Worldline Pay Online Watcher

AK Payment 27.05.2004

Dr. Andreas Schikarski

Überblick

- **Kartenbetrug und Fraud - Module**
- **WLP Online Watcher**
- **Einsatz des WLP Online Watchers bei Visa Austria**

Probleme mit Fraud?

"Card related crime is the fastest-growing criminal activity in the UK – and throughout europe, payment card systems are under unprecedented attack from well-organized and financed criminal gangs"

(European Card Review Nov/Dec 2000)

" Der Betrug mit Scheck- und Kreditkarten stieg 2003 in Deutschland rasant. Die Zahl der Delikte wuchs, wenn beim Bezahlen nur eine Unterschrift zu leisten ist und keine PIN-Nummer (Geheimzahl) gefordert wird. Die Polizei registrierte im vergangenen Jahr insgesamt 64.507 solcher Fälle, nahezu 60 Prozent mehr als 2002."

(Kriminalstatistik des deutschen Innenministers für 2003)

Fraud – Typen: Kreditkarte

- **Counterfeit fraud (Kartenfälschung)**
  - Physische Kopie der Karte
  - Elektronische Kopie der Karte
    - Skimming (Mitschneiden der Magnetstreifendaten)
- **Card not present fraud**
  - Daten des Magnetstreifens
  - Mailorder / Telephone order
  - Internet
- **Lost or stolen cards**
- **Mail non-receipt fraud**
  - Karte/PIN auf dem Postweg abfangen
- **Identity theft**
  - Kartenantrag
  - Konto auf anderen Namen ummelden
- **ATM Fraud**
  - PIN ausspionieren, Karte stehlen / kopieren

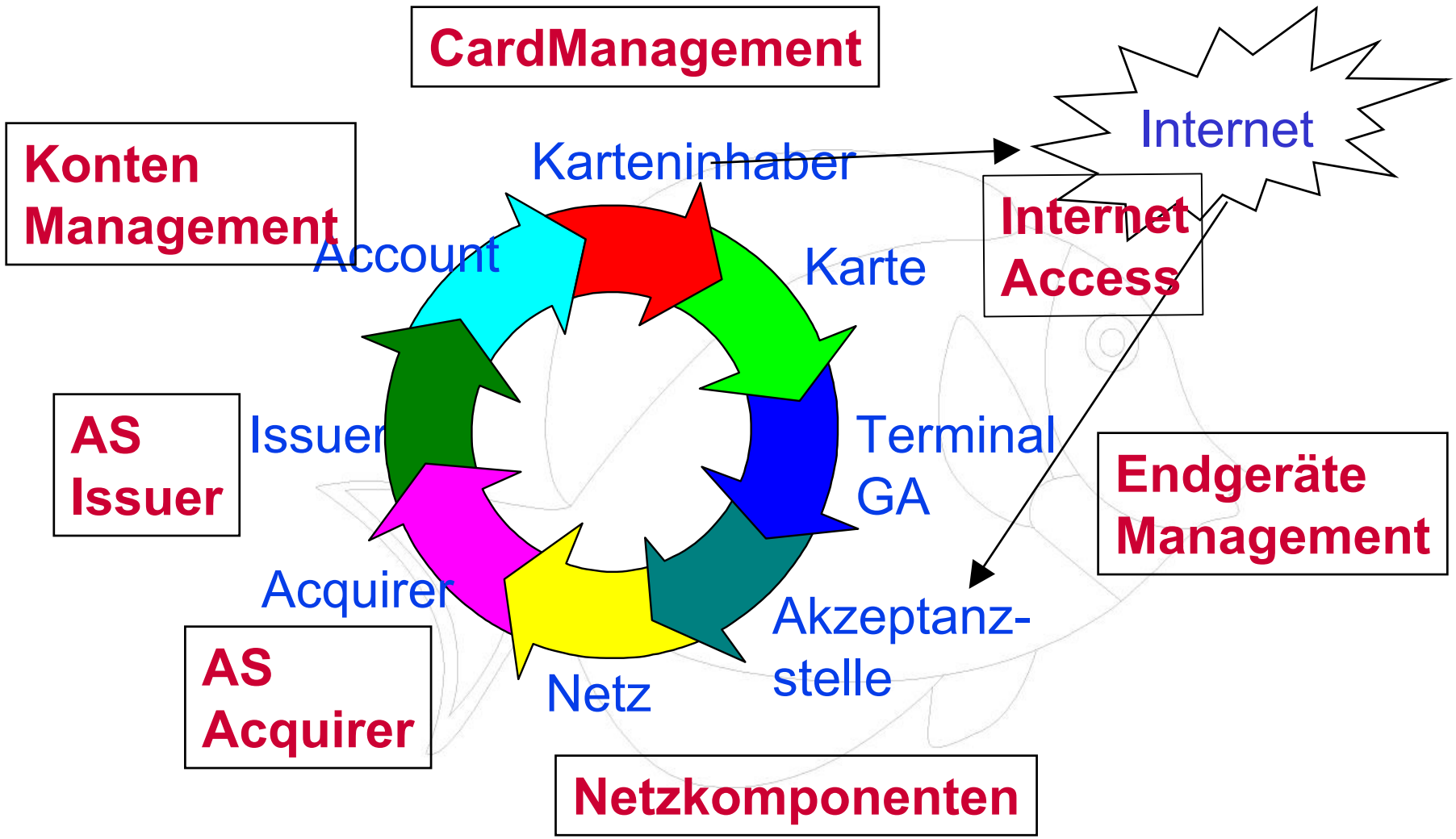
Fraud in Zahlen

- **Beispiel England:**
- **Gesamtverlust durch Fraud 2001: 411.4 Million Pound**

Counterfeit card	160.3	(39%)
Card not present	95.7	(23%)
Lost /stolen	114.0	(28%)
Mail non-receipt	26.7	(6%)
Application fraud	6.6	(2%)
Other	8.0	(2%)

(Quelle: UK APACS/ cardwatch.org)

Kartenzahlungszyklus



Fraud Control in Transaktionssystemen

- **Online Transaktionssysteme**
  - Netzwerk routing/switching (NOV-Verbund)
  - Acquirer Systeme (Kopfstellen; Ersatzautorisierung)
  - Issuer System (Autorisierer)
- **Fraud Erkennung**
  - Erkennen von betrügerischen Transaktionen,
  - Alarmgenerierung, Auswertung, Ergreifen von Gegenmaßnahmen
  - Z.B. Scannen von Transaktionen im Batch, herausfinden von Betrugsmustern
- **Fraud Verhütung**
  - Prüfen aller Transaktionen auf Betrugsverdacht,
  - Ablehnen verdächtiger Transaktionen
  - Z.B.: online prüfen gegen regelbasiertes System

Klassifizierung von Online Fraud Modulen

- **Parametrisierbare, implementierte Regelwerke**
  - Karteneinsatz: wie oft ? Welche Umsätze ?
  - Filialwanderung
  - Geschwindigkeitsprüfung (geographisch)
  - Kilometerzähler/Tankstand
  - Beispiel: POSEIDON OLTP Fraud Modul
- **Editierbare, interpretierte Regelwerke**
  - Beispiel: WLP Online Watcher
- **Künstliche Intelligenz**
  - Beispiel: VISOR (Visa International Europe)

Vor- und Nachteile von Fraud Modulen

- **Parametrisierbare, implementierte Regelwerke**
  - + effiziente Implementierung
  - - Regelwerke bekannt
- **Editierbare, interpretierte Regelwerke**
  - + sehr schnelle Reaktion auf neue Fraud-Muster
  - + sehr breites Regelspektrum
  - - Aufwände im Regelmanagement
- **Künstliche Intelligenz**
  - + (theoretisch) unbegrenztes Regelspektrum
  - + kein Regelarchitekt notwendig
  - - Resultate oft nicht nachvollziehbar
  - - aufwändiges “Füttern” der Systeme

Überblick

- Kartenbetrug und Fraud - Module
- **Worldline Pay Online Watcher**
- Einsatz des Worldline Pay Online Watchers bei Visa Austria

Worldline Pay Online Watcher

- Frühzeitiges Erkennen betrügerischer Transaktionen
- Online-Überwachung von Payment Systemen über benutzerdefinierte Betrugserkennungs-regeln
- Alarmgenerierung bei Erkennung eines Betrugverdachts,
- Ggf. Einfluss auf Transaktionsantwort
- Einfache/flexible Handhabung

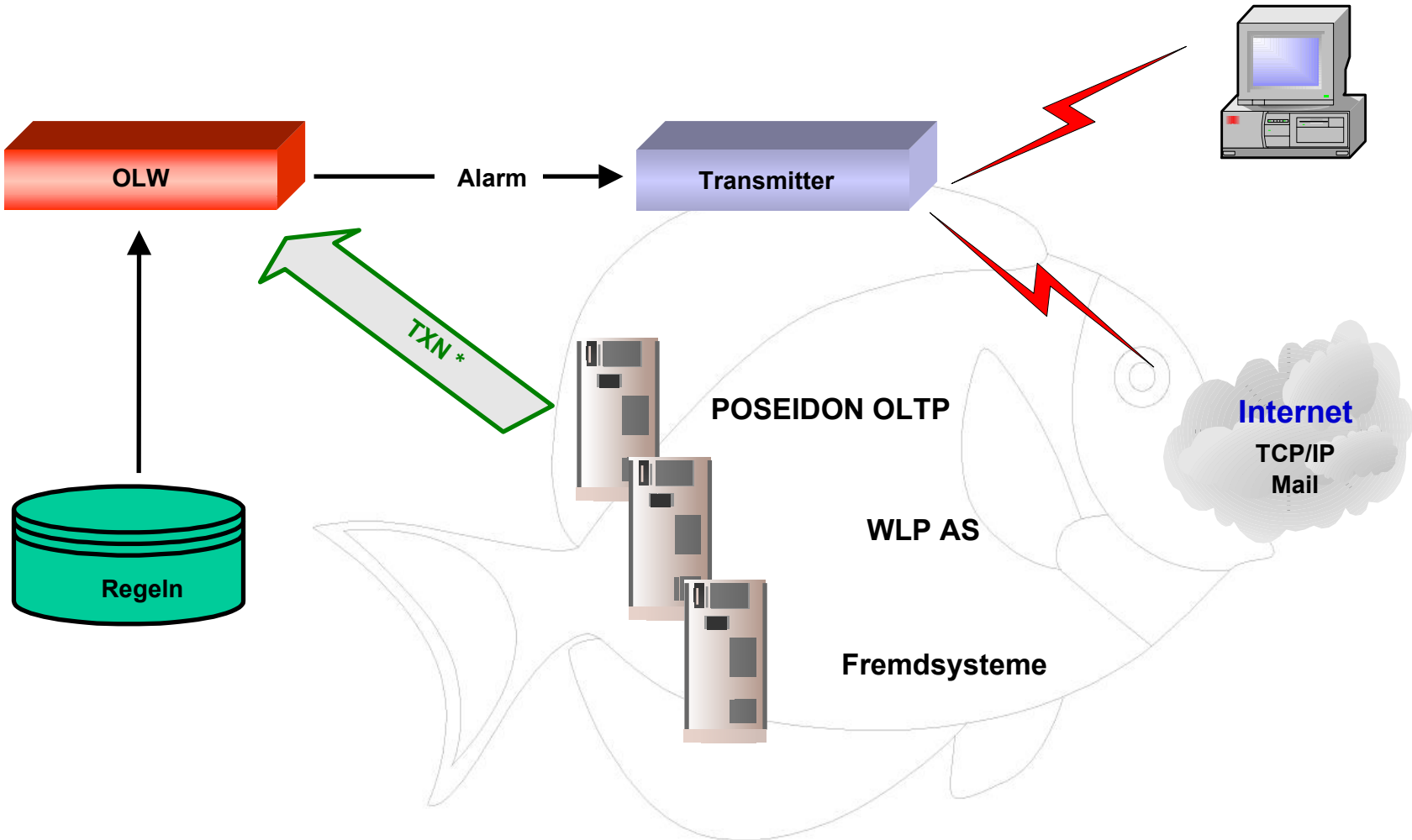
Anwendungsbeispiele Online Watcher

- Unüblich hoher Branchenumsatz im Inland, z.B. Flugreise teurer als 2500 €
- Gefälschte Karten werden im Ausland exzessiv für unübliche Einkäufe eingesetzt (z.B. Optik in Südostasien, Lebensmittel in Lateinamerika)
- Neu herausgegebene Karten werden bei der Zustellung entwendet und sofort eingesetzt
- Diebe testen gestohlene Karten am GAA

Ablauf Worldline Pay Online Watcher

- Online Watching Prozess „Watcher“ liest beim Start Regeln aus der Datenbank
- Alle Transaktionen werden asynchron oder synchron an den Watcher übergeben
- Regeln werden angewandt
- Bei Zutreffen Alarmgenerierung und /oder Rückgabe eines passenden Antwortcodes
- Veröffentlichung von Alarmmeldungen bei Betrugsverdacht über Transmitter-Prozess

Skizze Ablauf OLW



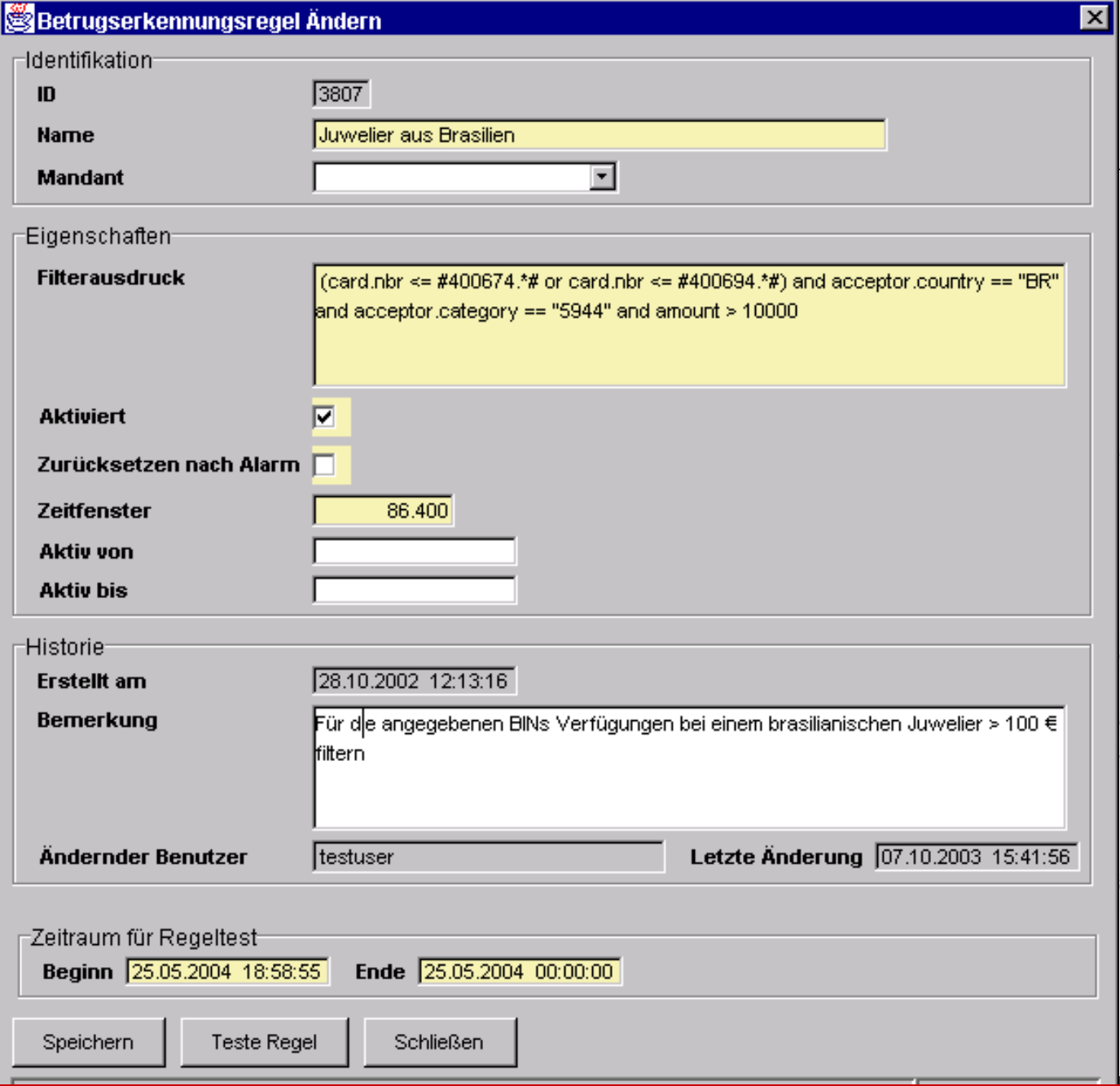
TQL: Online-Anfragesprache für Transaktionen

- Einfache, getypte interpreter-Sprache des WLP Transaktionsprotokolls
- Konstanten, Variablen, Operatoren und Funktionen
- Interne und externe Felder der Transaktion können als Variable abgefragt werden
- Spezialfall „Filter“ gibt Boolean zurück
- Verwendung für Regelwerke WLP OLW (Filter, Regeldimensionen, Inhalt der Alarm-Mail) sowie in WLP AS (Workflow)

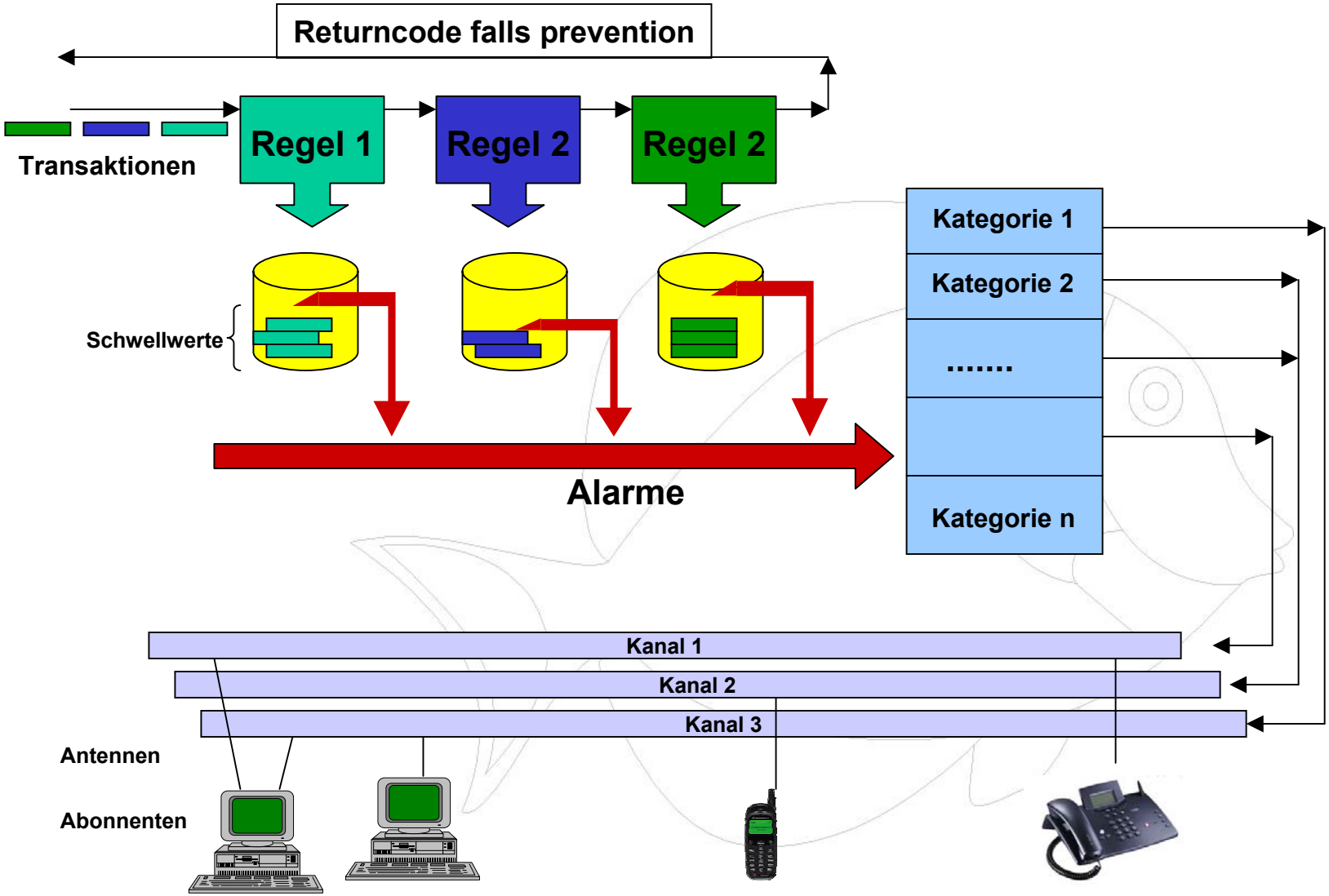
Regelbeispiel

- **Filtern aller Transaktionen, für die gilt**
  - Issuer = x oder Issuer = y
  - Einsatz in Brasilien in einer Juwelerie nach 20 Uhr
  - Betrag > 100 €
- **Sammeln der Transaktionen in 2-dim Taschen-Feld**
  - Karten-Nummer
  - Merchant-ID
- **Schwellwerte zur Alarmgenerierung: Anzahl und Gesamtbetrag der Transaktionen in einer Tasche**
  - 2 Transaktionen und mind. 600 € -> Alarm
  - 3 Transaktionen und mind. 1000 € -> Ablehnung
- **Verweildauer der Transaktionen in einer Tasche**
  - 24 Stunden

Regelscreen: Beispiel



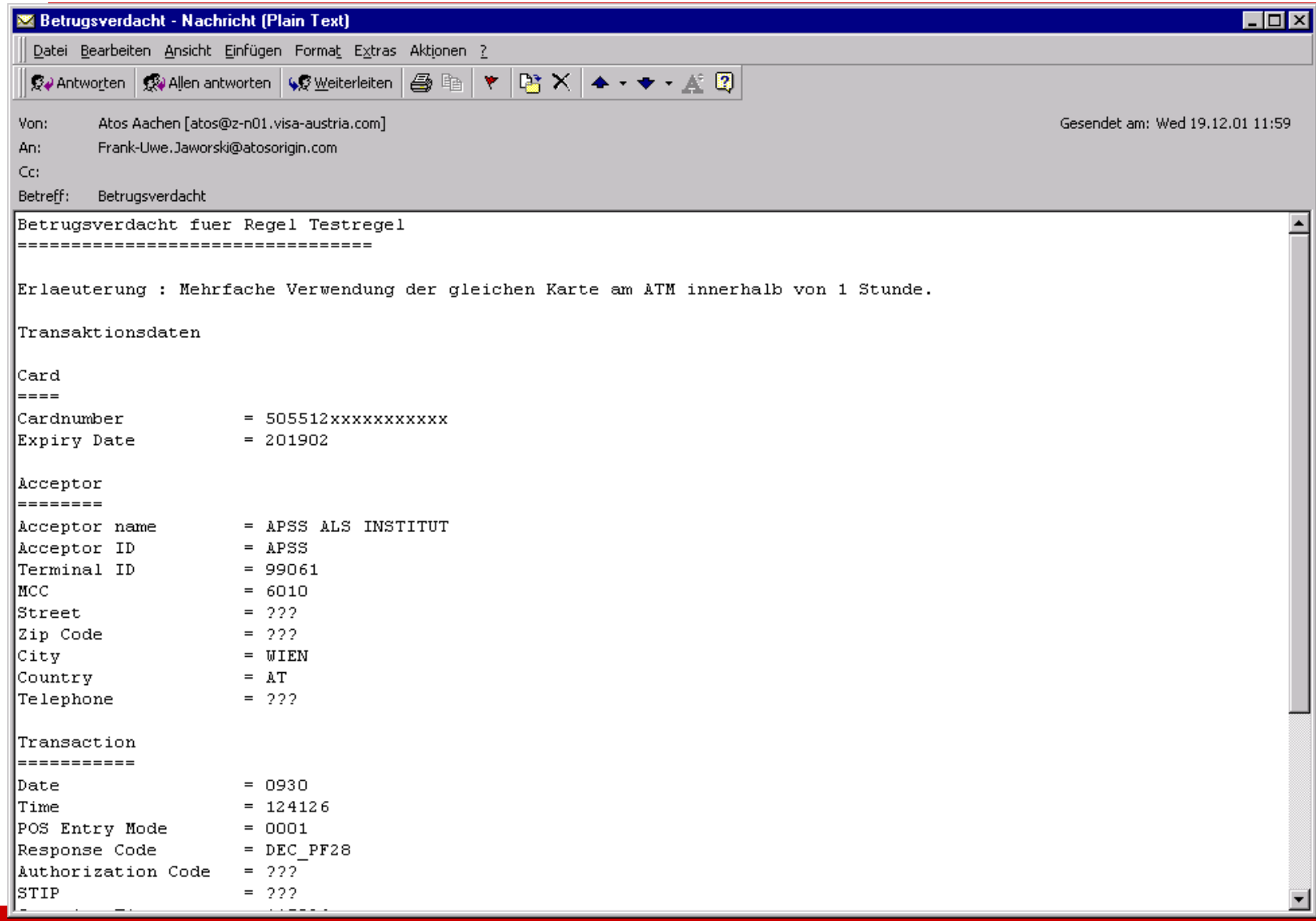
Online Watcher: Prinzip



Alarmierungskonzept WLP OLW

- Schwellwerte der Regeln werden frei wählbaren Betrugskategorien zugeordnet, z.B. „schwerer Betrug“, „Kartenmißbrauch in Lateinamerika“
- Für jede Betrugskategorie wird festgelegt, auf welchem Kanal Betrugsalarme veröffentlicht werden
- Alarm: Senden einer Nachricht auf einem Kanal
- Verteilen der Nachricht an die Antennen, die den Kanal abonniert haben
- Abonnenten der Antennen erhalten die Nachricht per Mail

Alarmierung



Betrugsverdacht - Nachricht (Plain Text)

Datei Bearbeiten Ansicht Einfügen Format Extras Aktionen ?

Antworten | Allen antworten | Weiterleiten

Von: Atos Aachen [atos@z-n01.visa-austria.com]
Gesendet am: Wed 19.12.01 11:59
An: Frank-Uwe.Jaworski@atosorigin.com
Cc:
Betreff: Betrugsverdacht

```
Betrugsverdacht fuer Regel Testregel
====================================

Erlaeuterung : Mehrfache Verwendung der gleichen Karte am ATM innerhalb von 1 Stunde.

Transaktionsdaten

Card
====
Cardnumber            = 505512xxxxxxxxxx
Expiry Date           = 201902

Acceptor
========
Acceptor name         = APSS ALS INSTITUT
Acceptor ID           = APSS
Terminal ID           = 99061
MCC                   = 6010
Street                = ???
Zip Code              = ???
City                  = WIEN
Country               = AT
Telephone             = ???

Transaction
===========
Date                  = 0930
Time                  = 124126
POS Entry Mode        = 0001
Response Code         = DEC_PF28
Authorization Code    = ???
STIP                  = ???
```

Regeltest

- Anwendung der Regeln auf abgespeicherte Transaktionen eines zurückliegenden Zeitraumes
- Ausgabe der Transaktionen, die zu einem Alarm geführt hätten
- Testen der Regeln erfolgt vom GUI aus über einen eigenständigen Server

Flexibilität

- Regeln werden vom Benutzer per GUI definiert
- Regeltest per GUI

➢ schnelle und einfache Möglichkeit, neue Regeln einzubringen

➢ schnelle Antwort auf neue Betrugsmuster

➢ Wahlweise zur Erkennung/Alarmgenerierung oder

➢ Betrugsprävention einsetzbar

Weitere Informationen

Andreas Schikarski

Product Manager

Payment Systems Integration

Atos Origin GmbH

Tel.: 02408 148 174

Fax: 02408 148 204

e-mail: Andreas.Schikarski@atosorigin.com

Überblick

- Kartenbetrug und Fraud - Module
- Worldline Pay Online Watcher
- Einsatz des Worldline Pay Online Watchers bei Visa Austria