

DIE SCHULSERVICEKARTE

EINSATZ EINER SMART CARD ALS AUSWEIS IN SCHULEN

HTBLA Weiz
DI. Wolfgang Haidvogel
Dr. Karl Widdmannstraße 40
A 8160 Weiz

Version 2.0.0

Revisionsgeschichte

13.03.03 Version 1.0.0: Erster Entwurf
09.11.03 Version 2.0.0: Ergänzung der Feldlängen bei den Chipdaten,
Anpassung der Daten an die in der Zwischenzeit realisierte Karte

EINSATZ EINER SMART CARD ALS AUSWEIS IN SCHULEN

Für den Einsatz einer Smart Card als elektronischen Schüler-, Lehrer- und Verwaltungspersonalausweis (Schulservicekarte) mit persönlichem Security Token sind folgende Qualitäten zu betrachten:

OBERFLÄCHE

Grundsätzlich ist von mindestens drei unterschiedlichen Kartentypen auszugehen, die rein optisch leicht unterscheidbar sein sollten – etwa durch die Farbgebung einer Kartenseite – vorzugsweise jener Seite die nicht den Chipkontakt trägt – hier als Vorderseite bezeichnet. Die sogenannte Chipseite könnte in der Hoheit der Schulverwaltungen liegen und von diesen individuell gestaltet werden. Ein Unterschriftsfeld kann auf dieser Seite vorgesehen sein.

Die drei Kartentypen:

- Schülersausweis
- Lehrerausweis
- Verwaltungsausweis

Da die Karte auch als Sichtausweis verwendbar sein muss, muss die Oberfläche zum nachträglichen Aufbringen von Daten, auf den mit dem Basislayout bereits vorgesehenen Kartenrohling, geeignet sein. Dies ist bei der Definition der Qualität der Kartenoberfläche zu berücksichtigen. Das übliche Verfahren zum Aufbringen solcher individuellen Daten ist das Thermotransfer- bzw. Thermosublimationsverfahren.

SCHÜLER AUSWEIS

Folgende Daten sollten auf diese Weise fix auf eine Schülerkarte aufgebracht werden, wobei hier von der Vorderseite auszugehen ist:

- Name und Adresse der Schule
- Eindeutige Ausweisnummer, bestehend aus Schulkenzahl und einer den Ausweisinhaber eindeutig kennzeichnenden Zahl (z. B. die verschlüsselte Sozialversicherungsnummer)
- Akadem. Grad
- Vorname(n)
- Nachname
- Geburtsdatum
- Lichtbild

Um eine Verwendbarkeit des Ausweises über einen längeren Zeitraum zu gewährleisten ist für veränderliche Daten ein wiederbeschreibbarer Bereich vorzusehen – die Technologie, die hier vorgeschlagen wird, ist ein sogenannter Thermochromicstreifen.

Dieser wiederbeschreibbare Bereich sollte Platz für folgende Informationen bieten:

- Gültigkeitsdatum
- Klasse oder Jahrgang
- Infozeilen (mind. 4 Stück, z.B. für die Eintragung von Linien der Verkehrsmittel für die Schülerfreifahrt)

Es ist davon auszugehen, dass die Ausgabe und das Aufbringen der veränderlichen und der fixen Daten auf eine Karte von den einzelnen Schulen eigenverantwortlich (selbst oder outgesourct) durchzuführen sein wird, da diese ja die Hoheit über die Schülerdaten

haben. Um diese Rolle so einfach wie möglich zu gestalten sollte die Karte in einem höchstmöglichen Fertigungsgrad vorgefertigt werden.

LEHRER-/VERWALTUNGS AUSWEIS

Folgende Daten sollten auf diese Weise fix auf eine Schülerkarte aufgebracht werden, wobei hier von der Vorderseite ausgegangen wird:

- Name und Adresse der Schule
- Eindeutige Ausweisnummer, bestehend aus Schulkennzahl und einer den Ausweisinhaber eindeutig kennzeichnenden Zahl (z. B. die verschlüsselte Sozialversicherungsnummer)
- Amtstitel
- Akadem. Grad
- Vorname(n)
- Nachname
- Lichtbild

Da auf diesen Ausweisen keine dynamisch veränderbaren Daten vorgesehen sind, kann auch der wiederbeschreibbare Thermochromicstreifen entfallen.¹ Diese Karten können auch als sogenannte Hybridkarten mit einem zweiten Chip, der kontaktlos arbeitet, ausgestattet werden. Damit sind Zutrittskontrollen u. ä. für den Benutzer komfortabler zu gestalten.

DATENAUSTAUSCH

Die Personalisierung der Karten, d. h. Bedrucken den unveränderlichen Daten und das Schreiben der Daten in den Chip kann in der jeweiligen Schule oder außerhalb (andere Schule, sonstiger Dienstleister) erfolgen. Zum einfacheren elektronischen Datenaustausch zwischen den Beteiligten wurde ein Dateiformat erarbeitet.

HARDWARE

Als Hardwareplattform werden grundsätzlich sogenannte „Security Controller“ eingesetzt, die sich dadurch auszeichnen bereits auf Hardwareebene bestimmte Schutzmechanismen implementiert zu haben – z.B. ein Metal Shield. Diese Eigenschaften sind wesentlich in der Auswahl für eine sichere Smart Card basierende Lösung, da nur durch die ausgewogene Kombination von Hardware und Software ein ausgewogenes Schutzniveau zu erreichen ist.

Neben diesen Mechanismen sind auch einige Grundfunktionalitäten als Hardwareimplementierungen wichtig, um überhaupt für einen solchen Anwendungsfall einsetzbar zu sein – dies sind unter anderem:

- Smart Card entsprechend der Norm ISO 7816
- Möglichkeiten zur (sicheren) digitalen Signatur und Verschlüsselung mit Schlüsselgenerierung auf der Chipkarte
- PIN zum Verifizieren des Benutzers
- Filesystem und Befehlssatz nach ISO 7816 - 4
- Vergabe von individuellen Schreib/Leserechten für jeden Datensatz mit entsprechend strengen Authentisierungsmethoden, wie z. B. eine Terminalkarte

¹ Die exakte Gestaltung einer Karte solchen Schulservicekarte wurde inzwischen festgelegt: Layout-Spezifikation elektronischer Schülerservicekarte vom 18.08.2003, HTBLA Spengergasse, Ing. Walter Weiß.

APPLIKATIONEN

Vor allem bei der Auswahl des Kartenbetriebssystems ist zu berücksichtigen, dass eine größtmögliche Flexibilität beim Einrichten von Applikationen auf der Smart Card gegeben ist. In der Regel ist darunter das Einrichten von Datenstrukturen im Speicher des Kartencontrollers zu verstehen. In seltenen Fällen bedeutet dies auch das Nachladen von ablauffähigem Code, falls eine Applikation zum Beispiel ein spezielles Kommando, das vom Betriebssystem in seiner Standardausprägung nicht geboten wird.

Zu berücksichtigen ist dabei auch der Aspekt der Wechselwirkung mit der Terminalumgebung. Dies ist z.B. bei der Geldbörsenapplikation Quick der Fall, die eine seitens der Europay akzeptierte Umgebung, sowohl auf der Karte, als auch im Terminalbereich voraussetzt.

Die heute vorgesehenen Applikationen sind:

IDENTIFIKATION

Die auf der Kartenoberfläche vermerkten Daten sind zwecks elektronischer Verarbeitbarkeit auch im Chip gespeichert. Auch diese Daten sind in der Zwischenzeit in einer Zusammenarbeit zwischen dem Autor und den Firmen Austria Card und APSS (Austrian Payment System Services) definiert und spezifiziert.² In Klammer sind die jeweiligen Feldlängen angeführt.

Im öffentlichen Bereich der Karte

- 1) Unveränderliche Daten
 - a) Versionskennung (1)
 - b) Schulkenzahl (7)
 - c) Ausstellungsdatum (8)
 - d) Personal- oder Schülernummer (16)
 - e) Personengruppe (Schüler, Lehrer, Verwaltungspersonal) (1)
 - f) Laufende Nummer (wegen Verlust) (1)
 - g) Amtstitel (30)
 - h) Akademischer Grad (30)
 - i) Vorname (40)
 - j) Nachname (40)
 - k) Geburtsdatum (8)
- 2) Veränderliche Daten
 - a) Klasse bzw. Jahrgang (10)
 - b) Gültigkeitsdatum Beginn (8)
 - c) Gültigkeitsdatum Ende (8)
 - d) Flags für diverse Berechtigungen, die Offline verfügbar sein sollen (8)
- 3) Daten für den Fahrausweis
Dieser Datensatz ist noch zu definieren, insgesamt 2 Dateien mit 256 Bytes sind auf der Karte vorzusehen.
- 4) Zur freien Verfügung der einzelnen Schule
Z. B. für spezielle Login- Daten für das schuleigene Netz. Zwei Dateien mit je 256 Bytes
- 5) Datenbereich für Partner
Noch näher zu spezifizieren. Ein Datenbereich mit 200 Bytes, in dem Partnern, Sponsoren u. a. die Möglichkeit gegeben werden kann, Daten zur Verfügung zu stellen.

² APSS: Spezifikation Kundenkarte, Projekt Schülerkarte Version 1.2 vom 14.07.2003

- 6) Datenbereich für den Karteninhaber
Drei Dateien mit je 1024 Bytes zur Verfügung des Karteninhabers, Zugriff geschützt mit eigenen PINs für das Lesen und Schreiben.

Im geschützten Bereich der Karte

- Zertifikate
- Privater Schlüssel

Diese Daten werden während des Personalisierungsvorgangs auf dem Chip geschrieben.

AUTHENTISIERUNG

Wie bereits in einem eigenen Kapitel dargestellt ist für den Zugang zu einem Web Portal (der Schule oder des Ministeriums) eine (sichere) Authentisierung erforderlich. Je nach Sicherheitsanforderungen können hier unterschiedliche Methoden zur Authentisierung und Autorisierung vorgesehen werden.

DIGITALE SIGNATUR

Die digitale Signatur beruht primär auf zwei Grundfunktionalitäten einer Smart Card:

- Berechnung eines Hash Wertes
- Verschlüsseln dieses Hash Wertes mit dem privaten Schlüssel, der dem für die Signatur zu verwendenden Zertifikates zugeordnet ist.

Abhängig vom verwendeten Standard (CSP oder PKCS) sind die dafür notwendigen Daten in entsprechenden Datenstrukturen auf der Karte gespeichert.

VERSCHLÜSSELUNG

Die Verschlüsselung von Daten beruht im Kontext einer Zertifikats- und Smart Card basierenden Lösung auf sogenannten Hybridverfahren, da die eigentliche Verschlüsselung der Massendaten immer auf symmetrischer Basis erfolgt. Für die sichere Übertragung dieses meist Sitzungs-individuellen symmetrischen Schlüssels werden asymmetrische Algorithmen verwendet (der symmetrische Schlüssel wird mit dem Public Key des Empfängers verschlüsselt). Zum Entschlüsseln dieses für die Entschlüsselung der Massendaten notwendigen Schlüssels beim Empfänger wird die Smart Card verwendet, da nur diese den Private Key des Empfängers kennt und anwenden kann.

DOMÄNEN LOGIN

Smart Card Leser an jedem PC der Schule zum Login. Kerberos V5 ist als Standard anzustreben, im Bereiche der Schulen sind (übergangsweise) Verfahren vorzusehen, die von den EDV-Kustoden einfach administrierbar sind.

ZUTRITTSKONTROLLE

Um den Zugang zu diversen Räumlichkeiten, die nicht jedermann zugänglich sein sollen, zu regeln werden an den Eingängen zu diesen Räumlichkeiten Chip Karten Lesegeräte installiert, die die Berechtigung einer Person/Karte prüfen und gegebenenfalls den Zugang freigeben oder nicht. Dabei können sowohl kontaktbehaftete wie auch kontaktlose Chipkarten zum Einsatz kommen.

ENTLEHNUNG

Zur Dokumentation der Entlehnung von schuleigenen Geräten, Büchern u. ä. wird diese Applikation eingesetzt, wobei die Verwaltung der entliehenen Gegenstände außerhalb der Karte stattfindet. Bei der Bibliotheksapplikation ist eine Schnittstelle mit einem ISBN-Barcodeleser und der Bibliothekssoftware vorzusehen.

„SCHUL-GELDBÖRSE“

Hier sind mehrere Systeme, je nach Anwendungsfall, auch im parallelen Einsatz möglich:

1. Öffentliche Geldbörse (Quick)
Auf der Smart Card befindet sich eine Geldbörse der österreichischen Banken. Sie kann an jedem Bankomat mittels einer zweiten Karte aufgeladen werden und wird im Schulbereich zur Bezahlung von Kopien und div. nicht kostenfreien Dienstleistungen der Schule (Mensa,) eingesetzt.
Die Applikation erfordert eine Bezahlmöglichkeit an jeder Einsatzstelle. Die Bezahlstation ist entweder ein handelsübliches Quickterminal, mit fixen oder variablen Preisen, oder ein geeigneter Chipkartenleser und eine Anbindung ans Internet (Quick im Internet). Damit verbunden ist die hohe Sicherheit der nach Bankstandard erfolgenden Zahlung. Nachteilig sind der recht hohe Aufwand und die Kosten für das Clearing.
2. Private zentrale Geldbörse
Diese Geldbörse ist keine Geldbörse im eigentlichen Sinn, sondern beruht auf einer zentralen Verwaltung von Geldbeträgen eines Schülers auf einem zentralen System. Diese zentrale Verwaltung bietet im Gegensatz zu einer „echten“ Geldbörse wie z.B. Quick den Vorteil einer „Verlustsicherheit“. An den Akzeptanzgeräten wie z.B. Kopierern sind Smart Card Lesegeräte installiert, die die Benutzung erst nach einer erfolgreichen Identifikation, bzw. Authentisierung des Nutzers erlauben. Das Guthaben wird im jeweiligen Gegenwert der Dienstleistung vom Guthabenkonto abgebucht. Das hier verwaltete Geld kann nur innerhalb der Schule benutzt werden, es handelt sich also um eine geschlossenen Geldbörsenlösung. Applikation mit durchschnittlich hohem Aufwand für Technik und Verwaltung.
3. Private Geldbörse auf der Karte
Auf der Smart Card sind mehrere Geldbörsen vorgesehen, die an einer oder mehreren Stellen „gefüllt“ werden können. Sie dienen zum Bezahlen von Kleinbeträgen wie Kopien und Drucken direkt am Kopieren bzw. PC. Einfache Applikation mit geringem Aufwand. In etwa gleichwertig mit 2, allerdings, wie normales Geld, nicht verlustsicher, dafür lässt sich der Weg des Geldes nicht nachverfolgen (Datenschutz).

SERVICE POINT

Ein oder mehrere PCs mit Chipkartenleser und Drucker in entsprechender Bauweise (z. B. als Kiosk) an Plätzen hoher Frequenz (Eingangshalle z. B.). Im Folgende sollen rein exemplarische Einsatzmöglichkeiten angegeben werden:

- 1) Druck von
 - a) Schulbesuchsbestätigungen
 - b) Diversen Formularen
 - c) Druckanforderung von Skripten
 - d)
- 2) Aufladen von privaten Börsen
Banknotenleser und Aufbuchsoftware
- 3) Bezahlung mit Quick von Dienstleistungen im Zusammenhang mit der Schule
 - a) Werkstattkosten

- b) Schikurs bzw. Sommersportwochen
 - c) Elternvereinsbeitrag
 - d)
- 4) Funktionen für die Schulverwaltung
- a) Zeiterfassung für das Hauspersonal
 - b)
- 5) Verlängern der Gültigkeit des Ausweises
Thermochromicdruck der Klassen- und Gültigkeitsdaten.

FAHRTAUSWEIS

- 6) Ein Einsatz des Schüler Card als Fahrtausweis für die Schülerfreifahrt ist vorzusehen. Die Erfordernisse für das wiederbedruckbare Feld und die Daten auf dem Chip müssen, abhängig von den jeweiligen Verkehrunternehmen, definiert werden.