FORSCHUNGSZENTRUM JÜLICH GmbH

Jülich Supercomputing Centre
52425 Jülich, ☎ (02461) 61-6402

Beratung Netzwerk, ☎ (02461) 61-6440

Technische Kurzinformation

FZJ-JSC-TKI-0365
Martin Sczimarowsky
06.02.2017

JuNet/INTERNET
Einsatz von X.509 – Zertifikaten

1. Einleitung

Ohne den Einsatz von Verschlüsselungsverfahren ist die Übertragung von Informationen über das Internet aufgrund der Abhörbarkeit der Netze und der Manipulierbarkeit der Inhalte unsicher. Dienste wie das Web oder Mail bieten von sich aus weder Vertraulichkeit noch Möglichkeiten, sich beispielsweise von der Authentizität von Servern oder der korrekten Urheberschaft einer Nachricht zu überzeugen. Dieser Mangel kann mit dem Einsatz sogenannter **public-key**-Verfahren beseitigt werden.

2. Sichere E-Mail: digitale Signatur und Verschlüsselung

In diesem Abschnitt soll das Verfahren am Beispiel von E-Mail kurz erläutert werden.

Grundlage von **public-key**-Verfahren ist ein Schlüsselpaar. Dieses hat die Eigenschaft, dass Information, die mit einem der Schlüssel kodiert wurde, mit dem jeweils anderen – und **nur** mit diesem – wieder entschlüsselt werden kann. Einer der beiden Schlüssel (private key) wird vom Eigentümer streng geheim gehalten, während der andere potentiellen Mail-Partnern frei zugänglich ist (public key). Ein solches Schlüsselpaar erlaubt beispielsweise das Signieren oder Verschlüsseln einer Mail, natürlich auch die Kombination aus beidem:

- wird eine Mail mit dem öffentlichen Schlüssel des Empfängers **verschlüsselt**, so ist sichergestellt, dass ausschließlich der Empfänger den Inhalt wieder dekodieren kann, da nur er den zugehörigen privaten Schlüssel kennt
- wird eine Mail mit dem privaten Schlüssel des Absenders verschlüsselt (**signiert)**, so kann sich der Empfänger mit dem zugehörigen (und zugänglichen) öffentlichen Schlüssel davon

überzeugen, dass der Absender authentisch ist

In beiden Fällen ist ein **verantwortungsvoller Umgang mit dem privaten Schlüssel** und das **Vertrauen in die Gültigkeit eines öffentlichen Schlüssels** die Voraussetzung für die Anwendbarkeit des Verfahrens. Zwischen einem öffentlichen Schlüssel und seinem Inhaber gibt es allerdings keinerlei Verknüpfung. Um sich zu vergewissern, dass ein fremder öffentlicher Schlüssel, den man zum Verschlüsseln oder zum Prüfen einer Signatur verwenden will, demjenigen gehört, von dem man meint, dass er ihm gehört, müsste man diesen öffentlichen Schlüssel persönlich austauschen, was aber im allgemeinen nicht praktikabel ist.

Abhilfe schafft eine sogenannte **Certification Authority (CA).** Die konkreten CA-Informationen in diesem Dokument beziehen sich auf die Zertifizierung in der sogenannten **Global**-Zertifizierungshierarchie des DFN-Vereins (aktuell in der 2. Generation, seit Februar 2017)

3. Aufgaben einer CA

Hauptaufgabe einer CA ist es, eine vertrauenswürdige Verknüpfung zwischen einem Benutzer oder einem Server und einem zu diesem Benutzer/Server gehörenden öffentlichen Schlüssel herzustellen. Dies geschieht, indem die CA diese Zugehörigkeit mit geeigneten Maßnahmen überprüft und den öffentlichen Schlüssel auf dieser Basis beglaubigt. In diesem Prozess erzeugt die CA ein elektronisch signiertes Dokument (**Zertifikat**), das den öffentlichen Schlüssel beinhaltet.

Da hierbei sehr strenge und genau dokumentierte Verfahren eingesetzt werden, vererbt sich das Vertrauen in die ausstellende Instanz (CA) auf die von ihr ausgestellten Zertifikate. Konkret bedeutet dies, dass ein Benutzer, der auf die gewissenhafte Arbeit der DFN-CA vertraut, ohne Bedenken alle von ihr ausgestellten Zertifikate verwenden kann.

Mit Hilfe des öffentlichen Schlüssel der CA kann ein Benutzer ein Zertifikat prüfen und insbesondere den darin enthaltenen öffentlichen Schlüssel des Inhabers auslesen, um ihn zum Beispiel im Mail-Verkehr zu verwenden. Sofern er der CA vertraut, kann er sicher sein, dass die von dieser CA ausgestellten Zertifikate gültig sind und dass er sich auf die darin enthaltenen Daten von Benutzern oder Servern verlassen kann.

Durch Zertifizierung von CA’s durch übergeordnete Instanzen entsteht eine Vertrauens-Hierarchie. Die DFN-Global-Hierarchie umfasst die folgenden drei Stufen (in absteigender Reihenfolge):

- **T-TeleSec GlobalRoot Class 2**
- **DFN-Verein Certification Authority 2**
- **DFN-Verein Global Issuing CA**

Die oberste Instanz in dieser Kette (**T-TeleSec GlobalRoot Class 2)** wird von den Browser-Herstellern als vertrauenswürdig akzeptiert und ist in den gängigen Anwendungen (Browser, Mail-Programme) bereits eingebaut ist, .

Eine weitere Aufgabe einer CA ist die Verwaltung von CRLs (Certificate Revocation Lists), in

denen zurückgezogene Zertifikate veröffentlicht werden. Die Zertifizierungsrichtlinien einer CA sind in einer jedermann zugänglichen **CA-Policy** schriftlich niedergelegt.

4. Die DFN-CA

Das Forschungszentrum nutzt eine DFN-CA (**DFN-Verein Global Issuing CA)**. Diese verwaltet Zertifikate für Benutzer und Server des Forschungszentrums und ermöglicht dadurch den Einsatz kryptographischer Verfahren zur Sicherung der Datenübertragung. Das JSC-Dispatch fungiert als Schnittstelle zur CA (**Teilnehmerservice, E-Mail: ts@fz-juelich.de**).

Die Zertifikate der DFN-CA sind **nicht *qualifiziert*** im Sinne des deutschen Signaturgesetzes, d.h. eine auf ihrer Grundlage erzeugte elektronische Signatur kann **eine handschriftliche Unterschrift *nicht* ersetzen**. Ein Link auf die Zertifizierungs-Richtlinien findet sich auf der Homepage des FZJ-Teilnehmerservices (*http://www.fz-juelich.de/ias/jsc/zertifikate*). Dort finden sich auch die Routinen zum Anfordern, Suchen, Zurückziehen von Zertifikaten, sowie weitere Dokumentation zum Thema.

5. Generieren eines Benutzerzertifikats

Zum Generieren eines **Benutzerzertifikats** sind allgemein folgende Schritte erforderlich:

- der Benutzer erzeugt auf seinem Rechner mit Hilfe eines Browsers ein Schlüsselpaar (private / public key) und übermittelt den öffentlichen Schlüssel an die CA. Er benutzt dazu die Web-Schnittstelle des FZJ zur DFN-CA (*https://pki.pca.dfn.de/fzj-ca-g2/pub*).
- Alle mit ***** gekennzeichneten Felder des Web-Formulars sind auszufüllen. Im Namensfeld dürfen nur Namensbestandteile stehen, die auch im weiter unten erwähnten amtlichen Ausweis stehen. Dies gilt insbesondere für Titel. Abschließend wird ein pdf-Dokument des **Zertifikatsantrags für ein Nutzerzertifikat** angezeigt, das ausgedruckt wird.
- Der Benutzer stellt sich unter Vorlage eines amtlichen gültigen Ausweispapiers mit Lichtbild (Personalausweis oder Reisepass) beim **Teilnehmerservice** des FZJ (JSC-Dispatch, Geb 16.4, R. N 201, Tel 5642) vor und verpflichtet sich durch Unterzeichnung des Zertifikatsantrags dazu, die Regeln der Zertifizierungsstelle einzuhalten und insbesondere seinen privaten Schlüssel nicht weiterzugeben.
- Der Teilnehmerservice überprüft die Angaben zur Person und erzeugt auf deren Basis ein Zertifikat: dabei signiert die DFN-CA die Angaben zur Person und den öffentlichen Schlüssel der Person mit ihrem eigenen privaten Schlüssel. Anschließend wird der Benutzer per Mail über die Ausstellung des Zertifikats informiert. Diese Mail enthält neben wichtigen Erläuterungen zwei Web-Links. Der erste dient zum **Einbau der Zwischenzertifizierungsstellen** in den Browser, der andere zum **Einbau des Zertifikats** in den Browser.

Achtung: beide Import-Schritte müssen wie beschrieben ausgeführt werden und zwar unbedingt mit dem Browser, mit dem der Zertifikatsantrag erzeugt wurde. Das Zertifikat findet sich anschließend unter der Rubrik **Eigene Zertifikate** in der Konfiguration der Browser.

- Um einem Verlust des Schlüsselmaterials vorzubeugen und um es ggfs. auch auf einem anderen Rechner oder in einer anderen Applikation nutzen zu können, sollte dieses nun zunächst unbedingt gesichert werden. Der Browser bietet dazu eine Exportfunktion, die eine standardisierte Containerdatei mit dem privaten Schlüssel und dem Zertifikat erzeugt. Diese Datei hat standardmäßig die Erweiterung **p12,** sie muss unbedingt mit einem starken Passwort geschützt werden.

6. Integration von Benutzerzertifikaten in Anwendungen

Ein so erzeugtes Benutzerzertifikat zusammen mit dem privaten Schlüssel kann nun in Anwendungen genutzt werden, um Mail elektronisch zu signieren, sich bei bestimmten Services zu authentifizieren (z.B. für das FZJ-interne WLAN) oder verschlüsselte Mail zu lesen.

Um selber E-Mail für einen bestimmten Partner verschlüsseln zu können, benötigt man dessen Zertifikat. Der einfachste Weg, dieses zu bekommen, besteht darin, den Partner zu bitten, eine signierte Mail zu senden. Beim Lesen dieser Mail bauen die gängigen Mail-Programme das Zertifikat des Partners automatisch in ihren Zertifikatspeicher ein.

Damit eine Anwendung ein Benutzerzertifikat (z.B. für elektronische Signaturen) verwenden kann, muss grundsätzlich die im vorigen Abschnitt erwähnte Containerdatei mit den Mitteln der Anwendung importiert werden.

Mozilla: Bei den Mozilla-Produkten gilt dies für jede einzelne Anwendung (Einstellungen → Erweitert → Zertifikate anzeigen → Ihre Zertifikate).

Windows: Microsoft-Anwendungen, die mit Zertifikaten arbeiten, greifen auf einen gemeinsamen Zertifikatsspeicher zu. Zur Verwaltung der Zertifikate kann der Internet Explorer genutzt werden (Einstellungen → Internetoptionen → Inhalte → Zertifikate → eigene Zertifikate) oder alternativ das Systemprogramm **certmgr.**

Um jederzeit auf verschlüsselte Mail zugreifen zu können, sollten auch abgelaufene eigene Zertifikate im Zertifikatsspeicher belassen werden. Eine Sicherungskopie dieser Zertifikate muss zusätzlich aufbewahrt werden.

7. Serverzertifikate (ssl)

Zum Generieren eines Server-Zertifikats sind folgende Schritte erforderlich:

- Erzeugen eines **Certificate Signing Requests (CSR).** In einigen Fällen bieten die Anwendungen Tools zum Erzeugen dieser Datei, in anderen Fällen muss der Request mit Hilfe von **openssl** erzeugt werden. Die Angaben im Distinguished Name eines Servers sind zum Teil strikt vorgegeben. Eine Anleitung findet sich in der Dokumentation (http://www.fz-juelich.de/ias/jsc/DE/Leistungen/Dienstleistungen/Zertifikate/Dokumentation/_node.html: **Information Server-Zertifikate**)

- Übermittlung des Requests an die CA mit Hilfe der Web-Schnittstelle (https://pki.pca.dfn.de/fzj-ca-g2/pub). Hierbei muss auch das für den jeweiligen Service passende Zertifikatsprofil ausgewählt werden.

- Übermittlung des unterschriebenen Zertifikatsantrags an den Teilnehmerservice (JSC Dispatch). Die Vorlage eines Ausweises ist beim Beantragen eines Global-Serverzertifikats nicht erforderlich. In diesem Fall ist eine verlässliche Zuordnung durch den im Internet eindeutigen Namen des Rechners gegeben.

- Ein Link zum Zertifikat wird dem Antragsteller per Mail mitgeteilt.

8. Allgemeine Hinweise zu Benutzerzertifikaten

Schlüssel und Zertifikat sind zunächst nur auf dem Rechner/Browser verfügbar, auf dem sie erzeugt/eingebaut wurden. Wenn **private key** und **Zertifikat** später auf einem anderen Rechner oder in einer anderen Anwendung benötigt werden, kann beides mit Browser-Funktionen in eine passwortgeschützte Datei exportiert und später aus dieser Datei an anderer Stelle wieder importiert werden. So ist zum Beispiel vorzugehen, wenn ein mit Firefox beantragtes Zertifikat zur Absicherung des Mailverkehrs in Thunderbird benötigt wird.

Es empfiehlt sich in jedem Fall, mit der Export-Funktion der Anwendungen eine Sicherungs-Datei mit dem Schlüsselmaterial zu erzeugen, sie dabei mit einem starken Passwort zu sichern und anschließend sicher zu hinterlegen. Sofern man Email-Verschlüsselung zum Schutz vertraulicher Daten anwendet, müssen **auch abgelaufene Zertifikate mit den zugehörigen privaten Schlüsseln unbedingt sicher aufbewahrt** werden. Bei Verlust des privaten Schlüssels sind die verschlüsselten Daten **unwiederbringlich verloren**.

Benutzerzertifikate haben derzeit eine Gültigkeitsdauer von 3 Jahren. Rechtzeitig vor Ablauf wird ein Benutzer von der CA per Mail daran erinnert, dass er ein neues Zertifikat erzeugen muss.

Um Mail-Partnern das eigene Zertifikat mitzuteilen, reicht es aus, diesen eine signierte Mail zu schicken. Die gängigen Mail-Clients extrahieren das Zertifikat beim Lesen der signierten Mail automatisch und speichern es für die spätere Verwendung.

Weitere Informationen zum Thema Zertifikate finden sich auf den Seiten des JSC (JSC Online). Weiterhin sind z.B. die FAQ auf den Web-Seiten des DFN-Vereins hilfreich (https://www.pki.dfn.de/faqpki/).