Turning PSD2 from a Threat to an Opportunity

Adaptable, Risk-Based Dynamic Authentication

The business world is generally not overly enthusiastic about learning they will soon be subject to new regulations, but where there is change there is opportunity. PSD2 is going to have a significant impact on digital commerce in Europe and will have global implications. With the advent of PSD2 all electronic financial transactions, with a few exceptions, will be subject to Strong Customer Authentication (SCA) requirements. This could be a potential pain point for users or it could be a competitive differentiator for you. Traditional, rigid modes of authentication are giving way to a new approach, one that dynamically aligns business needs with security based on risk-analysis, preserving the customer experience.

PSD2 in a Nutshell

PSD2 is an update to the Payment Services Directive (PSD) that was adopted in 2007 by the European Commission (EC). PSD created the legal foundation for a Single Euro Payments Area (SEPA); essentially establishing a single market for payments (i.e. credit transfers, direct debits, cards) in the European Union. There has been tremendous innovation in the online economy in the last decade meaning that many new services and vendors have been born that are not covered by the original scope of the PSD, making an overhaul essential. The stated objectives of PSD2 are to:

- Make cross-border payments as easy, efficient and secure as 'national' payments within a Member State
- Reduce the cost of transactions
- Make payments more secure
- Increase protection for the consumer
- Foster innovation and competition in payment services
- Create a level playing field for all players, including new ones

Some of The Most Important Changes Explained

1. PSD2 will have a much broader geographical reach, now, all transactions with 'one leg out' (at least one party is located within the EU) will be in scope vs. the previous requirement of 'two legs out.'
2. Increased requirement for securing online payments using Strong Customer Authentication. SCA must use two or more of the following independent factors:

- Knowledge – something only the user knows (password, PIN)
- Possession – something only the user possesses (key material, token)
- Inherence – something uniquely identifying to user (fingerprint, biometrics)

In addition, a unique authentication code will be required for remote transactions (internet, mobile) that can tie the transaction to a specific amount and payee.

3. Inclusion of new players, allowing third-party providers (TPPs) access to (payment) accounts (XS2A) from banks, of course with consumer permission. This will give TPPs the ability to make payments on the consumer's behalf and provide an overview of various payment accounts.

What about Brexit?

The United Kingdom submitted notice to the European Commission on 31st March 2017, which set in motion a two-year period of negotiation as prescribed by Article 50 of the Lisbon Treaty, during which the UK would be able to negotiate the withdrawal of its 44-year membership from the European Union. During this timeframe, all current and proposed EU legislation would become enshrined into UK law. As such, PSD2 precedes the earliest possible time for Brexit to take place. At this point, under the proposed Great Repeal Act, it will be incorporated into the UK statute book.

How to Turn PSD2's SCA Requirement from a Threat to an Opportunity

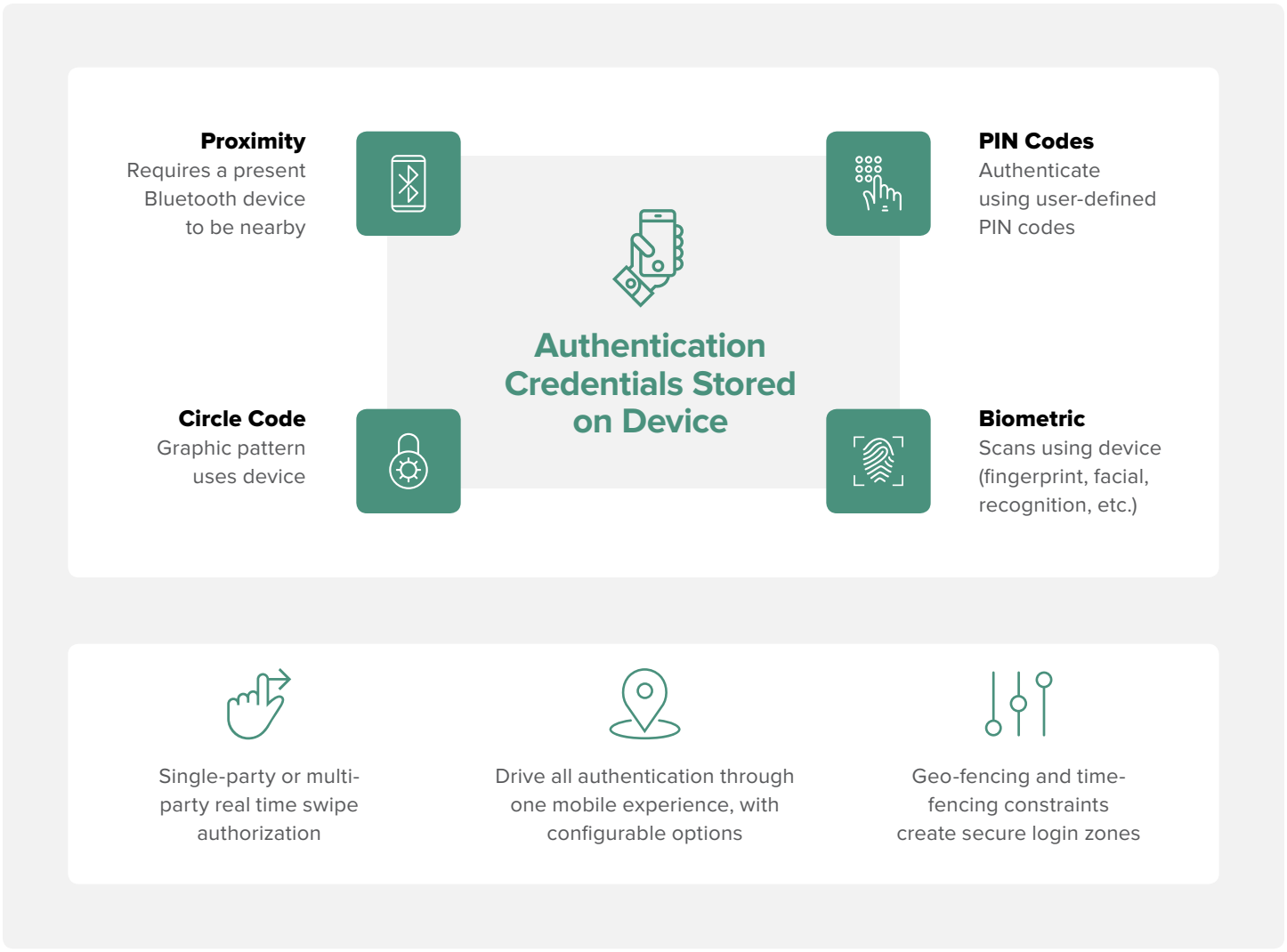
With the changes mandated by PSD2, there is a real market opportunity to transform how we think about consumer authentication. Financial institutions are under increasing pressure from consumers to offer omni-channel customer access, e.g. access to financial accounts over mobile devices, via phone using interactive voice response (IVR), on the web, and in person at a branch.

Providing omni-channel financial services will be further complicated by the requirement for SCA, and could degrade the user experience. Imagine the consumer needing to remember different authentication factors for each access channel. For the phone, it's a fingerprint. For web access, it's mother's maiden name. For IVR access, it's a requested vocal statement, 4-digit PIN or replying to an SMS one-time use password.

iovation's LaunchKey solution provides a seamless omni-channel consumer authentication service that balances security with user experience. The lightweight SDK can be deployed through your own application, managing all digital and physical authentication processes. LaunchKey allows you to quickly authenticate good customers across multiple platforms, from today's web or mobile app to tomorrow's omni-channel experience across call centers, kiosks, ATMs and IoT devices. LaunchKey provides the broadest set of authentication methods and unifies customer experience utilizing a number of configurable authentication options such as biometrics, geofencing, pattern codes, and proximity detection. This allows the user's device to be used for both independent authentication factors, satisfying SCA requirements without sacrificing the user experience.

Reducing the Risk of Data Breaches and Massive Fines!

Traditional authentication approaches can also increase your risk exposure by centrally storing authentication credentials that can subsequently be stolen. After the General Data Protection Regulation (GDPR) goes into effect in May, 2018, companies transacting in the EU could face possible fines of upwards of €20m or 4 percent of worldwide turnover (learn more about GDPR from our Solution Brief). iovation's multifactor authentication solution, LaunchKey, solves for this issue by storing credentials on the device, rather than in a central database that can be breached.



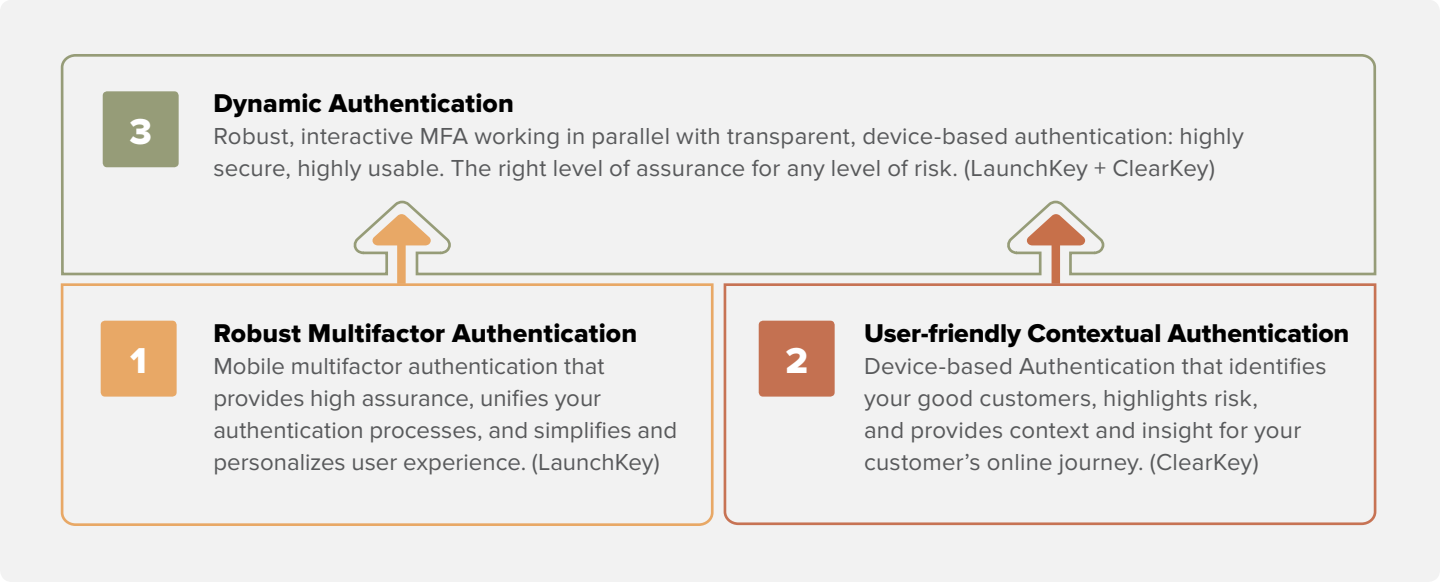
Risk-Based Transaction Analysis

SCA is required each time a payment is made, except for some exemptions such as transactions below a certain threshold or if the user has been previously identified through transaction risk analysis. To be allowed the exemption based on transaction risk analysis, the solution must be operating in real-time and must verify a transaction against anomalies in user behavior. Check points shall include the following:

- Previous spending patterns of the payer
- Payment transaction history of the payer
- Location of the payer and the payee at the time of the payment
- Previous use of the access device or the software provided to the payment service user for SCA

iovation's Dynamic Authentication Suite takes a multi-layered approach to authentication that adapts to your company's specific authentication policies in real time. It combines two or more authentication and authorization technologies into a seamless solution that delivers the right level of authentication based on perceived risk. Coupling a lightweight, transparent, device-based authentication layer with a robust and interactive mobile multifactor authentication solution. When these otherwise independent solutions are bound by a common policy, different authentication factors can be required from the user at different touch points based on risk assessment.

iovation's deep device intelligence allows us to provide financial institutions with real-time data on payment transaction history, location of the payer and payee at time of payment, and to determine previous use of the access device provided to the payment service user for SCA. This intelligence coupled with your data on previous spending patterns of the payer will allow your business to confidently decide to accept, reject or review each transaction. Ultimately allowing your institution to reduce the overall number of transactions subject to SCA without sacrificing the customer experience.



PSD2 will without a doubt have a significant impact on digital commerce not just in Europe, but globally. Make sure your business is not only prepared but positioned to seize this opportunity.

iovation®

Ready to get started? If you would like to see a free demo, please visit www.iovation.com/demo or email us at info@iovation.com

PORTLAND • PH +1 (503) 224-6010 • EMAIL info@iovation.com **LONDON** • PH +44 (0) 800 058 8731 • EMAIL uk@iovation.com