Updates zu TCS/KIT-CA/Zertifikaten

Einschub: Google verschärft Regeln für E-Mail-Empfang

- Google Mail verschärft ab Februar, Detail siehe DFN-Mailsupport
  - Korrektes SPF, DKIM, DMARC und ARC
    - Die ersten drei sind seit Herbst 2023 flächendeckend am KIT implementiert
  - Unsubscribe-Links nach RFC 8058 für Massenmails
- Bei mehr als 0.3% Verstößen werden ab April alle Mails vom KIT hart abgelehnt
  - Google-Doku suggeriert: es zählen nur menschliche Beschwerden?

- Bisher: „Klarer“ Spam schon immer ausgehend abgewiesen, potentieller Spam nicht
- Jetzt: potentieller Spam mit niedrigem Spam-Score Richtung Google wird zurückgewiesen

Themen

- Trust bei Server-Zertifikaten
  - DFN-PKI vs. GÉANT TCS/Sectigo vs. Let‘s Encrypt
  - Typosquatter-Domains
- Signieren von Dokumenten

DFN-PKI vs. GÉANT TCS/Sectigo vs. Let‘s Encrypt

- DFN-PKI ist rum, keine Zeit mit Nostalgie vertrödeln

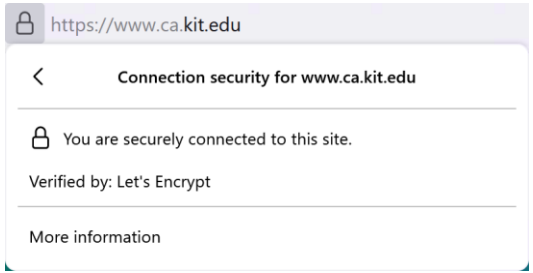
- Let‘s Encrypt: *domain-validiert* (DV)
- GÉANT TCS/Sectigo: *organisations-validiert* (OV)

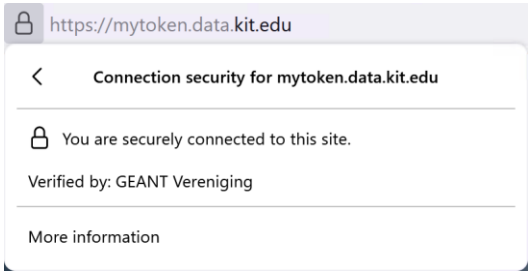
- Für DV-Zertifikat muss nur geprüft werden, ob der Antragsteller Kontrolle/Besitz über die Domain hat. Damit landet auch nur die Domain im Zertifikat.
- Für OV-Zertifikat wird zusätzlich noch die Identität der Organisation geprüft und im Zertifikat vermerkt.

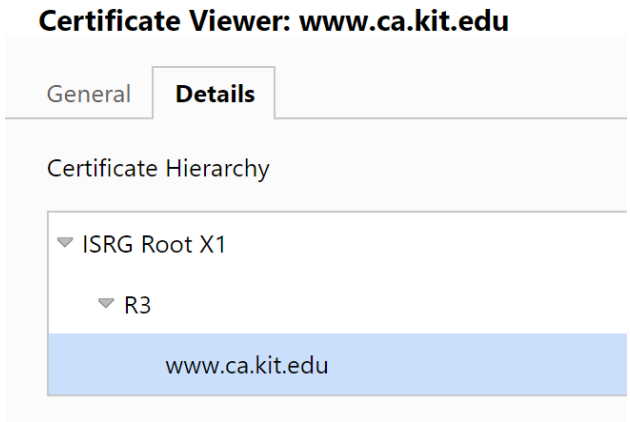
Prüfung der Trust-Chain sinnvolles Hilfsmittel?

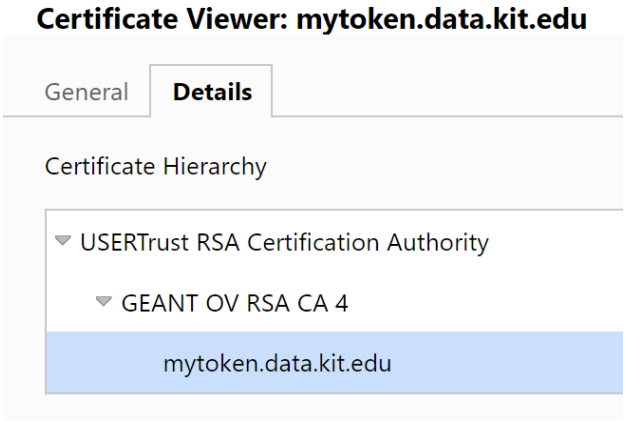
- Akademisch: Nutzer prüfen relevante Marker nicht (zu versteckt, fehlendes Wissen)
- EV-Zertifikate waren sichtbarer und haben sich nicht durchgesetzt.
- „Let‘s Encrypt ist die CA der Spammer“
  - Let‘s Encrypt ist **die** CA des Internets (325 Millionen gültige Zertifikate). Das inkludiert die Spammer. Reicht deswegen aber nicht als Erkennungs-Merkmal.
- GÉANT TCS wechselt das alle 5 Jahre. Ist also nicht beständig
  ⇝ schwer den Nutzern beizubringen.

Details prüfen (oben Firefox, unten Edge)?

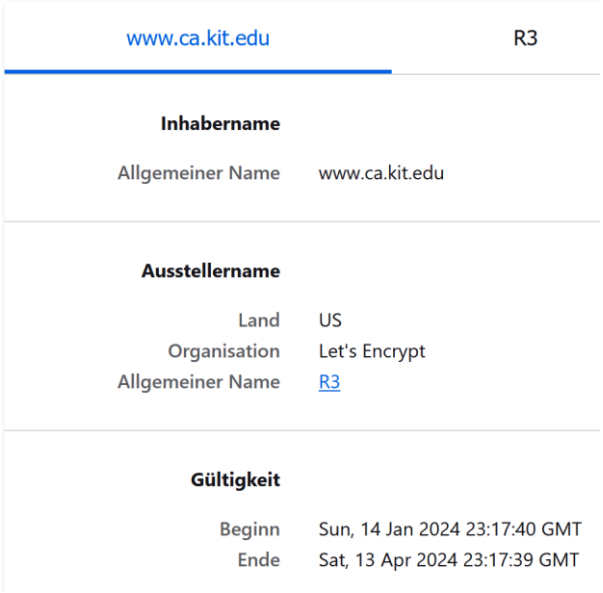


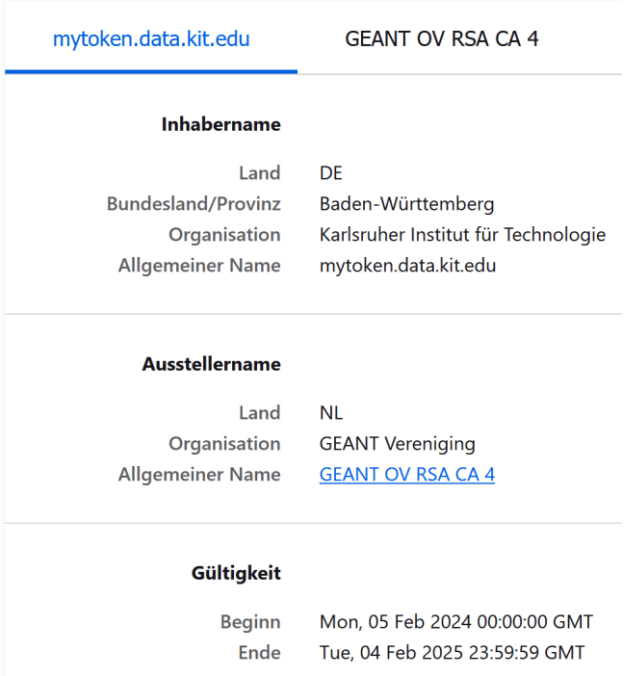






Details in Firefox





Typosquatter-Domains

- 𝒦ℓT.edu ≠ kit.edu
  - Real (Punycode): **xn--kl-de6n.edu**
- Der Angriff auf den Nutzer findet hier vor der HTTPS-Verbindung statt.
- Prüfung der Chain würde helfen, macht aber niemand (korrekt).
- Akademisch: solange die Nutzer fröhlich auf **kitt-administator-edu.yolasite.com** ihr Passwort eingeben, muss kein Angreifer besser sein als das.
  - Wer keine Domainnamen kritisch anschaut, prüft erst recht keine Zertifikatsketten

OV (GÉANT TCS/Setigo) > DV (Let‘s Encrypt)?

- Let‘s Encrypt prüft Domain-Ownership via ACME mittels Challenge (**http-01** und **dns-01**)

- Was macht wir?
  - Sectigo kennt unsere Domains a priori ☑
  - Berechtigung Antragsteller prüfen ist für uns dann Detektivarbeit:
    - NETVS-Zugang?
    - ITB?
    - Geheimwissen („die X betreibt Y“)?
    - Org-Diagramme und Webseiten ansehen
- ⇝ wir machen de facto **dns-01**, nur schlechter als ACME

Trust (technisch/operativ)

- Trust/Vertrauensstellungen existieren immer in einem Umfeld/Kontext. Die Standards unterscheiden sich hier und sind auch nicht statisch:
  - Microsoft Trusted Root Program
  - Trusted root certificates for Apple operating systems
  - Mozilla Included CA Certificate List
  - Google Chrome Root Store
  - Adobe Approved Trust List (AATL)
  - Oracle Java Root Certificate program
  - CA certificates trusted by Gmail for S/MIME
  - …

Trust (technisch/operativ)

- Globaler Trust geregelt durch das CA-Browserforum
  - Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates (plus EV)
  - Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates
  - Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

- Kurz: CAs, deren *Zertifikate im Browser als sicher akzeptiert* werden sollen, müssen sich an diese Regeln halten
- Das schlägt sich dann in den Policies der einzelnen CAs nieder

Trust (juristisch)

- eIDAS-Verordnung & Vertrauensdienstegesetz
  - Definiert für Europa verbindliche Standards für digitale Unterschriften und weitere trust-basierte Prozesse
- Gibt dort drei Type von Signaturen
  1. elektronische Signatur
  2. fortgeschrittene elektronische Signatur
  3. qualifizierte elektronische Signatur (QES)
- Eine Dokumentensignatur mit einem DFN-/GÉANT TCS-Zertifikat ist eine *fortgeschrittene elektronische Signatur*.
- QES ist (juristisch) äquivalent zu einer klassischen Unterschrift
  - Vorgeschrieben für bestimmte Tätigkeiten: Abfallwirtschaft, Rechtsgeschäfte, …

Wie bekommt man ein Zertifikat für eine QES?

- Es gibt bei der EU eine Liste von akkreditierten Anbietern
  - Keine der dem KIT zugänglichen CAs steht da drauf

- Für QES braucht man
  - Die richtige CA
  - Zertifizierte Hardware (Reader und Smartcard)
  - ~~€€€~~
  - Individuell (oder eSeal für Orgs)

〰 wir können weder mit der alten KIT-CA noch mit Sectigo „gescheite“ Dokumentensignaturen erzeugen

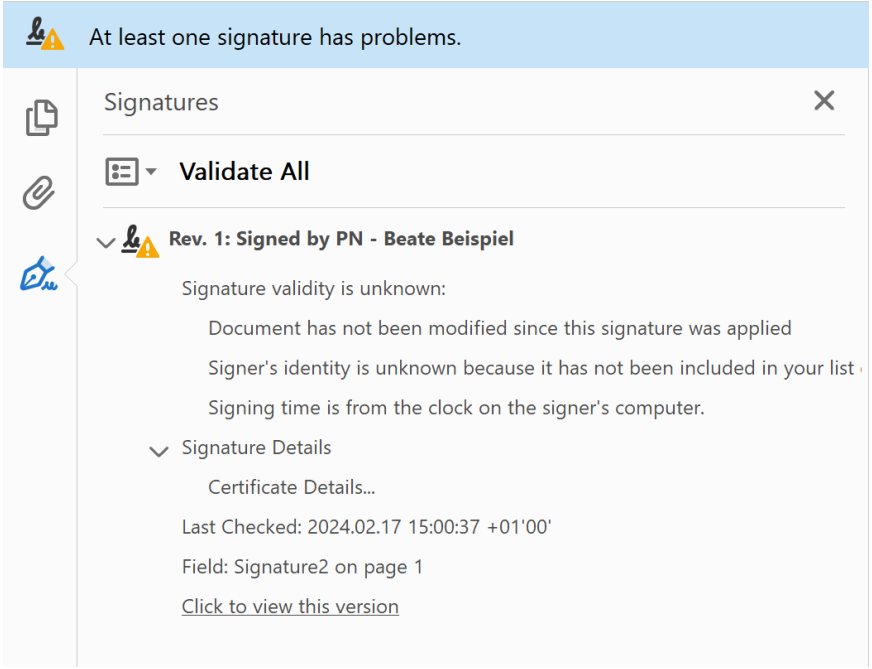
Validierung in der Praxis

- Wie erinnern uns an die Folie mit Trust und Kontext?
- Jeder PDF-Reader hat da was Eigenes
- Goldstandard ist der Acrobat Reader mit seiner AATL
  - Die AATL inkludiert die EIDAS-Liste und prüft auch nach deren Vorgaben
- Die anderen Reader machen irgendwas…

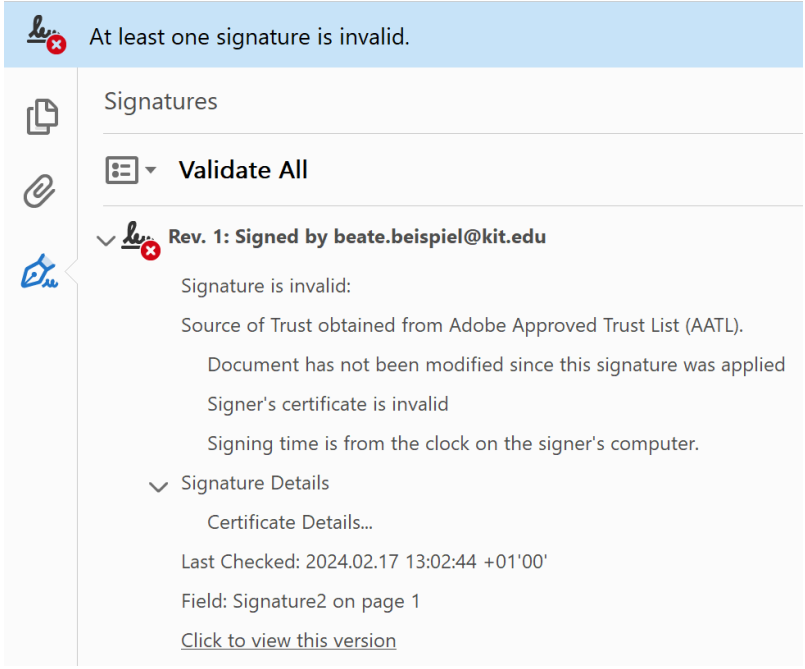
- Problem: *relevant* ist immer die Betriebsumgebung des Empfängers!

Wie sieht das dann aus im Adobe Reader?

DFN-PKI

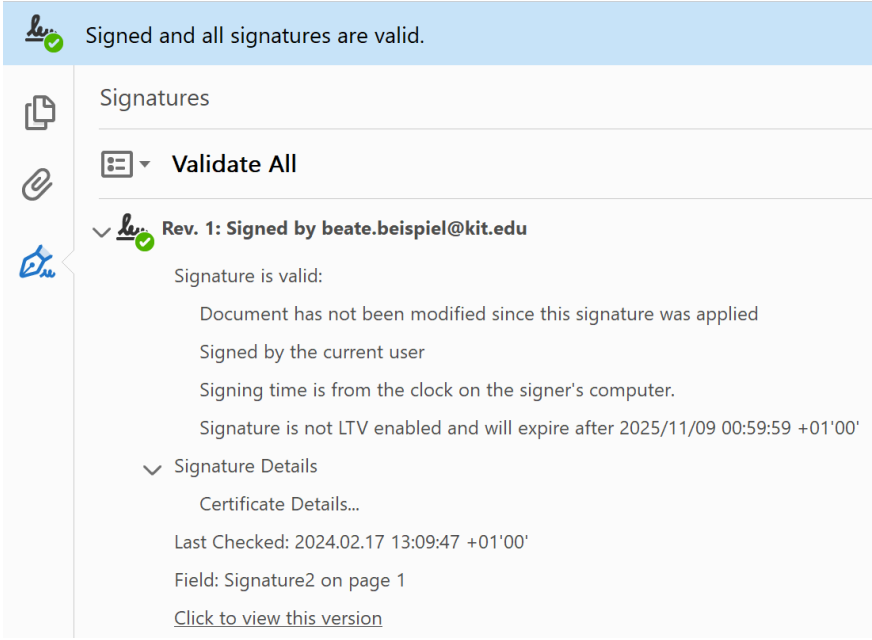


Sectigo



Trust für DFN/Sectigo nachrüsten?

- Für **alle** Empfänger nötig
- Fragil: geht bei Updates kaputt
- Man könnte dafür custom Adobe-Reader-Pakete bauen oder Anleitungen schreiben, aber
  - das darf dann nie bei den Juristen oder Abfallwirtschaftsmenschen installiert werden
  - Muss rigoros gemanaged werden
- Der Prozess ist auch nicht sehr endkunden-freundlich
  - Siehe bspw. Anleitung der Uni Münster



Digitale Signaturen?

- Optionen hängen vom Empfängerkreis ab
  - Unbekannt/weltweit: QES kaufen
  - » ich und meine drei Kolleg:innen«:
    frickelt‘s halt in den Adobe Reader rein
  - Alles andere: 😳?
- Digitale Geschäftsprozesse besser über
  - Portale mit starker Authentifizierung
  - Notfalls: Dokumente in signierte E-Mail packen und E-Mail archivieren
- Siehe auch Whitepaper von bwUni.digital dazu