DIE WICHTIGSTEN ARTIKEL DER AKTUELLEN RTS

Zur Identifizierung von unautorisierten oder betrügerischen Zahlungsvorgängen müssen Payment Service Provider ein Transaction Monitoring System aufbauen.

Artikel 2: General Authentication Requirements

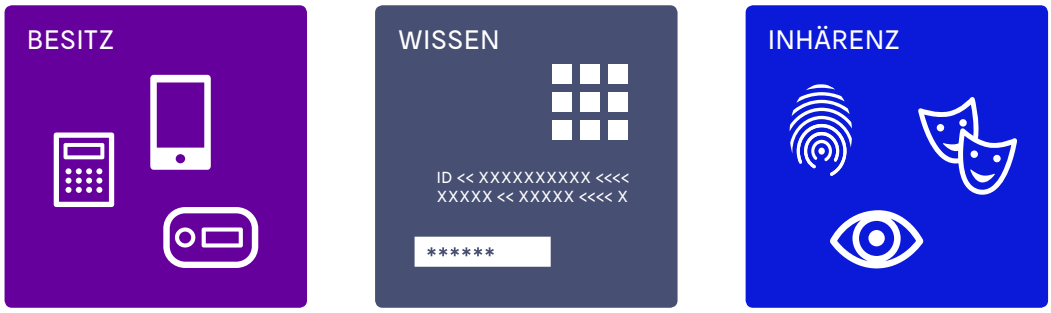
Zur Identifizierung von unautorisierten oder betrügerischen Zahlungsvorgängen müssen Payment Service Provider (PSP) – sowohl Banken als auch Drittanbieter – ein Transaction Monitoring System aufbauen, das alle Transaktionen in Echtzeit prüft und bewertet. Dazu werden die jeweiligen Zahlungsdetails (Höhe des Geldbetrags, Empfänger, etc.), bekannte Betrugsszenarien und die kundentypischen Gewohnheiten herangezogen. Außerdem sind die verwendeten Geräte und die Software auf Manipulation bzw. Infizierung durch Viren zu prüfen.

Artikel 4: Authentication Code

Im Zuge der Strong Customer Authentication ist ein zusätzlicher Authentication Code zu erzeugen, der nur einmalig für den Zugriff zum Online-Banking-Portal oder zur Auslösung einer Zahlung oder einer potenziell „gefährlichen“ Aktion genutzt werden darf. Bei der Erzeugung des Codes muss sichergestellt sein, dass er nicht kompromittiert werden kann und im Falle eines unerlaubten Zugriffs keinerlei Rückschlüsse über die verwendeten Verfahren zur Strong Customer Authentication gezogen werden können.

Eine Strong Customer Authentication ist vergleichbar mit der heute bekannten Zwei-Faktor-Authentifizierung. Jedoch werden in der RTS keinerlei Vorgaben gemacht, wie die Zwei-Faktor-Authentifizierung genau durchgeführt und welche Technologien verwendet werden sollen. Bedingung ist nur, dass zwei der folgenden drei Elemente genutzt werden sollen.

- Besitz (z.B. ChipTAN, Token, Smartphone)
- Wissen (z.B. Passwort, PIN, ID-Nummer)
- Inhärenz (z.B. Iris-Scan, Fingerabdruck, Gesichtserkennung)



Dabei muss der Payment Service Provider sicherstellen, dass die jeweiligen Elemente gegen einen unerlaubten Zugriff geschützt sind. Im Falle eines Passwortes wäre der Schutz etwa eine sichere und verschlüsselte Speicherung in den Bankensystemen. Oder im Fall einer App die Prüfung auf Viren oder einen Jail Break der Geräte.