IU Internationale Hochschule

Fernstudium

Studiengang: Bachelor of Engineering - Robotics

6. Semester

Modul: DLBISIC02-01 - Kryptografische Verfahren

Tutor:in: Nils Kannengießer

Fallstudie zum Thema: Zahlung mit Kreditkarte

Einführung der Kreditkartenzahlung in einem mittelständischen deutschen Onlineshop

INTERNATIONALE
HOCHSCHULE

Datum: 20.05.2025

Verfasser: Timo Kliesch

Matrikelnummer: IU14072463

I. Inhaltsverzeichnis

II. Abkürzungsverzeichnis

API ..... Application Programming Interface

BDSG ..... Bundesdatenschutzgesetz

BIN ..... Bank Identification Number

CVC / CVV ..... Card Verification Code / Card Verification Value

DSGVO ..... Datenschutz-Grundverordnung

EMV ..... Europay International, Mastercard, Visa (Technologie-Standard für Chipkarten)

HSM ..... Hardware Security Module

MAC ..... Message Authentication Code

NFC ..... Near Field Communication

OWASP ..... Open Web Application Security Project

PAN ..... Primary Account Number (Kreditkartennummer)

PCI-DSS ..... Payment Card Industry Data Security Standard

PSP ..... Payment Service Provider

PSD2 ..... Payment Services Directive 2 (Zweite EU-Zahlungsdiensterichtlinie)

QKD ..... Quantum Key Distribution (Quanten-Schlüsselverteilung)

RSA ..... Rivest-Shamir-Adleman (asymmetrisches Verschlüsselungsverfahren)

SCA ..... Strong Customer Authentication

SSL ..... Secure Sockets Layer

TAN ..... Transaktionsnummer

TLS ..... Transport Layer Security

TPM ..... Trusted Platform Module

USB ..... Universal Serial Bus

2FA ..... Zwei-Faktor-Authentifizierung

1. Einführung der Kreditkartenzahlung in einem mittelständischen deutschen Online-Shop

In vielen mittelständischen Onlineshops ist Vorkasse noch immer eine verbreitete Zahlungsoption. Der Wunsch nach zusätzlicher Kreditkartenzahlung entsteht häufig aufgrund steigender Kundenerwartungen und Wettbewerbsdrucks. Kreditkartenzahlungen gelten jedoch als besonders sicherheitskritisch. Sie bringen viele beteiligte Parteien ins Spiel (Karteninhaber, Händler, Acquirer, Issuer und Kartennetzwerke) und bergen verschiedene Risiken wie Kartenbetrug oder Missbrauch gespeicherter Daten. Insbesondere im „Card-not-present"-Szenario (Online-Zahlung) kann die Authentizität der Karte nicht durch physische Kontrolle gewährleistet werden. Daher muss der Online-Shop für die neue Zahlungsschnittstelle strenge Sicherheits- und Datenschutzanforderungen erfüllen. In diesem Kontext werden beispielsweise nur die minimal notwendigen Daten über verschlüsselte Verbindungen übermittelt. Kundennamen etwa werden bei der Autorisierung nicht mitgesendet, und schon an den Netzwerkknoten sind lediglich Teile der Kontodaten sichtbar (DKB, März, 2022). Diese Herausforderungen erfordern eine sorgfältige Planung unter Berücksichtigung der gesetzlichen Vorgaben und technischer Schutzmaßnahmen.

2. Rechtliche Rahmenbedingungen

Der Einsatz von Kreditkartenzahlungen unterliegt in Deutschland und der EU strengen regulatorischen Vorgaben. Die Zweite Zahlungsdiensterichtlinie (PSD2) schreibt beispielsweise eine „starke Kundenauthentifizierung" (Strong Customer Authentication, SCA) für Online-Zahlungen vor. Hierzu gehört mindestens eine Zwei-Faktor-Authentifizierung (2FA), etwa durch TAN- oder Push-Verfahren. Online-Zahlungsdienste wie PayPal müssen diesen Vorgaben folgen, indem etwa jedem Konto eine Telefonnummer zugeordnet und für Zahlungsbestätigungen eine SMS-TAN versendet wird. Auch Kreditkartenzahlungen fallen unter PSD2, was bedeutet, dass Banken und Zahlungsdienstleister bei Transaktionen zusätzliche Sicherheitskontrollen durchführen müssen.

Neben den gesetzlichen Vorgaben der PSD2 spielt der Payment Card Industry Data Security Standard (PCI-DSS) eine zentrale Rolle. PCI-DSS ist ein branchenweit anerkanntes Regelwerk (kein Gesetz), das Unternehmen vorschreibt, wie Kreditkartendaten technisch und organisatorisch zu schützen sind. Jede Organisation, die Kartenzahlungen akzeptiert, muss die in PCI-DSS definierten Maßnahmen vertraglich umsetzen. Dazu zählen unter anderem Verschlüsselung der Datenübermittlung, strikte Zugriffsbeschränkungen auf die Daten sowie regelmäßige Updates und Sicherheitsüberprüfungen (z. B. Penetrationstests) (DKB, März, 2022). Insbesondere verbietet PCI-DSS das Speichern sensibler Authentifizierungsdaten. Weder der Prüfcode (CVC/CVV) noch der magnetische Streifen (Track 2 Data) dürfen nach der Autorisierung im Shop-System abgelegt werden.

Schließlich ist auch der Datenschutz ein wichtiger Faktor. Kreditkartendaten gelten als personenbezogene Daten (z. B. Kontoinhaber-Name, Kontonummer), sodass die EU-Datenschutz-Grundverordnung (DSGVO) und das ergänzende Bundesdatenschutzgesetz (BDSG) Anwendung finden. Seit dem 25. Mai 2018 ist die DSGVO in allen Mitgliedstaaten unmittelbar geltendes Rech (Müller, 2018, S.55). Dies bedeutet, dass der Online-Shop beim Umgang mit Kartendaten alle Grundsätze der DSGVO beachten muss (Zweckbindung, Datenminimierung, Speicherbegrenzung etc.). Das neue BDSG nennt als empfohlene Maßnahmen explizit unter anderem Pseudonymisierung und Verschlüsselung von Daten (Müller, 2018, S.56). Tokenisierung, also das Ersetzen der echten Kartennummer durch einen irreversiblen Token ist eine praxisnahe Umsetzung dieser Vorgabe und verringert das Risiko bei der Speicherung von Zahlungsdaten. Auch organisatorisch sind Maßnahmen gefordert. Dazu zählen die Beschränkung des Zugriffs auf die Kartendaten auf einen engen Nutzerkreis und das Führen lückenloser Protokolle, wer wann auf die Daten zugegriffen oder sie verändert hat (Müller, 2018, S.56).

3. Ablauf der Kreditkartenzahlung

Kreditkartenzahlungen folgen typischerweise einem Vier-Parteien-System (DKB, März, 2022) (Karteninhaber, Händler, Acquirer, Issuer) beziehungsweise fünf Parteien, wenn man das Kartennetzwerk (Visa/Mastercard) gesondert zählt. Der technische Ablauf bei einer Online-Zahlung lässt sich vereinfacht wie folgt beschreiben.

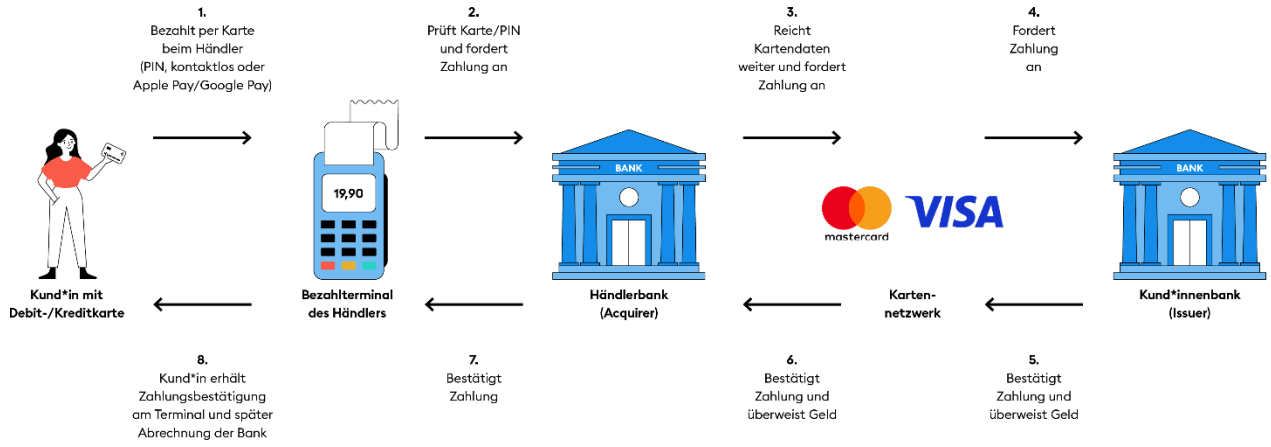
1. Übermittlung der Kartendaten: Der Kunde gibt seine Kreditkartennummer, das Ablaufdatum und ggf. den CVC ins Web-Formular des Shops ein. Über eine sichere TLS-Verbindung gelangen diese Daten zum Zahlungs-Gateway und weiter zur Händlerbank (Acquirer). Im Datensatz ist die Bank-Identifikationsnummer (BIN) der Karte enthalten; anhand der ersten Ziffer (z. B. „4“ für Visa, „5“ für Mastercard) erkennt das System das zuständige Kartennetz (DKB, März, 2022).

2. Autorisierung durch Issuer: Der Acquirer leitet die Transaktionsanfrage an das Kartennetz weiter, das sie an die ausgebende Bank (Issuer) des Karteninhabers sendet. Die Issuer-Bank prüft, ob die Karte gültig und ausreichend gedeckt ist. Hier fließen Prüfungen zur Kartenstatus, Kontodeckung und Betrugsverdacht ein. Bei positiver Prüfung sendet der Issuer eine Genehmigung zurück an das Kartennetz und dann an den Acquirer. Im negativen Fall erfolgt eine Ablehnung.

3. Bestätigung und Clearing: Erhält der Acquirer die Freigabe, meldet er dies ans Shop-Terminal, und die Bestellung gilt als bezahlt. Gleichzeitig wird die Belastung des Kartenkontos in Höhe des Betrags durchgeführt. Der Issuer bucht dem Kunden das Geld ab und überweist es über Clearingprozesse an die Händlerbank. Der gesamte Vorgang dauert üblicherweise nur Bruchteile einer Sekunde (DKB, März, 2022). Anschließend kann der Händler die bestellten Waren ausliefern, da er die Zahlungsgarantie erhalten hat.

4. Sonderfall „Card Not Present“: Im Online-Shop liegt die Karte dem Händler physisch nicht vor. Die Verifizierung erfolgt daher nicht über Chip/PIN, sondern über die dreistellige Prüfnummer (CVC) auf der Kartenrückseite. Häufig wird die Transaktion zusätzlich durch das 3D-Secure-Verfahren abgesichert: Dabei wird über eine separate Bestätigungsstufe (z. B. Tan in einer Banking-App, Biometrie) sichergestellt, dass der Karteninhaber die Zahlung veranlasst (DKB, März, 2022).

Abbildung 1: So funktioniert eine Kartenzahlung



Quelle 1: Übernommen von DKB, 2022

Durch diese Abfolge zahlen am Ende der Händler und seine Bank eine kleine Interbankenprovision an Issuer und Kartennetz, und die Zahlungsdaten gelangen nur verschlüsselt und in reduzierter Form durch das System. Erst im Abrechnungsprozess werden alle Informationen (Kundendaten, Transaktionsbetrag) zusammengeführt (DKB, März, 2022). Dieser Vier-Parteien-Ablauf stellt die technische Grundlage dar und definiert Verantwortlichkeiten zwischen Shop, Acquirer und Kartenorganisation.

4. Technische und organisatorische Sicherheitsanforderungen

Für eine sichere Implementierung müssen zahlreiche technische und organisatorische Schutzmaßnahmen beachtet werden.

- Verschlüsselung: Die Verbindung zwischen Kundenbrowser und Shop muss durch TLS/SSL abgesichert sein. TLS gewährleistet Vertraulichkeit (symmetrische Verschlüsselung) und Integrität (MAC) sowie Authentizität der Serverzertifikate. Auch alle internen Kommunikationsstrecken im System sollten verschlüsselt oder tokenisiert werden. Kartendaten im Ruhe-Zustand müssen verschlüsselt gespeichert werden, oder sie

verbleiben überhaupt nicht im Klartext auf den Shop-Servern. Gemäß DSGVO/BDSG ist die Verschlüsselung personenbezogener Daten ausdrücklich empfohlen (Müller, 2018, S.56).

- Zugriffskontrollen: Der Zugriff auf das Zahlungssystem und Kartendaten muss streng reglementiert sein. Nur autorisierte Personen dürfen auf relevante Systeme zugreifen (Prinzip „Need-to-know“). Dies schließt auch die Beschränkung administrativer Rechte auf ein Minimum ein (Müller, 2018, S.56). Alle API-Schlüssel, Passwörter und Zertifikate sind sicher zu verwahren, und es sollte regelmäßig geprüft werden, ob Benutzerkonten korrekt zugewiesen sind.
- Logging und Monitoring: Sämtliche Zugriffe auf Kartendaten und sicherheitsrelevante Ereignisse müssen lückenlos protokolliert werden. Nach BDSG/DSGVO müssen die Verantwortlichen über jede Veränderung an personenbezogenen Daten Rechenschaft ablegen können (Müller, 2018, S.56). Das Log-Management umfasst hierbei sowohl das Erfassen von Transaktionen als auch die Überwachung auf Anomalien. Außerdem sind Systemlogs und Audit-Trails so zu gestalten, dass Manipulationen erkennbar und nachweisbar sind.
- Tokenisierung/Pseudonymisierung: Kunden können ihre Kreditkartendaten speichern, jedoch sollte der Shop nur ein Token (einstelliger Schlüssel) hinterlegen, das die Kartendaten im Hintergrund referenziert. So verbleiben sensible Daten nur beim Payment Service Provider oder im verschlüsselten Verzeichnis. Dieser Pseudonymisierungsansatz entspricht den DSGVO-Anforderungen (vgl. BDSG §22 Abs.2 Nr.6: Pseudonymisierung) (Müller, 2018, S.56).
- Regelmäßige Sicherheitsprüfungen: Gemäß PCI-DSS müssen kritische Systeme ständig aktualisiert und auf Schwachstellen getestet werden (DKB, März, 2022). Dazu gehören regelmäßige Penetrationstests, Schwachstellen-Scans und Updates von Betriebssystemen sowie Webserver- und Datenbank-Software. Angemessene Antiviren- und Intrusion-Detection-Systeme erhöhen die Sicherheit weiter. Auch das implementierte Payment-Plugin oder die Schnittstelle zum Zahlungsdienstleister sollte nach jeder Änderung (z. B. Update) erneut getestet werden.
- Starke Kundenauthentifizierung (SCA): Für jeden Zahlungsvorgang muss das System die Zweifaktor-Authentifizierung der PSD2 unterstützen. Im Checkout-Prozess ist beispielsweise 3D-Secure 2.0 einzusetzen, damit der Kunde den Kauf mit einem Einmalcode oder über eine Banking-App bestätigt. Dies ergänzt die Verschlüsselung und verhindert unautorisierte Transaktionen (Müller, 2018, S.56).
- Organisatorische Maßnahmen: Neben Technik sind auch Prozesse wichtig. Der Shopbetreiber sollte Datenschutzbeauftragte(n) benennen und Mitarbeitende zum Umgang mit Kartendaten schulen. Es müssen Richtlinien zur Datenaufbewahrung und -löschung

vorliegen (etwa automatisches Löschen veralteter Zahlungsdaten). Bei unerwarteten Vorfällen (z. B. Datenpanne) ist ein Incident-Response-Plan vorzuhalten, um schnell Gegenmaßnahmen einzuleiten.

Zusammengefasst müssen für die Einführung von Kreditkartenzahlungen nicht nur moderne Verschlüsselungstechniken (TLS, Tokenisierung) und Netzwerksicherheit implementiert werden, sondern auch strenge organisatorische Prozesse folgen. Dabei spielen die vorstehend genannten Standards wie PCI-DSS und die Datenschutzgesetze eine verbindliche Rolle. Wird jeder Schritt (Datenübertragung, Speichern, Zugriff, Monitoring) nach diesen Vorgaben abgesichert, kann das Risiko von Betrug und Datenpannen deutlich minimiert werden (DKB, März, 2022); (Müller, 2018, S.56).

5. Detaillierte Beschreibung ausgewählter technischer Maßnahmen zur Datensicherheit

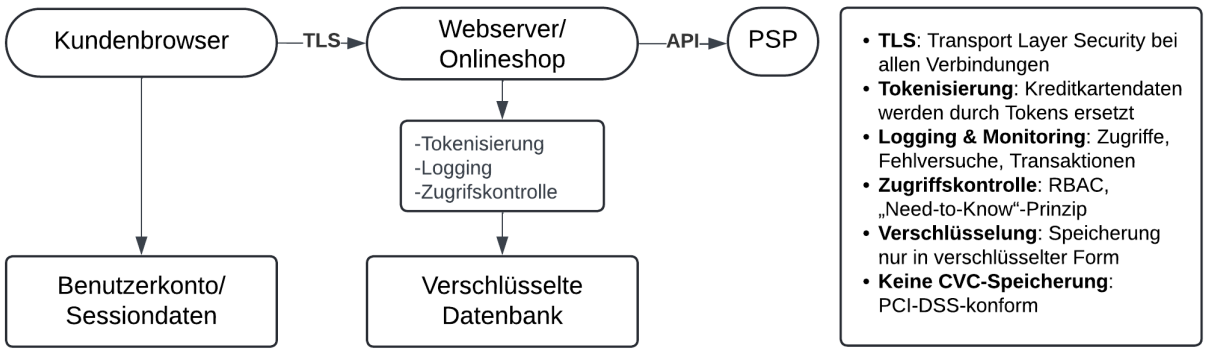
In einem Internet-Shop müssen sensible Zahlungsdaten sowohl im Ruhezustand als auch während der Übertragung verschlüsselt werden. Dazu gehört erstens die Verschlüsselung im Ruhezustand („Encryption at Rest“), also die sichere Speicherung von Datenbanken und Dateien auf Servern. Dabei sollten alle Kartendaten in der Datenbank nur in unlesbarer Form abgelegt werden. Typische Ansätze sind beispielsweise die symmetrische Verschlüsselung ganzer Datensätze oder die Verwendung kryptografischer Hashfunktionen für Teile der Daten. Nach PCI-DSS dürfen gespeicherte PANs (Kreditkartennummern) nicht im Klartext vorliegen, sondern müssen durch Einweg-Hash, Trunkierung oder Tokenisierung geschützt werden (PCI Security Standards Council, 2024, S. 90); (Müller, 2018, S.535). Auch Passwörter und andere Zugangsdaten müssen niemals im Klartext, sondern nur als Hashwert gespeichert werden. So schreibt etwa die IT-Sicherheitsliteratur vor: „Speicherung der Hashwerte von Passwörtern, nachdem sie mittels eines Sicherheitsalgorithmus gehasht worden sind“. Hierfür können Hardware-Sicherheitsmodule (HSM) eingesetzt werden, um Kryptoschlüssel vor unbefugtem Zugriff zu schützen.

Zweitens ist die Verschlüsselung bei der Übertragung essenziell („Encryption in Transit“). Kreditkartendaten, die zwischen Browser und Server ausgetauscht werden, müssen zwingend über SSL/TLS laufen. Dabei sollten ausschließlich aktuelle TLS-Versionen mit starken Algorithmen zum Einsatz kommen; veraltete Protokolle wie SSL oder frühe TLS-Versionen sind aufgrund bekannter Lücken zu deaktivieren. Hierzu empfiehlt PCI DSS, „strong cryptography and security protocols“ zu verwenden, damit PAN-Daten im offenen Netzwerk geschützt bleiben. Zusätzlich sind Webserver so zu härten, dass nur notwendige Dienste laufen. Unnötige Software, offene Ports oder unsichere Standardkonfigurationen sind zu entfernen und stets gepatcht. Sicherheitsrichtlinien fordern eine „angemessene Trennung von Aufgaben“ und die Umsetzung des Prinzips des geringsten Zugriffs. Damit werden Angriffe erschwert, wie es im OWASP-Top-10-Sicherheitskontext unter „Security Misconfiguration“ gefordert.

Ein weiterer Aspekt ist die Tokenisierung von Kartendaten. Anstatt die vollständige Kartennummer zu speichern, kann die PAN durch einen Token ersetzt werden, der außerhalb der PCI-Zone generiert wird. PCI DSS listet „Index Tokens“ als zulässige Methode, um gespeicherte PANs unlesbar zu machen (PCI Security Standards Council, 2024, S. 90). Durch Trunkierung, Hashing oder Tokenisierung lässt sich sicherstellen, dass ein gestohlenes Datenpaket allein nicht ausreicht, um die originale Kartennummer zu rekonstruieren. So hält der Standard fest: „Ist eine gekürzte und eine hash-basierte Version derselben PAN vorhanden, müssen zusätzliche Kontrollen verhindern, dass daraus die Original-PAN rekonstruiert werden kann (PCI Security Standards Council, 2024, S. 90). Damit lässt sich auch den PCI-Restriktionen genügen, etwa der Non-Retention von Card-Verification-Daten, die keinesfalls gespeichert werden dürfen (PCI Security Standards Council, 2024, S. 90).

Zusätzlich zu Verschlüsselung und Tokenisierung sind sichere Serverkonfigurationen unerlässlich. Webserver und Datenbanksysteme müssen so konfiguriert sein, dass sie für Angreifer möglichst wenig Angriffsfläche bieten. Das beinhaltet die Entfernung oder Deaktivierung überflüssiger Dienste, restriktive Firewall-Regeln sowie die konsequente Anwendung von sicheren HTTP-Headern. Experten betonen, dass unsichere Standardkonfigurationen, nicht benötigte offene Ports oder ausführliche Fehlermeldungen vermieden werden müssen, um „Security Misconfiguration“ zu verhindern. Ebenso sollten alle Kommunikationsendpunkte durch Zertifikate authentifiziert werden. So schreiben BaFin-Richtlinien, Transaktions-Websites müssten beispielsweise mit Extended-Validation-Zertifikaten versehen sein, um Phishing zu erschweren. Solche Zertifikate garantieren die Identität des Shops und verhindern Man-in-the-Middle-Angriffe.

Abbildung 2: Einfaches Architekturdiagramm der Sicherheitsmaßnahmen



Quelle 2: Eigene Darstellung

Schließlich gehören zum Härtungskonzept auch regelmäßige Sicherheitsprüfungen (Penetrationstests, Schwachstellenscans) und ein durchgehender Entwicklungsprozess nach Secure-Coding-Prinzipien. Sicherheitslücken wie SQL Injection oder Cross-Site-Scripting müssen bereits beim Programmierprozess adressiert werden (Müller, 2018, S.672). So wird empfohlen, schon während der Entwicklung Warnungen des Compilers und Code-Analyse-Tools zu eliminieren

sowie Sicherheits-Tests in die QS-Verfahren zu integrieren (Müller, 2018, S.672). In Summe lässt sich sagen, dass nur der konsequente Einsatz von starker Verschlüsselung (in Ruhe und bei der Übertragung), gut gehärteten Servern und modernen Schutztechniken (Tokenisierung, zertifikatbasierte Authentifizierung) einen akzeptablen Schutz der Kreditkartendaten gewährleisten kann (Müller, 2018, S.535).

6. Bewertung der technischen Handlungsoptionen (Self-Hosting vs. PSP)

Bei der Einführung der Kartenzahlung kann das Unternehmen wählen, ob es das Zahlungssystem selbst hostet oder einen externen Payment Service Provider (PSP) nutzt. Beim Self-Hosting würde der Online-Shop bzw. seine interne IT-Abteilung die Zahlungsabwicklung komplett übernehmen. Das schafft zwar maximale Flexibilität und Kontrolle (z. B. Auswahl eigener Verschlüsselungs- und Speicherlösungen), bringt jedoch hohen Aufwand mit sich. In diesem Szenario muss der Shop-Betreiber alle PCI-DSS-Anforderungen eigenständig erfüllen und nachweisen (PCI Security Standards Council, 2024). Dies umfasst teure Zertifizierungen, kontinuierliche Audits und ein umfassendes Sicherheitsprogramm. Zudem liegt die volle Haftung für Datenverlust oder Missbrauch der Karteninhaberinformationen beim Unternehmen selbst. Schon Herresthal weist darauf hin, dass in Akquisitionsverträgen häufig das Missbrauchsrisiko per Rückbelastungsklausel auf das verkaufende Unternehmen (das „Vertragsunternehmen“) übertragen wird (Herresthal, 2019, S.365). Konkret bedeutet dies, verlangt ein Karteninhaber sein Geld zurück, kann die Bank vom Händler die Rückzahlung fordern, wenn Manipulation oder Betrug vorliegt (Herresthal, 2019, S.365).

Dagegen bietet ein externer PSP (etwa Stripe, PayPal, Adyen usw.) den Vorteil, dass viele sicherheitstechnische Aufgaben delegiert werden. Kundenleiten ihre Daten direkt an den PSP weiter (Stichwort „Gegenanfrage“) oder nutzen offizielle Schnittstellen, wodurch der Online-Shop die Kartendaten kaum berührt. Der PSP übernimmt dann die PCI-Zertifizierung seiner Infrastruktur. Theoretisch könnte so die Compliance-Last sinken. Das Unternehmen wird nicht vollständig von seiner Verantwortung für Kartendaten entbunden. Gemäß PCI DSS muss das Unternehmen stets eine Liste aller involvierten Drittanbieter pflegen; und „die Nutzung eines PCI-DSS-konformen Drittanbieters macht ein Unternehmen nicht selbst konform“, es bleibt in der Pflicht (PCI Security Standards Council, 2024, S.16-17). Vielmehr kommt es auf die vertragliche Aufteilung der Verantwortlichkeiten an. PCI-Richtlinien fordern daher schriftliche Vereinbarungen, die festschreiben, welcher Teil der Datensicherheit vom Provider sichergestellt wird (PCI Security Standards Council, 2024, S.316).

Die Vor- und Nachteile beider Optionen lassen sich so zusammenfassen. Beim Self-Hosting behält das Unternehmen alle Daten vor und kann individuelle Schutzmaßnahmen umsetzen, zahlt aber deutlich höhere Einrichtungskosten und haftet im Schadensfall selbst. Es benötigt ggf. eine eigene Anbindung an Banken und Kreditkartenorganisationen (Acquirer-Verträge) sowie eigene Zertifikate und Netzwerke. Ein externer PSP entlastet dagegen den Shop-Betreiber organisatorisch. Er

übernimmt technisch die Verarbeitung und Lagerung der Kartendaten, kümmert sich um 3-D-Secure-Prozesse, Betrugsprävention und regulatorische Reports. Die Bindung an den PSP limitiert jedoch die Gestaltung (z. B. können eigene Anpassungen am Zahlungsflow schwerer umzusetzen sein) und verursacht zusätzlich Transaktionsgebühren. Hinzu kommt juristisch betrachtet eine geteilte Haftung. PSD2 beispielsweise legt nahe, dass im Zahlungsprozess der zahlerische Zahlungsdienstleister (also in der Regel die Bank oder das IT-System des Zahlers) für die korrekte Zahlungsausführung haftet (Richtlinie (EU) 2015/2366, 2015, Erwägungsgrund 86). In Verträgen wird jedoch oft klargestellt, dass auch der Händler bei Betrug in Regress genommen werden kann (Herresthal, 2019, S.365); (Richtlinie (EU) 2015/2366, 2015, Erwägungsgrund 86). Letztlich muss das Unternehmen also genau prüfen, welche Risiken es trägt. Ein global tätiger PSP wird hohe Sicherheitsstandards garantieren (DKB betont „hohe Sicherheitsanforderungen und strikte Regeln“ für alle Zahlungsdienstleister), doch die Händler sind durch Rückbelastungen (Chargebacks) weiterhin exponiert (Herresthal, 2019, S.365).

Tabelle 1: Vergleichstabelle Self-Hosting vs. Payment Service Provider

Kriterium	Self-Hosting	Payment Service Provider
Kontrolle	Volle Kontrolle über Infrastruktur, Datenverarbeitung und Customizing	Eingeschränkte Anpassungsmöglichkeiten, abhängig von PSP-APIs
Flexibilität	Eigene Sicherheitsarchitektur, individuelle Prozesse	Vorgaben durch PSP, z. B. bei Zahlungsablauf oder Sicherheitsprotokollen
Sicherheitsaufwand	Sehr hoch: PCI-DSS, Audits, Penetrationstests, Logging, Tokenisierung etc.	Viele Sicherheitsmaßnahmen übernimmt der PSP
Kosten (Setup)	Hoch (Hardware, Personal, Zertifizierungen, Implementierung)	Geringe Einstiegskosten, da Infrastruktur des PSP genutzt wird
Kosten (laufend)	Geringer bei großen Volumen (nach Implementierung)	Laufende Transaktionsgebühren, evtl. Gebühren pro API-Call
Rechtliche Haftung	Volle Haftung bei Datenpannen oder Rückbelastungen (Chargebacks)	Teilweise vertraglich übertragene Haftung (Händler kann trotzdem belangt werden)
Compliance-Aufwand	Eigenverantwortlich für PCI-DSS, DSGVO, BDSG	PSP ist zertifiziert, aber Händler bleibt in Mitverantwortung
Implementierungs-geschwindigkeit	Langsam: Planung, Test, Zertifizierung erforderlich	Schnell integrierbar mit PSP-Modulen oder Plugins

Zukunftsfähigkeit/ Updates	Eigene Verantwortung für Migration auf neue Standards (z. B. Post-Quantum)	PSP übernimmt in der Regel Updates & neue Standards automatisch

Quelle 3: Eigene Darstellung

7. Integration von Sicherheitsaspekten ins Projektmanagement (Security-by-Design)

Gemäß dem Security-by-Design-Prinzip sind Sicherheitsanforderungen bereits in den frühen Projektphasen fest zu verankern. Schon in der Planungs- und Anforderungsphase müssen die Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) definiert und Bedrohungen analysiert werden. IT-Sicherheitsexperten betonen, dass nur durch die „systematische und durchgängige Berücksichtigung von Risiko, Sicherheit, Kontinuität, Datenschutz und Compliance im Lebenszyklus" eines Systems eine durchgängige Sicherheit erreicht werden kann. In der Praxis bedeutet das etwa vor Beschaffung oder Entwicklung eines Zahlungssystems wird eine Risikoanalyse durchgeführt (z. B. PCI-Risiko-Assessment), und anhand eines Phasenmodells werden sukzessive Sicherheitsmaßnahmen geplant. In späteren Phasen (Design, Entwicklung, Test) werden diese Anforderungen dann schrittweise umgesetzt und überprüft. Hierzu zählt auch der Einsatz von Secure-Coding-Standards und Code-Reviews, wie sie in Kapitel 5 beschrieben sind.

Die Security-Governance begleitet alle Projektphasen. Sie stellt sicher, dass Verantwortlichkeiten und Prozesse definiert sind. Beispielsweise sollte es einen Security Officer oder -Beauftragten geben, der Policies zu Kartendatenverarbeitung festlegt. Empfohlen wird darüber hinaus ein gestaffeltes Sicherheitskonzept mit Aufgabentrennung und dem Least-Privilege-Prinzip. Dies bedeutet, dass niemand in einem Team mehr Rechte hat als für seine Aufgabe nötig (z. B. getrennte Rollen für Entwicklung, Betrieb und Prüfung). Alle Projekt-Ergebnisse unterliegen zudem einem Konfigurations- und Änderungsmanagement (Change Management), sodass nachträgliche Änderungen nachvollziehbar sind.

Zur Absicherung und Kontrolle gehört die regelmäßige Durchführung von Audits und Tests. Bereits während der Implementierung sollten automatisierte Tests (z. B. Penetrationstests, statische Code-Analysen) eingeführt werden. Später werden Akzeptanz- und Sicherheitstests durchgeführt, um die Einhaltung der Vorgaben zu verifizieren (DKB, März, 2022). PCI DSS fordert etwa, dass externe Schwachstellenscans und Prüfungen (z. B. von Code- und Netzwerkänderungen) in den Entwicklungs- und Betriebsprozess integriert werden (DKB, März, 2022). Das Betreiben von Logging- und Monitoring-Systemen ermöglicht es, sicherheitsrelevante Ereignisse zeitnah zu erkennen und zu reagieren. Insbesondere nach Produktivsetzung sollten regelmäßige Sicherheitsaudits und Reviews zum Standard gehören, um Aktualität von Software und Einhaltung der Compliance sicherzustellen. All diese Maßnahmen, von der initialen Risikoanalyse, bis hin zu fortlaufenden Audits zeigen, dass Sicherheit auf allen Ebenen des Projektmanagements zu verankern ist. Nur so kann das Projekt „lebenszyklusimmanent" resilient gegen Angriffe sein.

8. Ausblick auf zukünftige Sicherheitsanforderungen

In den kommenden Jahren werden neue Technologien und Bedrohungen die Sicherheitsanforderungen weiter verändern. Ein zentrales Thema ist die Post-Quantum-Kryptografie. Quantencomputer könnten klassische Verschlüsselungsverfahren zukünftig brechen. Daher arbeiten Kryptographen an quantensicheren Algorithmen (sogenannte Post-Quantum- oder „Quantum Safe“-Kryptografie), die auch gegenüber Quantenangriffen widerstandsfähig sind (Hagemeier, 2019, S. 634). Staatliche Förderprogramme (z. B. in Deutschland) unterstreichen die Bedeutung dieser Entwicklung. Während klassische Schlüsselverteilungen noch stark auf RSA oder ECC setzen, wird es nötig sein, zukunftsfähige Verfahren einzuführen, beispielsweise gitterbasierte oder codebasierte Verfahren, die derzeit als Kandidaten für quantensichere Systeme gelten (Hagemeier, 2019, S. 634). Parallel dazu gewinnt die Quantenkryptografie selbst (z. B. Quanten-Schlüsselverteilung) an Interesse, um vertrauliche Kanäle physikalisch abzusichern (Hagemeier, 2019, S. 634). Für den Online-Handel bedeutet dies, dass künftige Zahlungssysteme sowohl klassisch- als auch quanten-resistente Algorithmen implementieren und bei Bedarf aktualisieren müssen.

Auch neue Authentifizierungsverfahren spielen eine zunehmend größere Rolle. Die Standard-3D-Secure-Verfahren entwickeln sich beispielsweise zu Zwei-Faktor- oder Mehr-Faktor-Methoden weiter. So wird mittlerweile in vielen Fällen nicht nur eine SMS-PIN gesendet, sondern etwa eine TAN-App mit biometrischer Freigabe (Fingerabdruck, Gesichtserkennung) verwendet (DKB, März, 2022). App-basierte Zahlungssysteme (Apple Pay, Google Pay etc.) nutzen schon heute biometrische Merkmale zur Bestätigung von Transaktionen (DKB, März, 2022). Biometrische Authentisierungstechniken werden allgemein vielfältiger. Fingerabdruck, Iris- oder Gesichtsscanner an Endgeräten sind bereits verbreitet, und WebAuthn/FIDO2 ermöglichen hardwarebasierte (z. B. USB- oder NFC-Token) sowie biometrische Logins. Generell erweitern sich die Faktoren von der klassischen Kombination Besitz (Karte) und Wissen (PIN) über Biometrie bis zu Verhaltensbiometrie. Bereits jetzt empfiehlt die IT-Sicherheitsliteratur beispielsweise USB-Token mit integriertem Fingerabdrucksensor als Zwei-Faktor-Lösung (Müller, 2018, S.535). Auch die Analyse von Nutzerverhalten (Klick-Pattern, Tipp-Geschwindigkeit) wird künftig zur laufenden Authentifizierung beitragen (Müller, 2018, S.531). Zudem werden Technologien wie Client-Zertifikate und hardwaregestützte Sicherheit (z. B. TPM, Secure Enclave) wichtiger, um die Serverauthentizität zu garantieren und Manipulation zu verhindern.

Schließlich ist zu erwarten, dass auch organisatorische Anforderungen steigen, regulatorische Vorgaben werden schärfer, Datenschutzvorschriften (z. B. DSGVO) fordern Verschlüsselung oder Löschfristen. Für den Zahlungsverkehr könnten neue Branchenstandards entstehen (nachträgliche Chip-on-Phone-Verfahren, Tokenisierung per Blockchain, biometrische Smartcards, etc.). Bereits heute müssen Entwickler sich auf Plattformen wie EMV 3D-Secure 2.x und PSD2-konforme

Authentisierung einstellen. Insgesamt gilt, die Systeme müssen so flexibel aufgebaut sein, dass sie mit zukünftigen Kryptographie- und Authentifizierungsstandards mithalten können.

9. Schlussfolgerung und Bewertung der Umsetzung im Hinblick auf Unternehmensziele, Nutzen, Risiken, Einschränkungen

Die Einführung der Kreditkartenzahlung in dem betrachteten Online-Shop bringt sowohl einen klaren geschäftlichen Nutzen als auch erhebliche Aufwände mit sich. Zum einen ermöglicht sie, neue Kundensegmente zu erschließen und den Umsatz zu steigern, ein wichtiges Unternehmensziel im E-Commerce. Kunden erwarten die Bequemlichkeit, mit gängigen Zahlungsmitteln wie Kreditkarten oder Mobile-Payments bezahlen zu können, was letztlich die Zufriedenheit erhöht und Kaufabbrüche senkt. Um dieses Potenzial zu realisieren, wurde ein umfassendes Sicherheitskonzept umgesetzt. Sichere Speicherung und Übertragung von Zahlungsdaten, Tokenisierung, gehärtete Server sowie ein durchgängiges Sicherheitsmanagement (Audit, Governance, Schulung) (Müller, 2018, S.535). Dadurch erfüllt das Projekt die Branchenanforderungen (etwa PCI DSS) und schafft eine vertrauenswürdige Infrastruktur. Wie die DKB zusammenfassend festhält, gelten für alle an einer Kartenzahlung beteiligten Institutionen „umfangreiche Anforderungen zum Schutz von Kartendaten, Verschlüsselung bei der Übermittlung, Restriktionen beim Zugriff […] sowie regelmäßige Tests, um die Sicherheit der Systeme zu prüfen“ (DKB, März, 2022).

Dennoch bleiben Restrisiken. Technisch konnte durch die Maßnahmen ein hohes Sicherheitsniveau erreicht werden, doch absolute Sicherheit gibt es nicht, neue Angriffsszenarien oder Zero-Day-Schwachstellen können auch künftig auftreten. Haftungsseitig wurde versucht, Risiken durch Verträge mit der Bank bzw. dem PSP zu begrenzen, doch wie analysiert ist es üblich, dass die Bank das Missbrauchsrisiko bei Kreditkartenbuchungen mittels Rückbelastungsklauseln auf den Händler verschiebt (Herresthal, 2019, S.365). Das bedeutet im Fall eines tatsächlichen Betrugsblatts bleibt der Online-Shop im Zweifelsfall für den Schaden verantwortlich. Hieraus ergibt sich eine betriebswirtschaftliche Beschränkung der Umsetzung. Trotz aller Sicherheitsmaßnahmen ist die Haftung aufgrund gesetzlicher und vertraglicher Rahmenbedingungen beschränkt kontrollierbar.

Zusammenfassend kann festgehalten werden, dass die Umsetzung der Kreditkartenzahlung gut mit den Unternehmenszielen in Einklang steht. Sie erweitert das Produktangebot und stärkt die Marktposition des Unternehmens. Der erzielte Nutzen (Marktzugang, Kundenvertrauen, Wettbewerbsfähigkeit) ist hoch. Gleichzeitig erfordert der Betrieb jedoch kontinuierliche Investitionen in Sicherheit und Compliance. Die getroffene technische Lösung stößt an Limitationen. Neben den genannten Haftungsrisiken unterliegt sie dem Wandel der Technik (stetige Updates, mögliche Migration auf Post-Quantum-Verfahren) und dem Kostendruck (PCI-Audits, Transaktionsgebühren). Insgesamt wurde das Projektziel erreicht, indem eine durchdachte Sicherheitsarchitektur implementiert wurde, doch die langfristige Effektivität hängt davon ab, ob das Unternehmen die

notwendigen Ressourcen aufbringt, um mit den künftigen Anforderungen Schritt zu halten (Herresthal, 2019, S.365).

III. Literaturverzeichnis

- Deutsche Kreditbank AG. (o. D.). *Rasanter Datenfluss: Das passiert bei einer Kartenzahlung*. März 2022, https://www.dkb.de/finanzwissen/rasanter-datenfluss-das-passiert-bei-einer-kartenzahlung

- Europäische Union. (2015). *Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG*. Amtsblatt der Europäischen Union, L 337, 35–127. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32015L2366

- Europäische Union. (2016). *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)*. Amtsblatt der Europäischen Union, L 119, 1–88. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679

- Hagemeier, H. (2019). Kryptografie – heute und zukünftig: Grundbaustein für IT-Sicherheit. *Datenschutz Und Datensicherheit - DuD*, *43*(10), 631–635. https://doi.org/10.1007/s11623-019-1178-3

- Herresthal, C. (2019). Die Neustimmung der Kreditkartenzahlung und die Reichweite der Haftung des Acquirers beim Kreditkartenmissbrauch. *Zeitschrift Für Bankrecht Und Bankwirtschaft*, *31*, 353–368. https://doi.org/10.15375/zbb-2019-0603

- Müller, K.-R. (2018). IT-Sicherheit mit System *Definitionen zum Sicherheits-, Kontinuitäts- und Risikomanagement*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-22065-5_6

- PCI Security Standards Council. (2024). *Payment Card Industry Data Security Standard: Requirements and Testing Procedures (Version 4.0.1)*. https://www.pcisecuritystandards.org/

IV. Abbildungs-/ Tabellenverzeichnis