Minimal PSD2 compliance in ONE simple step

Do you have a mobile app?

Is your app enrolled for each individual user?

N → Adding Callsign Mobile SDK can provide possession plus inherence if required (e.g. swipe, fingerprint or face)

Meets Strong Customer Authentication (SCA)

- Must have 2 out of 3 elements:
  1. Knowledge (Something you know)
  2. Possession (Something you have)
  3. Inherence (Something you are)
- Elements must be independent
- Language specific interface
- For Cards: SCA elements shouldn't be readable by staff at any time

Adding Callsign Web SDK can provide behavioural & Biometric 2FA

Adding Callsign Mobile App / SDK can provide 2FA via a push notification

Adding Callsign Telephony can provide 2FA via outbound call or SMS

N → Does your web app do 2FA at login ?

Do you have a website?

Y

Does it have compromise detection?

N → Adding Callsign Mobile SDK can provide sophisticated detection and protection against: Jailbreak, root, Malware, Anti cloning

Provides Risk Analysis

- Real-time risk analysis
- Detect unauthorized or fraudulent payment transactions
- Take into account normal user behavior in the circumstances
- At a minimum, must take into account:
  - A list of compromised/stolen authentication elements
  - Payment transaction amounts
  - Known fraud scenarios
  - Signs of malware in any sessions of authentication procedure
  - Abnormal device usage

Adding Callsign Web SDK provides malware detection and device fingerprinting

N → Does it have protection against malware & unusual device usage?

Y

Does it generate an authorisation code for logon and payment events?

N → Adding Callsign Mobile SDK provides digital signing of transactions and events – this can act as an authentication code under PSD2 rules

Provides Authentication Code and Dynamic Linking

- Payer is aware of payee and amount
- One time authentication code
- Authentication code is specific to payee(s) and total amount
- Protected against fraudulent code
- Not possible to generate from previous code
- Authentication code is related to consented amount to be blocked on card
- Not derivable to/from SCA elements
- For cards: Authentication codes are not readable by any staff at any time

Adding Callsign Mobile App / SDK can provide dynamic linking via push authorisation

Adding Callsign Telephony can provide dynamic linking via outbound call or SMS

N → Does it have an out of band approval process for new payments?

Y

Both Mobile & Website

Do you want to apply exemptions?

Y → Integrating Callsign Policy Manager provides a central management and "codification" of RTS exemptions (e.g. 90 day log-on rule, trusted beneficiary etc.)

N → **Okay, you can always choose to add these at a later date.**

Exemptions may not be a requirement, but if you don't apply them, you may incur increased costs and deliver poor customer experience, as SCA will need to be applied in **ALL** cases.

Y

Callsign Policy Manager

Manage exemptions with the Callsign Policy Manager:

- Build multi-factor authentication journeys that are uniquely tailored to your own business, customers, products or services
- Policies can be built using natural language, so any team member, whether that's risk, compliance or customer experience, can understand them
- Policies can be built using templates that include features like PSD2 specific rules, and configurable and scalable SCA rulesets
- Create dynamic user journeys that can reduce authentication steps for your customers

©2019 Callsign Inc., All Rights Reserved.