RUB

RUHR-UNIVERSITÄT BOCHUM

Großgeräteantrag 2013

NFC- Studierendenausweis

Dezernat 6 - Informations- und Kommunikationsdienste
Abteilung 3 - IT-Systeme, Software-Integration

Inhaltsverzeichnis

Antrag
NFC-Studierendenausweis

mobil & sicher

1 Überblick

Antragstellende Hochschule:	Ruhr-Universität Bochum
Ansprechpartner:	Marcus Klein, Haiko te Neues, Martina Rothacker
Zusammenfassung:	Evaluierung der NFC-Technologie für Studierendenausweise und deren Nutzung mit mobilen Geräten
Durchführungszeitraum endet:	28.02.2014
Bewilligungszeitraum endet:	31.12.2013

2 Motivation

Bereits im Jahre 1997 wurde an der Ruhr-Universität Bochum eine multifunktionale Karte mit Kryptochip für Studierende eingeführt. Ziel dabei war es, eine Infrastruktur zu schaffen, die es im Sinne eines virtuellen Studierendensekretariates ermöglicht, Verwaltungsprozesse in Selbstbedienung durchzuführen und somit den Komfort für Studierende zu erhöhen. Im Fokus stand dabei die Möglichkeit einer sicheren Zwei-Faktor-Authentifizierung mittels Kryptochip. Diese neue Funktionalität wurde genutzt, um sich sicher an einem zentralen Portal anzumelden, in dem verschiedene Dienstleistungen in Selbstbedienung zur Verfügung gestellt wurden. Dazu gehörten zum Beispiel der Druck der Studierendenbescheinigung oder die Änderung der eigenen Adresse.

Mit der Inbetriebnahme eines neuen Campusmanagement-Systems im Jahre 2005 kam erstmals die elektronische Signatur im größeren Stil zum Einsatz. In diesem neuen System mussten viele Aktionen im Rahmen der Verwaltung von Studien- und Prüfungsleistungen von den Studierenden elektronisch signiert werden, damit sie ausgeführt wurden. Dies sollte die Urheberschaft belegen, die Integrität gewährleisten und somit die Verwendung von Papier überflüssig machen.

Ein weiterer Meilenstein wurde zur Einschreibung zum Wintersemester 2009 erreicht. Das bisher eigene proprietäre technische Layout des Kryptochips wurde durch den

PKCS#15-Standard ersetzt. Weiterhin wurde die im Hause betriebene PKI zum DFN-Verein verlagert.

Die Vorteile einer standardkonformen Karte mit Zertifikaten vom DFN-Verein zur Authentifizierung und elektronischen Signatur liegen auf der Hand. Allerdings ist das größte Problem dieses technischen Systems seine Komplexität. Den Nutzern diese Komplexität näher zu bringen, ist sehr schwierig und in den meisten Fällen erfolglos. Als Ende 2012 die ersten Zertifikate nach drei Jahren ausliefen und erneuert werden mussten, stieg der Supportaufwand trotz „einfacher" Selbstbedienungsmechanismen rapide an. Parallel dazu fiel die Notwendigkeit der elektronischen Signatur von Vorgängen im Campusmanagement-System aufgrund einer neuen rechtlichen Einordnung gänzlich weg.

Somit dient die Studierendenkarte der Ruhr-Universität heute ausschließlich als sicheres und sehr viel genutztes Medium zur Zwei-Faktor-Authentifizierung. Die elektronische Signatur kommt auf Seiten der Studierenden nicht mehr zum Einsatz und auch zukünftige Anwendungsfälle sind nicht erkennbar.

3 Ziel

Studierende sollen ihre gewohnten elektronischen Dienstleistungen der Universität mit ihrem Smartphone nutzen können. Damit der mobile Zugriff sicher ist, soll die Authentifizierung mit dem Studierendenausweis erfolgen.

Der derzeitige Ausweis ist dazu aufgrund seines kontaktbehafteten Kryptochips nicht geeignet. Eine sichere Zwei-Faktor-Authentifizierung ist auch ohne teure Kryptochips möglich. Nearfield Communication (NFC) bildet dabei das Bindeglied zwischen einer sicheren Authentifizierung mittels Studierendenausweis und den mobilen Geräten. Zunehmend viele Smartphones können standardmäßig mit NFC-Karten kommunizieren. Eine elektronische Signatur ist mit dieser Technologie nicht möglich, wird aber auch nicht benötigt.

Die Gesamtkosten NFC-basierter Studierendenausweise sind aufgrund der wegfallenden Komplexität einer PKI und der geringeren Materialkosten signifikant niedriger als die zertifikatsbasierter Kryptokarten bei vergleichbarem Nutzen.

Darüber hinaus bietet eine entsprechend konfektionierte NFC-Karte die Möglichkeit, beliebig komplexe Berechtigungsszenarien im universitären Umfeld abzubilden.

Das hier beantragte Vorhaben soll ein Leuchtturmprojekt für andere Hochschulen darstellen. Die Ergebnisse dieses Projekts werden so ausgelegt sein, dass sie von anderen Hochschulen leicht an ihre lokalen Gegebenheiten angepasst werden können.

4 NFC Technologie

Nearfield Communication (NFC) ist ein internationaler Standard. Er beschreibt die Datenübertragung mittels der Funktechnologie *„Radio-Frequency Identification“* (RFID) zwischen Geräten bis zu einer Distanz von 10 cm und einer Datenrate von 424 kBit/s. Die Einsatzszenarien reichen dabei neben reiner Datenübertragung von Micropayment (bargeldloses Bezahlen von Kleinbeträgen) über Zutrittsberechtigungen bis zu Authentifizierungsvorgängen.

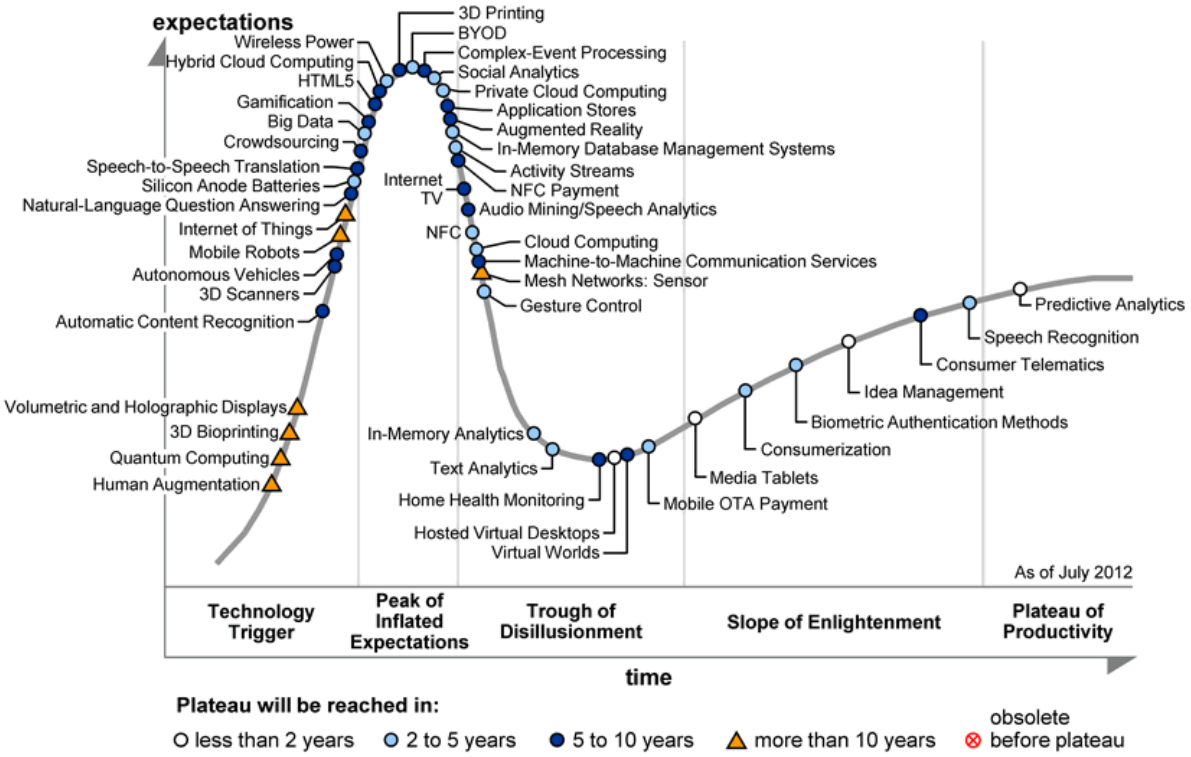

Abbildung 1: 2012 Gartner Hype Cycle for Emerging Technologies Special Report
(Quelle: http://www.nfcworld.com/2012/08/16/317281/gartner-places-nfc-in-trough-of-disillusionment/)

NFC ist derzeit ein Trendthema. Der Gartner Report des Jahres 2012 sieht eine Marktdurchdringung der allgemeinen NFC Technologie in ca. zwei bis fünf Jahren. Man kann also davon ausgehen, dass zunehmend viele (nicht nur mobile) Geräte mit dieser Technologie ausgestattet werden. Die Vorteile dieser Technologie greift die Ruhr-Universität auf, um Ressourcen einzusparen und trotzdem das Serviceangebot für die Studierenden zu steigern.

5 Projekt

Das Ergebnis dieses Projektes soll es ermöglichen, dass ein Studierender sich mit dem NFC-Studierendenausweis sicher an seinem mobilen Gerät an den gewohnten Diensten anmelden kann. Dieser Use Case „sichere Authentifizierung“ steht im Fokus der Betrachtung und soll prototypisch umgesetzt werden.

In der Konzeptphase wird aber sehr wohl ein weit universellerer Ansatz verfolgt. Dort werden weitere Use Cases berücksichtigt. Ebenso sollen alle Dienste, die derzeit vom „normalen“ PC aus mit dem zertifikatsbasierten Kryptochip-Ausweis erreichbar sind, mit dem NFC-Studierendenausweis erreichbar sein. Diese Szenarien sollen aber nicht in diesem Projekt umgesetzt werden.

Use Case „sichere Authentifizierung“
Studierende starten auf ihrem mobilen, NFC-fähigen Gerät die Authentifizierungs-App, halten ihren NFC-Studierendenausweis an das Smartphone, geben die PIN ein und sind dann im personalisierten Portal oder einer entsprechenden Webanwendung angemeldet.

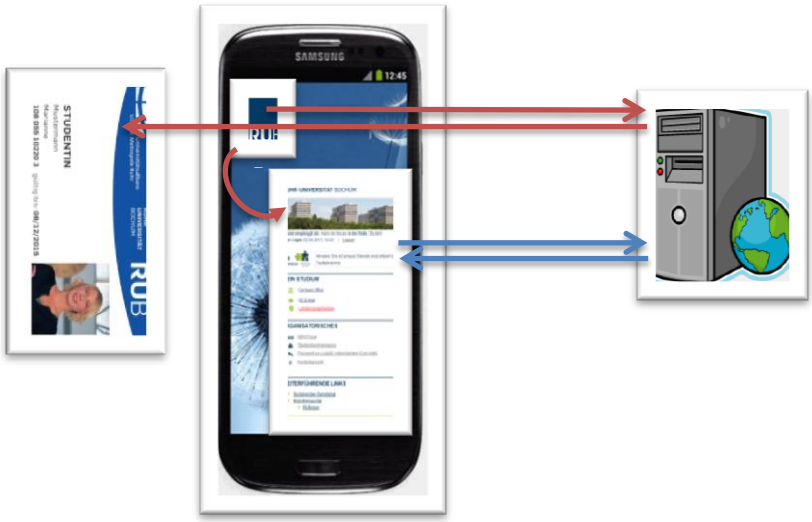

Abbildung 2: Use Case Authentifizierung

Die Umsetzung gliedert sich in eine vorangestellte Konzeptionsphase und drei anschließende, parallele Implementierungsphasen. Es muss eine *NFC-Karte* konfektioniert, eine *App* und ein passendes *Backend System (Access Management)* entwickelt werden.

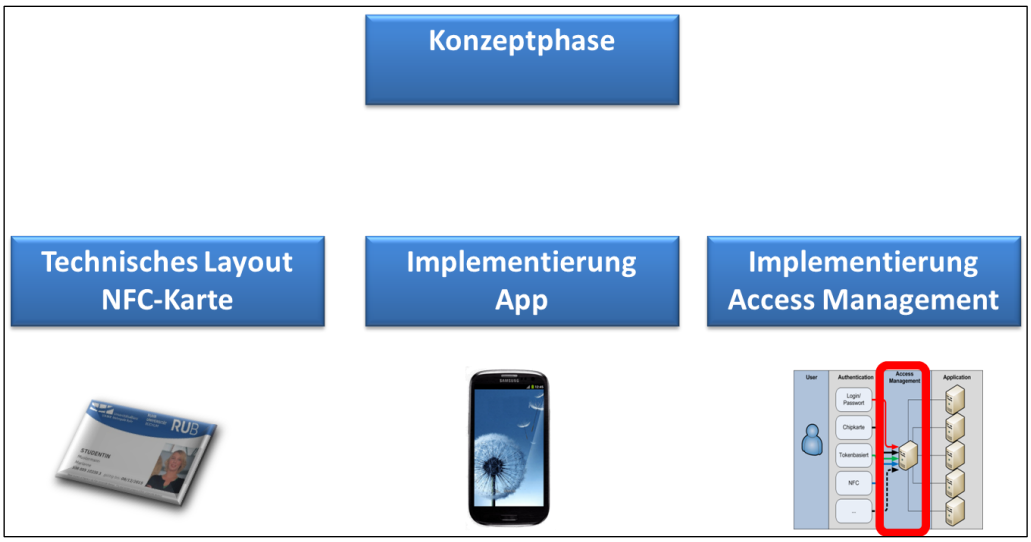

Abbildung 3: Phasen der Umsetzung

5.1 Konzeptphase

Es soll ein universelles Konzept erarbeitet werden, das es möglichst vielen Betreibern erlaubt, mit ihren Use Cases unabhängig voneinander die Karte zu nutzen, ohne dass dabei unüberwindbare Abhängigkeiten entstehen. Folgende Use Cases sind derzeit im universitären Umfeld denkbar:

- Sichere Authentifizierung gegenüber elektronischen Diensten, insbesondere auch von mobilen Geräten aus
- Parkraumbewirtschaftung
- Zutrittsberechtigung
- Zahlfunktion
- Drucken/Kopieren/Scannen
- Ausleihe Bibliothek

Jeder Use Case kann zu einer eigenständigen Applikation auf der Karte samt seinem (bestehenden) Backend System führen. Die Eigenständigkeit der Applikation wird auf der Karte durch Verwendung eigener kryptografischer Schlüssel realisiert. Nur der Inhaber dieser Schlüssel, also der Betreiber des Use Cases, kann festlegen, welche Daten in „seiner“ Applikation auf der Karte gelesen und geschrieben werden können.

Das Management der kryptografischen Schlüssel ist dabei von besonderer Bedeutung, hat es doch massive Auswirkungen auf den kompletten Kartenlifecycle in Bezug auf:

- Initialisierung
- Personalisierung
- Ausgabe
- Nutzung
- Sperren und Freigeben
- Defekt und Umtausch.

Bei der Erarbeitung eines geeigneten Schlüsselmanagements nehmen Sicherheit und Datenschutz eine zentrale Rolle ein. Die Daten, die in den Applikationen gespeichert und verarbeitet werden, müssen den jeweiligen Anforderungen entsprechen. Deswegen wird ein spezielles Sicherheitskonzept erarbeitet, das beispielsweise Maßnahmen beinhaltet, die verhindern, dass nicht gewünschte wechselseitige Auswirkungen zwischen den Applikationen möglich sind. Diese Maßnahmen sollen prototypisch in dem Use Case „Sichere Authentifizierung“ umgesetzt werden. Das Sicherheitskonzept wird in Verbindung mit externen Beratern entwickelt und soll so ausgelegt sein, dass es als Basis für ein nachgelagertes Audit genutzt werden kann.

5.2 Technisches Layout der NFC-Karte

Auf Basis der in der Konzeptphase erarbeiteten Ergebnisse soll das technische Layout der Karte bestimmt und prototypisch umgesetzt werden.

5.3 Implementierung der Authentifizierungs-App

Die App soll die Kommunikation zwischen dem Backend System und der Karte ermöglichen. Da das Know How zur Entwicklung von Apps für mobile Geräte mit den unten aufgeführten Anforderungen nicht an der Hochschule vorhanden ist, wird angestrebt, das requirements engineering mit Hilfe externer Dienstleister durchzuführen. Die Entwicklung soll komplett vergeben werden.

Funktionsablauf der App

Der Ablauf ist dabei so, dass nach Start der App die Karte an das Gerät gehalten werden muss. Danach soll durch kryptografische Verfahren zwischen App, Karte und Backend System die sichere Authentifizierung erfolgen. Dabei wird dann im Erfolgsfall serverseitig ein URL mit Sessionid erstellt und an die App übergeben. Mit diesem Wertepaar ruft die App dann den auf dem Gerät installierten Browser auf. Somit ist der Nutzer in seiner Webanwendung *sicher* angemeldet.

Abbildung 4: PIN-Eingabe an der App

Anforderungen an die App

Neben den funktionellen Anforderungen gibt es weitere Bedingungen, die erfüllt werden sollen. Die App soll prototypisch für Android Geräte implementiert werden. Perspektivisch dürfen aber weitere marktrelevante mobile Betriebssysteme, wie Windows 8 und iOS, nicht ausgeklammert werden. Derzeit wird auf Mifare DESFire Technologie im Kartenbereich gesetzt. Weitere RFID-Kartensysteme müssen ebenso bedacht werden.

Nach Ablauf der Programmiertätigkeit muss der Sourcecode der Hochschule gut dokumentiert zur Verfügung gestellt werden. So soll eine Weiterentwicklung im Haus, durch andere Hochschulen oder Dienstleister gewährleistet werden.

5.4 Implementierung des Access Managements

Damit bestehende Webanwendungen für den beschriebenen Use Case genutzt werden können, ist es sinnvoll, ein Access Management (AM) einzusetzen. Ansonsten müsste jede Webanwendung gesondert eine Schnittstelle zur App realisieren. Sinnvoller und effizienter ist deswegen die einmalige Implementierung eines speziellen NFC-Moduls für das Access Management. Die angeschlossenen Webanwendungen kommunizieren über standardisierte Protokolle (SAML).

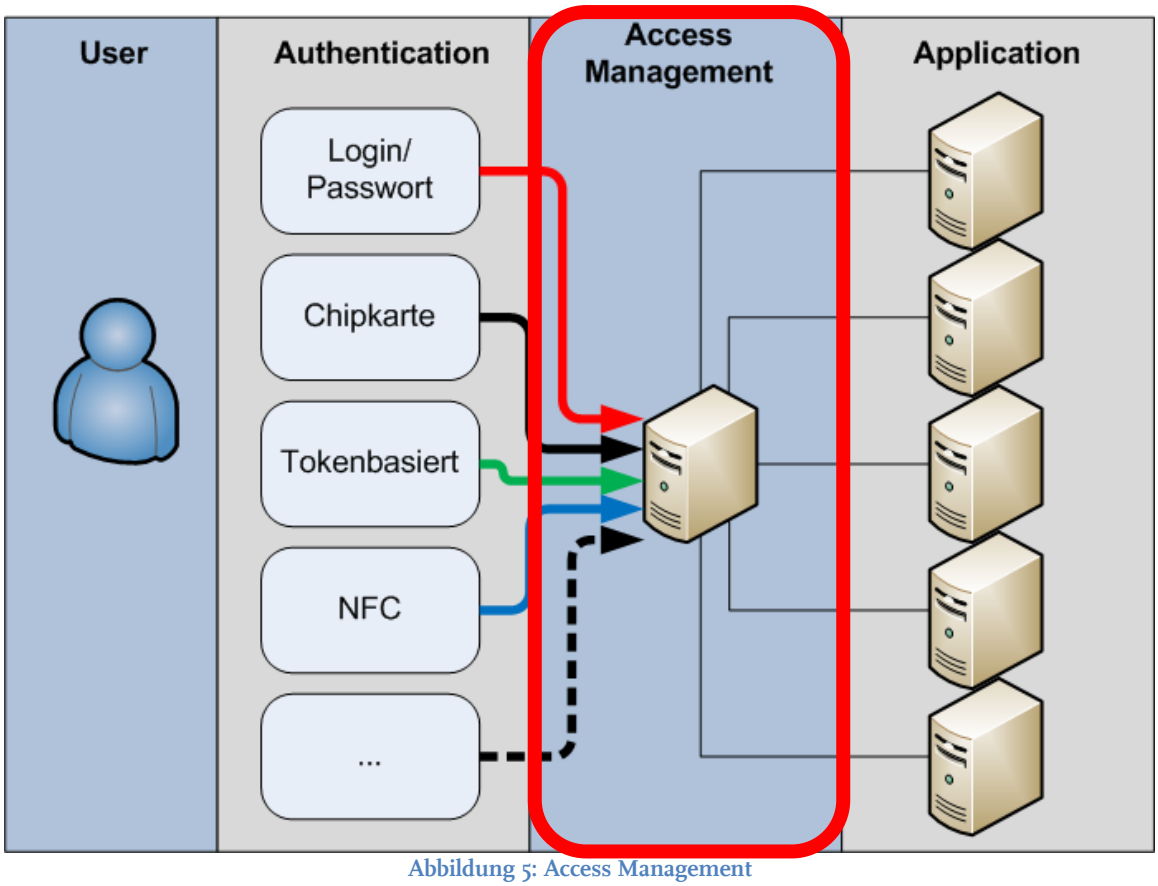

Abbildung 5: Access Management

Ein weiterer Vorteil eines solchen Access Managements ist, dass beliebig viele weitere Authentifizierungsverfahren eingebunden werden können.

OpenAM NFC-Auth Modul

Die Ruhr-Universität hat zu diesem Zwecke das Opensource Produkt OpenAM evaluiert und eingeführt. Im Rahmen dieses Projektes soll dafür ein Modul entwickelt und implementiert werden, das die Kommunikation mit der Karte bzw. der App realisiert.

Das Modul realisiert die kryptografischen Verfahren der Authentifizierung. Nach erfolgreicher Anmeldung veranlasst es dann die Generierung einer Sessionid im Access Management. Jede angebundene Webanwendung kann beim Access Management die ihm übergebene Sessionid verifizieren lassen.

Das Access Management ist via LDAP mit dem Identity Management verbunden. Somit kann das Authentifizieren bzw. Autorisieren mit weiteren Attributen verknüpft werden.

Um im Rahmen dieses Projektes zeitnah ein NFC Modul zu entwickeln, das zudem weiter- und wiederverwendbar ist, sollen externe Dienstleistern hinzu gezogen werden.

6 Die Ruhr-Universität Bochum

Die Ruhr-Universität Bochum gehört mit fast 39.000 Studierenden im Wintersemester 2012/2013 zu den zehn größten Universitäten Deutschlands. Ebenso gehört sie zu den forschungsstärksten Universitäten der Republik. Sie befand sich sowohl in 2007 als auch in 2011 in der Endrunde der vom Bund geführten Exzellenzinitiative und konnte sich jeweils in zwei von drei Förderlinien durchsetzen.

Fast alle Studiengänge werden als Bachelor-Master-Programme angeboten. Die Exzellenzprogramme haben sich international einen Namen gemacht: Die Research School ist ein internationales Kolleg zur strukturierten Forschungspromotion in den Lebenswissenschaften, den Natur- und Ingenieurwissenschaften und den Geistes- und Gesellschaftswissenschaften. Untereinander, national und international stark vernetzte, fakultäts- und fachübergreifende Forscherverbünde (Research Departments) schärfen das Profil der RUB, hinzu kommen ein unübertroffenes Programm zur Förderung von Nachwuchswissenschaftlerinnen und -wissenschaftlern und eine hervorragende Infrastruktur.

Personen im Wintersemester 2012/2013		
Studierende		38.675
	Geistes- und Gesellschaftswissenschaften	22.749
	Ingenieurwissenschaften	7.506
	Naturwissenschaften	6.126
	Medizin	2.118
	Zentrale Einrichtungen	176
Mitarbeiter		5.634
	Professorinnen und Professoren	408
	Juniorprofessorinnen und –professoren	67
	Wissenschaftliches Personal	2.724
	Nichtwissenschaftliches Personal	2.435

Fakultäten und Studiengänge				
Fächergruppen	**Fakultäten**	**Bachelor**	**Master**	**Sonstige**
Geistes- und Gesellschaftswissenschaften	11	37	95	7
Ingenieurwissenschaften	**3**	**7**	**10**	**-**
Naturwissenschaften	5	12	12	2
Medizin	**1**	**-**	**1**	**1**
Gesamt	20	56	118	10