Verwendung digitaler Signaturen im Hochschulbereich

Prof.Dr.Michael Anders, Fachhochschule Wedel, Wedel, 18.11.2011

Teaser:

Wer sich noch nicht mit Kryptographie beschäftigt hat denkt beim Begriff "Chiffrierung" an Agentenfilme, denkt an Verschlüsselung und geheime Nachrichten. Moderne kryptographische Techniken bieten aber auch andere, weniger bekannt Möglichkeiten. So können z.B. Hochschulzeugnisse, Gutachten oder Empfehlungsschreiben in fälschungssicherer, digitaler Form signiert werden. Absolventen haben dann die Möglichkeit digitale Zeugnisse beliebig zu vervielfältigen und authentifiziert für Online-Bewerbungen zu verwenden.

Kryptographie: Was sind symmetrische und asymmetrische kryptographische Verfahren?

Auch wer sich noch nie näher mit Kryptographie beschäftigt hat, kennt meist das in Abbildung 1 dargestellte Muster der Übertragung einer geheimen Botschaft: Der Sender kennt wie der Empfänger einen geheimen Schlüssel. Mit diesem Schlüssel erzeugt der Sender eine Chiffre und sendet sie auf unsicherem Kanal - z.B. als Telegramm - zum Empfänger. Der Empfänger kann mit dem geheimen Schlüssel die Nachricht entschlüsseln.

Dies ist ein Verfahren der symmetrischen Kryptographie. Das Wort "symmetrisch" wird verwendet, weil Verschlüsseler und Entschlüsseler den gleichen geheimen Schlüssel verwenden. Solche Verfahren sind seit Jahrhunderten bekannt und bilden bis heute das Rückgrat der geheimen Übermittlung von Nachrichten über unsichere Kanäle. Aktuell wird überwiegend das Verfahren "AES" verwendet [http://de.wikipedia.org/wiki/Advanced_Encryption_Standard].

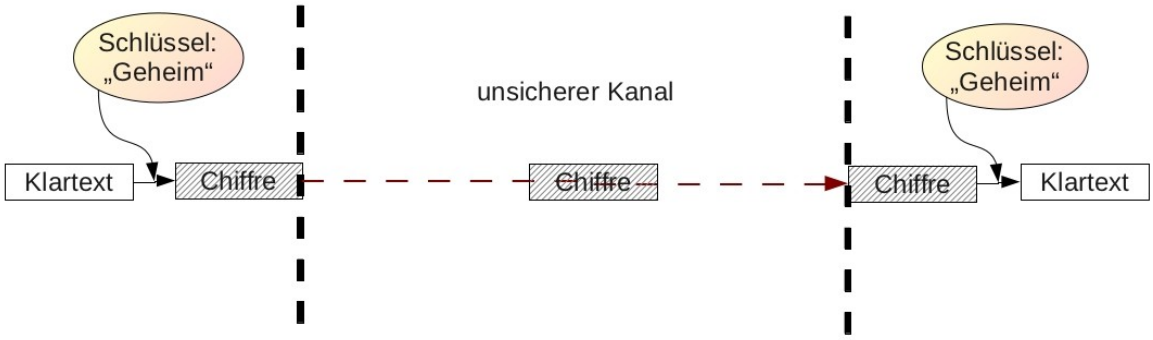

Abbildung 1: Übermittlung einer geheimen Nachricht mit symmetrischer Verschlüsselung

Allerdings ist vor etwa 30 Jahren ein gänzlich neues Gebiet, die asymmetrische Kryptographie, entdeckt worden. Hierbei besteht jeder Schlüssel aus einem öffentlichen Teil, der jedermann zugänglich sein sollte und aus einem privaten Teil, der nur dem Inhaber des Schlüssels bekannt ist. Mit dem privaten Teil kann z.B. eine Signatur erstellt werden, mit dem öffentlichen Teil wird sie geprüft. Diese asymmetrischen Verfahren ermöglichen erst die Vielzahl neuer Anwendungen, die die moderne Kryptographie heute bietet.

Möglichkeiten der asymmetrischen Kryptographie: Die Chiffre

Die nächstliegendste Anwendung eines kryptographischen Verfahrens liegt in der Chiffrierung und Dechiffrierung. Zum Verschlüsseln wird der öffentliche, jedermann zugängliche Schlüssel des Adressaten benutzt. Entschlüsseln ist nur mit dessen privatem Schlüssel möglich und kann daher auch ausschließlich vom Inhaber des privaten Schlüssels ausgeführt werden. Es ist nicht möglich, aus der

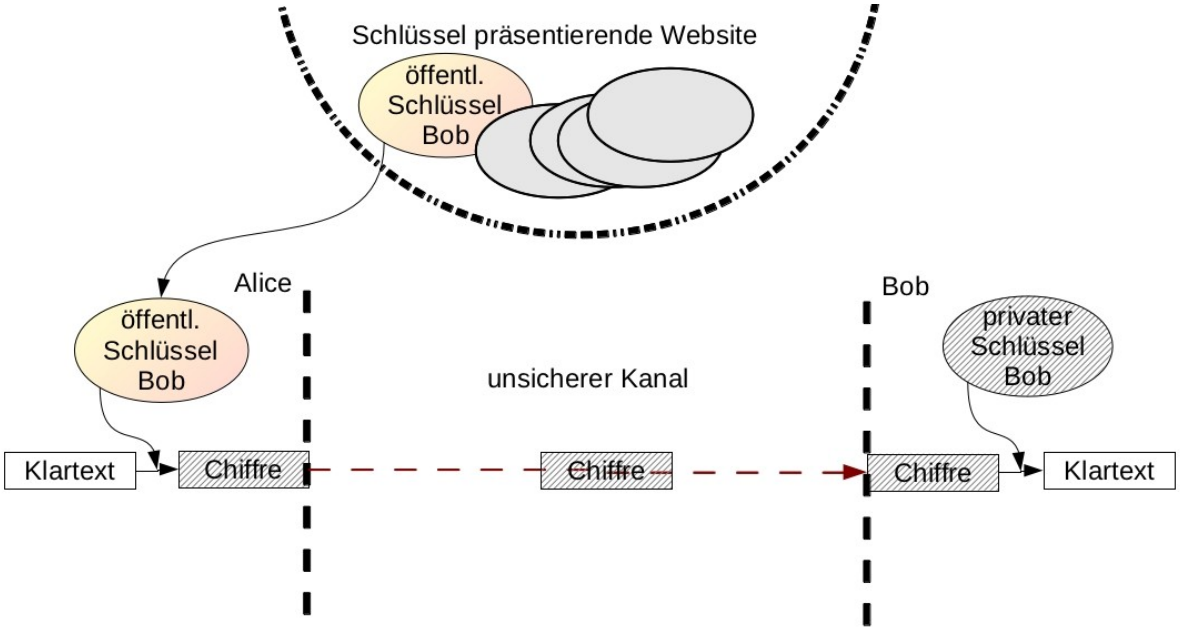

Abbildung 2: Übermittlung einer geheimen Nachricht mit asymmetrischer Verschlüsselung.

Kenntnis des öffentlichen Schlüssels auf den privaten Schlüssel zu schließen. Der Absender verschlüsselt gezielt für einen ganz bestimmten Adressaten und ist auch selbst nicht mehr in der Lage, die erzeugte Chiffre wieder zu entschlüsseln. Hierbei ist es von höchster Sicherheitsrelevanz, dass dem Chiffrierer der "wahre", unverfälschte öffentliche Schlüssel des beabsichtigten Empfängers zur Verfügung steht.
Dieses Verfahren kann an einer Hochschule von Dozenten und Assistenten genutzt werden, um dem Prüfungsamt per Mail Prüfungsergebnisse oder andere schützenswürdige personenbezogenen Daten vertraulich zukommen zu lassen.

Möglichkeiten der asymmetrischen Kryptographie: Die Signatur

Weiterhin besteht die Möglichkeit, durch digitale Signatur Notentabellen, Zeugnisse oder Gutachten zu Authentifizieren (sie kommen sicher vom Inhaber des privaten Schlüssels) und die Integrität zu prüfen (sie sind nicht auf dem Weg vom Sender zum Empfänger geändert worden). Signiert wird mit dem privaten Schlüssel. Niemand außer dem Inhaber des privaten Schlüssels kann eine gültige Signatur erzeugen, aber jeder kann mit Kenntnis des öffentlichen und sinnvollerweise veröffentlichten Schlüssels die Signatur prüfen. So könnten etwa Dozenten Gutachten über die Eignung von Studenten für Stipendien digital signieren und Gutachten und Signatur dem Studenten zur Weitergabe auf einem Memory Stick übergeben.
Die Anwendung mit dem größten unmittelbaren Nutzen wäre wohl die Herausgabe von durch die Hochschulleitung digital signierten elektronischen Abschlusszeugnissen. Kein Student müsste mehr beglaubigte Kopien von Zeugnissen für Bewerbungen anfertigen lassen und könnte einen online Bewerbungsvorgang mit sicher belegten Zeugnissen versehen.
Ein typischer Anwendungsfall trat im Frühjahr 2011 auf. Es wurde von unseren Bachelor-Absolventen, die sich an anderen Hochschulen um die Zulassung zu Master Curricula bewarben, häufig die Vorlage des Modulhandbuches ihres Studiengangs verlangt. Die massenweise Verschickung solch umfänglicher Papierdokumente ist unsinnig, teuer und umständlich. Wir haben durch unser Prüfungsbüro und auf meiner Homepage eine mit dem weiter unten beschriebenen Tool "Academic Signature" digital signierte elektronische Version des Modulhandbuches für unsere Studenten zur Verfügung gestellt. So konnten durch die Studiengangleitung kommentierte und inklusive Kommentar

authentifizierte elektronische Versionen des Modulhandbuchs papierlos per Mail verschickt werden.

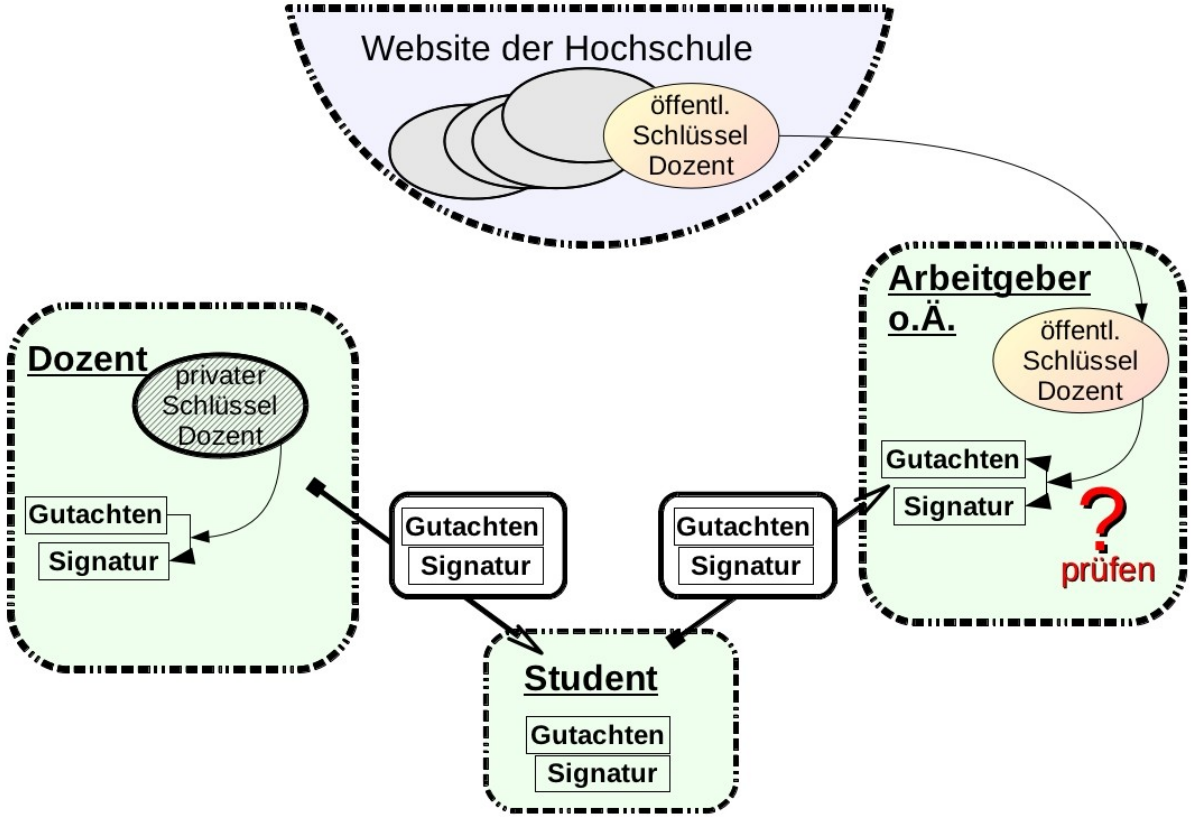

Abbildung 3: Mögliche Anwendung der digitalen Signatur zur Authentifizierung eines Gutachtens. Bislang wird dieses Muster nur auf der Ebene einzelner Dozenten für Gutachten, Bestätigung von Prüfungsleistungen oder Empfehlungsschreiben angewandt. Eine systematische Anwendung durch eine deutsche Hochschulverwaltung ist mir bisher noch nicht bekannt.

Möglichkeiten der asymmetrischen Kryptographie: Der Zeitstempel

In einer Dreierkonstellation ist in Verbindung mit einer Signatur auch eine Notar- oder Zeugenfunktion denkbar. Der Unterzeichner erhält von einem Klienten ein Dokument, fügt einen Kommentar hinzu und signiert mit seinem privaten Schlüssel die Gruppe aus Dokument und Kommentar.
Üblicherweise wird der Kommentar des Unterzeichners Datum und Uhrzeit enthalten und weiterhin sinnvollerweise auch den Namen des Klienten. Der Klient kann damit gegenüber einer dritten Partei nachweisen, dass er zu dem vom Unterzeichner genannten Zeitpunkt in Besitz dieses Dokuments war. Diese Variante der Signatur nennt man auch einen Zeitstempel.
Der Unterzeichner fungiert als vertrauenswürdiger Zeuge für die Richtigkeit des Zeitstempels. Hierbei braucht der Unterzeichner gar nicht über das Dokument im Klartext zu verfügen. Es reicht, eine Chiffre oder sogar nur einen "digitalen Fingerabdruck" (=Hashwert) in Unkenntnis des Dokumenteninhalts mit dem eigenen Zeitkommentar zusammen zu signieren. Dies nennt man eine blinde Signatur. Der Klient muss lediglich seinerseits sicherstellen, dass für Dritte zu einem späteren Zeitpunkt der Offenlegung diese Chiffre oder der Hashwert nachvollziehbar eindeutig dem Klardokument zugeordnet werden kann.
Wer ein Musikstück komponiert, ein Drehbuch geschrieben, ein Layout für eine Imagekampagne erstellt oder anderes geistiges Eigentum erzeugt hat, muss sich nicht selten damit an einen potenziellen Verwerter mit sehr viel größerer Macht wenden. Dies verursacht bei misstrauischen Autoren Sorge um die spätere Anerkennung der Urheberschaft durch den Verwerter. Hierbei kann ein zu frühem Zeitpunkt erstellter Zeitstempel diese Sorge um die spätere Anerkennung der Urheberschaft erheblich mindern.

Ein Zeitstempel ist natürlich nicht identisch mit dem Nachweis der Urheberschaft. Wenn aber z.B Herr Beethoven einen für ihn ausgestellten Zeitstempel von 1805 zur Melodie von "Let it be" vorweisen

könnte, wären die Beatles durchaus in Erklärungsnöten. Es kostet wenig Mühe, einen Zeitstempel zu erzeugen. Deshalb sollte bei geistigem Eigentum frühzeitig der erste vollständige Entwurf des Manuskriptes, der Komposition o.Ä. mit einem Zeitstempel einer vertrauenswürdigen Instanz versehen werden.
Ich halte es für sinnvoll, einen solchen Zeitstempelservice für Studenten und Absolventen einer Hochschule kostenfrei anzubieten. Einzelne Absolventen oder Studenten könnten beim Einstieg in Ihr Berufsleben durchaus Bedarf dafür haben.

Asymmetrische Kryptographie: Verbreitung in der Hochschuladministration

Angesichts der Tatsache, dass diese Möglichkeiten schon seit mindestens zwei Jahrzehnten bestehen ist die flächendeckende Abwesenheit im administrativen Bereich der Hochschulen erstaunlich.
Ich selbst bin im Herbst letzten Jahres von der größten deutschen Stipendien vergebenden Organisation um eine Stellungnahme zur Eignung eines Studenten für ein Auslandsstudium gebeten worden. Hierzu wurden - immerhin in elektronischer Form- Formulare übermittelt. Nach begleitender Anweisung sollten diese ausgedruckt, explizit mit „Schreibmaschine“!! ausgefüllt und per Brief zurückgeschickt werden. Die Zeit bis zum Einsendeschluss war äußerst knapp und das Verfahren wurde aus diesem Grunde zu einer Zitterpartie für den Studenten.
Solche Prozeduren sind nicht mehr zeitgemäß und legen ein erschreckendes Beharrungsvermögen von Verwaltungen bloß. Gerade für den Hochschulbereich sollte man eine größere Beweglichkeit erwarten dürfen.
Genau dieser Vorgang hat auch den Anstoß geliefert, eine Softwarelösung für Signaturerstellung, asymmetrische Chiffrierung und kryptographisch sichere Zeitstempel für die Anwendung im Hochschulbereich zu entwickeln. Diese Anwendung steht nun jedermann kostenfrei zur Verfügung.

Asymmetrische Kryptographie: Etablierte Verfahren

Es gibt derzeit drei weit verbreitete und als sicher anerkannte Verfahren der asymmetrischen Kryptographie, für deren Bezeichnung sich die folgenden Kürzel eingebürgert haben: RSA, elGamal und ECC.

Asymmetrische Kryptographie: Das RSA-Verfahren

Das RSA-Verfahren [http://de.wikipedia.org/wiki/RSA-Kryptosystem] ist nach den Anfangsbuchstaben der Namen der Entwickler Rivest, Shamir und Adleman benannt und wurde von diesen 1977 publiziert und 1983 patentiert. Der Patentschutz ist im Jahre 2000 abgelaufen. Es ist das älteste und heute am weitesten verbreitete Verfahren der asymmetrischen Kryptographie. Jeder Internetbrowser wird bereits mit einer Vielzahl an integrierten öffentlichen Schlüsseln ausgeliefert. Bei der Durchsicht meines Browsers „Firefox“ habe ich ausschließlich öffentliche Schlüssel für das RSA Verfahren vorgefunden(Die öffentlichen Schlüssel sind Hauptbestandteil der sogenannten „Zertifikate“). Die anderen beiden Verfahren werden augenscheinlich hier nicht verwendet.
Die Sicherheit des RSA-Verfahrens beruht auf der Schwierigkeit, große Zahlen in ihre Primfaktoren zu zerlegen. Natürlich steigen die Anforderungen an Schlüssellänge mit dem technischen Fortschritt und steigender Prozessorleistung. In diesem Fall ist allerdings der wissenschaftliche Fortschritt hin zu immer besseren Faktorisierungsalgorithmen ein noch stärkerer Treiber als der Fortschritt bei der Prozessorleistung. Man erwartet in den nächsten Jahren rasant steigende erforderliche RSA-Schlüssellängen, die bald die Praktikabilität des Verfahrens einschränken könnten. Eine Schlüssellänge von 1024 Bit gilt derzeit als marginal sicher, ist aber noch sehr weit verbreitet. Am 12.Dezember 2009 wurde die Faktorisierung eines 768 Bit RSA Moduls durch Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Pierrick Gaudry, Alexander Kruppa, Peter Montgomery, Joppe W. Bos, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann publiziert [http://eprint.iacr.org/2010/006]. Man muss wohl davon ausgehen, dass entsprechend ausgestattete Institute hochentwickelter Länder, wie z.B. die US-Amerikanische NSA[http://www.nsa.gov/] bereits heute zur Faktorisierung von 1024 Bit Zahlen in der Lage sind. Homebanking Anwendungen arbeiten meist mit einer RSA-Schlüssellänge von 2048 Bit.

Asymmetrische Kryptographie: Das elGamal-Verfahren

Das elGamal Verfahren wurde 1985 von Taher ElGamal publiziert [Taher ElGamal (1985). "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms". *IEEE Transactions on*

Information Theory **31** (4): 469–472. doi:10.1109/TIT.1985.1057074.] Es ist damit das zweitälteste der heute etablierten asymmetrischen Verfahren. Es beruht auf der Schwierigkeit, den diskreten Logarithmus einer Zahl modulo einer großen Primzahl zu bestimmen.
Die Sicherheit des ElGamal Verfahrens ist bei gleicher Bit-länge des privaten Schlüssels vergleichbar mit der Sicherheit des RSA Verfahrens. Wie beim RSA-Verfahren verursacht die Verbesserung der Angriffsalgorithmen einen stärkeren Druck hin zu größeren Schlüssellängen als die allgemeine Verbesserung der Prozessorleistung.
Das Verfahren unterliegt keinem Patent. Der älteste, vom US-amerikanischen NIST 1991 empfohlene Signaturstandard DSS beruhte ursprünglich allein auf dem ElGamal Verfahren zur Signatur(DSA). Später wurde diesem Signaturstandard DSS noch das RSA-Signaturverfahren und das ECDSA-Verfahren hinzugefügt.

Asymmetrische Kryptographie: Auf elliptischen Kurven basierende Kryptosysteme(ECC)

Die Anwendbarkeit elliptischer Kurven für die asymmetrische Kryptographie wurde 1985 von Victor Miller (IBM) and Neil Koblitz(University of Washington) entdeckt [Koblitz, N. (1987). "Elliptic curve cryptosystems". *Mathematics of Computation* **48** (177): 203–209. JSTOR 2007884., Miller, V. (1985). "Use of elliptic curves in cryptography". *CRYPTO* **85**: 417–426. doi:10.1007/3-540-39799-X_31].
Das Muster des Verfahrens gleicht dem des ElGamal Verfahrens. Allerdings wird eine andere Arithmetik verwendet. Die Exponentiation des ElGamal Verfahrens wird durch eine anders definierte, rechnerisch aufwändigere "Punktmultiplikation" auf der elliptischen Kurve ersetzt. Die mächtigsten nicht generischen Attacken auf RSA und ElGamal können bei sorgfältig gewählten Kurvenparametern nicht auf Kryptosysteme mit elliptischen Kurven angewandt werden. Deshalb sind bei elliptische Kurven erheblich kleinere Schlüssellängen sicher, als bei den asymmetrischen Verfahren der ersten Generation (RSA, ElGamal).
Das auf elliptischen Kurven beruhende Kryptosystem gilt als das fortgeschrittenste und zukunftssicherste Kryptosystem. So erlaubt z.B. die amerikanische Regierung für Dokumente der Kategorie "Secret" für eine Übergangszeit noch RSA und ElGamal mit 2048 Bit Schlüssellänge [http://www.nsa.gov/ia/programs/suiteb_cryptography/]. Diese sollen aber in naher Zukunft durch 256-bit ECC (=Elliptic Curve Cryptosystems) ersetzt werden. Für Geheimnisse der Stufe "Top Secret" sind ausschließlich ECC-Verfahren mit mindestens 384 bit Schlüssellänge zugelassen.
Die Patentsituation scheint kompliziert. Grundsätzlich ist das ECC-Verfahren bei der Entdeckung ohne Patentschutz der Allgemeinheit zugänglich gemacht worden("Public Domain"). Allerdings hat insbesondere die Firma Certicom [http://www.certicom.com/] eine Vielzahl an Patenten auf Techniken zur besonders effizienten Implementierung der ECC-Algorithmen erworben. Manche Autoren sind der Meinung, man könne diese Patente nicht umgehen und andere teilen diese Auffassung nicht. Insbesondere der in Deutschland basierte Zusammenschluss "ECC-Brainpool"[http://www.ecc-brainpool.org/] vertritt die Ansicht, dass eine Implementierung einer ECC-Software lizenzfrei möglich ist. Tatsächlich hat Certicom im Mai 2007 gegen Sony wegen Rechteverletzung zweier ECC-Patente in den USA geklagt[http://en.wikipedia.org/wiki/ECC_patents]. Sony berief sich auf zwei zuvor veröffentlichte wissenschaftliche Publikationen und erreichte im Mai 2009 die Abweisung der Klage von Certicom.

Asymmetrische Kryptographie: Vergleichende Bewertung der etablierten Verfahren

Wie bereits im letzten Abschnitt erwähnt, vertritt die amerikanische NSA(National Security Agency) die Meinung, bei sicherheitskritischen Anwendungen sollte komplett das RSA oder ElGamal-Verfahren durch das auf elliptischen Kurven basierende Kryptosystem ersetzt werden[http://www.nsa.gov/business/programs/elliptic_curve.shtml]. In der folgenden Tabelle wird die Schlüssellänge verschiedener Verfahren bei vergleichbarem Sicherheitsniveau gegenübergestellt.

	Schlüssellänge bei modernen Symmetrischen Algorithmen(bit)	Schlüssellänge bei asymmetrischen Verfahren der ersten Generation(RSA, ElGamal)	Schlüssellänge bei elliptischen Kurven (ECC)
marginale Sicherheit	80	1024	160
	112	2048	224
US: SECRET	128	3072	256
US: TOP SECRET	192	7680	384
	256	15360	521

Tabelle 1: Schlüssellängen vergleichbaren Sicherheitsniveaus für moderne symmetrische Verfahren, für asymmetrische Verfahren der ersten Generation und für das moderne ECC-Verfahren. Die Zahlenwerte stammen aus einem Dokument der NSA[http://www.nsa.gov/business/programs/elliptic_curve.shtml]. Es gibt einen ähnlichen Vergleich vom BSI(Bundesamt für Sicherheit in der Informationstechnik). Die von der US-Regierung für Dokumente der Geheimhaltungsstufe "SECRET" und "TOP SECRET" vorgeschriebenen Niveaus sind in Zeile 3 und 4 ausgewiesen. Für die Kategorie "TOP SECRET" ist real nur noch das ECC-Verfahren zulässig und die Zahl 7680 der mittleren Spalte als rein hypothetisch aufzufassen [http://www.nsa.gov/ia/programs/suiteb_cryptography/].

Tools: Neuer Personalausweis und andere Smartcard basierte Tools

Wie vor einiger Zeit in Medienkampagnen durch die deutschen Behörden verbreitet, bietet der neue deutsche Personalausweis die Möglichkeit, mit geeigneten Zusatzgeräten elektronische Signaturen zu erstellen. Ich habe selbst im Frühjahr 2011 einen neuen Personalausweis erhalten und ihn für die Verwendung digitaler Signaturen vorbereiten lassen. Ich habe anschließend versucht, als privater Nutzer real die Fähigkeit zur digitalen Signatur zu erhalten. Das Ergebnis war ernüchternd. Keine der angeschriebenen Firmen war willens und in der Lage, meinen Ausweis für digitale Signaturen auszustatten, oder mir als privatem Nutzer auch nur das Verfahren zu nennen, nach dem digitale Signaturen erstellt werden können sollen. Nach daraufhin von mir eingeholter Auskunft der Bundesnetzagentur gab es zu diesem Zeitpunkt kein Unternehmen, das elektronische Signaturfähigkeit für die Ausweise privater Nutzer einrichten kann und/oder will.
Es gibt aber kommerziell erhältliche Smartcard basierte Tools die z.B. von Hochschulen gegen Lizenzgebühr genutzt werden könnten[siehe z.B. http://www.telesec.de/tcos/index.html]. Hierbei liegt der öffentliche Schlüssel des Unterzeichners nur auf der Smartcard vor und muss die Karte niemals verlassen. Der eigentliche Signaturvorgang erfolgt auf der Smartcard. Die Authentifizierung des Benutzers gegenüber einer Smartcard kann deutlich sicherer sein, als über die Tastatur direkt gegenüber einem PC. Der Unterzeichner muss im Besitz der Karte(und eines Lesegeräts) sein und über Kenntnis der PIN verfügen. Nach einer bestimmten Anzahl fehlgeschlagener Authentifizierungsversuche, das Bundesamt für Sicherheit in der Informationstechnik (BSI) fordert maximal 3, wird der Zugang gesperrt. Nur Smartcard basierte Tools erlauben, der eigenhändigen Unterschrift rechtlich gleichgestellte sogenannte qualifizierte Signaturen zu erzeugen. Ich habe im Oktober 2011 exemplarisch die im Internet veröffentlichten Datenblätter der Firma Telesec ausgewertet. Die Auswertung ergab, dass der sicherlich hochseriöse Anbieter auf Signaturkarten für die qualifizierte Signatur Algorithmen verwendet(als Hash: SHA-1 oder RIPMED 160, und als symmetrischer Algorithmus: DES, 3DES oder IDEA), die schon seit mindestens Juni 2008 nicht mehr vom BSI empfohlen werden[BSI ref: https://www.bsi.bund.de/cae/servlet/contentblob/477256/publicationFile/30629/BSI-TR-02102_V1_0_pdf.pdf]. Ich vermute, dass dieses möglicherweise bestehende Sicherheitsrisiko dem schwerfälligen Zertifizierungsprozess geschuldet ist und sich bei anderen Anbietern der qualifizierten elektronischen Signatur ebenso finden wird. Auf direkte Anfrage bei Telesec wurde mir mitgeteilt, dass

eine Auslieferung von Karten, die mit den vom BSI empfohlenen Algorithmen arbeiten in den nächsten Monaten geplant sei.
Weiterhin ist Teil des Geschäftsmodells, dass der Schlüssel vom Systemanbieter generiert und auf die Karte übertragen wird. Da zur Signatur ein kryptographisch sicherer Zufallszahlengenerator auf der Karte vorhanden sein muss, wäre es technisch am sichersten, den Schlüssel in der Karte bei Installation durch den Benutzer zu erzeugen. Dies wird gleichwohl nicht getan.
Es ist Teil des Sicherheitskonzeptes und des Geschäftsmodells, dem Signaturberechtigte keinen direkten Zugriff auf den Schlüssel zu geben. Dies dient dazu, den Signaturberechtigten vor Erpressung und auch vor eigener Nachlässigkeit oder Inkompetenz zu schützen. Allerdings wird hiermit der Signaturberechtigte auch an den Systemanbieter gebunden. Im Sicherheitskonzept führt dies zu einem Mischstatus sowohl des Unterzeichnungsberechtigten als auch des Systemanbieters: Der Unterzeichnende darf den Schlüssel nicht auslesen können, aber ihn benutzen, der Systemanbieter kennt und generiert den Schlüssel, muss ihn aber sicher wieder "vergessen". Ich persönlich halte dieses Konzept für problematisch. Die sich dadurch neu bildenden Sicherheitsgrenzlinien sind vielleicht schwer, aber in jedem Fall nur unelegant durch technische und organisatorische Maßnahmen zu verteidigen. Dieses Konzept erscheint aber als einziges geeignet, jedermann unabhängig von persönlicher Kompetenz die qualifizierte elektronische Signatur auf hohem Sicherheitsniveau sogar über einen nachlässig gepflegten Windows PC zu erlauben.

Tools: PGP

Es gibt seit vielen Jahren kostenfrei verfügbare Tools zur asymmetrischen Verschlüsselung und zur digitalen Signatur. Die Urversion dieser Tools heißt PGP [http://de.wikipedia.org/wiki/Pretty_Good_Privacy], aber inzwischen sind auch anders benannte Varianten vergleichbaren Funktionsumfanges verbreitet(PGP, GnuPG, OpenPGP, GPG4Win, PGPI, MacPGP, GPG Tools, WinPT, ..) Diese Tools sind grundsätzlich gut geeignet zur Anwendung im Hochschulbereich für die oben angeführten Anwendungsmöglichkeiten. Nach meinem Kenntnisstand stehen in diesen Tools die Verfahren der ersten Generation asymmetrischer Kryptographie, RSA und ElGamal, zur Verfügung.
PGP und viele abgeleitete Tools haben einen hohen Reifegrad erreicht und verfügen über die korrekte Implementation der zugrunde liegenden Algorithmen hinaus üblicherweise über ein hohes Niveau an professionellem "Security Engineering". So kann z.B. während des Ablaufs sicherheitskritischer Rechenoperationen die Auslagerung von relevantem RAM-Speicherinhalt auf ausgelagerte Swap-Bereiche der Festplatte blockiert sein.
Über eine Implementation des zukunftsfesteren ECC in diesen Tools ist mir bisher noch wenig bekannt. Bei GnuPG scheint an einer Umsetzung des ECC-Systems gearbeitet zu werden. Es steht aber in der aktuellen Version nicht zur Verfügung.
Weiterhin ist aus meiner Sicht die automatisch erfolgende Integration dieser Software Tools in das System des Benutzers und das selbstständige Tätigwerden der Tools hinderlich. Es ist nicht immer transparent, wann diese Tools was genau tun. So erzeugt z.B. meine Installation (GPG) mit der Signatur einer Mail offenbar automatisch auch eine Zeitdokumentation. Als Benutzer werde ich nicht darüber informiert, ob es sich dabei um meine Systemzeit handelt oder ein Zeit-Server abgefragt wird. Der Benutzer wird nicht informiert, inwiefern diese Zeitangabe kryptographisch gesichert verankert ist und ob er eine Möglichkeit hat, diese Zeitinformation ggf. zu unterdrücken oder zu korrigieren. Nach meiner Ansicht sollte ein kryptographisches Tool für die Signatur von Gutachten, Zeugnissen o.Ä. höchste Transparenz aufweisen. Es sollte nur tätig werden, wenn es vom Benutzer manuell aufgerufen wird und für den anstehenden Signaturvorgang ausdrücklich ermächtigt wird. Besonders beim RSA Verfahren kann eine automatisch erstellte Signatur eines ungeprüften Dokumentes durchaus ein erhebliches Sicherheitsrisiko darstellen.
Es erscheint mir weiterhin bei PGP nachteilig, dass auch viele nicht geheime und nicht verschlüsselte Daten in der radix64 Codierung ausgetauscht werden und dadurch die Lesbarkeit für Menschen und damit Transparenz unnötig verloren geht. PGP und dessen Verwandte sind in ihrer Benutzerschnittstelle für den Mail-Verkehr ausgelegt und optimiert, nicht für die manuelle Signatur einzelner Dokumente. Es wäre aber durchaus denkbar, durch Einsatz einer geeigneten graphischen Benutzeroberfläche PGP oder dessen Verwandte auch für die Verwendung z.B. der Signaturfunktion im Hochschulbereich zu verwenden. PGP ist sicherlich das ausgereifteste Tool und erlaubt dem kompetenten Benutzer im Gegensatz zur Smartcard einen privaten Schlüssel selbst zu erzeugen, der niemals außerhalb seines persönlichen Kontrollbereichs vorlag.

Tools: Academic Signature

Seit dem Frühjahr 2011 steht auf der Website http://www.fh-wedel.de/~an/crypto/Academic_signature_eng.html das Programm "Academic Signature" in einer Windows und einer Linux Version kostenfrei zur Verfügung. Dieses Tool ist für den Einsatz im Hochschulbereich konzipiert und optimiert. Chiffrierung, Signatur nach dem ECDSA-Verfahren und kryptographisch sichere Zeitstempel basieren auf dem modernen ECC-Verfahren. Standardmäßig wird eine Schlüssellänge von 256 Bit verwendet, die ein vergleichbares Sicherheitsniveau wie eine 3072-bit RSA-Implementierung bietet. Das Programm nutzt außer der Verwendung von projektiven Koordinaten keinerlei eventuell patentierte spezielle Techniken zur Effizienzsteigerung. Da projektive Koordinaten [http://en.wikipedia.org/wiki/Projective_space] schon seit Jahrhunderten in der Mathematik bekannt sind, sollten keine Patentkonflikte auftreten können. Trotzdem kann mit einem handelsüblichen Netbook bei sehr begrenzter Rechenleistung eine 256-bit Signatur in etwa einer Sekunde erstellt werden.

Signaturen und Zeitstempel liegen als Textfile vor und sind menschenlesbar. Alle Tätigkeiten des Tools erfolgen nur, wenn Sie explizit und manuell durch den Benutzer ausgelöst werden. Dies erfordert einen gewissen Kenntnisstand des Benutzers. Hierbei ist aber ein Grundverständnis z.B. der Abbildungen 2 und 3 dieses Artikels ausreichend. Der Benutzer sollte in den Grundzügen wissen, was beim Erstellen einer digitalen Signatur passiert. Nur durch Verbreitung solcher Grundkenntnisse kann meines Erachtens eine Akzeptanz der Verwendung neuer kryptographischer Techniken aufgebaut werden.

Seit fast einem Jahr setze ich Academic Signature routinemäßig für die Authentifizierung von Gutachten, Leistungsbestätigungen für Gaststudenten und Empfehlungsschreiben und für geschützten Datentransfer zu Kollegen und zwischen heimischem Arbeitsplatz und Hochschulbüro ein. Es besteht die Möglichkeit für unsere Studenten und Absolventen von mir mit dem Tool Academic Signature manuell erstellte ECDSA-Zeitstempel für Dokumente, Chiffren oder Hash-Werte zu erhalten.

Als nachteilig muss gesehen werden, dass das Tool recht neu ist und bislang nur von mir als Einzelperson entwickelt und gepflegt wird. Wie PGP erlaubt es keine qualifizierte Signatur aber ebenso wie bei PGP und im Gegensatz zur Kartenlösung kann der private Schlüssel ohne Beteiligung und Kenntnis fremder Instanzen innerhalb des eigenen Kontrollbereichs erzeugt werden. Der gegenüber PGP mangelnden Reife steht der Vorteil hoher Transparenz und Verwendung der neusten und zukunftsfestesten Algorithmen gegenüber.

Tools: Vertrauensmodelle

Grundsätzlich kann durch kryptographische Techniken kein Vertrauen erzeugt, sondern nur von einer primär vertrauenswürdigen Instanz abgeleitet und an eine bisher nicht zweifelsfrei vertrauenswürdige Instanz weitergegeben werden. Dabei gibt es verschiedene Modelle zur Ableitung des Vertrauens.

Vertrauensmodelle: Kette des Vertrauens - Chain of Trust

Der Anwendung der Signaturfunktion des neuen deutschen Personalausweises oder anderer Smartcard Lösungen liegt das Modell der "Chain of Trust" zugrunde. Eine zentrale Autorität signiert die öffentlichen Schlüssel von nachgelagerten Instanzen, nachdem sich die zentrale Autorität auf konventionellem Wege von der Identität der nachgelagerten Instanz und von der korrekten Übermittlung des öffentlichen Schlüssels dieser Instanz überzeugt hat. Dadurch kann gegenüber Dritten, die der primären Instanz vertrauen, Vertrauen auf die nachgelagerte Instanz übertragen werden. Die nachgelagerte Instanz wiederum kann ihrerseits wieder öffentliche Schlüssel der nächst tieferen hierarchischen Ebene signieren. Ein durch eine hierarchisch höherstehende Instanz signierter öffentlicher Schlüssel, der noch um mehr oder weniger sinnvolle Informationen angereichert sein kann, wird üblicherweise "Zertifikat" genannt. Ein Zertifikat verknüpft also einen öffentlichen Schlüssel einer Instanz mit einem öffentlichen Schlüssel einer höheren Instanz. Jeder Leser kann in seinem Internet Browser eine Liste der dort abgelegten Zertifikate ansehen.

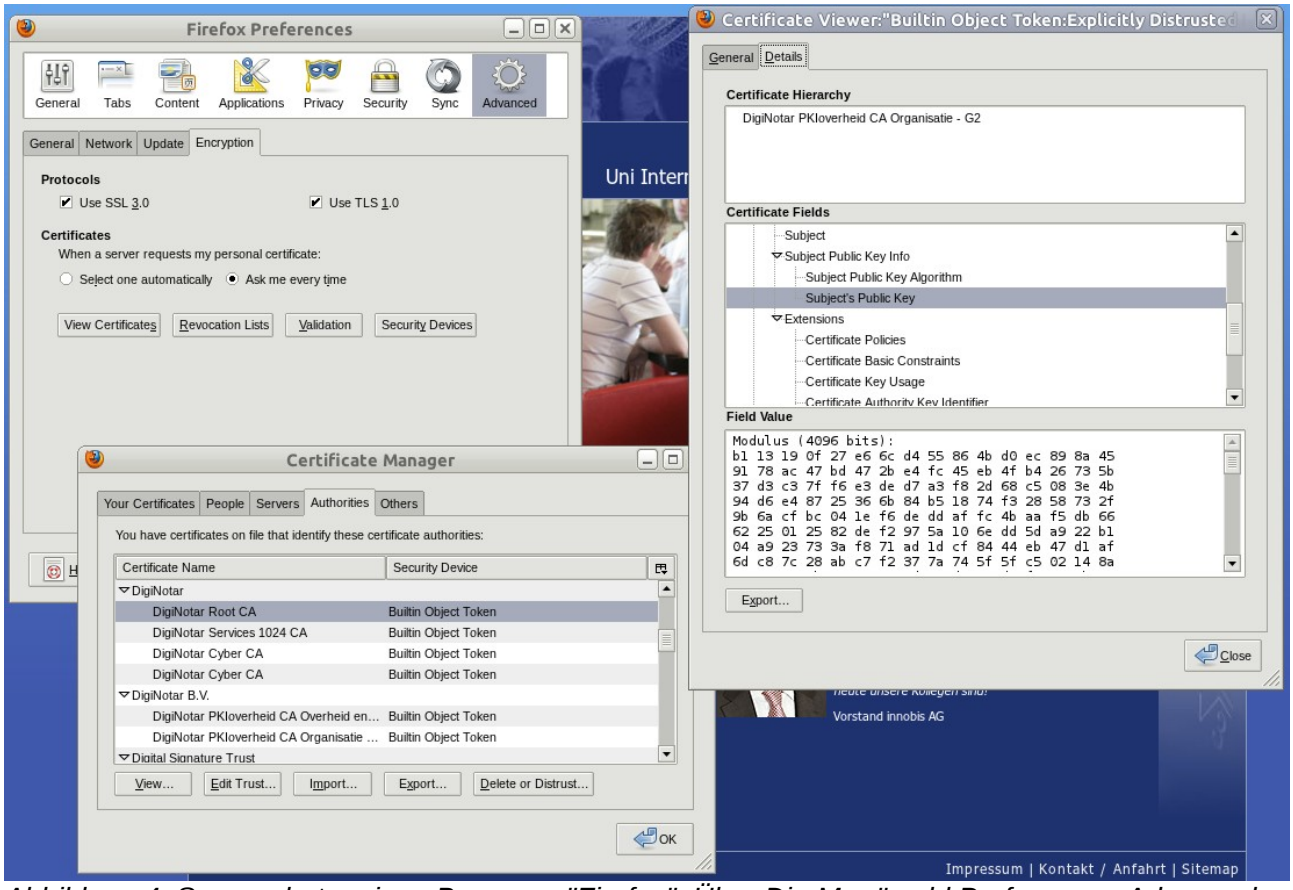

Abbildung 4: Screenshot meines Browsers "Firefox". Über Die Menüwahl Preferences-Advanced-Encryption-View Certificates-Authorities wurde hier als Beispiel das Root Zertifikat der Firma DigiNotar zur Ansicht ausgewählt. Es entbehrt nicht einer gewissen Ironie, dass ausgerechnet die inzwischen insolvente, durch einen banalen Hackerangriff im September 2011 fatal kompromittierte Firma DigiNotar durch die exorbitant große RSA-Schlüssellänge von 4096 Bit auffällt.

Diese Vertrauensstruktur kann von der zentralen Autorität über viele hierarchische Ebenen bis herunter zu Privatpersonen wie dem Autor oder dem Leser dieses Artikels ausgedehnt werden. Wenn einer Instanz in dieser Struktur z.B. dem Leser das Zertifikat einer Fremdinstanz, z.B. des Autors präsentiert wird, kann der Leser feststellen, ob sich die Kette der Zertifikate des Autors bis zur zentralen Instanz hinaufverfolgen lässt. Ist dies der Fall und vertraut der Leser der zentralen Instanz, kann der Zuordnung des öffentlichen Schlüssels zum Autor vertraut werden. In diesem Fall könnte also der Leser dem Autor eine mit dem öffentlichen Schlüssel des Autors chiffrierte Nachricht zukommen lassen und sicher sein, dass tatsächlich nur der Autor die Nachricht dechiffrieren kann. Der Leser kann dann darauf vertrauen, dass ihm nicht von einem Angreifer ein falscher öffentlicher Schlüssel untergeschoben wurde, um die für den Autor bestimmte Nachricht abfangen und dechiffrieren zu können.

In der Praxis funktioniert eine solche "PKI" (=Public Key Infrastructure) wegen der Vielzahl an möglichen Angriffsstellen oft nicht problemlos. Dies führt ein Vorfall aus dem September 2011 erneut vor Augen[http://en.wikipedia.org/wiki/DigiNotar]. Hier wurde eine hierarchisch hoch liegende Instanz, die niederländische DigiNotar BV auf simple Weise erfolgreich attackiert. Der Angreifer konnte sich u.A. gefälschte Zertifikate für die Firmen Google und Microsoft verschaffen.

Für den Einsatz im akademischen Bereich wäre der Einsatz des neuen deutschen Personalausweises in Verbindung mit diesem Vertrauensmodell meiner Auffassung nach zu bürokratisch, wenn denn diese Funktionen überhaupt zur Verfügung stünden. Der Einsatz einer funktionierenden, kommerziellen Smarcard-basierten Lösung wäre denkbar.

Vertrauensmodelle: Netz des Vertrauens - Web of Trust

Das "Web of Trust" ist als Vertrauensmodell zuerst von PGP implementiert worden[http://en.wikipedia.org/wiki/Web_of_trust]. Es ist nicht hierarchisch. Teilnehmer signieren gegenseitig öffentliche Schlüssel von Personen, denen sie vertrauen und bestätigen damit Ihr Vertrauen in die Zuordnung der Person zum entsprechenden Schlüssel. Diese Signaturinformationen

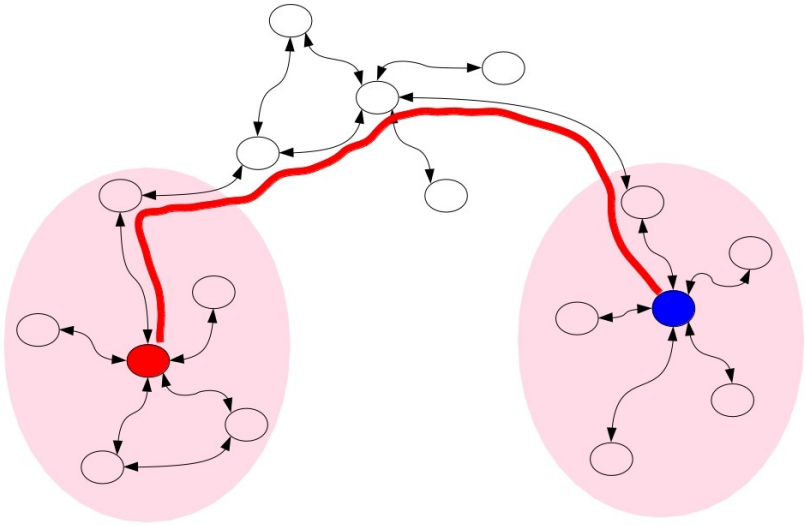

Abbildung 5: Netz des Vertrauens. Jeder Teilnehmer hat einen bestimmten lokalen Kreis, dem er vertraut. Die Kreise der Teilnehmer können überlappen und ein Netz bilden. Hier besteht durch die breite rote Linie angedeutet eine durchgehende Verbindung im Netz des Vertrauens zwischen den beiden durch ausgefüllte Symbole symbolisierten Teilnehmern. Ohne sich gegenseitig vorab zu kennen, können die beiden Teilnehmer davon ausgehen, dass die Zuordnung von Personenname zu öffentlichem Schlüssel vertrauenswürdig ist und z.B. vertraulich Daten austauschen.

werden auf zentralen Servern zusammengeführt. Dort können solche lokalen Vertrauensbeziehungen zu einem übergreifenden Netz des Vertrauens zusammengefügt werden. Wenn ein Teilnehmer mit einem anderen, ihm zunächst nicht bekannten Teilnehmer sicher kommunizieren möchte, braucht er den öffentlichen Schlüssel des Kommunikationspartners aus vertrauenswürdiger Quelle. Besteht im Netz des Vertrauens mindestens eine zwar indirekte, aber durchgehende Verbindung des Vertrauens zum anderen Teilnehmer, so kann der erste Teilnehmer davon ausgehen, dass die Verbindung von öffentlichem Schlüssel zur Person des Kommunikationspartners korrekt ist. Tatsächlich ist das Muster nicht ganz so simpel wie eben dargestellt, sondern es wird aus dem Netz ein quantitativer Parameter für die Vertrauensstärke der Verbindung beider Teilnehmer gebildet.

Das von PGP nutzbare Netz des Vertrauens transportiert keine verlässlichen Daten zur beruflichen Position der Teilnehmer und ist deshalb in der gegenwärtigen Form als Basis für Signaturverifikation im Hochschulbereich nicht nutzbar.

In der Praxis birgt die Teilnahme am Netz des Vertrauens gewisse Risiken für den Schutz persönlicher Daten, die im oben bereits zitierten Wikipedia Artikel ausgeführt sind. Diese Risiken können das ursprüngliche Ziel von PGP, die Sicherung der Privatsphäre, konterkarieren. Deshalb wird PGP oder seine Verwandten von vielen Hochschulangehörigen genutzt, ohne sich am Netz des Vertrauens zu beteiligen oder darauf zurückzugreifen. PGP kann auch auf Basis des nachfolgend beschriebenen "Mosaik des Vertrauens" genutzt werden.

Vertrauensmodelle: Mosaik des Vertrauens - Mosaic of Trust

Der von mir gewählte Ausdruck Mosaik des Vertrauens bezeichnet einen Mechanismus, mit dem der Teilnehmer die Vertrauenswürdigkeit einer Schlüsselzuordnung zu einer Person, die Vertrauenswürdigkeit vorgeblicher Attribute einer Person und die Gültigkeit eines Dokumentes auf Basis verschiedener Quellen bewertet. Dies ist auch das Vertrauensmodell, mit dem allseits die Vertrauenswürdigkeit von Papierdokumenten eingeschätzt wird. Folgende Mosaiksteine tragen bei Papierdokumenten zur Bildung des Vertrauens bei:

1.) Der semantische Test - Ist das Papier in einer dem vorgeblichen Verfasser angemessenen sprachlichen Form abgefasst?

2.) Kennen wir Namen und die berufliche Position des vorgeblichen Verfassers oder überzeugen uns auf unabhängigem Wege eingeholte Informationen von der Kompetenz des Verfassers, solche Dokumente auszugeben?

3.) Ist das Dokument auf dem Firmen/Hochschulbriefbogen geschrieben und kennen wir die Firma/Hochschule?

4.) Trägt das Dokument die (uns vielleicht sogar bekannte) Unterschrift des vorgeblichen Verfassers als handschriftlichen Schriftzug mit Tinte und/oder trägt das Dokument ggf. einen Stempel der Institution?

5.) Ist das Dokument unverändert (oder sehe ich "Kratzspuren" im Text)?

6.) Ist das Dokument auf dem erwarteten Weg z.B. Postsendung zu mir gelangt und sind Absender und Poststempeldaten plausibel?

Bei digitalen Dokumenten und Signaturen gilt das gleiche Grundmuster, aber die Mosaiksteine müssen punktuell etwas angepasst werden:

1.) Der semantische Test muss unverändert bestanden werden.

2.) Identische Fragen zu Namen und Position des vorgeblichen Verfassers wie zuvor bei Papierdokumenten. Informationen können falls nötig auch über das Internet eingeholt werden.

3.) Kann ich der von mir gewählten Quelle des öffentlichen Schlüssels des vorgeblichen Verfassers vertrauen?
Üblicherweise wird der öffentliche Schlüssel in der Firmen/Hochschul-Internetdomäne präsentiert: Ist die Schlüssel präsentierende Seite korrekt in den Internetauftritt der Firma/Hochschule eingebettet? Ist die Firma/Hochschule und deren Webseiten vertrauenswürdig?

4.) Ist die Signatur des Dokuments bei Prüfung gegen den von mir eingeholten öffentlichen Schlüssel des vorgeblichen Verfassers korrekt?
Bei korrektem Ausgang ist sowohl die Urheberschaft des Verfassers als auch die Unverändertheit des Dokumentes bestätigt.

5.) Optional: Ist ein ggf. vorhandener Zeitstempel korrekt und ist die bestätigte Zeit plausibel ?

6.) Ist das Dokument auf dem erwarteten Weg z.B. Mail zu mir gelangt und sind Absender und Begleitdaten plausibel?

Bei digitalen Dokumenten wie bei Papierdokumenten werden wir üblicherweise durch eine Kontaktaufnahme mit dem vorgeblichen Verfasser nachhaken, wenn auch nur einer der Mosaiksteine fehlt oder die Beantwortung der entsprechenden Frage nicht überzeugend ist. Sind alle Mosaiksteine vorhanden, werden wir dem Dokument vertrauen. Es ist durchaus möglich, sinnvoll und auch üblich, öffentliche PGP-Schlüssel im radix64 Format auf der in eine Hochschuldomäne eingebettete eigenen Website zu präsentieren. Dadurch können PGP und dessen Verwandte auch im Kontext des Mosaik des Vertrauens angewandt werden.

Das Mosaik des Vertrauens ist nach meiner Auffassung das am besten für die Anwendung im Hochschulbereich geeignete Vertrauensmodell. Willkürlich herausgegriffene Webseiten zweier Kollegen, die offensichtlich auf dieses Muster zurückgreifen, finden Sie z.B. unter: http://feynman.mit.edu/ike/homepage/index.html und http://wwwhome.ewi.utwente.nl/~sape/ .

Auch das oben beschriebene neue Tool Academic Signature legt dieses Vertrauensmodell zugrunde. Den öffentlichen ECC-Schlüssel des Verfassers dieses Artikels können Sie unter der Webadresse

http://www.fh-wedel.de/~an/crypto/academic_signature_key.html, eingebettet in den Webauftritt der Fh-Wedel erhalten.

Einsatz im Hochschulbereich: Ausblick

Auf der Ebene einzelner Hochschullehrer werden die neuen Möglichkeiten der asymmetrischen Kryptographie bereits punktuell genutzt und die Anwendung wird sich weiter verbreiten.

Ich bin überzeugt davon, dass in einiger Zeit die Mehrzahl der Hochschulen zusätzlich zu den klassischen Zeugnissen auch von der Hochschulleitung digital signierte digitale Zeugnisse ausgeben werden. Der hohe Nutzwert für die Absolventen, die dramatisch erhöhte Fälschungssicherheit und die immer weitere Verbreitung von Online-Bewerbungen lassen keine andere Prognose zu.

Es ist allerdings schwer, die Zeit zu prognostizieren, die bis zur Etablierung verstreichen wird. Sicherlich hängt sie in großem Maße von der Aufgeschlossenheit der Hochschuladministrationen gegenüber Neuerungen ab. Wenn keine Smartcard Lösung gewählt wird, sollte dort auch die Bereitschaft vorhanden sein, sich einfache Grundkenntnisse der Kryptografie anzueignen und sich gegenüber Apple, Microsoft oder anderen Instanzen die ggf. verlorene Hoheit über den eigenen Computer und dessen Festplatte zurückzuerobern.

Die Kosten dafür, digitale Signierung von Zeugnissen und Diplomen mit der höchsten, ohne Smartcard erreichbaren Sicherheitsstufe zu realisieren, sind sehr überschaubar. Man benötigt ein ausschließlich für den Zweck der Signatur vorgesehenes Notebook, das nach der Installation relevanter Programme(PGP o.Ä.) keine Netzwerkverbindung mehr hat und einen Safe für die Verwahrung dieses Notebooks. Weiterhin sollte eine Einweisung für den Unterzeichner der Zeugnisse und ggf. das Personal des Prüfungsamtes erfolgen. Für den Transport der Dokumente und Signaturen zwischen Signatur-Notebook und der Außenwelt sollten frisch formatierte oder fabrikneue Memory Sticks oder SD-Karten verwendet werden. Auf einer besonders gut geschützten Hochschul-Website können die öffentlichen Schlüssel gegenwärtiger und früherer Unterzeichner von Zeugnissen präsentiert werden. Weiterhin benötigt man natürlich ein Software Tool zur Signatur und ein für jeden frei erhältliches Tool zur Verifikation. Selbst wenn man von den hier dargestellten organisatorischen Maßnahmen aus Gründen der Praktikabilität gewisse Abstriche macht, wird man in aller Regel dennoch ein vielfach sichereres Verfahren erhalten, als derzeit mit Papierzeugnissen realisiert wird.

Bei kompetentem, sicherheitsbewussten Verhalten des Unterzeichners wären meines Erachtens die aussichtsreichsten Angriffe 1.) ein banaler Erpressungsversuch, 2.) ein Angriff auf die den öffentlichen Schlüssel präsentierende Website oder 3.) die Auswertung der während der Unterzeichnungen durch das Netbook abgestrahlten elektromagnetischen Strahlung von einem benachbarten Raum aus.

Die Entwickler von Tools für Signaturen, Chiffren und Zeitstempeln sind aufgerufen, die Nutzung der neuen Möglichkeiten unter maximaler Transparenz und Kontrollierbarkeit zu implementieren. Nur dann werden Personen bereit sein, mit großer Selbstverständlichkeit digitale Signaturen herauszugeben oder zu akzeptieren. Der Signierer muss das Gefühl haben, die digitale Signatur genauso direkt kontrollieren und ggf. im letzten Moment zurückhalten zu können, wie eine eigenhändige Unterschrift mit Tinte auf Papier.