RUB

RUHR-UNIVERSITÄT BOCHUM

Großgeräteantrag 2015

Implementierung NFC-Studierendenausweis

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

Inhaltsverzeichnis

Antrag
NFC-Studierendenausweis

Implementierung

1 Überblick

Antragstellende Hochschule:	Ruhr-Universität Bochum
Ansprechpartner:	Marcus Klein, Haiko te Neues, Martina Rothacker
Zusammenfassung:	Vorbereitung des technischen Roll-outs des NFC-Studierendenausweises
Durchführungszeitraum endet:	29.02.2016
Bewilligungszeitraum endet:	31.12.2015

2 Motivation

Seit 1997 wird an der Ruhr-Universität Bochum (RUB) eine multifunktionale Karte mit Kryptochip als Ausweis für die Studierenden eingesetzt. Der primäre Einsatzzweck dieser Karte war die Realisierung einer sicheren Zwei-Faktor-Authentifizierung sowie die Möglichkeit zur elektronischen Signatur. Diese wurde in den letzten Jahren aufgrund einer neuen rechtlichen Einordnung als Einsatzzweck für den Studierendenausweis gegenstandslos. Aktuell beschränkt sich die Nutzung des Kryptochips der Studierendenausweise daher auf die Zwei-Faktor-Authentifizierung. Parallel dazu ist im Jahr 2013 die Bereitstellung von RUB-Dienstleistungen auf mobilen Endgeräten in den Fokus gerückt. Da der bisher genutzte Kryptochip des Studierendenausweises einen kontaktbehafteten Chipkartenleser voraussetzt, ist der Kryptochip für den mobilen Einsatz ungeeignet.

Aus dieser Situation heraus wurde im Jahr 2013 das Projekt ›NFC-Studierendenausweis‹ initiiert. Ziel war, eine auf der NFC-Technologie basierende Alternative zu dem bisherigen Kryptochip zu evaluieren, die mit mobilen Geräten funktioniert, und diese in Form eines Proof-of-Concept praktisch zu testen. Das Projekt sollte die technischen Rahmenbedingungen für ein sicheres mobiles Serviceangebot schaffen und dabei gleichzeitig die Nutzbarkeit der kostengünstigeren NFC-Karte als Alternative zur Kryptokarte prüfen.

Die Ergebnisse dieses Projektes sind sehr vielversprechend ausgefallen: Es wurde nachgewiesen, dass sich mit der NFC-Karte eine sichere Authentifizierung auf dem Niveau der bisherigen Kryptokarte realisieren lässt. Des Weiteren konnte der Einsatz im mobilen

Umfeld in Form einer Android-App erfolgreich getestet werden. Die NFC-Karte ist daher generell als Ablösung für den bisherigen kryptochip-basierten Ausweis geeignet.

Aufgrund dieser Ergebnisse – dem erweiterten Einsatzbereich der Karte und der potentiell erheblichen Kostenreduktion gegenüber den bisherigen Ausweisen – empfiehlt es sich, die Idee ›NFC-Ausweis‹ weiterzuverfolgen. Im nächsten Schritt müssen daher die Voraussetzungen bzw. Grundlagen für die Entwicklung eines Roll-outs geschaffen werden. Es gilt zu prüfen, wie die Massenproduktion sowie die Nachbearbeitung der Ausweise realisiert und wie das Authentifizierungskonzept aus dem mobilen Umfeld auf die PC-Welt übertragen werden kann.

3 Ziel

Das Ziel dieses Projektes ist, die technischen und organisatorischen Grundlagen zu schaffen, um ein Roll-out der NFC-Karten angehen zu können. Dazu muss ein Konzept entwickelt werden, das die automatisierte Provisionierung der NFC-Studierendenausweise in großer Stückzahl umfasst. Dieses Konzept muss dabei sowohl die vorhandene Infrastruktur als auch die erforderliche Software beinhalten. Als Nachweis für die Machbarkeit müssen alle konzipierten Komponenten prototypisch umgesetzt und praktisch getestet werden.

Da die Anzahl und die Inhalte der Applikationen auf der NFC-Karte über ihren Lebenszyklus hinweg variabel sein können, muss darüber hinaus ein System konzipiert und entwickelt werden, das eine nachträgliche Bearbeitung der NFC-Karten ermöglicht. Dabei gilt es zu evaluieren, auf welche Art eine zentrale Nachkonfektionierung seitens des Kartenausgebers (Universität) aber auch eine dezentrale Nachkonfektionierung seitens der Drittanbieter (z.B. Druckzentrum oder Bibliothek) erfolgen kann.

Hinsichtlich des Karteneinsatzes durch Drittanbieter muss zudem ein geeignetes Schlüsselmanagement konzipiert und umgesetzt werden. Drittanbieter sollen die Möglichkeit erhalten, ihren eigenen Applikationsschlüssel in ihrer eigenen Infrastruktur zu betreiben. Dafür ist zu erarbeiten, auf welche Weise die passenden Schlüssel erzeugt und wie diese während der Laufzeit des jeweiligen Dienstes sicher gespeichert werden können. Da Drittanbieter in der Regel nicht über das passende Sicherheits-Know-How verfügen, soll darüber hinaus eine umfassende Handlungsanweisung für diese erarbeitet werden. Diese soll in Form eines ›Baukastens‹ erstellt werden, der verpflichtende Abläufe und Maßnahmen für Szenarien wie Schlüsselkompromittierung (d.h. Verlust des Vertrauens in die Informationssicherheit), Schlüsseländerung oder die Einstellung des Dienstangebotes spezifiziert.

Für den breiten Einsatz der NFC-Karte ist des Weiteren eine Middleware[1] für die Integration von PCs analog zu dem im Vorgänger-Projekt erarbeiteten Mobil-Konzept erforderlich. Es muss evaluiert werden, auf welche Weise sich die NFC-Karte betriebssystem- und browserübergreifend einsetzen lässt. Ziel ist es, dass die NFC-Karte von den drei großen Betriebssystemen Windows, Linux und Mac OS werden kann und die Softwarelösung dabei hinsichtlich Umfang und Komplexität durch ein universitäres Entwicklerteam wart- und betreibbar ist.

Alle Konzepte und Umsetzungen sollen dabei grundlegend so ausgelegt sein, dass diese mit geringem Aufwand auch auf andere Universitäten bzw. Organisationen übertragbar sind. Es soll keine RUB-spezifische Insellösung konzipiert werden.

4 Projekt

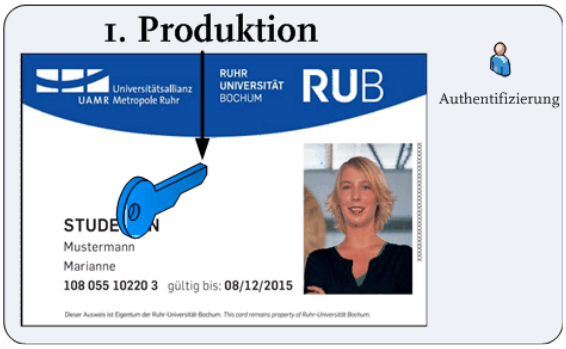
Aus der geplanten Zielsetzung ergeben sich insgesamt vier Arbeitspakete, die es umzusetzen gilt:

1. **Erstausstellung**
   Konzeption & prototypische Umsetzung der Erst-/Massenausstellung von NFC-Karten
2. **Nachkonfektionierung**
   Konzeption & prototypische Umsetzung der Nachkonfektionierung bestehender Karten
3. **Schlüsselmanagement**
   Erarbeitung von organisatorischen & technischen Maßnahmen zum Umgang mit kryptografischen Schlüsseln
4. **Middleware**
   Konzeption & prototypische Umsetzung einer PC-Middleware für die NFC-Karten-Nutzung

4.1 Erstausstellung von NFC-Karten

Im Vorgänger-Projekt wurden das Layout der NFC-Karte entwickelt und Testkarten speziell für die jeweiligen Anwendungsfälle manuell produziert. Für ein Roll-out des NFC-Studierendenausweises muss daher im nächsten Schritt erarbeitet werden, auf welchem Wege große Stückzahlen für den Alltagsbetrieb in Studierendensekretariaten und während der Einschreibephasen produziert werden können.

[1] Als Middleware wird in diesem Kontext eine Software bezeichnet, die als Vermittler zwischen Betriebssystem, Applikationen bzw. generell IT-Komponenten fungiert.



Im ersten Schritt soll dazu ein Softwarepaket konzipiert werden, das die Provisionierung von Karten für alle Studierenden einer Hochschule unter Verwendung der NFC-Technologie ermöglicht. Im Rahmen dieser Konzipierung soll überprüft werden, welche Lösungen bzw. Lösungsansätze im universitären Umfeld bereits existieren und wiederverwendet werden können.

Die Provisionierung einer NFC-Karte soll dabei sowohl die Initialisierung des NFC-Chips, mit mindestens einer Applikation (Authentifizierung), als auch die optische Personalisierung des Ausweises durch einen Aufdruck beinhalten. Ziel der Provisionierung ist ein Ausweis, mit dem sich ein Student per NFC oder visueller Prüfung ausweisen kann.

Das Provisionierungskonzept soll darüber hinaus die Aufbringung von weiteren Applikationen (z.B. Drucken/Kopieren/Parken/Schließen) vorsehen. Je nach Mindestanforderung an den Studierendenausweis soll es möglich sein, alle initial benötigten Applikationen automatisch während der Erstausstellung aufzubringen.

Das konzipierte Softwarepaket soll sich zudem einfach in die Produktionsabläufe und technische Infrastruktur der Hochschulen integrieren lassen. Die Kartenproduktion soll je nach Gegebenheiten direkt während der Einschreibung, als Massenproduktion im Batch-Verfahren oder aber von einer anderweitigen Ausgabestelle (z.B. Studierendensekretariat) erfolgen können. Das Konzept soll daher eine, auf Standardtechnologien basierende Schnittstelle vorsehen, die eine einfache Integration der Produktionssoftware in die unterschiedlichen Einsatzszenarien ermöglicht.

Im zweiten Schritt soll die zuvor konzipierte Software als Prototyp praktisch umgesetzt werden. Folgende Komponenten gilt es dabei auf ihre Machbarkeit/Eignung hin zu prüfen:

- ➔ Einbindung des NFC-Backends (aus dem Vorgängerprojekt) für die Massenproduktion
- ➔ Universelle/standardisierte Schnittstelle
- ➔ Produktionsclient als Beispiel-Implementierung der Schnittstelle

4.2 Nachkonfektionierung von NFC-Karten

Die NFC Karte unterstützt verschiedene Anwendungsfälle, für die unterschiedliche Applikationen mit eigenen Schlüsseln genutzt werden.

Da sich die Anzahl an benötigten Applikationen über die Lebenszeit der Karte hinweg ändern kann, bzw. der Student gegebenenfalls individuell entscheiden muss, welche Dienste er nutzen möchte, muss es auch nachträglich möglich sein, weitere Applikationen auf die Karte aufzubringen.

Dazu soll in einem ersten Schritt ein Konzept entwickelt werden, in dem eine sichere und gleichzeitig praktikable Aufbringung neuer sowie die Aktualisierung bestehender Applikationen erarbeitet wird. Dabei gilt es zu beachten, dass Inhaber und Betreiber der jeweiligen Applikationen neben der Hochschule als Kartenausgeber auch Drittanbieter (z.B. Bibliothek, Druckzentrum, etc.) im Hochschulumfeld sein können. Aus diesem Grund soll die Nachkonfektionierung so konzipiert sein, dass diese bei Bedarf auch von den jeweiligen Applikationsinhabern innerhalb der eigenen Infrastruktur durchgeführt werden kann.

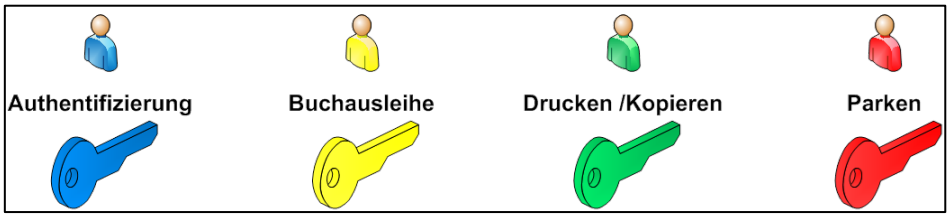
Darüber hinaus soll das Konzept einen ›Self-Service‹ vorsehen. Es soll geprüft werden, ob es technisch machbar ist, für Studierende eine Nachkonfektionierung in Form von Selbstbedienungs-Terminals oder idealerweise als Tool für den eigenen PC oder das eigene Mobilgerät anzubieten. Neben einem deutlichen Plus an Usability für Studierende können auf diese Weise der Aufwand sowie die Komplexität für den jeweiligen Drittanbieter und damit die Gesamtkosten für den Roll-out einer neuen Applikation deutlich gesenkt werden.

Im zweiten Schritt sollen die zuvor erarbeiteten Konzepte in Form eines Proof-of-Concept praktisch getestet werden. Neben der reinen Funktionsfähigkeit gilt es dabei insbesondere die Integrationsfähigkeit der einzelnen Komponenten zu prüfen: Wie hoch ist der Zusatzaufwand für den Drittanbieter? Wie einfach und verständlich lässt sich der ›Self-Service‹ für den Endnutzer umsetzen?

4.3 Schlüsselmanagement

Das technische Gesamtsystem zeichnet sich unter anderem durch die Backend-Kartenkommunikation aus: Server im Backend wickeln die Kommunikation mit den NFC-Karten ab. Diese Server verfügen, in einem speziell gesicherten Bereich, über kryptografische Schlüssel, mit deren Hilfe sich der jeweilige kartenspezifische Schlüssel ermit-

teln lässt und somit die Kommunikation zwischen Server und Karte ermöglicht wird. Abhängig vom hinterlegten Schlüssel können die Daten auf der Karte gelesen oder geschrieben werden, sogar das Aufbringen und Löschen von Applikationen ist möglich.



Den hinterlegten Schlüsseln kommt somit eine besondere Bedeutung zu. Zur Wahrung der Eigenständigkeit der Applikation wird jede Applikation mit eigenen Schlüsseln angelegt. Diese können dem Drittanbieter übergeben werden. Dazu muss aber ein geeignetes Schlüsselmanagement inklusive Handlungsanleitungen erarbeitet werden. Dies ist insbesondere wichtig, da die Drittanbieter erfahrungsgemäß nicht das nötige Sicherheits-Know-How haben. Zum Schlüsselmanagement gehört:

1. **Erstellung eines Applikationsmasterschlüssels**
   Schlüssel müssen zufällig generiert werden.
2. **Aufbewahrung des Applikationsschlüssels**
   Neben der sicheren Erzeugung muss neben dem Aufspielen auf den entsprechenden Servern auch eine geeignete Aufbewahrung des Schlüssels in Betracht gezogen werden.
3. **Einsatzszenarien definieren**
   Zu jeder Applikation werden Lese-/Schreib- und Editierschlüssel festgelegt. Es muss definiert werden, welche Schlüssel in welchen Servern zu welchen Einsatzszenarien hinterlegt werden.
4. **Maßnahmen bei Schlüsselkompromittierung definieren**
5. **Maßnahmen bei Einstellung des Betriebs definieren**

Zu all diesen Punkten müssen Konzepte und Handlungsalternativen erarbeitet werden. Es soll also ein ›Baukasten‹ spezifiziert werden, den die Drittanbieter in ihren Produkten umsetzen müssen, um die Karten nutzen zu können.

Dazu müssen diverse Probleme gelöst werden, z.B.:

- ➔ Wie können Karten zentral produziert werden, damit die Nutzer nicht bei jedem Drittanbieter persönlich erscheinen müssen, um die entsprechenden Applikationen und Schlüssel zu erhalten?
- ➔ Wie sehen entsprechende Szenarien bei Störungen, Defekten oder Neuausstellung von Karten aus?
  Prinzipiell ist es denkbar, dass ein Drittanbieter völlig autonom eine Applikation

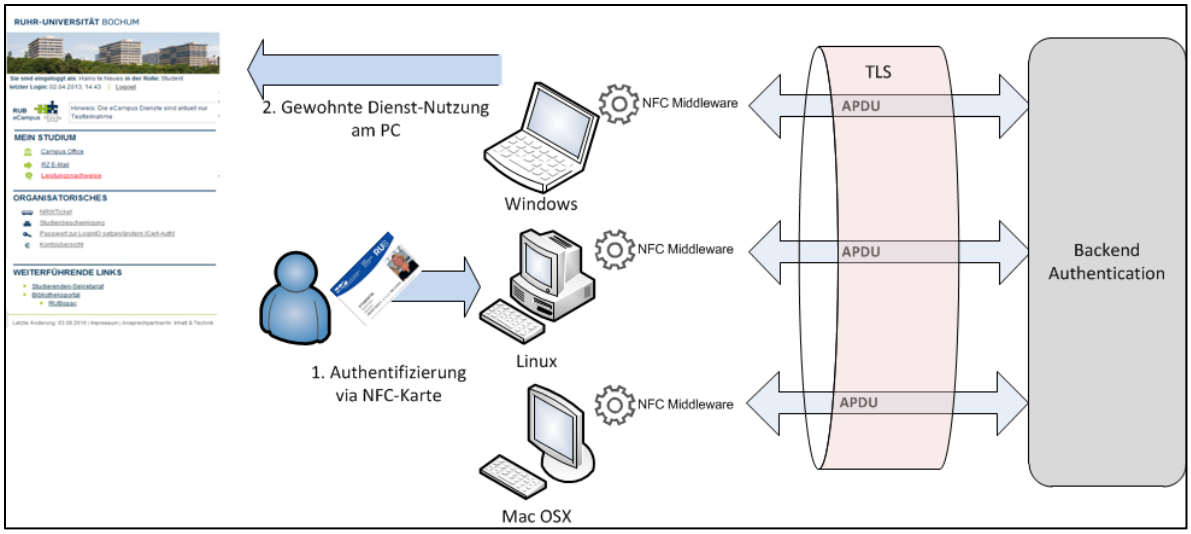
auf die Karte aufbringt. Dies führt aber beim Nutzer zu dem Problem, dass zum Beispiel bei Neuausstellung einer Karte wegen Defekts der Nutzer diese neue Karte nicht mit allen vorher vorhandenen Funktionen erhält. Er muss sich eine neue Karte erstellen lassen und anschließend zum autonomen Drittanbieter gehen, um sich dort seine Applikation wieder aufspielen zu lassen. Auch für diese Szenarien müssen Konzepte entwickelt werden.

4.4 Middleware zur Verwendung von NFC-Karten an PCs

Die Authentifizierung mit der NFC-Karte und einem mobilen Endgerät wurde im Vorgänger-Projekt erfolgreich umgesetzt. Derzeit gibt es jedoch noch keine Lösung für den Einsatz der Karte an einem herkömmlichen PC. Ein Konzept für diesen Bereich ist Voraussetzung für einen universalen Einsatz der NFC-Karte und die Ablösung der Kryptokarte.

In dem hier beantragten Projekt sollen daher entsprechende Konzepte für eine Middleware erarbeitet und die passenden Client-Softwarekomponenten prototypisch erstellt werden.

Die Middleware soll die drei großen Betriebssysteme Windows, Linux und Mac OSX unterstützen. Im ersten Schritt muss evaluiert werden, welche technischen Möglichkeiten für eine Umsetzung existieren und aus organisatorischer Sicht sinnvoll sind.



Der Nutzer soll durch die Middleware in der Lage sein, sich ebenso wie mit der App gegenüber dem NFC-Backend mit der NFC-Karte zu authentifizieren. Nach erfolgter

Authentifizierung, soll der Nutzer seine Online-Dienste wie gewohnt in seinem Browser nutzen können.

Es gilt dabei einen Ansatz zu finden, der in Punkto Entwicklungs- und Wartungsaufwand den der mobilen Lösung nicht deutlich übersteigt. Die Middleware soll ihrem Aufwand nach von einer universitären Entwicklungsabteilung eigenständig weiterentwickelt und gewartet werden können.

5 Die Ruhr-Universität Bochum

Die Ruhr-Universität Bochum zählt mit über 42.000 Studierenden im Wintersemester 2014/2015 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 sowie eine hervorragende Infrastruktur.

Personen im Wintersemester 2014/2015		
Studierende		42.718
	Geistes- und Gesellschaftswissenschaften	25.643
	Ingenieurwissenschaften	7.358
	Naturwissenschaften	7.094
	Medizin	2.358
	Zentrale Einrichtungen	265
Mitarbeiter		5.634
	Professorinnen und Professoren	403
	Juniorprofessorinnen und –professoren	64
	Wissenschaftliches Personal	3266
	Nichtwissenschaftliches Personal	2380

Fakultäten und Studiengänge				
Fächergruppen	**Fakultäten**	**Bachelor**	**Master**	**Sonstige**

Geistes- und Gesellschaftswissenschaften	11	38	95	3
Ingenieurwissenschaften	3	7	12	–
Naturwissenschaften	5	12	15	–
Medizin	1	–	1	1
Gesamt	20	57	123	4