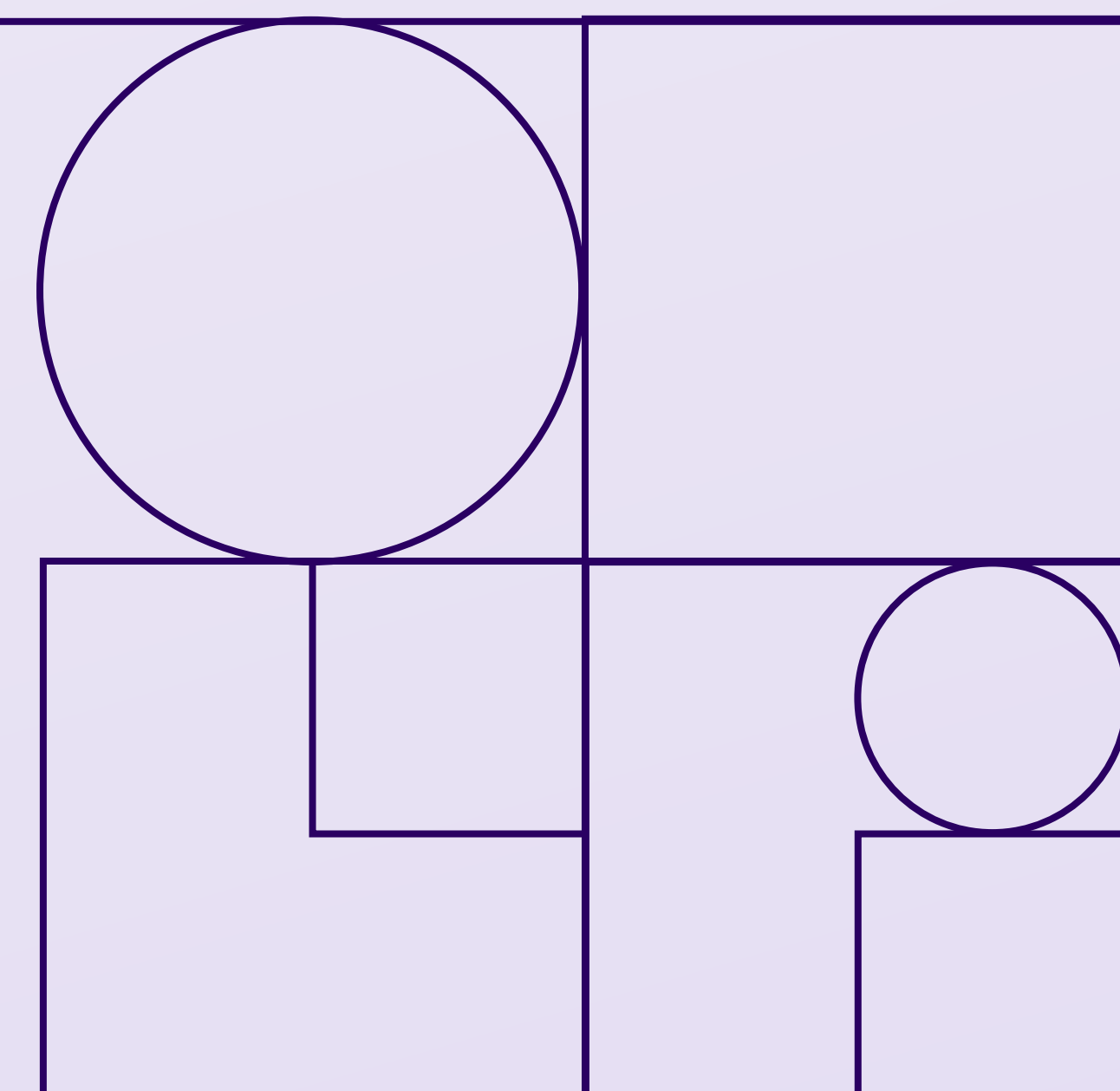




The eSigning Playbook

A no-regret guide to choosing
the right eSignature tool



<div>Electronic Signing: Legal framework & eSignature types</div> <div>2</div>	<div>Index</div> <div></div>
<div>Signing with Signicat: Choose your route</div> <div><ul style="list-style-type: none">● The API integration route: Tailor it, integrate it, sign!● The portal route: Signatures ready to go!● Timestamps, validation, preservation & e-sealing – The extra layers of trust</div> <div>5</div>	<div>Protected and always ready with Archive</div> <div>15</div>
	<div>Which signing solution is right for you?</div> <div>16</div>
<div>Sign with Signicat: Find the perfect fit</div> <div>14</div>	<div>Real-word case study: Best practices from If Insurance</div> <div>17</div>

Electronic Signing: Legal framework & eSignature types

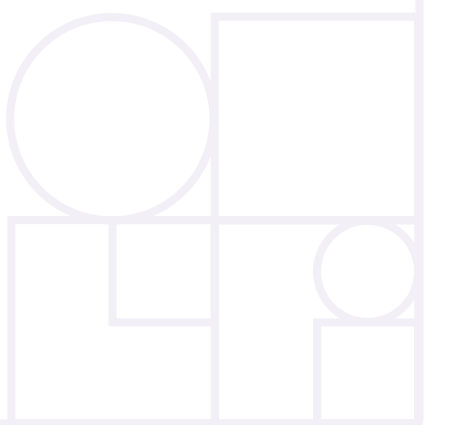


It's no news that electronic signing has become vital for organisations, especially in regulated sectors like finance, insurance, and government. **The demand for efficiency, security, and legal compliance has made electronic signatures indispensable.** Unlike traditional signatures on paper, electronic signatures provide verification capabilities, confirming the signer's identity and ensuring the document's integrity.

In the EU, electronic signatures are governed by the **eIDAS regulation**, which provides a legal framework for their use, establishing standards for electronic signatures, trust services, and electronic transactions.

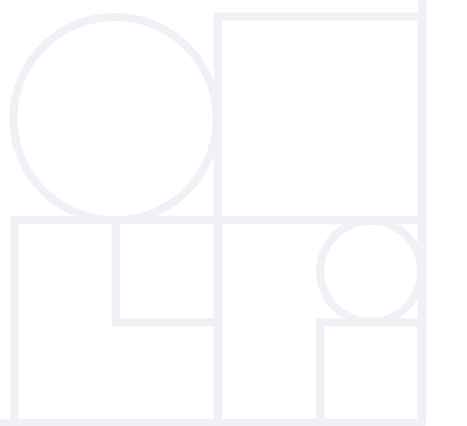
eIDAS can be summarised in three key points:

- Recognises the legal validity of SES, AES, and QES.
- Defines QES as being legally equivalent to handwritten signatures.
- Ensures interoperability across the EU.



Good-to-know:

Qualified electronic certificates for qualified signatures used to require in-person identity verification under eIDAS. Since 2021, however, national schemes have enabled secure and **fully digital verification through automated video identification**. This eliminates the need for in-person processes while maintaining the highest level of security.



The three types of eSignatures recognised by eIDAS—Simple, Advanced, and Qualified—each serve different purposes and are designed for specific use cases, depending on the assurance level required or the risk involved in the transaction.

Simple Electronic Signature (SES)

It's the simplest form of electronic signatures. It could be a scanned image of a handwritten signature, a quickly drawn signature created using a mouse or finger on a screen, or a tick in a box to agree to terms online.

Characteristics:

- Low level of security and authentication.
- Low evidential value.
- Identity confirmation methods include SMS OTP or email verification.

When to Use:

Commonly used for low-risk transactions, e.g., signing for package deliveries or internal memos.

Advanced Electronic Signature (AES)

AES is a step above SES, offering higher security by linking the signature to the signer using encryption, making it unique to the signer, able to verify their identity, securely created under their sole control, and ensuring any data changes are detectable.

Characteristics:

- Moderate or high level of security, depending on the strength of the signer's identification, other implementation aspects, and the country's legislation.

When to Use:

Medium and high-risk transactions or legal documents and agreements where identity confirmation is critical, e.g., contracts for private businesses.

Qualified Electronic Signature (QES)

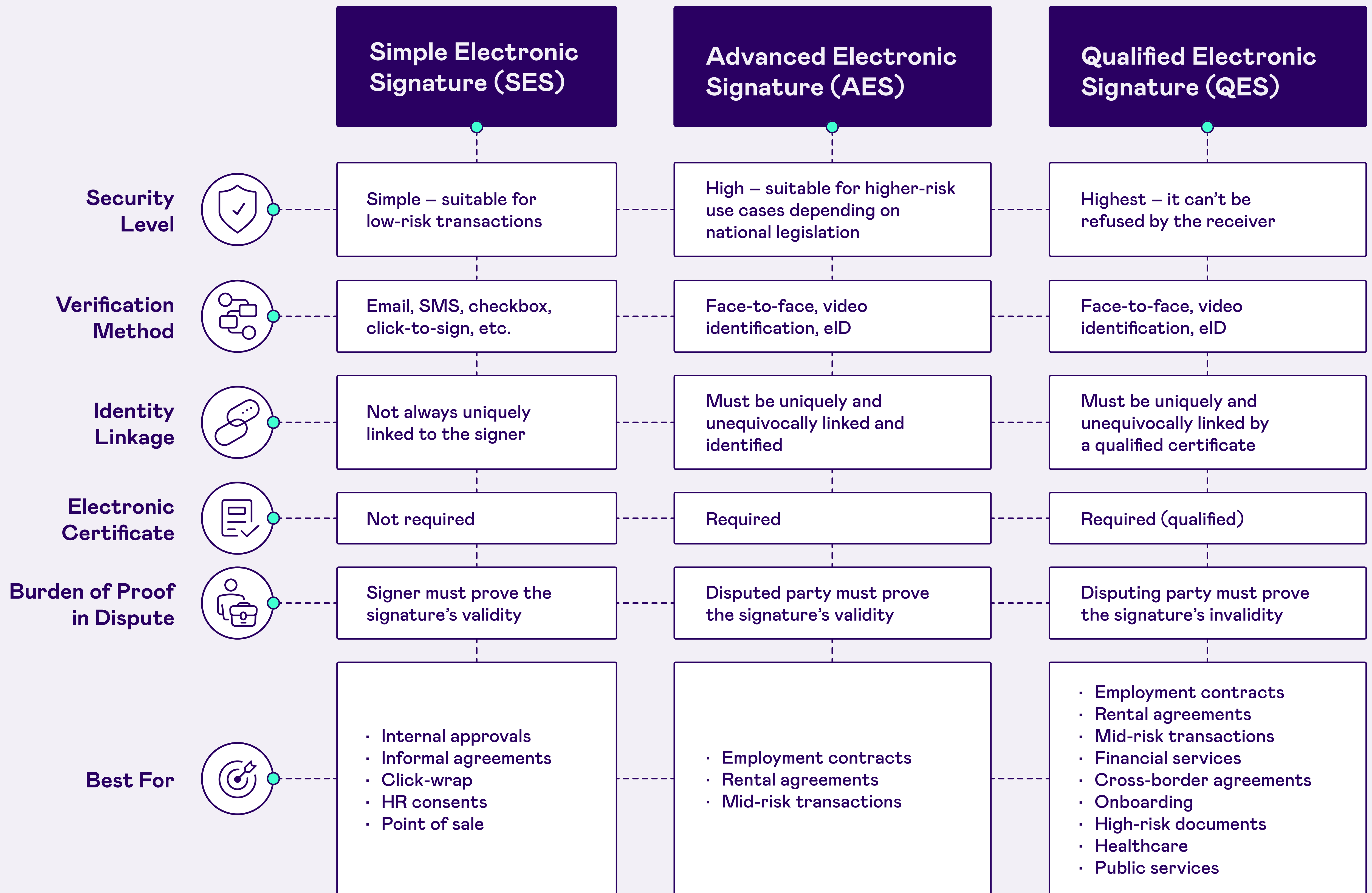
The gold standard of electronic signatures, QES complies with the highest EU regulations. A QES offers the highest level of security and legal assurance.

Characteristics:

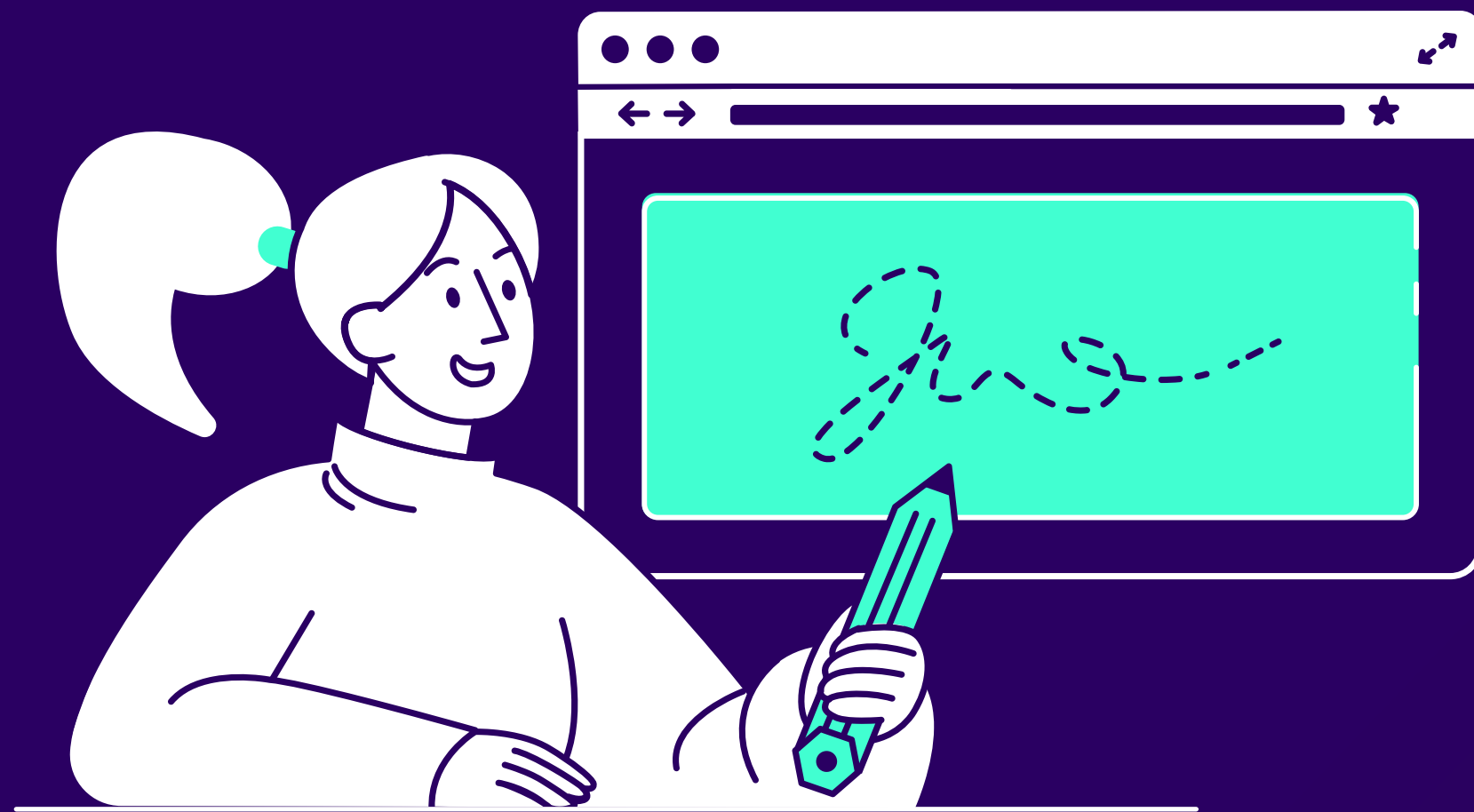
- Guaranteed signature acceptance for all purposes and cross-border, perfect for high-risk, global operations.
- Based on a qualified certificate issued by a trusted authority.
- Requires strong evidence of the signer's identity.
- Requires a qualified electronic signature creation device (QESCD)

When to Use:

High-risk transactions, such as mortgage approvals, medical records, or governmental approvals.



Signing with Signicat: Choose your route

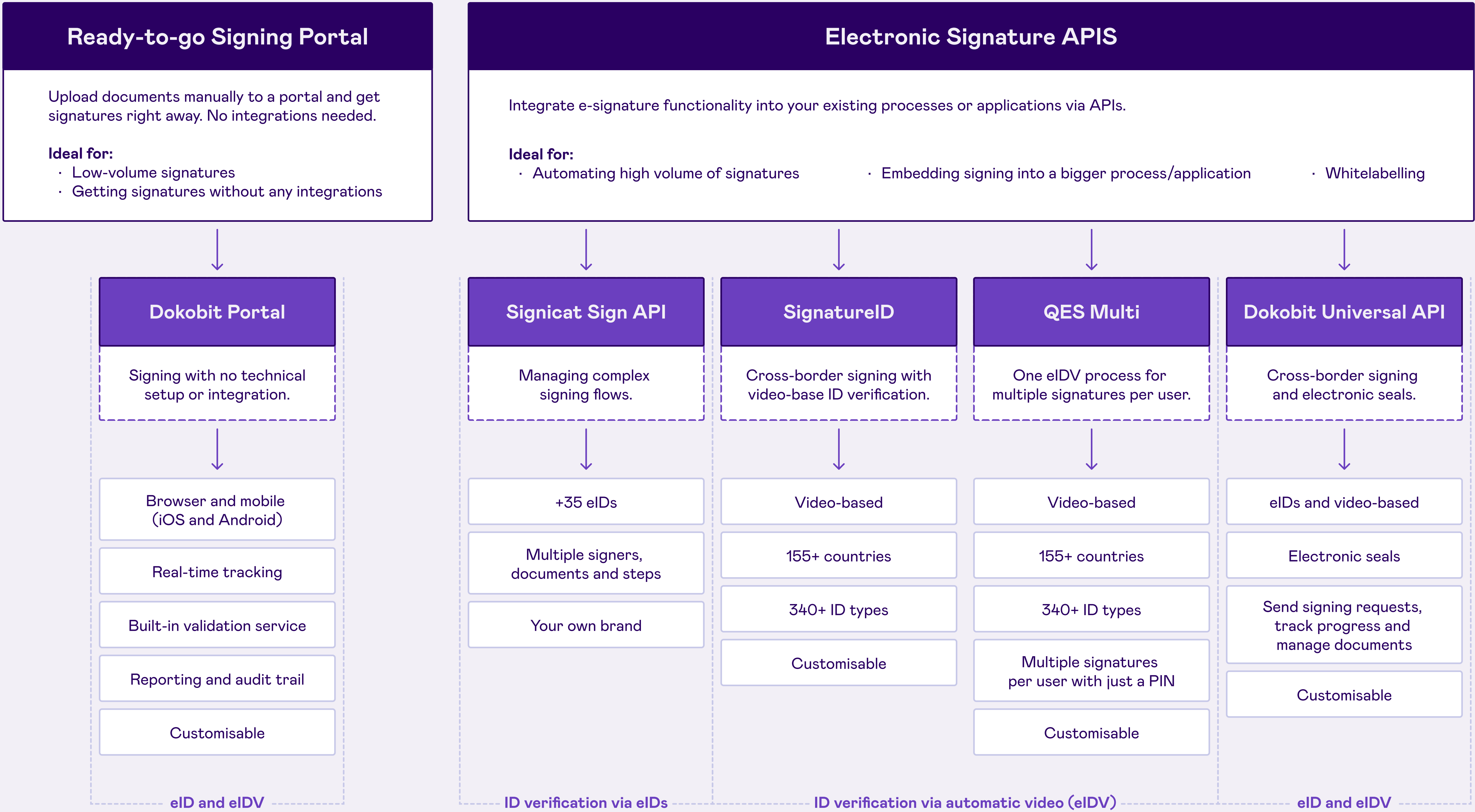


Signicat provides a robust suite of electronic signing solutions, tailored to meet diverse business needs. Whether an organisation needs simple e-signatures for quick agreements or advanced, highly secure signing options for sensitive documents, Signicat delivers. **Signicat's signatures can automate document workflows, significantly reducing manual tasks and saving valuable time.** Compliance with regulatory standards is built into the platform, ensuring peace of mind for industries with strict legal requirements. Additionally, Signicat's secure encryption protects sensitive data, reducing the risk of fraud or tampering.

The user-friendly interfaces also enhance customer satisfaction, making the signing process seamless and efficient.

You can choose between two implementation options based on your organisation's needs: a **tailored API integration** or a **ready-to-use portal**. The implementation route offers flexibility and customisation, while the portal route provides speed and simplicity for immediate use. Below, we dive into the differences between the routes, product features, and where they can help.

Signicat signing in one view



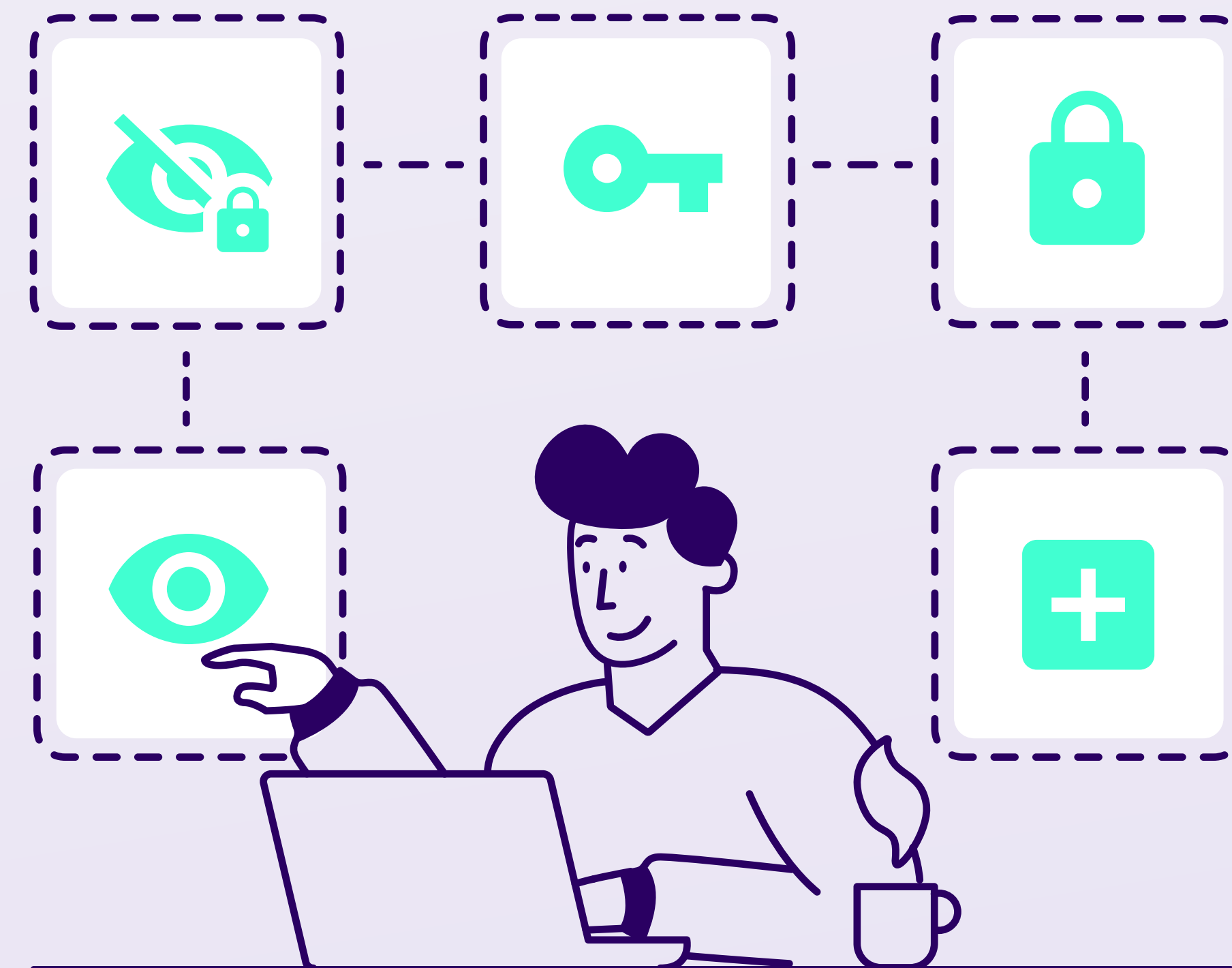
The API integration route: Tailor it, integrate it, sign!

Signicat's Electronic Signature APIs

Signicat's API solutions make it easy to **bring e-signing into your own systems**, whether that's a website, an app, or an internal workflow. Users can sign contracts directly within your platform, keeping the process straightforward, consistent and compliant with eIDAS, KYC/AML and GDPR regulations.

By enabling signing in a familiar environment, you **build trust and make the experience more comfortable** for users. It also gives you full control over how signing fits into your processes.

APIs are especially useful for **organisations handling high volumes or operating in regulated sectors** like banking, insurance, or payments. They offer a reliable, secure, and scalable way to manage signing as part of your everyday operations. Signicat offers a diverse portfolio of APIs tailored to various signing use cases and business requirements. Let's explore them.





Signicat Sign API

The Sign API is a great fit for organisations that **deal with complex or large-scale signing flows** and operate in markets with strong adoption of electronic identities, like the Nordics and Netherlands.

What It Does

The Sign API is based on electronic identities (eIDs) and supports all three eIDAS-compliant signature levels – Simple, Advanced, and Qualified. It **works with 36+ eIDs across Europe**, making it ideal for secure, cross-border signing.

You can use the API to create and manage signing workflows with multiple documents, signers, and steps. Whether it's a single document or a complex, multi-stage process, the API gives you an easy way to manage everything securely and efficiently from your own systems.

The API also supports **white-labelling and branding**, so everything – from invitation to signing – looks and feels like part of your organisation's own service.

Ideal for

- **Cross-border eID-based signing:** Works with **36+ European eIDs**
- **Handling complex workflows:** Manage multiple signers, documents, and signing steps.
- **Control and flexibility:** Adapt the process to your organisation's legal and business needs.
- **Developer-friendly integration:** Well-documented and easy to integrate.

How it works:

1. Prepare and upload documents from your organisation's workflows, system or app.
2. Signers receive an email invitation to authenticate and sign using their eID.
3. Signatures are collected and sealed with a tamper-proof audit trail.
4. Completed documents and signature evidence are returned to the customer and stored securely – either in your organisation's system or in Signicat's archive.



SignatureID

SignatureID is an API that offers the capability of **signing when your users don't possess an eID**. This makes it an excellent solution for regions where eIDs aren't commonly used or for organisations aiming to expand into those markets.

What It Does

SignatureID uses **advanced AI-powered video identification technology** to verify users' identity instantly and automatically, delivering the highest level of assurance when needed. The process is fully compliant with eIDAS regulations, enabling SignatureID to support all three signature levels: Simple, Advanced, and Qualified, including QES Once and QES Multi, Signicat's QES that allows organisations to issue qualified certificates and signatures.

This API offers versatile use, either **standalone or integrated with the Sign API, Dokobit Portal, or Universal API** (these last two supporting QES Multi). It simplifies identity verification, enabling secure onboarding and contract signing in one simple process.

Ideal for

- **Signing in markets without an eID or where eIDs are not widespread:** Facilitates signing in regions where eIDs are not yet widely adopted, or for organisations looking to expand into these markets.
- **Aligning with your processes:** Align the process with your organisation's legal, business, and regulatory requirements for assurance and signature standards (SES, AES, or QES)
- **Scaling globally:** AES supports 155+ countries and 340+ ID types via video identification, QES supports 88+ and 181+ respectively.
- **Customisation for consistent UX:** Customise the process with your organisation's logo and colours.
- **Easy integration:** Pre-coded framework for easy implementation.

How it works:

1. The user starts video-based identity verification.
2. They show their passport or ID document (front and back) on camera.
3. A biometric check confirms the face matches the ID and that the user is present in real time and they can sign with an AES.
4. If signing with a QES, a human oversees the whole verification process in real time, approves it, and a qualified certificate is issued.
5. Documents can now be signed with the same level of assurance as in-person signing.
6. Every time the user makes a signature request, they have to go through the entire identity verification process.

QES Multi

QES Multi is one of SignatureID’s supported signatures, designed to provide not only signed documents but also a **reliable way to create additional signatures in the future**. Users are given a password and a one-time password system that allows them to sign documents later using the qualified certificate issued by SignatureID. Perfect for organisations in **markets without eID infrastructure or expanding** to those regions.



What It Does

QES Multi combines **real-time video identification with biometric verification** to confirm users’ identities swiftly and securely and issue qualified electronic certificates. With this API, identity verification is only required once. Once the qualified certificate is issued, users can sign with a QES just by using a password and a one-time password (OTP) as often as they need within the organisation’s services. For instance, when opening a bank account, users can verify their identity through video identification. Once verified, they can sign any other contracts or agreements (like loans or mortgages) with a qualified electronic signature by simply using an OTP—**no need to repeat the verification process, avoiding frustration**.

Use cases include internal corporate signing, signing for HR companies, and fintechs looking to expand their service offerings, among others.

Ideal for

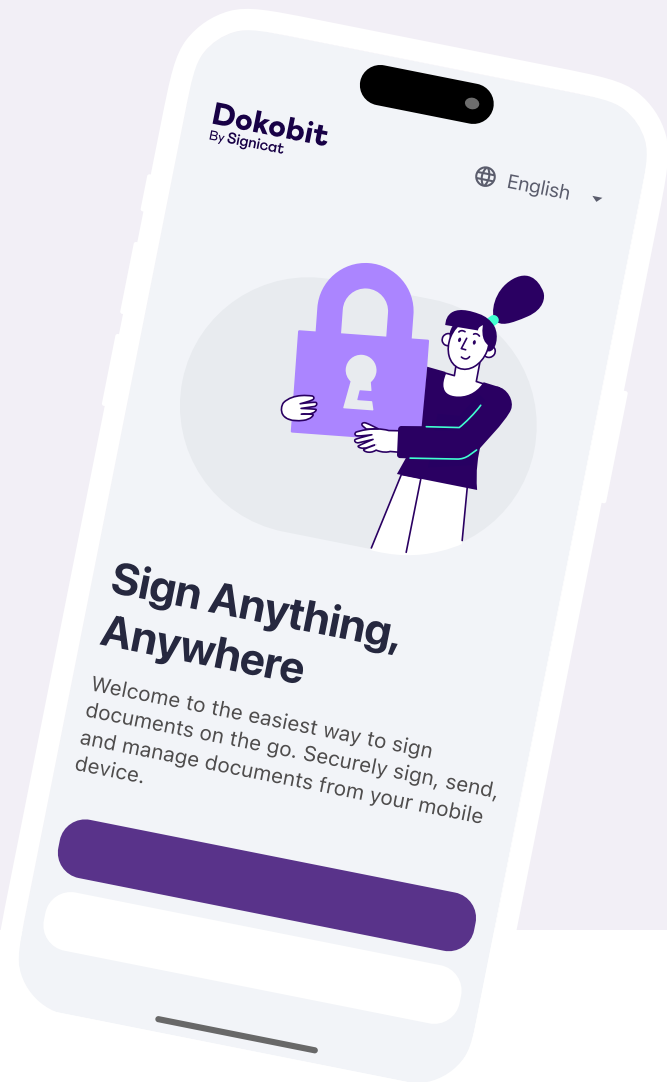
- **Multiple signatures by the same signer:** Highly regulated industries that require multiple signatures over time by the same user
- **Minimising drop-offs:** Complete sign-ups quickly, on any device, at any time.
- **Legally binding signing across the EU:** Fully compliant and equivalent to handwritten signatures.
- **Scaling globally:** Supports 88+ countries and 181+ ID types via video identification.
- **AI-powered fraud prevention:** Real-time AI-based video processing, ID verification, and biometric checks.
- **Easy integration:** pre-coded framework for easy, customisable and branded implementation.

How it works:

1. The user starts video-based identity verification.
2. They show their passport or ID card (front and back) on camera.
3. A biometric check confirms the face matches the ID and that the user is present in real time.
4. A qualified certificate is issued after successful verification.
5. The user chooses a PIN for future signatures.
6. Documents can now be signed using just the OTP– no need to repeat the video process.

Dokobit Universal API

The Dokobit Universal API is an alternative to the Sign API, ideal for **collecting legally valid signatures and sealing documents across multiple countries**. It supports a wide range of European eIDs, all signature levels (including QES Multi), electronic seals, and qualified signature validation to ensure document accuracy. Perfect for integrating the Dokobit Portal with API-based signing.



What It Does

With the Universal API, you can send signing requests, track progress, and manage signed documents – all from your existing environment. You can customise the look and feel with your own branding, so the experience stays consistent for your users.

The API also supports **electronic seals – a way for organisations to seal documents rather than sign them personally**. It’s useful in scenarios where a document needs to show that it was issued by a company or institution, like a university diploma or an automatically generated certificate. Built-in qualified validation lets you verify that documents signed elsewhere are authentic and valid.

The API **integrates with Microsoft Power Automate**, making it easier to automate document workflows within Office 365 tools.

The Universal API can also be used together with the Dokobit Portal (covered below), allowing you to support different teams or use cases within your organisation.

Ideal for

- **e-Sealing:** Apply seals to documents to confirm their origin and authenticity.
- **Customising workflows:** Flexible support for different document types and signing flows.
- **Branded experience:** Add your logo and colours to emails and signing pages.
- **Qualified validation:** Check the authenticity, validity and level of signatures and e-seals on received documents.
- **Developer-friendly integration:** Straightforward to integrate, with clear documentation and support.

How it works:

Internal signing:

1. A document is uploaded from your internal system via API.
2. The signer is redirected to a branded signing window.
3. They sign using their eID or other available signing method, and the signed document is returned to your system (it can also be shared with the signer).

External signing:

1. A signing invitation is sent to a third party via email.
2. The recipient clicks the link and signs in a branded signing window.
3. The signed document is returned to your system or optionally added to their Dokobit Portal account (it can also be shared with the signer).

The portal route: Signatures ready to go!

Dokobit

The Dokobit Portal is a **ready-to-use web solution for electronic signing and document handling**. It's ideal for teams or companies that want to start signing documents right away – with **no technical setup** or integrations needed.

Dokobit supports a wide range of country-specific and international eIDs with different signature levels. If a signer doesn't have an eID that can be used for a qualified e-signature, they can still create one through video-based identification – using an ID document, a device with a camera, and Wi-Fi.

The portal also includes a **mobile app for iOS and Android**, so signing and tracking can be done on the go. Features like shared document categories, approvals and access management make it especially useful for team-based signing.

Additionally, the portal and mobile apps include a **built-in qualified validation service** to verify whether signatures on documents received from other parties are valid and qualified.

Ideal for

- Getting started right away – ready to use in your browser and mobile apps
- Clear and user-friendly interface for all parties
- Real-time tracking to stay on top of progress
- Storing signed documents securely in one place
- Legally binding e-signatures accepted across the EU

It's a great option for **small to medium-sized organisations or teams** that need a fast, compliant, and reliable way to collect signatures, or **enterprises with a volume of signatures or usage pattern that don't require API integration**—for contracts, approvals, HR documents, or agreements— without involving developers or IT teams.

How it works:

1. Upload the document directly in the portal.
2. Add signers.
3. Send signing invitations via email or SMS.
4. Users sign with their national eID or via video-based identification.
5. Track progress in real time and get notified when signing is complete.
6. Store signed documents and audit trails securely in the portal.

Timestamps, validation, preservation & e-sealing

The extra layers of trust

When it comes to electronic signing, **a signature is only as trustworthy as the evidence that supports it.** That's why Signicat also offers time-stamping, validation, e-sealing, and signature preservation. They ensure signatures can be reliably validated over time, which is especially important when using **qualified electronic signatures (QES)**.



Timestamps as proof that an electronic signature or document existed at a specific moment in time, ensuring its validity at the time of signing. According to eIDAS, a signature is valid if it was valid when signed, and a timestamp guarantees this. By adding a qualified timestamp, the validity of the signature is preserved, even if events like the expiration of signer certificates occur after the signing. This is essential for preventing potential fraud, such as backdating a signature after accessing a private key. potential fraud, like someone trying to backdate a signature after gaining access to a private key.



Signature validation allows you to check whether an e-signature or e-seal is still valid and compliant. It provides firm evidence that a signature is valid—or was valid at the time of signing—and confirms if it truly qualifies as a QES. If there are any variations, it highlights what they are and whether they matter. This is especially important when documents are received from external parties or need to be kept for many years.



Electronic seals work like a digital organisation stamp. Instead of an individual signing, an organisation can seal a document to show it originated from them and hasn't been altered. This is useful for official statements, invoices, diplomas, or other documents where the sender's identity and the content's integrity need to be crystal clear.



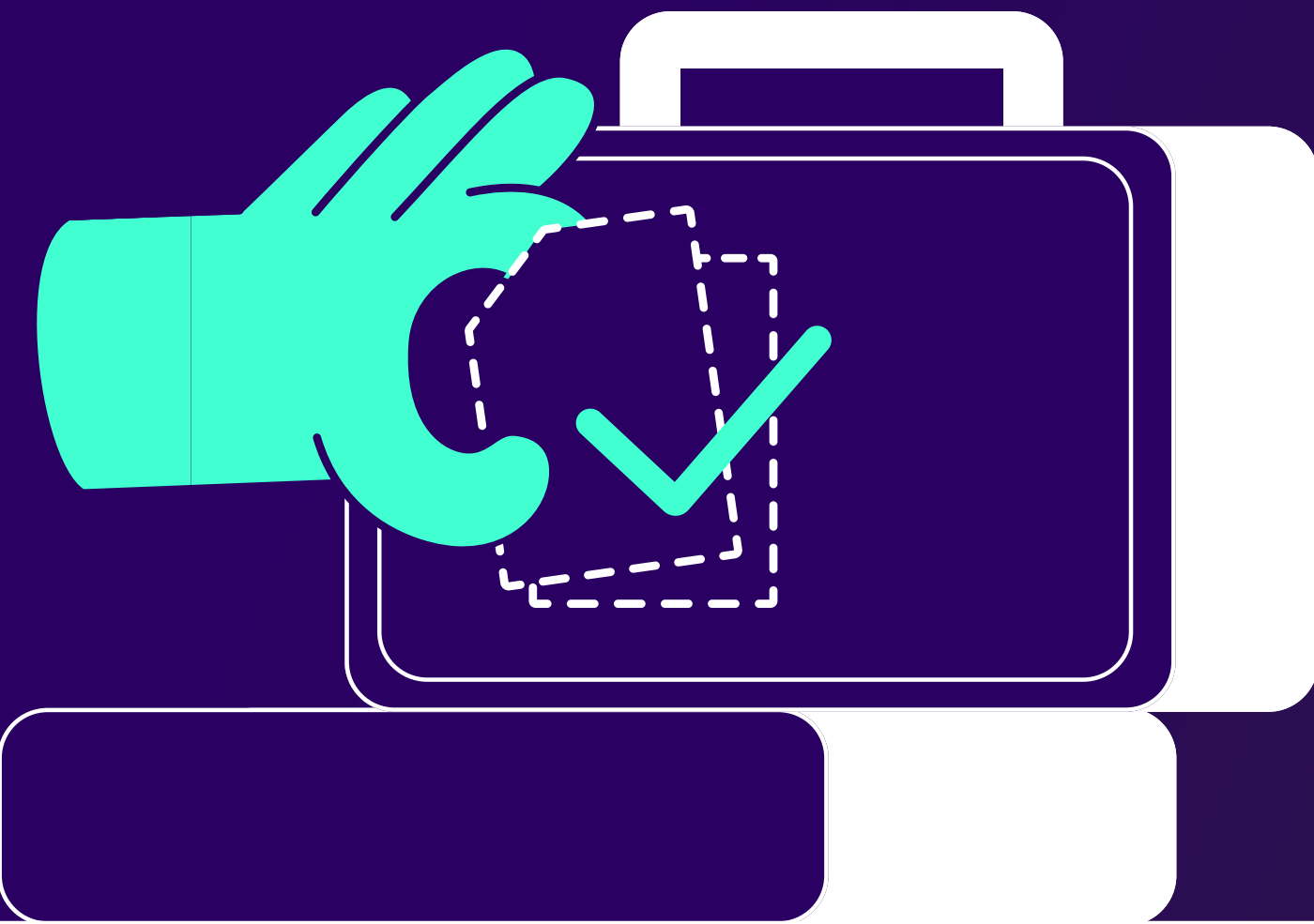
Signature preservation ensures your document signatures remain valid over time by adding new timestamps or seals every 3 years. By doing this, Signicat maintains the signature's proof of validity in the long term, regardless of the certificate's expiration.

Together, these services round out your organisation's e-signing process – ensuring every document is not just signed, but also secure, trusted, and future-proof.

Sign with Signicat: Find the perfect fit

	Sign API	SignatureID	QES Multi	Dokobit Universal API	Dokobit Portal
Integration Required	Yes – via API	Yes – via API	Yes – via API	Yes – via API	No – web portal
Target Users	Organisations with complex signing flows and strong eID market presence (e.g. Nordics)	Organisations operating in or expanding into low-eID adoption markets (e.g. UK, Spain)	Highly regulated industries needing repeated user QES over time (e.g. finance)	Organisations in the Baltics or broader EU needing eID support and e-sealing	SMEs or teams needing a fast, no-code signing solution (e.g. HR contracts)
Signature Levels Supported	SES, AES, QES	SES, AES, QES (including QES Once)	QES (multi-use via PIN)	SES, AES, QES	SES, AES, QES
eID Dependency	✓	✗	✗	✗	✗
ID Verification Method	eID	AI-based video identification (eIDV)	AI-based video identification (eIDV)	eID or/and video-based	eID or/and video-based
Signing platform	Within your system or app	Within your system or app	Within your system or app	Within your system or app	Web portal or mobile app
Customisation	Full control over branding and workflow	Customisable look & feel	Customisable look & feel	Customisable look & feel, branding, and workflow logic	Branding available, but less flexible than APIs
e-Sealing Support	✗	✗	✗	✓	✓
Signature Validation Service	✗	✗	✗	✓	✓
Ideal For	High-volume, cross-border, and flexible signing	Expanding globally or onboarding users without eIDs	Highly regulated institutions needing multiple QES signing	Advanced signing and sealing flows that support multiple teams	Teams needing a ready-to-go signing solution
Product Page	Sign API	Ask our experts	QES Multi	Dokobit Universal API	Dokobit Portal

Protected and always ready with Archive



Signicat's Archive Service

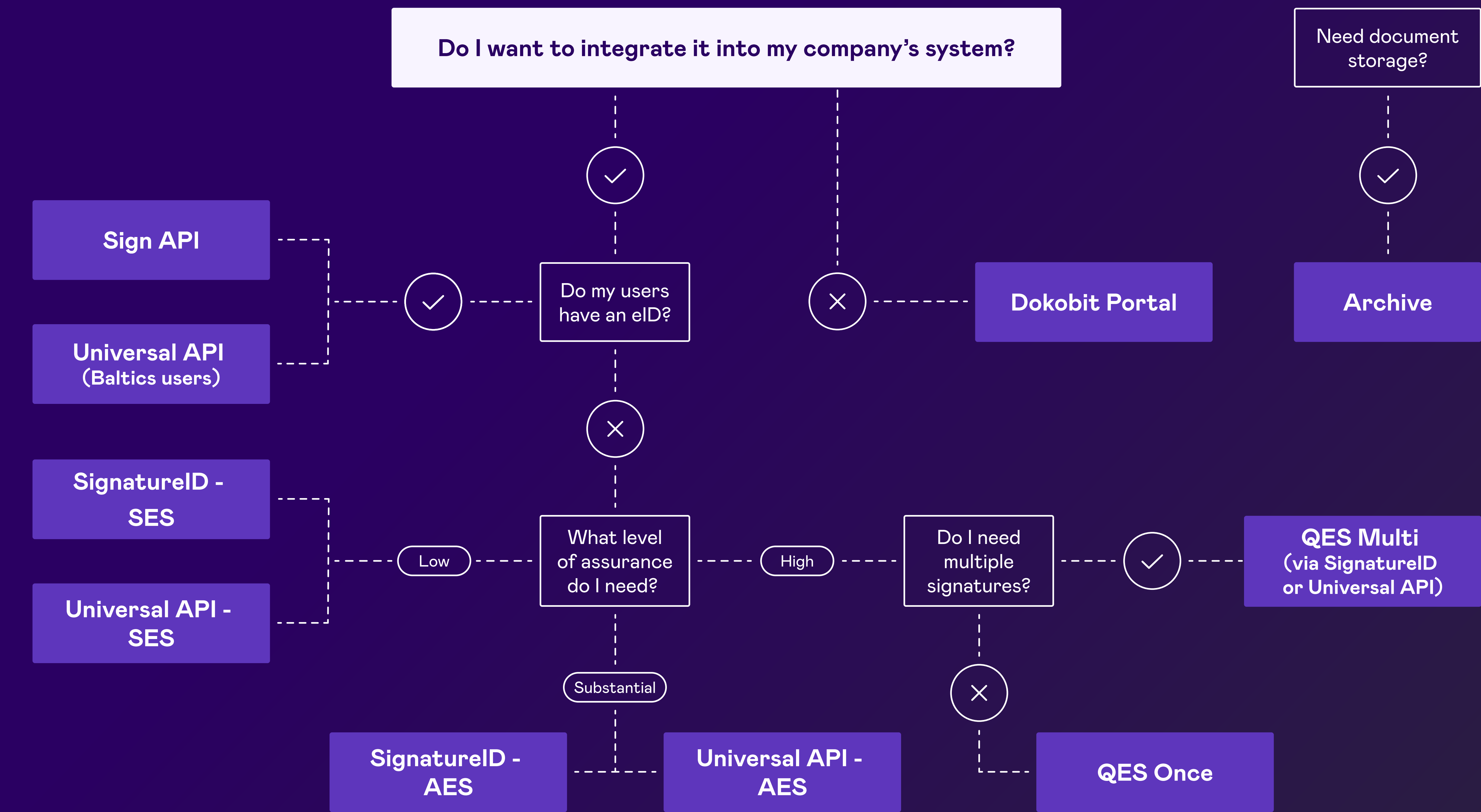
Preserving essential documents and critical files requires a flexible solution that adapts to an organisation's needs. Signicat's Archive Service easily integrates with existing systems, offering **secure, long-term storage that complements any signing product**. Tailored for highly regulated sectors, it provides security, compliance, **audit readiness**, and peace of mind.

The Benefits of the Archive Service:

- Ensure security with **advanced encryption, threat monitoring, access controls, and up-to-date backups** to protect data integrity.
- Adapt to growing needs with **scalable infrastructure** for optimal storage performance.
- Find and manage data efficiently using **metadata, custom keys, and bulk actions** like erasure or downloads.
- Preserve integrity with **qualified electronic seals** and generate **automated reports** for compliance and confidence from storage to retrieval.
- **Access stored documents across systems** and platforms without losing format or usability.



Which signing solution is right for you?



Real-word case study: Best practices from If Insurance

How the leading Nordic non-life insurer expanded secure digital services across borders

The largest non-life insurance company in the Nordic region with 3.7 million customers, needed to **scale secure digital authentication across borders while maintaining customer trust and regulatory compliance**. Partnering with Signicat since 2009, it expanded its use of Signicat's solutions from the Nordics into the Baltics to support growing digital demands.

Signicat solutions powering If Insurance:

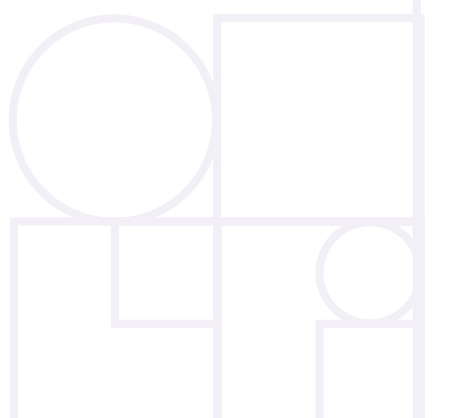
- **eID Hub:** Provided secure, compliant authentication using a wide range of national eIDs across Finland, Sweden, Norway, Denmark, Estonia, Latvia, and Lithuania.
- **Electronic Signing APIs:** Enabled legally binding electronic signatures within customer journeys, helping reduce fraud and support fully digital service delivery.

This setup allowed If to:

- **Boost customer engagement and satisfaction** through secure, user-friendly digital channels
- **Accelerate expansion** with scalable identity services adaptable to new markets
- **Gain better insight** into customer behaviour with millions of secure digital interactions
- **Support risk management and fraud reduction** by using trusted digital identities for secure customer logins
- **Build long-term trust** with customers through consistent and compliant digital experiences
- **Ensure compliance** across European regulatory frameworks, including eIDAS

Final Takeaways

Signicat helped the insurance company turn its digital identity infrastructure into a competitive advantage. Using **Signicat's eID Hub and Signicat's Electronic Signing API suit**, they unified identity verification across countries, provided secure eSigning, and boosted customer satisfaction while enabling growth in new markets. Their approach shows how the right technology partner can support long-term success in regulated industries.



To wrap up your electronic signing journey, remember that **the right solution doesn't just tick a compliance box**—it empowers your organisation to operate smarter, faster, and with greater confidence. Whether you're integrating complex workflows through robust APIs or getting started instantly with the Dokobit Portal, Signicat offers a **flexible and future-ready signing ecosystem**. By choosing the appropriate tools for your organisation's needs, you ensure every signature is secure, every process is efficient, and every customer interaction builds trust.

[Check our electronic signing site](#)

[Talk to an expert](#)

