DuD
Datenschutz und Datensicherheit

Signatur-Profiles

Volker Hammer

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.

Profile dienen der Aufbereitung von Standards für die Praxis. Dementsprechend können Signatur-Profiles (üblich ist die englische Sprechweise) helfen, Signaturen einfacher oder besser zu implementieren und die praktische Nutzung zu fördern.

Standards sollen keine spezifische Lösung für ein einzelnes Problem bieten, sondern eine einheitliche Lösung für vielfältige gleichartige Probleme. Sie abstrahieren deshalb und werden in der Regel allgemein formuliert. Häufig findet man sogenannte „generische" Standards. Sie beschreiben, wie in einem bestimmten Kontext eine Lösung zu entwickeln ist, geben für die konkrete Problemstellung der Anwendung aber nur wenige Hinweise. Oft enthalten sie Anpassungs- und Erweiterungsmechanismen.

Ein bekanntes Beispiel für einen solchen Standard ist X.509, in dem ein generisches Zertifikats-Format definiert wird. Solche Vorgaben helfen für technische Realisierungen sehr viel weiter, weil sie u.a. das Problem strukturieren, grundsätzliche Entwurfsentscheidungen treffen und Kodierungsregeln festlegen. Oft sind sie aber so allgemein, dass sie viele Lösungsalternativen offen lassen. Für die Praxis sind dann noch viele Entwurfs- und Implementierungsentscheidungen zu treffen, z.B. in Profiles. Sie dienen z.B. dazu:

- durch Einschränkungen der Mächtigkeit eines Standards die Implementierung zu vereinfachen,
- Interpretationsmöglichkeiten zu begrenzen und den Standard zu präzisieren,
- anwendungsspezifische Anpassungen vorzunehmen
- die Interoperabilität zwischen verschiedenen Ausprägungen des Standards zu erhalten oder zwischen Produkten einer Klasse zur verbessern,
- Sicherheitsprobleme auszuschließen,
- Standards aus verschiedenen Bereichen miteinander abzustimmen.

Profiles definieren Untermengen oder Präzisierungen eines Standards. Sie halten sich aber innerhalb des Standards und schärfen quasi seinen Umriss. Durch den Einsatz von Profilen wird vermieden, dass verschiedene inkompatible Standards entstehen

Für den Einsatz von Profiles gibt es viele Beispiele:

- Abbildung 1 zeigt, wie der Ausgangsstandard X.509[1] über die „Kaskade" der Profile von PKIX[2] und ISIS-MTT[3] ein-

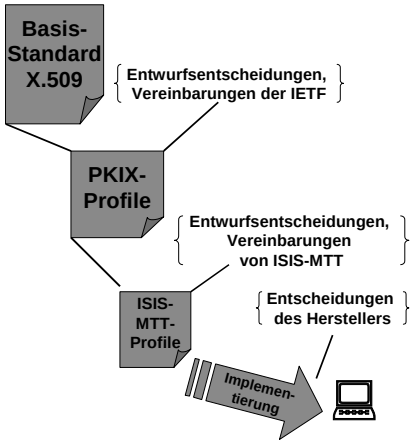

Abb. 1: Kaskade von Profiles

  geschränkt wird und schließlich in ein Produkt einfließt.
- Sogenannte *Protection Profiles* werden im Standard der Common Criteria eingeführt.[4] Mit ihnen werden die generischen Sicherheits- und Evaluierungsmaßnahmen auf konkrete Systeme übertragen.
- Innerhalb der Unified Modeling Language (UML) stellt ein Profil eine Anpassung der Modellierungssprache an spezifische Domänen oder Anwendungskontexte dar.[5] Es klärt für Modellelemente ihre anwendungsspezifische Semantik.

Der XML Signaturstandard des World Wide Web Konsortiums spezifiziert ein generisches Signaturformat, für entfernte und lokale Objekte, für einfache oder komplex strukturierte Objekte, für ganze Objekte oder Teile von ihnen, einschließlich verschlüsselter Teile.[6] Man kann auch mehrfache, parallele oder hierarchisch verschachtelte Signaturen erzeugen. Alle Kombinationen sind zulässig.

Diese Menge von Alternativen erlaubt für eine Problemstellung der Integritätssicherung vielfältige Lösungen. Um Eindeutigkeit für die Anwendungen zu erreichen, Lösungen zu vereinfachen und damit auch Sicherheitsprobleme zu vermeiden, könnten Profiles eingesetzt werden. Sie müssten einerseits den XML-Sprachumfang für Signaturen einschränken und parallel dazu die Erzeugung und Prüfung von Signaturen mit dem Processing der eigentlichen Anwendung abstimmen. Nur so kann beispielsweise sichergestellt werden, dass ein „Transform" geprüft und auch am Display angezeigt wird.

Sinnvoll sind möglicherweise anwendungsspezifische XML Signatur-Profiles. Bisher ist im XML-Umfeld der Begriff „Profil" aber noch nicht in diesem Sinne etabliert. Derzeit wird in der W3C Technical Architecture Group aber unter den Schlagworten „XML Profil" und „Subset" über die Notwendigkeit einer Untermengenbildung diskutiert,[7] wenn auch mit einer gewissen Skepsis wegen möglicher Einschränkungen für die Interoperabilität. zwischen den Anwendungsbereichen.

[1] International Telecommunication Union: X.509, 2000.
[2] RFC 3280, z. B. ftp://ietf.org/
[3] www.teletrust.de oder www.t7-isis.de
[4] Z.B. unter http://www.bsi.de/zertifiz/

[5] Für ausgewählte UML-Profile siehe z.B. www.jeckle.de/uml_spec.htm#profiles
[6] Grimm/Jeckle in diesem Heft.
[7] http://www.w3.org/2001/tag/ilist