

SCA - 2FA - MFA

Description	SCA stands for Strong Customer Authentication and became mandatory with 3-D Secure 2.0 .
Beschreibung	SCA (Strong Customer Authentication) steht für starke Kunden-Authentifizierung und wird mit 3-D Secure 2.0 explizit gefordert.

English	Deutsch
SCA stands for Strong Customer Authentication and is technically done with 2FA (two factor authentication) or MFA (multiple factor authentication). The authentication checks the credentials provided by a person. The authentication is performed in two steps: 1. a person provides information and claims to be "Mr. Miller" (DE: Authentisierung) 2. this information is checked and either confirmed or rejected (DE: Authentifizierung) Please note: In the German language, there is a difference between "Authentisierung" (somebody claims to be somebody) and "Authentifizierung" (verification of provided credentials). In the English language, there is no such difference; both are referred to as "authentication". Basically, there are three different types (factors) of authentication: • something you know, e.g. username/password • something you have or own, e.g. smartphone, token generator (hardware or software) • some unique biological feature of your body (biometrics), e.g. fingerprint, face proportion, iris, or vein structure SCA defines that for "strong customer authentication" at least two types of the latter must be used to authenticate a payment before initiating (authorizing) a payment – meaning that username and password are not sufficient. 2FA / MFA is also used to protect other accounts like Google, Amazon, Facebook, eBay, PayPal, ... You can find a list of websites supporting 2FA / MFA here: https://2fa.directory	SCA bezeichnet die starke Kundenauthentifizierung und wird in technischer Hinsicht mittels 2FA (two-factor authentication) oder MFA (multiple-factor authentication) durchgeführt. Die Authentifizierung überprüft die Daten, welche von einer Person als Identitätsnachweis angegeben werden. Im Deutschen wird zwischen „Authentisierung“ und „Authentifizierung“ unterschieden: • Bei der Authentisierung werden von einer Person Informationen bereitgestellt, um einen Identitätsnachweis zu erbringen jemand behauptet, "Herr Müller" zu sein. • Bei der Authentifizierung werden diese Informationen überprüft. Die Authentifizierung erfolgt also stets nach der Authentisierung und überprüft die bei der Authentisierung bereitgestellten Daten. Im Englischen werden beide Schritte als "authentication" bezeichnet: • Bei der Autorisierung schließlich werden nach einer positiven Authentifizierung die erlaubten Rechte der authentifizierten Person abgeleitet. Die Authentifizierung kann erfolgen durch • etwas, das man weiß, z.B. ein Passwort • etwas, das man besitzt, z.B. Personalausweis, Mobiltelefon, Token-Generator • etwas, das man "ist", d.h. ein einmaliges biologisches Körpermerkmal (Biometrie) wie z.B. der Fingerabdruck, Gesichtszüge oder die Struktur der Iris... SCA definiert, dass für die "starke Kundenauthentifizierung" mindestens zwei dieser drei Arten für eine Authentifizierung verwendet werden müssen, bevor eine Zahlung initiiert (autorisiert) wird – was bedeutet, dass Benutzername / Passwort nicht ausreichen. 2FA / MFA wird auch verwendet, um andere Konten wie Google, Amazon, Facebook, eBay, PayPal, ... zu schützen. Eine Liste von Websites, die 2FA / MFA unterstützen, findet sich hier: https://2fa.directory