Fiorano
Enabling change at the speed of thought

PSD2 – Opportunities beyond compliance

PSD2 will open up the European financial landscape. This whitepaper outlines how Banks can think beyond compliance and leverage Fiorano to seize new opportunities created.

Contents

1. An Industry in Flux

Payment transactions are changing worldwide with payments becoming consumer centric. Consumer centric payments offer ease of use to customers' banking experience. New forms of payments coming into force require retaining high levels of security due to the entry of Third Party Providers (TPPs). The entry of TPPs entertain new payment methods such as via mobile devices demanding a seamless experience. These changes impact Banks' customer base whereby new payment services lure customers away from traditional banking. Amongst these changes is also the introduction of whole new currencies in the form of cryptocurrencies with traditional Banks set to distribute block-chain currencies in the future. All these changes demand technology that enables quick, secure and seamless payment transactions.

The Payment Services Directive 2 (PSD2) to be issued by the European Union (EU) has been mandated in effort to create a level playing field across financial institutions dealing with payments. This is to ensure that the opportunities and changes within the Banking industry can be seized and acted upon by enabling regulated implementation of new forms of payment transactions. PSD2 requires that Banks **securely** expose their customer **Account** and **Payment** data, given the customer has **consented,** to **third parties** via **APIs in a regulated manner**.

While PSD2 may be considered disrupting to traditional Banking, its strength lies in enabling adoption of new opportunities. These opportunities are offered via new app-based products and services and monetization of these services using API Management tools. A move towards PSD2 mandates that changes meet Regulated Technical Standards (RTS). The RTS, in turn, regulates the access to payment accounts (X2SA), sets the basis for Strong Customer Authentication (SCA), ensures consumer Rights and thereby allows more forms of payment transactions to enter the market. In the long term, the PSD2 directive hopes to secure an efficient and safe Single Euro Payments Area (SEPA) within Europe.

A case in point is the recent announcement (November 02nd 2017) by DBS Bank of their banking API developer platform, the largest by a bank anywhere in the world, with the objective of boosting the banks lead in creating innovative and customer-centric experiences. At launch, DBS bank had 155 APIs available across more than 20 categories, with more being added in response to demand.

2. PSD2 Aims and Implementation

PSD2 uses technology to regulate new entrants into the payment market. New entrants enable innovation and competition in Banking while securing the Rights of Consumers and creating new forms of Transaction opportunities. PSD2's underpinning regulatory mandate is implemented via the RTS which requires implementing Secure Access (XS2A) to consumer accounts along with Strong Customer Authentication (SCA) for digital payments. Payments regulated include those initiated by the payer (card payments) and do not include payments initiated by the payee (direct debit payments).

Aims:

- **Securing the Rights of Consumers:** This ensures consumers Reduced Liability, a basis for Recourse and more attractive Service offerings.

- **Reduced Customer Liability**: Securing the rights of consumers has resulted in consumers not being held liable for unauthorized payment transactions. Consumers can still be held liable where the consumer/payee has acted fraudulently, where personal security credentials were not kept safe or when the payee did not report loss/theft of the payment means.

  From a technological point, it is now the responsibility of the Bank and/or the Payment Service Provider to prove the transaction was authenticated using security credentials provided and was not affected by a technical breakdown at the time access to account. Technical stability and security such as SCA, become more than ever central to payment operations.

- **Right of recourse:** If payment service providers such to provide SCA, they become liable to compensate other payment service providers in case of breaches and/or failings. If the liability of a Payment Service Provider (PSP) is attributable to another PSP, that PSP or intermediary becomes responsible to compensate for losses incurred in case of a failure to use SCA.

- **Better Services for Consumers**: With PSD2 Banks will experience, due to better offerings to consumers by competitors, a loss in revenue with customers having the choice of leaving traditional Banks. This in addition to revenue reductions faced by Banks due to the caps on interchange rates via the Multilateral Interchange Fees (MIF) regulation (0.3% for credit card issuers and 0.2% for debit cards). Banks are in a race to deliver better and more attractive services for customers to counter attract and retain customers.

  With PSD2, in a race to deliver better services, the scope of payments by Banks and/or PSPs will include non-EEA currencies. The scope payments will now include: All payments in the European Economic Area (EEA) currencies that are carried out within the EEA; payments carried out in any currency where all participant PSPs are located within the EEA; payments in every currency, where only one of the participant PSPs are within the EEA.

In a nutshell, while offering consumers better services within the geographical remit of the directive (Europe), the impact of PSD2 will, nonetheless, impact payment transactions globally.

Implementation:

To enable the initiation of these payments in a regulated manner, as per the PSD2 directive, Third Party Providers (TPPs) are to have access to a Bank's customer online account details to initiate these payments. Banks are mandated to oblige.

Access to Accounts (XS2A) via APIs: Banks must now, with customer consent, allow TPPs access to customer accounts. This allows TPPs to **access payment Account Information** Services [AIS], **Initiate Payments** Services [PIS] and access information on availability of funds in the payment account a payment initiated by a payee. Banks use APIs that allow TPPs to access, with consent of customer, the above payment information services.

Using APIs Banks are now mandated to allow TPPs that may be Payment Initiation Service Providers (PISPs) to initiate payment transactions with customer consent and to allow TPPs that may be Account Information Service Providers (AISPs) to access balances and transaction data from payment accounts with customers authorization via customer consent.

Strong Customer Authentication (SCA): Opening up the Banking information to TPPs that include Payment Service Providers (PSPs) requires that all payments made by a payee (with the exception of low-risk payments) is verified via secure authentication.

PSD2 requirement mandates for a strong, 2-factor customer authentication (2FA) via its RTS so as to allow access to account information (using secure APIs). This strong, 2FA must meet two out of three personal authentication criteria of either **Possession** (something one possesses such as a token), **Knowledge** (something one knows such as a password) or **Inherence** (something unique to one such as an individual's biometric reading). Consent and Identity Management remain strong features of SCA are delivered as part of the Fiorano PSD2 Solution.

3. The RTS Explained

Requirements for communication between Banks and Third Part Providers (TPPs):

With consumer consent, Banks are mandated to offer TPPs access to payment accounts (using a secure API or a dedicated interface). If a dedicated interface is offered by Banks to TPPs to access payment accounts, the interface must provide the TPPs a level of availability and performance similar to that offered by the Banks to its customers. The TPPs must also be offered the same level of contingency measures as that offered by the Bank to its customers in case of unplanned unavailability.

Under the RTS, where security remains a key, there remain exemptions as well.

I. Requirements of SCA and Exemptions Under SCA:

As mentioned earlier, PSD2 requirement mandates for a strong, 2-factor customer authentication (2FA) via its RTS so as to allow access to account information (using secure APIs). This strong, 2FA must meet two out of three personal authentication criteria of either Possession (something one possesses such as a token), Knowledge (something one knows such as a password) or Inherence (something unique to one such as an individual's biometric reading).

Under the RTS requirements the SCA must produce an authentication code dynamically linked to the transaction amount and the payee. The code is dynamically linked in a manner whereby it is rendered invalid given any change in the amount and/or the payee. However, under the RTS, SCA need not be applied for transactions that fall under a specified list of exemptions (see table below):

Type	Threshold	Restrictions
Inquiry of balance and transaction information	None	SCA is required the first time and 90 days after the last SCA
Contactless payments	50 euros	SCA is required if the cumulative value exceeds 150 euros or after five transactions without SCA
Remote payments	30 euros	SCA is required if the cumulative value exceeds 100 euros or after five transactions without SCA
Payments at unattended terminals	None	None
Recurring payments	None	Payee and value of payment must be the same for each transaction
Trusted beneficiaries ('white list')	None	SCA must be applied when the user creates or amends the list
Payments to user's own account	None	Accounts are held at the same bank and in the name of the same natural person
Transaction risk analysis	Various	Risk-based authentication is allowed for low-risk transactions, as detailed in the next section

Table 01: SCA Threshold and Restrictions (Exemptions)
Source: EBA, Aite Group

II. SCA Exemptions based on Transactional Risk Analysis:

An exemption for the application of SCA allows PSPs to implement risk-based authentication under certain conditions (as opposed to not implement risk-based authentication under other conditions). The Exemption Threshold Value (ETV) that applies to SCA is dependent on the PSPs fraud rate for remote card-based payments and credit transfers. The maximum ETV is 500 euros as detailed in the table below:

	Reference fraud rate	
ETV	Remote card-based payments	Credit transfers
500 euros	0.01%	0.005%
250 euros	0.06%	0.01%
100 euros	0.13%	0.015%

Table 02: Reference Fraud Rate
Source: EBA

The reference fraud rates for remote card payments are difficult for PSPs to meet. However, it is possible for PSPs to capitalize on how low fraud rates can enable gaining a competitive advantage in the market for customers.

This exemption can be triggered by payees' and payers' PSPs. The payer's PSP will, however, have the final say, irrespective of shared responsibility, for triggering the exemption. To use this exemption, PSPs are required to have real-time transaction-monitoring mechanisms to assess/score the risk of the transaction as 'low'.

III. Requirements for Transaction Monitoring and Analysis:

Under the RTS, PSPs are to implement transaction monitoring to detect unauthorized or fraudulent payment transactions. All monitoring solutions must cover risk-based factors related to: (a) Compromised or stolen authentication details (b) Amount of each transaction (c) Fraud scenarios that are known (d) Malware infection in the authentication process.

For transactional risk analysis, under the RTS requirements, exemptions for transaction monitoring are more demanding. For exemptions to be allowed, solutions must operate in real time and must verify a transaction against anomalies in the behavior of the user. These anomalies may be present in payer: (a) Spending patterns (b) Transaction history (c) Location (d) Use of device and/or software.

PSPs require advanced fraud detection and transaction monitoring systems so as to have advanced digital identity management capabilities, to comply with these requirements. Only then can PSPs apply risk-based authentication with due diligence and in real-time.

IV. SCA Requirements for TPPs:

To access a customer's bank account TPPs require explicit consent from the customer allowing the TPP to access the customer's details. Under the RTS, TPPs may rely on SCA procedures of the account-holding bank or issuer. The User will be directed by the TPP to the bank's authentication server to obtain a token. This token can then be used to access the payment account. By using the Bank's authentication server to access the payment account, the User's credentials are not accessed by the TPP, as shown below:

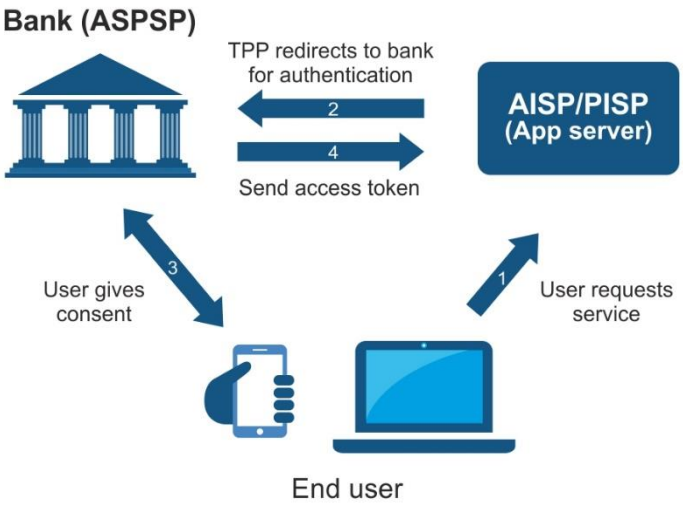

Illustration 03: SCA Requirement

A customer's personalized security details, issued by their Bank, may be requested by the TPP. However, a TPP is required to: (a) Keep these personalized credentials secure. (b) Not display these credentials at any given point of time. A TPP may issue the Customer/User with its own credentials only if it has an agreement with the Bank of the User, allowing the User to accept those credentials. To access a customer's account a TPP must identify itself to the Bank, using a qualified certificate under the eIDAS regulation, each time the account is accessed.

V. Requirements for Using SCA Over Smartphones:

A PSP may use a smartphone for SCA and related applications using its own software (without owning or accessing the device). Since the SCA elements comprising 2FA are independent they can be hosted/accessed on a single device. If hosted on a single device, the RTS requirements entail that there are separated secure environments within the devise's installed software for 2FA. The RTS requirements also entail that the devise not be altered by a payer or third party and with mechanisms installed to minimize the consequences of alterations, if these has been carried out on the device.

4. Requirements for PSD2 Compliance

A move towards PSD2 mandates that changes meet Regulated Technical Standards (RTS). These, as discussed in the previous section include X2SA, SCA and greater consumer rights all aimed to secure an efficient and safe, and thereby regulated, payments market. In Table 04, below, these same RTS compliance requirements are presented in a tabulated form:

Sl. No.	Category	Requirement
1	API Specifications	API Versioning, Management & Publishing
1.a		API Definitions
1.b		Secured API invocation
1.c		API Usage monitoring
1.d		Developer tools (SDKs, Sandboxes, documentation)
2	Strong Customer Authentication	Consent Management
2.a		Third party Authentication (oAuth + 2FA)
2.b		Fine grained access control & entitlements
3	Incident Reporting	Security Incident Reporting
3.a		Fraud & penetration monitoring
3.b		Anomaly detection

Table 04: RTS Compliance Requirements
Source: Fiorano

I. Impact on Banking in the UK

The impact on traditional banking in the UK is due to the changes mandated in the PSD2 allowing new entrants into the payments market. The related impact on the sector could potentially contribute to UK banks losing up to 43% of their current payments revenue by 2020.[1] The new breed of payment initiation service providers will erode 33% of online debit card transaction volumes and 10% of online credit card transaction volumes.[2]

Despite the threats, there are many opportunities present in PSD2 such as being innovative in creating new revenue streams. These revenue streams can attract customers based around a focus on customer centric banking such as extended ecosystems centered on the 'everyday bank'. As with any innovation the opportunities will be present to those who embrace them from the outset.

PSD2 seeks to encourage innovation and competition into the market, thereby creating a more consumer centric sector. PISPs, as an example, could offer cheaper alternative for internet payments while AISPs could allow aggregate of customer bank account data from different

[1] Finextra

[2] Finextra

accounts. This would enable a clearer analysis of customer data, transactions and analysis of spending trends, resulting in a better service for the customer.

Innovation can be in myriad other areas such as Payment Initiation, Advanced Aggregation Applications, Card-less Withdrawals, Couponing, Instant P2P Payments, to name a few. Consumers could now maintain one account and use many other financial services via TPP Applications.

Application Programming Interfaces (APIs) are central to Applications as data/information is published via the API Gateway to TPP Applications. API Platforms are also used to monetize and provide insights as well as services around the data received. It is imperative, then, for banks to leverage API integration to develop a customer centric ecosystem using their own banking portals. The steps that Banks can follow in for preparing for the changes driving their sector are:

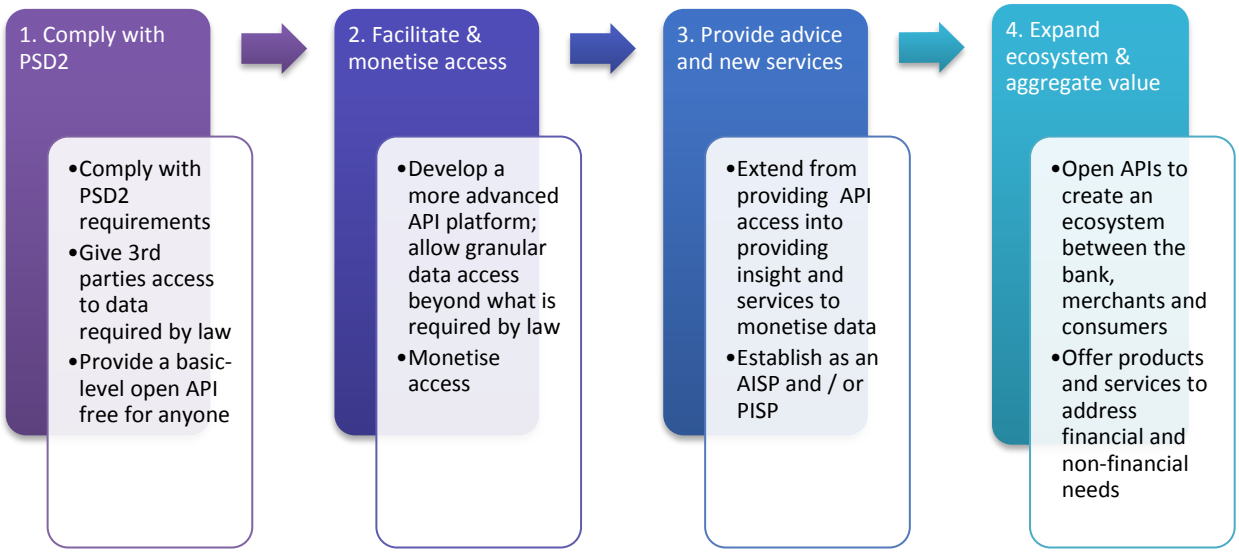

Illustration 05: Strategic Changes to the Banking Sector

5. The role of APIs

I. API proposals and PSD2

PSD2 aims to regulate the European Payments market. PSD2 also aims to promote the emergence and encourage competition in innovative in the mobile and internet Payments market in Europe.

The changes that the Banking industry is facing are documented in earlier sections. The most significant implication is that of accessibility of customer data to third parties. The core of the changes entails the mandated aspect for Banks to grant PISPs, AISPs or other TPPs access to their online account/payment services which include Access to Accounts (X2SA) via APIs.

APIs are crucial in enabling the X2SA component of PSD2 implementations. API Management platforms where API management servers allow enterprise data to be exposed in the form of REST or Web Services (REST more often being preferred because of its inherent flexibility), with each exposed REST Service referred to as an "API", is crucial in enabling the X2SA component of PSD2.

The API is essential as it can securely expose enterprise data (from a file, database or other enterprise system) or data an internal enterprise application. In any given enterprise, there may be tens to hundreds of exposed APIs running on and managed by an API Management platform.

An API Management Platform comprises server technology that enables data **security**, **metering**, **monitoring** and **management** of APIs. **Security** descriptors provide the enterprise fine-grained control over which end-users and user-groups may (or may not) access an API. **Metering** consists of when a count is maintained of the number of times an API has been called, together with a list of applications that make the calls. Metering limits can be set as charges on a per-call (or other) basis for all API calls. **Monitoring** allows system administrators to track APIs that use maximum resources (in terms of CPU, memory) and enable mapping of related information to identify hotspots and contention. This information can be used to decide how to split an API call-load over multiple API Management servers (provided the underlying solution allows for this scaling-out process). **Management**, consists of a view of the overall implementation of API Management across the enterprise. This includes a synopsis of the API security, metering and monitoring processes running across multiple servers within and outside an enterprise firewall.

As stated in previous sections, PSD2 requires Banks to expose selective account information to TPPs. The account information to be exposed to TPPS is to be done so, as mandated by the RTS, in a secure, managed, metered and monitored environment. Given the role of API Management discussed in the previous paragraph, API Management is essential to Banks in they are to expose the relevant information, in the manner mandated, to TPPs. API Management servers implement security standards mandated by the PSD2 RTS including, importantly, the O-Auth standard. The use of API Management technology dramatically simplifies PSD2 implementation thereby enabling faster time to compliance. Fiorano's API Management Platform and Out-of-the-box PSD2 solutions meet the standards and requirements for PSD2 compliance stated in the sections above.

6. Fiorano's "Best-In-Class" API Management Platform

API Management servers implement security standards mandated by the PSD2 RTS. The Fiorano API Management Platform has the capability to implement requirements, of PSD2 and beyond, highlighted in the sections above. These standards and requirements include security, metering, monitoring, management and developer support.

To accommodate the growth envisioned in the Banking sector, advantages of using the Fiorano API Management Platform architecture is that it allows for linear scalability thereby allowing the infrastructure to grow as required. An illustration of the Fiorano API Management architecture and its components is provided below:

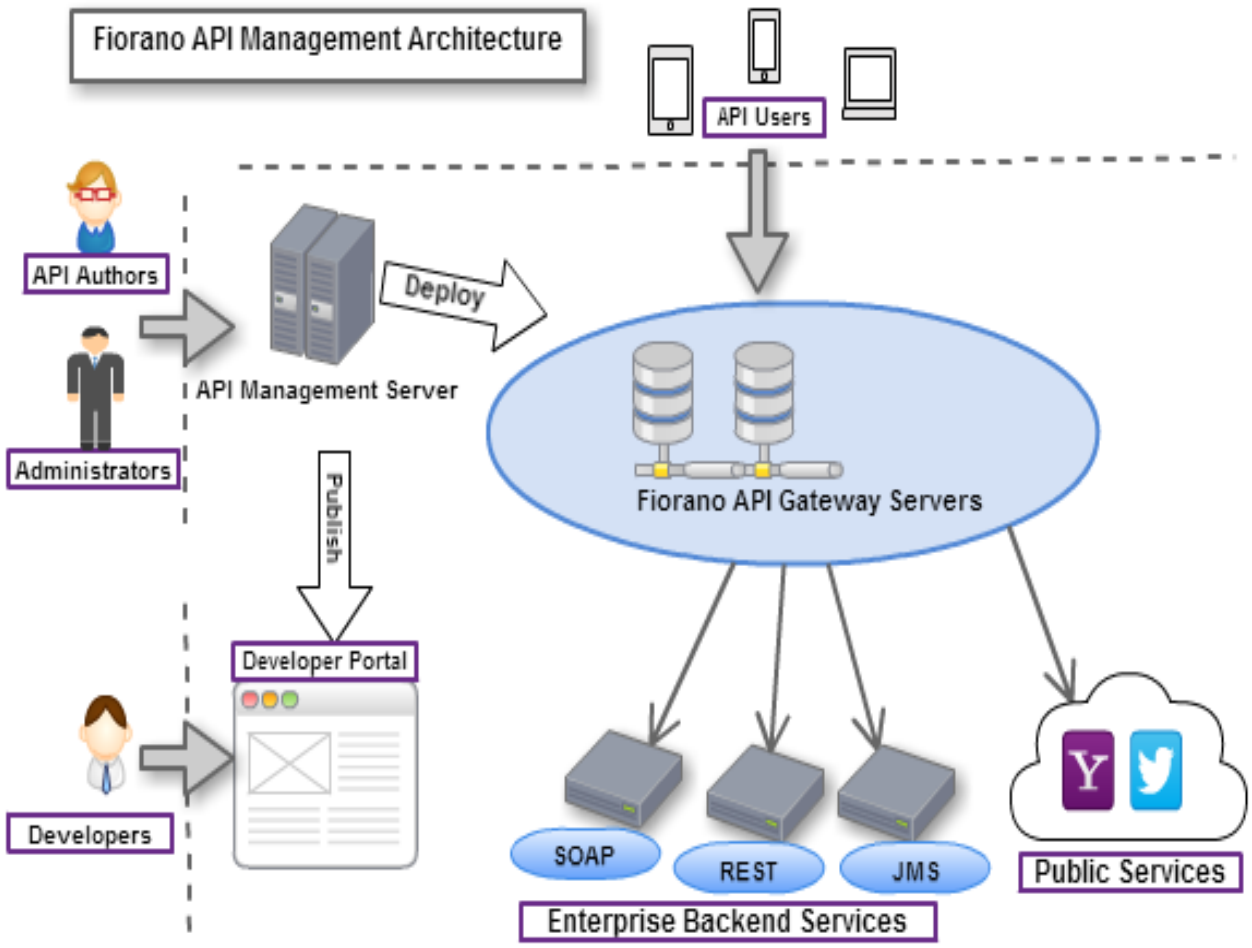

Illustration 06: Fiorano API Management Architecture
Source: Fiorano

The Fiorano API Management System comprises a central API 'Management' server which serves to administer and control a network of available API 'Gateway' servers. Multiple API Gateway servers, all

that may be controlled by a single Management Server, may host several hundred APIs in the form of REST or Web-service(s) calls. The Fiorano API Management server works with all REST or Web-services or JMS based systems implemented within an enterprise. With the Fiorano API Management server, there are no dependencies on the creation of the REST or Web-service(s) that need to be managed and exposed as API(s).

Crucially, as highlighted earlier in this section, Fiorano's best-in-class API Management architecture scales linearly. As the number of APIs to be hosted increases, additional API Gateway servers are deployed as 'peers', allowing the load to be distributed across multiple servers thereby enabling a build-as you grow strategy. A strategy to be invaluable for the coming changes and growth in the new payments market within the Banking and TPP sectors.

7. Fiorano PSD2 "end-to-end" Solution

I. Overview:

The Fiorano PSD2 Platform consists of all foundational infrastructure technology requirements that banks need to create an open banking platform and become PSD2 compliant.

II. Fiorano PSD2 Solution components:

Illustration 07: Fiorano PSD2 Solution components
Source: Fiorano

The Fiorano PSD2 Platform offers a comprehensive implementation of the PSD2 RTS at two Levels. **Level 1 implementation** provides core API and Consent Management infrastructure required to become PSD2 compliant without the necessity of becoming a third-party such as an AISP, PISP or ASPSP. Level 1 PSD2 RTS implements over 60% of the sections of the RTS. The remaining sections are specific to TPPs and are covered under the Level 2 PSD2 RTS implementation. **Level 2 implementation** provides additional functionality and business benefits associated with being a full TPP, beyond the Level 1 compliance which provides the bare (associated) components.

III. Compliance requirements met by the Fiorano API and PSD2 Solutions:

No.	Category	Requirement	Fiorano PSD2 platform
1	API Specifications	API Versioning, Management & Publishing	**Fiorano API Management**
1.a		API Definitions	
1.b		Secured API invocation	
1.c		API Usage monitoring	
1.d		Developer tools (SDKs, Sandboxes, documentation)	
2	Strong Customer Authentication	Consent Management	**Fiorano Consent Management**
2.a		Third party Authentication (oAuth + 2FA)	**Full support for 2FA via. oAuth / other formats**

2.b		Fine grained access control & entitlements	**Fiorano Consent Management**
3	Incident Reporting	Security Incident Reporting	**Cisco Professional Services delivered by Fiorano**
3.a		Fraud & penetration monitoring	
3.b		Anomaly detection	

Table 08: Fiorano's RTS Compliance Requirements
Source: Fiorano

IV. Compliance requirements met by the Fiorano PSD2 RTS Level 1 PSD2 Implementation:

No	Article / RTS	Fiorano PSD2 - Level I
1	**1. (b), (d)**	Fiorano API Management: OAuth, Proof Key Code Exchange
2	**4. 1, 2, 3 (a), 3 (b):** *Security Measures for the application of Strong Customer authentication (SCA)*	OEM SCA integration options
3	**Article 5. 1, 2, 3** *Dynamic Linking*	Fiorano API, For 2, 3, partial functionality is in the TPP App
4	**Article 6. 1, 2** *Requirements of the elements characterized as knowledge*	Fiorano API and TPP app
5	**Article 7. 1, 2** *Requirements of the elements categorized as possession*	Fiorano API and TPP app
6	**Article 10. 1, 2** *Payment account information*	Fiorano API – base functionality with Rules
7	**Article 11. a, b** *Contactless payments at point of sale*	Fiorano API – base functionality with Rules
8	**Article 12** *Transport and parking fares*	Fiorano API – Rules Configurations
9	**Article 14** *Payments to self*	Fiorano API – Rules Configurations
10	**Article 15** *Low-value transactions*	Fiorano API – Rules Configurations
11	**Article 18 1, 2** *Invalidation and optionality of exemptions*	Fiorano API – Rules Configurations
12	**Article 26. 1., 2 (a), 2 (b)** Traceability	Fiorano API – core security functionality
13	**Article 27. 1, 2, 3, 4, 5, 6** *Communication Interface*	Fiorano API – core functionality
14	**Article 28**	Fiorano ESB – core functionality

	Obligations for dedicated interface	
15	**Article 29 1** *Certificates*	Fiorano API – core functionality
16	**Article 30 1, 2, 3, 4, 5** *Security of communication session*	Fiorano API - core functionality
17	**Article 31** *Data exchanges*	Fiorano API - core functionality

Table 09: Compliance requirements met by Fiorano PSD2 RTS Level 1 PSD2 Implementation
Source: Fiorano

A requirement central to compliance is that of Strong Customer Authentication (SCA). SCA requirements encompass Third Party Authentication in the form of oAuth and 2FA. The Fiorano PSD2 Solutions comes with an embedded Identity and Consent Management system.

8. Fiorano Identity and Consent Management

I. Consent Management:

Banking customers play a pivotal role in legitimizing the use and disclosure of their account information. They provide access to and disclosure of this information by giving and/or withdrawing their consent to disclose information at any instance.

Under the PSD2 regulation, consent plays a crucial role in granting or removing access rights to customers' Bank account information by Banks/TPPs. Depending on the context in which the access is being executed, to access account information or to initiate a payment transaction, different consent policies are applied. The execution of these instructions need certain information 'sets' to be consented to by the customer either implicitly or requested explicitly. Customer consent can be obtained explicitly in writing or implicitly through the context within which the instruction executed carries information obtaining consent. Since account information is sensitive, the Banks/TPPS access this information only when needed.

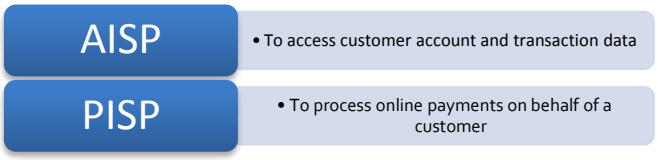

Illustration 10 : Customer consent requirements in PSD2
Source: Fiorano

Customers may grant consent to execute a batch of remote electronic payment transactions to one or several payees. In the absence of such consent, payment transactions are considered unauthorized. The consent to execute a payment transaction or a series of payment transactions is given in the form of an agreement between the payer and the payment service provider. The granted consent can be withdrawn by the customer at any time, but no later than the moment of irrevocability.

II. Fiorano PSD2 – Consent Management

Fiorano Consent management allows Banks to achieve regulatory compliance by offering choices and control over customer data usage. With Fiorano Consent management, Banks can request and capture customer consent to use their data while complying with PSD2 regulations. Fiorano provides Banks customer consent and permission over customer data usage while tracking data interactions. Fiorano creates and converts customer consent into data rights accessible across all data systems, enabling a trusted relationship between the customer and the data processors, thereby giving customers secured rights over their personal data.

With Fiorano Consent Management, Banks are able to:

- Configure requirements for customer consent collection.
- Expand to different channels to collect customer consent.
- Configure access control for consent validation.

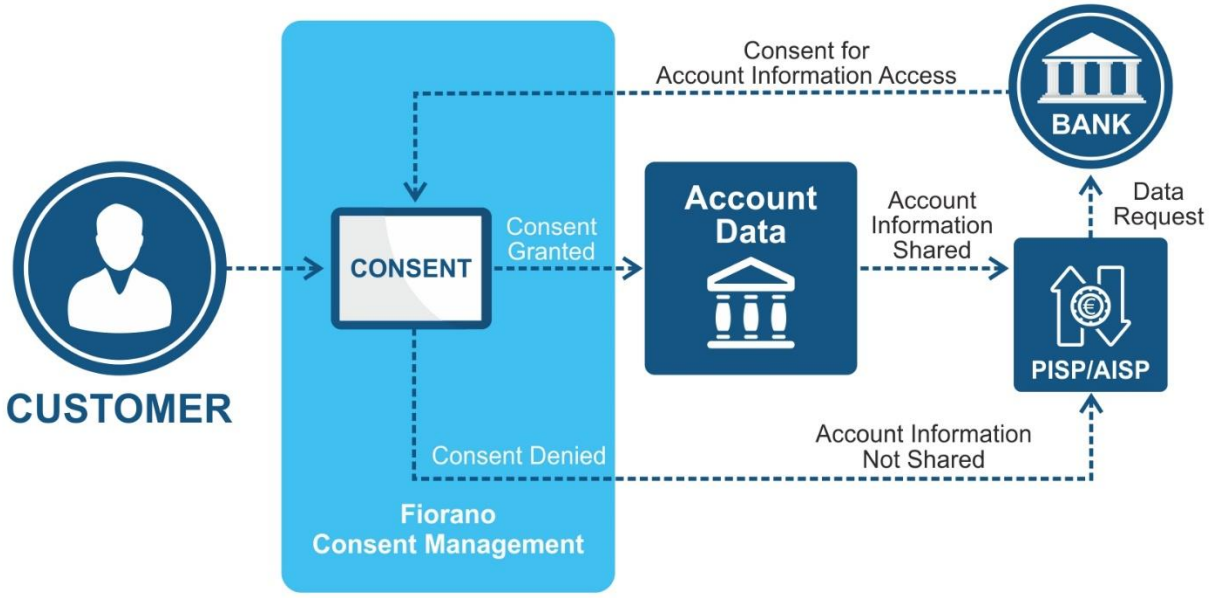

Illustration 11: Workflow Based Consent with Fiorano Consent Management

Fiorano Consent Management Key Features:

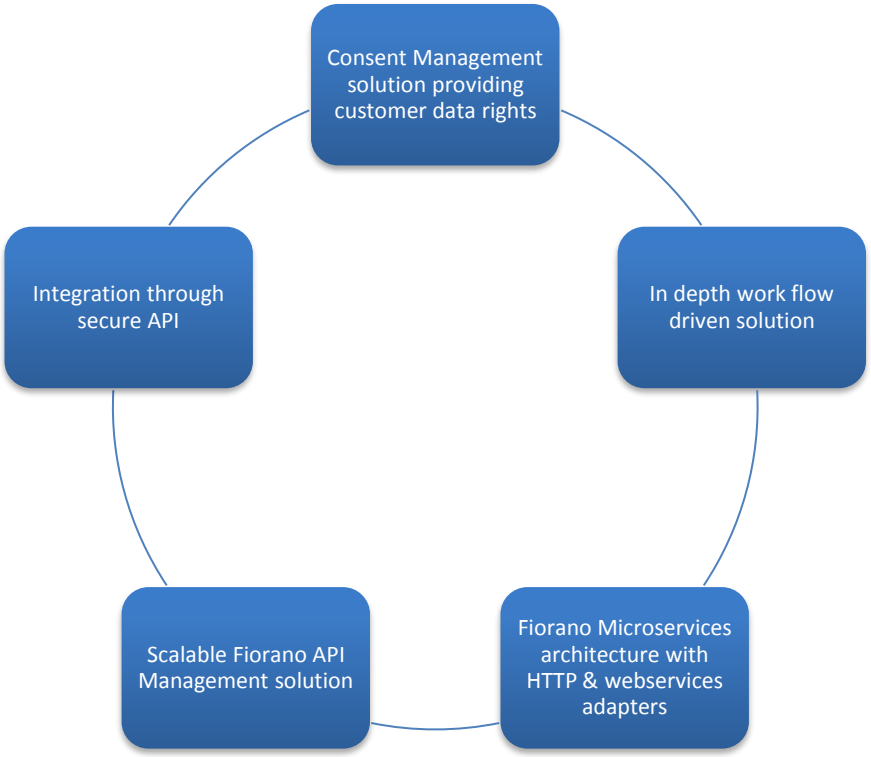

Illustration 12: Fiorano Consent Management Flow

Fiorano Identity Management Key Features:

With Fiorano Identity Management, Banks can identify, authenticate and authorize information access by connecting user rights with pre-defined identities. By setting levels for access and permissions, Fiorano Identity Management ensures that only those users/entities that are authenticated access authorized information.

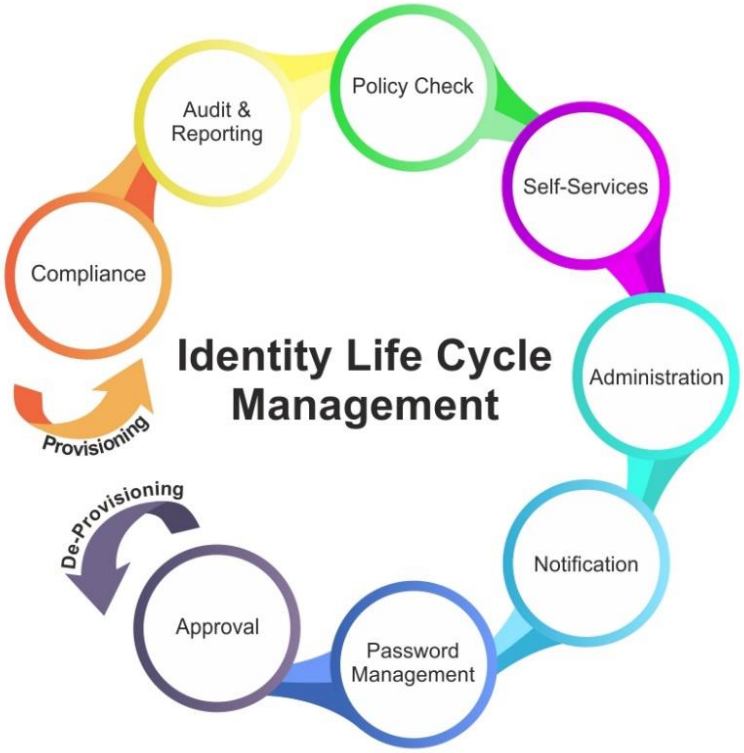

Illustration 13: Fiorano Identity Management Flow

Fiorano Identity Management allows Banks to extend access to information systems across on-premises applications, mobile apps and SaaS tools without compromising security. Built on the Apache® Syncope™ 2.0 digital identity and access management system, Fiorano Identity Management provides a framework with policies and technology needed to support digital identity management. The system keeps identity data consistent and synchronized across repositories, data formats and models.

9. Fiorano PSD2 Solution Information Exchange Specifications

All information exchanges to/from core banking platforms and the Fiorano API Management server are via XML messages. Wherever specified, the Fiorano PSD2 solution follows ISO message requirements as described in the RTS, including the implementation of the ISO 20022 message format.

Fiorano API Management supports both SOAP and REST-based web-service endpoints provided by the Bank's middleware system or through web-services supported by the bank's core banking system.

Five sample APIs with corresponding parameters are listed below. *Note that the request and response message format can be either XML or JSON.*

APIs and their Corresponding Parameters:

I. PaymentInitiationService API:

Overview: This API is used for initiating a payment between different accounts within the same bank or across different banks.

Request Parameters:

Transaction Type	*[This is to indicate the transaction type initiated by the bank]*
Debit Account Number	*[The Account Number for which the amount needs to be debited]*
Debit Currency	*[Debit Account Currency type]*
Debit Amount	*[Amount to be debited]*
Credit Account Number	*[The Account Number to which the amount needs to be credited]*
UKSortCode/BIC	*[This code is used for cross- bank payments]*
Credit Currency	*[Currency in which amount would be credited]*

Response Parameters:

Transaction ID	*[If the core banking provides, this would be a unique ID returned by the core banking system]*
Transaction Type	*[This would be same as transaction type passed from the input request]*
Debit Account Number	*[Same as in request parameter]*

Debit Currency	*[Same as in request parameter]*
Debit Amount	*[Same as in request parameter]*
Credit Account Number	*[Same as in request parameter]*
Credit Currency	*[Same as in request parameter]*

II. GetAccountDetails API and BalanceEnquiry API:

Overview: This API is used to retrieve account details of a customer from within the Bank. If the customer has multiple accounts, the APIs will return all the accounts belonging to the customer at that bank.

Request Parameters:

Customer ID	*[Unique ID which is assigned to each customer of a bank]*
Currency	*[If the customer has multiple accounts with different currency types, this parameter is used to query accounts belonging to a particular currency type. If not set, the API returns all accounts]*

Response Parameters:

Account ID	*[Account number]*
Currency	*[Currency type for this account]*
Customer ID	*[Same as in request parameter]*
Customer Name	*[Name of the customer]*
Working Balance	*[Account balance for this account]*

III. GetExchangeRate API:

Overview: This API is used to query the exchange rate set within the core banking system.

Request Parameters:

From Currency	*[Currency type to be converted from]*
To Currency	*[Currency type to be converted to]*

Request Parameters:

Mid Rate	*[Exchange rate between buy and sell rate]*
Buy Rate	*[Buy rate of the currency]*
Sell Rate	*[Sell rate of the currency]*

IV. TimeForTransactionCompletion API:

Overview: This API is used to inform (prior to initiating transaction) the customer about time taken to complete a transaction.

Request Parameters:

Transaction type	*[This parameter would indicate the payment/transaction type]*

Request Parameters:

Time Taken	*[Time taken to complete a transaction/ payment type mentioned in the request parameter]*

V. PaymentCompletionStatus API:

Overview: This API call provides the status of the payment initiated using the "PaymentInitiationService" call. For example, status would be "payment in progress" / "payment waiting for approval" / "payment completed".

Request Parameters:

Transaction ID	*[Transaction ID returned by "PaymentInitiationService" call]*

Request Parameters:

Status Flag	*[Status flag to indicate the status of the payment Initiated]*

Table 14: Sample APIs with Corresponding Parameters
Source: Fiorano

All information exchanges are performed via XML or JSON messages. Wherever specified, the Fiorano PSD2 solution follows ISO message requirements as described in the RTS, including the implementation of the ISO 20022 message format, as mentioned above.

10. References

- EBA: *Draft Regulatory Technical Standards*
- Accenture Payment Services: *A catalyst for new growth strategies in payments and digital banking*
- Aite: *Creating value and managing risk in the world of PSD2*
- Strategy&PWC: *Catalyst or threat, strategic implications of PSD2 for Europe's banks*
- PWC*: PSD2 – a game changing regulation*
- Deloitte: *Anticipating the challenges and opportunities of PSD2*
- Innopay
- Digital Ventures: *Introduction to Open Banking*
- Finextra: www.finextra.com *"Banks Set to Lose 43% pf Payments Revenue Under PSD2."*
- Finextra: FInextra.com. "Banks set to loose 43% of retail payments under PSD2."

Disclaimer:

Fiorano®
Enabling change at the speed of thought®