Realisierung eines Sicherheits- und Rechtemanagements für elektronische Prüfungen an Hochschulen mittels Software-Proxy

Andreas Hoffmann[1], Roland Wismüller[1], Markus Bode[2]

Lehrstuhl Betriebssysteme und verteilte Systeme,
Fachbereich 12 – Elektrotechnik und Informatik, Universität Siegen
Hölderlinstraße 3, 57068 Siegen
[1]{andreas.hoffmann, roland.wismueller}@uni-siegen.de
[2]mb@qapp.de

Abstract:. Elektronische Prüfungen werden vor allem an Hochschulen immer beliebter. Die Anzahl an elektronischen Prüfungssystemen nimmt stetig zu. Was bislang aber die Systeme nur sehr unzureichend sicherstellen können, ist die Rechtssicherheit und den Datenschutz. Dieser Beitrag beschreibt, wie die Umsetzung des Lösungskonzepts der elektronischen Gesundheitskarte auf die elektronischen Prüfungen an Hochschulen angewendet werden kann. Dadurch werden die vielfältigen sicherheits- und datenschutzrechtlichen Anforderungen unabhängig vom verwendeten Prüfungssystem durch standardisierte Verfahren umgesetzt.

1 Einleitung

Aufgrund des Bologna-Prozesses und der damit gewünschten Schaffung eines europäischen Hochschulwesens spielen elektronische Prüfungen eine immer größer werdende Rolle. Abschlüsse sollen vergleichbar sein und Mobilitätshemmnisse aufgehoben werden, so dass eine Einführung der Bachelor- und Master-Studiengänge (BA/MA) sinnvoll erscheint. Mit der Umstellung auf die BA/MA Studiengänge erhöht sich allerdings auch die Anzahl der Prüfungen, was wiederum einen erheblichen Mehraufwand für die Prüfer bedeutet. Die Vorteile von elektronischen Prüfungen, im Vergleich zu den papierbasierten Prüfungen liegen auf der Hand. Teilweise ist eine vollautomatische Auswertung von Prüfungen möglich. Durch kürzere Korrekturzeiten können Studenten ihren Studienverlauf besser planen und Prüfer können die eingesparte Zeit in eine Verbesserung der Lehre investieren.

Allerdings sind elektronische Prüfungen in vielen Fällen nicht ohne weiteres möglich, da rechtliche Aspekte beachtet werden müssen und Prüfungsfragen in der Regel überarbeitet und an das Prüfungssystem angepasst werden müssen (vgl. [Re08]). Eine vom Studenten abgegebene Unterschrift, sei es auf Papier oder elektronisch, ist notwendig, damit dieser seine Angaben nicht abstreiten kann [Ki08]. Außerdem sollten Prüfungsfragen nicht vor der Freigabe einer Prüfung einsehbar sein, so dass es einem Angreifer nicht möglich ist, diese durch einen Einbruch in das Prüfungssystem offen zu legen.

In diesem Beitrag wird die Realisierung eines Konzeptes vorgestellt, das die Signierung und Verschlüsselung von Inhalten in Prüfungssystemen erlaubt, so dass alle rechtlichen Anforderungen und der Datenschutz umgesetzt werden können. Die Realisierung ist unabhängig vom verwendeten Prüfungssystem und bietet über die elektronischen Prüfungen hinaus einen multifunktionalen Nutzen.

2 Problemstellung

2.1 Rechtliche Anforderungen

Die rechtlichen Anforderungen, die an eine schriftliche papierbasierte Prüfung gestellt werden, müssen auch für elektronische Prüfungen gelten [Ki08]. Die papierbasierte Durchführung kann nach § 126 Abs. 3 BGB durch die elektronische Form gemäß § 126a BGB ersetzt werden, wenn *„…das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist.“*. Daraus ergibt sich die Notwendigkeit einer sog. sicheren Signaturerstellungseinheit (SSEE), auf der die Geheimhaltung des privaten Schlüssels gewährleistet werden kann (§ 17 Abs. 1 SigG). Unter einer SSEE sind Hardwarekomponenten wie Chipkarten aber auch USB-Tokens zu verstehen.

Eine rechtssichere Identifikation der Prüfungsteilnehmer kann wie bei den Papierprüfungen durch eine Aufsicht erfolgen, die die Daten von Studierenden- und Personalausweis vor der Prüfung abgleicht. Für die elektronischen Prüfungen könnte dies aber auch mittels qualifizierenden digitalen Signaturen erfolgen. Auch die Autorisierung des Studierenden muss vor der Prüfung überprüft werden.

Damit der Studierende seine Angaben nicht abstreiten kann, aber auch der Dozent die gestellte Prüfung nicht abstreiten kann, muss die Verbindlichkeit sichergestellt werden. Dies kann ebenfalls durch den Einsatz von qualifizierenden digitalen Signaturen erfolgen. Des Weiteren muss dem Studierenden während der Prüfung die Möglichkeit gegeben werden, seine Antworten zu kontrollieren und auch zu ändern.

Die Betrugssicherheit ist eine weitere wichtige Anforderung, die an elektronische Prüfungen gestellt wird. Im Kontext elektronischer Prüfungen ist hiermit die missbräuchliche Verwendung von Hardware und Software gemeint, die dem Studierenden auf verschiedene Art und Weise eine unerlaubte Hilfestellung geben kann.

Wie bei den schriftlichen Prüfungen sind auch die elektronischen Prüfungen als eigenständige Prüfungsform in der Prüfungsordnung aufzunehmen. Das gilt auch für die Zulässigkeit des Antwort / Wahl Verfahrens (Multiple/Choice). Ebenfalls in der Prüfungsordnung muss geregelt sein, was passiert, wenn der Studierende eine Prüfung aufgrund von einem Systemausfall nicht beenden kann bzw. diese unterbrochen wird.

Außerdem gilt es die Chancengleichheit für alle Prüfungsteilnehmer zu wahren (Gleichheitsgrundsatz). Jedoch gibt es keine absolute Prüfungsgerechtigkeit. Unterschiedliche

PC-Kenntnisse sind als unvermeidbar hinzunehmen und bedeuten keine Beeinträchtigung des Gleichheitsgrundsatzes [Ki08].

Des Weiteren wäre eine anonyme Bewertung der Prüfungsdaten durch den Dozenten wünschenswert. Dies würde die Objektivität der Bewertung gewährleisten. Denn mittlerweile werden auch so genannte offene Fragen in elektronischen Prüfungen umgesetzt, die vom Dozenten nachbewertet werden müssen. Allerdings besteht auf Anonymität der Teilnehmer kein Anspruch [ZB07].

2.2 Datenschutz

Der Zweck des Bundesdatenschutzgesetztes (BDSG) ist in § 1 Abs. 1 BDSG definiert: „*Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.*“ Welche Form des Umgangs mit den personenbezogenen Daten gemeint ist, lässt sich anhand der Grundprinzipien des BDSG erklären [Bo08]: Prinzip des Erlaubnisvorbehalts, Zweckbindungsprinzip, Erforderlichkeitsprinzip und die Prinzipien der Datenvermeidung und der Datensparsamkeit. Das Prinzip des Erlaubnisvorbehalts besagt, dass schutzwürdige personenbezogene Daten nur aufgrund von Gesetzen oder einer Einwilligung des Betroffenen erhoben und verarbeitet werden dürfen (§ 4 Abs. 1 BDSG).

Der Zweck der Erhebung und Vermeidung muss zudem in der Einwilligung oder dem Gesetz ausdrücklich und eng umfasst bezeichnet werden (Zweckbindungsprinzip). Der Grundsatz der Erforderlichkeit besagt, dass nur solche Daten erhoben, verarbeitet und genutzt werden dürfen, die für den jeweiligen Anwendungszweck benötigt werden und somit erforderlich sind. Daraus ergibt sich auch die Tatsache, dass die Daten die nicht erforderlich sind, nicht verwandt werden dürfen und somit auch nicht einmal erhoben werden dürfen.

Das Ziel der Datenvermeidung und der Datensparsamkeit ist es, der Gefahr der Profilbildung von Betroffenen vorzubeugen. Die Datenvermeidung kann allerdings gerade bei elektronischen Prüfungen nur schwer realisiert werden. Dennoch kann das Datenvermeidungsprinzip erreicht werden, indem die personenbezogenen Daten anonymisiert werden (vgl. § 3a BDSG). Eine Abschwächung der Datenvermeidung aus datenschutzrechtlicher Sicht ist die Datensparsamkeit, die vor allem durch das Pseudonymisieren von personenbezogenen Daten erreicht werden kann.

2.3 Problembeschreibung

Die Schwierigkeit ist, die sich teilweise widersprechenden Anforderungen wie z.B. Authentizität und Anonymität in ein Konzept zu integrieren [HW08]. Des Weiteren muss das Konzept in bestehende Systemlandschaften integrierbar sein. Denn die Anforderung nach Verbindlichkeit setzt die Verwendung von qualifizierenden digitalen Signaturen voraus, was wiederum einen hohen administrativen und infrastrukturellen Aufwand bedeutet. Somit muss das Konzept einen multifunktionalen Nutzen bieten können.

Bei der Signierung der Prüfungsangaben ist darauf zu achten, dass der Studierende genau sieht, was er gerade elektronisch unterschreibt. Außerdem ist die Protokollierung des Prüfungsverlaufs ein wichtiger Bestandteil einer rechtssicheren Prüfung. Nur das, was der Studierende sieht, und das was er an Angaben in Abhängigkeit dieser Sicht getätigt hat, kann von ihm verantwortet werden.

Zusätzlich sind die datenschutzrechtlichen Anforderungen von entscheidender Bedeutung. Hier gilt es transparente und standardisierte Verfahren zu verwenden, um die Grundprinzipien des Datenschutzes sicher zu stellen.

3 Sicherheitskonzepte existierender Prüfungssysteme

Das „Online Learning And Training“ (OLAT) liegt aktuell in der Version 6 vor und wurde an der Universität Zürich entwickelt. Die Software wird nach der Apache 2.0 Open Source Lizenz vertrieben und darf auch modifiziert werden. Das Sicherheitskonzept wurde zwar speziell auf die Rechtssicherheit hin entwickelt, kann aber z.B. nur die Integrität und die Vertraulichkeit, nicht aber die Verbindlichkeit der Daten gewährleisten. Dazu werden Logfiles nach der Klausur auf CD geschrieben, bzw. die Daten werden bei der Übertragung über HTTPS verschlüsselt. Zur Authentifikation werden lediglich eine UserID und ein Passwort benötigt. Die Betrugssicherheit wird durch das Sperren von nicht genehmigten Webseiten erreicht. Das Rechte- und Rollenkonzept orientiert sich an dem Policy-Konzept von Java. Es existieren Benutzer, die einer oder mehreren Gruppen angesiedelt sind, und eine Policy, die dann eine Kombination von einem Recht, einer Gruppe und einer Ressource darstellt.

Das LPLUS Testmanagement System ist eine kommerzielle Software für computergestützte Prüfungen von der Firma LPLUS GmbH. An der Universität Bremen erfolgt die Anmeldung am System über eine eindeutige PIN, die vor der Prüfung nach der Kontrolle der Autorisierung des Studenten ausgehändigt wird. Die Beantwortung und Auswertung einer Prüfung wird als Hardcopy gespeichert und ist so komplett nachvollziehbar. Die Vertraulichkeit wird nur über das Rollen- und Rechtesystem realisiert, so dass bestimmte Personen gezielt Sichten auf das System und Lese- und/oder Schreibrechte für bestimmte Bereiche bekommen. Diese Rechte werden von einem Super-Administrator vergeben, so dass es auch möglich ist, dass dieser die Prüfungsfragen einsehen und an Studenten unerlaubt verteilen kann. So ist es aber auch möglich, dass z.B. nur ein zentraler Personenkreis Zugriff auf die Prüfungsprotokolle oder Ergebnisse erhält, der dann im Auftrag der Prüfer die entsprechenden Daten aus dem System ausliest. Dieser Personenkreis wird zur Verschwiegenheit und Wahrung des Datenschutzes verpflichtet, könnte aber theoretisch auch widerrechtlich Prüfungsfragen verbreiten, da eine Verschlüsselung der Prüfungsfragen nicht stattfindet. Zur Authentifizierung nutzt man die in Programmen gängige Methode eines Benutzernamens und Passworts. Zusätzlich stehen Logfiles zur Verfügung, über die nachvollzogen werden kann, welcher Student wie lange an einer Frage gearbeitet hat. Die Integrität und damit die Verbindlichkeit der Prüfungsfragen und -antworten kann nicht garantiert werden. Eine Möglichkeit zur Integritätsprüfung ist das Ausdrucken der Antworten und Unterschreiben dieses Protokolls durch den Student.

ILIAS (Integriertes Lern-, Informations- und Arbeitskooperations-System) ist ein auf OpenSource Basis existierendes Learning-Management-System, das auch ein Modul zur Durchführung von computergestützten Prüfungen besitzt. Das Rechte- und Rollenmanagement unterscheidet sich von anderen Systemen dahingehend, dass hier jeder Prüfungsteilnehmer vor der Durchführung eine IP-Adresse eines Prüfungsrechners zugewiesen bekommt. Diese Zuordnung wird auch protokolliert. Während der Prüfung kann der Status der Bearbeitung eines jeden Teilnehmers überwacht werden. Im Anschluss an die endgültige Abgabe der Prüfung öffnet sich eine Druckansicht, die die gegebenen Antworten beinhaltet. Ab diesem Moment kann keine Kommunikation mit dem System mehr erfolgen. Die Übersicht der Antworten wird dann über einen Browser ausgedruckt. Der Ausdruck gibt neben den gegebenen Prüfungsantworten auch Auskunft über die genutzte IP-Adresse und die Matrikelnummer des Studenten. Diese Informationen befinden sich auf jeder ausgedruckten Seite. Im Anschluss muss jede Seite des Ausdrucks handschriftlich unterschrieben werden. Die unterschriebenen Ausdrucke werden dann auch archiviert.

Die bestehenden Systeme können zwar durch entsprechende Rechte- und Rollenmanagements Authentizität und Autorisierung gewährleisten, die Verbindlichkeit aber nur durch Medienbrüche. Die Prüfungsangaben der Studenten werden ausgedruckt, unterschrieben und dann archiviert und die elektronischen Daten nach der Auswertung gelöscht. Der Ausdruck der Prüfungsangaben z.B. erfolgt dann auf den in den Prüfungslaboren befindlichen Druckern. Bei Massenprüfungen ist ein entsprechendes Druckaufkommen vorprogrammiert, dass durch Personal geregelt werden muss. Spezielle Datenschutzkonzepte existieren nicht.

4 Realisierung eines Sicherheitskonzeptes

4.1 Realisierungsansatz

In [HW08] haben wir ein virtuelles, ticketbasiertes Dateisystem für elektronische Prüfungen auf Basis des Lösungskonzeptes der elektronischen Gesundheitskarte (eGK) dargestellt [Fr05]. Es wurde ein Sicherheitskonzept vorgestellt, das die verschiedenen Anforderungen bezüglich der Sicherheit elektronischer Prüfungen umsetzt. Dazu zählen vor allem die Verbindlichkeit der Prüfungsangaben, die Authentizität der Teilnehmer und die Umsetzung aller datenschutzrechtlichen Anforderungen. Das Konzept ermöglicht somit u.a. die Anonymität der Teilnehmer trotz Authentizität und gewährleistet, dass jeder Akteur „Herr seiner Daten“ bleibt. Dies wird dadurch erreicht, dass nur derjenige Zugriff auf Datenobjekte eines anderen hat, der zuvor durch die Bereitstellung eines sog. TicketToolkits dazu ermächtigt wurde.

Der Dozent kann dadurch im Vorfeld nur denen die Teilnahme an der Klausur erlauben, die sich z.B. über das Prüfungsamt angemeldet haben und damit zur Teilnahme berechtigt sind. Den Teilnehmern wird in diesem Falle eine Berechtigung für das Dateisystem des Dozenten gegeben, das der Klausur entspricht. Dieser Zugriff kann nur durch den Einsatz einer elektronischen Studierendenkarte erfolgen. Für die

Klausurdurchführung und –auswertung gilt das Gleiche, nur umgekehrt. Die Studierenden erlauben dem Dozenten (und evtl. weiteren Korrektoren) explizit, die Prüfungsdaten einzusehen. Durch die hierarchische Anordnung des Dateisystems werden dabei die persönlichen Daten des Studierenden von den Prüfungsdaten getrennt. Dadurch wäre auch eine anonyme Bewertung möglich, denn der Dozent sieht nur die Prüfungsdaten und keine Matrikelnummer o.ä.

Dadurch ergibt sich eine weitere Anwendungsmöglichkeit, wie z.B. die Durchführung von anonymen Selbsttest zur Klausurvorbereitung. Der Dozent erlaubt nur den Studierenden die Teilnahme, die seine Veranstaltung besuchen. Die Studierenden führen den Selbsttest durch und erlauben dem Dozenten nur den Zugriff auf die gemachten Angaben, nicht aber auf ihre Matrikelnummer oder Namen. Dadurch ist sogar die Anonymität trotz Authentizität möglich. Weitere Anwendungsmöglichkeiten in diesem Falle wären z.B. auch Lehrevaluierungen.

4.2 Architektur

Ähnlich wie bei der elektronischen Gesundheitskarte erhält der Student eine elektronische Studierendenkarte, die bereits mit einem für ihn generierten privaten Schlüssel sowie Zertifikat ausgestattet ist. Das Zertifikat beinhaltet den öffentlichen Schlüssel, so dass ein Zusammenspiel beider Schlüssel mit dem System möglich ist.

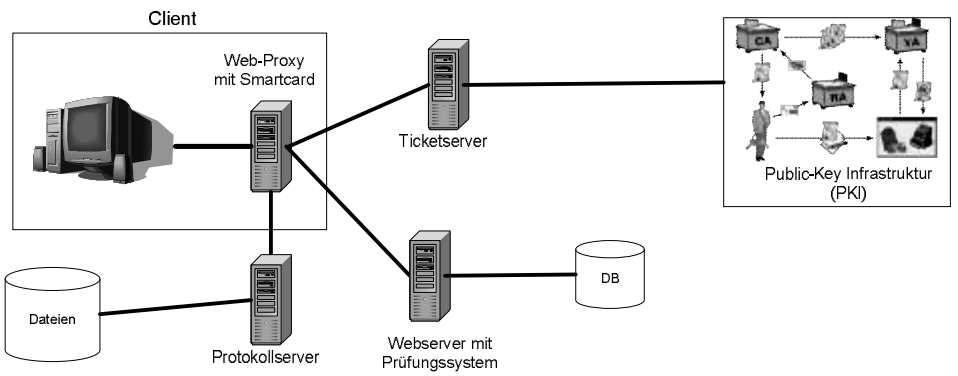

Abb. 1: Grob-Architektur

Abb. 1 zeigt eine Anordnung der neuen Infrastruktur für den sicheren Zugriff auf das Prüfungssystem. Der Prüfer bzw. Student, der über den Clientrechner „sicher“ auf das Prüfungssystem auf dem Webserver zugreifen will, wählt seinen Weg über den Web-Proxy, der zwischengeschaltet wird. Dieser hat Zugriff auf die elektronische Studierendenkarte sowie auf den Ticketserver, auf die PKI und den Protokollserver. Die Realisierung des Web-Proxy kann sich an dem Konzept des Proxy-Server für transparentes digitales Signieren von E-Learning Inhalten orientieren [ESS07]. Dieses Konzept basiert auf einem Proxy-Server für Lern-Management-Systeme (LMS) wie ILIAS oder Moodle.

Ticketserver, PKI und Protokollserver haben gemeinsam, dass sie als Webservice über das Internet erreichbar sind. Die Webservices akzeptieren allerdings nur authentifizierte

Anfragen, d.h. der Proxy signiert die Anfragen für den Benutzer automatisch bei der Kommunikation mit Ticket- und Protokollserver. Der PKI-Server erlaubt nur einen lesenden Zugriff, so dass hier auch eine Abfrage ohne Signatur möglich ist.

Der Protokollserver erhält vom Web-Proxy Informationen darüber, welche Daten zwischen Client und dem Web-Proxy geflossen sind. Der Proxy modifiziert die HTTP-Anfragen und HTTP-Antworten, so dass nachvollzogen werden kann, welche Daten der Client selbst verschickt und welche er empfangen hat. Nur diese Daten hat zum Beispiel der Student im Hinblick auf eine Prüfung und der rechtlichen Absicherung zu verantworten („What you see is what you sign"). Daher werden die HTTP-Anfragen durch den Protokollserver aufgezeichnet. Des Weiteren dient der Web-Proxy zur Umsetzung der Ver- und Entschlüsselung, sowie der Signierung und Verifizierung von Daten.

Die Public-Key-Infrastruktur (PKI) hält die öffentlich zugänglichen Zertifikate der Benutzer vor. Sobald die Hochschule ein Zertifikat für eine elektronische Studentenkarte ausstellt, wird dieses der PKI hinzugefügt. Dies ist notwendig, damit Benutzer Freigaben, so genannte TicketToolkits, im Ticketserver anlegen und Ticket- und Protokollserver signierte Anfragen verifizieren können.

Der Ticketserver implementiert die Funktionen des virtuellen Dateisystems der Telematik-Infrastruktur der elektronischen Gesundheitskarte ([HW08], [Fr05]). Er ist für die Erstellung und Verwaltung von Klausurschlüsseln (examKeys) obligatorisch. Über ihn wird der vertrauliche Zugriff auf Prüfungsfragen und Prüfungsantworten realisiert. Die examKeys liegen verschlüsselt für den Zugriff über bestimmte T-Nodes, also Knotenpunkte, die die Klausurschlüssel schützen, bereit. Grundsätzlich gilt: Nur wer über eine explizite Berechtigung (Ticket) auf einen T-Node verfügt, kann darauf zugreifen. Diese Berechtigung kann nur vom Ersteller des T-Nodes vergeben werden.

Die TicketToolkits regeln den Zugriff auf die Information, die hinter dem T-Node stehen. Wird ein T-Node gelöscht, gehen damit alle TicketToolkits und damit alle Freigaben verloren. Auch das Überschreiben oder Löschen einzelner TicketToolkits ist möglich, um gezielt Benutzer für die Freigabe zu (de-)aktivieren.

Jeder Benutzer hat ein eigenes Verzeichnis, das so genannte VROOT, das mit seiner Benutzerkennung (Matrikelnummer, DozentenID, etc.) verknüpft ist. In diesem werden Referenzen zu den freigegebenen T-Nodes gespeichert. Die Realisierung wird anhand der einzelnen Prüfungsprozesse und der in Abb. 2 dargestellten Ticketsystemstruktur beschrieben.

4.3 Klausurerstellung und -anmeldung

Die Vorbereitungsphase dient der Zusammenstellung der Klausur und dem Anmeldezeitraum für die Studierenden.

Zuerst einmal wird mittels Ticketserver ein neuer *T-Node* (#965677) und ein *examKey* (examKey A) durch den Dozenten erstellt. Der *examKey* ist ein symmetrischer Schlüssel, mit dem die Klausurfragen verschlüsselt werden. Der *examKey* ist wiederum sym-

metrisch mit einem *decodeKey* verschlüsselt und wird durch den *findKey* (#1222) im virtuellen Dateisystem identifiziert.

Für jede Klausur existiert genau ein T-Node. Für diesen T-Node wird nun für jeden der zur Klausur angemeldeten Teilnehmer ein TicketToolkit erzeugt. Dazu importiert der Dozent eine Liste der Teilnehmer, die er entweder aus einem Hochschul-Informationssystem exportiert hat oder aber direkt von den Prüfungsämtern erhalten hat.

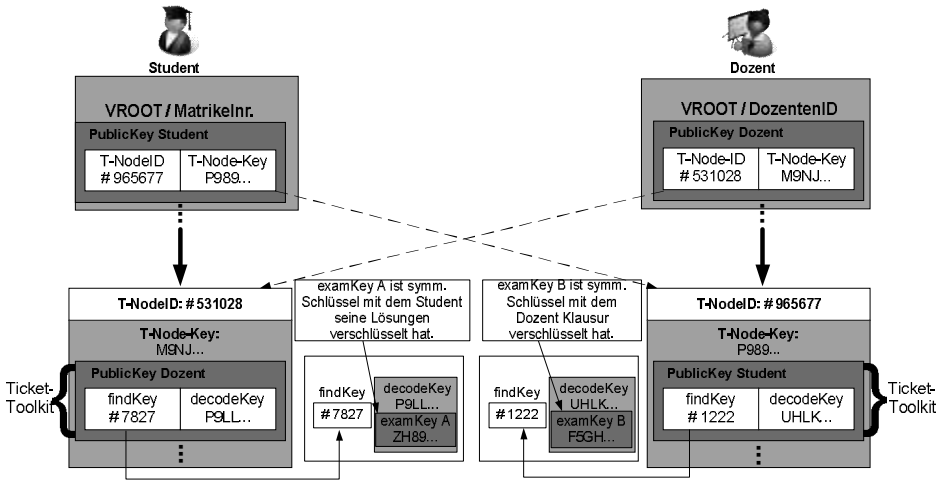

Abb. 2: Ticketsystemstruktur

Jedes der TicketToolkits wird mit dem öffentlichen Schlüssel des Teilnehmers (*„PublicKey Student“*) verschlüsselt und verweist auf den *examKey*. Der Ticketserver schreibt nun noch in das VROOT des angemeldeten Studenten die Informationen, welcher T-Node aufzusuchen ist und wo sich das TicketToolkit für den Studenten befindet. Zu diesen Informationen gehören die T-NodeID (#965677) und der T-Node-Key, die mit dem öffentlichen Schlüssel des Studenten verschlüsselt werden. Die T-Node-ID referenziert den T-Node, der T-Node-Key verschlüsselt die TicketToolkits des T-Nodes.

Zusätzlich erstellt der Ticketserver einen T-Node (#531028). Der T-Node enthält ein TicketToolkit für den Dozenten, das ihm erlaubt, auf die Prüfungsangaben des Studierenden (z.B. zur Auswertung oder Nachkorrektur) zuzugreifen. Auch hier wird ein symmetrischer examKey generiert, mit dem die Prüfungsangaben des Studierenden verschlüsselt werden. Ohne dieses TicketToolkit kann niemand außer dem Studierenden auf die Prüfungsangaben zugreifen. Für jede weitere Person, die an der Korrektur beteiligt sein soll, muss ein TicketToolkit erstellt werden. Der Student bestimmt, ob und ggf. wem er ein TicketToolkit ausstellt. Die Generierung kann auch erst nach der Klausurdurchführung erfolgen. Durch dieses Konzept bleiben sowohl der Student als auch der Dozent „Herr ihrer Daten“.

4.4 Durchführung

Wenn ein Student eine Klausur durchführen will, muss zuerst überprüft werden, ob er an der Klausur teilnehmen darf. Dazu muss der zur Klausur entsprechende T-Node (#965677) geöffnet werden. Sofern der T-Node im VROOT des Studenten enthalten ist, wird die Anfrage zusammen mit dem entsprechenden T-Node-Key weitergeleitet. Der Ticketserver öffnet daraufhin den gesuchte T-Node (anhand der T-NodeID) und entschlüsselt ihn mit dem symmetrischen T-Node-Key. So ist sichergestellt, dass ein T-Node mit einer öffentlichen T-NodeID nicht ohne Freigabe des Erstellers aufgerufen werden kann. Existiert für den Studenten ein TicketToolkit, wird das TicketToolkit verifiziert, indem ein Abgleich der Uhrzeiten stattfindet. TicketToolkits können minutengenau auf einen bestimmten Zeitraum eingeschränkt werden. Danach sendet der Ticketserver Zugriffsinformationen für den examKey, zurück. Das sind ein symm. Schlüssel (findKey) zum Auffinden des examKey und ein symmetrischer Schlüssel zum Entschlüsseln des examKey (decodeKey).

Nach der Entschlüsselung von findKey und decodeKey werden beide Schlüssel zum Ticketserver übertragen. Danach wird der examKey mit Hilfe des findKeys gesucht und mit Hilfe des decodeKey entschlüsselt. Der Proxy kann nun mit Hilfe des examKey die Klausur für den Studenten entschlüsseln. Damit der Student die Fragen sehen kann, werden die Daten per Hypertext Transfer Protocol (HTTP) übertragen. Die HTTP-Anfrage wird nun zum Server weitergeleitet, und die Antwort wird vom Proxy empfangen. Der HTTP-Body dieser Antwort kann verschlüsselte und signierte Inhalte beherbergen. Diese werden vom Proxy entsprechend einer definierten Notation erkannt und entschlüsselt bzw. verifiziert. Die Verifizierung einer digitalen Signatur kann mit Hilfe des Zertifikats bzw. des öffentlichen Schlüssels aus der PKI erfolgen. Das HTML-Dokument wird in diesem Vorgang sozusagen „entschlüsselt“.

Im letzten Schritt werden die HTTP-Daten zum Client weitergeleitet. Hierbei muss ggf. wieder der HTTP-Header angepasst werden, so dass Angaben wie die Content-Length stimmen. Es ist im Wesentlichen unerheblich, welche Daten im HTTP-Body enthalten sind. Eine Signierung und symmetrische Verschlüsselung von größeren multimedialen Inhalten ist somit ebenfalls möglich. Signatur- und Verschlüsselungsoperationen können beliebig hintereinander ausgeführt werden, zum Beispiel die Entschlüsselung von verschlüsselten und signierten Daten. Vom Proxy verschlüsselte bzw. signierte Daten haben eine feste Notation, so dass diese beim Parsen des HTML-Dokuments gefunden und entschlüsselt bzw. verifiziert werden können. Die Notation einer asymmetrischen verschlüsselten Information im HTML-Dokument sieht wie folgt aus:

```
<html>
  <head> … </head>
  <body>
       …
       !PROX-EN! Chiffretext !NE-XORP!
       …
  </body>
</html>
```

Der Schlüsseltext wird Base64-Enkodiert von den Zeichenfolgen *!PROX-EN!* und *!NE-XORP!* Eingeschlossen, wodurch eine genaue Abgrenzung der verschlüsselten Daten zu der restlichen Information möglich ist. Bei der Signierung von Daten werden neben dem Text auch die dazugehörige Signatur und das Zertifikat des Benutzers überliefert. Der Text liegt unverschlüsselt vor, so dass bei dem Wunsch nach Vertraulichkeit der signierte Text bzw. die o.g. Notation nachträglich noch verschlüsselt werden kann.

Nach Beendigung der Klausur wird ein Klausurbogen erstellt. Dieser beinhaltet sowohl alle Daten der Prüfung, als auch die Matrikelnummer, Datum des Bogens, Prüfungsfragen sowie die vom Student gegebenen Antworten. Dieser Bogen wird durch den Studenten signiert und im System hinterlegt. Zusätzlich erhält der Student den Hash-Code des Klausurbogens als Quittung angezeigt. Über diesen kann auch er nachvollziehen, ob ein Klausurbogen wirklich der ist, den er signiert hat.

4.5 Auswertung und Archivierung

Die Klausurauswertung kann bei Single- /Multiple-/ Matrix-Choice Aufgaben durch das Prüfungssystem direkt erfolgen. Bei Freitexten jedoch ist eine manuelle Korrektur durch den Dozenten nötig. Allerdings kann die Auswertung nur durch den Dozenten erfolgen, weil nur er die Erlaubnis hat die Prüfungsdaten des Studenten zu entschlüsseln. Es sei denn, es wurden weitere TicketToolkits für weitere Personen durch den Studenten erzeugt.

Die Archivierung der gesamten Prüfung erfolgt nach der Auswertung. Dazu werden alle Protokolldaten des Protokollservers sowie alle Prüfungsdaten zusammengeführt und durch den Dozenten signiert und verschlüsselt abgespeichert.

5 Proof-of-concept

Das in Kap. 4 beschriebene System ermöglicht die Umsetzung aller sicherheits- und datenschutzrechtlichen Anforderungen für elektronische Prüfungen. Nachfolgend wird die Anwendbarkeit an einem bestehenden Klausursystem beschrieben.

5.1 KLAUSIE (Klausursystem Universität Siegen)

KLAUSIE wird seit dem Sommersemester 2008 am Fachbereich Wirtschaftswissenschaften, Wirtschaftsrecht und Wirtschaftsinformatik der Universität Siegen eingesetzt. KLAUSIE ist ein auf PHP und MySQL basiertes System, mit dem Online-Tests auf Basis von Multiple- /Single- /Matrix-Choice, Lückentexte und Freitexte umgesetzt und durchgeführt werden. KLAUSIE verwendet bislang nur die üblichen Sicherheitsmechanismen wie SSL und die verschlüsselte Speicherung der Daten in der Datenbank. Zur Authentifizierung der Studierenden werden deren Studentenkennungen verwendet. Alle anderen Nutzer (Dozenten, Administrator, etc.) erhalten eine eigene KLAUSIE-Kennung.

Der Zugriff auf das Prüfungssystem KLAUSIE erfolgt nun über den vorgestellten Proxy. Beim Login wird das Passwort mittels der Smartcard signiert übertragen. Damit eine Verifizierung der Authentifizierungsdaten stattfinden kann, muss das Prüfungssystem minimal angepasst werden. Hier wird bisher das Passwort überprüft, nun müssen zusätzlich die Signatur des Passworts, als auch der korrekte Zusammenhang zwischen Signatur und der hinzukommenden Benutzerkennung überprüft werden. Dies ist über eine Anbindung des PKI-Servers als Schnittstelle möglich. Falls der Login ohne den Proxy stattfinden würde, stünde in der übermittelten Variable das eigentlich eingegebene Passwort ohne Signatur. Wenn jedoch der Proxy benutzt wird, überprüft der Proxy, ob die Signatur zu dem eingegebenen Passwort passt und ob das im String enthaltene Zertifikat das des Benutzers ist, der sich versucht einzuloggen. Danach wird das eigentliche Passwort aus dem Datenteil der Signatur ausgelesen und weiter verarbeitet.

Die Prüfungsangaben werden komplett verschlüsselt in der Datenbank gespeichert, so dass ein Angreifer keine vertraulichen Daten auslesen kann. Damit KLAUSIE nun die verschlüsselten Daten einlesen kann, wurde die Schnittstelle zur Datenbank angepasst. Hier werden die Ergebnisse lesender Operationen, wie zum Beispiel ein SELECT-Aufruf automatisch entschlüsselt und Schreiboperationen, wie INSERT und UPDATE, verschlüsselt. Bei einem SELECT stehen die aktuell gelesenen (verschlüsselten) Daten in einem Array zur Verfügung, die im Folgenden automatisch entschlüsselt werden. Vorhandene Signaturen werden dabei ignoriert, man könnte genauso gut nach einer fehlgeschlagenen Verifikation den Programmablauf abbrechen oder einen entsprechenden Hinweis ausgeben. Die zur Entschlüsselung notwendigen T-Node-IDs werden festgehalten, da mit diesen später eine Verschlüsselung der kompletten HTML-Ausgabe stattfindet.

Beim INSERT und UPDATE von Daten wird der vorhandene „unverschlüsselte“ SQL-Query durch einen Parser verschlüsselt. Dazu kennt KLAUSIE die vom Benutzer verwendete T-Node-ID und überprüft, ob im SQL-Query Daten vorkommen, die nur verschlüsselt in der Datenbank gehalten werden sollen. Diese Zuordnung wird über die Spaltennamen der Datenbank getroffen. Damit die Schlüsseltexte auch in die Datenbank geschrieben werden können, müssen Datentypen der Tabellenspalten ggf. geändert werden. So wurde die korrekte Antwort einer Single-Choice Aufgabe bisher als Integer gespeichert. Da diese Zahl nun aber verschlüsselt in der Datenbank steht, reicht der Integer-Datentyp nicht mehr, so dass eine Änderung in einen „Text“-Datentyp notwendig ist. Da nach dem Auslesen der Datenbank die Daten in KLAUSIE unverschlüsselt zur Verarbeitung vorliegen, müssen diese vor dem Senden einer Antwort zum Client wieder verschlüsselt werden. Dazu verschlüsselt KLAUSIE seine kompletten Ausgaben mit den o.g. T-Nodes.

6 Zusammenfassung

Elektronische Prüfungen können die traditionelle Lehre durch Selbsteinschätzungstests unterstützen und mit Online-Prüfungen auch einen hohen Arbeitsaufwand reduzieren. In diesem Beitrag wurden verschiedene Verfahren zur Absicherung von elektronischen Prüfungen diskutiert und eine Lösung für browserbasierte Prüfungen vorgestellt. Durch

den Einsatz einer PKI, symmetrischer und asymmetrischer Verschlüsselung, sowie dem Erstellen digitaler Signaturen und deren Verifizierung ist ein hohes Maß an Datenschutz und Datensicherheit gewährleistet. Dabei wurden Verfahren aus der Telematik-Infrastruktur der elektronischen Gesundheitskarte für elektronische Prüfungen umgesetzt. Dies sind u.a. T-Nodes, die den Zugriff auf einen symmetrischen Klausurschlüssel nur für mittels TicketToolkits freigegebene Personen erlaubt.

Eine Weiterentwicklung könnte die Einführung eines SQL-Proxy sein. Dieser würde sich zusätzlich zu dem Web-Proxy zwischen dem Klausursystem und der SQL-Datenbank befinden. Das hätte zur Folge, dass sich die Anpassung des Klausursystems auf ein Minimum beschränken würde. Denn nur die Verbindung zwischen Klausursystem und Datenbank müsste über den SQL-Proxy umgeleitet werden. So könnte dann die feingranulare Zugriffskontrolle über den SQL-Proxy erfolgen. Aktuell wird zu der Entwicklung eines SQL-Proxy an der Universität Siegen eine Diplomarbeit durchgeführt.

Außerdem bietet die in diesem Beitrag beschriebene Realisierung einen multifunktionalen Nutzen. Das Ticketsystem könnte auf die Einführung einer elektronischen Studierendenakte (eSA) angewendet werden. Der elektronische Studierendenausweis als Kombilösung für Semesterticket, Kopierkarten und Bezahlkarte in Form von EC- oder Geldkarte.

Literaturverzeichnis

[Bo08] Borchers, Christian M.: Die Einführung der elektronischen Gesundheitskarte in das deutsche Gesundheitswesen. Diss. Univ. Würzburg, Logos Verlag, Berlin, 2008.

[ESS07] Eibl, Christian J. ; Solms, SH B. ; Schubert, Sigrid: Development and Application of a Proxy Server for Transparently, Digitally Signing E-Learning Content in New Approaches for security, privacy and trust in complex environments (IFIP TC-11 22nd). 2007.

[Fr05] Fraunhofer Institut: Spezifikation der Lösungsarchitektur zur Umsetzung der Anwendungen der elektronischen Gesundheitskarte, 2005

[HW08] Hoffmann A., Wismüller, R.: Sicherheitskonzept für elektronische Prüfungen an Hochschulen auf Basis eines ticketbasierten, virtuellen Dateisystems In: Seehusen, S.; Lucke, U.; Fischer, S. (Hrsg.): Die 6. e-Learning Fachtagung Informatik - DeLFI 2008, Lübeck, 2008, S.197-208

[Ki08] Kirchner-Freis, Iris: Rechtliche Aspekte des eLearning und eAssessment : Ein Praxisleitfaden / Hrsg. Andree Kirchner; Hrsg. Iris Kirchner-Freis; Hrsg. MLS Rechtsanwaltsgesellschaft mbH; Iris Kirchner-Freis; Andree Kirchner; Antje Zimmermann. - Version 2.0. - Bremen: Kirchner, Andree, Prof. Dr., 2008

[Re08] Reepmeyer, J.; Onlineklausuren, In: Grob, H.L.; vom Brocke, J.; Buddendick, Ch. (Hrsg.); E-Learning-Management, Vahlen Verlag München, 2008, S. 255-274

[ZB07] Zimmerling W., Brehm R.: Prüfungsrecht, 3. Auflage, Carl Heymanns Verlag, Köln, 2007