ACONET Infoshare

Trusted Certificate Service (TCS)

03. Oktober 2025

aconet verein

aconet

ACONET Infoshare - Agenda

1. **Trusted Certificate Service**
   Kurt Bauer

2. **Q & A**

3. Kommende **Meetings**

TCS - Trusted Certificate Service

ACOnet Infoshare

Kurt Bauer

03. Oktober 2025

Themen

- allgemeine Entwicklungen
- aktueller Status & Demo
- Ausblick

Themen

- allgemeine Entwicklungen
- aktueller Status & Demo
- Ausblick

Gültigkeitsdauer Server Zertifikate

- Baseline Requirements – Section 6.3.2

Ausstellung am oder nach	Ausstellung vor	maximale Gültigkeitsdauer
	15. März 2026	398 Tage
15. März 2026	15. März 2027	200 Tage
15. März 2027	15. März 2029	100 Tage
15. März 2029		47 Tage

verringerte Gültigkeitsdauer gilt auch für die Validierung der Domains (DCV)

Domain Control Validation – Email based

- Baseline Requirements – Section 3.2.2.4.2
  - Kontakte aus WHOIS Einträgen dürfen nicht mehr verwendet werden (effective 15.01.2025)
  - Möglichkeiten:
    - pre-approved by the CA/B forum (BR Section 3.2.2.4.4)
      - admin@..., administrator@..., hostmaster@..., postmaster@..., webmaster@...
    - Email to DNS CAA Contact (BR Section 3.2.2.4.13 & Appendix A.1.1)
      - foo.bar.at CAA 0 issue “meine.ca.at“
foo.bar.at CAA 0 iodef mailto:zertifikate@bar.at
    - Email to DNS TXT Contact (BR Section 3.2.2.4.14 & Appendix A.2.1)

MPIC - Multi-Perspective Issuance Corroboration

- Baseline Requirements – Section 3.2.2.9
- verpflichtend seit 15.05.2025
- MPIC erhöht die Sicherheit von DNS- und CAA-Validierungen durch die Durchführung von Überprüfungen aus mehreren geografisch verteilten Standorten.
  Dieser Ansatz mindert das Risiko von Angriffen, indem sichergestellt wird, dass die Validierungsergebnisse in allen Regionen konsistent sind.
- → globale Erreichbarkeit der DNS Server sicherstellen

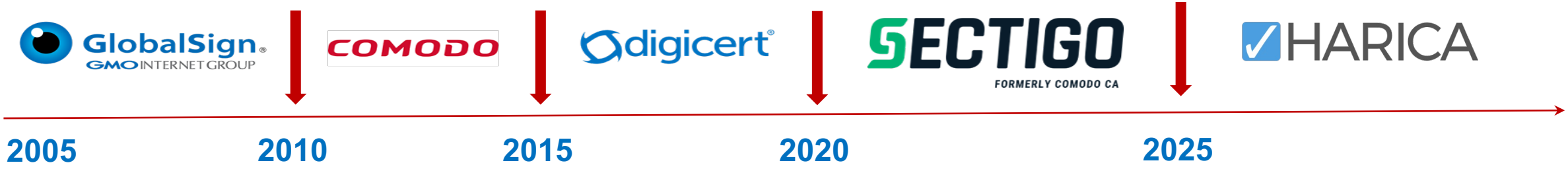
CAA Records & DNSsec

Bei Problemen mit DNSsec im Rahmen der Prüfung von CAA RRs ist die CA durch die Baseline Requirements verpflichtet den Antrag abzulehnen. ***https://dnsviz.net/***

Themen

- allgemeine Entwicklungen
- aktueller Status & Demo
- Ausblick

Rückblick bzw. Einordnung



- einseitige Beendigung des Service durch Sectigo mit 10.01.2025
- Übernahme der Basisfunktionalität durch Harica mit 14.01.2025
- sehr rasche und problemlose Validierung der Organisationen mit absichtlichem ‘slow start’
- kontinuierliche Weiterentwicklung und Erweiterung der Funktionalität seitens Harica
- sehr gute Kommunikation mit Harica – regelmäßige VCs mit GÉANT & TCS-PMA
- lange ‘issues list’, priorisiert durch TCS-PMA, wird fleissig abgearbeitet

aktueller Status - Portfolio

- im TCS Porfolio verfügbar
  - *TLS Server Zertifikate* – DV, OV (bis zu 100 SANs)
  - *S/MIME Zertifikate:*
    - ‘Email-only’ (*BR: Mailbox-validated*)
    - ‘For enterprises or organizations (IV+OV)’ (*BR: Sponsor-validated*)
  - *IGTF Zertifikate (falls benötigt beim ACOnet Team (tcs@aco.net) melden)*
    - TLS Server Zertifikate
    - AuthN Zertifikate
- alles andere kostet pro Zertifikat, wie im Portal angegeben

aktueller Status – S/MIME

- wie kommt man derzeit zu einem S/MIME Zertifikat
  - mit lokalem Account
    - ‘Email-only’ :
      - Authorisierung über Domain-Teil der Mailadresse
      - nur Email Verifikation
    - ‘For enterprises or organizations (IV+OV)’
      - Hochladen von Ausweisdokument, wird von Harica geprüft
      - Bestätigung durch ‘Enterprise Approver’ notwendig
  - ‘Bulk’ Ausstellung
    - p12 Passwort für alle Zertifikate durch Admin vorgegeben → Sicherheitsbedenken
  - API

aktueller Status – S/MIME

- SAML Self-Service Portal (für 'For enterprises or organizations (IV+OV)')
  - verfügbar, unter folgenden Voraussetzungen:
    - Teilnahme an der ACOnet Identity Federation (*SAML*) & edugain (*SAML interfederation*)
    - Übermittlung der notwendigen Attribute
      - givenName (oid:2.5.4.42)
      - surname (oid:2.5.4.4)
      - mail (oid:0.9.2342.19200300.100.1.3) *(aktuell wird nur die erste verwendet, sollten mehrere übertragen werden)*
      - edupersonTargetedID (oid:1.3.6.1.4.1.5923.1.1.1.10)
      - eduPersonEntitlement (oid:1.3.6.1.4.1.5923.1.1.1.7), mit einem der folgenden Werte:
        - urn:mace:terena.org:tcs:personal-user

        oder
        - urn:mace:terena.org:tcs:smime-sv-autoissue
  - keine weitere Interaktion von Beantragendem oder Admin notwendig

aktueller Status – ACME

- Enterprise ACME
  - OV Zertifikate
    - nur mit ‘pre-validated’ Domains
    - keine ACME Challenge
  - DV Zertifikate
    - ACME Challenge, falls Domain nicht validiert (nicht ‘pre-validated’)
    - Domain muss allerdings beim ‘Enterprise’ gelistet sein
  - Accountverwaltung für Einschränkung der Domains (EAB)
    - granulare Zuweisung von Domains/Hostnamen mittels Allow/Deny Liste
    - wahlweise inklusive oder exclusive Sub-Domains
  - kann nur von Enterprise Admin erstellt werden

aktueller Status – ACME

- personal ACME
  - “wie ‘lets encrypt’ von Harica”
    - nur DV Zertifikate
  - jedenfalls mit ACME Challenge
    - Domain muss allerdings beim ‘Enterprise’ gelistet sein
  - muss vom Enterprise Admin freigeschalten werden
  - steht dann jedem authentifizierten User zur Verfügung, der als ‘Teil des Enterprise’ erkannt wird (über Domain-Teil der Mailadresse)
  - 3 active ACME Accounts pro User möglich

aktueller Status – API

- schlechte bis keine Dokumentation
- AuthN nur mit Username/Passwort & 2. Faktor
- Beispiele zur Verwendung siehe https://wiki.univie.ac.at/display/tcs/FAQ#FAQ-api
- Verbesserungen versprochen bis Q3/2025
  - Token-based AuthN
  - zumindest komplette Swagger “Doku”

Themen

- allgemeine Entwicklungen
- aktueller Status & Demo
- Ausblick

Ausblick

- aktuelle Lösung mittels freihändiger Vergabe → max. 2 Jahre
- Beginn der Arbeiten für die Ausschreibung mit Q4/2025, Veröffentlichung Q1/2026
  - Auszug von davor zu beantwortenden Fragen:
    - notwendige Zertifikatstypen
    - ein Anbieter oder mehrere Anbieter
    - Änderungen der Preisstruktur (eventuell kein flat-fee Modell wie bisher)
    - …
- Was wünscht ihr euch vom zukünftigen Zertifikatsservice?
  - Ideen/Wünsche/Vorschläge bitte an tcs@aco.net

Danke!

aco.net

Kommende Meetings

- **ArgeZID** 15.-17.10.2025 @ St.Wolfgang
- **KUKIT Stammtisch** 21.10.2025 @ Volkskundemuseum Wien
- **ACONET Infoshare Künstliche Intelligenz** 23.10.2025 @ Online
- **ACOnet-TBPG** 6.-7.11.2025 @ Weltmuseum Wien
- **35 Jahre ACOnet** im Rahmen TBPG 6.11.2025 @ Weltmuseum Wien

Danke!

aco.net/verein