Banking the bits and the bytes

4 steps to a future-proof connectivity strategy for the finance sector

By Ivo Ivanov, CEO of DE-CIX International, the world's leading Internet Exchange operator and interconnection provider

To be fit for the modern world, banks and other financial service providers need to reduce their costs, develop new business models, activate new revenue streams beyond the standard set of financial services, and meet the needs and expectations of increasingly tech-savvy customers. They need to achieve full digitalization. To do this, it is necessary for banks and financial service providers to take a different approach to managing their data – these bits and bytes are the basic commodity of the digital age. These institutions need and want to become the moderator of their customer's entire financial life-cycle, across multiple sectors and value chains. This means that, as part of their journey towards transformation, they need to develop an interconnection strategy.

An interconnection strategy will provide a framework for considering the ways in which the bank wishes to control connectivity with its own digital resources, its partners, and its customers. It is worth breaking this process down into manageable steps in order to test, to gain experience, to understand the benefits of gaining control over the bank's interconnection infrastructure, and to develop a long-term strategy. The following four-step process will help financial institutions to develop their interconnection experience and build their strategy.

1. Starting with the basics – how interconnection helps IT systems to work efficiently and effectively

Before even thinking about the outward-facing systems, the first essential step is to ensure that internal systems are functioning effectively. Connections to cloud resources and applications like Microsoft 365 and Microsoft Dynamics for CRM and ERP systems must be seamless, high-speed, secure, and redundant – so that whatever happens, you still have access to your data and workloads.

Traditionally, cloud resources are accessed over the public Internet, with all the risks that this entails. By making use of a cloud exchange through a secure and high-performance interconnection platform, on the other hand, it is possible to connect the bank's network directly with the cloud provider's network, bypassing the public Internet. This strategy has multiple benefits: not only is the connection – and thus the data travelling through it – protected against malicious attacks against its resources, but also the direct connection means that the data doesn't have to travel so far. Because the further data needs to travel, the slower the response time will be, causing the lag that we sometimes experience on long-distance video calls and conferences, for example. We call this delay – the time it takes for a data packet to travel from a device connected to the Internet, such as a smartphone, to a server in the Internet, and back again – "latency": The lower the latency, the faster the response, and the better the performance of cloud applications and ultimately the user experience.

This is the case for accessing data in the cloud and using applications like video-conferencing systems, and becomes even more critical when it comes to processing transactions. Artificial intelligence applications, such as customer service bots or solutions for AI analytics and process automation, are further applications that need to be sourced from the cloud – and are extremely latency-sensitive. Therefore, direct interconnection to cloud resources and applications is the

foundation for progressive digital transformation. Latency truly is the new currency when it comes to the future of banking.

2. Security first: Interconnect directly and securely with other networks to control data pathways

Clearly, banks need to ensure the security of their systems and their customer data. But they also need to allow their end customers to connect to their services securely. Using the public Internet is a poor choice here, because there is no way to control the pathways that the data takes. The Internet was conceived as a "best effort" tool for communication, which is not sufficient for securing sensitive end-customer data. Therefore, banks need to bypass the public Internet, which they can do by setting up what is known as "peering". This means the direct interconnection between two networks on an interconnection platform (also known as an Internet Exchange or IX) so that they can bypass the long and potentially dangerous route over the public Internet. Peering gives the partners control over data pathways, minimizes the risk of security breaches, and means the data does not need to travel so far, resulting in a significant improvement in latency and thus performance. Peering directly with other networks enables financial institutions to offer their end customers a more secure and high-performance connection to their banking services.

Let's look at a couple of examples: Firstly, a bank customer accesses their account on the Internet banking platform of the bank. Regardless of how secure the banking platform itself has been made, and regardless of how secure the customer's Internet service provider (ISP) is, data will be passed between the two networks via the public Internet. When data travels via the public Internet, it may take long routes to the next point where, by chance, both networks – or their transit providers – are located in the same data center and have a direct fiber-optic interconnection. If, on the other hand, the bank "peers" directly with the customer's ISP, then this entire journey is much shorter and is also shielded against the risks of the open Internet. The data traffic can also be further protected by additional security services provided on the interconnection platform. And that would be the case not only for this customer, but also for every other customer of this ISP.[1]

The same goes for a webshop: A company runs a webshop with integrated payment services from the bank – but the connection of the webshop to the bank again flows over the public Internet. Suppose the company's own network is big enough: in that case, it could interconnect and peer directly with the bank. But SMEs remain dependent on connecting via their ISP. So, the SME and its customers can be best protected by ensuring their respective ISPs interconnect directly with the bank.

3. Meeting the regulatory and risk mitigation requirements for digital banking

With a framework for open banking having been introduced in the revised EU Payment Services Directive (PSD2), which came into effect in 2018, and with other regions following suit, like the US in 2021, banks are becoming obliged to make data available to third parties through their own application programming interface (API). This requirement forces banks to take strategic digital action and is just one of a range of new regulatory initiatives that aim at regulating digital banking. Managing the compliance of company policies and regulations (for example, in regard to data protection) becomes increasingly complex when connecting with a large number of different

[1] In this scenario, the customer would still need to take care of security for their own devices and connecting securely to the ISP, and the ISP and the bank networks secure the data for the rest of the journey.

partners. Here, the traditional method used in the financial sector – connections via MPLS[2] and data transport using intransparent IP transit[3], and bilateral agreements for each and every partner network – becomes a management nightmare. This can be simplified by creating a "closed user group" (CUG) – a private special-interest connectivity ecosystem set up on a secure and high-performance interconnection platform. In this case, the CUG would be under the control of the bank, as the owner. It bypasses the public Internet and securely connects the bank's network directly to the networks of its trusted partners and customers. Compliance with the stipulated policies and regulations can be made a mandatory prerequisite for participation in the ecosystem. In this way, the bank can set policies for all members of the ecosystem, and do so at the click of a button.

One particularly interesting regulatory initiative currently emerging in several jurisdictions is the requirement to mitigate the cloud concentration risk. Clearly, no bank should place all their eggs in one basket, and this goes also for digital infrastructure. To meet the requirements of cloud concentration risk mitigation, having a multi-cloud strategy is essential – and easy to manage without the risk of vendor lock-in if you use a data center neutral cloud exchange that offers a wide variety of cloud providers and services. Even in regions where such risk mitigation is not yet mandatory, it soon will be – and, to be frank, business logic demands that a bank that wants to provide its customers with the best security possible should adopt this kind of concentration risk mitigation plan.

But really mitigating the cloud concentration risk doesn't just stop at using different clouds. Why? Because it is also important to be able to access those clouds from physically independent locations. What help is a hybrid-cloud or multi-cloud strategy if you're limited to one single location to connect to your chosen clouds? If one connection fails, or one data center experiences an outage, you still have a single point of failure. Therefore, digital infrastructure must be conceived of as a distributed infrastructure involving a diversity of providers and multiple redundant pathways. This creates the resilience necessary for critical applications and data. Using a distributed cloud exchange platform which allows a multi-home set-up and a range of providers, as well as ensuring redundant connection to clouds and partner networks from physically separated locations, dramatically increases the resilience of connections and ensures continuous access to critical data.

4. Control the financial customer journey and develop new revenue streams through digital partnerships

Customers are demanding easy-to-use digital systems and flexible access to banking products, and are more willing to shop around for a better deal – for example, through the growing range of FinTech companies on the market. And with increasing competition from new players, banks and other financial service providers need to look into creating new revenue streams. One potential option is offering their services and products to new customer groups (e.g. in different geographical regions or for specific niche markets) through partners. They can develop their own payment service to be embedded in webshops. Banks can sell their services as white-label

---

[2] Multiprotocol Label Switching (MPLS) has been used for the past two decades for enterprises and banks to connect their branch offices to their headquarters. By labelling each data packet, MPLS allows critical data to be prioritized for transport. However, it is extremely inflexible, with waiting times of weeks to months for the implementation of an MPLS circuit.

[3] In IP transit, a customer (here, the bank) orders a bandwidth of connectivity to the Internet via a carrier or telecommunications provider. This transit provider then connects to other networks in order to pass data traffic through the public Internet. Downsides to IP transit include the cost and the fact that, because the telecommunications provider cannot connect to the entire set of networks that make up the Internet, the data traffic will be sent via multiple further networks across the Internet to reach its destination, with no control over the routing – therefore reducing both the speed (latency) and the security of the data traffic.

products, so that another bank (e.g. a Neo bank) can brand them accordingly and sell them on to new customer groups. They can – and in Europe and the UK are now obliged to – offer FinTechs access to customer data (on request and with consent) to be embedded in financial management and other types of applications, using an API based on open banking. What's more, by separating customer management from service management, they can also offer their services through partner banks to customers in other geographical locations, where they themselves do not have a banking license.

What all of these activities have in common is the need for open standards and interoperability, combined with highly secure and low-latency interconnection between the partners. The bank may want to make its banking infrastructure available to third parties for new products and services – but to do that, it must first ensure its digital infrastructure is up to the task.

There are many options, but the bottom line is this: For banks to become truly digitalized, they need to nurture a secure and private interconnection ecosystem with their trusted partners. By connecting with this ecosystem in a "closed user group" (CUG) set up on an interconnection platform, banks have all the benefits of peering, with the added advantage of an exclusive environment completely removed from the public Internet.

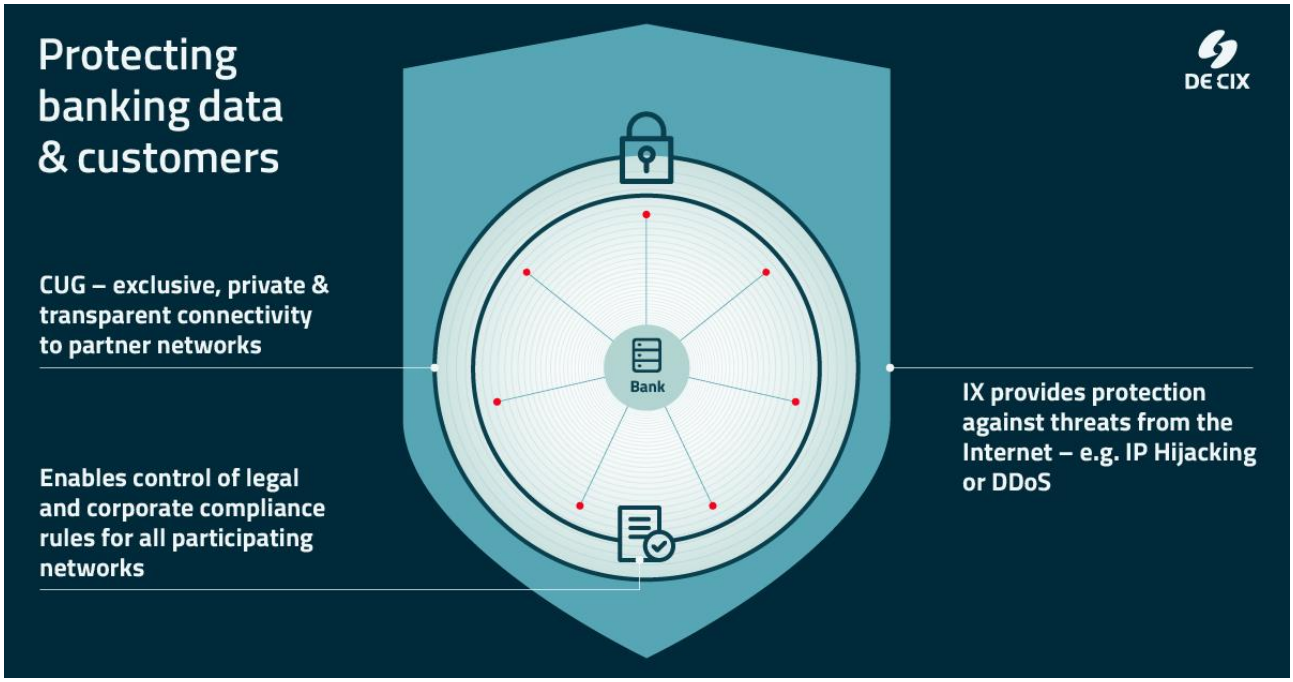

Figure 1: By creating a 'closed user group' (CUG), a bank can interconnect securely with all of their partners and ensure compliance with legal regulations and corporate policies. In addition, the CUG bypasses the public Internet, increasing the level of protection against cyber threats.

Another extension of this concept is the development of multi-cloud set-ups using workloads and computing resources involving multiple cloud service providers, accessed and managed via a cloud router service, something which has become part of the offering on well-developed interconnection platforms. This can be managed easily and at extremely reduced latency, therefore improving the performance and usability of cloud-based resources.

Conclusion: Take control of the financial data journey by controlling the digital infrastructure it travels through

Where does this leave us? We have seen that there are many benefits to digitalizing banking and financial services, and a range of risks that need to be mitigated. If they want to maintain their dominance in the financial sector, banks need to secure and control their network interconnections so that they can develop new revenue streams and business models.

In a nutshell, direct connections to other networks improve the speed, performance, and security of data transfer between partners. The bank or financial institution can connect with all of its required cloud partners securely, efficiently, and redundantly, and so properly mitigate the risk of cloud concentration. Beyond this, the diversity of infrastructure partners on an interconnection platform that is not only distributed, but also data center and carrier neutral, increases the redundancy and reliability of connections to resources and partners, and mitigates the risk of vendor lock-in and a single point of failure. Finally, to generate new revenue streams, the institution can create its own private and secure interconnection ecosystem of partners (a 'closed user group') which bypasses the public Internet. The interconnection platform can thus function as a one-stop shop for all the bank or financial service provider's interconnection needs throughout its journey towards full digital transformation.