

## Erfolgsgeschichten phion airlock – ICAP Module

### Complex Content Rewriting & Identity Mapping



**René Eberhard**  
Dipl. El.-Ing. HTL  
Betriebswirtschafts-Ing. FH NDS  
CEO, Partner

keyon AG  
Schlüsselstrasse 6  
8645 Jona  
Switzerland  
www.keyon.ch

Tel. +41 55 220 64 03  
Mobile +41 79 458 00 45  
Fax +41 55 220 64 01  
eberhard@keyon.ch

About keyon

## information security?

## just relax.

plan  
implement  
enforce  
control



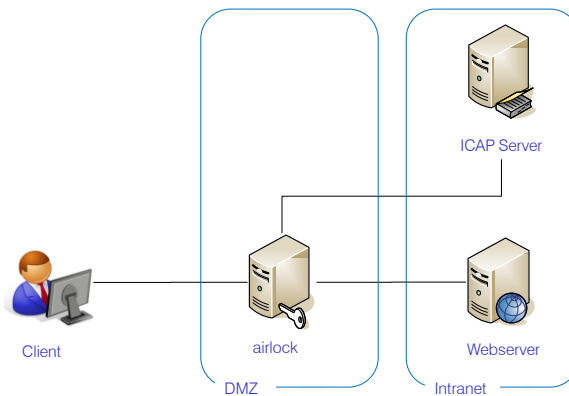
keyon for security reasons  
[www.keyon.ch](http://www.keyon.ch) / [info@keyon.ch](mailto:info@keyon.ch)

Internet Content Adaptation Protocol (ICAP)

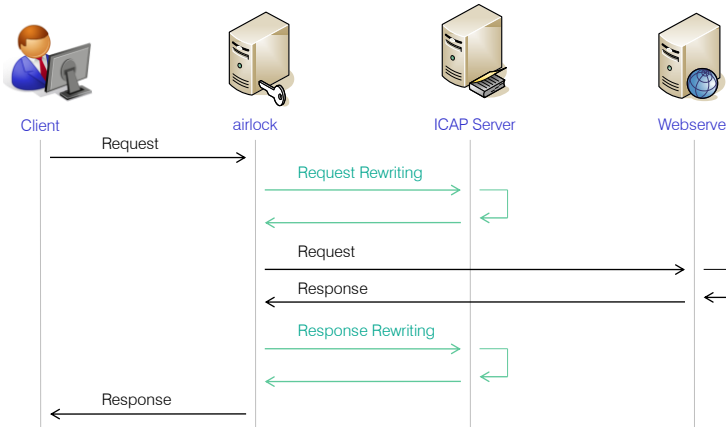
airlock & ICAP 1 – Complex Content Rewriting

airlock & ICAP 2 – Authentifizierung und Identity Mapping

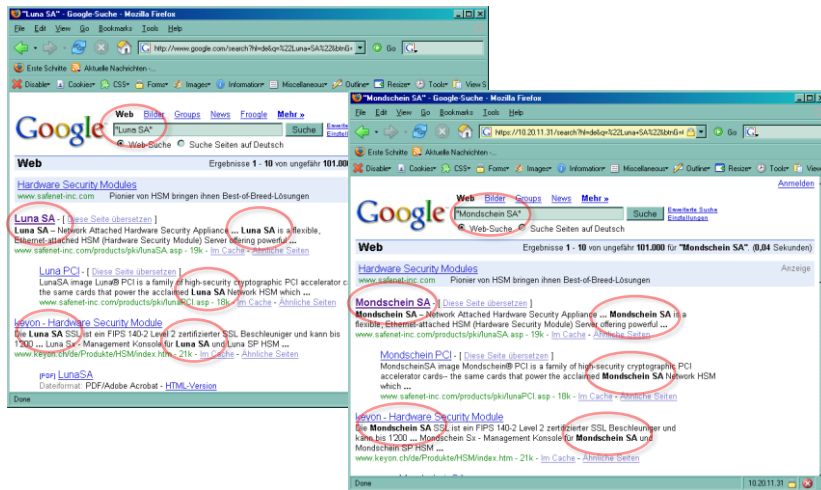
■ Übersicht – airlock ICAP Client (1/2)



### Übersicht – airlock ICAP Client (2/2)



### Übersicht – airlock ICAP Client – Simple Content Rewriting



## Agenda

Internet Content Adaptation Protocol (ICAP)

airlock & ICAP 1 – Complex Content Rewriting

airlock & ICAP 2 – Authentifizierung und Identity Mapping

## Erfolgsgeschichte 1

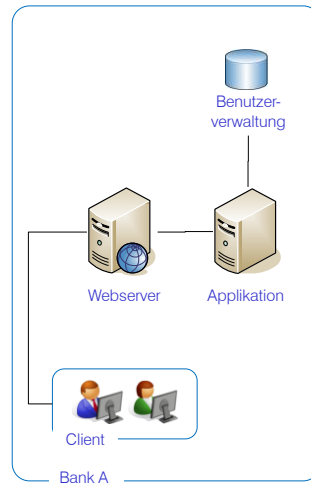
### ■ Ausgangslage

Schweizer Bank

Internationale Handelsapplikation von Finanzprodukten und Derivaten im Bereich B2B

Webapplikation (HTML basiert, keine Webservices oder analoge Schnittstellen vorhanden)

■ Ausgangslage



■ Zielsetzung

Bereitstellen der Applikation an Partnerbanken.

Partnerbank spezifisches look & feel

Partnerbank spezifische Kundendaten bleiben bei der Partnerbank

Partnerbank spezifische Administration von Rollen und Rechten

■ **Auswirkung**

Bereitstellen der Applikation an Partnerbanken

Zugriff von aussen – Sichern der eigenen Applikation und der Applikation der Partnerbanken

Partnerbank spezifisches look & feel

Dezentrale Anpassung der grafischen Oberfläche

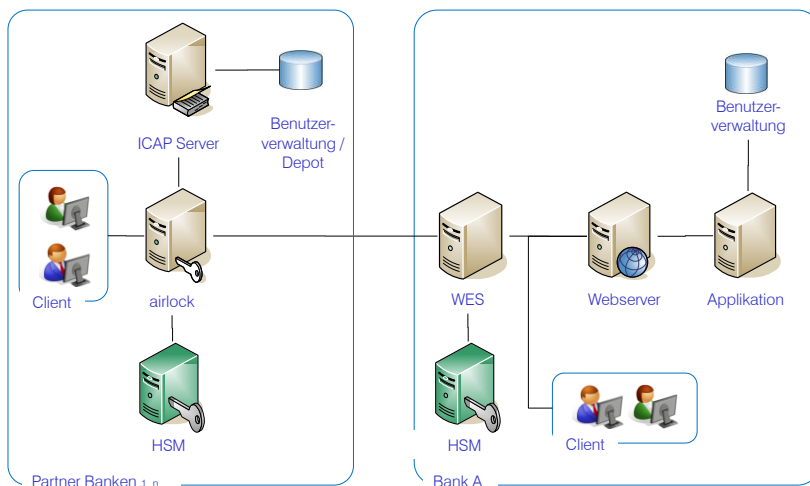
Partnerbank spezifische Kundendaten bleiben bei der Partnerbank

Dezentrale Anonymisierung aller kundenspezifischen Daten

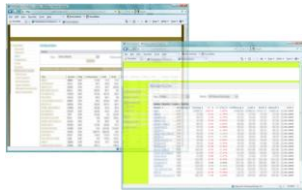
Partnerbank spezifische Administration von Rollen und Rechten

Dezentrale, partnerbankspezifische Vergabe von Rechten und Rollen

■ **Zielsetzung**

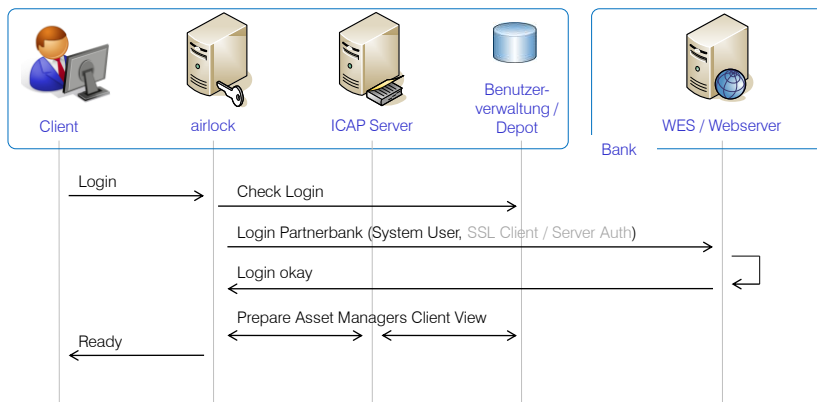


■ **Resultat**



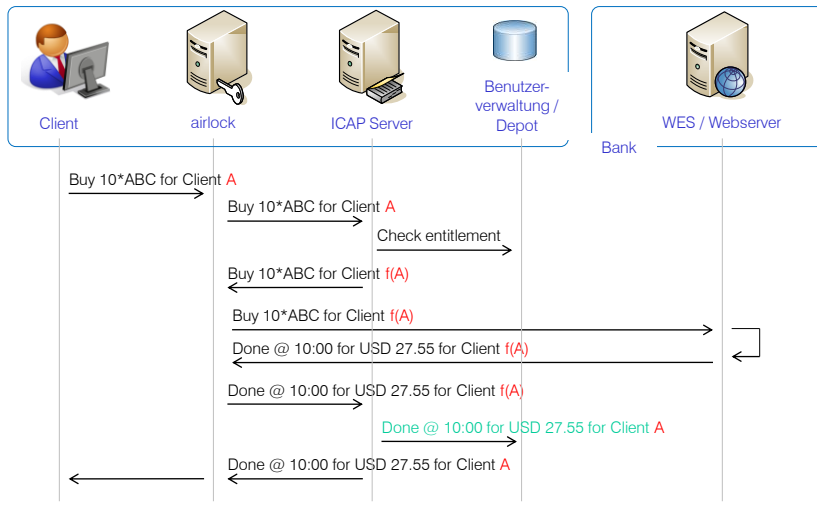
Es ist nicht „nur“ HTML Rewriting sondern eine Erweiterung und Anpassung der Applikations- und Berechtigungslogik

■ **Umsetzung Login – Vereinfachte Darstellung**



Der Asset Manager sieht „seine“ Kunden und kann entsprechende Transaktionen auslösen.

■ Umsetzung Transaktion – Vereinfachte Darstellung



■ Schlussfolgerung

airlock im Verbindung mit ICAP ist ein äusserst mächtiges Werkzeug (XML Validation, Content Filtering, etc.)



## Agenda

Internet Content Adaptation Protocol (ICAP)

airlock & ICAP 1 – Complex Content Rewriting

airlock & ICAP 2 – Authentifizierung und Identity Mapping

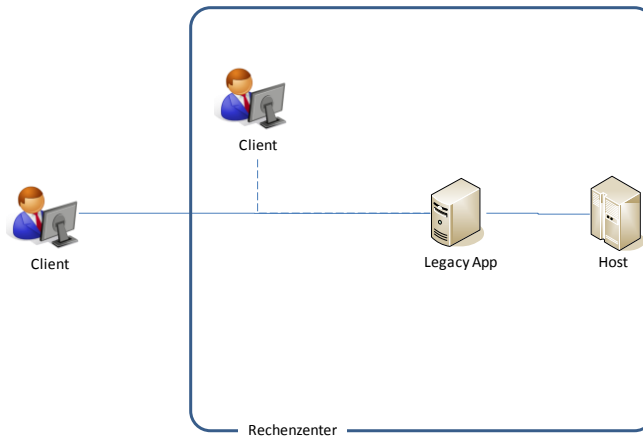
## Erfolgsgeschichte 2

### ■ Ausgangslage

Rechenzentrum

Bereitstellen von Webservices an interne und externe Kunden

■ Ausgangslage



■ Zielsetzung

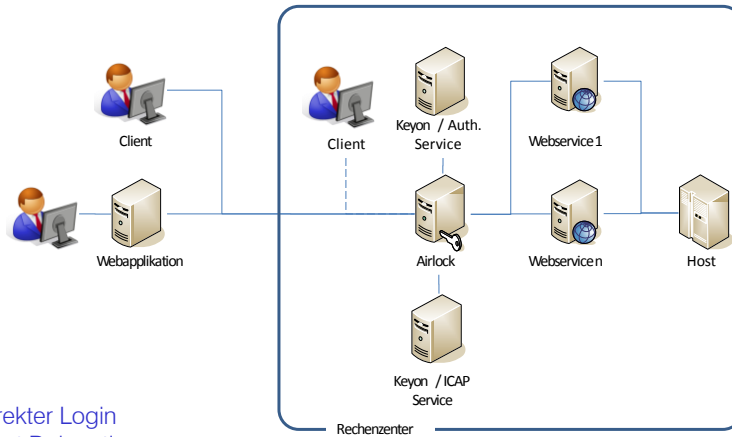
Bereitstellen einfacher Schnittstellen für die Nutzung der Host Applikationen über Webservices (WSDL)

Einheitliche Authentifizierung gegenüber Host Systemen, unabhängig von der Authentifizierung der Kunden

Unterstützung bestehender SOA Infrastrukturen

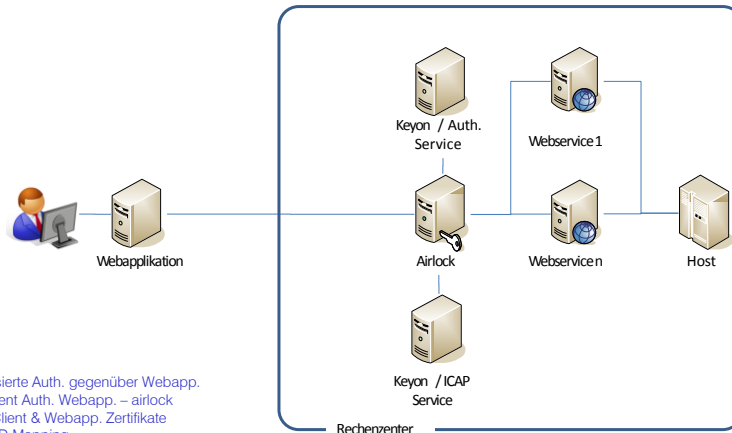
Unterstützung unterschiedlicher Sicherheitszonen

Zielsetzung



- Direkter Login
- Trust Delegation
- Unterstützung unterschiedlicher Auth. Verfahren und CAS

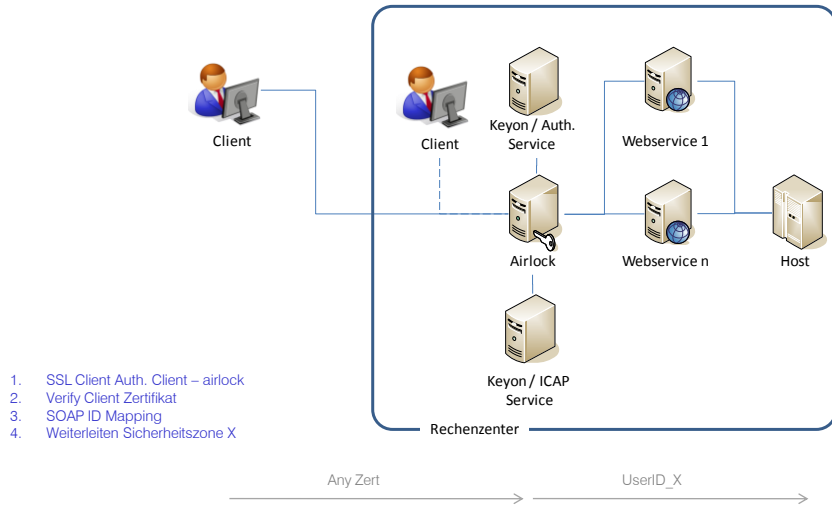
Umsetzung – Authentifizierungsverfahren 1 - Zertifikat



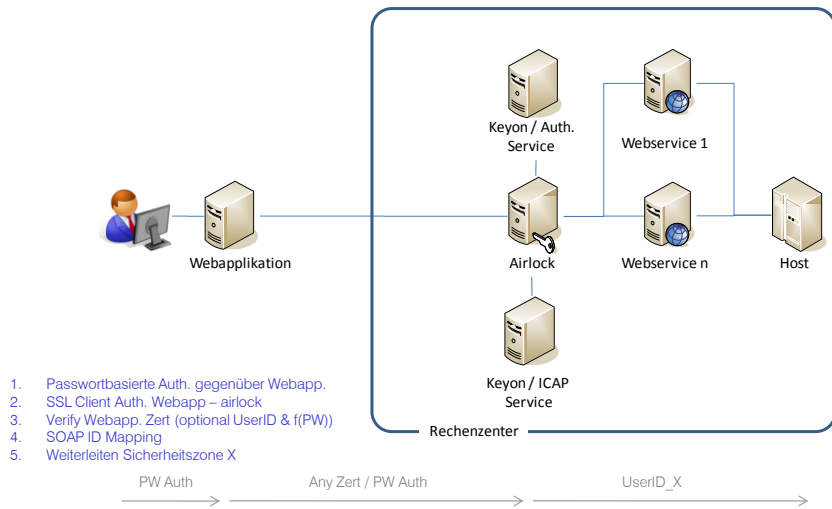
1. Zertbasierte Auth. gegenüber Webapp.
2. SSL Client Auth. Webapp. – airlock
3. Verify Client & Webapp. Zertifikate
4. SOAP ID Mapping
5. Weiterleiten Sicherheitszone X



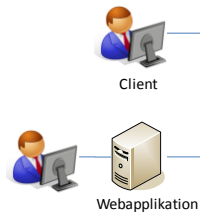
■ Umsetzung – Authentifizierungsverfahren 2 - Zertifikat



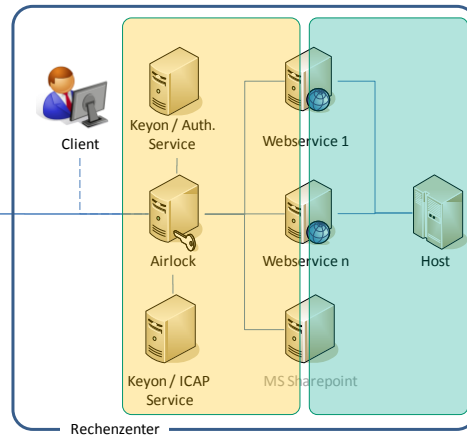
■ Umsetzung – Authentifizierungsverfahren 3 - Passwort



■ Schlussfolgerung



- Einheitlicher Login gegenüber Webservices
- Einheitlicher Login gegenüber Host



■ Schlussfolgerung

Einfache Umsetzung mit airlock & ICAP

Einfache Integration des umfassenden Authentifizierungs- und Identitymapping Frameworks von Keyon in airlock


Einfache Bereitstellung der Applikationen an interne und externe Kunden (WSDL)

Kostengünstiger Betrieb

Vielen Dank für Ihre Aufmerksamkeit



Bei Fragen stehen wir Ihnen gerne zur Verfügung.

 for security reasons