1. Summary

Der Aufbau und Betrieb einer zentralen Clearingstelle zum Ausgleich der Pfandströme von Einweg-Getränkeverpackungen in Deutschland stellt aus IT Sicht ein **Integrationsprojekt** mit extremen Anforderungen da. So wird die Clearingstelle mehr als 50.000 Vertragspartner bedienen müssen, ca. 800 unterschiedliche Abfüller und Importeure sind in das System einzubinden und schließlich werden die Transaktionsdaten aus ca. 75.000 Rücknahmesystemen unterschiedlicher Hersteller zu verarbeiten sein.

Bei der kommerziellen Bedeutung für den Betreiber der Clearingstelle und der Systembeteiligten müssen in den Machbarkeitsstudien und Risikoanalysen alle Komponenten unbedingt auch unter Sicherheitsgesichtspunkten bewertet werden. Dabei sind zum einen die **Betriebssicherheit** zu betrachten, zum anderen aber die **Manipulationsicherheit** zu untersuchen.

Die Betriebssicherheit wird in erheblichem Maße beinflußt durch die Komplexität der IT-Landschaft und durch deren Beherrschbarkeit.

Hier zeigen alle Erfahrungen, dass die Betriebsrisiken nur dann kalkulierbar bleiben, wenn

- die Anzahl der Schnittstellen so gering wie möglich gehalten wird,
- die Anbindung unterschiedlicher Systeme über EINE Integrationsplattform erfolgt,
- die Gesamtlösung im Betrieb an EINER Stelle zu überwachen ist,
- die Daten nur zwischen eindeutig authentisierten Sendern und Empfängern transaktions- und manipulationsgesichert übermittelt werden und schliesslich
- die jederzeitige Nachvollziehbarkeit gegeben ist.

Bei der Manipulationssicherheit ist zwischen der Manipulation von außen (zum Beispiel durch die Rückgabe gefälschter Pfandgebinde) und der Manipulation innerhalb des Clearingprozesses zu unterscheiden. Die Rückgabe von gefälschten Pfandgebinden soll mit mit einer technisch (und finanziell) aufwendigen Kennzeichnung und Erkennung der Verpackungen verhindert werden. Der Aufwand hierfür wäre jedoch nicht zu rechtfertigen, wenn nicht in dem gleichen Maße das Gesamtsystem gegen die Manipulation von innen geschützt wird, denn hier kann potentiell ein erheblich größerer Schaden entstehen.

2. Manipulations-Szenarien

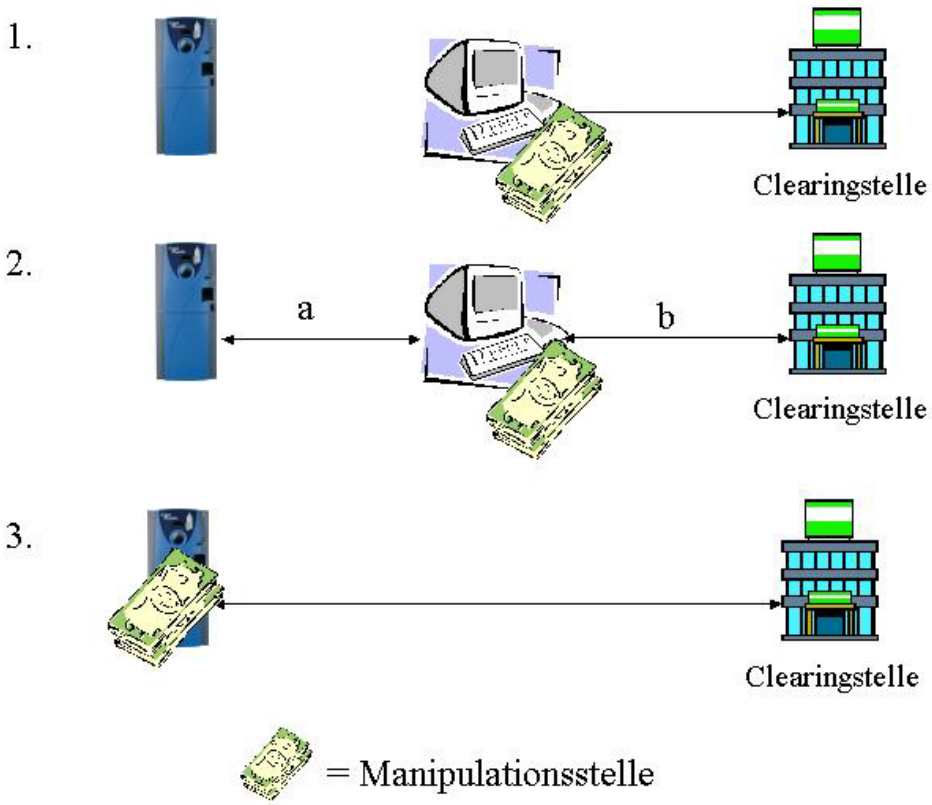
Eine Manipulationsmöglichkeit innerhalb des Systems besteht vor allem durch diejenigen Teilnehmer, die Pfandbeträge durch die Clearingstelle überhaupt erhalten können. Dies sind in erster Linie diejenigen Vertragspartner, die bei der Clearingstelle als Rücknehmer registriert sind und daher über eine entsprechende Kontoverbindung verfügen. Damit besteht das potentielle Risiko, dass Tausende von Teilnehmern INNERHALB des Systems der Clearingstelle Pfandtransaktionen vortäuschen, ohne das dem Gebinderücknahmen und Pfandauszahlungen an den Kunden gegenüberstehen.
(Zitat aus der Leistungsbeschreibung; *“Rücknehmer meldet überhöhte Rücknahmemengen an Clearingstelle durch Manipulation des Kommunikationssystems”)*

Dies kann geschehen,

1. indem der Clearingstelle Rücknahmeautomaten vorgetäuscht und fiktive Transaktionsdaten übermittelt werden: *Wenn der Rechner des Automaten direkt d.h. ohne gesicherte Kommunikationseinheit (c-Box) mit der Clearingstelle kommuniziert, kann über jeden PC ein Rücknahmeautomat simuliert werden und fiktive Daten für einen existierenden Rücknahmeautomaten übermittelt werden*, oder

2. indem umgekehrt dem Rücknahmeautomaten eine Clearingstelle vorgetäuscht wird, die Transaktionsdaten ausliest und manipuliert und diese anschließend an die Clearingstelle übermittelt: *Über einen PC werden Automaten angerufen und die Daten ausgelesen, anschließend werden die Daten manipuliert (hochgesetzt) und an die Clearingstelle weitergeleitet*

3. Schließlich besteht die Möglichkeit, dass die Datenverarbeitungseinheit des Rücknahmeautomaten selbst Transaktionsdaten vortäuscht oder manipuliert *z.B. könnten täglich die Zählerstände automatisch um 20% hochgesetzt werden; dazu bedarf es nur einer kleine Routine, die vor der Datenübermittlung an die Clearingstelle aufgerufen wird*



In allen Fällen werden scheinbare Pfandumsätze generiert, die durch Einreichung bei der Clearingstelle zur Auszahlung gelangen würden.

Ohne entsprechende technische Vorkehrungen wären geschickte Manipulationen praktisch nicht aufzudecken. Eine betrügerische Simulation von Gebinderücknahmen, die im Rahmen

von glaubhaften Schnwankungsbandbreiten (15-20%) läge und sich so einer automatisierten Plausibilitätsprüfung entziehen würde, wäre nicht nachzuweisen. Dies würde aber alleine ein Betrugsrisiko von 600 - 800 Mio € p.a. darstellen. Alleine die Kenntnis einer solchen Sicherheitslücke würde mit großer Wahrscheinlichkeit mehr kriminelle Energie anziehen als bei einer wesentlich aufwendigeren Fälschung von Pfandgebinden, die zudem noch rein manuell in den Umlauf gebracht werden müßten.

In den folgenden Abschnitten wird dargelegt, wie einer Manipulation innerhalb des Systems wirksam vorgebeugt werden kann.

3. Geringere Kosten durch Reduktion der Komplexität

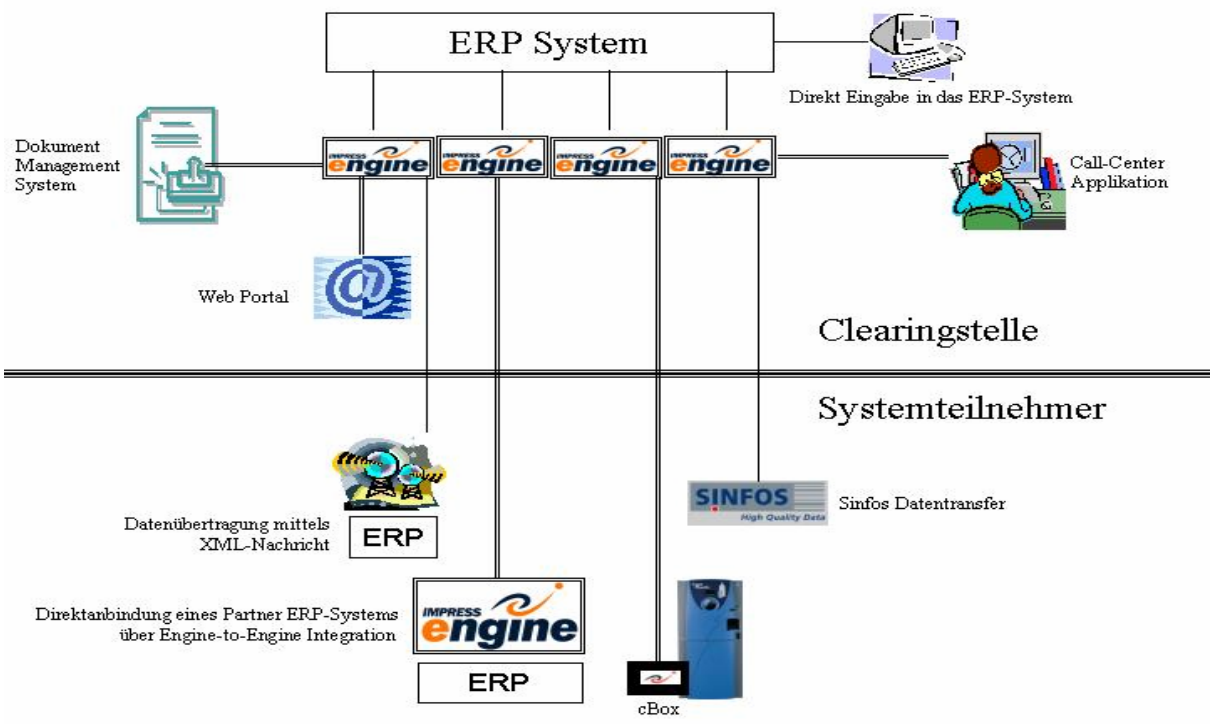
Jede IT-Landschaft muss beherrschbar sein – wenn sie mit kalkulierbaren Kosten betrieben werden soll. Und dies setzt voraus, das die Komplexität der Systemkomponenten und Schnittstellen auf ein Minimum reduziert wird. Für die Clearingstelle bedeutet dies, das alle Systemteilnehmer über eine einheitliche Plattform integriert werden. IMPRESS bietet dazu mit der **IMPRESS Engine** eine Integrationslösung, die die gestellten Anforderungen voll erfüllt. Das Produkt ist

- weltweit bei mehr als 100 Großkunden im Einsatz,
- auf unterschiedlichen Plattformen industrie-konform verfügbar (von Mini-Systemen bis Großrechner),
- auf synchrone, transaktionsgesicherte Anbindungen spezialisiert,
- als Ablaufplattform für ergänzende Applikationen wie Web-Frontends nutzbar,
- repository gestützt und erlaubt so auch aufwendige semantische Kontrollen, Fehlerüberprüfungen und die notwendige Historienführung.

Über eine Integrationsplattform wie die **IMPRESS Engine** können die unterschiedlichen Systemteilnehmer mit der Clearingstelle kommunizieren. Die ‚Schnittstelle' nach außen ist **einheitlich, gesichert (verschlüsselt) und skalierbar**. Die Anbindung kann synchron und transaktionsgesichert erfolgen, genauso sind XML Nachrichten möglich oder auch die ‚teilautomatisierte' Integration über Web-Frontends. Dabei erfolgt zu keinem Zeitpunkt ein direkter Zugriff auf die Buchungssysteme der Clearingsstelle, es wird immer vorher die ein- oder ausgehende Nachricht auf Authenzität und semantische Korrekheit geprüft und duch die IMPRESS Engine kontrolliert.

Und zusätzlich: Änderungen im Prozessablauf nach der Inbetriebnahme erfordern nur EINE Anpassung – an zentraler Stelle.

Im Schaubild ist dargestellt, wo der Integrationsbedarf beim Betrieb der Clearingstelle durch den Einsatz der IMPRESS Engine abgedeckt werden kann:



Neben der hier durch erreichten Vereinfachung des Gesamtsystems wird auch die Betriebssicherheit signifikant erhöht und letzlich die Betriebskosten durch Einsparungen bei der manuellen Überwachung spürbar gesenkt. Darüber hinaus ist aber zwingend notwendig, für die Abschätzung der Betriebskosten und die Risikobewertung auch die im System gegebenen Manipulationsmöglichkeiten zu betrachten.

4. Weniger Risiko durch höhere Sicherheit

Die Sicherheitsanalyse für den Betrieb der Clearingstelle ergibt zweifelsfrei, dass bei den vorgesehen Rücknahmesystemen das höchste Einzelbetrugsrisiko vorhanden ist. Daher ergibt sich hier zuerst die Notwendigkeit, Manipulationen vorzubeugen und die Revisonssicherheit zu erhöhen.

Ein sehr hohes Risiko ergibt sich vor allem dann, wenn unterschiedliche Rücknahmesysteme verschiedener Hersteller direkt und ungesichert mit der Clearingstelle kommunizieren. Die Manipulationsmöglichkeiten könnten nur dann eingegrenzt werden, wenn alle Automatenhersteller in allen angebotenen Automatentypen die gleiche von der Clearingstelle zertifizierte (und jeweils geprüfte) Sicherheitstechnologie verwenden würden. Dies scheint schon aus praktischen Erwägungen nicht sinnvoll zu sein. Darüber hinaus bestünde immer noch das Problem, das alle Automatenhersteller ein einheitliches Protokoll für die Kommunikation mit Clearingstelle verwenden müßten., und zwar einschließlich der Transaktionsmechanismen, Fehlerbehandlung u.s.w. Sinnvoll erscheint nur, die Rücknahmesysteme hard- und softwareseitig einheitlich an die Clearingstelle anzubinden.

IMPRESS bietet daher für die einheitliche Anbindung der Rücknahmeautomaten manipulationsgeschützte Kommunikationsboxen (im folgenden cBox) an, mit der das Betrugsrisiko für diesen Prozessschritt kleiner 0,5% gehalten werden kann.

Die cBox übernimmt folgende Aufgaben:

- Speicherung der für die Automatentransaktion gültigen und zugelassenen Produktstammdaten
- Speicherung und Validierung der Pfandtransaktionen am Einzelautomaten oder im Automatenverbund
- Speicherung von relevanten Prozessdaten des Automaten
- Einheitliche Schnittstelle und gesicherte Anbindung für alle Rücknahmesysteme
- Einheitliche Schnittstelle und gesicherte Übertragung der Daten zur Clearingstelle.

Verwendet wird ein bedienerloser Rechner. Dieser verfügt über eine batterie-gepufferte Flashdisk und kann somit ohne Lüfter im geschlossenen, geschützten Gehäuse betrieben werden. Die cBox verfügt über einen integrierten Power-Fail-Safe, integrierten Hardware-Watchdog und einen integrierten ID-Chip mit weltweit eindeutiger Kennung. Die cBox verfügt für die Anbindung der Rücknahmeautomaten über 2 Schnittstellen (Ethernet 10/100Mbit und RS232). Die Kommunikation erfolgt über TCP/IP. Das Protokoll kann zusammen mit den Automatenherstellern abgestimmt und definiert werden. Das Protokoll ist auf Sicherheit und Fehlertoleranz abgestellt, darüber hinaus aber extrem einfach gehalten, um die Implementierung in den Rücknahmeautomaten so einfach wie möglich zu halten. Neben den physikalischen Schnittstellen, die von allen Automatenherstellern unterstützt werden, wird als einziges Anforderung vorausgesetzt, das die angeschlossenen Automaten über einen eindeutigen Schlüssel identifiziert werden können (siehe Sicherheitskonzeption).

Für die Kommunikation mit der Clearingstelle ist die cBox mit einem ISDN Interface ausgestattet. Analoge Modem sowie DECT Module sind optional erhältlich.

Alle Daten werden verschlüsselt vollständig transaktionsgesichert übertragen.

5. Sicherheitstechnik

Für die Sicherheitstechnik der cBox wurden die folgenden Manipulationsmöglichkeiten betrachtet:

Verarbeitungsschritt	**Angriffsmöglichkeit**
Sensorik	Vortäuschen des Sicherheitsmerkmals
Datengenerierung	Vortäuschung des elektrischen Signals für ein gültiges Sicherheitsmerkmal
Datenverarbeitung	Vortäuschung gültiger Datensätze
Übertragung	Vortäuschung einer Rücknahmestelle, Vortäuschung einer Clearingstelle
Weiterverarbeitung	Manipulation von Einreichdateien

Ein Angriff auf die Sensorik wird durch die Wahl eines robusten, schwer fälschbaren, Sicherheitsmerkmals erschwert. Ein Angriff auf die Datengenerierung erfordert Zugang zu den elektrischen Signalen im Rücknahmeautomat. Durch eine enge Verzahnung zwischen Sensorik und Datengenerierung und die mechanische Kapselung der Einheit im Rücknahmeautomaten kann er wirksam verhindert werden.

Ein besonderes Gefahrenpotential besteht dagegen bei der Datenübertragung über ein offen zugängliches Netz. Konkret sind hier zwei Arten des Angriffs möglich:

- Der Angreifer täuscht der Clearingstelle eine Rücknahmestelle vor, übermittelt eine fiktive Einreichdatei und erschleicht sich so eine Pfandauszahlung durch die Clearingstelle.
- Der Angreifer täuscht der Rücknahmestelle eine Clearingstelle vor, übernimmt die Einreichdatei, manipuliert sie und reicht sie anschließend selbst bei der Clearingstelle ein.

Schließlich besteht die Möglichkeit, der Datenverarbeitung Transaktionsdaten vorzutäuschen. Hierdurch fingiert der Angreifer Pfandumsätze und erschleicht sich bei Einreichung einer derart manipulierten Datei ebenfalls die Auszahlung durch die Clearingstelle.

a. Sichere Kommunikation

Die Kommunikation lässt sich folgendermaßen sichern: Jedes Rücknahmesystem wird mit einem privaten, geheimen Schlüssel versehen. Der Schlüssel ist in der Clearingstelle bekannt. Beide Seiten verschlüsseln die Kommunikation mit diesem Schlüssel, d.h. ein Datenaustausch ist nur möglich, wenn beide den Schlüssel kennen. Dieses Verfahren erreicht die Authentizierung in beide Richtungen.

Wichtig für die Sicherheit dieses Verfahrens ist, dass der private Schlüssel geheim bleibt, d.h. vor Ausspähung geschützt ist. Der Schlüssel darf z.B. nicht im Klartext über den Kommunikationsweg übertragen werden. Das Verschlüsselungsverfahren ist so zu definieren, dass auch die längere Beobachtung des Datenstroms keinen Rückschluss auf den Schlüssel gestattet (Plain Text Attacks usw.). Der Schlüssel darf nicht auslesbar sein. Auf Seiten der Clearingstelle ist das kein Problem, hier kann die Umgebung gesichert werden. Das Rücknahmesystem ist jedoch unsicher, d.h. hier muss der Schlüssel in einem gesicherten Speicher abgelegt werden. Als kostengünstige Lösung bietet sich eine Chipkarte an.

Über die Chipkarte wird folgendes erreicht: Der darauf gespeicherte Schlüssel ist nicht auslesbar. Der Prozessor der Chipkarte kann ihn aber nutzen, um damit Daten zu verschlüsseln. Somit läßt sich der Schlüssel über ein von der Clearingstelle initiiertes Challenge-Response-Verfahren verifizieren. Die Chipkarte bietet zudem den Vorteil einer von der Gerätehardware unabhängigen Schlüsselverteilung. Damit sind flexible Sicherheitskonzepte umsetzbar.

Die Datenverarbeitung in der Rücknahmestelle geschieht in der Praxis in mehreren Schritten. Dabei entstehen Zwischenergebnisse, die teilweise nicht-flüchtig gespeichert werden. Mögliche Angriffspunkte auf die Datenverarbeitung sind das Fälschen von Eingangsdaten und die Manipulation von Zwischen- oder Endergebnissen.

Um hierfür Sicherheit zu erzeugen ist die Kombination folgender Maßnahmen erforderlich.

- Die Quelle für die Eingangsdaten, d.h. die Datengenerierung, ist zu validieren.
- Die Programme, mit denen die Daten verarbeitet werden, sind zu validieren.
- Zwischen- und Endergebnisse der Datenverarbeitung sind manipulationsgeschützt zu speichern.

Alle diese Maßnahmen lassen sich mit Hilfe der vorhandenen Chipkarte implementieren. In Konsequenz ist die Chipkarte ein praktikabler Weg, um sowohl die Kommunikation als auch die Datenverarbeitung sicher zu machen.

b. Sicherheit, kalkulierbare Gesamtkosten und extrem niedrige Ausfallrisken - die praktische Umsetzung:

Die gesamte Sicherheitstechnik wird innerhalb einer separaten Rechnereinheit implementiert, der sogenannten cbox. Sie wird zwischen Rücknahmeautomat und Kommunikationsleitung eingebaut. Bei mehreren Rücknahmeautomaten an einem Standort reicht in der Regel eine einzige cbox für deren Anbindung aus.

Die cbox beinhaltet die Chipkarte. Auf der cbox findet die gesamte Verarbeitung der Transaktionsdaten statt.

Diese Vorgehensweise bietet eine Reihe wichtiger Vorteile:

1. Die gesamte Sicherheitstechnik ist in einem standardisierten Produkt zusammengefasst, das unter alleiniger Kontrolle der Clearingstelle steht. Die Software der cbox wird unter sicherheitstechnischen Gesichtspunkten optimiert und zertifiziert.
2. Die cbox ist sozusagen der verlängerte Arm der Clearingstelle vor Ort. Damit wird der Gefahrübergang klar geregelt, d.h. die Clearingstelle ist verantwortlich für den sicheren, konsistenten Transport der Daten über die Kommunikationsstrecke. Das (Rest-) Risiko ist kalkulierbar.
3. Die Automatenhersteller werden beim Thema Informationssicherheit entlastet. Insbesondere ist keine spezielle Sicherheitszertifizierung der einzelnen Automatenmodelle notwendig. Im Hinblick auf die zu erwartende Modellvielfalt ist das ein wichtiger Aspekt und eine enorme Kostenentlastung.
4. Die gesamte Kommunikation zwischen Rücknahmesystem und Clearingstelle wird über die cbox abgewickelt. Der Automat muss sich nicht mit dem aufwendigen Handling von Kommunikationsprotokollen befassen.
5. Die Verteilung von Updates der Sicherheits- und Kommunikationssoftware wird vereinheitlicht und kann von der Clearingstelle aus per Fernwartung erfolgen.
6. Die Chipkarte ermöglicht ein Mitprotokollieren einiger ausgewählter Statistikdaten auf der Karte. So kann z.B. die Gesamtsumme des geschuldeten Pfandbetrags seit dem letzten Online-Abgleich mitgeschrieben werden. Selbst im Falle eines gravierenden Hardwareproblems ist diese wichtige Information mithin sicher.

c. Authentizierung der Kommunikationspartner (Clearingstelle und Rücknahmestelle)

Auf der Chipkarte der cbox ist ein privater Schlüssel gespeichert, der in der Clearingstelle bekannt ist. Mittels eines Challenge-Response-Verfahrens authentizieren sich beide Seiten gegenseitig ohne den Schlüssel preiszugeben.

d. Sicherung von Sendungen und Validierung der Datengenerierung

Alle Sendungen werden mit einer verschlüsselten Prüfsumme (Signatur) versehen. Der Empfänger der Sendung überprüft die Signatur und kann darüber die Korrektheit der Sendung verifizieren. Der verwendete Schlüssel wird dynamisch im Zusammenhang mit der Authentizierung gebildet. Das macht eine Rückwärtsberechnung des Schlüssels aus abgehörten Daten unmöglich.

Bei der erstmaligen Inbetriebnahme und im Servicefall muss der Rücknahmeautomat bei der cbox angemeldet (subskribiert) werden. Die Subskription ist nur möglich, wenn sie von der Clearingstelle freigeschaltet wurde. Sie wird typischerweise durch Eingabe einer PIN am Automaten zusätzlich abgesichert. Die PIN korrespondiert mit einem Eintrag auf der Chipkarte der cbox.

Bei der Subskription wird ein Schlüssel erzeugt, der innerhalb der Funktionseinheit Datengenerierung des Rücknahmeautomaten und in der Chipkarte der cbox abgespeichert wird. Dieser Schlüssel (Subscription Key) ermöglicht die Validierung des Automaten in nachfolgenden Transaktionen. Die Clearingstelle erhält über jeden Subskriptionsvorgang eine Mitteilung durch die cbox.

Die einzige Sicherheitsanforderung an den Rücknahmeautomaten in diesem Zusammenhang ist die sichere Speicherung des Subscription Keys, so dass er nicht von außen ausgelesen werden kann. Am besten geschieht das innerhalb der Datengenerierung, z.B. in einen EEPROM.

e. Validierung von Transaktionen

In der Datengenerierung und in der cbox laufen unabhängige Sequenzzähler, die durch die Subskription synchronisiert wurden. Bei jeder Transaktion inkrementieren beide Seiten den Sequenzzähler. Die Kombination aus Sequenzzähler und Subscription Key wird verwendet, um für jede Transaktion eine Signatur zu erzeugen.

f. Validierung der Programme auf der cbox

Jedes Programm auf der cbox wird mit einer Prüfsumme versehen, die mit dem privaten Schlüssel der cbox verschlüsselt wurde. Damit ist es unmöglich, ein unautorisiertes Programm auf die cbox zu laden.

g. Validierung der gespeicherten Daten auf der cbox

Zwischenergebnisse der Datenverarbeitung und die Einreichdatei werden ebenfalls mit einer verschlüsselten Prüfsumme gesichert, die auf dem privaten Schlüssel der cbox aufsetzt.

h. Datenabgleich zwischen cBoxen und Clearingstelle

Die gesamte Kommunikation erfolgt zudem transaktionsgesichert und synchron. Durch entsprechende Sicherungs- und Prüfverfahren wird einer Manipulation der Daten auf dem Übertragungsweg vorgebeugt. Die Transaktionssicherheit ist auch im Fall von Hardwarefehlern (Verbindungsabrüche oder Ausfall der cBox) gewährleistet. Die abgebrochene Transaktion wird dann auf beiden Seiten zurück gerollt und neu aufgesetzt.

Der Datenabgleich zwischen cBoxen und Clearingstelle kann abhängig von bestimmten Ereignissen oder zu festgelegten Zeitpunkten erfolgen. Dabei werden die gesammelten Transaktionsdaten und ggf. weitere Reports an die Clearingstelle übermittelt. Im Gegenzug lädt die Clearingstelle bei Bedarf neue oder geänderte Stammdaten auf die cbox.

Der Kommunikationsaufbau kann sowohl von der cBox als auch von der Clearingstelle aus erfolgen. Im Regelbetrieb wird jedoch die Clearingstelle den Prozess triggern, um bei der großen Anzahl an geplanten Automateninstallationen eine effiziente Lastverteilung zu

gewährleisten. Dazu ruft die zentrale Kommunikationsinstanz in der Clearingstelle zu definierten Zeitpunkten oder Ereignissen jede cBox über eine Wählleitung (ISDN) an (pull Methode), übermittelt geänderte oder neue Produktdaten und überträgt die Transaktionsdaten von der cBox an die Clearingstelle. Nach erfolgreicher Übertragung der Rücknahmedaten werden die Zähler der Rücknahmeautomaten auf Null zurückgesetzt. Im Falle von relevanten Prozessereignissen des Automaten (z.B. Abstellen der Entwertungsmechanik (Stanze, Schredder) während des Betriebes) werden diese direkt von der cBox an die Clearingstelle übermittelt (push Methode).

6. Zertifizierung

IMPRESS sieht einen Zertifizierungsbedarf für alle sicherheitsrelevanten Komponeten des Gesamtsystems. Durch den Einsatz einer einheitllichen Integrationslösung, die die Anbindung der Rücknahmesysteme mit einschließt, kann der Aufwand (und damit Vorlaufzeiten und Kosten) allerdings erheblich reduziert werden:

Diese cBoxen werden von der Clearingstelle unter dem Gesichtspunkten Datenspeicherung, Datenübertragung, Verschlüsselung, Authentisierung sowie Kommunikationsinterfaces und -protokollen zertifiziert. Damit ist sichergestellt, das die Clearingstelle ausschließlich in definierter Form Transaktionsdaten von den angeschlossenen Rücknahmesystemen erhält.

Für die Automatenhersteller ergibt sich daraus der Vorteil, das ausschließlich die eingebaute Sensorik für die Erkennung des Sicherheitsmerkmals zertifiziert sein muss und darüber hinaus nur eine einheitliche, klar definierte Schnittstelle zur cBox bedient werden muss.

Für weitere Informationen wenden Sie sich bitte an:

IMPRESS SOFTWARE AG
Rotenburger Strasse 21
30659 Hannover
Tel.: 0511 61071 – 0

www. IMPRESS.com
email: info@impress.com