6 IT-Grundschutz

Einleitung

Im deutschsprachigen Raum spielt der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) eine wichtige Rolle. Ursprünglich wurden durch das BSI schwerpunktmäßig Vorschläge für Sicherheitsmaßnahmen und –konzepte für Ministerien und öffentliche Stellen entwickelt, inzwischen kann man den IT-Grundschutz durchaus auch als relevanten Standard für Unternehmen und andere Institutionen einordnen. Zum Einen bietet IT-Grundschutz eine Möglichkeit, sich effektiv und effizient mit den Hausaufgaben der IT-Sicherheit auseinanderzusetzen, zum Anderen existiert mit dem seit 2006 geschaffenen „ISO/IEC 27001-Zertifikat auf Basis von IT-Grundschutz“ die Möglichkeit, einen Nachweis über die Implementierung eines Informationssicherheits-Managementsystems und der Umsetzung von konkreten organisatorischen und technischen Sicherheitsmaßnahmen zu erbringen.

Aus der bereits 1995 veröffentlichen ersten Version des IT-Grundschutzhandbuches wurden in 2006 die sogenannten BSI-Standards und die IT-Grundschutz-Kataloge entwickelt. IT-Grundschutz hat damit eine Entwicklung weg von einer überwiegend technischen Sicherheitssicht hin zu einem auch das Sicherheitsmanagement umfassenden Ansatz vollzogen.

6.1 Historie

Die verantwortliche Stelle für den IT-Grundschutz ist das 1991 etablierte Bundesamt für Sicherheit in der Informationstechnik (BSI) mit Sitz in Bonn. Im Jahr darauf wurde 1992 das sogenannte Sicherheitshandbuch veröffentlicht, ein erstes deutsches Rahmenwerk, in welchem Informationen über IT-Sicherheit zusammen gestellt wurden. 1995 wurde die erste Version des IT-Grundschutzhandbuchs veröffentlicht, welches einen modularen Ansatz mit sogenannten Bausteinen verfolgt und über die Zeit kontinuierlich weiterentwickelt wurde. Die erste Version 1995 verfügte über 18 Bausteine, 200 Maßnahmen und 150 Seiten, 2004 waren es bereits 58 Bausteine, über 700 Maßnahmen und gut 2.500 Seiten. Der Umfang ergibt sich aus konkreten und detaillierten Beschreibungen von Maßnahmen, Gefährdungen und Bausteinen, schreckte aber doch den ein oder anderen bei der Anwendung von IT-Grundschutz ab. Um die Anwendung zu erleichtern und zu fördern wurde eine neue Struktur gewählt.

Seit 2006 existiert eine an die ISO/IEC 27001:2005 angepasste Version von IT-Grundschutz, die das Informationssicherheitsmanagement (ISM) stärker in den Vordergrund stellt. In diesem Zusammenhang wurde zusätzlich das Grundschutzhandbuch in die BSI-Standards und die IT-Grundschutz-Kataloge aufgeteilt. Die konkrete Anwendung der Grundschutz-Methodik ist durchaus lesenswert in den Standards 100-x beschrieben. Die umfangreichen IT-Grundschutzkataloge dokumentieren die Gefährdungen und Maßnahmen im Detail und dienen als Nachschlage- und Referenzwerk. Zur vereinfachten Navigation kann eine HTML-basierte Version verwendet werden, Volltextsuchen sind einfach in einer PDF-Version möglich und zur Weiterverwendung von Textbausteinen wird eine Word-Version zur Verfügung gestellt. Die jeweils aktuelle Version kann kostenfrei von der Website des BSI herunter geladen werden, ist aber auch als kostenpflichtige Loseblattsammlung verfügbar.

Unternehmen und Behörden konnten sich seit 2004 nach IT-Grundschutz zertifizieren lassen, indem die Erfüllung der Maßnahmen aus dem Grundschutzhandbuch nachgewiesen und auf der Grundlage eines definierten Audit-Schemas durch lizenzierte Auditoren überprüft wurde. Seit

der Überarbeitung des IT-Grundschutzes existiert das ISO 27001-Zertifikat auf Basis von IT-Grundschutz. Zur Erlangung dieses Zertifikats müssen immer noch alle relevanten Maßnahmen der IT-Grundschutz-Kataloge implementiert werden, zudem muss nachgewiesen werden, dass durch entsprechende Rollen und Prozesse auch ein angemessenes Informationssicherheitsmanagmentsystem (ISMS) aufgebaut und implementiert ist.

Der IT-Grundschutz wird kontinuierlich weiterentwickelt. Sowohl die Standards als auch die Kataloge werden fortgeschrieben, inhaltlich überarbeitet und durch neue Bausteine erweitert.

6.2 IT-Grundschutz Ansatz

Der IT-Grundschutz verfolgt einen ganzheitlichen Ansatz zur Implementierung von Informationssicherheit in Behörden und Unternehmen. Infrastrukturelle, organisatorische, personelle und technische Sicherheitsmaßnahmen unterstützen ein angemessenes Sicherheitsniveau zum Schutz von geschäftsrelevanten Informationen und der Verfügbarkeit der Daten. Auch wenn jedes Unternehmen über eine individuelle IT-Infrastruktur und individuelle Anwendungen verfügt, ist die Zielsetzung des IT-Grundschutzes, für allgemeine Prozesse des Information Security Management Systems (ISMS) und für Komponenten (z. B. Router, Switch, Firewall, Server, Clients) Standardsicherheitsmaßnahmen zu definieren.

Im Mittelpunkt der Betrachtungsweise von IT-Grundschutz steht der Informationsverbund. Bei einem Informationsverbund handelt es sich um die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten zur Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung der Organisation.

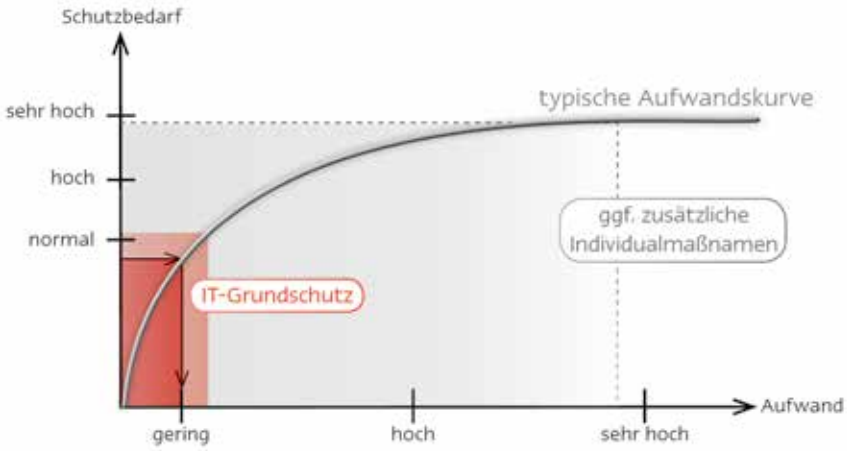
Für die konkrete Umsetzung von IT-Grundschutz ist eine klare Definition und Abgrenzung des zu betrachtenden Informationsverbunds notwendig. Im Falle einer geplanten Zertifizierung sollte die Definition im Vorfeld mit dem BSI abgestimmt werden, da an die Definition auch Anforderungen wie eine sinnvolle Mindestgröße gestellt werden. Für den definierten Informationsverbund sollen konkrete Sicherheitsmaßnahmen aus den IT-Grundschutz-Katalogen umgesetzt werden. Dabei ist eine Annahme des IT-Grundschutzes, dass typische Komponenten – z. B. Windows-Server, Unix-Server – zum Einsatz kommen. Zum Anderen ist gemäß der Vorgehensweise die Erfüllung der Grundschutzmaßnahmen für alle Systeme ausreichend, die keinem hohen oder sehr hohen Schutzbedarf aufweisen. Für alle Systeme bis zu einem normalen Schutzbedarf werden für den Grundschutzansatz pauschalierte Gefährdungslagen angenommen, die in den Gefährdungskatalogen für IT-Systeme und Anwendungen detailliert beschrieben sind. Eine umfassende Risikoanalyse muss nicht durchgeführt werden. Zum Schutz vor den Gefährdungen existieren durch das BSI vordefinierte Standard-Sicherheitsmaßnahmen, die in den entsprechenden Bausteinen katalogisiert sind. Das BSI hat hierdurch die Aufgabenstellung, ein Sicherheitskonzept für den Informationsverbund zu erstellen, erheblich vereinfacht. Lässt sich ein entsprechender Baustein finden, müssen die entsprechenden Maßnahmen umgesetzt werden um einem „normalen“ Schutzbedarf zu genügen. Für Systeme mit hohem oder sehr hohem Schutzbedarf bieten die Maßnahmen aber bereits eine gute Grundlage, um zusätzliche und individuelle Maßnahmen zum Schutz dieser Systeme zu identifizieren.

IT-Grundschutz ist aber deutlich mehr als das akribische Umsetzen von Sicherheitsmaßnahmen aus einem Katalog. Die Stärke von IT-Grundschutz liegt in dem Zusammenspiel von einem angemessenen Informationssicherheitsmanagement und der sorgfältigen Implementierung von Standard-Sicherheitsmaßnahmen und sinnvollen Ergänzungsmaßnahmen.

In Abhängigkeit von der Schutzbedarfsermittlung, die jedes Unternehmen und jede Behörde angepasst auf die eigenen Bedürfnisse durchführen muss, wird für IT-Systeme mit mindestens

„hohem“ Schutzbedarf oder für Systeme die nicht in den Bausteinen erfasst sind, eine ergänzende Sicherheitsanalyse notwendig.

Abbildung 6.1: Aufwand für IT-Grundschutz



Alles in allem ermöglicht IT-Grundschutz einen hohen Sicherheitsgewinn bei relativ niedrigem Aufwand – geschenkt bekommt man aber auch hier nichts. In der Summe sind die Aufwände zur vollständigen Umsetzung von IT-Grundschutz erheblich – „There is no free lunch!“.

6.3 IT-Grundschutz Dokumente

Die Dokumente zum IT-Grundschutz bestehen hauptsächlich aus den vier BSI-Standards (Stand Mai 2011) und den IT-Grundschutz-Katalogen, ergänzt um Hilfsmittel, Leitfäden und weitere Materialien. Seit der Umstrukturierung der Dokumente 2006 wird der Begriff IT-Grundschutzhandbuch offiziell nicht mehr verwendet. Die größten Teile des früheren Inhalts des IT-Grundschutzhandbuchs sind in den IT-Grundschutz-Katalogen zu finden, welche die Baustein-, Maßnahmen- und Gefährdungskataloge beinhalten.

Die BSI-Standards 100-x enthalten Informationen zum IT-Sicherheitsmanagement (100-1), Vorgehen nach IT-Grundschutz (100-2) und Risikoanalysen (100-3) sowie ergänzend auch zum Thema Notfallmanagement (100-4). Sie definieren den Rahmen für den IT-Grundschutz und beschreiben Methoden, Prozesse und Verfahren zur Gewährleistung von Informationssicherheit. Im Gegensatz zu den konkreten Maßnahmen der IT-Grundschutz-Kataloge beschreiben die Standards die allgemeinen Ansätze und Bedingungen für IT-Grundschutz.

Zusätzlich finden sich auf den Web-Seiten des BSI ergänzende Dokumente, Informationen und Werkzeuge zum Einsatz von IT-Grundschutz. Das GS-Tool und weitere Softwaretools zur Unterstützung der Planung und Umsetzung von IT-Grundschutz werden vom BSI und anderen Herstellern kommerziell oder teilweise auch als Open Source zur Verfügung gestellt. Eine Übersicht verfügbarer Tools ist auf den Web-Seiten des BSI dargestellt.

6.3.1 BSI-Standard 100-1: Managementsysteme für Informationssicherheit

Mit dem BSI-Standard 100-1 wird die Brücke zwischen dem IT-Grundschutz und anderen etablierten Standards für das Management von Informationssicherheit geschlagen. In diesem Standard werden die allgemeinen Anforderungen an ein Informationssicherheits-Managementsystem definiert. Der Standard ist kompatibel mit den Anforderungen aus dem Standard ISO/IEC 27001:2005 und bezieht sich auch auf die Empfehlungen aus dem Standard ISO/IEC 27002:2005. Im Gegensatz zu BSI-Standard 100-1 sind diese Standards kostenpflichtig und in hoher Qualität nur in englischer Sprache verfügbar.

Der BSI-Standard 100-1 wendet sich auch an das Management als Zielgruppe und bietet eine Einführung in den geordneten Umgang mit dem Thema Informationssicherheitsmanagement

ISMS Bestandteile

Im Rahmen von IT-Grundschutz wird mit „Informationssicherheitsmanagement“ der Prozess zur Steuerung der Informationssicherheit in Unternehmen und Behörden bezeichnet. Es muss beachtet werden, dass in diesem Zusammenhang von der „Leitungsebene“ gesprochen wird wenn die Führungskräfte gemeint sind.

Wichtige Bestandteile eines ISMS gemäß BSI sind:

- Management Prinzipien
- Ressourcen
- Mitarbeiter
- Ein definierter IT-Sicherheitsprozess mit den Bestandteilen
  - Sicherheitsleitlinie
  - Sicherheitskonzept
  - Sicherheitsorganisation

Durch diese Bestandteile wird das Informationssicherheitssystem nachvollziehbar definiert.

IT-Sicherheitsstrategie

In der IT-Sicherheitsstrategie muss festgelegt werden wie sich ein Unternehmen oder eine Behörde unter Berücksichtigung der eigenen Ziele und der Rahmenbedingungen ausrichtet. Das Bekenntnis der Leitungsebene zur IT-Sicherheitsstrategie wird in einer IT-Sicherheitsleitlinie dokumentiert.

Zur Umsetzung der IT-Sicherheitsstrategie wird eine IT-Sicherheitsorganisation aufgebaut und ein IT-Sicherheitskonzept erstellt.

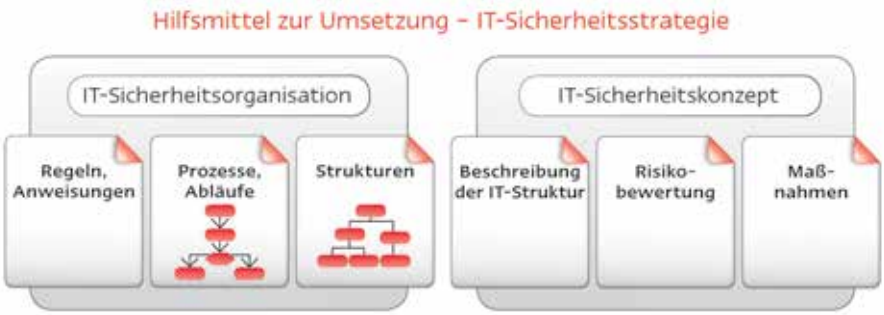
ISMS-Hilfsmittel

In der IT-Sicherheitsorganisation werden alle Regeln, Anweisungen, Prozesse, Abläufe und Strukturen mit Bezug zur Informationssicherheit abgebildet. Hier werden allgemeine Aspekte des Managements von Informationssicherheit behandelt.

---

1 Musterfolien für Schulungen zur Einführung in die Vorgehensweise nach IT-Grundschutz (Stand: 07.03.2011), *http://www.bsi.bund*

Abbildung 6.2: ISMS-Hilfsmittel nach IT-Grundschutz



Grafikvorlage: Bundesamt für Sicherheit in der Informationstechnik (BSI)[1]

In einem IT-Sicherheitskonzept werden in der Regel die IT-Struktur, Risikobewertungen und zugehörige Maßnahmen beschrieben.

PDCA-Modell

Beim Management von Informationssicherheit ist es wichtig, im Auge zu behalten, dass es sich nicht um ein Projekt im eigentlichen Sinne mit Projektbeginn und vor allem ein Projektende handelt, sondern, dass ein dauerhafter Prozess zur Aufrechterhaltung eines angestrebten Sicherheitsniveaus geschaffen werden muss. Häufig kann man in der Praxis zwar beobachten, dass die Etablierung von Informationssicherheit als Projekt startet. Die Ausrichtung auf ein ISMS als Prozess sollte aber von Anfang an im Fokus stehen.

Aufgrund der Ausrichtung am Standard ISO/IEC 27001:2005 spielt bei ISO 27001 auf Basis von IT-Grundschutz der frühere PDCA-Zyklus[2] eine wichtige Rolle.

Der Plan-Do-Check-Act-Ansatz mit den vier Phasen

- Planung und Konzeption (Plan),
- Umsetzung (Do),
- Überwachung und Erfolgskontrolle (Check) und
- Optimierung und Verbesserung (Act)

bildet die Grundlage für Informationssicherheitsmanagement als Prozess.

Durch diesen Ansatz wird sichergestellt, dass die Sicherheit fortlaufend an die jeweiligen Anforderungen angepasst wird und dadurch ein iterativer Verbesserungsprozess etabliert wird.

Ursprünglich lag der Schwerpunkt von IT-Grundschutz auf der reinen IT-Sicherheit. Das BSI erweiterte inzwischen allerdings das Blickfeld von IT-Grundschutz auf die Betrachtung von Informationssicherheit im allgemeinen Sinn. Hierbei spielt eine große Rolle, dass aktuell wichtige Informationen zu großen Teil als Daten in IT-Systemen gespeichert sind und verarbeitet werden.

2 Siehe Abschnitt 5.3.1

Grundschutz als ISMS des BSI

In der Praxis stellt sich für Sicherheitsverantwortliche häufig die Frage, wie Informationssicherheit im konkreten Fall umgesetzt werden kann. Die gängigen Standards zum Informationssicherheitsmanagement geben Verantwortlichen bei der Umsetzung viel Freiheit. Allerdings haben diese Freiheitsgrade den Nachteil, dass für den Aufbau eines Sicherheitsmanagementsystems viel Erfahrung und Know-how notwendig sind. Konkrete Handreichungen fehlen an vielen Stellen.

An dieser Stelle setzt das BSI an und stellt mit dem IT-Grundschutz einen Ansatz zur Verfügung, der zum Einen in den Standards die organisatorischen Anforderungen an ein ISMS beschreibt, zum Anderen aber auch in den IT-Grundschutz-Katalogen konkrete Hilfestellungen für technische und organisatorische Maßnahmen zur Umsetzung von Informationssicherheit bietet.

Ein kritischer Bereich bei der Etablierung von Informationssicherheit ist die an vielen Stellen geforderte Risikoanalyse, auf die dann aber in der Regel nicht weiter eingegangen wird. Effektive und effiziente Risikoanalysen sind aber häufig nur mit entsprechender Erfahrung durchzuführen und ressourcenaufwändig. Risikoanalysen stoßen häufig auf zwei große Hürden: Zum Einen müssen sie hohe Komplexität sowohl bei Geschäftsprozessen als auch in der IT-Landschaft bewältigen – allzuleicht verliert man sich in vielen Details. Zum Anderen dauern sie oft recht lange, dadurch kann sich die Ausgangslage bis zur Fertigstellung des Berichts bereits erheblich verändert haben.

Diesem Problem begegnet das BSI durch den Ansatz der Bereitstellung einer impliziten Risikoanalyse für die durch den IT-Grundschutz abgedeckten Standardszenarien. Im Grundschutz wird davon ausgegangen, dass für vergleichbare Systemlandschaften mit normalem Schutzbedarf ähnliche Bedrohungen existieren. Diese Bedrohungen wurden ausgiebig analysiert und bilden die implizite Risikoanalyse[3] als Grundlage für die im IT-Grundschutz ausgearbeiteten Sicherheitsmaßnahmen.

Daher müssen im IT-Grundschutz ergänzende Sicherheitsanalysen auch nur bei Vorliegen von hohem oder sehr hohem Schutzbedarf oder in einer Systemlandschaft, die nicht aus Standard IT-Systemen besteht, durchgeführt werden.

6.3.2 BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise

Bei dem BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise handelt es sich um das zentrale Werk des IT-Grundschutzes, da hier die wesentlichen Bestandteile der verbindlichen Vorgehensweise nach IT-Grundschutz festgeschrieben sind.

Bestandteile des Sicherheitsprozesses

Es ist wichtig, einen IT-Sicherheitsprozess zu etablieren. Falls dieser noch nicht existiert, muss er initiiert werden. Dazu muss eine Sicherheitsleitlinie erstellt und verabschiedet werden. Außerdem muss die Leitungsebene, d. h. die Geschäftsführung, Amtsleitung oder der Vorstand ein Sicherheitsmanagement einrichten. Hierzu müssen Rollen definiert und Ressourcen zur Verfügung gestellt werden.

Nach der Erstellung einer IT-Sicherheitskonzeption folgt eine Umsetzungsphase, in der fehlende oder nur teilweise umgesetzte IT-Sicherheitsmaßnahmen realisiert werden. Maßnahmen zur

3 Dokumentiert in den Gefährdungskatalogen der IT-Grundschutz-Kataloge.

Sensibilisierung für IT-Sicherheit und zielgruppenspezifische Schulungen sollten ebenfalls durchgeführt werden, um die Akzeptanz und Wirksamkeit von Sicherheitsmaßnahmen zu steigern.

Letztendlich muss die IT-Sicherheit im laufenden Betrieb kontinuierlich überwacht und aufrechterhalten werden.

Erstellung einer Sicherheitskonzeption

Abbildung 6.3 zeigt, wie eine IT-Sicherheitskonzeption nach IT-Grundschutz erstellt werden soll. Die einzelnen Schritte werden im weiteren Verlauf des Kapitels erläutert.

Am Anfang der Erstellung steht die Definition eines zu betrachtenden Informationsverbunds, welcher aus allen relevanten Anwendungen, Systemen, Netzen, Räumen, Gebäuden und Infrastruktureinrichtungen besteht. Für diesen Informationsverbund werden in der Strukturanalyse alle relevanten Informationen erfasst, es wird also eine Bestandsaufnahme durchgeführt. Zur Vereinfachung kann eine Reduktion der Komplexität durch Gruppenbildung gleichartiger Bestandteile erfolgen, beispielsweise gleichartige Systeme vereinfacht als ein System dargestellt werden. Als Ergebnis der Strukturanalyse soll ein bereinigter Netzplan vorliegen, der möglichst genau den Ist-Zustand des betrachteten Informationsverbunds beschreibt und einen guten Überblick der beteiligten Komponenten liefert.

Verantwortung der Leitungsebene

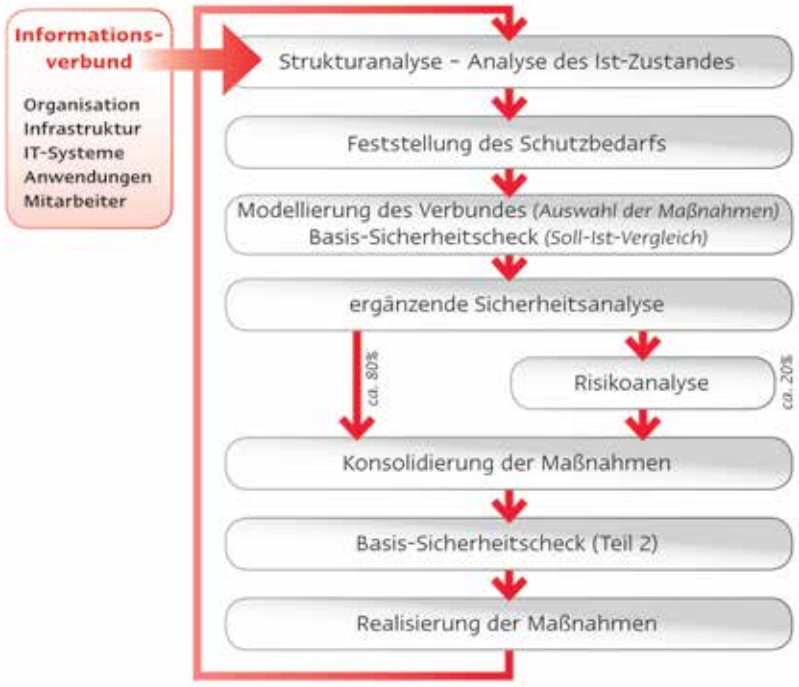
Aus der Gesamtverantwortung der Leitungsebene für ein Unternehmen oder eine Behörde leitet sich insbesondere auch die spezielle Verantwortung für die Informationssicherheit – in der Regel zum Schutz des Unternehmenswissens – ab. Die Umsetzung der Informationssicherheit kann delegiert werden. Allerdings verbleibt die Verantwortung für die Initiierung und insbesondere die Kontrolle der Umsetzung der Informationssicherheit bei der Leitungsebene.

Eine wichtige Verantwortung der Leitungsebene ist die Etablierung eines kontinuierlichen Sicherheitsprozesses, der den Anforderungen der Organisation Rechnung trägt. Hierzu müssen die Rahmenbedingungen gründlich analysiert werden und daraus abgeleitete Sicherheitsziele formuliert werden. In einer Sicherheitsleitlinie, oft auch als Sicherheits-Policy bezeichnet, sollen die Hauptziele knapp formuliert werden. Sie sollte mindestens die folgenden Punkte beinhalten:

- Stellenwert der IT-Sicherheit und Bedeutung der IT für die Aufgabenerfüllung
- Bezug der IT-Sicherheitsziele zu den Geschäftszielen oder Aufgaben der Institution
- Sicherheitsziele und die Kernelemente der Sicherheitsstrategie für die eingesetzte IT
- Zusicherung, dass die IT-Sicherheitsleitlinie von der Institutionsleitung durchgesetzt wird
- Leitaussagen zur Erfolgskontrolle
- eine Beschreibung der für die Umsetzung des IT-Sicherheitsprozesses etablierten Organisationsstruktur.

Der Aufbau einer angemessenen IT-Sicherheitsorganisation obliegt nach IT-Grundschutz ebenfalls der Leitungsebene. Hierzu müssen entsprechende Rollen, Aufgaben, Verantwortungen und Kompetenzen festgelegt werden. Allerdings verbleibt die Gesamtverantwortung bei der Leitungsebene. Es ist nicht erfolgversprechend, nur einen IT-Sicherheitsbeauftragten zu benennen. Ohne, dass außerdem angemessene Ressourcen bereitgestellt werden, kann Informationssicherheit nicht erfolgreich umgesetzt werden.

Abbildung 6.3: Erstellung einer IT-Sicherheitskonzeption nach BSI-Grundschutz



Grafikvorlage: Bundesamt für Sicherheit in der Informationstechnik (BSI)

IT-Strukturanalyse

Im Vordergrund der Betrachtungen steht beim IT-Grundschutz immer ein Informationsverbund. In der IT-Strukturanalyse werden alle für den Verbund wichtigen Informationen erfasst. Hierbei empfiehlt es sich in der Praxis, ausgehend von wichtigen Geschäftsprozessen die wichtigen Anwendungen und Informationen herauszuarbeiten und daraus die für diese erforderlichen Systeme abzuleiten. Folgende Schritte werden bei der Strukturanalyse durchgeführt:

- Erfassung der IT-Anwendungen und zugehörigen Informationen
- Erhebung der IT-Systeme
- Erhebung der Kommunikationsverbindungen
- Erfassung der IT-Räume
- Komplexitätsreduktion durch Gruppenbildung
- Erstellung eines reduzierten Netzplans und Auflistungen von Anwendungen, Systemen, Räumen und Kommunikationsverbindungen

Schutzbedarfsfeststellung

Vor der Definition von IT-Sicherheitsmaßnahmen muss der Schutzbedarf der IT-Komponenten festgelegt werden. Hierdurch wird den in der Regel beschränkten Ressourcen Rechnung getragen, so dass festgestellt werden kann welche Daten und Ressourcen besonders schützenswert sind.

Diese Festlegung muss individuell für jede Organisation unter Berücksichtigung der eigenen Bedürfnisse erfolgen, beispielsweise wird ein möglicher finanzieller Schaden von 100.000 Euro von einem mittelständischen Unternehmen anders bewertet werden als von einem Konzern. Die Methodik zur Festlegung des Schutzbedarfs soll nachvollziehbar sein.

Vorgegeben ist durch IT-Grundschutz, dass eine Komponente in eine der drei Schutzbedarfskategorien *normal, hoch* oder *sehr hoch* eingeordnet werden muss. Die beiden letzten Kategorien werden hier unter *erhöhtem Schutzbedarf* zusammengefasst. In älteren Versionen des Grundschutzhandbuches wurde noch die Kategorien „niedrig“ und „mittel“ unterschieden, diese wurden zur Stufe „normal“ zusammen gefasst.

Bei der Festlegung des Schutzbedarfs ist es sinnvoll, verschiedene Schadensarten zu betrachten, z. B. finanzieller Schaden, Haftungsschäden, Rufschäden, und diese nach Schadenshöhen in Schadensklassen einzuteilen. Diese werden je nach Organisation spezifisch festgelegt und durch die Unternehmensleitung verbindlich verabschiedet. Die Vorgaben für die Schutzbedarfsklassen sind im BSI-Standard 100-2 wie in Tabelle 6.1 charakterisiert

In der Praxis gestaltet sich die Schutzbedarfsfeststellung häufig als schwieriger als zunächst angenommen, da verschiedene Beteiligte durchaus unterschiedliche Sichtweisen auf den Schutzbedarf einzelner Komponenten haben können. Mag für einen Abteilungsleiter eine Arbeitsunterbrechung von einer Woche ernorme Ausmaße annehmen, kann es durchaus sein, dass unternehmensweit ein derartiges Problem nur eine untergeordnete Rolle einnimmt. Es ist daher wichtig, die Kategorien für das Gesamtunternehmen zu definieren und erst dann eine Schutzbedarfseinstufung durch den jeweiligen Verantwortlichen vornehmen zu lassen.

Tabelle 6.1: Charakterisierung der Schutzbedarfskategorien nach [BSI 1002]

Kategorie	Relative Schadenhöhe
normal	Die Schadensauswirkungen sind begrenzt und überschaubar
hoch	Die Schadensauswirkungen können beträchtlich sein
sehr hoch	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen

Der IT-Grundschutz-Ansatz ist ausgelegt für IT-Landschaften mit hauptsächlich normalem Schutzbedarf. Für Komponenten mit hohem oder sehr hohem Schutzbedarf ist eine ergänzende detaillierte Sicherheitsanalyse durchzuführen.

Im Weiteren wird beschrieben, wie der Schutzbedarf ermittelt wird.

Schutzbedarf IT-Anwendungen: Informationen werden durch IT-Anwendungen verarbeitet. Daher stehen diese auch am Anfang einer Schutzbedarfsanalyse. Für alle IT-Anwendungen muss der Schutzbedarf im Hinblick auf die Kernziele der IT-Sicherheit *Vertraulichkeit, Integrität* und *Verfügbarkeit* im Hinblick auf die verarbeiteten Informationen festgelegt werden. Dabei sind die vorher für die Organisation festgeschriebenen Kriterien für eine Klassifizierung anzuwenden. Der BSI-Standard 100-2 liefert konkrete Hilfestellungen für die Zuordnung durch Leitfragen zu den Kriterien

- Verstoß gegen Gesetze/Vorschriften/Verträge,
- Beeinträchtigungen des informationellen Selbstbestimmungsrechts,
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,

- Negative Innen- und Außenwirkung und
- Finanzielle Auswirkungen.

Der Schutzbedarf der Anwendung leitet sich aus den Schutzbedarfsfeststellungen für die Einzelkriterien ab.

Schutzbedarf IT-Systeme: Aus dem Schutzbedarf der IT-Anwendungen lässt sich der Schutzbedarf von IT-Systemen ermitteln. Hierbei wird in der Regel das sogenannte *Maximumsprinzip* angewendet, bei dem die möglichen Schäden aller betriebenen Anwendungen auf einem IT-System betrachtet werden. Die Anwendung mit dem höchsten Schutzbedarf bestimmt den Schutzbedarf eines IT-Systems. Für ein an sich weniger kritisches System kann allerdings ein erhöhter Schutzbedarf notwendig werden, wenn kritische Anwendungen auf Informationen aus diesem System angewiesen sind.

Wenn mehrere an sich nur „normale" IT-Anwendungen auf einem System verarbeitet werden, so kann es nach dem *Kumulationsprinzip* notwendig werden, einem System einen erhöhten Schutzbedarf zuzuordnen, da bei einem Systemausfall all diese Anwendungen gestört würden.

Dem gegenüber kann einem IT-System ein niedrigerer Schutzbedarf zugeordnet werden, wenn auf ihm nur Teile einer IT-Anwendung mit erhöhtem Schutzbedarf verarbeitet werden, beispielsweise einem einzelnen Server im Clusterbetrieb. Man spricht dann vom *Verteilungseffekt*. Der Schutzbedarf des Clusters kann durchaus hoch sein, der Schutzbedarf eines einzelnen Servers aber nur normal.

Schutzbedarf Kommunikationsverbindungen: Für die Feststellung des Schutzbedarfs von Kommunikationsverbindungen müssen kritische Kommunikationswege identifiziert werden. Hierbei müssen nach IT-Grundschutz die folgenden Verbindungstypen betrachtet werden:

- Außenverbindungen
- Verbindungen mit sensiblen Daten
- Verbindungen über die sensible Daten nicht übertragen werden dürfen

Schutzbedarf Räume: Der Schutzbedarf von Räumen leitet sich aus dem Schutzbedarf der in diesem Raum befindlichen IT-Systeme ab. Bei der Festlegung ist das Maximumsprinzip anzuwenden.

Gesamtschutzbedarf

Die einzelnen Schtuzbedarfsfeststellungen müssen zu einem Gesamtschutzbedarf zusammengefasst werden. Es gelten folgende Regeln:

- Maximumsprinzip: Die schwerwiegendste Auswirkung bestimmt Schutzbedarf
- Kumulationseffekt: Durch Kumulation mehrerer Schäden erhöht sich Schutzbedarf
- Verteilungseffekt: Eine IT-Anwendung mit hohem Schutzbedarf überträgt den Schutzbedarf nicht auf ein System, falls auf diesem nur Teile der Anwendung laufen, eine redundante Systemauslegung führt zu einem niedrigeren Schutzbedarf der Einzelsysteme.

Auswahl und Anpassung von Maßnahmen

Durch die IT-Grundschutzanalyse sollen die für einen Informationsverbund notwendigen Sicherheitsmaßnahmen ermittelt und deren Umsetzungsstatus überprüft werden.

Modellierung

Durch die Grundschutzmodellierung als erstem Schritt der IT-Grundschutzanalyse werden die für einen Bereich des Informationsverbunds notwendigen Sicherheitsmaßnahmen ermittelt. Der betrachtete Informationsverbund wird mit Hilfe der Bausteine aus den IT-Grundschutz-Katalogen

(siehe unten) nach festen Regeln nachgebildet. Hierbei werden verschiedene IT-Sicherheitsaspekte nach den in den IT-Grundschutz-Katalogen vorgegebenen Schichten betrachtet und Maßnahmen zugeordnet. Optional kann auch eine individuelle Gefährdungslage berücksichtigt werden.

In der Praxis ist die Modellierung ein kritischer Vorgang beim Einsatz von IT-Grundschutz. Eine korrekte Modellierung erfordert einige Erfahrung. Die Modellierungsvorschriften des BSI müssen sorgfältig befolgt werden.

Für ein betrachtetes System können durchaus mehrere Bausteine zur Anwendung kommen. So können z. B. für einen Datenbankserver mindestens die Bausteine *3.101 Allgemeiner Server* und *3.108 Windows Server 2003* anzuwenden sein. Der Baustein *5.7 Datenbanken* käme nicht zur Anwendung, dieser wäre einem Objekt der Schicht 5, in der Regel einer Datenbank(anwendung) zuzuordnen.

Als Ergebnis der Modellierung liegt ein IT-Grundschutzmodell des betrachteten Informationsverbunds vor. Dieses enthält alle nach IT-Grundschutz geforderten Standardmaßnahmen.

Basis-Sicherheitscheck

Bei dem Basis-Sicherheitscheck handelt es sich um einen Soll-Ist-Vergleich durch den der Umsetzungsgrad von Sicherheitsmaßnahmen abgeprüft wird. Sicherheitsmaßnahmen können einen der folgenden Umsetzungsstatus haben: *Ja, Nein, teilweise, entbehrlich*. *Entbehrlich* bedeutet in diesem Zusammenhang, dass höherwertige Maßnahmen greifen oder in Ausnahmen die Maßnahmenempfehlungen nicht relevant sind. Es bedeutet nicht, dass die Maßnahme nicht betrachtet werden soll!

In einem konkreten Beispiel könnte eine lokale unterbrechungsfreie Stromversorgung (USV) bei einzelnen Servern auf entbehrlich gesetzt werden, wenn eine zentrale USV vorhanden ist. Auf entbehrlich darf eine Maßnahme aber insbesondere nicht gesetzt werden, falls lediglich die Aufwände zur Umsetzung nicht getragen werden sollen.

Der Basis-Sicherheitscheck muss in der Praxis gut vorbereitet sein und wird in der Regel in Form von Fachinterviews mit den zuständigen Ansprechpartnern durchgeführt. Es schadet nicht, sich auch an entsprechenden Stellen durch Stichproben oder Sichtkontrollen von der Richtigkeit von Angaben zu überzeugen, sei es durch den Nachweis von Aussagen in Form von Textpassagen in Dokumenten oder konkreten Prüfung von Konfigurationsdetails an Systemen.

Ergänzende Sicherheitsanalyse

Für einige Objekte eines Informationsverbunds kann IT-Grundschutz nicht unmittelbar oder nicht ausschließlich angewandt werden. Dies betrifft Objekte, die einen erhöhten Schutzbedarf aufweisen, für die keine Bausteinen in den IT-Grundschutz-Katalogen existieren oder die in anderen als im IT-Grundschutz betrachteten Einsatzszenarien betrieben werden sollen. Für diese Objekte muss eine ergänzende Sicherheitsanalyse durchgeführt werden. Hierbei empfiehlt das BSI die folgende Vorgehensweise:

- Erstellung einer Gefährdungsübersicht
- Ermittlung zusätzlicher Gefährdungen
- Gefährdungsbewertung
- Maßnahmenauswahl zur Behandlung von Risiken
- Konsolidierung des IT-Sicherheitskonzepts

Bei der ergänzenden Sicherheitsanalyse ist die Risikoanalyse nach BSI-Standard 100-3 zu beachten.

Realisierungsplanung

In der Realisierungsplanung werden die nach dem Soll-Ist-Vergleich noch fehlenden oder nur teilweise umgesetzten Sicherheitsmaßnahmen zusammengefasst und konsolidiert. Dabei sollten die folgenden Aspekte geprüft und festgelegt werden:

- Kosten- und Aufwandsschätzung
- Umsetzungsreihenfolge
- Verantwortlichkeiten
- Definition von Schulung und Awareness-Maßnahmen

Letztendlich müssen die Realisierungsplanung und das erforderliche Budget durch die Leitungsebene verabschiedet und dann durch die IT-Sicherheitsorganisation umgesetzt werden.

6.3.3 BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz

Im BSI-Standard 100-3 wird die Einbindung von Risikoanalysen in die IT-Grundschutz-Vorgehensweise beschrieben.

In Fällen in denen ein hoher oder sehr hoher Schutzbedarf vorliegt, Systeme oder Anwendungen nicht durch die IT-Grundschutz-Kataloge abgedeckt sind oder Einsatzszenarien über den IT-Grundschutz hinausgehen muss nach IT-Grundschutz eine Analyse von IT-Risiken durchgeführt werden. In der Praxis ist dieses Vorgehen auch erforderlich, wenn im Rahmen von IT-Grundschutz Spezialumgebungen wie z. B. Leittechniksysteme oder Medizintechnik betrachtet werden. Im Standard wird eine Vorgehensweise beschrieben, durch die der Aufwand für die Durchführung der Risikoanalysen gering gehalten werden.

Als Ausgangspunkt für die Risikoanalyse bieten sich die Gefährdungskataloge aus den IT-Grundschutz-Katalogen an. Der Standard beschreibt eine Vorgehensweise zur Erstellung einer Gefährdungsübersicht unter Nutzung der Gefährdungskataloge. Zusätzliche Gefährdungen, die nicht in den IT-Grundschutz-Katalogen aufgeführt werden, müssen durch sorgfältige Betrachtung der jeweiligen Situation ergänzt werden. Hierbei können Dokumentationen und Veröffentlichungen von Schwachstellen hinzugezogen werden, z. B. aus Mailing-Listen, Schwachstellendatenbanken oder über spezialisierte Dienstleister. Eigene Bedrohungsanalysen müssen die Risikoanalyse abrunden.

Aus der Gefährdungsübersicht müssen die notwendigen ergänzenden Maßnahmen für die IT-Sicherheitskonzeption abgeleitet werden. Danach muss für alle Objekte, für die die IT-Grundschutz-Maßnahmen nicht ausreichen, entschieden werden, welche der folgenden Risikobehandlungsmethoden angewendet wird:

- Risikoreduktion durch zusätzliche Maßnahmen
- Risikoreduktion durch Umstrukturierung
- Risikoübernahme oder Risikoakzeptanz
- Risikotransfer

Abschließend müssen das IT-Sicherheitskonzept unter Berücksichtigung der Risikobehandlung konsolidiert werden und die Ergebnisse in den Sicherheitsprozess zurückfließen.

6.3.4 BSI-Standard 100-4: Notfallmanagement

Der BSI-Standard 100-4 zum Thema Notfallmanagement ergänzt die ersten drei BSI-Standards um eine Vorgehensweise, die für Unternehmen und Behörden einen Weg im Sinne des IT-Grundschutzes aufzuzeigt, auf den Umgang mit Krisen und Notfällen vorbereitet zu sein.[4]

6.3.5 IT-Grundschutz-Kataloge

Bei den IT-Grundschutz-Katalogen handelt es sich um den größten Teil dessen, was vor 2006 als IT-Grundschutzhandbuch bezeichnet wurde. Die IT-Grundschutz-Kataloge enthalten ihrerseits wiederum die Gefährdungs- und Maßnahmenkataloge sowie die IT-Grundschutz-Bausteine, durch die eine geeignete Verknüpfung von Systemen im Schichtenmodell mit Maßnahmen und Gefährdungen erfolgt.

Die Bausteine sind der umfänglichste Teil der IT-Grundschutz-Kataloge und betrachten die einzelnen Sicherheitsmaßnahmen für betrachtete Objekte insbesondere im Hinblick auf die Phasen des Lebenszyklusses: Planung und Konzeption, Beschaffung, Umsetzung, Betrieb, Aussonderung und grundlegende Notfallvorsorge. In der sich schnell verändernden IT-Landschaft besteht eine große Herausforderung für das BSI darin, die Bausteine stets aktuell zu halten und gleichzeitig neuen Entwicklungen rechtzeitig durch neue Bausteine Rechnung zu tragen. Für die detaillierte Beschäftigung mit den fachlichen Inhalten einzelner Bausteine bietet sich die Durchführung einer exemplarischen IT-Grundschutz-Modellierung an. Die Bausteine selbst sind gegliedert nach den Schichten:

- B1 Übergreifende Aspekte
- B2 Infrastruktur
- B3 IT-Systeme
- B4 Netze
- B5 IT-Anwendungen

Abbildung 6.4: IT-Grundschutz-Bausteine

Grafikvorlage: Bundesamt für Sicherheit in der Informationstechnik (BSI)

4 Die Inhalte dieses Standards sind Gegenstand im Kapitel 26.

Die Maßnahmenkataloge dienen dazu, an zentraler Stelle Sicherheitsmaßnahmen so zu beschreiben, dass in den Bausteinen geeignet referenziert werden kann. Dadurch können Dopplungen und Inkonsistenzen elegant vermieden werden. Die Maßnahmenkataloge gliedern sich in die Bereiche:

- M1: Infrastruktur
- M2: Organisation
- M3: Personal
- M4: Hard- und Software
- M5: Kommunikation
- M6: Notfallvorsorge

Ebenso wie die Maßnahmen sind auch die Gefährdungen zentral erfasst. Sie gliedern sich in die Bereiche:

- G1: Höhere Gewalt
- G2: Organisatorische Mängel
- G3: Menschliche Fehlhandlungen
- G4: Technisches Versagen
- G5: Vorsätzliche Handlungen

6.4 Tool-Unterstützung

In der Praxis wird man ein IT-Sicherheitsmanagement nach IT-Grundschutz kaum ohne eine geeignete Werkzeugunterstützung etablieren können. Auf dem Markt existieren Werkzeuge verschiedener Hersteller, die die Vorgehensweise nach IT-Grundschutz unterstützen. Exemplarisch seien an dieser Stelle stellvertretend für viele das IT-Grundschutz-Tool des BSI und das erste plattformübergreifende Open-Source-Werkzeug *verinice* genannt.

6.5 ISO 27001-Zertifizierung auf Basis von IT-Grundschutz

Zum Nachweis der erfolgreichen Umsetzung von IT-Grundschutz kann ein definierter Informationsverbund zertifiziert werden. Der Informationsverbund wird durch das Unternehmen oder die Behörde festgelegt und sollte vorab mit dem BSI abgestimmt werden. In Form eines Audits wird basierend auf dem verbindlichen, vom BSI veröffentlichten Prüfschema das Informationssicherheitsmanagement, die Referenzdokumente und die konkrete Implementierung vor Ort überprüft. Verläuft die Zertifizierung erfolgreich und wird der Bericht durch das BSI abgenommen, wird ein *ISO 27001-Zertifikat auf Basis von IT-Grundschutz* vom Bundesamt für Sicherheit in der Informationstechnik ausgestellt.

Es gibt drei Zertifizierungsstufen mit denen ein entsprechender Umsetzungsstatus nachgewiesen werden kann:

- Auditor-Testat Einstiegsstufe
- Auditor-Testat Aufbaustufe
- ISO 27001-Zertifikat auf Basis von IT-Grundschutz

Ein Auditoren-Testat ist zwei Jahre gültig und muss im folgenden Zeitraum durch eine höhere Stufe oder ein ISO 27001-Zertifikat auf Basis von IT-Grundschutz abgelöst werden. Auditor-Testate sollen den Einstieg in IT-Grundschutz erleichtern und erfordern weniger Maßnahmen als das Zertifikat. Sie können zur Veröffentlichung beim BSI angemeldet werden.

Die Zertifizierungsgrundlagen für das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz werden grundsätzlich auf der Web-Seite des BSI in [BSI-PGL] veröffentlicht. Sie beinhalten vor allem:

- ISO/IEC 27011:2005
- BSI-Standard 100-2
- IT-Grundschutz-Kataloge (in aktueller Fassung, Stand Juli 2013: 12. Ergänzungslieferung 2011)

sowie weitere Vorgaben und Musterdokumente.

Durch ein Audit nach ISO 27001 auf der Basis von IT-Grundschutz wird geprüft, ob die Anforderungen aus dem IT-Grundschutz erfüllt sind.

Vom Auditor werden die folgenden Prinzipien gefordert:

- Ethisches Verhalten
- Sachliche Darstellung der Ergebnisse
- Angemessene Sorgfalt
- Unabhängigkeit und Objektivität (keine beratende Tätigkeit innerhalb von zwei Jahren vor dem Audit)
- Vorlage von Nachweisen

Unabdingbare Eckpfeiler eines Grundschutz-Audits sind Nachweise zu:

- Sicherheitsniveau und Sicherheitszustand des Informationsverbunds
- Vollständigkeit der Dokumentation und der Sicherheitsmaßnahmen
- Transparenz der Umsetzung
- Aktualität der Ergebnisse
- Prozessen der Aufrechterhaltung der IT-Sicherheit.

Die Audits müssen durch den Auditor entsprechend sorgfältig durchgeführt und dokumentiert werden, damit sie als Grundlage der Zertifizierung durch das BSI dienen können.

Zusammenfassung

IT-Grundschutz verfolgt den Ansatz, durch Standard-Maßnahmen für Objekte in Informationsverbünden mit normalem Schutzbedarf auf einfache Weise ein angemessenes Sicherheitsniveau zu erreichen. IT-Grundschutz stellt dabei eine Vorgehensweise zur Umsetzung von ISO 27001 dar. Dabei spielen die BSI-Standards 100-1 bis 100-4 eine wesentliche Rolle. Diese werden ergänzt durch die in den IT-Grundschutz-Katalogen enthaltene sehr umfangreiche Sammlung an wesentlichen IT-Sicherheitsmaßnahmen. Der Umfang der standardisierten Kataloge ist dabei der Vielfalt und der Komplexität der vielfältigen IT-Systeme und der gegen sie gerichteten Bedrohungen geschuldet. Individuelle Lösungen sind in der Regel deutlich aufwändiger.

Literatur

[BSI-1001] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)

[BSI-1002] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise

[BSI-1003] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz

[BSI-1004] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* BSI-Standard 100-4: Notfallmanagement

[BSI-GSK] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* IT-Grundschutz-Kataloge

[BSI-PGL] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* Prüfgrundlage für Zertifizierungen nach ISO 27001 auf der Basis von IT-Grundschutz

[BSI-ZERT1] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Zertifizierungsschema

[BSI-ZERT2] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Auditierungsschema

Alle Dokumete sind zu finden unter
https://www.bsi.bund.de/IT-Grundschutz

12 Vertrauensmodelle und PKI-Komponenten

Einleitung

Digitale Signaturen, Benutzerauthentifikation und Verschlüsselung erfordern die Zuordnung von Schlüsseln zu einem Schlüsselinhaber. Dieses Kapitel beschreibt, wie öffentliche Schlüssel verteilt und verwaltet werden. Hierbei gibt es in der Praxis zwei konkurrierende Ansätze, die auf verschiedenen Vertrauensmodellen basieren. Ziel ist es, die beiden verschiedenen Ansätze zu verdeutlichen und ihre Funktionsweise darzustellen. Hierbei werden die einzelnen Komponenten und Prozesse einer Public Key Infrastruktur (PKI) verdeutlicht. Eine PKI wird benötigt, um den Einsatz von Verfahren der asymmetrischen Verschlüsselung zu unterstützen. Diese Verfahren verwenden Schlüsselpaare – bestehend aus einem privaten und einem korrespondierenden öffentlichen Schlüssel.[1]

Für die Erzeugung von digitalen Signaturen wird der private Schlüssel des Schlüsselpaars des Signierenden benötigt. Zur Verifikation von Signaturen benötigt der Prüfende den zugehörigen öffentlichen Schlüssel. Im Falle der Verschlüsselung verwendet der Absender einen öffentlichen Schlüssel des Empfängers zum asymmetrischen Schlüsseltransport[2]. Der Empfänger kann die Nachricht mit seinem privaten Schlüssel entschlüsseln. In beiden Fällen ist der Verwender des öffentlichen Schlüssels die *Relying Party* (Zertifikatsprüfer) – er muss darauf vertrauen können, dass der öffentliche Schlüssel und damit das Schlüsselpaar unter der Kontrolle des richtigen Kommunikationspartners steht. Daraus ergibt sich, dass die öffentlichen Schlüssel für alle Kommunikationspartner sicher verteilt und verwaltet werden müssen. Für eine skalierbare Lösung eines Schlüsselmanagements sollte zur Verteilung der öffentlichen Schlüssel außerdem möglichst kein persönlicher Kontakt erforderlich sein.

Wenn viele Kommunikationspartner, die sich gegebenenfalls gar nicht kennen, ihre Schlüssel austauschen wollen, reicht der Austausch des öffentlichen Schlüssels alleine oft nicht aus, um sicher miteinander kommunizieren zu können. Es wird eine eindeutige Zuordnung von öffentlichem Schlüssel und Schlüsselinhaber benötigt, die eine Relying Party überprüfen kann, um sich zu überzeugen, dass eine Nachricht tatsächlich von dem vermeintlichen Absender digital signiert wurde bzw. der öffentliche Schlüssel, der zur Verschlüsselung einer vertraulichen Nachricht verwendet werden soll, zweifelsfrei dem Empfänger zugeordnet werden kann.

Oft ist es außerdem erforderlich, Schlüssel im Fall einer Kompromittierung als ungültig zu kennzeichnen. Dazu ist es notwendig, dass Rückruf-Informationen zu ungültigen Schlüsseln gesichert verteilen werden können. Zur sicheren Verteilung und Verwaltung der öffentlichen Schlüssel gibt es in der Praxis zwei konkurrierende Ansätze:

- Das dezentrale Vertrauensmodell, das als *Web of Trust* bezeichnet wird
- Das zentrale Vertrauensmodell basierend auf einer *Public Key Infrastruktur* (PKI)

1 Siehe Abschnitt 11.7 und Abschnitt 11.8

2 Siehe zum Begriff auch Abschnitt 11.7. Umgangssprachlich wird für den asymmetrischen Schlüsseltransport häufig auch die Bezeichnung hybride Verschlüsselung verwendet.

12.1 Vertrauensmodelle

Für eine sichere Kommunikation bedarf es ein gewisses Maß an Vertrauen in die verwendeten Schlüssel. Um einem öffentlichen Schlüssel vertrauen zu können, muss die Echtheit des Schlüssels und die Zugehörigkeit zu einer Person von einer vertrauenswürdigen Stelle bestätigt werden. Nachfolgend werden zwei Modelle dargestellt, wie Schlüssel bestätigt und vertrauensvoll verteilt werden können.

12.1.1 Web of Trust

Das Web of Trust bietet keine zentrale technische oder organisatorische Infrastruktur, sondern die Verteilung der öffentlichen Teilnehmerschlüssel erfolgt selbstorganisiert in einen dezentralen Vertrauensmodell. Das Vertrauen basiert auf Gegenseitigkeit, wobei das Modell auch mittelbares Vertrauen zulässt, d. h. das Vertrauen in einen Schlüssel kann an einen Dritten weitergegeben werden. Das Web of Trust wird vorwiegend für private und persönliche Kommunikation verwendet, findet aber auch im geschäftlichen Umfeld Verwendung.

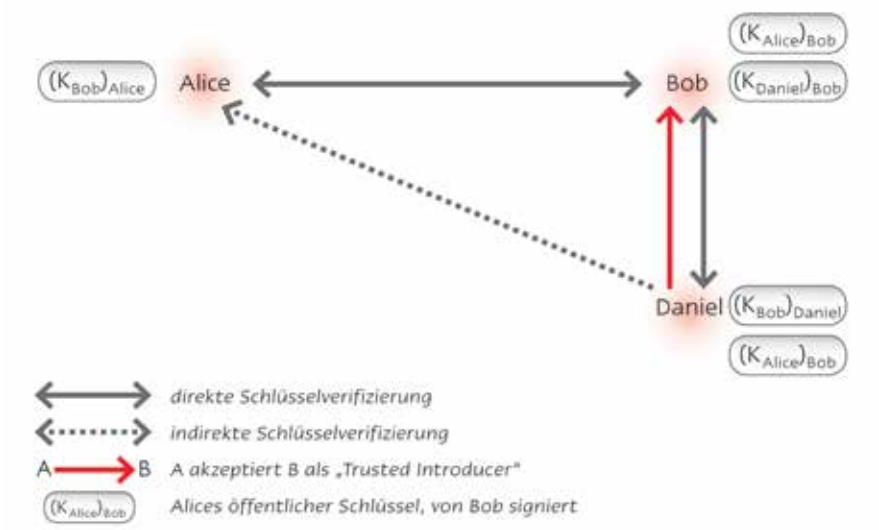
Der Schlüsselaustausch zwischen den Kommunikationspartnern erfolgt über eine persönliche Weitergabe des öffentlichen Schlüssels. Zur direkten Überprüfung des übermittelten öffentlichen Schlüssels werden Hash-Werte über den öffentlichen Schlüssel – sogenannte Fingerprints – verwendet. Sie erlauben einen effizienteren Vergleich des abgesandten mit dem empfangenen öffentlichen Schlüssel, als wenn der volle öffentliche Schlüssel abgeglichen werden müsste. Bei der digitalen Übertragung der öffentlichen Schlüssel sollte diese Überprüfung der Hash-Werte Out-of-Band, d. h. über einen anderen Kommunikationskanal erfolgen, z. B. über das Telefon. Alle Teilnehmer können die Echtheit von Schlüsseln, die sie so überprüft haben, auch mit einer eigenen Signatur bestätigen und weitergeben. Dabei muss nicht jeder Schlüssel von jedem anderen Teilnehmer bestätigt werden, sondern das Vertrauen in Schlüssel kann durch Teilnehmer auf der Basis von Signaturen anderer gewährt werden. Durch diese vielen und auch teilweise transitiven Vertrauensbeziehungen entsteht das Web of Trust. Mit dem Web of Trust ist somit ein direkter und schneller Schlüsselaustausch möglich, der allerdings ein persönliches Treffen oder eine zusätzliche Kommunikation voraussetzt und nur zwischen bekannten Kommunikationspartnern funktioniert.

Der Rückruf eines öffentlichen Schlüssels ist nur dann möglich, wenn dieser nicht an Dritte weitergegeben wurde. Wurde der Schlüssel weitergegeben, kann nicht sichergestellt werden, dass die Rückrufinformation alle Kommunikationspartner erreicht.

Im Vertrauensmodell Web of Trust bestätigt ein Schlüsselinhaber die Echtheit seines eigenen öffentlichen Schlüssels durch die Signatur mit seinem zugehörigen privaten Schlüssel, d. h. in der Regel sind alle Schlüssel selbstsigniert. Es gibt aber auch die Möglichkeit, verschiedene fremde Teilnehmerschlüssel von einer vertrauenswürdigen Instanz signieren zu lassen. Über das Konzept eines solchen *Trusted Introducers* kann auch – ähnlich wie im zentralen Vertrauensmodell – eine zentrale Instanz als Bestätigungsstelle fungieren. Der Trusted Introducer prüft öffentliche Schlüssel und bestätigt diese durch seine digitale Signatur. Typischerweise gibt es in einem Unternehmen einen oder wenige solcher Trusted Introducer. Der Vorteil eines Trusted Introducers besteht darin, dass externe Kommunikationspartner sich nur noch von der Echtheit des öffentlichen Schlüssels des Trusted Introducers überzeugen müssen und dann allen öffentlichen Schlüsseln vertrauen können, die von diesem Trusted Introducer digital signiert wurden, d. h. der externe Kommunikationspartner prüft nur noch die digitale Signatur des Trusted Introducers und muss nicht mehr die Fingerprints aller öffentlichen Schlüssel verifizieren. Die Sicherheit dieses Verfahrens beruht somit auf dem Vertrauen in einen Dritten. Wenn dieser Dritte unbekannt ist, muss sich der Kommunikationspartner von der Authentizität seines Schlüssels und seiner Vertrauenswürdigkeit überzeugen. Dann aber hat er den Vorteil, dass er alle vom Trusted Introducer signierten Schlüssel verwenden

kann. Die Verteilung der öffentlichen Schlüssel kann durch sogenannte Key Server erfolgen. Allerdings ist dann kein systematischer Rückruf von Schlüsseln mehr möglich, da potentiell jeder die Schlüssel vom Server abrufen kann und diese dann weit verbreitet sein können.

Abbildung 12.1: Ein Beispiel für ein Web of Trust



Die Rückrufinformation eines Schlüssels wird in diesem Verfahren über ein zusätzliches Attribut an den Schlüssel angehängt und dieser dann erneut auf einem Key Server publiziert. Verfahrensbedingt gibt es aber keine Notwendigkeit für einen externen Kommunikationspartner, einen bereits lokal vorhandenen öffentlichen Schlüssel erneut vom Key Server zu holen. Somit bleibt der Sperrvermerk gegebenenfalls unbemerkt.

Das Sicherheitsniveau des Web of Trust lässt sich nicht klar abschätzen. Im Allgemeinen ist nicht reglementiert und dokumentiert, wie Schlüssel erzeugt und Identitäten sowie Fingerprints überprüft werden. Die Sperrung von öffentlichen Schlüsseln kann nicht durchgesetzt werden.

Das Beispiel in Abbildung 12.1 zeigt, wie das dezentrale Vertrauensmodell funktioniert. Alice und Bob sowie Daniel und Bob haben ihre öffentlichen Schlüssel untereinander ausgetauscht und vertrauen sich gegenseitig. Daniel akzeptiert Bob als Trusted Introducer und hat damit auch eine indirekte Vertrauensbeziehung zu Alice (indirekte Schlüsselverifizierung).

12.1.2 Zentrales Modell der Public Key Infrastruktur

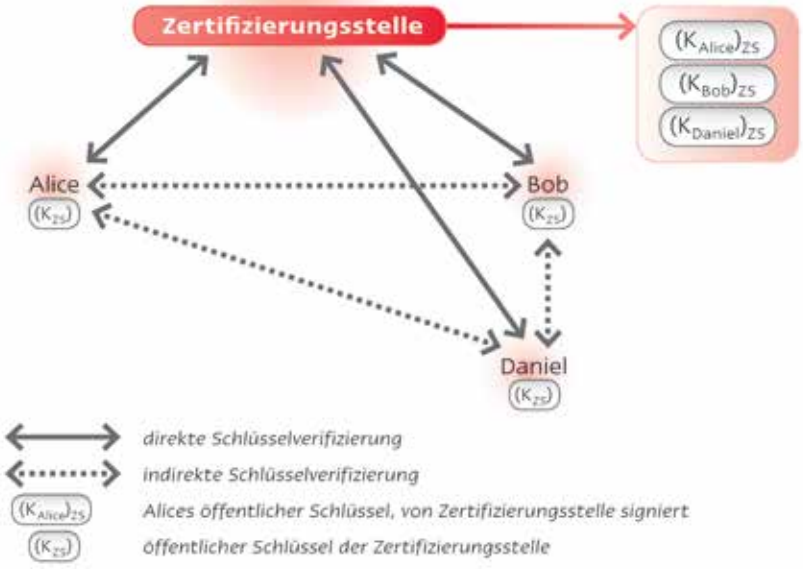
Das zentrale Vertrauensmodell basiert auf einer Public Key Infrastruktur (PKI). Durch die PKI werden die Dienste des Schlüsselmanagements erbracht. Die Prozesse und Verantwortlichkeiten sind klar geregelt. Die Regelungen für die PKI werden in Policy-Dokumenten festgelegt.

In der PKI werden die öffentlichen Schlüssel durch eine vertrauenswürdige Instanz – eine sogenannte Zertifizierungsstelle – bestätigt. Alle Kommunikationspartner, die einen durch die PKI bestätigten Schlüssel verwenden wollen, müssen nur dieser einen Zertifizierungsstelle vertrauen. Ein weiterer Vorteil ist, dass nur ein einziger gesicherter Schlüsselaustausch pro Teilnehmer mit der Zertifizierungsstelle nötig ist. Die Kommunikationspartner untereinander müssen ihre öffentlichen Schlüssel nicht mehr bilateral auf sichere Weise austauschen.

Die öffentlichen Schlüssel können in einem sogenannten Schlüssel-Verzeichnis publiziert werden. Es genügt, vor der Verwendung eines aus dem Verzeichnis abgerufen öffentlichen Schlüssels die Bestätigung der Zertifizierungsstellen zu überprüfen.

Das Beispiel in Abbildung 12.2 zeigt, wie das zentrale Vertrauensmodell funktioniert. Alice, Bob, und Daniel haben alle eine direkte Vertrauensbeziehung zu der Zertifizierungsstelle. Da alle der gleichen Zertifizierungsstelle vertrauen, haben sie auch untereinander eine indirekte Vertrauensbeziehung. Die Zertifizierungsstelle veröffentlicht alle von ihr bestätigten öffentlichen Schlüssel in einem Schlüssel-Verzeichnis.

Abbildung 12.2: Beispiel „Zentrales Vertrauensmodell“



12.2 Public Key Infrastruktur

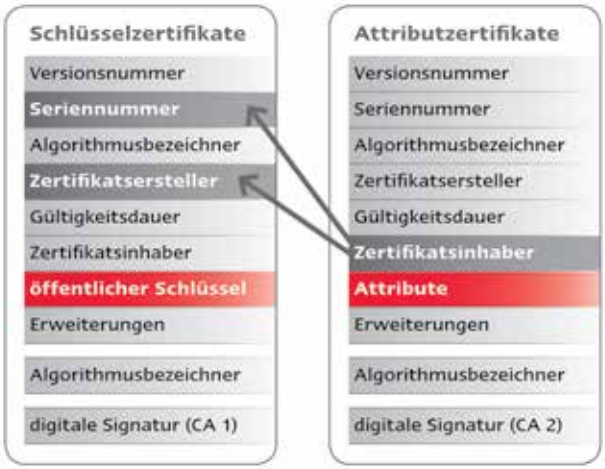
12.2.1 Zertifikate und CRLs

Die Bestätigung der Zuordnung zwischen Schlüsselinhaber und Schlüssel wird in einer PKI über Zertifikate ausgedrückt. Diese Zertifikate dienen als eine Art „elektronischer Personalausweis“. Ihr Format ist standardisiert.

Zertifikate werden von einer Zertifizierungsstelle oder englisch *Certification Authority* (CA) ausgestellt. Sie bestätigen in einem formal aufgebauten elektronischen Dokument mit ihrer Signatur, dass ein vorliegender öffentlicher Schlüssel dem benannten Schlüsselinhaber zugeordnet ist. Außer dem Schlüsselinhaber und dem öffentlichen Schlüssel enthält ein Zertifikat noch weitere

Attribute wie beispielsweise eine eindeutige[3] Seriennummer, einen Gültigkeitszeitraum und den Namen der Zertifizierungsstelle. Über die digitale Signatur der CA wird die Integrität und Authentizität der Zuordnung von öffentlichem Schlüssel und Schlüsselinhaber gewährleistet. Diese Zuordnung kann nicht unbemerkt verfälscht werden, es sei denn ein Angreifer hat den privaten Schlüssel der CA kompromittiert, der zur Signaturerstellung benötigt wird.

Abbildung 12.3: Aufbau von Schlüssel- und Attributzertifikaten



Zertifikate enthalten in der Regel außer dem Namen des Schlüsselinhabers, seinem öffentlichen Schlüssel, einer eindeutigen Seriennummer und einer Gültigkeitsdauer noch weitere Zusatzinformationen, z. B. Nutzungsbeschränkungen, alternative Namensformen oder Informationen für einen vereinfachten Aufbau des Zertifizierungspfades. Weitere Informationen finden sich bei [RFC5280] und [X509].
Neben den eben beschriebenen Schlüsselzertifikaten gibt es noch sogenannte Attributzertifikate (Abbildung 12.3), die zusätzliche Informationen an das Schlüsselzertifikat und damit an den Zertifikatsinhaber binden. Der Zertifikatsinhaber wird hierbei über eine Referenz auf sein Schlüsselzertifikat identifiziert. Hintergrund der Attributzertifikate ist das Bestreben, nicht zu viele personenbezogene Daten in das Schlüsselzertifikat aufzunehmen, sondern diese in ein oder mehrere Attributzertifikate auszulagern. Je nach Anwendung kann der Zertifikatsinhaber dann das Attributzertifikat auswählen, das die für diese Anwendung benötigten Informationen enthält.

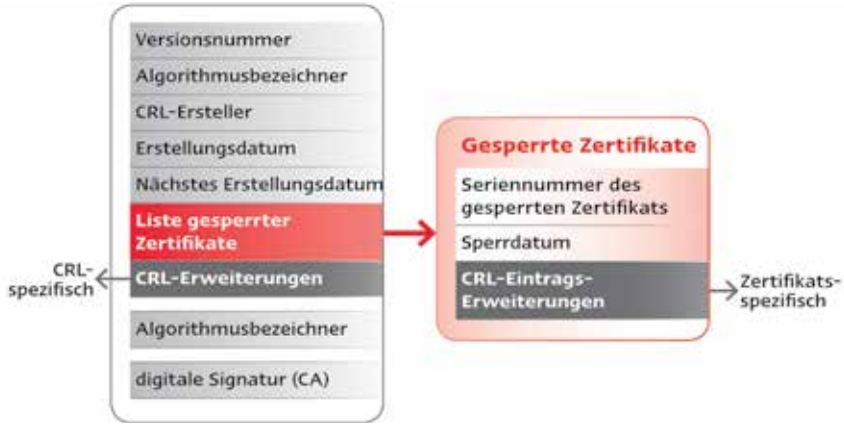
Soll ein Zertifikat zurückgezogen werden, z. B. weil der Schlüssel kompromittiert wurde oder der Schlüsselinhaber seinen Namen gewechselt hat, so setzt die CA die Seriennummer dieses zu sperrenden Zertifikats auf ihre Sperrliste (*Certificate Revocation List*, *CRL*). Eine CRL ist eine von der CA signierte Liste mit einer begrenzten Gültigkeit, welche die Seriennummern aller von dieser CA gesperrten Zertifikate enthält (siehe Abbildung 12.4) Für die Verifikation einer Signatur[4] holt sich die Relying Party stets die aktuelle CRL und prüft, ob die Seriennummer des zu prüfenden Zertifikats dort enthalten ist.

3 Die Eindeutigkeit gilt nur für alle von einer Zertifizierungsstelle ausgestellten Zertifikate. Zertifikate einer anderen Zertifizierungsstelle können die gleichen Seriennummern aufweisen.

4 Vgl. auch Abschnitt 11.8 und Abschnitt 12.2.3

Ein Nachteil von Sperrlisten ist, dass eine Sperrliste für einen definierten Zeitraum gültig ist, nämlich vom Erstellungsdatum bis zum nächsten geplanten Erstellungsdatum. Wird in diesem Zeitraum ein Zertifikat zurückgezogen, ergeben sich für die ausstellende CA zwei Alternativen: Entweder sie stellt umgehend eine neue Sperrliste aus oder sie wartet mit der Ausstellung der neuen Sperrliste bis regulär die nächste Sperrliste ausgestellt wird. Im ersten Fall gibt es zwei gültige Sperrlisten, d. h. ein Angreifer könnte z. B. die aktuelle Sperrliste im Verzeichnis durch die alte noch gültige Sperrliste ersetzen, um das gesperrte Zertifikat zu verheimlichen. Im zweiten Fall gibt es zwar immer nur eine gültige Sperrliste, aber die Sperrinformation wird dem Prüfer des Zertifikats bis zur Veröffentlichung der nächsten Sperrliste vorenthalten. Daher ist es empfehlenswert, bei Rückruf eines Zertifikats umgehend eine neue Sperrliste auszustellen und zu veröffentlichen, so dass für eine „Relying Party" die aktuellen Sperrinformationen sofort verfügbar sind. Allerdings gibt es in der Praxis einige Anwendungen, die sich keine aktuelle Sperrliste holen, solange die vorliegende Sperrliste noch nicht abgelaufen ist. Diese Restrisiken von nicht bekannten Sperrinformationen sind umso geringer, je kürzer der Ausstellungszyklus einer Sperrliste gewählt wird.

Abbildung 12.4: Aufbau einer Sperrliste für Zertifikate



Schlüsselzertifikate, Attributzertifikate und Sperrlisten werden in dem Standard X.509 definiert. Seit der Version 3 gibt es die Möglichkeit, über Erweiterungen zusätzliche Informationen in einem Zertifikat, einer CRL oder CRL-Einträgen hinzuzufügen. So können in X.509v3 Zertifikaten beispielsweise:

- zusätzliche Namensformen wie eine E-Mail-Adresse angegeben werden,
- zwischen Benutzer- und CA-Zertifikaten unterschieden werden,
- über sogenannte *KeyUsage-Bits* die Schlüsselverwendung eingeschränkt oder
- mehrere URLs spezifiziert werden, über die CA-Zertifikat und CRL heruntergeladen werden können.

12.2.2 Zertifizierungshierarchien

CAs stellen nicht nur Zertifikate für Endteilnehmer (Benutzer, Maschinen oder Server) aus, sondern auch für untergeordnete Zertifizierungsstellen. So entstehen Zertifizierungshierarchien mit einer Wurzelzertifizierungsstelle (Root CA) als obersten Knoten, mehreren zwischengeordneten

Zertifizierungsstellen (Intermediate CAs) und den Endteilnehmern als Endknoten. Die Root CA dient als Sicherungsanker für die gesamte Zertifizierungsinfrastruktur und muss bei jedem Teilnehmer mit großer Sorgfalt vor Manipulation geschützt werden. Gelingt es einem Angreifer den öffentlichen Schlüssel der Root CA bei einem Teilnehmer auszutauschen, der ein Zertifikat als Relying Party prüfen will, so kann er diesem beliebige Identitäten vorspiegeln, die er mit seiner eigenen CA zertifiziert hat. Jedes gefälschte Zertifikat unter dem lokalen manipulierten Schlüssel der Root CA wird stets erfolgreich verifiziert werden.

Die Root CA und die operativen CAs sollten immer durch eine Hierarchie getrennt sein, so dass das Zertifikat einer operativen CA bei Kompromittierung ihres privaten Schlüssels gesperrt werden kann. Ohne eine übergeordnete CA müsste die Sperrliste mit dem eigenen kompromittierten privaten Schlüssel signiert werden und würde somit keine sichere Aussage über den Sperrstatus der gesperrten Zertifikate erlauben. Insbesondere der Root CA-Schlüssel sollte besonders gegen Schlüsselverlust und -kompromittierung geschützt werden, z. B. durch Aufbewahrung in einem Tresor oder durch Erzeugung und Speicherung auf einem Hardware Security Module (HSM). So ist die Root CA als Vertrauensanker der PKI gut gesichert vor Kompromittierung und Missbrauch. Die Root CA wird nur benötigt, um gegebenenfalls weitere untergeordnete CAs zu zertifizieren und um – typischerweise jährlich – eine neue Sperrliste auszustellen. Nur das Zertifikat dieser Root CA muss an die externen Kommunikationspartner verteilt werden. Bedingt durch die sichere Verwahrung, den seltenen Einsatz und die höheren Sicherheitsmaßnahmen beim Betrieb der Root CA ist die Wahrscheinlichkeit einer Kompromittierung des privaten Root CA Schlüssels sehr gering. Die externen Kommunikationspartner können so mehr Vertrauen und eine größere Gewissheit über die Konstanz dieses Zertifikats haben, das sie bei sich in ihren Anwendungen aufnehmen und als vertrauenswürdig anerkennen müssen.

12.2.3 Verifikation einer digitalen Signatur

Zur Verifikation einer digitalen Signatur muss zunächst der Zertifizierungspfad vom Absender, der die Signatur erzeugt hat, bis hin zur einer für den Empfänger vertrauenswürdigen CA aufgebaut werden. Diese vertrauenswürdige CA kann die Root CA, aber auch eine untergeordnete CA sein, die sowohl im Zertifizierungspfad des Signierenden als auch der Relying Party liegt. Ein Zertifizierungspfad ist die Aneinanderreihung von Zertifikaten, die über die Signatur des Zertifikats und die Übereinstimmung der Namen des Zertifikatsausstellers mit dem übergeordneten Zertifikatsinhaber verkettet sind.

Beim Aufbau des Zertifizierungspfades müssen für jedes einzelne Zertifikat im Pfad

- die digitale Signatur,
- seine Gültigkeit,
- die Übereinstimmung des Namens von Zertifikatsaussteller und übergeordnetem Zertifikatsinhaber sowie
- sein Sperrstatus

überprüft werden.

Nur wenn die digitale Signatur des Absenders mathematisch korrekt verifiziert werden kann und ein gültiger Zertifizierungspfad – bestehend aus zeitlich gültigen und nicht gesperrten Zertifikaten – aufgebaut werden kann, ist die digitale Signatur des Absenders als gültig anzuerkennen.

Gültigkeitsmodelle

In [X509] standardisiert, weit verbreitet und anerkannt ist das sogenannte Schalenmodell für die Verifikation von Signaturen. Beim Schalenmodell müssen alle Signaturen einer Zertifikats-

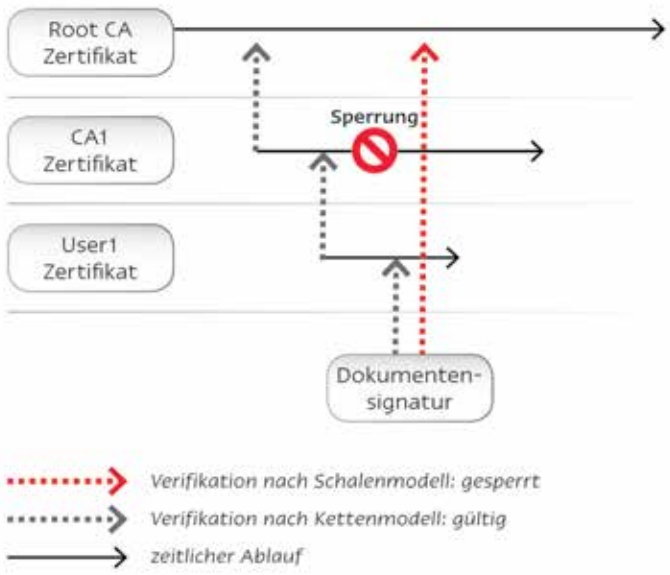
kette zu einem Zeitpunkt gültig sein. Dieser Zeitpunkt kann entweder der Signatur- oder der Verifikationszeitpunkt sein. Jedes untergeordnete Zertifikat muss bei diesem Modell in seiner Gültigkeit innerhalb der Gültigkeit des übergeordneten Zertifikats (Schale) liegen, daher der Name *Schalenmodell*.

Das sogenannte *Kettenmodell* ist aus dem deutschen Signaturgesetz abgeleitet. Das Signaturgesetz fordert, dass jede Signatur zum Erstellungszeitpunkt gültig gewesen sein muss. Jedes einzelne Zertifikat eines Zertifizierungspfades wurde zu einem anderen Zeitpunkt signiert. Somit gibt es mehrere „verkettete" Verifikationszeitpunkte, da jedes Zertifikat zu seinem Erstellungs- und Signaturzeitpunkt überprüft werden muss.

Bei einem gesperrten Zertifikat kann eine Überprüfung in Abhängigkeit vom verwendeten Gültigkeitsmodell zu verschiedenen Ergebnissen kommen. Angenommen ein CA-Zertifikat wird während seiner Laufzeit gesperrt. Als das CA-Zertifikat noch nicht gesperrt war, wurde von dieser CA ein Benutzerzertifikat ausgestellt. Der Benutzer hat mit diesem Zertifikat ein Dokument signiert. Sein Benutzerzertifikat ist zum Zeitpunkt der Verifikation nicht abgelaufen. Die Verifikation seiner digitalen Signatur führt – je nach verwendetem Gültigkeitsmodell – zu verschiedenen Verifikationsergebnissen (siehe Abbildung 12.5). Eine Verifikation gemäß dem Schalenmodell führt zu dem Ergebnis, dass die digitale Signatur ungültig ist, da das CA-Zertifikat zum Verifikationszeitpunkt gesperrt ist. Legt man das Kettenmodell der Verifikation zu Grunde, so erhält man ein positives Verifikationsergebnis: Die digitale Signatur ist gültig, da zu jedem Zeitpunkt einer Signaturerstellung (Dokumenten- oder Zertifikatssignatur) das zugehörige Zertifikat gültig war.

Der geeignete Verifikationszeitpunkt hängt vom Kontext ab: Beispielsweise ist es sinnvoll, für eine Dokumenten-Signatur gegen den Erzeugungszeitpunkt der Signatur zu prüfen. Für eine Authentisierungsanfrage, die mit einem Zertifikat unterlegt ist, muss dagegen die Gültigkeitsprüfung auf den aktuellen Zeitpunkt abstellen.

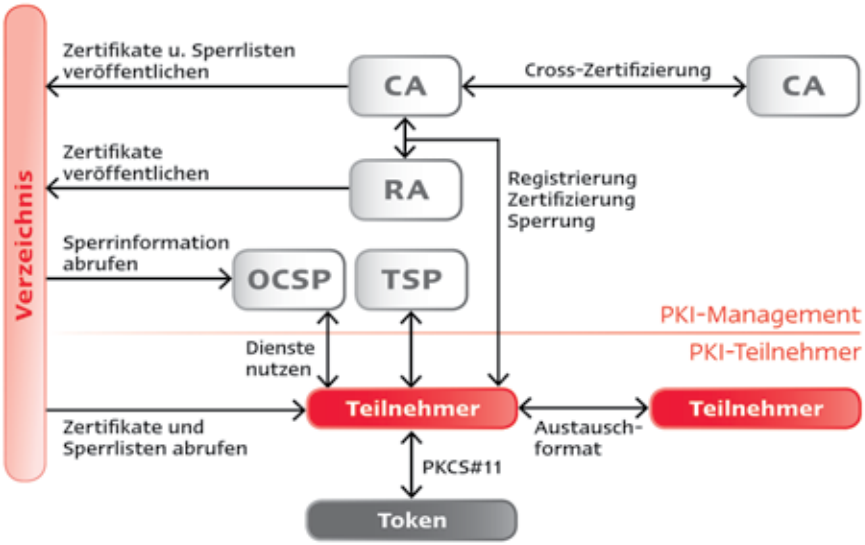
Abbildung 12.5: Vergleich der Gültigkeitsmodelle für die Signaturprüfung



12.2.4 Komponenten und Prozesse einer PKI

Die einzelnen Komponenten und Kommunikationsbeziehungen einer PKI sind in Abbildung 12.6 dargestellt. Zusätzlich zu den dargestellten Instanzen gehören zum Aufbau und zur Inbetriebnahme einer PKI auch die Beschreibung der organisatorischen Abläufe und die rechtlichen Regelungen für den Betrieb und die Leistungen der PKI. Im Bereich der elektronischen Signaturen gehört zu letzterem beispielsweise das Signaturgesetz (SigG).

Abbildung 12.6: Komponenten einer PKI



Zertifizierungs- und Registrierungsstelle

Eine PKI besteht aus verschiedenen Instanzen. Zunächst gibt es die bereits dargestellten CAs, die digital signierte Gültigkeitsbestätigungen, die Zertifikate, nach eindeutigen Regeln ausstellen.

Doch bevor ein Zertifikat ausgestellt werden kann, muss der Benutzer registriert und seine Identität überprüft werden. Diese Registrierung erfolgt oft losgelöst von der Ausstellung der Zertifikate durch sogenannte Registrierungsstellen (*Registration Authority*, RA). Die Auslagerung der RA-Funktionalität aus dem Kontext der eigentlichen CA bietet sich an, wenn eine Organisation über verschiedene Standorte verteilt ist und die CA zentral betrieben wird. An den einzelnen Standorten können die Benutzer durch die lokalen RAs registriert werden. Diese leiten die erhobenen und überprüften Registrierungsinformationen zur Zertifizierung auf sicherem Weg an die CA weiter.

Verzeichnisdienst

Die CA veröffentlicht die ausgestellten Zertifikate und ihre CRL in einem Verzeichnisdienst (*Directory*). Diese Veröffentlichung erfolgt über standardisierte Verfahren in der Regel einem LDAP-Directory. Alle PKI-Teilnehmer benötigen lesenden Zugriff auf diesen Verzeichnisdienst, um Zertifikate und CRLs beziehen zu können.

Für den Verzeichnisdienst ist ein Mindestniveau an Daten-Integrität sicherzustellen, damit keine Zertifikate oder CRLs durch einen Angreifer gelöscht oder durch alte Versionen ersetzt werden

können. Durch solche Manipulationen mit ungültigen Zertifikaten oder CRLs könnte der Angreifer Denial-of-Service-Situationen auslösen. Gelingt ihm das Einspielen einer alten CRL, die zeitlich noch gültig ist, könnte er sogar die Sperrung eines Zertifikats vertuschen.

CA-Zertifikate und CRLs können alternativ oder zusätzlich zur Bereitstellung in einem Directory auch auf einem Web-Server im Internet veröffentlicht werden. Wenn die entsprechenden URLs in den Benutzerzertifikaten eingetragen werden, können die Clients diese Information auch dort automatisiert abrufen.

Online-Status-Auskunftsdienst

Eine Alternative zur Verwendung von CRLs ist der sogenannte Online Status-Auskunftsdienst (*Online Certificate Status Protocol Responder*, OCSP-Responder). Dieser OCSP-Responder liefert eine signierte Antwort zum Status eines angefragten Zertifikats. Dabei wird nicht das zu prüfende Zertifikat selber an den OCSP-Responder übergeben, sondern nur der Name (*Distinguished Name*) des Zertifikatsausstellers und die Seriennummer des Zertifikats. Dieses Tupel bildet immer eine eindeutige Referenz auf ein Zertifikat. Mögliche Antworten des OCSP-Responders sind „good", „revoked" oder „unknown". „Unknown" liefert der OCSP-Responder einer CA bei Anfragen zu Zertifikaten, die nicht von dieser CA ausgestellt wurden.

In der Regel basieren die Auskünfte eines OCSP-Responders auf einer CRL, d. h. der OCSP-Responder durchsucht die aktuelle CRL der CA auf die Seriennummer des angefragten Zertifikats und liefert „good" zurück, wenn die Seriennummer des Zertifikats dort nicht gefunden wird, bzw. „revoked", wenn die Seriennummer des Zertifikats in der CRL enthalten ist. Weitere Informationen finden sich in [RFC2560].

Wie bereits in der Beschreibung der Gültigkeitsmodelle im Abschnitt 12.2.3 dargestellt, gibt es in Deutschland mit den signaturgesetzkonformen Zertifikaten eine Sonderform der PKI. In Bezug auf Statusinformationen zu einem signaturgesetzkonformen Zertifikat gibt es in diesem Zusammenhang weitere Anforderungen: Ein signaturgesetzkonformer OCSP-Responder darf nicht auf Basis einer Negativliste, wie einer CRL, eine Statusauskunft erteilen, sondern die Auskunft muss auf einer Positivliste beruhen. Daher müssen signaturgesetzkonforme OCSP-Responder ihre Statusauskunft auf Basis einer Liste aller ausgestellten Zertifikate der jeweiligen CA treffen. Alle ausgestellten Zertifikate werden in einem Verzeichnisdienst verwahrt. So wird die Kompromittierung einer CA verbunden mit einer Totalfälschung von Zertifikaten ausgeschlossen. Dieser Verzeichnisdienst, der alle ausgestellten Zertifikate verwaltet, muss besonders geschützt werden, so dass auch bei Kompromittierung des CA-Schlüssels die bereits ausgestellten Zertifikate ihre Gültigkeit bewahren. Im signaturgesetzkonformen Umfeld würden dann alle Zertifikate, die in diesem Verzeichnisdienst enthalten sind, trotz Kompromittierung des CA Schlüssels weiterhin gültig bleiben. Um im Fall einer Kompromittierung einer CA zu erkennen, wenn neue Zertifikate mit alten bereits vergebenen Seriennummern ausgestellt wurden, muss bei der Statusanfrage der Hash-Wert des angefragten Zertifikats enthalten sein. So werden gefälschte Zertifikate bei der Statusanfrage an den signaturgesetzkonformen Verzeichnisdienst als „unknown" enttarnt.

Zeitstempeldienst

Über einen Zeitstempeldienst (Time-Stamp Protocol, TSP) können Zeitstempel eingeholt werden, um so beispielsweise die Existenz eines bestimmten Dokuments zu einem definierten Zeitpunkt oder um den Zeitpunkt der Signaturerstellung eines Anwenders nachweisen zu können. Ein Zeitstempel ergibt sich aus der Signatur eines Zeitstempeldienstes auf den Hash-Wert eines Dokuments, d. h. es werden keine vertrauenswürdigen Daten übermittelt, da nur der Hash-Wert des zu zeitstempelnden Dokuments an den Zeitstempeldienst gesendet wird. Weitere Informationen finden sich bei [RFC3161].

Zeitstempel werden in der Praxis z. B. eingesetzt bei elektronischer Einreichung von Patentanträgen, Einreichung von elektronischen Angeboten auf eine Ausschreibung oder bei der Sicherung von Datensätzen in Archivierungssystemen.

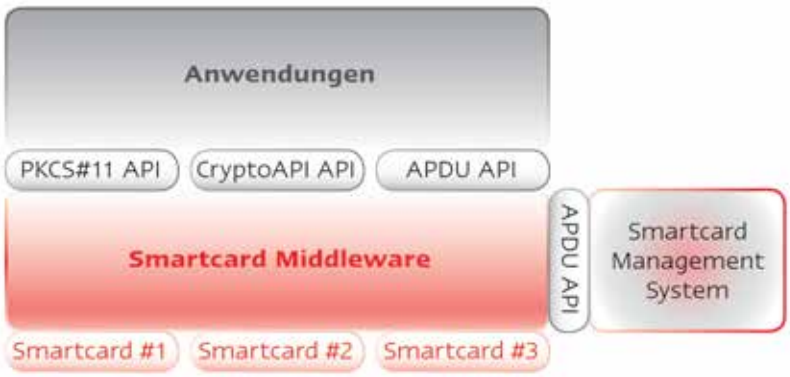
Personal Security Environment

Die Schlüssel und Zertifikate eines Benutzers müssen für ihn zugänglich gespeichert werden. Dies geschieht in einer persönlichen Sicherheitsumgebung, der sogenannten *Personal Security Environment* (PSE). Je nach angestrebtem Sicherheitsniveau kann ein Benutzer seine PSE in Software oder Hardware speichern.

Eine Speicherung des Schlüsselmaterials in Software ist nicht standardisiert, sondern von der Realisierung des jeweiligen Software-Herstellers abhängig. Anwendungen von verschiedenen Herstellern können daher in der Regel nicht die gleiche Software-PSE verwenden, wobei inzwischen viele Anwendungen den Microsoft Certificate Store unterstützen. Doch auch bei einer proprietären Speicherung des Schlüsselmaterials unterstützen die meisten Produkte ein standardisiertes Format zum Austausch des Schlüsselmaterials. Somit können existierende Schlüssel und Zertifikate aus einer Anwendung exportiert und in eine andere Anwendung wieder importiert werden. Dies ist dann notwendig, wenn Anwendungen jeweils ihre eigene PSE verwalten und diese das gleiche Schlüsselmaterial enthalten sollen.

Bei der Speicherung in Hardware sollten die Schlüssel möglichst schon auf der Smartcard oder dem USB-Token generiert werden, so dass der private Schlüssel niemals außerhalb der Hardware vorliegt. Im Folgenden werden Smartcards und USB-Token unter dem Begriff Hardware-Token zusammengefasst. Ein Hardware-Token zeichnet sich u. a. dadurch aus, dass der private Schlüssel nicht ausgelesen werden kann. Der Zugriff auf Hardware-Token ist standardisiert, so dass eine Vielzahl unterschiedlicher Anwendungen darauf zugreifen kann. Außerdem ist durch die Standardisierung auch gewährleistet, dass ein Wechsel des Hardware-Tokens möglich ist, ohne die Implementierung der Anwendung ändern zu müssen.

Abbildung 12.7: Schnittstellen zwischen Anwendung und Smartcard



In der Praxis weit verbreitet sind zwei alternative Schnittstellen, über die eine Anwendung auf ein Hardware-Token zugreifen kann: Entweder verwendet sie die PKCS#11-Schnittstelle und einen entsprechenden PKCS#11-Treiber für den Zugriff auf das Hardware-Token oder sie verwendet den Microsoft-Standard der Crypto-API, der über einen Cryptographic Service Provider (CSP) auf das Hardware-Token zugreift. Neben diesen beiden Möglichkeiten kann eine Anwendung auch

direkt Hardware-Token-spezifische Kommandos (*Application Protocol Data Unit*, APDU) an das Hardware-Token schicken. Diese APDU- Schnittstelle nutzt beispielsweise auch ein Smartcard-Managementsystem zur Personalisierung von Smartcards. Die verschiedenen Schnittstellen sind in Abbildung 12.7 dargestellt.

Smartcard-Managementsystem

Werden Schlüssel auf Hardware-Token gespeichert, bietet es sich an, diese Token mit Hilfe eines Smartcard-Managementsystems zu verwalten. Diese Systeme gewinnen aktuell immer mehr an Bedeutung, wenn z. B. zusätzlich temporäre oder permanente Ersatzkarten benötigt werden oder Benutzer über sogenannte Self-Services[5] ihre Token selber verwalten sollen.

Mit der Einführung von Smartcards in einem Unternehmen ist es naheliegend, die Benutzeranmeldung am Betriebssystem auch auf Smartcards umzustellen[6]. Die Smartcard lässt sich gut mit einem Unternehmensausweis kombinieren. So kann ein Benutzer beispielsweise mit derselben Karte – die einen kontaktlosen (Legic oder Mifare Chip) und einen kontaktbehafteten Chip enthält – Zutritt zum Gebäude und Zugriff auf seine Anwendungen erhalten. Benötigt er diese Karte auch zum Bezahlen in der Kantine, so kann darüber hinaus sichergestellt werden, dass mit dem Ziehen der Smartcard der Bildschirm des Benutzers während der Mittagspause gesperrt und vor unberechtigten Zugriffen geschützt ist. Die meisten auf dem Markt existierenden Smartcard-Managementsysteme können sowohl kontaktbehaftete als auch kontaktlose Chips personalisieren und auch Karten bedrucken. Diese Integration von Sicherheitsmaßnahmen in Smartcard-Managementsystemen führt in einigen Unternehmen dazu, dass die Bereiche IT-Security und Unternehmenssicherheit, die vorher eher nebeneinander koexistierten, nun gemeinsame Interessen und Ziele verfolgen und verstärkt zusammenarbeiten.

Smartcard-Managementsysteme benötigen eine Vielzahl an Schnittstellen, um in die bestehende Infrastruktur und Prozesse einer Organisation effektiv eingebunden werden zu können. So müssen sie auf die Smartcard zugreifen, einen Kartendrucker ansteuern, ein Zertifikat bei einer CA beantragen und auf die Backend-Systeme zugreifen können, in denen die Benutzer verwaltet und Zutrittsberechtigungen vergeben werden.

Schlüsselerzeugung

Bei der Schlüsselerzeugung wird zwischen zentraler und dezentraler Schlüsselerzeugung unterschieden. Beide Verfahren haben Vor- und Nachteile, die im Anschluss an die Beschreibung der beiden Ansätze erläutert werden.

Bei der zentralen Schlüsselerzeugung werden die Schlüssel von einer zentralen Instanz (CA oder RA) erzeugt. Die Anwesenheit des Benutzers ist nicht erforderlich, aber möglich. Je nach Gestaltung des Prozesses erhält der Benutzer seine Schlüssel, Zertifikate und PIN auf sicherem Weg übermittelt oder direkt vor Ort ausgehändigt. Der Ablauf einer Zertifizierung mit zentraler Schlüsselerzeugung könnte wie folgt aussehen:

1. Der Benutzer geht zu einer CA.
2. Die CA stellt die Identität des Benutzers fest und erzeugt ein Schlüsselpaar (privater und öffentlicher Schlüssel).

5 Self-Services (oder deutsch: Selbstbedienungstechnologien) ermöglichen einem Benutzer beispielsweise das selbständige Rücksetzen seiner PIN.

6 Windows Smartcard Logon: Statt seines Windows Passworts gibt der Benutzer die PIN seiner Smartcard an. Die Authentifizierung basiert auf Zertifikaten.

3. Die CA erstellt ein Zertifikat für den Benutzer, das mit dem privaten Schlüssel der Zertifizierungsstelle unterschrieben ist.
4. Der Benutzer erhält seinen privaten Schlüssel, sein Zertifikat, das seinen öffentlichen Schlüssel enthält, und das Zertifikat der CA.
5. Die CA stellt das Zertifikat des Benutzers in ein allgemein zugängliches Verzeichnis.

Bei der dezentralen Schlüsselerzeugung werden die Schlüssel vom Benutzer selber erzeugt und nur der öffentliche Schlüssel zur Zertifizierung an die CA übermittelt. Der Ablauf einer Zertifizierung mit dezentraler Schlüsselerzeugung könnte beispielhaft so aussehen:

1. Der Benutzer erzeugt ein Schlüsselpaar mit öffentlichem und privatem Schlüssel.
2. Der Benutzer geht zur CA bzw. RA und übergibt seinen öffentlichen Schlüssel.
3. Die CA bzw. RA stellt die Identität des Benutzers fest und überzeugt sich, dass er den zu dem öffentlichen Schlüssel gehörenden privaten Schlüssel besitzt.
4. Die CA erstellt ein Zertifikat für den Benutzer, das mit dem privaten Schlüssel der CA unterschrieben ist.
5. Der Benutzer erhält sein Zertifikat und das Zertifikat der CA.
6. Die CA stellt das Zertifikat des Benutzers in ein allgemein zugängliches Verzeichnis.

Ein Vorteil der zentralen Schlüsselerzeugung ist, dass die Aufgabe der Schlüsselerzeugung aus der Verantwortung der Benutzer genommen ist und so für den Benutzer einfacher und für das Help Desk mit weniger Aufwand verbunden und damit kostengünstiger ist. Oftmals lassen sich auch die Prozesse für eine Schlüsselhinterlegung[7] leichter umsetzen als im Falle der dezentralen Schlüsselerzeugung. Bei der dezentralen Schlüsselerzeugung ist der Benutzer für die Erzeugung seiner Schlüssel selber verantwortlich, was zwar einerseits zu Problemen und Fehlern führen kann, andererseits aber auch mehr Sicherheit für den Benutzer bedeutet, wenn sein privater Schlüssel stets nur in seinem Besitz ist. So kann niemand in seinem Namen eine digitale Signatur leisten. Andererseits kann er, weil er das Verfahren kontrolliert, auch absichtlich ein „schwaches“ Schlüsselpaar erzeugen und hinterher von ihm geleistete Signaturen mit dem Argument abstreiten, der Schlüssel sei kompromittiert.

Schlüsseltrennung

Während man früher beim Einsatz von Public Key Infrastrukturen für alle Benutzer nur ein einziges Schlüsselpaar vorgesehen hatte, ist es heute gängige Praxis, zwei oder gar drei verschiedenen Schlüsselpaare für jeden Benutzer zu erzeugen, um Schlüssel nach ihrem Verwendungszweck zu trennen. Typischerweise gibt es einen Signatur-, einen Authentisierungs- und einen Verschlüsselungsschlüssel. Die Trennung der verschiedenen Schlüssel ist durch die verschiedenen Anforderungen der jeweiligen Anwendung gerechtfertigt, so kann beispielsweise ein Verschlüsselungsschlüssel in einem Unternehmen hinterlegt werden, der Signaturschlüssel hingegen soll stets nur im Besitz des Anwenders verbleiben. Weitere Unterscheidungsmerkmale können die Gültigkeitsdauer oder die ausstellende CA sein.

Key Recovery

Bei Einführung von Verschlüsselung in einem Unternehmen muss entschieden werden, ob ein Key Recovery (Schüsselhinterlegung) oder ein Data Recovery (siehe unten) realisiert werden soll.

7 Siehe dazu nachfolgenden Abschnitt zu Key Recovery

Verschlüsselte Daten müssen auch bei Nicht-Verfügbarkeit des privaten Schlüssels – z. B. wenn der Mitarbeiter sein Hardware-Token verliert oder wenn er aus dem Unternehmen ausgeschieden ist – noch entschlüsselt werden können.

Um einen Verschlüsselungsschlüssel wiederherstellen zu können, muss dieser hinterlegt werden – im Fall von öffentlichen Schlüsselverfahren also der private Anwenderschlüssel, der zur Entschlüsselung dient. Kann im Bedarfsfall auf ihn zurückgegriffen werden, können verschlüsselte Daten auch nach Schlüsselverlust wieder entschlüsselt werden. Dabei müssen sowohl die Schlüsselhinterlegung wie auch der Schlüsselwiederherstellungsprozess geeignet abgesichert sein, denn sie sind lohnende Angriffsziele mit hohem Schadenspotential. Hinterlegte Schlüssel müssen sicher verwahrt werden und dürfen nur unter sehr abgegrenzten Bedingungen verwendet werden. Z. B. könnte der Zugriff durch ein Vieraugenprinzip abgesichert werden.

Wenn die Entscheidung für Key Recovery fällt, müssen zweckspezifische Schlüsselpaare eingesetzt werden. Hinterlegt werden sollen nämlich nur Entschlüsselungsschlüssel. Auf keinen Fall sollen Signatur- oder Authentisierungsschlüssel außerhalb der Kontrolle der Inhaber rekonstruiert werden können. In Abhängigkeit der existierenden Prozesse können die Schlüssel entweder zentral bei der CA oder bei einer dritten vertrauenswürdigen Instanz oder dezentral beim Anwender hinterlegt werden. Bei einer dezentralen Hinterlegung muss organisatorisch sichergestellt werden, dass jeder Benutzer seinen privaten Entschlüsselungsschlüssel sicher hinterlegt und dieser im Bedarfsfall berechtigten Dritten zugänglich ist, z. B. durch eine Reserve-Smartcard und einen PIN-Brief im Tresor.

Data Recovery

Im Gegensatz zur Schlüsselhinterlegung werden beim Data Recovery die Daten für einen Dritten mit verschlüsselt, der diese im Bedarfsfall entschlüsseln kann. Für Data Recovery ist keine Hinterlegung von privaten Nutzerschlüsseln notwendig. Für eine Data Recovery-Lösung müssen dagegen in der Organisation ein oder mehrere globale Recovery Keys eingeführt werden, die für alle Verschlüsselungsoperationen als zusätzliche Empfänger verwendet werden. Alle Daten werden nicht nur für den eigentlichen Empfänger verschlüsselt, sondern zusätzlich auch für mindestens einen Recovery Key.

Voraussetzung für eine Data-Recovery-Lösung ist, dass alle Verschlüsselungsanwendungen in einem Unternehmen die Verschlüsselung für einen zusätzlichen Empfänger – den Recovery Key – unterstützen. Asymmetrischer Schlüsseltransport mit Hilfe von Public-Key-Verfahren erlaubt effiziente Realisierungen, da nicht die Nachricht selbst, sondern nur der Sitzungsschlüssel für die verschiedenen Empfänger verschlüsselt werden muss.[8] Die Verschlüsselung für diesen speziellen Empfänger sollte keinen Zusatzaufwand für die Benutzer hervorrufen und möglichst technisch erzwungen werden.

Nachteil dieses Ansatzes ist, dass externe Kommunikationspartner z. B. beim Einsatz von verschlüsselter E-Mail in der Regel den Recovery Key nicht kennen und nicht unterstützen. Folglich sind verschlüsselte Nachrichten von Externen zunächst einmal nicht mit dem Recovery Key entschlüsselbar, sondern müssen beim ersten Entschlüsseln innerhalb des Unternehmens zusätzlich für einen Recovery Key mit verschlüsselt werden.

Beim Data Recovery können der Benutzer und der Recovery Agent beide jeweils mit ihrem privaten Schlüssel die verschlüsselte Nachricht entschlüsseln. Der Recovery Key wie auch der Recovery-Prozess sind – ähnlich wie für Key Recovery – interessante Ziele für Angreifer und weisen ein hohes Schadenspotential auf. Daher muss der Einsatz von privaten Recovery Keys

8 Vgl. zu Details auch Abschnitt 11.7

geeignet abgesichert sein, z. B. durch ein Vieraugenprinzip. Für den oder die Recovery Keys ist auch ein spezielles Key Management vorzusehen, da sich im Falle eines Wechsels des Schlüssels oder eines Zugriffsberechtigten besondere Anforderungen ergeben können, um die Verfügbarkeit des Recovery-Prozesses für alle Datenbestände sicherzustellen.

12.2.5 Policies für Public Key Infrastrukturen

Die Policies einer PKI bilden die Grundlage zur Vertrauensbildung bei PKI-basierten Anwendungen. Sie geben einer sogenannten *Relying Party* Aufschluss darüber, wie viel Vertrauen sie in eine PKI und in die Glaubwürdigkeit eines Zertifikats haben kann. Die Relying Party ist der Nutznießer, der Zertifikate zur Verifikation von Signaturen, zur Authentifikation von Benutzern oder zur Verschlüsselung von Daten verwendet und diese Zertifikate mit Hilfe der PKI-Dienste überprüft.

In einer *Certificate Policy* werden von der CA die Zusicherungen für die Sicherheit ihrer Infrastruktur, für die Verfahren zur Registrierung der Benutzer, für das Zertifikatsmanagement, und die Überprüfung der Abläufe innerhalb der PKI sowie für Haftung, Schadensersatz und Datenschutz festlegt. Eine Certificate Policy kann dadurch auch Vorgaben für nachgeordnete Zertifizierungsstellen enthalten. Durch diese öffentliche Dokumentation kann eine Relying Party das Sicherheitsniveau der CA und somit das Maß an Vertrauen in die ausgestellten Zertifikate einschätzen.

Nähere Informationen zu Certificate-Policy-Dokumenten finden sich im „Certificate Policy and Certification Practices Framework“ [RFC3647] und Secorvo White Paper „Das Policy-Rahmenwerk einer PKI“ [WP15].

12.3 Standards im Bereich PKI

Die zentralen Standards und Spezifikationen für Public Key Infrastrukturen sind:

- X.509 Standard

Tabelle 12.1: Ausgaben und Versionen des X.509-Standards

X.509- Ausgabe	Schlüssel-zertifikat	Sperrliste	Attributzertifikat
1. Ausgabe: 11/1988	Version 1	Version 1	
2. Ausgabe: 11/1993	Version 2	Version 1	
3. Ausgabe: 08/1997	Version 3	Version 2	Version 1
4. Ausgabe: 03/2000	Version 3	Version 2	Version 2
5. Ausgabe: 08/2005	Version 3*	Version 2	Version 2

- PKIX-Standards
- PKCS-Standards
- Common PKI Spezifikationen

* Umbennennung des des KeyUsage-Bits „nonRepudiation“ in „contentCommitment“

12.3.1 X.509 Standard

Der X.509 Standard ist ein ITU-IT-Standard und definiert das Format für Schlüsselzertifikate, Attributzertifikate und Sperrlisten sowie ein Verfahren zur Verifikation des Zertifizierungspfades. Die aktuellen Versionen dieser standardisierten Datenformate sind in Tabelle 12.1 dargestellt[10].

12.3.2 PKIX-Standards

Da der X.509v3 Standard [X509] eine sehr generische und komplexe Datenstruktur für Zertifikate und CRLs definiert, treten in der Praxis bei einer Vielzahl von unterschiedlichen Anwendungen und Umgebungen Interoperabilitätsprobleme auf. Um den X.509v3 Standard für eine Internet-PKI anwendbar zu machen, hat daher die PKIX-Arbeitsgruppe der *Internet Engineering Task Force* (IETF) eine Reihe von Internet-Standards, sogenannte *Requests for Comments* (RFC), festgelegt, mit denen eine praxisgerechte und interoberable Implementierung von PKI-Objekten, -Prozessen und -Produkten möglich werden soll.

Im [RFC5280] wird ein Zertifikats- und CRL-Profil definiert. Es legt fest, welche Erweiterungen im Rahmen der Möglichkeiten von X.509 verwendet werden müssen, sollen oder nicht verwendet werden dürfen. Der [RFC3739] definiert das Profil für ein qualifiziertes Zertifikat. Dieses Profil kann durch nationale Regelungen für die Verwendung im Rechtsverkehr anerkannt werden.

Die PKIX-Arbeitsgruppe hat noch viele weitere Internetstandards (RFC) für den Bereich der Internet-PKI veröffentlicht. Nennenswert sind außer den PKIX-Profilen noch die PKIX-Protokolle, wie beispielsweise die operationalen Protokolle zur Abfrage von Zertifikaten und Statusinformationen (LDAPv3, OCSP und die Verwendung von FTP und HTTP zum Transport von PKI Operationen) sowie die Certificate-Management-Protokolle. Darüber hinaus stammen das Zeitstempeldienstprotokoll (Time-Stamp Protocol [RFC3161]), das Policy and Certification Practices Framework [RFC3647] und verschiedene Protokolle zur Verifikation von Zertifikaten, CRLs und Signaturen von der PKIX-Arbeitsgruppe. Weitere Informationen finden sich bei [PKIX].

12.3.3 PKCS-Standards

Die Public Key Cryptography Standards (PKCS) sind sogenannte Industriestandards, die in offenen Arbeitsgruppen von vielen Akteuren aus Industrie und Wissenschaft unter Federführung von RSA Inc. seit 1991 entwickelt wurden. Der Fokus der PKCS Standards liegt auf technischen Aspekten der PKI und Kryptografie. Die derzeit relevanten PKCS Standards sind:

- **PKCS#1:** Der *RSA Encryption Standard* findet Verwendung in PKI-Komponenten, die den RSA-Algorithmus ausführen. Der RSA-Algorithmus wird dabei in der Regel in einem kryptografischen Schema zusammen mit anderen Verfahren verwendet, um Sicherheitsdienste wie Verschlüsselung oder digitale Signatur zu realisieren. Für die Implementierung gibt es verschiedene Realisierungsvarianten, die mehr oder weniger erfolgreich angreifbar sind. PKCS#1 macht Vorschläge für die sichere Implementierung des RSA-Algorithmus. Der PKCS Standard #1 wurde im Februar 2003 fast wortgetreu mit nur einigen Korrekturen als IETF RFC 3447[11] veröffentlicht.
- **PKCS#7:** Der *Cryptographic Message Standard* (CMS) spezifiziert ein Daten-Austauschformat und wird dort verwendet, wo kryptografisch behandelte Objekte mit anderen ausge-

10 *http://www.itu.int/rec/T-REC-X.509/en*

11 Siehe dazu die „Übersicht zu Standards der Informationssicherheit“

tauscht werden, z. B. eine E-Mail, ein Dokument oder ein Zertifikat. Die neuste Version der in PKCS#7 definierten Cryptographic Message Syntax wird durch RFC 5652[12] standardisiert.

- **PKCS#10:** Der *Certification Request Syntax Standard* wird verwendet, um Zertifizierungsanfragen an eine Zertifizierungsstelle zu richten.
- **PKCS#11:** Mit dem *Cryptographic Token Interface Standard* wird eine Programmierschnittstelle für Anwendungsprogrammierer zur Verfügung gestellt, die Hardware-Token in ihrer Anwendungssoftware nutzen möchten.
- **PKCS#12:** Der *Personal Information Exchange Syntax Standard* definiert ein Datenformat, mit dem das gesamte Schlüssel- und Zertifikatsmaterial inklusive dem privaten Schlüssel passwortgeschützt und portabel zum Transport[13] in einer Datei gespeichert werden kann.
- **PKCS#15:** Der *Cryptographic Token Information Format Standard* wurde im Jahr 2004 in ISO/IEC 7816-15 übernommen. Er spezifiziert die Anwendungsstrukturen auf einem Hardware-Token, d. h. die Verzeichnisstruktur und die notwendigen Datenelemente. Diese Strukturen werden in der Regel beim Initialisieren auf das Hardware-Token aufgebracht und ermöglichen konformen Anwendungen – ohne Abhängigkeit von einem bestimmten PKCS#11 oder CSP Treiber – auf Daten wie den privaten Schlüssel oder Zertifikate, die auf dem Hardware-Token gespeichert sind, zugreifen zu können.

Weitere Informationen finden sich bei [PKCS].

Die PKCS-Standards kommen in verschiedenen Produkt-Klassen zum Einsatz. Beispielsweise verwenden die aktuellen Web-Browser die Standards PKCS#1, #7, #10, #11 und #12. Smartcards nutzen PKCS#1, #11 und teilweise auch PKCS#15. PKI-Core und Client-Software unterstützt in der Regel PKCS#1, #7, #10, #11, #12 und gegebenenfalls auch PKCS#15. Diese breite Unterstützung von PKCS Standards zeigt ihre hohe praktische Relevanz.

12.3.4 Common PKI Spezifikationen

Die Common PKI (vormals ISIS-MTT) Spezifikation stammt von T7[14] und TeleTrusT[15]. Sie ist historisch gewachsen aus der Industrial-Signature-Interoperability-Specification (ISIS) und der Mailtrust-Spezifikation (MTT). Die Common PKI ist – ähnlich wie die PKIX-Profile – ein Profil über international verbreitete und anerkannte Standards für digitale Signaturen, Verschlüsselung und Public Key Infrastrukturen. Bei der Erstellung wurden mehr als 30 Basisstandards berücksichtigt. Die Common PKI ist auf den deutschen Markt ausgerichtet und berücksichtigt auch die Anforderungen für die qualifizierte elektronische Signatur nach dem deutschen Signaturgesetz (SigG). Die aktuelle Version der Common PKI Spezifikation besteht aus den folgenden Teilen:

- Part 1: Certificate and CRL Profiles
- Part 2: PKI Management
- Part 3: Message Formats

12 Siehe dazu die „Übersicht zu Standards der Informationssicherheit“

13 PKCS#12 wird auch als Format verwendet für den Ex- und Import von eigenem Schlüsselmaterial in und aus verschiedenen Anwendungen.

14 Der T7 e.V. ist eine Arbeitsgemeinschaft von Trustcenterbetreibern und Zertifizierungsdiensteanbietern im Bereich qualifizierter elektronischer Signaturen nach dem deutschen Signaturgesetz.

15 TeleTrusT Deutschland e.V. ist ein gemeinnütziger Verein und ein nichtkommerzielles Netzwerk mit Mitgliedern aus Industrie, Wissenschaft, Forschung und öffentlichen Institutionen. Sein Ziel sind verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik.

- Part 4: Operational Protocols
- Part 5: Certificate Path Validation
- Part 6: Cryptographic Algorithms
- Part 7: Signature API[16]
- Part 8: XML Signature and Encryption Message Formats
- Part 9: SigG-Profile[17]

Weitere Informationen finden sich bei [ComPKI].

Zusätzlich zu der Common PKI Spezifikation stehen eine korrespondierende Testspezifikation und ein Testbed Prototyp zur Verfügung. Mit diesen können Hersteller und Prüflabore PKI Produkte auf Konformität mit der Common PKI Spezifikation testen. Wenn alle Anforderungen der Spezifikation erfüllt werden, kann das Common-PKI-Siegel beim Common-PKI-Board[18] beantragt werden. Dieses Siegel ist ein Nachweis für Interoperabilität von Common-PKI-konformen Produkten und Lösungen. In Deutschland ist das Common-PKI-Siegel obligatorisch im Bereich E-Government für die Sicherung der E-Mail-Kommunikation und den gesicherten Dokumentenaustausch.

12.4 Verknüpfung von Public Key Infrastrukturen

Wenn einzelne Organisationen sich ihre eigene interne Public Key Infrastruktur (PKI-Domäne) aufgebaut haben und nicht nur interne PKI-Anwendungen einsetzten wollen, stellt sich die Frage, wie Teilnehmer aus unterschiedlichen PKI-Domänen miteinander sicher kommunizieren können, wenn sie keine gemeinsame Root CA haben. Ziel dieser Überlegungen ist es, dass mehrere PKI zusammenarbeiten und die Teilnehmer aus allen beteiligten Domänen einander vertrauen können.

Cross-Zertifizierung

Eine mögliche Lösung zur Verknüpfung mehrer PKI stellt die sogenannte Cross-Zertifizierung dar, bei der Zertifizierungshierarchien miteinander verknüpft werden. Dabei wird die eine Root CA von der anderen zertifiziert und umgekehrt. Ein Cross-Zertifikat unterscheidet sich in seiner Form nicht von einem untergeordneten CA-Zertifikat, d. h. es lässt in Struktur und Aufbau keinen Unterschied zu einem normalen Zertifikat erkennen. Cross-Zertifikate haben die zusätzliche Eigenschaft, dass sie einseitig oder beidseitig zwischen zwei CAs ausgestellt werden können.

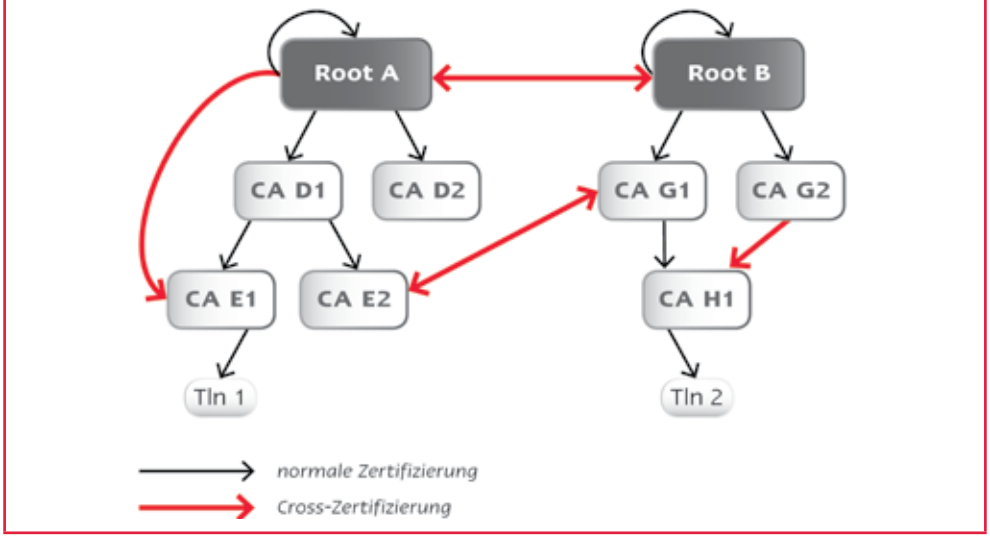
Theoretisch können mit einer Cross-Zertifizierung nicht nur die obersten Knoten, die Root CAs, miteinander verbunden werden: Prinzipiell könnten Cross-Zertifikate auch dafür genutzt werden, um Zertifizierungspfade (Zertifikatsketten) zu verkürzen. In der Praxis führen solche zusätzlichen Zertifikatspfade allerdings zu einer komplexeren Verifikation von Zertifikaten: Zunächst muss nämlich aus dem Graphen (siehe Abbildung 12.8) ein Zertifikatspfad ausgewählt werden. Cross-Zertifikate erhöhen die Zahl der möglichen Pfade, die nachverfolgt werden können. In jedem der möglichen Pfade können ein oder mehrere gesperrte Zertifikate auftreten, so dass dieser Zertifizierungspfad wieder verworfen werden muss. Daher werden in der Regel Cross-Zertifizierungen nur auf der Root-Ebene der PKI-Domänen durchgeführt.

16 Ersetzt den früheren Part 7 „Cryptographic Token Interface“ der Version 1.1

17 Bis Version 1.1 kein eigenständiger Part, sondern nur als Profile: „SigG-conforming Systems and Applications“

18 *http://www.t7ev.org/ws/T7-de/Common-PKI*

Abbildung 12.8: Cross-Zertifizierung



European Bridge CA

Eine Alternative zu Cross-Zertifikaten stellt in Europa die *European Bridge CA* (EB-CA) dar. Diese EB-CA stellt keine Zertifikate zur Verbindung von PKI-Inseln aus, sondern verteilt eine signierte Liste von geprüften und anerkannten Root-Zertifikaten an alle ihre Mitglieder. Alle Mitglieder schließen einen Vertrag mit der EB-CA und verpflichten sich auf die Einhaltung von Mindestanforderungen, z. B. Verfügbarkeit von Certification Policy (CP)[19] oder Certification Practice Statement (CPS) und erfolgreich absolvierte Interoperabiltitätstests. Somit entfallen für die Mitglieder der EB-CA die Einzelvereinbarungen und Prüfungen mit jeweils allen anderen Mitgliedern. Sie erhalten die Liste der vertrauenswürdigen CAs und müssen diese in ihre PKI-Anwendungen als vertrauenswürdig integrieren. Dieser Aufwand für die technische Umsetzung zur Integration der externen Root-Zertifikate muss trotz Zertifizierung durch die EB-CA geleistet werden.[20]

Die EB-CA war ursprünglich eine Initiative der Deutschen Bank und der Deutschen Telekom. Heute wird sie vom Teletrust e.V. betrieben. Weitere Informationen finden sich bei [BRIDGE].

Verteilung von Root-Zertifikaten

Die wohl verbreiteteste Art, PKI-Domänen miteinander zu verknüpfen, ist die Verteilung der Root-Zertifikate. Dazu muss das eigene Root-Zertifikat sicher an die externen Kommunikationspartner und das Root-Zertifikat der externen Kommunikationspartner intern verteilt und als vertrauenswürdig anerkannt werden. Etwas hochtrabend wird diese Variante der Verknüpfung von PKI-Domänen auch als *Cross Recognition* bezeichnet.

Um das Zertifikat der eigenen Root CA an alle Kommunikationspartner zu verteilen, bieten sich verschiedene Möglichkeiten:

19 Die European Bridge-CA stellt eine Certificate Policy mit Anforderungen an Bridge-CA Teilnehmer bereit: *https://www.ebca.de/publikationen/*

20 Im Fall der Verknüpfung von PKI-Domänen über Cross-Zertifikate fällt dieser Aufwand dagegen nicht an.

- Aufnahme des eigenen Root-Zertifikats in gängige Browser. Zur Aufnahme ist ein WebTrust-Gütesiegel für Certification Authorities[21] erforderlich.
- Zertifizierung der eigenen Root CA durch eine CA, deren Zertifikat bereits in gängige Browser integriert ist. Diese Dienstleistung bietet beispielsweise RSA mit ihrem „RSA Keon Root Signing Service“ oder GeoTrust mit ihrem Root Signing „GeoRoot“.
- Das Root-Zertifikat wird zum Download im Internet bereitgestellt. Die Relying Party, die das Root-Zertifikat herunterlädt, muss dessen Fingerprint über einen zweiten, unabhängigen Kanal beziehen und geeignet prüfen, um sich von der Korrektheit des Root-Zertifikats zu überzeugen.

Um ein externes Root-Zertifikat intern zu verteilen, muss im aufwendigsten Fall eine Installation des Root-Zertifikats auf jedem einzelnen Client vorgenommen werden. Wenn möglich, sollte die Verteilung der externen Root-Zertifikate daher schon beim Ausrollen einer PKI-Anwendung erfolgen. Wenn die PKI-Anwendungen den Microsoft Certificate Store verwenden und im Unternehmen ein Active Directory (AD) im Einsatz ist, können die Root-Zertifikate vom Administrator automatisch an alle Anwender verteilt werden. Gleiches gilt bei Einsatz von Lotus Notes und dem Lotus Domino Directory; auch hier können die Zertifikate vom Administrator automatisch an alle Anwender verteilt werden. Andernfalls muss ein Anwender, sofern er die nötigten Rechte besitzt, die benötigten externen Root-Zertifikate selber im Internet herunterladen und in seine PKI-Anwendung importieren.

Um den Benutzern die Handhabung zu vereinfachen, sind in den gängigen Browsern schon eine Vielzahl an Root-Zertifikaten als vertrauenswürdige Sicherungsanker vorinstalliert. Diesen Root-Zertifikaten und allen weiteren von diesen Root CAs ausgestellten CA-Zertifikaten vertrauen die Benutzer automatisch und in aller Regel unbesehen. Es findet keine Überprüfung dieser CAs z. B. anhand ihrer Certificate Policies statt. Eine solche Prüfung kann nur manuell erfolgen und ist daher sehr aufwändig. So bleibt es bzgl. der Prüfung und Akzeptanz von Root-Zertifikaten bei dem Spagat zwischen Benutzerfreundlichkeit durch vorkonfigurierte Root-Zertifikate auf der einen Seite und hohem Sicherheitsbewusstsein mit manueller Prüfung von Certificate Policies auf der anderen Seite.

12.5 Langzeitarchivierung

Elektronische Langzeitarchivierung bezeichnet die Aufbewahrung elektronischer Informationen für mehr als zehn Jahre. Im Kontext digital signierter Dokumente stellen sich hierbei neue zusätzliche Herausforderungen, insbesondere bei qualifizierten elektronischen Signaturen als Ersatz im Falle eines Schriftformgebots: Der Sicherheitswert der digitalen Signatur muss für den gesamten Archivierungszeitraum erhalten bleiben, um die Beweiskraft der elektronischen Signatur zu gewährleisten[22].

Die Langzeitsicherung von qualifizierten elektronischen Signaturen ist nicht gesetzlich verankert, aber immerhin als Hinweis in SigG §6 „Unterrichtungspflicht“ enthalten: „*Der Zertifizierungsdiensteanbieter [...] hat den Antragsteller darauf hinzuweisen, dass Daten mit einer qualifizierten elektronischen Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.*“

Der Sicherheitswert digitaler Signaturen vermindert sich zum Einen durch die rasante technische Weiterentwicklung von Hard- und Software (Vernetzung, Rechenkraft) und zum Anderen durch

21 *http://www.webtrust.org/*

22 Für qualifizierte elektronische Signaturen gilt der gesetzliche Anscheinsbeweis nach § 371a ZPO.

die Fortschritte der Kryptanalyse. So gibt es verschiedene Gründe, warum eine digitale Signatur erneuert werden muss. Diese Gründe können sein, dass:

- eine Schwachstelle in einem verwendeten Hash-Algorithmus aufgedeckt wird
- die Länge der Hash-Werte nicht mehr den aktuellen Anforderungen entspricht
- eine Schwachstelle in einem verwendeten Signatur-Algorithmus aufgedeckt wird oder
- die verwendete Schlüssellänge bei der digitalen Signatur nicht mehr den aktuellen Anforderungen entspricht.

Um den Sicherheitswert von digital signierten Dokumenten zu erhalten, kann entweder das Langzeitarchiv die Sicherheit der archivierten Dokumente garantieren oder der Sicherheitswert der digitalen Signatur kann über Nachsignierung bzw. „Erneuerung" von Signaturen umgesetzt werden. Dafür muss die erneute Signatur nicht zwingend von dem ursprünglich Signierenden geleistet werden. Im einfachsten Fall kann dies mit einem Zeitstempel von einem Zeitstempeldienst erfolgen.

Müssten in einem Langzeitarchiv regelmäßig neue Zeitstempel für den Hash-Wert eines jeden archivierten Dokuments eingeholt werden, wäre dies sehr ineffizient. Daher sieht der in [RFC 4998] beschriebene Lösungsansatz zur Langzeitarchivierung ein baumbasiertes Verfahren vor, einen sogenannten *Hashtree*. Über alle archivierten Dokumente werden in einer Baumstruktur gemeinsame Hash-Werte im Archivierungssystem gebildet und ein einziger Archivzeitstempel für den Hash-Wert an der Wurzel des Baumes eingeholt, der alle Dokumente gemeinsam signiert. Dieser Zeitstempel wird bei Bedarf erneuert.

Abbildung 12.9: Beispiel für einen Hashtree

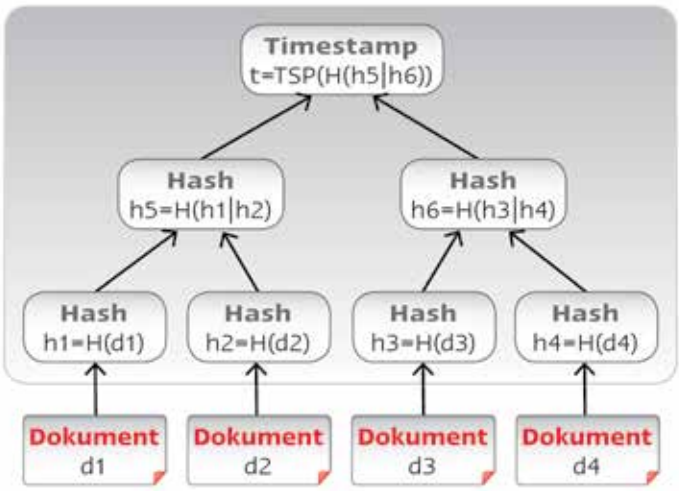


Abbildung 12.9 zeigt beispielhaft den Aufbau eines solchen Hashtrees. Die Blätter des Baumes bilden die Hash-Werte der einzelnen Dokumente. Auf den höheren Ebenen wird jeweils ein Hash-Wert über zwei Hash-Werte der darunter liegenden Ebene erstellt, d. h. pro Ebene wird die Anzahl der Hash-Werte auf die Hälfte reduziert. Der Zeitstempel t an der Wurzel des Baumes sichert in diesem Beispiel die archivierten Datenobjekte d1, d2, d3 und d4.

Wird ein archiviertes Dokument aus dem Archivierungssystem angefordert, so werden zusätzlich zum Originaldokument auch alle für die Zurückverfolgung des Hashtree-Weges benötigten Hash-

Werte vom Archivierungssystem zurückgeliefert, so dass die Überprüfung des Archivzeitstempels möglich ist. Bei einer erfolgreicher Verifikation des Zeitstempels ist der Nachweis gegeben, dass der Sicherheitswert und damit die Beweiskraft des angeforderten digital signierten Dokuments erhalten geblieben ist.

Dieser Lösungsansatz zur Langzeitarchivierung erfüllt zudem die Anforderungen des Datenschutzes zu Datensparsamkeit, da die Löschung von einzelnen archivierten Datenobjekten möglich ist, wenn diese nicht mehr erforderlich sind. Nur die Hash-Werte zu den gelöschten Datenobjekten müssen aufbewahrt werden, um jederzeit den Archivzeitstempel für den Hash-Wert an der Wurzel des Baumes verifizieren zu können.

Mit der technischen Richtlinie BSI-TR 03125 „Beweiswerterhaltung kryptografisch signierter Dokumente“ stellt das BSI einen Leitfaden zur Verfügung, der beschreibt, wie elektronisch signierte Daten und Dokumente über lange Zeiträume vertrauenswürdig gespeichert werden können. Konkret beschreibt diese technische Richtlinie einen Katalog von Anforderungen für eine beweiswerterhaltende Aufbewahrung elektronisch signierter Dokumente und Daten. Diese Anforderungen betreffen die Daten- und Dokumentenformate, das Speicherformat für Archivdatenobjekte sowie die Anwendungssysteme und Krypto-Module. Auf Grundlage der in dieser technischen Richtlinie definierten Prüfspezifikationen können Konformitätsprüfungen von IT-Produkten oder -Systemen zur Langzeitarchivierung durchgeführt werden.

Zusammenfassung

Die Verteilung und Verwaltung von öffentlichen Schlüsseln kann über ein Web of Trust dezentral organisiert oder mittels einer PKI zentral realisiert werden. Bei einer PKI werden die öffentlichen Schlüssel den Schlüsselinhabern über eine Art „elektronischen Personalausweis“ zugeordnet. Dieser Ausweis wird als Zertifikat bezeichnet. Die verschiedenen PKI-Komponenten und die Prozesse, die im Umgang mit Zertifikaten auftreten, müssen geeignet gestaltet werden. Die Regeln, nach denen dies geschieht, werden sinnvollerweise in Policy-Dokumenten festgelegt.

Für die Realisierung von PKI sind eine Vielzahl von Standards einschlägig. Neben dem X.509 Standard sind Internetstandards (RFCs), Public Key Cryptography Standards (PKCS) und in Deutschland – besonders wichtig im Behördenumfeld – die Common PKI Spezifikationen relevant.

Für einen organisationsübergreifenden Einsatz von öffentlichen Schlüsselverfahren müssen die einzelnen Public Key Infrastrukturen miteinander verknüpft werden. Diese Herausforderung muss hauptsächlich auf organisatorischer und rechtlicher Ebene zwischen den beteiligten Parteien bewältigt werden.

Literatur

[BRIDGE] *TeleTrusT: https://www.ebca.de/*

[BSI TR 03125] *BSI – Bundesamt für Sicherheit in der Informationstechnik (BSI):* BSI TR 03125 Beweiswerterhaltung kryptographisch signierter Dokumente, Februar 2011; *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_V1.1.pdf*

[ComPKI] *T7&Teletrust: http://www.t7ev.org/ws/T7-de/Common-PKI*

[PKCS] *RSA Laboratories: http://www.rsa.com/rsalabs/*
Zu den einzelnen Standards und ihren Aktualisierungen siehe die „Übersicht zu Standards der Informationssicherheit" in diesem Buch

[PKIX] *IETF: http://datatracker.ietf.org/wg/pkix/*

[RFC2560] *Myers, M.; Ankney, R.; Malpani, A.; Galperin, S.; Adams, C.:* X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP, Juni 1999

[RFC3161] *Adams, C.; Cain, P.; Pinkas, D.; Zuccherato, R.:* Internet X.509 Public Key Infrastructure – Time-Stamp Protocol (TSP), Aug. 2001

[RFC3647] *Chokhani, S.; Ford, W.; Sabett, R.; Merrill, C.; Wu, S.:* Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, Nov. 2003

[RFC3739] Santesson, S.; Nystrom, M.: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile, März; 2004

[RFC5280] *Cooper, D.; Santesson, S.; Farrell, S.; Boeyen, S.; Housley, R.; Polk, W.:* Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Mai 2008

[RFC5816] *Santesson, S.; Pope, N.*: ESSCertIDv2 Update for RFC 3161, März 2010

[RFC6277] *Santesson, S.; Hallam-Baker, P.:* Online Certificate Status Protocol Algorithm Agility, Juni 2011

[RFC6818] *Yee, P.:* Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Januar 2013

[WP15] *Barzin, P.; Kelm, S.:* Das Policy-Rahmenwerk einer PKI, Secorvo White Paper, März 2008; *http://www.secorvo.de/publikationen/secorvo-wp15.pdf*

[X509] *International Telecommunication Union:* Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks, ISO/IEC 9594-8:2005 (E), ITU-T Recommendation X.509, Aug. 2005