Prüfung von Zertifikaten

- Ist das Zertifikat korrekt signiert?
  (ist die entschlüsselte Signatur im Zertifikat gleich dem Hash des Zertifikats?)
- Ist das Zertifikat noch gültig?
  (welche Gültigkeitsdauer ist im Zertifikat gespeichert?)
- Ist die Person / Web-Domain / … im Zertifikat die richtige?
  (oder wurde das Zertifikat z.B. für eine andere Domain ausgestellt?)
- Wurde das Zertifikat widerrufen?
  (Prüfung gegen lokal gespeicherte CRL und/oder online z.B. via OCSP)
- Ist das Zertifikat vertrauenswürdig?
  (ist die Kette der Zertifikate bis zu einer Root CA ok?)

Die deutsche „Qualifizierte Signatur“

- Ist gesetzlich für bestimmte Rechtsgeschäfte zugelassen bzw. gefordert
  und in diesen einer echten Unterschrift gleichgestellt.
- Darf nur von geprüften (inländischen) Stellen ausgestellt werden
  (u.a. damit die langjährige Verwahrung und Prüfbarkeit sichergestellt ist).
- Ist im Format X509v3 gespeichert.
- Enthält Regelungen für in der Signatur bzw. im Zertifikat gespeicherte Attribute
  (z.B. rechtlich abgesicherte Berufsstands-Angaben wie Notar, Rechtsanwalt, …)
  und deren Gültigkeit bzw. Widerruf getrennt von der Signatur an sich.
- Enthält Regelungen für signierte bzw. rechtsgültige Zeitstempel
  (z.B. Nachweis „Zertifikat X hat zum Zeitpunkt Y existiert“).
- Hat erhöhte technische Anforderungen:
  - Private Key muss auf einer Chipkarte gespeichert sein
  - Private Key darf die Karte nie verlassen
    ==› Hash der zu signierenden Daten wird auf die Karte geschickt
    und von bzw. auf dieser verschlüsselt
  - Verwendung der Karte muss zusätzlich geschützt sein
    (z.B. durch Pin-Eingabe auf zertifiziertem Lesegerät)
  - Bei der Prüfung von Signaturen muss eine Online-Widerrufs-Abfrage erfolgen
    (via OCSP oder via CRL-Download über LDAP),
    Prüfung nur gegen eine lokal gespeicherte CRL reicht nicht
  - … (weitere Anforderungen für Lesegerät, Software, …)