Moderne PKI-Architektur an einer Hochschule

Hochschule für angewandte Wissenschaften München

Florian Ritterhoff
Prof. Dr.-Ing. Thomas Schreck

09. Februar 2023

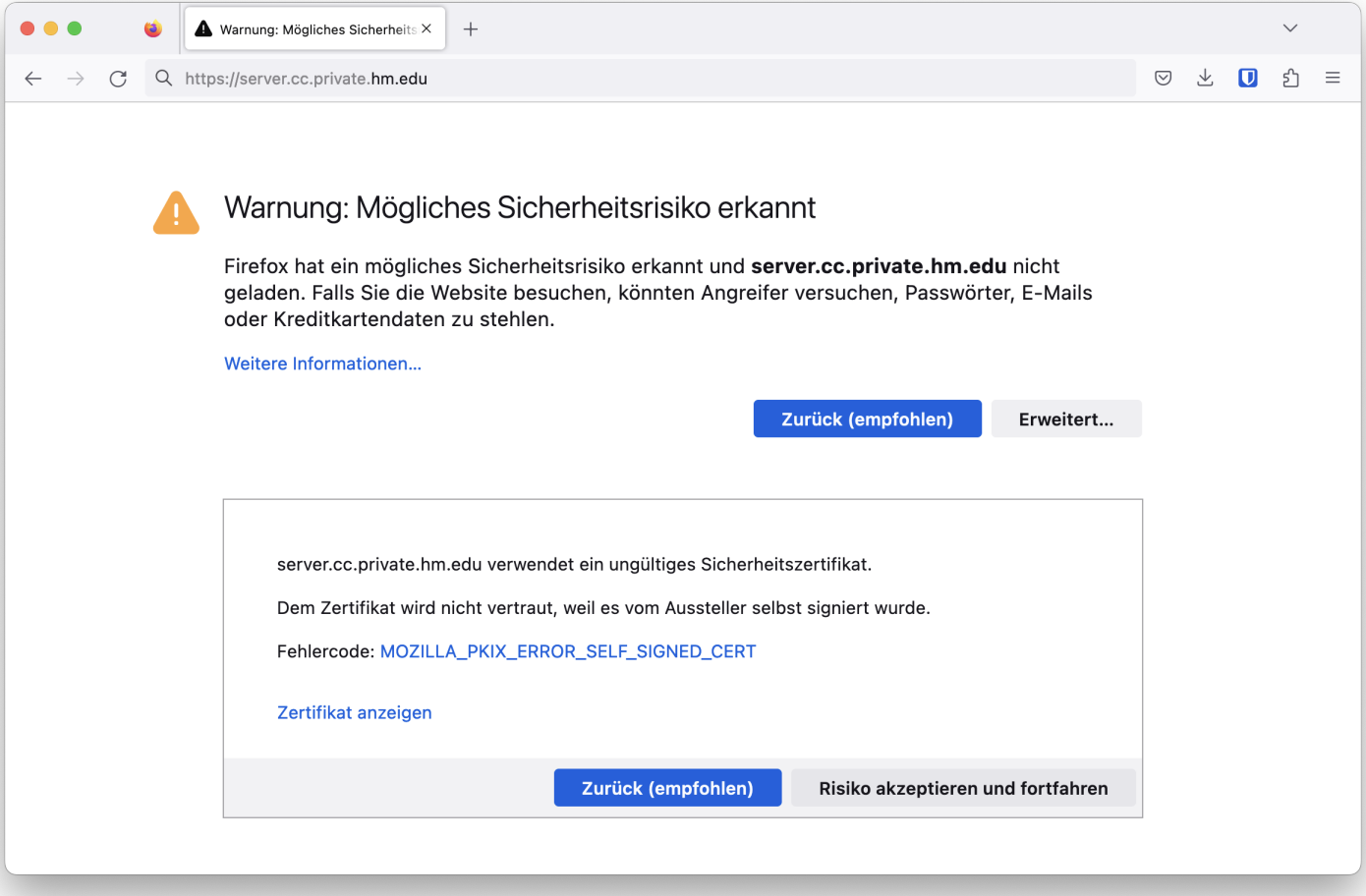
Gliederung

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

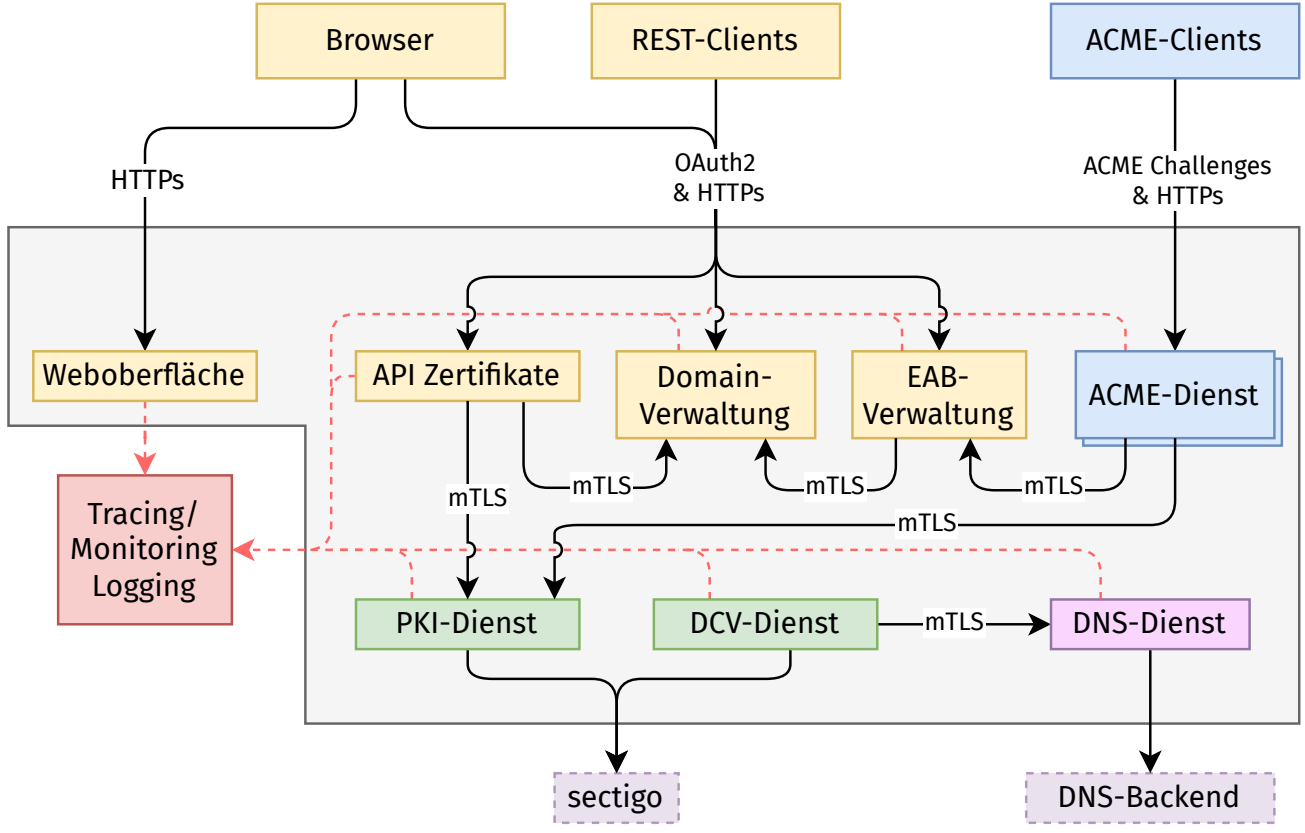
- Eigenständige Verwaltung der Zertifikate
- Automatisierung von Prozessen
- „Verbergen” von Schnittstellen, Oberflächen und Prozessen bei *sectigo*
- Anbieterunabhängigkeit
- Reduktion der Anfragen an zentrale IT

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
  $\rightarrow$ lediglich Austausch von DNS Dienst
- z.B. Möglichkeit der Integration vorhandener Domainverwaltungen
- z.B. (hoffentlich) Abbildung von SMIME BR Anforderungen

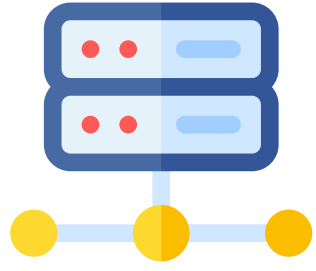
Eigener ACME Dienst

- 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 & entprechende 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

- ≈ 330 versch. FQDNs registriert
- ≈ 180 Serverzertifikate ausgestellt
  Überwiegender Anteil manuell per Web-UI; Geringer Anteil per ACME
- ≈ 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

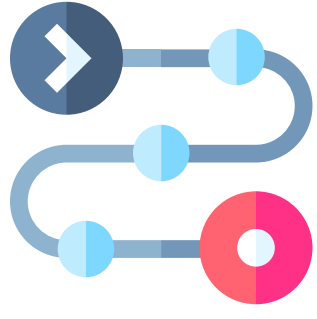
Erfahrungen

- 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

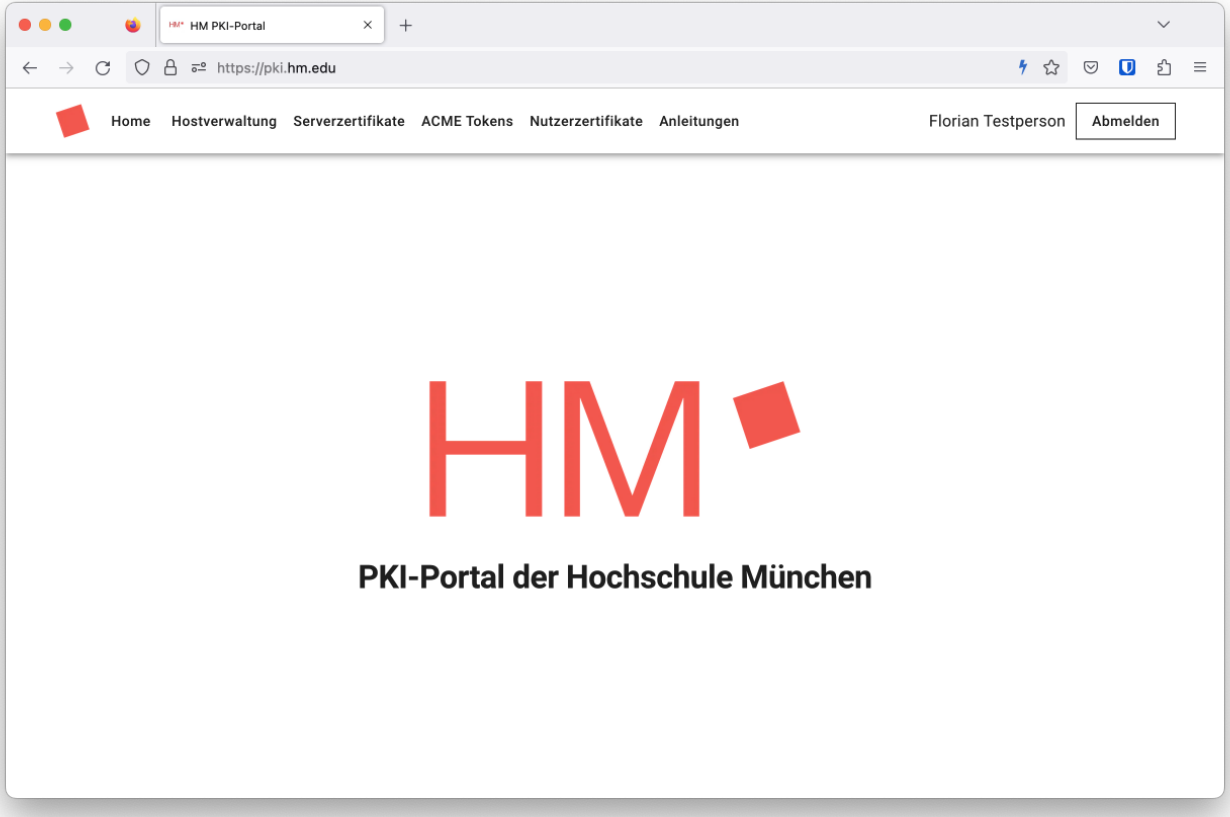
- Veröffentlichung aller Komponenten auf GitHub
  - Frontend: https://github.com/hm-edu/portal-frontend
  - Backend-Dienste: https://github.com/hm-edu/portal-backend
  - ACME-Dienst: https://github.com/hm-edu/certificates
  - `docker-compose`-Deployment: https://github.com/hm-edu/portal-deployment

⇒ Einsatz und Weiterentwicklung durch Community möglich und erwünscht

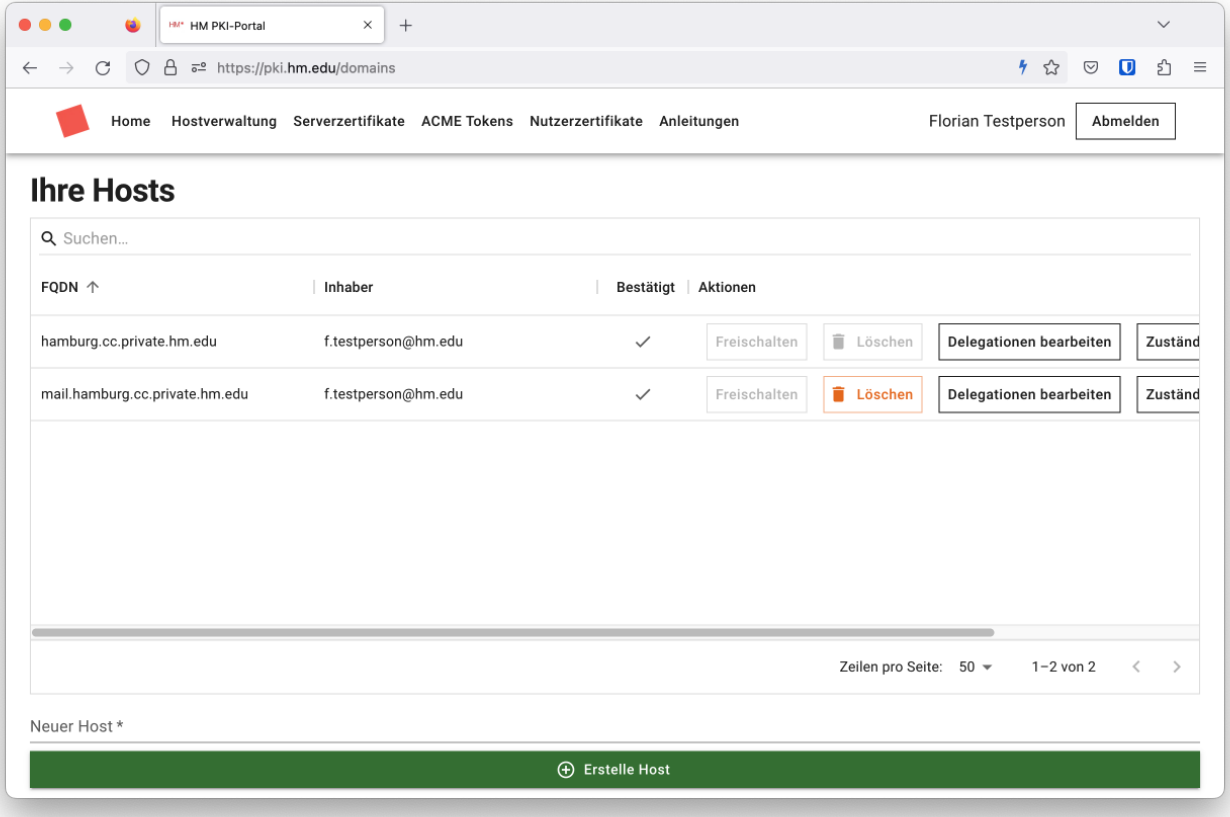
Vielen Dank für die Aufmerksamkeit!

Fragen?

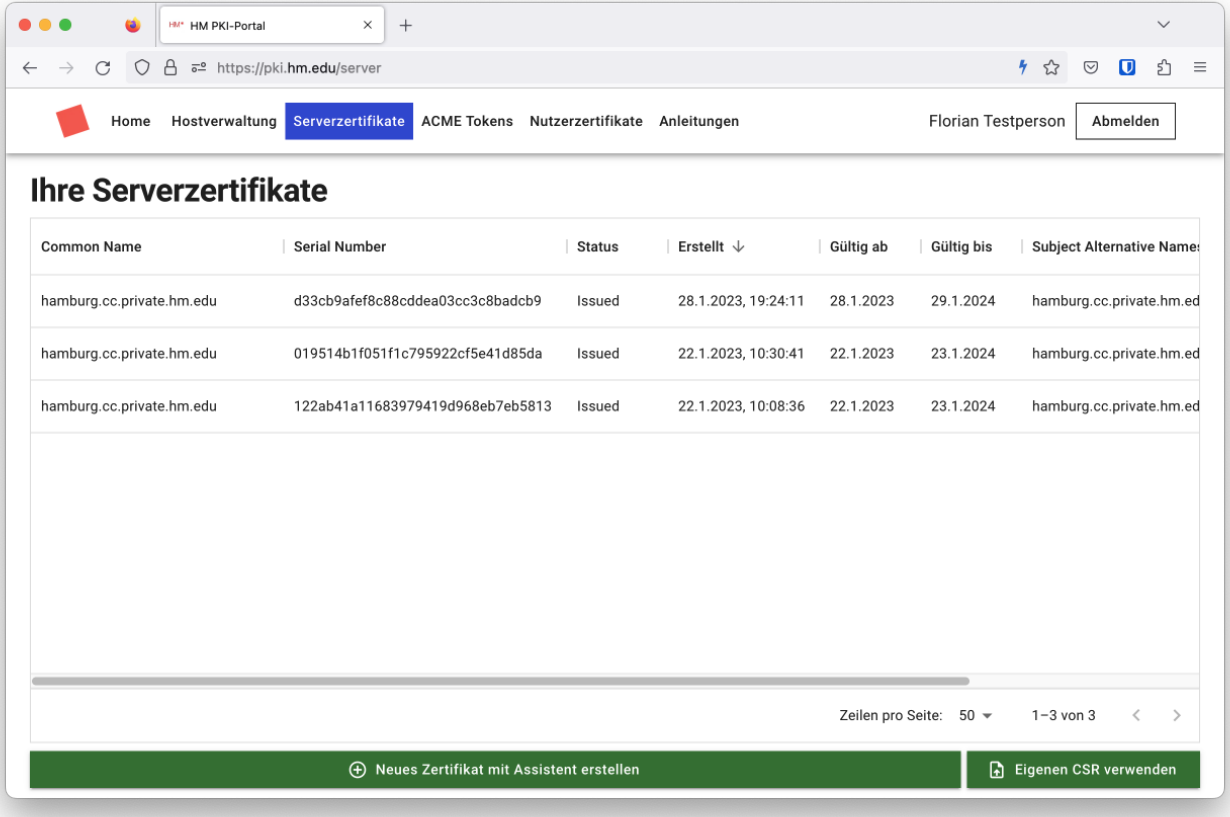
Screenshots



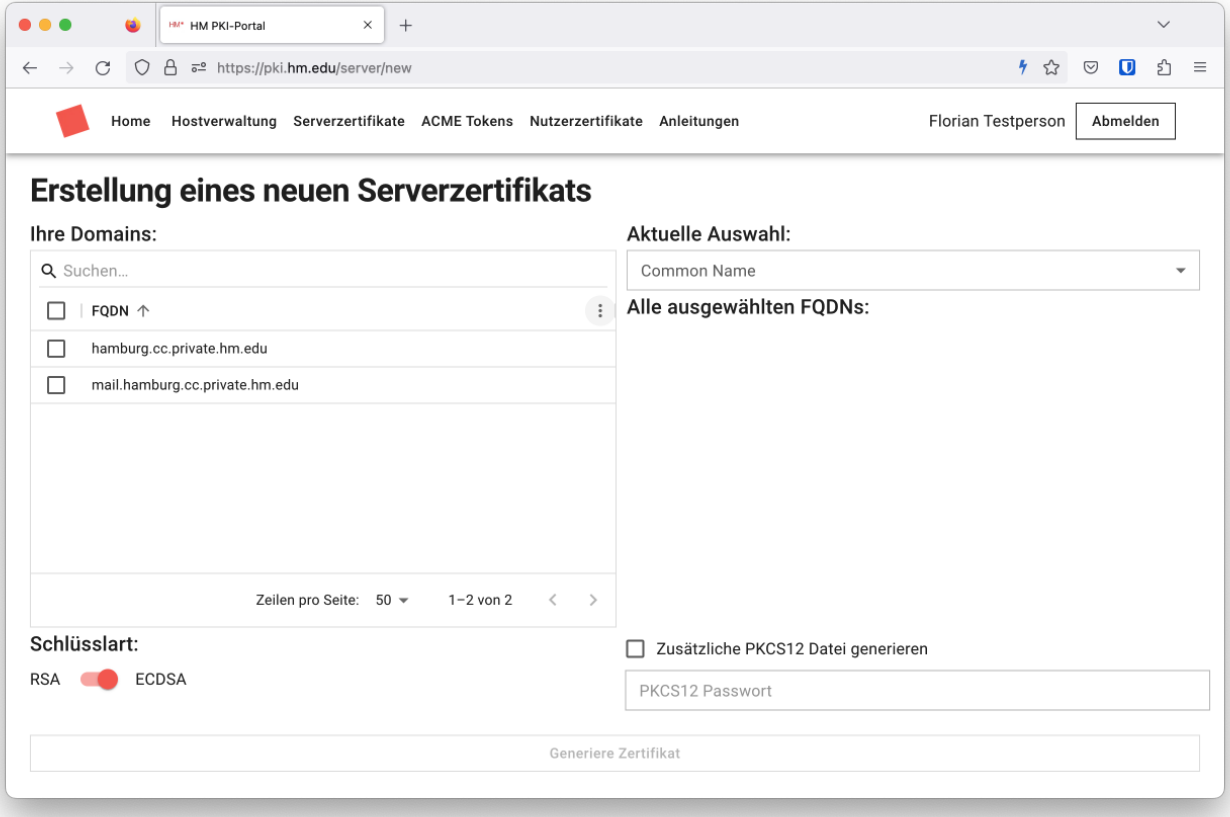
Screenshots



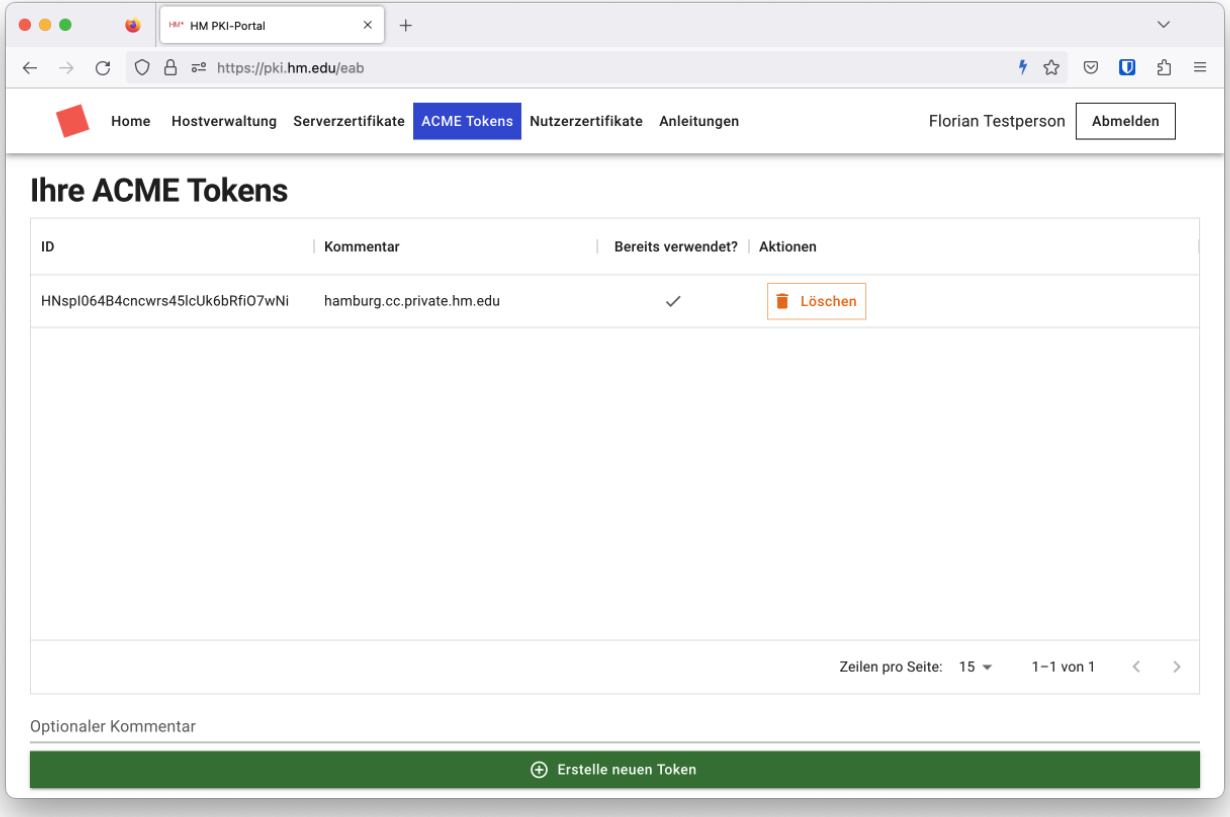
Screenshots



Screenshots



Screenshots



Screenshots