

# 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 ...

# p ö 3 š " | Ö | - 3 •

â \$ ö Ö W 3 Ö Ù D | 3 " ë - ö % ö 6 b ¥ ý â ' y x • " š Ö E 3 % | æ q š D • " |

â 6 b ¥ ý â ' y • " • " - š " š i " ñ - W 3 - " " | • " ö š Ñ • | ò " 3 š | W " y ÿ - 3 •

â • Ö % ö W š - 3 Ö • " | 6 b ¥ ý â ' y

â ó " | Ù " | ò " | š ö W š " Ø

• y Ö y } Ö } q } }

â \$ " 3 - š ò " | ò " | š ö W š " Ø

• q Ö q • Ö } q } ( ) £ £ n ç › t › B # P É 9 ) \* ä # n 9 ñ ~ £ n ^ 9 n # Û

) D - - 3 Ò š - 3 Ö " Ý ö Ö Ö Ù , " | Ö " ö % ö Ö Ý " ö Ö " ë D ë " 3 Ñ D | • " | - 3 Ö "

# p ö 3 š " | Ö | - 3 •

â ¥ W % ö Ñ D F Ö ¥ | y ö | - Ö š " • , " | š ö % W š " Ö ó " | Ù ö % " i y , ó ñ

â 6 " | ò " ö š 3 • ö £ š . | k î Ð 9

â ¥ ö % ö š • ö | " š D - q W š ö • " - ö š ó š | - š " | " 3 " ö 3 " | p D % ö ö Ö % ö ö " "

â , i E , " | Ñ W ö | " 3 D ö 3 " , ö W " 3 Ö " Ö x i • W - W Ö ñ D ö 3 " ¥ W % ö Ù D

â š " | 3 W š ö Ù " Ñ • | ó " | Ù " | ö š | Ö E W % š | q š

b • | ö 3 š " | 3 " ó " | Ù " | 3 ö % ö š - R Ö ö % ö ö - 3 • " ö 3 " ò " 3 š | W " ,

) ' D 3 ò " q š Ñ • | E ö 3 Ö W š ò Ù D 3 e F ¥ y y , ó - 3 • E | Ö W š ò Ñ • |

# D ö " "

â E ö Ö " 3 OE š j 3 • ö Ö " , " | Ý W š - 3 Ö • " | D " | š ö W š "

â - š D - W š ö OE ö " | - 3 Ö Ù D 3 â | D ò " OE OE " 3

â , " | • " | Ö " 3 Ù D 3 ó % ö 3 ö š š OE š " " 3 x ¶ • " | j % ö " £ 3 . . . 3 ð Æ 9 D ò

â 3 • ö " š " | - 3 W • ë j 3 Ö ö Ö " ö š

â é " • - š ö D 3 • " | 3 Ñ | W Ö " 3 W 3 ò " 3 š | W " y ÿ

# e | - 3 • W Ö " 3

â y | " 3 3 - 3 Ö ò Ý ö OE % ö " 3 \$ W % " 3 • - 3 • b | D 3 š " 3 •

â é " W ö OE ö " | - 3 Ö " ö 3 ò " 3 " | b - 3 š ö D 3 " 3 ö 3 " ö 3 ò " 3 " 3 3 Ý "

ï | ö % | D OE " | Ù ö % " OE ñ

â - OE Ñ • ë | - 3 Ö W " | b - 3 š ö D 3 W ö š j š " 3 ö 3 " ö Ö " 3 " 3 , D 3 š W

â ' D - - - 3 ö W š ö D 3 \$ W % " 3 • ý b | D 3 š " 3 • - ö š š " OE é E ó y y â y

â 3 • ö 3 • - 3 Ö W 3 ò " 3 š | W " 3 ó ë ö • • D " š ë



e " OE W - š W | % ö ö š " š - |

# \$ W % " 3 •

â y | " 3 3 - 3 Ö ò Ý ö Œ % ö " 3 Ù " | Œ % ö ö " • " 3 " 3 b - 3 š ö D 3 W ö š j š "

â é E ó y y â y 6 D - W ö 3 Ù " | Ý W š - 3 Ö

â é E ó y y â y E \$ y , " | Ý W š - 3 Ö

â é E ó y y â y D " | š ö W š Œ Ù " | Ý W š - 3 Ö

â , j E 6 ö " 3 Œ š

â D " | š ö W š Œ \$ W % " 3 •

â , W ö • ö " | - 3 Ö Œ Œ " | Ù ö % " "

â 6 ¥ ó 6 ö " 3 Œ š

# \$ W % " 3 •

i D • - W | " | - Ò • W - " | - R Ö ö % ö š " ö 3 Ñ W % ö " - OE š W - OE % ö • W |

â ò Ö \$ Ö 3 OE š " " Ù D 3 6 æ 3 W - ö % ö 6 ¥ ó q • W š " OE - ö š š " OE 7  
! " • ö Ö ö % ö - OE š W - OE % ö Ù D 3 6 ¥ ó 6 ö " 3 OE š

â ò Ö \$ Ö i R Ö ö % ö " ö š • " | y 3 š " Ö | W š ö D 3 Ù D | ë W 3 • " 3 " | 6 D -

â ò Ö \$ Ö i ë D ý " 3 š ö % ö ñ • • ö • - 3 Ö Ù D 3 ó i y i E \$ é 3 Ñ D | • " | -

# E ö Ö " 3 " | , i E 6 ö " 3 Œ š

â E | ò Ý ö 3 Ö " 3 Ù D 3 p ý ý â ý , ë W " 3 Ö " Œ Œ D Ý D ë Ñ • | ö 3 š " | 3  
ó æ Œ š " - "

â ' " ö 3 " 0 ö • % W | • ò " | š ö W š " x • W " ö 3 " ó % ë 3 ö š š Œ š " " ò

â , " | 3 • q Ñ " 3 Ö - ö š ö 3 š " | 3 " - â ' y 6 ö " 3 Œ š E ö 3 Œ W š ò Ù D 3 E  
) ¥ W % ë Ù D ò ö " ë • W | " ö š ò Ý ö Œ % ë " 3 Ö Ö Ö

â D " | š ö W š

â E \$ ý 6 W š " 3

â E 3 • 3 " š ò " |

# 3 • ö 3 • - 3 Ö ~ W 3. < î Ð 9

â , " | Ý " 3 • - 3 Ö Ù D 3 é E ó y y â y Ñ . | Œ j - š ö % ö " ¶ q " | W š ö D 3 " 3  
 â D " ö š Ù D | š " ö • " ö ó " | Ù " | ò " | š ö W š " 3 ö - , " | Ö " ö % ö è ò " , i E  
 â ¥ ö % ö è š • D - - " 3 š ö " | š " Œ e | W æ ö Œ š ö 3 Ö Ù D 3 D " | š ö W š Œ W 3 š  
 ó % ö è . Œ Œ " Ý R | š " | 3

â , " | Ý " 3 • - 3 Ö Ù D 3 , ó é Œ Ñ . | ó " | Ù " | ý - 3 • \$ " 3 - š ò " | ò " | š ö W

) 3 • " | - 3 Ö " 3 • " 3 E 3 • W 3 Ý " 3 • " | 3 Ù " | • D | Ö " 3

# b | D 3 š " 3 •

â \$ ö " š " š • " 3 E 3 • 3 " š ò " | 3 b " 3 š ö D 3 W ö š j š " 3 W " Ò • W " 3 • W

â y 3 š " Ö | ö " | š " e " 3 " | ö " | " 3 Ö Ù D 3 , ó é Œ D Ý ö " â ' , ó å y } 6 W š " ö  
â y • ò Ý Ö 3 W š ö Ù " | • W Ù W ó % | ö q š \$ ö • ö D š ë "

) E ö 3 Ñ W % ö " e " 3 " | ö " | " 3 Ö Ù D 3 D " | š ö W š " 3 W " % ö Ñ • | "

) â | ö Ù W š " | ó % ö • Œ Œ " Ù " | j Œ Œ š 3 ö " ó æ Œ š " - • " Œ E 3 •  
' " æ ý é " % D Ù " | æ - R Ö ö % ö Ê

• OE ö % ö " | - 3 Ö • " | ' D - - - 3 ö W š ö D 3

â ¶ q " 3 y 6 , D 3 3 " % ö š - 3 • ¶ - š ë } Ñ • | é E ó y ý â y OE

y - 6 " š W ö Ø ó ë ö • • D " š ë â - Ö ö 3 " 3 š q | " % ö " 3 • " ' D 3 Ö - |  
b - 3 š ö D 3 W ö š j š " 3 Ö

- Ñ • ë | - 3 Ö Ö - - Ö " • - 3 Ö

â â | D • " š ö Ù Ù " | Ý " 3 • " š Ø

â ' " • " | 3 " š " Ö , - Ö š " | - ö š y Ö š ö D ó " | Ù ö % " | " Ö ë

â ÿ " % ö 3 ö Ö % ö - R Ö ö % ö Ø

â , " | Ý " 3 • - 3 Ö Æ M G T E Q 0 q | Q U | G E 3 š Ý ö % " - 3 Ö Ö - - Ö " • - 3 Ö ñ  
â \$ W | " ý | " š W

â 0 " ö š " | " 3 Ñ D | • " | - 3 Ö " 3

â â D Ö š Ö | " ó ç • 6 W š " 3 • W 3  
â ¶ y 6 , ó ó ¶



E ö 3 Ñ • ë | - 3 Ö W 3 • " | p i

â â | D • " • " š | ö " • OE " ö š } q Ö ¶ š D • " | } q } }

â y 3 š " | 3 " 6 " W š ö Ù ö " | - 3 Ö • " | 6 b ¥ ý â ' y ò - - ' Ö ¥ D Ù " - • " |

â D - D | • 3 - 3 Ö Ù D 3 6 D - W ö 3 OE W 3 ò - OE š j 3 • ö Ö " y ÿ ý \$ " š | " - " | •

â 6 D - - " 3 š W š ö D 3 Ù D 3 b - 3 š ö D 3 W ö š j š " 3 ö 3 , D 3 - " 3 % " "

â ó - q q D | š - 3 • ó % ö - - 3 Ö Ñ • | ' D " Ö " 3

š " " " | ó š W 3 •

â ••q Ù " | OE % ö ö Ö b ç 6 ¥ OE | " Ö ö OE š | ö " | š

â y • q ó " | Ù " | ò " | š ö W š " W " OE Ö " OE š " š  
• " | Ý ö " Ö " 3 • " | 3 š " ö - W 3 " " q " | 0 " • ý y Ù e " | ö 3 Ö " | 3 š " ö

â % ö q \$ " 3 " š ò " | ò " | š ö W š "

# E | Ñ W ë | - 3 Ö " 3

â e " | ö 3 Ö " , " | Ý " 3 • - 3 Ö Ù D 3 , ; E W - Ñ Ö | - 3 • Ö Ö Ö

â Ö Ö Ö - - OE š j 3 • ö % ö " | ; ö Ö | W š ö D 3 Ù D 3 • " OE š " ë " 3 • " 3 ' D 3 Ö - | W š ö

" ö 3 Ñ W % ö " 3 6 W š " ö W - OE š W - OE % ö

â Ö Ö Ö - " ë | â W | W - " š " | W OE • " ö • " š OE E 3 % | æ q š x • W " ö Ö " 3 " | ó " | Ù

â Ö Ö Ö - 3 • " W 3 3 š " ý " % ö 3 ö

â Ö Ö Ö š " % ö 3 ö OE % ö 3 ö % ö š - R Ö ö % ö

E | Ñ W ë | - 3 Ö " 3

â \$ ö Œ W 3 Ö ø

ÿ " ö Ý " ö Œ " , " | Ý " 3 • - 3 Ö Ù D 3 Ö " ö % ö " - D " | š ö W š Ñ • | ó ë ö

) \$ " ò - Ö - 3 • 3 ö % ö š W • Ö " Œ q | D % ö " 3 " | - Œ š W - Œ % ö Ù D 3

ò - • " Ñ " š " 3 ó " | Ù ö % ö " â | D Ù ö • " | 3

# é D W • - W q

â E 3 Ö " | " , " | ò W ë 3 - 3 Ö - ö š y 6 | é • 6 â Ø  
 ò Ö \$ Ö š ö D 3 " 3 • " ö - Œ Œ % ö " ö • " 3 Û D 3 ¥ - š ò " | 3  
 ) 0 ö • " | | - Ñ " 3 Û D 3 ¥ - š ò " | ò " | š ö W š ĩ " 3 ñ  
 ) Ö Ö Ñ Ö y | W 3 Œ Ñ " | Û D 3 6 D - W ö 3 Û " | W 3 š Ý D | š ö % ö " ö

â 3 • ö " š " 3 " ö 3 " | ĩ ö 3 š " | 3 " 3 ñ ó - % ö " Ñ • | ¥ - š ò " | ò " | š ö W š "

â é " W ö Œ ö " | - 3 Ö Û D 3 E | ö 3 3 " | - 3 Ö Œ ý E ý | W ö Œ

â ó " š ò " 3 Û D 3 , é " % ö D | • Ø , " | • D š Û D 3 • " š Œ E 3 % ö | æ q š

- OE • ö %

â 3 • ö 3 • - 3 Ö Ù D 3 ó - W | š % W | • OE i 8 - • ö ' " æ ñ

â y 3 š " Ö | W š ö D 3 Ù D 3 6 b ¥ , D - - - 3 ö š æ â ' y Ù ö W ó ¶ â Ñ • | ó ë

, D | Ñ • ë | " 3 Ö • " | 3 Ý " 3 • " 3 Ö

# D - OE W - - " 3 Ñ W OE OE - 3 Ö

â | D • - W | " | % ö ö š " š - | x • ö " D ý " 3 ö OE š Ñ • | E | Ý " ö š " | - 3 Ö " 3

â 3 • ö " š " | - 3 W • ë j 3 Ö ö Ö " ö š - 3 • \$ " 3 - š ò " | Ñ | " - 3 • ö % ö " ö š •  
â | D ò " OE OE " ö 3 0 " • D • " | j % ö " - 3 • 3 • ö " š " 3 " ö 3 " OE " ö Ö " 3 " 3

â é " W ö OE ö " | - 3 Ö " ö 3 " | D - q " š š " 3 | ö • ~ £ Ý . W | D • Ö • Ý p OE % ö " 3  
p D % ö OE % ö ë " " | • 3 % ö " 3



# Zusammenfassung

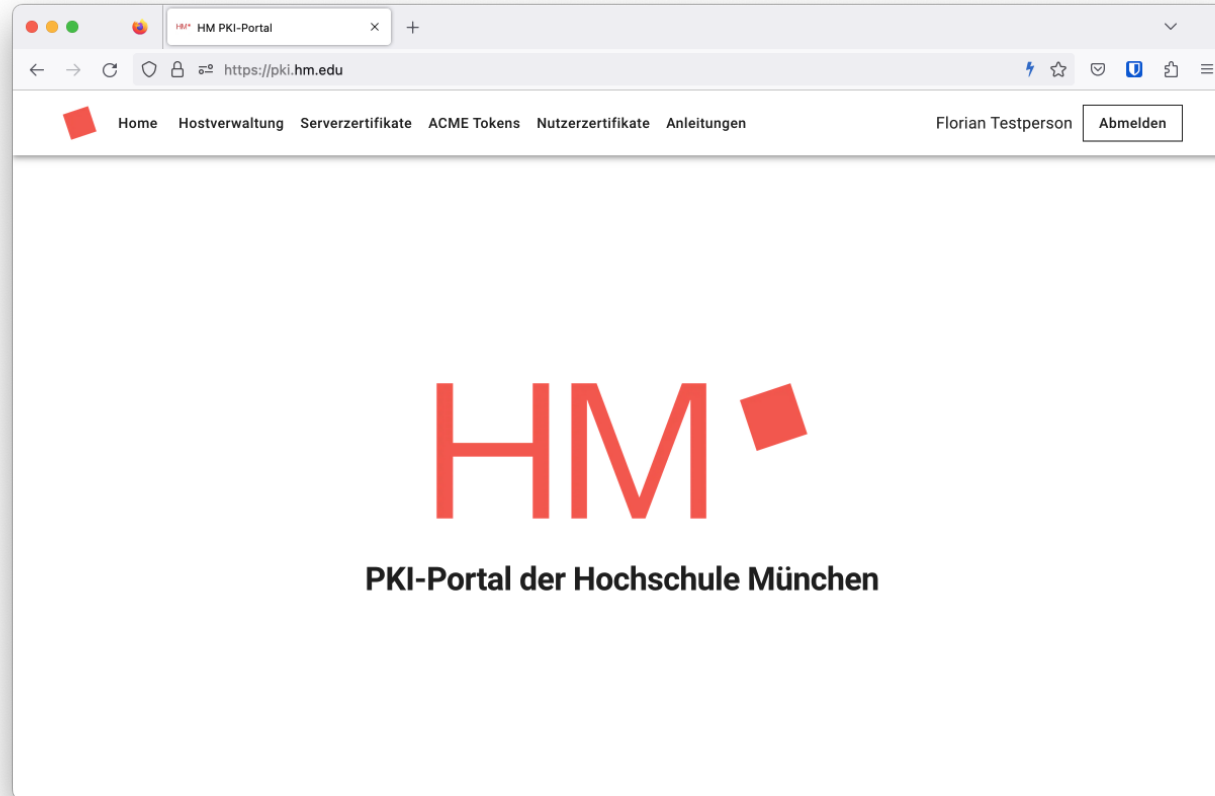
- Veröffentlichung aller Komponenten auf GitHub
  - Frontend: <https://github.com/hm-edu/portal-frontend>
  - Backend-Dienste: <https://github.com/hm-edu/portal-backend>
  - ACME-Dienst: <https://github.com/hm-edu/certificates>
  - **VbV^Xež Vb` cbf X**-Deployment: <https://github.com/hm-edu/portal-deployment>
- ) 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 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 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 right of the table area, 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 with a plus icon and the text "Neues Zertifikat beziehen".