



- Die SOA Security Standards gehen vom einzelnen Dienst aus, der in sich sämtliche Sicherheitsaspekte realisiert!



SOA Security Standards: Auf Messaging-Ebene



SOA Security Standards: Problematik



- Alle Sicherheitsaspekte – wie beispielsweise Identifikation, Authentisierung, Autorisierung, Integrität und Vertraulichkeit können mit den vorhandenen Standards abgedeckt werden.

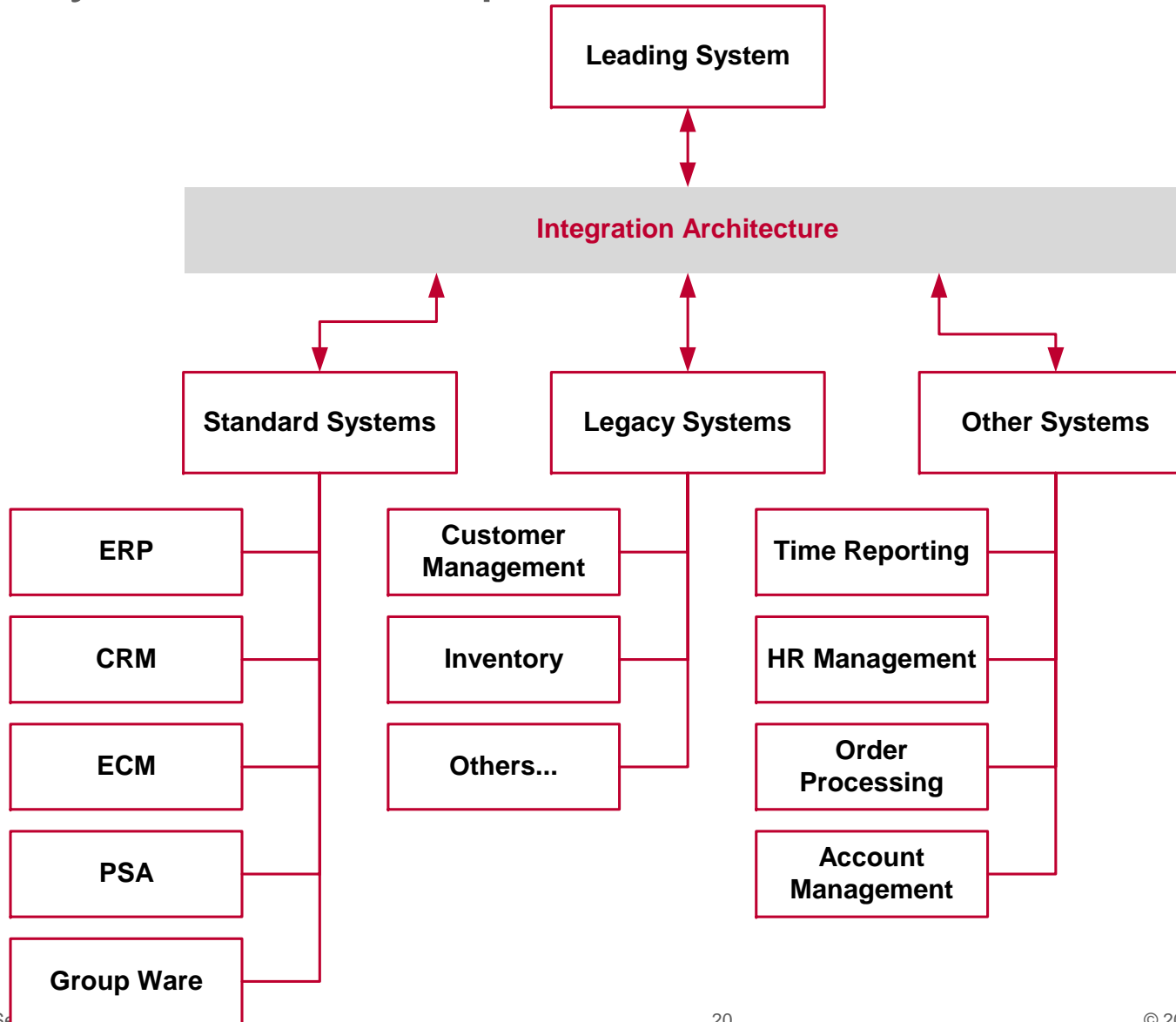
- **Aber:**
- Umsetzung ist sehr komplex
- Erschwert die Weiterverwendung bestehender Systeme
- Wird durch den Einsatz Standard-Software eingeschränkt
- **ALSO:** Nicht bei der Einführung einer SOA zu empfehlen!

Security Services: Grundidee



- Zentrale Bereitstellung von Sicherheitsmechanismen in einer SOA als Service
- = **Specialized Service**
- Entspricht einer zentralen Unternehmensfunktion, die von allen Anwendungen verwendet wird
- **Typische Anwendung: IAM**
- **Beispiel aus der Praxis:** Schnittstellenbau mit zentralem Security Service

Security Services: Bsp - Schnittstellenbau mit SOA



Security Services: Bsp - Schnittstellenbau mit SOA



- Ein typischer Anwendungsfall ist der Austausch von Daten zwischen verschiedenen Systemen im einen Unternehmen
- Zentrale Informationen, wie beispielsweise Kundendaten und Bestellungen werden von verschiedensten Applikationen in aktueller Form benötigt

Security Services: Schnittstellenbau - Konzept

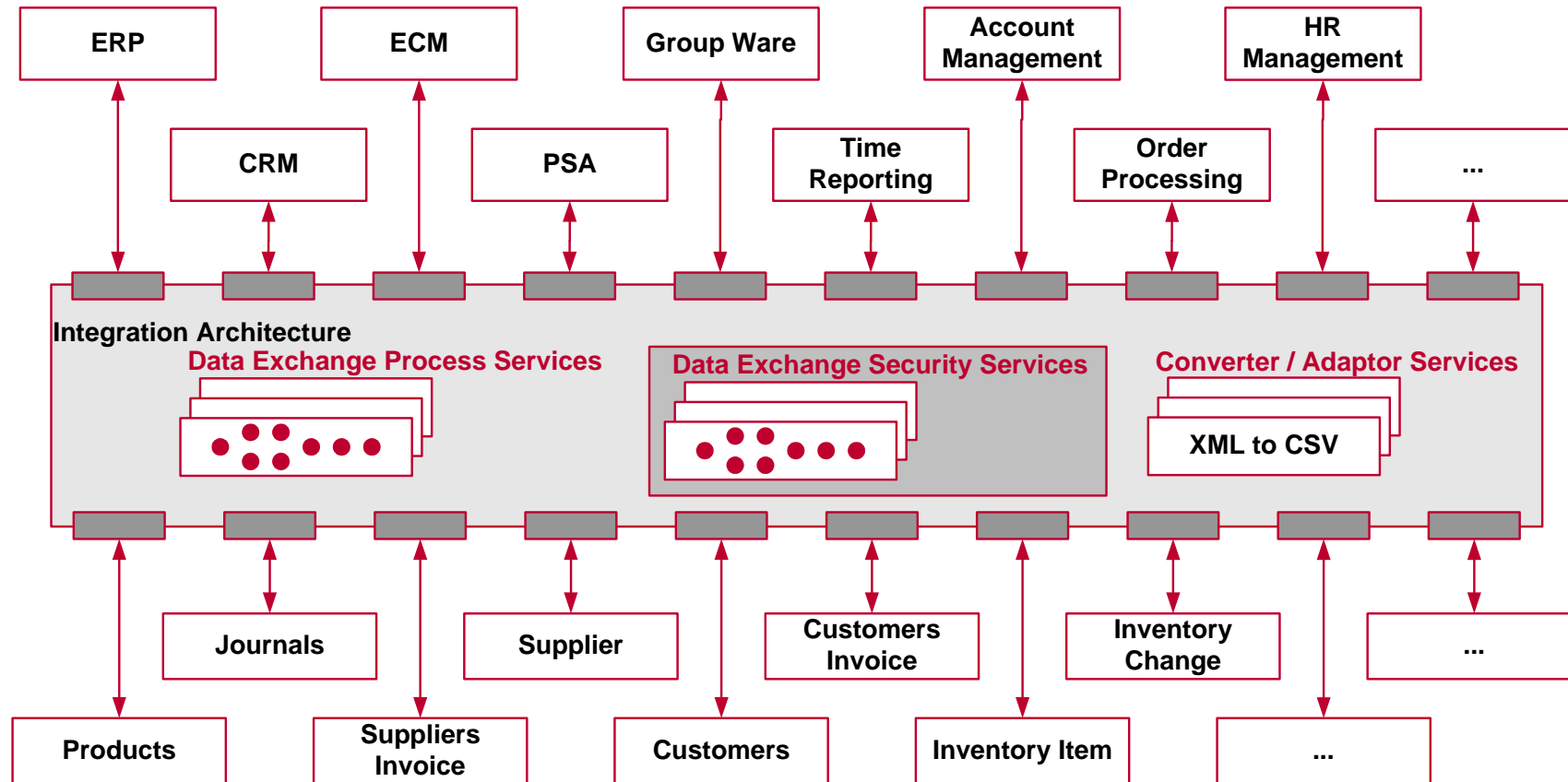


- Zentrale Informationen, wie Kundendaten, Bestellungen und Produktdaten werden von verschiedensten Applikationen in aktueller Form benötigt.
- Die Realisierung eines Datenaustausches basierend auf SOA bedeutet:
 - 1. Alle Schnittstellen zu den beteiligten System werden mittels Web Services standardisiert zugänglich gemacht.
 - 2. Der Datenaustausch zwischen den Systemen wird über BPEL gesteuert.
 - 3. Die Konversion von Daten erfolgt über spezialisierte Dienste, für die Business Rule Engines eingesetzt werden.

Security Services: Schnittstellenbau – mit SOA



Standard Systems / Legacy Systems / Other Systems



Leading System Interfaces

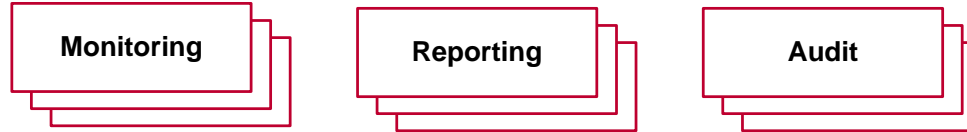
 Service Interface

Security Services: Schnittstellenbau – mit SOA

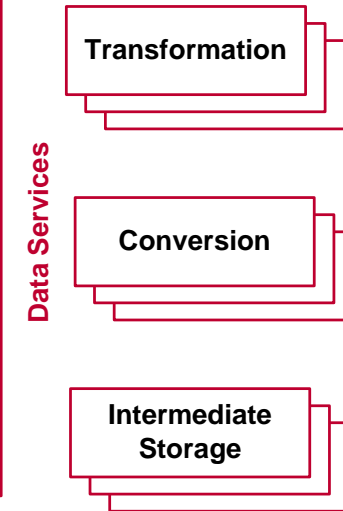
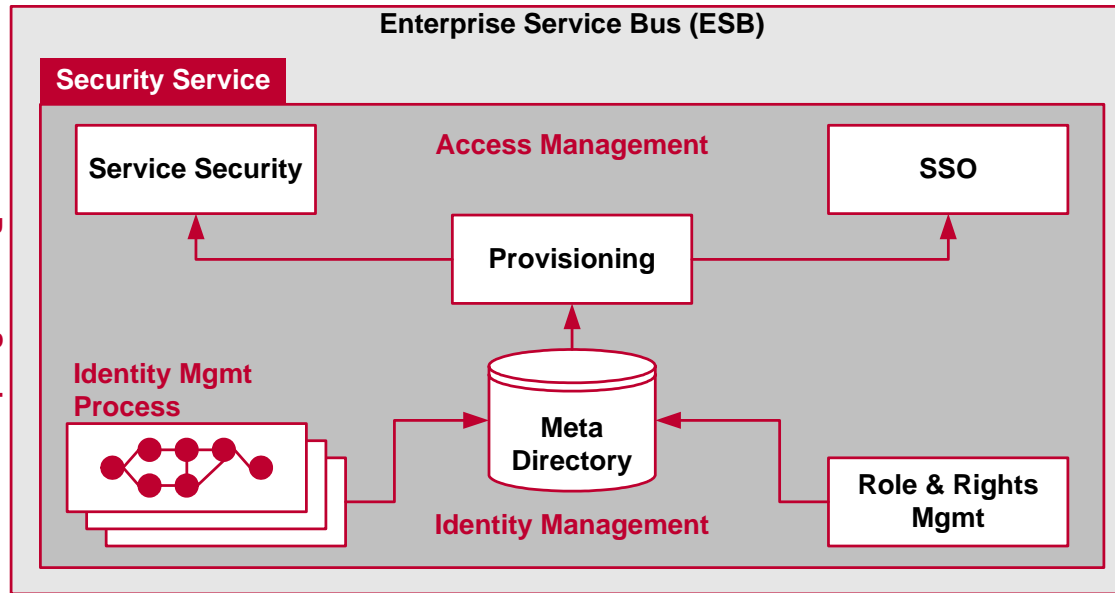
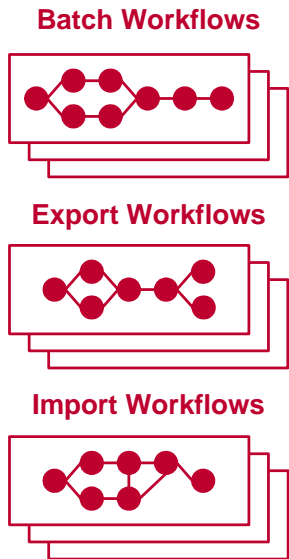


- Jedes beteiligte System (Leading System, Standard System, Legacy System oder andere) ist über eine Serviceschnittstelle zugänglich. Es existiert eine Schnittstelle für den Dateninput und eine für den Datenoutput.
- Jeder Import, jeder Export und jeder Batchlauf ist als Workflow realisiert.
- Alle Datenkonverter (Adaptoren) sind über eine Serviceschnittstelle zugänglich.
- Jeder Workflow weist wiederum eine Serviceschnittstelle auf.
- Jeder Aufruf einer Schnittstelle geht über den zentralen Security Service, der sämtliche Sicherheitsaspekte implementiert

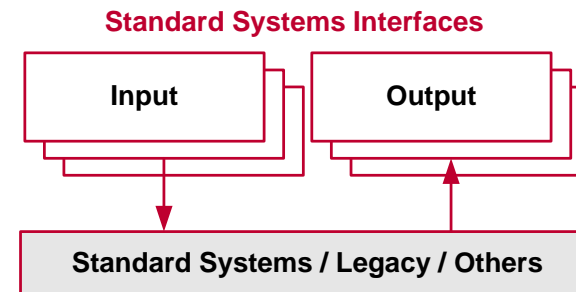
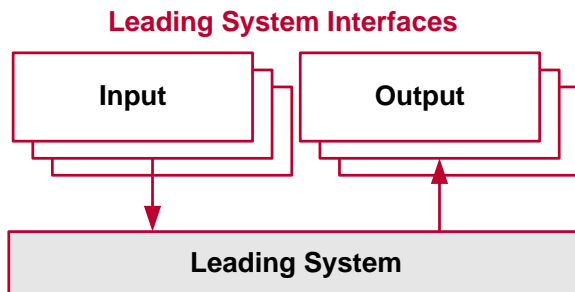
Security Services: Schnittstellenbau – mit SOA



Monitoring / Reporting / Audit Services



Application Services



Security Services: Schnittstellenbau – mit SOA



- **Monitoring Services:** Überwachung aller Schnittstellen Datentransfers und Workflows
- **Reporting Services:** Das Reporting aller Kennzahlen der Schnittstellen
- **Audit Services:** Speicherung und Bereitstellen der Historie aller Datentransfers
- **Transformation Services:** Transformation von Daten (als Business Rules)
- **Conversion Services:** konvertieren Daten in verschiedene Formate (als Business Rules)
- **Intermediate Storage Services:** Zwischenspeicherung von Daten
- **Batch, Export und Import Workflow Services:** Prozesse für die Ausführung von Interface Executions
- **Leading System Interfaces:** Service Interface zum Leading System
- **Standard System Interfaces:** Service Interface zu allen beteiligten Systemen

Security Services: Problematik



- Security Services bedeutet die zentrale Bereitstellung von Sicherheitsmechanismen in einer SOA als Services, die von allen anderen Komponenten einer SOA genutzt werden.

- **Merkmale:**
- Umsetzung bedeutet: Jeder einzelne Workflow geht über den zentralen Security Service
- Keine Absicherung auf Meldungsebene
- Grosser Betreuungsaufwand
- Nur für SOA auf Unternehmensebene zu empfehlen!

Security as Infrastructure: Grundidee



- Security as Infrastructure realisiert die sicherheitsrelevanten Aspekte einer SOA als Teil der Infrastruktur, beispielsweise als Appliance
- = Komponente der **Virtualized Infrastructure**

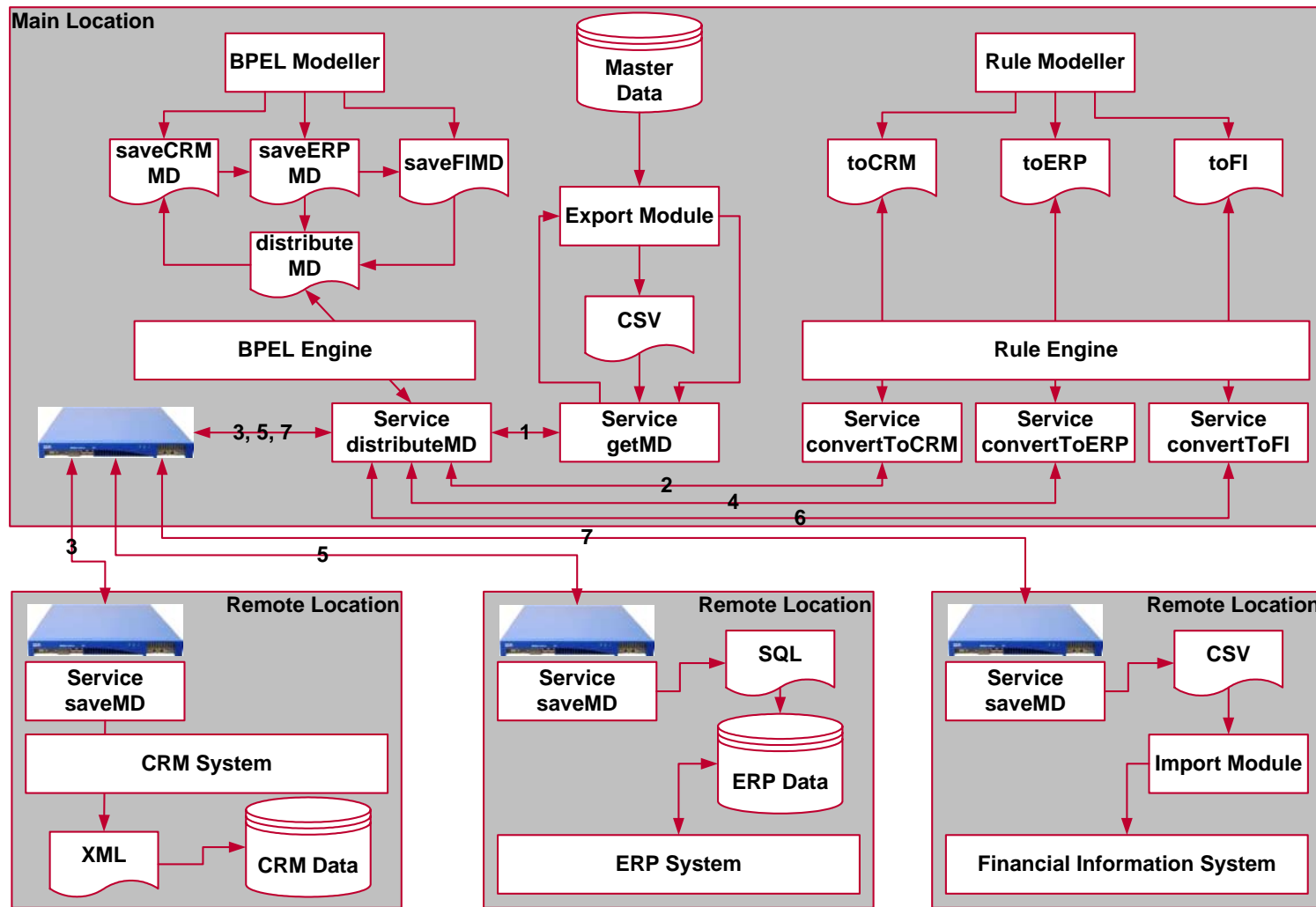
- **Beispiel aus der Praxis: MDM**

Security as Infrastructure: Beispiel



- **Beispiel:** IBM DataPower Integration Appliance
- Transformation Engine
- Content Based Routing
- XML/SOAP Firewall
- Data Validation
- SAML, LDAP, RADIUS
- Web Service Management
- Und was wir uns sonst so wünschen ;-)

Security as Infrastructure: Beispiel



Security as Infrastructure: Konsequenz



- Auf Architekturebene ist eine auf SOA basierte Lösung nicht beeinträchtigt oder eingeschränkt
- Sämtliche Service Calls gehen über im Minimum zwei solcher Appliances
- Aber: Fokussiert auf Security auf Meldungsebene

Security as Infrastructure: Problematik



- **Security as Infrastructure** realisiert die sicherheitsrelevanten Aspekte einer SOA als Teil der Infrastruktur. Sämtliche Sicherheitsmechanismen werden auf Meldungsebene realisiert. Daten, die zwischen den beteiligten Diensten ausgetauscht werden, werden abgesichert.

- **Merkmal:**

- **Teuer!**

- **Typische Nachteile einer Firewall**

Fazit



- **Neben den komplexen und unzähligen Standards haben sich vor allem zwei Lösungsansätze: „Security Services“ und "Security as Infrastructure".**
- **Security Services** bedeutet die zentrale Bereitstellung von Sicherheitsmechanismen in einer SOA als Services, die von allen anderen Komponenten einer SOA genutzt werden können.
- **Security as Infrastructure** versucht die sicherheitsrelevanten Aspekte einer SOA als Teil der Infrastruktur - beispielsweise als Appliance - so zu realisieren, dass die Anwendungen und die SOA Komponenten nicht mit Securityaspekten überladen werden.
- **Vielen Dank**

■ ■ ■ Herzlichen Dank!

