Für alle Fälle PKI

Mehr Sicherheit durch Zertifikate

Zahlreiche Anwender nutzen bereits das Angebot der DFN-PKI und haben ihre Zertifizierungsstelle an den DFN-Verein ausgelagert. So sind bis heute mehrere tausend Zertifikate für Nutzer und Server ausgestellt worden und bewähren sich seitdem im praktischen Einsatz. Dabei werden die Zertifikate oft nur für einen einzigen Zweck verwendet. Anhand von konkreten Nutzungsszenarien wird im Folgenden gezeigt, dass Zertifikate jedoch noch weit mehr leisten können.

Szenario 1: Signieren von E-Mails / Dokumenten

Durch die Verwendung von Zertifikaten können E-Mails und Dokumente mit einer digitalen Signatur versehen werden. Diese wird in erster Linie als Äquivalent für eine eigenhändige Unterschrift eingesetzt. Um eine digitale Signatur zu erzeugen, benutzt der Verfasser eines Dokuments sein Zertifikat und seinen dazugehörigen privaten Schlüssel. Der Empfänger kann dann anhand dieses Zertifikats die digitale Signatur überprüfen. Da das Zertifikat die Identität des Verfassers bestätigt, wird die Authentizität des signierten Dokuments und damit dessen Urheberschaft bestätigt.

Daneben wird mit einer digitalen Signatur sichergestellt, dass der Inhalt einer E-Mail oder eines Dokuments nach dem Signieren nicht verändert wurde. Als großes Anwendungsgebiet erweist sich das Signieren von E-Mails. E-Mails ohne Signatur sind nicht fälschungssicher und es kann technisch relativ leicht ein falscher Absender vorgetäuscht werden. Zudem werden E-Mails grundsätzlich im Klartext übertragen, was bedeutet, dass Nachrichten auf dem Übertragungsweg unbemerkt verändert werden können. Mit dem Einsatz von Zertifikaten, die die Authentizität des Verfassers gewährleisten und Änderungen am Dokument erkennen lassen, können diese Probleme einfach und wirkungsvoll gelöst werden.

In der Praxis gestaltet sich die Verwendung von digitalen Signaturen in vielen E-Mail Programmen wie z.B. Mozilla Thunderbird sehr einfach. Ist das Zertifikat inklusive des privaten Schlüssels einmal installiert, können E-Mails beim Versenden automatisch digital signiert werden. Über die Einstellungen lässt sich zudem festlegen, ob standardmäßig alle E-Mails unterschrieben werden oder ob der Verfasser gezielt nur einzelne E-Mails digital signieren möchte. Der Empfänger erkennt durch ein grafisches Symbol in Form eines Stifts die Gültigkeit der Signatur in der empfangenen E-Mail. Durch einen Klick auf dieses Symbol kann auch das Zertifikat des Absenders angezeigt werden (Abbildung 1). Wenn der Inhalt der E-Mail auf dem Übertragungsweg verändert wurde oder dem Zertifikat des Absenders nicht vertraut wird, wechselt das Symbol zu einem zerbrochenen Stift, so dass der Empfänger immer erkennen kann, ob Inhalt und Absender authentisch sind.

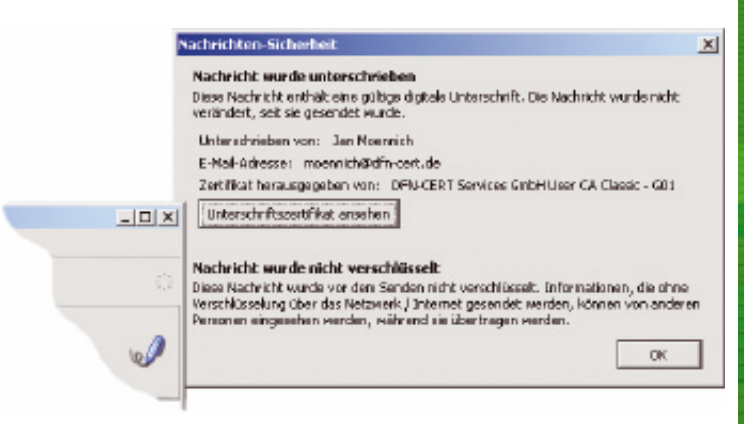

Abbildung 1: Prüfung einer digital signierten E-Mail

Auch einzelne Dokumente lassen sich so schützen. So bietet z.B. das Programm Adobe Acrobat eine Funktion an, um PDF-Dokumente digital zu signieren. Beim Lesen des Dokuments im Adobe Reader wird die Signatur verifiziert und deren Details werden angezeigt. Zusätzlich kann der Adobe Reader die Signatur als eine Art Stempel im Dokument selbst anzeigen (Abbildung 2), so dass der Hinweis auf eine digitale Signatur bei einem Ausdruck auch sichtbar gemacht werden kann.

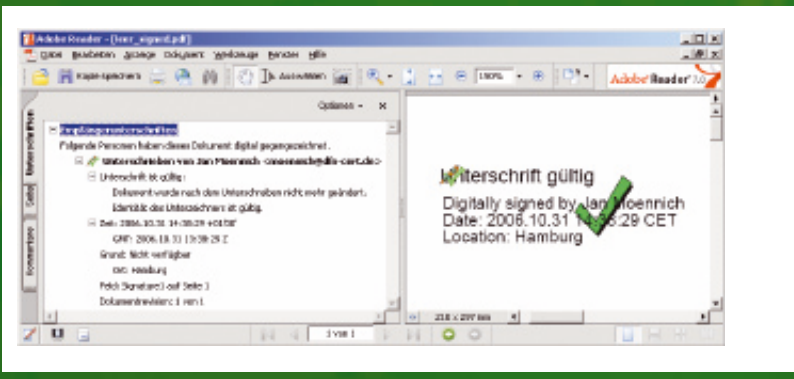

Abbildung 2: Digitale Signatur in einem PDF-Dokument

Szenario 2: Verschlüsseln von E-Mails / Dokumenten

Mit der Verschlüsselung von E-Mails oder Dokumenten wird die Privatsphäre von Personen und die Vertraulichkeit von Dokumenten und Nachrichten sichergestellt. Dabei wird ein Klartext durch die Verschlüsselung mit einem öffentlichen Schlüssel in einen Geheimtext umgewandelt, der nur mit dem entsprechenden privaten Schlüssel wieder in den Klartext zurückverwandelt werden kann. Damit ist es für Dritte, die nicht im Besitz des privaten Schlüssels sind, nicht möglich, den Geheimtext zu interpretieren, so dass der Text auch über unsichere Netzwerkverbindungen geschützt versendet werden kann.

Die Verschlüsselung von E-Mails gestaltet sich mit aktuellen E-Mail Programmen sehr einfach, so kann eine Nachricht vor dem Versenden durch nur einen Klick verschlüsselt werden. Dazu wird das Zertifikat des Empfängers einer verschlüsselten E-Mail benötigt. Programme wie Mozilla Thunderbird können die Suche nach einem Empfängerzertifikat vor dem Senden einer Nachricht automatisch und transparent für den Nutzer durchführen. Für die automatische Suche nach Zertifikaten der DFN-PKI muss unter „Extras", „Adressbuch" einmal ein neues LDAP-Verzeichnis mit den folgenden Daten angelegt werden: Hostname: ldap.pca.dfn.de, Basis-DN: o=DFN-Verein, c=DE, Port: 389, Suchfilter: (objectclass=*). Hierdurch können E-Mails an Empfänger aus dem Verzeichnis verschlüsselt werden, ohne dass deren Zertifikate vorher manuell installiert werden müssen.

Für die Verschlüsselung wird zunächst überprüft, ob das Zertifikat gültig ist und damit der darin enthaltene öffentliche Schlüssel wirklich dem Empfänger zuzuordnen ist. Dann wird die Nachricht mit dem öffentlichen Schlüssel aus dem Zertifikat verschlüsselt und an den Empfänger verschickt. Dieser kann als einziger mit seinem privaten Schlüssel die Nachricht wieder in den Klartext umwandeln.

Jan Mönnich
DFN-PCA
moennich@dfn-cert.de

Dr. Marcus Pattloch
DFN-Verein
pattloch@dfn.de

Gerti Foest
DFN-Verein
foest@dfn.de

Auch auf Dateien lässt sich die Verschlüsselung anwenden. So existiert beispielsweise das frei verfügbare Programm „Cryptonit“ (www.cryptonit.org), mit dessen Hilfe Dateien auf einfache Art und Weise verschlüsselt werden können (Abbildung 3). An dieser für Windows und Linux verfügbaren Software ist besonders hervorzuheben, dass sie als „Single-Executable“ ausgeliefert wird und damit keine Installationsprozedur durchlaufen werden muss. Unter Windows existiert weiterhin z.B. noch das EFS (Encrypted File System), mit dem der Inhalt von ganzen Verzeichnissen oder kompletten Laufwerken verschlüsselt werden kann.

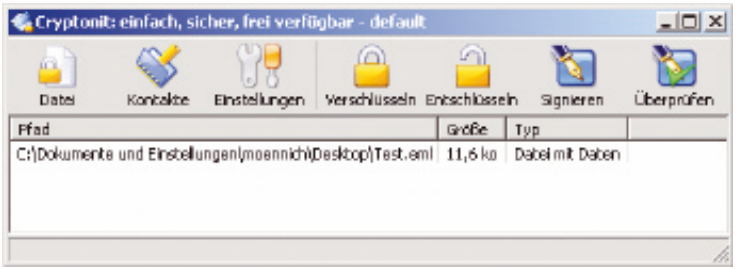

Abbildung 3: Verschlüsselung von Dateien

Szenario 3: Authentisierung von Nutzern

Nur der Inhaber eines Zertifikats ist im Besitz des dazugehörigen privaten Schlüssels. Deshalb kann auf dieser Basis auch eine Authentisierung zur Überprüfung der Berechtigung eines Nutzers vorgenommen werden. Der Nutzer sendet bei einer solchen sogenannten „Client-Authentisierung“ sein Zertifikat an einen Server und beweist (durch eine digitale Signatur), dass er im Besitz des privaten Schlüssels zu diesem Zertifikat ist. Der Server verifiziert das Zertifikat des Nutzers und kann diesem daraufhin den Zugang gewähren oder ihn ablehnen.

Die Client-Authentisierung kann z.B. für den Zugang zu geschützten Webseiten genutzt werden. Ein Webserver kann so konfiguriert werden, dass dieser von einem Nutzer zwingend ein Zertifikat für den Zugang verlangt. Die meisten Browser unterstützen bei dem Zugriff über das HTTPS-Protokoll diese Authentisierung durch ein Nutzerzertifikat. Da in dem Nutzerzertifikat bereits Daten über die Person enthalten sind, muss kein Nutzername mehr eingegeben werden. Durch die Verwendung des privaten Schlüssels ausschließlich auf der Seite des Nutzers, geht bei dieser Form der Authentisierung niemals ein Passwort über das Netzwerk.

Der Nutzen einer solchen Authentisierung kann am Beispiel des DFN-Webservers deutlich gemacht werden. Für Vertreter in der DFN-Mitgliederversammlung, Mitglieder des Verwaltungsrats und andere Gremien des DFN-Vereins gibt es auf dem DFN-Webserver Bereiche, die nur der jeweiligen Personengruppe zugänglich sind. Die Zugangskontrolle erfolgt für diese Bereiche „klassisch“ über Nutzername und Passwort. Mitglieder dieser DFN-Gremien können sich aber auch mit einem Zertifikat der DFN-PKI ausweisen. Damit entfällt die nicht selten notwendige Suche nach dem richtigen Passwort oder die Rückfrage beim DFN-Verein. Ein Klick auf die gewünschte Seite führt dann ohne weitere Interaktion zum richtigen Ziel.

Es gibt eine Reihe weiterer Anwendungen, die eine Client-Authentisierung durch Zertifikate akzeptieren. Wenn ein Zertifikat mit privatem Schlüssel auf einem Krypto-Token gespeichert ist, kann z.B. eine Nutzeranmeldung an einem Betriebssystem außer über Nutzernamen und Passwort auch über ein Zertifikat erfolgen. Diese Form der Anmeldung ist auch für den Zugang zu einem VPN oder zu anderen Netzwerkanwendungen möglich.

Szenario 4: Authentisierung von Webservern

Eine weit verbreitete Anwendung von Zertifikaten ist die Authentisierung von Webservern durch Zertifikate über das HTTPS-Protokoll. Dafür weist sich ein Webserver vor der eigentlichen Datenübertragung durch ein Zertifikat aus, das dem Client präsentiert wird. Durch die Verwendung einer digitalen Signatur beweist der Server, dass er im Besitz des privaten Schlüssels zu dem Zertifikat ist und damit die Identität hinter dem Zertifikat darstellt. Dadurch ist für den Client sichergestellt, dass er mit dem richtigen Webserver verbunden ist.

Ein weiterer Vorteil der Verbindung über das HTTPS-Protokoll besteht darin, dass der gesamte Netzwerkverkehr zwischen Client und Server verschlüsselt wird. Dabei wird ein zufällig generierter Sitzungsschlüssel verwendet, der nur den beiden Kommunikationspartnern bekannt ist. Dadurch können auch sicherheitskritische Informationen über ein unsicheres Netzwerk übertragen werden.

Diese Anwendung ist vor allem für Webanwendungen geeignet, in denen kritische Daten wie z.B. Kreditkartennummern oder andere personenbezogene Daten über das Internet gesendet werden. Auch können über eine solche Verbindung ohne Bedenken Passwörter im Klartext übertragen werden, da der gesamte Datenstrom inklusive der Daten im Kopf der Nachrichten verschlüsselt übertragen wird.

Fazit

Es existieren bereits viele Anwendungen, in denen Zertifikate sinnvoll integriert werden können, um die Sicherheit bezüglich der Authentizität und der Vertraulichkeit von Daten zu erhöhen. Die aktuellen Entwicklungen zeigen, dass die in der DFN-PKI verwendeten X.509 Zertifikate in Zukunft als ein universelles Mittel sowohl für die Verschlüsselung als auch für die Authentisierung eingesetzt werden können. Der Aufwand für den Nutzer ist häufig gering, da immer mehr aktuelle Anwendungen eine Unterstützung von Zertifikaten bieten.

Auch die Ausstellung von Zertifikaten ist durch die Möglichkeit der Auslagerung einer eigenen Zertifizierungsstelle an den DFN-Verein stark vereinfacht. Die ausgestellten Zertifikate enthalten u.a. immer den Namensraum der Einrichtung, sind voll standardkonform und können für alle Anwendungszwecke inklusive der oben genannten Szenarien eingesetzt werden. Die Auslagerung einer Zertifizierungsstelle im Rahmen der DFN-PKI ist im Dienst DFNInternet enthalten und kann damit von DFN-Anwendern ohne zusätzliches Entgelt genutzt werden. Alle Informationen zur DFN-PKI finden Sie unter www.dfn.de/pki. Für Rückfragen stehen wir unter pki@dfn.de zur Verfügung.

Hintergrund: Schlüssel und Zertifikate

Zertifikate basieren auf sogenannten asymmetrischen Verschlüsselungsverfahren. Bei diesen Verfahren wird ein Schlüsselpaar verwendet, das aus einem öffentlichen und einem privaten Schlüssel besteht. Während der öffentliche Schlüssel allgemein bekannt gemacht werden kann und zumeist sogar soll, verbleibt der private Schlüssel („das Geheimnis“) bei dessen Besitzer.

Alle Daten, die mit dem öffentlichen Schlüssel verschlüsselt werden, können mit Hilfe des privaten Schlüssels wieder in den Klartext entschlüsselt werden. Dieses Prinzip wird bei der Verschlüsselung von Daten angewendet. Die Daten können dabei mit dem für jeden zugänglichen öffentlichen Schlüssel verschlüsselt werden und sind dann nur für den Besitzer des privaten Schlüssels wieder rekonstruierbar.

Umgekehrt können alle Daten, die mit dem privaten Schlüssel verschlüsselt wurden, mit dem zugehörigen öffentlichen Schlüssel entschlüsselt werden. Dieses Prinzip wird z.B. bei der digitalen Signatur angewendet. Dabei wird eine Prüfsumme der zu signierenden Daten erstellt und mit dem privaten Schlüssel verschlüsselt. Wenn nun diese Prüfsumme mit dem frei zugänglichen (und von einer Zertifizierungsstelle bestätigten) öffentlichen Schlüssel aus einem Zertifikat entschlüsselt werden kann und der Prüfsumme der signierten Daten im Klartext entspricht, ist die Signatur verifiziert und es kann davon ausgegangen werden, dass die Daten nicht verändert wurden.

Jeder kann sich ein solches Schlüsselpaar aus öffentlichem und privatem Schlüssel selber erzeugen. Aber wie kann ein Dritter sicher sein, dass ein bestimmtes Schlüsselpaar auch wirklich zu einer bestimmten Person oder einem Computer gehört? Hier kommen Zertifikate ins Spiel, denn diese Bestätigung wird von Zertifizierungsstellen vorgenommen. Eine Zertifizierungsstelle überprüft die Daten und die Zugehörigkeit des öffentlichen Schlüssels zu einer Person, fasst diese zusammen und signiert die beiden Teile mit ihrem privaten Schlüssel.

Diese Kombination aus Daten einer Person, deren öffentlichen Schlüssel und der Signatur einer Zertifizierungsstelle, die diesen Zusammenhang bestätigt, bilden ein Zertifikat. Ein Zertifikat ist damit also eine Art „digitaler Ausweis“ mit integriertem Schlüssel, der von einer Zertifizierungsstelle überprüft und „gestempelt“ wurde. Jeder, der einer Zertifizierungsstelle vertraut, kann durch die digitale Signatur auch den Zertifikaten vertrauen, die von dieser ausgestellt wurden.

Um ein Zertifikat zu erhalten, muss bei einer Zertifizierungsstelle ein Zertifikatantrag gestellt werden. Zur Erzeugung dieses Antrags wird in der Regel das Schlüsselpaar bei dem Antragsteller selbst generiert. Dabei bleibt der private Schlüssel bei dem Antragsteller, der auch für dessen Speicherung und Verwaltung verantwortlich ist. Deshalb ist es diesem dringend zu empfehlen, eine Datensicherung des privaten Schlüssels durchzuführen. Für eine solche Sicherung eignet sich die Speicherung des Zertifikats inklusive des privaten Schlüssels in einer sogenannten PKCS#12 Datei, die mit einem Kennwort gesichert ist. Die meisten Anwendungen (wie z.B. Browser und E-Mail Programme) verwenden ebenfalls einen kennwortgeschützten Speicher für private Schlüssel. Eine weitere Möglichkeit besteht in der Verwendung von sogenannten Crypto-Token, welche private Schlüssel ebenfalls kennwortgeschützt und nicht extrahierbar auf einer Hardwarelösung (z.B. in Form eines USB-Sticks) speichern.

Wenn der private Schlüssel zu einem Zertifikat entwendet oder verloren wird, muss der Besitzer einen Antrag zur Sperrung des Zertifikats bei der Zertifizierungsstelle einreichen. Die Seriennummer des Zertifikats wird dann in einer Sperrliste aufgenommen, die von der Zertifizierungsstelle digital signiert und regelmäßig veröffentlicht wird. Diese Sperrlisten werden von den Anwendungen bei der Überprüfung eines Zertifikats berücksichtigt.

Zertifikate sind im Gegensatz zu dem privaten Schlüssel für die Öffentlichkeit gedacht. Normalerweise wird ein Zertifikat veröffentlicht, damit der öffentliche Schlüssel darin von anderen Personen für die Verschlüsselung von Daten und die Überprüfung von Signaturen benutzt werden kann. Deshalb können Zertifikate ungesichert im Klartext übertragen werden.

Ein Zertifikat ist von einer Zertifizierungsstelle signiert, deren Zertifikat wiederum von einer höheren Zertifizierungsstelle signiert sein kann. Dadurch entsteht eine „Kette“, in der ein Anwender immer der obersten Zertifizierungsstelle vertrauen muss. Diese oberste Zertifizierungsstelle hat ihr Zertifikat selbst signiert und wird auch „Wurzel-Zertifizierungsstelle“ genannt.