

# MODERNE PKI-ARCHITEKTUR AN EINER HOCHSCHULE

Hochschule für angewandte Wissenschaften München

---

Florian Ritterhoff

Prof. Dr.-Ing. Thomas Schreck

09. Februar 2023



# Gliederung

1. Einleitung

2. Architektur

3. Umsetzung

4. Betrieb an der Hochschule

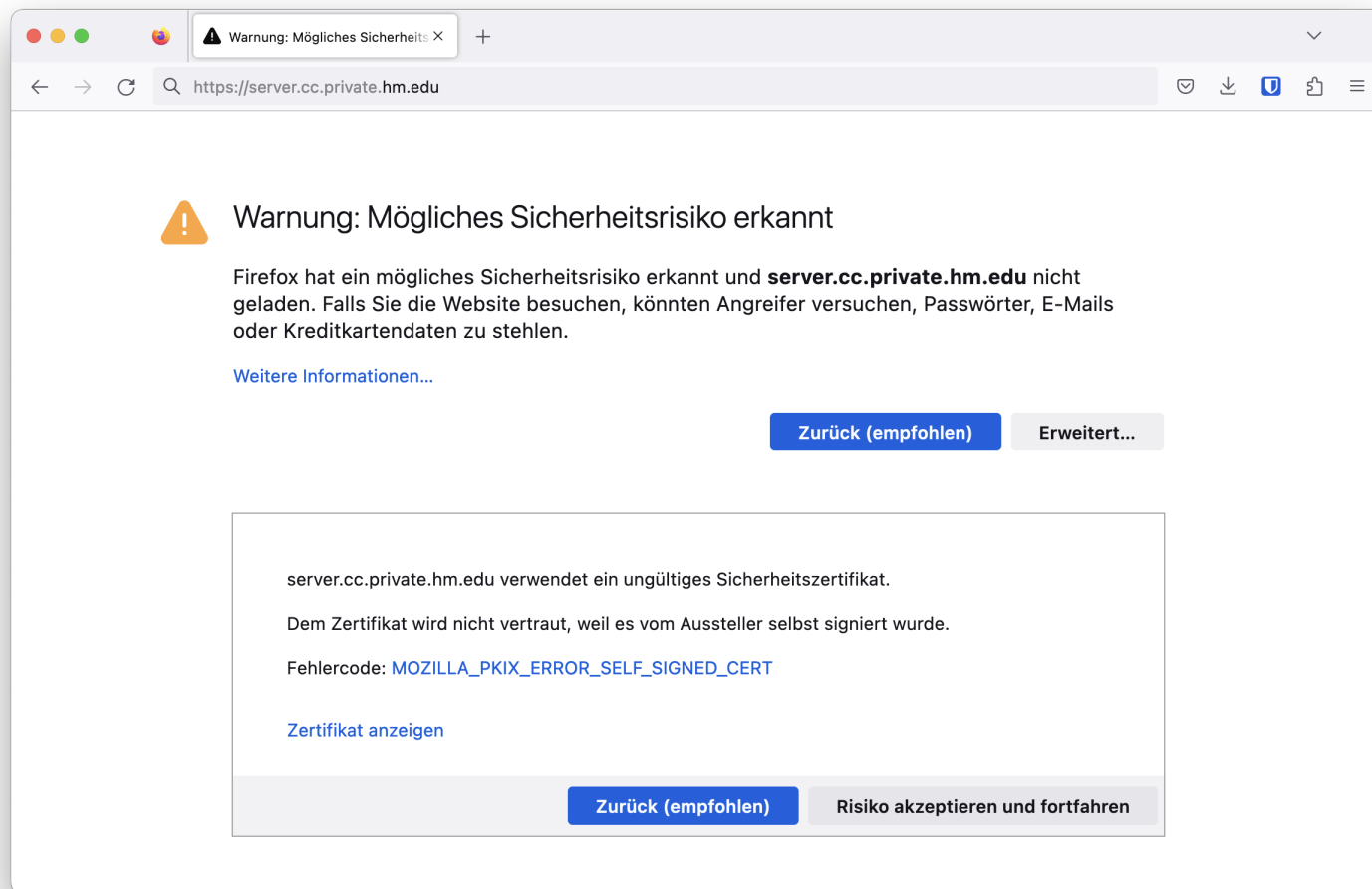
5. Zusammenfassung

# Motivation

... ein typischer interner Server an einer Hochschule ...

# Motivation

... ein typischer interner Server an einer Hochschule ...



# Hintergrund

- Bislang vornehmlich DFN-PKI, Let's Encrypt oder selbst signierte Zertifikate
- DFN-PKI bedeutet(e) manuelle Arbeit für zentrale IT und Systembetreiber
- Abschaltung der DFN-PKI
  - Serverzertifikate:  
31.12.2022
  - Benutzerzertifikate:  
30.08.2023 (*wegen neuer SMIME BR von CA/Browser Forum!*)  
⇒ Zukunft ungewiss; Vergleichsweise hohe Anforderungen!

# Hintergrund

- **Nachfolger:** GÉANT Trusted Certificates Service (TCS)
    - Derzeit Anbieter *sectigo*
    - Nicht direkt kompatibel mit Strukturen einer Hochschule
    - ACME Verfahren ohne Challenges, (damals) ohne Nachvollziehbarkeit und sehr langsam
  - **Alternative für Serverzertifikate:** Let's Encrypt
    - Für interne Server nicht möglich und keine zentrale Verwaltung vorhanden
- ⇒ Konzept für Einsatz von GÉANT TCS und Ersatz für Let's Encrypt notwendig

# Ziele

- Eigenständige Verwaltung der Zertifikate
- Automatisierung von Prozessen
- „Verbergen“ von Schnittstellen, Oberflächen und Prozessen bei *sectigo*
- Anbieterunabhängigkeit
- Reduktion der Anfragen an zentrale IT

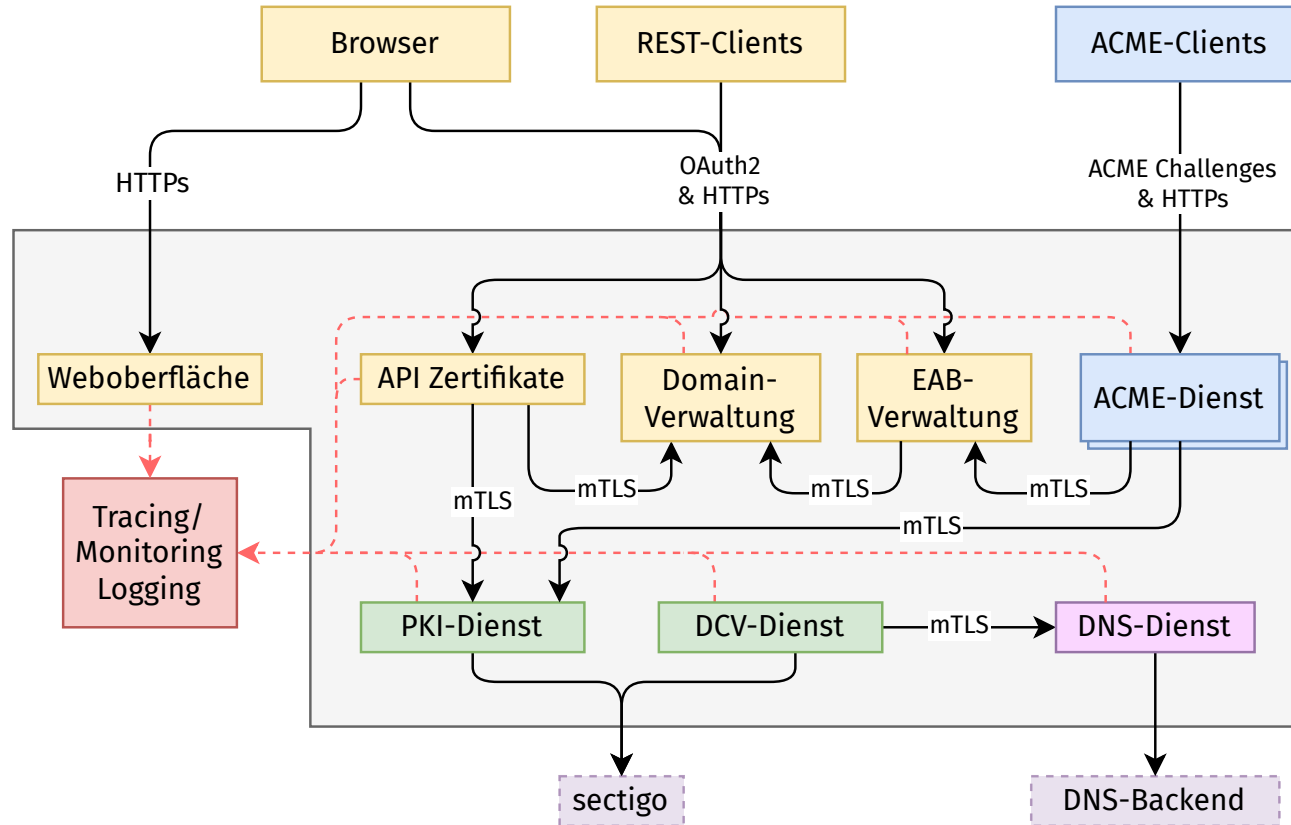
# Grundlagen

- Trennung zwischen „Backend“ und „Frontend“
- Realisierung einzelner Funktionen in einzelnen Anwendungen/Diensten („Microservices“)
- Ausführung aller Funktionalitäten in eigenen Containern
- Kommunikation Backend-Frontend mittels REST-API
- Anbindung an zentralen Shibboleth





# Gesamtarchitektur



# Backend

- Trennung zwischen verschiedenen Funktionalitäten:
  - REST-API Domainverwaltung
  - REST-API EAB-Verwaltung
  - REST-API Zertifikatsverwaltung
- ACME Dienst
- Zertifikats Backend
- Validierungsservice
- DNS Dienst

# Backend

Modularer Aufbau ermöglicht einfache Austauschbarkeit & Erweiterung

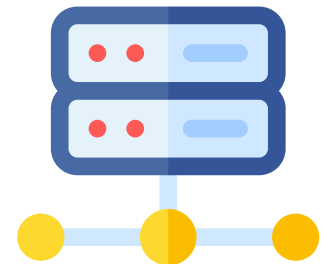
- z.B. Anstelle von Dynamic DNS Updates mittels AXFR Dienst mit REST-API  
→ lediglich Austausch von DNS Dienst
- z.B. Möglichkeit der Integration vorhandener Domainverwaltungen
- z.B. (hoffentlich) Abbildung von SMIME BR Anforderungen

# Eigener ACME Dienst

- Erzwingen von HTTP-Challenges sowohl für interne als auch für öffentliche Systeme
- Keine Wildcardzertifikate, da keine Schnittstelle zu DNS
- Verknüpfung mit internem PKI Dienst & Einsatz von External Account Bindings  
⇒ Nachvollziehbarkeit zwischen ...
  - Zertifikat
  - EAB-Daten
  - Endnutzer

# Anbindung an *sectigo*

- Verwendung von REST-API für sämtliche Operationen
    - Zeitvorteil bei Serverzertifikaten im Vergleich zu ACME
    - Nicht dokumentiertes „Graylisting“ von Zertifikatsanträgen bei bestimmten Schlüsselwörtern
  - Verwendung von CSRs für Server- und Benutzerzertifikate
- ⇒ Änderungen bei *sectigo* bleiben Endanwendern verborgen



# Frontend

- Bietet den Endnutzern Funktionalitäten aufbauend auf eigener REST-API
- Integrierte Generierung von CSR sowie PKCS#12 Dateien mittels Web-Crypto API bzw. nativer JavaScript Bibliothek
  - ⇒ Einfache Generierung von Zertifikaten auch für unerfahrene Admins
  - ⇒ Privater Schlüssel verlässt nie System des Endnutzers, jedoch kein Key-Recovery möglich!

# Absicherung der Kommunikation

- OpenID Connect und OAuth2 für REST-APIs

Im Detail: Shibboleth Plugin & entsprechende Konfiguration für OAuth2 Funktionalitäten.



# Auführungsumgebung

- Produktiv verwendet:
  - Kubernetes Cluster mit Istio Service Mesh
- Technisch möglich:
  - Verwendung von **docker-compose** (primär Entwicklungsumgebung)
  - Bare-Metal
- Weitere Anforderungen
  - PostgreSQL Datenbank
  - OIDC SSO



# Einführung an der HM

- Probebetrieb seit 20. Oktober 2022
- Interne Deaktivierung der DFN-PKI zum 7. November
- Zuordnung von Domains an zuständige IT-Betreuer der Fakultäten
- Dokumentation von Funktionalitäten in Confluence
- Support und Schulung für Kollegen



# Aktueller Stand

- $\approx$  330 versch. FQDNs registriert
- $\approx$  180 Serverzertifikate ausgestellt  
Überwiegender Anteil manuell per Web-UI; Geringer Anteil per ACME
- $\approx$  50 Benutzerzertifikate



# Erfahrungen

- Geringe Verwendung von ACME aufgrund ...
  - ... umständlicher Migration von bestehenden Konfigurationen zu ACME im Vergleich zu einfachen Dateiaustausch
  - ... mehr Parameter als bei Let's Encrypt, da eigener Server und External Account Bindings
  - ... „unbekannte Technik“
  - ... technisch nicht möglich



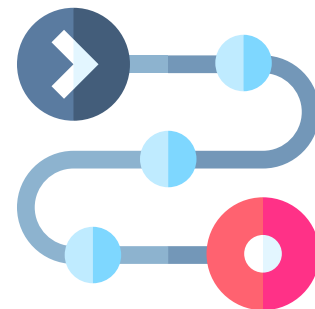
# Erfahrungen

- Bislang:  
Teilweise Verwendung von gleichem Zertifikat für Shibboleth und Webserver  
  
⇒ Bezug und nicht abgesprochener Austausch von Zertifikat führt zu defekten Service Providern



# Roadmap

- Engere Verzahnung mit IDM/LDAP:
  - z.B. Aktionen bei Ausscheiden von Nutzern
    - ⇒ Widerrufen von Nutzerzertifikat(en)
    - ⇒ ggf. Transfer von Domainverantwortlichkeiten
- Anbieten einer (internen) Suche für Nutzerzertifikate
- Realisierung von „Erinnerungs-E-Mails“
- Setzen von CAA Record: Verbot von Let's Encrypt



# Ausblick

- Anbindung von Smartcards (YubiKey)
- Integration von DFN Community PKI via SOAP für Shibboleth Service Provider

# Vorführung der Anwendung

# Zusammenfassung

- Modulare Architektur, die offen ist für Erweiterungen
- Anbieterunabhängigkeit und Benutzerfreundlichkeit durch Integration aller Prozesse in Weboberfläche und Anbieten eines eigenen ACME Dienstes
- Realisierung einer kompletten Middleware zwischen *sectigo* und der Hochschule München



# Zusammenfassung

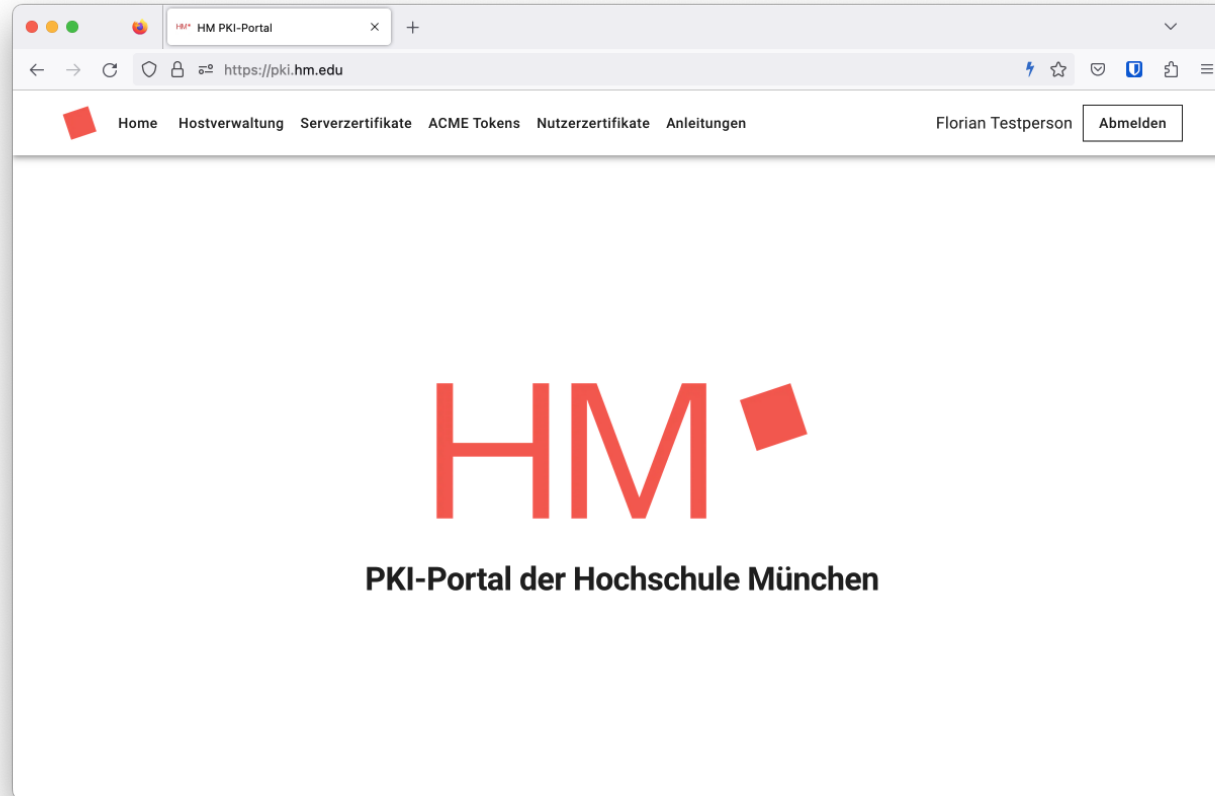
- Veröffentlichung aller Komponenten auf GitHub
  - Frontend: <https://github.com/hm-edu/portal-frontend>
  - Backend-Dienste: <https://github.com/hm-edu/portal-backend>
  - ACME-Dienst: <https://github.com/hm-edu/certificates>
  - **docker-compose**-Deployment: <https://github.com/hm-edu/portal-deployment>
- ⇒ Einsatz und Weiterentwicklung durch Community möglich und erwünscht





Vielen Dank für die Aufmerksamkeit!  
Fragen?

# Screenshots



# Screenshots

The screenshot shows a web browser window with the URL `https://pki.hm.edu/domains`. The page title is "HM PKI-Portal". The navigation menu includes "Home", "Hostverwaltung", "Serverzertifikate", "ACME Tokens", "Nutzerzertifikate", and "Anleitungen". The user is logged in as "Florian Testperson" and has an "Abmelden" button.

## Ihre Hosts

Suchen...

FQDN ↑	Inhaber	Bestätigt	Aktionen
hamburg.cc.private.hm.edu	f.testperson@hm.edu	✓	Freischalten  Löschen <b>Delegationen bearbeiten</b> Zustand
mail.hamburg.cc.private.hm.edu	f.testperson@hm.edu	✓	Freischalten  Löschen <b>Delegationen bearbeiten</b> Zustand

Zeilen pro Seite: 50 1-2 von 2

Neuer Host \*

Erstelle Host

# Screenshots

The screenshot shows a web browser window with the URL `https://pki.hm.edu/server`. The page title is "HM PKI-Portal". The navigation menu includes "Home", "Hostverwaltung", "Serverzertifikate" (highlighted), "ACME Tokens", "Nutzerzertifikate", and "Anleitungen". The user is logged in as "Florian Testperson" and there is an "Abmelden" button.

## Ihre Serverzertifikate

Common Name	Serial Number	Status	Erstellt ↓	Gültig ab	Gültig bis	Subject Alternative Name
hamburg.cc.private.hm.edu	d33cb9afef8c88cddea03cc3c8badcb9	Issued	28.1.2023, 19:24:11	28.1.2023	29.1.2024	hamburg.cc.private.hm.edu
hamburg.cc.private.hm.edu	019514b1f051f1c795922cf5e41d85da	Issued	22.1.2023, 10:30:41	22.1.2023	23.1.2024	hamburg.cc.private.hm.edu
hamburg.cc.private.hm.edu	122ab41a11683979419d968eb7eb5813	Issued	22.1.2023, 10:08:36	22.1.2023	23.1.2024	hamburg.cc.private.hm.edu

At the bottom of the page, there are two buttons: "Neues Zertifikat mit Assistent erstellen" and "Eigene CSR verwenden". The pagination shows "Zeilen pro Seite: 50" and "1-3 von 3".

# Screenshots

The screenshot shows a web browser window with the URL `https://pki.hm.edu/server/new`. The page title is "HM PKI-Portal". The navigation menu includes "Home", "Hostverwaltung", "Serverzertifikate", "ACME Tokens", "Nutzerzertifikate", and "Anleitungen". The user is logged in as "Florian Testperson" and has an "Abmelden" button.

## Erstellung eines neuen Serverzertifikats

**Ihre Domains:**

Suchen...

- | FQDN ↑
- hamburg.cc.private.hm.edu
- mail.hamburg.cc.private.hm.edu

Zeilen pro Seite: 50 1-2 von 2

**Aktuelle Auswahl:**

Common Name

**Alle ausgewählten FQDNs:**

**Schlüsselart:**

RSA  ECDSA

Zusätzliche PKCS12 Datei generieren

PKCS12 Passwort

Generiere Zertifikat

# Screenshots

The screenshot shows a web browser window with the URL `https://pki.hm.edu/eab`. The page title is "HM PKI-Portal". The navigation menu includes "Home", "Hostverwaltung", "Serverzertifikate", "ACME Tokens" (highlighted), "Nutzerzertifikate", and "Anleitungen". The user is logged in as "Florian Testperson" and has an "Abmelden" button.

## Ihre ACME Tokens

ID	Kommentar	Bereits verwendet?	Aktionen
HNspi064B4cncwrs45lclUk6bRfi07wNi	hamburg.cc.private.hm.edu	✓	<a href="#">Löschen</a>

Optionaler Kommentar

[+ Erstelle neuen Token](#)

Zeilen pro Seite: 15 | 1-1 von 1

# Screenshots

The screenshot shows a web browser window with the URL `https://pki.hm.edu/user`. The page title is "HM PKI-Portal". The navigation menu includes "Home", "Hostverwaltung", "Serverzertifikate", "ACME Tokens", "Nutzerzertifikate" (highlighted), and "Anleitungen". The user is logged in as "Florian Testperson" and has an "Abmelden" button.

## Ihre Nutzerzertifikate

Serial Number	Status	Gültig bis	Aktionen
07:0D:E7:43:73:8B:9A:A1:DD:C4:5E:36...	issued	28.1.2024	<a href="#">Widerrufen</a>
B8:7E:9B:E5:E7:BF:A9:5A:CF:D7:22:FE:2...	issued	22.1.2024	<a href="#">Widerrufen</a>

At the bottom of the table, there is a pagination control: "Zeilen pro Seite: 50" and "1-2 von 2".

At the bottom of the page, there is a green button: "Neues Zertifikat beziehen".