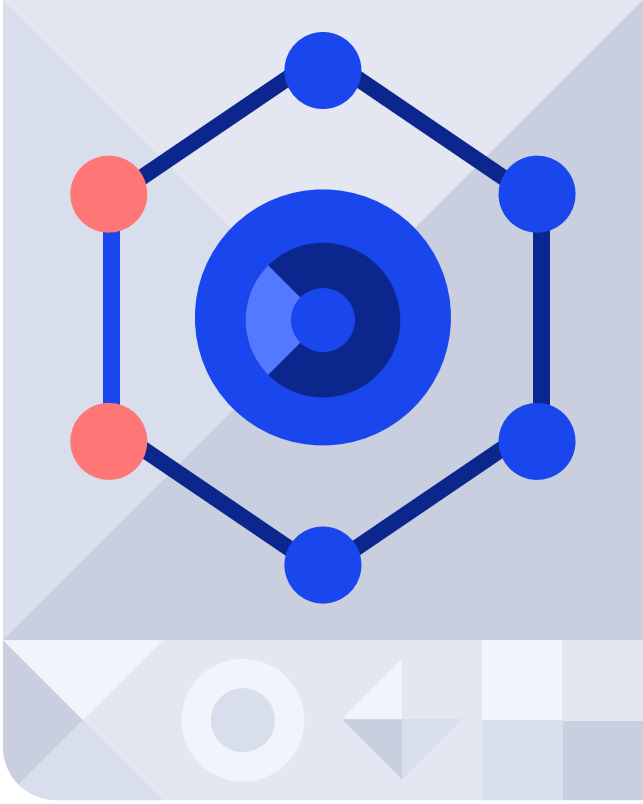
SALTEDGE

Open Banking Ecosystem in Testing Mode

Report based on testing **2000+** PSD2 account information and payment initiation APIs in **31** countries upon analysing **39** criteria

Open Banking Reality



2019 was a year of trial and error for everyone - for banks to build API channels, third party providers to unpuzzle and integrate with them, and for regulators to facilitate the process of interaction between both entities. Meanwhile, Salt Edge was positioned at the heart of it all, and continues to be, by both building and consuming PSD2 account information and payment initiation APIs.

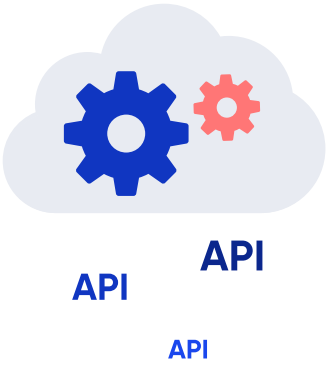
In 2020, the industry still faces the challenge to make sure that technical environments improve for the benefit of the entire open banking community.

Advancing on its path to provide a pan-European open banking ecosystem, Salt Edge has already integrated more than **2000+ PSD2** account information and payment initiation APIs, and from the other side - it has built 70+ APIs for banks and eWallets.

With the scope to inform the open banking community in Europe and beyond, Salt Edge is sharing its thorough evaluation of banks' API implementations.

Knowing inside out the specificities of all the open banking API standards (i.e. Berlin Group, UK Open Banking, Czech Standard, Slovak, STET, PolishAPI, etc.) and the strict RTS requirements, Salt Edge has created a report on testing PSD2 account information and payment initiation APIs. The report is based on the analysis of 39 criteria, which include the ease of integration, the possibility to test various scenarios in the sandbox, the overall compliance with the RTS requirements, and even how responsive to inquiries the banks are.

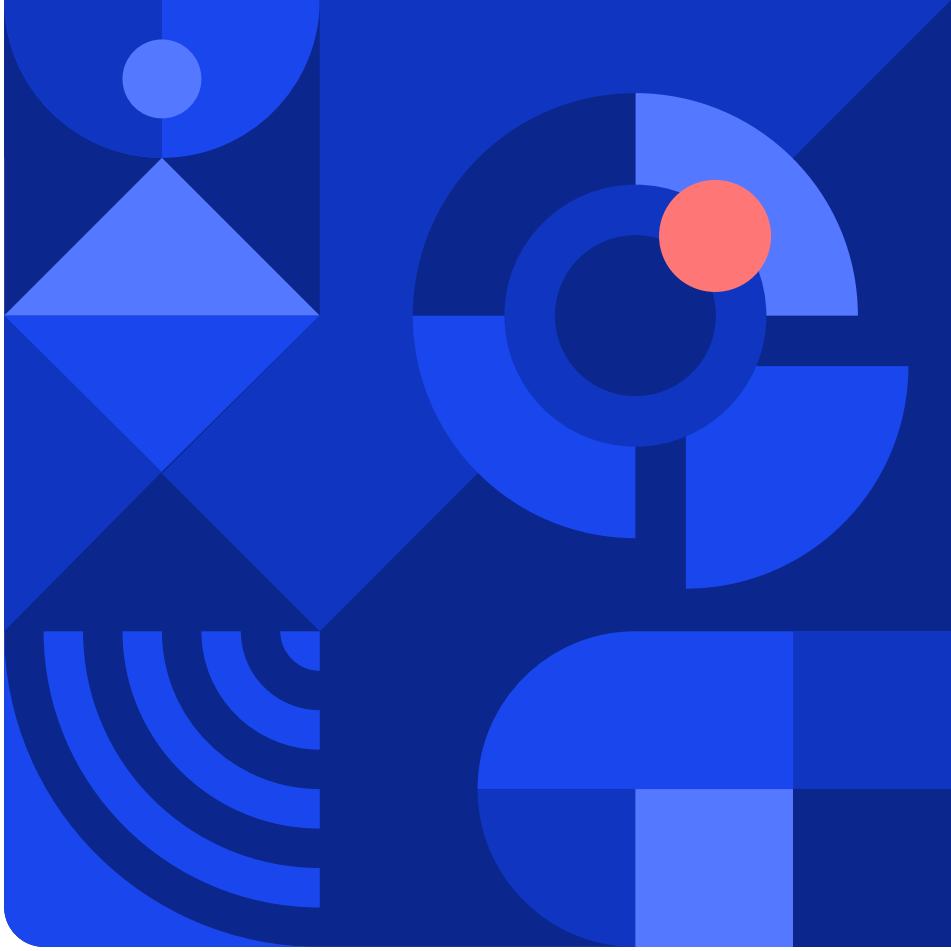
We encountered various issues while integrating with bank channels, some of them adding unnecessary friction to the process. Luckily, so far, we found the large majority of banks to be receptive to our feedback and open to improving their channels. The situation varies from country to country, with the UK leading the way.



While the Open Banking standard in the UK set explicit requirements for standard interfaces, in continental Europe the API standards (NextGen, STET, etc.) leave space for adaptations and interpretations within the same standard. This allows banks to implement custom versions of APIs, which, as a result, requires lengthy deciphering by third party providers (TPPs) in order to integrate them one by one.

Many banks look toward monetizing their APIs by building value-added offers. Therefore, they need to understand that to do so, their APIs should work seamlessly and be reliable for communication, and the process of interaction with the interface should be user-friendly. With several banks, Salt Edge was the first or among the first 3 TPPs to test their APIs. It is encouraging to see that some banks are open to listening and adjusting their interfaces.

Starting from September 2019, Salt Edge has been observing that the speed of banks' reaction, quality of documentation and availability of APIs are improving every month.



We encourage all TPPs and banks that plan to act as TPPs to share their experience, be open with banks during the integration and claim a well-functioning environment for building a business.

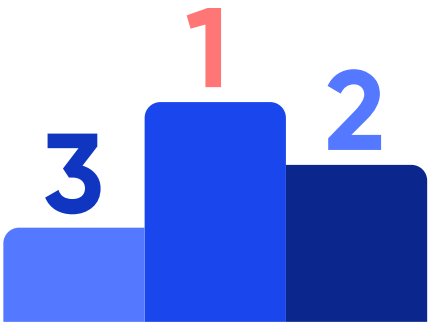
We learned that keeping a collaborative attitude from both sides helps us go through the integration more smoothly. There is a vital need for cooperation between banks and TPPs for open banking to accomplish its initial goal.

API evaluation results

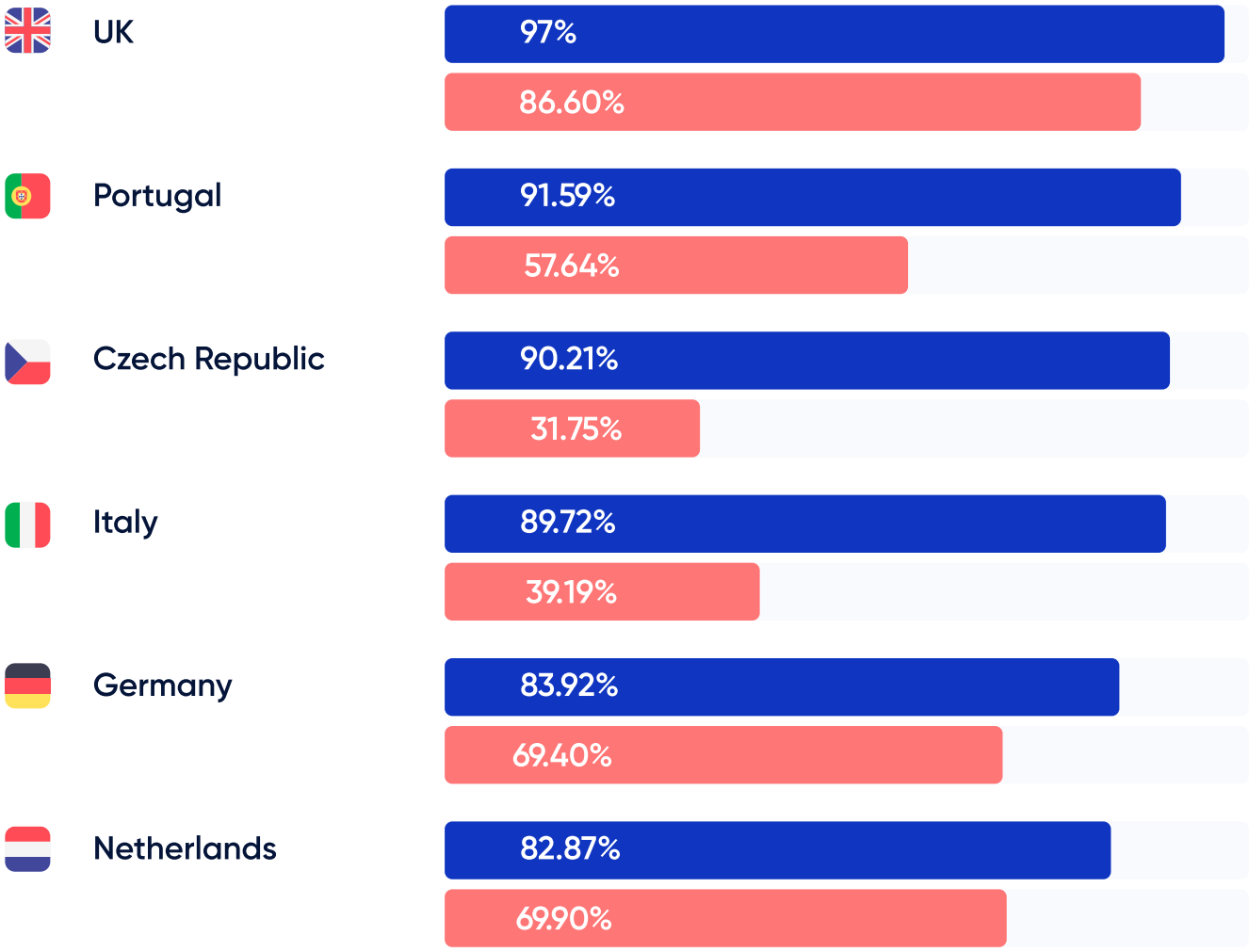
Top 6 EU countries with highest API availability

The level of tech maturity in the financial sector of different EU markets is far from uniform. Based on the API availability, the UK stands out, with the weighted average in the country being 97%. This means that during the first 3 months of 2020, out of 100 API requests we sent - in 97 cases the UK banks' APIs accepted the request. The countries with highest API availability are: the UK - 97% , Portugal - 91.59%, the Czech Republic - 90.21%, Italy - 83.92%, Germany - 83.92%, and the Netherlands with 82.87%.

These numbers take into account only whether the APIs accepted the request - i.e. the APIs were available. Yet, they do not say if the APIs responded back. The reality drastically changes when actually considering the successful response rate of these API channels throughout Europe. The biggest contrast in results can be seen in the Czech Republic, the number dropping from 90.21% (weighted average) of requests received by Czech banks and where only 31.75% of them were successfully responded to.



It's 2020 and Europe still registers mostly one-way communication from TPPs to banks. The reality is that on average, banks successfully reply back to only half of TPP requests.



Open banking heroes with up to 5-day integration

Some banks do it better than others. Integrating with the below banks was a blast: clear documentation, seamless flows, support of dynamic TPP registration, and fast communication with the support team. With some of them, the integration process actually took one day. A round of applause goes to:

UK	Revolut, Ulster Bank, LLOYDS BANK, monzo, BANK OF SCOTLAND, Danske Bank
Germany	COMMERZBANK
Finland	Nordea
Netherlands	Triodos Bank
Austria	ERSTE, Bank Austria
Romania	BCR, BRD GROUPE SOCIETE GENERALE
Czech Republic	ČESKÁ SPOŘITELNA, KB

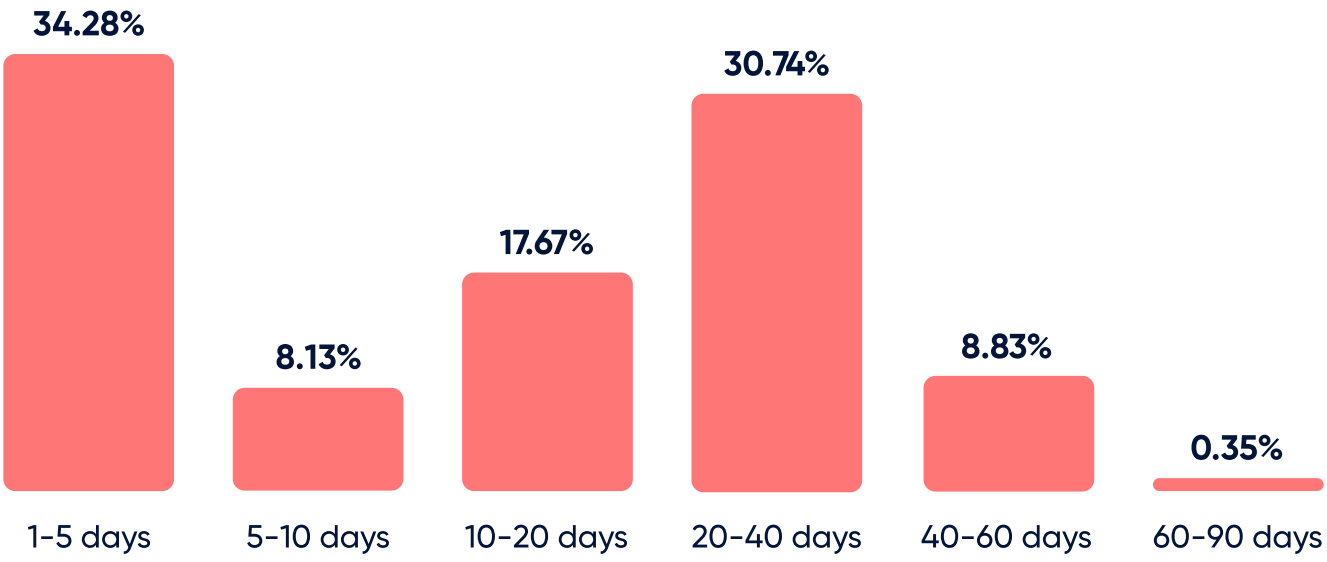
38% of APIs do not fully meet the chosen API standard

A great number of banks have implemented their **APIs without being in full compliance with the declared API standard** (e.g. NextGen, Open Banking UK). For example, having many mismatches in parameter location, formats of data, field types, etc. and these differences not being documented anywhere. Only after a lengthy discussion with the bank representative, these mismatches were identified.

One big group of banks from Germany publicly announced that it has migrated from a custom API implementation to Berlin Group standard without mentioning that it is only for the sandbox environment and the migration for production is planned for the next 6 months. Thus, after Salt Edge went through all the adjustments for the migration to match Berlin Group standard, the bank 'confessed' that it is not yet in production and as a result Salt Edge had to revert to previous implementation.

42% of API integrations required less than 10 days

In regards to integration time, many factors greatly influence the speed of integration, like how fast the banks' support answer, whether the documentation is clear and contains all the necessary parameters, the language of the documentation, and many more. We encountered various bugs and assisted the banks in solving them. It has been an ongoing process of collaboration with banks to help them adjust their APIs and move closer to compliance.

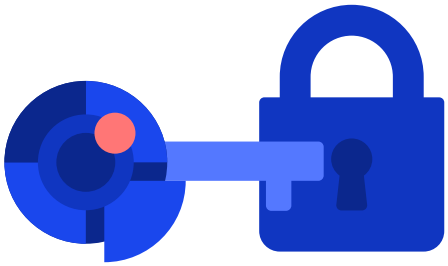


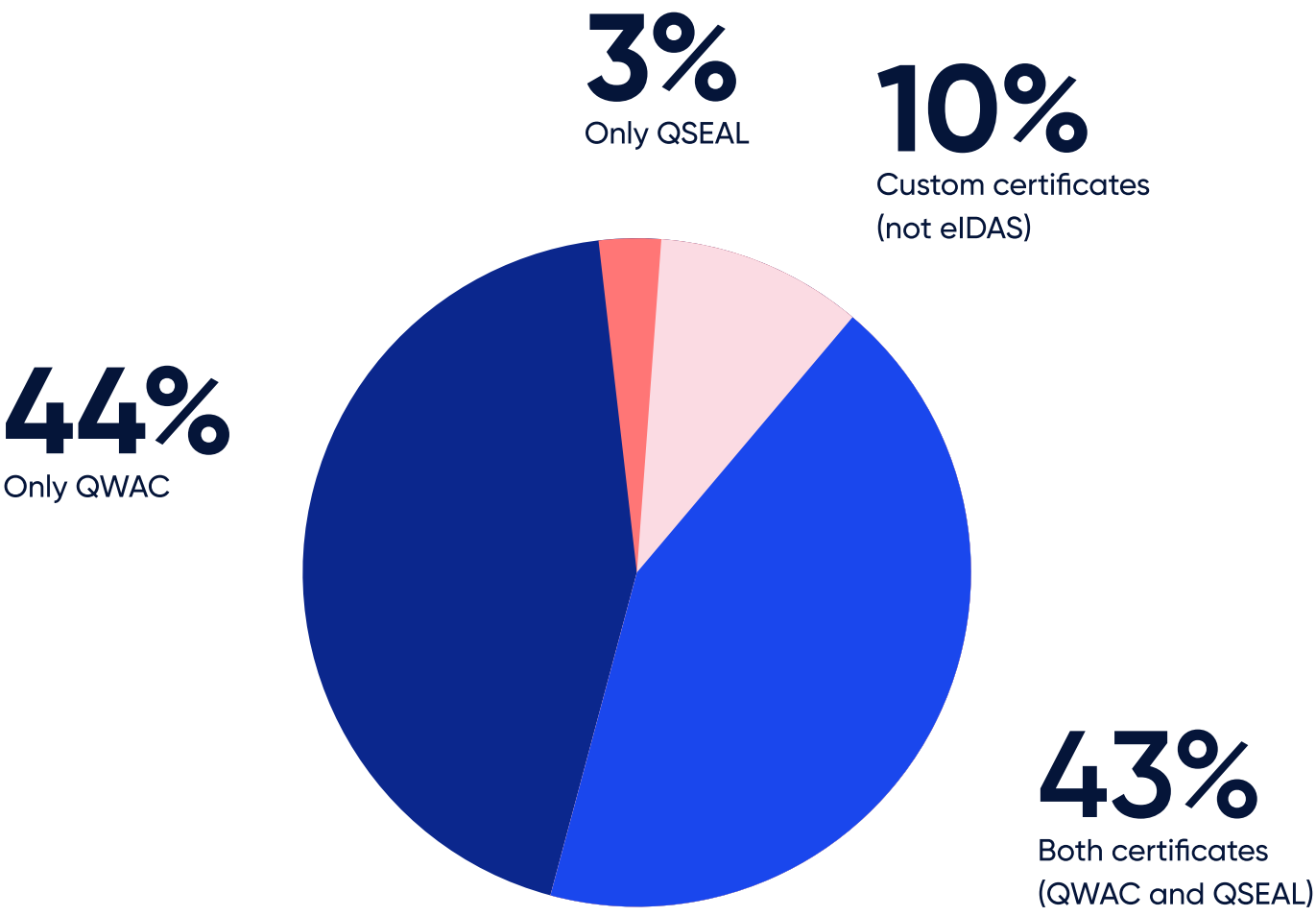
Time for integrating bank APIs

43% of APIs request both QWAC and QSEAL certificates for identification

Is it a big number? To answer this question, let's examine the role of each certificate.

QWAC guarantees confidentiality (nobody else could have read the data) **and authenticity** (that the data was not changed between the endpoints) of the information transferred through the API. **QSEAL is used for signing requests**. The entity receiving digitally signed data can be sure who signed it and that the data has not been changed since being signed. Unlike QWAC, QSEAL can **trace and log the communication sessions**. We can conclude that for the benefit of the customers' data security, traceability of TPPs' actions and confirmation of their identity, ideally, all banks should require both QWAC and QSEAL certificates (for **more insights**). Unfortunately, we identified banks that did not require any type of qualified identification certificate.





Banks' choice for TPP identification certificates

In regards to eIDAS certificates, there are banks across Europe that only accept certificates issued by specific QTSPs. This limitation can stop the integration process entirely until banks implement adjustments on their side.

57% of banks support dynamic TPP registration

Dynamic registration represents an automatic method of registering with the bank's platform to gain access to the relevant APIs. This type of registration can entirely eliminate lots of manual work such as the need to create an account in the bank's developer portal, manual fill-in data, and email exchanges. Dynamic registration means presenting a valid TPP eIDAS certificate and in return receiving a set of instructions to start the integration with the API, both sandbox and live environments.

Dynamic registration makes a big difference at scale. Imagine a big group of banks with branches in many countries and having to manually register with each of them separately. And now, take into account that in Europe there are 6000+ banks. It may take months. With dynamic registration you can get access to them all at once. But in order to use this feature, TPPs' technical service providers should have a mechanism in place to dynamically register with banks. For example, Salt Edge API supports dynamic registration and enables its clients to connect with banks faster.

46% of banks don't offer the possibility to test various scenarios

A good service implies, besides solving a problem, having seamless connection and user-friendly flow. To offer qualitative services, third parties need to test their apps before providing the service to customers. And this is the role of sandbox - to enable third parties to conduct functional testing of their applications and understand how they interoperate with the bank's interface.

Unfortunately, up until now only 20% of integrations offer the possibility to test API errors and only 54% of banks enable testing multiple use cases. The rest of banks' sandboxes can be quite useless due to limited testing cases - supporting only a set of predefined requests and parameters, while giving the same mocked response to any request.

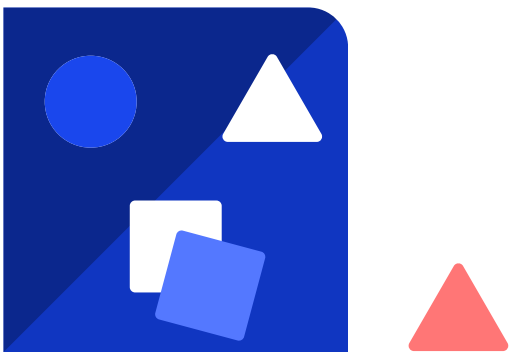
Another striking example that impeded the testing process was the requirement to be in the bank's intranet (physically be there) to generate and receive the one-time password (OTP) for SCA testing.

63% of banks have similar sandbox and live environments

For obvious reasons, the live environment of a bank API should be as close as possible to the sandbox environment. And yet, 37% of 2000+ integrated APIs do not have similar environments.

The most prominent discrepancy that we encountered was a group of banks having the sandbox in an upgraded API version and the live environment in an older one. Another, already common factor that differentiates the two environments is strong customer authentication (SCA) implementation. Quite often, the SCA flow in production is different from what was tested in sandbox.

This implies that TPPs may launch their service with possible errors and will be able to identify and correct them only after end-users report a problem. Consequently, the services offered by TPP can be of bad quality due to discrepancies between environments created by banks.



18% of APIs require several SCA journeys to integrate just 1 payment account

18% of API integrations, specifically banks in Italy, Poland and in some other countries, require separate consents for accessing different types of data of the same account, for account information purposes. Each consent is accompanied by strong customer authentication.

Here is a simple example of the AISP journey for an end-customer that wants to connect 2 bank accounts (1 current account and 1 card account for transaction history going back to more than 90 days) to a third party app:

1. **Go through SCA to get the list of bank accounts**
2. **Go again through SCA steps to get the list of cards**
3. **SCA to get the balances of current account and history of transactions for more than 90 days**
4. **SCA to get the balances of card account and history of transactions for more than 90 days**

If an end-customer has more than 2 payment accounts in the same bank, there will be more authentication flows, at least one for each additional payment account.

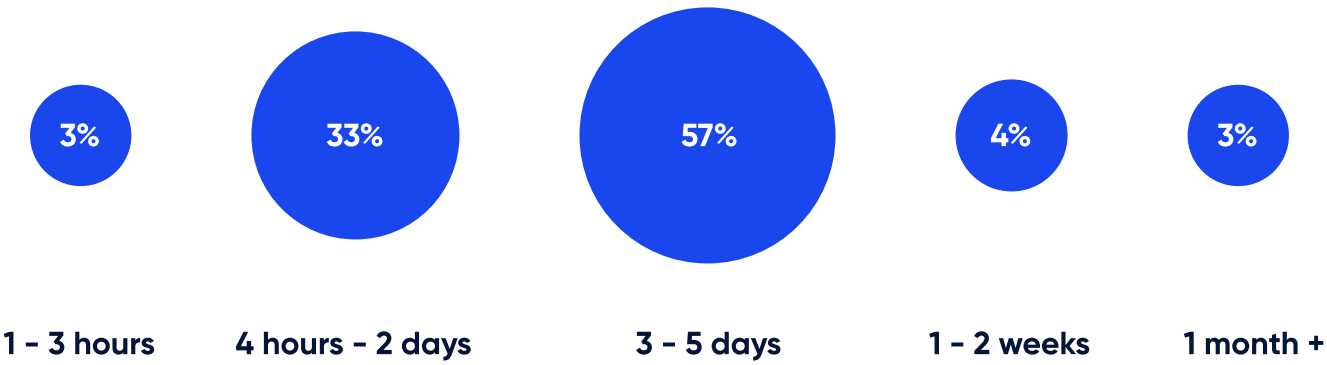
Going through the same authentication steps multiple times in order to connect a single end-user account for data aggregation purposes adds friction to user flow. As a result, based on PSD2 - it represents an obstacle for TPPs in providing payments services.

57% of banks reply to inquiries in 3 - 5 days*

During this marathon of integrating APIs, with some tech experts from banks we've become well-acquainted. Chats on Slack, WhatsApp, email conversations and daily phone calls helped in speeding up many processes. The best experience was when we didn't even have to contact the bank.

Nevertheless, the support team of more than half of the banks could take several days to respond. As inquiries could go from banks to their technical service provider that built the API and then back to Salt Edge, the overall process often led to misinterpretation.

*The banks that did not reply at all were not integrated yet, thus not included in this report.



Banks' response time to inquires

22% of integrations come with faulty documentation

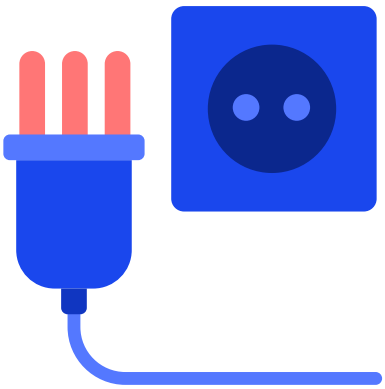
The documentation is the instruction on how to integrate an API. The more complete it is, containing all the necessary parameters, the less interaction is needed with banks' support. We encountered documentation with the same information being doubled in different places but with mismatches. Others come in PDF format, only 2 pages long, and with missing information. Several banks actually had the documentation in SDK format, so third parties have to reverse engineer it in order to read it - definitely adding extra friction.

A bank would, in general, have the documentation in two languages but each of them for a different API version and without mentioning which one is the latest one. We also notice improvements; some banks that initially had the documentation in the local language, now have it in English as well.

39% of banks have broken endpoints in their developer portal

While integrating with the banks' APIs, we encountered many broken endpoints.
Just some of the many examples are:

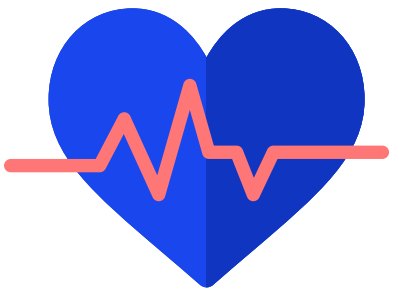
- Being unable to log out from the developer portal
- Filling-in the developer portal registration form and afterwards not being able to submit it
- Contact form not working
- Impossibility to create a 'testing app' account in the developer portal of the bank in order to receive the testing identification certificate - due to inactive links



28% of APIs had downtimes during the integration

When downtimes happen while the sandbox is being integrated, it results in lengthening the process by hours, days or even weeks. While API downtimes are not critical for sandbox environments, it can be alarming when it happens in production environments - especially without notifying third party providers. There are good examples of advance notification for planned downtimes being applied by several banks (UniCredit, Nordea, DNB, etc.) or even notification of unplanned downtime were sent by Credit Agricole, Volks Raiffeisenbanks, Banca Sella, TSB and others.

Most banks do not have any mechanism for notifying about unplanned and even planned downtimes. This contradicts the RTS requirements (Article 32 and 33).



51% of banks do not accept test certificates in their sandbox

There can be three approaches toward TPP identification in a sandbox:

1

The first case is when, after registering with the banks' portal, the banks generate their own test certificates for TPPs. These certificates usually do not contain specific identification information about the TPP or their PSD2 licence. When this approach is used, banks do not support and do not accept eIDAS test certificates.

2

The second approach is when the banks accept exclusively production eIDAS certificates. It might be a burden for those TPPs that don't currently have an eIDAS certificate or are in the process of registration or authorization with national authority, but want to test banks' sandbox.

3

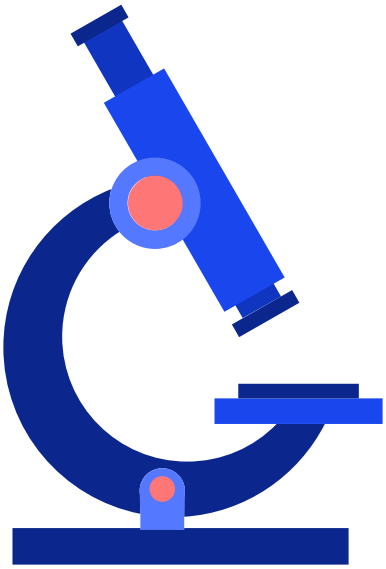
The third approach is when the bank accepts both TPP's test or production eIDAS certificates for identification.

The first and second approaches are adopted by 51% of banks.

Methodology

Salt Edge has conducted the evaluation of 2000+ PSD2 account information and payment initiation APIs from 31 EU countries, against 39 criteria, while integrating these channels. The most interesting findings are presented in this report - with the goal of informing market players of the current situation of the banks' PSD2 readiness across the EU.

To maintain an objective and equidistant approach, the criteria of analysis were chosen to be technical and clear, and thus - to exclude human factor errors. For certain calculations, weighted average was computed as not to have skewed responses toward the countries that have more banks compared to those with less banks.



About Salt Edge

Salt Edge is a financial API platform with PSD2 and open banking solutions. The company has two main vectors of activity: enabling third parties to get access to bank channels via a unified gateway, and developing the technology necessary for banks to become compliant with PSD2 requirements.

ISO 27001 certified and AISP licensed under PSD2, the company employs the highest international security measures to ensure stable and reliable connections between financial institutions and their customers.

Connected to 5000+ financial institutions from 70 countries worldwide and built 70+ PSD2 APIs

Trusted by 100+ financial institutions

Salt Edge solutions that empower financial institutions to benefit from PSD2

Open Banking Gateway

The Gateway allows businesses to have access to payment accounts of their end-customers from EU and beyond, for aggregation of data and payment initiation capabilities, via one simple integration. The solution incorporates data enrichment services like transaction categorization, merchant identification, and financial insights which adds real value to raw data.

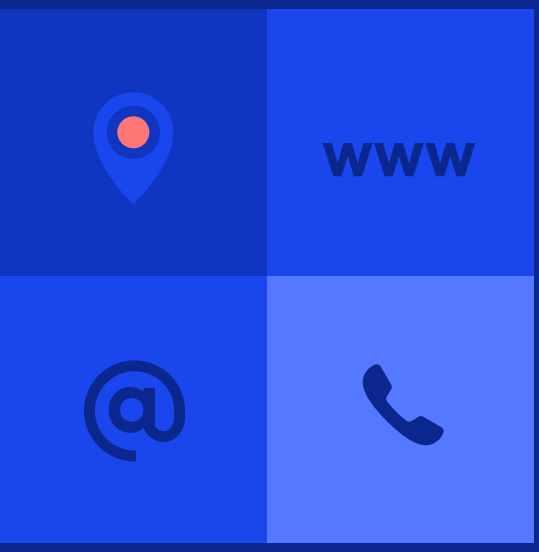
In case the client does not have a PSD2 licence, Partner Program is the solution that empowers them to connect in a secure and compliant manner to the desired banks across Europe.

PSD2 Compliance Solution

PDS2 Compliance solution enables banks and eWallets to become compliant with the regulatory and technical requirements in one month: from API provision to meeting SCA requirements, TPP verification system, and consent management API. It is a cloud-based solution allowing institutions to spend minimal resources on integration and further maintenance. The system updates, monitoring, and support is handled by Salt Edge.

We are happy to **show you** how Open Banking Gateway works and which are the advantages of PDS2 Compliance Solution.

SALTEDGE



+44 2039 363505

sales@saltedge.com

www.saltedge.com

Level 39, One Canada Square,
Canary Wharf, London E14 5AB, UK