TCS Middleware an der Hochschule München

Hochschule für angewandte Wissenschaften München

Florian Ritterhoff

17. Oktober 2023

Gliederung

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

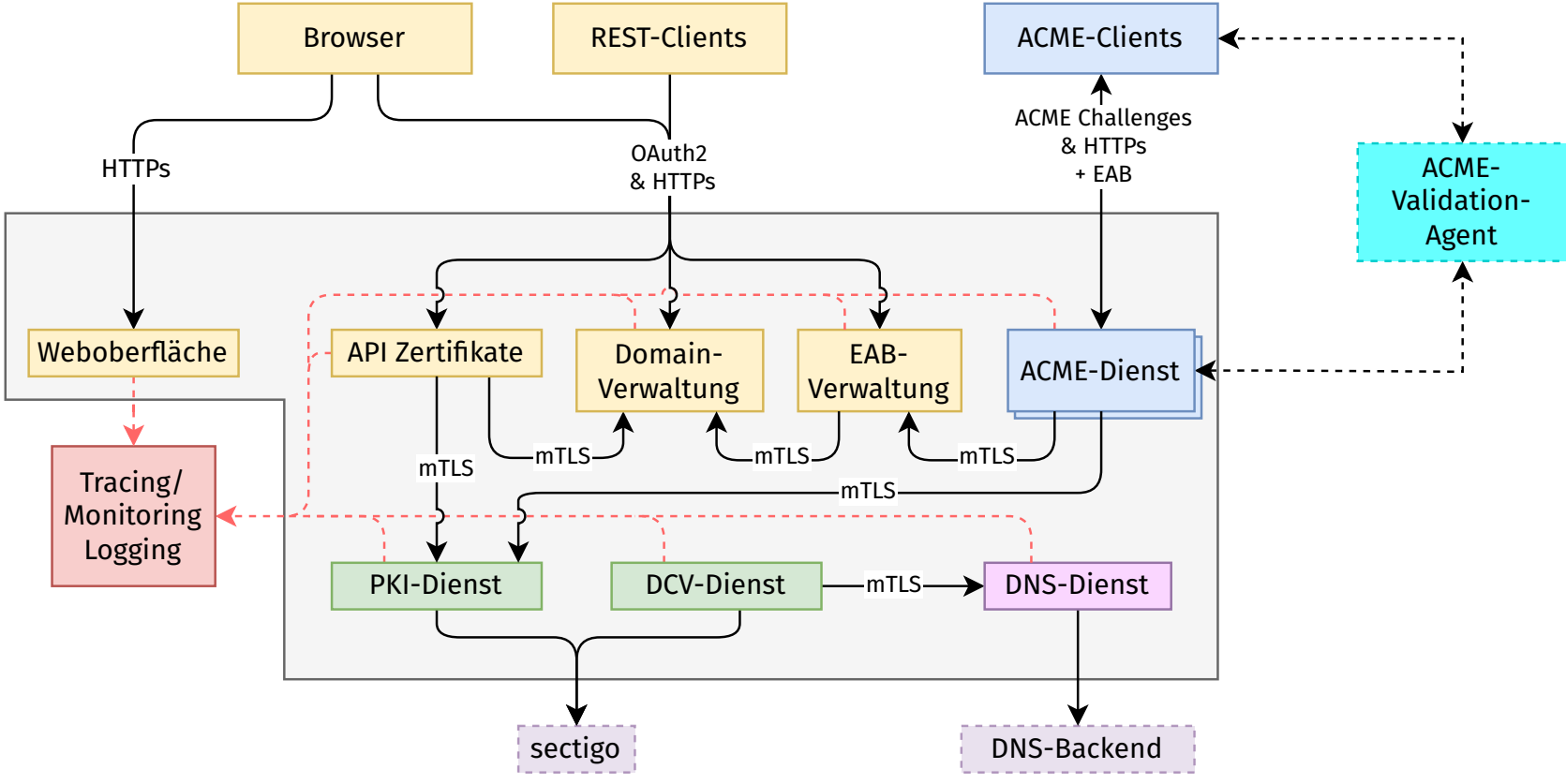
- Eigenständige Verwaltung der Zertifikate durch Admins und normale Angestellte
- Automatisierung von Prozessen
- „Verbergen” von Schnittstellen, Oberflächen und Prozessen bei *sectigo*
- Reduktion der Anfragen an zentrale IT

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
  $\rightarrow$ 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

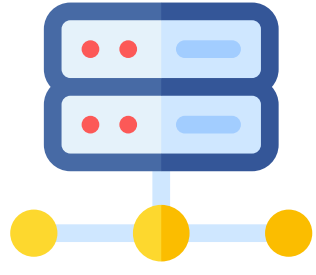
Anbindung an *sectigo*

- 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

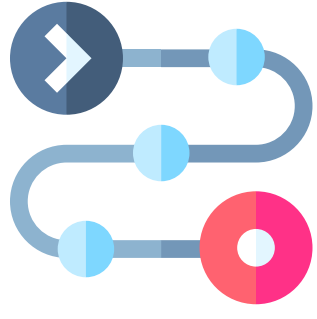
  ⇒ Bezug und nicht abgesprochener Austausch von Zertifikat führt zu defekten Service Providern

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

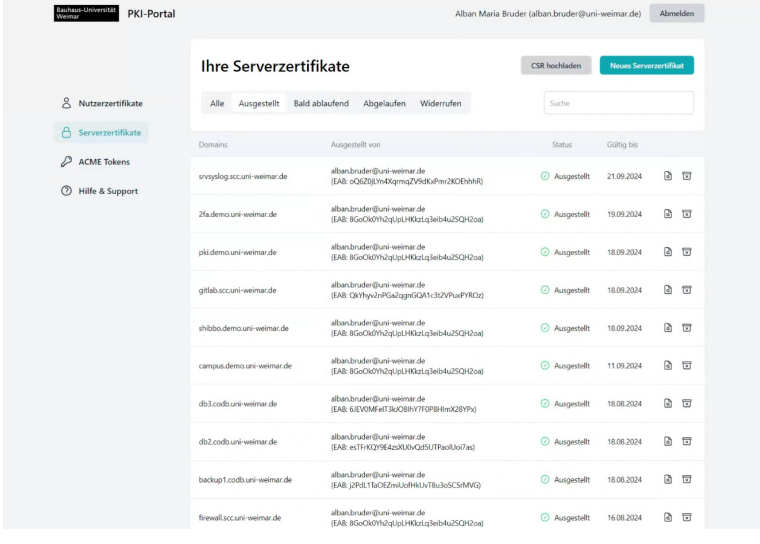
Zusammenfassung

- 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

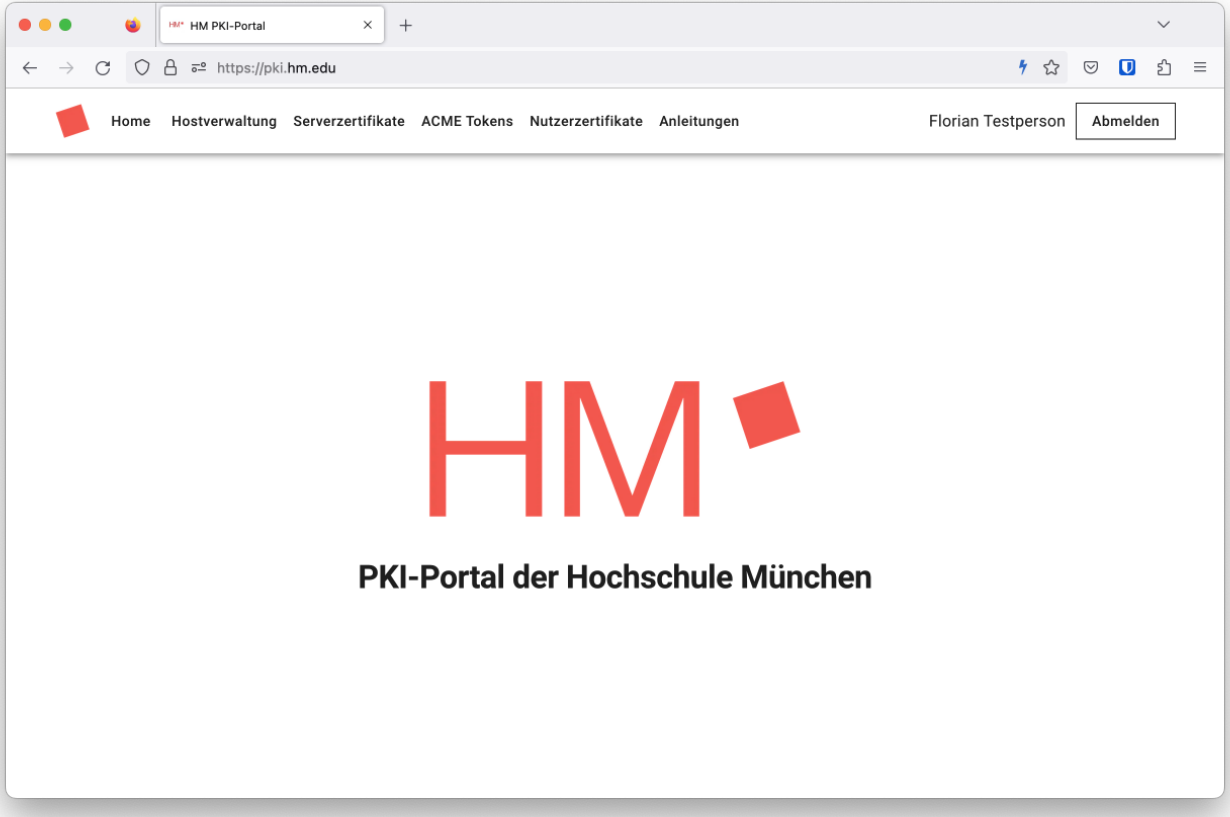


- Probebetrieb an der Uni Würzburg (einige Anpassungen ausstehend)

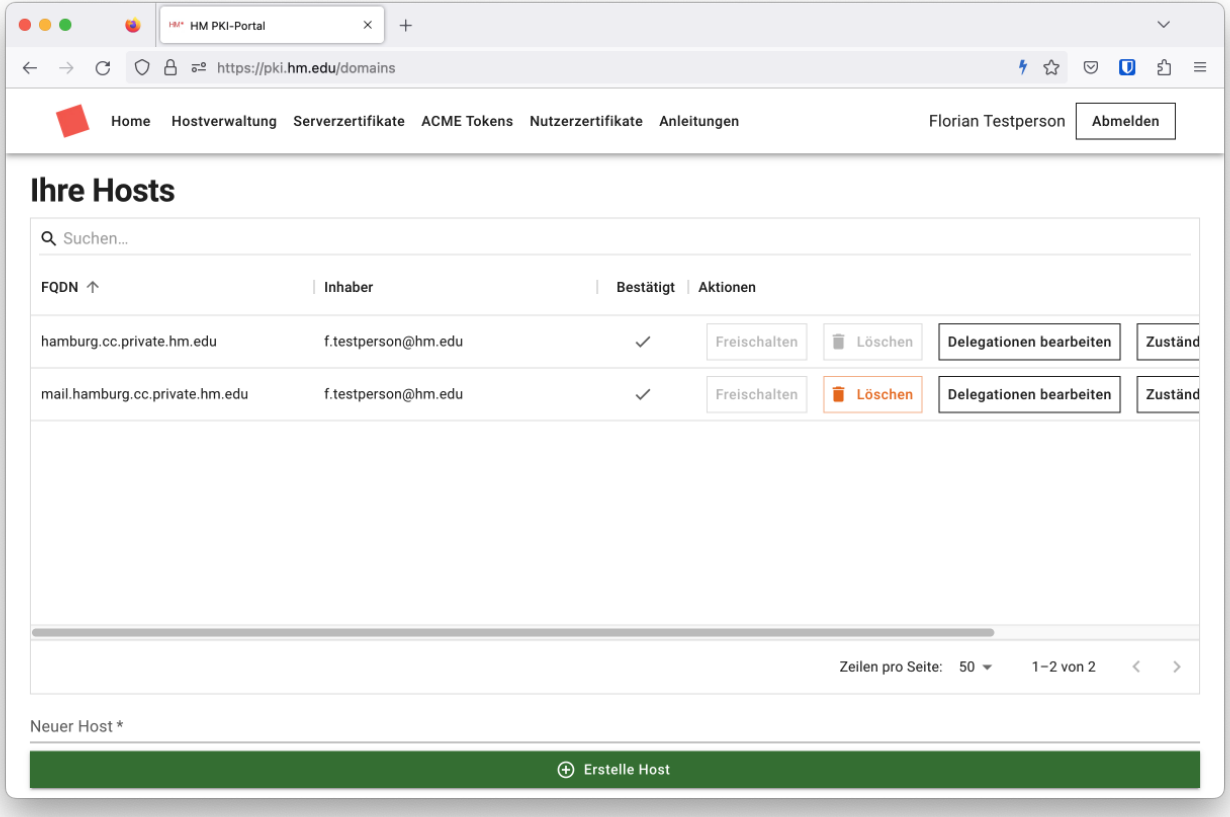
Vielen Dank für die Aufmerksamkeit!

Fragen?

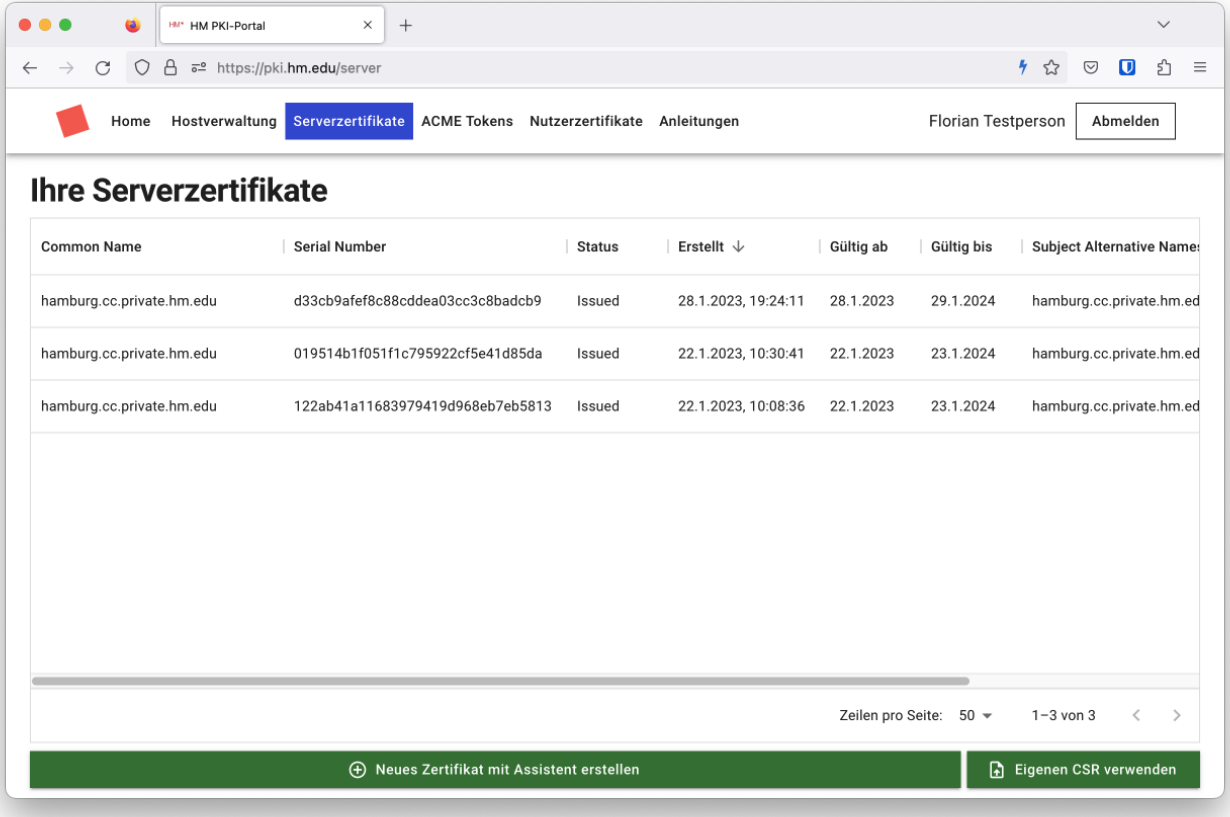
Screenshots



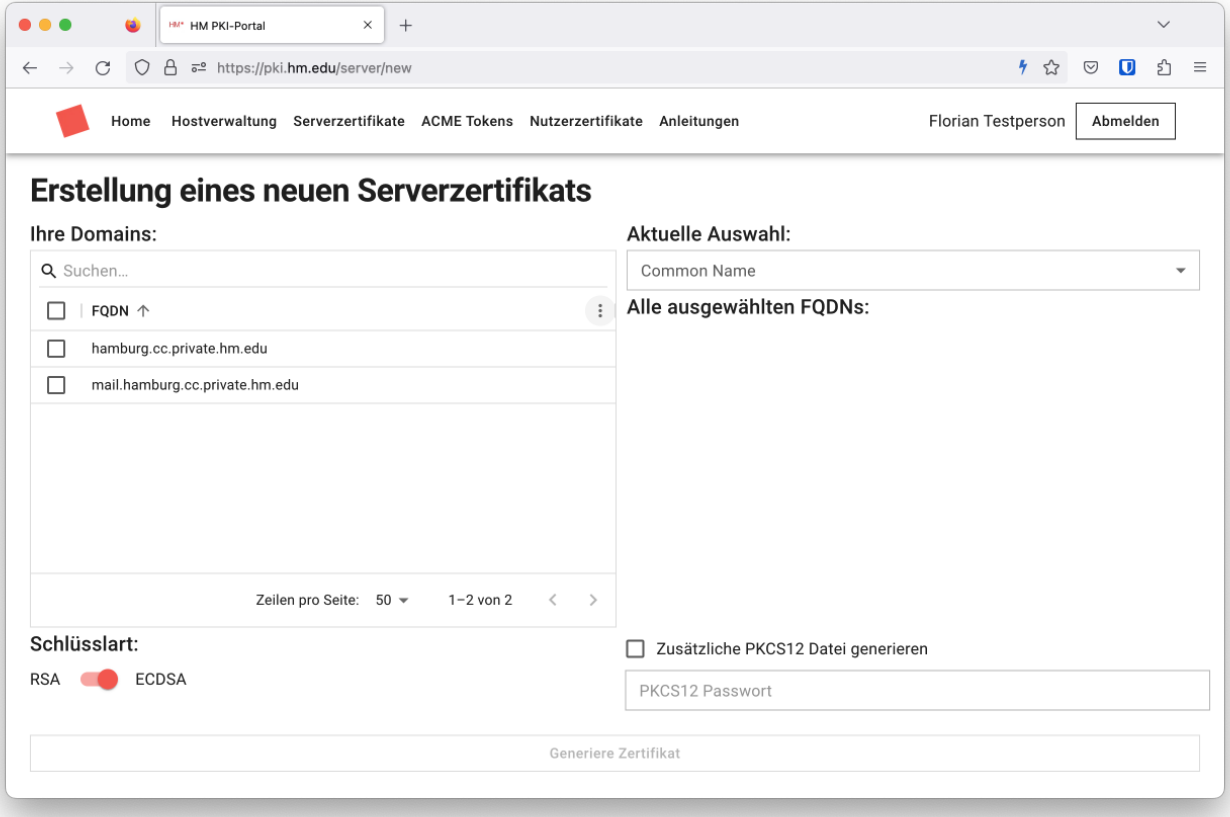
Screenshots



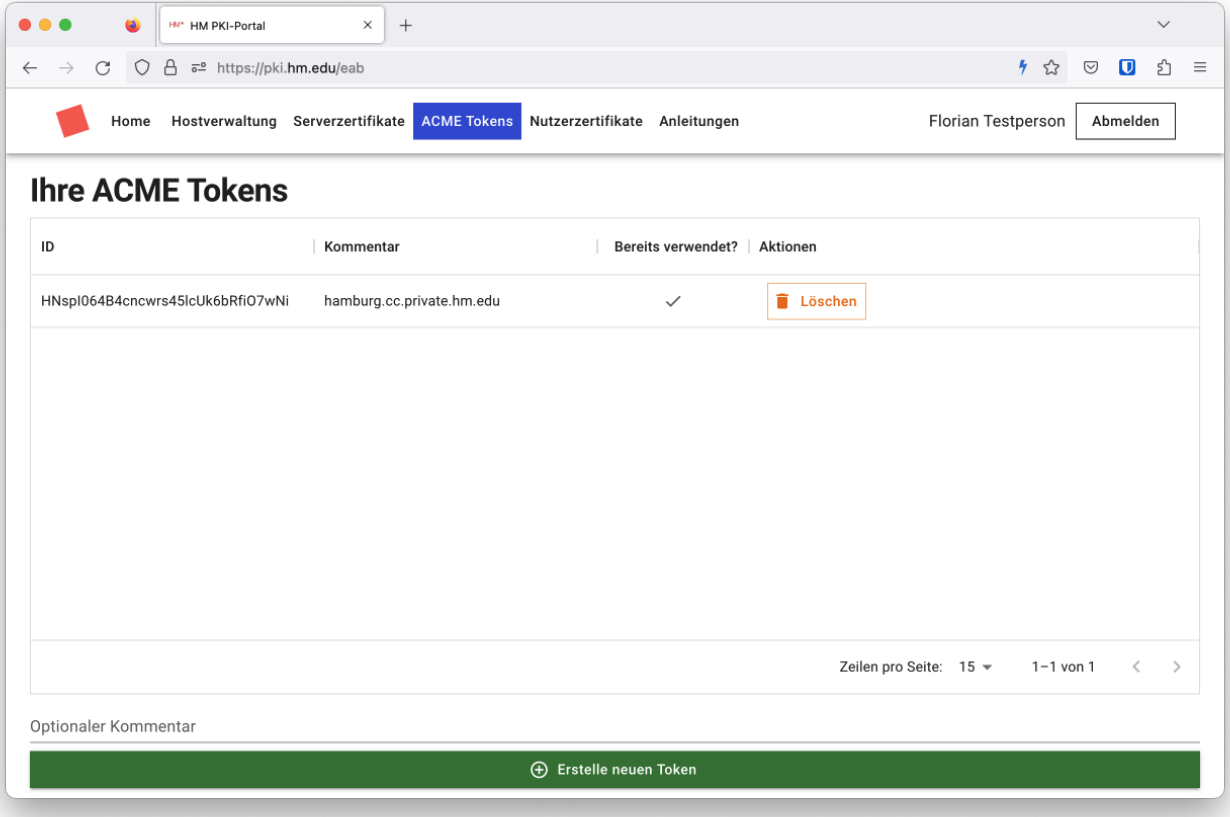
Screenshots



Screenshots



Screenshots



Screenshots