Aspekte der Authentifizierung und Signaturen anhand der Erfahrungen eines produktiven Internetservice zur Archivierung digitaler persönlicher Dokumente

Prof. Dr. Reiner Hüttl

FH Rosenheim
Fachbereich Informatik
huettl@fh-rosenheim.de

Abstract: Es gibt seit Jahren die Techniken zur sicheren Übertragung und Abspeicherung digitaler Daten in einer vernetzten Welt: Digitale Signaturen, PKI, Verschlüsselungstechniken, Hardware-Token, etc. Daraus würde man folgern, dass es nicht weiter schwer wäre, darauf aufbauend einen sicheren Internetdienst zur Kommunikation und Abspeicherung privater Daten zu implementieren. In der Praxis befindet sich ein solches Sicherheitskonzept in einem kontroversen Spannungsfeld gegenläufiger Interessen, bei dem die ursprünglichen Ziele nicht selten aus den Augen verloren werden. Der folgende Beitrag beschreibt die Stadien eines sicheren Internetdienstes von der Konzeption bis zur Realisierung anhand einer real existierenden Anwendung.

1 Einleitung

Als Anwendung betrachten wir einen Internetservice zur Archivierung vertraulicher Dokumente. An diesem Dienst sind, wie in Abb. 1.1 zu sehen, drei Parteien beteiligt: Die Dokumentenerzeuger, das Dokumentenarchiv und die Benutzer. In diesem Service werden digitale Dokumente, wie z.B. Kontoauszüge, Telefonrechnungen, auf eine sichere Art und Weise zu den Kunden übertragen und anschließend dauerhaft gespeichert. Als Vermittler fungiert hier eine vertrauenswürdige dritte Instanz, an die solche Dokumente automatisch übertragen werden. Dort werden sie klassifiziert, strukturiert in Benutzerkonten eingestellt und dauerhaft archiviert. Die Benutzer haben wiederum durch das Internet 24 Stunden und weltweit Zugriff auf die Daten.

2 Sicherheitskonzept und Implementierung dieses Konzepts

Zunächst werden im Rahmen einer Sicherheitspolitik (*Security Policy*) die strategischen Sicherheitsziele, Sicherheitsgrundsätze und Rahmenbedingungen festgelegt, um eine ausreichende IT-Sicherheit zu erreichen

Abb. 1.1 Die Beispielanwendung: ein Internetarchiv

Für das beschriebene Internetarchiv sind folgende Sicherheitsziele festgelegt:

- Integrität der Information
- Wahrung der Vertraulichkeit der Daten
- Nichtabstreitbarkeit und strenge Authentifizierung
- Verfügbarkeit bei Bedarf

Zu jedem der angestrebten Sicherheitsziele gibt es bereits bewährte technische Verfahren aus dem Bereich der Kryptographie [SC96]. Die Integrität der Dokumente kann z.B. durch digitale Signaturen bewiesen werden. Solche Signaturen können auch bei der Authentifizierung eingesetzt werden. Zur Wahrung der Vertraulichkeit bieten sich Verschlüsselungstechniken an, sowohl bei der Übertragung der Daten als auch bei der Ablage. Das letzte Ziel, die Verfügbarkeit, wird durch eine mehrschichtige skalierbare Architektur mit redundanten Komponenten erreicht.

Nach Analyse der möglichen Verfahren, Algorithmen und vorhandenen Standards bietet sich für den Internet-Service ein Sicherheitskonzept mit folgende Vorgaben an:

- Verschlüsselte Übertragung aller Daten
- Verschlüsselung von Daten auf Server-Seite und auf Client-Seite
- Mehrstufige Authentifizierungslevel (z.B. Benutzername und Passwort, SmartCard mit Pin-Eingabe)
- Automatische Digitale Signaturen bei der Ablage zum Schutz der Dokumente
- Digitale Signaturen auf Benutzerseite zur Nichtabstreitbarkeit
- Hohe Verfügbarkeit durch Auswahl zuverlässiger Soft- und Hardware
- Einsatz von speziellen Hardwarekomponenten zur Erreichung höherer Sicherheitsniveaus

Solch ein Konzept kann im Rahmen der geforderten Entwicklungszyklen und des Kostendrucks im Internet normalerweise nur schrittweise umgesetzt werden. Es ist aber möglich, die wesentlichen Sicherheitsziele zu berücksichtigen und eine ausbaufähige Sicherheitsarchitektur zu entwerfen. Wesentlich ist, das man hier auf offene Standards

setzt, proprietäre Hardware vorerst nicht berücksichtigt und möglichst wenig Voraussetzungen auf den Clientrechnern bei den Kunden verlangt.

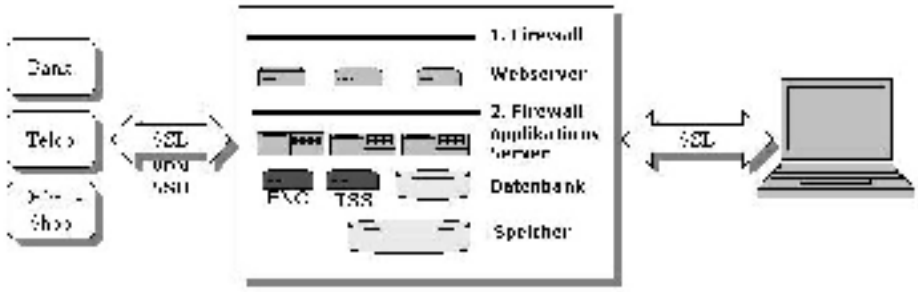

Abb. 2.1 Multi-Tier Sicherheitsarchitektur eines Internetdienstes mit Verschlüsselung (ENC) TimeStampService (TSS) und sicherer Übertragung (SSL)

Der erste Kern einer Sicherheitsarchitektur ist in Abb. 2.1 zu sehen. Er enthält eine verschlüsselte Übertragung aller Daten ohne Einschränkung, basierend auf den SSL, SSH, oder VPN. Nach der Übertragung werden alle vertraulichen Daten in einem mehrstufigen Verschlüsselungsverfahren mit dem AES (Advanced Encryption Standard) archiviert. Zusätzlich werden alle eingehenden Dokumente automatisch mit einer digitalen Zeitstempel-Signatur versehen, zum Beweis der Integrität der Dokumente. Die Authentifizierung wird zunächst mit dem vielseitigsten Verfahren, Benutzername – Passwort, realisiert. Die ganze Applikation, die ja nicht nur aus Sicherheitskomponenten besteht, wird in eine mehrstufige Systemarchitektur von Firewalls, Web- und Applikations-Server eingebettet. Alle Komponenten sind redundant ausgelegt und es werden bewährte Systeme eingesetzt (z.B. Unix Workstation, J2EE Container).

Die offene Architektur und Verwendung von Standards lässt Optionen für einen Ausbau der Sicherheitsstufen zu:

- Höhere Authentifizierungslevel mit Software-Zertifikaten oder hardware-geschützte Zertifikate (SmartCards)
- Einbau von Hardware-Einheiten für die SSL-Verschlüsselung und die digitalen Signaturen (Zeitstempeleinheiten)
- Client-seitige Verschlüsselung von Dokumenten mit Maßnahmen zum Keyrecovery
- Client-Signaturen aufbauend auf einer PKI (Public Key Infrastruktur)

3 Randbedingungen

In diesem Abschnitt kommen nun die Randbedingungen unter denen sich ein Sicherheitskonzept behaupten muss. Die Sicherheit in einem komplexen System wird nicht durch die eingesetzten mathematischen und technischen Verfahren gegeben. Sie ist vielmehr eine Kette von Verfahren und Prozessen und nur so stark wie ihr schwächstes Glied [SC00]. Bei allen Sicherheitsmassnahmen ist die Bequemlichkeit und mangelnde

Sensibilisierung für Sicherheitsaspekte beim Menschen zu beachten. Insbesondere alle Prozesse mit menschlicher Beteiligung sind potentielle Gefahrenherde für die Unterwanderung des Sicherheitskonzeptes.

3.1 Mobilität

Eine Hauptmotivation für das Internet ist die weltweite Verfügbarkeit der Dienste und damit eine grenzenlose Mobilität. Dies bedeutet, das der Benutzer nicht immer auf seinen eigenen PC zurückgreifen kann. Damit fallen alle proprietären Clients aus dem Konzept. Nur was ein Standard-Browser in einem beliebigen Internetcafe darstellen kann, ist geeignet. Dadurch sind aber Digitale Signaturen auf der Client-Seite, zumindest basierend auf SmartCards, nicht generell einsetzbar. Denn in absehbarer Zukunft wird dafür keine Infrastruktur allgemein verfügbar sein. Als einzige Alternative verbleiben Ansätze, den Schlüssel verschlüsselt über den Server auf einen beliebigen Client zu laden. Solche Verfahren werden aber nicht den Standard eines Signaturgesetzes erreichen.

3.2 Kosten und Zeitdruck

Die immer kürzeren Entwicklungszyklen und der steigende Kostendruck in der Internetbranche führen auch bei der Sicherheit zu Kompromissen. Dies führt zu Teilrealisierungen des ursprünglich geplanten Konzeptes und zu einem eher zurückhaltenden Einsatz von teurer Hardware, die einen höheren Schutz für die kryptographischen Operationen bieten würde. Erschwerend kommt hier hinzu, das Sicherheit meist nicht sichtbar ist und selten als Funktionalität verkauft werden kann.

3.3 Integration mit Fremdsystemen

Als Internetservice ist es sehr schwer alleine zu überleben. Deshalb wird oft durch offene Schnittstellen und einer flexiblen Produktgestaltung eine Integration zu den großen Webseiten angestrebt. Ein Ausprägung ist die Portalintegration. Hier verschwindet der Service beinahe oder vollständig in dem Webportal des Partners und damit z.B. die Sichtbarkeit der SSL Verbindung. Die zweite Ausprägung ist eine SingleSignOn Authentifizierung. Der Kunde hat sich lediglich bei der Partnerseite zu authentifizieren. Bei einer Anfrage des Archivierungsdienstes wird er ohne weitere Belästigung an das Internetarchiv weitergeleitet. Damit reduziert sich die Qualität (oder steigert sich in seltenen Fällen) auf den Sicherheitslevel der Partnerseite. Das eigene Sicherheitskonzept wird völlig übergangen. Das liegt daran, das die großen Partner und der eigene Vertrieb und Marketing solche Strategien trotz Sicherheitsbedenken forcieren.

3.4 Projektgeschäft

Kleine Internetservices können ihr Produkt selten in unveränderter Version anbieten. Speziell bei großen Kunden ist oft eine projektspezifische Erweiterung notwendig.

Solche Erweiterungen entstehen immer unter großen politischen und zeitlichen Druck. Nicht selten werden dabei die Grundprinzipien des Sicherheitskonzeptes aus pragmatischen Gründen verletzt. Zudem schafft jede Sonderlösung, jede zusätzliche Schnittstelle neue Angriffspunkte auf das zentrale System.

3.5 Services und Mehrwertdienste

Internetdienste wollen ihren Kunden meist Mehrwert durch zusätzliche Dienste anbieten. Solche Dienste basieren auf den Kundendaten, in unserem Beispiel die Dokumente des Kunden. Dazu müssen die Daten des Kunden für den Service lesbar sein, was der Privatsphäre des Kunden widerspricht. Zusätzlich werden dadurch verschiedene Verschlüsselungstechniken stark eingeschränkt. Zentrale Services können nicht mit Daten arbeiten die z.B. persönlich durch den Kunden auf dem Client verschlüsselt wurden.

3.6 Prozesse

Als letzter und wohl einflussreichster Faktor zur Unterwanderung der Sicherheit gilt der Faktor Mensch. Zum Betrieb eines sicheren Internetdienstes sind eine Menge von Operatoren erforderlich, die Zugriff auf das System haben. Kritische Prozesse sind hier z.B. das Key-Management für die Verschlüsselung und die Signaturen. Es kann aber auch schon durch nachlässige oder unwissende Administration der beteiligten Rechner der Internetdienst in Gefahr geraten. So kann eine Standardkomponente wie z.B. das Betriebsystem, eine Firewall oder ein Webserver in der Kette der Sicherheit das im ursprünglichen Konzept nicht vorhersehbare schwächste Glied werden.
Ein weiteres Hindernis für die Sicherheit ist die Bequemlichkeit der Menschen. Die führt z.B. zu leicht erratbaren Passwörtern oder reduziert die Bereitschaft zum Einsatz von zusätzlicher Hardware.

4 Beispiel Authentifizierung

Bei der ursprünglichen Konzeption war es selbstverständlich, das ein sicheres Internetarchiv verschiedene Authentifizierungslevel anbietet. Von zu Hause sollte sich der Kunde mit seiner SmartCard über einen sicheren SSL-Handshake authentifizieren. Da eine weltweite Verfügbarkeit von Rechnern mit eingebauten SmartCard-Lesegeräten nicht sichtbar ist, fällt diese Lösung für einen mobilen Einsatz momentan aus.

Also bietet man weiterhin den konventionellen Zugang mit Benutzername und Passwort an. Hier kann man einige zusätzliche Maßnahmen einführen, wie z.B. eine Mindestqualität der Passwörter. Solche Maßnahmen zu Steigerung der Passwortqualität können aber durch den Menschen unterwandert werden indem er einfache Schemas verwendet. Ein weiterer wichtiger Zusatz ist eine automatische Sperre für einen gewissen Zeitraum nach mehreren Fehlversuchen.

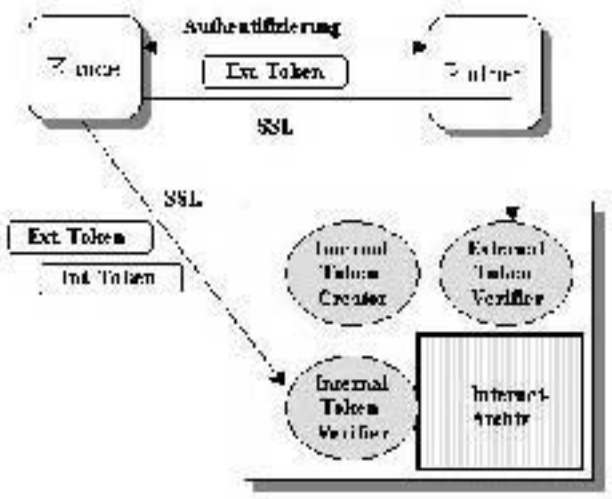

Abb. 4.1: Single-Sign-On Verfahren

Durch die oben bereits erwähnten Einflüsse der Integration mit anderen Diensten kommt jetzt noch das Authentifizierungsverfahren Single-Sign-On in Spiel. Bei einem Single-Sign-On Verfahren authentifiziert sich der Benutzer bei einer Instanz und erhält einen unverfälschbaren Token. Dieser Token wird bei allen weiteren Anfragen mitgesendet und ermöglicht den Zutritt zu anderen Diensten. Jeder Dienst kann noch einen weiteren Token hinzufügen. Dieses Verfahren ist ursprünglich bei großen Firmen im Intranetbereich eingesetzt worden, wo es kontrollierbar ist und viele Vorteile bietet. Im Internet aber bedeutet das: „Ich vertraue einer fremden Instanz die korrekte Authentifizierung meiner Benutzer an“. Bei dem Internetarchiv sind damit alle Partnerseiten der Dokumentenprovider mögliche Eintrittspunkte in das Archiv. Das Vertrauen würde eventuell noch einer Online-Bank entgegengebracht werden, bei einem Online-Shop als Eintrittspunkt in ein Archiv ist die Akzeptanz sicherlich deutlich geringer.

Eine Alternative zur Authentifizierung bei mehreren Partnerseiten bieten reine Authentifizierungsdienste. Hier kann man sich zentral anmelden und anschließend bei allen dort registrieren Internetservices ungehindert eintreten, z.B. Microsoft .NET Passport [MI02]. Bei diesem Ansatz hat der Authentifizierungsdienst die volle Kontrolle über das Benutzerverhalten im Web, was z.B. eine Akzeptanz eines Microsoft Passport so schwierig macht.

Was bietet unter diesen Bedingungen unser real existierender Internetdienst als Authentifizierungsverfahren an? Natürlich das Standardverfahren mit Benutzername und Passwort. Zertifikate zur Authentifizierung werden zwar vom Server unterstützt, mangels Existenz von Zertifikaten bei den Kunden kommt dieser Zugang nur in projektspezifischen Sonderfällen zum Tragen. Schließlich wurde auch ein Single-Sign-On-Verfahren in einem Projekt unter hohem Zeitdruck realisiert, ohne vorher ein Gesamtkonzept für Single-Sign-On zu erstellen.

5 Beispiel Signaturen

Als vor Jahren das Signaturgesetz verabschiedet wurde [Si97], erwarteten alle einen stark wachsenden Markt an digital signierten Dokumenten. Für ein Internetarchiv ist eine digitale Signatur ideal zum Nachweis der Integrität der Dokumente. Es entstanden vielfältige Szenarien von Prozessketten in denen Dokumente über mehrere Schritte verarbeitet werden und jeweils von den bearbeiteten Personen digital signiert werden. Nach einigen Jahren ist etwas Ernüchterung eingetreten. Von einer Verbreitung von Signaturkarten im Endkundenbereich kann keine Rede sein. Die Kosten für die Hardware und die Zertifikate übersteigen die Gewinnspannen, die ein Internetarchiv einnehmen kann. Inzwischen hat bereits ein, nach dem deutschen Signaturgesetz zertifiziertes TrustCenter, seinen Dienst wieder geschlossen.

Daraus ergeben sich für den Internetdienst folgende Strategien:

- Konzentration auf server-seitige Signaturen
- Abwarten bis die großen Firmen (z.B. Banken) die Infrastruktur für die digitale Signatur inklusive Support an die Endkunden verteilt haben

Die server-seitigen digitalen Signaturen sind ein überschaubares aber mächtiges Instrument zum Nachweis der Integrität. Man versieht hier ein Dokument mit einem digitalen Zeitstempel. Das bedeutet in der Signatur ist nicht nur ein Hash-Wert der Daten sondern auch eine streng kontrollierte Zeit enthalten. Bei solchen Signaturen handelt es sich nicht um persönliche Unterschriften, aber sie geben dem Dokument einen rechtlichen Wert. Dieser kann noch durch den Einsatz von zertifizierten Hardware-Einheiten gesteigert werden.

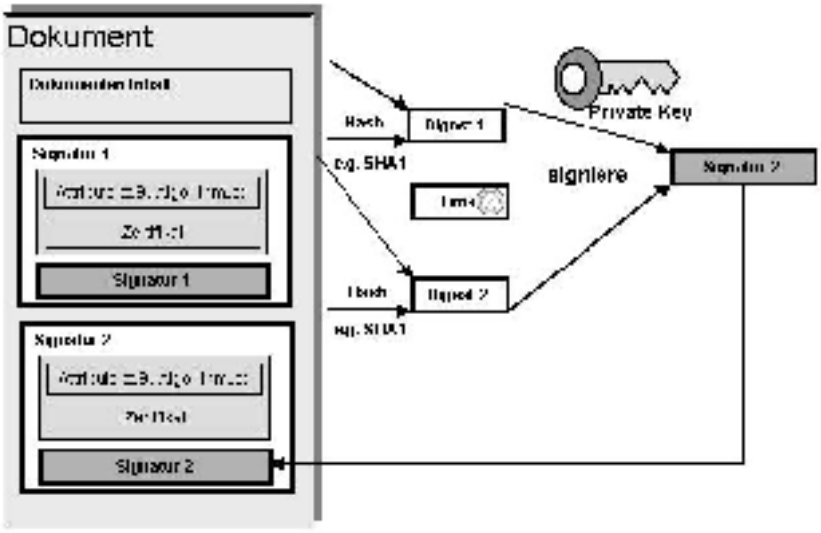

Abb.5.1 Schematische Darstellung der Signaturerneuerung

Eine weitere wichtige Entscheidung bei Signaturen sind die unterschiedlichen Formate. Neben dem allgemeinen Standard PKCS#7 haben sich auch Signaturformate für einzelne Dokumentformate z.B. XML und PDF, entwickelt. In einem Archiv sind Dokumente ein Leben lang aufzubewahren und deshalb Formate mit langfristigen Perspektiven zu wählen

Die langfristige Archivierung wirft ein weiteres Problem auf. Nach durchschnittlich 2 Jahren läuft ein Zertifikat aus. Damit verlieren auch die Signaturen, die mit diesem Zertifikat gemacht wurden ihre Gültigkeit. Die Lösung für das Archiv besteht in einer Signaturerneuerung (s. Abb. 5.1). Hierbei wird die bestehende Signatur durch eine neue Signatur in eine Art Umschlag gepackt.

6. Ausblick

Sicherheit ist in offenen Netzen eine wesentliche Voraussetzung damit überhaupt Dienste, die mit persönlichen Daten handeln, entstehen können. Wie der Artikel gezeigt hat sind aber auf dem Weg von der Planung bis zur Umsetzung viele Hindernisse zu überwinden. Ein gestiegenes Bewusstsein für Sicherheit in den letzten Jahren hat dazu geführt, dass zumindest die Basistechnologien für die Sicherheit in die Dienste integriert sind. Aber die Sicherheit ist ein kontinuierlicher Prozess, der bei jeder Weiterentwicklung eines Produktes berücksichtigt werden muss. Leider steht die Sicherheit oft in Konkurrenz zum Kosten- und Zeitdruck sowie dem Verlangen nach neuen Produkt-Features.

Literaturverzeichnis

[MI02] Microsoft .NET Passport, http://www.passport.com

[SI97] SigG Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG) (BT-Drs. 13/7934 vom 11.06.1997)

[SC96] Angewandte Kryptographie, Bruce Schneier, Addison-Wesley , 1996

[SC00] Secret and Lies, Digital Security in a Networked World, Bruce Schneier, Wiley Computer Publishing, 2000