

TCS MIDDLEWARE AN DER HOCHSCHULE MÜNCHEN

Hochschule für angewandte Wissenschaften München

Florian Ritterhoff

17. Oktober 2023



Gliederung

1. Einleitung

2. Architektur

3. Umsetzung

4. Betrieb an der Hochschule

5. Zusammenfassung

Hintergrund

- Bislang vornehmlich DFN-PKI, Let's Encrypt oder selbst signierte Zertifikate
 - Sectigo bietet zwar theoretisch ACME aber ohne Challenges
 - Ständige Veränderung der Oberflächen, Prozesse und Funktionen bei sectigo
 - **Alternative für Serverzertifikate:** Let's Encrypt
Für interne Server nicht möglich, Einsatz von ACME wäre zwingend notwendig und keine zentrale Verwaltung vorhanden
- ⇒ Konzept für Einsatz von GÉANT TCS und Ersatz für Let's Encrypt notwendig

Ziele

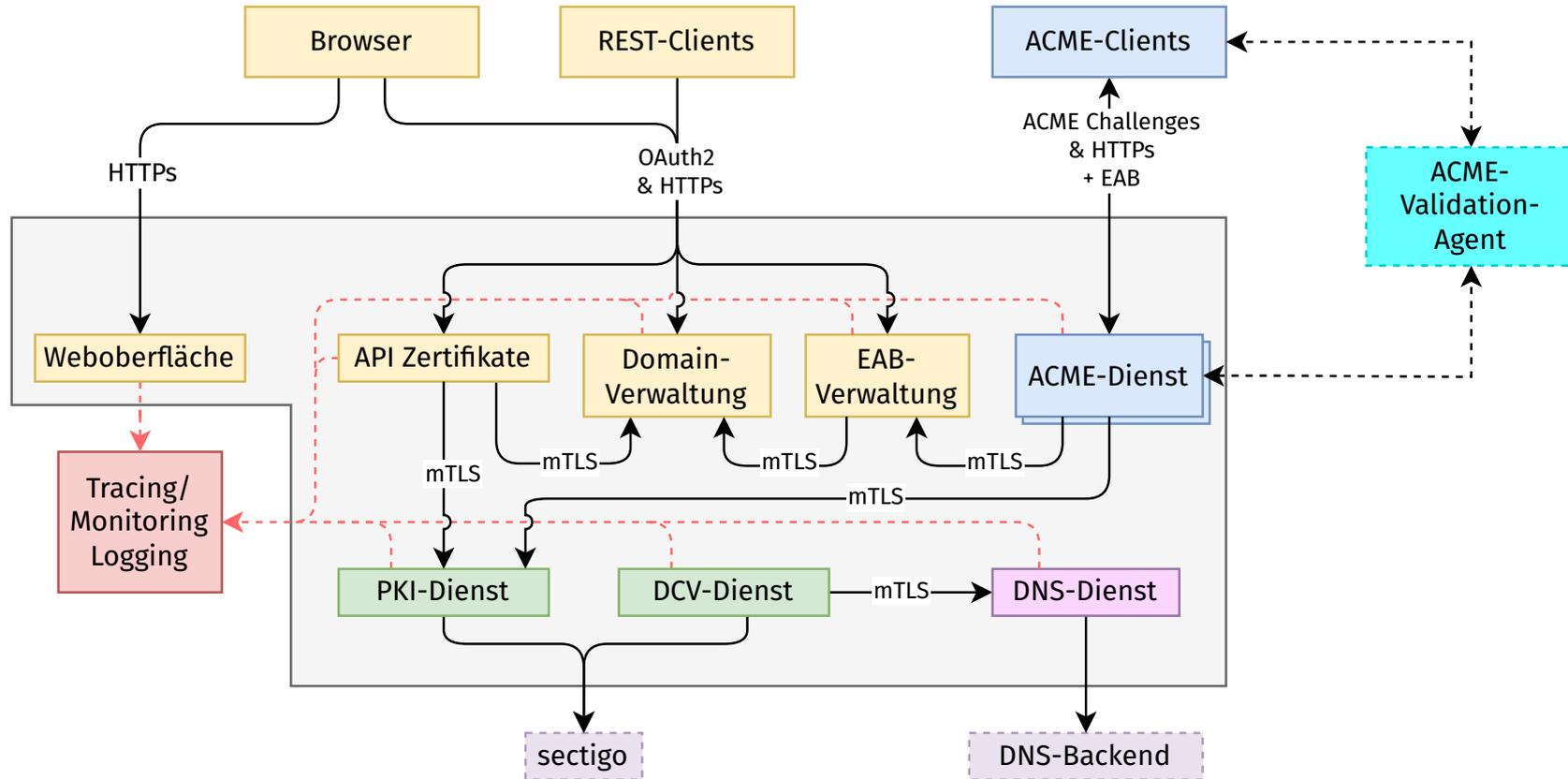
- Eigenständige Verwaltung der Zertifikate durch Admins und normale Angestellte
- Automatisierung von Prozessen
- „Verbergen“ von Schnittstellen, Oberflächen und Prozessen bei *sectigo*
- Reduktion der Anfragen an zentrale IT

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
- Abbildung von SMIME BR Anforderungen
- Realisierung von eigenen „Erinnerungs-E-Mails“

Eigener ACME Dienst

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

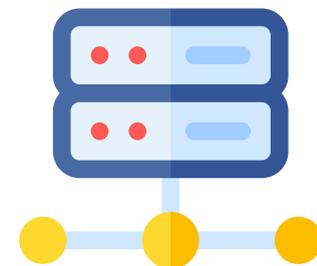
Anbindung an *sectigo*

- Verwendung von REST-API für sämtliche Operationen
- Verwendung von CSRs für Server- und Benutzerzertifikate

⇒ Änderungen bei *sectigo* bleiben Endanwendern (bislang) verborgen

New API admin type replacing standard admin with „WS API use only” privilege. This allows for easier identification and management of admins for API usage.

... We will see ...



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

- ≈ 720 versch. FQDNs registriert
- ≈ 650 Serverzertifikate ausgestellt
ca. Hälfte manuell per Web-UI bzw. ACME
- ≈ 80 Benutzer mit Benutzerzertifikaten



Erfahrungen

- Immer noch 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
 - ... eigenwillige Netzwerkarchitekturen



Erfahrungen

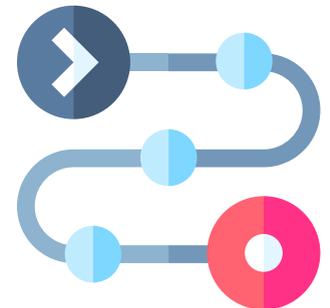
- Bislang:
Teilweise Verwendung von gleichem Zertifikat für Shibboleth und Webserver

⇒ Bezug und nicht abgesprochener Austausch von Zertifikat führt zu defekten Service Providern



Roadmap

- Setzen von CAA Record: Verbot von Let's Encrypt → Verwendung bereits jetzt überschaubar!
- 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



Ausblick

- Einbindung von `acme-dns` für Wildcard Zertifikate oder Systeme ohne ACME Funktion
- Integration von DFN Community PKI via SOAP für Shibboleth Service Provider

Vorführung der Anwendung

Zusammenfassung

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

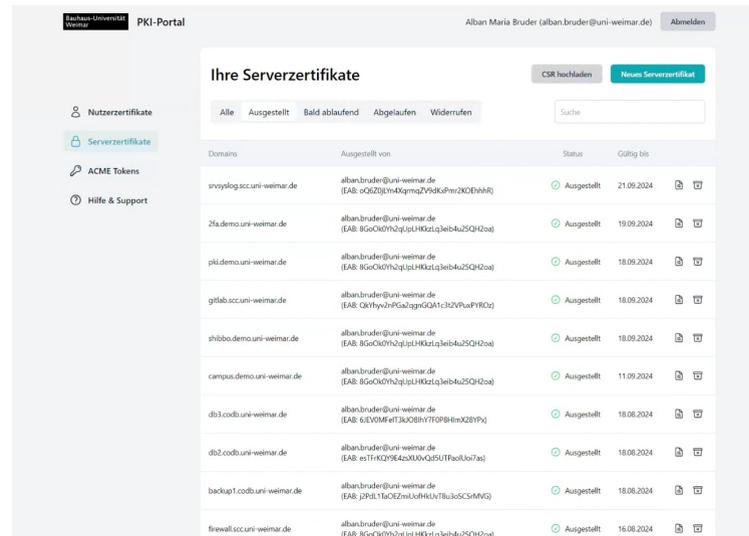
Zusammenfassung

- 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



Zusammenfassung

- Adaptierung an der Bauhaus Uni Weimar mit eigenem Frontend



The screenshot shows the 'Ihre Serverzertifikate' (Your Server Certificates) page in the Uni Weimar PKI-Portal. The page is for user Alban Maria Bruder (alban.bruder@uni-weimar.de). It features a navigation menu on the left with options for 'Nutzerzertifikate', 'Serverzertifikate', 'ACME Tokens', and 'Hilfe & Support'. The main content area has a title 'Ihre Serverzertifikate' and buttons for 'CSR hochladen' and 'Neues Serverzertifikat'. Below the title is a filter bar with tabs for 'Alle', 'Ausgestellt', 'Bald ablaufend', 'Abgelaufen', and 'Widerrufen', along with a search input field. The main part of the page is a table listing certificates with columns for 'Domäne', 'Ausgestellt von', 'Status', and 'Gültig bis'. Each row includes a 'Details' icon and a 'Refresh' icon.

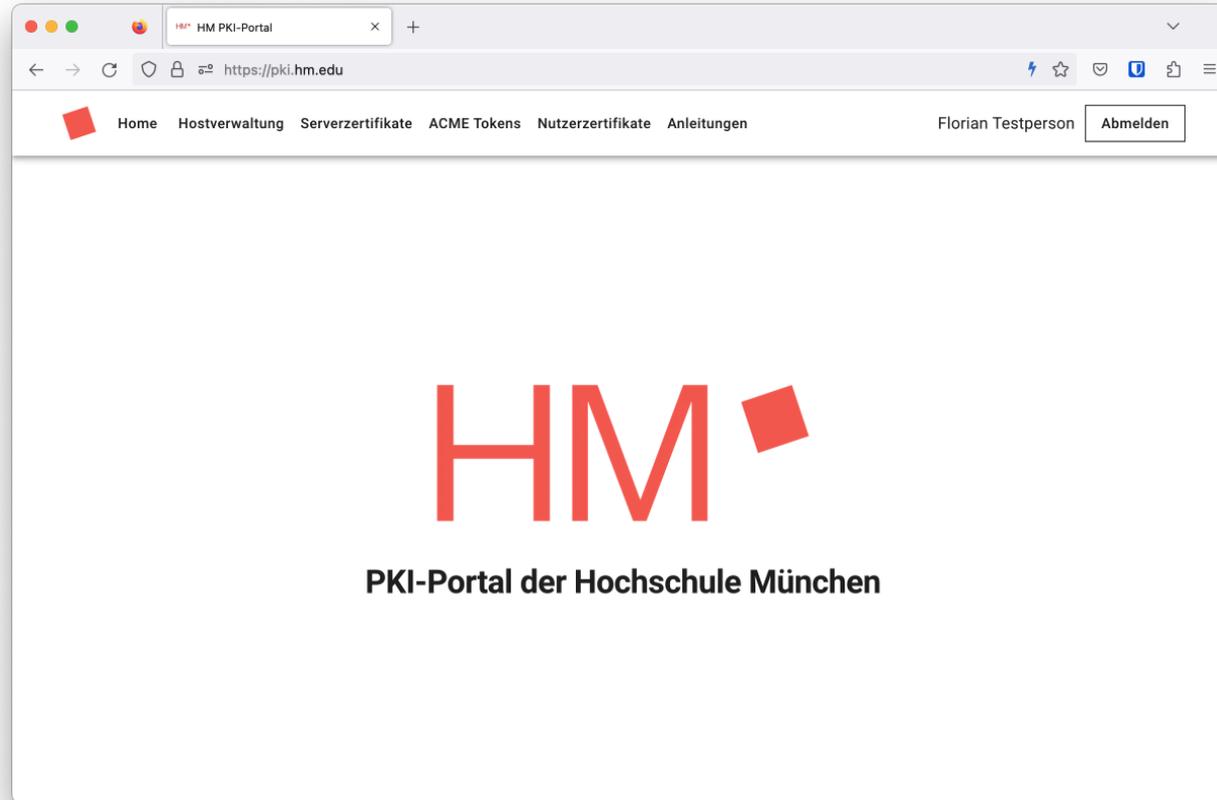
Domäne	Ausgestellt von	Status	Gültig bis
invyslog.scc.uni-weimar.de	alban.bruder@uni-weimar.de (FAR: c02d293b4d89mq2Vh8qPm+2X0E9AR)	Ausgestellt	21.09.2024
zfu.demo.uni-weimar.de	alban.bruder@uni-weimar.de (FAR: 8Gc3x0Yh2qLjLHkzLq3eb4u25Qh2ae)	Ausgestellt	19.09.2024
pkidemo.uni-weimar.de	alban.bruder@uni-weimar.de (FAR: 8Gc3x0Yh2qLjLHkzLq3eb4u25Qh2ae)	Ausgestellt	18.09.2024
gitlab.scc.uni-weimar.de	alban.bruder@uni-weimar.de (FAR: QeHyx0Pca2gmgQA1c3ZVpuPY8Cq)	Ausgestellt	18.09.2024
zhibu.demo.uni-weimar.de	alban.bruder@uni-weimar.de (FAR: 8Gc3x0Yh2qLjLHkzLq3eb4u25Qh2ae)	Ausgestellt	18.09.2024
campus.demo.uni-weimar.de	alban.bruder@uni-weimar.de (FAR: 8Gc3x0Yh2qLjLHkzLq3eb4u25Qh2ae)	Ausgestellt	11.09.2024
db3.ccod.uni-weimar.de	alban.bruder@uni-weimar.de (FAR: 6UEVMF4t13uQ8BvY70P8l6mX20Y9j)	Ausgestellt	18.08.2024
db2.ccod.uni-weimar.de	alban.bruder@uni-weimar.de (FAR: esTfK0Y9E4z3XUQ4SUTPaclko7az)	Ausgestellt	18.08.2024
backup1.ccod.uni-weimar.de	alban.bruder@uni-weimar.de (FAR: j2Ht1Bc0ZmL6dHkU7Bk3e5CS4MVQ)	Ausgestellt	18.08.2024
firewall.scc.uni-weimar.de	alban.bruder@uni-weimar.de (FAR: 8Gc3x0Yh2qLjLHkzLq3eb4u25Qh2ae)	Ausgestellt	16.08.2024

- Probebetrieb an der Uni Würzburg (einige Anpassungen ausstehend)



Vielen Dank für die Aufmerksamkeit!
Fragen?

Screenshots



Screenshots

HM PKI-Portal

https://pki.hm.edu/domains

Home Hostverwaltung Serverzertifikate ACME Tokens Nutzerzertifikate Anleitungen Florian Testperson Abmelden

Ihre Hosts

Suchen...

FQDN ↑	Inhaber	Bestätigt	Aktionen
hamburg.cc.private.hm.edu	f.testperson@hm.edu	✓	Freischalten Löschen Delegationen bearbeiten Zustand
mail.hamburg.cc.private.hm.edu	f.testperson@hm.edu	✓	Freischalten Löschen Delegationen bearbeiten 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 has 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 "Eigenen CSR verwenden". The page footer 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	✓	Löschen

Optionaler Kommentar

[+ Erstelle neuen Token](#)

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	Widerrufen
B8:7E:9B:E5:E7:BF:A9:5A:CF:D7:22:FE:2:...	issued	22.1.2024	Widerrufen

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](#)