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

eCollabSec – Plattform für elektronische Collaboration mit integrierter Sicherheit

Dipl.-Ing.(FH) Peter Kußmann, Phone: ++49.3943-659-364, Fax: ++49.3943-659-399, E-Mail: pkussmann@hs-harz.de, Hochschule Harz, Friedrichstr. 57-59, 38855 Wernigerode

Dipl.-Inf.(FH) Martin Henning, Phone: ++49.3943-659-341, Fax: ++49.3943-659-399, E-Mail: mhenning@hs-harz.de, Hochschule Harz, Friedrichstr. 57-59, 38855 Wernigerode

Prof. Dr. Hermann Strack, Phone: ++49.3943-659-341, Fax: ++49.3943-659-399, E-Mail: hstrack@hs-harz.de, Hochschule Harz, Friedrichstr. 57-59, 38855 Wernigerode

Abstract

Um elektronische Dokumente gemeinsam zwischen verschiedenen Partnern und Plattformen gesichert austauschen und bearbeiten zu können, wurde eine elektronische Collaboration-Plattform für domänenübergreifende und gesicherte elektronische Kooperationsformen von Hochschulen, Unternehmen und Verwaltungen entwickelt. Diese Plattform für hochschulübergreifende Kooperationen wurde im Auftrag des Kultusministerium des Landes Sachsen-Anhalt konzipiert und auf Basis von internationalen Webstandards (wie WebDAV) sowie von Groupware-, eGovernment- und Security-Basiskomponenten (wie OSCI, PKI LSA) umgesetzt.

Keywords: domänenübergreifende und gesicherte eCollaboration, Knowledgemanagement, WebDAV, Security, eGovernment-Standards, OSCI

1 Problem- und Anforderungsanalyse

Um einrichtungs- und netzdomänen-übergreifend elektronische Dokumente mit differenzierten Anforderungsprofilen insbesondere zu Collaborations- und Sicherheits-Aspekten austauschen und transparent bearbeiten zu können, soll zur Lösung eine elektronische Plattform zur entsprechenden Dienstekopplung unterschiedlicher Akteure im Bereich der hochschulübergreifenden Kooperation (s. unten) im Sinne eines Collaboration-, Dokumenten- und Knowledge-Managementsystems für das Kultusministerium Sachsen-Anhalt konzipiert und aufgebaut werden. Ein erster Anwendungsbereich ist hierbei eine landesweit verteilte Arbeitsgruppe zum Hochschulmarketing und entsprechend zugeordnete Verfahrensszenarien, bei dem das Kultusministerium Sachsen-Anhalt (MK LSA) als auch weitere externe Akteure wie die Hochschulen des Landes und das Wissenschaftszentrum Sachsen-Anhalt (WZW) entsprechende Dokumente gesichert austauschen sowie transparent bearbeiten können (ggf. parallel). Die abzubildenden Szenarien-Varianten zerfallen dabei in zwei Gruppen bzgl. der Kommunikations- und Collaboration-Anforderungen und Charakteristika:

A1) Informelle Collaboration-Szenarien mit sensitiver elektronischer Dokumentenbearbeitung und –übersendung unter vertrauenswürdigen Akteuren in geschlossenen Gruppen, ohne gruppen-internes Konkurrenz- bzw. Gefährdungspotential, dabei auch mit netzwerkdomänen-übergreifenden Nutzungen.

A2) Formelle Zustellungs-Szenarien für sensitive elektronische Dokumente/Prozesse mit Sicherheits-Ansprüchen und Zustellnachweis-Bedarfen auch in offenen oder erweiterbaren Gruppen, mit auch gruppen-internen Konkurrenz- bzw. Gefährdungspotentialen (Beispiel: offene Förderantragsverfahren und Förderbescheide).

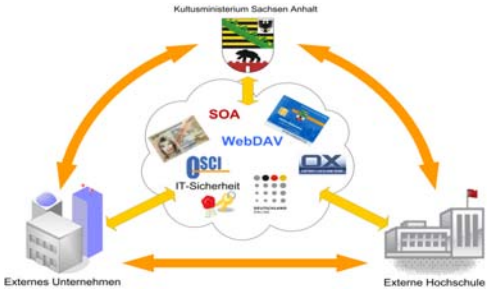

Abbildung 1: Akteure und -Dienstestruktur in eCollabSec

Für die Anforderungsspezifikation wurden Kernanforderungen für die Auswahl der Zielarchitektur und relevanter Bausteine in einer Anforderungsliste für die Szenarien-Varianten A1 und A2 zur domänenübergreifenden und gesicherten elektronischen Zusammenarbeit von Hochschulen und Einrichtungen festgehalten (siehe Tabelle 1).

Anf1:	Dokumentenintegrierte One-Click referenzierbare Hyperlinks auch zwischen Office-Dokumenten verschiedener Netzwerk- und Dateisystem-Domänen (alternativ zu proprietäten Office-Lösungen im Intranet)
Anf2:	Transparent gesichertes Groupware- u. Dokumentenmanagement in heterogenen Umgebungen mittels Standards
Anf3:	Gesicherte Zustellungen/Zustellnachweise: „Elektronisches Einschreiben mit Rückschein“
Anf4:	Elektronische Rechtsverbindlichkeit und Authentizität/Integrität: qualifizierte elektronische Signatur
Anf5:	Weitgehende Nutzung von internationalen Webstandards sowie von eGovernment- und Security-Basis-komponenten sowie von offenen Systemen (OpenSource).
Anf6:	Informelle Kollaboration und formale rechtverbindliche Verwaltungsverfahren auf einer integrierten ePlattform

Tabelle 1: eCollabSec-Anforderungen

Nach entsprechend kriterienorientierter Auswahl von Plattformen und Bausteinen für die Lösungsarchitektur, unter Einbindung von Tests und kriterien-orientierten Anpassungen, wurden Vorbereitungen für ein Roll-Out des Systems unter Einbindung entsprechender Dienstleister eingeplant und damit die Überführung in ein Produktivsystem, inklusive der Auswahl eines entsprechenden Betreibermodells.

2 Standards, Komponenten und Plattformen für Lösungen

Zur Umsetzung des Vorhabens wurde in Absprache mit dem Auftraggeber eine entsprechende Vorauswahl an Systemen und Bausteine getroffen. Die breite (integrierte) Wiederverwendung von Systemen und Bausteinen stand dabei im Vordergrund, evtl. ergänzende (Software-)Entwicklungen bzw. – Anpassungen wurden nur auf geringe Umfänge beschränkt. Die Auswahl konzentrierte sich vor dem Hintergrund der IT-Nutzungsprofile und –vorkenntnisse der Anwender auf folgende Arten bzw. Funktionsbereiche von Collaboration-Systemen bzw. deren Kombination: Groupware-Systeme für unternehmensübergreifende Zusammenarbeit, Dokumentenmanagement-Systeme oder Portal-Systeme.

Für eine effiziente, komponentenorientierte Umsetzung auf Basis von Standards stehen im Land Sachsen-Anhalt verschiedene eGovernment-Basiskomponenten und Sicherheitsinfrastrukturen zur Verwendung bereit, die für entsprechende Realisierungen und Integrationen zur Vollelektronisierung von Fachverfahren unter Aspekten von Rechtsverbindlichkeit, Datenschutz und IT-Sicherheit vorgesehen sind:

- Basiskomponente PKI-LSA inkl. Public-Key-Infrastruktur Sachsen-Anhalt (PKI LSA) insb. für fortgeschrittene und qualifizierte elektronische Signaturen
- Basiskomponente VPS/OSCI zur gesicherten, rechtsverbindlichen, nachweisbaren und datenschutzkonformen Zustellung von elektronischen Dokumenten und Daten auch durch ungesicherte Netzwerke (z.B. Internet).

- Weitere Sicherheitsinfrastrukturen wie Firewalls und Virtual Private Networks (VPN) im Landesverwaltungsnetz [Q4, Q5, Q6].

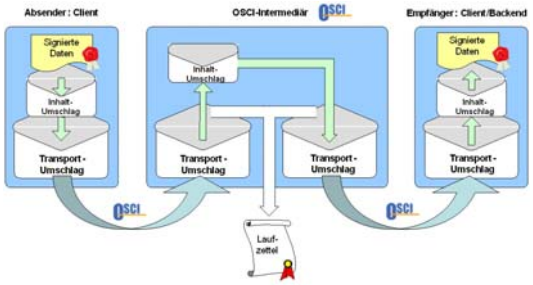

Abbildung 2: OSCI mit Zustellnachweisen (Laufzettel) und verschlüsselten Umschlägen (mit Ende-zu-Ende-Verschlüsselung für Inhaltsdaten)

3 Kriterien zur Lösungsauswahl und Realisierung

Für die Entwicklung und Realisierung einer integrierten Collaboration-Plattform sowohl für informelle Collaboration- als auch formelle Zustellungsszenarien auf Grundlage von Basissystemen und Komponenten wurde ein Kriterienkatalog zur Lösungsauswahl erstellt, siehe Tabelle 2.

3.1 Basissystem

Das Basissystem sollte die notwendigen Grundfunktionalität abbilden, um ausgewählte Aspekte des Dokumenten-, Content- und Knowledge-Management im Sinne insbesondere von informellen Collaboration-Szenarien umsetzen zu können.

Krit1:	Integrationsfähigkeit in heterogene Teilnetzwerke
Krit2:	Unterstützung von Benutzer- und Rollenmanagement
Krit3:	Integres Verhalten des Systems bei konkurrierenden Zugriffen
Krit4:	Unterstützung standard-basierter Benutzer- und Autor-schnittstellen (Web-Oberfläche und WebDAV für Dokumentenzugriff), Desktop-artiger virtueller Arbeitsplatz [Q11]
Krit5:	Verteilbarkeit der Architektur (Skalierbarkeit, Performance)
Krit6	Allgemeinere Sicherheitsanforderungen: transparent im Webbetrieb / softwarebasiert, Server- und Client-Authentisierung, Vertraulichkeit und Integrität für Kommunikation und Dokumente, Zugriffsschutz
Krit7:	Speziellere Sicherheitsanforderungen: rechtsverbindliche elektronische Dokumenten-Signaturen und nachweisbare Dokumentenzustellungen nach eGovernment-Standards für geschlossene (org-interne) und offene Nutzergruppen.
Krit8:	Optionale weitere Funktionen, wie z.B. automatisierte Aktualisierungsmeldungen mittels RSS-Feeds.

Tabelle 2: Kriterien des eCollabSec-Basissystems

3.2 Integrierte Collaboration-Plattform

Das integrierte Zielsystem sollte vor allem eGovernment-Basiskomponenten integrieren, um auch für erweiterte Anwendungsbereiche insb. für Szenarien mit Anforderungen an gesicherte und rechtsverbindliche Verfahrenselektronisierungen auf OSCI-Basis einsetzbar zu sein. Die resultierende Anforderungsspezifikation bildete die Grundlage für die in AP2 (Analyse existierender Standards/Systeme) durchgeführte Auswahl von einzusetzenden Komponenten und das Design der ausgewählten Architektur, auf deren Basis dann ein Systemprototyp umgesetzt wurde (Basissystem-Weiterentwicklung durch zyklisches Rapid Prototyping mit Nutzertests/Feedback).

4 Realisierung

Ausgehend von den Anforderungen und Kriterien für die eCollabSec-Plattform (siehe Tabelle 2) wurden mehrere Basissysteme untersucht (z.B. OpenExchange, OpenGroupware, Typo 3, BSCW, etc.) und resultierend der „Open-Xchange-Server 6“ für

die Realisierung ausgewählt, wobei folgende Systemeigenschaften von besonderer Relevanz waren [Q10]:

- WebDAV-Schnittstellen für Distributed Digital Authoring
- OneClick-Feature für Office-Dokument-eingebettete Hyperlinks
- integrierte automatisierte Versionierung für Dokumente
- vielfältige Schnittstellen/Konnektoren (z.B. für Outlook) + mobile connectivity
- kommerzielle Support- und Pflegeleistungen.

Bei ersten Funktionstests wurde eine Reihe von Fehlfunktionen identifiziert. Für weitere Diagnosen wurde die Durchführung von Zugriffen mittels Netzwerkscannern aufgezeichnet und mit XML-Tools auf Standard-Konformität analysiert. Hierbei wurden die Fehlerursache identifiziert, diese mit Lösungsvorschlägen an den Hersteller zur Behebung übermittelt. Beispielhaft seien hier folgende Fehler genannt:

- no_browser_webdavdirectorylisting,
- no_pdf_doubbleklick_in_webdav,
- no_direct_document_open_over_webdav,
- big_file_upload_error.

Für die gesicherte Integration des „Open-Xchange-Server 6“ inkl. WebDAV-Schnittstellen als Basissystem wurde ein Sicherheitskonzept entwickelt und umgesetzt, u.a. mit Konfiguration von SSL/TLS für Client+Server-Authentifikation, so dass ein verschlüsselter Zugriff nur mit entsprechenden Client-Zertifikaten möglich ist (CA der DOI [Q3]). Für die integrierte Collaboration-Plattform wurde ergänzend die Zustellungsfunktionalität mittels OSCI-Basiskomponenten [Q1] in einem Zugangsportal eingebunden.

5 Fazit

Die wichtigen Teilszenarien für informelle (Authoring) und formelle elektronischer Collaboration (Zustellung) konnten in einer integrierten Collaboration-Plattform auf Basis von Internet- und eGovernment-Standards umgesetzt werden. Erste Anwendungstests waren erfolgreich. Die stufenweise Überführung vom Test- in den Echt-Betrieb wird unter Auswahl und Umsetzung eines geeigneten Betreibermodells vorbereitet.

Literatur:

[Q1] Strack, H.; Karich, Ch.; Werner, H.: Evaluation von Signaturanwendungs- und OSCI-Komponenten für den standardisierten Einsatz im Land Sachsen-Anhalt (öff. Teil), für MI LSA Ref. 45, Hs-Harz, Wernigerode, 2008

[Q2] Hannemann, Kirbs, LIZ: PKI Sachsen-Anhalt Teilnehmerhandbuch, Halle/Saale, 2009

[Q3] DOI-Netz e.V. Deutschland-Online Infrastruktur: Teilprojekt PKI - Certificate Policy (CP) / Certification Practice-Statement (CPS) - DOI-CA [DOI101], 2010

[Q4] Ministerium des Inneren – Sachsen-Anhalt (ed.): RderL. des MI - *PKI-LSA* 45.23-02840-01, Magdeburg, 2006

[Q5] Arbeitskreis eGovernment von der Konferenz der Datenschutzbauftragten des Bundes und der Länder (ed.): DS in DMS - Datenschutz bei Dokumentenmanagementsystemen, Magdeburg, 2006

[Q6] Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (ed.): DSDS in Projekten -Datenschutz und Datensicherheit in Projekten - Projekt- und Produktivbetrieb, 2009

[Q7] Ministerium der Justiz des Landes Sachsen-Anhalt (ed.): VV-DSG-LSA -Verwaltungsvorschriften zum Gesetz zum Schutz personenbezogener Daten der Bürger, Magdeburg, 2009

[Q8] Bundesministerium der Justiz (ed.): SigG – Signaturgesetz , 2001

[Q9] Bundesministerium der Justiz (ed.): SigV – *Signaturverordnung, 2001*

[Q10] Open Xchange Server benutzerhandbuch, Open-Xchange Inc., 2009

[Q11] Webdav - Web-based Distributed Authoring and Versioning – RFC 2518,