IDEMIA

PSD2 regulation and SCA make financial transactions safer than ever in Europe

The Payment Service Directive 2 (PSD2) was issued by European legislators to establish a transparent, simple and fair market, include more players, cover all electronic transactions and of course reduce fraud through better user authentication. It is a great opportunity for banks, fintech companies and other service providers to propose alternative online and mobile payment solutions that will diversify the customer's payment experience. What's more, it will further foster initiatives to simplify other types of financial transactions such as account aggregation or loan agreements, while increasing consumer protection.

1 KEY MILESTONES

JANUARY 2018
Deadline for PSD2 implementation into national laws and regulations.

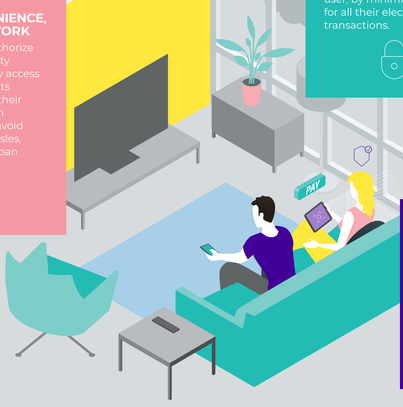
MARCH 2018
Publication in the official journal of the EU of the Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA), required for transaction security and data protection.

SEPTEMBER 2019
Final deadline to comply with SCA RTS.

2 KEY ADVANTAGES

MORE CONVENIENCE, LESS PAPERWORK
Users can now authorize banks or third-party fintechs to directly access their bank accounts in order to see all their transaction data in one place and to avoid multiplatform hassles, for instance for a loan application.

GREATER SECURITY
SCA dynamically links all transactions to a specific amount and payee, further protecting the user, by minimizing risks, for all their electronic transactions.



SIMPLIFIED ONLINE PAYMENTS
Users can now save time at checkout for frequent online purchases by authorizing merchants to initiate payments directly from their bank accounts.

3 BUT, WHAT IS SCA ?

A key goal of PSD2 is to reduce the risk of fraud for electronic transactions and enhance customer data protection.

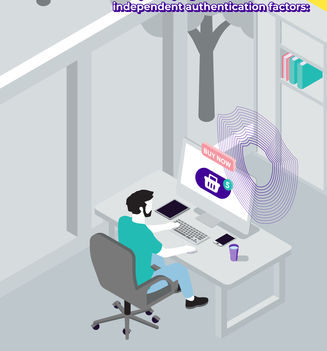
HOW IS THIS DONE?

By verifying at least 2 out of 3 independent authentication factors:

1. **INHERENCE FACTOR**
   What I am
   Physical biometrics such as fingerprint, face or iris

2. **POSSESSION FACTOR**
   What I have
   Smartphone, smartcard, USB token

3. **KNOWLEDGE FACTOR**
   What I know
   Password, passphrase, PIN, sequence, Q&A



Simply put, SCA must be used each time the user makes a financial transaction. However, to avoid too much friction in the user experience, there are some exemptions like low-value and recurring payments.

4 FURTHER REMOVE FRICTION
WITH OUR TOP-NOTCH, EFFORTLESS AND SCA-COMPLIANT AUTHENTICATION SOLUTIONS

CLOUD AUTHENTICATION SERVICE
An authentication hub that is capable of **asking for the right authentication factor(s)** whatever the channel (online, via call center, in branch) and can **analyze risk levels** to reach higher exemption thresholds and to offer the safest and most adapted solution for every sensitive operation.

RISK LEVEL ASSESSMENT
=
ADAPTED AUTHENTICATION MEANS

MOBILE AUTHENTICATOR SOLUTION: CLOUDCARD+
A mobile solution that can **combine up to three authentication factors** – PIN, smartphone and biometrics – providing a convenient, less invasive and highly secure way to prove user identity.

MOBILE & BIOMETRICS COMBINATION
=
SEAMLESS USER EXPERIENCE

ALWAYS STRIVING FOR BIGGER AND BETTER

With the Cloud Authentication service and the Mobile Authenticator solution, IDEMIA provides financial institutions with a comprehensive answer to SCA requirements with the goal of offering end-users an all-encompassing experience that focuses on security, continuity, convenience and most importantly, the human factor.