SwissBanking

July 2020

Open Banking

An overview for the Swiss financial centre

Contents

Foreword

Open banking is one of the key issues shaping the future development of the financial sector internationally. It has gained traction in part due to regulatory requirements both within the European Union (EU) and in countries outside Europe. However, open banking – business models based on the standardised and secure exchange of data between the bank and reliable third party providers – is often seen as merely a first step towards a platform economy in which data are exchanged across sectors and processed to add value for customers, the economy and society.

The role of banks is central here: with their extensive customer base and the trust placed in them, they are well placed to lead the way in a cross-sector ecosystem. They are also equipped to play a key role in defining data protection, rules for the ethical use of data, and standards for interfaces and infrastructure. The Swiss financial centre therefore has a unique opportunity to shape the future financial ecosystem by acting in concert with the key players.

This document was drawn up by a working group headed by the Swiss Bankers Association (SBA). It intends to create the conditions for facilitated cooperation between banks and third party providers, and further advance the market-driven implementation of open banking in Switzerland. It offers a structured definition of open banking from the perspective of the Swiss banking sector and lays down fundamental guidelines for the relevant legal issues.

This SBA document contains legally non-binding recommendations and assessments which can be referred to when further implementing open banking business models. It does not claim to be exhaustive. It will be updated and supplemented as necessary to take account of future developments in technology and the law. The latest version is available on the SBA website.

Authors in alphabetical order

Matthias Häfner, Valiant Bank
Martin Hess, Swiss Bankers Association
Richard Hess, Swiss Bankers Association
Roger Huber, Zürcher Kantonalbank
Friederich Kersting, PostFinance
Matthias Plattner, Julius Bär
Jürg Schär, UBS
Sven Siat, SIX
Cornelia Stengel, Swiss Fintech Innovations
Stephanie Wickihalder, Credit Suisse
Marco Wüst, Raiffeisen Switzerland

Our particular thanks go to the external experts for their valuable contributions in the form of discussions and additions to this document.

Executive Summary

The Swiss Bankers Association (SBA) recognises the significant potential of open banking for the Swiss financial centre. It is therefore actively contributing to the creation of an environment that facilitates business models based on open banking, thus increasing the competitiveness of Switzerland's financial centre. At the same time, it must be ensured that if interfaces are opened to third parties, trust in the financial centre remains strong. Regulatory measures such as the enforced opening of interfaces are not expedient. Free competition and customer needs in particular must and will dictate how open banking is implemented in Switzerland. It should remain the decision of the banks whether and with which third party provider (TPP) they wish to work. The following three points are crucial to a continued positive evolution going forward:

1. A clear strategic positioning

Collaboration with various third party providers in an open banking ecosystem is first and foremost a strategic issue. It requires institutes to specifically address the question of how to handle customer data and share them in the ecosystem in future. As part of this, each institute will require a clear positioning regarding its own offering and must define its own role in developing that offering. This will create a sound basis for the subsequent selection of specific partners and services.

2. Legal requirements based on the specific arrangement

Owing to its market-driven approach, Switzerland currently has no specific legal and regulatory requirements for open banking. Essentially, banks are free to decide for themselves who they work with and who is allowed access to their interfaces. This ensures that the collaboration between bank and third party provider is based on market forces and specific use cases that add value for customers. In terms of a legal assessment, an important distinction has first to be made between outsourcing and open banking. This will give rise to differing sets of requirements. In the context of open banking, the nature and intensity of the interaction between bank, third party pro-vider and customer needs to be examined. The more closely the bank and third party provider cooperate in open banking, the more the customer will rely on the bank to audit the provider and take a degree of responsibility for its services. For example, customers will view active marketing as an indicator of close cooperation.

3. API standardisation specific to business domains

Open standardisation of Application Programming Interfaces (APIs) is an important prerequisite for seamless docking of third parties and error-free data sharing. There are already standards on the Swiss market for interfaces that allow access to account information and enable payments to be submitted. It is important to take account of the different levels and their degree of standardisation, because heterogeneity generally leads to complexity and higher costs. In the medium term, it is therefore reasonable to expect a small number of standards – often just a single one – to prevail in each business domain (e.g. account information, payments, mortgages, pensions).

1. Open banking in Switzerland

Drivers of open banking

Changing customer needs, new stakeholders and new technologies are posing challenges for traditional banks. Against this backdrop, open banking will have a lasting and transformative impact on the banking sector. In a world where the value chain is becoming increasingly fragmented, with customers being served by many different financial services providers such as banks, fintechs, neobanks and service providers from other industries, the question is no longer whether open banking will establish itself, but only in what form. Growing competition and evolving regulatory requirements are acting as catalysts in this process.

In Switzerland, the focus of open banking remains on corporate customers. The offering is being continually refined to meet customer needs and reflect market conditions, and can increasingly offer new possibilities for private customers going forward. One development closely connected to open banking is the emergence of cross-sector ecosystems, to which the financial services industry can add value.

With the controlled opening up of standardised interfaces, customers benefit from a high pace of innovation and therefore competitive offerings, while also enjoying a high degree of stability and reliability. Corporate customers can, for example, improve their liquidity planning by integrating accounting software. Both corporate and private customers can gain an overall view of their financial situation by integrating various accounts from different providers.

For banks, collaboration with third party providers by means of standardised interfaces boosts efficiency and generates new potential sources of revenue. Open banking makes it possible to improve the customer experience as a result of seamless transitioning between different offerings. Data sharing also enables banks to access third party data and use them to offer innovative products. It also allows them to position themselves as key players or solution providers in a platform economy, tap new revenue channels efficiently, and reach a larger customer base.

For third party providers such as fintechs, meanwhile, open banking offers the prospect of launching their products and services with fewer technical and regulatory requirements (e.g. no need for a banking licence). Cooperation with established financial services providers gives them access to a broad customer base, enabling them to rapidly scale their business model. Depending on the circumstances, the reverse may also be true.

Open banking vs. outsourcing

Open banking comprises three elements

The SBA defines open banking as a business model based on the standardised and secure exchange of data between the bank and reliable third party providers, which can also be other financial services providers.

- **"Standardised":** Open standardisation of interfaces is a prerequisite for seamless third party docking and error-free data exchange.[1] The standardisation of interfaces should to the greatest extent possible be based on recognised market standards.
- **"Secure":** Ensuring data confidentiality and security requires technological safeguards.
- **"Reliable":** The maintenance of system integrity requires that third parties are only granted access to the interface if they meet certain quality criteria – in particular, the highest technical requirements. The decision to share a customer's data is always made by the customer itself. With an appropriate offering from third party providers, the bank positions itself as a reliable partner and protects the interests of its customers. In doing so, every bank contributes to the security and stability of the Swiss financial centre and underscores why customers should continue to place a high level of trust in Swiss banks in the future.

1 In addition to docking of third party providers and fragmentation of the value chain, open banking is an important precondition for and driver of "Software as a Service (SaaS)" offerings in the financial services industry. Only through standardisation can software manufacturers and IT providers deliver the solutions financial services providers are looking for. This fact will have a crucial impact on financial services providers' IT architectures and accelerate the trend away from monolithic towards best-of-breed architecture.

Economic and legal differences from outsourcing

Open banking and outsourcing are related but not synonymous. In its Circular 2018/3, the Swiss Financial Market Supervisory Authority (FINMA) defines outsourcing as follows[2]:

> Outsourcing within the meaning of this circular occurs when a company mandates a service provider to perform all or part of a function that is significant to the company's business activities independently and on an ongoing basis.

Common to both open banking and outsourcing is the involvement of third parties, but there are both economic and legal differences:

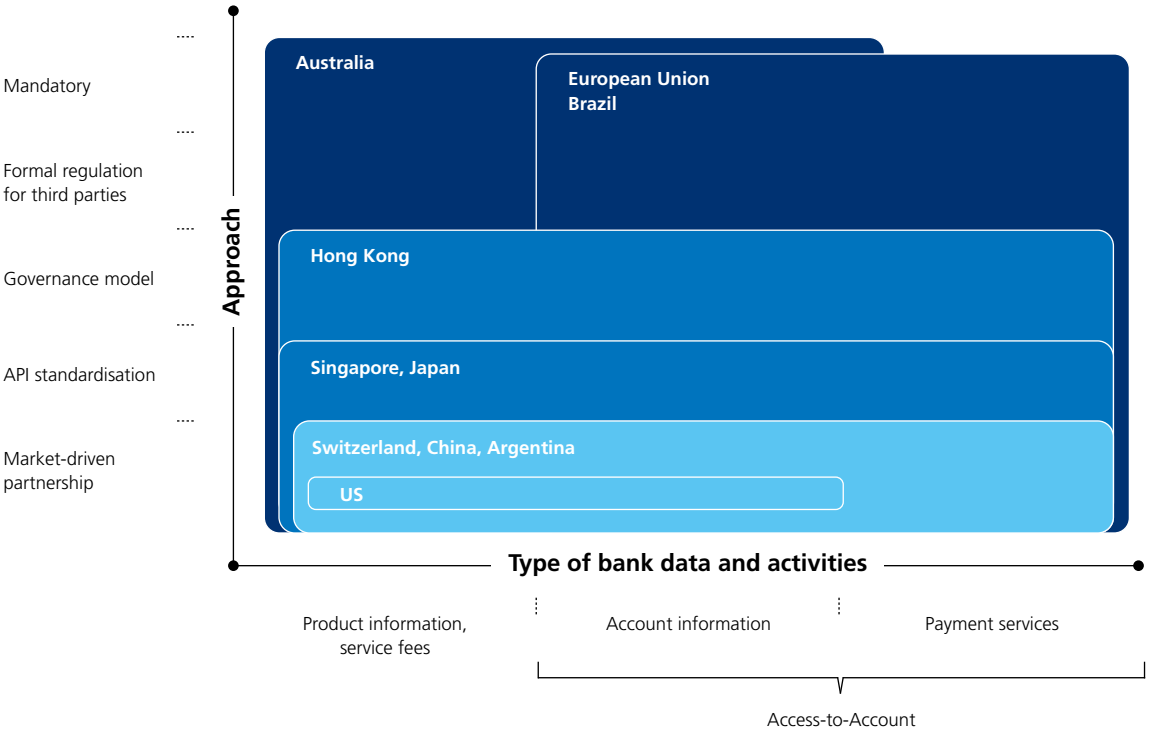
- In **outsourcing**, the third party acts solely on behalf of, under instructions from and in the interest of the instructing bank. The instructing bank must retain control of the service provided. The outsourced function is part of the instructing bank's value chain and is subject to the latter's duty of due diligence towards the customer.
- In **open banking**, the third party acts not on behalf of the bank but primarily on behalf of and in the interest of the customer. With the customer's consent, the third party accesses some of that customer's data at the bank or is supplied with them in order to process them and offer the customer added value. The bank thus has no control over the service provided by the third party. Because this means that the duty of due diligence towards the customer lies with the third party, the open banking service requires the customer's consent.

2 As opposed to the definition of third party data processing under the Data Protection Act (FADP), which is broader.

2. International developments

Internationally, supervisory authorities and regulators have adopted a range of measures to establish the frameworks for open banking. These vary in terms of the regulatory approach and the scope and nature of the bank data and activities subject to regulated data sharing (see figure 1).

Fig. 1: A comparison of international open banking frameworks



Category 1: Data sharing prescribed
Category 2: Data sharing encouraged
Category 3: Market-based approach with no explicit rules on data sharing

Source: SBA, based on Basel Committee on Banking Supervision (2019).
Report on open banking and application programming interfaces. https://www.bis.org/bcbs/publ/d486.pdf

Overall, these approaches can be divided into four categories.[3] Switzerland is pursuing a market-based approach and therefore falls into category 3.

- **Category 1: Data sharing mandatory**
  Banks are obliged to share with third parties the data for which the customer has granted consent. Third parties must register with a regulatory or supervisory authority and are normally subject to strict checks by government bodies.
  Examples: Australia, Brazil, EU, India, Mexico, South Africa, UK.
- **Category 2: Data sharing encouraged**
  Authorities have issued guidelines containing recommended standards and technical specifications.
  Examples: Hong Kong, Japan, Singapore, South Korea.
- **Category 3: Market-based approach with no explicit rules on data sharing**
  No explicit rules or guidelines requiring or prohibiting the sharing of data by banks with third parties with the customer's permission.
  Examples: Argentina, China, Switzerland, US.
- **Category 4: Regulation subject to clarification[4]**
  Jurisdictions that are currently introducing specific regulatory requirements or are actively considering doing so.
  Examples: Canada, Russia.

3 Basel Committee on Banking Supervision (2019). Report on open banking and application programming interfaces. https://www.bis.org/bcbs/publ/d486.pdf

4 Not shown in figure 1.

3. Creating the right conditions

Framework – freedom of contract and market-driven solutions

Under the market-driven approach adopted by Switzerland, there are currently no specific legal and regulatory requirements for open banking. Essentially, banks are free to decide for themselves who they work with and who is allowed access to their interfaces. This ensures that the collaboration between bank and third party provider is based on market forces and specific use cases that add value for customers.

In Switzerland there is no obligation for banks to share customer data with third party providers. Automated access to interfaces is at the discretion of the bank concerned. Accordingly, there is currently no regulatory requirement for licensing and authorisation of third party providers to simplify or replace the prior audit of third party providers.

From the bank's perspective, it is advisable to subject potential third party providers to certain prior checks. The key issue here is the nature of the collaboration arrangement between bank and third party provider. The specific approaches and points to consider when auditing third party providers are explained in greater detail in section 4.

Strategy – clear positioning

The bank needs a clear positioning based on its offering
From the bank's perspective, the primary aim of open banking must be to offer added value to customers by supplementing its own offering with innovative products and services. Characteristic features of such offerings are that they:

- **are created in collaboration with third parties.** This means that fintechs, for example, or other established solution providers such as manufacturers of accounting systems are systematically integrated into the flow of information and offerings to the customer.
- **complement the bank's classical offering.** Existing bank data are enhanced by using third party data to create new information for customers or present that information to them in a new context.

This requires the bank to have a clear idea of which offerings it wants to combine with what specific added value. In other words, the bank must ensure that open banking fits in with its overall strategy, brand positioning and offering strategy.

When implementing open banking, the bank can then consider the following fundamental questions for guidance:

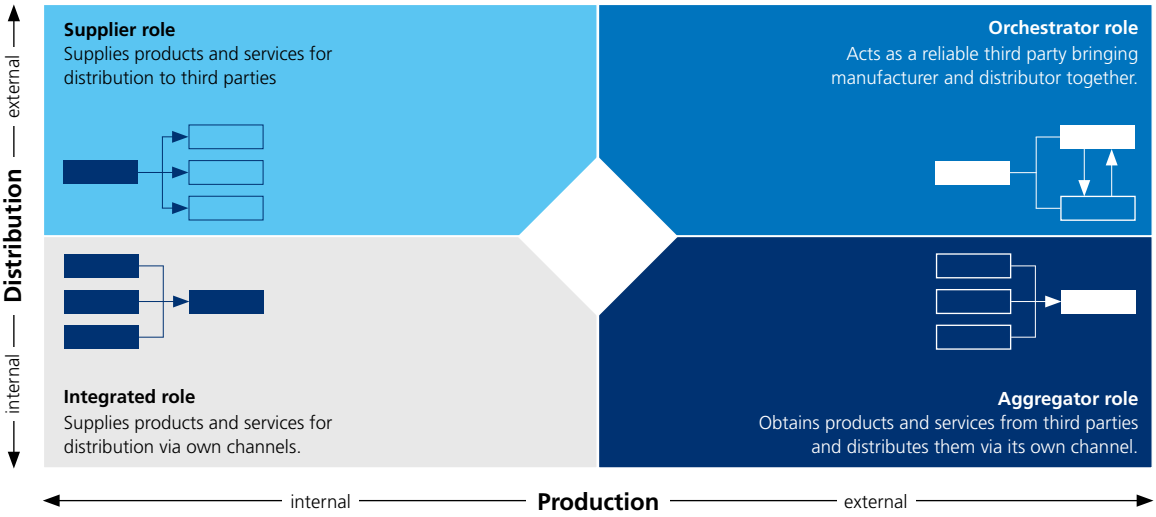
- Which customer segments should the open banking offering reach?
- What offering strategy has been employed for those customer segments until now?
- What added value and product offerings are offered to those customer segments?
- What role do existing "non-banking added values" (e.g. loyalty programmes, tax and cyber security advice services, e-government services) play?
- What customer experiences is the bank aiming to deliver, and via what "user journeys"?
- What price policy is in place for each segment?

Clear positioning of open banking within a bank's offering strategy lays a stable foundation for the later selection of specific partners and services.

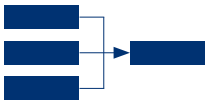
Clarifying the bank's own role in development of offerings

Based on the strategic positioning of open banking in development of offerings, the bank must decide what role it wishes to play in implementation. There are four base models for this, which can be characterised as follows:

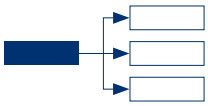
Fig. 2: Possible roles of banks in an open banking ecosystem



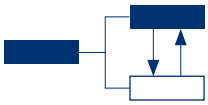
Source: SBA, based on Capgemini (2020). World FinTech Report.



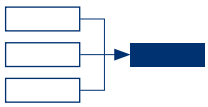
"Integrated role": Typically, established (full-service) banks develop and produce their products and services in-house and distribute them exclusively via their own channels. This integrated approach has worked well in past decades and built up a high level of trust and security among customers. In this model, the banks control the customer interface. Individual services can also be delegated to third party providers via outsourcing. To remain competitive in this model over the long term, comprehensive capabilities are required – in both production and distribution.



"Supplier role": In this model, the bank makes its products and services available for distribution by third parties. The customer interface is controlled by various third party providers. To remain competitive in this model over the long term, efficient production and provision of products and services are required, in order to lower the marginal unit costs (economies of scale).



"Orchestrator role": In this model, the bank acts as a reliable party bringing customer and product manufacturer together. The bank can continue to control the customer interface. To remain competitive in this model over the long term, the bank needs the capacity to integrate third party offerings into its own offering range (such as e-banking).



"Aggregator role": In this model, the bank obtains the products and services from third parties and then distributes them via its own channels. The customer interface is the most important asset. To remain competitive in this model over the long term, "best-in-class" capabilities in UX/UI and a high level of competence in customer acquisition via digital channels are required.

A bank can also take on a number of these roles simultaneously (e.g. integrated model with downstream supplier approach). The bank can potentially also take on the role of platform provider, supplying the infrastructure and information for participants in the ecosystem.

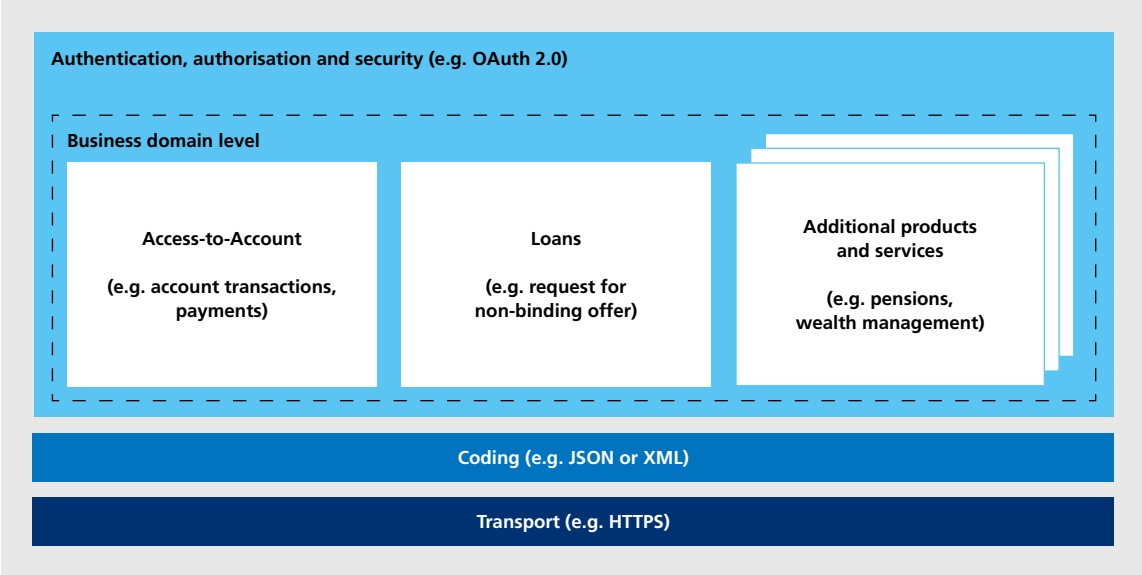
For this to work successfully, all the necessary actors need to be systematically interlinked. This is especially true in product management with the information flows related to the development of open banking. Implementation will only succeed if the bank is able to rapidly assess developments of ideas and offerings, select suitable partners and integrate them in a targeted manner. The bank should specifically aim to build up these capabilities and carefully plan how it is going to do so; this may require investments in new human and technological resources. It may be helpful to work systematically with established third party providers that work closely with the market in the banks' interest and, through their own experience of building a platform, have acquired knowledge about current developments, existing offerings and their success on the market.

Infrastructure – standardising the API

Different levels of standardisation

In Switzerland today, banks are already giving third party providers selective access to their customers' accounts and/or data by opening up the customer interface in the interest of both sides. However, there is no legal requirement for them to do so. For the purpose of further discussion with a view to standardising interfaces and analysing potential solutions, it is important to understand the various interface levels and the degree to which they are standardised.

Fig. 3: Illustration of the various levels of API standardisation



Source: SBA.

The figure shows various levels that come into play when sharing data via APIs. If we take the analogy of data being transferred by post, for example, the transport level is provided by the postal service. This is largely standardised worldwide. The coding level is the document format, e.g. DIN A4. This too is standardised internationally. Authentication and authorisation ensure that only the correct addressee can read the content. Finally, the business domain level is the content of the document. The information it holds and how the addressee processes it will, however, differ markedly depending on the context of the business transaction.

The situation in the digital world is comparable. The transport and coding levels are almost completely standardised at the global level (e.g. HTTPS[5], JSON[6], REST[7]). Likewise, there are standards for authorisation such as OAuth 2.0[8], on which the Swiss open banking solutions also build. Given the countless transactions at the business domain level, this is where standardisation presents the biggest challenge. Some areas, such as payment services, are standardised internationally (e.g. via the international message standard ISO 20022, which SIX is responsible for implementing in Switzerland). For other areas, however, the standards that open banking initiatives can call on are limited in their suitability. This is especially true of topics particularly relevant to Switzerland, such as pensions.

Fig. 4: Comparison of the degree of standardisation of the various standardisation levels

Level	Question	"Postal service analogy"	"Digital world"	Degree of standardisation
Business domain	What information needs to be included, where and how?	Content of the document, varies depending on the context of the business transaction	e.g. Berlin Group NextGenPSD2 XS2A, SFTI Common API, Swiss NextGen API	Depending on the business domain concerned
Authentication Authorisation Security	How is the user authenticated? What is the user allowed to do?	e.g. Privacy of correspondence	z.B. OAuth 2.0, Open IDConnect	Medium (a group of defined and established flows)
Coding	In what structure are the data transferred?	Format of the document e.g. DIN A4	e.g. JSON, XML	High
Transport	How are data transferred?	Postal service and other providers	e.g. HTTPS	High

Source: SBA.

5 Hypertext Transfer Protocol Secure
6 JavaScript Object Notation
7 Representational State Transfer
8 Open Authorization 2.0

Standardisation requires a joint approach

There are already standards on the market for interfaces that allow access to account information and enable payments to be submitted. As a general principle, heterogeneity leads to complexity and therefore to higher costs. In the medium term, it is therefore reasonable to expect a single standard to prevail on the market for each business domain (account information, mortgages, pensions, etc.).

Open standardisation of interfaces is an important precondition for a more comprehensive open banking ecosystem in Switzerland. This will ensure that the various market participants can dock seamlessly, without errors, as well as share and make use of data securely. Standardisation efforts in which everyone taking part is pursuing the same objective are easier to implement than those in which stakeholders with complementary interests and business models are involved. But what, specifically, needs to be considered in order to achieve standardisation?

The first step should be to identify all the stakeholder groups affected and establish their expectations in terms of benefits as well as their concerns. A representative number of actors from each group should be involved, though not necessarily in a continuously active way. Collaboration on an advisory board or as a participant in a "sounding" or "review" can suffice.

The organisational structure of the standardisation initiative will then be geared to the various aspects relevant to open banking: IT, banks' business requirements and the overarching legal and regulatory framework. These various perspectives may best be addressed by setting up working groups focusing on distinct issues, with the various work packages then coordinated with them.

Three strategies for standardisation in Switzerland

There is a choice of three strategies for standardising APIs in Switzerland:

- Adopting an existing standard (e.g. Berlin Group NextGenPSD2 XS2A[9], Open Banking UK[10]).
- Using various existing standards as the basis for a Swiss standard.
- Designing a Swiss standard from scratch.

The first of these is less of an option, because the specific features of payment services in Switzerland are not replicated to the desired degree by any of the currently available standards. The third – designing a Swiss standard from scratch – is very time-consuming and, to the extent that recognised standards already exist internationally, not expedient. That leaves the option of developing a national standard based on and drawing from existing standards. This offers the "best of all worlds", with concepts from existing standards being integrated and supplemented to reflect specifically Swiss circumstances. International interoperability plays a key role here.

Standardisation initiatives in Switzerland

In view of the increasing visibility of open banking, a number of initiatives in Switzerland are now attempting to further advance the standardisation of interfaces and, mostly, develop a Swiss API standard, but without addressing specific issues surrounding the legal and regulatory framework.

9 https://www.berlin-group.org/
10 https://www.openbanking.org.uk/

The current open banking initiatives differ from previous standardisation initiatives in following respects especially:

- They relate exclusively to interfaces via which banks communicate externally: customer-centred services supplied either directly or via third parties.
- Previous initiatives were typically focused inwards. One example is ISO 20022, a message standard for information exchange primarily between banks (or rather between customer-side backend systems such as enterprise resource planning (ERP) systems and banks). Agreed within the sector, it has become the generally accepted standard both internationally and in Switzerland.

Typically, the existing initiatives start out by addressing the issues of account access and payment services, as these have become the focus of attention in discussions surrounding PSD2 (see Glossary). In terms of initial content, therefore, they are comparable, but there are significant differences when it comes to their objectives and the strategies for achieving them. Essentially, the initiatives in Switzerland can be subdivided into the following categories:

- **Standardisation initiatives and knowledge platforms:** These focus on creating an open API standard for Switzerland. They mostly start out from existing international standards (e.g. Berlin Group NextGenPSD2 XS2A) and seek to adapt them for the Swiss financial centre. The primary goal is standardisation at the business domain level. Examples include the activities of Swiss Fintech Innovations' (SFTI) Common API working group and the openbankingproject.ch initiative.
- **Platforms and marketplaces** These initiatives aim to develop a comprehensive operational solution (e.g. platform, API marketplace) for participants in the financial ecosystem (including banks, third party providers and fintechs). The solutions are based either on open standards from standardisation initiatives or proprietary, individual APIs.[11] This category also includes European providers that have gained experience of developing APIs and marketplaces in the context of PSD2 and are now expanding their offering into Switzerland.

11 Current examples include (as of June 2020): SIX b.Link platform, Swisscom Open Banking Hub, inventx Open Finance Platform. In Switzerland, the central infrastructure provider SIX is the only provider currently covering all three key aspects, via b.Link: setting standards, building a platform and supporting TPPs with the relevant technology.

- **Offerings from technology providers:** Most providers of core banking software in Switzerland offer their own marketplaces and platforms based on their own API standards.[12]

Thus there is considerable synergy potential among the individual initiatives in Switzerland, but a degree of competition is also at work. There is already continual exchange between them, with the aim of reducing the large number of APIs to a minimum. The SBA acts as a mediator and coordinator between the various initiatives.

Further elements are being developed as needed

Experience from markets that are already further advanced in developing open banking shows that with the growing adoption of open banking, other elements may become relevant to supporting the development of the ecosystem. Given sufficient demand, it is likely that these will be developed and made available by market participants in Switzerland too. They include, in particular:

- **Dispute management:** Defining a standardised, transparent procedure for dealing with conflicts between parties involved in the open banking ecosystem.
- **Customer experience:** Defining guidelines for a uniform customer experience (e.g. when granting consent).
- **Quality assurance:** Ways of, for example, checking the availability of interfaces.

12 Current examples include (as of June 2020): Finnova Open Platform, avaloq.one and the finstar core banking system from Hypothekarbank Lenzburg.

4. Which legal aspects do banks need to examine?

Requirements depending on the type of arrangement involved

Supervisory law requires banks to maintain an organisation appropriate to their business model and have a corresponding system of risk management in place at all times. Data protection legislation and bank-client confidentiality also impose certain requirements on the sharing of customer data. In order to assess the legal requirements applicable to a specific open banking arrangement, an important distinction must first be made between outsourcing and open banking (see p. 9 above).

If the model involves open banking rather than outsourcing (for which the general, specifically designed rules apply), the next step is to examine the nature and intensity of the interaction between bank, third party provider and customer.

The closer the collaboration between bank and third party provider on open banking, and the more the two emphasise their cooperation and market it to their customers accordingly, the more customers will wish to be reassured that their bank has subjected the third party provider to certain quality audits.

Conversely, there are open banking arrangements in which a bank only forwards a customer's data to a third party provider when the customer has requested it to do so, and the provider then processes the data for the customer in order to offer them added value. The looser the link between bank and third party provider, the lower the requirements in terms of auditing.

Various increments are possible between these two extremes. Open banking may also take place between two or more banks.

The legal requirements applicable to each arrangement must therefore be carefully analysed. The bank should in all cases clarify the following issues in particular:

- **Clear legal foundations** and possibly **contractual agreements** covering collaboration and data flows, both towards the customer and towards third party providers.
- Compliance with fundamental **data protection and data security requirements**:
  - Data protection plays a key role in open banking arrangements, partly due to the legal obligations of both bank and third party provider, and partly with regard to the reputation of the parties involved – and, ultimately, of the entire financial centre.
  - In any event, the data protection legislation allows for the possibility of open banking, particularly when the initiative for data sharing comes from the customer. For that reason, it is especially important for customers to know at all times what data are being shared with third party providers
  - When it comes to data security, the use of standardised interfaces can reduce risks by making established templates available. It is also advisable to keep the interfaces up to date with the latest technology at all times and, together with the third party provider, define processes for dealing with any data leaks, so that everyone involved can meet their obligations if a leak occurs and the customer can be protected in the best way possible.
  - The security standards should be "appropriate" and reflect the latest technological developments and the regulatory requirements imposed by FINMA.
- **Transparency** for customers
  - Customers should be informed at all times of what is happening to their data. Their consent to the transfer of data in each case should be as specific as possible. They should also be informed of the data sharing and consent to it voluntarily.
  - Customers should enjoy transparency and control over the conditions under which their data are accessed (e.g. via a dashboard giving them full control).

It is to be expected that as the collaboration between bank and third party provider grows, the requirements concerning the legal basis for it will become increasingly stringent. In such cases, the following aspects of supervisory law may become relevant:

- Auditing the third party provider for **compliance with regulatory requirements** (Financial Services Act FinSA, authorisation requirements, etc.).
- Auditing the third party provider's **business model** with a view to preventing fraud.
- Auditing the third party provider's **data protection strategy** and data security.

The bank must always examine whether and to what extent the requirements concerned apply to its chosen business model, to ensure that it complies with its supervisory law obligations at all times.

Auditing third party providers

If the intensity of the collaboration between bank and third party provider requires the bank to audit the provider (see previous section), this may be done in a number of ways.

Essentially there are three different approaches a financial institution can pursue:

- **Carrying out bilateral audits of third party providers**, with the bank drawing up a list of criteria based on the regulations. During the audit, every third party provider wishing to access the financial institution's interfaces must demonstrate to it that these criteria are complied with, with the audit being repeated at a frequency determined by the financial institution. This approach allows the audit to be tailored as individually as possible to the needs of the financial institution in question. It can lay down the criteria itself and carry out the audit of its own accord. However, this is likely to be the most time-consuming approach for both sides. It is also very limited in its scalability, since every third party provider would have to undergo a third party provider audit at every financial institution.
- **Standardised third party provider audit by a "trusted party"** which meets the legitimate expectations regarding business form, staff and technical requirements. This approach requires the creation of a "label" that does not yet exist for the Swiss market. However, the SIX's admission test for participants in its b.Link platform is one potential solution. It was defined in close collaboration with banks and third party providers and therefore ensures that all the key audit criteria from the banks' perspective are taken into account. The procedure is applied to banks and third party providers and comprises tests of the company and its technical security infrastructure/precautions. The test is carried out by external parties on behalf of SIX. An assessment report compiled by the external party for SIX forms the basis for SIX to decide whether to let the participant join the b.Link platform. Once the test has been successfully completed, SIX requires an annual update of the relevant information. The test itself need only be carried out once and is then recognised by all participants in the b-Link platform.

- **Relying on existing certifications.** Alternatively, the financial institution could rely on existing certifications such as ISO 27001 when auditing third party providers and complying with its duty of due diligence. These allow a third party provider to demonstrate compliance with certain processes and controls. It should be noted, however, that they were not drawn up specifically for open banking and can therefore only give the financial institution limited information on compliance with security criteria, such as the secure storage of tokens authorising access to customer data. This approach has the merit of efficiency because it is based on international standards, but each financial institution must, in consultation with its internal compliance unit, decide how far the relevant ISO certificates suffice for it to meet its duties of loyalty and due diligence when auditing third party providers. For third party providers that do not already possess such certification and must apply for it, this often involves a significant investment.

Designing the contractual framework

Once a bank and a third party provider decide to cooperate, the next issue is the contractual arrangements. Unlike when outsourcing, the parties in an open banking environment are free in this respect. The contractual agreements will vary depending on the nature and intensity of the interaction between bank, third party provider and customer. The following are some of the points that need to be considered:

- **Rules on the use of data sharing:** What data are shared, and for what purpose?
- **Data protection:** How is data protection ensured at all times?
- **Rights and obligations in relation to access to the interfaces:** Who is responsible for what duties towards the customer with a view to achieving the best possible coordination between the parties?
- **Communication with the customer:** What measures are taken to ensure that customers know at all times who is processing their data, where this is being done, and what the potential risks may be?
- **Rules on incident management:** What process is adopted if the integrity of the data used is compromised?
- **Security standards:** What security standards are applied?

- **Liability:** Who is responsible for what duties towards the customer with a view to achieving the best possible coordination between the parties?
- **Rules on the third party provider audit:** How and with what frequency are third party providers audited?
- **Rules on release management, with particular regard to critical security releases:** How and at what intervals are releases carried out?

As with the third party provider audit, there are also various approaches to agreeing the contractual framework:

- **Bilateral agreements with third party providers:** Here, each financial institution draws up its own contract documentation governing access to its interface and concludes those contracts with every third party provider. This gives the bank the greatest degree of freedom to individualise its contract documentation, but it is time-consuming for the third party provider and the financial institution, while offering little scalability.
- **Definition and conclusion of a standardised contract in a platform setup:** This is a contractual arrangement whereby each party is a participant in a platform and only must sign one contract with the platform operator. It has the merit of scalability. This approach has been adopted by b.Link, for example, with a standardised set of contract documentation that each participant signs with the platform provider, allowing them to then share data with other platform participants.

In summary, the parties involved in open banking arrangements have a great degree of freedom, both in the selection of suitable partners and in the relationship between bank and third party provider.

Glossary

Term	Definition
Access to Account (=XS2A)	Access to customer accounts that banks are required to grant in connection with PSD2 third party providers. Specifically, it involves giving third party providers "non-discriminatory access" to customer accounts via Application Programming Interfaces (APIs), in order to provide Payment Initiation Services (PISs) and Account Information Services (AISs).
Application Programming Interface (API)	An interface between programs designed to facilitate interaction between them via a set of rules and specifications.
Open API	An interface that enables access to data based on a public standard. Also known as an external or public API.
Data	Logically connected components of an information item that can be processed electronically.
PSD2 (Payment Services Directive 2)	An EU directive that, among other things, requires banks in the EU to allow third party providers access to bank accounts. Switzerland is not required to implement PSD2 (either directly or indirectly), as it is not a member of the EU or EEA and no such obligation is contained in the bilateral agreements with the EU.

Further Reading

Accenture (2018). It's Now Open Banking.

BCG (2018). Retail Banks Must Embrace Open Banking or Be Sidelined.

Basel Committee on Banking Supervision (2019). Report on open banking and application programming interfaces.

Capgemini (2020). World FinTech Report 2020.

Deloitte & Business Engineering Institute St. Gallen (2019). Ecosystems 2021 – what will the future bring? Shaping and positioning of the financial services industry. (Report only available in German)

ndgit (2019). Open Banking APIs worldwide.

Institute of Financial Services Zug IFZ (2020). IFZ Fintech Study 2020.

Institute of Financial Services Zug IFZ (2019). IFZ Sourcing Studie 2019. (Study only available in German)

McKinsey & Company (2019). The last pit stop? Time for bold late-cycle moves. McKinsey Global Banking Annual Review 2019.

McKinsey & Company (2017). Data sharing and open banking.

Open Data Institute & Fingleton Associates (2014). Data Sharing and Open Data for Banks.

SwissBanking

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
P.O. Box 4182
CH-4002 Basel

office@sba.ch
www.swissbanking.org