Veröffentlicht in: Tagungsband der 12. Nachwuchswissenschaftlerkonferenz mitteldeutscher Fachhochschulen, Hochschule Harz, Wernigerode, 2011.

eCampus-Services & -Infrastrukturen – eGovernment-Komponenten- und Service-orientierte elektronische Campusverwaltung mit verbesserter Sicherheit

FKZ: 11.03-08 / EFRE-Maßnahme „Neue Technologien“, 11.03/41.03

M. Hennning, mhenning@hs-harz.de, Hochschule Harz, Friedrichstr. 57-59, 38855 Wernigerode
Hendrik Werner, hwerner@hs-harz.de, Hochschule Harz, Friedrichstr. 57-59, 38855 Wernigerode
P. Kußmann, pkussmann@hs-harz.de, Hochschule Harz, Friedrichstr. 57-59, 38855 Wernigerode
Dr. Nico Brehm, nico.brehm@repugraph.com, RepuGraph GmbH, Alte Leipziger Str. 50, 99734 Nordhausen
Prof. Dr. Hermann Strack, hstrack@hs-harz.de, Hochschule Harz, Friedrichstr. 57-59, 38855 Wernigerode

Abstract:

eGovernment-Standards und -Basiskomponenten werden zur Verbesserung der prozessorientierten Umsetzung von Campus-Systemen an Hochschulen und deren Sicherheit kriterienorientiert eingesetzt, im Rahmen des F&E-Projekts „eCampus“. Drei Architekturansätze bis zu Weiterentwicklungen serviceorientierter Architekturen (SOA) werden identifiziert.

Keywords: eGovernment-Basiskomponenten, OSCI, Qualifizierte rechtverbindliche elektronische Signatur, Verfahrenselektronisierungen**,** HIS, SOA, eCampus, Standardisierung

1 Einführung

Im Rahmen des Projekts eCampus - Services & -Infrastrukturen für gesicherte u. verbindliche vollelektronische Hochschulverwaltungen sollen ausgewählte Verfahrenselektronisierungen für Verwaltungsprozesse an Hochschulen untersucht und auf Basis verfügbarer eGovernment-Standards und -Komponenten umgesetzt werden. Unter Einsatz von innovativen eGovernment- und Sicherheitskomponenten, sowie der Integration entsprechender Architekturmodelle (u.a. auf Basis des eGovernment-Standards OSCI) soll dabei gewährleistet werden, dass sensitives Kommunikations- und Datenmanagement in den ausgewählten Szenarien nach Standards nachweisbar abgesichert, datenschutzkonform umgesetzt und elektronische Dokumente rechtsverbindlich elektronisch signiert werden können.

2 eCampus - sensible Daten und Prozesse an Hochschulen

Sensitive Kommunikations- und Datenmanagement-Anteile in den ausgewählten Szenarien sollen abgesichert, datenschutzkonform umgesetzt und elektronische Dokumente rechtsverbindlich elektronisch signiert werden können - unter Nutzung von Synergien und Kostenentlastungen aus dem Bereich der Umsetzung des eGovernment-Aktionsplans Sachsen-Anhalt (u.a. Pflegevertrag Governikus und PKI LSA). In Feldversuchen werden dabei die Realisierungen evaluiert, insbesondere auf Akzeptanz und Nutzerfreundlichkeit bei folgenden Fachverfahren betrachtet:

1) eTOR (Prüfungsdatenaustausch mit externen Hochschulen),
2) eExamReg (Prüfungsanmeldungen und -bewertungen),
3) eZeugnis (Zeugniskopien),
4) ePraxReg (Vereinbarung für Praxissemester),
5) eBafögSch (Leistungsscheine für Bafög),
6) eSchein (studentische Bescheinigung).

In diesem Papier werden die Fachverfahren/Prozessszenarien eExamReg ausführlicher betrachtet. Vor dem Hintergrund des Zielsetzungsspektrums eCampus wurden folgende Kriterien für entsprechende Konzeptionen und Umsetzungen entwickelt.

Tabelle 1: Kriterienkatalog Sicherheitsziele

Nr.	Kriterium
K1	Sicherung Vertraulichkeit, Authentizität, Integrität
K2	Rechtsverbindlichkeit/Signatur von elektr. Dokumenten
K3	Datenschutzkonformität
K4	Realisierung nachweisbarer Zustellungen (Verbindlichkeit)
K5	Nutzerentlastung bzgl. Signatur- & PKI-Checks
K6	Nutzung von Internet-Standards (u.a. XML/SOAP)
K7	Integration von XML und (Verwaltungs-)Standards
K8	Integrationsfähigkeit bzgl. Campusmanagementsystemen (z.B. HIS)
K9	Kosteneff. Nachnutzung von eGov.-Komponenten & Wartung
K10	Vertrauenswürdigkeit von Komponenten & Services
K11	Handhabbarkeit
K12	Kosten-Nutzen.

3 Architekturen und eGovernment-Komponenten in eCampus

Hinsichtlich Umsetzungen von Sicherheitsaspekten stehen eGovernment- und Sicherheits-Standards wie OSCI und PKI nach Signaturgesetz mit wiederverwendbaren Komponenten zur Verfügung:

- volle Rechtsverbindlichkeit: für elekt. Dokumente (PKI/Signatur) und deren Zustellung (OSCI),
- hochwertige Sicherheit sowie Vertrauenswürdigkeit für die Signaturstufen „Qualifizierte Signatur (QES)“ und „Akkreditierte (qualifizierte) Signatur (AKQES)“,

OSCI (Online Service Computer Interface) ist in Verwaltungen und Wirtschaft im Einsatz und ermöglicht die abgesicherte und rechtsverbindliche (nachweisbare) Zustellung von Nachrichten zwischen den Teilnehmern. So bildet OSCI das Verfahren „Einschreiben mit Rückschein“ elektronisch ab, in dem nachweisbare Zustellungen durch das Erzeugen von sogenannten Laufzetteln (signiert durch den OSCI-Intermediär) für jeden OSCI-Nachrichtenaustausch durchgeführt werden. Mittels OSCI wird u.a. durch Ende-zu-Ende-Verschlüsselungen und Signaturen sichergestellt, dass Vertraulichkeit, Integrität und Authentizität personenbezogener Daten bei der Übertragung über unsichere Netze, wie dem Internet, gewährleistet werden können. Daher wird OSCI auch entsprechend von der Konferenz der Datenschutzbeauftragten von Bund und Ländern empfohlen [SENPRE2005].

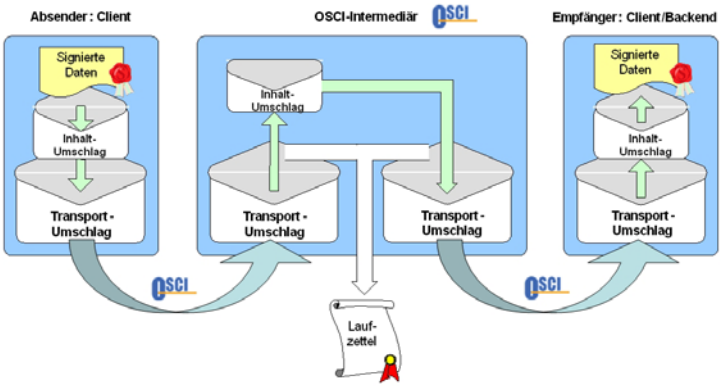

Abb. 1: OSCI-Infrastruktur

Für die Standards PKI/QES und OSCI können wesentliche eGovernment-Basiskomponenten LSA im Projekt eCampus zur Verfügung gestellt werden: PKI LSA, OSCI-Clients Govello & EGVP, OSCI-Intermediär(Server)/Governikus, vgl. [LDVK2010]. Mittels OSCI und vorgenannter eGovernment-Basiskomponenten können, maßgeblich Anforderungen und Ziele aus Kapitel 2, mittels folgender Sicherheitsfunktionen, erfüllt werden:

Tabelle 2: OSCI - Gegenüberstellung Sicherheitsziele und Sicherheitsfunktionen

Ziele / **Si-Funktionen**	Vertrau-lichkeit	Integrität	Authenti-zität	Nichtabstreit-barkeit	Zurechenbar-keit/Verbindlichkeit
Verschlüsselung	☺				
Entschlüsselung	☺				
Signatur		☺	☺	☺	☺
Signaturprüfung		☺	☺	☺	
Zertifikatsprüfung		☺	☺	☺	
Zeitstempel					☺
Laufzettel/Quittierung				☺	
Benutzerauthentisierung			☺		
Nachrichten-IDs			☺		

Im Vergleich zum Kriterienkatalog (s. **Fehler! Verweisquelle konnte nicht gefunden werden.**) ergibt sich damit das OSCI für das Erreichen der Sicherheitsziele geeignet ist. Hinsichtlich der Integrationsfähigkeit von Basiskomponenten, Standards und Diensten lassen sich zudem drei grundsätzliche Architekturansätze aufzeigen, mit denen sich entsprechende Integrationen von zusätzlichen (OSCI-) Sicherheitsfunktionen in ein eCampusmanagement-Systeme (wie HIS) umsetzen (nach Strack/Richter et.al [LDVK2010]).

A-CPM1. OSCI-Schalen-Architektur für eCampus-Systeme
A-CPM2. Builtin-SicherheitsArchitektur für eCampus-Systeme
A-CPM3. SOA-eCampus-Architektur.

Die Built-In-Architektur verfolgt dabei den Ansatz, dass die für das Projektumfeld notwendigen (OSCI-)Sicherheitsfunktionalitäten und -techniken direkt in das eCampus-System integriert werden (wie z.B. zukünftig in HISinOne), die SOA-eCampus-Architektur als deren Spezialfall berücksichtigt dabei zusätzlich SOA/WebService-Standards auch außerhalb von OSCI. Die Schalen-Architektur hingegen kennzeichnet sich dadurch, dass durch die Einbindung von bereits bestehenden eGovernment-(OSCI)Komponenten existierende eCampus-Systeme um zusätzliche „Sicherheitsschalen“ auf OSCI-Basis ergänzt werden, z.B. zum Ersatz schwachstellenbehafteter Eingabe-Schnittstellen auf Web-Basis (http/SSL) für elektr. Prüfungsdaten in herkömmlichen eCampus-Systemen.

4 Konzeption und Umsetzung eCampus-Verfahren am Beispiel

Die Abkürzung eExamReg steht für eine Elektronisierung der Prüfungsanmeldung und -bewertung. Zur Darstellung dient hier der Vorgang der Prüfungsbewertung. Folgende Risiken und Schwachstellen sind im IST-Ablauf beispielhaft erkennbar:

1) Gefälschter Prüfungsdateneintragungen auf Basis von einfacher Nutzername-Password-Authentifikation für webbasierte Prüfungssysteme.
2) Selbst bei Einsatz weiterer Zugangssicherungen zum Online-Prüfungssystem (z.B. persönliche Prüferzertifikate) verbleiben erhebliche Risiken bzgl. der Integrität, Authentizität und damit Verbindlichkeit der elektronischen eingetragenen Prüfungsdaten (derzeit: ergänzend Einreichung der Prüfungsdaten zusätzlich papiergebunden mit Unterschriften an das Prüfungsamt).

Auch bei der Übertragung auf Einsatzszenarien für studentische Prüfungsanmeldungen können ähnliche Risiken bzgl. Verbindlichkeit durch die herkömmliche elektronische Datenhaltung und deren Sicherungen bei Online-Anmeldungssystemen entstehen. Beim bisherigen Ablauf des Verfahrens gibt es folgende Probleme: Vielzahl von Medienbrüchen bei Noteneingabe, Mangelnde Authentizität & Integrität, Mangelnder Datenschutz bzgl. der Notenübersendung, Mangelnde Verbindlichkeit und Nichtabstreitbarkeit, Zusätzlicher Vertrauensanker auf Papier notwendig.

Die folgende Abbildung 2 veranschaulicht den neu-strukturierten Vorgang der Prüfungsbewertung nach dem Prinzip der OSCI-Schalensicherheitsarchitektur. Eine erste entsprechende Prototyp-Umsetzung der Schalensicherheitsarchitektur als OSCI-HIS-Mediator zur Kopplung OSCI-gesicherter und QES-signierter elektr. Prüfungsdateneingaben wurde in eCampus entwickelt.

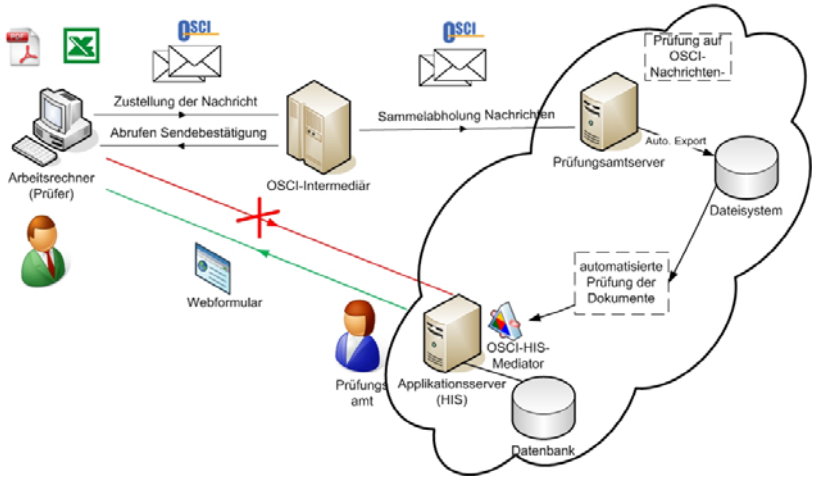

Abb.: 2: eExamReg Konzept-Zukünftiger Ablauf mit OSCI-HIS-Mediator

Die Prüfungsdaten werden mittels gesicherten OSCI-Transfer nach Sicherheits- und Signaturprüfungen unter Erzeugung signierter Quittungen und Logs automatisch vom Mediator über eine einzig noch geöffnete Web-Eingabeschnittstelle in das herkömmliche eCampus-System übergeben (z.B. HIS). Die Web-Abruf-Schnittstelle für das Lesen/Anzeigen von so eingetragenen Bewertungen bleibt unberührt. Prüfungsamtsmitarbeiter sind damit von allen Eingabetätigkeiten entlastet und prüfen nur noch Logs. Ausgehend von bestehenden SOA-Konzepten wird in eCampus ein Architekturvorschlag unter Integration weiterer Sicherheitsfunktionalität wie Web Service Security und OSCI 2.0 entwickelt, der als Grundlage für zukünftige Software-Infrastrukturen zur elektronischen Verwaltung von Hochschulen zu betrachten ist. Der Vorschlag wird als „*eCampus Reference SOA*“ bezeichnet, vgl. Brehm/Strack in [LDVK2010] und eröffnet weitere Integrationsmöglichkeiten bzgl. Funktionalität und Sicherheit auch für neuartige Campussysteme wie HISinOne.

5 Fazit

Auf Basis der entwickelten Konzepte, der Test- und Betriebserfahrung mit Komponenten werden Realisierungen und Integration bzgl. der einzelnen Fachverfahrenselektronisierungen mit gutem Erfolgspotential weiter verfolgt. Dabei ist u.a. unter Kosten-Nutzen-Gesichtspunkten die Wiederverwendung von OSCI- und Signatur-Komponenten nach Landespflegevertrag Governikus besonders attraktiv.

Literatur

[SENPRE2005] Pressestelle Senat Bremen: Datenschutzbeauftragte empfehlen Bremer Entwicklung bundesweit. http://www.senatspressestelle.bremen.de/detail.php?id=11601,

[eCaAn2009] Projektgruppe Strack, Richter: Antrag und Vorhabensbeschreibung „eCampus-Services & -Infrastrukturen“. Hs Harz, 2009

[LDVK2010] Projektgruppe Strack, Richter: LDVK-Bericht „eCampus-Services & -Infrastrukturen - für eine gesicherte & verbindliche elektron. Hochschulverwaltung“. Hs Harz, 2010

[SiStLSA2008] Strack, H.; Karich, Ch.; Werner, W.: Evaluation von Signaturanwendungs-und OSCI-Komponenten für standardisierten Einsatz LSA. Studie, Hs Harz, 2008

[StrEun2007] Strack, H., Karich Ch.: „A Distributed Architecture for the Management of Transcripts of Records and Student Mobility Data within the Bologna Process Framework“; in: Proceedings of EUNIS 2007 Conference, Universities of Grenoble and University P.M. Curie of Paris, France, 2007