20.06.2002
Michael Dyrna

Hauptseminar im Sommersemester 2002
Entwicklung sicherer Systeme

Anwendungsbeispiel: Smartcard-basierte elektronische Geldbörsen

Diese Ausarbeitung ist im Rahmen eines Vortrags im Seminar „Entwicklung sicherer Systeme“ im Sommersemester 2002 an der Technischen Universität München entstanden.

Sie soll zur Nachbereitung des Seminar-Vortrags dienen. Wer sich noch tiefergehend mit den vorgestellten Inhalten beschäftigen möchte, dem seien besonders folgende Werke empfohlen:

- Wolfgang Rankl, Wolfgang Effing: Handbuch der Chipkarten, Hanser, 1999
- http://www.eurosmart.com/Activities/DownloadArea/Files/CPP9909.pdf
- http://www.commoncriteria.de
- http://www.cepsco.org

Zahlungssysteme unterliegen einer immer fortwährenden Weiterentwicklung; die optimale Lösung, die von Kunden wie Händlern und Dienstleistern gleichermaßen anerkannt ist, ist noch nicht gefunden. Dieses Problem ist sicherlich ein großes Hemmnis für die Akzeptanz gerade von E-Commerce, weil die Verbraucher den gebräuchlichen Bezahlverfahren (i.d.R. Kreditkarte) nicht vertrauen – aufgrund der bestehenden Sicherheits-Risiken wohl zurecht. Eine für beiden Seiten adäquate Lösung sind smartcard-basierte elektronische Geldbörsen, die ein sehr viel höheres Maß an Sicherheit bieten und die Gegenstand dieser Arbeit sind.

I. Zahlungsverkehr mit Karten

1. Chipkarten

Eine Chipkarte ist eine Karte aus Kunststoff in einem genormten Format, in deren Körper eine integrierte Schaltung versteckt ist, die über Elemente zur Datenübertragung, zum Speichern von Daten und zur Verarbeitung von Daten verfügt. Die Datenübertragung kann dabei entweder über Kontakte an der Oberfläche der Karte erfolgen oder kontaktlos durch elektromagnetische Felder.

Die Chipkarte bietet gegenüber der Magnetstreifenkarte (z.B. EC-Karte, heute verbreitete Kreditkarten) eine Reihe von Vorteilen. So ist zum Beispiel die maximale Speicherkapazität von Chipkarten

um ein vielfaches größer als bei Magnetstreifenkarten: Es werden bereits Schaltkreise mit mehr als 32 kB Speicher angeboten, während man auf dem Magnetstreifen nur rund 1000 Bit speichern kann.

Einer der wichtigsten Vorteile liegt jedoch darin, dass die in der Chipkarte gespeicherten Daten gegen unerwünschten Zugriff und gegen Manipulation geschützt werden können. Da der Zugriff auf die Daten nur über eine serielle Schnittstelle erfolgt, die vom Betriebssystem und einer Sicherheitslogik gesteuert wird, ist es möglich, geheime Daten in die Karte zu laden, die niemals mehr von außen gelesen werden können. Diese Daten können dann nur noch vom internen Rechenwerk des Chips verarbeitet werden. Grundsätzlich können die Speicherfunktionen Schreiben, Löschen und Lesen sowohl per Hardware als auch per Software eingeschränkt und an bestimmte Bedingungen geknüpft werden. Dies ermöglicht die Konstruktion einer Vielzahl von Sicherheitsmechanismen, die auf spezielle Anforderungen der jeweiligen Anwendung maßgeschneidert werden können.

Weitere Vorteile der Chipkarten liegen in der hohen Zuverlässigkeit und Lebensdauer im Vergleich zur Magnetstreifenkarte, deren Umlaufzeit im allgemeinen auf ein bis zwei Jahre begrenzt ist.

Chipkarten werden in Speicherkarten und Mikroprozessorkarten eingeteilt. Gemeinsam ist beiden, dass die Datenübertragung mit der Außenwelt über einen seriellen I/O-Port abläuft.

Eine Speicherkarte besteht im wesentlichen aus einem Speicher (meist ein EEPROM, electrical erasable read only memory) und einer Sicherheitslogik. Im Speicher werden die für die Anwendung erforderlichen Daten abgelegt. Die Sicherheitslogik, welche im einfachsten Fall nur aus einem Schreib- und Löschschutz für den Speicher oder einzelnen Bereichen des Speichers besteht, kontrolliert den Zugriff auf den Speicher. Es gibt aber auch Speicherchips mit einer komplexeren Sicherheitslogik, die auch einfache Verschlüsselungen durchführen können.

Das Herz des Chips einer Mikroprozessorkarte ist der Prozessor und der Speicher: Ein ROM, ein EEPROM und ein RAM. Das ROM enthält das Betriebssystem des Chips und wird während der Herstellung eingebrannt. Das EEPROM ist der nichtflüchtige Speicher des Chips, in dem Daten oder auch Programmcode unter Kontrolle des Betriebssystems geschrieben und gelesen werden können. Das RAM ist der Arbeitsspeicher des Prozessors. Dieser Speicherbereich ist flüchtig, und alle darin enthaltenen Daten gehen verloren, wenn die Spannungsversorgung des Chips abbricht (i.a. weil die Chipkarte aus dem Kartenleser gezogen wird).

Chipkarten finden Anwendung u.a. im Zahlungsverkehr, als SIM-Karte zur Authentifikation eines Mobilfunkteilnehmers in GSM, als Telefonkarte zur Speicherung und Verarbeitung eines vorbezahlten Guthabens, als Krankenversicherungskarte zur Speicherung der Versicherungsdaten oder als Karte zur Speicherung von privaten Schlüsseln beispielweise zur Realisierung einer digitalen Signatur.

2. Chipkarten im Zahlungsverkehr

In den letzten Jahren haben sich Chipkarten im Bereich des elektronischen Zahlungsverkehrs etabliert. Das Markspotenzial dieses Bereichs ist aufgrund der sehr hohen Stückzahlen enorm.

Chipkarten bieten sich aufgrund ihrer Eigenschaften hervorragend für den Bereich des Zahlungsverkehrs an: Im Chip können problemlos und manipulationssicher Daten aufbewahrt werden. Die Handhabung ist aufgrund der Größe und Robustheit der Karten ohne Probleme möglich. Durch ihre Rechenfähigkeit ist es möglich, völlig neue Wege im Zahlungsverkehr zu gehen. Dies sieht man sehr deutlich bei elektronischen Geldbörsen in Form von Chipkarten, die einzig und allein mit diesem Medium realisierbar sind.

Die Vorteile von Chipkarten zur Abwicklung von Zahlungsverkehr liegen für Banken und Händler darin, dass sich die Kosten für die Bargeldbearbeitung reduzieren. Durch offline arbeitende elektronische Geldbörsen entfallen weitestgehend die Datenübertragungskosten für die Transaktionen. Das Risiko durch Raub und Vandalismus sinkt, da bei elektronischen Zahlungssystemen kein Bargeld mehr durch Diebe gestohlen werden kann. Desweiteren ist der schnellere Bezahlvorgang ein stichhaltiges Argument, da dadurch Optimierungen im Kassenbereich möglich werden. Auch kann man einfachere und billigere Automaten bauen, da die Geldschein- und Münzprüfeinheit nicht mehr benötigt wird.

Auch der Kunde hat durch diese Bezahlart Vorteile, wenn auch weniger: So fällt zum einen das Problem mit nicht vorhandenem Kleingeld weg, und zum anderen ist so ein schnelleres Bezahlen an Automaten möglich.

3. Kredit-, Debitkarte und elektronische Geldbörse

Es gibt drei grundsätzliche Modelle für den elektronischen Zahlungsverkehr in Verbindung mit Chipkarten: Kreditkarten, bei denen *nach* Inanspruchnahme der Leistung bezahlt wird („pay later“), Debitkarten, bei denen *bei* Inanspruchnahme der Leistung behalt wird („pay now“), und elektronische Geldbörsen, welche vorbezahlt sind („pay before“).

(a) Kreditkarten

Wenn man mit Kreditkarte (z.B. VISA, Mastercard) zahlt, wird der dazugehörige Betrag nach einiger Zeit vom Konto abgebucht. Die dabei entstehenden Kosten trägt der Händler. Sie sind in der Regel umsatzabhängig und bewegen sich in der Größenordnung von zwei bis fünf Prozent des Kaufpreises.

Da für Kreditkarten weitestgehend Magnetstreifenkarten verwendet werden, ist die Fälschungssicherheit sehr gering: Das Kopieren der Daten auf dem Magnetstreifen auch eine andere Karte ist relativ unkompliziert möglich. Als zusätzliches Sicherheitsmerkmal dient nur die Unterschrift des Kunden und dir Möglichkeit, die Karte sperren zu lassen, wenn man ihren Verlust bemerkt.

Der Vorteil für den Händler liegt darin, dass er vom herausgebenden Unternehmen der Kreditkarte eine Zahnungsgarantie für die abgerechneten Umsätze hat. Die Kosten durch Betrug scheinen im Moment noch nicht „hoch genug“ zu sein, als dass die Kreditkartenunternehmen auf Chipkarten umstellen würden.

(b) Debitkarten

Vor allem in Deutschland sind Debitkarten (z.B. EC-Karte) sehr verbreitet. Die Karten ermöglichen es, unmittelbar bei dem Bezahlvorgang dem Händler oder Dienstleister den Betrag zu überweisen. In der Regel wird sowohl bei Debit- als auch bei Kreditkarten der eigentliche Bezahlvorgang bei höheren Geldbeträgen über eine Bonitätsanfrage bei einem Hintergrundsystem autorisiert.

Mit der Fälschungssicherheit verhält es sich genauso wie bei den Kreditkarten.

Der Vorteil für Händler und Kunden liegt in den geringeren Kosten, weil keine weiteres Unternehmen außer der Bank am Bezahlvorgang beteiligt wird.

(c) elektronische Geldbörse

Bei elektronischen Geldbörsen (z.B. Geldkarte) wird vor dem Bezahlvorgang elektronisches Geld (electronic value, EV) auf die Karte geladen. Dieses wird vom Karteninhaber beim Laden in bar oder mit einem bargeldlosen Verfahren erhoben. Beim eigentlichen Bezahlvorgang wird der Saldo in der Karte des Kartenbenutzers erniedrigt und parallel in der elektronischen Geldbörse des zweiten Beteiligten (i.d.R. Händler oder Dienstleister) erhöht. Dieser reicht dann die erhaltene elektronische Geldsumme beim Börsenbetreiber ein und erhält daraufhin den entsprechenden Geldbetrag.

Das Verfahren hat für den Kartenbenutzer drei erhebliche Nachteile: Beim Aufladen der Karte erhält er für „echtes“ Geld elektronisches Geld. Wirtschaftlich betrachtet, gibt er dem Börsenbetreiber also einen zinslosen Kredit, da er sein elektronisches Geld erst später verbraucht, das echte Geld aber sofort in den Besitz des Börsenbetreibers übergeht. In der Summe der vielen Kartenbenutzer ist das für den Betreiber eine erhebliche Zusatzeinnahme.

Ein schwerwiegender Nachteil wäre gegeben, wenn der Börsenbetreiber in Konkurs ginge, dann kann es nämlich passieren, dass das aufgeladene elektronische Geld wertlos wird. Bei „echtem“ Geld dagegen wird der Gegenwert vom Staat garantiert. Als Folge sind in einigen Staaten deshalb Bestrebungen im Gange, die dass diese Art von Karten nur von Banken oder ähnlichen Instituten ausgegeben werden dürfen, die eine Sicherheitsleistung bei einer staatlichen Stelle hinterlegen, damit bei einem Konkurs der umlaufende Betrag gedeckt ist.

Der dritte nennenswerte Nachteil für den Benutzer liegt im Verluste des elektronischen Gelds bei Defekt der Chipkarte. Falls diese anonym ist, besteht auch für den Börsenbetreiber keine Möglichkeit, den letzten gespeicherten Betrag herauszufinden, und das elektronische Geld wäre genauso wie Bargeld einfach verloren. Die Robustheit eines Chips ist verständlicherweise geringer als die von Scheinen und Münzen. In der Praxis gehen die Börsenbetreiber meist einen Kompromiss ein: Da der Börsenstand bei der letzten Online-Aufladung bekannt ist, kann man den in der Börse befindlichen Betrag ungefähr abschätzen und dem Kunden erstatten.

4. Offene vs. geschlossene Systemarchitektur

Man muss bei elektronischen Zahlungssystemen zwischen offenen und geschlossenen Architekturen unterscheiden. Ein offenes System steht grundsätzlich mehreren Anwendungsbetreibern zur Verfügung und kann für den allgemeinen Zahlungsverkehr zwischen verschiedenen Instanzen verwendet werden. Im Gegensatz dazu lässt sich ein geschlossenes System nur für Bezahlungen bei einem einzigen Systembetreiber benutzen.

Am Beispiel einer Telefonkarte mit Speicherchip sei die technische Seite hier kurz verdeutlicht. Bei Speicherkarten werden bei der Bezahlung lediglich irreversible Zähler dekrementiert. Es ist dazu nicht notwendig, in die Terminals eine genaue Buchführung über die Anzahl der herabgezählten Einheiten zu betrieben. Es muss lediglich sichergestellt sein, dass der Zähler in der Karte bei einer Inanspruchnahme der Leistung (also beim Telefonieren) auf jeden Fall herabgezählt wird. Das Terminal ist damit also eine Art „Maschine zur Vernichtung von elektronischen Geldeinheiten“. Natürlich wird man in der Praxis für jedes Terminal einen Saldo führen, doch werden die abgebuchten Einheiten nur innerhalb des Börsenanbieters verrechnet. Ein Betrug bei der Verrechnung der Einheiten zwischen Terminalbesitzer und Börsenbetreiber ist damit von Grundsatz her nicht möglich, da beide der gleichen Institution angehören. Der große Nachteil für den Benutzer besteht darin, dass er für jedes System, dass er benutzen und mit einer Geldbörse bezahlen möchte, eine eigene Karte benötigt.

Im Gegensatz dazu können bei offenen Systemen Terminalbesitzer und Börsenbetreiber unterschiedliche Firmen sein. Der Benutzer benötigt also nur eine einzige Karte, mit der er viele verschiedene Dienstleistungen in Anspruch nehmen kann. Der Börsenbetreiber muss bei der Abrechnung der Terminalumsätze prüfen können, ob diese korrekt und nicht manipuliert sind. Dies muss im Systemkonzept von Anfang an berücksichtigt werden – i.d.R. durch sichere Transaktionen –, da sonst eine Abrechnung des Terminalbesitzers mit dem Börsenbetreiber sehr schwierig oder gar unmöglich ist.

5. Zentrale vs. dezentrale Systemarchitektur

Der Systemaufbau von elektronischen Zahlungsverkehrssystemen mit Chipkarten kann sowohl zentral als auch dezentral sein. Bei einer zentralen Systemarchitektur wird jede Bezahlung direkt und online mit dem Hintergrundsystem ausgeführt. Bei einer dezentralen Architektur werden Transaktionen nur vor Ort durchgeführt, und die Terminals können über lange Zeit offline, d.h. ohne Verbindung mit dem Hintergrundsystem, arbeiten.

Gerade im Zahlungsverkehr ist die Systemsicherheit der wichtigste Aspekt. Deshalb tendiert man oft zu einem zentral aufgebauten System, weil damit der Systembetreiber alle Fäden in der Hand hat. Kommt allerdings keine Kommunikationsverbindung zustande, so ist auch die Bezahlung nicht möglich. Ein zentral betriebenes System hat aber trotzdem einige Vorteile: Die eingehenden Transaktionen können beispielsweise unmittelbar und in Echtzeit mit der aktuellen Sperrliste verglichen werden. Schlüsselwechsel und Software-Updates für Terminals und Chip-Karten lassen sich direkt am Hintergrundsystem ohne Zeitverzögerung durchführen.

Diesen Vorteilen stehen aber auch größere Nachteile gegenüber. In vielen Ländern sind die Telekommunikationsgebühren so hoch, dass es sich für einen Händler nicht lohnt, eine Standleitung zum Hintergrundsystem einzurichten oder für jede Transaktion über eine Wählverbindung Kontakt aufzunehmen. Ebenfalls ist die Ausfallsicherheit des Telefonnetzes in manchen Gegenden nicht auf einem Niveau, das zu jedem beliebigen Zeitpunkt eine Online-Verbindung zu einem übergeordneten Computer zulässt.

Aufgrund ihrer aktiven Natur eignen sich Chipkarten hervorragend für dezentrale Systeme, da sich in ihnen ein Teil der Systemsicherheit vor Ort befindet. Dies ist auch der große Vorteil gegenüber passiven Magnetstreifenkarten, die keinerlei Abläufe im System erzwingen können.

Gerade der Einsatz von elektronischen Geldbörsen im Automatenbereich erfordert zwangsweise ein dezentrales System, da diese teilweise über Wochen und Monate völlig autark arbeiten und keinerlei Möglichkeit besteht, zu einem vorhandenen Kommunikationssystem Kontakt aufzunehmen. Dazu kommt das wesentlich günstigere Verhalten in bezug auf Ausfallsicherheit: Fällt das Hintergrundsystem aus, dringen die Auswirkungen meist überhaupt nicht bis zu den Händlerterminals vor.

Aber auch dezentrale System haben Nachteile, und die liegen vor allem im Bereich der Systemverwaltung. Für die Systemsicherheit ist es unabdingbar, dass die Terminals immer mit der aktuellen Sperrliste arbeiten. Dies ist einer der Gründe, warum es üblich ist, dass Terminals in vielen Systemen mindestens einmal pro Tag eine Online-Verbindung zum Hintergrundsystem aufbauen müssen. Dabei werden die entstandenen Transaktionsdaten zum Hintergrundsystem übertragen und im Gegenzug verschiedene Verwaltungsdaten zum Terminal transferiert, wie beispielsweise neue Software, ein neuer Schlüsselsatz, die aktuelle Sperrliste und Daten zum Laden in der Karte des Kunden.

Oft wählt man in der Praxis einen Mittelweg zwischen beiden Architekturen. Man versucht damit, alle Vorteile zu vereinigen. Dabei geht man folgendermaßen vor: Sowohl Terminal als auch Chipkarte können aufgrund von bestimmten Bedingungen eine Online-Verbindung erzwingen. Kann diese nicht hergestellt werden, so kommt der Zahlungsvorgang nicht zustande. Einige typische Bedingungen sind

die Höhe des zu übertragenden Betrags, die Anzahl der offline ausgeführten Transaktionen, die Zeit seit der letzten Online-Transaktion, Zufall oder die manuelle Aktivierung am Terminal. Diese Bedingungen führen dazu, dass jede Karte regelmäßig eine direkte Verbindung zum Hintergrundsystem aufnimmt. Damit behält der Systembetreiber die Kontrolle. Terminals und Automaten, an denen nur geringe Beträge umgesetzt werden, kann man von den obigen Online-Zwängen ausnehmen, da selbst im Betrugsfall dabei nur geringer Schaden entstehen kann und man sich dafür den Anschluss an ein Kommunikationsnetz spart.

6. Grobe Systemstruktur

Große Zahlungsverkehrssysteme bestehen grundsätzlich aus vier Komponenten, nämlich dem Hintergrundsystem, den Terminals, dem Netzwerk und den Chipkarten.

Das **Hintergrundsystem** besteht aus den Teilen Clearing und Verwaltung. Im Clearing werden alle eingehenden Transaktionen mit den Banken, Händlern und Kartenbesitzern verrechnet. Im Verwaltungsteil werden alle administrativen Abläufe wie die Verteilung von Sperrlisten, Austausch von Schlüsseln und Software-Updates geregelt.

Als Komponente mit dem höchsten Vertrauensgrad dienen **Chipkarten**, entweder als Geldbörse oder als Sicherheitsmodul für die verschiedenen Terminalarten. Ihre Aufgabe ist die Speicherung und der Transport von elektronischem Geld.

Die **Terminals** teilen sich in Lade- und Bezahlterminals auf. Gemeinsam ist beiden eine Kartenleseeinheit. Das Terminal ist somit die Schnittstelle zwischen Chipkarte und Hintergrundsystem.
Das **Netzwerk** verbindet das Hintergrundsystem mit den Terminals. Es kann leitungs- oder paketorientiert sein und ist in der Regel völlig transparent, d.h. es leitet alle Nachrichten unverändert vom Sender zum Empfänger weiter.

II. EN 1546: Branchen-übergreifende elektronische Geldbörse

1. Einführung

Die CEN-Norm EN 1546 legt funktionale und sicherheits-relevante Anforderungen an eine branchenübergreifenden elektronischen Geldbörse (Intersector Electronic Purse and Purchase Device, IEP) fest. Sie wurde von 1991 bis 1998 vom „Comité Européen de Normalisation“ in 6 Personenjahren Arbeit erstellt.

Vollständig beschrieben sind darin alle Komponenten von der Chipkarte über die Terminals mit Sicherheitsmodulen bis zum Hintergrund- und Clearing-System. Sie normt auf etwa 300 Seiten Strukturen, Funktionen, die Sicherheitsarchitektur, Datenelemente, Protokolle und Zustände.

Die Norm ist öffentlich und sehr detailliert. Das hat zwei wichtige Vorteile: Zum einen eignet sie sich dadurch sehr gut, um im Rahmen eines Seminars die Architektur samt allen funktionalen Abläufen

genau zu untersuchen, und zum anderen macht es sie natürlich sicherer als andere Systeme, deren Sicherheit (zumindest teilweise) auf Geheimhaltung von Informationen beruht.

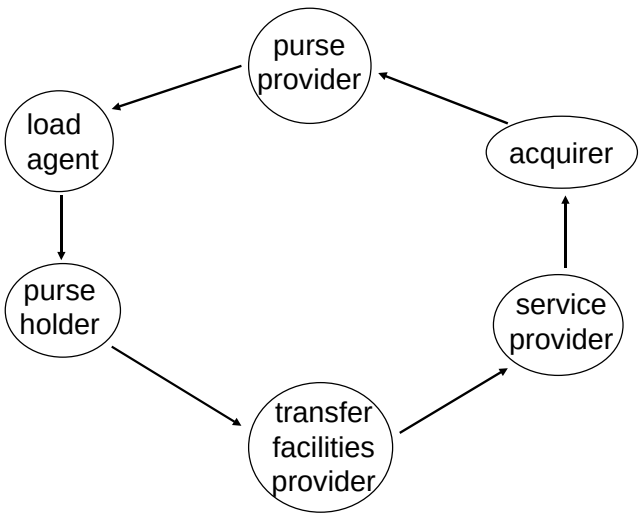
EN 1546 wurde bisher in einigen konkreten Entwicklungen umgesetzt: So hat der Betreiber Danmønt in Dänemark eine dieser Norm entsprechende Geldbörse innerhalb seines bestehenden Systems eingeführt. Weiterhin entsprechen die Geldbörse „Quick“, die sich in Österreich auf allen ausgegebenen EC-Karten befindet, und das weltweit angebotene „VISA Cash“ der Norm.

Das große Potenzial von EN 1546 liegt darin, dass es verschiedenen Betreibern ermöglicht, elektronische Geldbörsen oder Teilkomponenten zu entwickeln, die zueinander kompatibel sind. Dies ist als wesentliche Voraussetzung für den Erfolg eines Zahlungssystems dieser Art zu betrachten. Bei GSM hat die Normung zu europa- und bald weltweiter Verbreitung geführt, während die vielen zueinander inkompatiblen Mobilfunk-Netze in USA beispielsweise keine weite Verbreitung gefunden haben.

Ein Nachteil der Norm darf allerdings auch nicht verschwiegen werden: Sie versteht sich mehr als Rahmenwerk denn als genaue Angabe der verwendeten Bits und Bytes und lässt somit sehr großen Spielraum für die konkrete Implementierung, dass zwei Systeme, die beide auf EN 1546 basieren, nicht zwingen kompatibel zueinander sein müssen. Schon bei der Verwendung von zwei unterschliedlichen Verschlüsselungs-Algorithmen wäre das der Fall.

2. Systembeschreibung

Akteure



Die Pfeile stellen den Fluss des elektronischen Geldes dar.

- Der Börsenbetreiber (purse provider) hat die Gesamtverantwortung (insbesondere für die Sicherheit) und ist der Verwalter des Systems.

- Für den Benutzer der elektronischen Geldbörse wurde der Begriff „Börseninhaber“ (purse holder) festgelegt.

- Der Leistungsanbieter (service provider) ist derjenige, der Leistungen (Waren oder Dienstleistungen) anbietet, die der Benutzer mit seiner elektronischen Geldbörse bezahlt.

- Der Acquirer übernimmt die Errichtung und Verwaltung der datentechnischen Verbindung zwischen Börsenanbieter und Leistungsanbieter. Er kann die von der Zahlungseinrichtung kommenden einzelnen Transaktionen zusammenfassen.

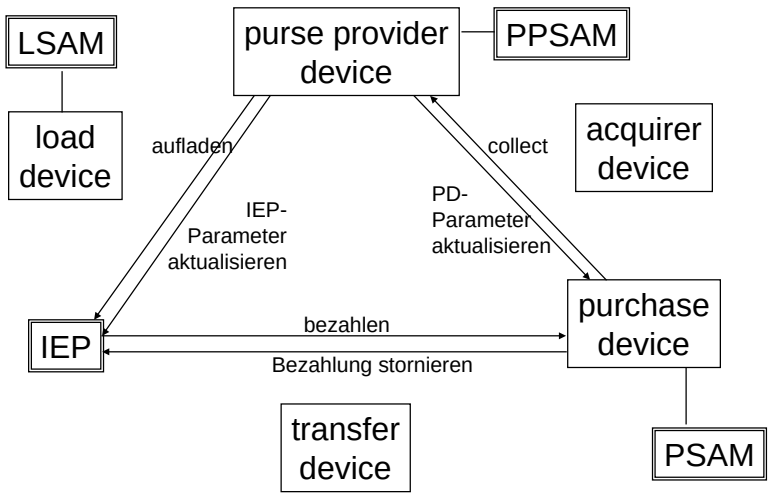
- Der Aufladebevollmächtigte (load agent) kann die Geldbörse gegen Bezahlung aufladen.

- Der transfer facilities provider ist der Anbieter des Telekommunikationsnetzwerks zur Übertragung von Transaktionen. Er muss nur die transparente Datenübertragung garantieren und muss keinerlei Sicherheitsfunktionalität bereitstellen.

Diese sechs Teilnehmer müssen nicht real existieren, sondern sind virtueller Natur. Ihnen sind real existierende technische Komponenten zugeordnet, von denen einige sicher und einige unsicher sind. Die sicheren Komponenten haben die Eigenschaft, dass in ihnen Informationen verarbeitet und gespeichert werden können, ohne dass sie von außen manipuliert werden können. Bei den nicht sicheren ist dies theoretisch möglich. Das Gesamtsystem ist dabei aber so ausgelegt, dass Manipulationen zu keinen Auswirkungen hinsichtlich der Gesamtsicherheit führen.

Aufladeeinrichtung (load device), der Zentralrechner des Börsenbetreibers (EV provider device) und Zahlungseinrichtung (purchase device) sind mit einem Sicherheitsmodul (secure application module, SAM) ausgestattet. Diese Sicherheitsmodule und die Geldbörse selbst zählen zu den sicheren Komponenten.

Komponenten & Funktionen



Die doppelt eingerahmten Module sind sicher. SAM steht für „Secure Application Module“ (Sicherheitsmodul).

- Aufladen (load): Der Geldbörse wird über den load agent ein Betrag elektronisches Geld gutgeschrieben, das der Börsenbetreiber erstellt. Der Börsennutzer bezahlt den Gegenwert in „echtem“ Geld.

- Bezahlen (purchase): Der Geldbörse wird ein Betrag elektronisches Geld abgezogen, während dem purchase device derselbe Betrag gutgeschrieben wird. Der Börsennutzer erhält dafür eine Leistung.

- collect: Einer oder mehrere Beträge elektronisches Geld, das einer Menge von im purchase device gespeicherten Bezahltransaktionen entspricht, wird dem Börsenbetreiber über ein acquirer device übertragen. Der Leistungsanbieter erhält dafür den entsprechenden Betrag „echtes“ Geld.

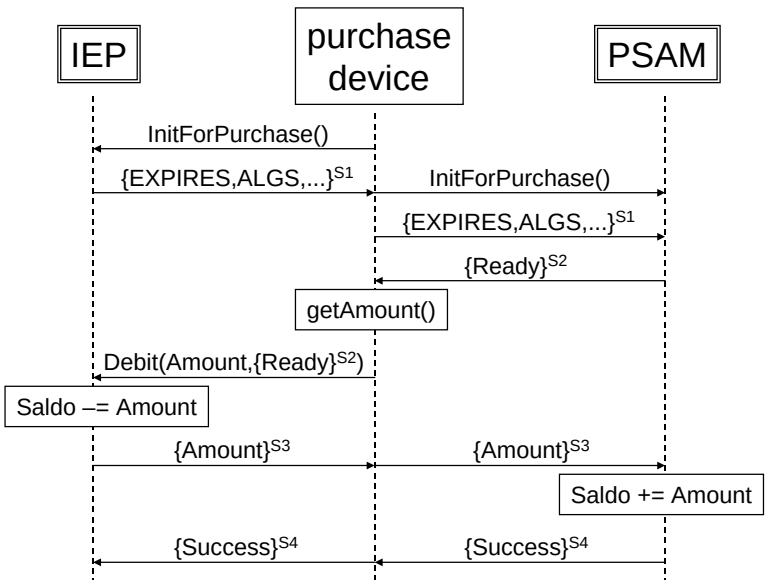
- Bezahlung stornieren (last purchase cancellation): Eine Bezahltransaktion wird rückgängig gemacht. Dazu wird dem purchase device der entsprechende Betrag abgezogen und der Geldbörse gutgeschrieben. Die Transaktion darf noch nicht an den Börsenbetreiber übertragen worden sein, und es muss sich um die unmittelbar letzte Transaktion der Geldbörse handeln.

- IEP-Parameter aktualisieren (update IEP parameters): Interne Parameter der Geldbörse werden durch den Börsenbetreiber aktualisiert. Dabei kann es sich zum Beispiel um Bezahllimits oder Übertragungsschlüssel handeln.

- PD-Parameter aktualisieren (update PD parameters): Internet Parameter des purchase device werden durch den Börsenbetreiber aktualisiert.

Ein wesentliches Paradigma bestimmt alle Funktionen: Der Abzug von elektronischem Geld geht dem Gutschreiben immer voraus, so dass es in keinem Fall möglich ist, durch Manipulation oder Unterbrechen der Datenübertragung zwischen den Komponenten Geld zu erzeugen. Das ungünstigste Ergebnis solcher Eingriffe ist somit die Vernichtung von elektronischem Geld.

Exemplarisch soll nun der (erfolgreiche) Ablauf eines Bezahl-Vorgangs betrachtet werden. Das heißt, auf die Darstellung der Teilabläufe zum Rollback im Fall eines Fehlers wird verzichtet.



An einem Bezahlvorgang sind die elektronische Geldbörse (IEP), das Bezahl-Terminal (purchase device) und das Sicherheitsmodul im Bezahl-Terminal (PSAM) beteiligt.

Nach der Hardware-Initialisierung von IEP und PSAM durch das Terminal, die in der Grafik nicht dargestellt ist, sendet das Bezahl-Terminal ein Initialisierungskommando an die Geldbörse. Nach dem Empfang erhöht die Geldbörse ihren Transaktionszähler, signiert einige Datenelemente wie das Ablaufdatum und die verwendeten Algorithmen mit der Signatur S1 und sendet diese an das Terminal, das sie zusammen mit einem Initialisierungskommando unverändert an das PSAM weiterleitet. Das PSAM prüft die Daten und die Signatur. Nach positiver Überprüfung weiß das PSAM, dass die über-

tragenen Daten unverändert sind und dass die Geldbörse vom Börsenbetreiber autorisiert ist und erhöht ebenfalls seinen Transaktionszähler.

Im nächsten Schritt signiert auch das PSAM einige Datenelemente mit S2 und sendet sie an das Terminal. Das Terminal fragt von außerhalb den zu buchenden Betrag ab und sendet ihn (unsigniert) zusammen mit den mit S2 signierten Datenelementen und dem Kommando „Debit“ an die Geldbörse.

Nach positiver Überprüfung der Signatur und Feststellen eines ausreichenden Saldos erniedrigt die Geldbörse ihren Saldo um den erhaltenen Betrag, signiert den Betrag mit S3 und sendet ihn an das Terminal, das ihn unverändert an das PSAM weiterleitet.

Nach positiver Prüfung der Signatur erhöht das PSAM seinen Saldo um den empfangenen Betrag, signiert einen positiven Return Code mit S4, sendet diesen an das Terminal, das ihn unverändert an die Geldbörse weiterleitet.

Nach Überprüfung von S4 durch die Geldbörse ist die Transaktion beendet.

3. Protection Profile in Common Criteria

Wie in dem Vortrag „Entwicklungsprozess und Konstruktion sicherer Systeme“ erklärt wurde, handelt es sich bei den Common Criteria um einen internationalen Standard zur systematischen Evaluierung von IT-Systemen. Dabei kann es sich bei dem Evaluierungsgegenstand (EVG oder TOE: target of evaluation) um Hardware, konkrete Softwareimplementierungen, eine Kombination aus beidem oder – wie im Fall von EN 1546 – um ein nicht implementiertes System-Design handeln.

EN 1546 ist mit der Evaluierungsstufe „EAL 4“ zertifiziert worden. Das bedeutet, dass die Projektteams, die die Norm erarbeitet haben, die Architektur, die Funktionen und das Sicherheitsmodell „semi-formal“ – also nicht-mathematisch, aber für den Experten plausibel nachvollziehbar – beschreiben mussten. Das Dokument, das diese Beschreibung samt Schlüssigkeitsbeweis für ein nicht-implementiertes Design enthält und als Evaluierungsgrundlage dient, heißt bei Common Criteria „Protection Profile“ (PP, Schutzprofil). (Im Gegensatz zum Protection Profile ist das „Security Target“ (ST) das Dokument, was als Grundlage zur Evaluierung von konkreten Produkten dient.)

Das Protection Profile ist die Beschreibung der Anforderungen an die Funktionalität und Vertrauenswürdigkeit bezogen auf ein Sicherheitsproblem für ein späteres Produkt oder System. Es ist unabhängig von der späteren Implementierung zu verfassen und stellt eine Sammlung von wiederverwendbaren Anforderungen dar. Dies umfasst auch Anforderungen an die Benutzer des Systems.

Da die Sicherheits-Analyse der EN-1546-Norm im nächsten Punkt anhand von Auszügen des sog. „Protection Profile“ durchgeführt werden wird, soll hier zunächst der allgemeine Aufbau und die genauen Inhalte eines PP eingeführt werden.

Aufbau eines Protection Profile

Kapitel 1: Einleitung (PP Introduction)

In diesem Kapitel werden die formalen Aspekte des Protection Profile beschreiben. Neben den Namen, Version der Common Criteria, Verfasser und angestrebte Evaluierungsstufe werden auch Informationen zum Evalierungsstand des PP gemacht. Dieses Kapitel ist wichtig für die Registrierung, hier werden die Kurzzusammenfassung und Stichwörter aufgezeigt, unter denen das PP später schneller zu finden und zuzuordnen ist.

Kapitel 2: Beschreibung des EVG (TOE Description)

In diesem Kapitel wird der Evaluationsgegenstand, d.h. das Produkt, die Produktfamilie oder Systeme, hinreichend genau beschrieben. Dabei ist zu berücksichtigen, dass hier schon auf die Stimmigkeit zur möglichen späteren Aussagen über Einsatzumgebung etc. zu achten ist. Insbesondere müssen hier schon erste Aussagen zu den Grundbedrohungen Verlässlichkeit, Integrität und Vertraulichkeit gemacht werden. Die wichtigen zu schützenden Teile des EVG werden hier angesproch.

Kapitel 3: EVG Einsatzumgebung (TOE Security Environment)

Hier wird die Sicherheitsumgebung des EVG beschrieben, d.h. für den EVG oder die EVGs werden dargestellt:

- Annahmen zur Einsatzumgebung (wie wird der EVG benutzt? physikalischer Schutz? personelle Annahmen über Ausbildung, Vertrauenswürdigkeit?)
- Bedrohungen (Risikoanalyse; welche Ressourcen brauchen Schutz? welchen Bedrohungen gibt es? welche Angriffe muss man annehmen? etc.)
- Organisatorische Sicherheitspolicies (Zugangsregeln? Informations-Fluss-Regeln? Gesetze? Regeln? etc.)

Kapitel 4: Sicherheitsziele (Security Objectives)

Aus den Definitionen der Sicherheitsumgebung des EVG (Kapitel 3) ergeben sich in diesem Kapitel die Sicherheitsziele.

Die Ziele werden, wenn notwendig, getrennt für den EVG und die Umgebung des EVG. In einigen Teilen des PP wird später beschrieben, wie die Sicherheitsziele des EVG mit seiner Umgebung diese Ziele erfüllt und abdeckt.

Kapitel 5: IT Sicherheitsanforderungen (IT Security Requirements)

Das Kapitel 5 ist das Herz des PP nach Common Criteria und beschreibt anhand des in den CC Kapiteln 2 und 3 vorgegebenen Kataloges die Sicherheitsanforderungen für den EVG, die Vertrauensklasse, sowie die Sicherheitsanforderungen für die IT-Umgebung. In einigen Fällen ist es sinnvoll, auch Sicherheitsanforderungen an die Nicht-IT-Umgebung zu formulieren. Dann nämlich wenn Annahmen, Bedrohungen und Ziele in Bezug auf die Nicht-IT-Umgebung im Kapitel 3 genannt werden.

Kapitel 6: Schlüssigkeitsbeweis (Rationale)

Schließlich werden die Aussagen über die Einsatzumgebung (Annahmen, Bedrohung und Policies), auf die Sicherheitsziele und die Sicherheitsziele auf die Sicherheitsanforderungen abgebildet.

Formal kann das Anhand von Tabellen geschehen, die u.a. feststellen, dass jede Bedrohung und Policy auch von einem Sicherheitsziel angesprochen wird.

Im weiteren wird nun sowohl in Text-Form als auch mittels Tabellen nachgewiesen, dass jedes Sicherheitsziel durch eine Sicherheitsanforderung erfüllt wird. Dies kann sowohl nur durch Sicherheitsanforderung an den EVG geschehen oder aber mit Unterstützung der Sicherheitsanforderungen für die IT- und Nicht-IT-Umgebung.

4. Sicherheitsanalyse von EN 1546

Im folgenden soll nun die Sicherheitsanalyse von EN 1546 dargestellt werden. Dazu werden die Kapitel 3 bis 6 des zugehörigen Protection Profile herangezogen. (Kapitel 2 des PP – Beschreibung des EVG – ist eine etwas formalere Beschreibung als im vorangegangenen Kapitel dieses Vortrags.)

Das vorliegende Protection Profile ist sehr „kürzellastig". Für das Verständnis sollten daher die in den vorangegangenen Abschnitten eingeführten Abkürzungen geläufig sein.

Kapitel 3: EVG Einsatzumgebung

Im Kapitel 3 identifiziert das Protection Profile Annahmen zur Einsatzumgebung (assumptions), Bedrohungen (threats) und organisatorische Sicherheitspolicies (organisational security policies) des Evaluierungsgegenstandes. Die Benennung erfolgt systematisch durch hierarchische Buchstabenkürzel. Assumptions beginnen mit „A.", threats mit „T." und organisational security policies mit „OSP.".

Eine von drei Annahmen ist zum Beispiel, dass der Load Agent die Fähigkeit hat, einen sicheren Zustand anzunehmen, wenn während einer Lade-Transaktion ein Fehler auftritt (A.LD).

Die sieben Klassen von Bedrohungen sollen etwas genauer betrachtet werden. Das PP identifiziert:

- Geldwäsche (money laundring, das Verschleiern von Geldfluss)
- Vortäuschung (usurpation, das Eindringen von nicht-autorisierten Actors, die eine falsche Identität vorgeben)
- Wiedereinspielung (replay, siehe unten)
- Fehler (failure, gemeint sind Übertragungsfehler)
- Fälschung einer Transaktion (forgery)
- Abstreiten einer Transaktion (false repuditation)
- Integritätsverlust (loss of integrity, gemeint ist unautorisierte Veränderung der Datenelemente in Geldbörse oder Sicherheitsmodul)

Für jede dieser sieben Klassen identifiziert das PP dann systematisch, bei welchen Transaktionen, actors und/oder devices die Bedrohung auftreten kann und was die Folge davon ist. Am Beispiel von Wiedereinspielungen soll dies exemplarisch dargestellt werden.

Bei einer Wiedereinspielung hört ein Angreifer eine Transaktion zwischen zwei devices ab, um sie später erneut an eines der beiden devices zu senden. Um alle Bedrohungen durch Wiedereinspielung zu identifizieren, müssen alle sinnvollen Kombinationen von Transaktionen und devices abgedeckt werden:

- Replay einer Lade-Transaktion an IEP. (T.RPLY_LD)
  Mit derselben Transaktion werden verschiedene IEP eine IEP mehrmals geladen.
  Folge: Erzeugung von EV.
- Replay einer Bezahl-Transaktion an PD. (T.RPLY_PCH_C)
  Mit derselben Transaktion erhalten verschiedene PD oder ein PD mehrmals Geld.
  Folge: Erzeugung von EV.
- Replay einer Bezahl-Transaktion an IEP. (T_RPLY_PCH_L)
  Mit derselben Transaktion werden verschiedene IEP oder eine IEP mehrmals belastet.
  Folge: Vernichtung von EV.
- Replay einer Storno-Transaktion an IEP. (T.RPLY_LPC_C)
  Mit derselben Transaktion erhalten verschiedene IEP oder eine IEP mehrmals Geld.
  Folge: Erzeugung von EV.

- Replay einer Storno-Transaktion an PD. (T.RPLY_LPC_L)
  Mit derselben Transaktion werden verschiedene PD oder ein PD mehrmals belastet.
  Folge: Vernichtung von EV.
- Replay einer collect-Transaktion von A. (T.RPLY_CLT)
  Die selbe Transaktion wird dem Acquirer mehrmals gesendet.
  Folge: Erzeugung von EV.

Durch die Systematik, mit der jede Klasse von Bedrohungen analysiert wird, wird subjektiv klar, dass die Aufzählung vollständig ist.

Das PP identifiziert weiterhin zwölf organisatorische Sicherheitspolicies. Exemplarisch sollen hier vier davon aufgezählt werden:

- „Debit always precedes credit during transaction.“ (OSP.DEB_BEF_CRED)
- „The A and the LA are trusted agents of the EVP.“ (OSP.A_LA_TRUSTED)
- „The IEP shall have a unique indentification within the system.“ (OSP.IEP_ID)
- „The SP can only be collected by his A.“ (OSP.SP_A_CLT)

Kapitel 4: Sicherheitsziele

Aus den Annahmen, Bedrohungen und Sicherheitspolicies aus Kapitel 3, leitet das Protection Profile in Kapitel 4 Sicherheitsziele ab. Diese werden unterteilt in Ziele für den Evaluierungsgegenstand selbst und für dessen Umgebung.

Das vorliegende PP leitet für EN 1546 insgesamt 19 solcher security objectives ab, von denen vier exemplarisch aufgezählt werden:

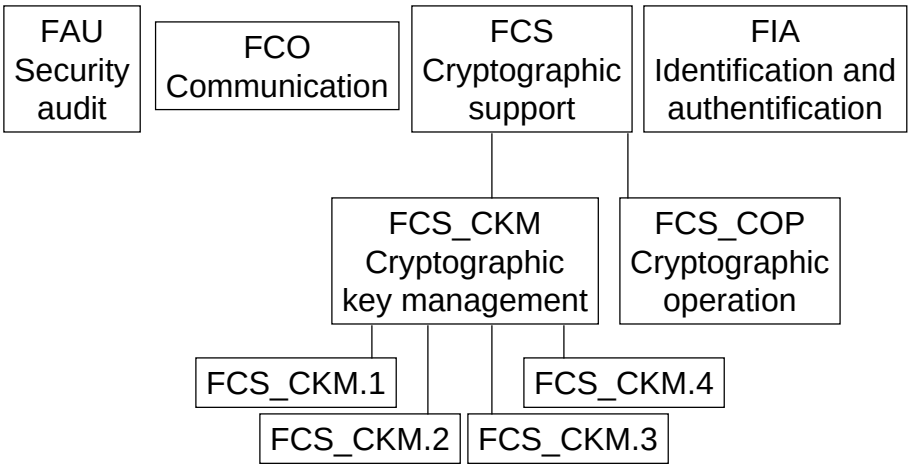
- O.EV: „The TOE security functions shall provide the means to avoid unauthorized creation or loss of EV.“
- O.REPLAY: „The TOE security functions shall ensure that replayed transactions are detected and countered.“
- O.LIMIT: „The stored EV in the IEP shall be limited by the value of a maximum amount.“
- O.SYSTEM: „The EV provider shall guarantee the EV in IEP system [...]. The actors of the system [...] shall apply the system security policy. [...]“

Es ist anzumerken, dass an dieser Stelle noch nicht erklärt wird, wie die Sicherheitsziele mit den Eigenschaften der Umgebung in Kapitel 3 zusammenhängen, sondern sie werden im PP zunächst nur aufgezählt.

Kapitel 5: IT Sicherheitsanforderungen

Das Kapitel 5 des Protection Profile ist die Hauptverbesserung der Common Criteria gegenüber ITSEC, von denen sie abgeleitet sind. Die Common Criteria definieren nämlich eine großen Katalog von allgemeinen IT Sicherheitsanforderungen (IT security requirements), aus denen die Entwickler eines Protection Profile oder Security Target eine Untermenge auswählen können und nur um die Namen von Actors, devices und Transaktionen ergänzen müssen, die für das System spezifisch sind. Dieses „Baukastensystem“ erleichtert sowohl die Zertifizierung als auch die spätere Umsetzung in eine konkrete Implementierung.

Den Katalog von security requirements teilt Common Criteria hierarchisch in elf Klassen ein, die jeweils mehrere Familien enthalten. Jede Familie wiederum enthält verschiedene Komponenten. Die folgende Grafik soll das zeigen:



Das vorliegende PP wählt eine Untermenge von 26 funktionalen Anforderungen aus, die es wörtlich zitiert, und die Ergänzungen, um es für die elektronische Geldbörse zu spezifizieren, gibt es meist in Tabellenform.

Beispielhaft soll das an der Anforderung „FPT_RPL.1“ (Klasse „Protection of the TOE security functions“, Familie „Replay“, Komponente 1) – Replay Detection – gezeigt werden.

Wörtliches Zitat aus CC: „The TSF shall detect replay for the following entities: [entities]
The TSF shall perform [actions] when replay is detected.“

Spezialisierung auf Evaluierungsgegenstand in Form einer Tabelle:

Iteration	entities	actions
Replay detection of IEP of a load by LA	LD (load)	- If equals to last ld then no more action - If different from last ld ignore and/or trace
Replay detection by PD of a purchase by IEP	IEP (purchase)	- If equals to last pc then no more action - If different from last pc ignore and/or trace
Collect	PD (collect)	collect interrupt
LPC	PD (LPC)	LPC interrupt

Auch hier ist wieder anzumerken, dass an dieser Stelle noch nicht erklärt wird, wie die Sicherheitsanforderungen mit den Eigenschaften der Umgebung in Kapitel 3 und den Sicherheitspolicies aus Kapitel 4 zusammenhängen, sondern sie werden im PP zunächst nur aufgezählt.

Neben den hier behandelten funktionalen Anforderungen gibt es auch noch Anforderungen an die Sicherheitsstufe (sog. TOE security assurance requirements), die hauptsächlich das Verhalten des Entwicklers und seine Zusammenarbeit mit der zertifizierenden Stelle festlegen und hier nicht dargestellt werden.

Kapitel 6: Schlüssigkeitsbeweis

Erst in diesem Kapitel erfolgt der Nachweis über die Zusammenhänge der vorherigen drei Kapitel. Während bisher nur aufgezählt wurde, beginnt hier die Argumentation.

Kapitel 6 unterteilt sich logisch in zwei Teile. Zunächst müssen die Annahmen, Bedrohungen und organisatorischen Sicherheitspolicies (Kapitel 3) auf die Sicherheitsziele (Kapitel 4) abgebildet werden. Danach folgt die Abbildung der Sicherheitsziele auf die Sicherheitsanforderungen (Kapitel 5).

Wenn man also voraussetzt, dass Kapitel 3 die Bedrohungen vollständig identifiziert hat und die beiden Abbildungen schlüssig dargelegt werden und vollständig sind, kann man von der Sicherheit des Evaluierungsgegenstandes ausgehen.

Abbildung Bedrohungen <> Sicherheitsziele

Das Protection Profile von EN 1546 stellt den ersten logischen Nachweisschritt in Form einer Tabelle dar, die für jede Bedrohung und Sicherheitspolicy den oder die Sicherheitsziele aufzählt, die sie verhindern bzw. durchsetzen. Jede Beziehung referenziert einen Absatz, in dem sie in Textform erklärt ist.

Zum Beispiel wird die Bedrohung „Geldwäsche“ durch das Sicherheitsziel „O.LIMIT“ und alle Bedrohungen, die Wiedereinspielung betreffen, durch „O.EV“ und „O.REPLAY“ verhindert:

Threats	Security objectives for the TOE	Security objectives for the environment	Para
T.LAUND_MON	O.LIMIT		138
...	...		...
T.RPLY_*	O.EV, O.REPLAY		159ff
...	...		...

Die Erklärung der zweiten Beziehung in Textform:

„The threat T.RPLY_LD is addressed by the security objectives for the TOE O.EV and O.REPLAY:

- the objective O.EV is applicable to the IEP and ensures EV flow preservation so that fraudulent creation of EV in the IEP is not allowed
- the objective O.REPLAY is applicable to the IEP and ensures that the IEP will operate in a continuous secure state in case of load replayed transactions; the replayed transaction will be detected and rejected by the IEP.“

Abbildung Sicherheitsziele <> Sicherheitsanforderungen

Auch der zweite logische Nachweisschritt ist in Tabellenform gegeben. Hier sind in einer Dimension alle (!) Sicherheitsziele und in der anderen alle (!) funktionalen Sicherheitsanforderungen angetragen. Kreuze geben an, welche Anforderung welches Ziel abdeckt. Der Nachweis ist vollständig, wenn jedes Ziel von mindestens auf eine Anforderung abgebildet wurde.

Security Objectives / Requirements	O.LIMIT	O.EV	...	O.REPLAY	...
...					
FDP_IFC.1	X	X			
...					
FPT_RPL.1		X		X	
FPT_RVM.1	X	X		X	
...					

In einer weiteren Tabelle wird der Nachweis über jede Anforderung aus der vorangegangenen Tabelle in Textform geführt.

Für FPT_RPL.1 heißt es zum Beispiel: „This requirement imposes that the TOE is capable of replay detection which contributes to O.REPLAY, indirectly contributes to integrity of user data (O.EV, O.INTEG_DATA)“

III. CEPS

1. Einführung

CEPS steht für „Common Electronic Purse Specifications“. Die 1999 vorgestellten Spezifikationen definieren Anforderungen an alle Komponenten, die eine Organisation braucht, um ein globales, branchen-übergreifendes elektronisches Geldbörsensystem zu implementieren, wobei die Interoperabilität zu anderen Organisationen gewährleistet werden soll. (Es ist also mit GSM im Mobilfunk vergleichbar.)

CEPSCO ist ein Konsortium von Organisationen, die mit der Weiterentwicklung von CEPS betraut sind, die CEPS implementieren werden, die für die Verbreitung von CEPS sorgen werden und als Forum für Anliegen und Verbesserungsvorschläge für CEPS agieren. Zu CEPSCO gehören zum Beispiel EURO Kartensysteme (Deutschland), CB Cartes Bancaires (Frankreich), Europay International und VISA International.

Die Autoren von CEPS haben die fehlende Interoperabilität zwischen den verschiedenen existierenden Geldbörsensystemen als Hauptgrund für die fehlende Verbreitung und Akzeptanz identifiziert und darauf und auf die Internationalität den Schwerpunkt gesetzt.

CEPS umfassen drei Spezifikationen:

- CEPS Business Requirements – identifiziert Marktbedürfnisse, Zustand des Markts, Gewinnmöglichkeiten und Ziele für ein elektronisches Geldbörsensystem (Sicherheit, Komponenten, Transaktionen)
- CEPS Functional Requirements – identifiziert funktionale Anforderungen für Sicherheit, Komponenten und Transaktionen
- CEPS Technical Specification – spezifiziert Algorithmen, Kommandos, Protokolle, Datenelemente genau, um Interoperabilität zu gewährleisten

Derzeit haben Organisationen aus über dreißig Ländern zugestimmt, CEPS zu implementieren. Weitere 200 Organisationen haben Lizenzvereinbarungen für CEPS unterzeichnet.

2. Unterschiede zu EN 1546

Das erklärte erste Ziel von CEPS ist die Internationalität und Interoperabilität. Der wichtigste Unterschied zu EN 1546 ist deshalb, dass CEPS in den „Technical Specifications“ technische Details so genau spezifiziert, dass der Implementierung kein Raum für Inkompatibilität gelassen wird. EN 1546

dagegen hat zwar die Konzepte genormt, aber zwei Systeme, die beide der Norm entsprechen, sind deshalb nicht miteinander kompatibel.

Die Notwendigkeit, eine international einsetzbare elektronische Geldbörse zu schaffen, ist in der heutigen Zeit besonders durch das Internet und darüber abgewickelten E-Commerce gegeben. Momentan gebräuchliche Bezahlsysteme sind entweder bei den Kunden nicht beliebt (typischerweise Kreditkarte) oder bei den Händlern (typischerweise Rechnung). Momentan verfügbare elektronische Geldbörsensysteme sind für Händler viel zu teuer einzuführen, weil jedes nur einen kleinen (auf maximal ein Land eingeschränkten) Kundenkreis abdeckt.

Das Ziel der Interoperabilität ist nur durch noch weitergehendere Sicherheitseigenschaften als in EN 1546 zu bewerkstelligen, da der Börsenanbieter jetzt nicht mehr alleine für die Sicherheit verantwortlich sein kann. Eine (sichere) Schnittstelle zwischen Börsenanbietern muss gegeben sein, damit der Käufer des einen Anbieters beim Händler des anderen Anbieters bezahlen kann. (Das ist vergleichbar mit Roaming in GSM.)

Auch in der Funktionalität ergeben sich einige Erweiterungen zu EN 1546:

- Die Verarbeitung von verschiedenen Währungen wird durch „slots“ in der Geldbörse realisiert. Jeder slot kann elektronisches Geld einer bestimmten Währung aufnehmen.
- Neben einer Load-Funktion gibt es auch eine Unload-Funktion, mit der elektronisches Geld in „echtes“ Geld getauscht wird.
- „Incremental purchase“ bezeichnet die schrittweise Bezahlung einer Dienstleistung, wie es zum Beispiel zum Telefonieren sinnvoll ist: Nach einer einleitenden Transaktion kann nach und nach mehr Geld übertragen werden, ohne dass für jede Einheit eine eigene Transaktion gestartet werden muss.
- Währungsumtausch wird unterstützt.