REVISED
2020 EDITION

THE TRICKY ENCOUNTER

A Norfico and Konsentus White Paper about the connections between Financial Institutions and Third Party Providers under PSD2

NORFICO
NORDIC FINTECH CONSULTING

Konsentus

TABLE OF CONTENTS

Overview of abbreviations	3
Foreword	4
Setting the scene	6
Identifying and authenticating TPPs	7
The EBA registers	7
Whose responsibility?	8
National or European coverage	8
A matter of security	9
Digital certificates	9
Who issues the certificates?	10
What if a certificate must be revoked?	11
Conclusion - the business implications	12
Top 5 issues that ASPSPs need to consider	13
QWACs and QSealCs explained	14

Overview of abbreviations

AISP	Account Information Service Provider
API	Application Programming Interface
ASPSP	Account Servicing Payment Service Provider (e.g. a bank)
EBA	European Banking Authority
EEA	European Economic Area
eIDAS	Electronic Identification, Authentication and Trust Services
NCA	National Competent Authority
PISP	Payment Initiation Service Provider
PSD2	The Revised Payment Services Directive
QSealC	Qualified electronic Seal Certificate
QTSP	Qualified Trust Service Provider
QWAC	Qualified Website Authentication Certificate
SCA	Strong Customer Authentication
TPP	Third Party Provider

Foreword

The EU's revised Payment Services Directive – PSD2 – is probably one of the most ambitious and impactful pieces of legislation ever to be enforced in the European financial industry.

Not surprisingly, the implementation across Europe comes with a high degree of complexity and offers many challenges. Some of these challenges have to do with the introduction of new roles in the industry, others are due to the obligations and liabilities attached to some of these new roles. The remaining challenges result from the rather tricky new encounters between some of the players, notably the so-called Third Party Providers (TPPs) and the European Financial Institutions (i.e. Credit Institutions (banks), Payment Service Providers (PSPs) and Electronic Money Institutions (EMIs)), which, in PSD2 terms, are referred to as Account Servicing Payment Service Providers (ASPSPs).

The crux of the matter is that PSD2 allows a TPP to gain access to an ASPSP's customers' payment accounts - provided customer consent has been given. However, if something goes wrong, liability typically lies with the ASPSP. For instance, if it turns out that account access is given to a TPP who isn't who it claims to be, and fraudulent transactions take place, the ASPSP would be liable.

PSD2 was adopted by the EU Parliament as early as October 2015 and entered into force in January 2016. The European Banking Authority (EBA) initiated discussions on The Regulatory Technical Standards (RTS) in December 2015. These continued to 2016 with the final draft of the RTS for Strong Customer Authentication and Common and Secure Communication[1] (RTS for SCA and CSC) being released in February 2017 and approved by the EU in September the same year. Apart from some delays in implementation of SCA, all regulatory requirements put in place by PSD2 are now in effect. This means that the financial services market has moved beyond a general compliance race to a much more diverse situation where TPPs are now starting to deploy and grow their services on a much wider scale.

Around the time of the EBA market consultation on the draft standards in 2016, the founders of Konsentus started to wonder how the new directive would eventually cater for a completely new situation when - somewhere down the road - presumably thousands of new TPPs would knock on the doors of the c. 6,000 European banks asking for access to accounts – as granted to them by the new directive.

>>back to content

The Konsentus TPP Identity and Regulatory checking service was built on the idea of developing adequate services for ASPSPs and to help make their encounters with TPPs less tricky.

In 2017, the Danish fintech consultancy Norfico started asking the same questions as Konsentus had and wrote the first version of the White Paper The Tricky Encounter[2]. In this new version of the White Paper written in collaboration by Norfico and Konsentus, we intend to deliver an updated overview of the current situation for TPPs and ASPSPs in this new Open Banking ecosystem.

As we will see, even though the EBA and the National Competent Authorities (NCAs) across Europe, who are together responsible for paving the way and enabling Financial Institutions and TPPs to engage under safe conditions, there are still open questions and challenges that need to be resolved.

Currently, only 30% of the European Economic Area's (EEA) ASPSPs have implemented dedicated interfaces for TPPs, clearly showing that we still have a very long way to go before PSD2 and access to accounts is working in practice as intended.

As part of this revised White Paper, we have included a list of recommendations. These recommendations are written mainly for ASPSPs as the liability lies with them for any fraudulent activity that takes place as a result of an encounter with a TPP going wrong. However, the rest of the White Paper is as relevant for the other side of the encounter – the TPPs – as well as for the regulators across Europe.

Please do not hesitate to contact Norfico or Konsentus with any questions regarding the content of this White Paper.

Happy reading!
Konsentus & Norfico

1. https://norfi.co/TE2
2. https://norfi.co/TE1

>>back to content

Setting the scene

According to the Revised Payment Services Directive (PSD2) - Article 66 and 67 - all European ASPSPs must comply with the Directive's requirement for Access to Accounts. What this means is that ASPSPs must grant Third Party Providers (TPPs) access to their customers' payment accounts (with prior consent from the customer), unless the ASPSP believes a TPP to be unauthorised or fraudulent.

This might sound relatively simple, but a closer look at the implications of these requirements and the foundations for complying with them reveals a high degree of complexity.

The encounter between ASPSPs and TPPs raises a lot of complicated questions and in this White Paper we intend to shed some light on those which are most important.

Despite the fact that these encounters take place every day, the main questions are still related to how an ASPSP ensures that a TPP is who it claims to be and that the TPP has the rights to access a consumer's payment account for account information or payment initiation.

ASPSPs carry a heavy security obligation on behalf of their customers (the Financial Institution account holders) when allowing access to an account. On top of the security related matters comes the importance for an ASPSP to ensure that it will not damage its reputation or the trust of its clients - a trust that in many cases has been built up over many years.

The European Banking Authority (EBA) has established a pan-European register of TPPs which Financial Institutions may use to identify TPPs. This central register however is dependent on NCAs for input and the quality of their registers is still questionable. A register with TPP names on it does not, on its own, provide assurance that the TPPs knocking on the ASPSP's doors are who they claim to be.

Something more than a list was needed so it was decided to use eIDAS[3] certificates to identity the TPPs. But despite this decision, a lot of issues remain about eIDAS certificates and how to use them - more on this later in the paper.

These might seem like technicalities, but looking further into these questions, it becomes clear that they touch on somewhat fundamental and yet unsolved problems which could potentially have a major impact on a Financial Institution's business.

3. eIDAS (Electronic Identification, Authentication and Trust Services) is an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. It was established in EU Regulation 910/2014 of 23 July 2014 on electronic identification [Wikipedia]

>>back to content

Identifying and authenticating TPPs

One of the core questions is the still unresolved problem of how European ASPSPs can easily and securely identify TPPs wanting to obtain access to Financial Institutions customers' payment accounts following PSD2's Article 66 for Payment Initiation Services Providers (PISPs) and Article 67 for Account Information Services Providers (AISPs):

> Article 66. **Rules on access to payment account in the case of payment initiation services.** 1. Member States shall ensure that a payer has the right to make use of a payment initiation service provider to obtain payment services as referred to in point (7) of Annex I. The right to make use of a payment initiation service provider shall not apply where the payment account is not accessible online."

And:

> Article 67: **Rules on access to and use of payment account information in the case of account information services.** 1. Member States shall ensure that a payment service user has the right to make use of services enabling access to account information as referred to in point (8) of Annex I. That right shall not apply where the payment account is not accessible online."[4]

4. https://norfi.co/TE3

The EBA registers

Article 14 of the PSD2 directive mandates the member states to establish a public register of "authorised payment institutions and their agents". This register of approved TPPs, who can obtain access to European Economic Area (EEA) Financial Institutions' customer accounts (provided the account holder has given his or her approval), should be based on national registers provided by the NCAs in all the member states, and each should be updated "without delay" whenever a change occurs.

The following article (15) appoints overall responsibility for the register on a cross-European level to the EBA.

The European Banking Authority (EBA) now publishes two registers of Payment Service Providers (PSPs) that can act as Third Party Providers (TPPs), as defined by the Second Payment Services Directive (PSD2):

- Payment institution register
- Credit institution register.

These registers contain information provided by the 31 NCAs of the EEA which are the legal entities responsible for regulating the financial conduct of Payment Service Providers established within their home Member State.

According to the EBA, the purpose of these registers is to 'increase transparency and ensure a high level of consumer protection' within the European Single Market.

Whose responsibility?

Unfortunately, the good intentions with these registers have so far turned out to be difficult to realise in practice. When looking at how the registers are created, maintained, and updated, and how the liability is organised, several overall problems become evident. As we will show, even though it is now more than two years since the EBA submitted the draft RTS on SCA and CSC under PSD2[5] to the Commission, the quality of the registers is still debatable.

Despite the registers being available on the EBA's website, the EBA does not assume responsibility for updating them nor for the quality of the content. On its website, the EBA has a disclaimer covering the Payment Institution Register and a similar one for the Credit Institution Register:

> "The present Register has been set up by the EBA solely on the basis of information provided by national competent authorities of the EEA Member States. Therefore, unlike national registers under PSD2, this **Register has no legal significance and confers no rights in law**. If an unauthorised institution is inadvertently included in the Register, its legal status is in no way altered; similarly, if an institution has inadvertently been omitted from the Register, the validity of its authorisation will not be affected."[6]

Early on, the EBA stated that it did not have the resources needed to ensure that the central registers were updated instantly. Responsibility for maintaining the central registers and ensuring all changes and updates are made, therefore needed to lie with alternative organisations.

The NCAs were assigned the responsibility. It was - and still is - unclear how well and efficiently these tasks are being performed. The NCAs rarely have experience in operating systems for handling automatic updates of a central European registry - let alone in real-time - to fulfil the requirement for updates and notifications "without delay". These registers have in general been designed with the end-consumers in mind. Having an online service where an EU citizen can access a list of licensed TPPs via their browser is one thing, but it is quite another to have an industrial-grade online database that ASPSPs can access in real-time for transaction authorisation.

National or European coverage

Maintaining central real-time, industry-grade online registers is not a simple task, and even though we called in our original paper for a central independent specialist body, this has not happened. However, the EBA has established technical standards for member states for the registration and distribution of TPP data and updating the EBA's central registers, with the aim of ensuring consistent procedures across all the EEA countries.

However, even though member states all have national registers[7], the limitations of these must be recognised.

For instance, some NCAs only keep currently authorised TPPs on their register. They completely remove a TPP record from their register if, and when, that TTP's authorisation has been withdrawn. This only enables ASPSPs to check the current regulated status of a TPP and not what its status was in the past, which can make dispute cases difficult to manage.

5. https://norfi.co/TE11
6. https://norfi.co/TE5
7. *The full list can be found here:* https://norfi.co/TE5

>>back to content

Another major issue is related to the TPPs' right to passporting – i.e. taking their licence from one country to another within the EEA. If a TPP wants to passport its license, it must notify its 'home country NCA' about which countries it wishes to service. The home country NCA then notifies the NCAs of all the other countries where the TPP wants to offer its services. If the other member states do not object, the TPP is free to provide services in the other member states. But these rights to passporting are not included in the issued eIDAS certificates and experience shows that the national registers do not necessarily contain complete and updated passporting information. If an ASPSP were to do proper validation of the passporting rights, it would need to check the NCA registers of both the TPP's and the ASPSP's home country.

Finally, the current availability of the registers is far from financial services grade standards. Between November and December 2019, NCA register uptime was below 99% for 7 of the 31 NCAs, with the lowest up-time being only 82%.[8]

8. *Source: Konsentus system monitoring*

These problems may seem inconsequential, but the fact is that in a situation whereEuropean Financial Institutions are unable to perform a fast and trustworthy assurance of TPPs wanting access to customer accounts, they may face serious difficulties meeting the requirements of PSD2.

A matter of security

Obviously, ASPSPs cannot jeopardise security by opening up their APIs to TPPs unless they have absolute certainty of their identity and regulated status. However, as shown above, the quality of the registers to enable confirmation of the identity and regulated status to take place still leaves quite a lot to be desired.

But the problem presented is even more complicated than this. Just getting the registers in place doesn't solve the problem of verifying a particular TPP's identity and rights. The register only addresses one part of the problem. ASPSPs still need to be able to ascertain whether a TPP, claiming to be one of the TPPs recorded in the register, is actually that TPP.

Following Article 15 in PSD2, the "EBA shall make the register publicly available on its website," and since this means that anybody can find the names of the TPPs registered and claim that they are one of them, a secure authentication method and procedure is needed for the ASPSPs to ensure that the TPPs are who they claim to be.

Digital certificates

The directive itself does not suggest any method in particular to securely establish the identity of a TPP knocking on an ASPSP's door. This has led to discussions about how to efficiently implement the support for proper authentication of TPPs.

The EBA organised a workshop in April 2016 with the participation of ASPSPs and TPPs. Three different kinds of certificates were discussed, but one was highlighted as the preferred option:

> Option 1: website certificates issued by a qualified trust service provider under an eIDAS policy, that would, in particular, include the name of the institution, its licensing number, the competent authority that has delivered the license, and the services provided by the PSP"[9]

9. *https://norfi.co/TE7, p. 21. Option 2 was: "website certificates issued by a general Certificate Authority." And option 3 was: "bilaterally agreed certificates."*

>>back to content

This option since became part of the RTS for SCA and CSC[10], specifying that for the purpose of identification, payment service providers shall rely on qualified certificates for electronic seals as referred to in article 3(30) of the eIDAS Regulation[11] or for website authentication as referred to in article 3(39) of the same regulation.

The EBA further clarified their opinion on the use of eIDAS certificates[12] which was that two types of eIDAS certificates could be used: QWACs[13] and QSealCs[14] and recommended the use of both. The choice lies with ASPSPs as they have the responsibility for the security of the communications. (See fact box for more information about the two types of certificates).

However, while these certificates - especially in combination - ensure identification and secure communication, they do not contain up to date information about the current status and rights of the TPP holding the certificate.

Yet another unsolved problem is that the issued certificates can be valid for up to two years but, may not be updated to reflect any changes in the legal status and rights of the TPPs. This again limits the purpose of the certificates - to purely being identification of TPPs but not authentication of their rights to interact with ASPSPs.

Who issues the certificates?

One of the challenges remaining is that QTSPs can issue a range of certificates; some of these come under the eIDAS standard, others do not.

Also, not all QTSPs are regulated and approved to issue PSD2 eIDAS certificates (which have been modified for PSD2 purposes). This is causing confusion, not only about how to use the certificates, but also about who are the approved QSTPs that can issue PSD2 eIDAS certificates to TPPs. The EBA has an informal list on its website of QTSPs approved to issue PSD2 eIDAS certificates, but not a formal trusted list for online verification.

Furthermore, we have observed that even when QTSPs are approved to issue PSD2 modified eIDAS certificates, in some cases they are struggling to get the right reference or identification number for a TPP. This is due to it currently being unclear as to where to get this information. Some go to the EBA register, others to the national NCA register. Even though you would expect the ID format to be the same, we have seen cases where the identification number for the same TPP differs between the registers which again complicates the authentication processes for ASPSPs.

10. *https://norfi.co/TE2, Article 34(1)*
11. *https://norfi.co/TE8, Article 3(30) of Regulation (EU) No 910/2014 (eIDAS Regulation)*
12. *https://norfi.co/TE10, EBA-Op-2018-7 - Opinion of the European Banking Authority on the use of eIDAS certificates under the RTS on SCA and CSC.*
13. *Qualified Web Authentication Certificate certificates validate the identity and role of a TPP, while encrypting and authenticating sensitive data.*
14. *Qualified eSeal Certificate certificates "seal" app data, sensitive documents and other communications to ensure they are tamperproof and originate from a trustworthy source.*

>>back to content

In fact, if ASPSPs are trying to provide an in-house TPP checking solution, they would need to establish connectivity with over 70 QTSPs for identity verification and access over 117 registers across 31 NCAs and the EBA registers to verify a TPP's regulated status. Obviously, this stop-gap solution of manually checking every single TPP will fall short very soon when the number of approved TPPs starts increasing all over Europe.

Despite the fact that eIDAS certificates are an important innovation, their use adds even more complexity to the ASPSP's handling of the increasing number of new TPPs approaching them for access to customers' payment accounts.

Finally, obtaining the correct certificates can also prove to be a challenge for TPPs as the EBA has only provided high-level guidance for TPPs about where to obtain eIDAS certificates. TPPs would benefit from a list of QTSPs approved to issue eIDAS certificates and information about the procedures.

What if a certificate must be revoked?

Who is going to monitor issued certificates across Europe? Is it the NCAs who will follow the EBA's advice on requesting revocation of eIDAS certificates? And how do we know that they are acting on this advice if a TPP's regulatory status has changed and therefore their certificate needs to be revoked?

While the procedures will inevitably vary from NCA to NCA, the most likely scenario will be that the NCA will primarily respond in a reactive rather than proactive manner if, and when, they receive complaints from ASPSPs or consumers.

The fact that a TPP qualifies for a certificate at a certain point in time does not mean that it still meets the requirements a year or two later. For example, if a TPP goes out of business or its regulatory status changes, it should request its certificates to be revoked by its QTSP. However, this can be a time consuming and expensive activity and may not be a high priority for a TPP.

It is the QTSP who can technically revoke a TPP's certificates, but it will only do this when requested by, either the TPP or, the NCA where the TPP is registered. Although QTSPs will check the status of a TPP when the certificates are issued, they have no obligations to monitor the regulatory status of TPPs thereafter.

The uncertainty related to managing certificates leads to new questions that ASPSPs need to ask themselves before opening the door to an unknown TPP. It is not enough for an ASPSP to rely only on a TPP's eIDAS certificates. They also need to check the current regulatory status of the TPP which can only be done by looking on the NCA registers. This will give the ASPSP the evidence required as to why a request for account access may be rejected.

>>back to content

Conclusion - the business implications

As the discussion above shows, the complexity of managing the many potential issues and immature processes and procedures related to the encounters between TPPs and ASPSPs is extremely high. ASPSPs are mandated to open up access to account data to TPPs while at the same time assuming all the risk. Disregarding the challenges is not an option.

In the UK, we are already seeing a significant number of TPPs making use of the new Open Banking option of getting access to consumers' accounts to provide innovative and competitive services. As at January 2020, 168 TPPs were authorised to operate in the UK market – 116 domestic and another 46 with the ability to passport services in from other countries. Also, many more were awaiting regulatory approval from the UK Financial Conduct Authority (FCA).

In terms of transaction volume, in January 2020, over 321.3 million Open Banking transactions were conducted in the UK[15]– showing an average monthly increase of more than 30%.

15. https://norfi.co/TE9

One of the essential prerequisites for a successful roll-out of PSD2 is a rock-solid and highly efficient system for identifying and verifying the regulatory status of TPPs during their interactions with ASPSPs. Whilst many countries are seeing low volumes of transactions with registered TPPs, this currently isn't seen as a critical issue. However, taking the example of the UK and the expectation that volumes across the EEA will significantly increase over coming months, the magnitude of this issue will soon become apparent and consequently, put ASPSPs under a lot of pressure.

The obvious need for a dedicated entity to help solve these problems and cut through the complexity is why Konsentus has looked at ways to automate and potentially eliminate the risky part of the tricky encounters.

Moreover, for an ASPSP not to be prepared for an increasing inflow of requests from TPPs and not having smooth processes and procedures in place may potentially result in huge extra time and resource costs to manually handle the pressure.

In conclusion, the simple message is that when it comes to PSD2 Open Banking and the smooth and secure interaction between the various players, due care is highly recommended. The issues that have been outlined above are no longer of a technical or regulatory matter, they are strategic business issues and fundamental to the future success of banks and their ability to adapt their business in an ever evolving open and dynamic ecosystem.

>>back to content

Top 5 issues that ASPSPs need to consider

How can ASPSPs protect themselves from potential fraud as well as financial and reputational risk as they prepare for the increasing interaction with TPPs?

1. Ensure communication is secure. All communication between the TPP and the ASPSP should be encrypted using Mutually authenticated Transport Layer Security (MTLS) based on eIDAS QWACs.

2. Check the identity of the TPP. Check that the TPP identity corresponds with the information given in the eIDAS certificate and that the eIDAS certificate is current. In addition, check that the certificate has been issued by an approved PSD2 Qualified Trust Service Provider (QTSP).

3. Check the regulated status of the TPP who wants to communicate with them. Use the authorisation number of the TPP from the eIDAS certificate to verify the regulated status of the TPP on its home NCA register. There are 31 NCAs and each NCA might have multiple registers (e.g. credit institution register, EMI register, Payment Institution register). There are over 117 different registers across the EEA. Check the TPP is on the register, what its current regulatory status is and the payment services it's authorised to provide.

4. Check the function/action the TPP is requesting is consistent with their regulated permissions. Is the service the TPP is requesting (e.g. access to account data or initiate a payment) consistent with the payment services they have been authorised to provide, e.g. Account Information Services (AIS) or Payment Initiation Services (PIS)?

5. Validate the TPP has got the customer's explicit consent to access the account or initiate payments on their behalf. Check directly with the customer that the function the TPP is asking to perform has been explicitly consented to by the customer using Strong Customer Authentication (SCA) mechanisms.

Making the encounter between ASPSPs and TPPs less tricky is much more than just a trivial technical exercise. In fact, for ASPSPs, it is very much a business issue. For an ASPSP not to address this issue carefully and not make the access to account for TPPs as smooth and secure as possible would undoubtedly be a rather hazardous mistake from a business perspective.

Banks from certain parts of Europe, which have not yet registered the same activity and growth of PSD2 initiated transactions as the UK, should be careful not to jump to the conclusion that the number of TPPs approaching the banks will stay low. The UK has been an Open Banking frontrunner however, we are starting to see significant growth in other EEA markets such as Germany, Sweden, France and the Netherlands. There is no reason to believe that the UK pattern is not going to be replicated throughout the rest of Europe, it's only a question of how soon.

What this means is that ASPSPs all over Europe should be preparing their PSD2 interfaces to accept large volumes of TPP requests now rather than waiting and seeing what happens. Unless they address these business issues, ASPSPs are potentially laying themselves open to unauthorised third parties accessing data that they are not allowed to access and negatively impacting their customers – the bank account holders. This has a number of additional detrimental implications for ASPSPs such as financial loss (through having to compensate their customers), reputational risk, brand damage and customer attrition.

>>back to content

Moreover, for an ASPSP not to be prepared for an increasing inflow of requests from TPPs and not having smooth processes and procedures in place may potentially result in huge additional time and resource costs to manually handle the increased requirements.

In conclusion, the simple message is that when it comes to PSD2 Open Banking and the smooth and secure interaction between the various players, due care is highly recommended. The issues that have been outlined above are no longer of a technical or regulatory matter, they are strategic business issues and fundamental to the future success of banks and their ability to adapt their business in an ever evolving open and dynamic ecosystem.

QWACs and QSealCs explained

In order to identify a TPP, PSD2 regulation recommends ASPSPs to use both a Qualified Website Authentication Certificate (QWAC) and a Qualified Electronic Seal Certificate (QSealC). The information they contain comprises:

- The TPP's unique authorisation number
- The PSD2 roles for which the TPP has been authorised/registered
- The name of the National Competent Authority (NCA) where the TPP is authorised/registered

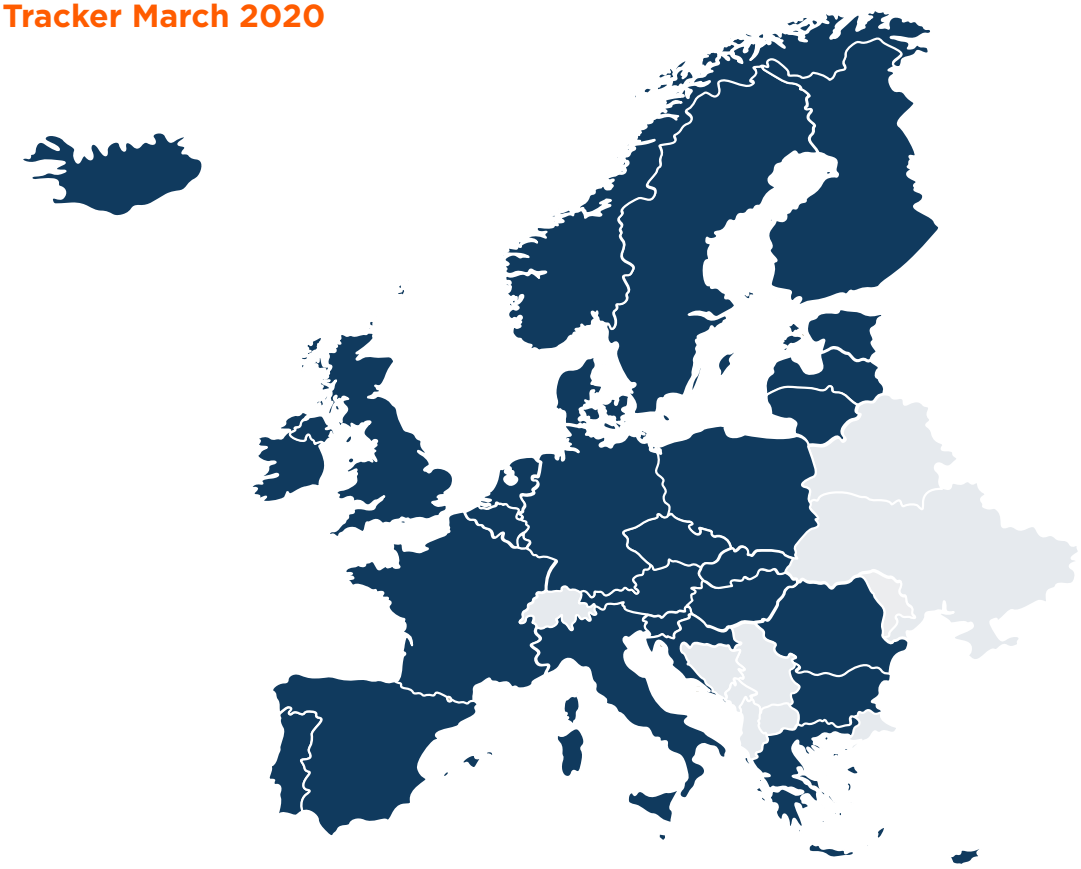
QSealCs and QWACs have different roles. Between them they ensure secure communication between a TPP and ASPSP takes place, as well as maintaining the integrity and proof of origin of the message itself.

- QSealCs: Qualified electronic Seals provide integrity and proof of origin of the signed message data over time but doesn't provide confidentiality.

- QWACs: eIDAS QWACs ensure the confidentiality, integrity and authenticity of data communicated between the TPP and ASPSP but only during transmission.

>>back to content

TPP Tracker March 2020



	HOST	TOTAL INCL. PASSPORTED
Austria	2	76
Belgium	10	79
Bulgaria	3	59
Croatia	1	56
Cyprus	2	52
Czech Republic	4	67
Denmark	5	75
Estonia	2	62
Finland	7	76
France	15	93
Germany	33	106
Great Britain	135	187
Greece	0	57
Hungary	4	59
Iceland	0	51
Ireland	6	76
Italy	1	76
Latvia	0	59
Liechtenstein	0	50
Lithuania	7	62
Luxemburg	1	66
Malta	0	55
Netherlands	9	86
Norway	2	70
Poland	2	70
Portugal	0	70
Romania	0	58
Slovakia	0	61
Slovenia	1	55
Sweden	24	93
Spain	2	79

Key: HOST | TOTAL INCL. PASSPORTED

>>back to content

About Norfico

Norfico is the first agency in the Nordics to combine strategic advisory with content and communication services with a dedicated focus on fintech.

From its base in Copenhagen Fintech Lab, Norfico serves clients in Europe and North America delivering both content and context in the increasingly complex financial services industry.

For more information about Norfico, please visit www.norfico.net or twitter.com/Norfico.

Kristian T. Sørensen

Michael Juul Rugaard

About Konsentus

Konsentus protects Financial Institutions for PSD2 Open Banking. Our Software as a Service (SaaS) solution consolidates data from a multitude of regulatory databases and registers, providing the information to our customers in real-time enabling them to comply with PSD2 Open Banking access to accounts. Issued through simple cloud-based RESTful APIs, our easy to implement service helps Financial Institutions reduce risk, limit liability and fight fraud by ensuring data is only ever given to legitimate and regulated Third Party Providers (TPPs).

Headquartered in the UK, with operations across Europe, Konsentus' world-class TPP identity and regulatory checking solution gives Financial Institutions the confidence they need to growth their business whilst knowing they are delivering against regulatory requirements and protecting their customers.

For more information about Konsentus, please visit www.konsentus.com, linkedin.com/company/Konsentus or twitter.com/KonsentusOB

Brendan Jones

Paul Meadowcroft