SEPA –aktueller Stand der Standardisierungsprojekte

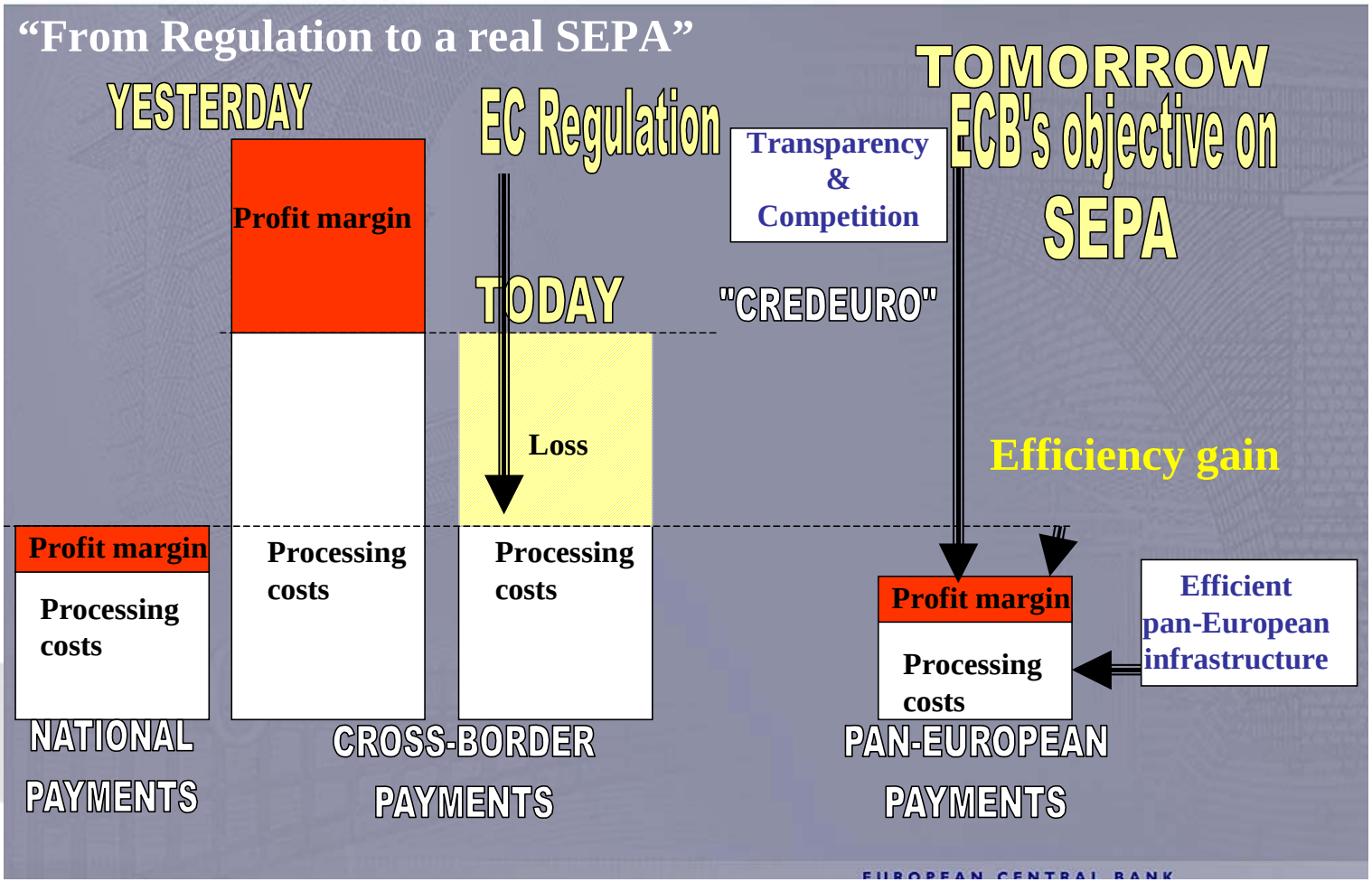
Regine Quentmeier,
SRC Security Research & Consulting GmbH
Bonn - Wiesbaden

Überblick

- Veränderte Rahmenbedingungen als Hintergrund für die europäische Standardisierung
- Standardisierung in Europa (SEPA)
  - Karte-Terminal-Schnittstelle
  - Terminal-Acquirer-Schnittstelle (Terminal-Host)
  - Issuer-Acquirer-Schnittstelle
  - Hamonisierung von Sicherheitsanforderungen und Zulassung
- TOP Down Protection der SEPA-Standardisierung durch den EPC

Veränderte Rahmenbedingungen

ECB: What is SEPA?

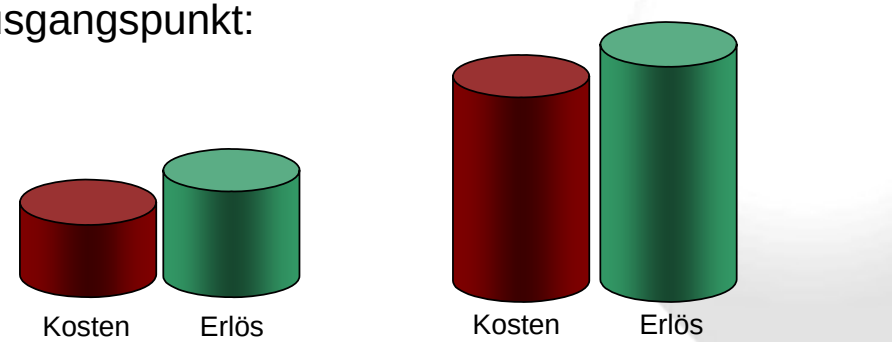


Veränderte Rahmenbedingungen

Zunehmender Rentabilitätsdruck bei grenzüberschreitenden Transaktionen (1)

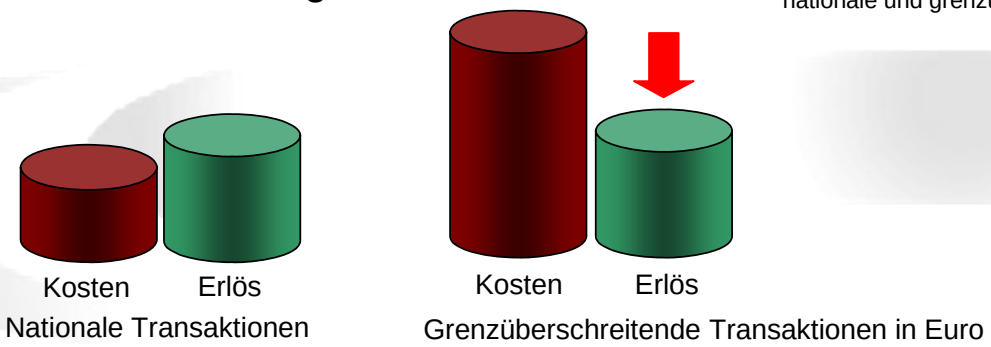
Gewinn- und Verlustrechnung (Prinzipdarstellung):

Ausgangspunkt:



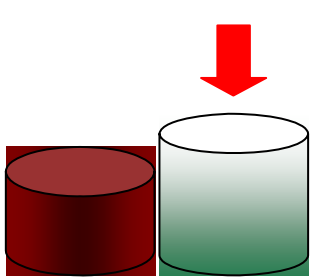
EU Preisverordnung 2560/01:

Gleicher Preis für Karteninhaber und Händler
für grenzüberschreitende und nationale Transaktionen
in der Euro-Zone, trotz unterschiedlicher Kostenstrukturen für
nationale und grenzüberschreitende Transaktionen



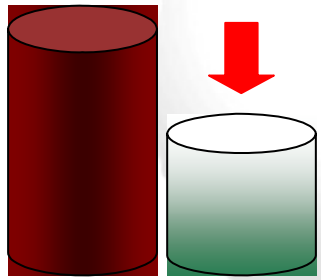
Veränderte Rahmenbedingungen

•Zukunft: Wettbewerbsbehörden üben zusätzlichen Druck auf die •Interchange•Fees•aus



•Kosten •Erlös

•inländische Transaktionen



•Kost •Erlös

•grenzüberschreitende Transaktionen in Euro

•Nationale Systeme sind kostengünstiger als derzeitige internatio•nale Zahlungssysteme.

•Erfordernis substantieller Einsparungen, besonders für
•grenzüberschreitende Transaktionen im Euro-Raum

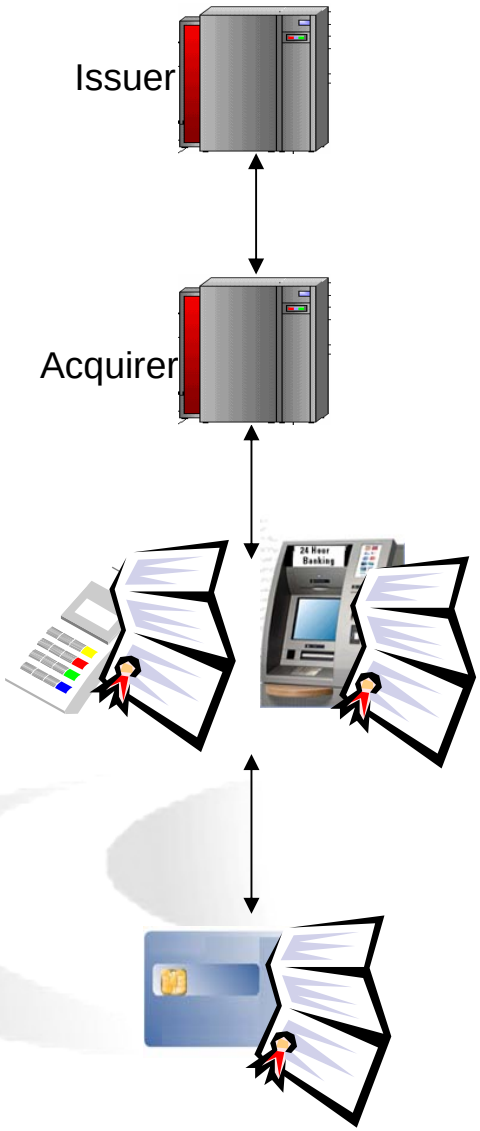
Europäische Standards

- Wesentliches Mittel zur Kostensenkung
- Einheitliche Abwicklungsstrukturen
- Harmonisierung der Verfahren (SEPA)
- Reduzierung von kostenträchtigen Umsetzungsleistungen
- Möglichkeit von Straight Through Processing

Europäische Standards

- Forderung der europäischen Regulierer EU und EZB
- Commitment der europäischen Kreditwirtschaft im EPC
  - Vier Standardisierungsdomains
    - Karte – Terminal-Schnittstelle
    - Terminal – Host-Schnittstelle
    - Issuer – Acquirer-Schnittstelle
    - Gegenseitige Anerkennung von Zertifizierungen und Zulassungen von Produkten

Europäische Standardisierungs-Initiativen im Überblick



THE *Berlin* GROUP
A EUROPEAN INITIATIVE
WORKING FOR CARD PAYMENTS IN EUROPE

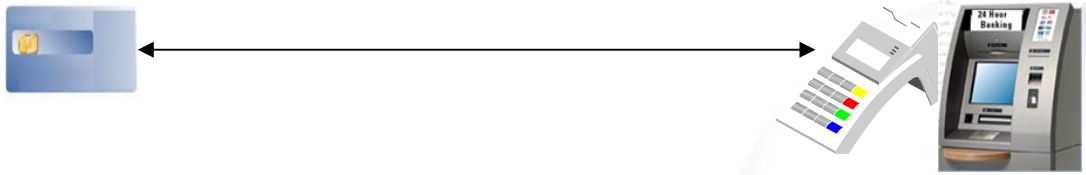
ERIDANE/EPAS

Common Approval Scheme
A EUROPEAN INITIATIVE
FOR CARD PAYMENTS IN EUROPE

CIR Common Implementation Recommendations

Common Approval Scheme
A EUROPEAN INITIATIVE
FOR CARD PAYMENTS IN EUROPE

Card to Terminal Interface



Relevante Standards:

Governance:

Zielarchitektur:

aber: Zahlungssystem-spezifische Anforderungen an die Implementierung

Unterschiedliche Implementierungen bei Terminal- und Kartenherstellern

Interoperabilitäts-Probleme

Performance-Probleme

Card to Terminal Interface

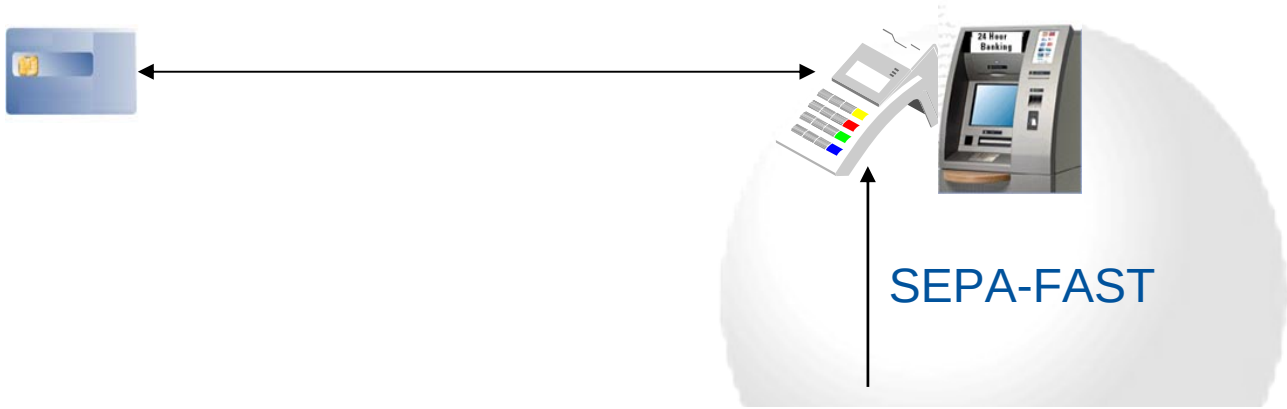
1. Schritt: Harmonisierung der Kartenanforderungen

   Entwicklung der Common Payment Application CPA

   Ausgabe in Deutschland ab Ende 2007

Common Implementation Recommendations – Initiative (CIR)

Card to Terminal Interface



2. Schritt: Harmonisierung der Terminalanforderungen

   Entwicklung der ***Financial Application Specification for SCF-Compliant EMV Terminals (SEPA-FAST)***

Common Implementation Recommendations – Initiative (CIR)

SEPA-FAST V1

- **Erste Version SEPA FAST (*SEPA-FAST V1*) wird berücksichtigen**
  - **Kompletten Terminal Transaction Flow**
    - **Terminal-to-card interface**
    - **Terminal-to-cardholder interface**
    - **Exception handling**
  - **Financial Services**
    - **Bezahl-Service mit (automatischen) reversals und referrals**
    - **Refund Service**
    - **Storno Service**
  - **Fertigstellung August 2008**

Effizienz und Wettbewerb

Harmonisierung der Kartenplattform (CPA):

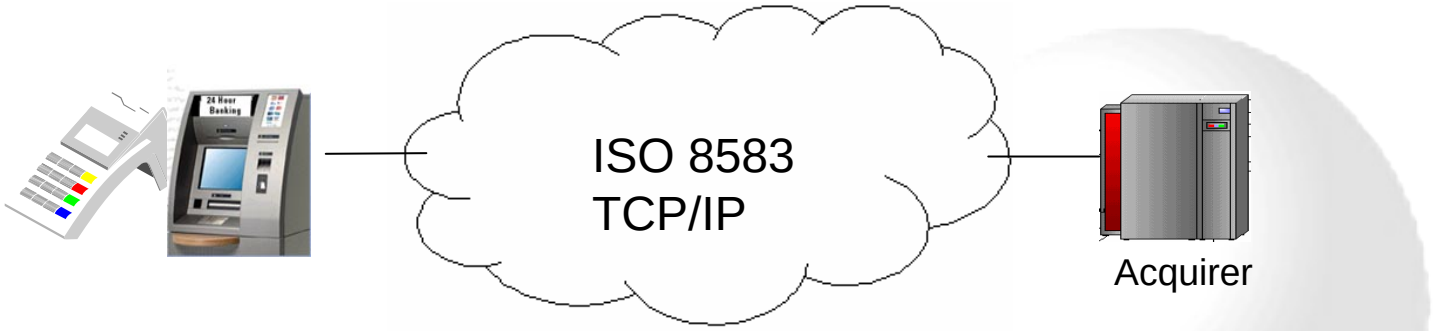
- Kostensenkung durch gemeinsame Plattform für dual Issuer
- Höhere Flexibilität im Produktportfolio durch individuell gestaltbares Risikomanagement

Effizienz und Wettbewerb

Harmonisierung der EMV-Terminalanwendung (SEPA-FAST)

- Interoperable Abläufe über alle Transaktionsarten
- Performancesteigerung
- Höhere Flexibilität für einzusetzende Anwendungen
- Unterstützung eines einheitlichen „Look & Feel“ für den Karteninhaber
- Unterstützung eines „One-Stop-Shoppings“ für Terminals bei Funktionstests und Zulassung innerhalb der SEPA (Vgl. CAS)
- Minimierung von Customizing bez. Reduzierung von Aufwänden für Customizing durch Parametrisierung

Terminal to Acquirer Interface



Standards:

Governance:

Zielarchitektur: ? ?

Es gibt heute keinen technischen Standard für die Kommunikation zwischen Terminal und Acquirer!

- ⇨ Vielzahl unterschiedlicher Implementierungen
- ⇨ Begrenzte Terminalmärkte
- ⇨ Schwierigkeiten in der Umsetzung neuer technischer Anforderungen

EPAS / ERIDANE

- **Electronic Protocol Application Software EPAS**

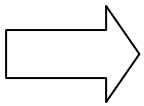
- **ERIDANE**
  - **Innovative funktionale und Sicherheitsarchitektur für den Point of Interaction POI**

ERIDANE

Terminal to Acquirer Interface

ERIDANE / EPAS-Projekt

- **Terminal-Host-Interface (EPAS)**
- **Terminal-Kasse-Schnittstelle (EPAS)**
- **Terminal-Management-Schnittstelle (EPAS)**
- **Terminal-PIN-Pad Schnittstelle (ERIDANE)**
- **Standardisierte Sicherheitsarchitektur für Terminals (ERIDANE)**



Neue Terminalarchitekturen (Applikationsserver)

Kostensenkung für Terminals

Öffnung von Märkten

Einfachere Softwareänderungen (Time to Market für neue Anwendungen)

- **Voraussichtlicher Abschluss der Arbeiten: 09/2007**

EPAS

Ziele

- **Protokoll-Interoperabilität**
  - **Unabhängigkeit vom POI und Sales System**
  - **Unabhängigkeit von der Systemarchitektur und vom Integrationsgrad des POI**
  - **Unabhängigkeit von Transportprotokollen (alle Verbindungstypen sollen unterstützt werden mit TCP/IP als Standard-Transportprotokoll)**
- **Lieferung von Software durch Hersteller in einer Demonstrationsphase (Proof of Concept)**

Beschreibung

- Schaffung einer neuen modularen Terminal- und Sicherheitsarchitektur durch
  - Definition von POI-Komponenten (einheitliche Sichtweise und Funktionstrennung)
  - Standardisierung der POI internen Schnittstellen
  - Standardisierung der POI externen Schnittstellen (wird von EPAS übernommen)

ERIDANE
Effizienz und Wettbewerb

- Abbau von Interoperabilitätsbarrieren durch heutige rein herstellerspezifische Lösungen
- Reduzierung von Kosten
  - Anwendungsentwicklung, -installation und –änderung, Vereinfachung der Zertifizierung (Teilkomponentenzulassung)
- Entwicklung von Anwendungssoftware weitgehend unabhängig vom POI (einheitliche API für sämtliche POI-Komponenten)
- Geringer Portierungsaufwand
- Abdeckung nicht nur von Zahlungssystem-Anwendungen, sondern auch anderer Anwendungen wie Gesundheitswesen oder Verwaltungsapplikationen

Acquirer to Issuer Interface

Relevante Standards:

Governance:

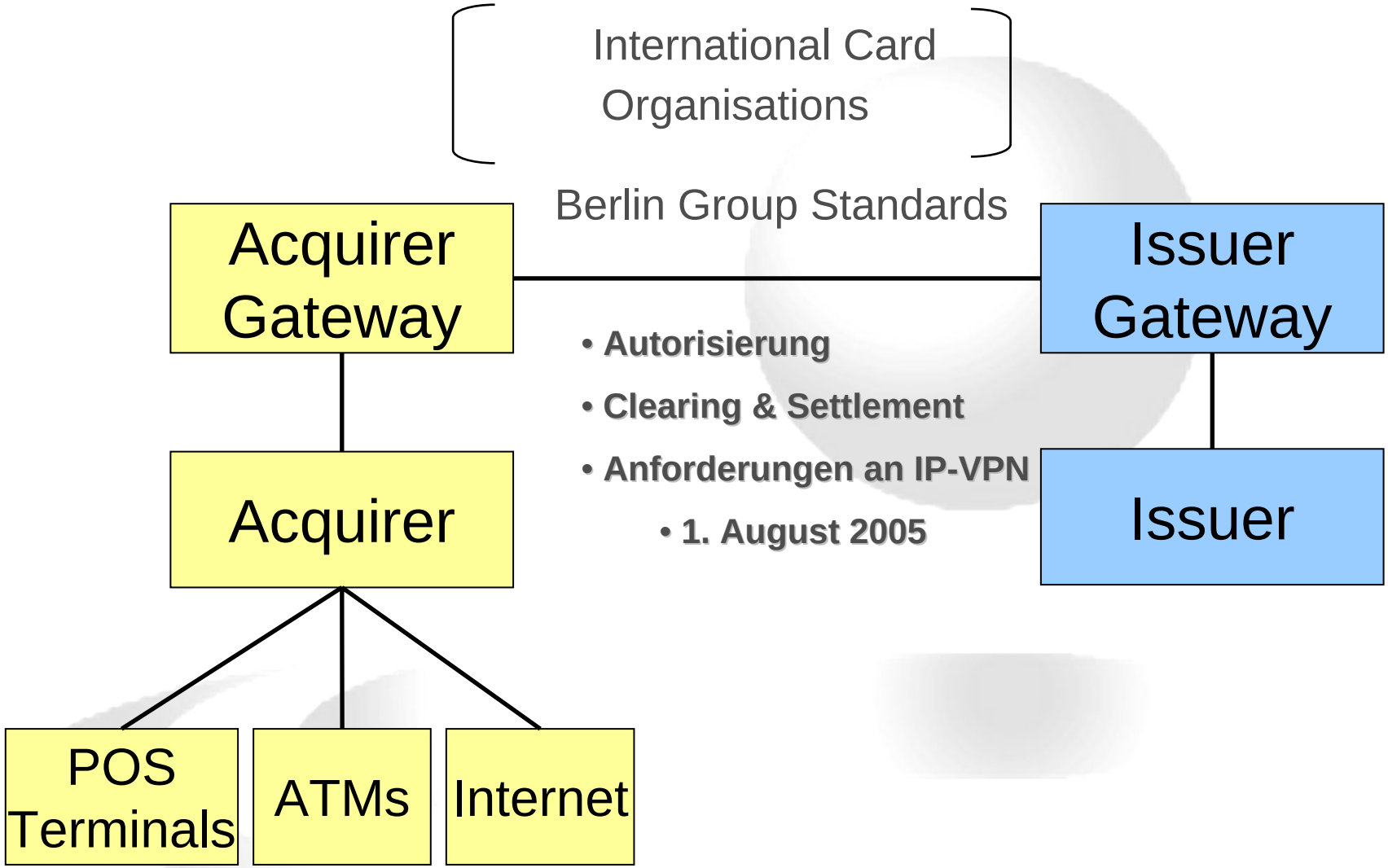
Zielarchitektur: ?

?

Zahlungssystemspezifische Standards, unterschiedliche Implementierungen je Zahlungssystem, obwohl Institute i.d.R. Dual Issuer sind.

Acquirer to Issuer Interface

Berlin Group-Schnittstellen



Berlin Group-Schnittstellen

Autorisierung

- **übersichtlich**
- **schlank**
- **effizient**

Effizienz und Wettbewerb

- **Beispiel Maestro:**
  - **Kostenerhöhung wegen Zahlungssystementgelten:**
    - **Management entscheidet über Höhe der Systementgelte (Erhöhung um rund € 3 Mio. p.a. in 2006)**
    - **Belastung nationaler Transaktionen mit Zahlungssystementgelten (SEPA-Pricing)**
  - **Keine Möglichkeit, höhere Erträge zu generieren**
  - **Tendenziell zurückgehende Einflussmöglichkeiten auf produktpolitische Entscheidungen**

Scenario	1	2
	"old" Pricing	"new" Pricing
1. Acquirer Fees		
1.1. Transaction Processing Fees		
1.1.1. MC Clearing fee	95.141,73	
1.1.2. MC Clearing & Settlement fee		285.030,08
1.1.5. MC File Transmission Fee	89.790,69	89.790,69
1.2. Fees on processed amount		
1.2.1. MC Assessement Fee	1.104.467,48	
1.2.2. MC Settlement Fee	285.030,08	
1.2.3. SEPA Maestro/Cirrus Volume Fees		310.179,80
1.2.4. Intra-European Cross-Border Fee		155.928,22
Total Acquirer	1.574.429,99	840.928,79
2. Issuer Fees		
2.1. Transaction Fees		
2.1.1. MC Authorisation Fee new		758.111,89
2.1.2. MC Authorisation Fee old	2.281.041,23	
2.1.4. MC Clearing & Settlement Fee		592.934,00
2.1.5. MC Clearing Fee	675.120,91	
2.1.6. MC File Transmission Fee	412.031,95	412.031,95
2.2. Fees on processed amount		
2.2.1. MC Assessment Fee	7.505.885,13	
2.2.2. SEPA Maestro/Cirrus Volume Fees		1.250.980,85
2.2.3. Currency Conversion Assessement		4.860.954,18
2.2.4 MC Settlement Fee	714.846,20	
2.2.5 Intra-European Cross-Border Fee		664.806,97
2.4. Card-specific costs		
2.4.1 MC Card Fee old	3.965.958,48	
2.4.2. MC Debit Card Fee new		10.816.250,40
Total Issuer	15.554.883,90	19.356.070,24

Effizienz und Wettbewerb

- Wegfall des Intermediärs (Kosten)
- Schnelle Abstimmung über Implementierung und Weiterentwicklung, kurze Wege
- Möglichkeit von grenzüberschreitenden „on us“-Transaktionen
- Mehr Flexibilität im Issuer-Produktportfolio
- Verbesserung der Akzeptanz im Acquiring
- Stärkung des Wettbewerbs

Implementierungen

- BV-Zahlungssysteme – SSB (Italien), GA produktiv seit August 2006, POS produktiv seit April 2007
- BV-Zahlungssysteme – Seceti (Italien), GA Mai 2007
- BV-Zahlungssysteme – Equens (Niederlande), Beginn Mai 2007
- BV-Zahlungssysteme – Eufiserv, produktiv seit März 2007 (spanische GA)
-
-

Komponentenzertifizierung

Relevante Standards:

Governance:

Zielarchitektur: **mutual recognition for type approval** ?

Zahlungssystemspezifische Anforderungen

Separate Zulassungen pro Zahlungssystem und Land

Komponentenzertifizierung

Common Approval Scheme
A EUROPEAN INITIATIVE
FOR CARD PAYMENTS IN EUROPE

Step 1: - Harmonisierte Sicherheitsanforderungne (based on PCI PED)
- Harmonisierte Evaluierungsmethode der Einhaltung

Step 2: Gegenseitige Anerkennung von Sicherheitszertifizierungen und Zulassungen

Abdeckung von Chipkarten und Terminals

Einbeziehung der PCI PED Requirements als „Base Line“

Offene Kommunikation der Projektergebnisse gegenüber internationalen Zahlungs-systemen und Europäischer Kommission

Voraussichtlicher Abschluss der Arbeiten: Ende 2007

CAS Cards Working Group

- Generic Security Target für CC-Evaluierung von Karten fertiggestellt
- Abstimmung mit ISCI abgeschlossen (Zertifizierungsstellen, Labors, Hersteller)
- Pilotevaluierungen werden vorbereitet, Cartes Bancaires und ZKA als Vorreiter?
- ZKA wird Zulassungsverfahren entsprechend umstellen

CAS Terminal Working Group

- CAS Sicherheitsanforderungen für den Point of Interaction (POI) wurden definiert durch
  - PCI PED + ... und
  - PCI PED - ..... und
  - PCI PED delta.

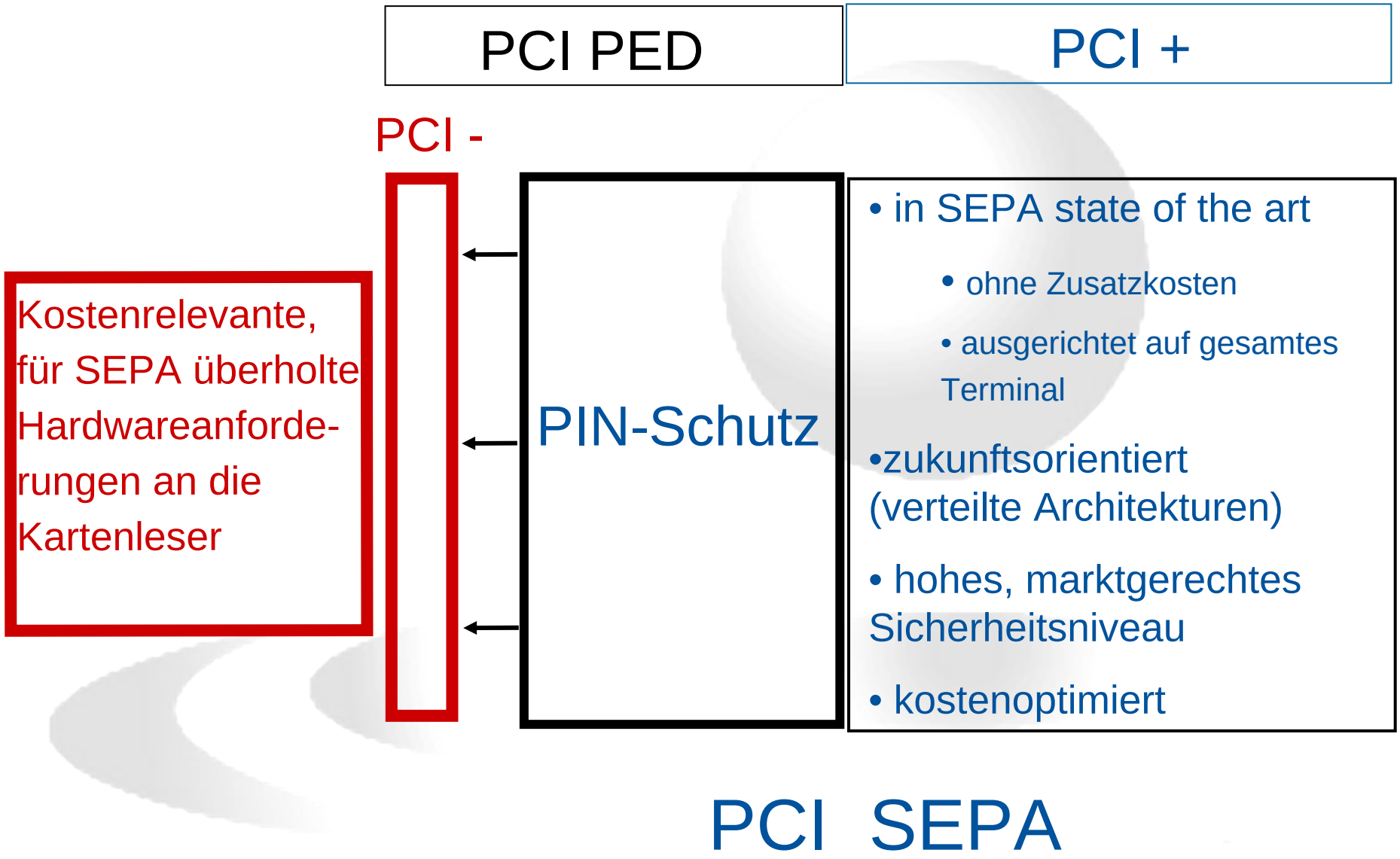
CAS, PCI PED + - Anforderungen

- **Ausdehnen der Anforderungen auf das gesamte POI, nicht mehr nur PED und PIN-Schutz**
  - **Z.B. Ergänzung um Nachrichtenintegrität und Nachweis von Komponentenauthentizität**
- **Höhere Anforderungen an Hersteller-Dokumentation**
  - **Guideline für die Dokumentation des Lebenszyklus (gemäß CC)**
  - **Als Basis für die Evaluierung von z.B. Ablaufkontrolle, Einflüsse anderer Anwendungen (gemäß “high and low level design documentation” aus CC)**
  - **Source Code-Analyse begrenzt auf PIN-Schutz**

CAS, PCI PED - Anforderungen

- Verzicht auf Anforderungen an den Kartenleser
  - Zum Schutz der Klartext-PIN
  - Zum Schutz der Magnetstreifendaten (neu in Version 2.X)
    - Neue Hardware-Anforderung
    - Redesign des Terminals
- Forderung nach PCI-SEPA
  - SEPA als fortgeschrittener EMV-Markt
    - Outphasing „unsicherer“ EMV-Eintrittslösungen (SDA, Klartext-PIN)
    - Migration zu sicheren EMV-Lösungen (DDA, verschlüsselte PIN)
    - Return on Invest für Kartenausgeber und Acquirer in der SEPA

PCI SEPA


PCI PED
PCI +
PCI -
Kostenrelevante, für SEPA überholte Hardwareanforde-rungen an die Kartenleser
PIN-Schutz
• in SEPA state of the art
• ohne Zusatzkosten
• ausgerichtet auf gesamtes Terminal
•zukunftsorientiert (verteilte Architekturen)
• hohes, marktgerechtes Sicherheitsniveau
• kostenoptimiert
PCI SEPA

CAS Status Terminal Subgroup

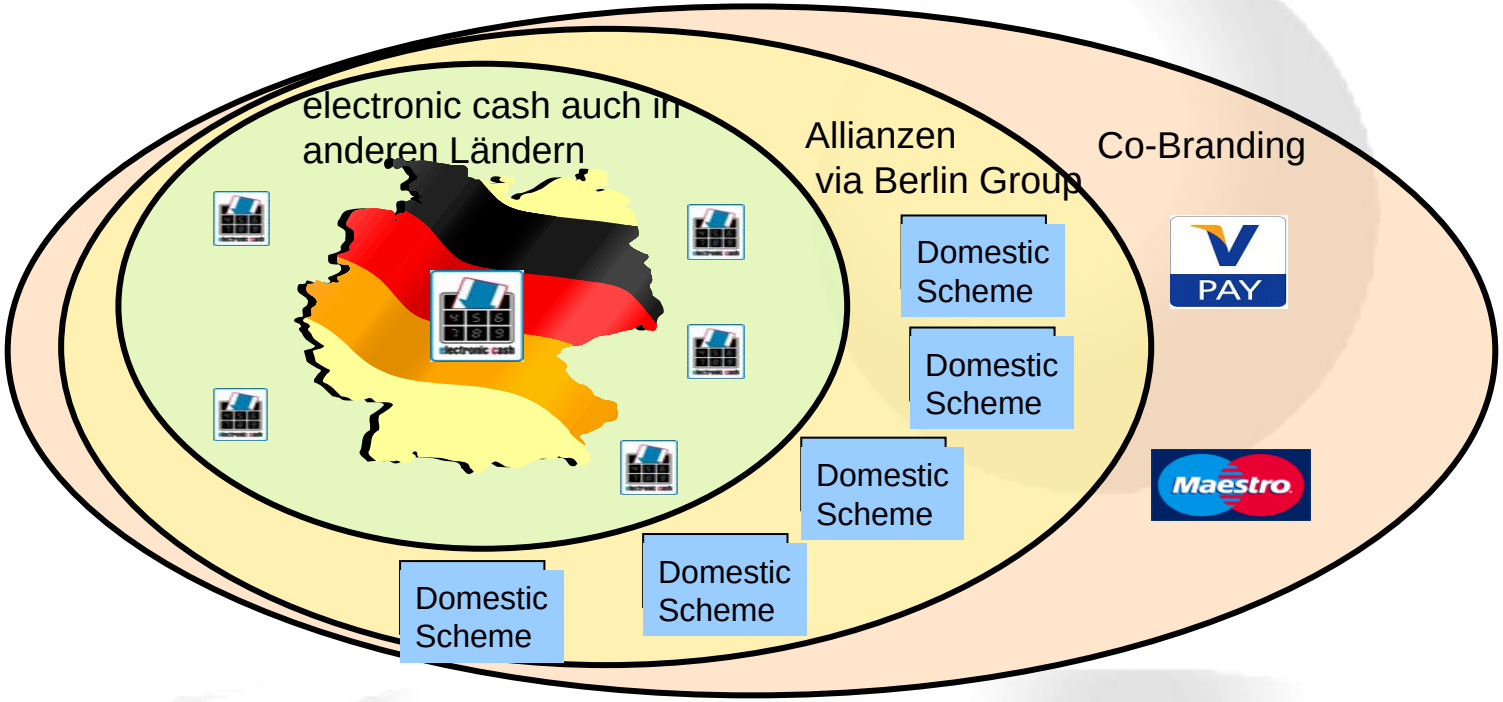
- **Derzeitiger Schwerpunkt: Evaluierungsmethode**
- **Für Karten Common Criteria-Evaluierung**
  - **Hohe Qualität**
  - **Standard bietet optimale Basis für eine vergleichbar und nachvollziehbar durchgeführte Evaluierung**
  - **Bereits im Markt etabliert**
- **Für Terminals ergeben sich Alternativen**
  - **Evaluierung gemäß PCI POS PED Requirements oder**
  - **CC Evaluierung für das POI**
  - **Auswahl-Kriterien sprechen eindeutig für CC (erster Kandidat)**
    - ***Derzeit Durchführung einer Machbarkeitsstudie (Protection Profile)***

Effizienz und Wettbewerb

- **Kostensenkung**
  - **durch Minimierung von Test- und Evaluierungsaufwand insgesamt (eine Evaluierung innerhalb der SEPA, Wiederverwendbarkeit von Evaluierungen)**
  - **Harmonisierung der Evaluierungsverfahren**
    - **Standardisierte Grundlage und Durchführung**
  - **Wegfall von Reibungsflächen zwischen unterschiedlichen Anforderungsprofilen**
    - **ZKA, CB, SecureCom, Currence (PCI+) etc.**
    - **PCI, MC, Visa**
- **Harmonisierung der Sicherheit von Karten und Terminals auf hohem Niveau in Europa**

Effizienz und Wettbewerb

Möglichkeiten zur Entwicklung von SCF-compliant Produkten:



- **Allianzen verbunden durch Berlin Group-Standards**
- **Gegenseitige Anerkennung von Zertifizierung durch CAS-Standards**
- **Systemschnittstellen gemäß CIR und EPAS/ERIDANE-Standards**

Zusammenarbeit in Europa

CIR	CAS	EPAS	Eridane
APACS	APACS	Banksys	Banksys
Banksys	Banksys	Cartes Bancaires	Cartes Bancaires
Cartes Bancaires	Cartes Bancaires	Cetrel	Cetrel
Cetrel	Cetrel	Europay Austria	Interpay
Europay Austria	Interpay	Interpay	Sermepa
Interpay	Pan Nordic Card Association	Pan Nordic Card Association	APACS (observer)
MBNA	Sermepa	Sermepa	Thales
Pan Nordic Card Association	SIBS	SIBS	Ingenico
RBS	Sistema 4B	Atos	MoneyLine
Sermepa	SSB	BP	Gemalto
SIBS	ZKA	Galitt Group	SRC/ZKA
Sistema 4B		Ingenico	Sagem Monetel
SSB		Integri	
Telekurs		Lyra	
ZKA		MoneyLine	
		RSC	
		SRC/ZKA	
		Thales	
		Thales Espana	
		Total	
		University of Applied Science	
		Wincor	

Welche Standards sind für ein „SEPA for cards“ erforderlich?

EPC SEPA Cards Framework SCF:

- **„In order for the objectives of this Framework to be achieved, SEPA-level interoperability must be ensured in the following 4 domains:**
  - **cardholder to terminal interface,**
  - **cards to terminal (EMV),**
  - **terminal to acquirer interface (protocols or minimum requirements),**
  - **acquirer to issuer interface, including network protocols (authorization and clearing).“**

- **„A common process for the certification of terminals, cards, and network interfaces will be defined in line with the principle described in Chapter 2.3.2.“ „Card schemes will engage in mutual recognition for type approval. Any terminal certified for SEPA transactions by a certification body in one SEPA country can be deployed in any SEPA country for acceptance of SEPA cards across all SCF compliant schemes.“**

Top Down Protection durch den EPC

EPC Founding Workshop (Januar 2007)

- **CAS, CIR und EPAS/ERIDANE wurden als „EPC identified initiatives“ anerkannt.**

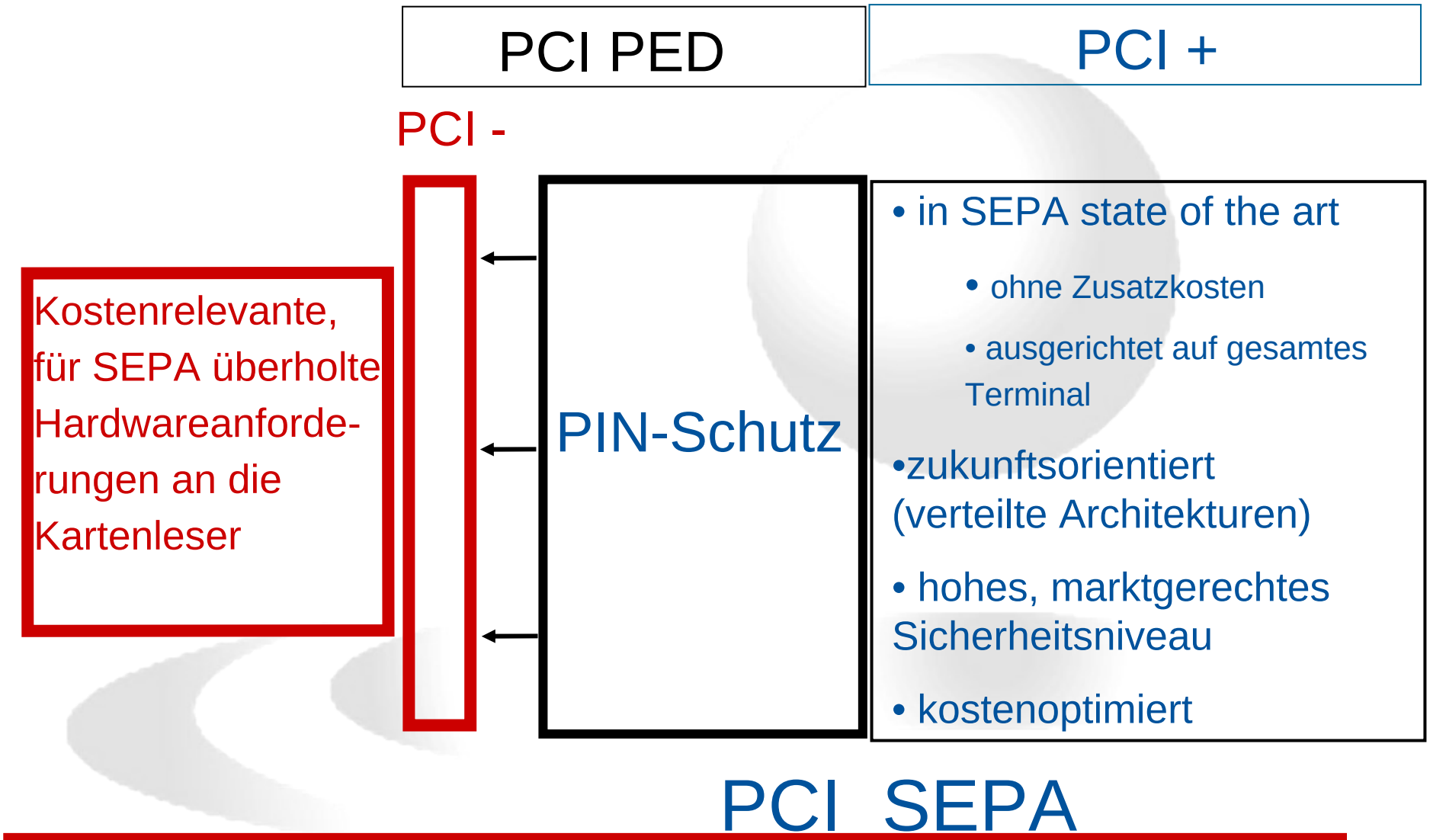
  Acquirer to Issuer-Schnittstelle zunächst Expert Group

- **Einbezug der internationalen Kartensysteme MasterCard und Visa**

TOP Down Protection durch den EPC

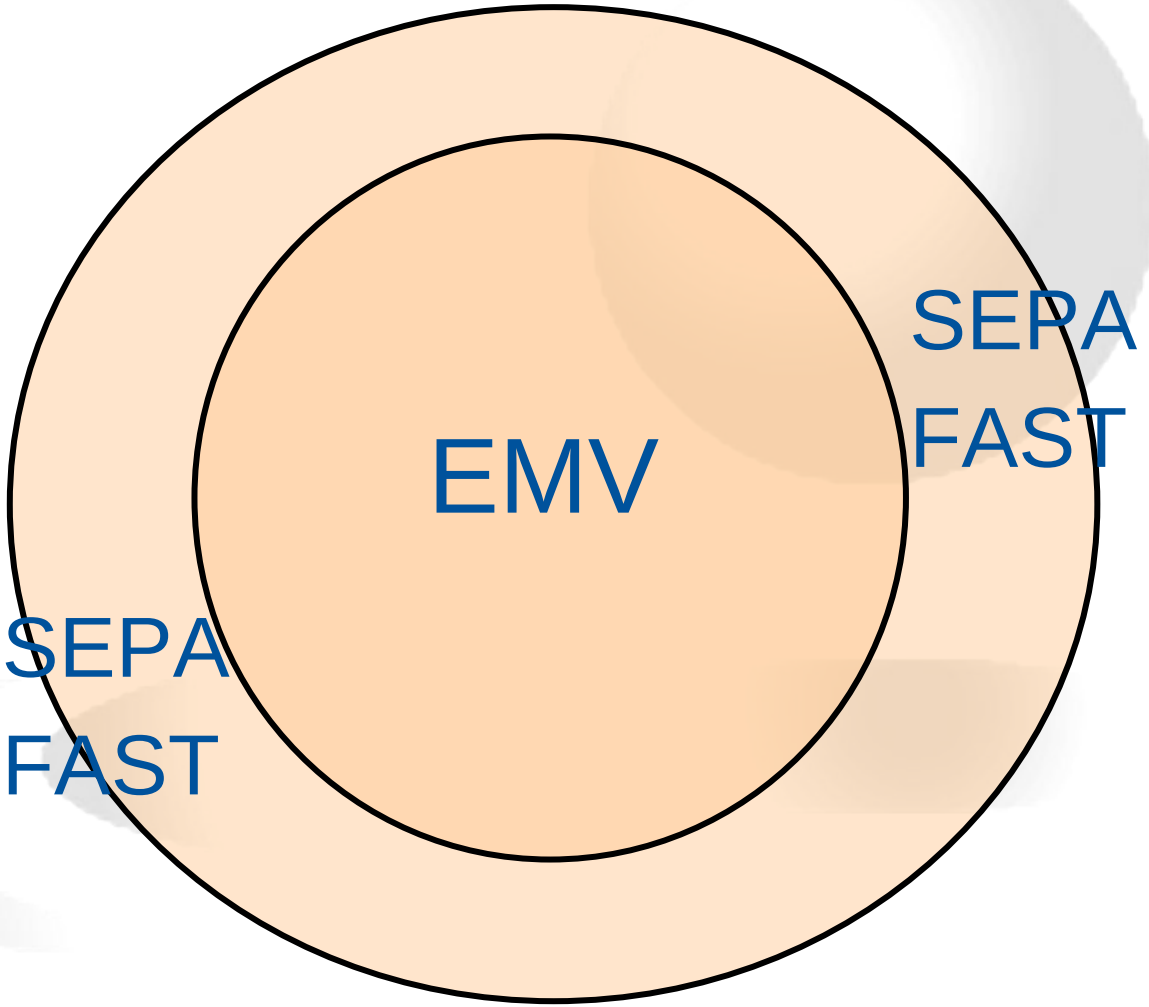
- **Stand heute**
  - **Diskussionen müssen auf EPC-Ebene erneut geführt werden**
  - **Die internationale Zahlungssysteme stehen vor neuen Herausforderungen**
    - **Verhandlungen auf gleicher Augenhöhe**
    - **Öffnung des Marktes für**
      - ***Zulassungsinfrastruktur***
      - ***Anforderungen an ZV-Komponenten (Governance)***

PCI SEPA (Situation Typ 1)



SEPA FAST (Situation Typ 2)

Die SEPA-Anforderungen ergänzen die internationalen Anforderungen



Kontakt

SRC
Security Research & Consulting GmbH
Graurheindorfer Str. 149a
53117 Bonn

Tel. **+49-(0)228-2806-0**
Fax: **+49-(0)228-2806-199**
E-mail: **info@src-gmbh.de**
WWW: **www.src-gmbh.de**