Chancen und Möglichkeiten von SmartCards im universitären Umfeld

Erik Donner

Siemens AG 2001

1 Mögliche Bedrohungen im universitären Umfeld

Universitäten sind in vielerlei Hinsicht Bedrohungen ausgesetzt. Diese Bedrohungen lassen sich grob in physikalische und logische Gefährdungen unterteilen. Diese können sowohl vom sowohl vom internen(Studenten, Mitarbeiter, interne Dienstleister) als auch vom externen (Fremdfirmen, Besucher,...) universitären Umfeld ausgehen.

Typische physikalische Bedrohungen sind:

- Einbruch
- Diebstahl

Gefährdungen aus dem logischen Bereich sind

- Manipulation von Arbeitsergebnissen
- Veränderungen von Ergebnissen aus Forschung und Lehre
- Gezielte Angriffe auf Rechner (Würmer, Syn Flooding, usw.)
- Gebührenmissbrauch an Telefonsystemen
  Spoofing

Eine häufige, oft vernachlässigte und daher eine besonders gefährliche Bedrohung , ist das sogenannte Social Engineering. Dabei wird auf persönlicher Ebene, z.B. in Gesprächen, versucht an geheime Daten oder Informationen zu kommen.

Prinzipiell gibt es für jede der o.a. Bedrohungen spezifische Gegenmassnahmen. In den meisten Fällen werden diese auch umgesetzt und für die Dauer ihres Einsatzes aktualisiert und gepflegt.

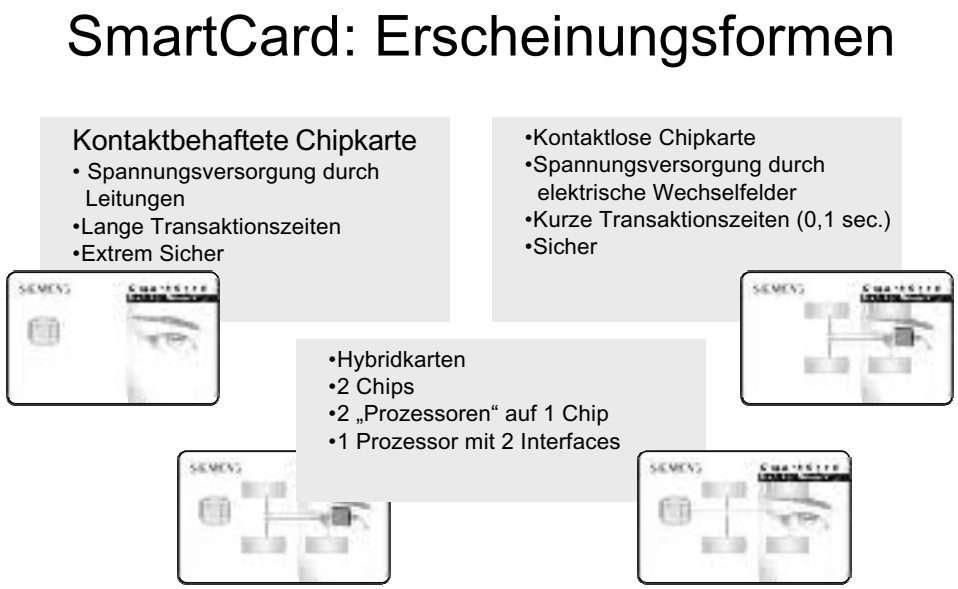
Trotz wirksamer Einzelmaßnahmen existiert in den meisten Fällen kein übergreifendes Sicherheitskonzept zur Integration der Systeme. Daraus resultiert ein erhöhter Aufwand für das Management wogegen die Akzeptanz durch die Benutzer sinkt und damit auch der Effekt der Sicherheitsmaßnahme.

Ziel sollte es also sein, eine Technologie oder ein Medium zu finden, welches sowohl von den Nutzern als auch von den Abteilungen akzeptiert wird, die es letztendlich betreiben.

2 Erscheinungsformen von SmartCards

SmartCards sind heute in verschiedenen Erscheinungsformen verfügbar. Die äusseren Abmessungen sowie die Kontaktflächen für die kontaktbehafteten Chipkarten sind in gemäß den Normen ISO 7816.XX standardisiert.

Eine bekannte und weit verbreitete Chipkarte ist die Krankenversichertenkarte. Sie beinhaltet einen kontaktbehafteten Chip, der als sicherer Speicher für Daten dient. Eine Weiterentwicklung dieser Chipkarte enthält sogenannte Prozessor-Chips, welche eigenständig Programme ausführen können. Die Speicherbereiche dieser Prozessorchips sind vor Zugriff Unbefugter stärker gesichert. Die sicherste Variante der kontaktbehafteten Chipkarte speichert die Daten auf einem Prozessorchip mit Kryptocoprozessor. Diese zusätzliche Recheneinheit im Chip wurde speziell für die Ausführung von kryptografischen Verfahren zur Verschlüsselung oder Signatur von Daten optimiert.



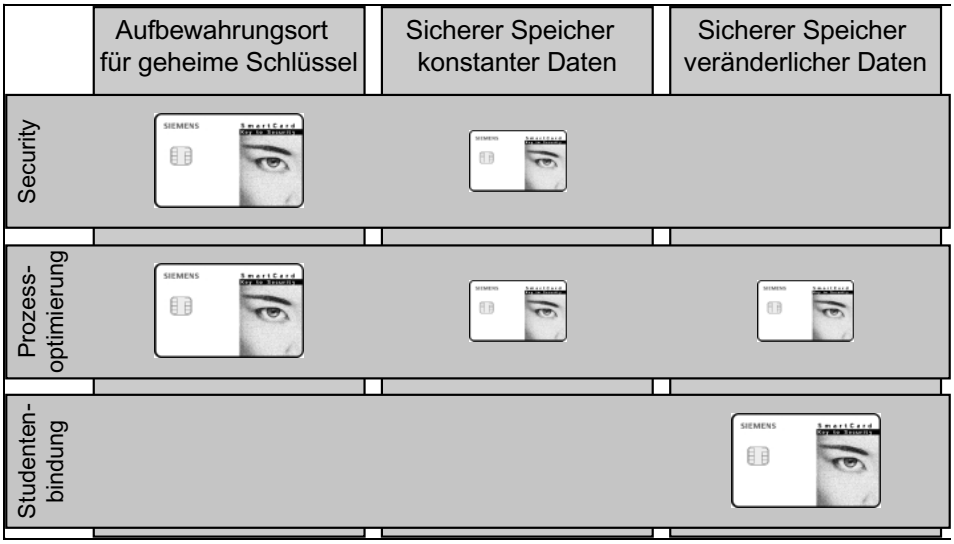
Kontaktlose Chipkarten werden in den meisten Fällen zur Unterstützung von Zutrittskontrollen, Zeiterfassung oder Kantinenabrechnungen genutzt. Dabei übertragen die Chipkarten in einem Abstand von wenigen Zentimetern zur Leseeinheit meist nur einfache Daten wie Identifikationsnummern.

Bei einer Kombination der beiden o.a. Datenträger auf Chipkarten spricht man von sogenannten Hybridkarten, auf der beide Systeme logisch unabhängig voneinander funktionieren. Die Dual-Interface Karte besitzt nur einen Datenträger mit zwei Zugriffsmöglichkeiten auf die Daten. Weiterhin sind noch Kombinationen mit diversen anderen Datenträgern, wie z.B. Magnetstreifen, Barcode o.ä., auf der Chipkarte denkbar. Eine solche Kombination von Datenspeichern auf einem Medium bietet aus unserer Sicht eine ideale und für die Nutzer gewohnte Integrationsplattform für ein homogenes Schutzkonzept.

3 Einsatzmöglichkeiten der SmartCard Typen

Die Eigenschaften von SmartCards qualifizieren dieses Medium für bestimmte Einsatzzwecke unterschiedlich gut. Diese Tatsachen erfordern, dass im Vorfeld die geeigneten Datenspeicher für die einzuführende Karte näher betrachtet werden müssen.

Im universitären Umfeld spielen neben der Speicherung von geheimen Informationen als Anwendung im Security Bereich auch weitere Optionen eine wichtige Rolle. So bietet eine SmartCard die Möglichkeit der Prozessoptimierung und der Einbindung zusätzlicher Dienste - aus meiner Sicht ein hervorragendes Medium zur Bindung der Studenten an die entsprechende Universität und der gebotenen Dienstleistungen.



Die Chipkarte als Aufbewahrungsort für geheime Informationen zur Verschlüsselung und Signatur von Dokumenten und Daten ist für Anwendungen im Bereich Prozessoptimierung durch die entfallenden Medienbrüche bei Unterschriften(hierarchien) ein sogar von der Gesetzgebung präferiertes und empfohlenes Medium.

Die beispielsweise für die Identifikation des Nutzers an Zutrittskontrollen oder Zeiterfassungssystemen notwendigen Daten werden einmalig auf die kontaktlosen Chips geschrieben und danach nicht mehr verändert. Hier wird der Vorteil einer SmartCard als Integrationsmedium für mehrere Dienste sehr deutlich, der ermöglicht, nicht für jede Anwendung ein gesondertes Medium nutzen und verwalten zu müssen.

Die Bindung der Studenten , die immer mehr als Thema im Bereich der Kundenbindung zu sehen ist, wird gerade in der derzeitigen Situation vieler Universitäten (Bindung von Budgets an Studentenzahlen) immerrelevanter. Mit der Studentenkarte können so Fahrausweise für die örtlichen Verkehrsbetriebe, Zugänge zu elektronischen Lehrmaterialien oder die Rabattierung der Leistung von Partner-Unternehmen umgesetzt werden. Letztere Anwendung wird auch durch das seit dem 25. Juli 2001 gefallene Rabattgesetz unterstützt.

4 Chancen durch die Einführung von SmartCards/Nutzergruppen

Chipkarten werden durch ihre starke Akzeptanz bei den Nutzern und bei den Herausgebern in den meisten Fällen als Identifikationsmedium jeglicher Art eingesetzt. Das Spektrum reicht vom einfachsten Fall, der rein optischen Identifikation durch eine Kontrollperson, bis zu hochtechnologisierten Authentifikationen mittels asymmetrischer Kryptografie.

Die an den unterschiedlichen Universitäten eingesetzten Ausweise sind vielfältig und werden von den verschiedensten Bereichen und Organisationen herausgegeben. Die hinterlegten Funktionen eines Ausweises umfassen im wesentlichen die eines Studentenausweises, eines Mitarbeiterausweises oder einer Zutrittskontrollkarte für das Rechenzentrum aber auch die oft oft unterschätzten Anwendungen zum Bezahlen am öffentlichen Kopierer, der möglichen Abrechnung privater Telefongespräche der Studenten bis hin zur Parkberechtigung für Studenten und Mitarbeiter.

Eine einwandfreie und unwiderlegbare Identifikation von Nutzern an Rechensystemen ist für Nutzer und Anbieter von Vorteil. Dem Nutzer kann, im Idealfall unabhängig von der Hardware, seine persönliche Oberfläche zur Verfügung gestellt werden, oder er hat die Möglichkeit, vertrauliche Emails sicher zu versenden. Aus Sicht der Dienstleistungen kann eine sichere Autorisierung an den Zugängen zu Netzwerkressourcen und damit die Vertraulichkeit z.B. von Personal- oder Forschungsdaten gewährleistet werden. Der Einsatz eines einheitlichen Mediums zu Identifikation und der weiteren Möglichkeit der Einführung einer Public Key Infrastruktur lässt sich ein homogenes Sicherheitskonzept für das Rechnernetz der Universität aufbauen.

Erfahrungen aus bisher durchgeführten Projekte an Universitäten und anderen schulischen Einrichtungen haben gezeigt, daß die Nutzung der Chipkartenoberfläche als Werbefläche für Firmen und Krankenkassen sehr interessant ist ..

Die Einführung der Technologie SmartCard kann daher auch durch diese Werbeeinnahmen finanziert werden. Umfragen haben gezeigt, dass sich auf diese Weise zumindest die Kosten für das Medium der Karten, die je nach Ausprägung und Menge zwischen DM 10 und DM 25 liegen, refinanzieren lassen.

Die potenziellen Nutzer einer solchen Karte finden sich sowohl auf der Seite der Dienstanbieter als auch auf Seiten der Anwender. Nutzergruppen können sein:

- Rektorat und Verwaltung
- Wissenschaftsbereiche/*Unternehmen auf dem Campus*
- Universitätsbibliothek
- Rechenzentrum
- ASTA
- *Studentenwerk*
- *ÖPNV*

Die durch Kursivschrift gekennzeichneten Organisationen können durch externe Gelder die Finanzierung der Einführung einer Chipkarte unterstützen

In der Kombination von Diensten auf einem anerkannt sicheren Medium liegt, bei einem Zusammenschluss der Herausgeber **eines** Ausweises ein grosses Optimierungspotenzial in finanzieller und organisatorischer Hinsicht brach. Leider sind in diesem Rahmen keine pauschalen Aussagen hinsichtlich der einzusparenden Kosten möglich, da jede universitäre Einrichtung auf anderen Prozessen aufsetzt.

5 Risiken bei der Einführung von SmartCards

Die oben beschriebenen verschiedenen Nutzergruppen stellen nicht selten in sich geschlossene Organisationen mit eigenen Zielen und vor allem Budgets dar. Bei der Einführung einer übergreifenden Technik zur Integration von Diensten ist eine gemeinsame Definition des Mediums und der darauf versammelten Anwendungen eine grosse, wenn nicht sogar die grösste Herausforderung. Hierbei ist es besonders wichtig, dass alle potentiell beteiligten Parteien von Anfang an gleichberechtigt an den Planungsgesprächen teilnehmen. Bereits abgeschlossene Projekte haben gezeigt, dass es sehr hilfreich ist, einen externen Berater für die Projektplanung und –abwicklung hinzuzuziehen, der die Gespräche zwischen den Beteiligten moderiert, steuert sowie seine Erfahrungen einbringt.

In enger Beziehung zu den eben angesprochenen Koordinierungsgesprächen steht auch die Diskussion der Datenströme bei einem solch komplexen Unterfangen. Besonderes Interesse daran haben die Vertretergremien der Mitarbeiter und Studenten. Aus meiner Sicht können Widerstände oder Irritationen in diesen Gremien am besten aufgehoben werden, wenn von Anfang an klar ist, welche Daten zu welchem Zweck übertragen und/oder gespeichert werden. In diesem Zusammenhang sollte auch eine Trennung von Funktionen zum Zugriff auf Daten besprochen werden, damit keine Konzentration an Administrationsrechten und damit ein Sicherheitsrisiko entsteht.

Ein weiterer Punkt, welcher die Einführung einer SmartCard in einer Universität behindern kann, ist die Dimension eines solchen Vorhabens. Es ist aus meiner Sicht immer sinnvoll, nicht sofort die gesamte mögliche Bandbreite an Applikationen auf der Karte zu integrieren. Die Struktur der Chips (kontaktlos & kontaktbehaftet) und auch der Magnetstreifen oder andere Datenträger bieten die Option, Dienste schrittweise zu integrieren. Es kann z.B. problemlos zuerst nur der kontaktlose Teil genutzt werden und später die IT-Applikationen zu integrieren. Voraussetzung dafür ist allerdings eine detaillierte und realistische Planung im Vorfeld (z.B. muss der kontaktbehaftete Chip direkt bei der Beschaffung auf der Karte implementiert werden), die eine Erweiterung der Applikationen auf der Karte berücksichtigt.

Die umfassende Einführung einer SmartCard mit vielen Applikationen wirft das Problem der Konsolidierung der Datenbestände auf, die für die Personalisierung der Karte notwendig sind. Im Üblichen existieren bei den Anwendern zu jeder Applikation spezifische Nutzerdatenbanken, die teilweise die gleichen Daten (Name, Vorname, Matrikelnummer,...) enthalten. Diese Datenbanken müssen abgeglichen werden, damit bei einer notwendigen Sperrung einer Chipkarte auch die Benutzerkonten in den Hintergrundsystemen gesperrt werden können. Besondere Aufmerksamkeit bei der Einführung einer solchen Karte muß also auf das Thema Chipkartenmanagement gelegt werden.

Die aufgeführten Punkte sind Beispiele für mögliche Probleme, die bei der Einführung der Chipkarte auftreten können. In den meisten Fällen können diese jedoch durch eine gute Projektvorbereitung und Projektstruktur bereits ausgeräumt werden. Andere Punkte sind dadurch vermeidbar, indem ein Auszug aller Verantwortlichen und Anwender zeitgleich und gleichberechtigt in die Entscheidungen einbezogen werden, sich aktiv in den Projektverlauf einbringen und alle notwendigen Daten offengelegt werden.

6 Ansatz einer Vorgehensweise bei der Einführung einer SmartCard

Im folgenden soll abschliessend ein Vorschlag für die Vorgehensweise bei der Einführung einer multifunktionalen Chipkarte erläutert werden, der sich bei bisherigen Projekten bewährt hat.

6.1 Spezifizierung der Chipattribute der Karte

Im ersten Schritt muss diskutiert werden, welche Dienste in welcher zeitlichen Reihenfolge (kurz, und mittelfristig 2-5 Jahre) auf die Karte gelegt werden. Die Applikationen auf der Karte ziehen sehr oft auch Anpassungen an vorhandenen Hintergrundsystemen nach sich, die zu diesem Zeitpunkt abgeschätzt und budgetiert werden müssen. An diesen Applikationen kann in einem nächsten Schritt festgelegt werden, welcher Dienst auf welchem Datenträger untergebracht werden soll. Dabei sollten z.B. vorhandene Chipkartensysteme auf eine Migration überprüft werden. In den meisten Fällen sind vorhandene Magnetstreifensysteme kostengünstig auf kontaktlose Technologien umzustellen. Bei der Auswahl der Hersteller für die einzelnen Datenträger auf der Karte spielt insbesondere bei den Kryptochips die Treiberunterstützung für die Standardschnittstellen (PKCS# XX, CSP) sowie die vorhandene Einbindung in Applikationen z.B. zur Anmeldung an Betriebssysteme eine wesentliche Rolle.

6.2 Design der Karte

Eine nicht zu unterschätzende Aufgabe stellt die Gestaltung der optischen Merkmale der Karte dar. Nachdem die Datenträger festliegen, deren Position auf dem Kartenkörper genormt ist, geht es hier um die variablen Grössen wie Lichtbild, Name etc. Hierbei fließen Meinungen der Werbeträger, Mitbestimmungsgremien der Nutzer (Personalrat, asta) aber auch technologische Beschränkungen ein. Bei einer Herstellung der Kartengrundlayouts durch einen Kartenproduzenten ist das gewünschte Design hinsichtlich der Farbechtheit zuprüfen. Eine Sicherheit bringt hier die Fertigung von Testkarten gemäß dem festgelegten Kartenlayout. Zu berücksichtigen ist, daß die Abstimmung und Prüfung dieser Maßnahmen sehr oft die Zeit von mehreren Monaten in Anspruch nehmen kann.

6.3 Personalisierungs- und Chipkartenverwaltungssystem

Sind die o.g. Punkte festgelegt, ist die zentralste Komponente einer Chipkarteninfrastruktur, das Personalisierungs- oder Chipkartenverwaltungs-
system zu definieren. Als Eingangsgrössen dienen hier die evtl. vorhandenen und einzubindenden Systeme der Datenlieferanten und die zu personalisierenden Datenträger. An dieser Stelle muss der Prozess der Personalisierung für die Erstausgabe und für den Dauerbetrieb festgelegt werden. Wichtig sind hier nicht nur neu auszugebende Karten sondern auch die Behandlung von Änderungen (z.B. Namenswechsel) oder notwendige Vorgänge zur Sperrung einer Karte in allen Systemen. Wird zusätzlich eine Public Key Infrastruktur geplant, müssen Punkte wie zweifelsfreie Identifizierung des Antragstellers von Zertifikaten oder der Transport der PIN festgelegt werden.

6.4 Spezifizierung Pilot

Mit den Ergebnissen der obigen Punkte kann ein erster Pilot, der nur eine kleine Benutzergruppe und einige Applikationen umfassen sollte, durchgeführt werden. Besonderes Augenmerk sollte hier auf den Rollout-Prozessen der SmartCard liegen.

Nach erfolgreichem Abschluss des Piloten kann die Einführung der Chipkarte geplant werden. Dabei ist sicherlich der Semesterwechsel in den Universitäten und das Einschreiben der Studenten in das neue Semester ein effektiver Zeitpunkt. Dabei können sowohl bereits Studierende als auch neue Studenten Ihren Studentenausweis erhalten. Aufgrund von Lieferzeiten von zwischen 2-4 Monaten bei Chipkarten in größeren Stückzahlen ist die Erstausgabe von Ausweisen langfristig zuplanen.