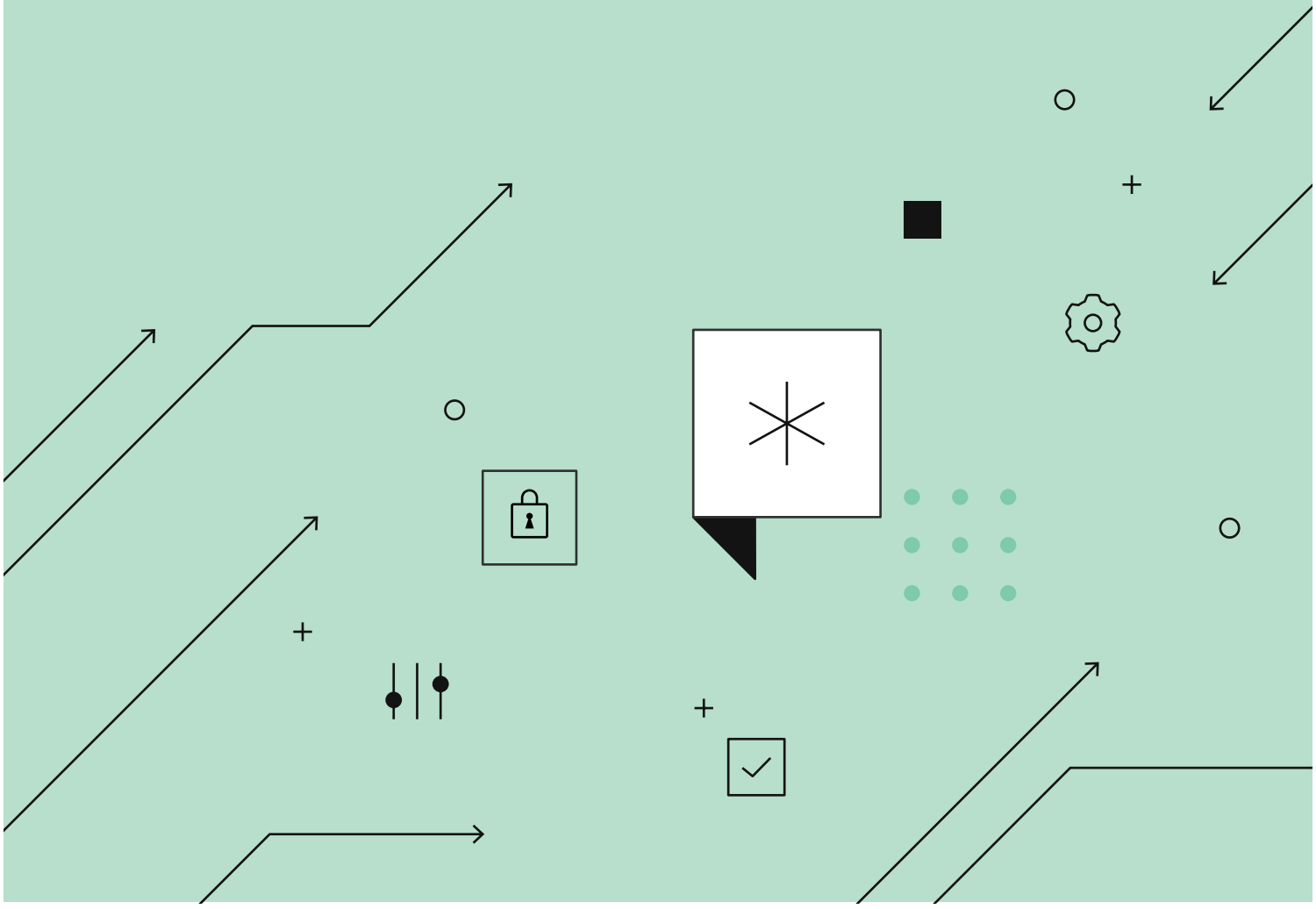
PLAID

plaid.com/uk

Authentication and Authorisation

Enhancing the financial data sharing experience



Content

Executive summary

Consumers continue to adopt digital financial services at a growing rate. Financial activities that were once manual like building a budget, investing in the stock market, and saving for retirement are now fully digitised, and consumers look to the internet or the app store for the financial solutions they once found at bank branches.

Many digital financial services are provided by fintech applications that run on consumer-permissioned financial data. Data sharing has become a distinct consumer experience, with consumers taking action to connect their payment accounts and other financial accounts to the third parties whose services they want to use. Networks have stepped in to deliver connectivity in the digital financial ecosystem, building two-way integrations that allow consumers to permission their data across financial institutions and fintech providers.

In the UK and EU, the introduction of strong customer authentication (SCA) under the Revised Payment Services Directive (PSD2) has laid out the specific requirements firms must meet if they want to provide online or digitised services powered by financial data to consumers.

As consumers add more digital services to their lives - a trend that's accelerating as a result of the COVID-19 pandemic - the data sharing experience becomes increasingly important. This is especially true in financial services, where consumers build connections across a complex web of financial institutions and fintech applications. Well over two-thirds of UK adults (72%) used online banking and over half (50%) used mobile banking to access their financial information in 2019.[1] A growing number of fintech tools, such as small business accounting software and digital mortgage loan providers, require consumers to share their data from multiple financial accounts.

In the UK, Open Banking Standards have been developed to ensure consumers go through a simple and consistent authentication journey. However, that is not enough to provide consumers control over their financial lives. Consumers need to be able to control all of their financial data across their various account providers, and not just the data held by their payment account provider. Developers and regulators are already considering the next stage of consumer-powered data sharing - open finance, which goes beyond open banking to include other products and services including pensions, mortgages and investments.

Data sharing has become a distinct consumer experience.

72%

Well over two-thirds of UK adults (72%) used online banking and over half (50%) used mobile banking to access their financial information in 2019.[1]

[1] https://www.ukfinance.org.uk/system/files/UK-Payment-Markets-Report-2020-SUMMARY.pdf

This paper focuses on two discrete functions at the heart of the data sharing experience – authentication and authorisation. This paper also discusses how the industry can improve upon OAuth, a data sharing protocol adapted from the social media landscape that presents certain issues for financial data sharing. We identify what makes financial data sharing different; set forth principles for how authentication and authorisation should work; evaluate OAuth against those principles; and highlight how networks are best positioned to provide data sharing experiences that are neutral, consistent, consumer-controlled, and can innovate alongside changing technologies.

Regulators and policymakers should give consumers the ability to control all of their financial data in order to ensure API powered consumer data sharing is successful. Meanwhile, the ecosystem needs to build on the current authorisation and authentication models to ensure that they can work in an open finance context. As the ecosystem, regulators, and policymakers explore how to give consumers more control over their data, the authorisation experience should be empowering for consumers, adaptable to changing technologies, and neutral with regards to which products consumers want to use.

If the digital financial ecosystem is to meet its potential and enable consumers to fully take control of their financial lives, then the industry must look to networks to continue providing data sharing experiences that grow alongside the ecosystem and keep consumers at its core.

The ecosystem needs to build on the current authorisation and authentication models to ensure that they can work in an open finance context.

What makes financial data sharing different?

As the digital financial ecosystem explores how to build data sharing experiences, it is tempting to seek precedent in other industries – after all, digital transformation is making many ecosystems more reliant on data sharing, from retail to enterprise to social media.

Two elements make financial data sharing different: the fragmented structure of the financial services ecosystem, and the competitive dynamics felt across financial institutions and fintech companies.

The digital financial services ecosystem is uniquely fragmented, with thousands of financial institutions and thousands of fintech applications. Social media data sharing, on the other hand, consists of only a small number of major providers like Twitter and Facebook, which allow their users to share data with thousands of microservices. The fragmentation within financial services gave rise to networks, which entered the ecosystem as a fourth-party to provide data connectivity.

Within the "many-to-many" ecosystem are a variety of competing products and services. Fintech applications provide services that financial institutions also provide, like budgeting tools and investing platforms. As some fintechs become more like traditional financial institutions by obtaining their own regulatory permissions, and banks increase their investment in digital services, this competitive overlap will intensify. This introduces a dynamic where data holders might be incentivised to obstruct data access in order to keep their customers close.

As financial technology expands into more sectors, there are distinct stakeholders in the ecosystem that must be optimised for simultaneously in a balanced, neutral way. A network layer can balance interests and promote innovation by delivering data sharing solutions that fit this ecosystem's many-to-many structure and prevent competitive dynamics from disrupting both the consumer's control of their data and the consumer's potential to access the best possible service from their chosen provider. This starts by exploring the critical elements of the data sharing experience and building a principles-driven approach.

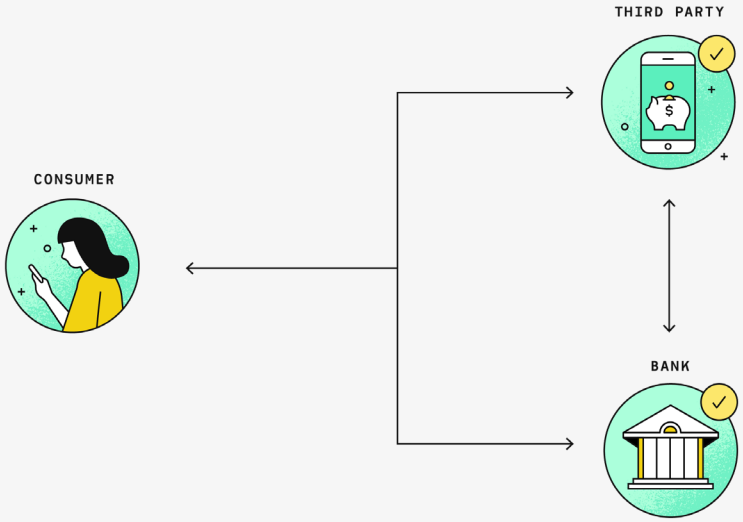
A network layer can balance interests and promote innovation.

2-party versus 4-party systems

In the course of the industry's digital transformation, the number of parties involved in providing financial services has grown from two (consumer-bank, one-to-one); to three (consumer-bank-fintech, few-to-many); to four (consumer-bank-network-fintech, many-to-many).

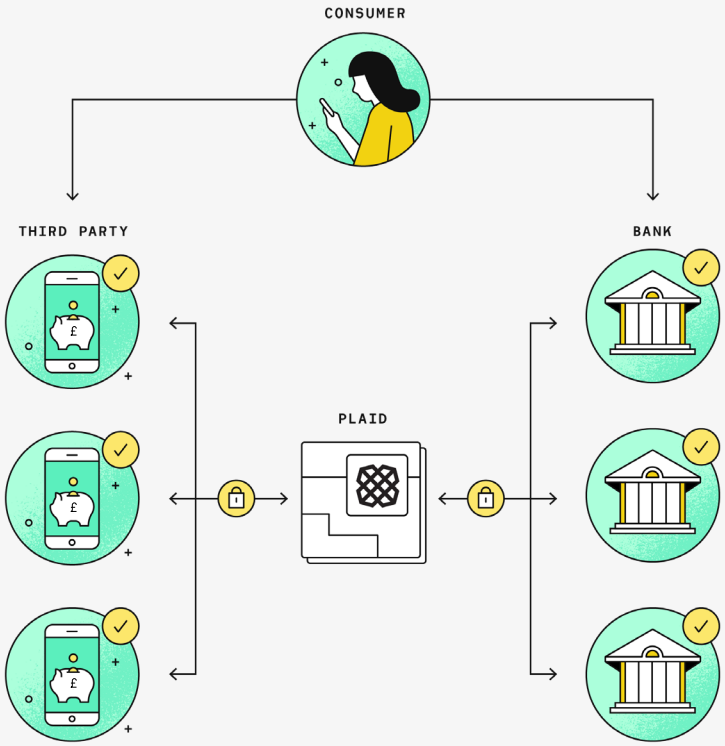
2-party

In the analog era, interactions took place in-person between a customer and teller at a bank branch. In digital banking, these one-to-one engagements take place on bank websites or mobile applications, where consumers log in using their credentials before viewing balances, making transfers, or buying products.



3-party

As digital financial services began to take hold, early personal financial management services like Mint would ask consumers for their online banking credentials in order to pull data from the bank website. Many of these services came of age while social media was taking off, with websites like Facebook and Google standing up their own interfaces to allow consumers to share data with third parties.



3 and 4-party

In the fintech era, consumers increasingly connect multiple payment accounts to multiple fintech applications, and networks have stepped in as fourth parties to enable connections across a **many-to-many ecosystem**. In this ecosystem, data sharing is initiated at the application-level: consumers download an application, and as part of their enrollment in the application are guided through the process of connecting their payment accounts.

Authentication and Authorisation

At the heart of financial data sharing experiences are two core functions: authentication and authorisation. Typically these take place during consumer enrollment in a new digital service – a consumer signs up for a digital application, and the provider requests that the consumer permission their data from their financial institution. Authentication is how consumers verify to their financial institution that they own the account containing their data, and authorisation is how consumers select which elements of their data they want to share.

In the analog era of financial services, authentication and authorisation were indistinguishable. A bank customer only needed to walk into a branch and present identification to be able to manage their finances. But as financial services digitised, and consumers began to connect their bank accounts with third and fourth parties, these functions separated, with consumers authenticating across a range of providers, and authorising pieces of data for specific use cases.

In 2018, PSD2 required financial institutions to introduce SCA, meaning that a payer must authorise their payment transactions using two of three independent authentication elements. The three independent authentication elements are:

- Knowledge – something you know i.e. password or pin
- Possession – something you possess i.e. mobile phone
- Inherence – something you are i.e. biometrics

The goal of SCA is to reduce fraud and increase security for consumers. By introducing these new authentication requirements for third party providers (TPPs) and financial institutions, payments within Europe are safer and more secure.

In the UK, the development of the Open Banking ecosystem has been spearheaded by the work of the Financial Conduct Authority (FCA) and the Open Banking Implementation Entity (OBIE). Amongst other things, the FCA has provided guidance on the different authentication models under PSD2 in their Approach Document.[2] Meanwhile, OBIE has created the Open Banking Standard, to help ensure Open Banking is implemented simply and consistently across providers. Part of those Standards includes suggested consumer journeys for authentication.[3]

[2] https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf

[3] https://standards.openbanking.org.uk/customer-experience-guidelines/authentication-methods/latest/

Through regulatory guidance and Standard-setting bodies, general principles for authentication have developed with the best interest of consumers and TPPs in mind:

1. **Build on normal:** More and more consumers are using mobile applications for their everyday banking needs, and these applications rely on biometrics for log-in compared to a consumer inputting their security credentials. A consumer should be able to use the methods they are already using to log-in when authenticating with their financial institution (e.g. FaceID).
2. **Simple customer experience:** Just because the consumer decides to use a TPP does not mean they should have to go through more steps, delay or friction in the customer journey. It should be the same journey as if they were interacting directly with their financial institution.
3. **SCA Once:** It is not expected that SCA would be required more than once when facilitating authentication for a single session of access to account information or single payment initiation.
4. **No Obstacles:** Authentication should be simple and secure. Financial institutions should not introduce additional requirements, steps or confusing language that might discourage consumers from using open banking services.

While these are good stepping stones, data sharing is quickly becoming more relevant and prevalent to consumers' everyday lives. To ensure consumers' best interests are protected, some additional principles are required. These include:

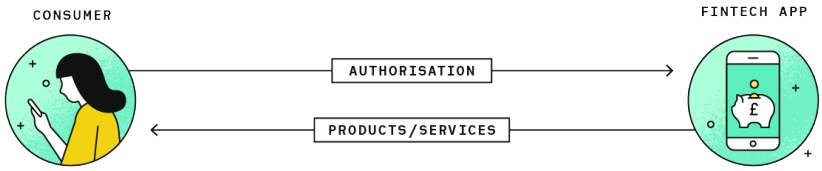
- **Consumer-controlled:** Authorisation should enable consumers to control all of their financial data, while making them fully aware of the implications of their data sharing. Consumers should be able to control their data sharing by toggling connections on and off, and revoke connections when they are done using a fintech application.
- **Use-case driven:** Consumers share data in order to reap the benefits of a service, so the elements of data they share should be determined by the use-cases they are seeking. Authorisation must therefore be able to narrowly scope data and provide the necessary data to power the consumers' desired use-cases.
- **Without interference:** Consumers should be able to freely choose products for themselves from across the entire fintech and financial services ecosystem without limitation. They should not feel tricked or misled about what data they are sharing or the consequences of their doing so.

Misconceptions of authorisation and authentication

Under PSD2, the concepts of access and consent are legally captured by authorisation and authentication; however, they only work for the initial connection between consumers, TPPs and financial institutions.

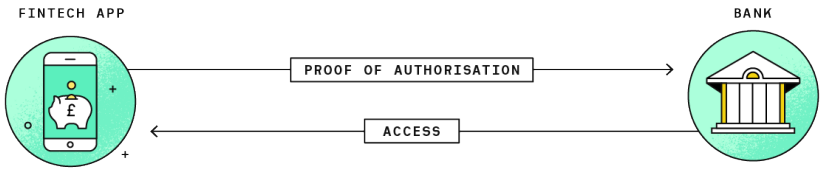
When a consumer first initiates a connection with a TPP, they are authorising the TPP to access, use and store their data.

AUTHORISATION



Once the consumer has given the TPP their authorisation, the TPP then goes to the consumer's financial institution to authenticate the consumer's identity and prove the TPP has the right to access the data. The financial institution will then grant the TPP access.

AUTHENTICATION



A key issue of PSD2 is that policymakers have conflated authorisation and authentication in a way that interferes with policy objectives and the development of open banking. An example of this is industry's misinterpretation of the 90 day "reuthentication" requirement. The purpose of 90 day "reauthentication" is to ensure that consumers actively re-engage **with the TPP** and continue to consent to the use of their data **by the TPP**.

Reauthorisation only occurs between the consumer and the TPP. Whereas, reauthentication only occurs between the financial institution and the TPP. Financial institutions should have no role in reauthorisation. For the 90 days requirement the use of the term “reauthentication” rather than “reauthorisation” means financial institutions are involved in the process to the detriment of consumers and the ecosystem.

The consequences of this misinterpretation can already be felt among TPPs, as there is a misalignment of interest between TPPs, consumers and financial institutions as well as a misunderstanding of how the reauthorisation process should work.

Without a clear and agreed interpretation of the party responsible for 90 day “reauthentication” there are no clear incentives to improve the customer journey. This directly opposes PSD2’s policy goals of competition and innovation by leaving the TPP and consumer relationship in the hands of the financial institution.

KEY FEATURES OF AUTHORISATION AND AUTHENTICATION

Authorisation	Authentication	90 Day “reauthentication”
Given by consumer	Given by financial institution (FI)	Given by consumer
Expires	Expires	Expires
Can be revoked	Can be denied	Can be revoked
TPP controls customer journey	FI controls customer journey	FI controls customer journey
—	—	Authorisation
—	—	Consent refresh

Building data sharing experiences that work

While the ecosystem looks to build data sharing experiences, some industry actors have identified existing protocols as potential solutions. There is risk, though, in anchoring too closely to existing specifications and protocols, which can introduce brittleness and a limited perspective into what is at its core an evolving principles problem. Instead, the financial data sharing ecosystem should build its own authentication and authorisation infrastructure that abides by the above principles and fits the industry's unique structure. This involves achieving three critical goals:

- Minimise credentials-sharing
- Provide seamless and consistent experiences
- Preserve the ability to innovate
- Do not let duplicitous security requirements kill the customer journey

Financial data sharing ecosystem should build its own authentication and authorisation infrastructure.

Minimise credentials-sharing

The sharing of consumer credentials is consistently a top security concern, and must be minimised in order to reduce risk. SCA was developed to stop consumers from sharing their credentials to combat fraud and increase the security of online payments in Europe. Several mechanisms exist to limit the proliferation of consumers credentials, including tokenisation and end-to-end encryption. Networks and financial institutions can limit the visibility of credentials by swapping them out for tokens. Tokenisation can take place either by the entity holding the consumers' data, where the token would be passed back to the network for future data retrieval, or at network level, where credentials can be purged after tokenisation.

Provide seamless and consistent experiences

Seamlessness and consistency will ensure consumers remain at the centre of the digital financial ecosystem. For consumers, authentication and authorisation are merely a means to the end of reaping the benefits of digital financial tools that rely on their data. These processes should therefore minimise the gap between a consumer selecting and using applications of their choosing. To ensure familiarity, comfort and understanding, consumers should be guided through a consistent set of screens to ensure that connectivity and data permissioning is consent-driven. The OBIE in the UK is a good example of seamless, consistent Standards that encourage consumers to use open banking products and services.

Preserve the ability to innovate

Solutions must be adaptive both to changing consumer demand and the increasing sophistication of bad actors. New technologies like biometrics and the internet-of-things can enhance both consumer experience and security, so authentication mechanisms must be able to integrate these tools as they arise. Poorly designed data sharing solutions may present lock-in challenges, in which they cannot adapt quickly and therefore lack the ability to force the abandonment of authentication techniques made obsolete by a fast moving and consumer driven market.

Do not let duplicitous security requirements kill the customer journey

Consumer trust and security are paramount to the success of consumer powered data sharing, but security requirements should not create unnecessary friction that damages the customer experience and overall success of data sharing. PSD2 SCA requirements pose a direct threat to the uptake of open banking products and services and are the reason for a large number of high consumer attrition rates.

Does OAuth solve these problems?

In short: no. OAuth is an access delegation protocol designed by Twitter engineers in 2007 after they realised consumers had begun sharing their credentials with third parties. OAuth has since been widely adopted in the three-party social media ecosystem, where massive technology companies like Twitter and Facebook provide identity services to their billions of customers and maintain authentication endpoints for the thousands of untrusted and non-competing third-party providers that request consumers' data.

Due to its foothold in social media, OAuth was identified by some as a potential solution when financial data sharing came to prominence in the late 2010s. Several financial institutions went so far as to adapt OAuth as their authentication and authorisation solution, while others explored different avenues and awaited the verdict on OAuth's utility in this space.

While perspectives on OAuth are still evolving, after some experimentation it has become clear that OAuth presents difficulties when transposed from the social media ecosystem to digital financial services. The protocol leaves financial data sharing experiences lacking along several lines:

Consistency

Under many current OAuth implementations at financial institutions, consumers are redirected across different pages each time they connect accounts. This can interrupt the consumer journey and open space for competitive interference to undermine data sharing experiences.

Consumer Control

OAuth is mostly an authentication and access delegation protocol; it doesn't speak specifically to authorisation. This can result in disparate authorisation controls, in which consumers' ability to manage their data differs depending on which financial institution they connect with.

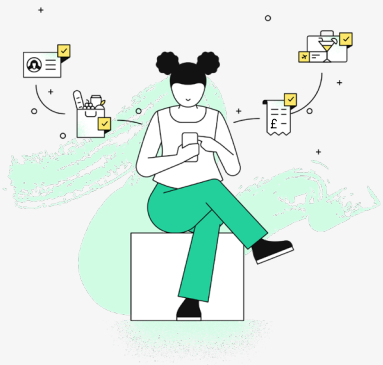
Granularity

OAuth is a broad specification and its scopes are largely pre-defined, meaning it is built to deliver permissions (to allow consumers to say, "yes, you can access my data"), but not scope resources granularly. This makes it difficult to precisely scope data for specific use-cases.[4]

Adaptability

OAuth endpoints require management from both providers and developers. Each time new technology comes along that makes old authentication technology obsolete, OAuth providers would need to flow down changes across the entire ecosystem, with every downstream financial application needing to modify how they access data. This is a complex endeavour which requires business relationship management with all data recipients.

[4] https://medium.com/oauth-2/transaction-authorization-or-why-we-need-to-re-think-oauth-scopes-2326e2038948



PSD2 Authentication Models

Since the introduction of PSD2 in 2018 three authentication models have developed:

1. **Embedded** – TPPs or Technical Service Providers (TSP) design the consumer interface, and the consumer presents their security credentials to the TPP/TSP via this interface. The TPP/TSP forwards these to the financial institution via the financial institutions PSD2 compliant dedicated interface.
2. **Redirection** – the most commonly used method. The consumer does not give the TPP/TSP their security credentials, rather they get redirected from the TPP/TSP's consumer interface into the financial insitution's dedicated interface.
3. **Decoupled** – the consumer provides their security credentials to an approved device or application that is separate from the application or web browser where they are making a purchase or giving their consent to access their account information. The approved device or application sends a message to the financial institution confirming the security credentials of the consumer.

Each model presents its benefits and challenges. Arguments have been made that the redirection and decoupled models are preferred because the consumers security credentials are exchanged directly between the consumer and financial institutions, while embedded models require the consumer to exchange their security credentials between TPPs/TSPs and the financial institutions. While the embedded model is SCA-RTS compliant it does present a higher risk to consumers who have to share their personalised security credentials to TPPs/TSPs.

Regardless of the authentication model used, the goal is to create the best experience for consumers while ensuring increased security. PSD2 considers these goals and has introduced several exemptions available to financial institutions to leverage, including payments to trusted beneficiaries, low-value payments (including contactless payments) and transaction risk analysis payments.

Networks solve these problems

Where OAuth's limitations introduce barriers to the industry's growth, networks are uniquely positioned to address these challenges and deliver data sharing experiences that move the digital financial services ecosystem forward.

Three elements highlight the unique value networks bring to solving the authentication and authorisation challenges present in OAuth: **interoperability, rules enforcement**, and **visibility across the ecosystem**.

Networks can provide consistent and secure data sharing experiences.

Interoperability

Networks' interoperability across financial institutions and fintech providers means they can provide consistent and seamless data sharing experiences. This includes both a consistent consumer interface across all bank and fintech data connections, which helps consumers build comfort, confidence, understanding and consent; and also a recognised set of controls for consumers managing those data connections. Additionally, networks can minimise credentials-sharing by relying on tokenisation at network level. This means no parties outside of financial institutions and networks ever need to touch credentials, and networks can encrypt and purge credentials for tokens immediately.

Rules enforcement

In four-party ecosystems, fintech providers seeking to access consumer-permissioned data must establish a business relationship with the network enabling that connectivity. Networks therefore mandate sound privacy and security practices and establish requirements on third party providers that receive consumer data. This solves for OAuth's adaptability problem, in which ecosystem complexity makes flowing down changes difficult – Plaid, for example, collaborates with financial institutions to adapt additional security measures like enhanced authentication requirements, and forces the adoption of these requirements across the entire ecosystem from a central nexus.

Where maintaining authentication and authorisation technology can generate significant IT costs for financial institutions, it is a business imperative for networks, whose customers reward them for providing seamless and consistent experiences back to consumers. Networks whose business models are centred around delivering connectivity to a growing ecosystem are incentivised to position themselves in a neutral way and promote innovation that benefits all parties.

That's why Plaid is building Plaid Exchange, a new data sharing platform to serve financial institutions looking to advance their digital strategies. The Plaid Exchange platform is built to provide consistent, secure, and adaptable data sharing consumer experiences across the financial ecosystem. Plaid Exchange comes with APIs to enable consistent and granular data sharing experiences; dashboards that allow financial institutions to monitor their data flows; and security features that are only made possible by networks' unique visibility across the ecosystem. By taking on the business of building authentication and authorisation functionality for financial data sharing, networks like Plaid can continue to invest in advancing technologies that meet the needs of all parties and contribute to the ongoing development of this ecosystem.

Plaid Exchange is only available to US-based clients; however, PSD2 and open banking provide a unique opportunity for Plaid Exchange. In the UK, the OBIE paved the way for open banking through the customer experience guidelines (CEGs).[5] The CEGs provide guidance for open banking powered products and services by combining regulatory requirements and customer feedback. The CEGs include a requirement for TPPs to create access dashboards to give consumers a one-stop-shop for monitoring their consents.

Done effectively, access dashboards are one of the best ways to provide consumers with a clear list of TPPs that have access to their financial data. They can also provide the functionality for a consumer to revoke consent. One aspect of Plaid Exchange allows participating banks and fintechs to provide consumers with an access dashboard that lets them view and manage the consents they have given. This type of easy to use consent dashboard increases transparency and gives consumers more control over their data, ultimately building their trust and willingness to use more products and services that rely on their financial data.

[5] https://www.openbanking.org.uk/wp-content/uploads/Customer-Experience-Guidelines.pdf

The Path Forward

Going forward, networks are building all-in-one data sharing platforms that will allow digital financial services to continue to grow with consumers' adoption of open banking products and services. These include authentication and authorisation solutions that improve upon OAuth by providing consistent experiences across all providers while enabling flexibility across the ecosystem.

Financial institutions investing in digital transformation already look to vendors to provide infrastructure that helps their customers improve their financial lives. Working with networks on a vendor basis to provide authentication and authorisation for financial data sharing would advance financial institutions' digital strategies, and provide their customers with access to the entire digital financial ecosystem.

Europe is already looking at the next steps in consumer powered data sharing – open finance. The European Commission issued a consultation on a New Digital Finance Strategy for Europe[6] while the FCA issued a Call for Input on Open Finance[7] in December 2019. Open finance focuses on building and expanding on open banking to a wider set of accounts including but not limited to mortgages, pensions, savings and insurance.

By having access to more accounts, TPPs will be able to provide consumers with a whole suite of bespoke products and services built off their financial data. Open finance will have an impact on every area of a consumer's financial life, making traditionally disconnected and confusing accounts easily accessible. That being said, regulators, policymakers and industry will need to work together to ensure the authentication models used in open finance build on and improve the models we see in open banking.

It is time for the digital financial services ecosystem to leverage the resources at its disposal, acknowledge aligned principles, and establish the next generation of authentication and authorisation infrastructure for financial data sharing. Networks are best positioned to provide authentication and authorisation that works for consumers, financial institutions, fintech companies, and the ecosystem at large.

[6] https://ec.europa.eu/info/consultations/finance-2020-digital-finance-strategy_en

[7] https://www.fca.org.uk/publications/calls-input/call-input-open-finance

About Plaid

Plaid is a fintech company which builds the technical API infrastructure that connects individuals, financial institutions, and fintech developers – giving consumers power over their own financial data.

Launched in 2013 and headquartered in San Francisco, a quarter of US bank accounts are now linked by Plaid to a range of fintech apps that can help consumers carry out essential financial tasks such as save for retirement, make a budget or transfer money.

Plaid expanded to Europe in 2019 to better enable fintechs and developers to build creative PSD2 compliant solutions on top of the developing open banking infrastructure. Authorised in the UK as an payment institution with permission to carry out account information services and payment initiation services, Plaid is looking to build on its experience of creating digital financial infrastructure to deliver the best in class API experiences for European consumers.

Ben White: bwhite@plaid.com

Kat Cloud: kcloud@plaid.com

PLAID HEADQUARTERS
1098 HARRISON ST.
SAN FRANCISCO, CA 94103

PLAID C/O FORA SPACE
35-41 FOLGATE ST
SPITALFIELDS, LONDON E1 6BX, UK