

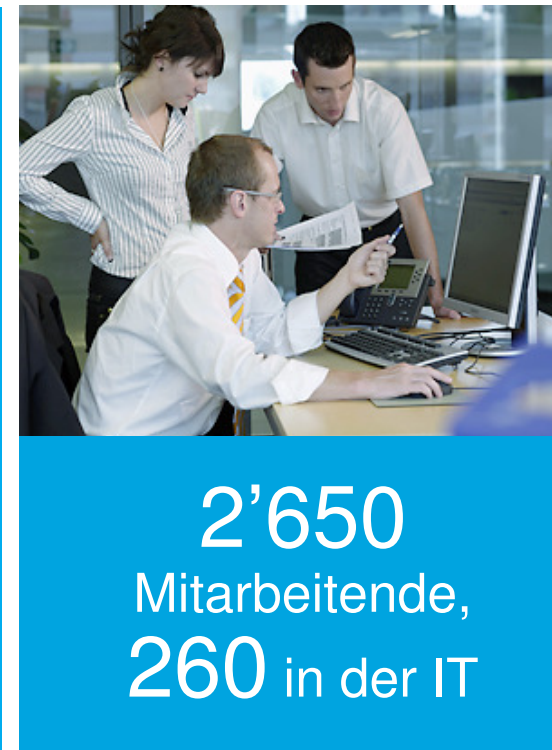
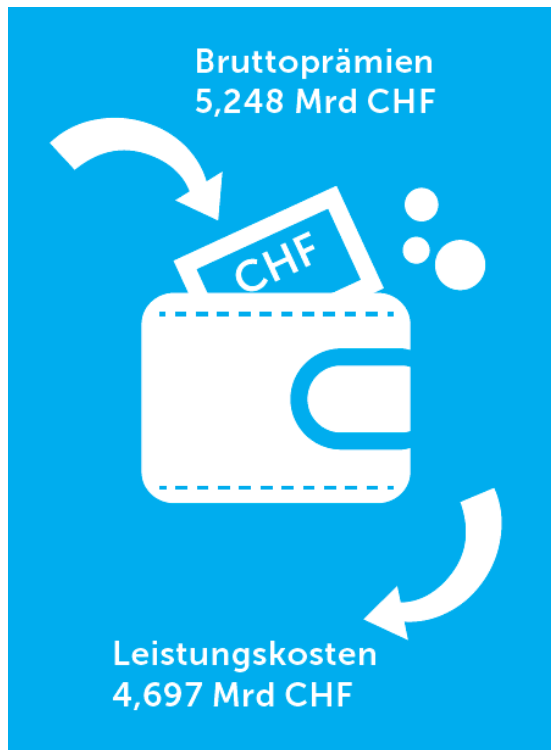
IT-Security als Enabler

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

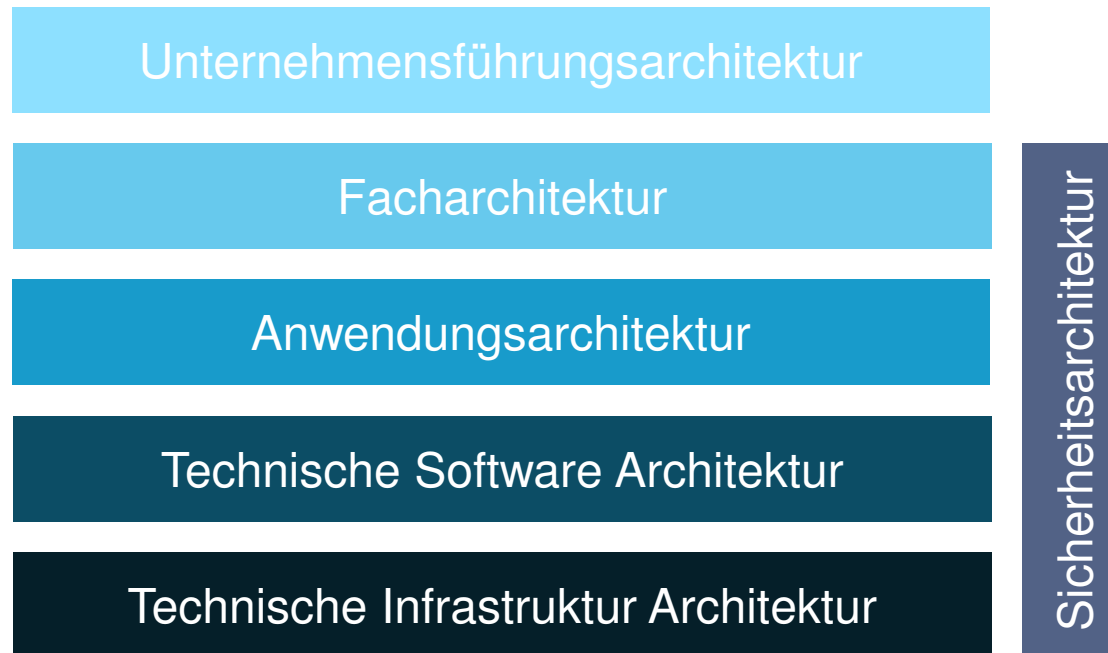
Netclose Community Treffen, Horw, 24.09.2014
Stefan Allemann, CSS Versicherung



CSS Versicherung: Kennzahlen 2013



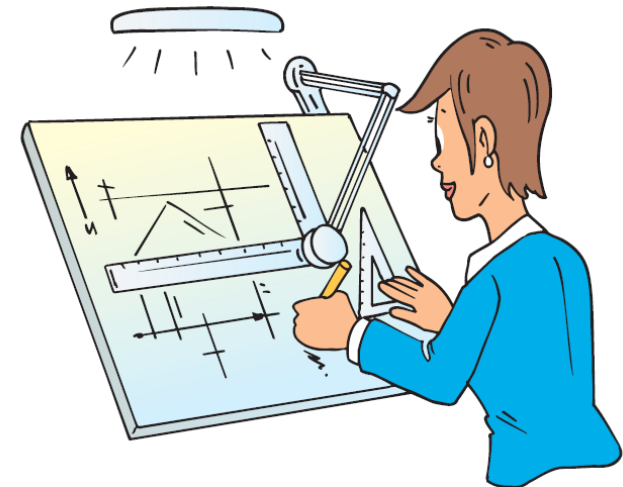
Security-Architektur bei CSS



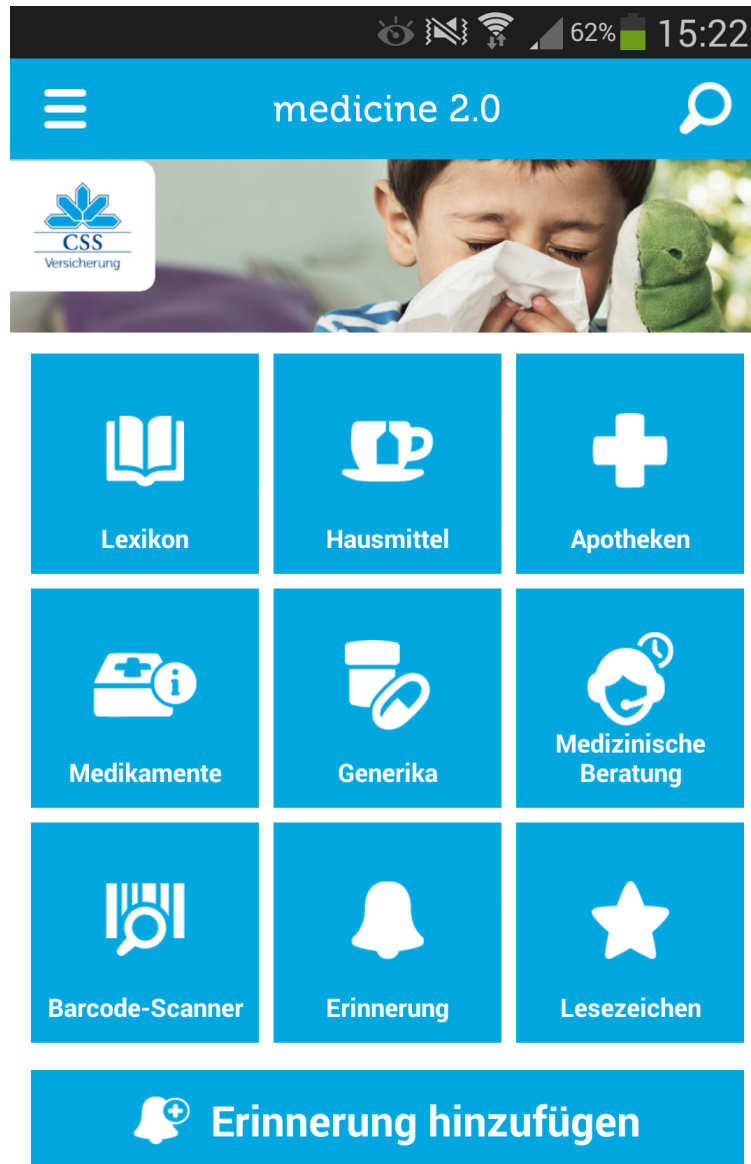
Security-Architektur bei CSS

- **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)



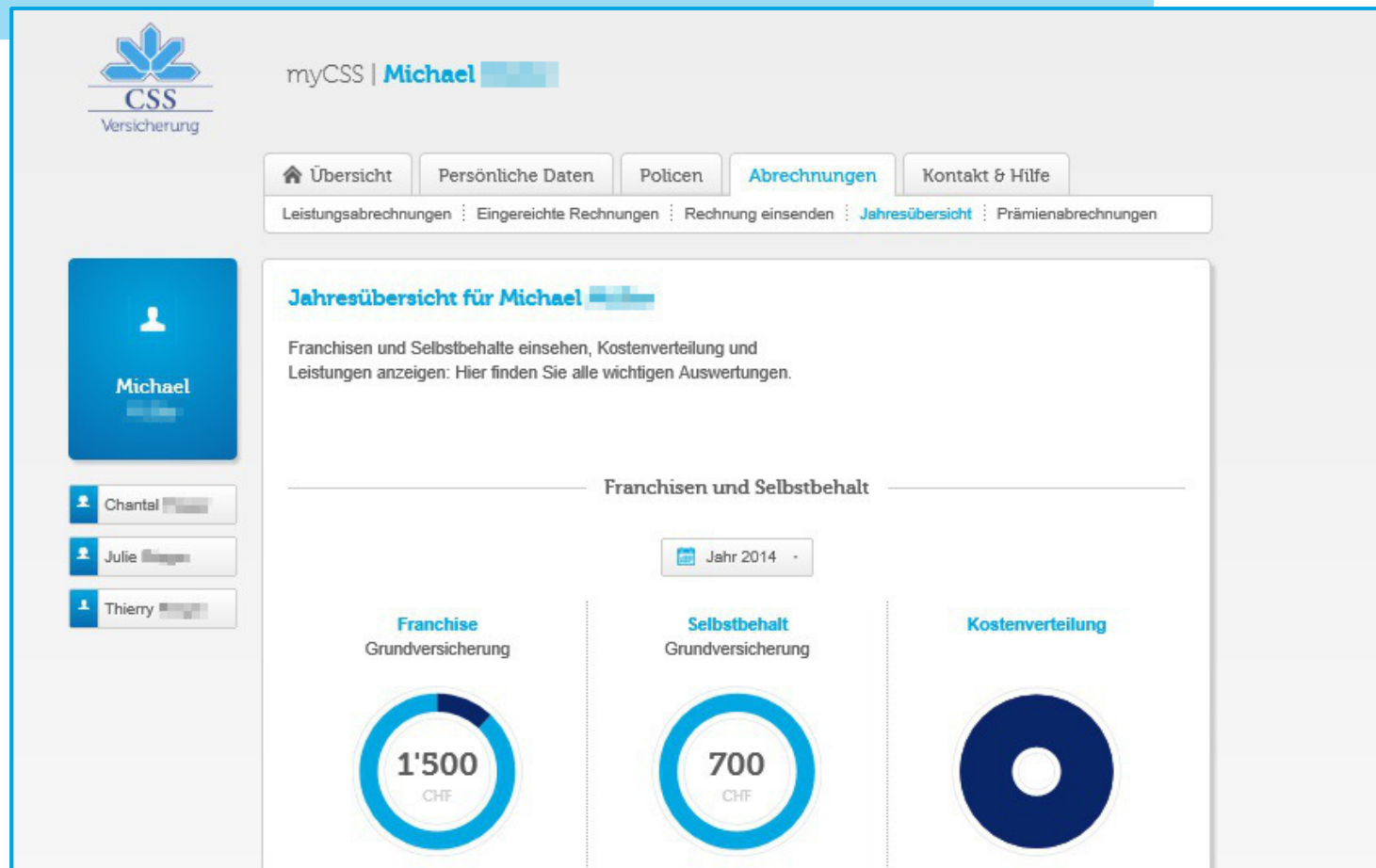
E-Business bei CSS



myCSS – Portal für Privatkunden

Nutzen für Kunden

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



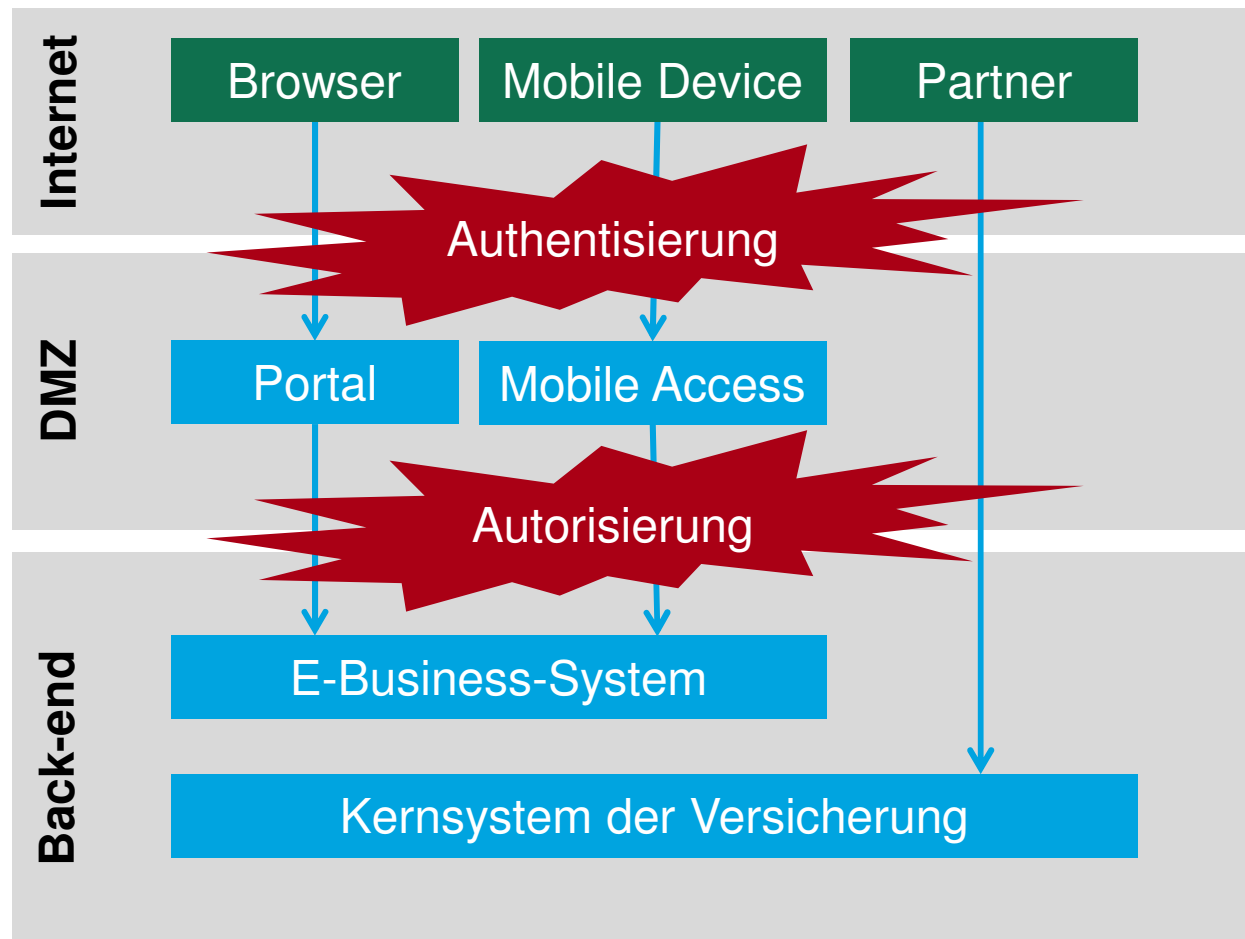
myCSS – Portal für Privatkunden

Herausforderung

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

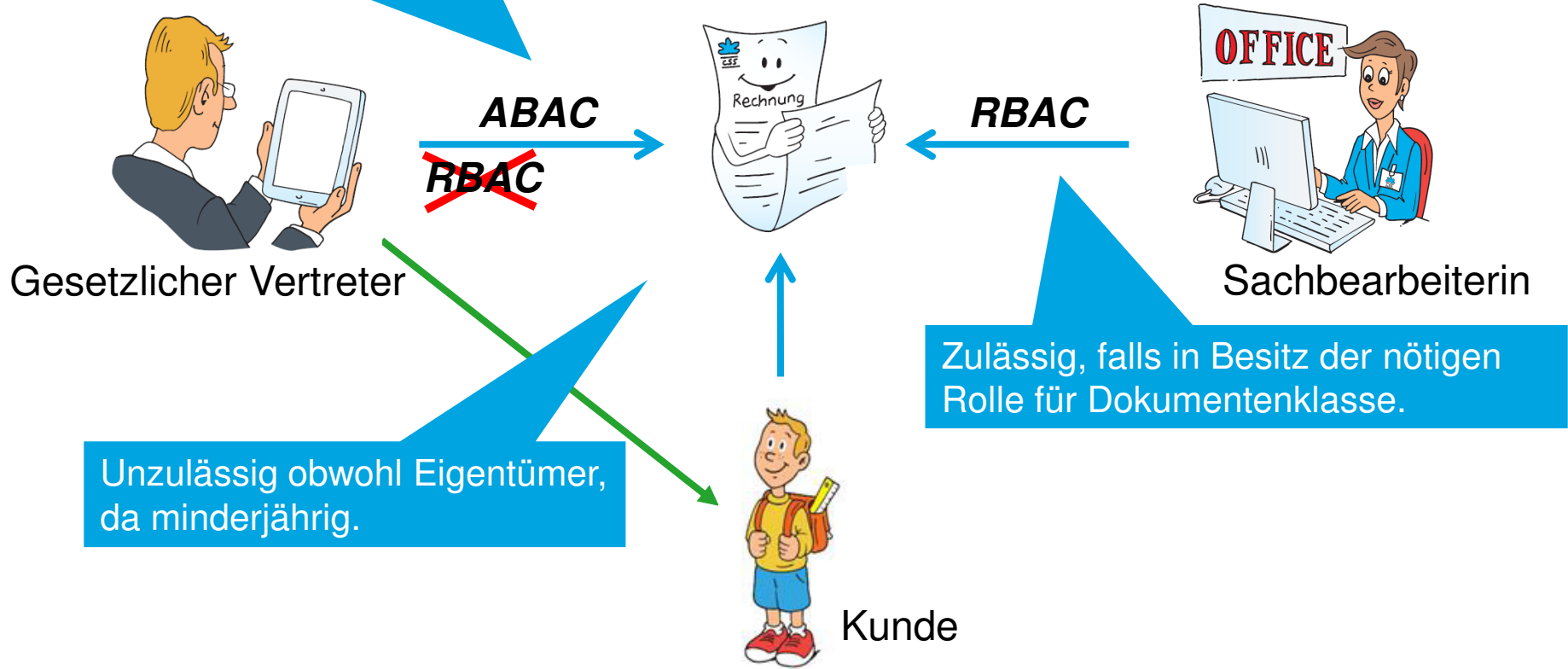
The screenshot displays the myCSS portal interface for a user named Michael. The top navigation bar includes links for 'Übersicht', 'Persönliche Daten', 'Policen', 'Abrechnungen', and 'Kontakt & Hilfe'. Below this, a secondary menu lists 'Leistungsabrechnungen', 'Eingereichte Rechnungen', 'Rechnung einsenden', 'Jahresübersicht', and 'Prämienabrechnungen'. The main content area is titled 'Jahresübersicht für Michael' and contains a description: 'Franchisen und Selbstbehalte einsehen, Kostenverteilung und Leistungen anzeigen: Hier finden Sie alle wichtigen Auswertungen.' A sidebar on the left, highlighted with a red box, shows a profile card for Michael and a list of other family members: Chantal, Julie, and Thierry. The dashboard features three circular charts under the heading 'Franchisen und Selbstbehalt' for the year 2014: 'Franchise Grundversicherung' at 1'500 CHF, 'Selbstbehalt Grundversicherung' at 700 CHF, and 'Kostenverteilung'.

Herausforderungen bei E-Business



Autorisierung von Dokumentenzugriffen

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



Attribute Based Access Control (ABAC)

Beziehung
Teammitgliedschaft

Zuständiges Team

Zugriffsart

Authentisierungsstärke

Benutzeridentität

Rolle

Eigentümer

Erstelldatum

Ressourcentyp

Ressourcenuntertyp

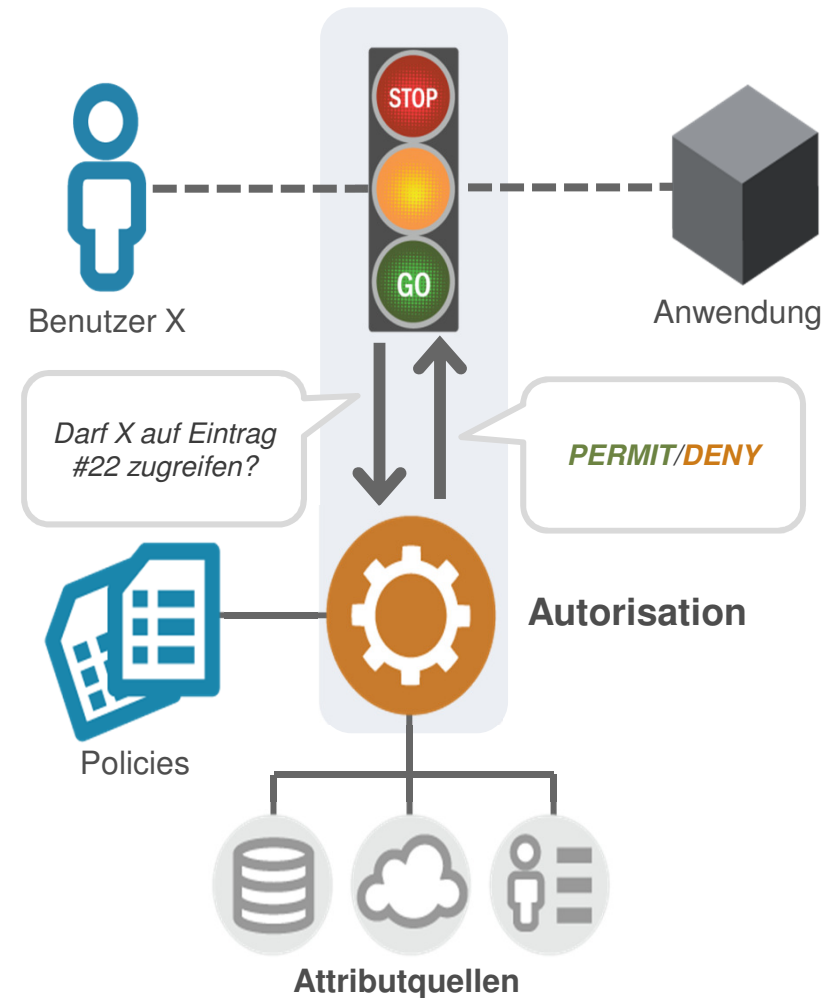
Gerätetyp

Regionale Zuordnung

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



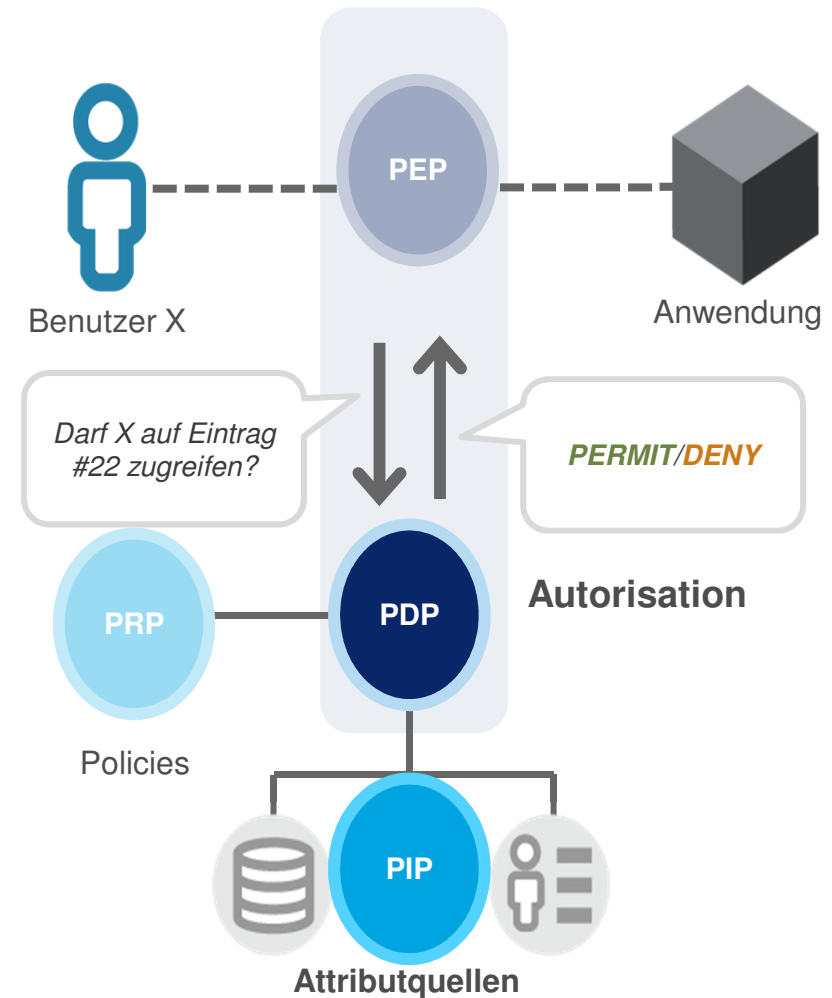
XACML – eXtensible Access Control Markup Language

PEP – Policy Enforcement Point

PDP – Policy Decision Point

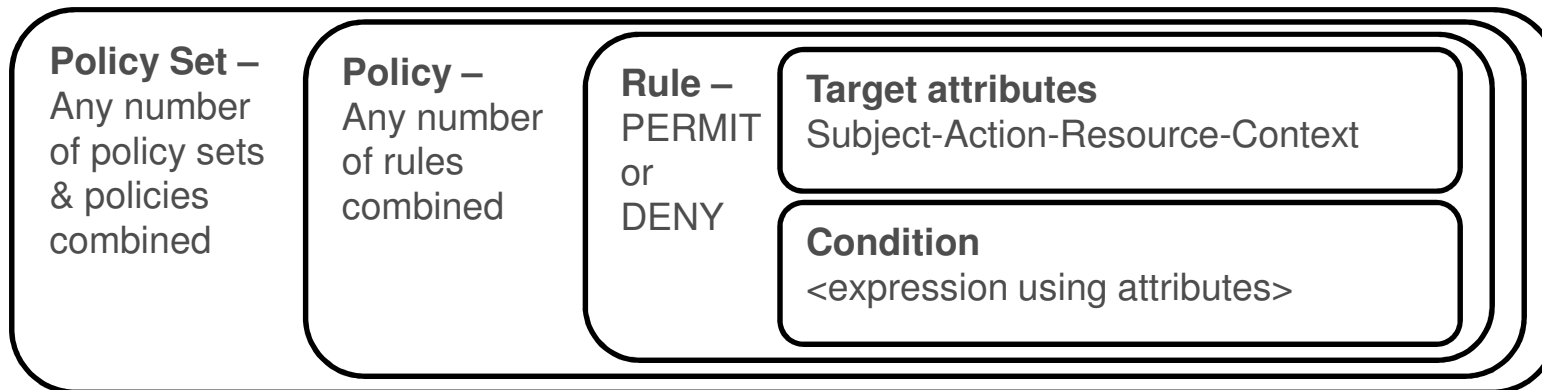
PIP – Policy Information Point

PRP – Policy Retrieval Point

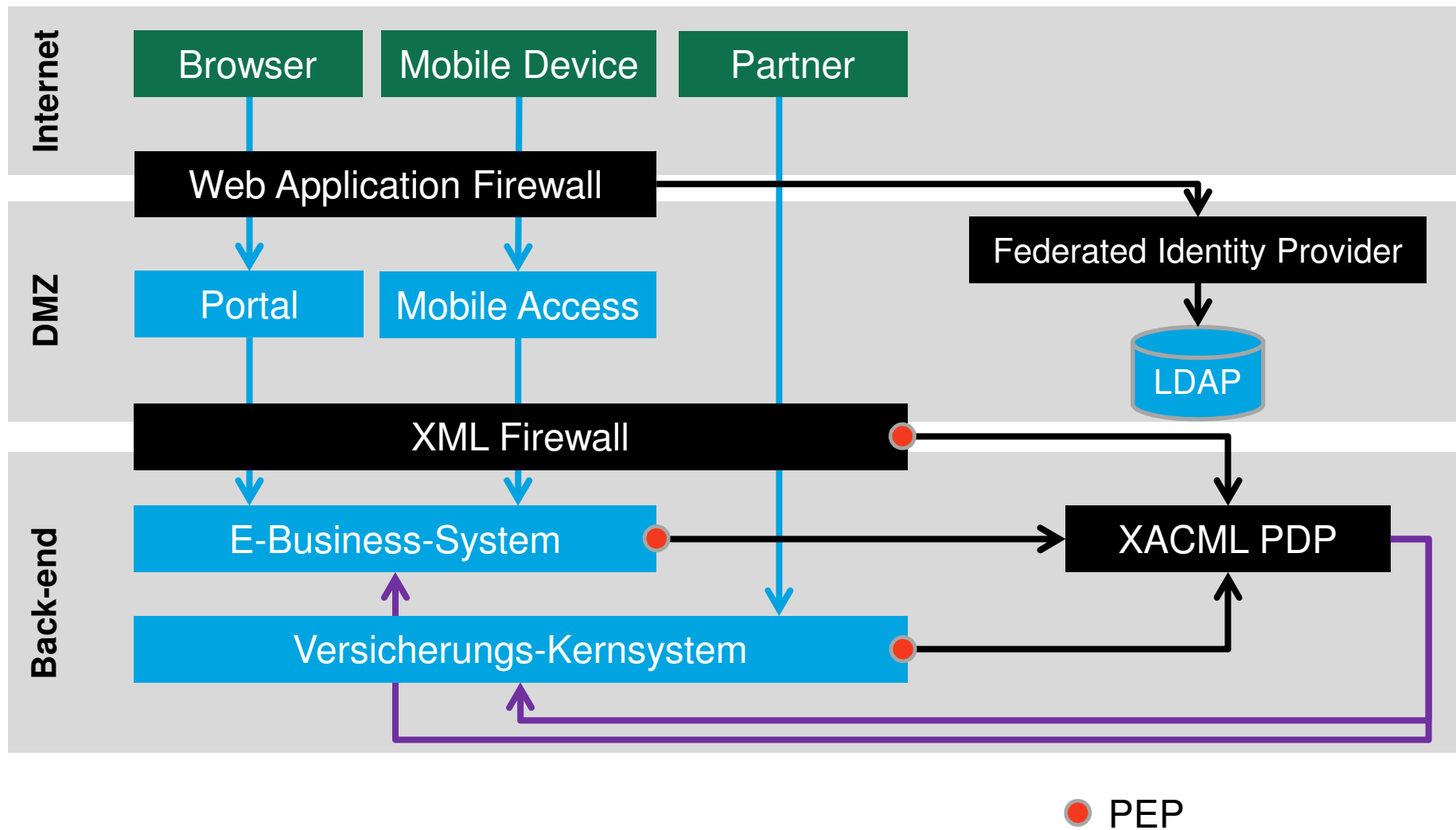


Attribute Based Access Control (ABAC)

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

Der gewünschte Service ist momentan nicht verfügbar. Bitte versuchen Sie es zu einem späteren Zeitpunkt nochmals.

Time	Service	Message
20140716 16:35:17.247	ESEBDMSQuery [/ceo35/es_kuzu/ESEBdmsquery]	Message processed with HTTP error code

XML Firewall

Leistungsabrechnung

Leistungsabrechnungen einsehen, Guthaben prüfen: Hier finden Sie alle Leistungen in

WARNING	-5	PDP response: Deny
WARNING	-5	ERROR Detected: PERMISSION DENIED
WARNING	-5	PERMISSION DENIED
WARNING	-5	XACML request: <Request xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os">...
WARNING	-5	XACML response: <?xml version="1.0" encoding="utf-8"?><soapenv:Envelope...

DENY

- Request node
 - access-subject
 - subject-id = 00001111
 - group-id = medusaStrong
 - group-id = medusa
 - group-id = privatkunde
 - group-id = synthUser
 - action
 - action-id = VIEW
 - environment
 - pep-id = XML SSG
 - service-id = ESEBDMSQuery/1
 - resource
 - Content
 - resource-type = 21
 - creation-date-time = 2013-07-05T00:00:00+02:00
 - resource-owner = 00000042
 - resource-id = readDokumentEB

PERMIT

- Request node
 - access-subject
 - subject-id = 00001111
 - group-id = medusaStrong
 - group-id = medusa
 - group-id = privatkunde
 - group-id = synthUser
 - partner-roles = LE
 - action
 - action-id = VIEW
 - environment
 - pep-id = XML SSG
 - service-id = ESEBDMSQuery/1
 - no-attribute-finders = true
 - resource
 - Content
 - resource-type = 21
 - creation-date-time = 2013-07-05T00:00:00+02:00
 - resource-owner = 00000042
 - resource-id = readDokumentEB

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

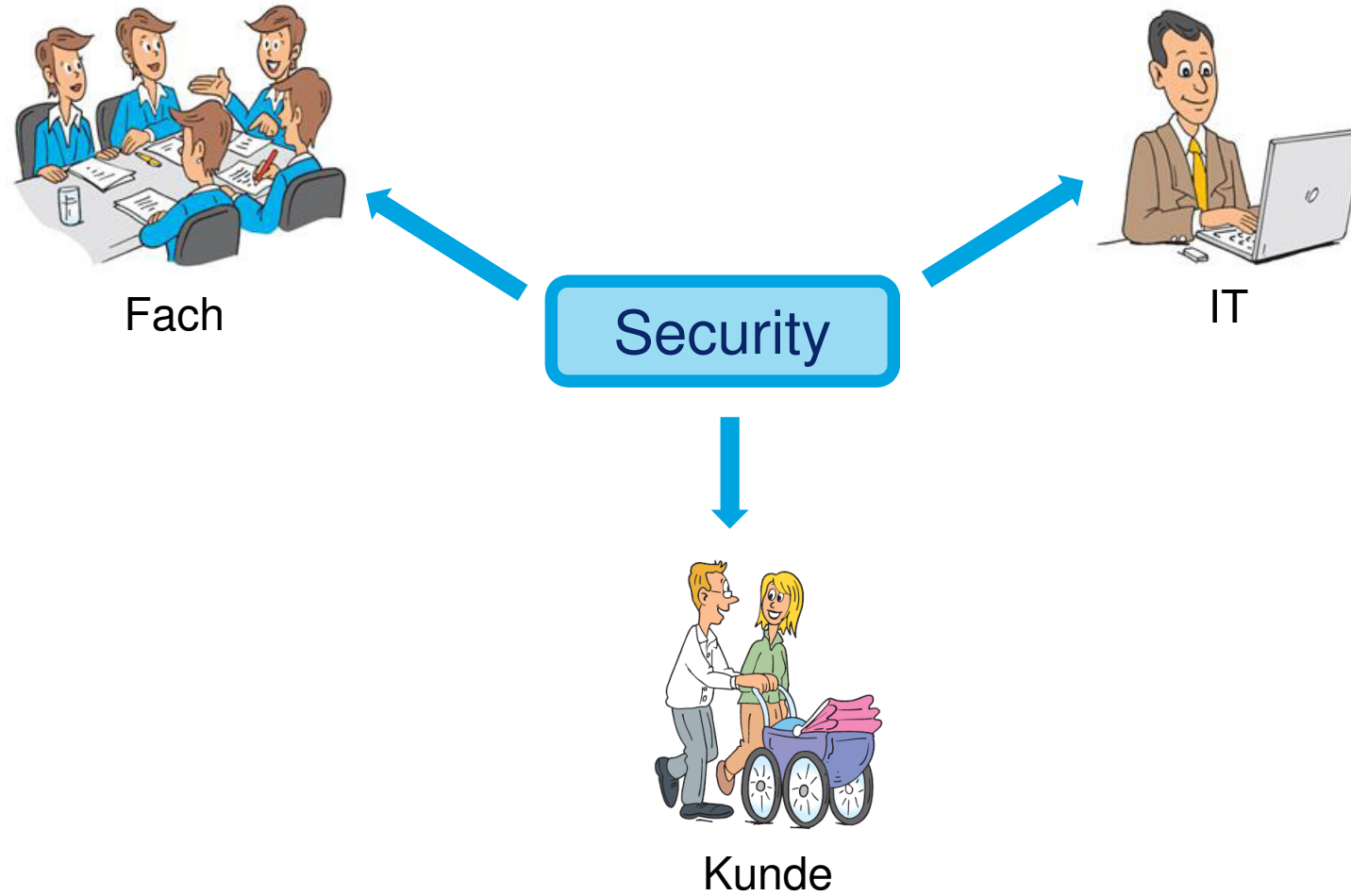
Kennzahlen

67 Dienste aus
14 Applikationen
auf der
XML Firewall

417
Autorisierungs-
policies

2'000'000
Entscheidungen
täglich

Security als Enabler



Herzlichen Dank für Ihre Aufmerksamkeit!

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

@SierraAlpha_CH

