

CHANCEN FÜR EIN EUROPÄISCHES PAYMENT-SYSTEM

PSD2 als Türöffner

Durch die Digitalisierung des Einkaufens werden Payment-Systeme in Zukunft eine immer wichtigere Rolle im Alltag spielen. Heute sind kartengestützte Verfahren im stationären sowie verschiedenste Online-Bezahlmethoden im elektronischen Handel weit verbreitet. Zu den bekannten Verfahren gesellen sich immer neue Bezahlmethoden hinzu. Technologien wie der Nahfunkstandard NFC, die zweidimensionalen QR-Codes oder standardisierte Schnittstellen wie FinTS ermöglichen die technische Umsetzung. Ergibt sich daraus die Chance zu einem echten europäischen Payment-System?



In der ersten Zahlungsdiensterichtlinie sind Payment-Systeme, die nur die technische Möglichkeit zur Durchführung von Zahlungen bieten, nicht berücksichtigt worden. Daher unterliegen viele dieser Dienste momentan keiner Beaufsichtigung. Dies wird sich zum nächsten Januar mit der neuen Zahlungsdiensterichtlinie ändern. PSD2 steht in den Startlöchern und wird maßgeblich für Payment-Systeme innerhalb des europäischen Binnenmarkts sein.

Neben der Stärkung sicherheitstechnischer Anforderungen, wie einer starken Kundenauthentifizierung, möchte die EU den Wettbewerb zwischen den verschiedenen Payment-Systemen steigern und dadurch innovative Dienste fördern. Für FinTechs bietet die neue Richtlinie großartige Chancen, denn für alle Drittanbieter von Zahlungsdiensten müssen Banken innerhalb der EU künftig eine entgeltfreie Schnittstelle bereitstellen, über die z. B. Zahlungen ausgelöst oder Kontoinformation abgerufen werden können.

Auch die eIDAS-Verordnung, welche die neue Gesetzesgrundlage für Vertrauensdienste festlegt, wird in diesem Ökosystem in Europa und darüber hinaus eine wichtige Rolle einnehmen, wenn wir die Möglichkeit und die schnelle Veränderung durch den Digitalisierungsprozess intelligent nutzen.

Instant Payments können ein weiterer Treiber und die Chance zu einem europäischen Payment-System werden. Durch die

sofortige Zahlung wird Geld innerhalb von Sekunden transferiert und steht dem Zahlungsempfänger zur weiteren Nutzung zur Verfügung. All diese Neuerungen benötigen innovative IT-Sicherheitstechnologien, die neben starken Sicherheitsmechanismen einen hohen Komfort für die Benutzer bereitstellen müssen.

Bei der Einführung eines innovativen Payment-Systems ist vor allem eines zu beachten: Der neue Bezahlendienst braucht messbare Vorteile gegenüber anderen bereits etablierten Verfahren. Kosten, Geschwindigkeit, Sicherheit und Benutzerfreundlichkeit müssen deutlich verbessert werden, um Akzeptanz auf Kunden- sowie Händlerseite zu generieren. Aus gesellschaftlicher Sicht wäre ein Bezahlendienst aus Deutschland oder Europa zu begrüßen. Benutzerfreundlichkeit und Sicherheit stehen im direkten Konflikt zueinander. Vor allem Kunden wollen sich nicht beim Online Checkout oder Bezahlen an der Kasse mit langen und komplizierten Authentifizierungsvorgängen herumschlagen.

Das Institut für Internet-Sicherheit – if(is) – hat mehrere interessante Forschungsprojekte durchgeführt, die sich mit einem neuen Bezahlendienst für moderne und zukunftsorientierte Anwendungen beschäftigten. Heraus kam die innovative XignQR-Technologie, eine schnelle, benutzerfreundliche und sichere Authentifizierungs- und Signaturanwendung. Sie ermöglicht das Ausfüh-

ren von Transaktionen in Sekundenschnelle. Durch die bald geltenden EU-Verordnungen ist jetzt der beste Zeitpunkt, einen neuen Bezahlendienst einzuführen.

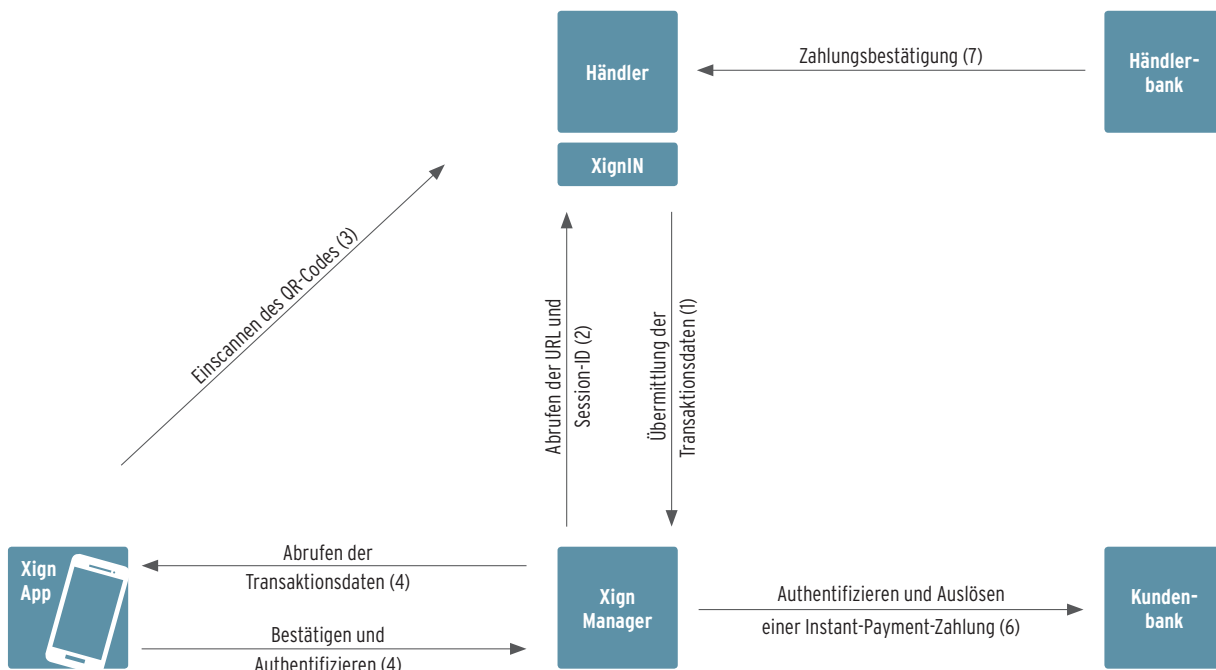
PSD2 als Herausforderung für den Finanzsektor

Die Payment Service Directive 2 (PSD2) ist vom Europaparlament beschlossen und verabschiedet worden und muss bis zum 13. Januar 2018 in nationales Recht umgesetzt werden. In Deutschland ist die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) dafür verantwortlich.

Durch die PSD2 muss auch das Zahlungsdiensteaufsichtsgesetz (ZAG) angepasst werden. Inwieweit weitere Gesetze (z. B. KWG oder BGB) überarbeitet werden müssen, entscheidet die Aufsichtsbehörde. Die neue Zahlungsdiensterichtlinie verfolgt primär zwei Ziele: Schaffung von Transparenz und Sicherheit sowie Innovationsförderung und mehr Wettbewerb. Darüber hinaus soll die bestehende Rechtsunsicherheit der ersten Richtlinie beseitigt werden.

Mit dem Inkrafttreten der PSD2 werden sogenannte dritte Zahlungsdienste¹ in Zahlungsauslöse- sowie Kontoinformationsdienste unterschieden. Zahlungsauslösedienste benötigen in Zukunft eine Genehmigung von der jeweiligen Aufsichtsbehörde. Kontoinformationsdienste erlauben die Konsolidierung von Kontoinformationen bei ei-

1 | Lösungsansatz: XignPay Instant Payment über Drittanbieterschnittstelle



nem oder mehreren Zahlungsdienstleistern und sind bei der entsprechenden Bundesbehörde lediglich registrierungspflichtig. Eine wichtige Neuerung im Rahmen der PSD2 ist der Kontenzugang für Dritte. Für Kontoinformations- sowie Zahlungsauslösedienste müssen Banken entgeltfreie Schnittstellen zur Verfügung stellen. Diese können von Dritten genutzt werden, um eigenen kostenpflichtige Dienste voranzutreiben. Aktuell lassen sich auf der Internetseite der Deutschen Kreditwirtschaft Anforderungen an diese Schnittstelle nachlesen, die eine Ähnlichkeit mit der etablierten FinTS-Schnittstelle vermuten lassen.

Die Europäische Bankenaufsicht definiert im Rahmen der PSD2 die Regulatory Technical Standards (RTS). Im Wesentlichen geht es dabei um drei Bereiche: eine starke Kundenauthentifizierung, Sicherheitsmechanismen der standardisierten Drittanbieterschnittstelle und Ausnahmen von der starken Kundenauthentifizierung.

Die starke Kundenauthentifizierung steht als Synonym für eine Zwei-Faktor-Authentifizierung. Dazu müssen zwei unabhängige Elemente aus den drei Kategorien Wissen (Passwort, PIN), Besitz (Smartphone, Smart-

card, Token) und Biometrie (Fingerabdruck, Iris-Scan, Stimmenerkennung) eingesetzt werden. Zur Implementierung der RTS sind derzeit 18 Monate vorgesehen.

Instant Payments und eIDAS bieten neue Chancen

Instant Payments (SEPA Instant Credit Transfer, SCT Inst) basieren auf den bereits bekannten SEPA-Überweisungen. Bis zu 15.000 € sollen innerhalb von zehn Sekunden auf dem Empfängerkonto zur Verfügung stehen, und zwar rund um die Uhr und grenzübergreifend in allen 34 SEPA-Ländern.

Die Kombination von Instant Payments und der in der PSD2 definierten Kontoschnittstelle für dritte Zahlungsdienstleister lässt interessante Anwendungsfälle sowohl für den stationären als auch den Online-Handel zu. Doch inwieweit Kunden und Handel wirklich von dem neuen Dienst profitieren werden, ist abzuwarten. Instant Payments sind eher eine Evolution als eine Revolution in der Payment-Welt.

Mit der neuen eIDAS-Verordnung besteht eine gesetzliche Grundlage in der EU, qualifizierte Fernsignaturen zu erstellen. Sie wurden

im alten deutschen Signaturgesetz und der deutschen Signaturverordnung nicht berücksichtigt. Durch diese Neuerung können künftig Transaktionen, ohne das umständliche Hantieren mit Signaturkarten und Lesegeräten, freigegeben werden. Ein Dienstanbieter kann seinen Nutzern eine mobile Signaturanwendung, z. B. mithilfe von Smartphones anbieten, die bequem und sicher überall zur Verfügung steht, um Banktransaktionen auszuführen.

Status quo: Verbreitung von Payment-Systemen

Im stationären Handel sind neben Bargeld vor allem kartengestützte Zahlungssysteme stark verbreitet und werden durch den Einsatz neuer Technologien noch benutzerfreundlicher.² Das kontaktlose Zahlen via NFC wird besonders von Banken und Kreditkartenunternehmen vorangetrieben und wird sich als Standard im stationären Handel durchsetzen.

Bis zum Jahr 2020 müssen alle Händler, die in Europa VISA-Zahlungen akzeptieren wollen, ihre Kassenterminals auf die neue Technologie aufrüsten. Die Technologiegig-

ganten Samsung und Apple nutzen die Chance, um Smartphones mit der notwendigen Technologie auszustatten und so eigene Bezahldienste zu etablieren. Auch Online-Händler bieten eine Vielzahl von Bezahlverfahren an, damit der Kunde seine favorisierte Methode nutzen kann. Dabei ist die beim Kunden beliebte Rechnung für Händler das teuerste Verfahren,³ die Sofort-Überweisung das günstigste.

XignQR: Eine passende Lösung

XignQR ist eine PKI-basierte innovative Authentifizierungs- sowie Signaturanwendung aus Deutschland. Am (if)is wurde dazu das Start-up XignSys gegründet. Es bietet ein starkes und innovatives Multi-Authentifizierungstool an, das die Identitätsprüfungen in nur einem Vorgang bündelt.

Darüber hinaus können mit der Applikation serverseitige Signaturen nach dem eIDAS-Abkommen durchgeführt werden. XignQR stellt die technische Infrastruktur zur Verfügung und erlaubt einen Authentifizierungsprozess von der Zwei-Faktor-Authentifizierung bis hin zur Multi-Faktor-Authentifizierung.

Das System besteht aus insgesamt drei Komponenten, wobei ein Hardware Security Token optional hinzugefügt werden kann. Die weiteren Elemente sind die Smartphone-Applikation, über die sich der Nutzer registriert und anmeldet, der Xign-Manager als zentrale Komponente und Vertrauensanker sowie die Einbindungskomponente XignIN auf der Seite des Händlers.

XignQR kann als eigenständiges Payment-System XignPay oder als Technologielieferant für Payment Service Provider dienen. Zur Nutzung des Dienstes XignPay müssen neben der erforderlichen Genehmigung von der BaFin weitere technische Schnittstellen geschaffen werden, um Zahlungen durchzuführen. Beispielsweise kann

nach Zustimmung der Deutschen Kreditwirtschaft der Zugriff auf das electronic-cash-System über ein virtuelles Terminal erfolgen. Dabei wird, wie beim Bezahlen mit der Girocard, eine Autorisierungsprüfung auf dem Kundenkonto durchgeführt.

Eine weitere Alternative kann die künftige Drittanbieterschnittstelle im Rahmen der PSD2 sein, über die Zahlungen direkt vom Kundenkonto ausgelöst werden können. Gekoppelt mit Instant Payments kann so ein revolutionäres Payment-System im europäischen Wirtschaftsraum entstehen. Die Abbildung zeigt den Lösungsansatz für den Online-Bereich, um Instant Payments über die Drittanbieterschnittstelle mit dem Payment-System XignPay auszulösen. ► 1

Für die Nutzung des Dienstes muss sich der Benutzer zuerst registrieren oder auf die registrierten Kunden der Banken zugreifen. Zum Durchführen einer Zahlung werden die Transaktionsdaten durch die XignIN Einbindungskomponente auf der Händlerseite zum Xign-Manager übermittelt (Schritt 1). Dann sendet der Xign-Manager eine URL sowie Session-ID zurück an den Händler (Schritt 2), der diese Daten beispielsweise als QR-Code dem Kunden präsentiert. Anschließend scannt der Benutzer den QR-Code ein (Schritt 3).

Diese Informationen dienen der App als Einstiegspunkt, um die Transaktionsdaten vom Xign-Manager abzurufen und auf dem Smartphone des Nutzers anzuzeigen. Der Benutzer überprüft die Transaktionsdaten und bestätigt die Zahlung (Schritt 5). Der Xign-Manager authentifiziert sich gegenüber der Kundenbank und löst eine Instant-Payment-Zahlung an den Händler aus (Schritt 6). Innerhalb von zehn Sekunden wird das Geld gutgeschrieben und steht auf dem Händlerkonto zur Verfügung. Zum Schluss erhält der Händler von seiner Bank die Bestätigung des Zahlungseingangs (Schritt 7).

FAZIT

Durch die Bausteine PSD2, Instant Payments und eIDAS sind die Chancen, ein einzigartiges und europaweites Payment-System aufzubauen, ideal. Insbesondere Drittdienstleister werden durch die vorgeschriebene Kontozugang-Schnittstelle für Dritte profitieren. Dadurch können Zahlungen bei einem kontoführenden Institut ausgelöst und Kontoinformationen, wie die Verfügbarkeit eines Geldbetrags, geprüft werden. Die Verfügbarkeit eines Geldbetrags ist jedoch nicht mit einer Zahlungsgarantie gleichzusetzen. Zur Identifizierung beim Zugriff auf ein Zahlungskonto sollen qualifizierte Zertifikate auf Basis der eIDAS Verordnung genutzt werden, diese können beispielsweise von einem qualifizierten Vertrauensdiensteanbieter ausgegeben werden. Die Chancen, aus Deutschland heraus ein neues, zukunftsorientiertes Bezahlssystem einzuführen, sind enorm. Es braucht nur mutige und weitsichtige Akteure, die diesen wichtigen Markt nicht anderen Playern überlassen möchten.

Autoren: Prof. Norbert Pohlmann ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit - if(is) an der Westfälischen Hochschule in Gelsenkirchen. Stephan Reinert war im Rahmen seiner Masterarbeit ebenda als wissenschaftliche Hilfskraft beschäftigt.

- 1 Dritte Zahlungsdienste sind alle Dienste, die das Auslösen von „Zahlungsaufträgen auf ein bei einem anderen Zahlungsdienstleister geführtes Zahlungskonto“ ermöglichen (beispielsweise Giropay oder Sofort-Überweisung). Bislang war zur Ausübung eines solchen Dienstes keine Genehmigung seitens der BaFin oder anderer Aufsichtsbehörden notwendig.
- 2 www.ehi.org/de/pressemitteilungen/kartenzahlung-waechst-bar-geld-bleibt.
- 3 Vgl. ibi research, Studie „Gesamtkosten von Zahlungsverfahren im E-Commerce August 2016: Ergebnisse zu den Kosten von Kreditkarten nach der MIF-Verordnung“.