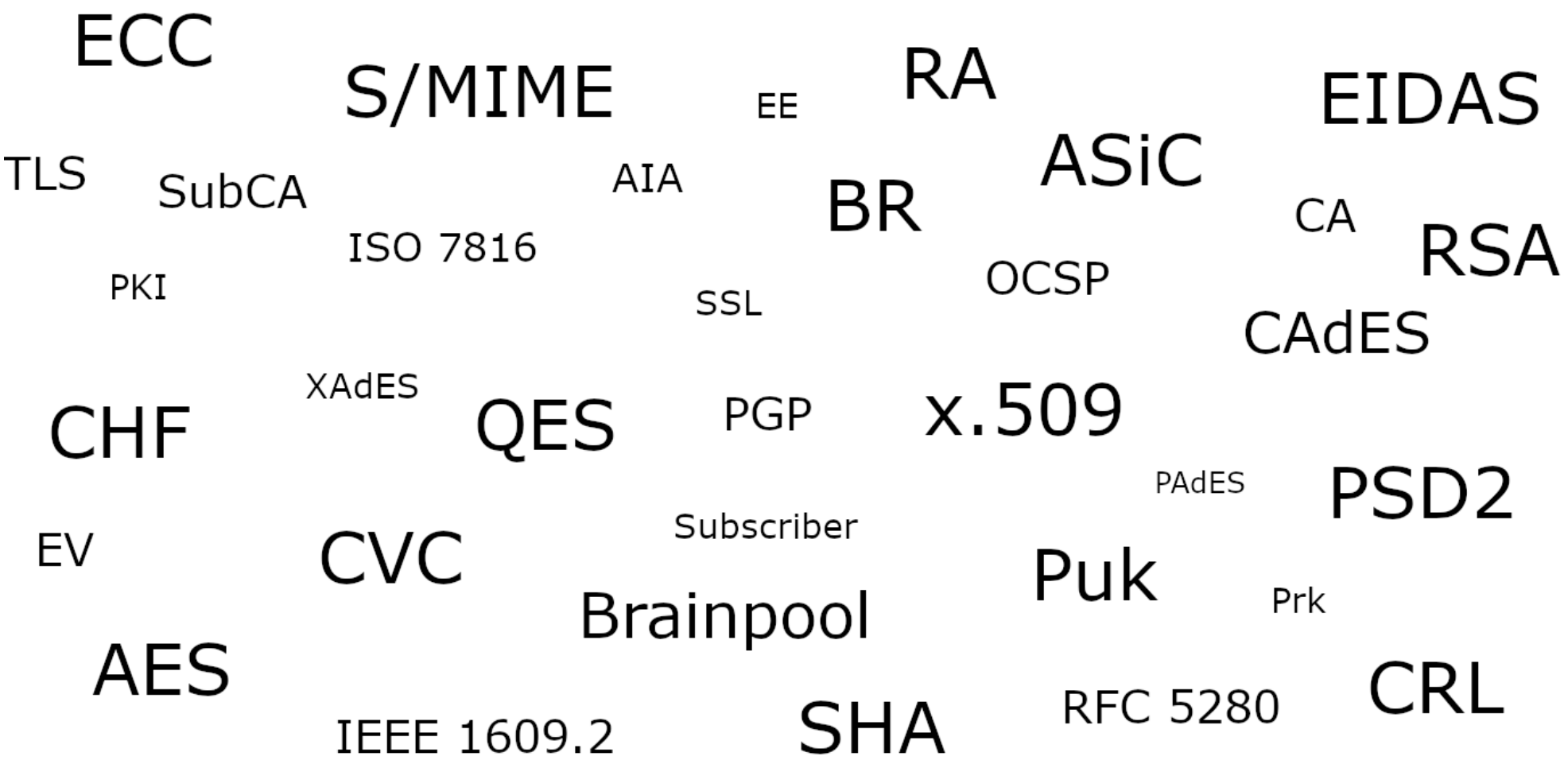
TeleTrusT-EBCA "PKI-Workshop" 2020

Berlin, 01.10.2020

"Qualitätssicherung von elektronischen Zertifikaten"

Christoph Bröter, achelos GmbH

Qualitätssicherung von elektronischen Zertifikaten



Christoph Bröter

- Universität Paderborn
- Seit 2011 achelos GmbH
  - Seit 2015 Konzeption, Realisierung und Beratung im Kontext PKI
    - RU/TU PKI des deutschen Gesundheitswesens
    - Div. eHealth Testsysteme
    - eIDAS Inspector
      - Testsuite zur Konformitätsprüfung digitaler Zertifikate
      - Unterstützung diverser Spezifikationen
        - ETSI EN 319 412, CAB Forum BR, CAB Forum EV, RFC 5280

Motivation (Qualitätssicherung von elektronischen Zertifikaten)

- Zertifikate sind die Essenz einer PKI
  - Inhärentes Vertrauen
- Hohe Medienaufmerksamkeit
  - Presse
  - cert.sh, censys.io
  - Vertrauensentzug
- Vertrauensverlust selbst bei geringer Anzahl an Fehlausstellungen
  - Antragssteller
  - Aussteller (TSP)

Was ist ein Public-Key-Zertifikat

- Digitaler Identitätsausweis
- Technische Umsetzung
  - Metadaten (z.B. Identitätsdaten, Validitätsdaten, Verifizierungsdaten,..) + digitale Signatur einer Trusted Party über jene Metadaten
  - Metadaten
    - z.B. issuer, subject, public key, validity period, keyusage, authority information access, …
  - Digitale Signatur des Hashwertes der Metadaten erstellt von einer Trusted Party (CA)
    - $SIG_{CA_{PRK}}(Hash(m))$

- Standards und Normen
  - RFC 5280 (X.509)
  - ISO 7816 Part 8 (Card verifiable certificate)
  - RFC 4880 (PGP)
  - IEEE 1609.2 (Verkehrstelematik)

Workshop Inhalte

- Erarbeitung eines Konzeptes zur Qualitätssicherung von digitalen Zertifikaten
  - Wie werden die Anforderungen identifiziert?
  - Wie werden die Tests realisiert?
  - Wie werden die Tests getestet?
- Anwendung des Konzeptes am Beispiel mehrerer Spezifikationsanforderungen
- Gegenüberstellung der Konzepte und anschließende Diskussion
- Vorstellung der Diskussionsergebnisse im Plenum

Workshop Inhalte

Aufgabe: Bitte erarbeiten Sie (pro Gruppe) ein Konzept zur Qualitätssicherung von digitalen Zertifikaten. Verwenden Sie hierzu das Beispiel-Zertifikat „MyTestCert“ und die bereitgestellten Spezifikationsausschnitte. Das zu erstellende Konzept soll die Gebiete Anforderungsmanagement, Testrealisierung und Qualitätssicherung beinhalten.

- Unter Anforderungsmanagement wird die Identifizierung von Testinhalten und das Erstellen eines Anforderungskataloges verstanden.
  - Wie werden die Anforderungen identifiziert?
  - Welche Anforderungen gibt es?
- Testrealisierung bezieht sich auf die Umsetzung eines Tests, welcher die Erfüllung der Anforderungen sicherstellt.
  - Welche Parameter sind nötig?
  - Welche Ergebnisse sind gefordert?
- Unter Qualitätssicherung ist das Verifizieren, dass der erzeugte Test die entsprechende Anforderung prüft, zu verstehen.
  - Werden Beistellungen benötigt, wenn ja welche?
  - Wie sieht das Rückgabeergebnis aus?

Weiterhin soll das Konzept in der Lage sein Anforderungsänderungen, von kurzen Intervallen, zeiteffektiv umsetzen zu können (Spezifikationsanhebung).

Workshop Public-Key-Zertifikat

- MyTestCert
  - tbsCertificate
    - version = v3
      - serialnumber = 01 02 03 04 05 06 07 08…. octet string der Länge 20
    - signature = SHA256withRSA
    - issuer = TeleTrust CA
    - validity
      - notBefore = 01-10-2012
      - notAfter = 01-11-2020
    - subject
      - organizationName = TeleTrust (Bundesverband IT-Sicherheit e.V.)
    - subject public-key info
      - RSA
        - modulus = 01 02 … octet string der Länge 256
        - exponent = FF FF
    - extensions = not present
  - signatureAlgorithm = SHA256withRSA
  - signatureValue = valid

RFC 5280 Sec. 4.1.2.5

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

4.1.2.5. Validity

The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. The field is represented as a SEQUENCE of two dates: the date on which the certificate validity period begins (notBefore) and the date on which the certificate validity period ends (notAfter). Both notBefore and notAfter may be encoded as UTCTime or GeneralizedTime.

CAs conforming to this profile MUST always encode certificate validity dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime. Conforming applications MUST be able to process validity dates that are encoded in either UTCTime or GeneralizedTime.

The validity period for a certificate is the period of time from notBefore through notAfter, inclusive.

CAB Forum BR v1.6.3 Sec. 6.1.5

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

(3) Subscriber Certificates

	Validity period ending on or before 31 Dec 2013	Validity period ending after 31 Dec 2013
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA-512	SHA1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)	L= 2048, N= 224 or L= 2048, N= 256	L= 2048, N= 224 or L= 2048, N= 256

* SHA-1 MAY be used with RSA keys in accordance with the criteria defined in Section 7.1.3.
** A Root CA Certificate issued prior to 31 Dec. 2010 with an RSA key size less than 2048 bits MAY still serve as a trust anchor for Subscriber Certificates issued in accordance with these Requirements.

***L and N (the bit lengths of modulus p and divisor q, respectively) are described in the Digital Signature Standard, FIPS 186-4 (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf).

CAB Forum EV v7.1.3 Sec. 9.2.1

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

9.2.1. Subject Organization Name Field

Certificate field: *subject:organizationName* (OID 2.5.4.10)

Required/Optional: Required

Contents: This field MUST contain the Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein. A CA MAY abbreviate the organization prefixes or suffixes in the organization name, e.g., if the official record shows "Company Name Incorporated" the CA MAY include "Company Name, Inc."

When abbreviating a Subject's full legal name as allowed by this subsection, the CA MUST use abbreviations that are not misleading in the Jurisdiction of Incorporation or Registration.

In addition, an assumed name or DBA name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis.

If the combination of names or the organization name by itself exceeds 64 characters, the CA MAY abbreviate parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field does not exceed the 64-character limit; provided that the CA checks this field in accordance with section 11.12.1 and a Relying Party will not be misled into thinking that they are dealing with a different organization. In cases where this is not possible, the CA MUST NOT issue the EV Certificate.