

Recht der Zahlungsdienste

1. 2026

Betriebs-Berater Geldverkehr

Alle RdZ-Beiträge sind auch online in der R&W-Online-Datenbank abrufbar

EDITORIAL

Ulrich Binneböbel:

Preiswettbewerb und Transparenz: Potenzial des Surcharging für den Handel

1

AUFSÄTZE

AUFSICHTSRECHT

Dr. Matthias Terlau:

Agentic Payments

4

Prof. Dr. Cornelia Manger-Nestler:

Zahlungstoken und Zahlungsverkehrsfreiheit

12

Dr. Sarah Wrage und Stefanie Franz:

Zahlungsdienstleister im Absatzfinanzierungsaufsichtsgesetz: Auswirkungen und Herausforderungen

20

Dr. Christian Zumpf:

Einordnung des Factoring als Zahlungsdienst

28

Wolfgang Otte:

Veränderungen der Prüfungspflichten bei grenzüberschreitenden Zahlungen und Echtzeitüberweisungen nach der ZahlPrüfV

36

STEUERRECHT

Katharina Wagener und Dr. Steffen Rapp:

CESOP – Meldepflicht für Zahlungsdienstleister

44

LÄNDERREPORT

Dr. Judith Sild:

RdZ-Länderreport Liechtenstein: Aktuelle Entwicklungen im Aufsichts-, Zivil- und Steuerrecht für Zahlungsdienste

52

TECHNIK-SCHLAGLICHT

Nikolaos Mekras und Andri Bremm:

PCI DSS 4.0 und Tokenisierung: Auswirkungen und praktische Umsetzung für Händler

67

PCI DSS 4.0 und Tokenisierung: Auswirkungen und praktische Umsetzung für Händler

Lange galt im digitalen Handel: „Daten sind das neue Öl“. Für Zahlungsdaten (cardholder data) hat sich dieses Verständnis jedoch grundlegend gewandelt. Wie *Hemkemeier* (RdZ 2020, 138ff.) zeigt, ist das Sicherheitsgefühl der Kunden ein zentraler wirtschaftlicher Faktor – Vertrauen wird zur Voraussetzung für den Wandel. Gleichzeitig hat sich die Bedrohungslage verschoben: Angriffe richten sich nicht mehr primär gegen Händlerinfrastruktur, sondern gegen den Browser des Kunden. Client-Side Attacks wie Digital Skimming oder Magecart kompromittieren Drittanbieter-Skripte innerhalb der Digital Supply Chain und greifen die Primary Account Number (PAN) bereits vor der Verschlüsselung ab. Für Händler ist dies besonders kritisch: Sie haften für Sicherheitsverletzungen in einer Umgebung, die sie technisch nur begrenzt kontrollieren können. Der Schutz der Checkout-Integrität wird damit zur regulatorischen und wirtschaftlichen Pflicht. Diese veränderte Bedrohungslage und der steigende regulatorische Druck verschieben die Rollen und Risikoprofile aller Beteiligten. Der nachfolgende Beitrag entwickelt vor diesem Hintergrund Lösungsansätze.

Nikolaos Mekras und Andri Bremm

Digital Supply Chain als Haftungsfalle für Händler

Händler tragen juristisch Verantwortung für eine Umgebung (den Browser des Kunden), die sie technisch nicht kontrollieren können, was einen strukturellen Zielkonflikt zwischen Marketing (Umsatz durch dynamische Features/Tracking) und Compliance/IT-Security (Abschottung) erzeugt. Jede neue Integration wird zum potenziellen Einfallstor für Angreifer und zum Compliance-Verstoß nach der Anforderung des Payment Card Industry Data Security Standard (PCI DSS) 6.4.3 zur Malware-Prävention und zum Schutz vor JavaScript-Manipulation, wenn sie nicht rigide überwacht wird. Der Händler muss faktisch die IT-Sicherheit seiner Zulieferer (Chatbot-Anbieter, Analytics-Dienste) auditieren (vendor management). Versagt ein Drittanbieter, fallen der Reputationsschaden („Datenleck bei Händler XY“) und die Haftung nach der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Datenschutz-Grundverordnung] – DSGVO, ABIEU vom 4.5.2016, L 119, 1) auf den Händler zurück. Die Verarbeitung der Cardholder Data (u. a. PAN) wird somit vom bloßen Prozessschritt zum unkalkulierbaren Betriebsrisiko.

Für Payment Service Provider (PSP) und Acquirer verschiebt sich die Value Proposition. Die reine Abwicklung der Zahlung (processing) wird zur Commodity. Der wahre Wert für den Händler liegt nun in der Fähigkeit des PSP, Komplexität zu abstrahieren. Der PSP muss seine Frontend-Komponenten härten, bspw. iFrames und Software Development Kit (SDK), sodass sie selbst in einer „feindlichen“ Umgebung (einem kompromittierten Händler-Shop) sicher funktionieren (*technologische Aufrüstung*). Er

muss garantieren, dass sein iFrame resistent gegen Cross-Site Scripting (XSS) und Clickjacking ist. Der PSP wird zum *Enabler* des „Descoping“ und muss durch Architektur sicherstellen, dass der Händler nie mit PAN-Daten in Berührung kommt. Gelingt dies nicht, verliert der PSP seine wirtschaftliche Relevanz, da er dem Händler die regulatorische Last nicht mehr abnehmen kann.

Descoping als Grundlage für reibungslose Checkout-Journey

Die Antwort auf die strengen Anforderungen des PCI DSS 4.0 darf nicht zu Lasten des Einkaufserlebnisses gehen. Im E-Commerce gilt: Jeder Reibungspunkt im Check-out ist ein potenzieller Kaufabbruch. Die strategische Lösung für Händler besteht daher darin, Sicherheit und User Experience (UX) nicht als Gegensätze, sondern als integrierte Einheit zu betrachten.

Der Wandel vom Redirect zur nahtlosen Integration prägt die moderne Zahlungsabwicklung. In der Vergangenheit wurde „Sicherheit“ oft durch einen harten Bruch in der Customer Journey erkaufte: Der Kunde wurde für die Zahlungseingabe via Redirect auf die externe Seite des PSP umgeleitet. Dieser Medienbruch – oft begleitet von einem Designwechsel und einer Änderung der URL – führte nachweislich zu Vertrauensverlust und Kaufabbrüchen (Baymard Institute, Cart & Checkout Usability Research, <https://baymard.com/research/checkout-usability>, Abruf: 23.1.2026). Die moderne Antwort hierauf ist die technische Entkopplung mittels Hosted Fields oder iFrame-Lösungen. Der Kunde verbleibt visuell im Shop-Umfeld des Händlers. Die Eingabefelder für Kartendaten werden vom sicheren Server des PSP geladen und lassen sich mittels Cascading Style Sheets (CSS) so gestalten, dass sie sich konsistent in das Corporate Design des Händlers einfügen.

Technisch nutzt diese Architektur die Same-Origin Policy des Browsers. Da das Eingabefeld (Origin: PSP) und der Shop (Origin: Händler) getrennt sind, berühren die sensiblen PAN-Daten zu keinem Zeitpunkt die Systeme des Händlers (maximales descoping). Für den Händler führt dies zu einer deutlichen Reduktion des Compliance-Aufwands (i. d. R. Self-Assessment Questionnaire – SAQ), da die Verarbeitung der Zahlungsdaten vollständig beim PSP verbleibt. Gleichzeitig bleibt die Interaktion für den Kunden konsistent, was eine positive Checkout-Erfahrung unterstützt.

Die Grenzen des Descoping unter PCI DSS 4.0 zeigen sich trotz technischer Auslagerung der Dateneingabe. Auch diese Lösung entlässt den Händler nicht vollständig aus der Verantwortung: Da der iFrame in die Seite des Händlers eingebettet ist, bleibt die Umgebung (parent frame) im Fokus der neuen Überwachungsanforderungen (Req. 6.4.3 und 11.6.1). Dennoch ist das Outsourcing der Dateneingabe an den PSP die einzige wirtschaftlich sinnvolle Methode, um operative Sicherheit und moderne UX zu vereinen.

Da die Frontend-Isolation nur die Eingabe schützt, ist für die Verarbeitung eine Tokenisierung unverzichtbar. Würde die echte Kartennummer (PAN) in das Händler-Backend zurückfließen, wäre der Sicherheitsgewinn hinfällig. Stattdessen erhält der Händler ein Surrogat (token), das Prozesse wie Gutschriften oder Subscriptions ermöglicht, ohne sensible Daten zu speichern. Strategisch entscheidend ist hierbei die Wahl der Architektur: Händler müssen zwischen proprietären PSP-Token und unabhängigen Scheme Token abwägen, um ihre zukünftige Unabhängigkeit zu sichern.

Wahl der Token-Architektur als strategische Entscheidung

Mit der Entscheidung für Tokenisierung, ist das „Wie“ gelöst, aber noch nicht das „Was“. Für Entscheidungsträger und Juristen ist zentral, dass Token nicht gleich Token ist. Die gewählte Architektur beeinflusst unmittelbar Flexibilität, Kostenstruktur und die Datenhoheit des Händlers und entscheidet faktisch über Portabilität oder Vendor Lock-in.

Traditionell vergeben PSP eigene, proprietäre Gateway Token. Der Händler sendet die Kartendaten an den PSP, dieser speichert sie in seinem Tresor und sendet eine zufällige Zeichenfolge (z. B. TOK_12345) zurück. Das daraus resultierende strategische Risiko liegt in der fehlenden Portabilität. Die Token sind nur innerhalb des jeweiligen PSP gültig und verlieren bei Multi-Acquiring (Nutzung mehrerer Zahlungsdienstleister zur Kostenoptimierung oder Ausfallsicherheit) oder Anbieterwechsel ihre Funktion. Migrationen sind technisch komplex, teuer und vertraglich eingeschränkt. Der Händler begibt sich in einen klassischen Vendor Lock-in.

Die Antwort der Kartenorganisationen auf dieses Problem sind sog. Scheme Token (auch Network Token), die direkt vom Netzwerk ausgegeben werden, etwa über Mastercard Digital Enablement Service (MDES) oder Visa Token Service (VTS). Dank netzwerkseitiger Verankerung sind Scheme Token PSP-übergreifend nutzbar. Ein zentraler Vorteil ist das automatisierte Lifecycle-Management: Das Scheme aktualisiert Token im Hintergrund, wodurch wiederkehrende Zahlungen (subscriptions) stabil bleiben und ungewollte Ausfälle (involuntary churn) minimiert werden. Die Schemes forcieren diesen Standard strategisch gegen Alternativen wie Open Banking. Über ökonomische Anreize wird die Adoption erzwungen: Händler profitieren von reduzierten Gebühren und technisch bedingt höheren Genehmigungsraten (approval rates). Die klassische PAN-Nutzung wird hingegen zunehmend sanktioniert, was den Token zum wirtschaftlichen Standard macht.

Der Einsatz von Scheme Token in Multi-Acquiring-Landschaften erhöht die Komplexität. Fordert derselbe Händler für eine Karte über PSP A und später über PSP B einen Token an, entstehen i. d. R. zwei unterschiedliche Network Token. Dies ist kein Designfehler, sondern systembedingt, da mehrere Token parallel für einen Payment Account existieren können, etwa pro Gerät oder Nutzungskontext. Für den Händler entsteht dadurch ein Zuordnungsproblem, etwa bei Betrugsprävention, Loyalty-Programmen oder Limits. Hier kommt die PAR als „Single Source of Truth“ ins Spiel. Sie ist ein nicht-sensitiver, 29-stelliger alphanumerischer Identifikator, der fest mit dem zugrundeliegenden Kartenkonto verknüpft ist. Unabhängig von Token oder PSP bleibt die PAR identisch und ermöglicht damit eine eindeutige Wiedererkennung über Kanäle und Acquirer hinweg.

Praktische Implikationen für die Händler-IT

Das Datenmodell muss angepasst werden, da nicht der einzelne Token, sondern die PAR als globaler Anker für das Zahlungsprofil eines Kunden dienen sollte. Auch die Reconciliation verändert sich. Der Abgleich der Abrechnungsdaten (settlement files) über verschiedene Acquirer hinweg hat auf Basis der PAR zu erfolgen, um einen „Single Customer View“ zu gewährleisten. Die Kombination aus Scheme Token für die Transaktion und PAR für die Datenhaltung erlaubt Händlern erstmals eine weitgehende Unabhängigkeit von einzelnen Dienstleistern bei gleichzeitig hohen Genehmigungsraten (EMVCo, EMV® Payment Tokenisation Specification – Technical Framework, <https://www.emvco.com/specifications/emv-payment-tokenisation-specification-technical-framework/>, Abruf 23.1.2026).

Die technische Umsetzung reicht von Browser-Härtung bis zur Biometrie und basiert strategisch auf Scheme Token und Hosted Fields. Die praktische Kür besteht nun darin, diese Architektur technisch so zu implementieren, dass sie den harten Anforder-

rungen von PCI DSS 4.0 standhält und gleichzeitig als Sprungbrett für modernste Authentifizierungsverfahren dient. Mit Blick auf den Browser führt an Subresource Integrity (SRI) und einer Content Security Policy (CSP) kein Weg vorbei.

Der sichere Einsatz von Hosted Fields erfordert CSP und SRI, da die Verarbeitung sensibler Zahlungsdaten zwar in den iFrame des PSP verlagert wird, die Shop-Seite des Händlers jedoch weiterhin sicherheitsrelevant bleibt. Manipulationen im Parent Frame können die Integrität des Zahlungsprozesses gefährden, weshalb der PCI DSS 4.0 dies mit Req. 6.4.3 und 11.6.1 ausdrücklich adressiert. SRI schützt fremde Skripte (z. B. das PSP-JavaScript zur Einbindung der Hosted Fields) durch kryptographische Prüfsummen gegen Manipulation (Mozilla, Subresource Integrity, https://developer.mozilla.org/de/docs/Web/Security/Defenses/Subresource_Integrity, Abruf: 23.1.2026). Weitaus mächtiger als SRI ist der Einsatz einer strikten CSP. Die Überwachung der verwendeten CSP, ist ein Teil für die Erfüllung der PCI-DSS-Anforderung 11.6.1 („Kontinuierliche Überwachung der Shop-Seite bzgl. Manipulation“). Die CSP definiert über Hypertext Transfer Protocol (HTTP) Header verbindlich, welche Inhalte der Browser laden und ausführen darf, und wird damit zu einem zentralen Kontrollinstrument der Frontend-Sicherheit. Sie ermöglicht es, die Herkunft externer Ressourcen zu begrenzen, den Abfluss von Daten an nicht autorisierte Ziele zu unterbinden und die Ausführung unsicherer Skripte zu verhindern (Mozilla, Content Security Policy, <https://developer.mozilla.org/de/docs/Web/HTTP/Guides/CSP>, Abruf: 23.1.2026).

Diese Form der Browser-Härtung wirkt umso besser, je schlanker und kontrollierter die Seite ist. Je weniger Third-Party-Skripte, desto stabiler ist die Compliance und desto geringer ist das Risiko von Manipulationen. Warum das zählt, zeigt ein typisches Angriffsmuster: Ein kompromittiertes Analytics-Skript aus dem Tag Manager blendet unbemerkt Overlays ein und versucht Formjacking. Eine konsequent umgesetzte CSP trägt dazu bei, dass die Hosted Fields isoliert bleiben und sensible Zahlungsdaten wirksam vor clientseitigen Angriffen geschützt werden.

Erhöhte Sicherheit durch Gerätebindung

Nachdem CSP und Hosted Fields bereits die Erfassung der Kartendaten absichern, sorgen Device Binding und Delegated Authentication dafür, dass Sicherheit und User Experience zusammenwachsen. Die Leitidee: Ein gestohlenen Scheme Token bleibt außerhalb des autorisierten Endgeräts wertlos, während die starke Kundenauthentifizierung nahtlos im Checkout läuft.

Das Scheme Token fungiert als stabiles Card-on-File-Artefakt. Beim initialen Enrollment, typischerweise im Rahmen einer stark authentifizierten Zahlung, wird die PAN tokenisiert und gleichzeitig ein gerätegebundener kryptografischer Schlüssel in einer

hardwaregeschützten Umgebung erzeugt (FIDO Alliance, FIDO UFA Specifications, <https://fidoalliance.org/specifications/download/>, Abruf 23.1.2026). Der private Schlüssel verbleibt ausschließlich auf dem Endgerät, der öffentliche Schlüssel wird mit dem Scheme Token und dem Kundenkonto verknüpft. Optional belegt eine Attestation, dass es sich tatsächlich um einen hardware-gesicherten Schlüssel handelt. So entsteht eine Gerätebindung, die Sicherheit by Design bietet und zugleich datenschutzfreundlich ausgestaltet ist.

Die Folgezahlungen unterscheiden sich je nach Kanal, bleiben aber konzeptionell gleich: Eine transaktionsspezifische Challenge mit Betrag, Händler und Nonce wird lokal signiert. Der Nonce ist eine einmalige, nicht vorhersagbare Zeichenfolge, die pro Vorgang generiert wird, um Replay-Angriffe zu verhindern. Die Signierung unterscheidet sich für Webseiten und native Apps.

Im Web initiiert der Händler WebAuthn oder Secure Payment Confirmation (W3C, Web Authentication: An API for accessing Public Key Credentials, <https://www.w3.org/TR/webauthn-2/>, Abruf 23.1.2026). Der Kunde bestätigt per Biometrie oder Personal Identifier Number (PIN), die Signatur entsteht im Hardware-Backed Keystore. „Biometrie am Origin“ ersetzt den Redirect in die Bank-App. Der PSP validiert die Fast-Identity-Online-(FIDO-)Assertion, verknüpft sie mit dem Scheme Token und erzeugt das notwendige Token-Kryptogramm für die Autorisierung. Erst durch das Kryptogramm lässt sich eine sichere Zahlung für ein Scheme Token ausführen. In Apps erfolgt die Signatur über Plattform-Keystore und die Operating System Biometrie.

Delegated Authentication verlagert die starke Kundenauthentifizierung vom Issuer zu Händler/PSP und erfordert eine formale Programmzulassung durch die Schemes. Der PSP übermittelt den „Proof of Authentication“, der sich in den Autorisierungsdaten widerspiegelt, etwa über Electronic Commerce Indicator (ECI)-Wert sowie Authentifizierungsdaten wie Accountholder Authentication Value (AAV) bzw. Accountholder Verification Value (AVV). In Kombination mit der höheren Token-Assurance der Gerätebindung resultieren daraus bessere Genehmigungsraten und weniger False Declines. PSD II (ABIEU vom 23.12.2015, L 337, 35) bleibt eingehalten, FIDO-zertifizierte Authentificatoren regeln Governance und Haftung (European Banking Authority, Regulatory Technical Standards on Strong Customer Authentication and secure communication under PSD2, <https://www.eba.europa.eu/legacy/regulation-and-policy/regulatory-activities/payment-services-and-electronic-money-0>, Abruf 23.1.2026).

Zentral ist das Lifecycle-Management: Bei Gerätewechsel erfolgt ein Re-Binding mit Step-up (bspw. per EMV 3DS-Challenge). Verlorene

oder kompromittierte Geräte werden serverseitig entkoppelt, zusätzliche Geräte sauber eingebunden. Token-Lifecycle-Updates der Schemes halten Kartendaten aktuell – ohne erneuten Kundeneingriff.

Rechtliche und ökonomische Implikationen für das Ökosystem

Die Implementierung von Scheme Token und hardware-gestützter Authentifizierung ist mehr als ein IT-Upgrade. Für die juristische Bewertung von Zahlungsrisiken und Datenschutzkonzepten können sich fundamentale Verschiebungen ergeben, die es zu analysieren gilt.

Liability Shift: Im klassischen E-Commerce trägt oft der Händler das wirtschaftliche Risiko für Kartenbetrug (chargebacks), insbesondere wenn keine 3D-Secure-Authentifizierung stattfindet. Der Einsatz von Scheme Token i.V.m. Device Binding kann diese Risikoverteilung verschieben (Visa, Visa Core Rules and Visa Product and Service Rules, 18.10.2025, <https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf>, Abruf: 23.1.2026). In den Autorisierungsdaten fungieren Werte wie der ECI und der Token Authentication Verification Value (TAVV) als Nachweis einer abgesicherten Transaktion. Für den Händler entsteht dadurch ein messbarer ökonomischer Effekt: Betrugsrisiken und Rückstellungen sinken, ohne dass Conversion-Raten durch aggressive Fraud-Filter beeinträchtigt werden.

Crypto-Shredding: Auch im Datenschutzrecht eröffnet Tokenisierung neue Spielräume. Das Recht auf Löschung nach Art. 17 DSGVO scheidet häufig an technischen Realitäten verteilter Back-up-Systeme. Das Crypto-Shredding bietet hier einen anerkannten Ausweg: Statt Daten physisch zu löschen, wird gezielt der kryptografische Schlüssel vernichtet. Ohne Schlüssel sind die Daten faktisch nicht mehr rekonstruierbar und gelten als gelöscht. Die Konzentration auf Schlüsselverwaltung statt Datenlöschung reduziert den operativen Compliance-Aufwand erheblich.

Benefit für die Machine Economy

Die Welt entwickelt sich dahin, dass nicht mehr die Absicherung menschlicher Eingaben im Browser im Zentrum steht, sondern autonome Maschinen ohne manuellen Check-out handeln und bezahlen.

Ein Vorreiter dieser Entwicklung ist der Mobilitätssektor. Der Standard ISO 15118 (Plug & Charge: International Organization for Standardization, ISO 15118-2, Road vehicles – Vehicle-to-Grid Communication Interface, <https://www.iso.org/standard/55366.html>, Abruf 23.1.2026) skizziert bereits heute eine Realität, in der sich Elektrofahrzeuge an der Ladesäule per Zertifikat authentifizieren und Zahlungen ohne App oder Ladekarte auslösen. Diese Logik lässt sich zum Konzept „Vehicle as Wallet“ erweitern, bei dem Fahrzeuge eigenständig Parkgebühren, Maut

oder Energie beziehen. Die Freigabe der Zahlung erfolgt dabei nahtlos, etwa durch Kameras im Innenraum, die den Fahrer biometrisch identifizieren, oder durch die reine Maschinen-Identität bei Kleinstbeträgen. Tokenisierung bildet dabei die sicherheitstechnische Grundlage, da hinterlegte Zahlungs-Token selbst bei physischer Kompromittierung des Systems nicht extrahierbar sind.

Auch KI-Agenten (z. B. Einkaufs-Bots) benötigen in solchen Szenarien eigene, kontrollierbare Zahlungsfähigkeiten. Sogenannte Bound oder Agentic Token können mit technischen Restriktionen (policies) versehen werden, etwa nach Händlerkategorie, Betrag oder Zeitfenster. Tokenisierung ermöglicht damit programmierbares Geld, das autonome Interaktion erlaubt, ohne die finanzielle Kontrolle des Menschen oder Unternehmens aufzugeben.

Konsequente Umsetzung als Business Enabler

Was als Reaktion auf Client-Side Attacks und den regulatorischen Druck durch PCI DSS 4.0 begann, erweist sich als struktureller Katalysator für eine moderne Zahlungsarchitektur. Tokenisierung und konsequentes Descoping reduzieren nicht nur Angriffsflächen, sondern verschieben Sicherheit vom operativen Risiko zur architektonischen Eigenschaft. Händler entziehen Angreifern die ökonomische Motivation und gewinnen zugleich regulatorische Stabilität. Compliance wird damit vom Kostenfaktor zum funktionalen Enabler. Der Nutzen zeigt sich unmittelbar in einer robusteren UX, etwa durch biometrisch abgesicherte „One-Click-Check-outs“, und perspektivisch in vollständig automatisierten Zahlungskontexten wie autonom agierende Fahrzeug. Der PCI DSS 4.0 ist somit nicht der Bremsklotz, sondern das Fundament für eine skalierbare und vertrauenswürdige Machine Economy.

AUTOREN



Nikolaos Mekras ist Principal Consultant und Experte für Digitale Plattformen im Zahlungsverkehr bei der Senacor Technologies AG in München.



Andri Bremm ist Technical Lead und Architekt für skalierbare Zahlungssysteme bei der Senacor Technologies AG in München.