uniChip: Die universelle Chipkartenlösung für den Hessischen Justizvollzug

Elisabeth Heinemann, Christian Pries und Carsten Will*

FG Wirtschaftsinformatik 1:
Entwicklung von Anwendungssystemen
Technische Universität Darmstadt
Hochschulstr. 1
64283 Darmstadt
heinemann@winf.tu-darmstadt.de
christian.pries@gmail.com
unichip@gmx.net

*ADV Leitstelle Justizvollzug Hessen
Stabsstelle des Hessischen Ministeriums der Justiz
Vor den Löserbecken 6
64331 Weiterstadt
c.will@adv-leitstelle.hessen.de

Abstract: Die vorliegende Arbeit beschreibt die Einführung einer multifunktionalen Chipkarte im hessischen Justizvollzug. Sie unterstützt kryptographische Funktionen, die Zeiterfassung der Bediensteten und ist offen für weitere Anwendungsfelder. Umgesetzt wurde das Projekt im Rahmen eines Forschungsauftrages zwischen der ADV-Leitstelle des hessischen Justizministeriums und dem Fachgebiet Wirtschaftsinformatik 1 der Technischen Universität Darmstadt. Ein Prototyp des Systems wurde von den beteiligten Studenten und Mitarbeitern des Auftraggebers auf dem Hessenstand der CeBIT vom 9. bis 15. März 2006 präsentiert.

1 Das Projekt uniChip

Ein Blick in die Brieftasche zeigt, wie vielfältig das Einsatzspektrum von kartenbasierten Identifikationssystemen ist. Es finden sich z.B. Chipkarten von der Bank für den bargeldlosen Zahlungsverkehr neben Magnetkarten vom Arbeitgeber zur Zeiterfassung oder zum Zutritt auf das Betriebsgelände. Ein wachsendes Interesse an der medienbruchlosen Dokumentenverwaltung führt zusätzlich zur Einführung von Signaturkarten. Bei herkömmlichen Lösungen steht den großen Einsatzmöglichkeiten der Karten ein entscheidender Nachteil entgegen: für jede Funktionalität ist ein eigenes Trägermedium erforderlich. Ein Arbeitgeber muss für seine Mitarbeiter also ggf. mehrere Systeme mit mehreren Karten verwalten. Dies ist der Ansatzpunkt für das Projekt *uniChip*. Die Einführung der digitalen (elektronischen) Signatur für das hessenweite elektronischen Dokumentenmanagementsystem DOMEA[1] und die Vereinigung aller sonstigen Funktionen unter dem gemeinsamen Dach der dazugehörigen Chipkarte. Die vorliegende Arbeit beschreibt die Implementierung der Lösung im hessischen Justizvollzug. Das Projekt wurde im Rah-

[1] DOMEA®: Government Content Management System für die öffentliche Verwaltung der Firma OpenText, ursprünglich im Zusammenhang mit der Entwicklung des DOMEA® Konzepts durch die Koordinierungsstelle für Informationstechnik in der Bundesverwaltung beim Bundesministerium des Inneren (KBSt) entstanden und seit 1997 standardprägend (vgl. www.domea.com und [DO05]).

men eines Forschungsauftrages von Studenten der Wirtschaftsinformatik der TU Darmstadt im Wintersemester 05/06 umgesetzt. Auftraggeber war die ADV Leitstelle, die als Stabstelle des hessischen Justizministeriums die EDV des Justizvollzugs betreut[2]. Durch die besondere Konstellation mit Beteiligten aus öffentlicher Verwaltung, universitärer Forschung und Wirtschaft (Lieferanten von Hard- u. Software) konnte das Know-How aus allen drei Bereichen erfolgreich eingebracht werden. Die besonderen logistischen, rechtlichen und organisatorischen Voraussetzungen galt es dabei als bindend und als von „gewöhnlichen" Projektumfeldern abweichend zu bedenken.

Der Aufbau der Arbeit folgt den Entwicklungsschritten bei der Implementierung von uniChip. Neben einigen Definitionen beinhaltet Abschnitt 2 die Beschreibung der Ausgangssituation und der Ziele, die mit dem Projekt verbunden waren. In Abschnitt 3 folgt ein Blick auf die praktische Umsetzung. Einmalig beim Vorgehen der Projektgruppe ist sicherlich die sprachkritische Rekonstruktion des Anwenderwissens in einem Fachkonzept (Abschnitt 3.1). Es stellt die gemeinsame Basis bei der Kommunikation zwischen dem Auftraggeber aus der Verwaltung und dem verwaltungsfremdem Auftragnehmer dar und bildet die Grundlage für die technische Realisierung (Abschnitt 3.2). Die Arbeit schließt mit einem Fazit.

2 Grundlagen, Voraussetzungen und Ziele

Die ADV-Leitstelle ist in der Verwaltung des Landes Hessen Vorreiter beim Einsatz von elektronischen Dokumentenmanagementsystemen. Beispielhaft ist die auf DOMEA basierende „elektronische Gefangenenakte – Basis Web" (vgl. [HeJu06]). Der nächste logische Schritt bei der Digitalisierung, Rationalisierung und medienbruchlosen Gestaltung von Arbeitsabläufen ist die Einführung der digitalen Signatur. Neben den Funktionen einer handschriftlichen Unterschrift garantiert sie die Schutzziele Authentizität (Echtheit der Identität des Unterzeichners ist nachprüfbar), Integrität (eine unbemerkte Manipulation des Dokumentes ist nach der Unterzeichnung ausgeschlossen) und Verbindlichkeit (Unterzeichner kann Aktion im Nachhinein nicht abstreiten) (vgl. [Ecke03], S. 6-10). Die digitale Unterschrift selbst wird mit einer mathematischen Funktion unter Zuhilfenahme eines Schlüssels berechnet[3] und im Dokumentenmanagementsystem als Anhang des eigentlichen Dokumentes verwaltet. Jeder potentielle Unterzeichner muss also im Besitz eines geheimen Schlüssels sein, der unter seiner alleinigen Kontrolle steht. Die Überprüfung einer Unterschrift geschieht mit dem öffentlichen Schlüssel, der mit dem geheimen des Unterzeichners korrespondiert.[4] Die Kombination von beiden Schlüsseln bezeichnet man auch als *Schlüsselpaar*.

---

[2] ADV steht für „Automatisierte Datenverarbeitung", EDV für „Elektronische Datenverarbeitung". In den 1970er Jahren kennzeichnete der Ausdruck ADV den Einsatz der Informations- und Kommunikationstechnologie (des Computers) in öffentlichen Verwaltungen und Behörden, während der Ausdruck EDV für den Einsatz dieser Technologien in der Privatwirtschaft oder in Unternehmen verwendet wurde.

[3] Vom Dokument wird ein Hashwert gebildet und dieser mit dem geheimen Schlüssel des Unterzeichners verschlüsselt.

[4] Der verschlüsselte Hashwert wird mit dem öffentlichen Schlüssel entschlüsselt und mit einem neu berechneten Hashwert des Dokumentes verglichen. Die mathematischen Grundlagen von Signaturverfahren wie RSA finden sich in [Buch03, S. 203-220].

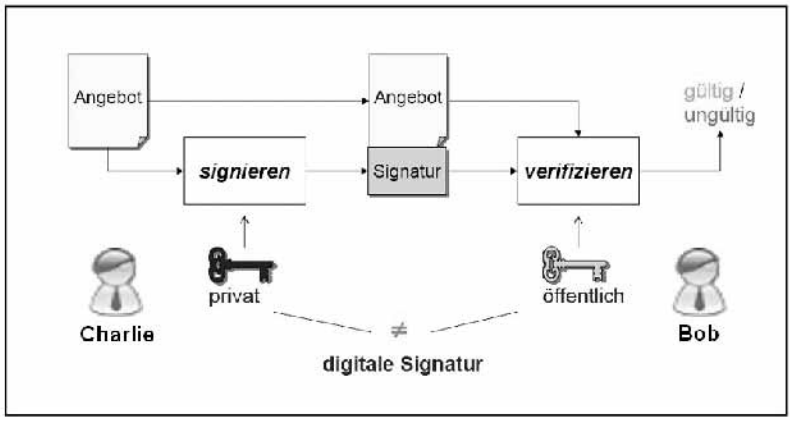

Abbildung 1: Ablauf Digitale Signatur [Buch06]

Abbildung 1 verdeutlicht die Abläufe. Charlie signiert mit seinem geheimen (privaten) Schlüssel, und Bob überprüft die Signatur mit dem dazugehörigen öffentlichen Schlüssel. Die Signatur kann nur vom Unterzeichner stammen, weil der private Schlüssel allein unter seiner Kontrolle steht. Es bleibt zu klären, wie Bob Vertrauen in die Echtheit von Charlies öffentlichem Schlüssel gewinnen kann. Das Mittel der Wahl sind Zertifikate. Sie binden öffentliche Schlüssel an die Identität ihres Besitzers. Damit Zertifikate nicht manipuliert werden können, sind sie von einer vertrauenswürdigen Instanz, der Zertifizierungsstelle (Trustcenter, CA), ausgestellt und unterschrieben. Die Anwender müssen also lediglich die CA als Vertrauensanker wählen, um sich von der Authentizität der öffentlichen Schlüssel aller anderen Teilnehmer überzeugen zu können. Das gesamte System mit Zertifizierungsstelle, Zertifikaten und vielen anderen Elementen heißt auch Public-Key-Infrastruktur (PKI). Spricht man also hier von der Einführung der digitalen Signatur, ist eigentlich der Aufbau einer PKI gemeint.[5]

Die Nutzung von Chipkarten bei der Erstellung einer digitalen Signatur ist nicht erforderlich. Der komplette Vorgang kann auf dem PC des Anwenders stattfinden. Eine fortgeschrittene oder qualifizierte Signatur nach deutschem Signaturgesetz verlangt allerdings den Einsatz von Chipkarten als Trägermedium der geheimen Schlüssel und Einheit zur Erstellung der Signaturen.[6] Diese Chipkarten besitzen ein speziell gehärtetes Betriebssystem und sind gegen Angriffe von außen geschützt. Nur die qualifizierte elektronische Signatur ist der eigenhändigen Unterschrift gesetzlich gleichgestellt.[7]

Mit der Einführung einer Chipkarte sind bei uniChip neben der Signatur noch andere Anwendungsfelder verbunden. Den Nutzern soll es möglich sein, sich an ihrem Computer nicht mehr mittels Passwort, sondern mit der Karte zu authentifizieren. Danach sollen

---

[5] Eine Alternative besteht im Einkauf von Zertifikaten eines externen Zertifizierungsdiensteanbieters. Dieser Weg wurde allerdings im Projekt uniChip nicht verfolgt.

[6] Die Berechnungen finden auf der Karte statt. Der geheime Schlüssel verlässt also nie die Karte.

[7] Eine umfassende wissenschaftliche Einführung in das Themengebiet digitale Signatur und PKI findet sich in [Ecke03] S. 290-365.

alle weiteren Anmeldevorgänger an Fachanwendungen (hier DOMEA und SP-Expert[8]) automatisiert und für den Anwender transparent ablaufen (Single-Sign-On, SSO).

Die im Umfeld PKI wichtigsten Anforderungen und bei der Implementierung von uniChip zu klärenden Fragestellungen sollen nun aufgeführt werden:

- Aufbau einer PKI unter Vorgaben der Stabstelle Hessen-e-Government [HeG06]; Kompatibilität zur künftigen Hessen-PKI gewährleisten
- Einkauf von Hard- u. Software (Karten, Kartenlesern, CA-Management Software)
- Erweiterung von DOMEA um die Funktion digitale Signatur unter den speziellen Voraussetzungen der öffentlichen Verwaltung
- Anbindung der PKI an das Active Directory von Windows zur Authentifikation mittels Chipkarte
- Verknüpfung der Authentifikationsverfahren der Fachanwendungen mit der Authentifikation von Windows zum Single-Sign-On
- Erstellung eines Konzeptes zur Personalisierung und zum Handling der Karten
- Erstellung eines Changemanagement- und Einführungskonzepts zur Sicherstellung der Akzeptanz bei den Bediensteten (auch bei RFID)
- Erarbeiten geeigneter Schulungskonzepte

Diese Aufstellung erhebt nicht den Anspruch der Vollständigkeit. Die technische Realisierung wird in Abschnitt 3.2 beschreiben.

Die Konzeption von uniChip geht über die bisher beschriebenen kryptographischen Funktionen hinaus. Um zusätzliche Anwendungsfelder, wie die Zeiterfassung, Zutrittskontrolle oder eine Bezahlfunktion zu unterstützten, ist eine weitere Trägertechnologie erforderlich. In der Vergangenheit wurden hierfür vor allem Magnetstreifen eingesetzt. Ihre Speicherkapazität, Robustheit, Flexibilität und Sicherheit entspricht allerdings nicht mehr dem heutigen Stand der Wissenschaft. Deswegen soll im Rahmen von uniChip auf eine kontaktlose Technologie (RFID) umgestellt werden. Ein entsprechender Chip, der über eine Entfernung von bis zu 50 cm beschrieben und ausgelesen werden kann, befindet sich neben dem „Krypto-Chip“ auf der im Rahmen von uniChip eingeführten Chipkarte. Das erste Anwendungsfeld stellt die elektronische Zeiterfassung der Bediensteten des Justizvollzuges dar. Die von ihnen bisher benutzte kontaktbehaftete Karte wird dabei im Rahmen des Roll-Outs von uniChip ersetzt. Daneben wird das gesamte Zeiterfassungssystem mit Terminals in allen Justizvollzugsanstalten auf eine gemeinsame Online-Plattform umgestellt, die von der ADV-Leitstelle in Weiterstadt administriert wird.

Wie im Bereich der PKI sollen auch für den Themenbereich RFID die mit uniChip verbundenen Ziele und Aufgaben aufgeführt werden:

---

[8] SP-Expert: Software für die Personaleinsatzplanung und integrierte Online-Zeitwirtschaft der Firma Ingersoll Rand – Security Technologies. Vgl. www.interflex.de und [SPX05].

- Herstellung einer einheitlichen, kontaktlosen Zeiterfassung und Zeitdatenbewirtschaftung auf der Zentralplattform SP-Expert[9] für alle Bediensteten des hessischen Justizvollzuges unter Berücksichtigung der folgenden Anforderungen:
  - Einrichtung einheitlicher Zeiterfassungsterminals in allen hessischen Justizvollzugsanstalten,
  - Zentrale Anbindung der Zeiterfassungsterminals und -Software an die ADV-Leitstelle
- Konzept zur Personalisierung der Chipkarten unter Berücksichtigung der Möglichkeit eines Dienstortwechsels unter Beibehaltung der Chipkarte
- Offenhaltung weiterer Nutzungsmöglichkeiten für ein potentielles einheitliches hessenweites Chipkartensystems
- Dokumentation des Projekts als grundlegende Qualitätssicherungsmaßnahme

Die Anforderungen im Umfeld PKI und RFID beeinflussen sich gegenseitig. Besonders bei der Personalisierung folgt aus dem Einsatz der Karte im sicherheitskritischen Bereich Kryptographie, dass auch die Personalisierung des RFID-Chips direkt im Justizvollzug geschehen muss. Die Auslagerung dieser Tätigkeit an den Lieferanten des Zeiterfassungssystems, wie bei vielen Unternehmen üblich und auch bei den alten kontaktbehafteten Karten durchgeführt, ist deswegen nicht mehr möglich.

3 Umsetzung

Das Projekt uniChip orientiert sich an dem *Multipfad-Vorgehensmodell* nach Ortner [Or05]. Exemplarisch wird nun die Lösung der Kommunikationsproblematik zwischen den beteiligten Gruppen anhand eines Fachentwurfes beschrieben. Danach kann auf die konkrete Umsetzung der Anforderungen aus Abschnitt 2 eingegangen werden.

3.1 Fachentwurf

Im Multipfad-Vorgehensmodell folgt auf die Voruntersuchung mit dem Ergebnis Pflichtenheft die Phase des Fachentwurfes. Damit sollen Kommunikationsprobleme behoben werden, die zwischen Auftraggeber, Entwicklern und späteren Benutzern durch die Verwendung unterschiedlicher Sprachräume und -ebenen auftreten. Ohne Fachentwurf besteht die Möglichkeit von Missverständnissen beim Informationsaustausch, die eine erfolgreiche und allen Anforderungen gerecht werdende Entwicklung gefährden. Das Fachgebiet Wirtschaftsinformatik 1 der TU Darmstadt sieht gerade bei der Überbrückung dieser Sprachdefizite die Hauptaufgabe von Wirtschaftsinformatikern im Rahmen der Entwicklung von Anwendungssystemen.

[9] SP-Expert: Software für die Personaleinsatzplanung und integrierte Online-Zeitwirtschaft der Firma Ingersoll Rand – Security Technologies. Vgl. www.interflex.de und [SPX05].

Ziel ist also, die fehlerfreie Kommunikation zwischen den verschiedenen Interaktionspartnern durch Einigung auf eine gemeinsame *Terminologie* zu gewährleisten.

Im methodenneutralen Fachentwurf spielt vor allem die Gebrauchssprache des Anwenders eine wichtige Rolle. Er verfügt über das nötige Fachwissen und kennt die Anforderungen an das zu entwickelnde Anwendungssystem. Konkret bedeutet dies z.B., dass die Fachanwender von DOMEA am genauesten wissen, was eine digitale Signatur für sie leisten muss. Die Gebrauchssprache von Anwendern zeichnet sich aber zumeist durch Redundanzen, synonyme Wortverwendungen und andere sprachliche Defizite aus und ist selten in sich logisch konsistent oder gar die gewünschten Aussagen „auf den Punkt bringend". Es ergibt sich die Notwendigkeit einer Rekonstruktion entsprechender Fachaussagen, damit sie von den Entwicklern korrekt umgesetzt werden können.

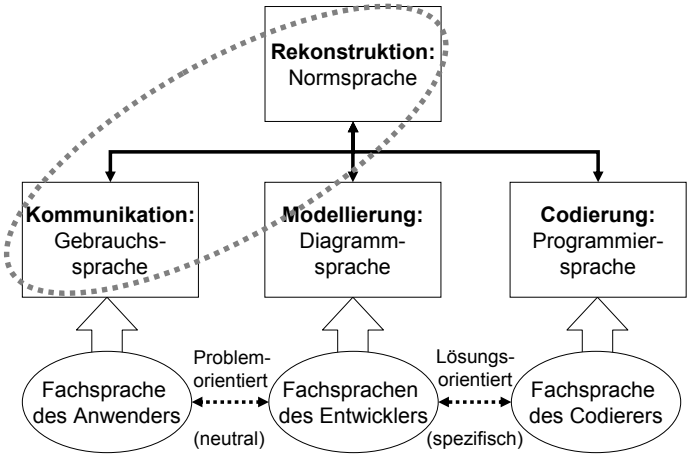

Abbildung 2: Sprachen im Entwicklungsprozess (vgl. [He06], S. 44)

Der erste Schritt im Fachkonzept besteht in der Erfassung entwicklungsrelevanter Aussagen [Or05]. Dabei wurden in uniChip folgende Methoden herangezogen:

- Gespräche und Interviews mit künftigen Benutzern und mit Fachleuten in punkto der zu integrierenden Systeme ebenso wie hinsichtlich der gesetzlichen Vorgaben,
- entsprechende Fachliteratur,
- vorhandene Dokumentation bzgl. SP-Expert, DOMEA, Hessen-PKI, etc.

Eine Aussage gilt als entwicklungsrelevant, wenn sie *anwendungsübergreifend*, *systemunabhängig* sowie *sprach- und sachgerecht* ist. Dann wird sie in Schritt 2 zur Rekonstruktion der Fachbegriffe auf dem Weg zu einer einheitlichen Terminologie herangezogen. Die Teilschritte sind dabei nach [Or05]:

- zunächst die Ermittlung geeigneter Fachbegriffskandidaten,
- die anschließende Definition gemäß geeigneter Definitionsverfahren und
- zuletzt die Beseitigung auftretender Sprachdefekte.

Insbesondere der letzte Punkt war innerhalb der ADV-Leitstelle von größerer Bedeutung als zunächst angenommen, da unter den Bediensteten nicht selten Uneinigkeit bei der Verwendung bestimmter Begriffswörter herrschte. Die Vorgehensweise zur Klärung solcher im Fachentwurf zu behebenden Sprachdefekte zeigt folgendes Beispiel:

Kartenlese- und Schreibgerät	
Kurzdefinition	Gerät zum Lesen und Beschreiben einer Chipkarte.
Langdefinition	Kartenlese- und Kartenschreibgerät $=_{DF}$ Gerät, welches es ermöglicht, den Inhalt des *Kryptochips* auf den Ausweisen zu lesen und diesen durch Beschreiben der *Chipkarte* zu verändern. Werden Signiervorgänge in E-Mails oder Fachapplikationen wie *DOMEA* verlangt, so erfolgt der Transfer der benötigten Daten des *Zertifikats*, welches auf der Karte vorliegt, über das Kartenlesegerät des Arbeitsplatzes.
Sprachdefekt(e)	Vagheit
Aussagen	Um eine *digitale Signatur* zu erstellen, ist die Eingabe des *PINs* am Kartenlese- und Kartenschreibgerät erforderlich.
Beziehungen zu anderen Begriffen	- Chipkartensystem - digitale Signatur
Aufgetretene(s) Problem(e)	Als Kartenlese und Kartenschreibgerät soll NICHT die *Codierstation* für den *LEGIC-Chip* auf der Chipkarte verstanden werden.

Neben der in obigem Beispiel auftretenden *Vagheit* als sprachlichem Defekt mussten noch eventuelle *Homonyme*, *Synonyme*, *Falsche Bezeichner* und *Äquipollenzen* aufgedeckt werden. Bis auf letzteren wurden tatsächlich alle Defekte identifiziert und entsprechend behandelt (aufgehoben oder zwecks Kontrolle dokumentiert).

Das Ergebnis des Fachentwurfes ist ein Fachkonzept mit einer einheitlichen Terminologie. Diese ist Grundlage für die Dokumentationen und Konzepte, die in den späteren Phasen der Entwicklung von uniChip entstanden sind. Den Mitarbeitern der ADV-Leitstelle kann es deswegen als umfassendes Nachschlagewerk für die Bereiche PKI und RFID dienen. Auch für zukünftige Erweiterungen, die in Zusammenarbeit mit anderen Partnern umgesetzt werden, kann das Fachkonzept als Basis dienen.

3.2 Technische Realisierung

Abbildung 3 zeigt die unterschiedlichen Komponenten des Anwendungssystemes uniChip. Im Zentrum steht die universelle Chipkarte für die Bediensteten des Justizvollzuges. Es handelt sich um eine Telesec Netkey E 4 Karte. Sie wurde nach positiven Erfahrungen im Rahmen des Pilotversuches Hessen-PKI (vgl. [Brin05]) ausgewählt und genügt den Anforderungen des Projektes. Die von der Fa. Kobil gelieferten Kartenlese- u. Schreibgeräte (mit Pineingabe) konnten ebf. bei der Hessen-PKI bereits getestet werden. Da die IT-Infrastruktur des hessischen Justizvollzuges auf Servern mit dem Betriebssystem Microsoft Windows 2003 basiert und die dazugehörigen Erweiterungen zum Betrieb

einer PKI schnell und kostengünstig beschafft werden konnten, setzt uniChip auf Microsoft PKI-Komponenten auf. Im Verlaufe des Projektes wurde klar, dass die Zertifikate lediglich den Ansprüchen an eine fortgeschrittene Signatur nach Signaturgesetz genügen können.

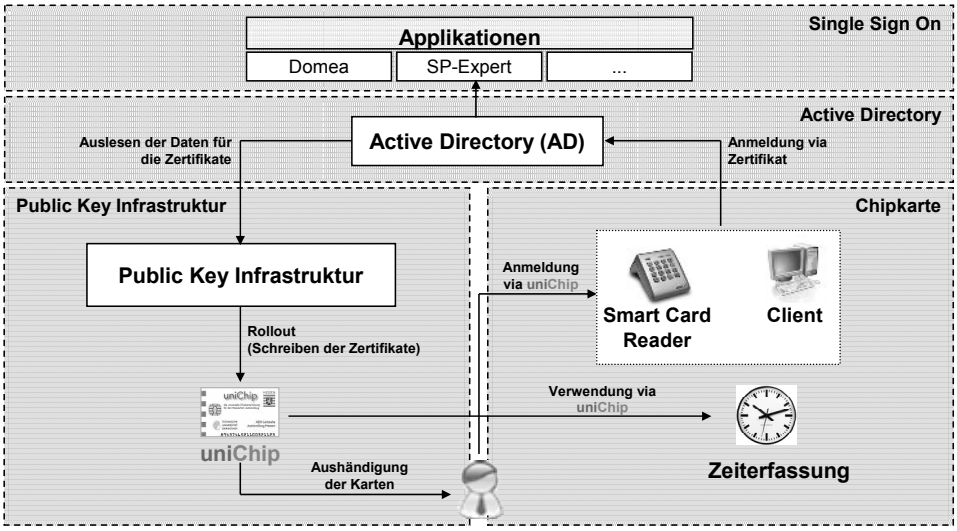

Abbildung 3: Gesamtübersicht des Projektes uniChip

Die Einführung einer qualifizierten Signatur ist im gegebenen Rahmen nicht möglich. Ins Zentrum der Bemühungen rückte deswegen die hessenweit erstmalige digitale Signatur im elektronischen Dokumentenmanagementsystem DOMEA. Die notwendigen Anpassungen wurden gemeinsam mit Entwicklern des Herstellerunternehmens OpenText realisiert. Ein Dokument kann von mehreren Nutzern signiert werden, ist aber nach jeder Signatur für die Weiterbearbeitung gesperrt. Bei Änderungen muss zunächst eine Kopie erzeugt werden, sodass mit der Signatur gleichzeitig eine Aufstellung über die verschiedenen Versionen eines Dokumentes entsteht. Dies entspricht der Funktionalität „Handzeichen“ in DOMEA erweitert um die Schutzziele der digitalen Signatur. Praktisch muss sich zur Signatur die Chipkarte im Kartenleser befinden, und der Anwender muss die Benutzung seines geheimen Schlüssels durch PIN-Eingabe autorisieren.

Im Bereich Single-Sign-On kann die Authentifizierung am Windows-PC mittels Chipkarte vom Administrator durch Policies festgelegt werden. Die am Anmeldevorgang beteiligten Komponenten Microsoft PKI, Kobil Kartenlese- u. Schreibgerät, Netkey E 4 Karte und Zertifikat arbeiten problemlos zusammen. Wichtig ist, dass die bei der Registrierung gewählte Zertifikatsvorlage der gewünschten Funktionalität entspricht. Die neueste Version von DOMEA sieht SSO vor, wenn der interne Benutzername dem Windows-Benutzernamen entspricht. Dies ist nach den Benennungskonventionen im Justizvollzug der Fall. Für SP-Expert ist eine solche Übereinstimmung nicht nötig. Dafür verlangt die Software beim erstmaligen Start allerdings eine erneute PIN-Eingabe. Dies scheint gerechtfertigt, da in SP-Expert sensible Personaldaten verarbeitet werden.

Das Konzept von uniChip sieht vor, dass das Roll-Out der Karten nach der zentralen Personalisierung des RFID-Chips geschieht (siehe Abschnitt RFID). Die Schlüssel und Zertifikate können die Bediensteten anschließend an ihrem PC mit einem Registrierungsagenten auf ihre Chipkarte aufbringen. Für die in uniChip verfolgten Einsatzziele ist dieses Vorgehen hinreichend. Eine zentrale Schlüsselerzeugung inkl. Key-Backup ist nicht erforderlich, da keine Verschlüsselungszertifikate erzeugt werden. Die Administration der PKI erfolgt zentral aus der ADV-Leitstelle.

Die Festlegung auf eine RFID-Technologie und einen Dienstleister zur Zeiterfassung ist eine strategische Entscheidung, die später nur unter großem Kostenaufwand (Austausch aller Karten bzw. Terminals) korrigiert werden kann. Wichtig ist, dass die Kontrolle über das gesamte System inkl. der Personalisierung der Karten beim Auftraggeber, also bei der ADV-Leistelle liegt. Als RFID-Technologie wurde Legic gewählt. Ihr Speicherbereich kann für duzende verschiedene Anwendungen unterteilt bzw. segmentiert werden. Ein Segment kann nur beschrieben werden, wenn man im Besitz einer sog. IAM-Karte ist. Da sich diese im Falle von uniChip im Herrschaftsbereich der ADV-Leitstelle befindet, kann ein Dritter niemals eine Karte eines Bediensteten des Justizvollzuges fälschen (vgl. [Mada06], S. 5). Die zweite Festlegung betrifft das Kodierschema, also das Format der Daten, die auf das Segment des Legic-Chips geschrieben werden. Legt man sich auf ein eigenes Schema fest, so kann es vorkommen, dass die Leseterminals für die Zeiterfassung ohne Anpassungen nicht in der Lage sind, das entsprechende Segment auszulesen. Verwendet man das Schema eines Terminalherstellers, können damit ggf. nicht die Voraussetzungen des Auftraggebers abgedeckt werden. Im Falle von uniChip wurde ein Mittelweg gewählt und ein vorhandenes Kodierschema an die Gegebenheiten der ADV-Leitstelle angepasst. Die Personalisierung selbst findet zentral statt. Beim Verlust einer Karte kann der verantwortliche Dienstplaner des Bediensteten über ein standardisiertes Formular eine neue aus der ADV-Leistelle anfordern. In der Zwischenzeit sollen die Arbeitszeiten manuell in SP-Expert erfasst werden. Für die sukzessive Einbeziehung der JVAs in das neue Zeiterfassungssystem wurde im Rahmen von uniChip ein Stufenplan erstellt. Dieser beinhaltet u.a. die Schulung der Bediensteten, Installation der neuen Terminals, Kodierung und Auslieferung der Karten und schließlich Anbindung an das neue Online-Zeiterfassungssystem. Ein entscheidender Vorteil zum bestehenden System ist, dass die Bediensteten auch beim Wechsel ihres Dienstortes die Zeit erfassen können, ohne dass zusätzliche Anpassungen erforderlich werden. Daneben kann das System nun zentral administriert werden. Eine redundante Datenhaltung in den JVAs und in der ADV-Leistelle entfällt.

Durch die offene Konzeption von uniChip können auf den Legic-Chip zukünftig weitere Segmente für Funktionalitäten wie Zutrittskontrolle oder bargeldloses Bezahlen aufgebracht werden.

4 Fazit

Mit uniChip wurde im hessischen Justizvollzug eine zeitgemäße Lösung eingeführt, die für viele Anwendungsszenarien offen ist. Das Potential zur Rationalisierung von Arbeitsabläufen bei der medienbruchlosen Dokumentenverwaltung in DOMEA konnte mit dem auf der CeBIT präsentierten Prototyp bereits der Öffentlichkeit vorgestellt werden.

Single-Sign-On schafft Akzeptanz durch das einfache und bereits vertraute Verfahren der PIN-Eingabe. Für den Anwender ergibt sich durch die einmalige und transparente Authentifizierung eine enorme Zeitersparnis, für Systemadministratoren bedeutet der Wegfall des Aufwandes durch vergessene Passwörter eine deutliche Arbeitserleichterung. Summa summarum verspricht uniChip Kosteneinsparungen bei einem Plus an Sicherheit.

Im Bereich der Zeiterfassung haben sich durch die Einführung von uniChip vor allem zwei Innovationen ergeben:

- Alle Mitarbeiter können ihre Arbeitszeitbuchungen am Zeiterfassungsterminal durch einen kontaktlosen, in uniChip integrierten Legic-Chip durchführen und
- sämtliche Mitarbeiterinnen und Mitarbeiter des Justizvollzuges werden in dem Modul Zeitdatenbewirtschaftung des Verfahrens SP-Expert abgebildet. Hierdurch ergeben sich für den hessischen Justizvollzug enorme Einsparungspotentiale, da eine redundante Datenhaltung in unterschiedlichen lokalen Zeiterfassungssystemen entbehrlich geworden ist.

Das Projekt „uniChip“ folgt den bereits existierenden Vorgaben des landesweiten Projekts Hessen-PKI und kann somit als ein weiterer, erfolgreicher Baustein der hessischen E-Government-Strategie betrachtet werden.

Die Autoren möchten dazu ermutigen, bei ähnlichen Projekten die Zusammenarbeit zwischen öffentlicher Verwaltung und universitärer Forschung zu suchen. Die im Rahmen von uniChip gemachten Erfahrungen, besonders das gemeinsame Lernen von- und miteinander, waren für ADV-Leitstelle, Universität und Studenten durchweg positiv.

5 Danksagung

Großer Dank gebührt den Studenten, die im Wintersemester 2005/2006 im FG *Wirtschaftsinformatik 1 – Entwicklung von Anwendungssystemen* ihr Wirtschaftsinformatikpraktikum absolviert haben. Ohne ihr außerordentliches Engagement und ihren fachlichen Input wäre das Projekt uniChip nicht zu einem so erfolgreichen Ende gebracht worden. Gleicher Dank gebührt den beteiligten Mitarbeitern der ADV-Leitstelle, die den Studenten in besonderer und nachahmenswerter Weise die logistischen, fachlichen und menschlichen Voraussetzungen für das gute Gelingen des Praktikums geboten haben.

Literaturverzeichnis

[Brin05] Brinkmann, K.: Erfahrungen beim Aufbau einer PKI für das Land Hessen. http://www.iuk-bw.de/Koopadv/Erfahrungen%20beim%20Aubau%20einer%20PKI%20f%FCr%20das%20Land%20Hessen_Dr.%20Brinkmann.pdf, Abruf am 10.08.2006.

[Buch03] Buchmann, J.: Einführung in die Kryptographie. 3., erw. Aufl., Springer, Berlin, 2003.

[Buch06] Buchmann, J.: Vorlesungsunterlagen zur Veranstaltung Public Key Infrastrukturen. cdc.informatik.tu-darmstadt.de, Abruf am 01.06.2006.

[DO05] Installationshandbuch für DOMEA®. Stand 12/2005.

[Ecke03] Eckert, C.: IT-Sicherheit. Konzepte – Verfahren – Protokolle. 2. Auflage, Oldenbourg Verlag, München, 2003.

[He06] Heinemann, E.: Sprachlogische Aspekte rechnerunterstützten Denkens, Redens und Handelns. Eine Wissenschaftstheorie der Wirtschaftsinformatik. Dtsch.-Univ.-Verlag, Wiesbaden, 2006.

[HeG06] www.hessen-egovernment.de, Abruf am 26.06.2006.

[HeJu06] Hessisches Ministerium der Justiz: Elektronische Gefangenenpersonalakte. www.hessen-egoverment.de%2Firj%2Fservlet%2Fprt %2Fportal%2Fprtroot%2Fslimp.CMReader%2 FHMdI%2FeGovernment_Internet%2Fmed%2F382%2F38250039-6f80-7b01-be59-264 4e9169fcc%2C44444444-4444-4444-4444-444444444444.pdf, Abruf am 26.06.2006.

[Mada06] Marx Datentechnik: Berührungslose Datenträger. http://mada.de/DOWNLOADS/DATENTRAEGER/datentraeger%20rfid.pdf, Abruf am 10.08.2006.

[Or05] Ortner, E.: Sprachbasierte Informatik. Wie man mit Wörtern die Cyber-Welt bewegt. EAGLE-Verlag, Leipzig, 2005.

[SPX05] Installationshandbuch für SP-Expert. Stand 12/2005.