

Desperate House-Hacking: Hintergründe über Automaten zur Pfandrücknahme

**Nils Magnus
magnus@linuxtag.org**

**24C3 Chaos Communication Congress
27. - 30. Dezember 2007
Berlin**

Einleitung

- Nils
- Bin kein Anwalt
- Verantwortungsvolles Hacking
 - Untersuchung der Mechanismen
 - Reflektieren der Hintergründe
 - Bewertung von Aufwand und Nutzen
- Mehr Workshop als Vortrag

Hintergrund

- Ziel: Auswirkungen von Verpackungen auf die Umwelt verringern
- Verpackungsverordnung 1991 ins Leben gerufen (BM Töpfer)
- 1998 grundsätzlich novelliert (BM Merkel)
- bis 2003 von BM Trittin gegen Widerstände im Einzelhandel umgesetzt

Betroffen

- Relevant ist §8, Abs 2 VerpackV i. d. F. v. 19. Juli 2007:
 - Bier
 - Wasser (inkl. Sport-Durstlöscher etc.)
 - „Limo“ bzw. „Soda“
 - Alk < 15%

Nicht betroffen

- Fruchtsäfte, -nektare etc.
 - Milchgetränke,
 - „diätetische Getränke im Sinne des § 1 Abs. 1 der Diätverordnung, ausgenommen solche für intensive Muskelanstrengungen, vor allem für Sportler, im Sinne von Anlage 8 Nr. 7 dieser Verordnung, und Mischungen dieser Getränke sind keine Erfrischungsgetränke (...)“
 - Getränke in Kartons und Schläuchen
 - Wein
 - Alk > 15%

Ausnahmen

- untransparente Sonderformen, z. B.:
 - Biermischungen mit Pfand
 - Saft-Vodka ohne Pfand (je nach Mischung)
- Heute: Rücknahme jeder Verpackung, solange irgendwann mal Pfand dafür gezahlt wurde
- Im Zweifelsfall: Verbraucherzentrale
- Geschäfte unter 200m² müssen nur Verpackungen zurücknehmen, die sie auch verkaufen

Pfandarten und ihr Erfolg

- Dosenpfand:
 - Nach Einführung der Regelung ist die Dose in Deutschland fast ausgestorben (weniger als 20% vor der Einführung)
- Einwegpfand
 - Großer „Gewinner“ der Aktion, große Steigerungsraten
- Mehrwegpfand
 - Potentieller Verlierer, Anteil an den Verpackungen stagniert bzw. geht zurück
 - **Einzigste Ausnahme: Bier**

Pfandsysteme

- VerpackV von 1998: Bei Schwellwert von $< 72\%$ wird Pfandsystem notwendig
- 1. Januar 2003:
 - Pfand wird Pflicht
 - Rücknahme nur selbst verkaufter Verpackungen durch Händler
- 1. Oktober 2004:
 - Alle angebotenen Verpackungen müssen zurückgenommen werden

Insellösungen

- Diverse Bon- und Logo-Systeme:
 - P-System, Lekkerland (viele Tankstellen, Kioske etc.)
 - Spar-System (fusioniert mit P-System)
 - Aldi
 - Lidl
 - Plus/Tengelmann
 - REWE
 - Metro



Einheitliches System

- Seit 1. Mai 2006 einheitliches System
- betrieben von der DPG Deutsche Pfandsystem GmbH
 - Bundesvereinigung der Deutschen Ernährungsindustrie und Hauptverband des Deutschen Einzelhandels
 - Non-Profit, keine operativen Aufgaben, kein Einblick in Daten
 - Regelt Pfand-Clearing
 - Aktuelle Schätzungen: bis zu 18 Mrd. Verpackungen

DPG-System

- Overengineerertes Monster der Bürokratie und Technik?
- Händler bemängeln hohen Aufwand („Vorgaben zur Erstellen von Rechnungen und Mengenmeldungen durch die Dienstleister“, 100 Seiten)
- Konzept: Roland Berger



Automaten

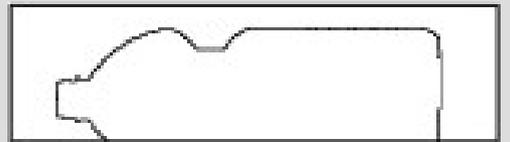
- Einige Hersteller (Auswahl):
 - Tomra Systems
 - RAP Vario



- Interessante Geschäftsidee:
Rücknahmeautomat mit Slot-Machine

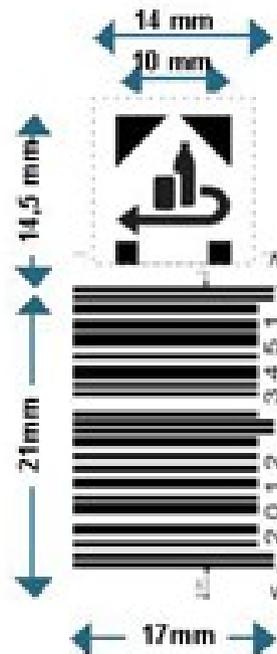
Messkriterien (Theorie)

- Logo
 - Spezialfarbe
 - angeblich bestimmte Eigenschaften unter Licht
 - nur von zertifiziertem Hersteller
- Gewicht (steht potentiell in gs1-Daten)
- Flaschenfarbe (gs1)
- Form
- Barcode
- In der Realität: ???



Spezifikation für's Label

DPG-Kennzeichen und EAN



- Der EAN-Code ist als **Leitercode** auf den Gebinden aufzubringen. Dies **erleichtert** die **Lesbarkeit** im Automaten bei Rotation und Vorschub
- Der EAN-Code kann in der **Größe variieren**, von mind. **0,8 x** bis max. **2,0 x** der GS1-Zielgröße. Bei einem Verkleinerungsfaktor von 0,8 auf die Zielbreite von 21,28 mm ergibt sich eine Mindestbreite von 17,03 mm
- Bei der Aufbringung des EAN-Codes sind Ruhezonon zu beachten. Die Ruhezonon von DPG-Kennzeichen und EAN- Feld können ineinander übergehen
- Der EAN-Code muss den GS1-Spezifikationen entsprechen (Nummernvergabe und graphische Anforderungen)
- Der EAN-Code muss auf einem weißen Hintergrund aufgebracht werden

DPG-Farbe

- Die DPG-Markierung darf nur mit einer speziellen DPG-Farbe gedruckt werden. Die DPG-Farbe weist unter unterschiedlichen Beleuchtungen unterschiedliche Eigenschaften auf. Die DPG-Farbe wird von den von der DPG ausgewählten Herstellern bereitgestellt. Die Preise für die DPG-Farbe sind in einem Rahmenvertrag zwischen der DPG und den Herstellern barbe umgehen können. Im Merkblatt Zertifizierung sind alle wesentegrenzt.
- **Zertifizierung von Verwendern DPG-Farbe**
- Nur zertifizierte und von der DPG zugelassene Dosenhersteller und Etikettendrucker dürfen die DPG-Farbe auf Verpackungen bzw. Etiketten aufbringen. Im Rahmen der Zertifizierung müssen die Verwender DPG-Farbe nachweisen, dass sie ordnungsgemäß mit der Flichen Informationen zur Zertifizierung von Dosen- und Etikettenherstellern zusammengefasst, und dort werden die Kontaktdaten der zugelassenen Zertifizierungsstellen genannt.

DPG-Markierung

- Um eine gute Auslesbarkeit der DPG-Markierung während des Rücknahmeprozesses zu garantieren, ist die Einhaltung von Vorschriften bei der Aufbringung des EAN-Codes und der DPG-Markierung einzuhalten. Der EAN-Code ist ausnahmslos als Leitercode auf den Gebinden aufzubringen. Es kann zwischen einem 8- und einem 13-stelligen EAN-Code gewählt werden. Die DPG-Markierung ist mittig über dem EAN-Code zu platzieren.
- Die Vorgaben für Größe und Farbe des EAN Codes orientieren sich an GS1-Vorgaben. So kann der EAN-Code von mind. 0,8 bis max. 2,0 der GS1-Zielgröße variieren. Eine weitere Anforderung zur Gewährleistung einer guten Auslesbarkeit ist die Einhaltung von Ruhezeiten rund um die DPG-Markierung. Dies erleichtert der Ausleseeinheit das Lokalisieren der DPG-Markierung auf dem Gebinde und beschleunigt somit den Ausleseprozess. Der EAN-Code muss auf weißem Hintergrund aufgebracht werden. Details zu den Vorgaben zur Aufbringung von EAN-Code und DPG-Markierung finden sich in einem Auszug aus der Technischen Verfahrensbeschreibung.

Barcodes

- Als Barcodes sind EAN-8 oder EAN-13 erlaubt (verbreitet)
- Aufbau der „GTIN“:
 - Land, Hersteller
 - Produktnummer, Prüfsumme
- Spezifiziert von der gs1-Gruppe
- Abfrage mit dem gepir-System im Web:
 - http://www.gepir.de/v3_client/

Identification			
Information Provider	4000004000	Last Change:	
Item GTIN	0400894802	Child items identification	Number Contained
Description			
Manufacturer's GLN	4053400000		
Item name	Jever Pilsener 0,33 l Fla Mw		
Brand name	Jever Pilsener		
Trade Item Unit	BASE_UNIT_OR_EACH		
Classification			
Category Code			
Measurement values			
Size	Net content		
More Info	http://www.sinfos.de		

Mit Barcodes arbeiten

- Barcodepedia:
 - <http://de.barcodepedia.com/4008535110689/>
- Barcodes mit PHP erzeugen:
 - <http://www.ashberg.de/php-barcode/>

ashberg.de - PHP-Barcode - Konqueror

Dokument Bearbeiten Ansicht Lesezeichen Extras Einstellungen Hilfe

http://www.ashberg.de/php-barcode/inc Google-Suche

Barcode Creation

Code:	<input type="text" value="4021375072399"/>
Size:	<input type="text" value="2"/>
Encoding:	<input type="text" value="Best fit"/>
	Hint: The most used barcode you can see on every supermarket-items is EAN (-13)
	<input type="button" value="Create-Bars"/>

Creation-Result

Image

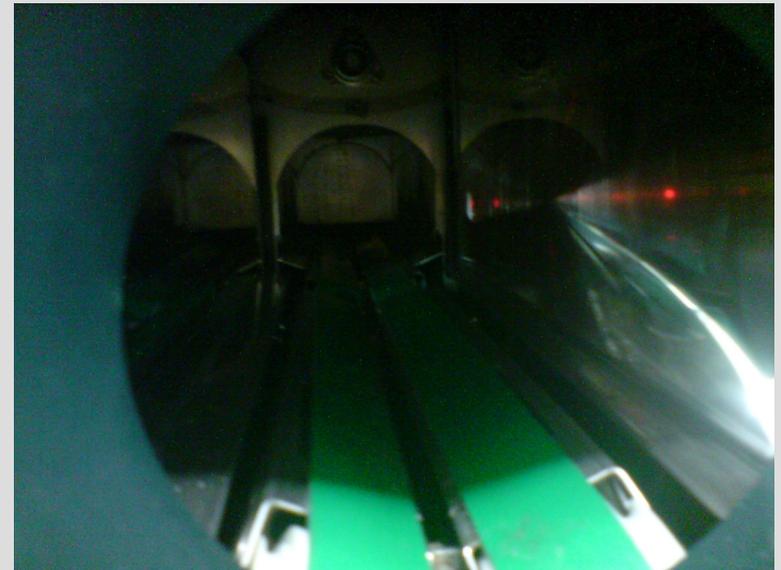


4 0 2 1 3 7 5 0 7 2 3 9 9

HTML-Code (Table with 1x1 black and white images)

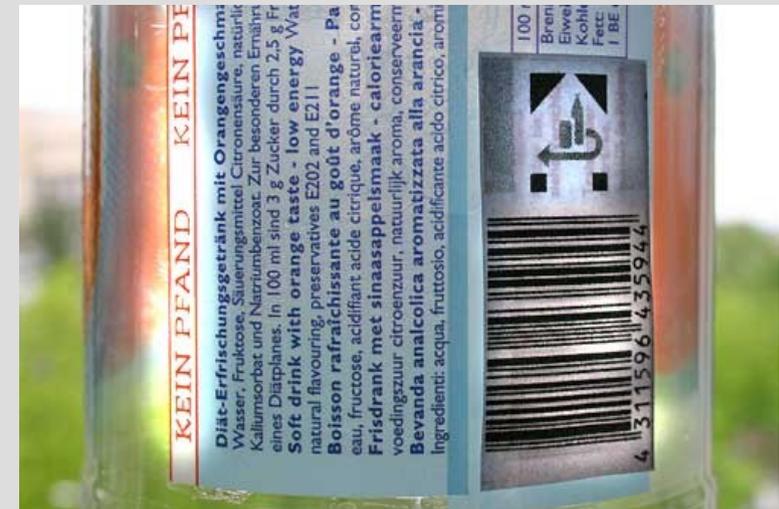
Voruntersuchungen

- Abkleben von Barcodes
- Abkleben von Pfand-Logos
- Kreuz-Umlabeln (Vertauschen von zwei gültigen Labels)
- Ergebnis: Die meisten Geräte sind sehr liberal
- Mehr Forschung an unterschiedlichen Geräten notwendig



Pfandbetrug I

- DIY-Ansatz, Home-Variante:
 - Barcode und Logo fotografieren
 - ausdrucken
 - aufkleben
 - funktioniert oft
- Viele Automaten haben keine aufwändigen Sicherungssysteme
 - Scan nach Barcode



Schadenspotential

- Im Einzelfall überschaubar
 - Gibt es Skaleneffekte?
 - Vergleich mit Kreditkartenbetrug
- Vermutlich Teil einer Risikobetrachtung
 - einige 100 Mio Euro nicht eingelöster Pfand wird Privat-Missbrauch vermutlich kompensieren

Pfandbetrug II

- Enterprise-Approach:
 - Oktober 2006 in Itzehoe
 - 150.000 Litauische Flaschenfälschungen
 - Wert: 37.500 Euro
 - wurden von Polizei auf Parkplatz gestellt
- Modellrechnung
 - 1 Flasche pro Sekunde (geübter Einlöser)
 - Parallel-Betrieb an zwei Automaten
 - 20 Stunden, 50 Minuten
 - rd. 1800 € Stundensatz, abzüglich der Herstellungskosten, aber viel Arbeit ...

IT-Ansatz

- Nicht zentraler Ansatz dieses Workshops
- Komplexes System aus Konten von Treuhändern, Händlern, Herstellern, etc.

DPG Deutsche Pfandsystem GmbH Roland Berger Strategy Consultants

Der Erstinverkehrbringer ist immer auch Pfandkontoführer – Pfandkontodienstleister kann nur Erfüllungsgehilfe sein

Ausgewählte Begrifflichkeiten (1)

nicht trennbar

Erstinverkehrbringer (EIV)

- Erstinverkehrbringer sind Unternehmen, die DPG-Verpackungen erstmals auf dem deutschen Markt in Verkehr bringen (insbesondere Abfüller und Importeure)
- Abweichende Vereinbarungen der beteiligten Unternehmen sind in bestimmten Fällen zulässig

Pfandkonto

- Ein Pfandkonto ist ein Konto, auf dem die Pfandgelder für in Verkehr gebrachte DPG-Verpackungen für die Forderungssteller des DPG-Systems verwaltet werden
- Die Einrichtung eines separaten Bankkontos ist nicht erforderlich

Pfandkontoführer (PKF)

- Pfandkontoführer ist jeder, der ein Pfandkonto führt und an den Pfandgeldforderungen gestellt werden

Pfandkontodienstleister (PKD)

- Pfandkontodienstleister ist ein von der DPG zugelassener Dienstleister, dessen sich der Pfandkontoführer zur technischen Abwicklung der Pfandkontoführung einschließlich des Anschlusses an die Stammdatenbank bedient
- Der Pfandkontodienstleister ist Erfüllungsgehilfe des Pfandkontoführers gem. § 276 BGB

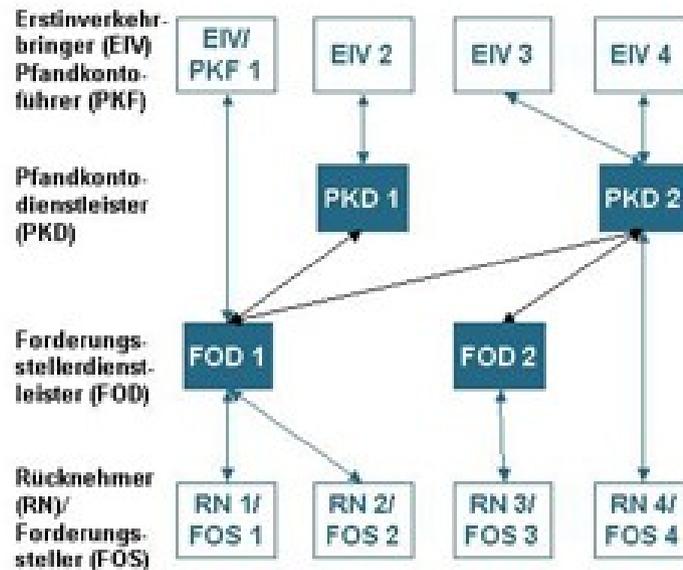
© 2007 DPG Deutsche Pfandsystem GmbH | www.dpg.de | Tel: +49 (0) 201 2400-1000

Hoher Aufwand

- Behälter müssen beispielsweise physikalisch vernichtet werden
- Aufwändige Prozesse

EIV und RN können Dienstleister beauftragen, die untereinander als "Bündelungsschnittstelle" abrechnen

Funktionsweise "Modulare Dienstleistung"



Quelle: Roland Berger, DPO



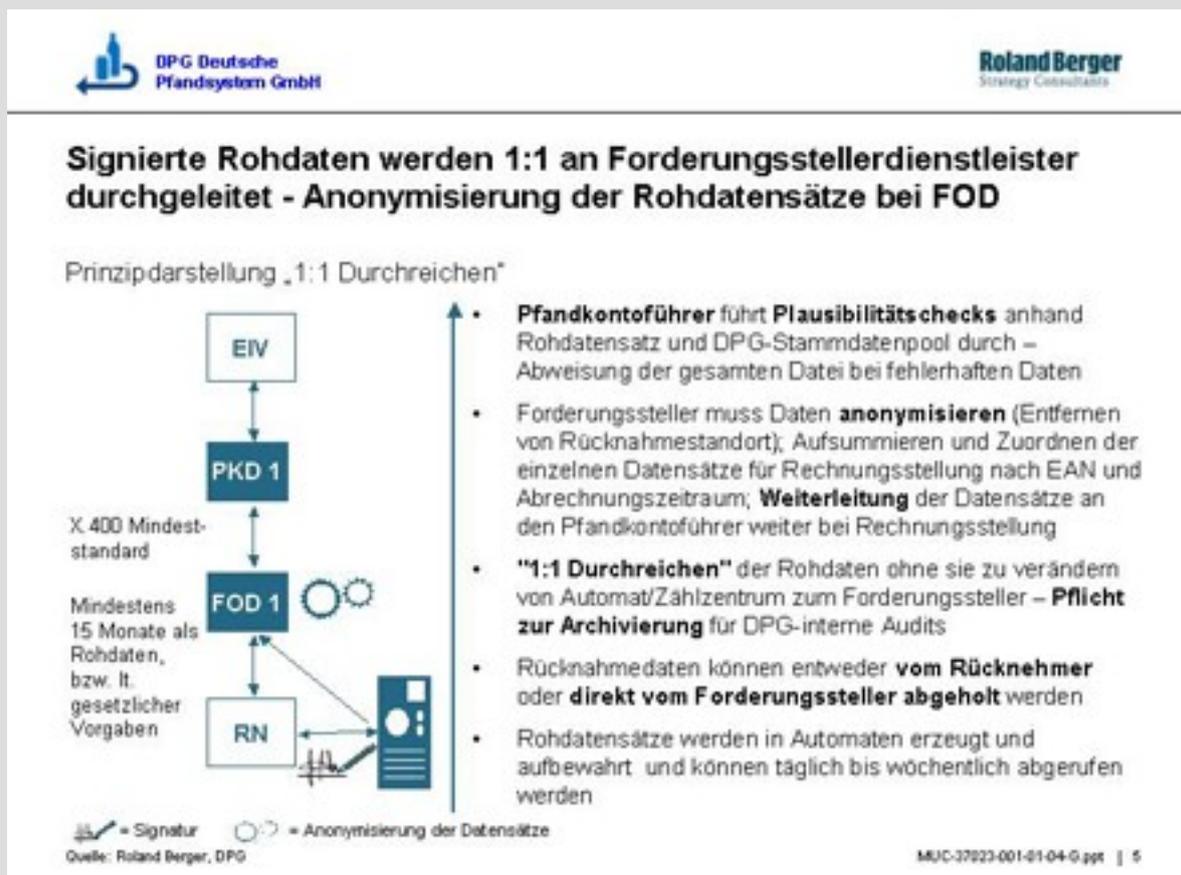
Vorteile:

- Jeder **Dienstleister** bietet unterschiedliche Dienstleistungen an
- Jeder **Kunde** (hier Händler) kann **modular** die Dienstleistungen **beauftragen** – auch **Aufteilung** der Aufgaben an **mehrere DL** möglich
- **Hohe Wettbewerbsintensität**
 - innerhalb der "Ebenen"
 - "Ebenen"-übergreifend (DL für Erstinverkehrbringer und Rücknehmer)

MUC-37923-001-01-04-0 ppt | 3

Security

- Jeder Behälter bekommt einen eigenen, elektronisch signierten Datensatz
- Aufwändiges „E-Mail“-System: X.400?!
- PKI-Infrastruktur
- Datenschutz?



Konzept Sicherheit

- Im Bereich der Datensicherheit muss dem Datenfluss, entlang dessen die Clearingmeldung generiert und transportiert wird, die höchste Aufmerksamkeit geschenkt werden. Dafür wird für jedes zurückgenommene Gebinde (in Rücknahmeautomaten oder im Zählzentrum) ein Datensatz erzeugt. Dieser Datensatz wird im Automaten signiert und anstelle der zurückgenommenen Einweggetränkeverpackung über den Forderungssteller an den Pfandkontoführer "zurückgegeben".
Um die Integrität der Rohdatensätze zu gewährleisten, wird ein asymmetrisches Public/Private-Key Verfahren zur Erzeugung von digitalen Signaturen eingesetzt. Die Vorgaben zur Signierung von Rohdatensätzen sind in der Signaturspezifikation beschrieben. Jeder einzelne Rohdatensatz, der im Automaten erzeugt wird, wird mit dem Private Key des jeweiligen Automaten digital signiert und zum Forderungssteller/-dienstleister übertragen. Um diese Daten verwenden zu können, ist es notwendig, die öffentlichen Schlüssel aller Automaten allen Systemteilnehmer bekannt zu machen. Dies geschieht durch Ablage der Public Keys in der Stammdatenbank. Der Forderungssteller/-dienstleister anonymisiert die Rohdaten vor Weitergabe an den Pfandkontoführer/-dienstleister.

Abrechnung

- Mit der Rechnung (in Papierform oder elektronisch) übermittelt der Forderungssteller/-dienstleister dem Pfandkontoführer/-dienstleister die ihn betreffenden, signierten Rohdatensätze elektronisch, verdichtet nach EAN und Rechnungszeitraum. Bevor ein Pfandkontoführer/-dienstleister eine Pfandabrechnung vornimmt, kann er auf Basis des Rohdatensatzes und den Stammdaten zur Automatenutzung der DPG-Stammdatenbank die Plausibilität der Rechnung prüfen. Die Abwicklung der Pfandabrechnung zwischen Pfandkontodienstleister und Erstinverkehrbringer kann durch eine bilaterale Vereinbarung geregelt werden.

Links

- Einige Bilder wurden von den jeweiligen öffentlichen Websites der Organisationen und Hersteller als Zitat übernommen
- Einige Bilder wurden aus der Wikipedia entnommen und stehen unter CC
- Übersichts- und Hintergrundinformationen dank Hilfe von Wikipedia und diversen Blogs
 - <http://larryluca.wordpress.com/2007/06/18/>

Kontakt

- Nils Magnus
magnus@linuxtag.org



- Schamlose Werbung:
 - LinuxTag vom 28. - 31. Mai 2008 hier in Berlin
 - CfP läuft noch bis zum 11. Januar!
- Einladung:
 - Free-Software-End-of-Year-Lounge-Reception
 - Morgen, 28.12.2008 ab 20 Uhr bei newthinking (Tucholskistr. 48)