pwc

kuppingercole ANALYSTS

THE FUTURE OF BANKING:

Innovation & Disruption in light of the revised European Payment Services Directive (PSD2)

KuppingerCole
Study March 2017

About KuppingerCole

KuppingerCole, founded in 2004, is an international and independent Analyst organization headquartered in Europe. The company specializes in offering neutral advise, expertise, thought leadership and practical relevance in Information Security, Identity & Access Management (IAM), Governance (IAG), Risk Management & Compliance (GRC) as well as all areas concerning the Digital Transformation. KuppingerCole supports companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges. Maintaining a balance between immediate implementation and long-term viability is at the heart of KuppingerCole's philosophy.

As a core element of KuppingerCole's research the company provides different types of reports with thought leadership and a vendor-neutral view on the status of the markets, products, and vendors. KuppingerCole's qualified analysts continuously research and update the company's online research library, and perform manufacturer-independent advisory services.

Further, KuppingerCole organizes conferences, workshops, and webcasts in all fields of identity focused on information security, IAM, Cloud, Digital Risk and Digital Transformation. KuppingerCole's yearly European Identity & Cloud Conference is Europe's leading event for thought leadership and best practice in this area and covers the latest and future topics regarding the challenges in digital business.

KuppingerCole is the best advisory partner in making your business successful in the era of Digital Transformation.

Find additional information on our website and follow us on Social Media

www.kuppingercole.com

@KuppingerCole

Find us under: KuppingerCole

Foreword

The revised Directive on Payment Services (PSD2) forces European banks to open their data and infrastructure. Initially the focus will be on payments and access to accounts and fulfilling regulatory requirements. However, when banks and third-party providers will be able to use APIs more strategically, a world of opportunities arises. Creating and testing new models and concepts faster, cross-selling new products and services into new markets and use the consumer behavior and preference data that accrue from these activities to develop the insights needed to create additional new consumer products and services.

And there is no time to wait. Consumers live a bigger part of their lives online every day. They want to use the device of their choice and an authentication process they are familiar with and have started to embrace the kinds of services and companies that PSD2 will foster. Customer identification needs to be easy, authentication adaptive, and sharing API's needs to be secure.

From this, European banks should start embracing the possibilities of open banking soon since third-party providers and FinTech companies are already well on their way. They should not wait until the implementation of PSD2.

PwC can help. We offer a wide range of services to help European banks to expand their offerings, better serve their customers, and grow their market share and revenues.

My name is Gerald Horst of PwC Everett. PwC Everett provides best-in-class solutions for all the cybersecurity-related challenges of your online banking business. We are part of the PwC network of firms in 157 countries with more than 223,000 people in committed to delivering quality in assurance, tax, and advisory services. Tell us what matters to you and find out more by visiting us at **www.pwc.com** or call Mark van der Horst – Senior Client Executive Identity for Financial Services at **+316 1838 8539**.

Gerald Horst
Partner

Mark van der Horst
Senior Client Executive

Table of Content

The Future of Banking: Innovation & Disruption in light of the revised European Payment Services Directive (PSD2)

In early 2017 KuppingerCole performed a survey amongst the industries affected by PSD2. The primary focus of the survey was on Strong Customer Authentication, API Strategy and KYC & Customer Identity Management, in the context of the changing requirements imposed by PSD2. The results shed light on the lack of preparation and maturity of banks and other institutions, for the anticipated changes imposed by PSD2.

KuppingerCole has requested PwC to join forces during the creation of this report on the future of banking. Collaboratively they have combined the results of the survey with PSD2 and Financial Services domain knowledge to give an insight in the current state of and planning for compliancy to PSD2.

The impact of PSD2 on banks and other parties

The Finance Industry is facing a profound change with the introduction of PSD2, an update to the 2007 EU Directive on Payment Services. The directive, which comes into force on January 13, 2018, continues Europe´s goal to modernize, unify and open its financial landscape. The main objectives of PSD2 are:

- Driving Europe´s finance industry to an integrated and more efficient payments market.
- Protecting consumers by making payments safer and more secure.
- Creating a playground for (new) payment service providers and an increase in competitive pressure.

PSD2 requires banks to separate distribution and delivery of financial services from their core production environment, so that two different levels of regulation can be implemented: a tight regulation for the production part and a light regulation for the service delivery layer. This new architecture is opening the door for a "platformication" trend where organizations move away from closed and proprietary banking apps, to a new breed of community networks. This trend can already be seen with crowd funding and peer lending platforms. To keep up with all the new players and their platforms, banks need to leave their comfort zone and improve delivery of their services to meet the needs of their hyper connected customers in the world of digital business.

Amongst the changes PSD2 will impose, there will be new requirements for strong customer authentication, mandating payment providers to support Multi-Factor Authentication (MFA) for most payments. There will be exemptions for the use of MFA in PSD2. These exemptions in combination with the changing competitive landscape will result in an up rise of Adaptive Authentication as it will be the differentiating factor for banks and other financial institutions. The use ofAdaptive Authentication allows the requirements of PSD2 and other regulations to be met, while at the same time mitigating fraud risk and increasing customer convenience.

Another area of great change will be API Management and API Security. API stands for Application Programming Interface, a technical term used to describe a programmatic interface to access applications. With PSD2, supporting open APIs for a variety of use cases and third parties will become mandatory. Notably, PSD2 itself does not mention the term APIs in its documents. However, it is to be expected that APIs will be the secure standard for banks to ensure safe access for authorized third parties to customer payment data. This is even more expected because PSD2 prohibits the use of screen scraping approaches. Organizations must prepare for managing (e.g. scalability) and protecting such APIs.

PSD2 imposes a variety of new challenges to payment providers and these must be fulfilled within a relatively short period: organizations need to be compliant with PSD2 from January 13th, 2018. Given the complexity of some of these requirements, such as implementing a secure, future-proof, and convenient approach on MFA/AA or opening secure, well-managed APIs, time is running out.

PSD2 will change the competitive landscape for traditional banks

PSD2 will change the competitive landscape by creating a playground for new players in the finance industry and increasing competitive pressure. There are three fundamental areas of change by the PSD2 regulation:

- PSD2 extends the scope of the previous directive. It affects payments in all currencies and, in particular, all payments where at least one provider is located in the European Economic Area.
- The security requirements for the initiation and processing of electronic payments are tighter. This involves new requirements for Strong Customer Authentication (SCA).
- It introduces Third Party Providers (TPPs) as a new group of players. TPPs are permitted to provide certain types of account information and payment related services.

Of these changes, the TPPs will have the biggest impact on the payment markets and established players. TPPs can become the primary point of contact for a customer as customers can, for example, initiate payments via a TPP. The banks must open their interfaces to enable such payments, as well as enabling access to bank account details. This allows new players to enter the market, offering basic banking services without a banking license. The technical challenges that are related to opening up a bank's services are covered in more detail in this study.

PSD2 introduces multiple risks for banks including, being reduced to an infrastructure provider by the TPPs which are able to position themselves between the banks and their consumers. This erodes payment fees due to the conversion of fee generating transactions (such as credit card payments, debit card payments and SDDs) into SCTs initiated out of the customer's account, which does not generate a fee for the banks.

The opportunities created by PSD2 also apply to banks. Banks will have to go beyond compliance and must rethink the business models they can apply. This could include, an aggregator of account information, an API platform provider to make money off of API calls and kick-backs or white-labeling TPP services to large retailers.

Traditional banks must find an answer to the threat these new players impose on their established business models. They can do this by offering competitive, user-centric services themselves. Furthermore they could interface with other banks, to provide a comprehensive service that improves the relationship with their existing customers and is attractive to new customers. In this context, the changes that come with the PSD2 regulation are both a threat and an opportunity.

The question is, what will drive the adoption of new propositions under PSD2? Adoption will obviously hinge on client consent; this will only be obtained if the new propositions add value for the consumer, both functionally and from a user experience perspective. The first players to enter the market with a proposition that ticks these boxes can make PSD2 work very well for them.

Information Security Investment Plans in the Context of PSD2

Meeting the PSD2 requirements will require many of the organizations within its scope to invest in Information Security. The survey asked for the current and planned investments for four groups of technologies. Strong Authentication is top of the list, with more than five out of six of organizations investing in this field.

Of these four technical areas, two relate directly to changes imposed by PSD2. Strong Authentication is mandatory for fulfilling the new security requirements, in particular Strong Customer Authentication. API Security Management forms the foundation for opening APIs to TPPs, another key requirement of PSD2.

In contrast, the other three areas including, fine-grained access control, API Security Management, and Fraud Monitoring, show lower investment rates, ranging from 44 % to 57 %. The entire area of opening and securing APIs and providing access to third parties (in particular TPPs) does not appear to have sufficient attention of many organizations. The relatively low rate for Fraud Monitoring investment could indicate that such technologies are already in place in many of the organizations. The shortcomings in implementing API Security Management does not necessarily lead to the conclusion that Financial Service Providers (FSPs) don't open up APIs. However, organizations should not open up APIs without adequate API Security Management, for both security and compliance reasons.

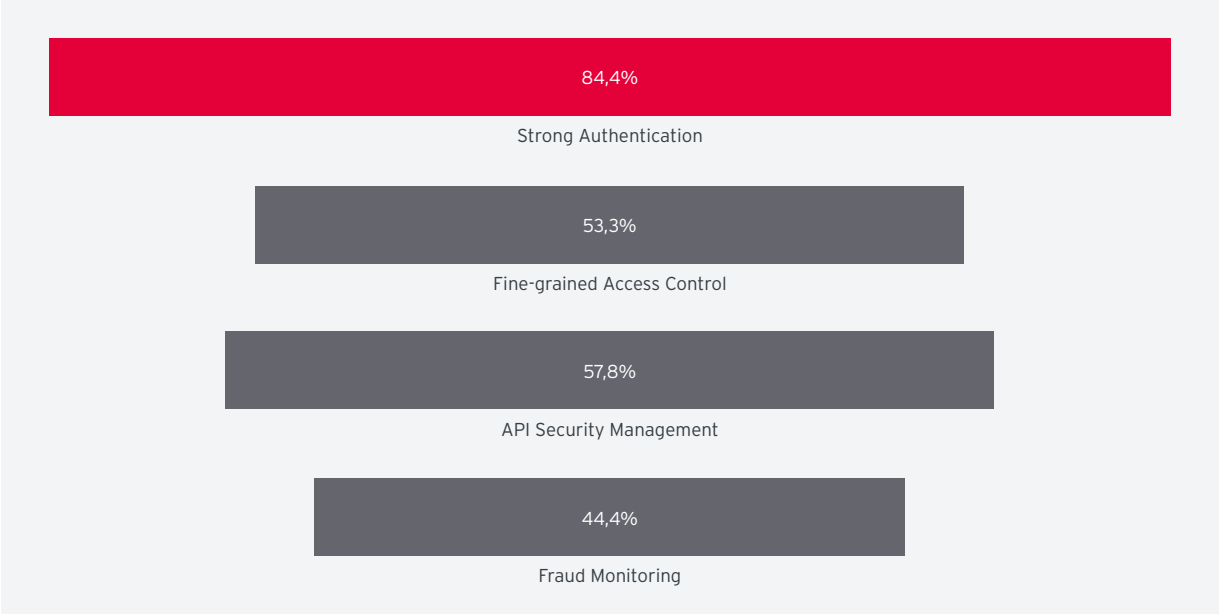

Fig. 1: Strong Authentication is top of the list of Information Security investments in the context of PSD2

The other two areas form the foundation for an open, yet secure, business that complies with the PSD2 regulation. Efficiently managed, granular access control across all systems, is a key element of IT security architectures. Fraud management, on the other hand, helps mitigating fraud risk. Fraud management is of particular interest in the context of PSD2, given that there have been many misconceptions during the PSD2 consultation period regarding the role of Risk-based Authentication (RBA). Mitigating fraud risk remains mandatory, also in the light of the full regulatory landscape banks and other financial service providers have to deal with.

Look for the opportunities.

PSD2 as a directive, strengthens certain requirements, such as those for authentication around payments. However, it is also an opportunity to invest in future-proof technologies that will better serve your customers. Use this opportunity to increase business agility and competitiveness by better serving your customers and enabling new FinTech-style business models.

Strong Customer Authentication: Status and Planning

Strong Customer Authentication (SCA) is one of the key aspects of PSD2 and will affect the authentication approaches used to secure payments. In the domain of SCA and authentication technologies, there are three terms of high relevance:

- MFA (Multi-Factor Authentication) describes approaches that support two or more factors for authentication for example, a combination of "what you know" and "what you have". A common variant is 2FA for Two-Factor Authentication.
- RBA (Risk-Based Authentication) bases authentication decisions on risk, which is calculated for example, based on the context of the user, such as the device they are using, their current location, as well as other factors. The "risk appetite" is primarily controlled by the authentication provider.
- AA (Adaptive Authentication) combines the adaptiveness of authentication technologies in MFA with the adaptiveness based on the risk. It is about combining MFA with broad support for different authenticators with RBA.

The above concepts are not new or unique to PSD2. MFA, or the common variant 2FA, has been on the radar for payments for quite a while and is not subject to change within PSD2. The EBA definition of 2FA (Two-Factor Authentication) is as follows:

> "A procedure based on the use of two or more of the following elements– categorised as knowledge, ownership and inherence: (i) something only the user knows, e.g. static password, code, personal identification number; (ii) something only the user possesses, e.g. token, smart card, mobile phone; (iii) something the user is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the Internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data."

It is not the concepts that are new but the way that they can, should and will be combined by PSP's in order to comply to the upcoming legislation and as a way to differentiate from market peers.

The current state of PSD2 formalization is that payments above 30 € will require MFA (concretely 2FA), however there are a few exemptions. The use of a single factor for authentication in combination with RBA or "transaction risk analysis" will remain accepted. PSD2 will offer a get-out clause. Over a period of 18 months the effect of using these technologies will be monitored to ensure that safeguards are effective in reducing fraud.

During the consultation period a common misconception observed was that "RBA is not allowed anymore by PSD2". PSD2 in its initial state did not accept the sole use of one authentication factor in combination with RBA for securing financial transactions. However, the use of RBA alongside MFA always has been permitted. We strongly recommend this combination, with a high flexibility in the supported authentication mechanisms, such as full support for Adaptive Authentication (AA). This allows balancing convenience with regulatory and security requirements.

Payments	1FA	1FA/MFA	2FA/MFA	2FA/MFA + RBA
below 30 €	✓	✓	✓	✓
at unattended terminals (e.g. parking meters, transport tickets)	✓	✓	✓	✓
above 30 €	✗	✓ Allowed with get-out clause (18 month monitoring period)	✓	✓

Table 1: Overview of allowed authentication concepts for different types of payments

When looking at the current state of authentication technologies in use particularly at PISPs and AISPs, the clear majority still uses a username and password. PIN-based approaches are also widely used, as well as other "what you know" based approaches including, additional passwords, passphrases, plus other types of information such as bank account numbers.

In the field of OTPs (One Time Passwords), software-based approaches are more frequently used than hardware based concepts. For both areas, including the out-of-band SMS, a significant increase is to be expected over the next few years. Notably, in the context of PSD2, not all OTP approaches are mapped to the possession of a factor, i.e. some do not count as "what you possess" factors.

Biometric authentication is rarely used today (5.7 % of the respondents). Despite the strong increase in availability over recent years, it will remain a technology used by only one third of the companies surveyed. This can be considered remarkable at the least because biometric authentication is available as a standard feature on many of the mobile devices currently in use.

The FIDO Alliance standards UAF (Universal Authentication Framework) and U2F (Universal Second Factor) appear to gain ground around biometric authentication amongst the respondents. While most companies plan on implementing FIDO standards, this is not within the next year. FIDO provides a standardized interaction between authentication mechanisms, in particular biometrics and the backend authentication systems. These standards are essential for flexibility and support a broad variety of mobile devices that have integrated biometric authentication.

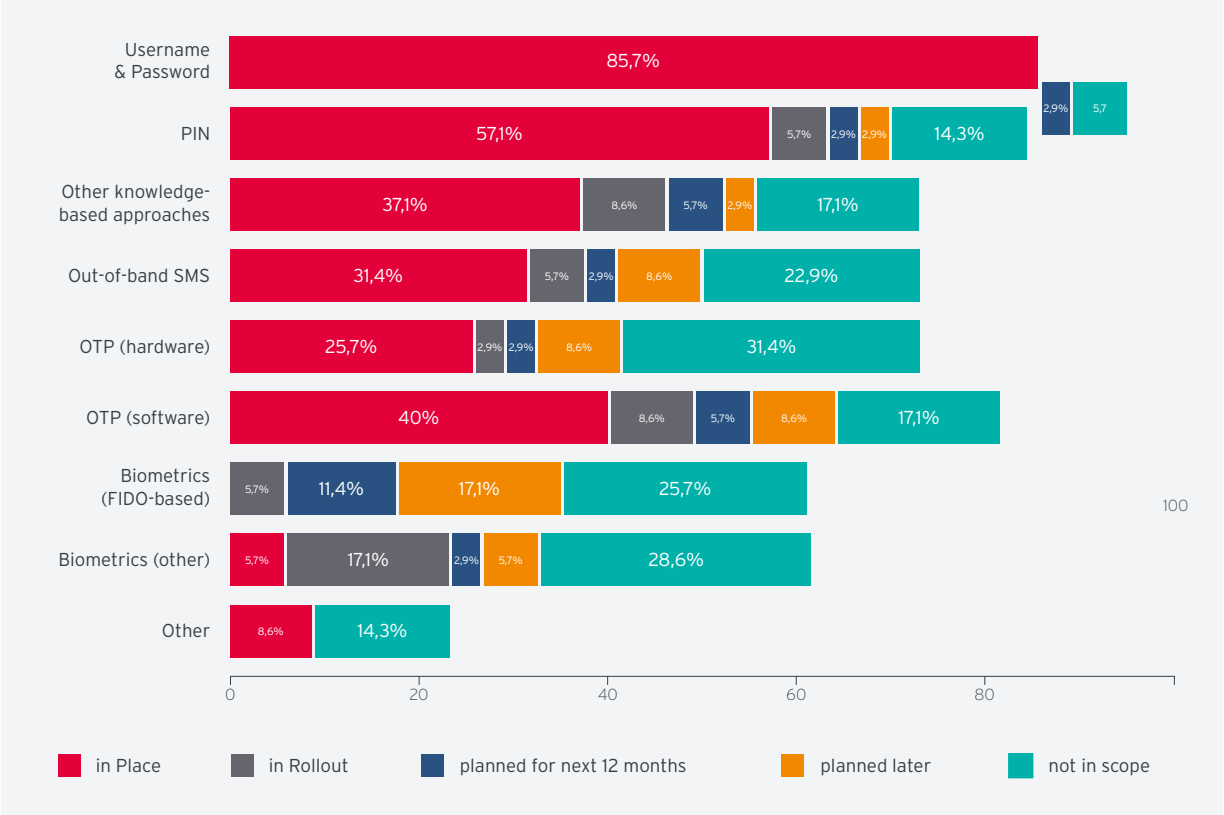

Fig. 2: Current and planned investments in strong authentication technologies (multiple answers allowed)

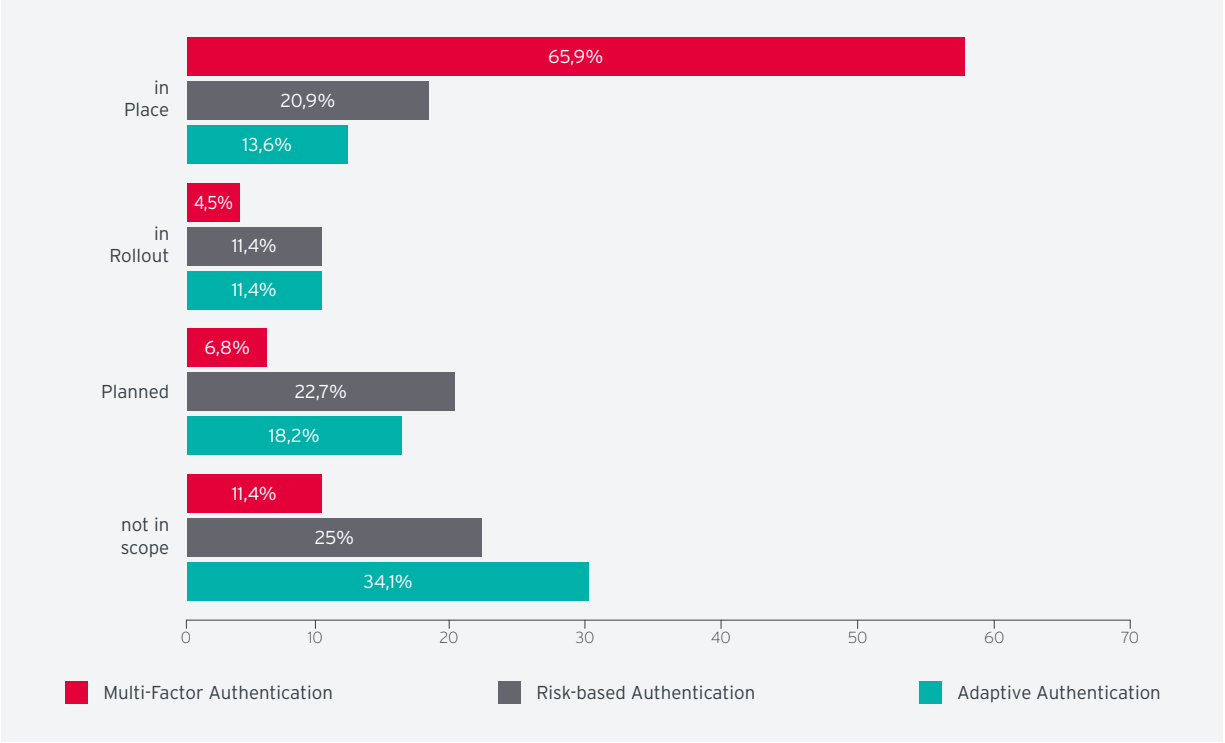

Fig. 3: Risk-based and Adaptive Authentication are gaining ground slowly

Looking at the current state and future plans for MFA, AA and RBA, we observed a major lack of support for the customers' demand for convenience. While close to 90 % of the organizations already support MFA or plan for it, only 13.6 % already have Adaptive Authentication support in place. While that number will continue to grow, with concrete and planned rollouts that will add up to approximately another 30 %. There are still many organizations showing shortcomings in that field.

Adaptive Authentication is allowed by PSD2, if the minimum requirements for strong authentication, such as 2FA, are met. PSD2 does not mandate the use of always the same two authentication factors for all use cases and customers, nor does it forbid adding RBA to the initial strong authentication. Authentication is allowed to adapt to the customers' needs and preferences within the limits of the regulation. For example, using the strong built-in authentication of the device of the customer's preference. Supporting various combinations of authenticators increases customer convenience and positively impacts customer relationships. The addition of RBA also mitigates the risk of fraud.

Customers expect to be able to use the device of their choice and the authentication process that they are familiar with, such as built-in biometrics, or any other authentication method that is convenient to them. The lack of support for Adaptive Authentication and biometrics stands in stark contrast to this expectation.

> **Many of the organizations affected by PSD2 have not yet found a solution that supports both the evolving SCA requirements of PSD2 and the need to provide convenient customer authentication.**

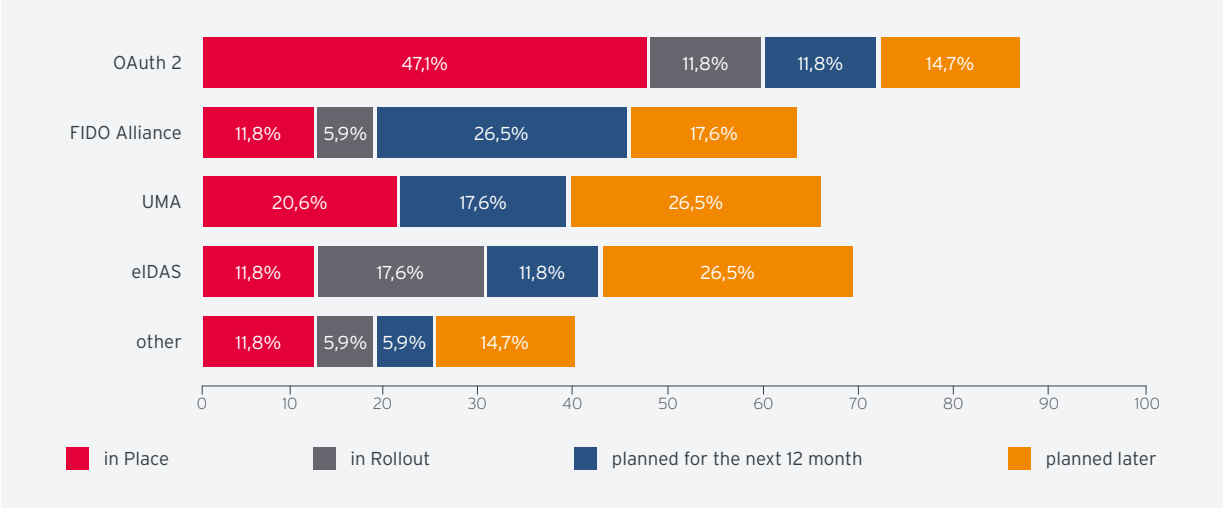

Fig. 4: Relevant authentication and authorization standards in use and planned (multiple answers allowed)

Another question in the survey looked at the authentication and authorization standards in use and planned. While most of these are not directly related to PSD2, they play an important role with respect to customer convenience and, for eIDAS specifically, for the initial customer identification. Furthermore, we observe a potential using established standards for PSD2 authentication codes with slight extensions and modifications.

OAuth2 is by far the most significant standard, frequently used in combination with OpenID Connect, while it is expected that FIDO Alliance standards will gain momentum. UMA (User Managed Access), an important standard for granting and controlling access to customer data, will slowly increase in relevance, as well as support for eIDAS (electronic Identification and Authentication Services). The rather limited support for eIDAS is surprising, given that it is an essential standard for cross-border support of electronic identities. However, eIDAS is expected to grow from 11.8 % today to approximately 30 % over the course of the next 12 months.

> **In summary, the state of and planning for Strong Customer Authentication in the context of PSD2 can be rated as being inadequate.**

Organizations do not provide sufficient support for customer convenience, while trying to meet regulatory requirements. Neither do they support the variety of existing standards that could assist in achieving this. We still observe a gap in standardization for the various specific requirements of transaction security, such as authentication codes and linkable codes.

Do not limit yourself to just meeting the regulations.

PSD2 increases the requirements for authentication. However strictly following the regulation will increase costs with little advantage. Using strong Adaptive Authentication will allow you to support all consumer devices, mitigate risk, and become independent of single authentication technology vendors. Go for Adaptive Authentication.

API Security: Status and Planning

As well as the new requirements on Strong Customer Authentication, PSD2 will impose new regulatory requirements for financial institutions to provide APIs for third party access to their systems. This access of TPPs (Third Party Providers) is a challenge from both a business and a technical perspective, the latter particularly in context of securing such APIs. The main reason is to allow new service providers to create solutions for managing payments and bank accounts across different banks and can foster competition.

There is a variety of services in scope of this change. In particular banks will have to provide a fairly broad range of APIs, the list includes, amongst others, APIs for:

- Access to accounts.
- Information about branches and ATMs.
- Access to transaction information, such as transaction history.
- Initiation if payments.

This means that managing and securing these public APIs is essential. Management includes: having a repository of all publicly accessible APIs, as well as having tools in place to manage scalability, versioning and other capabilities. API Security is about providing security for such APIs in order to protect them against attacks. Security measures range from SCA and authentication codes with dynamic linking to packet inspection.

Given that APIs will provide direct or indirect access to the core systems of banks and other financial institutions, managing both performance and security is essential. Performance becomes a critical factor if a growing number of TPPs access the APIs. Security obviously is mandatory, from both a regulatory and a cyber security perspective. To comply with regulations, SCA and transaction security are equally important, regardless whether the customers access the systems directly or via a TPP. From the cyber security perspective, each API provides an interface not only to the TPP, but also to attackers.

PSD2 offers some guidance on how to secure APIs. As part of the requirements for SCA, the concept of authentication codes is introduced. These authentication codes are basically bearer tokens that are received upon successful authentication or authorization and can be used by TPPs to access a bank's public API on behalf of a customer. Additional requirements exist that explicitly relate the token to, for example, a specific transaction or that dictate that certain authentication codes can only be used once.

Knowing that PSD2 will become effective in early 2018, it is astonishing that around 60 % of the responding organizations, which include all types of parties affected by PSD2, claim they do not yet provide publicly accessible APIs. These numbers reveal that, aside that there are some organizations that do not provide APIs, most organizations lack centralized API Management and API Security. Looking at the state of online banking and the general way banks operate with partners, we know that most banks already expose certain APIs. If they had a well thought out API Management and API Security in place, they would be aware of the APIs they already expose today, such as APIs for online banking and other capabilities.

Even more astonishing, particularly considering the PSD2 requirements, is that only about one third of the banks already claim to provide publicly available APIs. Even worse, only one in four of the banks replied that they will add further APIs within the next 12 months.

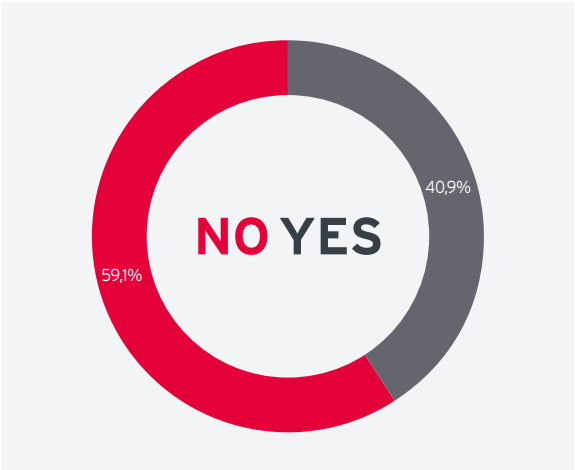

Fig. 5: Most organizations affected by PSD2 do not yet expose publicly accessible APIs

> **Many of the banks are insufficiently aware of the upcoming PSD2 requirements. They are also technically not well enough prepared to provide third parties with well managed and secure access to payment related customer data.**

This situation is made more difficult by the fact that EBA does not suggest a standard for banking API's. The banks will have to define their own APIs, which will cause significant problems for the AISPs and PISPs that are to use that variety of APIs.

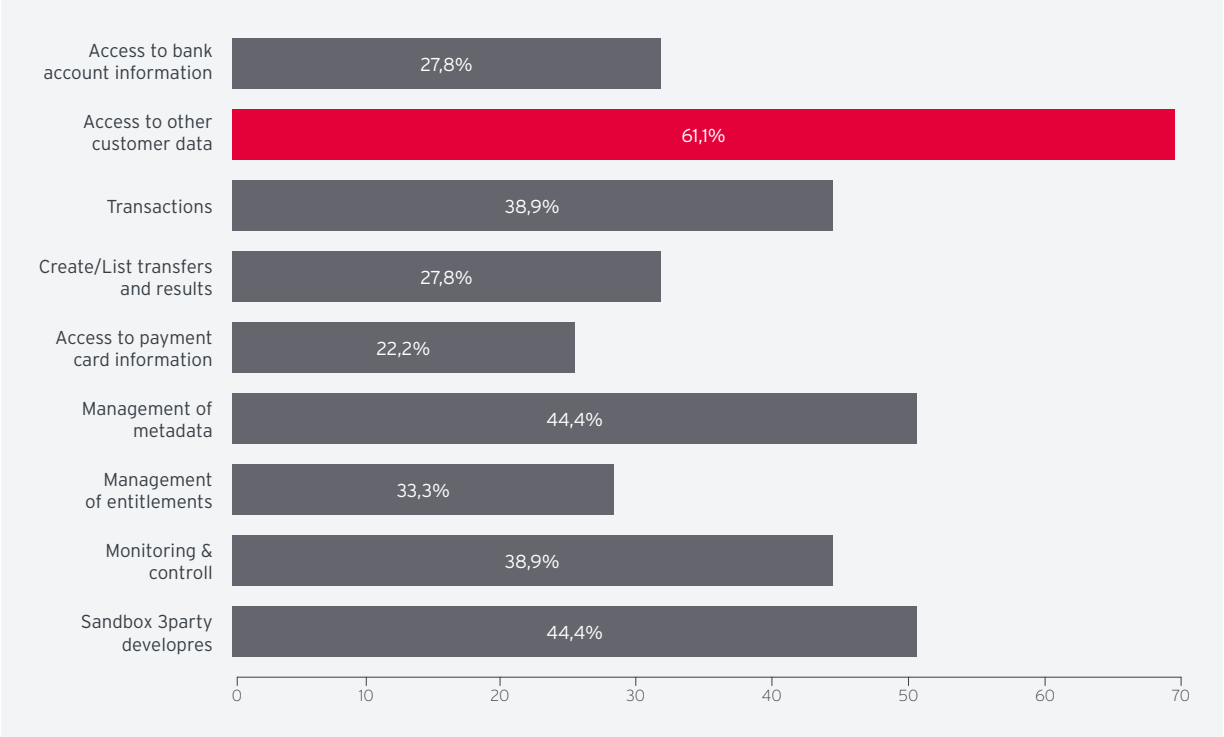

Fig. 6: Detailed view on the API capabilities supported today (multiple answers allowed)

Looking at the numbers shown in figure 1, it is clear that both the state of API security solutions and the investments planned by financial institutions for API security solutions, is too limited. Only 58% of the responding organizations plan on investing in this area, even though API security solutions are mandatory for organizations that provide or consume APIs. With the need to both provide and consume more APIs, it would be expected for that percentage to be far higher.

When looking at the API capabilities supported today, we get a very mixed result. Access to customer data is most common, while payment and bank account related APIs are rarer. PSD2 mandates both APIs for account information and for payment initiation.

Additionally, we asked for the types of APIs supported. The results show a clear trend towards support of REST-based interfaces. The number of organizations supporting REST-based interfaces is roughly double the number of organizations that provide XML-based interfaces (for example those based on the SOAP standard). While this is not directly related to the aspect of API security, it is an indicator that seems to go against the overall thought that banks are being conservative when it comes to API strategy.

“We observed a strong need for financial institutions to rethink and redefine their API Management and Security strategies, as well as their strategy for providing APIs in the context of PSD2.”

Become a consumer as well as an API provider.

PSD2 requires you to grant third parties access via APIs. Use this opportunity to create new and open services for your customers as well as providing services for the ones who aren't yet your customers. If you serve your customers well, they will reward you with their loyalty. Look at your opportunities and strengths, as well as the possible threats.

KYC & Customer Identity Management: Status and Planning

Another aspect covered by the survey is how customers are identified. This is relevant both in the context of PSD2 and the general KYC related regulations. Initially confirming the customer identity is frequently a cumbersome task. In many cases, customers must show up personally at a branch of their bank or at another trusted location. This needs to be taken into account before deploying an approach for the ongoing authentication for signing-on and transactions. There is also a trend towards supporting new approaches, such as video based identification.

Currently only 8.9 % of the respondents provide support for online identification such as video chat. A majority of about 58 % of the organizations still rely on traditional, offline identification in a branch office.

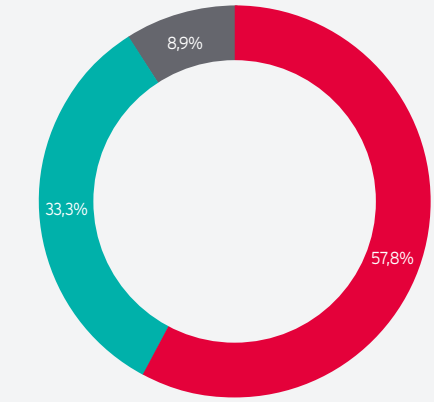

Fig. 7: Approaches in use for customer identification

“This result indicates that many financial institutions are still immature when it comes to balancing regulatory compliance with customer convenience.”

Customers have to go through many inconvenient processes, from showing up personally at a branch of a bank, to collecting a variety of documents to provide proof of identity. The number of more convenient approaches available is growing. Several of these methods are already accepted by some national regulators and auditors. However, adoption rate is still very low. While there is a need for adapting regulations to the new technical opportunities of customer identification, banks also need to review what is already feasible today, beyond their traditional identification schemes.

Provide better services through improved knowledge of your customers.

The better you know your customer, the better the service you can provide. Advanced Customer Identity Management is the cornerstone that enables KYC and multi-channel customer services. PSD2 gives you the opportunity to deliver great service to your customers by simplifying identification; providing each person working in customer service, with the information they need, at the time they need it, within the regulatory constraints.

Conclusions and Recommendations

The results of the survey demonstrate that many financial institutions are unprepared for PSD2. Many organizations seem ill informed, in particular those parties within the organization that must be involved in the preparation for PSD2. Furthermore, a clear majority of organizations show a lack of support for the changing requirements for Strong and Multi-Factor Authentication, API Management and Security, and KYC support and Customer Identification.

We have three recommendations for financial institutions and other payment providers affected by the upcoming PSD2 regulation:

- Make your authentication adaptive: MFA is a must for compliance with PSD2, while AA (Adaptive Authentication) is the key to success. It is about supporting MFA in a way that is convenient to the customer and adaptive to the ongoing evolution of authentication technologies.
- Share, manage and secure your APIs: There is no way for in scope organizations to avoid providing APIs to third parties. While most organizations do share APIs, few do so in a controlled manner. Prepare to share APIs in a controlled, managed, and well secured manner, based on centralized API Management and Security Tools.
- Revisit customer identification: There is a need to balance regulatory compliance and customer convenience. Consider the new approaches for identifying customers and understand the impact of eIDAS. Customer identification can be achieved better than ever before.

PSD2 can be a driver in increasing the competitiveness of traditional financial institutions, by increasing agility and customer convenience. However, it also can become a factor in losing ground to the new competitors, which commonly are more advanced in supporting adaptive authentication and API security.

> **We strongly recommend aligning forces to have the required changes done before PSD2 becomes effective: Ensure that all departments potentially affected by changes imposed by the PSD2 regulations are informed and collaborate closely. This involves both business and IT departments. This collaboration will help organizations succeed in achieving PSD2 compliance while serving their customers well. We strongly recommend designating a PSD2 leadership team consisting of business people, internal audit, and IT experts.**

The Survey Sample

The survey was carried out in January and February 2017, with 89 respondents. The participants were from various organizations affected by PSD2, ranging from banks and insurance companies to FinTechs, financial service providers, retail and eCommerce organizations. This provides a good sample covering the entire breadth of payment providers and other parties involved in the value chain being impacted by the PSD2 regulation.

The respondents are well-distributed across the organizational hierarchy, with a fair distribution across PISPs, AISPs, traditional banks, ranging from C-level employees (including such of large financial institutions) to the program and project managers, and include auditors and other job titles.

The responsibilities of the respondents were also well distributed. While there is a slight over representation of people with responsibilities related to Identity & Access Management. Respondents with responsibilities for Digital Innovation were also well represented at 54 %.

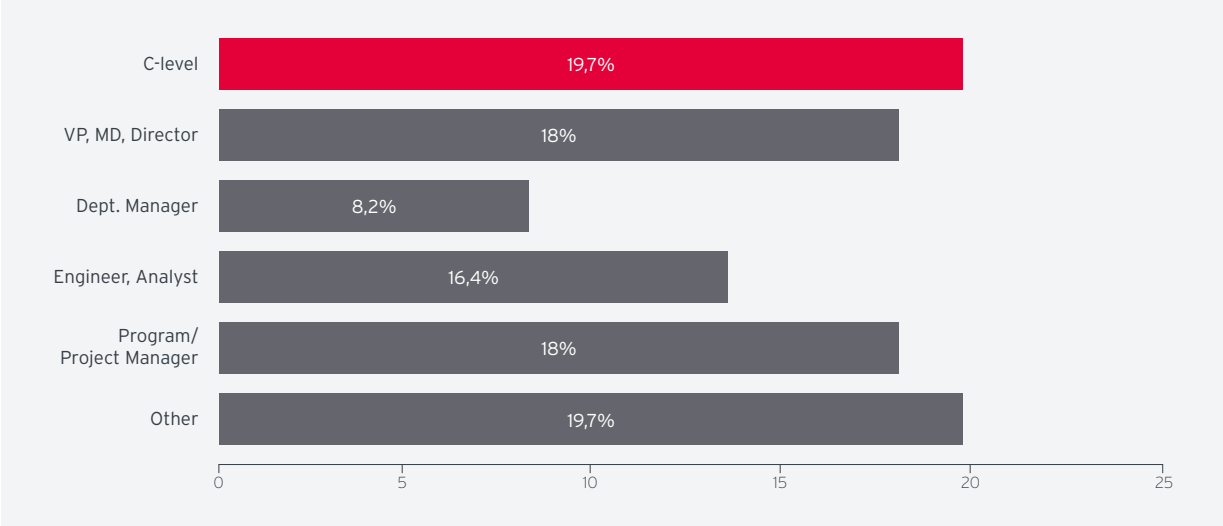

Fig. 8: Participants in the survey came from all job levels

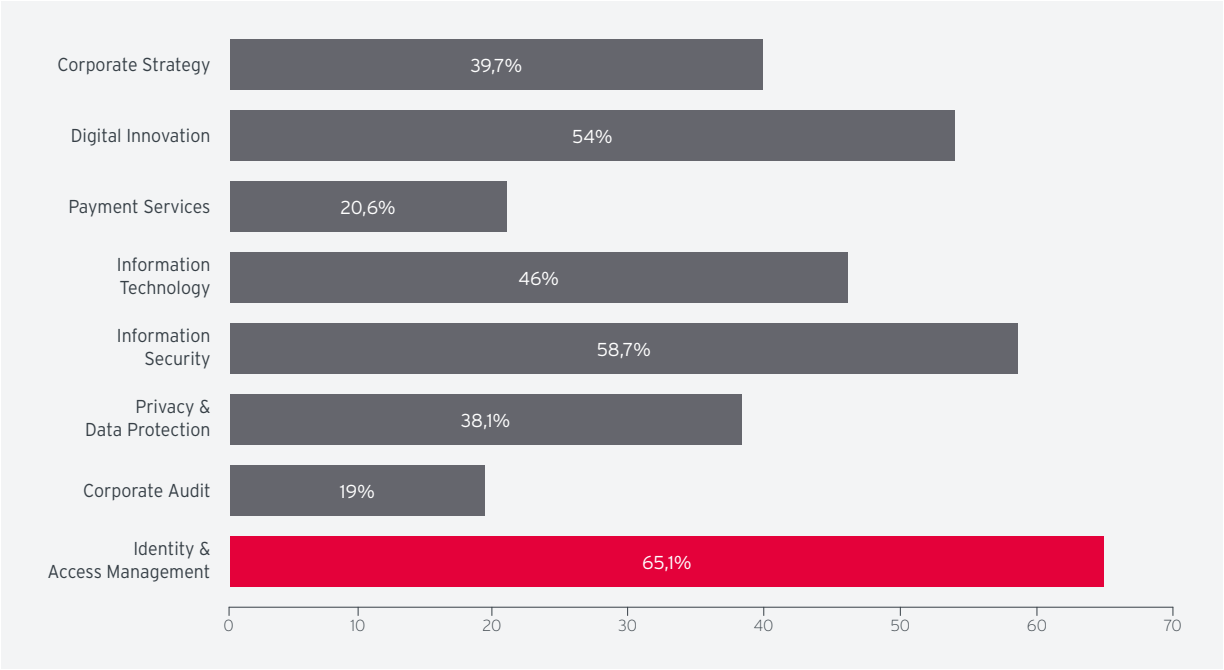

Fig. 9: The responsibilities of the respondents (multiple answers allowed)

A majority (65.1%) of organizations who took part in the survey, are directly affected by the PSD2 regulation. They include organizations with different roles such as PISP (Payment Initiation Service Provider), AISP (Account Information Service Provider) and ASPSP (Account Servicing Payment Service Provider). The others comprise companies that take active roles in either supporting PISPs, AISPs, or ASPSP, or are in other ways affected by the upcoming PSD2 regulation, such as a service provider of KYC related services.

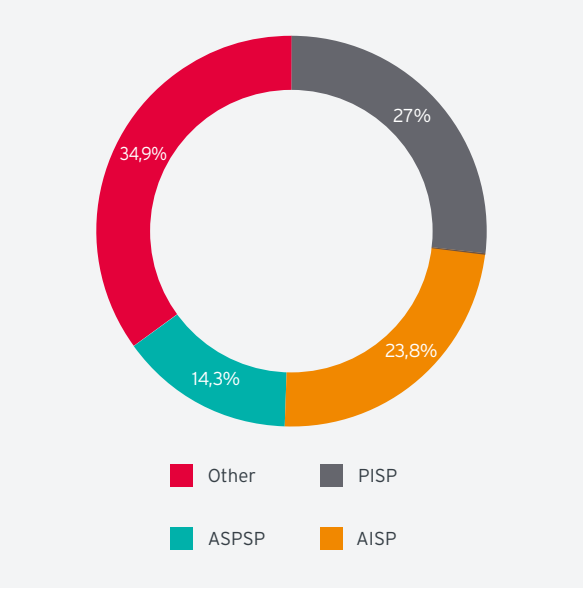

Fig. 10: The distribution of company roles in the context of PSD2.

Author

KuppingerCole

Martin Kuppinger
Founder and Principal Analyst

mk@kuppingercole.com

Reviewers

PwC

Chris van Diemen
Manager PwC

Review Lead

Rogier Adelaar
Senior Manager PwC

Tommie van der Bosch
Manager PwC

Xinthia Krielaart
Consultant PwC

KuppingerCole Ltd.
Sonnenberger Str. 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 - 0
Fax +49 (211) 23 70 77 - 11
www.kuppingercole.com