

DeLFI 2009

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

Dipl.-Ing. Andreas Hoffmann

Universität Siegen
Fachbereich Elektrotechnik und Informatik
Lehrstuhl Betriebssysteme / verteilte Systeme

17.09.2009

Agenda

- Einleitung
- Sicherheits- und rechtlich relevante Anforderungen an ePrüfungen
- Datenschutz vs. Datensicherheit
- Sicherheitsarchitektur für ePrüfungen
- Realisierung mittels Client-Proxy
- Zusammenfassung und Ausblick

Einleitung

- BA/MA Einführung erhöhte die Zahl der Prüfungsleistungen
- Elektronische Prüfungen kompensieren Mehraufwand bei Massenprüfungen
- *Aber: Besonders große Bedenken betreffen den Datenschutz und die Datensicherheit elektronischer Prüfungen*

Rechtliche Anforderungen

- Rechtliche Anforderungen unabhängig von Durchführungsart (auf Papier, elektronisch)
- Nach § 126 Abs. 3 BGB kann die papierbasierte Form durch die elektronische Form gem. § 126a BGB ersetzt werden (siehe [Ki08])
 - Bedingung: „...das elektronische Dokument mit einer qualifizierenden digitalen Signatur versehen ist.“
 - Qualif. Digitale Signatur: elektronische Unterschrift bzw. eindeutiges Siegel die den Unterzeichner und die Unversehrtheit der Daten erkennen lässt → Zertifiziert durch vertrauenswürdige Instanz
 - Notwendigkeit: Sichere-Signatur-Erstellungseinheit (SSEE) – Chipkarten, USB-Tokens
- Nichtabstreitbarkeit der Prüfungsangaben und –fragen
- Authentifizierung und Autorisierung der Teilnehmer
- Protokollierung des Prüfungsverlaufes des Studierenden

Rechtliche Anforderungen

- Betrugssicherheit
- Prüfungsordnung
 - Elektronische Prüfungen als eigenständige Prüfungsform aufnehmen
 - Multiple/Choice Verfahren
 - Regelungen bei Systemausfall
- Gleichheitsgrundsatz / Chancengleichheit wahren
 - Vergleichbare Bedingungen für alle Teilnehmer
 - Unterschiedliche PC-Kenntnisse sind als unvermeidbar hinzunehmen
 - Nice to have: Anonyme Bewertung der Prüfungsleistungen
Aber: Kein Anspruch auf Anonymität!
- Prüfungseinsicht und Archivierung
- Datenschutz

Datenschutz	Datensicherheit
<ul style="list-style-type: none"> - Datensparsamkeit / -vermeidung 	<ul style="list-style-type: none"> - Erhebung und Speicherung von Prüfungsdaten - Erfassung der Prozesse / Prozessbeteiligten
<ul style="list-style-type: none"> - Anonymität 	<ul style="list-style-type: none"> - Personalisierter Zugang - Authentifizierung der TN - Eindeutige Zuordnung TN <-> Prüfung
<ul style="list-style-type: none"> - Löschung der Spuren 	<ul style="list-style-type: none"> - Nachvollziehbarkeit des Prüfungsablaufes - Nichtabstreitbarkeit der Prüfungsdaten - Archivierung der Prüfungsdaten
<ul style="list-style-type: none"> - Schutz der Grundrechte 	<ul style="list-style-type: none"> - Schutz des Systems

vgl.: Schaar, Peter: Datenschutz und IT-Sicherheit, 15 Jahre IT-Grundschutz, Vortrag zum Jubiläum des IT-Grundschutzes, Bonn, 23. Juni 2009

Problemstellung

- Widersprechende Anforderungen:
z.B. Anonymität \leftrightarrow Authentizität
- Integration in bestehende Systemlandschaften
- Qualifizierende digitale Signaturen:
 - Hoher administrativer und infrastruktureller Aufwand
→ nur für einen multifunktionalen Einsatz an Hochschulen sinnvoll
 - „What you see is what you sign“
- Datenschutz: Verwendung von standardisierten und transparenten Verfahren

Status Quo existierender Systeme

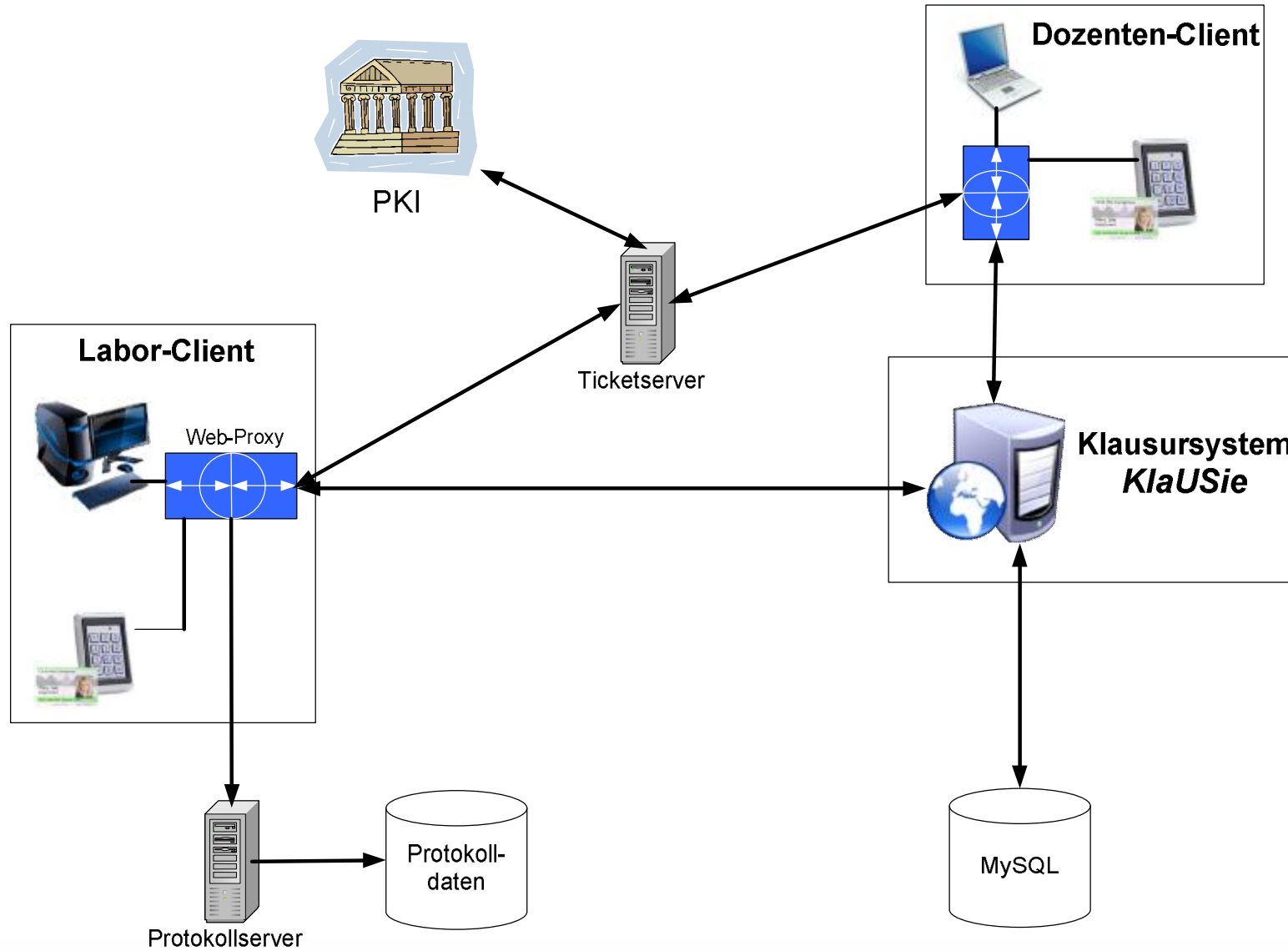
- LPLUS, OLAT, ILIAS
- Gewährleisten Authentizität und Autorisierung durch Rechte- / Rollenmanagement
- Verbindlichkeit, Archivierung nur durch Medienbrüche
 - Ausdruck und Unterschrift der Angaben
 - Archivierung der Ausdrücke
 - Löschung der elektronischen Daten nach Auswertung

Realisierungsansatz

- Basierend auf dem Lösungskonzept der eGK [HW08]
 - Virtuelles, ticketbasiertes Dateisystem
 - Standardisierte Verfahren
 - Realisierung aller Sicherheitsanforderungen
 - Verbindlichkeit durch qualif. dig. Signaturen
 - Anonymität trotz Authentizität
 - Akteure bleiben „Herr ihrer Daten“
 - Vergabe von feingranularen Berechtigungen (Tickets)

- Umsetzung mittels clientseitigen Proxy

Architektur



Web-Proxy

■ Aufgaben:

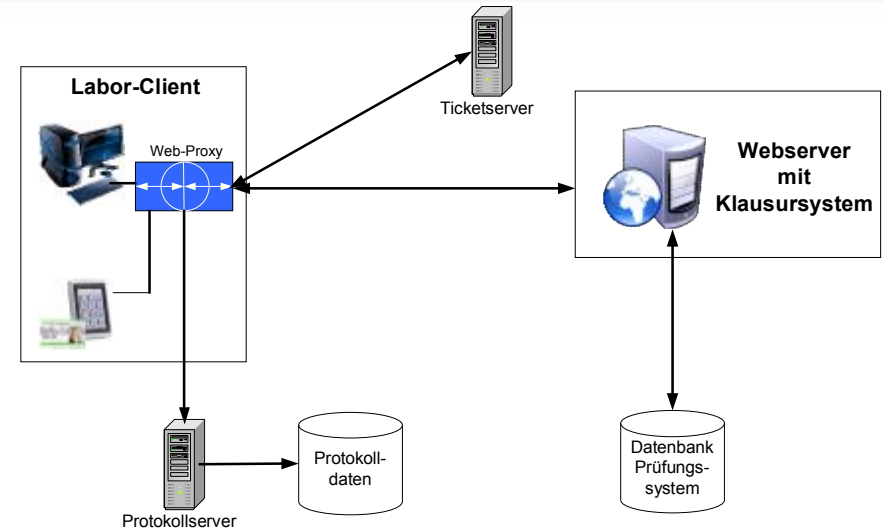
- Ver- und Entschlüsselung
- Signierung und Verifizierung
- Protokollierung des Prüfungsverlaufes

■ Browser → Proxy → Server

- Proxy empfängt vom Browser HTTP-Nachricht
- Proxy verschlüsselt Prüfungsinhalte im HTTP-Body ($\$_POST$ Variablen)
- Proxy berechnet Header-Felder (Content-Length) neu
- Proxy baut ggf. HTTP-Anfrage in HTTP(S)-Anfrage um (*http2https*)

■ Server → Proxy → Browser

- Proxy empfängt HTTP(S)-Nachricht vom Server
- Proxy entschlüsselt / verifiziert Prüfungsfragen bzw. -angaben
- Proxy berechnet Header-Felder (Content-Length) neu
- Browser stellt HTML-Seite dar



```

<html>
<head> ... </head>
<body>

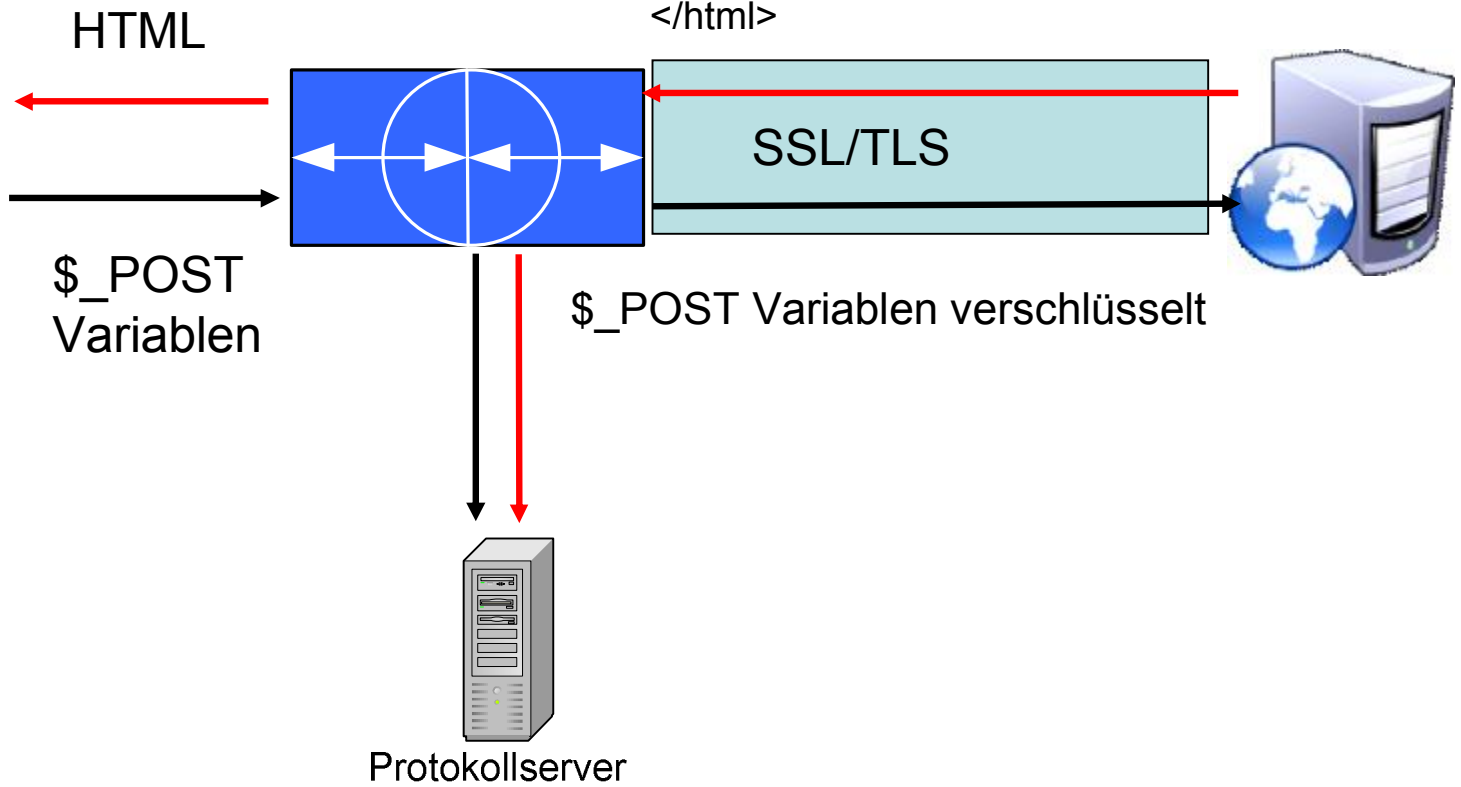
```

!PROX-EN! Chiffretext !NE-XORP!

```

...
</body>
</html>

```



Zusammenfassung

- PKI, qualifizierte dig. Signaturen, Ticketkonzept mit Web-Proxy
 - Datenschutz und Datensicherheit
- Aber z.Zt.: Anpassungen am Klausursystem notwendig
- Konzept auch für webbasierte Übungssysteme, Lehrevaluierungen, elektronische Studierendendateien einsetzbar
- Ausblick: Anpassungen an Klausursystemen minimieren durch serverseitigen Proxy

Kontakt:

andreas.hoffmann@uni-siegen.de
www.online-testen.com

Quellen:

- [HW08] A. Hoffmann, R. Wismüller: *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] Iris Kirchner-Freis: *Rechtliche Aspekte des eLearning und eAssessment : Ein Praxisleitfaden* / Hrsg. Andree Kirchner; Hrsg. Iris Kirchner-Freis; Hrsg. MLS Rechtsanwaltsgesellschaft mbH; 2008.