Anforderungen an eine starke Kundenauthentifizierung durch die Einführung von Instant Payments

van den berg
Payment Services

Software baut Brücken
Forum Software

21. September 2017 | 9:30 bis 17:00 Uhr
Tagungswerk Jerusalemkirche
Lindenstraße 85 | 10969 Berlin

Inhalt

- **Was sind Instant Payments?**
- Instant Payments und der Handel
- Instant Payments am POS
- Gesetzliche Rahmenbedingungen für mobiles Bezahlen
- Technische Herausforderungen

Definition

„Instant Payments“ ist eine elektronische Zahlungsverkehrslösung für

- Retail-Payments (für das Bezahlen am POS)
- Person-to-Person-Payments
- E-Commerce-Payments (für das Bezahlen im Internet)
- Gouvernement-Payments (für Gebühren, Abgaben und Steuern)

in EUR, die ständig (24/7) in den EUR-Ländern zur Verfügung steht.

Quelle: Pan-European instant payments in euro: definition, vision and way forward, ECB , 12.11.2014

Definition

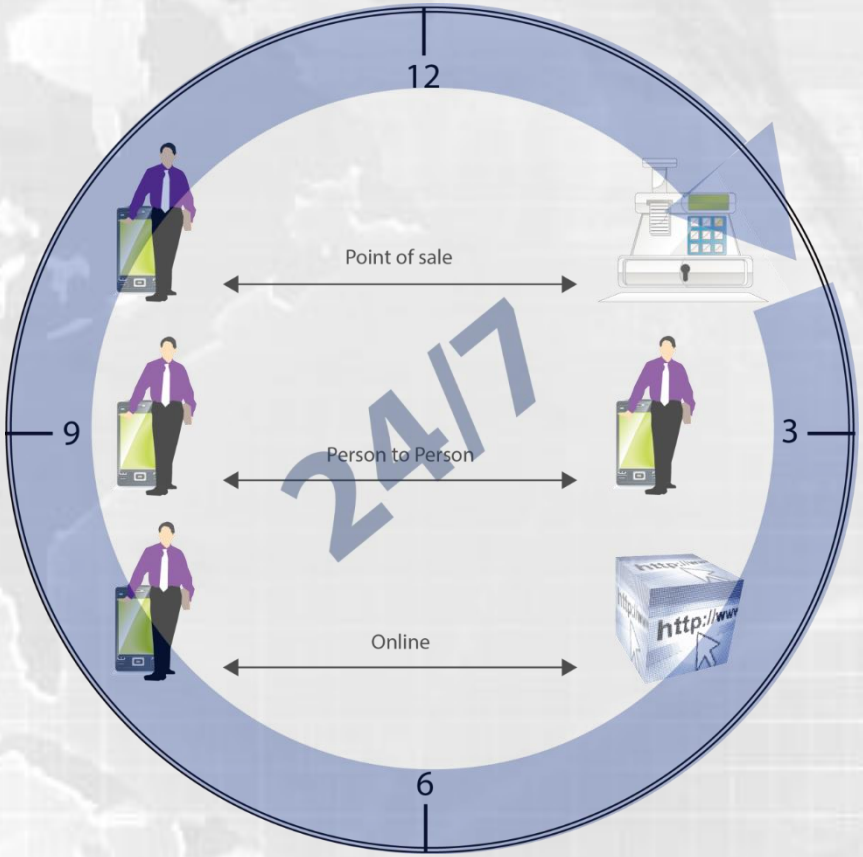
Sofort oder annähernd sofort (also innerhalb von Sekunden nach Auslösung der Zahlung)

- wird die Zahlungsnachricht an den PSP des Zahlungs-empfängers übermittelt.
- wird die Ausführung dem Zahler bestätigt.
- kann der Empfänger über den gutgeschriebenen Betrag verfügen*.

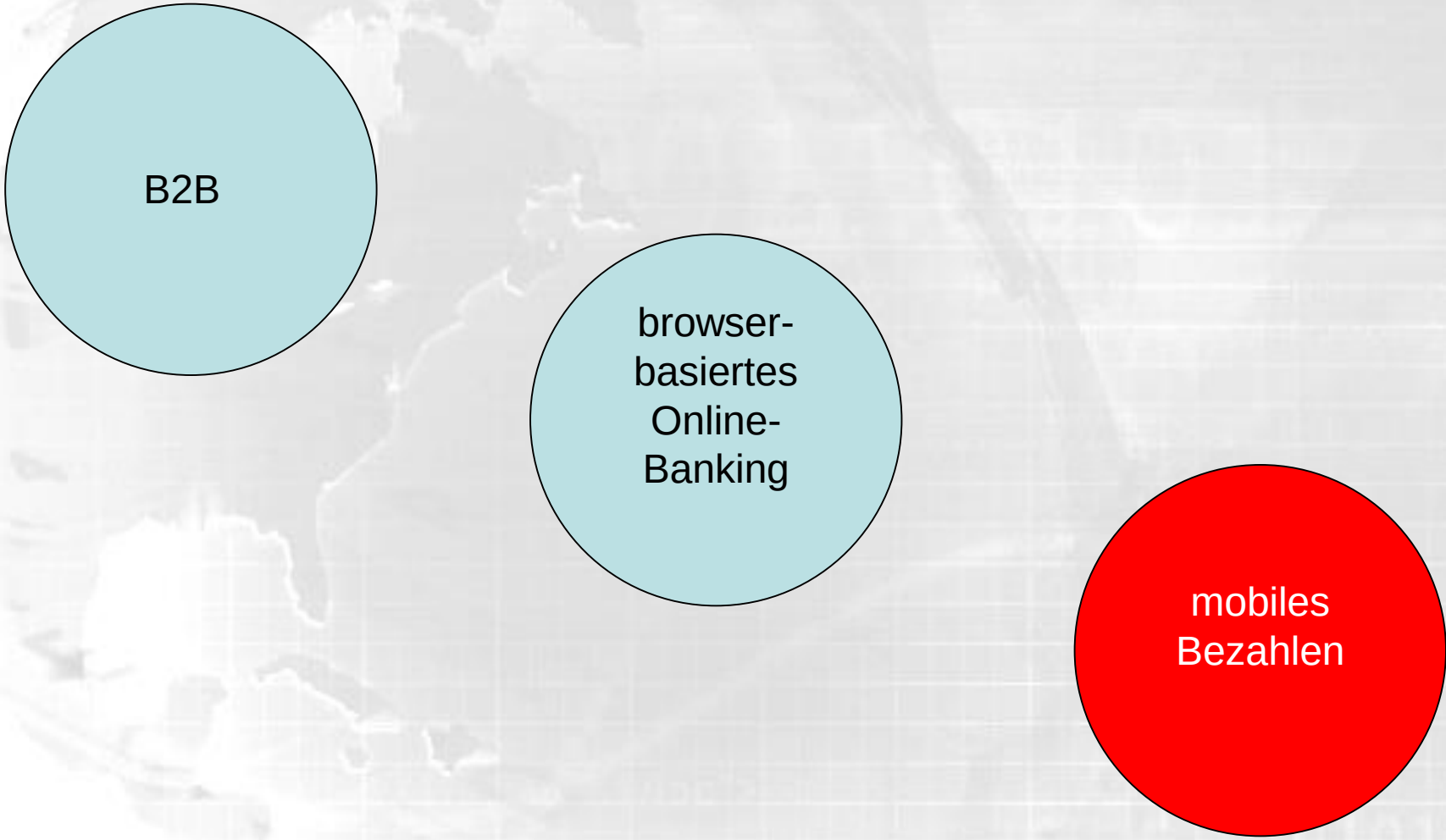
* Existierende Zahlungssysteme erfüllen die Anforderung an die sofortige Verfügbarkeit durch den Zahlungsempfänger nicht. Als Beispiel für solche Lösungen nennt die ECB: MyBank, Ideal, Sofort

Quelle: Pan-European instant payments in euro: definition, vision and way forward, ECB , 12.11.2014

24/7



Ausprägungen von Instant Payments



Mobiles Bezahlen

Person-to-Person - Zahlungen

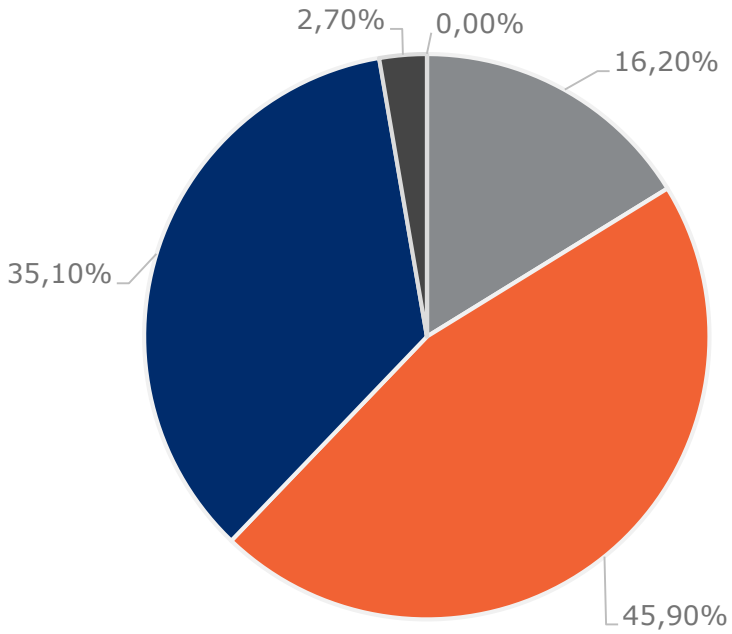
Zahlungen im e-Commerce

Zahlungen am POS

Inhalt

- Was sind Instant Payments?
- **Instant Payments und der Handel**
- Instant Payments am POS
- Gesetzliche Rahmenbedingungen für mobiles Bezahlen
- Technische Herausforderungen

Wie versiert sind Sie im Thema SEPA Instant Payments?



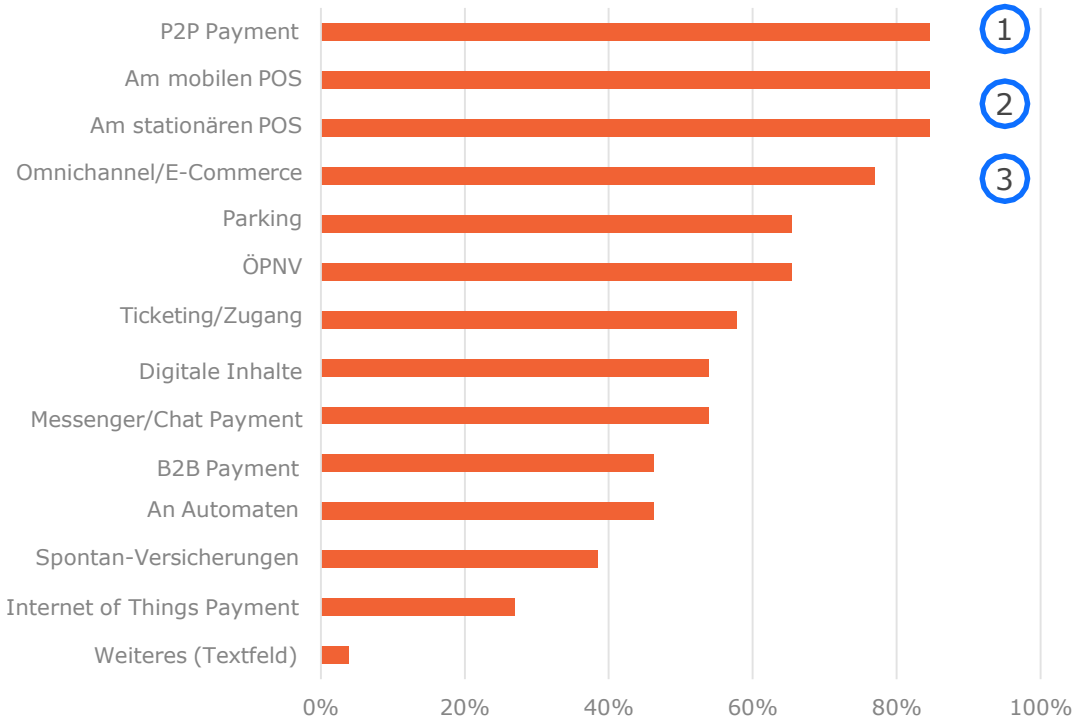
Ergebnisse fließen in die Bewertung ein

- Ich kenne mich sehr gut aus
- Ich kenne mich gut aus
- Ich kenne mich etwas aus

- Ich kenne mich noch nicht aus, beabsichtige aber, mich mit dem Thema zu beschäftigen
- Ich kenne mich nicht aus, das Thema interessiert mich nicht

Ergebnisse fließen **nicht** in die Bewertung ein

Wo sehen Sie Potential für SEPA Instant Payments? (Mehrfachauswahl möglich)

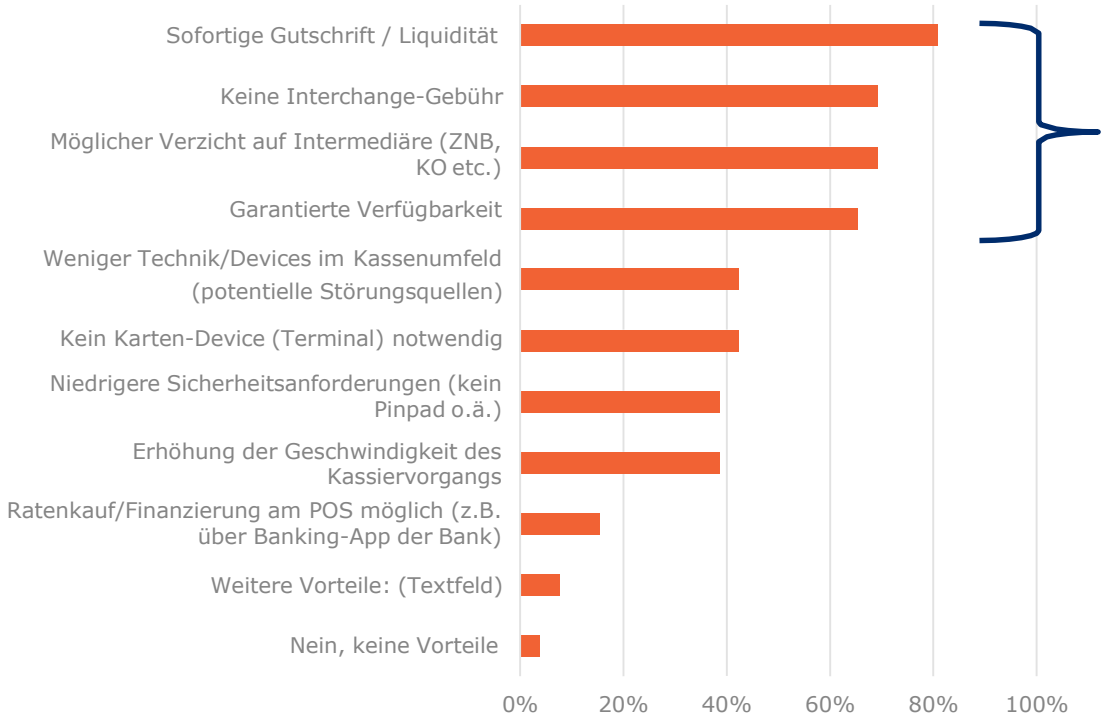


SEPA Instant Payments hat aus Sicht der Teilnehmer das höchste Potential für

1. Person to Person Payment
2. am POS (stationär und mobil)
3. im E-Commerce bzw. Omnichannel Handel

Ca. 2/3 der Teilnehmer sehen auch Transport (Parking, ÖPNV) im Fokus für SEPA Instant Payments.

Welche Vorteile sehen Sie in der Nutzung von SEPA IP am POS? (Mehrfachauswahl möglich)



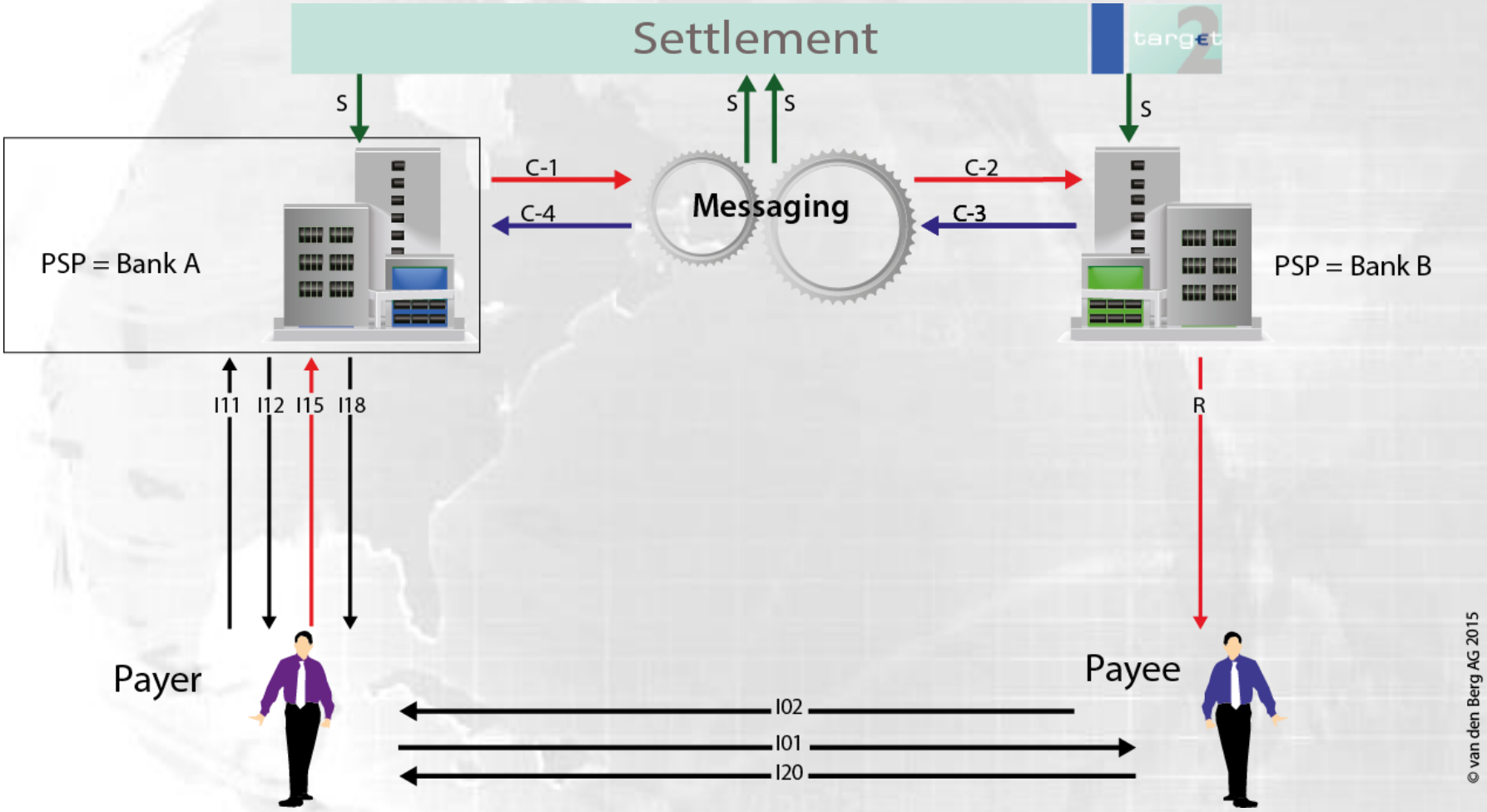
Händler schätzen Sicherheit und Kostenersparnisse:

1. die sofortige (und damit garantierte) Verfügbarkeit des Geldes
2. Ersparnisse durch Vereinfachung: weniger Dienstleister, keine Gebühren

Inhalt

- Was sind Instant Payments?
- Instant Payments und der Handel
- **Instant Payments am POS**
- Gesetzliche Rahmenbedingungen für mobiles Bezahlen
- Technische Herausforderungen

Settlement


Settlement
target 2
S
S
S
S
C-1
C-4
C-2
C-3
Messaging
PSP = Bank A
PSP = Bank B
I11
I12
I15
I18
R
Payer
Payee
I02
I01
I20
© van den Berg AG 2015

Instant Payments – ein Lösungsansatz

I01: Der Kunde (Payer) aktiviert an der Kasse seine Bezahl-App und wählt die Instant Payment als Bezahlverfahren.

I02: Der Händler (Payee) übermittelt die Zahlungsdetails

- seine Kontonummer
- den Betrag
- die End-to-End-ID
- den Verwendungszweck
- und zusätzliche Daten (z.B. für den elektronischen Kassenbon oder die elektronische Rechnung)

an die Bezahl-App des Kunden (Payer), die von dem PSP des Kunden (Bank A) oder einem Drittanbieter (PISP= Payment Initiation Service Provider) bereitgestellt wird.

Die Übermittlung zur Bezahl-App erfolgt mittels QR-Code, Strichcode oder App-to-App-Kommunikation.

I11: Die Bezahl-App erstellt den Auftrag zur Ausführung einer Instant Payment mit den Händlerdaten und bestätigt den Auftrag.

I12: Die Bank A fordert beim Kunden die Autorisierungsdaten an.

I15: Der Kunde autorisiert den Auftrag, z.B. mit einem Fingerabdruck.

Instant Payments – ein Lösungsansatz

C-1: Die Bank A sendet die Instant Payment an die Infrastruktur.

C-2: Die Infrastruktur prüft, ob die Verrechnung durchgeführt werden kann. Wenn dies der Fall ist, wird die Instant Payment an die Bank B weitergeleitet.

C-3: Die Bank B prüft, ob die Instant Payment angenommen werden kann und teilt das Ergebnis der Infrastruktur mit. Der Betrag wird dem Empfänger verfügbar gemacht, wenn die Bank B die Instant Payment annimmt.

R: Die Bank B informiert den Zahlungsempfänger aktiv oder passiv, dass über den Betrag verfügt werden kann.

C-4: Die Ergebnisse der Prüfungen werden an die Bank A weitergeleitet.

I20: Der Händler bestätigt den Kauf dem Kunden gegenüber.

I18: Die Bank A bestätigt die Ausführung bzw. die Nicht-Ausführung des Auftrags gegenüber dem Kunden.

S: Der Betrag wird von der Bank A zur Bank B transferiert (Settlement).

Instant Payments am POS

- Ein einfaches Verfahren ohne Intermediäre wie
  - Netzbetreiber
  - Karten-Gesellschaften
- Offen für Zahlungsauslösedienste

Inhalt

- Was sind Instant Payments?
- Instant Payments und der Handel
- Instant Payments am POS
- **Gesetzliche Rahmenbedingungen für mobiles Bezahlen**
- Technische Herausforderungen

Zielsetzung der PSD (in Bezug auf mobiles Bezahlen)

- Stärkung des Wettbewerbs
  - Zulassung von Zahlungsauslösedienste
- Erhöhung der Sicherheit
  - Einführung einer starken Kundenauthentifizierung

Stärkung des Wettbewerbs

Stärkung des Wettbewerbs durch Access to Account

(Artikel 66 Vorschriften für den Zugang zum Zahlungskonto im Fall von Zahlungsauslösediensten):

(1) Die Mitgliedstaaten stellen sicher, dass ein Zahler das Recht hat, die in Anhang I Nummer 7 genannten Zahlungsdienste (Zahlungsauslösedienste) über einen Zahlungsauslösedienstleister zu nutzen. Das Recht, einen Zahlungsauslösedienstleister zu nutzen, besteht nicht, wenn das Zahlungskonto nicht online zugänglich ist.

Stärkung des Wettbewerbs

Für die Zwecke der PSD2 bezeichnet der Ausdruck „Zahlungsauslösedienst“ einen Dienst, der auf Antrag des Zahlungsdienstnutzers einen Zahlungsauftrag in Bezug auf ein bei einem anderen Zahlungsdienstleister geführtes Zahlungskonto auslöst;

Starke Kundenauthentifizierung

Sicheres mobiles Bezahlen (Artikel 97 Authentifizierung):

(1) Die Mitgliedstaaten stellen sicher, dass ein Zahlungsdienstleister eine starke Kundenauthentifizierung verlangt, wenn der Zahler

a) online auf sein Zahlungskonto zugreift,

b) einen elektronischen Zahlungsvorgang auslöst,

c) über einen Fernzugang eine Handlung vornimmt, die das Risiko eines Betrugs im Zahlungsverkehr oder anderen Missbrauchs birgt.

Starke Kundenauthentifizierung

Sicheres mobiles Bezahlen (Artikel 97 Authentifizierung):

(2) Im Fall der Einleitung elektronischer Fernzahlungsvorgänge nach Absatz 1 Buchstabe b stellen die Mitgliedstaaten sicher, dass die Zahlungsdienstleister für elektronische Fernzahlungsvorgänge eine starke Kundenauthentifizierung verlangen, die Elemente umfasst, die den Zahlungsvorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen.

Für die Zwecke der PSD2 bezeichnet der Ausdruck „Fernzahlungsvorgang“ einen Zahlungsvorgang, der über das Internet oder mittels eines Geräts, das für die Fernkommunikation verwendet werden kann, ausgelöst wird.

Starke Kundenauthentifizierung

Für die Zwecke der PSD2 bezeichnet der Ausdruck „starke Kundenauthentifizierung“ eine Authentifizierung unter Heranziehung von mindestens zwei Elementen der Kategorien **Wissen** (etwas, das nur der Nutzer weiß), **Besitz** (etwas, das nur der Nutzer besitzt) oder **Inhärenz** (etwas, das der Nutzer ist), die insofern voneinander unabhängig sind, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist;

RTS

Für den Access to Account und das sichere mobile Bezahlen ist der „Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2” zuständig. Dieser ist noch nicht endgültig verabschiedet.

Inhalt

- Was sind Instant Payments?
- Instant Payments und der Handel
- Instant Payments am POS
- Gesetzliche Rahmenbedingungen für mobiles Bezahlen
- **Technische Herausforderungen**
  - **Starke Authentifizierung**
  - **Zugriff auf das Konto durch Dritte**

Zusammenfassung

Beim mobilen Bezahlen

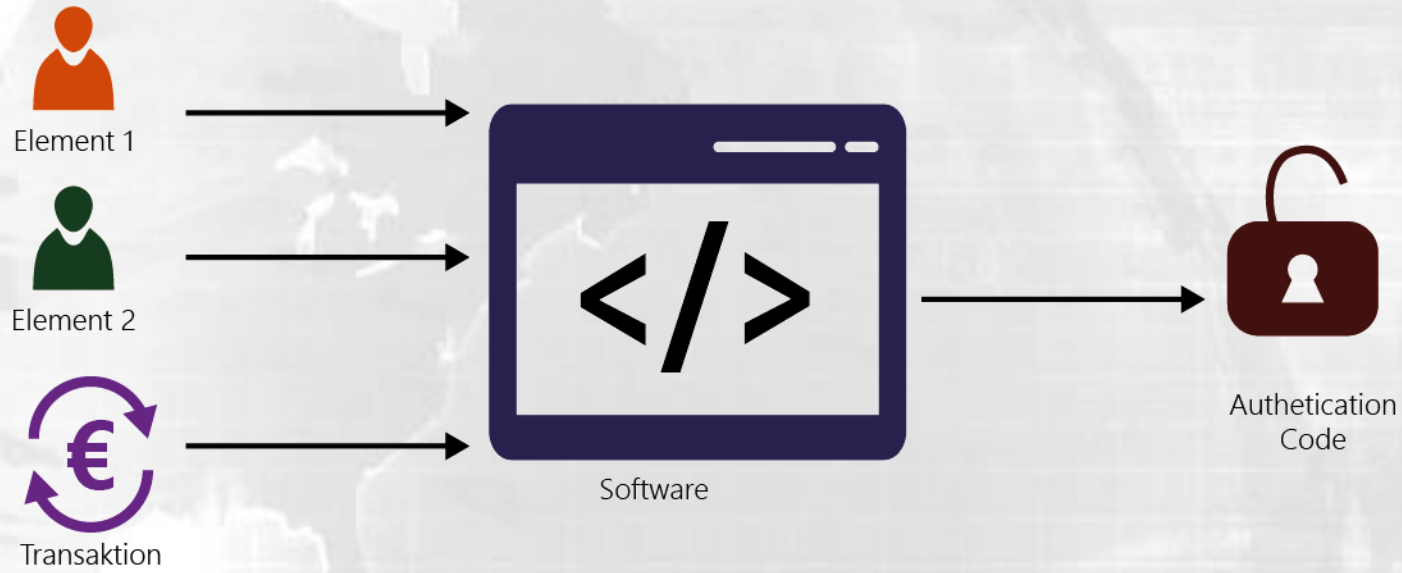
- wird eine **gesicherte Kommunikation** benötigt.
- wird eine **zwei Faktor Authentifizierung** benötigt.
- müssen die Authentifizierungs-Elemente aus zwei verschiedenen Kategorien stammen. Kategorien sind **Wissen**, **Besitz** und **Inherence.**
- muss der Authentifizierungscode bei einem Fernzugriff **dynamisch** mit dem **Betrag** und dem **Empfänger** der Zahlung verknüpft sein.
- auf einem Smartphone müssen **separated secure execution environments** verwendet werden.

2FA

Kunde
Bank
Zahlung initiiren
Zahlung authentifizieren
© van den Berg 2017

Requirements of PSD2

2FA


Element 1
Element 2
Transaktion
Software
Authetication Code
© van den Berg 2017

RTS – Starke Kundenauthentifizierung

- Zu diesem Zwecke treffen die Zahlungsverkehrs-dienstleister Sicherheitsmaßnahmen, um sicherzu-stellen, dass jede der folgenden Anforderungen erfüllt ist:
  - es können keine Informationen über die Elemente der starken Kundenauthentifizierung, die als Wissen, Besitz und Inhärenz kategorisiert sind, aus der Offenlegung des Authentifizierungscodes abgeleitet werden;
  - es ist nicht möglich, einen neuen Authentifizierungscode auf der Grundlage der Kenntnis eines vorher erstellten anderen Authentifizierungscodes zu generieren;
  - der Authentifizierungscode kann nicht gefälscht werden.

  (Artikel 4 (2))

RTS – Starke Kundenauthentifizierung

- Wenden Zahlungsdienstleister eine starke Kundenauthentifizierung … an, so ergreifen sie folgende Sicherheitsvorkehrungen:
  - der Zahler wird über den Betrag des Zahlungsvorgangs und des Zahlungsempfängers unterrichtet;
  - …. Jede Änderung des Betrages oder des Zahlungs-empfängers führt zur Ungültigkeit des generierten Authentifizierungscodes.

(Artikel 5 (1))

RTS – Starke Kundenauthentifizierung

- Die Zahlungsverkehrsdienstleister stellen sicher, dass die Verwendung der … genannten Elemente einer starken Kundenauthentifizierung Maßnahmen in Bezug auf Technologie, Algorithmen und Parameter unterliegt, die sicherstellen, dass die Kompromittierung eines der Elemente die Zuverlässigkeit der anderen Elemente nicht beeinträchtigt.

  Artikel 9 (1)

RTS – Starke Kundenauthentifizierung

- Wird eines der Elemente einer starken Kundenauthentifizierung oder der Authentifizierungscode über ein Mehrzweckgerät, einschließlich Mobiltelefone und Tablets, verwendet, ergreifen die Zahlungsdienstleister Sicherheitsmaßnahmen, um das Risiko einer Gefährdung des Mehrzweckgeräts zu reduzieren.

  Artikel 9 (2):

RTS – Starke Kundenauthentifizierung

- Bezüglich Artikel 9 (2) umfassen die Maßnahmen zur Reduzierung einer Gefährdung Folgendes:

  a) die Verwendung getrennter **sicherer Ausführungs-umgebungen** durch die in dem Mehrzweckgerät installierten Software;

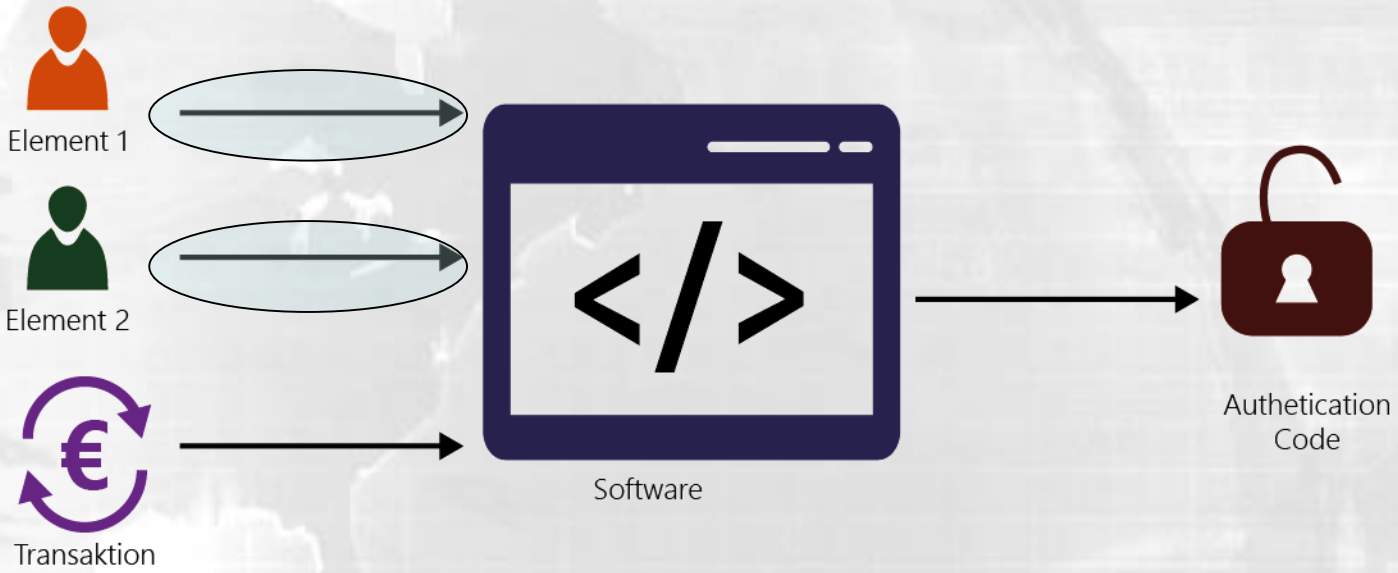
  (the use of separated secure execution environments through the software installed inside the multi-purpose device;)

  a) Maßnahmen, mit denen sichergestellt werden soll, dass weder die Software noch das Gerät vom Zahler oder von einem Dritten verändert wurden oder

  Maßnahmen um die Folgen einer solchen Änderung zu mildern, sofern sie stattgefunden hat. Artikel 9 (3):

  Artikel 9 (3)

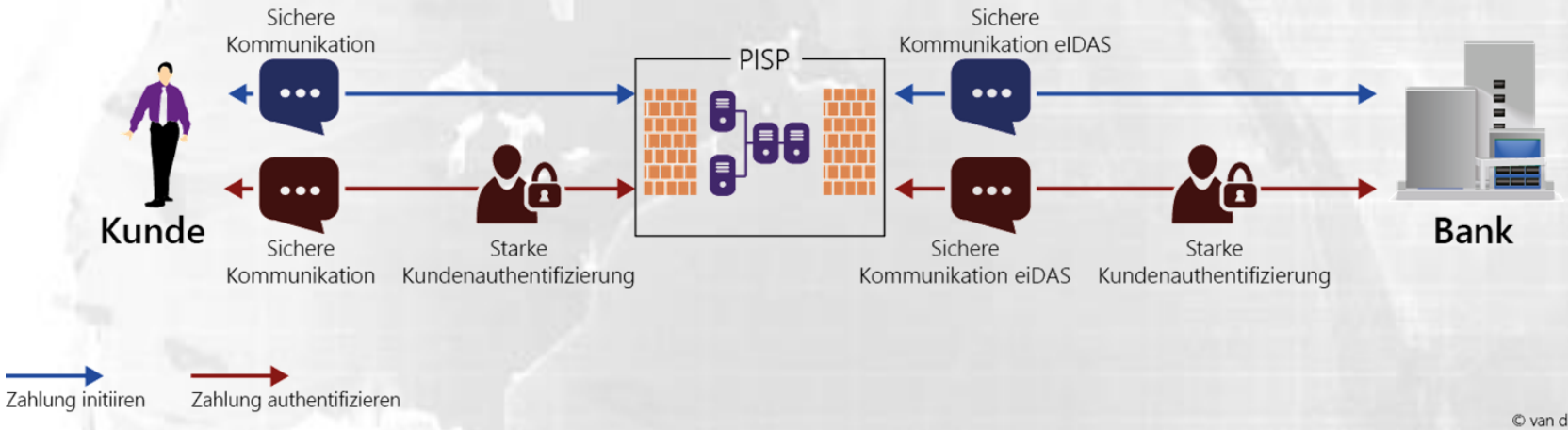
Secure Execution Environments



Inhalt

- Was sind Instant Payments?
- Instant Payments und der Handel
- Instant Payments am POS
- Gesetzliche Rahmenbedingungen für mobiles Bezahlen
- **Technische Herausforderungen**
  - **Starke Authentifizierung**
  - **Zugriff auf das Konto durch Dritte**

Payment Initiation via PISP



RTS – Access to Account - Zusammenfassung

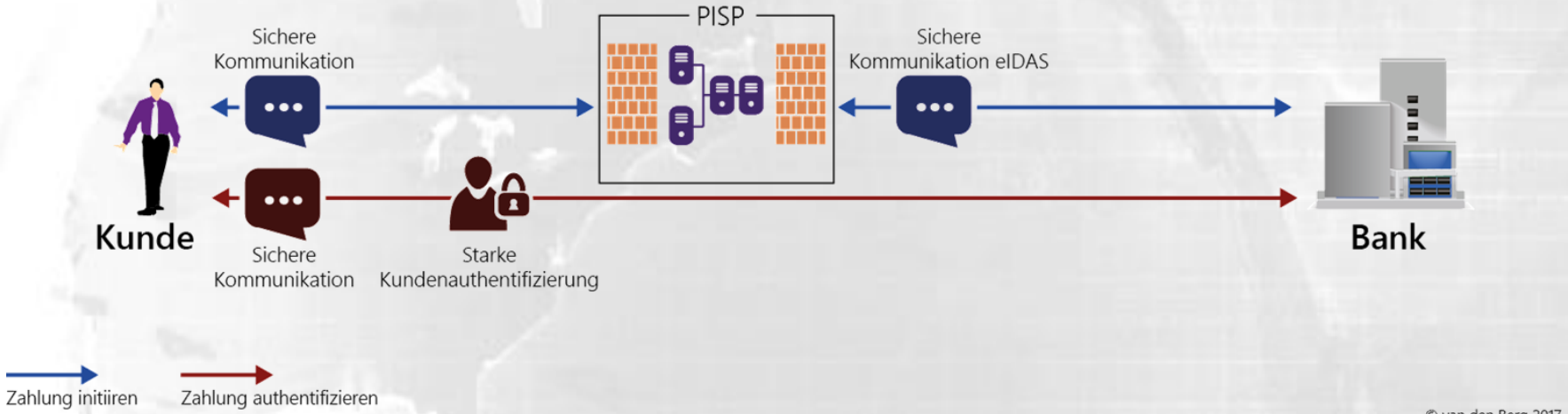
Für die von der kontoführenden Bank bereitgestellte Schnittstelle gilt:

1) Die Dokumentation ist kostenfrei bereitzustellen.
2) Änderungen müssen 3 Monate vor Inkrafttreten angekündigt und dokumentiert werden.
3) Die Schnittstelle muss die gleiche Funktionalität und Performance wie die selbstgenutzte Schnittstelle aufweisen.
4) Es ist eine kostenfreie Test-Infrastruktur bereitzustellen.
5) Die kontoführende Bank kann die selbstgenutzte Schnittstelle freigeben oder eine dedizierte Schnittstelle anbieten.

RTS – Access to Account - Zusammenfassung

6) Die PISP und AISP müssen sich gegenüber der kontoführenden Bank identifizieren können (nach eIDAS).
7) Eine sichere Kommunikation ist erforderlich.
8) Für die Authentifizierung kann auf die Infrastruktur der kontoführenden Bank zurückgegriffen werden.

Separate Authentifizierungs-App



Anforderungen an eine starke Kundenauthentifizierung durch die Einführung von Instant Payments

van den berg
Payment Services

Hans-Rainer van den Berg
CEO
van den Berg AG
Im Straßer Feld 3
52134 Herzogenrath
Fon: +49 (0) 2406 954 550
Fax: +49 (0) 2406 954 599
Email: hans-rainer.vdb@vdb.de
www.vdb.de