

# Interoperabilität

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.*

Mit Interoperabilität wird die Eigenschaft unterschiedlicher (informations-) technischer Systeme oder Komponenten bezeichnet, im beabsichtigten Sinne miteinander zu funktionieren, d. h. insbesondere Daten austauschen zu können. Interoperabilität ist daher immer dann erforderlich, wenn ein technisches System eine Leistung nur im Zusammenspiel mit anderen Systemen oder Komponenten erbringen kann.

Im Bereich der Datensicherheit ist (informationstechnische) Interoperabilität eine zentrale Eigenschaft von Sicherheitslösungen für sogenannte „offene Systeme“. Unter einem offenen System wird eine technische Einrichtung verstanden, die von Komponenten unterschiedlicher Hersteller genutzt werden kann, und deren sämtliche Schnittstellen und technischen Daten offengelegt bzw. standardisiert sind (z. B. das Mobilfunknetz oder das Internet). Überwiegend handelt es sich bei offenen Systemen um Infrastruktureinrichtungen: So ist ein Verkehrsnetz ein offenes System, wenn der Zugang oder die Nutzung technisch nicht beschränkt ist (z. B. durch vereinheitlichte Straßenmindestbreite, Straßenbelag, maximale Kurvenkrümmung, minimale Brückenhöhe etc. für Normfahrzeuge unterschiedlicher Hersteller).

In der Informationstechnik sind vor allem für eine allgemeine Nutzung bereitgestellte Kommunikationssysteme (Kabelnetze, Funknetze, Satellitennetze, ISDN, Internet etc.) als offene Systeme ausgelegt. Für die in diesen Systemen einsetzbaren technischen Komponenten (Vermittlungsstellen, Sende- und Empfangseinrichtungen, Endgeräte etc.) gibt es eine große Zahl von Standards, die Schnittstellen, Protokolle oder auch physikalische Eigenschaften festlegen, wie den GSM-Mobilfunkstandard oder die IETF-Internet-Standards. Diese Spezifikationen stellen sicher, dass Systeme und Komponenten, die ihnen genügen, miteinander interoperabel sind.

IT-Sicherheitslösungen, bei denen die Interoperabilität eine entscheidende Eigenschaft darstellt, sind insbesondere Produkte,

die die Verschlüsselung (der Empfänger muß entschlüsseln können) von oder die Erzeugung digitaler Signaturen zu Kommunikationsdaten (der Empfänger muß die Signatur prüfen können) ermöglichen.

## Beispiel

Ein schönes Beispiel für die Komplexität, die Interoperabilitätsanforderungen an technische Komponenten annehmen können, ist die im Auftrag des BSI entwickelte Interoperabilitätsspezifikation nach Signaturgesetz (Sigl).<sup>62</sup> Dabei waren insbesondere die folgenden Teilaspekte zu spezifizieren:

- ◆ **Zertifikate:** Für die verwendeten Signaturschlüsselzertifikate mußten die Formate, die Kodierung, die unterstützten Attribute und deren Bedeutung festgelegt werden. Dabei waren unterschiedliche Schlüsselzwecke (Zertifizierung, Signatur, Zeitstempelung etc.) zu unterscheiden. Eine wichtige Rolle spielen auch die Namenskonventionen zur eindeutigen Bezeichnung des Schlüsselinhabers.
- ◆ **Signatur:** Für unterschiedliche Signatortypen waren nicht nur die kryptographischen Verfahren und Parameter, sondern auch die Austauschformate und die neben den Nutzdaten zu signierenden Zusatzinformationen und deren Kodierung zu spezifizieren.
- ◆ **Anwendungsschnittstelle:** Wichtig war auch die Festlegung der Benutzerschnittstelle der Anwenderkomponenten (Anzeige-Komponente, Verzeichnisauskünfte, Zeitstempelprüfung etc.).
- ◆ **Zeitstempel:** Um einen einheitlichen Zugriff auf Zeitstempeldienste zu ermöglichen, mußten Protokolle, Zeitstempelungsverfahren und Datenformate für diesen Pflichtdienst von Zertifizierungsstellen festgelegt werden.

- ◆ **Verzeichnisdienst:** Sowohl die Ablage der Zertifikate in allgemein zugänglichen Verzeichnissen als auch der Zugriff auf diese Verzeichnisse und die Formate der Abfrageprotokolle waren festzulegen.
- ◆ **Gültigkeitsmodell:** Wegen der erheblichen Auswirkungen auf weite Teile der Interoperabilitätsspezifikation mußte frühzeitig eine präzise Festlegung des Gültigkeitsverständnisses für digitale Signaturen erfolgen.<sup>63</sup> Daraus war ein geeigneter Prüfprozess abzuleiten.<sup>64</sup>
- ◆ **Anwenderinfrastruktur:** Die Kommunikation der Anwenderkomponente mit Komponenten der Zertifizierungsstelle z. B. für die Übertragung dezentral generierter öffentlicher Schlüssel zur Zertifizierung erfordert ebenfalls die Spezifikation von Schnittstellen und Abläufen.
- ◆ **Signierkomponente:** Die Schnittstelle zu Hard- und Software-PSEs<sup>65</sup> wie bspw. Smartcards erfordert eine Spezifikation des Datenaustauschs (Kommandoschnittstelle) und der Datenformate der PSE-Elemente.

## Selbstregulierung

Die Gestaltung von Interoperabilitätsspezifikationen unterliegt meist der Selbstregulierung durch Herstellerzusammenschlüsse oder internationale Standardisierungsgremien. Dies ist oft eine erhebliche Investition, allerdings gewinnen Hersteller, sofern es ihnen nicht gelingt, einen proprietären „de-facto-Standard“ zu etablieren, mit vereinheitlichten Systemen Investitionssicherheit. Häufig entsteht ein Markt auch erst nach Durchsetzung von Interoperabilitätsstandards, da inzwischen viele Kunden Investitionen in proprietäre Lösungen aus Angst vor Herstellerabhängigkeit und späterer möglicher Inkompatibilität scheuen.

<sup>63</sup> Zum Gültigkeitsmodell des Signaturgesetzes siehe Baum, DuD 4/1999, S. 199-205.

<sup>64</sup> Siehe Hammer, in diesem Heft.

<sup>65</sup> PSE: *Personal Security Environment*, dient der sicheren Aufbewahrung privater Schlüssel.

<sup>62</sup> Siehe auch unter

<http://www.bsi.de/aufgaben/projekte/pbdigsig/index.htm>