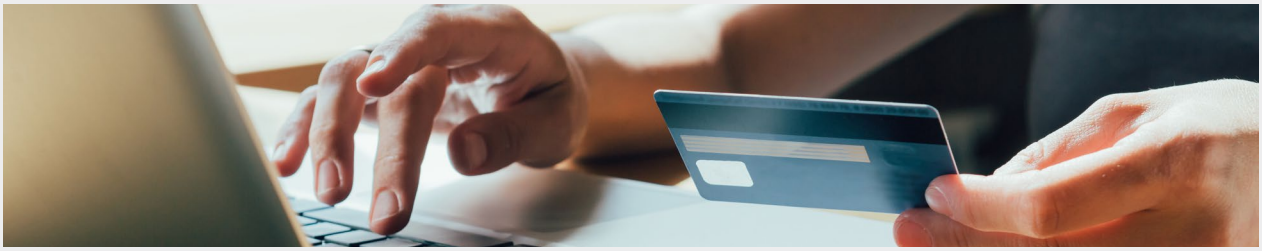
Mittelstand 4.0
Kompetenzzentrum
Augsburg

# DIE STARKE KUNDENAUTHENTIFIZIERUNG BEI ELEKTRONISCHEN ZAHLUNGEN



## WAS IST DIE STARKE KUNDENAUTHENTIFIZIERUNG?

Bei der starken Kundenauthentifizierung (SKA bzw. SCA) weisen Zahlende ihre Identität mit mindestens zwei der folgenden drei Faktoren nach:

- Wissen (z. B. Pin, Passwort)
- Besitz (z. B. Smartphone, Chip-Karte)
- Inhärenz bzw. Biometrie (z. B. Fingerabdruck, Stimme

Sie ist seit 14. September 2019 EU-weit Pflicht und kommt in der Regel dort bei allen elektronischen Zahlungen zum Einsatz, sowohl stationär als auch online. Für Kreditkartenzahlungen im Internet gilt noch bis Ende 2020 eine Übergangsfrist, während der nur ein Merkmal ausreicht.

## RECHTLICHE GRUNDLAGEN

- Richtlinie (EU) 2015/2366 über Zahlungsdienste im Binnenmarkt (PSD2)
- Delegierte Verordnung (EU) 2018/389 zu technischen Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation (RTS)
- Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz – ZAG)
- Bürgerliches Gesetzbuch (BGB), § 675c bis § 676c

## SO FUNKTIONIERT'S!

Durch die starke Kundenauthentifizierung soll bei bargeldlosen Zahlungen das Betrugsrisiko gesenkt bzw. die Sicherheit erhöht werden. Im stationären Bereich ist sie nichts Neues. Hier wurden bereits vor Inkrafttreten der neuen Regelung durch die physische Karte das Merkmal „Besitz" und durch die Eingabe der PIN das Merkmal „Wissen" nachgewiesen. Bei Zahlung im Internet änderte sich aber vieles. Bisher wurde bei der Zahlung mit Kreditkarte nur das Merkmal „Besitz" (Kreditkartennummer, Ablaufdatum und Prüfnummer) geprüft. Da es hier bei der technischen Erfüllung der Anforderungen, ein zweites Merkmal mit abzuprüfen, Probleme gab, hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) für diesen Fall eine Übergangsfrist bis 31.12.2020 gewährt. In der Zeit muss das Sicherheitsverfahren 3-D Secure eingeführt werden, das zusätzlich ein zweites Merkmal abfragt. Aktuell existiert bereits das Verfahren 3-D Secure 2.0, bei dem die kontextbezogenen Daten des Händlers analysiert werden und die Kunden nur bei risikoreichen Transaktionen aufgefordert werden, ihre Identität mittels zweitem Faktor zu verifizieren.www

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand 4.0
Kompetenzzentrum
Augsburg

# DIE STARKE KUNDENAUTHENTIFIZIERUNG IN DER PRAXIS

*3-D Secure 2.0: Die Identität wird bei einer Kreditkartenzahlung z. B. über das Push-TAN-Verfahren bestätigt.*

## GUT ZU WISSEN

Bei Lastschrift, Rechnung und Vorkasse haben Online-Händler keinen Handlungsbedarf. Wenn diese Kreditkartenzahlungen akzeptieren, müssen diese bis zum 31.12.2020 mit dem Sicherheitsverfahren 3-D Secure abgesichert werden. Die Payment Service Provider und/oder Kreditkarten-Acquirer der Händler können sie hierbei unterstützen. Zudem sollten alle damit zusammenhängenden Prozesse getestet und Kunden sowie Kundensupport über die Änderungen informiert werden. Des Weiteren können Anpassungen bei AGB und Datenschutzerklärungen notwendig sein.

## PRAXISBEISPIEL

In einem Online-Shop wird das Verfahren 3-D Secure 2.0 für Kreditkartenzahlungen eingesetzt. Während des Bezahlvorgangs gibt der Kunde seine Kreditkartendaten (Kartennummer, Ablaufdatum und Prüfnummer) ein. Diese Angaben werden zusammen mit den Transaktionsdaten der Bestellung durch den Payment-Service-Provider bzw. Kreditkarten-Acquirer des Händlers an die Bank des Kunden weitergeleitet und es wird um Authentifizierung des Kunden gebeten. Nun schätzt die Bank des Kunden aufgrund der übermittelten Daten das Betrugsrisiko ein. Wird das Risiko als sehr gering eingestuft und ist zudem der Betrag kleiner als 500 Euro, ist keine weitere Eingabe nötig. Besteht jedoch Betrugsverdacht, wird der Kunde durch eine zusätzliche Sicherheitsabfrage (z. B. mittels Push- oder SMS-TAN) zur erneuten bzw. erweiterten Bestätigung seiner Identität aufgefordert. Im Anschluss wird das Ergebnis der Authentifizierung an den Händler übermittelt und der Bezahlvorgang wird autorisiert oder abgelehnt.



IMPRESSUM

**Verleger:** Fraunhofer-Institut für Gießerei-, Composite- und Verarbeitungstechnik IGCV | Am Technologiezentrum 2 | 86159 Augsburg | Als rechtlich nicht selbstständige Einrichtung der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V. | Hansastraße 27c | 80686 München | Tel.: 0821 90678-0 | E-Mail: info@igcv.fraunhofer.de | **Vertretung:** Präsident des Vorstandes: Prof. Dr.-Ing. Reimund Neugebauer | **Text/Inhalt:** Nils Deichner, Sabine Pur, ibi research an der Universität Regensburg | **Bildnachweis:** Kolosov – stock.adobe.com (Vorderseite); SFIO CRACHO - stock.adobe.com (Rückseite) | **Druck:** Flyeralarm GmbH