Projekt digitales Dozentenbüro / öffentliche Schlüssel

M. Anders, Fachhochschule Wedel

Bei diesem Projekt geht es um die Nutzung moderner Techniken, um die digitale Signatur und hybride Verschlüsselung für den Büroalltag an einer Hochschule zu nutzen.

Vorab möchte ich diesbezüglich auf meine eigenen öffentlichen Schlüssel verweisen, die ich im Büroalltag in meiner Eigenschaft als Hochschuldozent verwende. Jeder Teilnehmer am Verfahren erzeugt für sich einen privaten Schlüssel, der geheim gehalten werden muss und einen daraus abgeleiteten öffentlichen Schlüssel, der manipulationssicher und öffentlich sichtbar abgelegt sein sollte. Im Idealfall kann durch den Ablageort nachgewiesen werden, dass der Schlüssel wirklich zum vorgeblichen Inhaber gehört. Dies kann beispielweise durch Ablage in der Internetdomain des Arbeitgebers erfolgen, wenn der Schlüssel für berufliche Tätigkeiten verwendet werden soll.
Mit dem privaten Schlüssel werden Dokumente digital signiert oder zugesandte Chiffrate dechiffriert. Mit dem öffentlichen Schlüssel werden Signaturen von Dritten geprüft und Klartexte gezielt für den Inhaber des zugehörigen privaten Schlüssels chiffriert. Aus dem öffentlichen Schlüssel ist es nicht möglich, auf den privaten Schlüssel zurückzuschließen.

Häufig müssen im Hochschulalltag Notenlisten und andere elektronische Dokumente mit wertenden personenbezogenen Daten per Mail verschickt werden. Besonders, wenn dieser Transfer von und nach außerhalb des Hochschulnetzes liegenden Mail-Konten durchgeführt wird, muss die Vertraulichkeit, Integrität und Authentizität auch gegen starke Angreifer geschützt werden. Dabei wird die Sicherstellung der Integrität und Authentizität im ureigenen Interesse der Hochschule liegen. Bezüglich der Vertraulichkeit kommen noch gesetzliche Anforderungen hinzu.
Um solche Transfers also sicher und gesetzeskonform durchführen zu können, benötigt man Software zur Erstellung und Prüfung digitaler Signaturen und zur hybriden Ver- und Entschlüsselung. Die Software sollte mit öffentlicher Lizenz verteilt werden, quelloffen und kostenfrei sein. Weiterhin ist der akademische Betrieb übersichtlich und persönlich genug, um eine kommerzielle PKI ausschließen zu können. Wenn man diese ausschließen kann, sollte man das auch tun, weil durch den Ausschluss eines Mittlers die Sicherheit immer nur erhöht, die Anzahl der Angriffsstellen immer nur verringert werden kann. So brauche ich sicherlich keine US-Firma als kommerziellen Mittler, wenn ich beispielsweise mit einem Kollegen an der Jade Hochschule Wilhelmshaven vertrauensvoll Schlüssel austauschen möchte.

Es gibt nach meiner Information im Bereich Signatur und hybride Verschlüsselung nur zwei diese Kriterien (öffentliche Lizenz, quelloffen, kostenfrei) erfüllende Software-Werkzeuge.
Als erstes ist GnuPG zu nennen.
GnuPG (Gnu Privacy Guard) ist die heute am weitesten verbreitete Umsetzung des OpenPGP Standards. Das Softwarepaket wurde 1999 von Werner Koch aus Erkrath bei Düsseldorf geschrieben und wird von ihm gepflegt.
Der OpenPGP Standard geht auf die Mutter aller Privatsphärenprogramme "PGP" (Pretty Good Privacy) zurück, das 1991 von dem US-amerikanischen Friedensaktivisten Phil Zimmermann entwickelt wurde. Phil Zimmermann musste aufgrund der Veröffentlichung von PGP im US-Rechtssystem diverse Sträuße ausfechten. Das Programm war in den USA als Waffe klassifiziert worden und ihm war illegaler Waffenexport zur Last gelegt

worden. PGP ist seit einiger Zeit nicht mehr frei erhältlich, es gibt lediglich kommerzielle direkte Nachfolger. Werner Kochs GnuPG hatte diese Lücke gefüllt.
GnuPG ist weit verbreitet, aber kann in der Benutzung etwas sperrig sein. Es verwendet nicht in jeder Version die modernsten Algorithmen und standardmäßig die nicht mehr ganz zukunftsfesten Kryptosysteme RSA und elGamal. Deshalb gibt es Bedarf für ein weiteres Verschlüsselungswerkzeug für manuelle Signatur und Verschlüsselung.

Das zweite hier zu nennende Werkzeug ist Academic-Signature.
Das Programm Academic Signature hat vergleichbare Grundfunktionen wie GnuPG, hat aber eine integrierte Benutzeroberfläche, nutzt als Kryptosystem das moderne ECC (Elliptische Kurven Kryptographie) und kann größere Schlüssellängen und Blockgrößen als GnuPG nutzen. Mit Academic Signature können Chiffrate erzeugt werden, die der Angreifer nicht von Rauschen unterscheiden kann und die keinerlei Rückschlüsse auf Sender oder Empfänger erlauben. Diese Eigenschaft wird mit dem Fachbegriff "negligible adversary advantage" benannt.
Academic Signature ist im Rahmen dieses Projektes von mir erstellt worden. Es ist primär für die manuelle Erzeugung und Prüfung von digitalen Signaturen ohne Einbeziehung eines kommerziellen Mittlers entwickelt worden.
Zusätzlich bietet es noch die Möglichkeit, einer Datei einen Zeitstempel beizufügen. Mit einem solchen Zeitstempel kann man für einen Klienten, z.B. den Einreichenden einer Abschlussarbeit, die Vorlage eines elektronischen Dokumentes zu einem bestimmten Zeitpunkt in einem genau bestimmten Zustand elektronisch bezeugen. Der Klient kann mit dem Zeitstempel und der Originaldatei gegenüber einer dritten Partei dieses Zeugnis nachweisen. Später wurden Funktionen für die Verschlüsselung hinzugefügt.

Im Rahmen dieses Projektes nutze ich beide Werkzeuge. Zu Beginn dieses Textes ist ein Link zu meinen öffentlichen Schlüsseln für die jeweiligen Werkzeuge angegeben.
Beide Werkzeuge nutze ich seit vielen Jahren für die Authentifizierung von mir erstellter Gutachten, Protokolle, Bewertungen und für Vereinbarungen mit Studenten. In meiner Funktion als Studiengangsleiter sind gelegentlich bestimmte Zusatzleistungen für die Zulassung zu einem Masterstudiengang mit Studienbewerbern zu vereinbaren. Eine solche digital signierte Vereinbarung in Form eines Tabellenblattes geht dann inklusive Signatur an die Verwaltung, an den Studenten selbst und an mich als Aussteller zur Archivierung des Vorgangs. Im Dokument selbst befindet sich immer der Hinweis auf die begleitende Signatur und auf den Verifikationsweg.
Weiterhin nutze ich die Werkzeuge GnuPG und Academic Signature für die Verschlüsselung von elektronischen Dokumenten im Transfer wie e-Mails, deren Dateianhängen, Arbeitsversionen von Abschlussarbeiten, für die Verschlüsselung von Klausuren vor dem Klausurtermin und für weitere zahlreiche Varianten schützenswerter Kommunikation.
Die Nutzung beider Werkzeuge ist komfortabel und wird auch von einigen Kollegen aus Lehre und Verwaltung geteilt.
Ich halte die Nutzung solcher digitaler Signaturen auch für digitale Abschlusszeugnisse für eine vielversprechende Option, die den Absolventen durch authentisierbare digitale Zeugnisse Online-Bewerbungen erheblich erleichtern würde.
Leider werden solche Anwendungen nach meinem Kenntnisstand aber in Deutschland und auch an meiner Hochschule bisher nicht erwogen.