Sicherheit im OnlineBanking:

Mit Sm@rtTAN optic für die Zukunft gut gerüstet

Online-Banking-Sicherheit der 3. Generation

Detlev Mergemeier
Portfoliomanagement Vertriebswege
GAD eG, Münster

© GAD 2010

Das Unternehmen

- IT-Beratungs- und Kompetenzcenter, Softwarehaus und Rechenzentrum für
  - 441 Volksbanken, Raiffeisenbanken sowie Retailbanken im deutschsprachigen Raum
  - WGZ BANK, DZ BANK, genossenschaftliche Verbundunternehmen

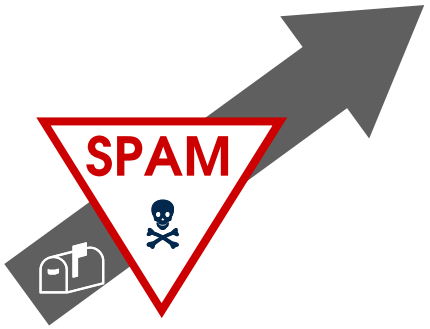
Agenda

1. **Entwicklungen und Tendenzen im Online-Banking**
2. Antworten des ZKA
3. Umsetzung bei der GAD eG
4. Ausblick in Produktdiversifikation

Tendenzen im Online-Banking – Waren die Sicherheitsprobleme damals absehbar?

GAD
IT für Banken

Marktprodukte für man-in-the-middle-attacks



Browser(un)sicherheit!

Online-Banking Nutzung

Chipkarten-Infrastruktur bisher nicht durchsetzbar!

SSL V3.0 ohne Client-Zertifikate

Java-Applets nicht mehr State-of-the-art!

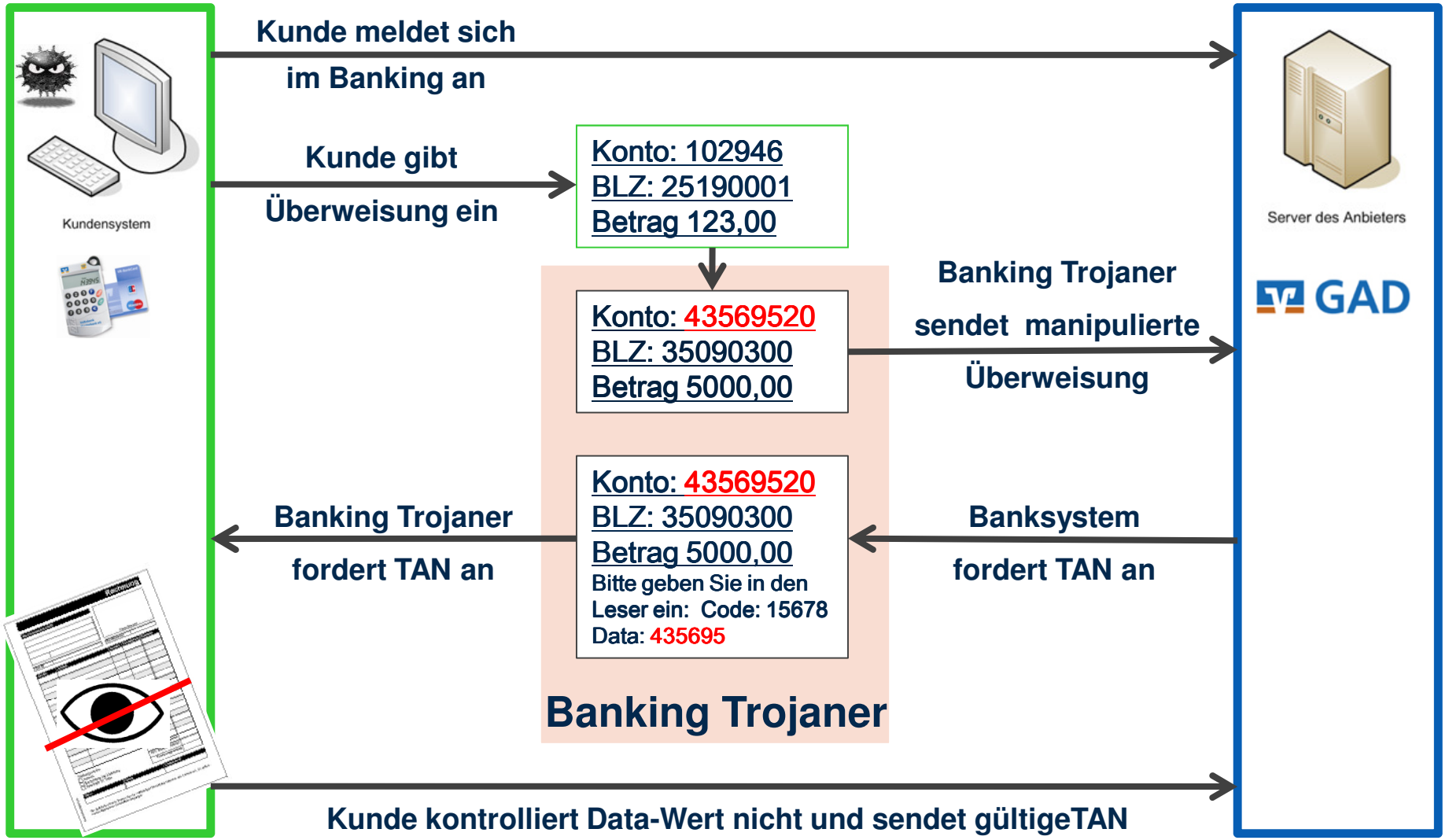
Geschlossenes Btx-Netz wird abgeschaltet!

Jdjnknkjnhenkndbvuieqjkfd
jkdnfv kjdnv njknv jkdnv
kxn kdjn jn cjn
Fdkhefnheknknjknekn
lkmvkmv lk
Kjhfnnuihen dnfg dir
dnnnf j

Wesentliche Angriffsarten treffen Kunden

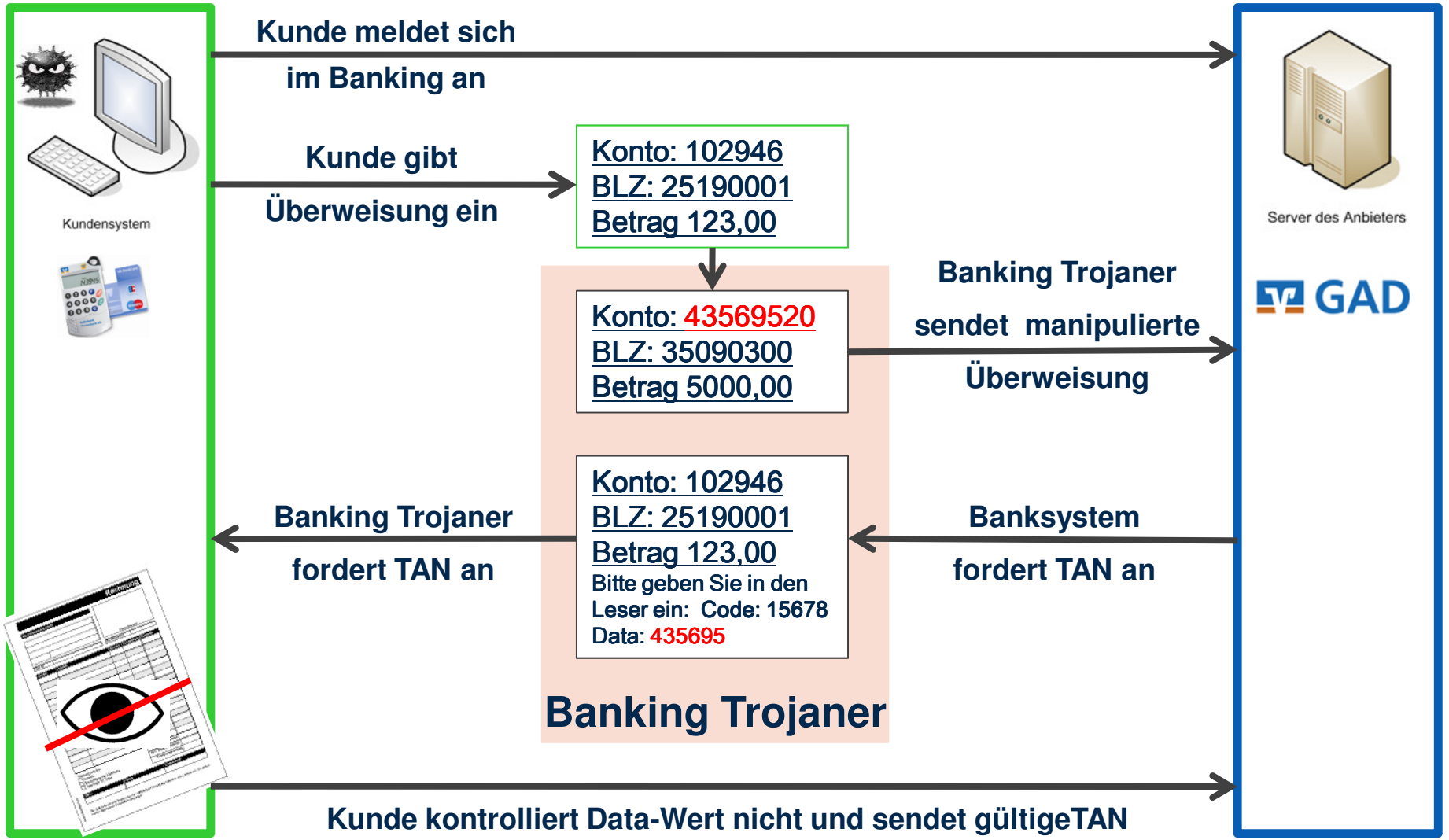
- Klassisches Phishing
  - eMails locken den Kunden auf nachgebildete WEB-Seiten und fragen viele iTANs ab
- iTAN-Diebe
  - Banking-Trojaner blenden direkt nach dem Login eine Abfrageseite für viele iTANs ein
- Echtzeitmanipulationen
  - Banking-Trojaner manipuliert eine Überweisung unsichtbar für den Kunden zugunsten der Betrüger. Durch Eingabe einer TAN (iTAN oder ohne Prüfung bei Sm@rtTAN plus) bestätigt der Kunde eine betrügerische Überweisung.
- Hintergrundüberweisung
  - Banking-Trojaner führt unsichtbar für den Kunden im Hintergrund eine Überweisung durch und erfragt unter einem Vorwand eine TAN.

Angriffsszenario Sm@rtTAN plus



© GAD 2010

Angriffsszenario Sm@rtTAN plus - Maskerade



© GAD 2010

Lösung: Der Auftragskontext muss in die TAN-Berechnung mit einfließen

Alternative 1: abgesetzte Einheit

- Relevante Auftragsdaten werden entweder optisch in ein TAN-Lesegerät übertragen oder müssen vom Kunden abgetippt werden (BackUp).
- Die Daten werden im Display des TAN-Lesegeräts angezeigt.
- Der Kunde kann die Daten dort prüfen und auf der TAN-Leser-Tastatur bestätigen.
- Die von der Chipkarte erzeugte TAN wird am Browser eingetippt.

Alternative 2: Kanaltrennung

- Relevante Auftragsdaten und die zugehörige TAN werden per SMS an ein registriertes Mobiltelefon übertragen.
- Der Kunde kann die Daten dort prüfen.
- Bei korrekten Daten tippt der Kunde die angehängte TAN am Browser ein.

Agenda

1. GAD Unternehmensprofil
2. Entwicklungen und Tendenzen im Online-Banking
3. **Antworten des ZKA**
4. Umsetzung bei der GAD eG
5. Ausblick in Produktdiversifikation

Das ZKA-Kompendium „Online-Banking-Sicherheit“ zeigt die Strategien des ZKA auf

- chipTAN
  - Optisch gekoppelt und manuell (BackUp)
  - Basis: Karte und TAN-Lesegerät
- mobileTAN
  - Rahmenbedingungen für den Einsatz

- … und für den angeschlossenen Betrieb:
  - HBCI-Karte
  - Secoder

Die Karte steht im Mittelpunkt.

ZKA Banken-Signaturkarte

Verlag_R2D2_04586142004

chipTAN-Eigenschaften auf Basis des HHD-Standards in der Version 1.3.2

- Integrierte Dialogsteuerung auf Basis eines „Start-Code“ mit
  - 9 Auftragsklassen
  - 10 Schablonen
  - 8 Basisdatenelementen
- Wesentliche Eigenschaften eines Auftragskontexts werden abgesichert
- Zufallszahl im Start-Code sorgt für die Freshness
  ➔ Daten müssen online bestätigt werden
- Zwei Betriebsarten:
  - manuell: Start-Code und Kontextdaten müssen eingegeben werden
  - optisch: Daten werden optisch übertragen und müssen nur noch mit „OK“ bestätigt werden

Neu in HHD V1.3.2: Start-Code enthält eine definierte Dialogsteuerung

Schablone

1	Betrag und Konto/IBAN
2	Konto/IBAN
3	Betrag
4	Konto/IBAN und Betrag
5	Betrag und Kontonummer
6	Kontonummer
7	Kontonummer und Betrag
8	Betrag und IBAN
9	IBAN
0	IBAN und Betrag

Dialogsteuerung im Start-Code bei manueller Betriebsart

Auftragsklassen

Auftrags-klasse k	Transaktionsdaten
1	Einzelauftrag, Inland
2	Einzelauftrag, SEPA
3	Einzelauftrag, Ausland
4	Sammelauftrag, Inland
5	Sammelauftrag, SEPA
6	Sammelauftrag, Ausland
7	Wertpapier
8	Laden PrePaid oder GeldKarte
9	Diverse

Basisdatenelemente

1	Betrag	9 + 2
2	Konto/IBAN	
3	OBanking-PIN	
4	Telefon	
5	Zusatzdaten	
6	Anzahl	
7	Kontonummer	12
8	IBAN	

Steuerung

9	1	7	1	<Zufallszahl>

Start-Code

```
Einzelauftrag
Inland
```
ok

```
Betrag:
        200,01
```

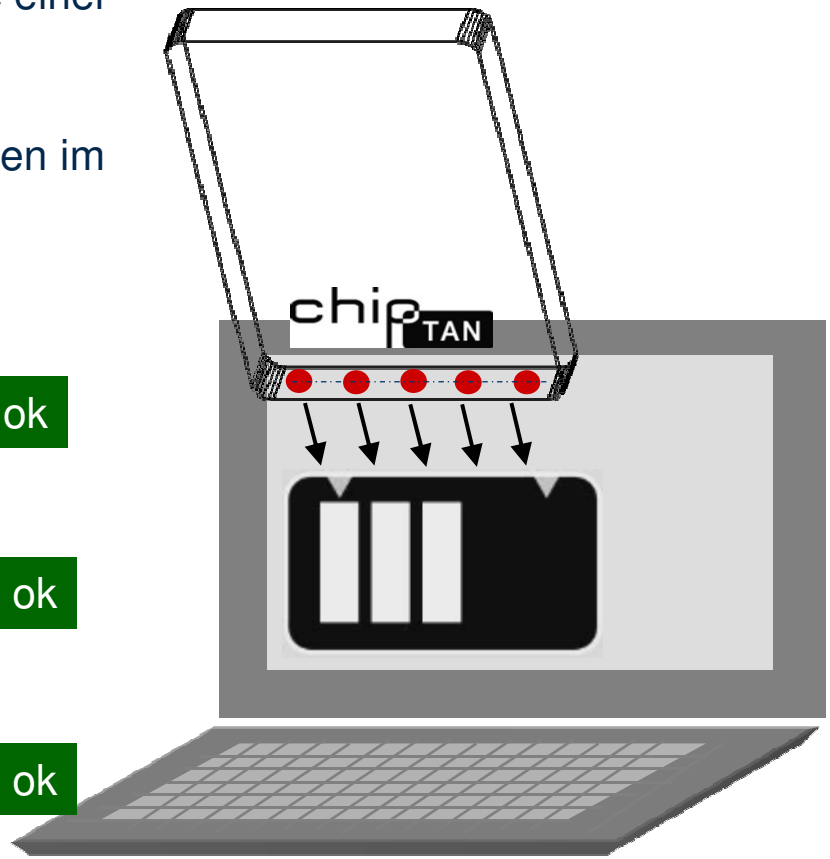
```
Kontonummer:
    0123456789
```

```
TAN:
        123456
```

Das Prinzip der optischen Kopplung bei chipTAN

- Über optische Sensoren werden die Signale einer animierten Grafik im Browser bzw. im Kundenprodukt empfangen
- Alle im Start-Code adressierten Felder werden im ersten Schritt komplett übertragen

- Anschließend werden sie dann einzeln angezeigt und müssen vom Kunden nur noch mit „OK“ bestätigt werden
- Mit Hilfe des ZKA EMV TAN-Generators auf der SECCOS-Karte wird die TAN berechnet



Agenda

1. GAD Unternehmensprofil
2. Entwicklungen und Tendenzen im Online-Banking
3. **Umsetzung bei der GAD eG**
4. Ausblick in Produktdiversifikation

Die Roadmap der Sm@rtTAN-Verfahren bei der GAD

Sm@rtTAN

Herbst 2003 bis Mai/Juni 2009

- Einstieg in Hardware
- TAN auf Knopfdruck
- Komfortgewinn
- Damals sicher:
  - TANs aufsteigend
  - nur 1 TAN statt 50

Sm@rtTAN plus 1.2

Seit Herbst 2006

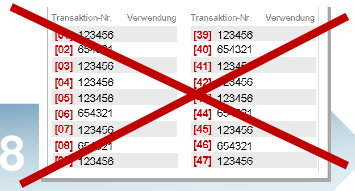
- Erster ZKA-Standard
- Auftragsdaten gehen in TAN-Berechnung ein
- Drastische Reduzierung möglicher Bedrohungen

Sm@rtTAN optic 1.3.2

Seit Frühjahr 2009

- Komfortgewinn durch optische Kopplung
- Manuell weiterhin als BackUp unterstützt
- Optimierte Dialoge bringen noch bessere Absicherung

TAN-Bogen bis Frühjahr 2008



Sm@rtTAN bis Frühjahr 2009

Fachrat-entscheidung 06.09.2007

Bei der GAD steht die Karte im Mittelpunkt

Sm@rtTAN –
die TAN per Knopfdruck

Sm@rtTAN plus und
Sm@rtTAN optic
– erhöhte Sicherheit

HBCI mit Secoder –
sicherheitsgeprüft

www.die-signaturkarte.de

Unterstützung der Banken durch GAD und DG VERLAG

GAD IT für Banken

- Umstellungslisten
  - Aufstellung über umstellungsrelevante TAN-Listen-Kunden
- Vergleichsrechnung

50 TAN pro Jahr,
50 TAN pro Bogen,
TAN Bogen =4,50 €
(günstig gerechnet)

=

Haltbarkeit Kartenleser
2-3 Jahre
ca. 8-10 Euro

Transaktion-Nr.	Verwendung	Transaktion-Nr.	Verwendung
[01]	123456	[39]	123456
[02]	654321	[40]	654321
[03]	123456	[41]	123456
[04]	123456	[42]	123456
[05]	123456	[43]	123456
[06]	654321	[44]	654321
[07]	123456	[45]	123456
[08]	654321	[46]	654321
[09]	123456	[47]	123456

Unterstützung der Banken durch GAD und DG VERLAG

Umstellung zu endlastig –
bei Banken und bei Kunden

UMSTELLUNGS-
TERMIN

- Abhilfe: Frühzeitige und ausführliche Information von Instituten und Kunden
- Bereitstellen von Informationsmaterial
  - Flyer, verständliche Verfahrensbeschreibungen
  - Hilfefunktionen, Flash-Animationen
- Frühzeitige Schulung von Bankmitarbeitern

Agenda

1. GAD Unternehmensprofil
2. Entwicklungen und Tendenzen im Online-Banking
3. Umsetzung bei der GAD eG
4. **Ausblick in Produktdiversifikation**

Die neue HHD V1.4 stellt eine Weiterentwicklung des Standards dar

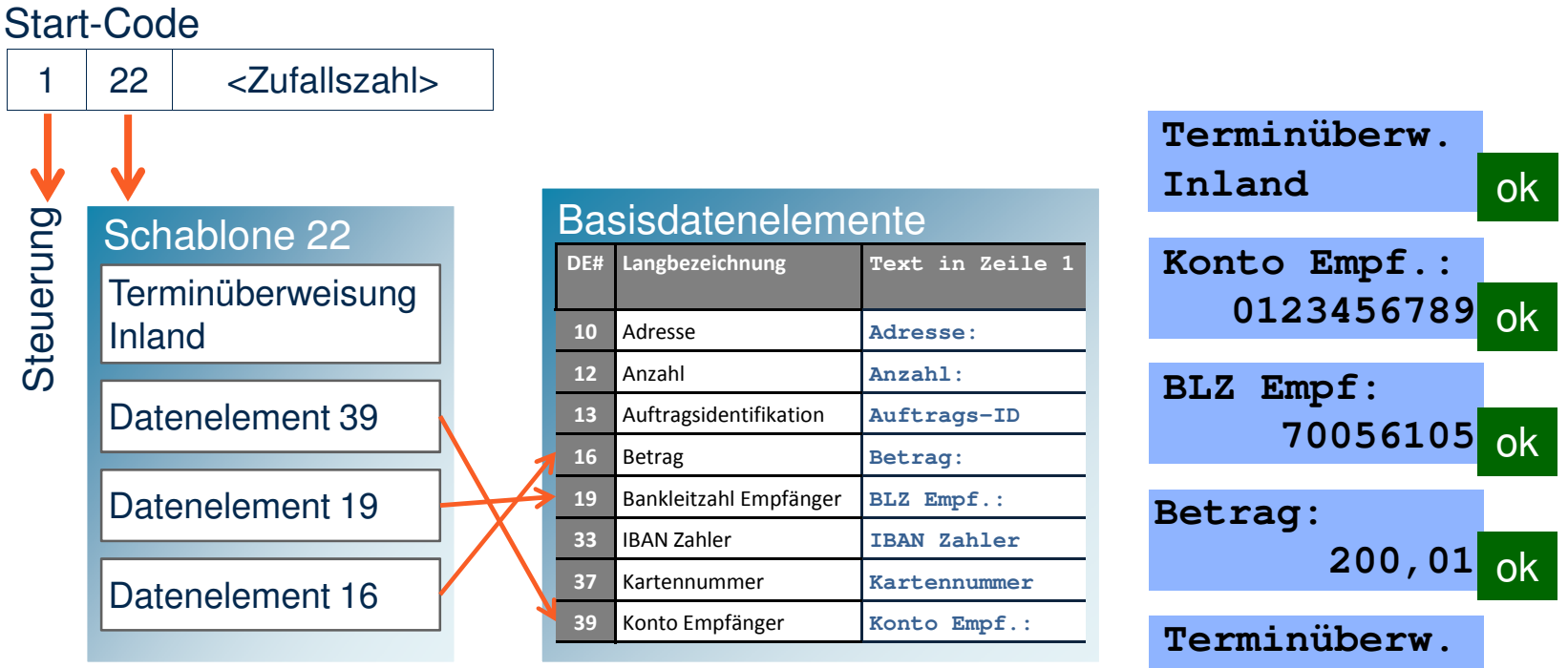
- HHD V1.4 schließt durch verfeinerte Dialogsteuerung weitere Restrisiken aus
- Ca. 70 Visualisierungsklassen und 40 Datenelemente decken nun den gesamten Bereich des Online-Banking ab
- Fachlich abgestimmte Schablonen ermöglichen einheitliches Sicherheitsniveau über alle Institute hinweg
- Die Selektionstechnik lässt aber auch Freiraum für spezielle Anwendungsgebiete
- IBANs können durch Subdialoge in bis zu drei Zeilen dargestellt werden
- Eine implizierte Versionsübermittlung sorgt für korrekte Verarbeitung bei Kunde und Institut
- Ansteuerung der SECCOS TAN Credit Applikation ermöglicht neue Szenarien im Kreditkartenbereich

HHD V1.4 Visualisierungsklassen – strukturiert und offen für zukünftige Anwendungen

Kennzeichen einer Visualisierungsklasse

Trennung nach	Zahlungsverkehr	Inland SEPA Ausland
	Richtung des Geldflusses	Überweisung Lastschrift
	optimale Verständlichkeit	„eigenes Konto“ „Konto Zahler“ „Empfänger Konto“ „Referenz Konto“
	spezialisierte Begriffe	„Auftrags-ID“ „Angebotsnummer“ „WKN“ oder „ISIN“ „Stücke/Nominal“ „Menge“

Der HHD V1.4 Ablauf mittels Schablonentechnik



Ausblick in Produktdiversifikation

- Ist der Schutz durch die aktuellen Verfahren ausreichend?

  geringe Restrisiken sind durch ZKA-Sicherheitsuntersuchungen und Gutachten identifiziert und bekannt.

  Diese werden auch in neuen Versionen in immer größerem Maße abgewehrt.

  Aber: gezwungenermaßen leidet dadurch der Benutzerkomfort.

- Weiterentwicklung ist als permanenter Prozess zu sehen,

  denn …

der Wettlauf mit den Angreifern wird weiter gehen.

Kontaktdaten:

Detlev Mergemeier
Portfoliomanagement / Produktfeld Vertriebswege
Tel.: 0251 7133 - 2612 ; Fax.: 0251 7133 – 92612
detlev.mergemeier@gad.de

GAD eG
GAD-Straße 2-6 - 48163 Münster
http://www.gad.de

© GAD 2010