Sparkasse

FAQ für Journalisten zu Apple Pay.

Version 1.0; Stand 12.2019

Nur zur internen Verwendung

Sparkasse

Inhalt

Sparkasse

1 Voraussetzungen

1.1 Welche Voraussetzungen müssen Kunden erfüllen, um Apple Pay mit der Sparkasse nutzen zu können?

Um Apple Pay nutzen zu können, muss der Kunde zunächst einige allgemeine Apple-Voraussetzungen erfüllen. Er benötigt:

- ein kompatibles Gerät,
- eine aktuelle Version von iOS, watchOS oder macOS,
- eine bei iCloud angemeldete Apple-ID mit Mindestalter 13 Jahre,
- eine auf dem iOS-Gerät aktivierte Face ID, Touch ID oder einen Gerätecode.

Darüber hinaus gelten spezifische Voraussetzungen für Apple Pay mit der Sparkasse. Kunden, die Apple Pay mit der Sparkasse für Zahlungen nutzen möchten, müssen:

- ein Privatkunde sein
- einen Online-Banking-Vertrag besitzen mit Nutzung des elektronischen Postfachs (ePostfachs) und des pushTAN- oder chipTAN-(inkl. chipTAN-QR-)Verfahrens
- eine Sparkassen-Kreditkarte (Mastercard/Visa) oder Sparkassen-Karte Basis (Mastercard/Visa) besitzen
- eine Sparkassen-Card (girocard) oder Sparkassen-Card Plus (girocard) besitzen
- der Kontoinhaber oder Mitkontoinhaber sein und eine Sparkassen-Kreditkarte oder Partnerkarte besitzen
- die Sparkassen-App (im folgenden S-App) auf dem Smartphone installiert haben

2 Kartendigitalisierung

2.1 Welche Sparkassen-Karten können die Kunden digitalisieren?

Folgende Sparkassen-Karten können für Apple Pay digitalisiert werden:

- Mastercard- und Visa-Kreditkarten:
  - Platinum
  - Gold
  - Standard/Classic
  - Basis
  - X-Tension/Vision
- Sparkassen-Cards und Sparkassen-Cards Plus (ab 2020)

Die zu digitalisierende Karte darf nicht gesperrt, gelöscht oder verfallen sein. Um eine Karte zu digitalisieren und kontaktlos per Smartphone einsetzen zu können, ist es nicht erforderlich, dass die zugrundeliegende physische Karte ebenfalls bereits kontaktlosfähig ist.

2.2 Wie wird/werden die Karte/n digitalisiert?

Für den Abruf einer digitalen Karte in der S-App muss der Nutzer am Online-Banking des Instituts teilnehmen und einen Online-Banking-Vertrag mit PIN/TAN abgeschlossen haben. Der Online-Banking-Teilnehmer muss identisch mit dem Karteninhaber sein, um digitale Karten abrufen zu können. Zusätzlich muss der Karteninhaber auch der Kontoinhaber oder Mitkontoinhaber des Kontos sein, für das er digital Karten bestellen möchte.

Den Prozess zur Erstellung einer digitalen Karte für Apple Pay kann der Sparkassen-Kunde über die S-App und bei der Kreditkarte/Basiskarte auch über die Apple Wallet anstoßen. In beiden Fällen ist die Authentifizierung des Sparkassen-Kunden ausschließlich über die S-App möglich.

Der Sparkassen-Kunde kann die TAN-Verfahren chipTAN/chipTAN-QR und pushTAN nutzen. Damit wird die Erstellung einer digitalen Karte mit einer 2-Faktor-Authentifizierung bestätigt. Diese erfüllt höchste Sicherheitsansprüche sowie die regulatorischen Vorgaben aus der zweiten Zahlungsdiensterichtlinie (PSD2).

Mit dem Hinzufügen einer Karte für Apple Pay wird ein digitales Abbild der zugehörigen physischen Karte erzeugt. Die Nutzungsgrenzen, Verfügungsrahmen und hinterlegten Sperren der physischen Karte gelten auch für die digitale Karte.

3 Datenschutz und Sicherheit

3.1 Wie sieht es mit dem Datenschutz bei Apple Pay aus?

Um den Kunden bestmöglichen Schutz zu bieten, gelten für Apple Pay hohe Datenschutz- und Sicherheitsstandards.

Der Datenschutz bei Apple Pay ist im Vergleich zu Wettbewerbslösungen schon im technischen Design der Plattform berücksichtigt. Die Hauptfunktionen von Apple Pay werden nur dezentral auf den mobilen Endgeräten in Form der Apple Wallet und der digitalen Karten in einem gesonderten Hardware-Sicherheitsmodul (Secure Element) abgebildet. Zentrale Systeme von Apple dienen lediglich der Kommunikation zwischen den Hintergrundsystemen der Kartenherausgeber und der Wallet des Kunden.

Im Rahmen des Transaktionsprozesses bekommt Apple zudem keine Kenntnis der Transaktionsdaten des Kunden. Zwar kann der Kunde sich eine Transaktionsbenachrichtigung an seine Apple Wallet senden und sich die letzten zehn Transaktionen mit der digitalen Karte des Geräts in der Wallet anzeigen lassen. Diese Informationen werden aber vom Kartenherausgeber verschlüsselt direkt an die Wallet auf dem Endgerät des Kunden geliefert.

3.2 Welche Sicherheitsstandards gelten für das Bezahlen mit Apple Pay?

Bei Apple Pay wird zur Authentifizierung jeder Kartenzahlung ab dem ersten Cent die Consumer Device Cardholder Verification Method – kurz CDCVM – genutzt. Die Kunden kennen und nutzen diesen Prozess bereits – etwa bei der Entsperrung des Smartphones, indem sie ihren Finger einscannen, den Gerätecode eingeben oder in die Kamera schauen.

Diese Funktion nutzen die Kunden in Zukunft auch, wenn sie mit ihrer digitalen Karte bezahlen, denn sie authentifizieren jede Zahlung per Touch ID, Face ID oder Eingabe des Gerätecodes. Die klassische Authentifizierungsmethode der Eingabe der Zahlungsverkehrs-PIN am PoS-Terminal entfällt.

Apple setzt bei Apple Pay, wie auch die Sparkassen-Finanzgruppe bei der App „Mobiles Bezahlen“, auf den weltweit führenden Technologiestandard NFC.NFC ist die Abkürzung für „Near Field Communication“ (Nahfeld-Kommunikation).

Für den Datenaustausch via NFC müssen iPhone oder Apple Watch und PoS-Terminal mit einem NFC-Modul (Antenne) und einer entsprechenden Software ausgestattet sein. Die übertragenen Daten zwischen iPhone bzw. Apple Watch und dem PoS-Terminal sind über die Kontaktlos-Schnittstelle auf das notwendige Minimum hinsichtlich Abwicklung und Absicherung der Bezahltransaktion reduziert. Eine Übermittlung von Käuferprofilen an Apple findet nicht statt.