

# Einführung und Betrieb von X.509-basierten Anwendungen

Michael Bell  
michael.bell@cms.hu-berlin.de

*Dieser Artikel soll primär einen Einblick in den Einsatz von Zertifikaten in der Verwaltung der Humboldt-Universität am Beispiel der E-Mail-Verschlüsselung der Personalabteilung geben. Sekundär soll dieser Artikel genutzt werden, um über einen fast schon chronologischen Aufbau den Entstehungsweg einer PKI-Anwendung nachzuzeichnen.*

Viele Entscheider entdecken oft Artikel wie den vorliegenden über funktionierende Endsysteme und fordern diese hoch entwickelten Systeme dann folgerichtig auch für ihre Einrichtungen. Die Entwickler sehen dies meist genauso. Leider gehen die Ideen zum Prozess einer solchen Einführung meist genauso schnell auseinander, wie die gemeinsame Einsicht gefunden wurde.

Die Entwickler auf der einen Seite sind mit den Wünschen der Entscheider überfordert, weil diese sich ein sofort funktionierendes System mit allen nur erdenklichen Features wünschen. Auf der anderen Seite verstehen die Entscheider oft nicht, warum es so problematisch ist, eine komplett beschriebene Anwendung nachzubauen. Eine schrittweise Einführung eines Systems ist schließlich auch teurer, als ein sofort zur Verfügung stehendes System. Eine einseitige Schuldzuweisung ist also fehl am Platz. Vielmehr ist ein Miteinander und Verständnis für die Probleme und Ziele der »anderen« Seite gefragt. Selbst Einrichtungen, die über eine langjährige Erfahrung verfügen, starten mit solchen komplexen Systemen nicht von 0 auf 100, sondern führen diese schleichend und meistens mit einem gewissen Evolutionsprozess ein. Oft ist es allerdings erforderlich Anwendungen sehr schnell zur Verfügung zu stellen, weil es einen akuten Bedarf gibt.

Bevor nun die eigentliche Lösung beschrieben wird, sei an dieser Stelle der Hinweis gestattet, dass auch diese Lösung nicht vom Himmel gefallen ist und

auf vielen Erfahrungen und auch Fehlern basiert, die wir machen durften – und das ist nicht ironisch gemeint. Es erfordert ganz im Gegenteil ein hohes Maß an Toleranz und viel Verständnis für technische Probleme seitens unserer Endkunden, um neue Technologien erfolgreich einführen zu können.

## Ursache und Wirkung

Der Ursprung für die Idee der Verschlüsselung von E-Mails mit personenbezogenen Daten war die anstehende Umstellung unseres Mailservers von Banyan VINES zu einem SMTP-konformen Dienst. VINES stellte einen proprietären Dienst zur Verfügung, der durch eigene proprietäre Protokolle und eine rudimentäre Verschlüsselung geschützt war. Mit dem Ende der Herstellerfirma und dem Auslaufen des Supports für das Produkt musste eine neue E-Mail-Lösung gefunden werden. Neben diversen Forderungen an die Funktionalität des Dienstes war von Anfang an klar, dass es sich um einen Standardserver handeln muss, weil niemand mehr bereit war, ein Risiko wie mit VINES einzugehen. Eine solche Umstellung verursacht mehr als nur kleine Schmerzen.

Aus organisatorischen und technischen Gründen stellte sich schnell heraus, dass dieser Mailserver, wie auch alle anderen Mailserver der Universität, außerhalb der Firewall stehen musste. Die Entscheidung fiel am Ende zugunsten des SuSE-E-Mailservers. Dieser basiert auf Open Source, war aber gleichzeitig ein kommerzielles Produkt, für welches sowohl Herstellersupport als auch Patches verfügbar waren. Mit dieser Entscheidung stand der CMS aber plötzlich vor gänzlich neuen Herausforderungen.

## Herausforderungen

Mit der Umstellung auf das neue System mussten die internen Arbeitsabläufe unter einem völlig neuen Aspekt betrachtet werden. Bis zu diesem Zeitpunkt konnte mit VINES davon ausgegangen werden, dass die Daten innerhalb des Mailsystems sicher waren. Nun wurden plötzlich personenbezogene Daten nicht nur im Klartext durch den Netzwerkbereich vor der Firewall transportiert, sondern sie lagerten dort auch in unverschlüsselter Form.

Dies war weder seitens des Datenschutzes noch gemäß unserem eigenen Selbstverständnis hinnehmbar. Allein das potentielle Risiko einer Kompromittierung von Daten unserer Mitarbeiter war in diesem Ausmaß inakzeptabel. Es ist keinem Mitarbeiter vermittelbar, dass seine persönlichen Daten bei der Personalabteilung zwar unter organisatorischen, aber nicht unter technischen Gesichtspunkten sicher sind.

Aus diesen sehr allgemeinen Anforderungen kristallisierte sich sehr schnell die Forderung heraus, dass die Daten außerhalb des Verwaltungsnetzes nur in verschlüsselter Form gelagert werden dürfen. Selbst ein Einbruch in den Mailserver oder in unsere zentralen Netzkomponenten sollte keine Kompromittierung kritischer Daten zur Folge haben. Des Weiteren sollte das System in Zukunft auch erweiterbar sein. Aus anderen Pilotprojekten hatten wir zu diesem Zeitpunkt bereits gelernt, dass proprietäre Lösungen immer Inseln mit hohem Wartungsaufwand und geringer Akzeptanz bilden. Die Nutzer haben einfach keine Lust auf n+1 verschiedene Systeme. Insbesondere verschwindet die Akzeptanz endgültig, wenn es nicht möglich ist, diese Systeme auf andere Nutzerkreise auszudehnen, dann tritt endgültig ein Unverständnis ein. Die IT-Verantwortlichen legten zusätzlich Wert auf ein

System mit zentraler Steuerung. Zum Schluss wollte niemand die Verantwortung für ein potentiell wackeliges Verschlüsselungssystem haben.

Das vorerst letzte Problem, welches einer Lösung bedurfte, war die Etablierung eines Key-Recovery-Systems, welches sowohl nichtwillentliche Schlüsselverluste als auch krankheitsbedingte Ausfälle und ähnliches kompensieren konnte. Die besondere Herausforderung bildete hier der Datenschutz, der zum einen gesetzlich vorgeschrieben und zum anderen für die Akzeptanz zwingend erforderlich ist. Nichts ist für ein neues System schlimmer, als wenn auf Seiten der Anwender die Angst besteht, dass ein unbefugtes Aufbrechen von E-Mails zwecks Überwachung oder anderer nicht legaler Ziele möglich ist. Ein solcher Vertrauensverlust würde das System innerhalb kürzester Zeit überflüssig machen und einen Großteil der Arbeitsabläufe innerhalb der Verwaltung blockieren.

## Voraussetzungen

Die Mitarbeiter der Abteilung DV in der Verwaltung konnten im Rahmen mehrerer DFN-Projekte bereits ausgiebig Erfahrungen mit verschiedenen Verschlüsselungsverfahren und PKIs sammeln. Die technologischen Grundlagen der verschiedenen Lösungsansätze waren also bereits vorhanden. Dies ist keinesfalls zu unterschätzen, da diese Erfahrung zum damaligen Zeitpunkt mehr als vier Jahre Zeitvorsprung ausmachte. Außerdem existierte schon eine X.509-basierte PKI.

Neben schwer messbaren Größen, wie z. B. vorhandenem Wissen und bereits bestehender Erfahrung, gab und gibt es auch handfeste Vorteile gegenüber anderen Einrichtungen. Sämtliche in Frage kommenden Verwaltungsrechner verfügen über eine einheitliche Installation mit standardisierter Software und ebenso standardisierten Wartungsverfahren. Zu dieser Standardsoftware gehört auch der Einsatz von Netscape bzw. Mozilla. Die PKI wurde zusammen mit Mozilla bereits für verschlüsselte Mail- und Web-Anwendungen benutzt. Dabei wurden sogar Smartcards erprobt. Die wesentliche Neuheit bestand in der Anzahl der

Nutzer. Es ging hier nicht um 10 oder 15 Nutzer, die verteilt über ein Jahr ihre Zertifikate bekommen sollten, sondern um mehr als 70 Nutzer, die gleichzeitig (maximal innerhalb eines Tages) die neue Technik bekommen mussten und dann eventuell dazu auch noch Fragen hatten.

## Lösungsansatz 1. Versuch

Wie der Name schon andeutet: *nobody is perfect*. Die Entscheidung für eine X.509-basierte PKI war gefallen, nachdem festgestellt wurde, dass die Infrastruktur zentral verwaltet werden muss. Genauso schnell schied Smartcards aus, da sie weder ausgereift waren, noch zum damaligen Zeitpunkt stabil genug liefen. Der Kostenfaktor war und ist auch nicht zu vernachlässigen, weil neben den hohen Anlaufkosten für Smartcards und Reader zusätzlich ein Wartungs- und Supportaufwand für Karten und DLLs auf den Rechnern entsteht. Aufgrund der vorhandenen Installationsbasis stand Netscape/Mozilla als S/MIME-Client ebenfalls von vornherein fest.

Die Erfahrungen mit unseren wenigen Testnutzern aus den Pilotprojekten hatten gezeigt, dass selbst technisch versierte Nutzer ihre liebe Mühe und Not mit der Online-Beantragung von Zertifikaten haben. Die oft nicht ausgereifte Oberfläche der Browser tat ihr Übriges. Als Verfahren für den Roll-Out wurde also der Versand von PIN-Briefen und die Verteilung von PKCS#12-Dateien beschlossen. Bei der Verteilung der PKCS#12-Dateien kam uns die homogene Infrastruktur unserer Verwaltungs-PCs zu Hilfe. Die Dateien konnten direkt über die Netzlaufwerke verteilt werden. Die Dateien selbst waren durch 128-Bit-Passwörter geschützt. Zusätzlich wurde eine zentral generierte Zertifikatsdatenbank zur Verfügung gestellt, da der Wunsch bestand, die schon erstellten Zertifikate der Kollegen gleich zur Verfügung zu haben.

Schließlich blieb als letzter Brocken noch das Key Recovery übrig. Die Notwendigkeit stand nie in Frage, aber wie sollte es etabliert werden, ohne dass die Mitarbeiter das Vertrauen in das System verlieren? Die Lösung war der Einsatz

eines separaten kryptographischen Schlüssels zur Verschlüsselung der privaten Schlüssel der Mitarbeiter und die Hinterlegung dieser gesicherten privaten Schlüssel in einem Safe in einem Umschlag, der nur in zwei Situationen geöffnet werden durfte:

1. Der Eigentümer (Mitarbeiter) stellt selber einen Antrag.
2. Der Abteilungsleiter ordnet dies mit schriftlicher Zustimmung des Datenschutzbeauftragten an, wenn es einen dringenden dienstlichen Anlass dafür gibt.

Der Datenschutzbeauftragte genießt im Normalfall – zumindest an der Humboldt-Universität – ein hinreichendes Vertrauen, um den Mitarbeitern die Sicherheit zu geben, dass ein Missbrauch ausgeschlossen ist. Er ist zudem inhaltlich nicht weisungsgebunden und war mit diesem Verfahren einverstanden.

Für das Key Recovery bleibt abschließend festzuhalten, dass wir es nicht ein einziges Mal einsetzen mussten. Allerdings erzwang es den Ausstieg aus der Hierarchie der DFN-PCA, weil Key Recovery im technischen Sinne dort nicht erlaubt war.

Im Laufe des Jahres 2004 wurden dann unsere Befürchtungen wahr und unsere Sicherheitsanalysen und -konzepte erwiesen sich leider als richtig. Der Mailserver der Verwaltung wurde gehackt. Neben dem nicht geringen Stress und dem Ausfall eines Großteils unserer Verwaltungsprozesse bewies gleichzeitig die Mailverschlüsselung ihre Wirksamkeit. Mails der Personalabteilung mit personenbezogenen Daten waren nicht gefährdet. Manchmal kann eine Katastrophe auch Vorsorgemaßnahmen bestätigen – ohne dass erst der vollständige Schadensfall eintreten muss. Es sollte aber niemand erwarten, dass wir jetzt Hurra rufen, wenn wir von Hackern besucht werden.

## Probleme

Natürlich sind komplexe Systeme nie eine Erfolgsgeschichte ohne kritische Nebentöne. PKI-Lösungen sind hier keine Ausnahmen. Die Lösung für das Key

Recovery zog mehrere negative Konsequenzen nach sich. Durch das Ausscheiden aus der DFN-PCA mussten wir plötzlich zwei Root-CAs verteilen – eine für alle (DFN-PCA) und eine für die Personalabteilung (HU-UV Root). Zusätzlich wurde unsere PKI nicht wirklich einfacher durch den Einsatz eines Verfahrens zum Key Backup. Organisatorisch war die Lösung stark von den eingesetzten »Technikern« abhängig. Es gab zwar eine starke Kontrollinstanz in Person des Datenschutzbeauftragten, aber in den Arbeitsprozess selbst waren zu viele Personen involviert.

Die entscheidenden Fragen waren also: Können wir in die DFN-PCA zurück und lässt sich der Aufwand reduzieren?

## Lösungsansatz 2. Versuch

CAs haben die von vielen als unschön bezeichnete Eigenschaft, dass sie irgendwann ablaufen. Gleichzeitig ist dies aber auch die Chance, einmal begangene Fehler nach einer gewissen Zeit korrigieren zu können. Unser Hauptproblem hieß Key Recovery und unsere Antwort war überraschenderweise eine rein organisatorische Lösung, die die technischen Probleme löste.

Ein kurzes Gespräch mit der Personalabteilung führte zu dem Ergebnis, dass der CMS einfach die PKCS#12-Dateien aufheben könnte und die PIN-Briefe mit 128-Bit starken Passwörtern nach der erstmaligen Installation der PKCS#12-Dateien in einem Safe hinterlegt werden. Der Zugriff auf diese Briefe – das Key Recovery – wird genauso kontrolliert wie beim technischen Verfahren. Dass heißt ohne den Mitarbeiter und ohne den Datenschutzbeauftragten geht gar nichts. Dies wird per Dienstanweisung sichergestellt.

Seit der Einführung des neuen Verfahrens wurde das Key Recovery wegen eines vergessenen Passwortes schon öfter benötigt, womit sich die Frage stellt, was in der Zeit vor dem neuen Verfahren passiert ist. Zitat: »Verschlüsselung funktionierte schon immer, nur die Entschlüsselung noch nie.« Mittlerweile wird sogar darüber nachgedacht, das Key Recovery ganz zu streichen und nur

noch ein einfaches Key Backup durchzuführen. Dies würde bedeuten, dass nur der Mitarbeiter selbst über die Wiederherstellung entscheidet, da aus Sicht des Arbeitgebers keine unwiederbringlichen Dinge in den E-Mails stecken können. Es bleibt festzuhalten, dass manchmal auch bei komplexen Fragestellungen die beste Lösung ein organisatorischer Prozess und nicht eine technische Sonderlocke ist. Fazit: Es gibt auch Nicht-Techniker mit coolen Ideen :)

## Immer noch Probleme

Wie jeder andere Mensch gewöhnen auch wir uns sehr schnell an einen gewissen Komfort und finden meist in kürzester Zeit neue Dinge, die uns nerven und den reibungslosen Betrieb – nein, nicht unseren Büroschlaf – behindern.

Die Erstellung einer neuen Cert-DB ist nicht nur aufwendig, sondern im Nachhinein nicht wirklich hilfreich. Am Anfang erspart man sich einen Punkt bei der Weiterbildung. Spätestens bei den ersten Neueinstellungen oder Versetzungen in der Personalabteilung gibt es ein Problem. Die Zertifikate sind nicht in den vorgenerierten Datenbanken der Browser und niemand weiß, wie man an die neuen Zertifikate der neuen Kollegen herankommt. Zusätzlich bekommen auch hin und wieder andere Personen Zertifikate. Diese finden manchmal auf magische Weise ihren Weg in das Mailprogramm und manchmal eben nicht. Ein hoher Aufwand mit einer Außerbetriebnahme aller Mailclients der Personalabteilung (zur Installation der neuen Cert-DB) in Kombination mit einem zweifelhaften Nutzen ruft nach Veränderung. Zusätzlich gehen bei der Aktualisierung der Cert-DB alle bereits nachinstallierten Zertifikate verloren.

## Lösungsansatz 3. Versuch

Der nächste Versuch wird sicherlich das Problem Cert-DB angehen. Dies ist aber eine eher kleine Änderung. Somit stellt sich die Frage: Sind wir nun glücklich und zufrieden (bis an unser Lebensende)? Selbstverständlich nicht.

Zum einen gibt es immer wieder neue Nutzer und zum anderen sind neue Anwendungen natürlich auch kein Problem. Die ersten Test-Nutzer, die Notebooks mit sensiblen Daten einsetzen, wurden bereits mit Smartcards für Festplattenverschlüsselung ausgerüstet. Zusätzlich ist der VPN-Bereich weiterhin in Bewegung. Die voranschreitende Dezentralisierung von IT-Systemen oder besser deren Nutzern wird die Anzahl der auftretenden Sicherheitsprobleme auch in Zukunft steigen lassen.

Es bleibt abschließend festzuhalten, dass wir für die Zukunft sicher gut gerüstet sind und uns genauso sicher die Arbeit nicht ausgehen wird. Perfekte Lösungen wird es nie geben, aber mit viel gutem Willen und beiderseitigem Verständnis wird es auch weiterhin funktionierende und vor allem sichere Lösungen geben – die hoffentlich nicht immer ihre Eignung in der Praxis beweisen müssen.