UNIVERSITÄT HOHENHEIM

NUTZERZERTIFIKATE: WARUM SIEHT MEIN NEUES S/MIME-ZERTIFIKAT ANDERS AUS?

Warum unterscheidet sich ein neues HARICA/GÉANT-TCS-Zertifikat vom bisherigen DFN-PKI-Zertifikat?

HANDREICHUNG

KIM | KOMMUNIKATIONS-, INFORMATIONS- UND MEDIENZENTRUM

Version 1.00

Inhalt

1 INFORMATION / HINWEIS

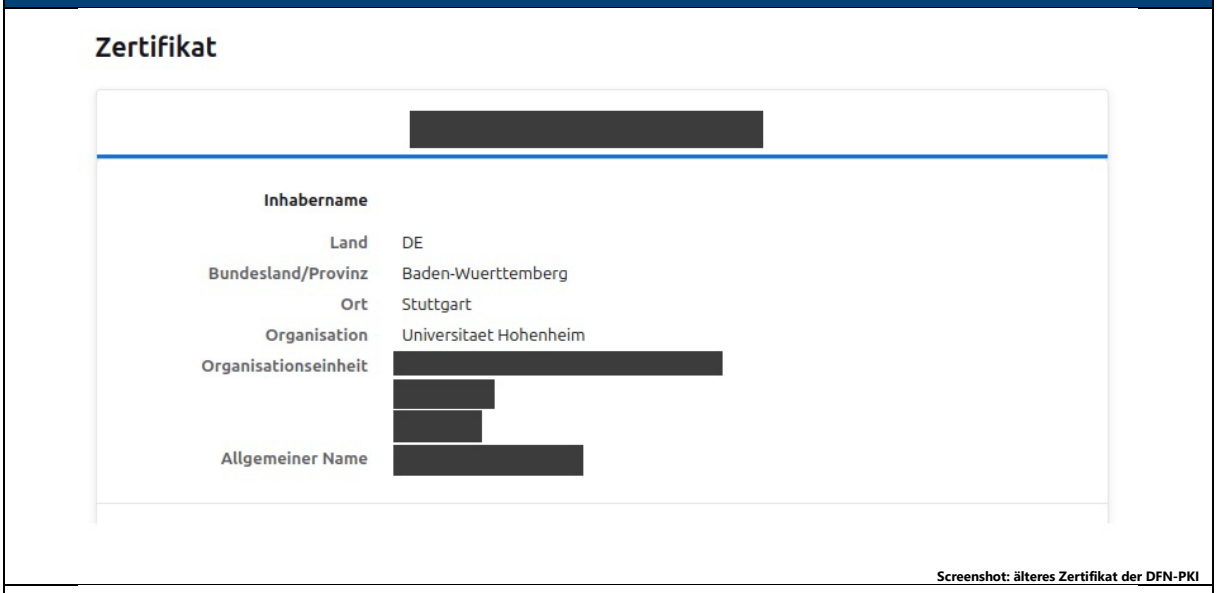
Dieses Dokument richtet sich an Beschäftigte der Universität Hohenheim, die ein neues S/MIME-Zertifikat über den GÉANT Trusted Certificate Service (TCS) – bereitgestellt durch HARICA – bezogen haben und feststellen, dass es im E-Mail-Client anders dargestellt wird als das bisherige Zertifikat der DFN-PKI. Es erklärt die Ursachen dieser Unterschiede technisch korrekt und quellenbelegt. Die Änderungen betreffen alle Beschäftigten gleichermaßen und sind kein Einzelfall.

Beispiel:

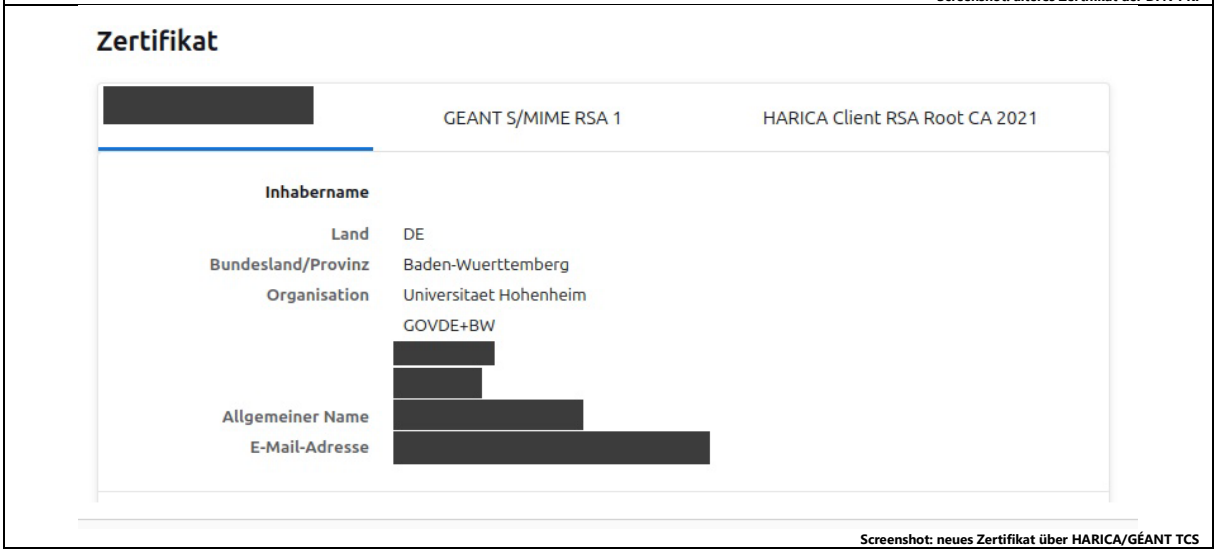
Gegenüberstellung: Altes DFN-Zertifikat vs. neues HARICA-Zertifikat

Die folgende Abbildung zeigt exemplarisch, wie ein S/MIME-Zertifikat im E-Mail-Client dargestellt wird – oben ein älteres Zertifikat der DFN-PKI, unten ein neues Zertifikat über HARICA/GÉANT TCS.

ABBILDUNG — Zertifikatsdetailansicht im E-Mail-Client



Screenshot: älteres Zertifikat der DFN-PKI



Screenshot: neues Zertifikat über HARICA/GÉANT TCS

Merkmal	Altes DFN-Zertifikat (oben)	Neues HARICA-Zertifikat (unten)
Organisationseinheit (OU)	Vorhanden – frei befüllbar (z. B. Abteilungsname)	Nicht vorhanden – durch S/MIME BR verboten
organizationIdentifier	Nicht vorhanden	Pflichtfeld: GOVDE+BW
E-Mail-Adresse im Subject	Nicht enthalten	Pflichtfeld im Sponsor-validated-Profil
Zertifikatskette (Tabs)	Nur End-Zertifikat sichtbar	Vollständige Kette: End-Zertifikat → GÉANT S/MIME RSA 1 → HARICA Client RSA Root CA 2021

2 WARUM FEHLT DIE „ORGANISATIONSEINHEIT“ (OU) IM NEUEN ZERTIFIKAT?

Ältere S/MIME-Zertifikate der DFN-PKI konnten ein frei befüllbares Feld **Organisationseinheit (OU)** enthalten – beispielsweise den Namen einer Abteilung oder Stabsstelle. In neuen Zertifikaten, die über HARICA/GÉANT TCS ausgestellt werden, ist dieses Feld nicht mehr vorhanden.

Das ist **kein Fehler, keine Entscheidung von HARICA und kein Problem mit dem Zertifikat selbst.** Es handelt sich um eine verbindliche Vorgabe des CA/Browser Forums, die seit dem **1. September 2023** für alle öffentlich vertrauenswürdigen S/MIME-Zertifikate weltweit gilt.

➢ NACHWEIS 1 — EINFÜHRUNG DER S/MIME BASELINE REQUIREMENTS

Quelle [1]: GlobalSign Advisory zu den neuen S/MIME BR (support.globalsign.com)

> *„CA/B Forum new set of standards called Baseline Requirements (BR), will take effect on September 1, 2023. It is a significant milestone for the security and privacy of electronic communications, as S/MIME Certificates are used to secure email communications and protect sensitive information."*

➢ NACHWEIS 2 — OU-FELD IST NICHT MEHR ZULÄSSIG

Quelle [2]: DigiCert Knowledge Base – Umsetzung der neuen S/MIME BR (knowledge.digicert.com)

> *„**Organization units (OU) are no longer supported.** If the Subject DN:OU is included in the certificate request, we will ignore the value and issue the certificate without it."*

DigiCert wird hier stellvertretend zitiert; HARICA ist an dieselben Regeln des CA/B Forums gebunden.

➢ NACHWEIS 3 — BESTANDSZERTIFIKATE SIND NICHT BETROFFEN

Quelle [2]: DigiCert Knowledge Base (knowledge.digicert.com)

> *„Certificates issued before August 29, 2023, can still contain the organization unit information [...]. The industry changes do not affect S/MIME certificates issued before August 29, 2023. You can continue to use these existing certificates until they expire."*

➢ NACHWEIS 4 — GÉANT TCS KÜNDIGT GEÄNDERTE SUBJECT-FELDER AN

Quelle [3]: GÉANT TCS Wiki – Trust Anchors and Intermediates (wiki.geant.org)

> *„At the same time, the subject naming of email signing 'S/MIME' certificates will change significantly – you cannot and must not rely on subject name uniqueness for these email signing certificates."*

3 WAS BEDEUTET DER EINTRAG „GOVDE+BW" IM NEUEN ZERTIFIKAT?

In neuen HARICA/GÉANT TCS-Zertifikaten erscheint im Bereich der Organisationsangaben ein Eintrag der Form **GOVDE+BW**. Dieser Wert ist kein Fehler, sondern ein neues **Pflichtfeld**: der sogenannte *organizationIdentifier*. Er wurde durch die S/MIME Baseline Requirements eingeführt und ist für alle Zertifikate verpflichtend, die Organisationsdaten enthalten.

➢ NACHWEIS 5 — ORGANIZATIONIDENTIFIER IST PFLICHTFELD

Quelle [4]: CA/B Forum – S/MIME Baseline Requirements, aktuell v1.0.14 (cabforum.org)

> *„The identifier **SHALL** be included in the Certificate subject:organizationIdentifier as specified in Section 7.1.4.2.2 and Appendix A."*

➢ NACHWEIS 6 — FORMAT UND HERKUNFT DES IDENTIFIKATORS

Quelle [5]: GlobalSign EPKI FAQs zu den S/MIME BR (support.globalsign.com)

> *„The Organization Identifier can be allocated by the national tax authorities (VAT), by a national or state trade register (NTR), or specified in ISO 17442 (LEI) for a legal entity named Organization Name."*

Das Format **GOVDE+BW** ist ein standardisierter, maschinenlesbarer Code:

Kürzel	Bedeutung
GOV	Government – staatliche bzw. öffentlich-rechtliche Entität
DE	Deutschland (Länderkürzel nach ISO 3166-1)
+BW	Baden-Württemberg (Bundeslandkürzel)

Der Wert klassifiziert die Universität Hohenheim als öffentlich-rechtliche Körperschaft des Landes Baden-Württemberg. Er **ersetzt** das frühere, nicht verifizierte OU-Freitext-Feld durch einen standardisierten, von der CA verifizierten Organisations-Nachweis.

4 WAS IST EIN „ZERTIFIKATSPROFIL" UND WELCHES WIRD FÜR BESCHÄFTIGTE VERWENDET?

Ein **Zertifikatsprofil** ist eine verbindliche Vorlage, die für einen bestimmten Anwendungsfall exakt festlegt, welche Felder ein Zertifikat enthalten muss, darf oder nicht darf. Vor Einführung der S/MIME Baseline Requirements existierte kein einheitliches Profil für persönliche E-Mail-Zertifikate – jede CA konnte eigene Felder und Strukturen wählen.

Die neuen S/MIME BR definieren vier klar voneinander abgegrenzte Zertifikatstypen, die anhand des Zertifikatsinhalts eindeutig unterscheidbar sind:

Typ 1

Mailbox-validated

Enthält ausschließlich die E-Mail-Adresse und/oder eine Seriennummer. Kein Personenname, keine Organisation.

Typ 2

Organization-validated

Enthält ausschließlich Organisationsdaten, z. B. für Funktionspostfächer. Kein Personenname.

Typ 3 — für Beschäftigte

***Sponsor-validated** (IV+OV)*

Enthält sowohl Organisationsdaten als auch den Namen der Person. Erfordert persönliche Identifizierung. Empfohlenes Profil für Beschäftigte einer Organisation.

Typ 1

Mailbox-validated

Enthält ausschließlich die E-Mail-Adresse und/oder eine Seriennummer. Kein Personenname, keine Organisation.

An der Universität Hohenheim kommen für Beschäftigte aktuell zwei Typen zum Einsatz: **Mailbox-validated (MV)** ist dabei der vorwiegend ausgestellte Typ und erfordert lediglich die Kontrolle über das E-Mail-Postfach. **Sponsor-validated (IV+OV)** ist der neuere, fachlich empfohlene Typ mit höherem Vertrauensniveau – er setzt jedoch eine persönliche Identifizierung der antragstellenden Person voraus, was mit mehr Aufwand verbunden ist und daher nicht für alle Beschäftigten gleichermaßen in Frage kommt.

➢ NACHWEIS 7 — DEFINITION SPONSOR-VALIDATED IN DEN S/MIME BR

[6]: Mozilla Security Policy Group – Profildefinitionen (groups.google.com)

> *„Sponsor-validated: the most common type of S/MIME certificate, often issued by an Enterprise to its employees. The Subject includes **organization details as well as attributes of a 'sponsored' individual.**"*

➢ NACHWEIS 8 — GÉANT TCS VERWENDET SPONSOR-VALIDATED FÜR PERSÖNLICHE E-MAIL-ZERTIFIKATE

Quelle [7]: GÉANT TCS 2020 FAQ (wiki.geant.org)

> *„This public S/MIME will use the **sponsor-validated profile** to insert the givenName and surname of the applicant alongside the organisation name."*

> *„since this template is of new sub-type **Public Sponsored Validated**, it can only be issued to persons with a validation type of High."*

➢ NACHWEIS 9 — HARICA TCS-PORTFOLIO WEIST SPONSOR-VALIDATED EXPLIZIT AUS

Quelle [8]: ACOnet Infoshare Oktober 2025 (aco.net) – österreichisches Pendant zum DFN, ebenfalls HARICA TCS-Nutzer

> *„S/MIME Zertifikate: ‚Email-only' (BR: Mailbox-validated) · **‚For enterprises or organizations (IV+OV)' (BR: Sponsor-validated)**"*

Das ACOnet nutzt denselben HARICA TCS-Dienst wie das DFN für Deutschland. Die Produktbezeichnung bestätigt, dass das Profil für Organisations-Beschäftigte im HARICA TCS ausdrücklich als Sponsor-validated geführt wird.

Technische Verifikation: Der Zertifikatstyp ist im Zertifikat selbst als Policy-OID hinterlegt. Die vier Typen haben eindeutige, standardisierte Kennungen:

2.23.140.1.5.1.x	Mailbox-validated
2.23.140.1.5.2.x	Organization-validated
2.23.140.1.5.3.x	**Sponsor-validated** — zu erwarten in Beschäftigten-Zertifikaten über HARICA TCS
2.23.140.1.5.4.x	Individual-validated

Die Policy-OID lässt sich auf einem **Linux-System** mit folgendem Befehl auslesen, sofern das Zertifikat als .pem-Datei vorliegt:

```
openssl x509 -in zertifikat.pem -text -noout | grep -A2 "Certificate Policies"
```

Beispielausgabe eines IV+OV-Zertifikats über HARICA TCS:

```
X509v3 Certificate Policies:
    Policy: 2.23.140.1.5.3.2
    Policy: 0.4.0.2042.1.3
```

Die erste OID 2.23.140.1.5.3.2 lässt sich wie folgt aufschlüsseln:

OID-Segment	Bedeutung
2.23.140.1.5	CA/B Forum – S/MIME Baseline Requirements (Basis-OID-Bogen)
.3	Zertifikatstyp: Sponsor-validated (IV+OV)
.2	Generation: **Multipurpose** (1 = Legacy, 2 = Multipurpose, 3 = Strict)

Die zweite OID 0.4.0.2042.1.3 ist eine ETSI-Policy-OID (ETSI TS 119 411, Lightweight Certificate Policy) und zeigt an, unter welchem europäischen Prüfrahmen HARICA als CA auditiert wird. Sie ist für die Einschätzung des Zertifikatstyps nicht relevant, aber ein Zeichen dafür, dass das Zertifikat unter einem anerkannten europäischen Prüfstandard ausgestellt wurde.

5 WARUM WAR DAS ALTE DFN-ZERTIFIKAT ANDERS AUFGEBAUT?

Die unterschiedliche Struktur des alten DFN-Zertifikats hat einen einfachen Grund: Zum Zeitpunkt seiner Ausstellung existierten noch keine verbindlichen, branchenweiten Regeln für den Inhalt von S/MIME-Zertifikaten. Jede CA – darunter auch die DFN-PKI – konnte eigene Profile und Feldbelegungen frei definieren.

➢ NACHWEIS 10 — FEHLENDE STANDARDISIERUNG VOR 2023

[9]: The SSL Store Blog – New S/MIME Standards Go Into Effect in September 2023 (thesslstore.com)

> *„Despite the widespread use of the S/MIME protocol, particularly among large enterprises,* ***previously there were few standards governing the way that Certificate Authorities (CAs) issue S/MIME digital certificates.***"

Der gleiche Artikel beschreibt den Zustand vor 2023 als „Wild West" – jede CA konnte nach eigenem Ermessen entscheiden, was in ein S/MIME-Zertifikat kommt. Mit den Baseline Requirements ist dieser Zustand beendet. Die sichtbaren Unterschiede zwischen altem und neuem Zertifikat sind die direkte Folge dieser Vereinheitlichung.

Das bedeutet konkret: Ein altes DFN-Zertifikat mit OU-Eintrag ist nicht „besser" oder „vollständiger" als ein neues HARICA-Zertifikat ohne OU. Es entspricht schlicht einem früheren, weniger regulierten Stand der Technik. Das neue Zertifikat folgt einem strengeren, international einheitlichen Standard.

- QUELLENVERZEICHNIS

[1] GlobalSign – Advisory: New S/MIME Baseline Requirements via CA/B Forum
https://support.globalsign.com/personal-sign-email/advisory/new-smime-baseline-requirements-cab-forum

[2] DigiCert Knowledge Base – New industry requirements for public Secure Email (S/MIME) certificates
https://knowledge.digicert.com/alerts/new-industry-requirements-for-public-secure-email-smime-certificates

[3] GÉANT TCS Wiki – TCS Trust Anchors and Intermediates
https://wiki.geant.org/spaces/TCSNT/pages/661521170/TCS+Trust+Anchors+and+Intermediates

[4] CA/Browser Forum – Latest S/MIME Baseline Requirements (aktuell v1.0.14, Stand Mai 2026)
https://cabforum.org/working-groups/smime/requirements/

[5] GlobalSign – FAQs: S/MIME Baseline Requirements for EPKI
https://support.globalsign.com/enterprise-pki/smime-baseline-requirements-epki-faqs

[6] Mozilla Security Policy Group – S/MIME Certificate Working Group, Profildefinitionen
https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/RjvEdwSWYKs/m/QhBILLYRAwAJ

[7] GÉANT TCS 2020 FAQ – Umstellung auf Sponsor-validated Profil
https://wiki.geant.org/display/TCSNT/TCS+2020+FAQ

[8] ACOnet Infoshare Oktober 2025 – Aktueller Status HARICA TCS Portfolio (PDF)
https://www.aco.net/fileadmin/verein/infoshares/aconet-infoshare_2025-10-03.pdf

[9] The SSL Store – New S/MIME Standards Go Into Effect in September 2023
https://www.thesslstore.com/blog/new-s-mime-standards-go-into-effect-in-september-2023/