Zugang und Zutritt zum IKA

Das Informations- und Kommunikationszentrum in Adlershof (IKA), das neben weiteren öffentlichen Bereichen auch die Dienstleistungen der Mathematisch-Naturwissenschaftlichen Zweigbibliothek der Universitätsbibliothek und des Rechenzentrums gemeinsam unter einem Dach anbietet, eröffnet auch ganz neue Möglichkeiten und Notwendigkeiten der Zugangs- und Zutrittssteuerung. Dieser Artikel beschreibt den Problemkreis und einige derzeit in Entwicklung befindliche Ansätze der Realisierung.

Der Umzug der sieben Mathematisch-Naturwissenschaftlichen Institute von ihren traditionellen Standorten in Berlin-Mitte auf den für die Humboldt-Universität neuen Campus in Adlershof ist bereits in vollem Gange. Die ersten Institute haben ihre Arbeit an neuer Stelle aufgenommen (Informatik, Mathematik, Chemie), weitere Institute (Physik, Psychologie) befinden sich in den Startlöchern.

Auch das Rechenzentrum wird seinen neuen Hauptstandort in Adlershof aufschlagen. Dabei wurde in der Planung von Anfang an das Ziel verfolgt, mehrere Serviceeinrichtungen der Universität, wie die Mathematisch-Naturwissenschaftliche Bibliothek, das Rechenzentrum und das Multimediazentrum, räumlich zu konzentrieren und technologisch aufeinander abzustimmen. Das Ergebnis ist das Konzept des Informations- und Kommunikationszentrums Adlershof (IKA) als zentrale Einrichtung für Information und Kommunikation. Das IKA wird den gesamten Wissenschafts- und Wirtschaftsstandort mit allen Dienstleistungen einer multimedialen wissenschaftlichen Bibliothek, eines Rechenzentrums, des Technologietransfers sowie den Diensten von Fachinformationszentren und -verlagen versorgen. Weiterhin werden in diesem Gebäude Konferenzräume und ein Hörsaalkomplex sowie weitere öffentlich nutzbare Dienstleistungsbereiche installiert.

Technologische Aspekte

Diese Angebotsbreite stellt natürlich auch besondere Anforderungen an die Technologie des Betriebes. Dem Kunden des IKA soll bei einem möglichst geringen notwendigen Verwaltungsaufwand während der Anmeldung und Nutzung von Diensten die breite ihm zugeordnete Angebotspalette zur Verfügung stehen. Dem Benutzer ist es letztendlich egal, welche Service-Einrichtung ihm den beantragten Dienst anbietet.

Für den Anbieter müssen der Betrieb und die Kundenverwaltung technologisch beherrschbar bleiben. Neben den Vorstellungen einer größtmöglichen Freizügigkeit für den Kunden sind natürlich auch einschränkende Aspekte zu berücksichtigen. Grundsätzlich muss aber das Angebot an Dienstleistungen am Bedarf der Benutzer ausgerichtet werden. Einschränkungen sollten nur aus technologischen, kapazitätstechnischen, sicherheitstechnischen oder rechtlichen Gründen erfolgen.

Um welche Dienstleistungen geht es hierbei? Seitens der Universitätsbibliothek sind es natürlich klassischerweise Angebote wie Buchausleihe, Lesesaaldienste, Katalogrecherchen, Vorbestellungen von Büchern usw. Darüber hinaus bietet die Bibliothek auch Dienste wie Beschaffung und Bearbeitung von Dokumenten, elektronische Informationsangebote, Zugriff auf den CD-ROM-Service und auf ausgewählte Datenbanken und natürlich die Nutzung von mit dem Internet verbundenen Öffentlichen Computerarbeitsplätzen (ÖCAP) an. Das Rechenzentrum stellt Dienste wie den klassischen PC-Saal, Kommunikations- und Internetdienste, den File-, Compute-, Datenbank-, Print- und Scanservice und den Hard- und Softwareservice zur öffentlichen

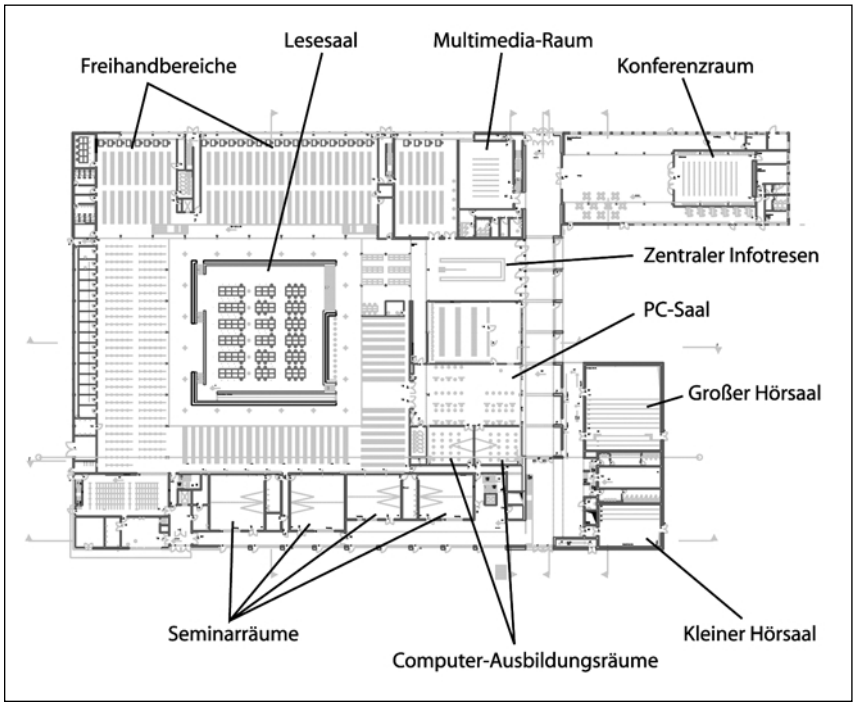

Abb. 1: Erdgeschoss – Öffentliche Arbeitsplätze

Nutzung bereit. Zu den Diensten des Multimediazentrums gehören in diesem Zusammenhang Print- und Scandienste, Video- und Fotoarbeiten, Bereitstellung interaktiver Anwendungen, Videokonferenzdienste u. v. m.

Aus Sicht der Technologie sind hierbei mehrere Aspekte zu berücksichtigen. Da ist als erstes die Unterscheidung von Zugang und Zutritt: Die Zugangskontrolle beinhaltet alle technischen und organisatorischen Maßnahmen zur Steuerung und Abrechnung der Benutzung von Diensten („Zugang zu IuK-Technik-basierten Diensten"). Dagegen umfasst die Zutrittskontrolle entsprechende Maßnahmen zur Steuerung sicherheitstechnischer Anlagen („Zutritt zu Räumen/Zonen/Boxen").

Aus Sicht der Arbeitsabläufe sind das Auftragshandling (Anmeldung, Modifikation und Stornierung), der Zugang zu den Diensten und der Betrieb einer Public Key Infrastructure (PKI) zu unterscheiden. Das Auftragshandling erfolgt mit einheitlicher Schnittstelle für alle angebotenen Dienstleistungen des IKA. Dem Kunden werden auf der Basis seiner institutionellen Herkunft eine Einrichtungsklasse und auf der Basis seines Status eine Benutzerklasse zugeordnet. Im Rahmen seines so definierten Berechtigungsraumes kann er die Nutzung von Dienstleistungen der Bibliothek und des Rechen- und Medienzentrums in Auftrag geben. Der Zugang für einen Großteil der Dienste erfolgt über entsprechend bereitgestellte ÖCAP. Auf der Basis der Authentisierung und damit seines Profils erhält der Benutzer entsprechende Berechtigungen. Die PKI stellt die grundlegenden Sicherheitsfunktionen für eine authentisierte und verschlüsselte Kommunikation in Netzwerken zur Verfügung. Diese Sicherheitsfunktionen sind allgemein die Vertraulichkeit, Authentizität und Integrität von Daten sowie der Aufbau einer gesicherten Verbindung. Eine PKI ist die Kombination aus Hard- und Softwareprodukten, Richtlinien und Prozeduren.

Der Zugang zu den Diensten erfolgt über die Authentisierung des Benutzers. Diese bildet neben der Berechtigungsprüfung die Grundlage für Verschlüsselungen, Signierungen, Abrechnungen oder Studienverwaltungsprozesse.

Und schließlich die Sicherheit: In diesem Zusammenhang sind folgende Aspekte zu berücksichtigen:

- Schutz der Installationen
- Beschränkungen aus rechtlichen Gründen (Lizenzschutz, Missbrauch usw.)
- Datenschutz in den Verwaltungsprozessen
- Schutz vor Diebstahl, Vandalismus und Zerstörung
- Individuelle Risiken für den Benutzer wie der Schutz seiner Daten und der Kommunikation

Realisierungsvorstellungen

Natürlich laufen die oben beschriebenen technologischen Vorstellungen auf die Einführung der Chipkarte hinaus: Die SmartCard mit Zertifikat als technische Basis für die Authentisierung zur Steuerung technologischer Arbeitsabläufe.

Bei der Definition des Kartendesigns gehen wir aus logischer Sicht von zwei unterschiedlichen Typen aus:

- SmartCard mit einem kontaktbehafteten Mikroprozessor mit Krypto-Coprozessor (Krypto-Chip)
- SmartCard mit einem kontaktlosen Mikroprozessor (Mifare-Chip)

Durch Verwendung einer Hybridkarte, die beide Prozessortypen auf einem gemeinsamen Kartenkörper vereinigt, hält der Benutzer physisch nur eine Karte in der Hand.

Der Krypto-Chip steuert den Zugang zu den Diensten des IKA. Die Authentisierung des Benutzers erfolgt zertifikatsbasiert, d. h. auf dem kontaktbehafteten Chip werden (mindestens) das Zertifikat sowie der private Schlüssel abgelegt. Der Mifare-Chip dient grundsätzlich zur Zutrittssteuerung. Die Authentisierung erfolgt über entsprechende Ident-Nummern auf dem kontaktlosen Prozessor (somit aus Sicherheitsgründen auch physisch getrennt vom Zertifikat).

Grundsätzlich werden auf der Chipkarte nur die zur Authentisierung notwendigen Daten abgelegt. Die Steuerung der Benutzerprofile erfolgt über entsprechende Hintergrundsysteme, die bei der Anmeldung bzw. der Authentisierung aktiviert werden. Es besteht somit keine Notwendigkeit, dass die SmartCard über

Abb. 2: Modell des IKA

das Zertifikat hinausgehende persönliche Daten wie Anschrift, Geburtsdatum oder Studiengang enthält.

Die entsprechenden Verwaltungsdatenbanken in den Hintergrundsystemen werden durch eine zentrale Benutzerdatenbank (Meta-Directory) gesteuert. Über diese erfolgen die Verwaltungsvorgänge wie Benutzeranmeldung, Zertifikatsvergabe, Definition des Benutzerprofils usw. Für das Teilsystem (Anwendung mit eigener Benutzerverwaltung) spezifische Daten werden an dieses weitergeleitet und ausschließlich dort abgelegt. Die Anmeldung des Benutzers zu einem Dienst erfolgt dann direkt im Teilsystem.

In der ersten Realisierungsstufe ist die Integration der Teilsysteme Zugang zu ÖCAP, Zugang zum Bibliotheksverwaltungssystem und Zutritt geplant.

Zugang zu ÖCAP: Dieser erfolgt notwendigerweise zertifikatbasiert. Der Benutzer meldet sich am ÖCAP an und erhält eine entsprechende Freischaltung von Diensten. Zu diesen gehören die allgemeinen IuK-Dienste an Computern und in lokalen Netzen (z. B. Software, Hardware, Plattformen, Speicherplatz, Peripherie), Bibliotheksdienste (Buch- und Zeitschriftenbestellung, Online-Recherchen, Zugang zu CD-ROM- und Dokumenten-Servern), Kommunikations-, Internet- und Mediendienste.

Zugang zum Bibliotheksverwaltungssystem: Dieser setzt eine Anpassung des Systems an die zertifikatbasierte Authentisierung per SmartCard voraus. Auf dieser Basis werden Dienste bereitgestellt wie Buchausleihe, aktive Nutzung der Online-Kataloge, Bezahlungen usw. Aus Gründen der Kompatibilität zu anderen Bibliotheken sowie der Möglichkeit des Fernzugangs (vom Campus in Mitte, von zu Hause) muss in der ersten Realisierung der notwendig zertifikatsbasierte Zugang dahingehend aufgeweicht werden, dass eine Authentisierung auch über eine Benutzernummer mit Kennwort und/oder über einen Barcode erfolgen kann.

Zutritt: Die Zutrittskontrollfunktion wird auf alle neu errichteten Gebäude in Adlershof ausgedehnt. Die Steuerung erfolgt über einen gemeinsamen Steuerungs-Server mit der Möglichkeit einer dezentralen Administration. Die Übertragung der Steuerungsfunktionen erfolgt verschlüsselt über das IP-Netz. Das Zutrittskontrollsystem ist zu der (zu errichtenden) Einbruchsmeldeanlage (EMA) kompatibel. Über die SmartCard besteht die Möglichkeit, die EMA VdS-zertifiziert scharf und unscharf schalten zu können.

Schlussbemerkungen

An den Hochschulen und Universitäten in Deutschland gibt es viele Realisierungsansätze zur Einführung von Chipkarten. Die Humboldt-Universität steht in einem intensiven Erfahrungsaustausch und ist interessiert an einer engen Zusammenarbeit mit anderen Einrichtungen. Die Spezifik der HU-Konzeption besteht insbesondere darin, mit der Einführung einer Zugangs- und Zutrittstechnologie die SmartCard als Basis für die Authentisierung einzuführen. Andere Anwendungen, wie beispielsweise die Automatisierung von Hochschul- und Studierenden-Verwaltungsprozessen, stehen vorerst nicht im Vordergrund, sind aber bei einer zukünftigen Erweiterung nicht ausgeschlossen. Anlass ist die Inbetriebnahme des IKA, wobei wir uns auf Grund der besonderen Voraussetzungen (Neubau, Planung auf der „grünen Wiese“, definierter Benutzerkreis) Realisierungschancen ausrechnen.

Lutz Stange
stange@rz.hu-berlin.de

So war es zu lesen in den RZ-Mitteilungen Heft Nr. 15/1997

Wir müssen jedoch immer wieder feststellen, wie erschreckend groß die Defizite im Sicherheitsbewußtsein vieler Benutzer sind, wie unbekümmert Paßwörter an andere weitergegeben werden (Teilweise werden sie sogar per E-Mail verschickt!) und wie wenig Klarheit darüber herrscht, welche Folgen ein derart leichtfertiger Umgang mit dem eigenen Account haben kann.