

dem empfangenen Fingerabdruck  $h(M)$  übereinstimmt. Ist  $h(M') = h(M)$ , dann gilt (zumindest mit überwältigender Wahrscheinlichkeit) aufgrund der Anforderungen, die an eine Hashfunktion gestellt werden, auch  $M = M'$ , die Nachricht ist also mit dem versendeten Original identisch.

Wendet Bob nun auf den Message Digest  $h(M)$  die Verschlüsselung *encrypt* mit seinem geheimen Schlüssel  $ks_B$  an, anstelle die vollständige Nachricht zu verschlüsseln, reicht es aus, zusammen mit der Originalnachricht  $M$   $encrypt(ks_B, h(M))$  anstelle von  $encrypt(ks_B, M)$  zu übertragen, um alle Anforderungen an eine digitale Signatur zu erfüllen. Die als Message Digest verwendete Funktion muß dazu allerdings die folgenden Voraussetzungen erfüllen, um als fälschungssicher gelten zu können:

- Aus einem gegebenen Message Digest Wert  $d$  ist es mit vertretbarem Aufwand nicht möglich, die originale Nachricht  $M$  zu rekonstruieren, für die gilt  $h(M) = d$ .
- Es ist mit vertretbarem Aufwand unmöglich, zwei unterschiedliche Nachrichten  $M$  und  $N$  zu finden, so daß gilt  $h(M) = h(N)$ .

Abb. 9.10 zeigt, wie eine mit einer digitalen Signatur über einen Message Digest versehene Nachricht versendet oder empfangen wird.

- Bob wendet zur Erzeugung des Message Digest die Hashfunktion  $h$  auf die zu versendende Nachricht  $M$  an und verschlüsselt  $h(M)$  mit der Verschlüsselungsfunktion *encrypt* und seinem geheimen Schlüssel  $ks_B$ .
- Bob versendet  $M$  zusammen mit  $encrypt(ks_B, h(M))$ .
- Alice wendet die Entschlüsselungsfunktion *decrypt* zusammen mit Bob's öffentlichem Schlüssel  $kp_B$  auf die empfangene digitale Signatur zu Bob's Nachricht  $encrypt(ks_B, h(M))$  an.
- Alice wendet die Hashfunktion  $h$  auf die empfangene Nachricht  $M'$  an und vergleicht, ob  $h(M') = decrypt(kp_b, encrypt(ks_B, h(M)))$  gilt.
- Sind die beiden Signaturen identisch, kann Alice davon ausgehen, daß die empfangene Nachricht tatsächlich von Bob stammt und auch während der Übertragung nicht verändert wurde.

Zur Erzeugung eines Message Digest wird heute in der Regel der von Ron Rivest entwickelte **MD5**-Algorithmus verwendet, der in RFC 1321 spezifiziert wurde, und der aus einem vorgegebenen Dokument eine 128 Bit langen Message-Digest berechnet. Ein weiterer Algorithmus, der speziell als Standard für die Kommunikation der US-Bundesregierung vorgeschrieben ist, ist der **Secure Hash Algorithm (SHA-1)**, der auf ähnlichen Prinzipien wie MD4, dem Vorgänger von MD5 beruht, und einen 160 Bit langen Message Digest erzeugt.

#### 9.2.4 Schlüsselverteilung und Zertifizierung

Sowohl symmetrische Verschlüsselungsverfahren mit geheimen Schlüsseln als auch asymmetrische Verschlüsselungsverfahren können nur zuverlässig funktionieren, wenn ein sicherer Austausch der Schlüssel gewährleistet ist. Müssen

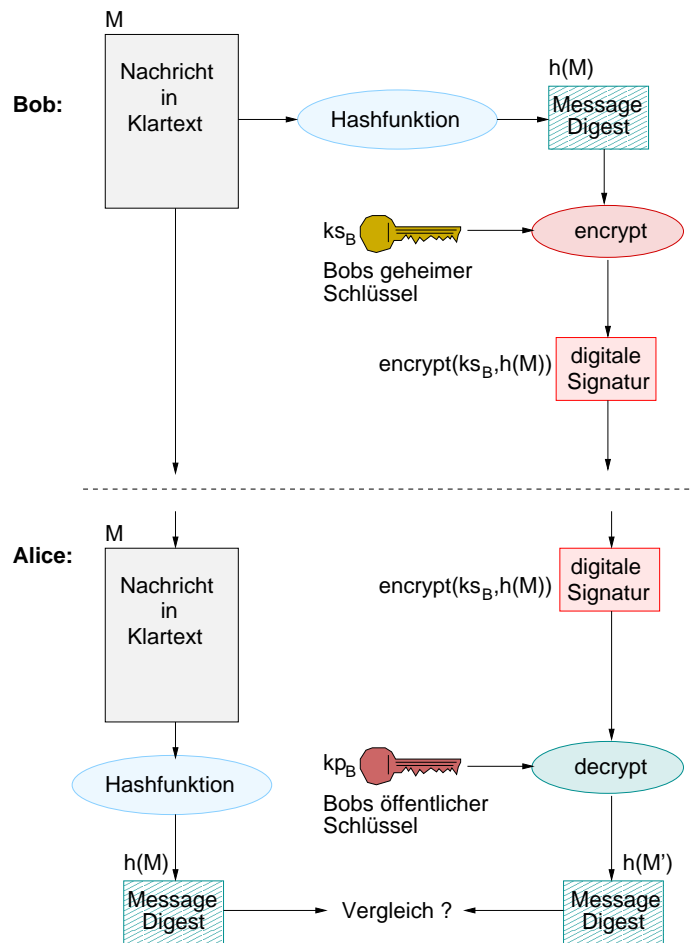


Abb. 9.10. Verwendung von digitaler Signatur und Message Digest

beim symmetrischen Verfahren jeweils die geheimen Schlüssel der beteiligten Kommunikationspartner ausgetauscht werden, die zur Entschlüsselung der versendeten Nachrichten notwendig sind, ist dies beim asymmetrischen Verfahren nicht notwendig. Hier muß statt dessen sichergestellt werden, daß der öffentliche Schlüssel eines Kommunikationsteilnehmers tatsächlich auch zu diesem gehört und nicht zu einem unberechtigten Dritten, der versucht, sich in eine vertrauliche Kommunikation einzuschleichen.

Dieser sichere Schlüsselaustausch wird durch die Einschaltung eines **vertrauenswürdigen Dritten (Trusted Intermediary, Trusted Third Party)** gewährleistet. Bei einem symmetrischen Verschlüsselungsverfahren, wird der vertrauenswürdige Dritte auch als **Schlüsselverteilzentrum (Key Distribution Center, KDC)** bezeichnet. Das KDC verwaltet die gemeinsamen

geheimen Schlüssel, die für eine sichere Kommunikation über ein symmetrisches Verschlüsselungsverfahren notwendig sind, so daß deren Verteilung zuverlässig und sicher erfolgt, ohne daß sich ein unberechtigter Dritter Zugang zu einem geheimen Schlüssel verschaffen kann. Bei einem asymmetrischen Verschlüsselungsverfahren dagegen muß für den öffentlichen Schlüssel eines Kommunikationsteilnehmers garantiert werden, daß er tatsächlich von diesem stammt. Der vertrauenswürdige Dritte, der dies gewährleisten soll, wird als **Zertifizierungsstelle (Certification Authority, CA oder Trust Center, TA)** bezeichnet. In der Regel bilden Zertifizierungsstellen eine Hierarchie mit einer Wurzelinstanz an der Spitze, verschiedenen untergeordneten Instanzen und den Nutzern. Eine derartige Hierarchie zusammen mit sämtlichen dazugehörigen organisatorischen Festlegungen (**Security Policy**) wird als **Public Key Infrastruktur (PKI)** bezeichnet.

**Schlüsselverteilzentrum (KDC).** Angenommen, Alice und Bob wollen über ein symmetrisches Verschlüsselungsverfahren miteinander kommunizieren. Allerdings haben sie keine Möglichkeit, den dazu notwendigen geheimen Schlüssel sicher auszutauschen. Dann müssen sie sich auf ein Schlüsselverteilzentrum (KDC) verlassen. Jeder Nutzer eines KDC muß sich dort registrieren, d.h. er hinterlegt bei der Anmeldung, bei der er seine Identität nachweisen muß, einen geheimen Schlüssel. Ein KDC verfügt also für jeden registrierten Nutzer über dessen geheimen Schlüssel.

Wie erlangen Alice und Bob, die beide beim KDC angemeldet sind, jetzt auf sichere Weise einen gemeinsamen geheimen Sitzungsschlüssel mit Hilfe des KDCs? Beide kennen anfangs jeweils nur ihre eigenen geheimen Schlüssel, d.h. Alice verfügt über den Schlüssel  $k_A$  und Bob über den Schlüssel  $k_B$ . Abb. 9.11 zeigt den Ablauf der Erzeugung und sicheren Verteilung eines gemeinsamen geheimen Sitzungsschlüssels für Alice und Bob.

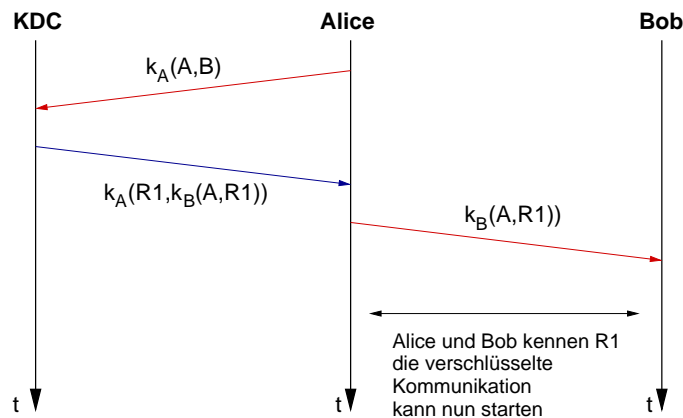
- Alice ergreift die Initiative und sendet eine mit  $k_A$  verschlüsselte Nachricht  $k_A(A, B)$  an das KDC, daß sie (A) gerne mit Bob (B) kommunizieren möchte.
- Das KDC verfügt über den geheimen Schlüssel  $k_A$  von Alice und kann daher Alice's Nachricht  $k_A(A, B)$  entschlüsseln. Daraufhin generiert das KDC einen zufälligen Schlüssel  $R1$ , der für die nachfolgende Kommunikation zwischen Alice und Bob als **einmaliger Sitzungsschlüssel** verwendet werden kann. Das KDC sendet dann eine mit  $k_A$  verschlüsselte Nachricht an Alice, die folgendes enthält:
  - den einmaligen Sitzungsschlüssel  $R1$  und
  - ein Wertepaar bestehend aus Alice's Namen  $A$  und dem Sitzungsschlüssel  $R1$ , das mit Bobs geheimen Schlüssel  $k_B$  verschlüsselt wird:  $k_B(A, R1)$ .

Das KDC sendet also die verschlüsselte Nachricht  $k_A(R1, k_B(A, R1))$  an Alice.

- Alice empfängt und entschlüsselt die Nachricht des KDC. Sie extrahiert den einmaligen Sitzungsschlüssel  $R1$  und speichert diesen für die nachfolgende

Sitzung mit Bob und leitet den zweiten Teil der Nachricht  $k_B(A, R1)$  an Bob weiter.

- Bob empfängt  $k_B(A, R1)$  und entschlüsselt die Nachricht mit seinem eigenen geheimen Schlüssel  $k_B$ . Bob erfährt dadurch den Kommunikationswunsch von Alice A und den gemeinsamen, einmaligen Sitzungsschlüssel R1. Die verschlüsselte Kommunikation zwischen Alice und Bob kann beginnen. Falls notwendig könnten Alice und Bob in der ersten Kommunikationsrunde nun sicher – verschlüsselt mit R1 – einen eigenen, auch dem KDC unbekannten gemeinsamen Schlüssel vereinbaren.



**Abb. 9.11.** Erzeugung und sichere Verteilung eines gemeinsamen geheimen Sitzungsschlüssels für Alice und Bob

Der am MIT in Massachusetts entwickelte Authentifikationsdienst **Kerberos**, der in RFC 1510 spezifiziert wird, liefert ein solches Schlüsselverteilzentrum für symmetrische Schlüssel. Über die o.a. Dienste des KDC hinaus verwaltet Kerberos zusätzlich noch Zugriffsrechte der angemeldeten Nutzer auf bestimmte Netzwerkressourcen und versieht den erteilten Sitzungsschlüssel mit einem Verfallsdatum, nach dem dieser von Bob nicht mehr akzeptiert wird.

**Zertifizierungsstelle (CA).** Eine Verschlüsselung mit Hilfe eines asymmetrischen Verschlüsselungsverfahrens birgt den Vorteil, daß kein sicherer Austausch von geheimen Schlüsseln erforderlich ist. Der jeweils notwendige öffentliche Schlüssel wird vom Eigentümer frei verteilt bzw. auf dessen WWW-Seite bereitgestellt. Allerdings liegt das Problem bei der asymmetrischen Verschlüsselung darin, daß der Kommunikationspartner sich darauf verlassen muß, daß der ihm dargebotene öffentliche Schlüssel auch tatsächlich der öffentliche Schlüssel seines Kommunikationspartner ist. Durch Vortäuschen einer falschen Identität kann die Authentifikation leicht unterlaufen werden (z.B. Man-in-the-Middle Angriff aus Abschnitt 9.2.2).

Asymmetrische Verschlüsselungsverfahren sind deshalb nur dann von Nutzen, wenn man sich auf die Authentizität der öffentlichen Schlüssel auch verlassen kann. Diese überprüfbare und fälschungssichere Bindung eines öffentlichen Schlüssels an einen Nutzer wird von einer **Zertifizierungsstelle** (CA) bezeugt.

Eine CA überprüft zunächst die Identität eines Nutzers (oder auch eines Rechners). Wie dabei die Identitätsprüfung vonstatten geht, ist der CA nicht vorgeschrieben. Erfolgt z.B. die Identitätsprüfung auf der Basis einer Email-Mitteilung, dann taugt das später ausgestellte Zertifikat nicht viel, da Email-Nachrichten leicht gefälscht werden können. Handelt es sich andererseits um eine staatlich anerkannte, die Normen des Signaturgesetzes erfüllende CA, dann kann man dem ausgestellten Zertifikat ohne Bedenken vertrauen. In jedem Fall muß die CA ihre eigenen Zertifizierungsrichtlinien bekannt geben, damit ein Nutzer die Qualität des Zertifikats und damit die Verlässlichkeit der übermittelten öffentlichen Schlüssel einschätzen kann.

Nachdem die CA die Identität eines Nutzers geprüft hat, erstellt sie ein **Zertifikat**, das den öffentlichen Schlüssel des Nutzers mit dessen Identität (Anschrift oder IP-Adresse) verbindet. Das Zertifikat wird von der CA digital signiert (siehe Abb. 9.12).

Um sicherzustellen, daß ein vom Nutzer übergebener öffentlicher Schlüssel tatsächlich mit seiner vorgegebenen Identität übereinstimmt, wird folgendermaßen vorgegangen.

- Wenn Alice mit Bob über ein asymmetrisches Verschlüsselungsverfahren kommunizieren möchte, sendet sie diesem ihre Nachricht zusammen mit ihrem Zertifikat (das Zertifikat kann auch von der CA angefordert werden).
- Die betreffende CA hat ihren eigenen öffentlichen Schlüssel allen Anwendern auf sichere Weise (z.B. Veröffentlichung an exponierter Stelle in einer renommierten Tageszeitung) zugänglich gemacht. Mit diesem öffentlichen Schlüssel der CA entschlüsselt Bob das Zertifikat von Alice.
- Kann Bob das Zertifikat entschlüsseln und stimmen die darin gemachten Angaben zur Identität mit denen von Alice überein, kann Bob sicher sein, daß er tatsächlich mit Alice kommuniziert und für die weitere Kommunikation deren öffentlichen Schlüssel verwenden.

### 9.3 Absicherung der Protokolle

Betrachtet man Sicherheitsziele und Sicherheitsanforderungen unter dem Blickwinkel des TCP/IP-Schichtenmodells, stellt sich die Frage, auf welcher Schicht welche Sicherheitsmaßnahmen am sinnvollsten und am effektivsten anzuwenden sind. Betrachten wir dazu die einzelnen Schichten des TCP/IP-Referenzmodells in absteigender Reihenfolge.

WWW

Kommunikation, Internetworking, Web-Technologien

Meinel, C.; Sack, H.

2004, XLII, 1178 S. In 2 Bänden, nicht einzeln erhältlich.,

Hardcover

ISBN: 978-3-540-44276-9