Market Guide for Electronic Signature

Published 6 July 2023 - ID - 39 min read

By Analyst(s): James Hoover, Tricia Phillips

Initiatives: Security of Applications and Data

While commoditization of electronic signature functionality has proliferated, complex regulatory requirements can complicate some use cases. Security and risk management leaders must balance identity, compliance, data security, business and IT strategy considerations in their selection of solutions.

Overview

Key Findings

- The market for electronic signatures has become largely commoditized, and basic electronic signature (BES) is increasingly offered as either core functionality in content services platforms (CSPs) or as a feature in other purpose-built software (such as contract life cycle management). Some organizations even bypass BES for unregulated, internal approval use cases that can be addressed with the native user authentication, workflow and audit trail capabilities in business-process-specific applications, such as ticketing systems, expense systems and HR platforms.

- Many organizations that rushed to select and deploy electronic signature capabilities in 2020 are reassessing the value provided by a fully fledged electronic signature solution — and whether it makes sense to pay for a premium product in a commoditized market.

- Global adoption has been slower than the adoption experienced in North America from 2020 to 2022, largely due to more complex legal and regulatory requirements and the requirement for country-specific trust service provider integrations.

- Identity-related functions are increasingly important or required from a regulatory standpoint in B2C or high-risk use cases. These can include strong user authentication, identity proofing, digital identity wallet integrations, or use of digital certificates issued by a trusted entity. These functions have increased the strategic relevance of trust service providers (TSP) and identity orchestration platforms.

Recommendations

Security and risk management leaders responsible for the security of applications and data and electronic signature technologies should work with lines of business to:

- Reevaluate the approval or BES capabilities available in applications supporting document management or other business processes. Identify use cases that can be adequately addressed without the use of a third-party electronic signature platform.
- Evaluate the importance of user experience, branding and control over the signing process from end to end and ensure that the selected technology supports long-term user interface and user experience (UI/UX) objectives. Pay particular attention to developer tools and customizations available, and where third-party branding is required.
- Select products that can integrate with government-sanctioned certificate authorities, trust service providers and digital identity wallets (or other identity verification capabilities). To inform this decision, identify the legal and regulatory requirements for each use case and geography.
- Reduce the footprint of data duplicated in multiple cloud and SaaS platforms, and ensure document portability requirements are defined and part of vendor selection criteria. Define requirements for long-term document storage, data residency, and retention across use cases.

Market Definition

Electronic signatures are a digital representation of an individual's agreement that is intended to be the equivalent of a "wet" signature. Electronic signatures encompass a set of methods that can be applied to a digital document to capture intent to sign, and consent to sign electronically. They do this by electronically gathering metadata related to all signing events, and creating an audit trail that is cryptographically sealed to ensure document authenticity, nonrepudiation and integrity of the electronically signed document. This audit trail may also contain various supporting evidence of the individuals signing the document, such as names, email addresses, identity proofing and authentication steps. Evidence details may vary with each product, but the audit trail provides evidence to support the legal value of the document.

A digital signature (as it relates to document signing) is a type of electronic signature that, in addition to the requirements of an electronic signature, also requires that each signer sign the document with a digital certificate that is explicitly issued to them. There are legal and regulatory nuances in many countries that affect the type of documents that can be signed digitally, the acceptable issuers of certificates for different use cases, and whether the certificate can serve an identity-proofing function.

Market Description

The market for electronic signature platforms is separated out by the ability to support legal and regulatory requirements, which vary significantly by geography and use cases. The market is also segmented according to support of business process and workflow requirements through API-level integrations or prebuilt connectors enabling configuration-level enablement.

An electronic signature can have the same legal status as a handwritten, wet-ink signature on a paper document when implemented in compliance with the laws or regulations applicable to the parties involved.

Digital signatures can offer more-robust e-signature processes by providing strong nonrepudiation (see Note 3), because cryptography provides proof of the integrity and origin of each individual's signature. However, this requires more complex operation (and higher cost), due to the requirement to use digital certificates for each signee (see Note 4).

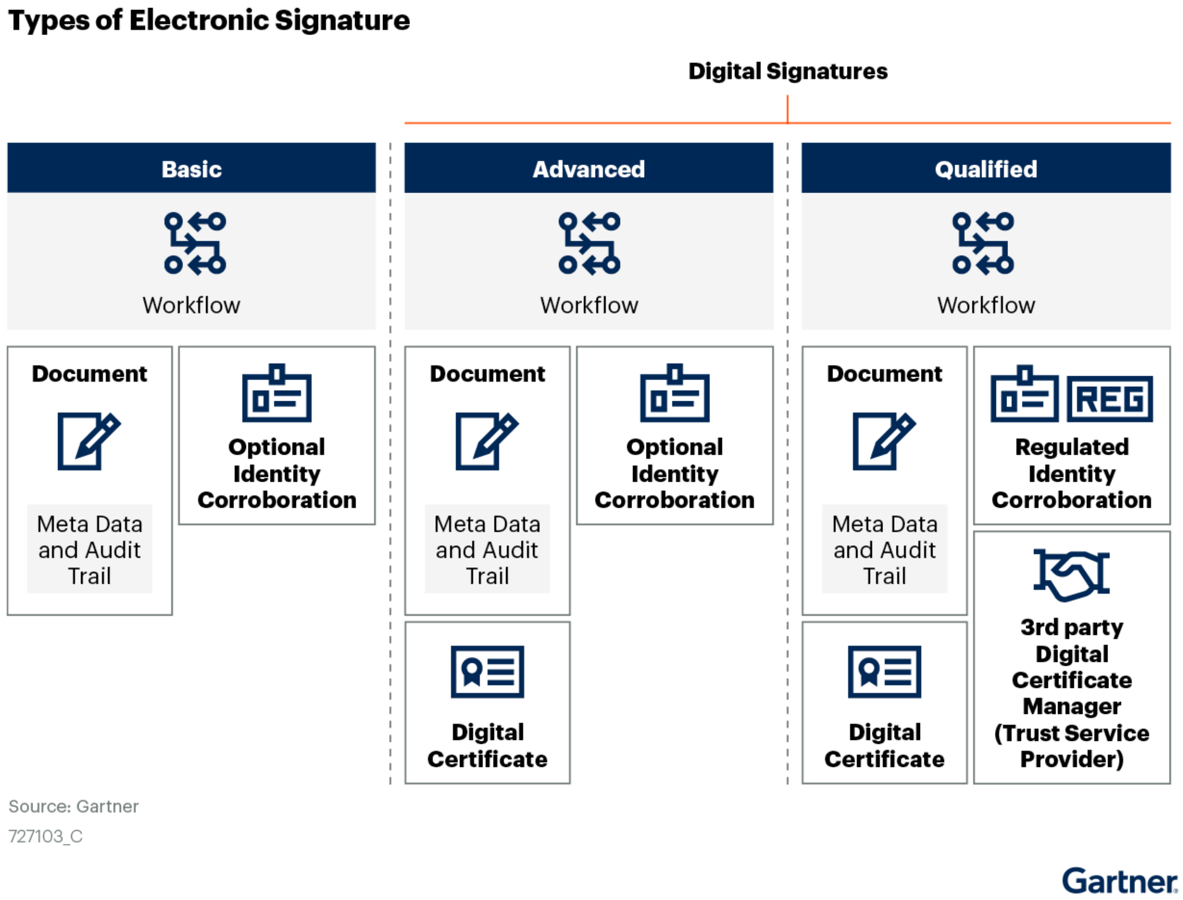
While the specific terms used for categories of electronic signature vary by country or region, electronic signatures generally fall into the following three categories (see Figure 1):

- **Basic (click-to-sign) electronic signature (BES)** — This type of electronic signature is sometimes called “standard” or “simple.” It does not use digital certificates assigned to an individual signer, opting instead to collect metadata about each signer, which is typically protected with a single digital certificate at the completion of the signing ceremony. This ensures that the document cannot be tampered with or altered. Countries such as Australia, Canada, Ireland, New Zealand, the U.K. and the U.S. have widely adopted click-to-sign because the legal construct for e-signatures in these countries is technology-neutral (although digital signatures, discussed below, would also be acceptable). Click-to-sign can be an attractive approach, due to its ease of implementation, low complexity and low impact on the user experience. In addition, some countries have additional laws that may accept the basic signature for specific use cases, even if there are national regulations in place that indicate the need for a digital signature.

- **Advanced electronic signature (AES)** — This type of signature uses self-acquired digital certificates assigned to each signer, which provides a high level of safeguarding against tampering or altering after the document has been signed. However, the level of identity assurance is determined by the issuer of the certificate and can vary dramatically based on the identity proofing and authentication practices enforced by the entity issuing and managing those certificates (from simple SMS or preshared code authentication to fully fledged document based identity verification).

- **Qualified electronic signature (QES)** — Many countries, including some in the Asia/Pacific region, the Middle East, mainland Europe and South America are more prescriptive in how e-signature technology can be used, and may require “qualified” e-signatures for some use cases. “Qualified” signatures rely on the use of a digital certificate that has been issued to an individual by a certified entity who has met defined requirements for identity proofing and user authentication at both the time of issuance, and the time of use (in the case of a multiuse certificate). This generally requires a standards-based process to assign a digital certificate to an individual or organization, based on a digital ID validated by a government- or industry-sponsored identity-proofing scheme. Certificates are provided either on a physical identity card or a hardware token, or they are issued onto the secure element of the key store of a mobile device or computer. Each digital ID process is typically unique to that country and some countries may have multiple schemes in use. It is important to check that any product supports the different digital ID schemes required or preferred for each country.

Figure 1: Types of Electronic Signature


Types of Electronic Signature
Digital Signatures
Basic
Workflow
Document
Meta Data and Audit Trail
Optional Identity Corroboration
Advanced
Workflow
Document
Meta Data and Audit Trail
Optional Identity Corroboration
Digital Certificate
Qualified
Workflow
Document
Meta Data and Audit Trail
REG
Regulated Identity Corroboration
3rd party Digital Certificate Manager (Trust Service Provider)
Digital Certificate
Gartner

Source: Gartner
727103_C

Document-centric identity-proofing functions can be mandated by governments (as qualified signatures). They may also be used to reduce the risk of identity fraud or identity disputes in a remote-signing event. These methods can be critical for the protection of high-risk use cases, but do carry additional cost, complexity around eID schemes, and impact to user experience (see Top Trends in Government for 2022: Digital Identity Ecosystems).

Market Direction

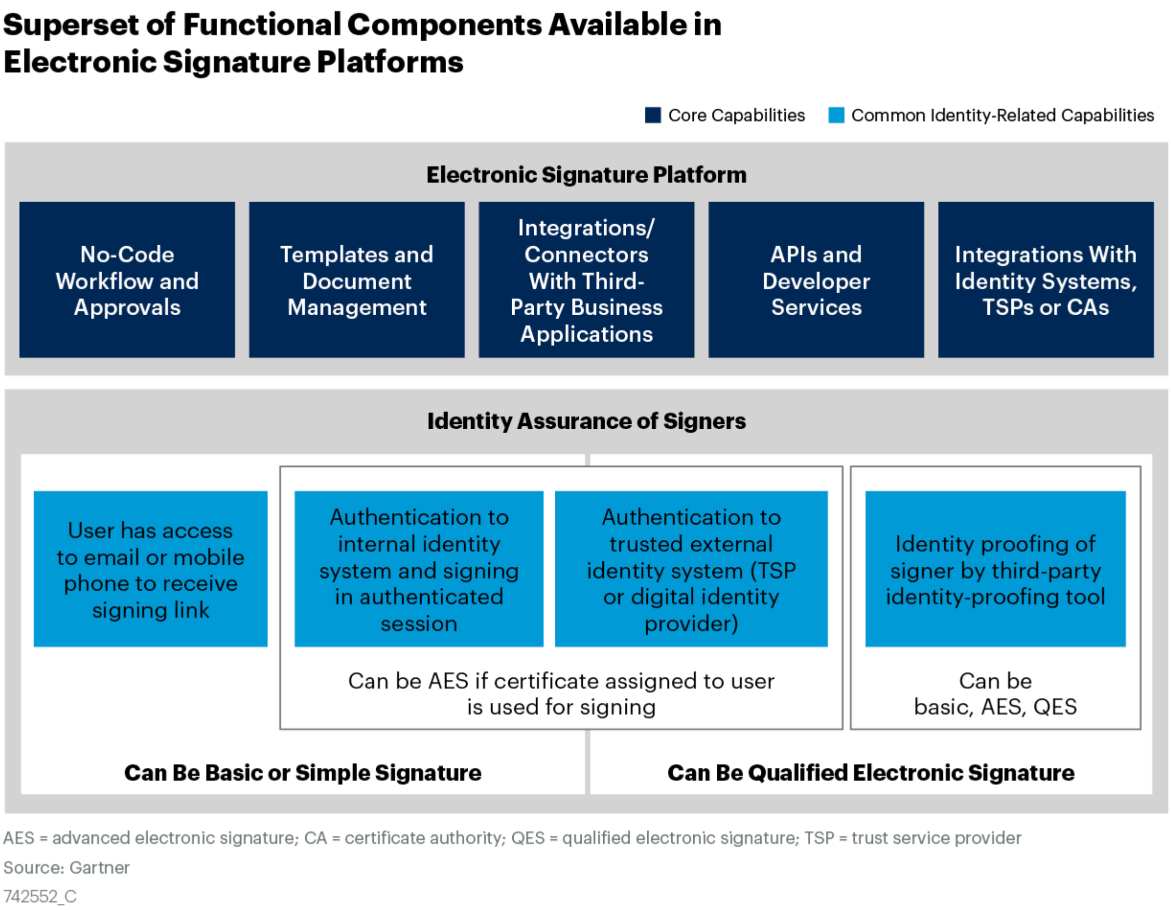
Most providers of electronic-signature platforms offer a range of services to support the electronic signature process. The extent of this varies significantly depending on geographic or industry focus. Capabilities supported by an enterprise electronic signature platform should include:

- Low-code custom workflow creation.
- Mobile-optimized signing experiences.

- Identity proofing and corroboration.
- Authentication and authorization.
- Certificate management.
- Template and document management.
- Prebuilt integration with a multitude of other business applications (such as ERP platforms, HR systems, document management and contract life cycle management applications).
- APIs and software development kits (SDKs).

Most enterprise or globally focused electronic signature providers also include or support integration with third-party certificate authorities, as well as trust service providers to support QES. However, it is critical to explicitly validate the level of out-of-the-box support for specific third parties. These integrations typically create a multicloud scenario that requires careful management of data residency impacts around the world (see Figure 2).

Figure 2: Super Set of Functional Components Available in Electronic Signature Platforms



Superset of Functional Components Available in Electronic Signature Platforms

■ Core Capabilities
■ Common Identity-Related Capabilities
Electronic Signature Platform
No-Code Workflow and Approvals
Templates and Document Management
Integrations/ Connectors With Third-Party Business Applications
APIs and Developer Services
Integrations With Identity Systems, TSPs or CAs
Identity Assurance of Signers
User has access to email or mobile phone to receive signing link
Authentication to internal identity system and signing in authenticated session
Authentication to trusted external identity system (TSP or digital identity provider)
Identity proofing of signer by third-party identity-proofing tool
Can be AES if certificate assigned to user is used for signing
Can be basic, AES, QES
Can Be Basic or Simple Signature
Can Be Qualified Electronic Signature

AES = advanced electronic signature; CA = certificate authority; QES = qualified electronic signature; TSP = trust service provider

Source: Gartner

742552_C

In addition to the core functionality of an enterprise electronic signature platform, many providers focused in regions with complex and dynamic regulatory requirements (such as eIDAS in Europe) have expanded their own capabilities via acquisition, development, or integration. This allows these providers to offer the functionality of a trust service provider (sometimes including the issuance of “qualified” signature certificates), discrete public key infrastructure (PKI) services, identity proofing or user authentication functionality. Increasingly, these providers can also offer integration with third-party digital wallet schemes, which can offer high-assurance identity verification.

B2E- and B2B-focused business-process-focused solutions have a varying level of sophistication with regard to the features and integrations that supplement the core electronic signature features. They can include simple to complex workflow features, support for various levels of identity corroboration and authentication requirements. They can also include integration to commercial off-the-shelf (COTS) business applications, from which business processes originate (such as CLM or procurement platforms, human resources tools, CRM, and document generation and management tools) and connectors to document management platforms. Additionally, integration to applications via a system of record (SOR) may be provided to allow data elements to be automatically linked to populate certain fields in a document. Also, once a document signing process is completed, it may be possible to export certain fields automatically back into an SOR.

Government to constituent (G2C) and B2C (as well as some higher-risk B2B- and B2E-focused use cases) often bring regulatory and legal requirements. This can create the need for integrations with multiple trust service providers (TSPs) or qualified TSPs (QTSPs), certificate authorities (CAs) and digital identity (ID) schemes for externally facing use cases (see Note 2). There are hundreds of regional or national players meeting country- or region-specific services. This has resulted in a relatively small number of truly global providers that can act as a cross-border platform for electronic signature workflow. These providers strategically develop, partner with, or integrate to dozens (or hundreds) of local CAs, TSPs or QTSPs. There are also a growing number of regionally focused providers with a handful of relevant QTSP, TSP or CA integrations.

In general, there is decreasing demand for the more traditional on-premises, digital signature appliances — the likes of which were historically used for the internal signing of documents. However, in some regions where data privacy and residency requirements are particularly strict or complex, there is still an appetite for hosted (on-premises or private cloud) software solutions. Legacy signing appliances could support digital certificate management and digital signing for internal documents (but generally lacked business-facing workflow tools or integrations with external platforms and tools). Now, we see demand for full-stack software platforms with the complete range of electronic signature platform capabilities replacing those products.

Embedded Solutions

As basic electronic signature becomes more and more commoditized, we see an increase in acquisitions and OEM agreements that enable basic electronic signature offered as an add-on feature or included as part of the core functionality (within a document management platform, for example). The functionality is generally quite basic compared to what would be offered by a full-stack electronic signature platform and usually lacks extensive support for advanced or qualified signatures, or integrations with identity verification tools. However, it can be sufficient for some use cases. Examples include Box's electronic signature offering to existing customers, and ServiceNow's built-in e-signature function.

Additionally, most modern technology platforms with a significant workflow component (for example, HR management, human capital management [HCM], CRM, contract life cycle management [CLM], content services, document management and others) have supported integrations with electronic signature providers. This enables the efficient application of electronic signatures for use cases and workflows completed through their system. Overall, this ensures that the end user is able to complete the entire workflow (for example, onboarding a new employee) in the system selected for those business processes. There is no need to hop between the business process platform and an electronic signature platform.

The leading electronic signature solutions provide APIs and SDKs to support these types of platform-level integrations. Many have built feature-rich connectors with popular platforms such as Salesforce, Microsoft 365, Microsoft Dynamics 365, SAP Ariba, Workday and Hyland. The depth of integration and simplicity of use of electronic signatures within the chosen business process platform are often key factors in vendor selection. Most vendors also offer strong support to help customers integrate to any application not currently supported, or to enhance or strengthen any existing API.

There has also been an increasing need for electronic signatures in low-complexity, high-volume use cases, where the traditional per-transaction or per-user pricing method is difficult to justify. Some examples are building permit applications, remotely signed petitions and onboarding of contractors in a mobile service marketplace. While the leading electronic signature providers offer API-based electronic signatures for this scenario, some vendors, such as HelloSign (a Dropbox company), have a developer-first product and sales strategy. This includes pricing models for high-volume API-enabled signatures (as well as the more traditional per-user model).

There is still significant demand for stand-alone electronic signature platforms with feature-rich user portals and custom workflow capabilities to support global, enterprisewide use cases. However, some sophisticated clients are exploring a strategy that matches use cases with the most appropriate and economical solution. It is increasingly common for organizations to use native electronic signature capabilities for low-complexity use cases and using a dedicated electronic signature product for more-complex use cases.

External Use Cases

External use-cases such as new-hire paperwork, customer agreements and financial services documents are the primary drivers for adoption of electronic signature technologies. These can be documents for individual customers, vendors or partners, but in all of these cases, the contract needs to be signed by someone external to the organization. This puts a greater burden on identity assessment to protect against fraud. Enterprise electronic signature platforms support a variety of authentication features (such as one-time passwords [OTP] for known and trusted recipients). They also support integration with identity proofing or high-assurance digital ID providers for higher-risk use cases.

Internal Use Cases

Low assurance internal signature processes continue to make up a noteworthy percentage of overall signature consumption. These use cases are often not legal documents, but rather use cases such as daily attestations of health, time sheet approvals, travel approvals and IT asset approvals. Many of these use cases have historically required a signature by policy. Nonetheless, they could be more appropriately handled with business process workflow automation features inherent in digital business platforms — such as ticketing systems, HR platform workflows, timekeeping and expense management systems.

Increasingly, SaaS-delivered business applications include workflow capabilities for their targeted business processes and use cases. Gartner sees more organizations maximizing their investment in these tools for low-risk, unregulated approvals, which just a few years ago may have required a wet or electronic signature. This trend is causing some organizations to reduce the subscription volume of electronic signatures that they purchase from a discrete electronic signature platform.

Many government and regulated industries have used a traditional self-managed, certificate-based digital signature solution for employees to digitally sign emails and documents (perhaps using the digital certificates issued to them on their smart cards, or using tokens). However, this is not where we are seeing the majority of demand. There have been improvements in the security posture for enterprise user authentication (including wide adoption of multifactor authentication [MFA] and single sign-on [SSO]). This has enabled low- and medium-assurance use cases to be performed without the application of a certificate-based digital signature (provided that the employee is required to authenticate prior to accessing the email account, network applications or SaaS applications where they are prompted to electronically sign a document). Rather, the basic electronic signature is sufficient for most internal use cases, when combined with the user-authentication protocols.

Ultimately, for any internal use case, it is important to weigh the value of creating and paying for each document using an electronic signature product against other processes that do not have additional costs. It is important to understand the value of adding a representative signature to a document while providing legal evidence through an audit trail document.

Changing Regulatory and Legal Requirements

Regulatory and legal requirements are another key driver in somewhat separated geographic markets. Vendors, primarily focused in the U.S. and Canada, offer electronic signature products that support the basic click-to-sign electronic signature type. This is due to the relatively vague identification and consent documentation requirements in the national regulations (the Electronic Signatures in Global and National Commerce [ESIGN] Act in the U.S. and the Personal Information Protection and Electronic Documents Act [PIPEDA] in Canada). However, these vendors may not have support for the more prescriptive and stringent requirements in other parts of the world.

The eIDAS framework (see Note 3) continues to set the standard for the global direction of e-signature regulations, as more countries are developing their own similar standards and technological requirements for high-assurance digital signatures. Many countries — including, but not limited to, India, Brazil, Mexico and Malaysia — have one or more government-approved CA that must be used for a qualified signature (the highest level of assurance). These certified CAs are, with some geographical variation, referred to as TSPs (see Note 4).

Because of these changing regulatory dynamics, a critical consideration in the selection of an electronic signature vendor is whether it can support integration with certified TSPs in countries where these regulatory structures are emerging.

The Intersection of Identity Verification and Electronic Signature

In some regions, like the EU, the requirements around identity corroboration for high-risk electronic signature use cases are regulated and explicit (requiring a QES). In other regions, it is left to the initiator of the document to determine the level of identity proofing or user authentication that may be necessary. However, for all use cases, there is a growing need for the use of digital and video ID techniques to support BES, AES and QES.

In the United States, there is a lack of identity standard for customer and citizen interactions that would be the equivalent of eIDAS. The closest thing to a “qualified” electronic signature is a document that requires a notarization in a state where it is allowed. The remote online notarization landscape is complex and dynamic with each state defining their own requirements (or lack thereof) for remote online notarization (RON).

While Gartner does not formally cover the RON market (or the TSP market), the relationship between electronic signature and identity verification, and the need for RON for high-value/high-risk use cases in the United States makes it a relevant topic for some clients. Vendors like Notarize have created an extensive platform that simplifies the business logic to determine whether a person can sign a particular document. This is based on the location of the business entity requiring the signature, the location of the signer, and the type of document. These vendors have RON technologies supporting scheduled and on-demand notarization using their network of independent notaries; or if preferred, an organization can have its own qualified notary public perform the notarization, and the platform simply provides the technology stack. Notarize does not offer an electronic signature platform, but it has partnered with Adobe to enable RON for documents signed through Adobe Acrobat Sign. Other notable vendors that offer both an electronic signature platform and a remote online notary capability include DocuSign and SIGNiX. However, increased legalization and interest in RON is driving significant advancement in this space, and we expect to see continued partnerships and feature development.

Market Analysis

While the core technology of electronic signatures is highly commoditized, the business, legal and regulatory requirements make the selection of an electronic signature provider or providers an important cross-functional initiative. Support for workflow features, specific platform integrations, user experience of signer and sender, and integration to TSPs in key markets can all drive the selection of one vendor over another.

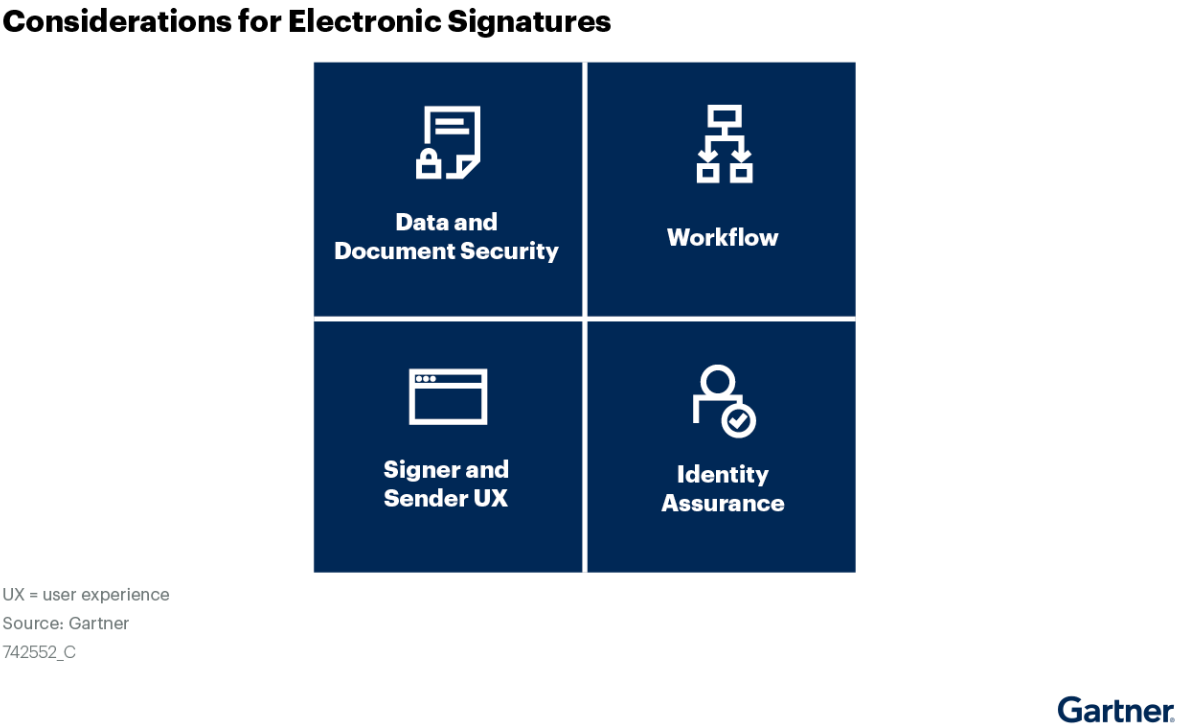
E-signature adds efficiencies as part of the digitization of paper-based processes, such as contracting, internal compliance processes, HR processes, and banking and insurance applications. ROI can be achieved through reduced processing time and savings in postage, courier and administrative fees, and physical storage and archiving costs, by using e-signature as an enabling technology. There are also opportunities to shorten customer acquisition time and improve onboarding and transaction completion. Ideally, this results in fewer customers going to competitors or canceling business transactions because of lag time or the effort required to fill out and return paper forms.

The selection of an electronic signature platform (see Figure 3) must include considerations of:

- Core functionality and workflow capabilities.
- The ability to meet identity assurance requirements (whether driven by regulatory and legal requirements or fraud and risk mitigation).
- The user experience of the sender and the signer, including the ability to white-label and customize the end-to-end experience if desired.
- Support for data security, privacy and retention and portability requirements.

Some vendors excel in one area but are weaker in others. Very few, if any, excel in all four categories. It is important to have the business (including product and development) and risk and legal teams detail their requirements in the identity assurance and UX categories. Security, IT leadership, and legal and compliance should define data security, privacy and residency requirements. This, combined with more detailed functional requirements, will enable an appropriately weighted set of requirements. In turn, this will enable the strategic selection of one or more providers for the organization’s various needs (see Note 7).

Figure 3: Considerations for Electronic Signatures


Considerations for Electronic Signatures
Data and Document Security
Workflow
Signer and Sender UX
Identity Assurance
Gartner

UX = user experience

Source: Gartner

742552_C

Licensing Models

Some of the leading providers offer multiple versions of their products. Most Gartner clients looking for a companywide solution across multiple use cases, platforms and departments find that the versions of the product that are best-suited for them are the enterprise versions. This is largely due to the security and compliance capabilities included in these product versions, such as SSO and organizational management, and the available connectors for common SaaS products, such as Microsoft 365, Workday and Salesforce. In an RFP, these enterprise-level products will check off almost all the same boxes in terms of functionality, including support for:

- SSO
- Delegated signing
- Organizational management
- Complex workflows
- Integrations into other applications
- Authentication and identity verification of signers

It is important to recognize that the core capabilities for signing a document with click-to-sign have reached commodity status for the most part. The differences come from the more nuanced user experience features (for the senders and the signers), some third-party integrations and industry-specific functionality. However, these features typically come with additional costs. Therefore, it is important to weigh the one-off cost of creating additional API functionality against higher per-document or per-user license costs.

Electronic signature products are generally licensed either by user or by “transaction.” User licenses typically have a transaction cap (for example, 100 transactions per user per year), which results in overbuying in some cases, and excessively complex licensing management in others. For this reason, we generally recommend transaction-based licensing to ensure maximum transparency for midsize to large enterprises. Smaller organizations that will perform a limited number of transactions per year by a small number of employees may find that the user-based licensing model is a better choice.

The price per transaction can vary significantly between providers, which can create some cost justification challenges across all use cases.

It is increasingly common that business use cases fall into two general categories:

- Low complexity/risk with less sensitivity to user experience.
- High complexity/risk with more sensitivity to user experience.

This division often aligns with internal use cases (low complexity/risk) and external use cases (higher complexity/risk). When a division exists and the expected volumes are significant, there may be justification for selecting a more sophisticated and expensive solution for the high-complexity use cases, and selecting a more cost-effective solution for the lower-complexity use cases. In a global organization, the division might come down to geography, and a country-specific solution may be the best choice for a segment of the business.

Supporting more than one electronic signature solution across the enterprise does theoretically reduce the volume discount that would be possible with a single-solution approach. However, in many instances, the cost difference between the complex solution and simple solution more than makes up for that theoretical loss of discount. Evaluate the requirements for each use case — including the platform integrations that are needed — to determine whether some use cases justify a custom-made solution.

A limited number of vendors offer alternative licensing schemes. Some of these, such as Citrix or Box, are part of an e-signature-as-a-feature approach, and others like SigniFlow and emSigner offer a self-hosted model.

Finally, attention should be paid to the highest-priority use cases and any differentiating features or experiences that support business objectives. For example, DocuSign has built out some extremely differentiated functionality for lending use cases, enabling a smoother loan application process for financial services, which can have benefits beyond the value of an electronic signature. Some of the leading global providers also offer supplemental products to support FDA 21 CFR Part 11 compliance. Look for a provider with a meaningful footprint in your specific industry to increase the likelihood that it has or will prioritize requirements that are specific to your use cases and compliance obligations.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

There are hundreds of electronic and digital signature providers globally, and increasingly there is little functional distinction between them. The areas discussed in this Market Guide will drive selection criteria — particularly those around the different adjacent capabilities (see Figure 2) including identity assurance, data and document security, and sender and signer UX. It is also important to understand how those capabilities meet the needs of various use cases across an organization.

The representative vendors listed are those most commonly mentioned in inquiry with global Gartner clients. As demand for electronic signatures increases, and regulatory requirements change, vendors are actively expanding their capabilities to meet evolving client needs. This is true of the representative vendors based in the EU and U.K. — many of whom have historically focused on traditional digital signatures, or acted as a trust service provider. Still, these vendors may not have previously focused on the softer side of electronic signature such as no-code workflow for business users, third-party platform integrations, or, more broadly, the user experience. These vendors are increasingly offering more user-friendly and self-service business workflow tools. They are also expanding their core trust services to be more flexible and support more diverse integrations to other TSPs and identity-assurance partners.

Similar expansions of functionality have occurred with vendors that historically focused on basic electronic signature (BES), but had little to no meaningful support for advanced, or qualified signatures, or identity assurance integrations for high risk use cases. These vendors may have also lacked the kind of multiregion hosting options required to support many data privacy and sovereignty requirements.

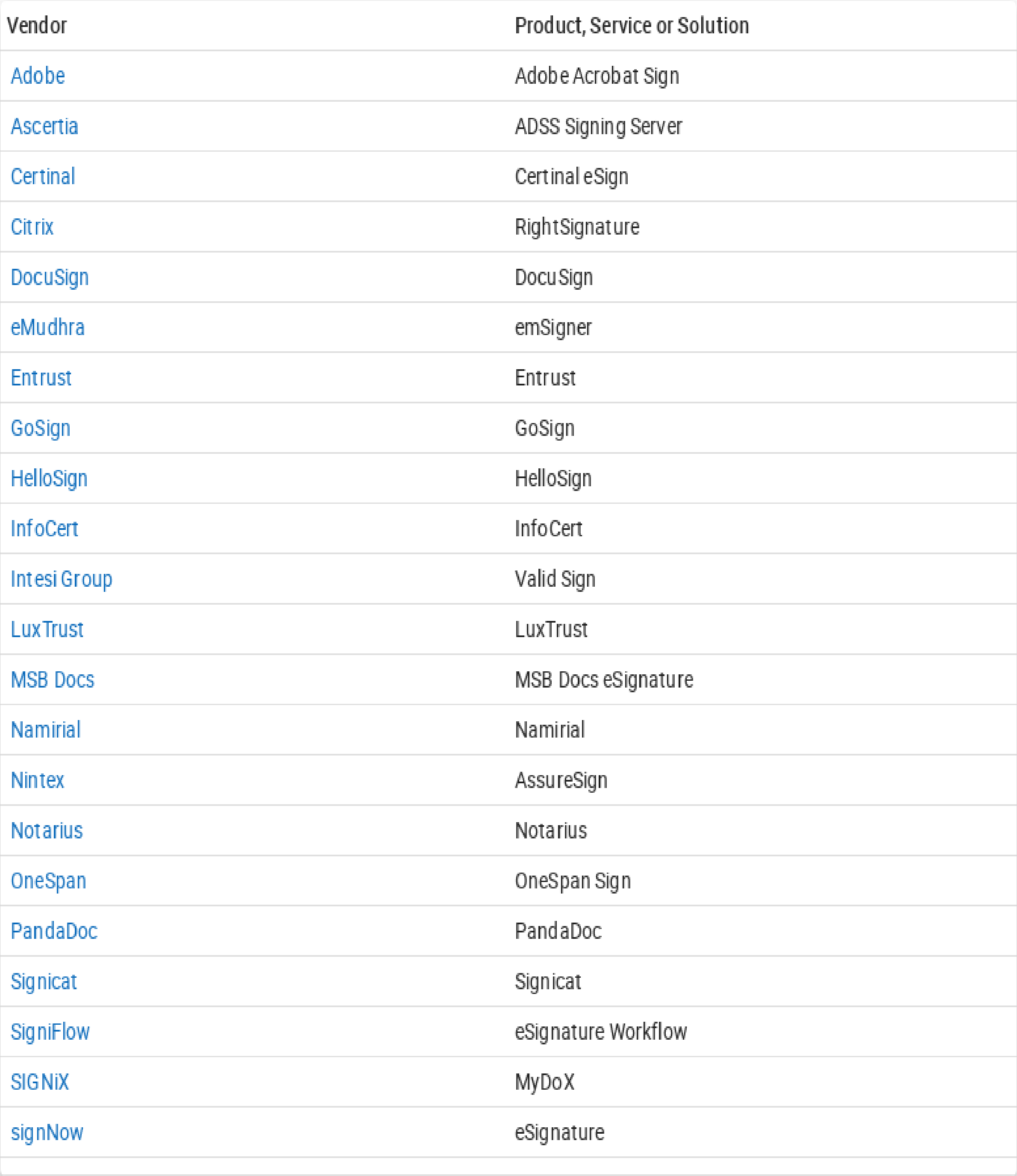
For these reasons, the separate categories for electronic signature providers detailed in the 2020 version of this Market Guide are no longer meaningful and have been omitted. For a comprehensive and current assessment of features offered by a particular vendor, it is recommended to contact that vendor.

Table 1 provides a list of providers (see Note 1).

The following representative vendors have been selected based on client interest, regardless of revenue or market share. Vendors in every category continue to invest in their products through expanded features and integrations. Therefore, the allocation of a vendor to a category is only directional and based on qualitative, rather than quantitative, product assessments, and may change by the time you read this research. Only vendors that offer a stand-alone electronic signature platform are included. Vendors whose core products are in document management, CLM or other markets, but who have electronic signatures available as a feature, are not included in the representative list.

Table 1: Representative Vendors in Electronic Signature

(Enlarged table in Appendix)



Vendor	Product, Service or Solution
Adobe	Adobe Acrobat Sign
Ascertia	ADSS Signing Server
Certinal	Certinal eSign
Citrix	RightSignature
DocuSign	DocuSign
eMudhra	emSigner
Entrust	Entrust
GoSign	GoSign
HelloSign	HelloSign
InfoCert	InfoCert
Intesi Group	Valid Sign
LuxTrust	LuxTrust
MSB Docs	MSB Docs eSignature
Namirial	Namirial
Nintex	AssureSign
Notarius	Notarius
OneSpan	OneSpan Sign
PandaDoc	PandaDoc
Signicat	Signicat
SigniFlow	eSignature Workflow
SIGNiX	MyDoX
signNow	eSignature

Source: Gartner (July 2022)

Market Recommendations

- Work with line of business (LOB) leaders to assess the enterprisewide priorities and requirements for electronic and digital signatures. Identify where a third-party signature solution is required, and where existing tools may provide workflow or signature capabilities that are sufficient.
- For external use cases, carefully consider UX and branding requirements, as some vendors do not allow white-labeling of the signing experience. Also consider whether the vendor can provide identity assurance functionality to meet rapidly changing regulatory requirements.
- Different use cases (internal versus external, or high-risk versus low-risk) may have dramatically different priorities and requirements (see Note 7). Don't be afraid to take a multivendor approach to electronic signatures if it meets your business priorities, provided that with this approach, you can still meet your legal, security and compliance requirements.
- Pay close attention to proliferation and fragmentation of sensitive data in multiple vendor clouds and concerns around residency, privacy and portability.

Note 1: Representative Vendor Selection

This Market Guide provides Gartner's coverage of the market and highlights the market definition, rationale for the market and market dynamics. Gartner is directly aware of more than 40 vendors that offer various forms of electronic signatures that align with several or all of the potential use cases, though hundreds exist.

The vendors named in this Market Guide were selected to represent several of the readily recognized vendor market origins described in the Market Introduction section. Readers should use Table 1 as a general guide for studying vendors, and should consider all applicable candidate vendors that interest them, whether or not they appear in this research.

Note 2: Legal Aspects and Disclaimer

Some vendors offer useful guidance as a starting point for the legal status of e-signatures and the preference for particular technologies within different countries. For example:

- Adobe's Electronic Signature Legality
- DocuSign's eSignature Legality Guide

- eMudhra's Global eSignature Compliance Guide
- OneSpan's Electronic Signature Legality

Disclaimer: Gartner does not practice law, and the opinions and recommendations in this document should not be construed as legal advice. Gartner recommends that entities subject to legislation seek legal counsel from qualified sources before implementing policy or products pertaining to regulated activities.

Note 3: eIDAS

EU Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation) was adopted by the Council of the EU on 23 July 2014. It became effective on 1 July 2016.

Note 4: The Role of CAs in the E-Signature Market

A CA is an internal or third-party entity that creates, signs and revokes digital certificates that bind public and private keys to user identities. A repository or directory stores digital certificates and certificate revocation lists (CRLs) to enable users to obtain the public keys of other users and determine revocation status.

In the context of regulations governing the use of digital signatures (such as in the EU or Switzerland), a third-party CA that meets certain requirements can be designated a TSP or QTSP. It can also be referred to as a certification service provider. The designation of QTSP confers a responsibility to provide identity assurance of signatories using robust mechanisms for identity proofing and authentication. TSPs facilitate a trust framework for electronic transactions to be conducted between countries and organizations. Specific regulations (such as eIDAS in the EU) govern how TSPs are established and provide their authentication and nonrepudiation services.

In the EU, a qualified TSP (or QTSP) plays a critical role in a qualified e-signature process. A qualified e-signature is important in the EU, because it is the only type of e-signature that is legally equivalent to a wet-ink signature, and it has mutual recognition of its validity by all EU member states. This mutual recognition is foundational for the creation of an EU-wide single market for e-signature.

A TSP can be granted qualified status by a supervisory governmental body, which gives it permission to provide qualified trust services used in creating QESs. Under eIDAS, the EU maintains the EU Trusted Lists, which is the central and definitive publication of TSPs that have been granted qualified status. Only TSPs on this list are allowed to provide qualified trust services, and they must adhere to strict guidelines set forth by eIDAS to maintain their qualified status.

QTSPs have been granted qualified certificates under eIDAS or other national schemes for digital signatures, seals and time-stamping for qualified digital signatures. These providers have integrations to one or more digital ID schemes or eIDAS-certified identity proofing tools. Global, enterprise electronic and digital signature providers will generally integrate with QTSPs to enable qualified signatures for use cases where they are required, and some are themselves certified as QTSPs (for example, DocuSign and InfoCert).

Note 5: Title 21 CFR Part 11

Part 11 of Title 21 of the Code of Federal Regulations (CFR) defines how electronic records and signatures are considered trustworthy by the U.S. Food and Drug Administration (FDA). If this use case is present, the e-signature vendor should be able to meet the technical requirements for achieving Title 21 CFR Part 11 compliance through native product features. Adobe Acrobat Sign, DocuSign, MSB Docs, signNow (airSlate) GoSign and others have purpose-built electronic signature modules available for compliance with this regulation.

Note 6: Long-Term Data Preservation

The concept of long-term data preservation — also known as long-term data validation (LTV) — is based on the fact that digitally signed documents can be used or archived for many years. Therefore, it should be possible to reliably and consistently confirm at any point in the future that an e-signature was valid at the time it was applied, despite subsequent advances in the underlying technology or cryptographic algorithms.

A set of standards have emerged to address these needs and to comply with eIDAS. They are maintained by the European Telecommunications Standards Institute (ETSI; see ETSI's Digital Signature for the most current specification documents), and comprise:

- XML Advanced Electronic Signatures (XAdES)
- PDF Advanced Electronic Signatures (PAdES)
- Cryptographic Message Syntax Advanced Electronic Signatures (CAdES)

Note 7: Business, Technical, and Security Requirements

Understanding Business Requirements

The first and most critical step in selecting an electronic signature solution is to enumerate and categorize the use cases. Use cases can be ad hoc and human-initiated, or they can be transactional and application-driven.

General use-case examples include:

- Business-to-business (B2B) — Nondisclosure agreements, procurement documents, and sales and service agreements.
- Business-to-consumer (B2C) — New account opening documents, loan applications, and sales and service terms.
- Business-to-employee (B2E) — Employment contracts, benefits paperwork and other employee onboarding processes. This category can also include employee-to-employee use cases. These may include interdepartmental documents or communication, approvals, memorandums of understanding. It also covers any other use case that may not be a legal document, but for which the business desires a formal consent or agreement and has no other means to satisfy the requirement. However, the benefits of ease of use must, of course, be weighed against a fee for each document created.

With input from business, legal, compliance, IT and security stakeholders, create an inventory of use cases, including requirements from each group. The information gathered may include, but will certainly not be limited to, the following information:

1. Name of use case.
2. Responsible business unit and department.
3. Internal or external signers.
4. Signer category (for example, employee, customer, vendor or partner).

5. Relevant data protection and privacy requirements

   - Does the document contain personally identifiable information (PII), protected health information (PHI), payment data, or other regulated or sensitive data? Are the use case and related documents subject to data residency or sovereignty requirements?

6. Policy-driven, legally-driven or compliance-driven?

   - In many internal use cases, the drivers of the requirement for an electronic signature are based on company policies and not laws.
   - Some industries have specific requirements for electronic signature, such as 21 Code of Federal Regulations (CFR) Part 11, the U.S. Food and Drug Administration's (FDA's) regulations for electronic documentation and electronic signatures (see Note 5).

7. If the policy is a legal document, which country has jurisdiction over this use case?

   - Does the law of that country support simple electronic signature for the use case, or does it require advanced or qualified signatures?

8. Which platforms or applications are involved in this business process?

9. What is the system of record?

10. What are the retention requirements? See Note 6.

11. What is the level of risk related to identity impersonation?

    - A document with financial implications may be at higher risk of identity fraud than other use cases, and would require a higher level of identity assurance.

12. What is the importance of user experience for sender and signer?

13. Does this use case require white-labeling, or would it be acceptable for the vendor's brand to be prominent to the signer?

14. What is the annual volume of this use case (how many documents, or packets of documents, need to be signed)?

15. What is the time spent processing the workflow, signature processes and digitization of documents related to this use case?

Understanding Technology and Security Requirements

Beyond the specific use-case-focused business requirements, compliance and security requirements will weigh heavily in the selection of a vendor shortlist. Requirements may include:

- **Deployment method**
  - Most workflow-focused electronic signature providers offer a SaaS delivery model, but only a few providers (including AlphaTrust, Ascertia, AssureSign, InfoCert, Namirial, OneSpan, emSigner by eMudhra, MSB Docs and signNow (airSlate) also offer a private cloud or on-premises deployment model.
  - Many government agencies in the U.S. require a FedRAMP-approved vendor. At the time of this writing, DocuSign, Adobe Acrobat Sign and OneSpan are the most common vendors selected by clients with FedRAMP compliance requirements.
  - The leading global solutions offering SaaS deployment have multiple global data centers, but it will be important to document the specific data residency requirements and confirm support with a potential solution provider.
- **Identity access management (IAM) functionality: Single sign-on (SSO)**
  - SSO is generally included in the “enterprise” version of the leading electronic signature products, and is sometimes available as a discrete add-on for less comprehensive versions of the products.

- **Organizational and administrative management tools**
  - Not all solutions have the type of sophisticated organizational management tools that may be needed in an enterprise deployment, so these requirements should be clearly defined. For example, workflows, templates and transaction history for HR use cases should not be visible to users responsible for customer service workflows. Identifying specific organizational scenarios will be important in the selection process for enterprisewide deployments that employ a heavy use of the provider's portal, rather than primary use through integrations into other business process workflow platforms.

- **Support, integration environments, reporting and self-service tools**
  - The leading providers vary in their approach to support and implementation services, with some including enterprise-level business and technical support in the core pricing, while others charge considerable support fees. In addition, some vendors may charge additional fees for APIs and authentication services. When comparing prices between vendors, it is critical to understand the full licensing and support models to ensure a like-for-like comparison.

- **Click-to-sign, digital signature or both**
  - Security and risk management leaders should work with line-of-business leaders and legal counsel to assess the jurisdictional e-signature requirements for each use case and select products that can integrate digital certificates to comply with national regulations, as needed (see Note 2).

- **API enablement**
  - Representational state transfer (REST) based or SOAP-based APIs are key to integrating with in-house or custom-built applications. Not all APIs are created equal. Some vendors offer sophisticated API sets that support many different methods and parameters with excellent documentation scalability and maintainability, whereas others are rudimentary. Therefore, an organization looking at doing integration work should analyze the APIs to determine whether they can support its integration plans.

- Identity assurance
  - This refers to the level of confidence that the credentials presented by a signer actually represent the real-world identity they purport to. Identity assurance combines and formalizes the evaluation of identity-proofing strength and authentication strength. There is no “one size fits all” approach, because a range of options address the different levels of assurance required by specific use cases.
  - For click-to-sign e-signature processes, many vendors support integration with third-party providers for identity proofing. These vendors often natively offer a variety of higher-trust authentication methods, including one-time password (OTP) tokens and out-of-band (OOB) authentication to bolster the default password-based authentication (see Manage the Critical Risks of Using Electronic Signature).
  - Digital signature products that support qualified e-signatures typically have identity assurance built into the process natively to provide the right level of confidence in the authenticity of the signer’s identity, as prescribed by eIDAS. This entails requiring identity proofing when users initially obtain a certificate and authentication when they subsequently use it — that is, when they digitally sign.
  - With any business use case, it is important to establish how identity proofing needs to be carried out as a process in order to gather sufficient legal evidence of the identity of each signee. QES are only available in specific countries and, with more and more cases of remote working, it will be increasingly difficult to meet the signees. Therefore, review whether and if any digital ID process is needed and available from the vendor, and ensure that it records sufficient evidence to support the legal requirements for each use case.

- Workflow and tracking
  - Functionality in this area can vary widely across products. IT security and LOB leaders should compare the functionality listed below against their requirements. The ability to track the progress of a number of documents from a single management console is important to providing operational predictability, especially when multiple signers are involved. Organizations should also review how documents are generated. Vendor pricing can depend on the number of users, transactions or signing methods. Understanding these bounds is important, because they can have a major impact on the cost.
    - **Document template creation** — Internal document creation workflow must address the number of individuals who will be involved in the creation of documents and which applications they will use. Ad hoc creation may require frequent support from IT, and, if many staff are involved, then the IT organization could be overburdened. The breadth of workflow capabilities — such as signer notification and multiperson signing ordered in serial or parallel — should be considered as well.
    - **Template creation and modification** — The simple creation and modification of templates from integrated products (such as Salesforce, SAP and Microsoft SharePoint) can be important. Many vendors offer APIs and the ability to integrate with proprietary applications. Organizations should check whether there are requirements for modifications to these applications and whether the vendor supports these changes. Always develop integrations to the e-signature product, rather than the other way around, to maintain flexibility with regard to changing vendors in the future.
    - **Centralized tracking** — The management console can monitor and track the status of multiple documents against each signee.

- Certificate management
  - Digital signatures can be used effectively. However, they require an internally managed or third-party certificate authority that often requires holistic management (for more information, see Technology Insight for X.509 Certificate Management). For use cases that involve the EU or other technology-prescriptive countries, security and LOB leaders should confirm that a vendor can address digital signature requirements for each country. This should include integration with CAs that are recognized nationally, and that support advanced or qualified e-signatures. These requirements could also include the use of advanced or qualified signature products.

- Audit trail preservation
  - All electronically signed documents should have an audit trail that captures the essential metadata and workflow associated with the signing ceremony to provide legally binding evidence and document integrity. This might include authentication attributes, date, time, consent ("I agree") and geographic location, as well as evidence of where the e-signature was added to the document by each signee. This could also include a cryptographic wrapper, as each e-signature is added, which seals the document to maintain its integrity.
  - Each click-to-sign vendor product is proprietary in its provision of the audit trail and may require different levels of support from the vendor or independent technical experts, if a legal challenge occurs. Security and risk management leaders should work with LOB leaders to consider ways in which they can preserve the derivative files and audit trail from the vendor's e-signature process (such as archiving in PDF/A format). This will mitigate the risk of moving from one vendor to another. In the EU, specific requirements must be met to ensure long-term data preservation (see Note 6).
  - The data collected and stored in the audit trail of a prospective vendor may need to be reviewed against data privacy policies and regulations (see The State of Privacy and Personal Data Protection, 2020-2022).

- **Cryptoagility**
  - Reliance on digital certificates increases the need to have a plan for long-term cryptoagility with regard to long-term retention requirements, and potential changes in the security of specific cryptographic methods and algorithms (see Better Safe Than Sorry: Preparing for Crypto-Agility). It is, therefore, important to be aware that if governments decide to change the cryptographic algorithms used for certificates in the future, this could change the status of any signed documents or digital ID technologies (and any evidence or documents stored in a digital vault).

- **Additional features and functionalities**
  - Where applicable, consider whether the product can be extended to include multilanguage support, training, integration with signature capture hardware (such as products from ePadLink or Topaz Systems), and 24/7 support.

Document Revision History

Market Guide for Electronic Signature - 22 December 2020

Market Guide for Electronic Signature - 16 January 2017

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Hype Cycle for Data Security, 2021

Market Guide for Identity Proofing and Affirmation

Innovation Insight for Decentralized Identity and Verifiable Claims

Top Trends in Government for 2022: Digital Identity Ecosystems

Table 1: Representative Vendors in Electronic Signature

Vendor	Product, Service or Solution
Adobe	Adobe Acrobat Sign
Ascertia	ADSS Signing Server
Certinal	Certinal eSign
Citrix	RightSignature
DocuSign	DocuSign
eMudhra	emSigner
Entrust	Entrust
GoSign	GoSign
HelloSign	HelloSign
InfoCert	InfoCert
Intesi Group	Valid Sign
LuxTrust	LuxTrust
MSB Docs	MSB Docs eSignature
Namirial	Namirial
Nintex	AssureSign

Notarius	Notarius
OneSpan	OneSpan Sign
PandaDoc	PandaDoc
Signicat	Signicat
SigniFlow	eSignature Workflow
SIGNiX	MyDoX
signNow	eSignature

Source: Gartner (July 2023)