Sicherheitskonzept für elektronische Prüfungen an Hochschulen auf Basis eines ticketbasierten, virtuellen Dateisystems

Andreas Hoffmann, Roland Wismüller

Fachgruppe Betriebssysteme und verteilte Systeme,
Fachbereich 12 – Elektrotechnik und Informatik, Universität Siegen
Hölderlinstraße 3, 57068 Siegen
{andreas.hoffmann, roland.wismueller}@uni-siegen.de

Abstract: Die elektronische Durchführung von Prüfungen hat in den letzten Jahren verstärktes Forschungsinteresse geweckt. Dabei spielt für die Gültigkeit dieser Prüfungen insbesondere die Erfüllung von Sicherheitskriterien eine wesentliche Rolle. In dieser Arbeit wird 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 orientiert sich am Modell der elektronischen Gesundheitskarte und ermöglicht somit u.a. die Anonymität der Teilnehmer trotz Authentizität und gewährleistet, dass jeder Akteur „Herr seiner Daten" bleibt.

1 Elektronische Prüfungen an Hochschulen

Prüfungen begleiten uns durchs Leben! Dies reicht von der Notenbildung in Schulen und Hochschulen über die Lernstandserhebungen sowie Vergleichsstudien oder Überprüfung von Bildungsstandards bis hin zur Überprüfung von Fachwissen bei Einstellungstests [Sc05]. Die Anfänge der Durchführung elektronischer Prüfungen finden sich Mitte der neunziger Jahre bei der Durchführung von Einstellungstests bei der Bundeswehr [SG99] wobei die Methode durch den Einsatz bei Medizinerprüfungen und Sprachtests (TOEFL, usw.) konsequent verbessert und erweitert wurde. Elektronische Prüfungen werden mittlerweile in vielen Bereichen erfolgreich eingesetzt. So ermöglicht die computergestützte Durchführung von Prüfungen z. B. die Reduktion des Korrekturaufwandes. Besonders bei vollständig computergestützten Klausuren (Multiple-/ Single-Choice) wird die Auswertung dadurch auf einen Tastendruck reduziert. Die kürzeren Korrekturzeiten tragen zu einer verbesserten Studienorganisation für Studierende bei, da sie zum einen Informationen zur Planung ihres weiteren Studienverlaufs zeitiger erhalten und zum anderen die Studiendauer verkürzt werden kann, da kürzere Zeiten zwischen der Erstklausur und dem Wiederholungstermin realistisch werden. Zusätzlich zur verbesserten Studienorganisation erhöht die computergestützte Durchführung von Prüfungen die Objektivität und Transparenz der Prüfungsergebnisse und bietet die Möglichkeit eines ausführlichen Feedbacks durch Zusatzinformationen.

Trotz der Vorteile von computergestützten Prüfungen berücksichtigen bestehende elektronische Prüfungssysteme wie z.B. *LPLUS*[1], *Questionmark Perception*[2] oder aber integrierte Lern-/Prüfungssysteme wie *ilias3*[3] nicht alle Sicherheitsanforderungen. Die Sicherheitsziele von elektronischen Prüfungen sind (vgl. [Ho07], [St06], [Br08]):

- Verbindlichkeit (Nichtabstreitbarkeit)
    - der Prüfungsangaben der Teilnehmer
    - der Klausurfragen des Prüfers
- Authentizität der Teilnehmer
- Anonymität der Teilnehmer bei freiwilligen Selbsttest
- Vertraulichkeit der Kommunikation
- Verfügbarkeit und Ausfallsicherheit
- Datenschutz

Vor allem die Umsetzung der Verbindlichkeit und des Datenschutzes mit Hilfe von standardisierten Methoden und Konzepten wurde bislang nicht beachtet. Außerdem gilt es die sich widersprechenden Anforderungen von Anonymität und Verbindlichkeit in ein Konzept zu integrieren.

Den Schwachstellen bestehender Systeme wird mit dem in dieser Arbeit vorgestellten Konzept einer Sicherheitsarchitektur Rechnung getragen. Das Konzept setzt anhand von transparenten und standardisierten Verfahren die genannten Sicherheitsanforderungen an elektronische Prüfungen an Hochschulen um und ermöglicht die weitere Verwendung von vorhandenen Prüfungssystemen bzw. Hochschulinformationssystemen. Dafür werden im folgenden Abschnitt zunächst verwandte Arbeiten diskutiert und Verbesserungspotentiale aufgezeigt, welche von der in dieser Arbeit vorgestellten Sicherheitsarchitektur aufgegriffen werden.

[1] http://www.lplus.de
[2] http://www.questionmark.com
[3] http://www.ilias.de

2 Verwandte Arbeiten

In [St06] wird ein Sicherheits-Stufenmodell für Online-Prüfungsverfahren beschrieben, das verschiedene Prüfungsverfahren klassifiziert (formativ, summativ)[4] und auf drei Sicherheitsstufen (*Keine zusätzliche Sicherheit, Daten-/Kommunikationssicherheit, Sichere Prüfungsumgebung*) verteilt. Dieses Modell findet in der Durchführung von Online-Prüfungen an der Uni Hannover mit dem ilias3-System Anwendung. Allerdings wird hier am Beispiel der Verbindlichkeit aufgezeigt, dass die Rechtsverbindlichkeit auf Kosten von Bedienbarkeit und Flexibilität, sowie durch Medienbrüche umgesetzt wird. Die Studenten führen die Prüfung online durch, und ihre Angaben werden in eine Datenbank geschrieben. Nach der Prüfungsdurchführung werden die Angaben der Studenten ausgedruckt. Jeder Student unterschreibt seinen Ausdruck. Die Prüfung wird elektronisch ausgewertet und die elektronischen Daten werden gelöscht. Nur die Papier-Ausdrucke werden archiviert. Aber selbst der Ausdruck der gemachten Angaben stellt rechtlich gesehen eine Grauzone dar. Denn laut der Zivilprozessordnung (ZPO) ist ein Computerausdruck nur dann eine Urkunde, wenn der Ausdruck im unmittelbaren Herrschaftsbereich des Ausstellers liegt [HS99]. Wenn nun die Angaben über einen Netzwerkdrucker ausgedruckt werden stellt sich schon die Frage ob der Netzwerkdrucker, auf dem auch die anderen Studenten ihre Angaben ausdrucken, im unmittelbaren Herrschaftsbereich des Studenten liegt. Ganz zu schweigen von den möglichen technischen und organisatorischen Problemen wie z.B. Druckerausfall und Koordinierung der Unterschriften.

In [Gr02] wird ein Testframework für eine Lernumgebung dargestellt. Hierbei werden die Prüfungen in einzelne Prüfungsprozesse untergliedert. Das Testframework verwendet eine RMI Middleware, bei der die Testmaterialien vollständig und verschlüsselt vom Server auf die Clients übertragen werden. Die Materialien werden dann im Browser-Cache zwischengespeichert, bevor sie mittels Java-Script in das Test-Applet geladen werden. Durch diesen Vorgang wird verhindert, dass während der Klausur Änderungen an den Fragen vorgenommen werden. Denn die gesamte Klausur befindet sich bereits auf den Clients. Dies setzt zwar prüfungsrechtliche Anforderungen um, aber die Authentifizierung und die Verbindlichkeit werden nicht sichergestellt. Außerdem ist die Frage nach der Verfügbarkeit nicht beantwortet, wenn der Client während der Prüfung ausfällt.

Die beschriebenen Konzepte decken nur einen Teil der Sicherheitsanforderungen an elektronische Prüfungen ab. Für eine rechtssichere Durchführung von elektronischen Prüfungen kommen die Konzepte deshalb nicht in Frage.

[4] *formativ*: Übungen, Selbsttests, etc.; *summativ*: Klausuren, bewertete Prüfungen, etc.

Daher muss ein Konzept entwickelt werden, welches Lösungen für die bestehenden Schwachstellen bereits existierender Konzepte bereitstellt. Bei der Entwicklung dieser Sicherheitsarchitektur kann auf bestehende Lösungsansätze für andere Problemkontexte zurückgegriffen werden. Ein Konzept, das alle Sicherheitsanforderungen an elektronische Prüfungen umsetzt, ist das Lösungskonzept der elektronischen Gesundheitskarte ([Fr05], [Ca06]).

3 Sicherheitskonzept für elektronische Prüfungen

Da die Sicherheitsarchitektur zur Herstellung der Rechtsverbindlichkeit elektronischer Prüfungen auf Teilen des Lösungskonzeptes der elektronischen Gesundheitskarte (eGK) aufbaut, wird im Folgenden zuerst näher auf die eGK eingegangen bevor in Abschnitt 3.2 aufgezeigt wird, wie die Adaption an die Durchführung elektronischer Prüfungen erfolgen kann.

3.1 Lösungskonzept elektronische Gesundheitskarte

Die elektronische Gesundheitskarte (eGK) wird aufgrund des Gesetztes zur Modernisierung der gesetzlichen Krankenversicherung eingeführt. Durch die Nutzung einer Chipkarte sollen viele Anwendungsfälle der medizinischen Versorgung, wie die elektronische Übertragung von Rezepten papierlos ablaufen. Um diesen Austausch zu gewährleisten, muss die eGK auf einer leistungsfähigen Infrastruktur basieren, damit die Patientendaten sicher transportiert werden können. Die bestehende Infrastruktur der Primärsysteme in Krankenhäusern, Arztpraxen und Apotheken können und sollen beibehalten werden, so dass die Anwendungen dieser Primärsysteme nur erweitert werden, ansonsten aber wie bisher genutzt werden können.

Die Infrastruktur muss hoch verfügbar und performant sein und dazu noch sicherstellen, dass ein Zugriff auf Daten nur mit der Einwilligung des Versicherten erfolgen kann („Patient bleibt Herr seiner Daten“) [Ca06]. Auch der Zugriff seitens des Leistungserbringers (Arzt, Apotheker, etc.) kann nur in Verbindung mit einem chipkartenbasierten Heilberufeausweis erfolgen. Allerdings kann der Versicherte für die Daten rollenbasierte (z.B. alle Apotheken) oder sogar auf Einzelpersonen bezogene Rechte zum Eingriff vergeben.

Basis dieser Infrastruktur sind qualifizierende digitale Signaturen, die auf einem gültigen Zertifikat beruhen. Das Zertifikat bescheinigt insbesondere die Zugehörigkeit eines öffentlichen Schlüssels zu dem Zertifikatsinhaber und wird von einer Zertifizierungsinstanz ausgestellt. Die Signaturen stellen die Verbindlichkeit (Nichtabstreitbarkeit) der Kommunikation, die Authentizität der Anwender und die Integrität der Daten sicher.

In Abb. 1 ist die Lösungsarchitektur der eGK dargestellt. Die zentralen Komponenten, die für die elektronischen Prüfungen von Interesse sind, sind die Konnektoren, die Access/Service-Gateways und die Zugangs- und Integrationsschicht (ZIS).

Die Konnektoren mit angeschlossener VPN-Box dienen dazu die Primärsysteme an die Kommunikationsinfrastruktur anzubinden. Dazu nimmt die VPN-Box Kontakt zu einem Access Gateway auf, das wiederum anhand der Zertifikate der Kommunikationsteilnehmer entscheidet, welches VPN benutzt werden soll. Die VPN enden dann in den jeweiligen Service Gateways, welche die Berechtigungen zu den entsprechenden Diensten kontrollieren. Die Dienste wiederum greifen auf die Datenbanken über die Zugangs- und Integrationsschicht zu.

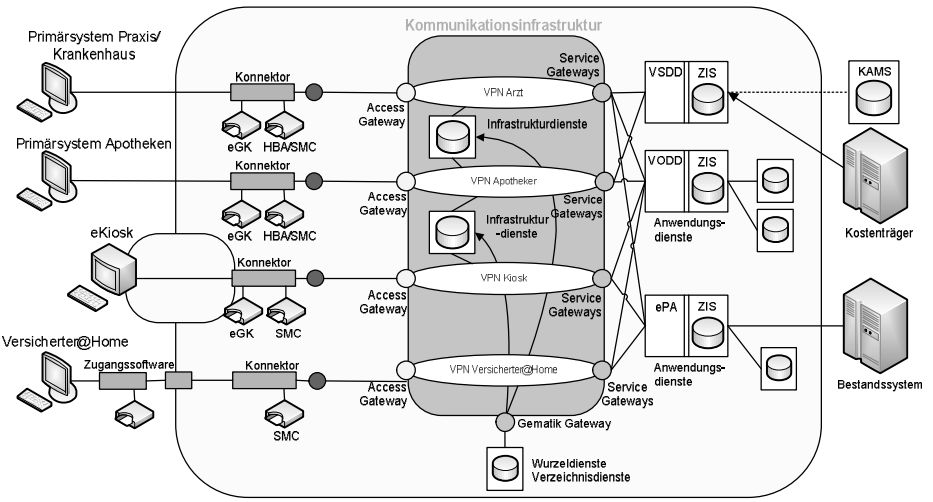

Abbildung 1: Lösungsarchitektur eGK [Fr05]

Die Zugangs- und Integrationsschicht (ZIS) ist die Schnittstelle zwischen dem Informatiksystem und den Datenspeichern. Durch sie wird der Zugriff auf die Daten transparent gestaltet, so dass es aussieht, als ob im Hintergrund ein gemeinsames virtuelles Dateisystem existieren würde, obwohl die Daten auf vielen Servern und sogar auf der eGK gespeichert sein können.

Auf die Daten auf den Servern dürfen nur autorisierte Personen zugreifen, was durch ein Rechtemanagement sichergestellt wird. Aufgrund der Sensibilität der Daten und der Struktur des Informatiksystems sind die Daten auch vor den Betreibern und Administratoren der Datenserver geschützt. Dazu gehört auch, dass es nicht möglich ist, den Datensatz einer bestimmten Person zuzuordnen. Um Daten vor einem Einblick zu schützen, werden diese verschlüsselt. Da bei einer größeren Datenmenge eine asymmetrische Verschlüsselung zu rechenintensiv ist, werden die Daten hybrid verschlüsselt. Der symmetrische Schlüssel, mit dem die Daten verschlüsselt wurden, wird mit dem öffentlichen Schlüssel der eGK verknüpft. Dies kann nur durch den zugehörigen privaten Schlüssel rückgängig gemacht werden, wozu der Versicherte seine Erlaubnis mit der Eingabe seiner persönlichen PIN gibt.

Um an die Datensätze zu gelangen, wird dem Leistungserbringer (Arzt, Apotheker, etc.) ein Ticket für diesen Datensatz ausgestellt. Um ein Ticket zu erstellen, muss die eGK anwesend sein, weil nur in dieser der benötigte geheime Schlüssel des Versicherten gespeichert ist, womit der Schlüssel für das Datenobjekt gewonnen werden kann. Die Einwilligung zum Erstellen eines Tickets gibt der Versicherte dadurch, dass er sich mit seiner PIN authentifiziert. Zum Erstellen eines Tickets ist es nicht nötig, dass der Heilberufsausweis anwesend ist. Jedes Objekt, ob Verzeichnis oder Datensatz ist einem sog. T-Node zugeordnet. Das Konzept des ticketbasierten, virtuellen Dateisystems ist in Abb. 2 dargestellt.

Zur Erstellung eines Tickets enthält der T-Node ein TicketToolkit, das angesprochen wird wenn ein Ticket erstellt, aber auch wenn ein Ticket geprüft werden soll. Ein Ticket enthält vor allem eine gespeicherte Zufallszahl (RND), die als Verifizierer genutzt wird, den Schlüssel, mit dem die Daten verschlüsselt wurden (SeK), und eine Kennzeichnung des Leistungserbringers der auf die Daten zugreifen möchte. Der Leistungserbringer weist sich mit seinem Zertifikat, das auf dem Heilberufsausweis gespeichert ist, aus. Weiterhin werden die ID des T-Nodes und die ID des Datenobjekts mit angegeben. Diese Maßnahme vereinfacht es der ZIS, den gewünschten Datensatz zu lokalisieren. Der Anwendung bleibt dabei verborgen, wo der Datensatz tatsächlich gespeichert wurde. Der lokalisierte Datensatz wird dann im verschlüsselten Zustand an den Konnektor gesendet, wo dann die Entschlüsselung erfolgt. Die ZIS hat weder die Berechtigung, noch die benötigten Algorithmen, um Datensätze zu ver- oder entschlüsseln.

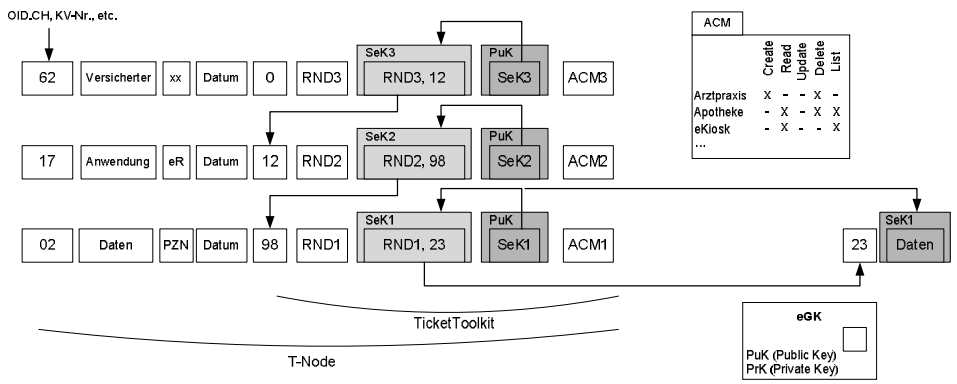

Abbildung 2: Ticketbasierte, virtuelle Dateisystem der eGK [Ca05]

Aufgrund der Verteiltheit der Daten, benötigt man Mechanismen zur Lokalisierung der Daten. Jedes Datenobjekt bekommt einen eindeutigen Identifizierer und wird einem oder mehreren Verzeichnissen zugewiesen. Dies geschieht über die Speicherung einer Liste von Verzeichnis-IDs in dem Datenobjekt. Die ZIS muss andererseits auch wissen, auf welchem Server die Objekte gespeichert sind. Daher werden in einem Verzeichnisobjekt Adressen von Serverprozessen, die das referenzierte Objekt behandeln, hinterlegt. Da ein Verzeichnis keine Hinweise auf eine Person enthält und auch nicht direkt auf die Datenobjekte verweist, ist es nicht nötig, die Verzeichnisobjekte zu verschlüsseln.

Jeder Versicherte hat genau ein Wurzelverzeichnis, dem eine ID, die mit der Krankenversichertennummer übereinstimmt, zugeordnet wird. Dieses Wurzelverzeichnis kann über einen speziellen Dienst der ZIS gefunden werden (Query-Dienst), ist aber genauso geschützt wie alle anderen Objekte.

Zusammenfassend lässt sich also sagen, dass das Lösungskonzept der eGK die Anforderungen an elektronische Prüfungen im Bezug auf die Verbindlichkeit (durch die digitalen Signaturen) und den Datenschutz (durch das ticketbasierte, virtuelle dateisystem) vollständig abdeckt und gleichzeitig in eine bestehende Systemlandschaft integriert werden kann. Da das Lösungskonzept der elektronischen Gesundheitskarte (eGK) jedoch aus einer sehr umfangreichen Informations-, Kommunikations- und Sicherheitsinfrastruktur besteht und eine derartige Telematikinfrastruktur nur sehr bedingt für den Hochschuleinsatz tauglich ist, erfolgt im folgenden Abschnitt keine vollständige Übernahme der Methoden sondern eine Anpassung auf den Problemkontext für elektronische Prüfungen.

3.2. Lösungskonzept der elektronischen Prüfungen

Erste Ansätze zur Übertragung der Sicherheitsanforderungen der elektronischen Prüfungen auf das Lösungskonzept der eGK zeigen, dass dies unter bestimmten Voraussetzungen und Anpassungen möglich ist [Be08]. So sind die entscheidenden Konzepte nahezu vollständig auf die elektronischen Prüfungen abbildbar. Eine erste Implementierung findet sich in [Br08], in der das so genannte Ticketkonzept der elektronischen Gesundheitskarte exemplarisch erfolgreich umgesetzt wurde.

Bei der Umsetzung der Sicherheitsarchitektur werden an die Infrastruktur bestimmte Voraussetzungen gestellt. So muss jeder Student bei der Immatrikulation eine elektronische Studentenkarte (eSK) ausgehändigt bekommen, auf der seine persönlichen Daten, ein privater Schlüssel und ein öffentlicher Schlüssel mit einem zugehörigen Zertifikat gespeichert sind. Ebenfalls bekommen die Mitarbeiter des universitären Lehrbetriebes je eine elektronische Prüferkarte (ePK), auf der ebenfalls persönliche Daten, der Status (Professor, Privatdozent, wissenschaftlicher Mitarbeiter) und ein zertifiziertes Schlüsselpaar gespeichert sind. Weiterhin muss eine hochschulweite Public-Key Infrastruktur (PKI) existieren und alle beteiligten Rechner müssen mit entsprechenden Smartcard-Readern ausgestattet sein.

Ein wesentlicher Unterschied zum Lösungskonzept der eGK ist, dass im Gesundheitssystem alle 80 Millionen Bürger der Bundesrepublik als Anwender betrachtet werden müssen. Bei Universitäten beläuft sich die Anwenderzahl zumeist im 5-stelligen Bereich. Während das System der eGK auf Grund der großen Teilnehmerzahl sehr gut skalieren muss, um alle Akteure bedienen zu können, ergeben sich für die Sicherheitsarchitektur zur Durchführung von elektronischen Prüfungen Vereinfachungen. Dazu zählt vor allem die Realisierung der Konnektoren als Software und zwar als Applet, anstatt als Hardware-Konnektor wie im Konzept der eGK vorgesehen. Das Applet stellt einen Container dar, in dem nicht nur die komplette Authentifizierung und Kommunikation mit dem Smartcard-Reader stattfindet, sondern auch die Klausurfragen in einem XML-Format dargestellt werden können (z.B. QTI)

(vgl. [Br08]). Das Applet wird von dem Access-Gateway geladen. Für bereits bestehende Prüfungssysteme könnte der Konnektor als eine Art Proxy fungieren, über den die komplette Kommunikation zwischen Clientanwendung und Server stattfindet (vgl. [Ei07]).

Weitere Anpassungen bestehen in der Schaffung einer sicheren Prüfungsumgebung auf den Systemen in den Rechnerpools, die für elektronische Prüfungen genutzt werden sollen. Das heißt, es darf dem Studierenden nicht ermöglicht werden, mit anderen Rechnern zu kommunizieren oder durch Programmaufrufe Zugriff auf Informationen zu erlangen. So muss auf jedem Rechner ein Benutzer mit bestimmten Einschränkungen eingerichtet werden. Der eingeschränkte Benutzer bekommt lediglich die Möglichkeit, einen Browser zu starten, andere Programme dürfen hingegen nicht ausführbar sein. Zudem wird durch diesen Benutzer nur eine gesicherte VPN-Verbindung zu einem speziellen Rechner im Rechnerpool zugelassen. Ein Applet prüft auch hier zunächst die Gültigkeit der Zertifikate auf der Karte und führt so eine Authentifizierung durch.

Auf einem speziellen Rechner im Rechnerpool meldet sich der Prüfer an. Dieser Rechner nimmt die VPN-Verbindungen der Rechner der Studierenden entgegen und multiplext diese auf eine VPN-Verbindung zu dem Klausurenserver. Dadurch wird sichergestellt, dass kein Prüfungsteilnehmer auf das Internet zugreifen kann. Der Prüfer muss vor Beginn der Prüfung den Namen bzw. die Adresse des Prüfungsservers eingeben. Der Rechner dient dann als Access Gateway für die Clients im gesamten Rechnerpool. Wenn die Switche, die in der Hochschule eingesetzt werden, über Managementfunktionen verfügen, kann das Hochschulrechenzentrum (HRZ) zeitweilig ein VPN auf Ethernet-Ebene einrichten. Wenn dies nicht erfolgen kann, muss der Gateway-Rechner ein VPN auf IP-Ebene aufbauen. Die Verbindung zwischen den Clients und dem Gateway-Rechner kann somit als verteilter Konnektor betrachtet werden.

Zugänge zur Infrastruktur

In Abb. 3 ist die Grobarchitektur für die elektronischen Prüfungen dargestellt. Es existieren verschieden Zugänge zur Infrastruktur. Bei allen Zugängen wird zunächst das Zertifikat gelesen und dieses verifiziert. Sollte das Zertifikat nicht gültig sein, so wird der Vorgang mit einer entsprechenden Hinweismeldung abgebrochen.

Die Studierenden müssen sich verbindlich zu einer Prüfung anmelden. Dazu nutzt der Studierende seine eSK an einem PC des Prüfungsamtes oder aber einen PC mit Smartcard-Readern in einem der Labore. Auch von zu Hause aus wäre eine Anmeldung möglich, wenn er über einen entsprechenden Smartcard-Reader verfügt. Der Studierende wählt die Prüfungen aus zu denen er sich anmelden möchte. Von dem Prüfungsamt erhält er dann ein zeitlich gebundenes Ticket für jede ausgewählte Prüfung, die ihn zur Durchführung der Prüfung berechtigen (vgl. [Br08]).

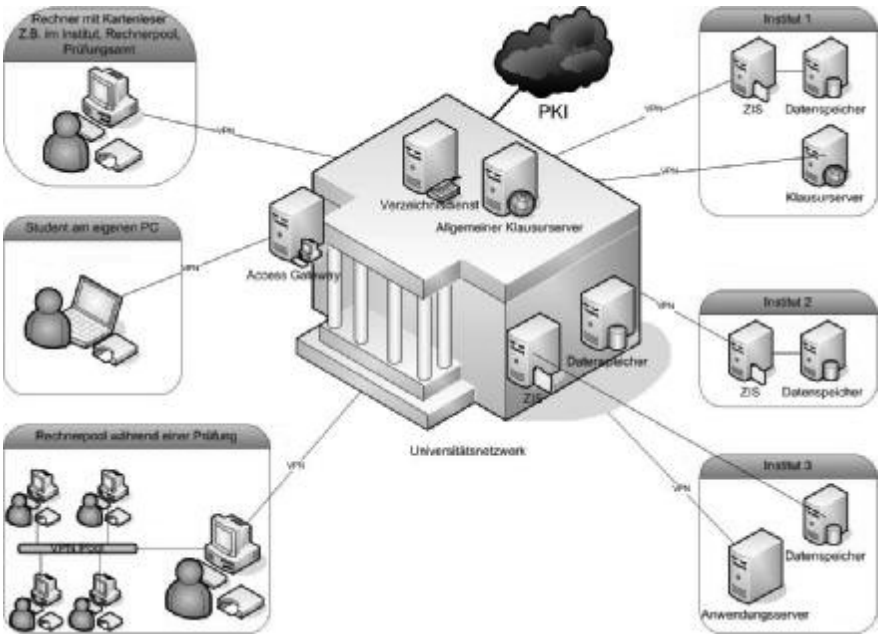

Abbildung 3: Grobarchitektur des Sicherheitskonzepts [Be08]

Zur Prüfungsdurchführung können nur die entsprechend ausgestatteten Rechner in den Laboren genutzt werden. Die Angaben der Studierenden werden durch den Konnektor auf ihren Clients verschlüsselt und signiert.

Der Prüfer meldet sich mit Hilfe seiner ePK am System an, um die Dienste zur Klausurerstellung zu nutzen. Zur Auswertung hat der Prüfer von den Studierenden Tickets mit der Berechtigung zur Einsicht in die Lösung nach der Prüfung erhalten. Zu diesem Ticket gehört ein weiteres, welches den Prüfer dazu berechtigt, die Ergebnisse online in die jeweilige elektronische Studentenakte des Studierenden zu schreiben. Entfällt das zweite Ticket so muss das Ergebnis wie bisher in Papierform dem Prüfungsamt zugestellt werden.

Das Prüfungsamt hat wiederum einen speziellen Zugang. Hier wird entweder ein installierter Proxy verwendet, oder aber wie bei der eGK ein Hardware-Konnektor, der zwischen den Primärsystemen und dem Hochschulnetz zwischengeschaltet ist. Somit könnten ggf. die Primärsysteme in den Prüfungsämtern ohne Anpassung weiter genutzt werden.

Informatiksystem

Das Informatiksystem besteht aus verschiedenen Servern, die innerhalb der Universität miteinander verbunden sind. Diese Server werden als verteiltes System betrachtet. Daher existiert innerhalb der Hochschule ein Server, der einen Verzeichnisdienst ausführt, bei

dem sich alle Dienste (Klausurdienste, Systemdienste, Sicherheitsdienste, etc.) registrieren. Dieser Server kann vom Hochschulrechenzentrum (HRZ) bereitgestellt und betrieben werden. Zusätzlich kann vom HRZ ein Access Gateway betrieben werden, über das Verbindungen angenommen und dann per VPN an die Dienstserver geleitet werden. Die Dienstserver führen die angebotenen Dienste aus.

In Abb. 3 sind die Zugangspunkte auf der linken Seite aufgezeigt, während die Anwendungs- und Datenserver auf der rechten Seite befinden. Beide Seiten werden über das universitäre Netzwerk verbunden, welches auch die Systemdienste beinhaltet.

Der Zugang zum Informatiksystem wird immer zuerst mit einer VPN-Verbindung zu dem Access Gateway gestartet. Auch alle weiteren Verbindungen werden durch VPN-Tunneln geschützt. Von dem Access Gateway wird das Applet geladen, welches die weiteren Funktionen beinhaltet. Auch wird eine Authentifizierung der Karte nur mit dem Applet vollzogen, daher werden Mechanismen gebraucht, damit das Access Gateway keinem Denial-of-Service unterliegt. Eine Möglichkeit wäre statt einem Access Gateway ein Cluster an Servern zu nutzen, die sich die Arbeit untereinander aufteilen können.

Zusätzlich müssen alle Verbindungen in den Gateways und auf dem Prüfungsserver protokolliert werden. Durch die Protokollierung wird die Rechtsgültigkeit der Prüfung gestärkt, da diese dadurch nachvollziehbar wird. Auf den Clients werden die Antworten mitprotokolliert. Auf der eSK werden die letzten Klausurteilnahmen aufgezeichnet. Aufgrund der geringen Speicherkapazität einer Smartcard werden die Protokollierungsdaten auf der Karte zyklisch gespeichert.

Damit können eventuell fehlende Daten reproduziert werden. Dazu können bei Betrugsverdacht die Prüfer Einsicht in die Protokolldaten nehmen, um dies zu belegen oder zu widerlegen. Die Protokollierung muss eine stattgefundene Kommunikation lückenlos belegen können. Da durch die Protokolldaten eine Zuordnung der Kommunikation zu den Kommunikationspartnern möglich ist, müssen diese Daten geschützt werden. Sie dürfen nur von vertrauenswürdigen Personen entschlüsselt werden können.

Datenspeicherung

Um die Daten sicher und anonym zu speichern, wird das System der Zugangs- und Integrationsschicht von der eGK übernommen. Dadurch können Daten auf mehreren Servern gespeichert werden. Die Datenserver können somit in den verschiedenen Instituten verwaltet sein. Jedes Institut könnte somit auf seinen eigenen Servern die Daten von ihren Prüfungen speichern. Durch die Nutzung der ZIS wird die vom Bundesdatenschutzgesetz geforderte Datensicherheit und Anonymität der Daten gewahrt.

Die Daten werden in unterschiedlichen Ordnern auf dem Klausurserver gespeichert. In einen Ordner kommen die Lösungen zu den Klausuren. Bei diesen Daten wird eine eindeutige Bezeichnung der zugehörigen Klausur mit angegeben, da die Lösungen ohne die Fragen abgespeichert werden.

In einem anderen Ordner werden alle relevanten Daten abgelegt, auf die das Prüfungsamt zugreift. Analog zur elektronischen Patientenakte wird dieser elektronische Studentenakte (eSA) genannt. In diese werden die ausgestellten Scheine von den Prüfern gelegt. Weiterhin speichert das Prüfungsamt Anmeldungen, Abmeldungen und Krankmeldungen. Alle weiteren für die Studienlaufbahn wichtigen Dokumente werden ebenfalls in der eSA abgelegt.

Durch die Verwendung des ticketbasierten Zugangs zu den Daten kann die Anonymität des Prüfungsteilnehmers noch besser gewahrt werden. Nach der Prüfung erhält der Prüfer nur ein Ticket zum Lesen der Lösung und ein Ticket zum Schreiben des Scheins in die eSA. Der Prüfer kann aus diesen Daten nicht ersehen, von wem die Lösung stammt, und diese daher vorurteilsfrei bewerten. Das Prüfungsamt bekommt das Recht, auf die Daten zuzugreifen, um diese zu prüfen.

4 Zusammenfassung und Ausblick

Die speziellen Sicherheitsanforderungen an elektronische Prüfungen an Hochschulen führten zu der Überlegung ein eigenes Sicherheitskonzept dafür zu entwickeln. Jedoch bedingte die Tatsache, dass für rechtsverbindliche Klausuren qualifizierende digitale Signaturen Voraussetzung sind, dass nach Lösungen gesucht werden musste, die eine multifunktionale Nutzung der Signaturen ermöglicht. Das Lösungskonzept der elektronischen Gesundheitskarte (eGK) setzt alle Sicherheitsanforderungen an elektronische Prüfungen um. Speziell die datenschutzrechtlichen Vorgaben werden durch standardisierte Verfahren vollständig implementiert („Student bleibt Herr seiner Daten“). Allerdings ist das Konzept der eGK für Hochschulen auf Grund der geringeren Nutzerzahlen überdimensioniert und muss entsprechend angepasst werden.

In diesem Beitrag wurde gezeigt, wie das Konzept der eGK auf elektronische Prüfungen übertragen werden kann. So erlaubt das dargestellte Ticketkonzept die Anonymität der Nutzer trotz Authentizität. Es wäre dadurch nicht nur möglich, computergestützte Klausuren „sicher“ durchzuführen sondern auch anonyme Online-Selbsttest und Online-Lehrevaluierungen.

Ein weiterer Fortschritt des dargestellten Konzeptes ist die Möglichkeit des hochschulübergreifenden Einsatzes. So können beispielsweise Studierende der Universitäten Köln und Bonn Prüfungen an beiden Hochschulen ablegen und sich diese anerkennen lassen. Mit dem vorgestellten Konzept könnte somit hochschulübergreifend ein einheitliches Sicherheitskonzept geschaffen werden.

Literaturverzeichnis

[Be08] Bernshausen, K.: Erstellung einer Sicherheitsarchitektur für Online Klausuren an Hochschulen auf Basis der Lösungsarchitektur der elektronischen Gesundheitskarte. Diplomarbeit Universität Siegen, 2008

[Br08] Brennscheidt, J.: Erstellung eines Sicherheitskonzepts für computergestützte Prüfungen mittels mobiler Ausführungsplattformen und digitaler Signaturen. Diplomarbeit Universität Siegen 2008.

[Ca05] Caumanns, J.: Management von Zugriffen auf medizinische Daten – Tickets und Berechtigungen. http://www.gkarte.iao.fraunhofer.de/publicdocs/050304_AB/Daten_und_Zugriffsmgmt.pdf, 2005

[Ca06] Caumanns, J.: Der Patient bleibt Herr seiner Daten – Realisierung des eGK-Berechtigungskonzepts über ein ticketbasiertes, virtuelles Dateisystem. In: Informatik-Spektrum, Jg. 29, Ausgabe 5, 2006, S. 323-331

[Ei07] Eibl, C.J.; von Solms, S.H.; Schubert, S.: Development and Application of a Proxy Server for Transparently, Digitally Signing E-Learning Content. In: Venter, H.; Eloff, M.; Labuschagne, L.; Eloff, J.; von Solms, R. (Eds.): IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, Springer Verlag, Boston, 2007, S. 181-192.

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

[Gr02] Graf, F.: Lernspezifische Sicherheitsmechanismen in Lernumgebungen mit modularem Lernmaterial. Dissertation, Fachbereich Informatik, Techn. Universität Darmstadt. 2001

[Ho07] Hoffmann, A.: Ein prozessorientiertes und dienstbasiertes Sicherheitsmodell für elektronische Prüfungen an Hochschulen. In Ch. Eibl, J. Magenheim, S. Schubert, M. Wessner (Hrsg.), DeLFI 2007: 5. e-Learning Fachtagung Informatik, GI-Edition-Lecture Notes in Informatics, P111, S. 297-298, 2007

[HS99] Hoeren, T., Schüngel, M.: Rechtsfragen der digitalen Signatur – Eine Einführung in Recht und Praxis der Zertifizierungsstellen, Erich Schmidt Verlag, Berlin, 1999

[Sc05] Schaffert, S.: Online-Prüfungen zur Zertifizierung informell erworbener beruflicher Kompetenzen. In: bwp@ Berufs- und Wirtschaftspädagogik, Ausgabe 8, 2005.

[SG99] Schmidt, J. U., Gutschow, K. (Hrsg.): Vom Papier zum Bildschirm – Computergestützte Prüfungsformen. Berichte zur beruflichen Bildung. W. Bertelsmann Verlag, Bielefeld, 1999

[St06] Steinberg, M.: Organisatorisches Konzept für Online-Prüfungsverfahren – Ein Stufenmodell für die Realisierung von Online-Assessment, http://www.sra.uni-hannover.de/fileadmin/uploads/Mitarbeiter/Steinberg/Publikationen/AP7_Org_Konzept_screen_V1.pdf, 2006