IT-Security als Enabler

Attribut-basierte Autorisierung (ABAC) für das neue Kundenportal der CSS

Netclose Community Treffen, Horw, 24.09.2014

Stefan Allemann, CSS Versicherung

CSS Versicherung: Kennzahlen 2013

Bruttoprämien
5,248 Mrd CHF

Leistungskosten
4,697 Mrd CHF

1,239

Anzahl Grund-
versicherte (in Mio.)

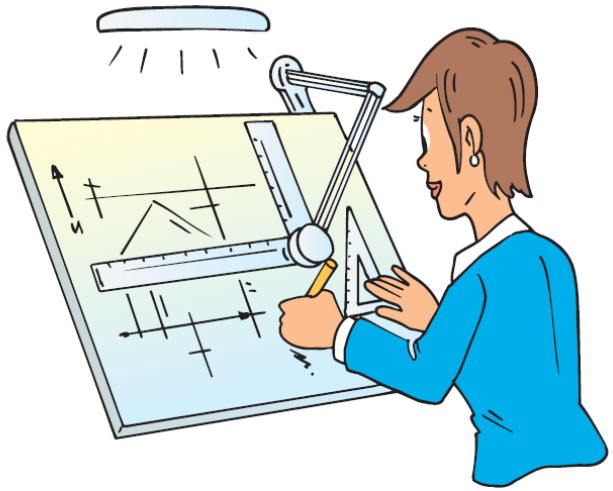
2’650
Mitarbeitende,
260 in der IT

Security-Architektur bei CSS

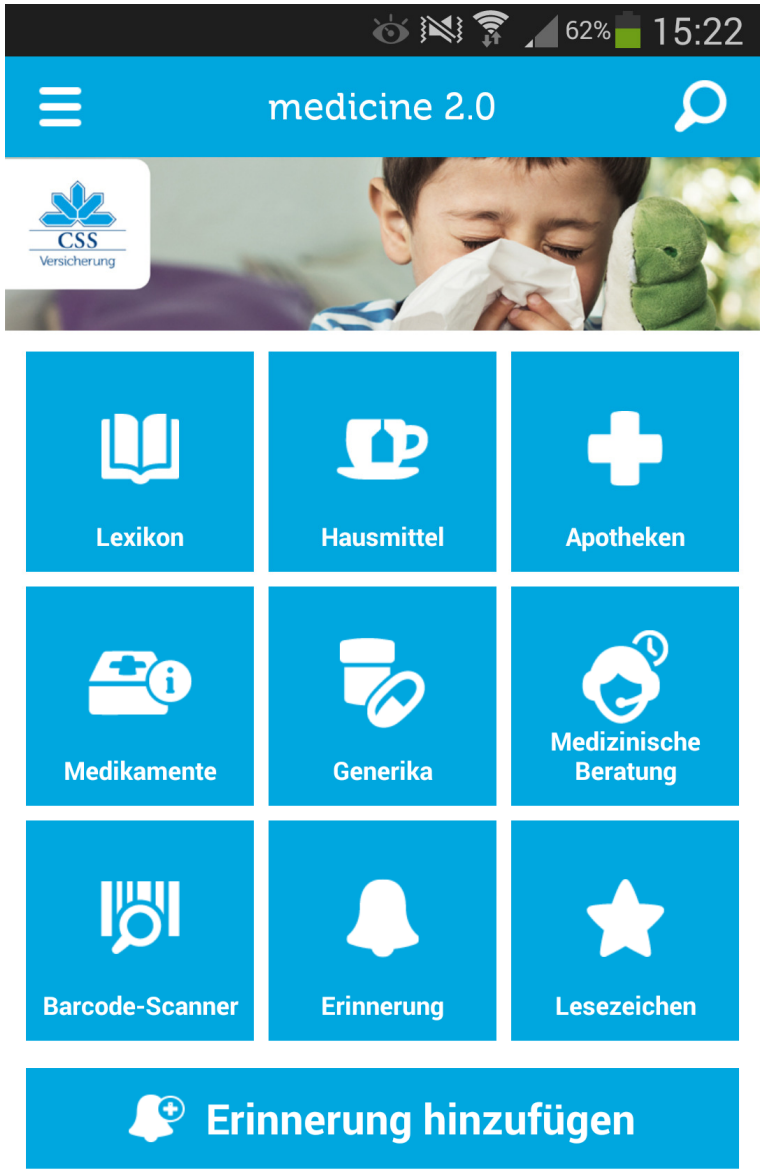
Security-Architektur bei CSS

- **Vorgaben** für Entwicklung und Systemtechnik
- **Reviews** von Anwendungen und Infrastruktur
- Unterstützung und **Beratung**

- Technische **Konzepte** und Security-Architekturen
- Bereitstellung/Entwicklung von Security-Komponenten
- **Identity- und Access-Management** (Architektur)



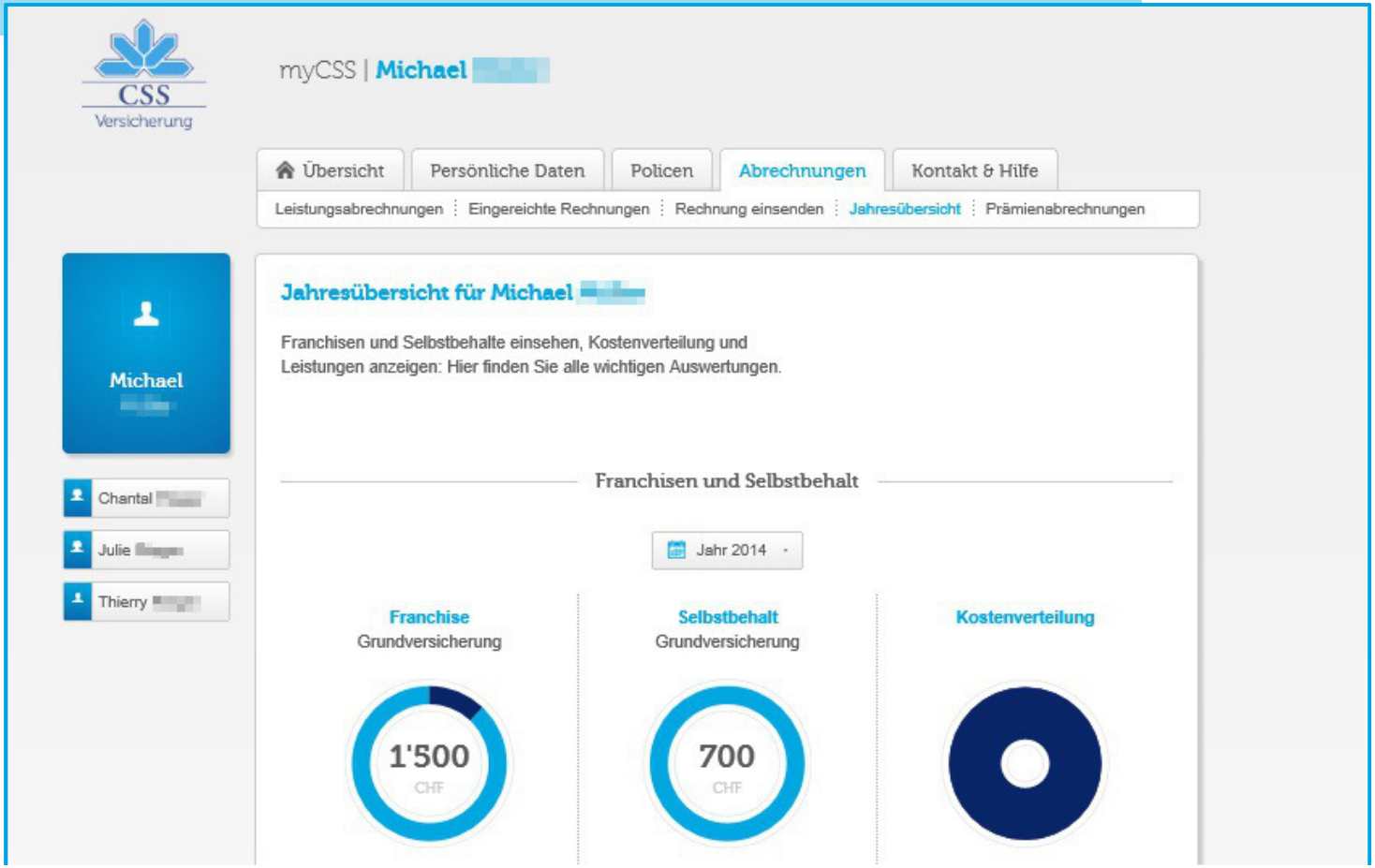
E-Business bei CSS



myCSS – Portal für Privatkunden

Nutzen für Kunden

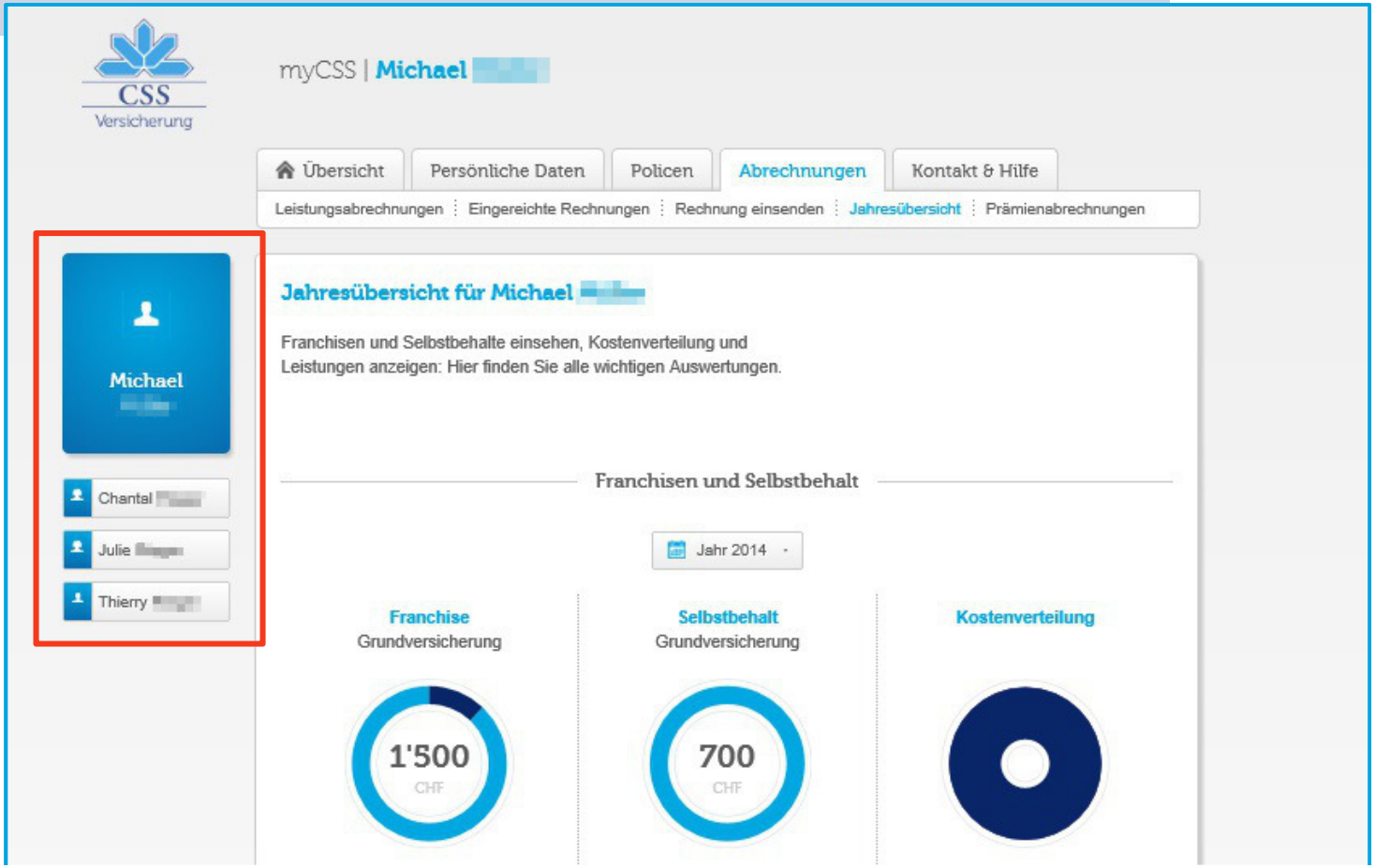
- Mit wenigen Klicks alle Versicherungsangelegenheiten erledigen
- Überblick über alle Daten und Kosten



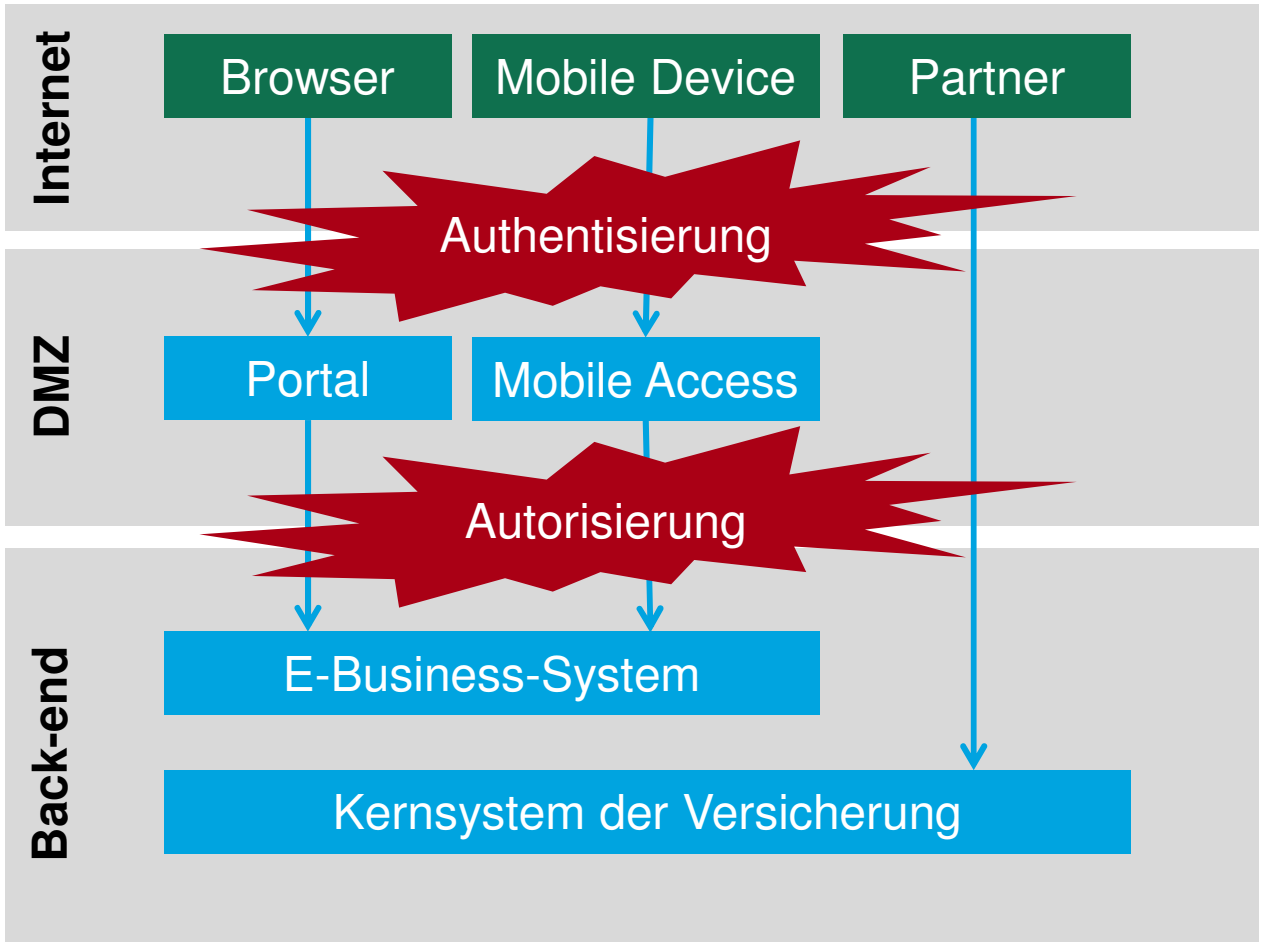
myCSS – Portal für Privatkunden

Herausforderung

- Zugriff auf alle Dokumente der Familie (je nach Berechtigung)



Herausforderungen bei E-Business



Autorisierung von Dokumentenzugriffen

Zulässig, falls entsprechende **Beziehung** (z.B. Prämienzahler) zum **Eigentümer** des **Dokumentes** zum **Erstellzeitpunkt** des Dokumentes vorhanden.

Gesetzlicher Vertreter

ABAC

~~***RBAC***~~

RBAC

Sachbearbeiterin

Zulässig, falls in Besitz der nötigen Rolle für Dokumentenklasse.

Unzulässig obwohl Eigentümer, da minderjährig.

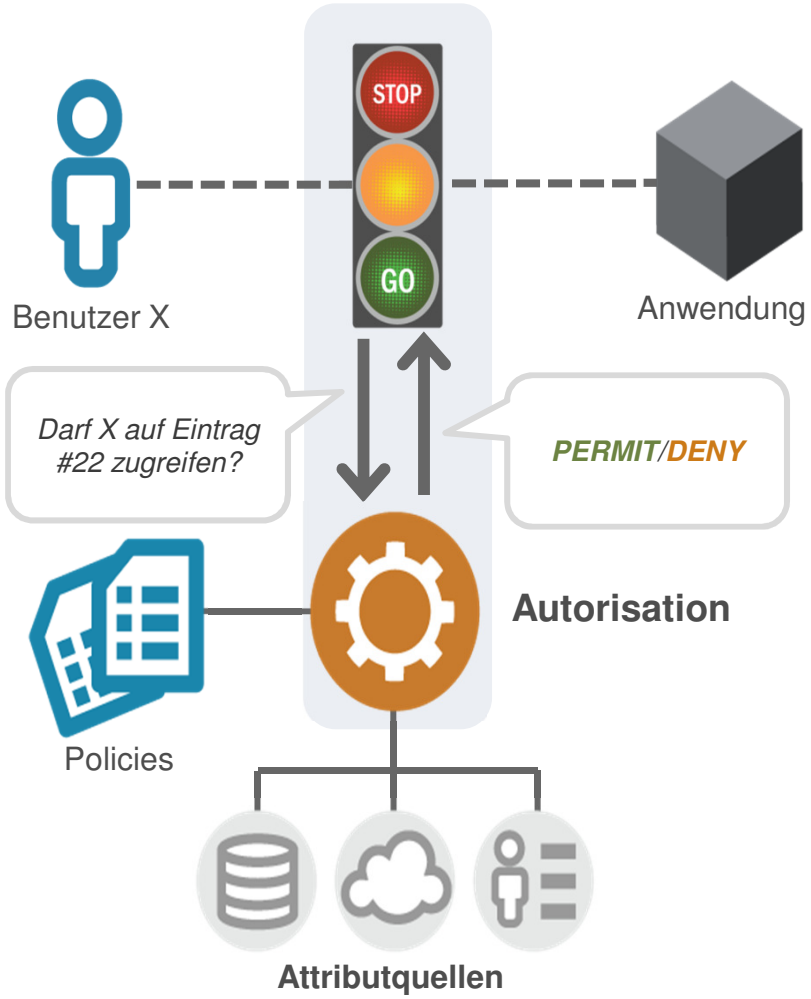
Kunde

Attribute Based Access Control (ABAC)

XACML: Extensible Access Control Markup Language

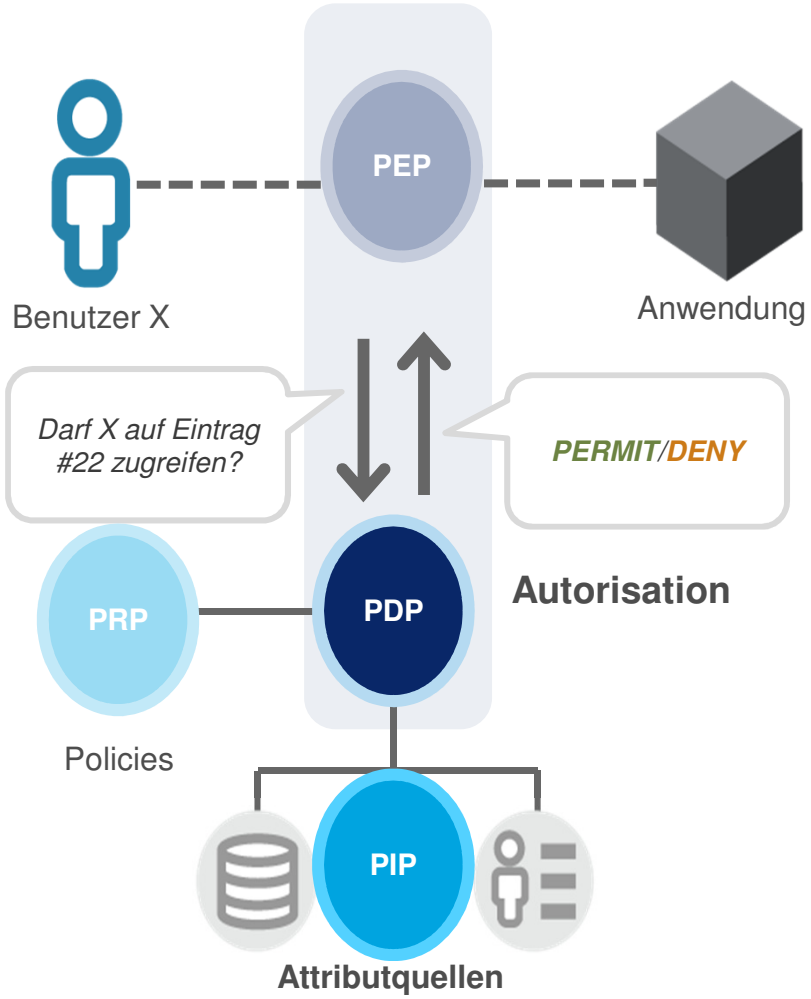
XACML – eXtensible Access Control Markup Language

1. Zugriff auffangen
2. Autorisationsdienst abfragen
3. Autorisationsdienst prüft Anfrage gegenüber vorhandene Policies
4. Unter Umständen auch externe Attributquellen abfragen
5. Eine Entscheidung– PERMIT oder DENY – wird abgegeben



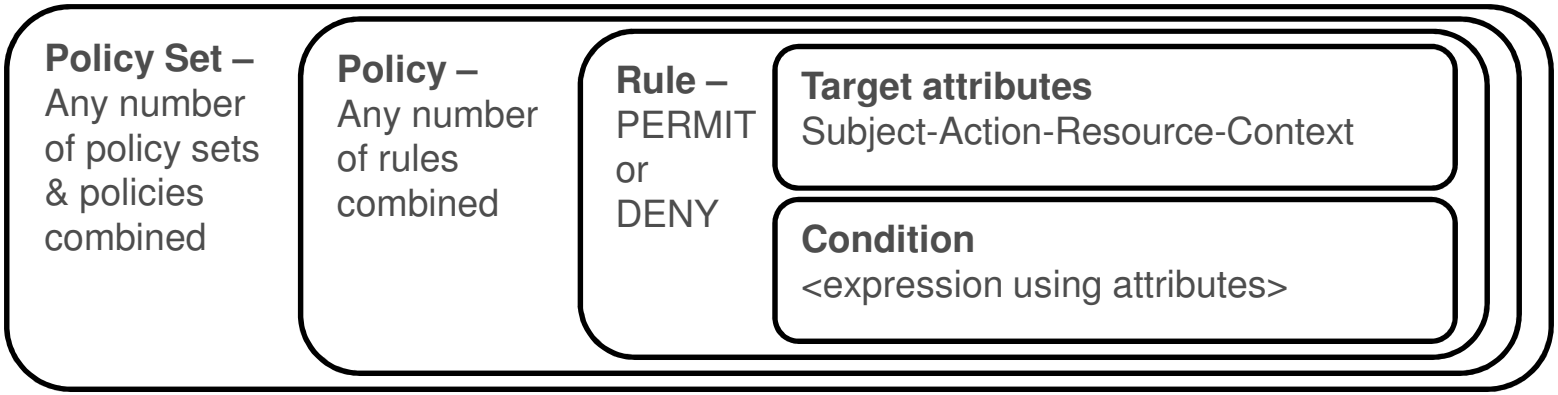
XACML – eXtensible Access Control Markup Language

PEP – Policy Enforcement Point
PDP – Policy Decision Point
PIP – Policy Information Point
PRP – Policy Retrieval Point

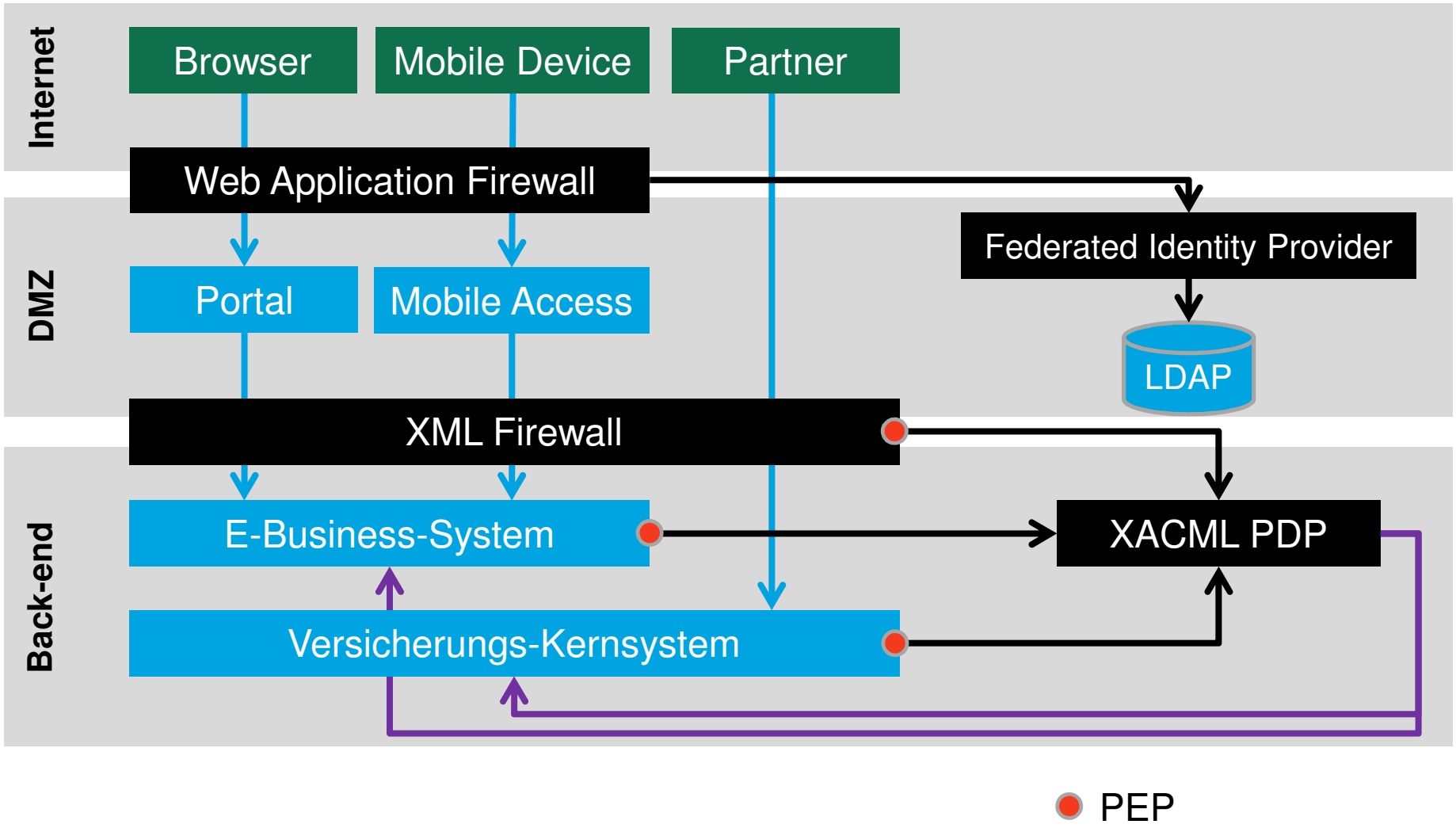


Attribute Based Access Control (ABAC)

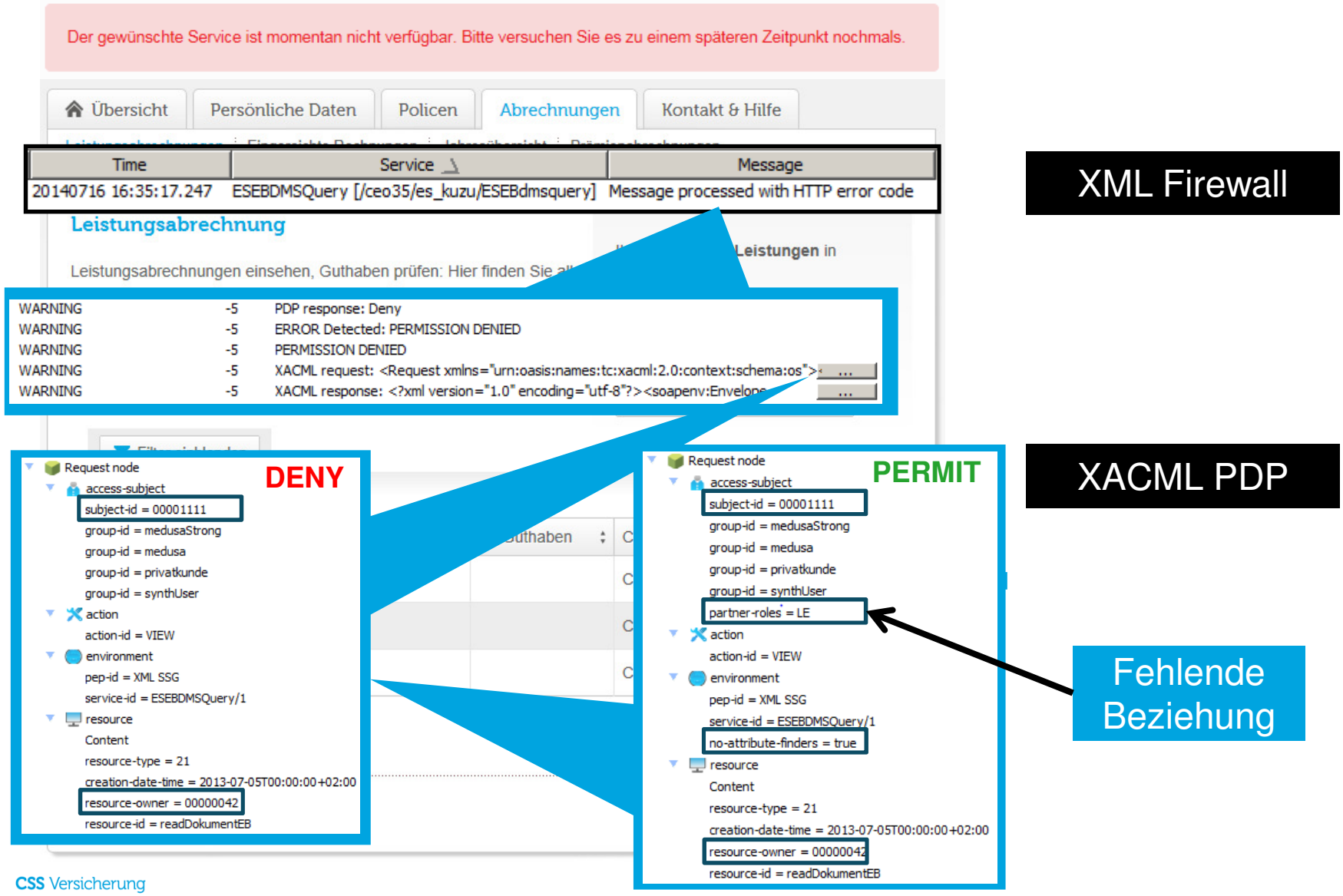
Effect	Subject	Action	Resource	Context	Condition
PERMIT	Doctor	Read	Patient record	Clinic network	Subject.clinic= resource.clinic
DENY	Engineer	Update	Drawing	PDM workstation	Subject.project≠ Resource.project
PERMIT	Bank client	Withdraw	Amount= $500	ATM Machine	Resource.amount< subject.account. balance



Herausforderungen bei E-Business



Sicht auf die Autorisierung



XML Firewall

XACML PDP

Fehlende Beziehung

Erfahrungen und Erkenntnisse

- Security **früh und zentral eingebunden**
- **Schnelle Lieferung in hoher Qualität**
- **Flexibilität** mit guter Testbarkeit
  - Fachlogik ohne Security testbar
  - Autorisierungstestfälle durch Nichttechniker formulierbar
  - Autorisierung in Unit-, Integrations- und Gesamtsystemtests

Fazit

- Die Architektur von ABAC passt sehr gut zu den Anwendungsfällen
- Herausforderungen, welche mit RBAC schlecht oder gar nicht lösbar sind, können mit ABAC elegant umgesetzt werden
- Externalisierter und zentralisierter Zugriffsschutz mit Rollenteilung führt zu einer klaren Separierung der Belange
- Durch die gute Testbarkeit werden bei Änderungen voraussagbare Resultate erzielt

Kennzahlen

67 Dienste aus
14 Applikationen
auf der
XML Firewall

417
Autorisierungs-
policies

2’000’000
Entscheidungen
täglich

Security als Enabler

Fach

IT

Security

Kunde

Herzlichen Dank für Ihre Aufmerksamkeit!

Stefan Allemann
Leiter IT-Security Architektur
CSS Versicherung
stefan.allemann@css.ch

@SierraAlpha_CH