ANALYST BRIEF
Sponsored by: Certinal

Modern signature solutions must be scalable, customizable, and globally compliant with identity- and trust-related regulations, and they must provide a single view into end-to-end digitally transformed signing processes across the enterprise.

Digital Signature Platform for Global Organizations

October 2022

Written by: Holly Muscolino, Group Vice President, Content Strategies and the Future of Work

Introduction

Industry analysts, including IDC analysts, have been talking about digital transformation for some time now. It should be clear that digital transformation is not a destination but a journey, one that presents opportunities for continuous improvement and increasingly better business outcomes.

IDC defines digital transformation (DX) as the act of transforming an organization into one that can scale all or part of its business and innovate at a pace that is an order of magnitude greater than that of traditional businesses. Organizations that invested in DX in 2021 saw a 27% increase in customer satisfaction, a 25% increase in operational efficiency, and a 25% increase in employee productivity, according to IDC's *Future Enterprise Resiliency and Spending Survey, Wave 4*, May 2022. Nonetheless, our research shows that one-third of organizations globally have DX initiatives that are still siloed, tactical, and disconnected from overall enterprise strategy.

AT A GLANCE

WHAT'S IMPORTANT

A ***compliant and secure*** esignature solution is critical for transforming document processes, particularly in multinational organizations.

KEY TAKEAWAYS

In the digital-first enterprise, business-critical document processes can operate anytime, anywhere. This not only ensures business continuity and provides optimal employee, customer, and partner experiences but also enables scalability, organizational agility, innovation, and competitive differentiation.

One critical but frequently overlooked component of an organization's DX strategy is the transformation of document workflows. Documents are the lifeblood of any business, and a cross-enterprise initiative to transform document-centric business processes must be part of any DX initiative. This is particularly true for mission-critical documents such as contracts, invoices, and sales agreements — the documents that are required to keep the business running. Transforming document processes becomes further complicated in highly regulated industries such as banking, insurance, logistics, and healthcare, where compliance with industry and government regulations is crucial. Another layer of complexity is added when an enterprise has a global footprint and both the source and the destination of documents may have different legal and compliance requirements.

Many indispensable document processes involve customized approval and signing workflows. A robust, scalable, compliant electronic signature (or esignature) solution, including digital signature capabilities, is a vital element of a modern and effective document technology stack to enable end-to-end, automated, and digitally transformed transaction document workflows.

Definitions

- **Electronic signature (esignature):** A legally agreed-upon replacement for uniquely identifiable physical acceptance or agreement to a form, document, or other digital source (eSignature software provides a secure and legal process for agreement/consent related to digital content, including authentication of signatories.)
- **Digital signature:** An advanced form of esignature that requires the signer to authenticate their identity using a digital certificate issued by an independent certificate authority (CA) (With digital signatures, the recipient can irrefutably confirm that a document was signed by the holder of a particular public key.)
- **Digital certificate:** A set of electronic credentials that attach the identity of the certificate owner to a pair of electronic encryption keys (one public and one private) that can be used to encrypt and sign information digitally (The main purpose of the digital certificate is to verify that a person sending a message is who they claim to be.)

Benefits and Challenges of eSignature Solutions

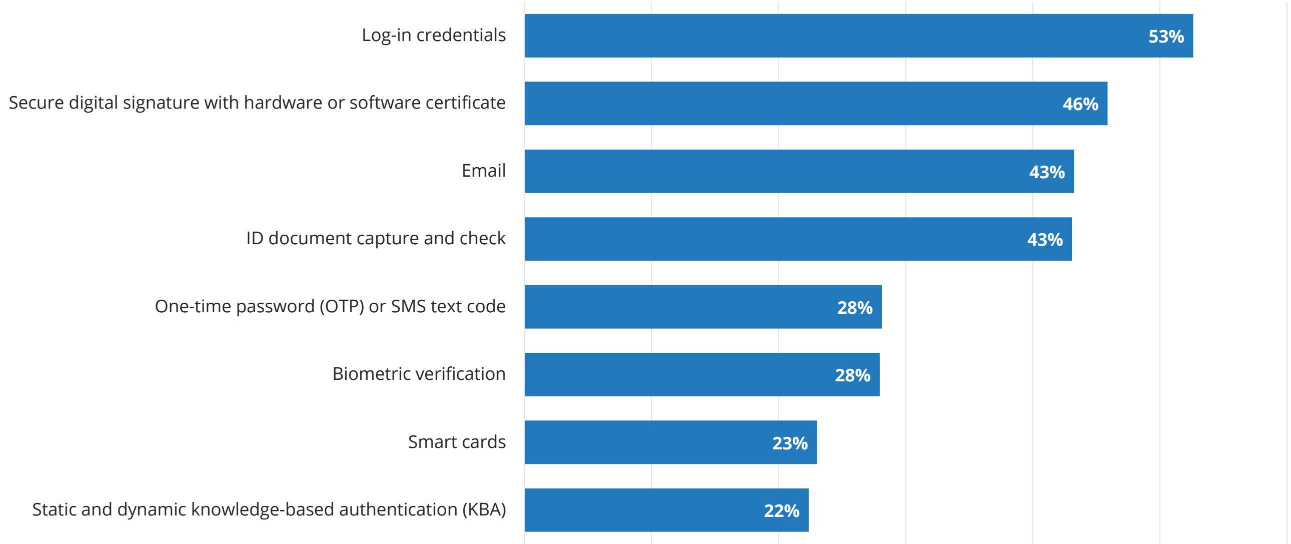
Companies that deploy esignature solutions, including digital signatures, experience multiple benefits, including greater document security, increased operational efficiency, improved customer and employee experiences, reduced transaction time, and increased productivity. All lead to better business outcomes.

But these benefits do not come without a set of challenges. First, there is an increased burden on CIOs and other senior IT managers in global or multiregional organizations who need to understand and comply with varied regulations across multiple geographies. Leadership must have a unified view of document flow across a global enterprise to effectively manage global document processes, especially those requiring signatures.

Second, those who initiate signing workflows must be certain of the validity of the signers and the authenticity of signatures, so solutions must have robust authentication capabilities. Though log-in credentials are most popular, recent IDC research shows that almost half of respondents in North America require secure digital signatures that are backed by hardware or software certificates for esignature workflows (see Figure 1).

FIGURE 1: ***Authentication Methods Required for eSignature Workflows***

Q *Which of the following authentication methods are required for the documents that originate in your organization and require signing?*



n = 608

Source: IDC's North America eSignature Market Survey, November 2021

In Europe, the qualified electronic signature (QES) is the standard for a secure electronic signature. QES is constructed with a qualified certificate for identifying the signer. This qualified electronic signature certificate consists of an electronic document that links the data of the signer and the validation of the QES signature to the unequivocal identification of the subject. The QES certificate must have been issued by a qualified certification authority or qualified trust service provider. The European Union (EU) regulation regarding electronic identification and trust services, known as electronic identification, authentication, and trust services (eIDAS), describes the different types of electronic signature that are legally acceptable in the EU.

eSignature Stakeholders: Emerging Roles

When deploying an esignature solution, don't neglect the human factor. The adoption of a transformed document-centric business process will require clear communication, training, and change management programs across all impacted stakeholders, including both IT and business resources as well as partners and customers. In addition, organizations should involve a larger team of stakeholders when selecting an esignature solution, including:

- Legal counsel to ensure compliance with laws pertaining to electronic signatures in various parts of the world
- Chief security officer to enforce better governance
- Procurement to ensure value for the price paid

Considerations When Evaluating eSignature Solutions

Regulations governing electronic signature vary by region and, in some cases, by country. Not surprisingly, almost 40% of respondents to IDC's survey told us that compliance with industry and government regulations is a top requirement for an esignature solution. Of course, this is particularly important for global organizations doing business in multiple regions.

Other questions to consider when evaluating an esignature solution are as follows:

- What types of authentication and permissions are required to initiate signing workflows? To access administrative capabilities?
- What types of dashboards and alerts are included? Can the user obtain status in real time for all signing workflows in progress across the organization?
- What is included in the signature audit trail? Who can access this information?
- Can the solution send to multiple signers, specify signing order, and specify authentication type by signer?
- Does the solution provide automated workflows, including those for routing and approval? Does it support conditional branching?
- How easy is it to integrate the esignature solution with other enterprise applications for end-to-end automation? What connectors and integrations are available out of the box?

> Organizations must involve a broad team of stakeholders when selecting a solution, including legal, security, and procurement in addition to IT.

Providers of esignature solutions, including digital signature, continue to add capabilities, particularly around automation and security. Artificial intelligence, machine learning, and advanced analytics can be leveraged for automated document generation, triggering signing workflows and decisioning within those workflows. Technologies such as blockchain are being explored to increase the security of signing workflows and support nonrepudiation. Prospective buyers should review a vendor's road map as well as existing capabilities.

Conclusion

In the digital-first enterprise, business-critical document processes can operate anytime, anywhere with minimal reliance on print infrastructure and paper, a particular physical location, or specific human resources. This not only ensures business continuity and provides optimal employee, customer, and partner experiences but also enables scalability, organizational agility, innovation, and competitive differentiation. A secure, robust esignature solution is critical for transforming document processes, particularly in multinational organizations.

During the recent health crisis, esignature solutions shifted from "nice to have" to mission-critical capabilities. To satisfy this need, organizations may have adopted short-term solutions that are not necessarily scalable or "enterprise grade." In some cases, an esignature solution may have been adopted because it was embedded in another enterprise solution. A global sourcing exercise within the esignature category may well reveal multiple vendor solutions across different business units, leading to identification of hidden costs that translate to savings.

Organizations must now review pandemic-era short-term solutions to ensure that they are scalable and customizable, can support a broad range of use cases, are globally compliant with identity- and trust-related regulations, and provide a single view into end-to-end digitally transformed signing processes across the enterprise.

Long-term, enterprise-grade solutions must also provide cost-effective pricing models, moving beyond per-wrapper pricing. Commercial viability to transform all wet signatures (external and internal) into digital will only accelerate adoption of DX initiatives and provide good value for the price paid.

> Organizations must now review pandemic-era short-term solutions to ensure that they are scalable and customizable, can support a broad range of use cases, are globally compliant with identity- and trust- related regulations, and provide a single view into end-to-end digitally transformed signing processes across the enterprise.

IDC offers the following guidance to organizations that are considering implementing esignature solutions:

- Adopt an esignature platform as part of a broader strategy for digitizing, automating, and transforming document-centric business processes. Unifying the electronic signature strategy will be most successful as part of an organization's overall digital transformation initiatives.
- Select technologies that integrate well with the organization's existing front-office and back-office business applications. eSignature solutions must "plug and play" with multiple enterprise applications and technology stacks.
- Develop metrics to measure progress including cost per signature, increased productivity, increased adoption, improved security and compliance, and improved customer and employee satisfaction.
- Seek vendors that are equipped with the necessary solutions and professional services expertise to address legal and compliance requirements related to content security, data privacy, and regulations globally.

About the Analyst

Holly Muscolino, *Group Vice President, Content Strategies and the Future of Work*

Holly Muscolino is the Group Vice President, Content Strategies and the Future of Work, responsible for research related to innovation and transformation in content solutions, including intelligent document processing, esignature, imaging and printing, and other content workflow services. Ms. Muscolino's core coverage also includes work transformation, technology and digital skills research, and the role of technology in driving the future of work.

MESSAGE FROM THE SPONSOR

Certinal is a wholly owned subsidiary of Zycus, the pioneer in Cognitive Procurement with over 21 offices globally. A familiar name and market leader with years of experience managing critical contracts and agreements, Zycus boasts over 350+ enterprise clients including Fortune 1000 enterprises and deployments of procurement and sourcing suite of products. In addition, Digital Signing has always been a focus area for Zycus. Thus, Certinal was born to offer a best-in-class Digital Transaction Management solution that will be easy to use, 100% secure to deploy, and legally compliant in 70+ countries. We stand committed to providing a one-stop solution to large enterprise customers, compliant with various security standards and conforming to regional regulations.

For more information, visit https://certinal.com/

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.