DuD
Datenschutz und Datensicherheit

Certification Practice Statement – CPS

Dirk Fox

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

Im Zusammenhang mit Public Key-Infrastrukturen (PKI) spielen sogenannte *Certification Practice Statements* (CPS) zunehmend eine wichtige Rolle.

Ein CPS ist eine Dokumentation der Arbeitsweise einer Zertifizierungsinstanz (CA) innerhalb einer PKI. Es beschreibt den konkreten Aufbau, die Abläufe, die technische Infrastruktur, die von der oder den CAs übernommenen Haftungsgarantien sowie die Umsetzung der Security Policy der CAs. Ein CPS dient mehreren Zwecken:

- Transparente Darstellung der Abläufe der Zertifizierungsdienstleistung,
- Beleg der Vertrauenswürdigkeit durch die Dokumentation des Aufbaus der Zertifizierungsstelle und der Umsetzung der Sicherheits-Policy,
- Zusammenfassung aller rechtlich relevanten Zusicherungen der Vertragsparteien,
- allgemeinverständliche Beschreibung der Verwendung ausgestellter Zertifikate.

Ein CPS ist häufig in Anlehnung an den „Lebenszyklus" einer CA strukturiert: von den Komponenten der Zertifizierungs-Infrastruktur bis zum Gültigkeitsablauf der ausgestellten Zertifikate. Es enthält üblicherweise Angaben zu den folgenden Themen:

- **Zertifizierungsinfrastruktur**
  - Aufbau (CAs, Registrierungsinstanzen, Zertifikatsverzeichnisse)
  - Arbeitsweise und Zusammenspiel der Instanzen
- **Zertifikatsspezifikation**
  - verwendete Signier- und Hashalgorithmen
  - Zertifikatsformate und Attributbelegung
  - Gültigkeitszeitraum
- **Zertifizierungsprozeß**
  - Antragstellung
  - Identitätsprüfung des Antragstellers
  - Generierung der Schlüssel
  - Publikation der Zertifikate
  - Aushändigung von Schlüsseln und Zertifikaten
  - Verlängerungszertifikate
  - Prozeß der Zertifikatssperrung (z.B. Ausgabe von Certificate Revocation Lists)
  - Auslauf von Zertifikaten
- **Sicherheit der CA (Security Policy)**
  - bauliche, technische und organisatorische Maßnahmen
  - Rollen und Kontrollen, eingesetztes Personal
  - Notfallkonzepte
  - Audit
- **Vereinbarungen und Zusicherungen**
  - Verpflichtungen des Antragstellers
  - Policy-Anforderungen an weitere CAs einer gemeinsamen Zertifizierungshierarchie
  - Haftung und Haftungsbegrenzung
  - Kosten für Antragsteller
- **Nutzung von Zertifikaten**
  - Bezugsmöglichkeit von Zertifikaten über Verzeichnisdienste
  - Prüfvorgang von Zertifikaten
  - Verwendung der zertifizierten Schlüssel

Ein sehr umfangreiches, in vieler Hinsicht vorbildliches (allerdings auf amerikanischem Recht fußendes) CPS findet sich bei Verisign Inc.[1]

Das Zertifikatsformat X.509v3 (1997) erlaubt es, als Standard-Extension im Zertifikat einen Verweis (z.B. eine Internet-URL) auf das im Zusammenhang mit diesem Zertifikat gültige CPS aufzunehmen. Ein solcher Hinweis gibt Empfängern des Zertifikats die Möglichkeit, die Zusicherungen zu prüfen, die die zuständige Zertifizierungsstelle für dieses Zertifikat übernimmt. Das CPS sollte bei elektronischer Bereitstellung digital signiert sein, damit die Integrität und Authentizität des Dokuments überprüft werden kann.

Ein CPS ist eine Selbstverpflichtungserklärung einer CA, die Kunden eine differenzierte Bewertung der angebotenen Zertifizierungsdienstleistung ermöglichen soll. Viele öffentliche Zertifizierungsstellen in den USA halten ein solches CPS für alle Kunden abrufbar bereit. Damit legen sie die Bewertung der Vertrauenswürdigkeit der Zertifizierungsdienstleistung in die Hände der Kunden.

Die American Bar Association hat eine Liste von Empfehlungen für die Erstellung eines CPS zusammengestellt, und einige amerikanische Bundesstaaten haben Beispiel-CPS-Dokumente herausgegeben.

Mit der Bindung der Betriebsgenehmigung einer öffentlichen Zertifizierungsstelle an das Vorliegen und die Umsetzung eines von unabhängigen Dritten regelmäßig überprüften Sicherheitskonzepts geht das deutsche Signaturgesetz einen anderen Weg: An die Stelle des Kundenurteils tritt eine vereinheitlichte (amtliche) Prüfung und Kontrolle.

[1] http://www.verisign.com/repository/CPS