NOMENTIA

WHITEPAPER

THE ADVANTAGES OF GLOBAL BANK CONNECTIONS AS A SERVICE

CONTENTS

A corporation’s connection to a bank is at the core of its operations. To be in business, you need to have a relationship with at least one bank and a solution for sending payments and receiving account information. Processes relating to cash outflows and inflows obviously need to be secure and run without interruptions. In addition, Treasury needs reliable and up-to-date data on transactions and account balances for accurate analyses, forecasts, and financial and business decisions.

Considering the critical importance of bank connectivity, surprisingly many corporations are still making do with online banking tools and manual processes for uploading and downloading data.

I. INTRODUCTION

Are Your Bank Connections Outdated?

The reality is that most organizations have multiple banking partners and therefore need to interface with a variety of bank communication channels. This translates, at worst, into a lot of manual work sending payment files and gathering account balance data. If the process is automated but the integrations are hosted on-premise, the IT department and Treasury have to deal with a considerable maintenance burden to keep the solution up-to-date and operational.

The bank connectivity solution impacts the fluency and security of your payments and on the efficiency of your daily routines in cash inflow processing. The chosen technologies also play a role in enabling straight-through-processing of payment files and account statements. Centralized bank connections help lay the foundation for improving cash visibility across your entire organization, and they can be the first step toward payment centralization, for example setting up a payment factory or an in-house bank.

This whitepaper focuses on explaining the benefits of modern bank connectivity as a service. We will explain different connectivity options, go over the things to consider when launching a connectivity project, and point out what to focus on when choosing a service provider.

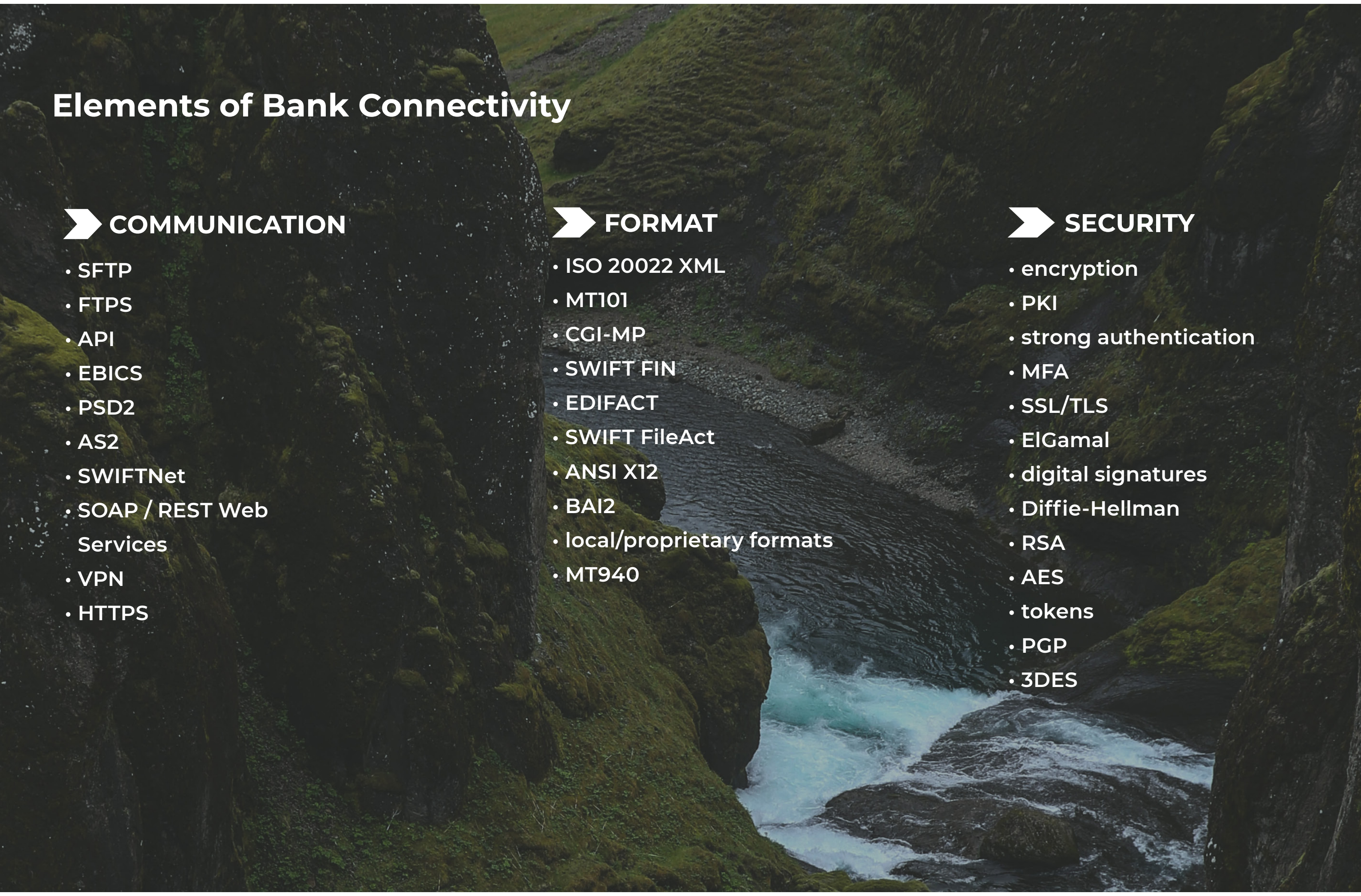
23%

of corporations originate payments from 11 or more banks*

**Source: Strategic Treasurer’s 2017 B2B Payments & Working Capital Survey*

II. BANK CONNECTIVITY IN A NUTSHELL
Technologies, Formats, and Security

There are numerous ways for a corporation to connect to a bank, from using online banking portals to direct host-to-host connections and connecting via the SWIFT network. In practice, a bank connection always consists of three parts: the technical connection for the communication between the bank and the corporation, the formats for the cash management messaging, and the information security and encryption practices.



Elements of Bank Connectivity

COMMUNICATION

- SFTP
- FTPS
- API
- EBICS
- PSD2
- AS2
- SWIFTNet
- SOAP / REST Web Services
- VPN
- HTTPS

FORMAT

- ISO 20022 XML
- MT101
- CGI-MP
- SWIFT FIN
- EDIFACT
- SWIFT FileAct
- ANSI X12
- BAI2
- local/proprietary formats
- MT940

SECURITY

- encryption
- PKI
- strong authentication
- MFA
- SSL/TLS
- ElGamal
- digital signatures
- Diffie-Hellman
- RSA
- AES
- tokens
- PGP
- 3DES

COMMUNICATION

The right choice of the bank connection channel depends on your organization's operating environment, banking strategy, and payment volumes, among other things. The requirements will also fluctuate as your business develops. At the end of the day, your connectivity solution should be able to scale in step with your business, enable straight-through processing of payment and account data, and ensure security and visibility.

In most cases, the most suitable and cost-efficient option is a combination of different channels in different geographical areas. For instance, if there are high payment volumes in a country, a direct connection can be the smartest choice in that market, whereas an organization with a globally centralized payment process is better off with a single-channel connection to the SWIFT network. Or you can utilize a host-to-host connection with your house bank and complement the solution with SWIFT to reach additional banks.

One thing is for sure: With the risk of fraud increasing, manual uploads of payment data to banks should not be a part of a modern corporation's bank connection strategy. In addition to being a slow and error-prone process, manual data entry means taking unnecessary risks and leaving the payment files vulnerable to tampering and fraud attempts.

Connection through regional standard protocols

- Includes EBICS (Electronic Banking Internet Communication Standard) which is mandatory in Germany but also in use in France, Austria, and Switzerland.
- Reach all the banks in a specific region with a standardized, secure and harmonized infrastructure.
- A standard communication channel is quick and easy to integrate.

Host-to-host connection

- A secure, affordable and reliable way to connect when the connections are implemented and maintained properly and updated regularly.
- The setup is always bank and customer-specific. The bank dictates the communication protocol(s), formats and security.
- Typical technologies used to build host-to-host connections include SFTP, FTPS, AS2, and Web Services (SOAP/RESTful)
- Today, SFTP is one of the most popular choices by the banks to provide connectivity. Often, SFTP is bundled with PGP encryption for improved security at the file level.
- SOAP-based traditional Web Services are popular especially among the Nordic banks. Now, the more modern RESTful Web Services are gaining in popularity with the second Payment Service Directive 2 coming into effect.

SWIFT connectivity options

- Worldwide SWIFT (Society for Worldwide Interbank Financial Telecommunication) network can be accessed through a SWIFT Service Bureau, a direct integration to SWIFT, or through a ready-made integration in a certified third-party system (Alliance Lite2 Business Application).
- A single channel solution to reach in practice any bank in the world for exchanging cash management and trade finance messages.
- A direct connection to SWIFT is costly and requires time and resource-demanding integration. On the other hand, with Alliance Lite2 Business Application, the connection is immediately operational, maintained for you and affordable, even with low volumes.

FORMAT

It has been said that the nice thing about standards is that you have so many to choose from. Treasurers and Finance professionals who are operating in an international business environment can undoubtedly agree. In a global environment, there are a myriad of country and bank-specific formats as well as developing industry standards according to which the payment data and account statements are being sent and received to and from banks.

In a multibank environment, different payment formats in different countries can even become a hurdle for streamlining the corporation's payment and account reconciliation processes and obscure cash visibility. Again, there are no right or wrong choices. You need to look at the requirements of your business, your system environment, and your banking partners, and also be prepared to adapt to changes as the standards evolve.

The safest choice for a multinational corporation today is the international ISO 20022 standard. Other traditional and popular formats in corporate-to-bank connectivity, such as SWIFT MT and EDIFACT messages, as well as local formats, have been losing popularity since ISO 20022 standard for financial messaging was published in 2004. The ISO 20022 standard is already widely supported and it is recognized as the standard of the future in the industry.

ISO 20022 standards contains a multitude of message schemas to be used in different business areas. All of them are based on XML (Extensible Markup Language). Currently, the most relevant formats for payment and cash management messaging between a corporate and a bank are:

- pain. 001.001.03 for payments (corporate-to-bank)
- pain. 008.001.02 for direct debits (corporate-to-bank)
- pain. 002.001.03 for payment status reports (bank-to-corporate)
- camt. 052.001.02 for intraday account report / balances (bank-to-corporate)
- camt. 053.001.02 for end of day account statements
- camt. 054.001.02 for debit and credit transaction details

It is also good to notice that while some banks offer state-of-the-art connectivity options, they only provide support for a limited amount of formats in that channel. First of all, you should always double-check that the formats you need are actually available in your chosen connectivity channel. Secondly, you should also check that the content and quality of the data is what you need.

What about APIs and the open banking promise of PSD2?

In September 2019, the second Payment Service Directive, PSD2, came into force, requiring European banks to open their Application Programming Interfaces (API) for service providers along with Strong Customer Authentication (SCA). It is a major disruption in the banking ecosystem and will open up new possibilities for corporate-to-bank connectivity as well. The biggest benefits are instant reporting with real-time account balance data and real-time payments.

Banks are on the journey to developing their APIs and planning strategies for open banking. In the first phase, the data that becomes available based on the minimum requirements of PSD2 will in most cases not be sufficient for corporations' payment and cash management processes. For the time being, APIs do not in most cases sufficiently cater for traditional corporate-to-bank connectivity needs. Neither do they allow sufficient reporting according to the ISO 20022 standard. Nevertheless, APIs do already enable new innovative services, such as real-time payments and balances. It is safe to assume that the existing bank connectivity technologies and APIs will coexist for a long time.

SECURITY

As your banking connections are the concrete channel for cash outflow processes in your organization, security should be a paramount concern. Banks and financial institutions offer a variety of methods for information security, but at the end of the day, it should be you who defines the level of security practices for the connectivity based on your organization's security and fraud prevention policies.

In addition to ensuring that the bank connection itself is safe and the data being transmitted is encrypted and validated (whether the connection is hosted on-premises or on a cloud platform), user rights management is a key security topic. There are a number of ways to authenticate users who authorize payment files. When establishing a secure cash outflow process, it is important to carefully manage the balance of securing payment processing and ensuring automation and usability.

Encryption

Encryption is used to scramble data so that it can be unscrambled only by someone in possession of key information. Encryption is done using ciphers which are sets of algorithms to make the data non-readable. In symmetric encryption, a single key is used with ciphers to both encrypt and decrypt data. In asymmetric encryption, encryption is based on a key pair: a public key is used with ciphers to encrypt data and a matching private key that is used to decrypt data. Since the keys play a critical role in encryption, it is very important to protect them from being stolen.

Any modern bank connection should enable encryption of the bank communication channel and preferably also the encryption of the content of the exchanged messages. Utilizing encryption on both levels provide protection for data in transit and data at rest.

Typically bank communication channel encryption is provided by the most commonly used HTTPS and SFTP protocols. Encryption of the content is a good practise especially if payments are processed as files (like in SFTP).

Digital Signatures

It is important to make a distinction between encryption and digital signatures. While encryption guarantees that the message has been exchanged safely, digital signature authorizes the content and ensures the integrity and non-repudiation of the message. This is obviously essential in the context of digital payments.

There are various options for digital signatures, ranging from personal tokens to corporate signature solutions. A personal token is personal, as the name states, and corporate signature (sometimes referred also as a corporate seal) is granted on a corporate level. Cryptographically, both approaches are equally strong. The difference is in the way the keys that are used for signature are distributed and maintained.

- Personal tokens provide the security for the individual but they bring about a cumbersome maintenance process. Maintaining the physical devices – worrying about losing them, replacing old ones, and ordering new ones for new employees – can cause a lot of work especially in global corporations who have relationships with dozens of banks.
- Corporate signatures are as secure as personal tokens when implemented appropriately, but they provide greater flexibility because you do not need to manage the physical devices. Corporate seals are a good solution when implementing a payment factory or a cash management solution with sophisticated user right management.
- Two-factor authentication via a mobile device is a more and more popular solution. It does not matter from the security perspective whether the authentication is provided by the bank (distributed signature) or by the payment factory supplier that processes your payments. Two factor authentication (or authorization) can be a part of corporate or a personal solution.

If you need to use the services of multiple banks, it is better to have centralized user rights management in your cash management or payment factory solution than to build multiple different solutions with each of the banks.

Whichever encryption and signature method you choose, attention should be paid to the cryptography strength. Some algorithms in the market have reportedly computational weaknesses and other vulnerabilities. When using a connection that is widely adopted, such as any type of SWIFT or EBICS connection, corporations can rely that the community has chosen to use strong enough algorithms. However, organizations like SWIFT or OWASP (Open Web Application Security Project) also offer information about best practice algorithms for those who want to be absolutely sure.

Things to figure out before deciding on your new bank connectivity solution

When you start to consider implementing a new bank connectivity solution and compare the different ways to connect, your first step should be to take a close look at your organization's banking strategy and examine the existing ways of sending payments and collecting accounts statement to and from your banks.
connections for your organization.

- The number of banking relationships. Make a list of all the banks your organization is connected with. Implementing a new connectivity solution is an opportune time to rationalize your banking infrastructure.
- The number of local business entities with connections to banks. Especially in a scattered operating landscape, it can be hard to gain an overview of the different payment processes in different countries and subsidiaries.
- The number of source systems. Paint a clear picture of your IT environment and the different source systems that are using payment data and account statement files (ERP system, Treasury Management system, Accounts Receivable solution...)
- Payment volumes and types. Find out the details on your banking activity, payment volumes, and payment types. Are you using the connections for supplier payments, bank statement reporting and/or trade finance messages?
- The number of file formats. Figure out all the different formats that are currently exchanged between your organization and the banks in different countries.
- Information security. Map out your current information security and encryption practices. Are you, for example, managing a number of bank tokens? With the implementation of a new connectivity solution, it is a good idea to focus also on updating and harmonizing the security of your corporate-to-bank connection.

When scoping a project, it is equally important to map out the future needs of your business and consider how the connectivity options and technologies affect the broader cash management roadmap in your organization. In the next chapter, we will discuss bank connectivity as a service and explain why it is the ultimate way to ensure future-proof bank connections for your organization.

III. WEIGHING THE OPTIONS

The Benefits Of Bank Connectivity as a Service

As detailed above, developing and maintaining corporate-to-bank connectivity requires extensive and up-to-date knowledge of connection technologies, payment traffic formats, and information security practices. It is an exhaustive exercise for any corporate Treasury and IT department.

If the bank connections are hosted and maintained in-house, it is a justifiable question to ask if this is something that the Treasury, Finance, and IT in your organization should spend their resources on? Very few organizations have real competence to implement and also systematically maintain these integrations.

A multibank structure gives corporate Treasury greater flexibility, helps diversify risk exposures, and supports business across locations. Even when working with multiple banking partners, it is a best practice for Modern Treasuries to opt for a single-point-of-access to handle company-wide cash outflow and inflow processes and manage related data. The advantages of multibank connectivity can be best achieved when the bank connections are acquired as a service.

#1 Get plug-and-play connectivity

IT is a scarce resource in many corporations. Implementing bank connections on-premises requires working through cumbersome integrations of technical banking messages and protocols to back office systems, which takes time, effort, and specialized know-how.

An experienced service provider can guarantee efficient, best practice integrations while you can avoid the myriad of technical specifications and the complexity of the integrations. Instead, you can concentrate on discussing the payment and account services in detail with your chosen banks and focus on the payment types and formats that are needed to support your business.

And if you later need to switch banking partners or add new connections, a service provider with ready-made connections can react and cater to the request more quickly than in-house IT.

#2 Pay as you go

The “As a service” approach has a lower cost of entry than implementing an on-premise solution. Instead of paying fixed capital expenses (CAPEX) you can choose a pay-as-you-go model where you are paying a variable operational expense (OPEX) based on your real usage of the service. The indirect costs of an in-house solution tend to balloon: after implementation, resources are needed in maintaining and updating the solution.

#3 Get round-the-clock monitoring

One of the biggest benefits of bank connectivity as a service is that the service provider takes the responsibility to continuously monitor the service and guarantees the availability according to the Service Level Agreement. Unless you have dedicated resources in your IT department, it is hard to reach the same level of support with an in-house set-up – especially in a global environment. If there are hiccups on a bank’s end of the connection, for example, your service provider will be quickly aware of the situation and take action to communicate it. In addition, a best-of-breed connectivity service includes alerts for transactions, keeping Treasurers and Finance professionals up-to-speed on the status of data transmission and informing on any failed attempts to send payment files or collect account statements.

#4 Get end-to-end security

Corporations' supplier payment processes remain an attractive target for cybercriminals. Thus, ensuring the security of your bank connections is paramount. Cloud platforms are heavily audited for vulnerabilities according to industry certifications and the connections between source systems and the platform are encrypted, which cannot always be said about the file transfers from ledgers to the banking software in a corporation's internal network. Eliminating manual work with automated data transfers will also eliminate the possibility of someone tampering with your payment data before sending it to the banks.

#5 Get futureproof functionality

Keeping up-to-date with all the bank regulations and developments in connection technologies, standards, and security protocols requires commitment. By choosing bank connectivity as a service you make sure that your solution is built according to best practices and that it is updated regularly. A dedicated service provider is following the development in the industry closely, keeping you up-to-speed on any coming changes or new possibilities that might have an effect on your connectivity.

IV. SIX THINGS TO FOCUS ON

Choose The Right Service Provider

Bank connectivity is a critical business function at the core of cash outflow and inflow processes, and each corporation has its own unique requirements for bank connections. When purchasing bank connectivity as a service, you need to find a partner with the right combination of technologies and expertise to manage your connections efficiently and in a way that best supports your business' current and future needs.

Here are the most important questions to focus on when choosing a service provider.

1 Does the service provider offer a variety of connectivity options to suit your specific needs?

- Proven expertise on establishing host-to-host connections in and out with different protocols and formats.
- Look for options of effortlessly joining the SWIFT Network and other available single-channel solutions

2 Do they have proven experience in format conversions and integrations?

- Check the service provider's ability to handle industry standards, such as ISO 20022 XML, but also regional and local bank formats and the conversions needed to meet the different requirements of your ERP, financial management and other systems.
- Look over their library of predefined formats and ask for experience in overcoming the special characteristics and expectations in your operating environment.

3 How independent is the solution?

- Go through the systems used for supplier payments, balance statements, trade finance, and forecasting, for example, and make sure the service provider has the competence to establish secure integrations to all of them.
- Does the bank integration layer allow automated workflows with your key systems?

4 Can the service provider ensure end-to-end security?

- Ask for the certificates against which the service provider's platform is audited and check if the security is regularly audited by independent professionals. Pay attention also to the encryption and digital signature technologies used to secure connections.
- Assess the solution's capabilities for user rights management and authentication to be able to build best practice security for your payment processing.

5 Do they monitor the service and guarantee availability?

- Especially if you are operating in a global environment, ensure 24/7/365 support for your bank connectivity.
- To guarantee continuous support for your business, examine the Service Level Agreement and make sure the service provider takes the responsibility to monitor the connections, alert on failed transactions and ensure disaster recovery.

6 Are they experts in cash management and offer a best practice solution?

- Centralizing bank connections is a key element in wider harmonization of cash management. Examine if the service provider has the expertise in payment and liquidity management to help you build a best practice approach to your cash outflow and inflow processes.
- Can they support you in the next step and offer solutions to make the most out of the centralized transaction and account data, with cash forecasting, payment, and account reconciliation solutions, for example?

V. TIME, COST, AND CONTROL

Building a Business Case for Global Bank Connectivity

Weigh in at least these benefits when calculating a business case for bank connectivity as a service in your organization.

- **Savings on implementation time and cost.** By connecting to a cloud platform, you get a flexible turn-key solution for bank connectivity. No need for local installations of software. You will also ensure your solution is scalable and new integrations can be done quickly and cost-efficiently when your business evolves.

- **Reduction on maintenance work for the IT department.** Bank connections, technical messages, and protocols are configured, hosted and maintained in one place by the service provider. They also keep up-to-date on the development of formats and standards and take care of necessary upgrades on your solution.

- **Freeing time for more value-adding work in your Treasury and Finance department.** By automating the messaging with your banking partners to collect account balance information or to send approved payments to banks, you save time on manual routines. Data on cash outflows and inflows is quickly available for efficient use in cash forecasts, accumulating additional benefits from improved liquidity planning.

- **Preventing payment fraud.** The service provider takes care of vulnerability and penetration testing of the platform and ensures security protocols are up-to-date. Automated and secure file transfers prevent tampering with payment files before they are sent to banks and eliminate so-called man-in-the-middle-attacks, which can be costly.

- **Independence of ERP systems and banks.** With bank connectivity as a service, you are not tied into one ERP or financial management solution. You are also free to choose and switch your banking partners, independently of your connectivity solution. This gives you more room to choose the most cost-efficient channels on each of your markets, for instance.

- **Ensuring availability and minimizing downtime.** The service provider monitors the connectivity and provides continuous support, alerting you and reacting quickly if there are, for instance, interruptions in the banks' services.

VI. AFTERWORD

Toward Cash Management Harmonization

If you wanted to sail across the ocean, would you train your workforce how to build the ship and sail before your journey? Or would you just buy a ticket and hop on board a ready-built, secure, and state-of-the-art vessel?

There are plenty of reasons why modern corporations tend to favor business support processes as a service.

Bank connections should be no exception. The best way to reap the true benefits of multibank connectivity is to choose them as a service.

For Treasury, centralizing bank connections can be the first step toward streamlining AP and AR processes on a group-level. Corporate-to-bank connectivity has also a key role in accurate cash forecasting. On the other hand, reducing connectivity costs and operational risks, increasing automation and security in payment processing, and improving visibility to cash balances should be reason enough for any corporate Treasury to take action to modernize their bank connectivity.

Now more than ever, being able to forecast your group's future funds while minimizing costs is key.

Author

Markus Makkonen
Product Manager

Markus has 10 years of experience from international and complex payment factory projects. Currently Markus is working as the product manager of Nomentia Cash Management Platform and bank connectivity.

NOMENTIA