Solution for PSD2

Online
BUSINESS TECHNOLOGIES

Introduction

What business trend lies behind of PSD2?

Technological advances have had a major impact on the financial market, banks have been challenged and emerging smaller competitors (FinTechs) and big technology providers (BigTechs) entering new markets have forced traditional banks to develop and innovate.

FinTech's growth is signalled by the increasing volume of investment in this sector year-on-year, a record 32.2 billion dollars in the second quarter of 2018, an increase of 3.2 times over the same period last year.

FinTech companies offer innovative solutions in many areas of financial services, such as providing account information and financial advisory services, payment services, international transfers, social lending, crowdfunding, while also implementing blockchain and other ground-breaking technologies.

The initial hostility of banks to FinTech has changed rapidly and more and more banks have started to think about cooperation with FinTech companies. In PWC's FinTech report released in 2017, 82% of banks reported that they will work with FinTech in 3-5 years. Cooperation with FinTech companies shows the development of so-called ecosystems, in which banks and FinTech companies using standard interfaces, APIs, make their services available to each other and jointly provide their services.

It is our expectation that this means that banks will have to provide all their services to external partners within 5 to 10 years.

The European Union supports the business trend and innovation detailed above with the PSD2 directive as it establishes the legal framework for cooperation between banks and FinTech companies in the field of payment services.

What is PSD2 and why is it unavoidable for banks?

The PSD2 (Payment Service Directive Revised) is the Directive 2366/2015 of the European Parliament and of the Council on payment services in the internal market, the promulgation of which has been the European Union's first step in promoting innovation, competitiveness and efficiency. The PSD2 directive allows customers to decide whether to use the current solutions of banks (such as the Internet or Mobile Bank) or to try FinTech's IT solutions to initiate online payments or query the account balance and transaction history.

Under the Directive, banks must make their payment services available to FinTechs free of charge and they must provide non-discriminatory access to orders received via FinTechs. At the same time, the directive expects to meet higher security requirements for online payments.

The banking sector has come to a turning point since every bank has to decide whether to comply only with these legal obligations or to try to exploit the business opportunities inherent in changes. You can choose anyway: our company offers an IT solution to support any selected strategy!

What are the governing requirements for IT solutions?

In addition to the PSD2 directive to be transposed into national law, several EU-level rules have been introduced that greatly influence the framework for IT solutions. Some of these detailed rules are Regulatory Technical Standards (RTS) that must be complied with in all Member States unchanged, or so-called Guidelines to be adopted into local regulations.

The requirements for IT solutions may be most clearly defined by the delegated regulation of the Commission (EU) 2018/389, which sets out the detailed provisions of the PSD2 Directive for strong customer authentication and common and secure open communication standards. This regulatory technical standard is usually referred to as the RTS on Strong Customer Authentication or RTS SCA.

RTS SCA has shaken the entire European market, and many interpretations have come to light in several points. The European Banking Authority (EBA), as the regulatory authority responsible for the partial regulation of PSD2, issued an opinion (EBA-Op-2018-04) to clarify the requirements, providing guidelines for market players and local authorities for RTS SCA interpretation.

Introducing DigiTie

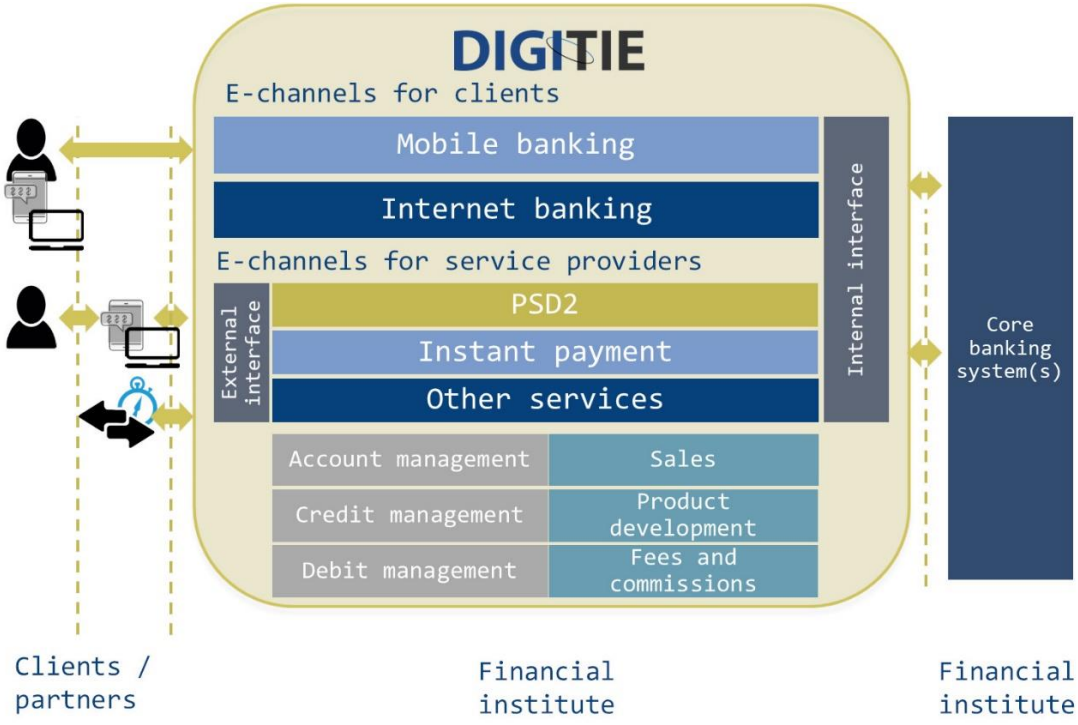
To fulfill the PSD2's IT requirements, we offer our DigiTie solution. But DigiTie also helps you to exploit the business opportunities!

DigiTie is a 24/7 software that handles a wide range of electronic channels (e.g. mobile banking, APIs) and is able to provide the complex services provided by the core banking system (e.g. account management and transaction management, lending, deposit management) even if core banking systems are not available.

Self-contained, complex service is one of DigiTie's biggest benefits.

The majority of the software serving electronic channels are more likely to mediate between the clients/partners' software (e.g. mobile banking, webshop) and core banking software, but have very limited potential for independent servicing in case of unavailability of the core banking software (e.g. typically they provide only balance and account information). DigiTie is completely different. DigiTie can provide complex services 24/7, such as handling overdrafts and instant payments (e.g. HCTInst/SCTInst). DigiTie can independently perform even a complete credit sales process. We can enable DigiTie to provide virtually any core banking service and to later synchronize with banking core systems to maintain consistency of background systems.

The DigiTie service concept is presented in the following figure.



DigiTie is able to provide direct electronic customer channels such as a mobile bank or an internet bank, but it can handle the standard interfaces (API) as well to provide orders and queries from financial institution partners.

DigiTie-supported services, like the MoonSol system, can be customized on demand: if, for example, a particular financial institution already has a well-established and customized Internet banking solution, DigiTie can be tailored to handle indirect electronic channels only.

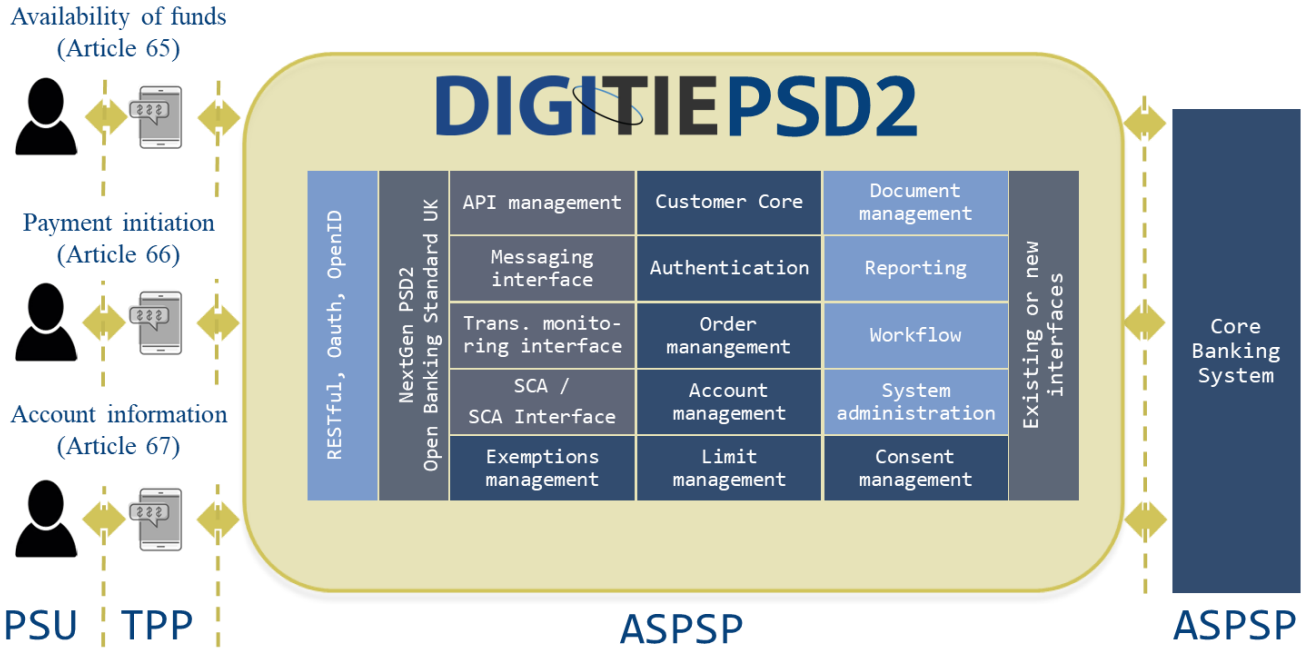
Due to DigiTie's customization, it is possible to gradually open services to the outside world, so it’s a viable option for a credit institution to provide, in a first round, only the services made obligatory by the PSD2 directive (availability of funds, payment initiation, account information), which can be followed by a number of services, such as instant payment (HCTInst / SCTInst), or online lending.

Another advantage of flexible customization is that DigiTie can be unique or uniform on demand. Many of our partners prefer that the DigiTie solution they use be "off the shelf", that is a software solution used by other customers and therefore cheaper, while others are insisting on more expensive, but competitive customized product. DigiTie, like MoonSol, can combine these "common" and customized elements in a unique way.

DigiTie can be operated cost-effectively. According to the requirements of a financial institution, DigiTie can be installed locally, in the IT infrastructure of the particular financial institution (on-premise), or DigiTie can be made available in centrally managed operation, as Software as a Service. In this latter case, the financial institution will have a separate DigiTie copy, but the operation will be managed by our company.

Introducing DigiTie PSD2

The DigiTie version for the PSD2 requirements – the DigiTie PSD2 – is presented in the following figure.



The DigiTie PSD2 provides interaction between users (PSUs, Payment Service Users), external service providers (TPPs, Third Party Providers) and the Bank with up to 24/7 availability, receiving, processing and forwarding incoming orders, and even incorporating the services of external systems into the process. DigiTie's PSD2 functions are completely modular, so some of its features (such as mobile application authentication) can be replaced by an existing IT solution that is already in use in the particular financial institution and can be upgraded later.

The DigiTie PSD2 brings harmony to the convenience of the bank, the bank's customers and the TPPs. It provides the bank with a forward-looking compliance with regulatory requirements that can be easily developed thanks to built-in technology. Customers of the bank have access to the highest level and the widest range of services, whether directly or indirectly, while their money and, which is also of paramount importance today, their data is also safe. DigiTie PSD2 provides transparency so you can clearly identify who, when and for what purpose can access your customers' accounts, and DigiTie PSD2 also keeps track of fraudulent signs.

The services and functions provided by the DigiTie PSD2 are described in detail in the next section.

In order to provide the services required by PSD2, the DigiTie PSD2 has two main interfaces as shown in the illustration.

In the direction of the TPPs, DigiTie PSD2 offers standard APIs that are developed, on demand, based on a major international PSD2 technical standard. Such technical standards may be e.g. the Open Banking UK standard, the Berlin Group NextgenPSD2 standard, or even the STET standard.

The other main direction of the interfaces is designed towards existing banking systems.

If full PSD2 functionality is implemented by DigiTie PSD2, this is basically an interface for the existing account management system(s) that is needed to serve payment initiations, account queries, and collateral testing. DigiTie PSD2 can be linked to account management systems with the interfaces to existing online banking solutions as well, as it has to provide access to payment services under PSD2 to banks, which are otherwise available for customers in online banking solutions. With this method, the complexity of implementation can be significantly reduced. Of course, it is also possible to create new interfaces.

The recommended DigiTie PSD2 solution can optionally have additional interfaces to other banking systems, such as an interface:

- in the direction of existing online banking and mobile banking applications (e.g. to allow the customer to customize DigiTie PSD2's limit management in their usual applications)
- using the mobile application authentication currently used by the bank for online banking and mobile banking solutions,
- to the current fraud control system used by the bank
- etc.

How does DigiTie PSD2 meet the PSD2 directive and RTS SCA specifications?

The following subsections show how the services and functions of DigiTie PSD2 provide our partners with the PSD2 directive and RTS SCA compliance.

Standard and secure communication

According to the RTS SCA communication between intermediary organizations (such as TPPs and banks) should be in conformity with (widely used) communication standards issued by an international or European standardization organization (see Article 30 (3) of RTS SCA). In addition, a secure exchange of data between the bank and TPPs should be allowed to reduce the risk of redirecting communications to third parties (see Articles 28, 35 of RTS SCA).

It is also a requirement for PISPs and AISPs that when personal credentials issued by the account manager are transmitted, the transmission is carried out via a secure and efficient channel (see Articles 66 (3) (b), 67 (2) (b) of PSD2).

The DigiTie PSD2 solution uses, and is based on industry-specific security and communication standards that meet the above-mentioned requirements. These include:

- ISO 20022, FAPI
- JSON Schema, JSON API and OPEN API
- TLS 1.2
- OAuth 2.0

Identifying TPPs and applying certificates

Based on the requirements of PSD2 and RTS SCA, a solution should be developed to identify TPPs (AISP, PISP, CBPII) and support the use of eIDAS certificates (see Articles 65 (2) (c), 66 (2) (d), 67 (2) (c) of PSD2, and Articles 30 (1) (a), 34 of RTS SCA).

The task of DigiTiePSD2 is to maintain the bank's security while serving the bank's customers, so during each API call, DigiTie PSD2 checks at the minimum the following:

- whether the calling party has the standard eIDAS certificate for TPPs, and whether it is valid,
- whether the TPP license (role) entitles the caller to access the given service,
- whether the TPP's license referred to in the certificate is valid at the given date in the central register.

Use of bank-provided customer authentication by TPPs

PSD2 requires AISPs and PISPs to be able to use all the authentication procedures the bank is otherwise providing to their customers (see Article 97 (5) of PSD2 and Article 30 (2) of RTS SCA)

The DigiTie PSD2 system has its own authentication solutions, and we have also prepared our system to use the existing procedures of the bank to authenticate customers, thus ensuring compliance with the above requirement.

Strong customer authentication

The PSD2 directive stipulates that when the payer accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses, strong client authentication is required, the detailed rules of which are contained in RTS SCA. (see Article 4 of RTS SCA)

The DigiTie PSD2 module can meet the requirements of strong customer authentication on its own, providing two kinds of solutions. The native support of the traditional solution, which is using a combination of static password and a secondary, dynamic password sent by SMS, can be complemented with mobile app based authentication.

External access authentication has three major forms. In these, as a common feature, authentication is carried out by the bank as it issues credentials to its customer; the bank and the TPP may agree otherwise, but these are subject to a specific contract and not PSD2.

- Redirect. The customer will be redirected from the TPP to the bank where he will perform the authentication as provided by the bank.
- Embedded. The customer's credentials are provided to the TPP who will provide the bank with the credentials, in a secure manner as required by the regulations.
- Decoupled. The client authenticates on a device/channel other than the one used by the TPP, e.g. using a dedicated mobile application provided by the bank for this purpose.

DigiTie PSD2 is currently providing the safest, redirected authentication for banks and customers. Naturally, a different (e.g. decoupled) authentication process can be deployed on request.

Dynamic linking

According to PSD2 and RTS SCA, for transactions, an authentication code should be used that implements the dynamic linkage for a given amount and a payee, even in the case of bundled transactions (see Article 97 (2) of PSD2 and Article 5 of RTS SCA).

The authentication solution of the DigiTie PSD2 system always connects the process and the codes of authentication to a given operation, ensuring that the customer's approval with the subject of the approval is dynamically linked. If an alteration occurs in any of these, such as if the amount or the payee changes when an order is submitted, or the range of available data changes in case of requesting account access, it causes the authentication to fail, and the authentication must be restarted.

Exemptions from strong customer authentication

The PSD2 regulation requires that the bank applies the same authentication exceptions if the client initiates a transaction through a TPP as if it was done directly through the channels provided by the bank. (see Articles 18 (2) (c) (v) and (vi), 18 (3), 30 (2) and 32 (3) of RTS SCA)

The DigiTie PSD2 module puts the banks in control of the exemptions offered by RTS SCA, since it can handle all of them, thus direct banking channels can be easily synchronized to use the same exemptions.

Account access for TPPs

Pursuant to the requirements of PSD2, it is necessary to ensure that card-based payment instrument issuers (CBPII), payment initiation service providers (PISPs) and account information service providers (AISP) have access to online payment accounts for the data required for their services. These specifications are set out in Articles 65, 66 and 67 of the PSD2 and Article 30 of RTS SCA.

In the APIs created in DigiTie PSD2, we created the three major service groups, as indicated in the previous figure. Through this, different TPPs can access the payment accounts as described in the API documentation, provided they have a consent from the account owner, specifying the details of the access, such as a particular transaction or a specific set of account details.

Provision of uniform account information

Under the regulatory framework, banks must provide AISPs with the same information that the user may otherwise see regarding the particular payment account and associated transactions (see Article 67 (2) (d) of PSD2, and Articles 30 (1) (b), 36 (1) (a) of RTS SCA).

The DigiTie PSD2 account information API is capable of returning to the AISPs the data that a particular customer has made available to them. The exact range of data is different for each bank, in each case adjusted to the range of data available on other channels, thus providing a personalized solution for each bank.

90-day re-authorization for AISPs

In accordance with the regulation, AISPs should be required to re-authorize account access within 90 days (see Article 10 (2) (b) of RTS SCA).

The DigiTie PSD2 module provides an opportunity to use the account access exemption provided by RTS SCA (when within the scope of the exemption) in such a way that DigiTie monitors, simultaneously with the client's access permissions for the given access, the date when the last strong client authentication occurred. If it has been done more than 90 days ago, it is required for the next access.

Counting access requests

The PSD2 specifies the minimum number of times banks have to provide access to their databases for AISPs (see Article 36 (5) of RTS SCA).

In DigiTie PSD2, similarly to the 90-day re-authorization, the number of access requests is supported, enabling AISPs to access a maximum of four times (or multiple times if agreed upon) within a 24-hour period, even without the presence of a client to the data of the authorized account, as required by RTS SCA.

Transfer via PISP

Pursuant to PSD2 and RTS SCA, users should be able to authorise and consent to transactions through PISPs (see Article 64 (2) of PSD2, Article 30 (1) (c) of RTS SCA).

The basic functions of the DigiTie PSD2 include the provision of dedicated interfaces required by the PSD2 to external service providers, and thus the submission and approval of payment orders initiated by the bank's clients through PISP, in case they have a payment account accessible online.

Revocation of already initiated transactions

According to the requirements of PSD2, provision should be made for the possibility that the customer may withdraw the already launched transactions in accordance with the PSD2 regulation, including regular transfer orders. (see Articles 64 (2), 80 (2), 80 (4) of PSD2)

In the DigiTie PSD2, the API for payment initiation provides PISPs with the option for querying the status of transactions and, if it is possible, initiate the retraction of the approval already granted by the client, and thus a future dated or a recurring transfer order (along with any remaining referrals) can be cancelled.

Fraud monitoring

According to PSD2, the organizations concerned must comply with the requirements for reducing the risk of fraud, carry out reliable and auditable data exchanges and allow payment monitoring (see Article 97 (3) of PSD2 and Articles 3, 22, 35 of RTS SCA).

DigiTie PSD2 supports filtering of suspected fraudulent transactions, providing an integrated solution that meets or even exceeds all the requirements of RTS SCA. In the process of authentication, it is capable of analysing the data at a level that can also help in establishing a strong customer authentication exception based on risk analysis. On the system's interface, the bank can monitor payment transactions, and the control parameters can be set freely on the fraud control system's interface.

Confirmation on the availability of funds

The PSD2 regulation requires banks to promptly confirm, on request, by a yes/no reply to CBPIIs whether there is sufficient coverage on a specific account to execute a specific transaction (see Article 36 (1) (c) of RTS SCA). Based on the Opinion provided by the EBA, the same service it to be provided to PISPs as well.

The availability of funds API is the basic function of the DigiTie PSD2. Customers have the option to authorize TPPs to conduct TPP coverage checks on their accounts, meaning that the DigiTie PSD2 can send a yes or no response to the TPP whether the required collateral is available on the client's account.

Support for technology providers

The regulation supports the access of technology service providers where the technology provider is accessing on behalf of a licensed operator (see Article 19 (6) of PSD2).

The DigiTie PSD2 module, as described above, assures the trustworthiness of the party on the other side of each communication link, so if a TPP is connected via a technology provider, but securely associated with its certificate, it can use the APIs as if connecting directly.

General expectations

In addition to the above, the DigiTie PSD2 still meets some other general requirements.

Change management

PSD2 requires the use of change management processes (see Article 30 (4) of RTS SCA).

The APIs provided by DigiTie PSD2 will have full documentation available to the bank, which will be upgraded prior to any additional version going live, so the bank can meet the obligation to inform imposed by RTS SCA.

Clear error messages

RTS SCA requires that in case of an unexpected error or event, an error message describing the cause of the failure be sent out (see Article 36 (2) of RTS SCA). During the creation of the DigiTie PSD2 solution, we also had to take into account the third group of users beyond the bank's customers and the bank, that is TPPs, to make them comfortable and smooth. This is in the bank's best interest since in this case fewer questions are raised by these providers, but the regulation also requires this. The standards used also support this RTS SCA requirement, and the API documentation, which is issued with the DigiTie PSD2 module, contains the error messages and their meaning in detail, with the main focus on clarity.

Transport and application security

The regulation requires that the IT solutions employed should work safely at application and transport levels (see Article 97 (3) of PSD2 and Article 30 (2) (c) 35 of RTS SCA).

When creating the DigiTie PSD2 application we have relied on our nearly 30-year banking system development experience to fully comply with bank-wide application and communication security requirements.

Traceability

PSD2 must ensure traceability of processes and events (see Article 29 of RTS SCA)

The DigiTie PSD2 system has sophisticated logging, which also provides an opportunity for traceability of processes.

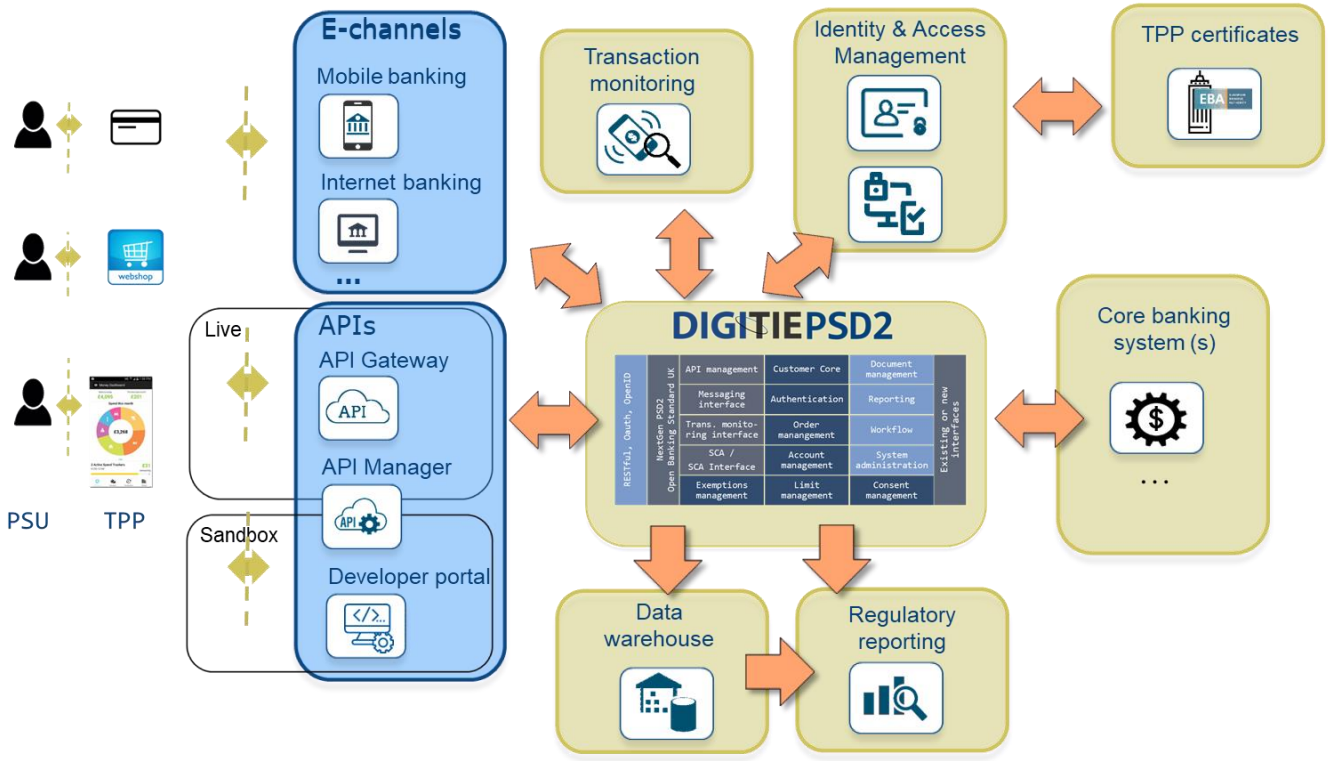
Performance and availability

PSD2's general expectation is that interfaces to TPPs should provide at least the same level of performance and availability as provided by the bank's user interface (e.g. online banking) (see Article 32 of RTS SCA).

The DigiTie PSD2 system is an important pillar of the DigiTie system designed to support digital banking. Another important leg of the DigiTie platform is the provision of 24/7 available services such as instant payment or online loan applications, so availability can easily match the level of other online channels.

The place of DigiTie PSD2 in the IT architecture

To really grasp the idea of where to position DigiTie PSD2, we provide this image:



Strictly for the basic functionalities, the goal of mere compliance and to supplement the already existing systems, DigiTie can function as a service layer with the required business logics to provide the required functionalities for the PSD2 dedicated interface.

To facilitate implementation, we have created the required interfaces for connecting to the external systems and these are part of the solution (not including the PSD2 API-s for TPPs):

Incoming (with typical source)

- User data change (e.g. new user, user deleted) (from ID management system)
- Account data change (e.g. new account for existing user, account permission change) (from core banking system)
- Manage white list (get, change) (from E-channels)
- Manage limits (get, change) (from E-channels)
- Manage consents (get, change) (from E-channels)
- Check fraud (transaction monitoring) (from E-channels)

Outgoing (with typical direction):

- Initiate payment (in core banking system)
- Cancel initiated payment (in core banking system)
- Get payment status (from core banking system)
- Request account information (from core banking system)
- Request fund information (from core banking system)
- Initiate fraud check (in TM system)
- Send user notification (through E-channels or core banking system)
- Check online status (any connected system)

Operation of DigiTie PSD2 (on-premise vs SaaS)

DigiTie PSD2 can be operated in various ways according to the needs of banks.

On one hand, our partners have the opportunity to install and operate the DigiTie PSD2 in their own IT environment (the so-called on-premise operation). This operating solution is generally preferred among our partners who have large IT developers' teams, and because of their internal policies, they want to keep IT systems running in their own hands.

In addition, our company undertakes the central operation of the DigTie PSD2 on a so-called Software as a Service basis.

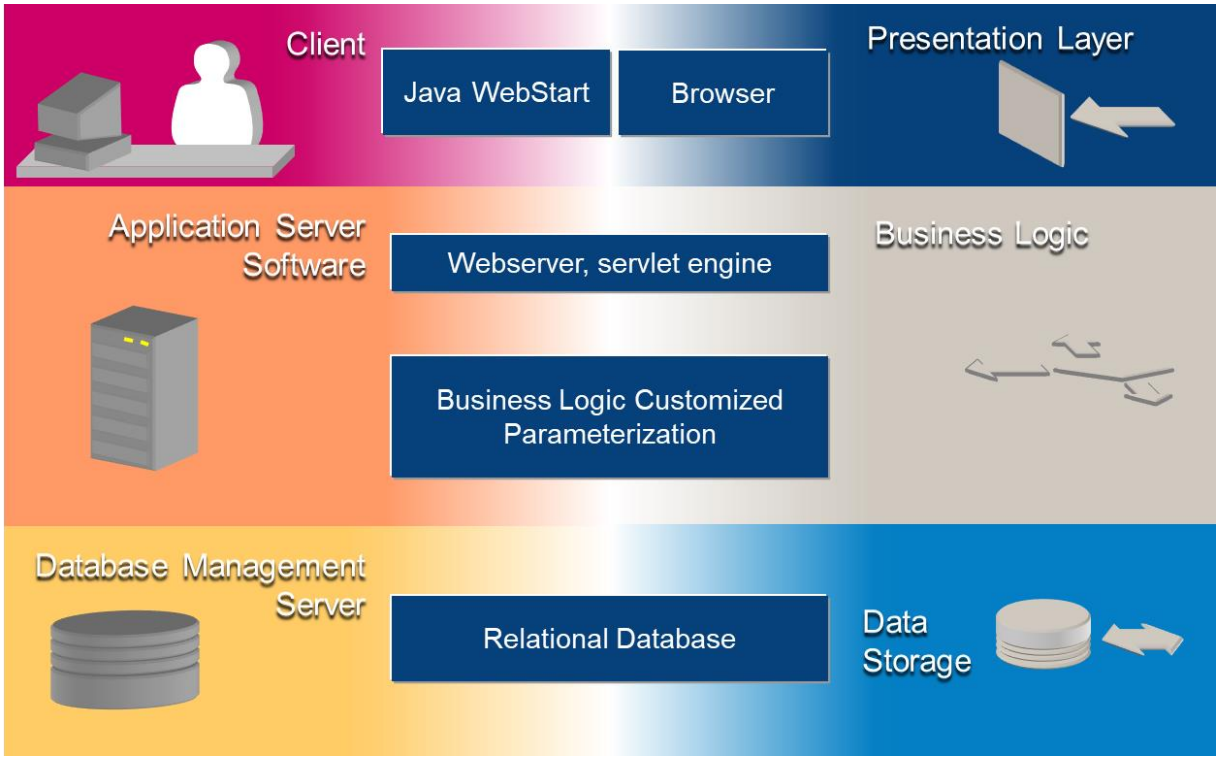
In this case, DigiTie's PSD2 operating platform is provided by our company and on this platform, we run DigiTie's PSD2 solution for several of our partners to connect DigiTie PSD2 instances with an Enterprise Service Bus (ESB) to the partners' PSD2 systems.

In relation to the operation of the PSD2 platform, our company performs the following tasks:

- creating a complete hardware architecture for DigiTie PSD2,
- installing and configuring operating systems, basic software and the DigiTie PSD2 software application both on the primary and on the disaster recovery site,
- operation of hardware infrastructure, operating systems, basic software, and DigiTie PSD2 software applications,
- creating and operating test environments,
- loading DigiTie PSD2 software releases into test or operating environments,
- establishing daily support and error-generating system environments,
- continuous monitoring of the operability of software applications,
- performance monitoring and, if necessary, intervention,
- in the event of a disaster, switching to the backup solution.

Technology

DigiTie PSD2 is based on a 3-tier architecture in which the following functional layers are defined:



DATABASE LAYER

User and business data are stored exclusively in the central relational database system. The currently supported RDBMSs are Oracle 12c or PostgreSQL 9.6. The supported database management platforms have been selected in line with the following requirements. The RDBMS should be

- platform independent so it should work under different operating systems
- widely available and widely accepted by professionals working on the fields of operation and IT audit
- robust and easily scalable
- capable of 24/7 operation with online backup procedures and remote location replication.

The development methodology applied by Online Business Technologies makes it possible that different database platforms can be supported through making changes only in the technology layer but without modifying the business logic. Due to this feature, our solutions can be easily adapted to further database management software e.g. DB2, MS-SQL.

BUSINESS APPLICATION LAYER:

All business logic runs on the application server. This layer is responsible for orchestrating the display layer, this defines the layout and the content of screens, manages screen controls for data entry and presentation, and performs checks associated with screens. A web server using a Java servlet provides the connection with the client under HTTPS protocol.

The operation of the business logic is unified, no matter if the client is a Java Webstart based or a browser-based solution (see later).

ACCESS / DISPLAY LAYER (CLIENT):

The display layer is a graphical user interface implemented under the thin client principle. This means that the client application does not store data on the client workstation and does not contain pre-installed software components. The client only manages data entry, the display of data and handles purely screen elements.

The display layer can be implemented on two different platforms:

- Java Webstart client. In the case of a Java Webstart based solution, the JAVA client program can be started from a browser or a shortcut icon placed on the desktop, and updates are managed automatically by the Java WebStart technology.
- Browser-based client. In the case of a browser-based solution, the applied technology elements are HTML5, CSS3 and Bootstrap JavaScript.

About Online Business Technologies

We are an innovative IT development company specialized in banking technology since 1989.

We provide a wide spectrum of highly flexible solutions necessary for banks to go digital, including modules to join FinTech ecosystems (e.g. PSD2, open APIs, instant payments), e-channel solutions, and state-of-the-art core banking modules to support front- and back-office operations (including account management, credits, deposit, GL etc.)

Our modules can be combined freely, we are able to deliver a standalone solution for a specific task (e.g. PSD2), or a series of modules covering the complete value chain (e.g. credit processes).

Our operations in numbers:

- Nearly 2500 years of banking, financial software development experience
- Our solutions are used by more than 8000 users
- Our solutions are used in more than 1000 branches by our customers
- Our partners serve more than 3 million customers with our solutions

OUR VALUES

UNIQUE COMPETENCE Our experience and professional knowledge in the field of credit institutions and finance is unique among IT providers.

CUSTOMIZED SYSTEMS With the help of our unique development and version management technology, our modules can be customized and implemented rapidly. We also have extensive experience in realizing unique functionality.

HIGH QUALITY Owing to the quality control system covering all of our activities and to the controlled development processes, our systems are of high quality and reliability.

QUICK RETURN Fast launching of developments that save customer resources, increased efficiency in management, flexible response to market trends – these all result in our customers gaining advantage in the rapidly changing financial market.

For more information check out our website: www.online.hu and contact us!

Online Business Technologies

H-1032 Budapest, Vályog street 3. | +36-1-437-0700 | https://www.online.hu/contact