The Future of Authorised Signatory Management and Digital Signing

CYGNETISE

Contents

With special contributions from:

APEX

VISTRA

JTC

Beyond Governance
Creating clarity, improving business

Introduction

In the modern global business world, organisations face an increasing number of security, audit and authorisation challenges. To simply manage their day-to-day operations, they are typically required to authorise multiple corporate officers or staff members, at different levels of seniority and spread across multiple locations, to manage their various corporate relationships and transactions. Entering binding contracts, making and approving payments are just a few critical business transactions that would require the signature of an authorised signatory.

Authorised signatory management, therefore, requires effective and constant control over both the identity of individuals authorised, and the scope of authorisation. If an authorisation process fails, the organisation may be responsible for unintended contractual arrangements or, at worst, exposed to a risk of fraud.

However, the current process of authorised signatory management is mostly manual, paper-based and inefficient. It often involves manually collecting individual signature data through PDF or other paper-based forms and collating it into Authorised Signatory Lists (ASLs) that are also usually stored locally in PDF format. In addition to being costly in terms of time and effort, the manual aspect of the process makes it highly prone to human error and mismanagement.

With the recent major shift to remote working and the increasing adoption of e-signatures due to the COVID-19 pandemic, organisations face even higher risk of signatory fraud and unauthorised signing. How can organisations ensure their e-signatories are appropriately authorised?

A comprehensive internal process, accompanied by sophisticated signatory authorisation technology, can significantly reduce the risks associated with managing signatories and increase the enforceability of digitally signed records.

In this report, we discuss what an authorised signatory is, the different types of authorised signatories, and the evolution and importance of authorised signatory management in today’s digital world. The report also includes opinions and perspectives of leading industry experts across different industries, as well as real-life examples and case studies.

What is an authorised signatory?

Simply put, an authorised signatory or signer is a person who's been given the right to sign documents on behalf of the authorising organisation. However, the term's meaning and interpretation seem to vary significantly across different jurisdictions and industries.

The different types of authorised signatories

Company signature authorisation

Designated officers/employees within an organisation who are authorised to process and approve official documents and third-party agreements on behalf of the organisation are often referred as "authorised signers".

The process of signature authorisation usually forms part of a broader "Delegation of Authority Policy" that establishes an internal procedure for appointing approval and signing authority, and defining the level of scope of that authority. The policy also includes a list of general responsibilities for authorised signers to follow when reviewing, approving and processing company contracts and official documentation.

For example, many organisations restrict signature authorisation to directors or senior employees and set contract value limits applying at different seniority levels and on a dual signatory ('4-eyes') basis. Typical signatory duties include:

- Dealing with organisation resolutions
- Signing and delivering official documents and agreements with third parties and serving as a company's agent
- Signing/authorising goods/product orders
- Signing/authorising permits, passes or time-sheets
- Giving any notices
- Executing any specific undertakings and approvals

Authorised signers on bank accounts

In banking, personal and business account holders can authorise someone else to manage their account. These people are also usually called authorised signatories. Many banks require account holders to be recognised as authorised signatories, too.

In terms of level of authority, authorised signers usually have the same access to the bank account as the account holder.

In business banking, however, the rights of authorised signers tend to differ across various jurisdictions and depend on local government's specific legislations. Some of the most common types of permissions held by authorised signers on business accounts are:

- Ability to sign checks/cheques
- Access to an account's balance
- Access to transactions history
- Ability to cancel payments on checks/cheques
- Ability to close the account

In the US, there are also specific rules for authorised signers on business accounts owned by limited liability companies (LLCs). Although an authorised signer is allowed to do business in the same way as the owner of the bank account (the LLC), he/she doesn't have the same legal responsibilities as account holders. This requires a highly trusted individual to be designated as the second authorised signer on an LLC business bank account. Legally, an authorised signer is permitted to make financial transactions from the account such as spending or approving company funds.

Signature authority can be given by an LLC to one or more individuals for all legal and financial documents or rights can be approved for only certain accounts or transactions. Moreover, sometimes different roles have the permission to sign off on specific paperwork. For example, a managing director or LLC president may be the authorised signer for the following documentation:

- Loan documents
- Partnership agreements
- Contracts

Whereas, the CEO of the LLC may have the authority to sign off on other documents, such as:

- Loans
- Cheques
- Any other finance-related paperwork

In personal banking, individual authorised signatories can usually use an account separately if the mandate says “several”, “any” or “either” authorised signatory can sign (that is, operate the account).

Otherwise, if a mandate requires “joint”, “both” or “all” (or in some cases “any two”) authorised signatories to sign or access the account together, it means that one authorised signatory alone cannot use the account. Other authorised signatories must also authorise the transactions. A bank cannot allow transactions or other activity without the consent of the other holders.

Trading authorisation on investment accounts

In brokerage, authorised traders refer to brokers or agents who are permitted to trade on behalf of the investor/client. In other words, trading authorisation allow an investor to grant certain level of authority to a third party for the purpose of trading on a designated trading account. This usually happens when an individual person decides to appoint a financial professional to receive financial advice.

Generally, there are two types of trading authorisation levels: full trading authorisation and limited trading authorisation. To establish the level of trading authorisation, the primary account holder is usually required to consent to the authorisation through an official formal document or contract.

From “paper” to “digital” – the evolution of authorised signatory management

In many organisations, the process of managing and distributing authorised signatory data is through the use of paper-based, manually-controlled authorised signatory lists.

This means that organisations face a huge administrative burden and operational risk between compiling, scanning, and distributing these lists. For every refresh, there is a re-paper and re-distribution.

Hundreds, in some cases thousands of staff hours are wasted every year on this task, costing organisations millions of pounds.

Authorised signatory management today

Authorised signatory lists were originally created to facilitate the management of authorised signatories and signature data by providing a level of confidence and accuracy.

Unfortunately, the process by which signatory lists are maintained and distributed brings with it a number of weaknesses, allowing for mistakes to be made, lists to become stale or be exploited and exposed to fraudulent activity.

What is the reality?

Due to the time-consuming nature of the task, lists are often not updated and redistributed for individual departures and arrivals, but instead a periodic change is often chosen. This inconsistent approach leads to scenarios where employees are both on the list when they should no longer be or are not on the list when they need to be.

53% of company secretaries said it takes a week or longer to refresh their signatory lists

Data from our survey on the management of signatory lists at ICSA Annual Conference

Signatory management of the future: Digital authorised signatory management

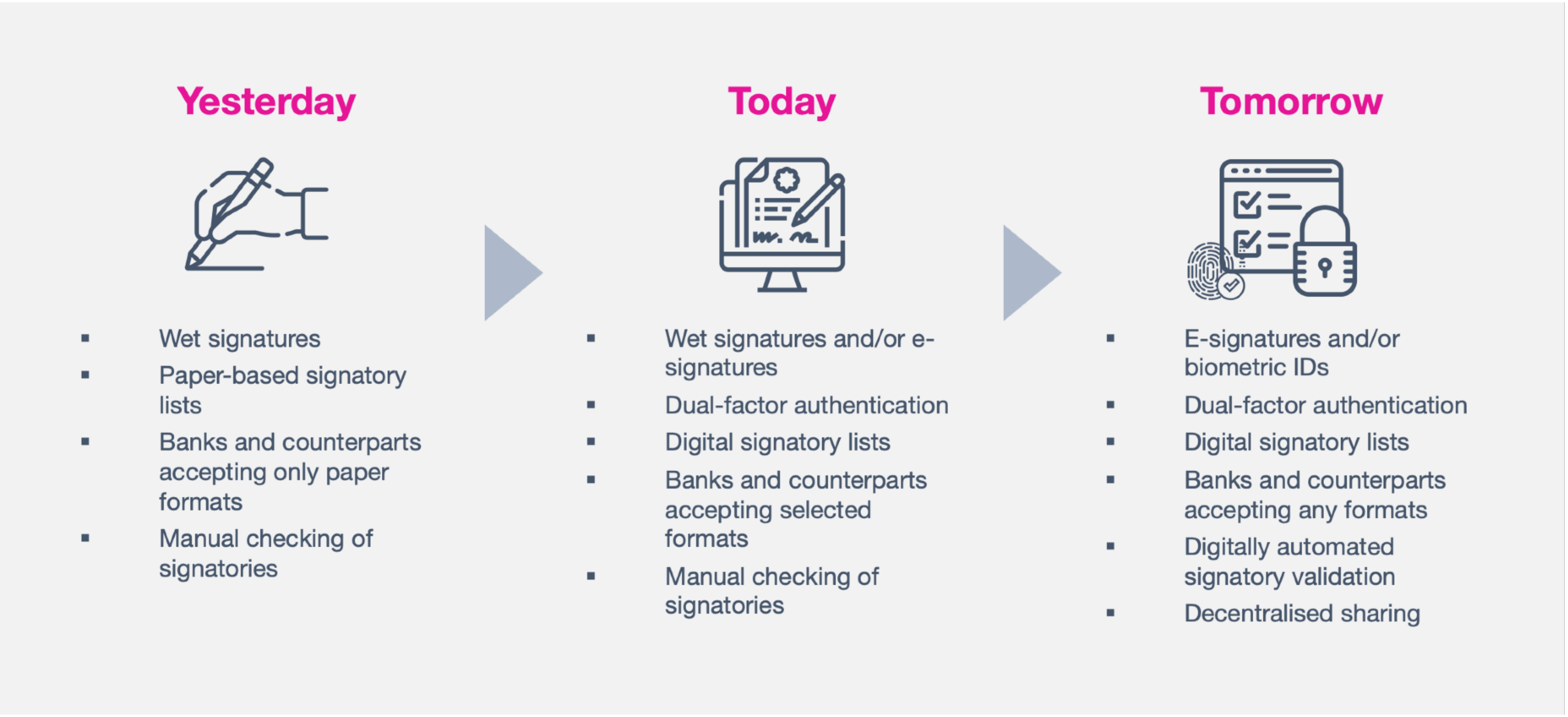
As with most operational deficiencies in business today, technology is sought to provide a solution and drive forward innovation. The nature of the authorised signatory lists process and its industry agnostic application means any technical answers to this problem must be simple, widely applicable and easy to integrate with legacy systems.

New advanced technologies like blockchain allow organisations to efficiently manage and share signatory lists in real time and have a complete and clear audit trail of all data changes. By digitally transforming the process of managing authorised signatory lists and using a dedicated signatory management solution like Cygnetise, organisations can now save over 90% of their admin costs and time, whilst significantly mitigating the risk of fraud.

"Technology can make a significant contribution to modern corporate governance by increasing transparency, streamlining the cumbersome duties around corporate governance, enhancing accountability and reducing human error."

Adam Jeffries, CIO, JTC

The evolution of authorised signatory management



Yesterday

- Wet signatures
- Paper-based signatory lists
- Banks and counterparts accepting only paper formats
- Manual checking of signatories

Today

- Wet signatures and/or e-signatures
- Dual-factor authentication
- Digital signatory lists
- Banks and counterparts accepting selected formats
- Manual checking of signatories

Tomorrow

- E-signatures and/or biometric IDs
- Dual-factor authentication
- Digital signatory lists
- Banks and counterparts accepting any formats
- Digitally automated signatory validation
- Decentralised sharing

The importance of authorised signatory management

In today's highly dynamic business world, effective authorised signatory management is key for the successful operations of any trading organisation, which manages multiple corporate relationships whether internally or for its clients. A failed authorisation can not only result in unnecessary operational costs for the organisation, but also expose it to a risk of financial loss due to fraud or litigation, which would be damaging for the organisation's reputation and brand.

What are the risks of a failed authorised signature?

A payment gets held up

Process / deal / transaction delays

A deal fails - may adversely impact deal chain

Deliberate fraud happens.
Someone signs that is not eligible

Failure to comply with internal controls and corporate governance policies

Whilst lists are exchanged and requested to be provided when authenticating signatures, there is the issue of human error/ignorance, where relevant parties simply do not check them. Commonly, this is because of time constraints and/or the aforementioned presumption that the signature must be valid and the signatory properly authorised.

Transaction delay

Usually, counterparts who access the authorised signatory data (ASLs) are reliant on the latest information/ASL version being sent to them, and have no control over the frequency with which they receive the data and/or how up-to-date it is. When there is a time-sensitive matter, having to refresh a list to match a signature can be so difficult that the deal or trade fails, or in which to reach agreement lapses.

> *"It's essential that the policy and signatory management system work hand in hand to ensure an efficient process for the execution of documents. Copies of paper-based signatory lists and a lack of a clear signatory policy means the company is exposed at risk, from both an authority and execution perspective."*

Michael Hackett, Company Secretary, Apex Group Ltd.

Fraud

Organisations on both sides of any transaction that require signatures are exposed to a high risk of fraud. Each day that a signatory list is inaccurate presents a serious fraud risk. This is particularly the case where a signatory leaves the organisation or is removed but the list is not updated or provided to those parties who rely on it. These persons can sign and the organisation will not know anything about it until it is too late.

Case study: Bank mandate fraud

A small company's owner had a business account with a local bank where he had two authorised signatories/mandates.

One day, he intended to use his business credit card to withdraw money from an ATM and his card was retained. He then contacted the bank and found that his name was no longer associated with his company's account.

After further investigation, it turned out that an ex-employee of the company had sent a formal letter to the bank requesting the existing account mandates to be replaced by him. The bank then changed the mandate accordingly and the fraudster received full access to the account.

Audit and compliance

From an auditor's perspective a company that does not demonstrate effective control over its finances and assets, for example failing to maintain accurate authorised signatory lists, will be deemed at risk. Many companies, especially in the banking sector, have statutory record-keeping obligations and are required to keep a clear audit trail of account-related documentation, including signatory data.

It is important that companies can demonstrate to their auditors that there is ongoing compliance with all relevant legal and regulatory requirements, internal account mandate controls and good corporate governance in relation to delegated authorities.

Regulated businesses

Regulated organisations, especially those managing or with fiduciary responsibility for third party funds and assets, ordinarily have an obligation to maintain effective systems and controls to prevent and deter financial crime. Failure by an organisation to do so, or where these are breached, could not only result in financial loss for itself or its clients, it will likely also be subject to regulatory sanctions or fines. A significant fraud or loss through negligence will impact its market reputation, insurance premiums or, at worst, its licence to operate may be suspended or revoked.

"Signatory data matters and a robust audit trail is essential to ensure correct oversight and process in place. A efficient signatory management system can drive 'Sustainable Governance' in a company."

Michael Hackett, Company Secretary, Apex Group Ltd.

"Regulators always emphasise the need for "systems and controls" to be put in place by their licensees and if these are missing or fail that is when a firm will find themselves on the wrong side of the regulator."

Tanya Scott-Tomlin, Chief Compliance Officer, Vistra

"Having a clear line of who is able to sign what document allows for a more streamlined audit to take place. If the accountability is transparent and widely understood, then internal controls within a company are effective. "

Erika Percival, CEO, Beyond Governance

Signatory authorisation and the use of e-signatures

Following the impacts of COVID-19 and the shift to remote working, many organisations have started to move from using "wet signatures" to adopting electronic signatures. While e-signing enables business continuity and promotes efficiencies, it can also expose organisations to higher risks of signatory fraud, unauthorised signing and errors.

What is an electronic signature?

According to the US Electronic Communications (ESIGN) Act 2000 and the 2019 Official Report by the UK Law Commission, an electronic signature is a signature in electronic form that is used on a digital document or communication.

Some of the most common types of electronic signatures include:

- a name typed at the end of an email,
- a scanned copy or photo of a hand-written signature,
- a signature made using a dedicated e-signature platform (e.g. DocuSign),
- a signature written onto a screen using a stylus.

What are the risks of using electronic signatures?

Generally, digital signatures tend to be more secure than traditional paper-based wet ink signatures as they're easier to track, especially if generated through a specific digital signature software. Digital signature software products or platforms also use encryption and decryption technology alongside public key infrastructure (PKI) adding an extra step of authentication to the signing process that aims to prevent tampering.

Despite this, there are still a number of risks organisations should consider when implementing e-signatures:

1) **Risk of fraud & reliability** – while using a dedicated digital signatory software platform can help solve any authentication issues of the e-signing process, there's still a high risk of signatory forging and fraud for organisations as technology can be compromised or hacked.

2) **Risk of unauthorised signing** – a major problem with both wet ink and electronic signatures is the risk of unauthorised signing. How can organisations ensure that all their signatories (including e-signatories) are appropriately authorised? How can they reliably monitor and report on their authorised signatories? Similarly, how do signatories know what exactly they are authorised to sign? This is particularly relevant where signatories act as such for multiple legal entities within corporate group.

3) **Risk of non-compliance** – in addition to regional and international electronic signature laws, organisations should also comply with rules and regulations for presenting documents, disclosures, and other information at certain stages during a transaction (e.g. MiFID, FCA). If organisations fail to comply, they face a risk of getting sanctioned and fined by regulatory authorities, lose accreditation status, or damage their brand equity.

> *"Firms migrating to digital signature platforms must remain mindful that fundamental legal principles continue to apply to digitally executed agreements."*
>
> ***Tanya Scott-Tomlin, Chief Compliance Officer, Vistra***

e-Signature best practice checklist

- □ Is your authorised signatory list up-to-date and easily accessible?
- □ Are all signatories available? If not, do you need to approve any additional signatories?
- □ Do you need to add any specific authorisations for the use of electronic signatures?
- □ Do your signatories have all required technical equipment to execute electronic signatures remotely (e.g. printer, scanner, camera, etc.)?
- □ Have you considered using e-signing and signatory management technologies to facilitate the process?

Conclusion

Building an effective authorised signatory management process can deliver some key direct benefits for organisations, such as lower operational costs, improved corporate transparency, easier compliance with internal controls and governance policies, and reduced operational and fraud risk.

With the increasing move to remote working and a “paper-free” office environment, digital signatory management is becoming more important than ever.

At Cygnetise, we have developed an application that solves the pain of managing authorised signatory lists, making it secure and efficient. Our technology enables users to update their lists in real time and has a variety of sharing mechanisms so that the counterpart can always have access to the most up-to-date information without you having to recompile and redistribute.

To learn more about Cygnetise and request a free demo, get in touch here

CYGNETISE