Advanced identity and mandate management as a service

Treasury business processes with tailored banking controls

Faced with increasing security concerns and risks of internal fraud, corporates and banks are looking for ways to extend controls on their banking communications. Banks have responded to such needs with advanced user identity and mandate management services, traditionally limited to their online banking channels, now also available on their direct connectivity channels.

Corporate treasurers and banks face a wide range of security, audit and traceability challenges. In a global business environment, corporates and banks share multiple banking relationships and accounts, across multiple jurisdictions. Just to enable the company's day-to-day operations, it is necessary to authorise multiple individuals, at various levels of seniority and across a spread of remote locations, to manage those banking relationships and accounts.

Treasury management today requires effective and on-going oversight not only of the actions of the (perhaps dispersed) community of individuals authorised to move money out of their company's bank accounts, but also of the wide range of tokens and devices that they use to achieve that aim. Each banking relationship may require the use of proprietary solutions in conjunction with the treasury's own processes. In a global operation, there is also scope for latencies in reporting processes. And yet no payment-specific authentication can be allowed to compromise on-going business efficiency.

Contents

Register for a webinar

Contact us

Share

Print

There is a further complicating factor. By definition, the authorisation process delegates the discretion to transact, in real time, in accordance with the company's operational needs. Reporting requirements must be rigorous, and compliant across jurisdictions, but they must also enable individuals to act with an appropriate degree of autonomy. If an authorisation process fails, control of company assets may fall into the hands of criminals. Treasuries and banks share responsibility for managing and protecting corporate liquidity in equal measure. Both are responding to the challenge.

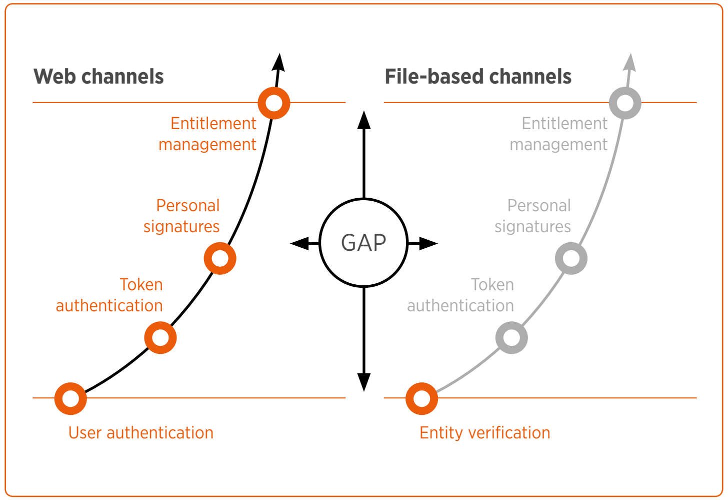
Fraud: the enemy is inside

Unfortunately, there is plenty of evidence that authorisation processes do fail. According to a study by Kroll Business Services, around 60% of fraud is committed by trusted, authorised employees who can escape detection for years. Indeed, such criminals are typically caught only by accident, rather than by the belated operation of an oversight system. Nor is the scale of fraud proportionate to the seniority of the individual committing it. An employee responsible for processing cabin crew allowances at Singapore Airlines was found to have transferred $35 million to his own bank accounts over thirteen years before being caught by chance.

Commenting on that case, the Commercial Affairs Department (CAD) of the Singapore Government described it as "a typical corporate fraud". It was typical, the CAD explained, in that it involved "a trusted, long-serving employee; superiors who failed to carry out proper checks; loop-holes in the system; and accidental discovery". If that is typical, corporates may be in trouble without knowing it. Another notable feature of the Singapore Airlines fraud was that the perpetrator had been a trusted employee of the airline for 12 years before he made his first fraudulent transfer.

Industry practice today: Variance between the online and file-based channels

Corporates and their banks have worked together for a long time to achieve effective controls over their banking communications, both to provide effective liquidity management and to detect and eradicate fraud. Technology has always been important, with internet-based tools taking increasing prominence. Banks now offer sophisticated identity- and mandate-management services, although historically these have tended to be developed to support the evolution of their online banking channels.



▲ Banking channels – industry practices

As a result, today there can be significant variance in the implementation of individual approvals for online banking provision, and for direct file-based channels whether these are on SWIFTNet, using local networks and domestic protocols or via proprietary host-to-host services offered by banks.

Contents

Register for a webinar
Contact us
Share
Print

It is becoming more and more standard practice to use two-factor authentication for online banking communication, using a password and a physical device. In some markets, this is or is becoming mandatory. In January 2013, for instance, the ECB (European Central Bank) issued a report recommending a robust set of guidelines in the fight against payment fraud. The report highlights the importance of clear operational traceability: "Payment Service Providers (PSPs) with no or only weak authentication procedures cannot, in the event of a disputed transaction, provide proof that the customer has authorised the transaction. PSPs should implement effective processes for authorising transactions, as well as for monitoring transactions and systems in order to identify abnormal customer payment patterns and prevent fraud."

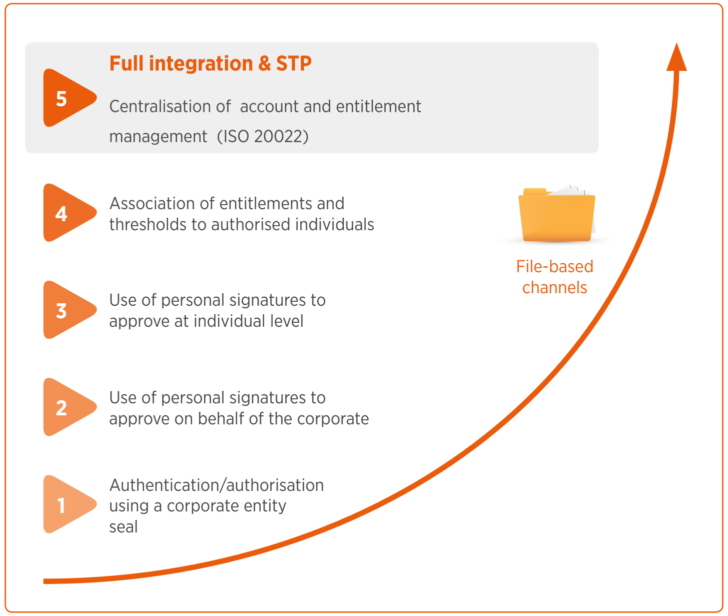
At the corporate end of an online communication channel, the physical device – the token – will typically be used for authentication of the authorised individual, and then to attach a signature to the transaction or payment event.

There may be multiple individuals at the corporate, each of whom has a different entitlement to instruct the bank and a different payment limit. At the bank end, the receiving bank will have in place a reference set of user profiles, linked to both user and token, which detail the entitlements and limits on what each user (with token) may do.

By contrast, where a corporate uses a file-based channel, industry practice so far has typically been to apply a single authentication stage. The file may be sent via a very secure channel, such as SWIFTNet, but the receiving bank will then only authenticate that the file does genuinely come from the corporate entity.

This is changing. Banks are extending their offering to a scale of four, and working towards five, levels of practice and mandate-management services for file-based channels:

The 5 levels of practice & mandate management services


5
Full integration & STP
Centralisation of account and entitlement management (ISO 20022)
4
Association of entitlements and thresholds to authorised individuals
File-based channels
3
Use of personal signatures to approve at individual level
2
Use of personal signatures to approve on behalf of the corporate
1
Authentication/authorisation using a corporate entity seal

▲ The 5 levels of practice & mandate management services

Practice level 1

Using a corporate entity seal

The first stage is the authorisation and authentication of the corporate entity using a corporate identity seal; the bank will verify that the file indeed comes from the corporate entity, but will process the instructions without further validation.

Practice level 2

Use of personal signatures to approve on behalf of the corporate

Secondly, there is the addition of physical tokens whereby individuals will add an electronic signature to the file sent to the bank. Individual

Contents

Register for a webinar
Contact us
Share
Print

staff will be in charge of signing the files with a token but this signature is on behalf and at the level of the corporate entity; at processing time the bank will only verify that the instructions were sent with a valid token assigned to the corporate customer but will not associate the token with personal signing authorities.

Practice level 3

Use of personal signatures to approve at individual level

The third level enables the bank to authenticate not only the corporate entity but also, separately, the individual by reference to a database of corporate signatories; signatories within the corporate use personal tokens associated with them for signing and approving transactions.

Practice level 4

Control of individuals' entitlements and thresholds

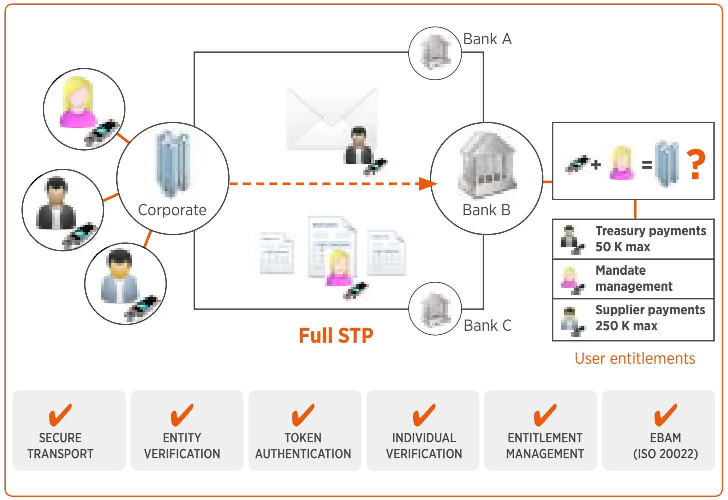
At the fourth level, banks offer mandate management services via the association of entitlements and thresholds with authorised individuals. Banks will authenticate the user identity and their profile before processing any transaction.

Banks may also offer services outside the file channel to provide an additional approval step prior to executing the received instructions. In such an implementation the file is sent over a secured file channel from the corporate entity to the bank. Before processing, the bank will wait until an authorised corporate signatory approves the instructions, typically using the banks web portal. The bank account management is currently performed in either of two ways. In the manual world, an amendment will be made to the annex of the electronic banking contract containing the list of authorised signatories and signing powers. But increasingly, electronic tools are being made available by banks to enable corporate users to self-maintain their signatories and entitlements. Such tools open the need for a fifth level whereby corporates can harmonise the administration of signatories and account management.

Practice level 5

Centralisation of account and entitlement management

The fifth level features the centralisation of account and entitlement management via ISO 20022. This fully integrated STP level enables corporates to use the same approval system with all their banking partners. Corporates can use electronic bank account management (eBAM) tools over SWIFTNet to manage signatories. Here, the solution moves from being proprietary bank-specific to being a multi-bank process.



▲ Centralisation of account and entitlement management (ISO 20022)

Banks are increasingly making available these further levels of authentication for file-based communication in response to corporate demand. For the bank it is also important to have in place effective procedures to ensure traceability and guarantee that only individuals entitled to do so have approved the banking instructions. Moreover, such capabilities are becoming a source of competitive advantage and revenue generation for banks. "We wanted our banks to be able to identify who's signing the file," says John Colleemallay, senior director – group treasury & financing, Dassault Systèmes. Provision is also increasingly delivering entitlement management linked to file signature. "For us, it is very important to do the right profiling of authorised persons within the corporates," says Carmela Gomez, head of global transaction product, BBVA.

File-based channels are coming into alignment with online banking provision in terms of security. Individuals and their authorisation

Contents

Register for a webinar
Contact us
Share
Print

thresholds are now factored into file-based authentication, and this enhancement of industry practice promises to deliver efficiencies including a probable reduction in the scope for fraud. The final, fifth level of authentication addresses another key issue: corporates must still handle multiple banking relationships.

Standards as enablers

Like many critical financial management processes, identity and mandate management is most efficient when standards are used to support centralisation, rationalisation and simplification. SWIFT has traditionally played an essential role in enabling interoperability with a range of standards and solutions simplifying banking communications. SWIFT's internationally recognised standards help corporates to reduce costs and risk, increase funds visibility and improve automation. This facilitates regulatory compliance. Today the global adoption of SWIFTNet as a secure communication channel for corporates is increasing with more than 1000 corporates connected and communicating with their banking partners on behalf of approximately 40,000 legal entities, using standards such as corporate identifiers (BIC) FileAct (pain, camt, acmt) and FIN (MT).

In this context SWIFT has developed 3SKey, a multi-bank digital identity solution available to corporates, to enable multi-bank exchange of personal signatures using a single universal token, regardless of the channel used (SWIFTNet, web channels and domestic networks). Tom Durkin, global head of integrated channel solutions, Bank of America Merrill Lynch, says: "Our clients look at standardising their connectivity around 3SKey as an identity solution. They are also working with us on standardising their formats around one of the ISO formats. We're certainly looking at it for the eBAM (electronic bank account management) channel." A multi-bank personal signature enables corporate users to simplify their banking security while increasing the operational traceability. In addition, personal signatures enable banks to offer extended services such as mandate management solutions to externalise and strengthen the corporate authorisation workflows.

> "Security is a major concern on the corporate side. We have enhanced our digital signing solution in the 60+ countries where HSBC offers Payments Services. Corporate customers can now monitor user entitlements online by using HSBCnet. We can check any amount against these user entitlements on any type of connectivity: SWIFTNet, Connect and HSBCnet."

Charles Dubarry, head of global direct channels and integration, HSBC

HSBC

Advanced mandate management practices

Dassault Systèmes implemented SWIFTNet and SWIFT's 3SKey multi-bank personal digital identity solution, launched at the end of 2010, to rationalise payments and banking relationships. Colleemallay says:

Contents

Register for a webinar

Contact us

Share

Print

“We were sending payments to many banks, many local banks, on local formats. Today, we have completely harmonised.” Dassault Systèmes now has reduced the number of banking partners, and has full STP for payments. Signature and security are achieved across the whole process via 3SKey.

“Our experience of 3SKey has been that it has allowed us to do three things. First, we were able to simplify all the devices we were using across Germany, France, the UK and Spain; secondly; 3SKey enabled us to upgrade our efficiency in using the SWIFT network; thirdly, we were able to harmonise our process and the way we work,” says Pierre Jalade, vice president, treasury at Airbus SAS, emphasising also that 3SKey is easy to use, and increases his firm’s control of its banking relationships.

Among banks offering 3SKey, BNP Paribas has distributed 5,000 3SKeys to around 1,000 customers since 2010. Stephanie Niemi, channels marketing, BNP Paribas Cash Management, says: “We provide a centralised service to check on users’ access rights and limits. With support for SWIFT corporate access in 35 countries globally, companies can be assured that the signature and user rights for each transaction are checked consistently through a central location.”

3SKey can also be used creatively by banks to enhance their service offering to corporates. HSBC is a notable exponent of this approach.

Managing liquidity safely is a never-ending battle. Technology provides tools to both the policeman and the criminal. As such, corporates and banks will continue to need enablers such as 3SKey that support the creation of cutting-edge treasury management processes with tailored controls.

For corporates, the priority must be to stay vigilant, both to threats but also to opportunities offered by technology to close those threats. For banks, the challenge is to recognise the importance of identity and mandate management services to maintaining relationships with key corporate clients and to respond accordingly. Implementing and making use of the advanced identity and mandate management services helps both corporates and banks to manage and protect against fraud and establish rigorous reporting and traceability of the authorisation process from transaction initiation at the corporate to bank execution.

> “We provide a centralised service to check on users’ access rights and limits. With support for SWIFT corporate access in 35 countries globally, companies can be assured that the signature and user rights for each transaction are checked consistently through a central location.”

**Stephanie Niemi, channels marketing,
BNP Paribas Cash Management**

BNP PARIBAS

Contents

Register for a webinar

Contact us

Share

Print