

Sicherheitsmanagement durch generische, objektorientierte Modellierung einer TrustCenter Software

Markus Ruppert¹, Markus Tak¹

¹Technische Universität Darmstadt
Alexanderstr. 10, D-64283 Darmstadt
{mruppert, [tak](mailto:tak@cdc.informatik.tu-darmstadt.de)}@cdc.informatik.tu-darmstadt.de

Zusammenfassung

Sicherheitsmanagement erfordert festgeschriebene Regeln und deren konsequente Umsetzung. Festschreiben und Umsetzen sind üblicherweise voneinander getrennte Arbeitsschritte. Eine Synthese dieser Arbeitsschritte brächte viele Vorteile. Ein Ziel des Projekts FlexiPKI [BuRT00] ist es, die Flexibilität und Sicherheit von Softwarekomponenten durch die Integration von Policymechanismen in diesen Softwarekomponenten zu verbessern. Dieses generische Konzept ergibt bei der Kombination solcher Softwarekomponenten eine Policybeschreibung und sorgt zugleich für die Umsetzung dieser Policy.

In diesem Artikel wird ein Projekt zur generischen und objektorientierten Modellierung einer TrustCenter Software beschrieben, die prototypisch bereits implementiert wird. TrustCenter Software ist zentraler Bestandteil von Public Key Infrastrukturen (PKI). Die Notwendigkeit einer solchen Modellierung und dem daraus resultierenden Redesign existierender Prototypen ergab sich aus den sich permanent verändernden Anforderungen an PKI und den praktischen Erfahrungen im Testbetrieb der Zertifizierungsstelle der AG Buchmann (LiDIA-CA).

1 Sicherheit ist nicht statisch

Die gesamte Sicherheitsinfrastruktur ist in einem ständigen Wandel begriffen. Konzepte, Standards, Mechanismen und Implementierungen, letztlich auch die gesetzlichen Vorgaben zur Absicherung von Daten und Kommunikation sind davon betroffen. Die Bedürfnisse an Sicherheitsmechanismen entwickeln sich z.T. erst aus dem gerade beginnenden allgemeinen Gebrauch sicherheitsbasierter Anwendungen. So sehen die Richtlinien für sichere drahtlose Kommunikation, Wireless Transport Layer Security (WTLS) [WTLS00], bereits heute die Verwendung alternativer kryptographischer Basismechanismen auf Basis von Elliptischen Kurven vor (ECDH / ECDSA).

Im August 2000 hat das deutsche Signaturgesetz Anpassungen erfahren, und die Spezifikation neuer Standards wie Online Certificate Status Protocol (OCSP), Non-Repudiation (NR), TimeStamping-Service (TSS) und Certificate Management Protocol (CMP) lassen neue Anforderungen erkennen, die bei der grundlegenden Definition von PKI noch nicht vorhersehbar waren.

Sicherheit und damit jede Form von Sicherheitsmanagement beginnt mit der Ermittlung des Sicherheitsbedürfnisses und einer anschließenden Bedrohungsanalyse. Danach werden Regeln abgeleitet und Maßnahmen festgelegt, die genau beachtet und umgesetzt werden müssen, um die geforderte Systemsicherheit zu erhalten [Grun00, ITSEC]. Dies läßt sich sehr anschaulich am Beispiel eines TrustCenters darstellen.

Datenaustausch mit einem WebServer oder ein *Zertifikat für das Signieren von ausführbarem Programmcode*. Das Endprodukt der Zertifizierung muß nicht zwangsläufig auf das Zertifikat beschränkt sein, sondern kann auch ein Software- oder Hardware-Personal Security Environment (PSE) umfassen. Das Endprodukt bestimmt somit auch, wo und auf welche Weise Schlüsselpaare generiert werden.

Allen Zertifizierungsanträgen ist gemeinsam, daß sie eine Überprüfung der Antragsdaten erfordern. Diese **Datenprüfung** geschieht zweckmäßig in verschiedenen Prozessschritten. Der erste Schritt wird immer die Prüfung der Vollständigkeit der Daten sein. Im zweiten Schritt wird die Syntax der vorhandenen Daten geprüft. Daran schließt sich eine semantische Prüfung an, die eine Plausibilitätsprüfung beinhaltet. Es folgt die Überprüfung der Identität des Antragstellers und der Korrektheit seiner Angaben (Staatsangehörigkeit, Zugehörigkeit zu einer Organisation, Berechtigung, etc.)

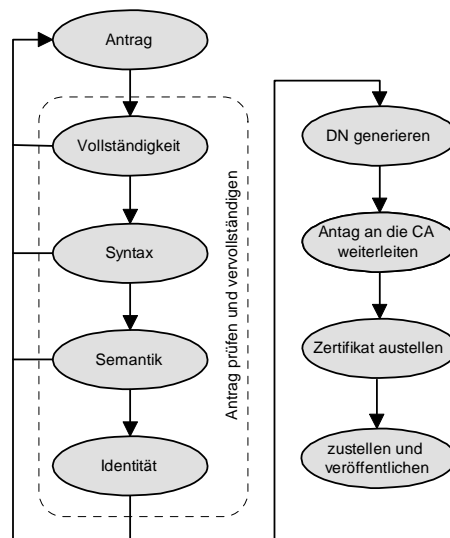


Abbildung 2: Zertifizierungsprozess

Die folgenden Zertifizierungsprozessschritte benötigen in der Regel keine weiteren Interaktionen mit dem Antragsteller. Aus den Antragsdaten muß ein eindeutiger Name (DN) für das Zertifikat generiert werden. Danach wird der Antrag von der RA unterzeichnet und an die CA übermittelt. In der CA wird die Korrektheit der Unterschrift geprüft und das Endprodukt der Zertifizierung erzeugt. Der letzte Prozessschritt beinhaltet die Zustellung des Produkts an den Antragsteller und die Archivierung und u.U. auch die Veröffentlichung des Zertifikats. Auch diese Verwaltungsprozesse sind wesentlicher Bestandteil des Sicherheits Managemets einer CA. Die Verfügbarkeit und Authentizität der Zertifikate und des Zertifikatsstatus sind Voraussetzung für eine funktionierende PKI.

Diese Prozeß-Sicht einer Zertifizierung läßt allerdings einige wichtige Aspekte außer Acht. Zum einen wird der Lebenszyklus eines Zertifikats durch weitere Vorgänge im und außerhalb des TrustCenters bestimmt, zum anderen wird die Reihenfolge und Art der Umsetzung der Abläufe in keiner Weise näher festgelegt. Diese Sichtweise trennt CP bzw. CPS vom Prozessverlauf. Um beide zu vereinen und auch bei Variation des Zertifizierungsprozesses konsistent zu halten, müssen Daten, Funktionen und Richtlinien in geeigneter Weise miteinander gekoppelt werden.

Wünschenswert wären Objekte, denen die Policyelemente inhärent sind. Objekte, die sich quasi selbst gegen Mißbrauch schützen bzw. sperren. Das „mündige Zertifizierungsobjekt“ sollte Ziel einer solchen Entwicklung sein, die sich auf beliebige Anwendungen ausweiten läßt.

3 Mündige Objekte

Betrachtet man die potentiell möglichen Prozeßverläufe und Attributkombinationen einer Zertifizierung (s. Abb. 3) und berücksichtigt dabei Zertifikatsinhalte, -bestimmung, verwendete Algorithmen und Schlüssel, sowie Verfahrensweisen die bei der Bearbeitung berücksichtigt werden müssen, dann wird die Zahl der Möglichkeiten schnell unübersichtlich und damit fehlerträchtig. Zum Teil bedingen Attributkombination und Prozessverlauf einander, zugleich haben beide wesentlichen Einfluss auf die Sicherheit der Zertifizierung und damit auf die Güte des Zertifikats.

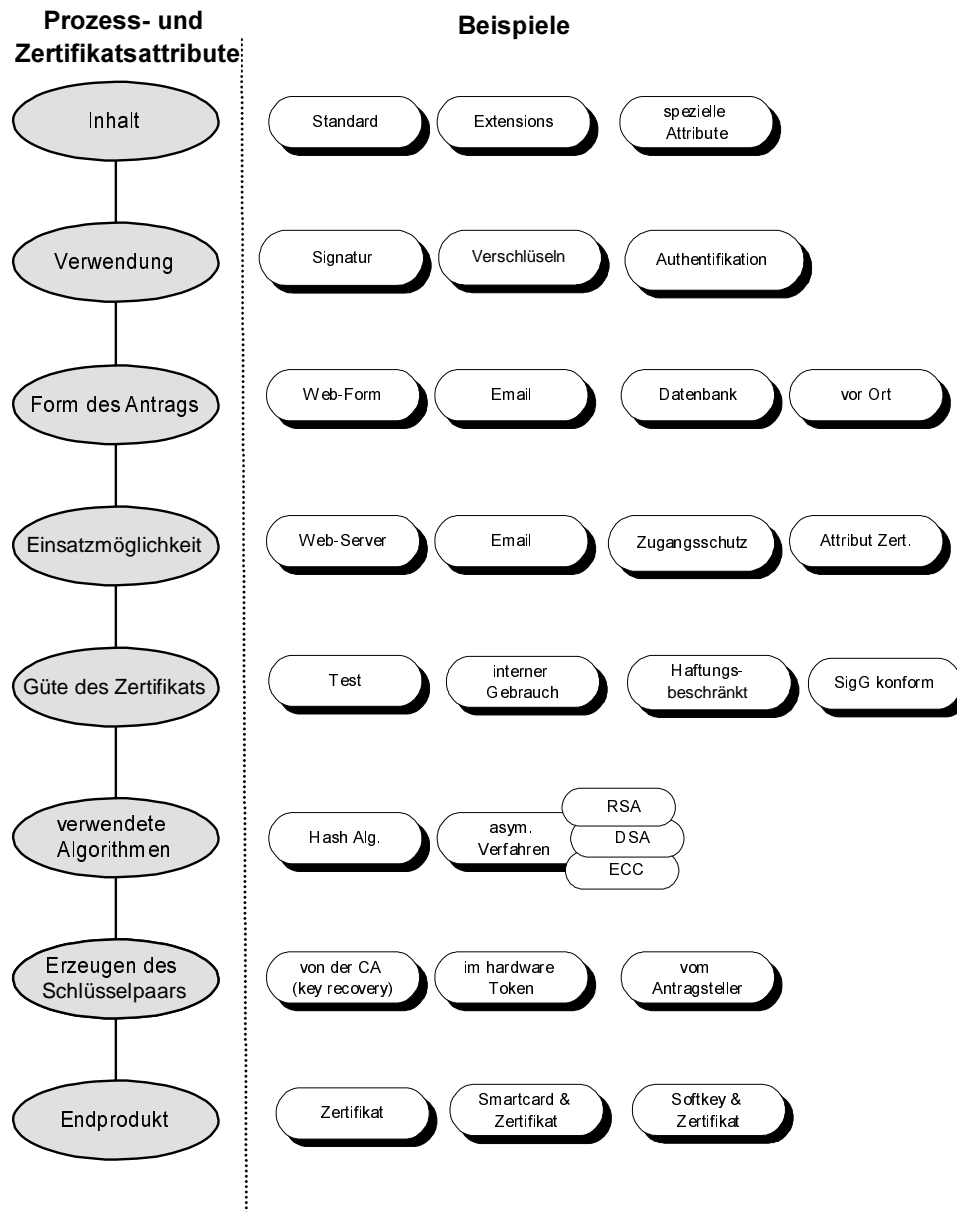


Abbildung 3: Variablen der Zertifikatsgestaltung und des Zertifizierungsprozesses

Ein Beispiel soll das verdeutlichen:

Inhalt: Standard, *Verwendung:* Signatur/Verschlüsselung, *Form des Antrags:* Email, *Erzeugung des Schlüsselpaars:* CA, *Signatur Algorithmus:* MD5withRSA, *Güte des Zertifikats:* interner Gebrauch, *Produkt:* Softkey (PKCS#12) & Zertifikat.

Für diese Kombination von Attributen, bei einer Abwicklung des TrustCenter internen Zertifizierungsprozesses mit entsprechend hohen Sicherheitsmerkmalen, müßte die Policy des Zertifikats den Gebrauch auf die Anwendungen in einer überschaubaren geschlossenen Benutzergruppe einschränken (Güte des Zertifikats: interner Gebrauch), denn die Form des Antrags: Email bietet keine ausreichende Identifizierungsmöglichkeit des Antragstellers für haftungsbeschränkte oder darüber hinaus gehende Zertifikatsverwendung. Für jede verwendete Kombination muß eine eigene Sicherheitsanalyse vorgenommen werden. Diese Bewertung erfolgt nach den in der CPS festgelegten Metriken und den Sicherheitspolicies des Anwenders. Diese Analyse erfordert einen hohen Aufwand.

Zwar läßt sich durch bewußtes Einschränken der Möglichkeiten und ein statisches Sicherheitsmanagement des TrustCenters ein hohes Maß an Sicherheit gewährleisten, aber die Brauchbarkeit der Zertifikate und die Anpassung an veränderte Sicherheitsanforderungen durch den technischen Wandel ist nicht mehr gegeben, TrustCenter dieser Kategorie sind mittelalterlichen Festungen vergleichbar, die sich einer veränderten Anforderungen nur schwer anpassen lassen. Besser ist es den gesamten Zertifizierungsvorgang einschließlich der damit verbundenen Zertifikats-, Schlüssel- und Chipkartenverwaltung in modularen Objekten zu bündeln.

Jede der Teilkomponenten, Attribute, Prozeßschritte und Policy werden durch eine Klassen- und Interface-Struktur in Objektkomponenten zusammengefaßt, die sich zu einem Zertifizierungsobjekt mit wohldefiniertem Prozessverlauf und wohldefinierter Produktgüte kombinieren lassen. Die Policy wird durch das Zertifizierungsobjekt selbst realisiert. Objekte, die kombiniert werden sollen, müssen dann sowohl funktional als auch sicherheitstechnisch zusammenpassen.

Die Policy Framework Working Group weist in dem Policy-Terminology-Draft [PFWG00] vom November 2000 mit Recht darauf hin, daß eine Transformation zwischen den unterschiedlichen Abstraktions- und Repräsentationsniveaus einer Policy in den meisten Fällen unscharf und unpräzise ist. Die in einem Policy-Repository definierten Regeln, Bedingungen und Aktionen können bei der Anwendung eine ungewollte Interpretation erfahren. Die Policy als aktives, sich selbst ausführendes Element entzieht sich einer solchen unscharfen Interpretation.

4 Ausblick

Ziel des Projekts ist es, ein Konzept systeminhärenter Policymechanismen zu entwickeln, das sich für IT Sicherheitsmanagement im objektorientierten Kontext einsetzen läßt, und eine unmittelbare Kopplung der Policymechanismen an die Prozesse und Applikationen gewährleistet.

Literatur

- [ABA195] American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Electronic Commerce, 1995.
- [BuRT00] J. Buchmann, M. Ruppert, M. Tak: FlexiPKI - Realisierung einer flexiblen Public-Key-Infrastruktur, Tagungsband der Konferenz Systemsicherheit:

Grundlagen, Konzepte, Realisierungen, Anwendungen, Vieweg Verlag,
ISBN 3-528-05745-9, 2000

- [CC2199] NIST, COMMON CRITERIA VERSION 2.1(aligned with IS 15408),
September 2000
- [Grun00] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzhandbuch,
Januar 2000
- [ITSEC] Information Technology Security Evaluation Criteria (ITSEC), 1991
- [PFWG00] IETF Policy Framework Working Group, Policy Terminology IETF-Draft-01,
November 2000
- [WTLS00] WAP-199-WTLS Wireless Application Protocol Wireless Transport Layer
Security Specification Version 18-Feb-2000, Wireless Application Forum,
Ltd. 2000