Frage & Antwort zum Thema PKI und Zertifikate

Jürgen Brauckmann, Leiter des PKI-Teams (Public Key Infrastructure) am DFN-CERT (Computer Emergency Response Team des Deutschen Forschungsnetzes) steht Prof. Andreas Hanemann Rede und Antwort.

Text: **Prof. Andreas Hanemann** (FH Lübeck)

Der Professor für Rechnernetze und Webtechnologien an der FH Lübeck, Andreas Hanemann, befragte den Experten des DFN-CERT im Rahmen seines MOOC (Massive Open Online Course) zum Thema Netzwerksicherheit. Das DFN-CERT beschäftigt sich insgesamt mit Sicherheitsthemen, die für das DFN-Netz und die angeschlossenen Hochschulen und Forschungseinrichtungen relevant sind. Das PKI-Team betreibt dabei eine Zertifizierungsstelle als Basis für die Zertifizierung in den Mitgliedseinrichtungen des DFN-Vereins. Da das Thema PKI auf allgemeines Interesse stößt, wollen wir Ihnen dieses Interview nun auch hier zugänglich machen.

Für welchen Zweck können Zertifikate aus einer PKI eingesetzt werden?

Obwohl die technische Basis von PKIs immer sehr ähnlich ist (asymmetrische Kryptographie, Zertifikate), können sehr unterschiedliche Einsatzszenarien abgebildet werden:

- Server können mit Zertifikaten beweisen, dass sie authentisch sind, und die Verschlüsselung von Verbindungen zu Clients ermöglichen. Diese TLS Serverauthentisierung ist z. B. großflächig im Einsatz bei Webservern mit dem Protokoll HTTPS und bei der sicheren Kommunikation zwischen Mail-Programmen und dem Mail-Provider über STARTTLS in SMTP/IMAP/POP.
- Personen oder Geräte können sich an einem Server anmelden (TLS Client-Authentisierung, z. B. verwendet im Webbrowser, oder 802.1X Geräteanmeldung im Netzwerk).
- E-Mails können mit S/MIME direkt Ende-zu-Ende, zwischen den Mailprogrammen der Kommunikationspartner, verschlüsselt werden.

Wie können Zertifikate für die Authentifizierung einer Person, eines Gerätes oder eines Servers verwendet werden?

Zertifikate verknüpfen einen Namen, z. B. eine E-Mail-Adresse oder eine Serveradresse, mit einem kryptographischen Schlüssel. Für eine erfolgreiche Authentisierung muss der Zertifikatinhaber zunächst nachweisen, dass er den zum präsentierten Zertifikat gehörenden geheimen kryptographischen Schlüssel besitzt. Nach diesem Nachweis muss der Prüfer untersuchen, ob der Name im präsentierten Zertifikat seinen Erwartungen entspricht (also z. B. dass der Server www.example.org tatsächlich ein Zertifikat mit dem Namen www.example.org übermittelt hat), und ob er dem Zertifikat und der ausgebenden Zertifizierungsstelle vertraut.

Wie wird das Vertrauen in Zertifikate geprüft?

Hierzu werden Root-CAs verwendet (von Microsoft „Vertrauenswürdige Stammzertifizierungsstellen“ genannt, von Mozilla einfach nur „Zertifizierungsstellen“). In der

prüfenden Software sind diese Root-CAs konfiguriert, normalerweise über eine vom Hersteller vorbereitete Liste, oder manuell ergänzt durch den Nutzer. Beim Prüfvorgang wird getestet, dass das zu untersuchende Zertifikat von einer Zertifizierungsstelle unterhalb einer bekannten Root ausgestellt wurde. Falls ja, wird dem Zertifikat vertraut.

Bevor ein Hersteller eine Root-CA in seine Software aufnimmt, muss der Betreiber der Root-CA die Einhaltung von formalen Kriterien nachweisen. Für Zertifikate für TLS gibt es herstellerübergreifende Kriterien, die sogenannten Baseline Requirements des CA/Browser Forums. Für andere Zertifikattypen gibt es nur herstellereigene Regeln.

Damit die Vertrauenswürdigkeit einer PKI sichergestellt wird, werden regelmäßig Audits durchgeführt. Wer führt diese durch und wie ist der Ablauf?

Für PKIs, die über eine Root-CA in Softwareprodukten von Microsoft, Apple, Oracle, Google oder Mozilla direkt vertrauenswürdig sind, ist ein jährliches Audit Pflicht. Hierfür gibt es verschiedene zulässige Audit-Standards, von denen die am häufigsten verwendeten „WebTrust for Certification Authorities“ und „ETSI TS 102 042“ sind. Eine Prüfung nach diesen Standards kann nur durch eine anerkannte Stelle durchgeführt werden, die bei einer nationalen oder internationalen Akkreditierungsstelle für Auditoren registriert ist. In Deutschland vergibt beispielsweise die DakkS GmbH die Berechtigung für Audits nach ETSI TS 102 042. Für WebTrust ist die zuständige Akkreditierungsstelle das American Institute of Certified Public Accountants und CPA Canada.

Bei einem Audit wird zunächst der Dokumentationsstand des Gesamtsystems geprüft: Ist die Dokumentation der baulichen, organisatorischen und technischen Gegebenheiten vollständig und aktuell? Sind die dokumentierten technischen Maßnahmen ausreichend und entsprechen sie dem Stand der Technik?

Im Anschluss wird geprüft, dass die dokumentierten Maßnahmen nicht nur auf dem Papier stehen, sondern auch tatsächlich umgesetzt werden. Dies geschieht durch eine Vor-Ort-Inspektion, die von der räumlichen Situation bis hin zu einzelnen Firewall-Regeln alle Aspekte des Gesamtsystems umfasst. Der Auditor selbst wird übrigens auch noch einmal überprüft: Der Prüfbericht wird durch eine unabhängige Stelle innerhalb der Organisation des Auditors auf Schwachstellen und Mängel untersucht.

Welche Schritte sind notwendig, wenn ein Benutzer oder ein Serveradministrator ein Zertifikat der DFN-PKI erhalten möchte?

Je nach Einsatzszenario werden unterschiedliche Verfahren zur Ausgabe von Zertifikaten verwendet.

Ein Weg ist die Beantragung über den Webbrowser. Für Nutzerzertifikate wird ein Webformular ausgefüllt, bei dessen Übermittlung direkt im Browser des Nutzers ein geheimer kryptographischer Schlüssel erzeugt wird. Der Nutzer erstellt dann ein Antragsformular und meldet sich mit diesem Formular bei dem Teilnehmerservice seiner Einrichtung.

Für Serveradministratoren, die ein Zertifikat für einen Server nutzen möchten, ist der Weg ähnlich: Sie müssen in ihrer Serversoftware einen Zertifikatrequest erzeugen, diesen in einem Webformular eintragen und sich wiederum mit einem Antragsformular an den Teilnehmerservice der Einrichtung wenden.

Verfahren mit einem höheren Automatisierungsgrad, bei denen die Zertifikaterstellung z. B. in eine Chipkartenproduktion eingebunden ist, sind in der DFN-PKI aber auch schon seit vielen Jahren im Einsatz. Diese Verfahren müssen aber immer stark auf die jeweilige Einrichtung zugeschnitten sein.

Wichtig: Bei Nutzerzertifikaten ist in der DFN-PKI im Sicherheitsniveau „Global“ stets eine persönliche Identifizierung notwendig, da mit dem Zertifikat beispielsweise Prüfungsanmeldungen zuverlässig durchgeführt werden können sollen.

Zertifikate haben eine begrenzte Lebensdauer. Wie lange sind die Zertifikate üblicherweise gültig? Wie läuft die Erneuerung ab?

Zertifikate werden mit einem Ablaufdatum versehen, da die in ihnen enthaltenen Daten regelmäßig überprüft werden müssen. Nutzerzertifikate sind in der DFN-PKI im Sicherheitsniveau „Global“ aktuell 3 Jahre, Serverzertifikate 39 Monate gültig. Die Laufzeit richtet sich dabei nach Vorgaben aus internationalen Richtlinien für Serverzertifikate.

Für die Erneuerung hat es sich als zweckmäßig erwiesen, denselben Ablauf wie für die Erst-Beantragung durchzuführen.

Zertifikate müssen manchmal für ungültig erklärt werden, z. B. wenn der private Schlüssel entwendet wurde. Welche Mechanismen gibt es dafür?

Um ein Zertifikat für ungültig zu erklären, muss es zunächst bei der Zertifizierungsstelle (CA) als gesperrt markiert werden. Im nächsten Schritt muss diese Sperrinformation durch geeignete Protokolle an diejenigen übermittelt werden, die die Zertifikate prüfen. Hierfür stehen grundsätzlich drei verschiedene Mechanismen zur Verfügung:

- Eine Certificate Revocation List (CRL) ist eine komplette Liste aller gesperrten Zertifikate einer CA. Sie wird von der CA zum Download angeboten, und kann automatisiert durch die Aufnahme der URL in die Zertifikate bezogen werden. CRL können sehr groß werden (einige Megabyte), sodass der Abruf z. B. nicht bei jedem Aufruf einer sicheren Webseite durchgeführt werden kann.
- Online Certificate Status Protocol (OCSP) ist ein Protokoll, bei dem eine Software die CA über eine Einzelabfrage nach dem Gültigkeitszustand eines einzelnen Zertifikates befragen kann. OCSP ist in den meisten Situationen besser geeignet als CRLs, wird von den Browserherstellern aber trotzdem kritisiert. OCSP weist zum einen typischerweise eine Latenz von bis zu 300ms auf, was Softwarehersteller als großes Hindernis für schnelles Webbrowsen betrachten, und kann zum anderen nicht in allen Situationen zuverlässig genutzt werden, z. B. hinter Captive Portals.
- Als dritten Mechanismus, der eine wachsende Bedeutung hat, sind herstellerabhängige Verfahren zu nennen, bei denen Softwarehersteller gezielt einzelne Zertifikate auf eine eigene Blacklist setzen. Google hat hierfür vor einigen Jahren ein Verfahren namens CRL-Set entwickelt, Mozilla arbeitet an einem ähnlichen Verfahren. Größtes Problem ist hierbei, dass nur die vom Hersteller als „relevant“ erachteten Zertifikate auf die Blacklist gesetzt werden.

Bietet die DFN-PKI CRL und/oder OCSP an?

In der DFN-PKI ist für alle Zertifikate CRL und OCSP verfügbar.

Sind nach der Erfahrung des DFN-CERT die Überprüfungen durch Browser bei ungültigen Zertifikaten ausreichend (man liest hier, dass als Default-Einstellung bei Zertifikaten mit nicht ermittelbarem Status von vertrauenswürdigen Zertifikaten ausgegangen wird)?

Tatsächlich prüfen einige Browser inzwischen gar nicht mehr selbst den Sperrzustand von Serverzertifikaten über OCSP/CRL, z. B. Google Chrome und viele mobile Browser. Die meisten Browser versuchen eine Sperrprüfung per OCSP durchzuführen, stellen bei Nicht-Erreichbarkeit des OCSP-Responders aber trotzdem eine Verbindung her. Der DFN-Verein stellt eine Testseite zur Verfügung, mit der man testen kann, inwieweit Software die Prüfung von Sperrzuständen durchführt.

Der Hash-Algorithmus SHA-1 wurde in den vergangenen Jahren als immer unsicherer eingestuft, so dass ein Wechsel auf SHA-2 erfolgen muss. Wie wird ein solcher Übergang organisiert?

Hierbei muss man berücksichtigen, dass ein Hash-Algorithmus in vielen verschiedenen Kontexten verwendet wird. Ein Anwendungsfall ist z. B. die Signatur von E-Mails: Von der E-Mail wird mit dem Hash-Algorithmus ein wenige Byte großer Fingerabdruck erzeugt, der dann mit einem Signaturverfahren wie RSA-PKCS#1 signiert wird. Hier wäre ein Update des Mail-Programms von Sender und Empfänger notwendig, um SHA-2 zu nutzen.

Ein anderer Anwendungsfall betrifft die PKI-Betreiber: Die Signaturen unter Zertifikaten werden ebenfalls mit Hilfe eines Hash-Algorithmus erzeugt. Hier müssen dann zunächst neu ausgegebene Zertifikate mit dem neuen Algorithmus signiert werden. Je nach Anwendung müssen gegebenenfalls auch bereits im Einsatz befindliche Zertifikate ausgetauscht werden. Das betrifft insbesondere Webserver, da viele Webbrowser inzwischen mehr oder weniger deutliche Warnmeldungen bei SHA-1-Zertifikaten darstellen. Ab 2017 werden viele Webbrowser voraussichtlich gar keinen Zugriff

mehr auf Webserver erlauben, die noch mit einem SHA-1-Zertifikat ausgestattet sind.

Ein großes Problem ist immer die Rückwärtskompatibilität: Während Webbrowser durch Autoupdate-Funktionen inzwischen eine hohe Agilität aufweisen, gibt es viele Geräte, die jahrelang im Einsatz bleiben sollen und nicht unbedingt jeden Algorithmus unterstützen. Das betrifft sehr hochpreisige Systeme wie Load-Balancer oder VPN-Konzentratoren, die aus Kostengründen natürlich jeweils so spät wie möglich ersetzt werden sollen. Aber auch die Kompatibilität mit Geräten, die viel in Entwicklungsländern verwendet werden, ist immer ein Thema. Wenn dort große Teile der Bevölkerung mit nicht-aktuellen Devices auf das Internet zugreifen, stellen sich bestimmte Fragen nach technischem Fortschritt ganz anders. Wäre es z. B. vertretbar, dass ein Anbieter eines sozialen Netzwerkes seine Verschlüsselungsalgorithmen so umstellt, das große Teile der Bevölkerung aus Entwicklungsländern nicht mehr an dem Dienst teilnehmen können? Diese Frage veranlasst zur Zeit Facebook, über ein System nachzudenken, bei dem Verbindungen zu alten Geräten noch mit SHA-1 signierten Zertifikate abgesichert werden, neue Geräte aber sicherere SHA-2-Zertifikate nutzen.

E-Mail-Verschlüsselung mittels PGP gilt als relativ schwer bedienbar. In einem Artikel forderte J. Schmidt vom Heise-Verlag beispielsweise dieses nicht weiter zu nutzen und durch Alternativen zu ersetzen. Wie sieht man beim DFN-CERT die Situation?

Die klassische E-Mail-Verschlüsselung, die Ende-zu-Ende mit eigenen Schlüsseln von Absender und Empfänger arbeitet, gibt es seit fast 25 Jahren. In dieser Zeit konnte die Usability nicht so gesteigert werden, dass sie von „Normal-Benutzern“ mit für sie erträglichem Aufwand freiwillig verwendet wird. Das betrifft sowohl PGP als auch S/MIME.

Dessen ungeachtet können beide Verfahren sehr gut in relativ homogenen Benutzergruppen verwendet werden, wenn entweder eine genügend große Motivation der Teilnehmer da ist, oder aber Support, z. B. von einem Rechenzentrum, vorhanden ist. Damit sind sowohl PGP als auch S/MIME nach wie vor unabdingbar für sichere und verlässliche Kommunikation.

Wo Jürgen Schmidt Recht hat: PGP und S/MIME sichern normalerweise keine Alltagskommunikation ab und schützen keine Personen, die keine eigene große Motivation zur sicheren Nachrichtenübermittlung haben. Wie der großflächige erfolgreiche Einsatz von Verschlüsselungsverfahren bei diversen Instant Messenger Diensten (z. B. dem von Jürgen Schmidt angeführten iMessage von Apple) gezeigt hat, kann man Nutzern aber durchaus Kryptographie und sichere Kommunikation quasi „unterschieben“, ohne dass man sie zu dem relativ hohen Aufwand von S/MIME und PGP zwingt.

Dazu braucht es aber einen neuen Denkansatz ohne ständige Verweise auf die bestehenden, für diesen Einsatzzweck gescheiterten Verfahren. Leider hat noch niemand gezeigt, wie neue sichere Verfahren herstellerübergreifend und interoperabel eingeführt werden können. ◆