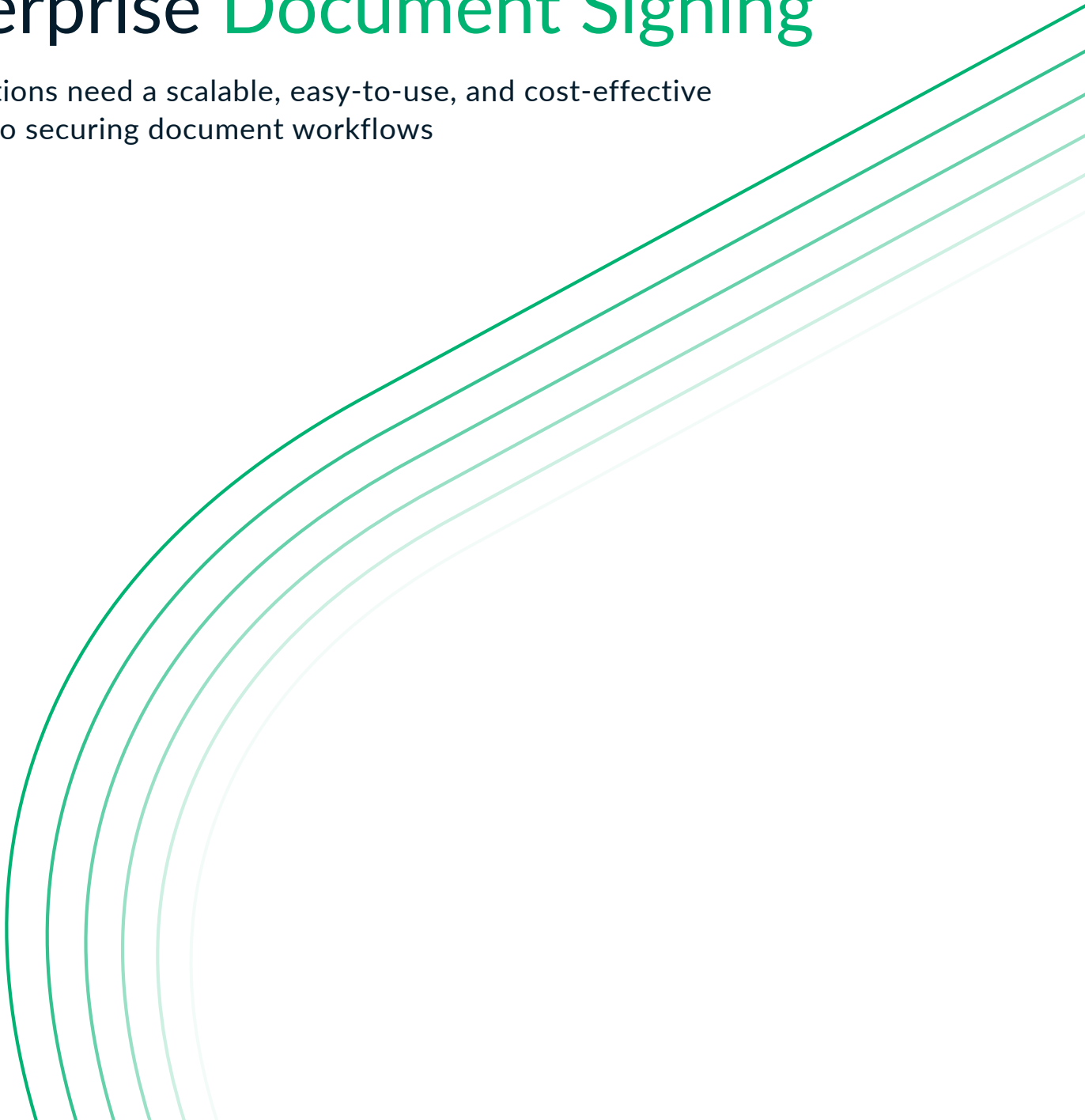


WHITE PAPER

Guide to Deploying Modern Enterprise Document Signing

Organizations need a scalable, easy-to-use, and cost-effective solution to securing document workflows

Four concentric, curved green lines that sweep from the bottom left towards the top right, creating a sense of motion and modern design.

Guide to Deploying Modern Enterprise Document Signing

In the last decade, the use of trusted digital signatures has exploded as businesses have undergone digital transformation, moving paper document procedures to online and mobile processes. This shift to digital documents has accelerated amidst the COVID-19 pandemic as people have been forced to work remotely. In tandem, increasing compliance and regulatory requirements around the world have forced organizations to adopt secure document exchange practices that go beyond simple electronic signatures and apply to document processes throughout the entire organization, not just legal agreements.

Today, the demand for secure document transactions is greater than ever. Research and Markets projects that the use of digital signatures will grow at a nearly 30% compound annual growth rate (CAGR) through 2030. This growth is being driven by the need for organizations to secure and validate the identity of signers, as well as the documents they are signing. In order to meet these needs, businesses are turning to digital signature applications such as Adobe Sign.

The use of digital signatures is growing 30% a year

However, authenticating signers and documents at scale remains a challenge for many businesses. For starters, businesses need to be able to handle an increasing number of transactions as they grow. This requires a signing solution that can be used on any device the user is using, from laptops and smartphones to tablets and beyond. And hardware tokens can be costly and impractical to manage, so a cloud-based signing solution is often the best option. Other key functionality considerations that provide more control over the signing process are knowing when documents have been digitally signed using timestamps and defining the timeframe that certificates are valid. For example, certificates need to be revoked when someone leaves the organization.

That is where Sectigo comes in. Sectigo's platform enables businesses to securely sign documents at scale with document signing certificates that maintain compliance and ensure high security. The platform is easy to use and can be tailored to meet the specific needs of your organization.





The Need for Enterprise Document Signing

Demand is growing for enterprise-grade digital document signing, as businesses look to improve efficiency and security in their document workflows. There are three primary drivers for this trend.

The first is the need for speed and efficiency in document workflows. With more business being conducted electronically, there is a demand for faster, more streamlined ways of exchanging documents. Traditional methods such as fax and paper are no longer adequate, and businesses are looking for ways to move to fully digital workflows via online and mobile solutions.

Furthermore, outdated paper methods are expensive and often lead to errors. Without an automated approval work-flow, documents can get stuck in limbo while people wait for signatures. In some cases, important documents may even be lost in the shuffle.

The second driver is the need for high security. Businesses have become more aware of the security risks associated with electronic document data, such as forged signatures or document manipulation after signing. Yet, conventional approaches to risk mitigation without document signing certificates may still expose organizations to costly fraud, including altered wire transfers or faked invoices. Digital signatures help to prevent this type of fraud, as well as many other security threats, by ensuring that the signature is genuine and the document is unaltered.

The third driver is compliance. Businesses must meet a variety of cybersecurity compliance requirements, and digital signatures are a key part of achieving compliance. By using digital signatures, businesses can ensure that their documents are authentic and tamper-proof, meeting the most rigorous compliance standards.

In this section, we will explore each of these drivers in more detail, and explain why businesses are turning to digital document signing.



Digital Transformation Drives Electronic Document Workflows

Enterprises of all sizes look to digitize their workflows in order to improve efficiency and collaboration. This shift is driven by the need to move away from paper-based processes and to take advantage of the latest technological advances. Most organizations these days rely on some form of electronic communication to exchange documents. Whether it's to send a purchase order to a supplier or to sign a contract with a customer, the ability to securely send and receive documents is critical to business operations. One area that benefits from this transformation is electronic document signing.

The use of digital signatures is growing rapidly, as evidenced by the fact that 92% of organizations currently use digital signatures (55%) or plan to do so in the next 12 months (37%) according to Sectigo product research (December, 2021). This is due, in part, to the fact that the technology has matured and is no longer limited to a handful of signers. It is now being used by all employees, from the C-suite to the front line.

92% of organizations use digital signatures or plan to do so

There are many benefits to using digital signatures in enterprise document workflows. Some of the most notable include:

- Increased efficiency and collaboration: Documents can be signed and exchanged quickly and easily, without the need for paper-based processes or faxes.
- Reduced costs: There is no need to print, sign, and scan documents, which can save time and money.
- Enhanced security: Digital signatures provide a high level of security, which is essential in today's environment.
- Regulatory Compliance: Many businesses are obliged to digitally sign documents to comply with regulations for confidentiality, validation and legal enforceability.



High Security Needs Go Beyond Electronic Signatures

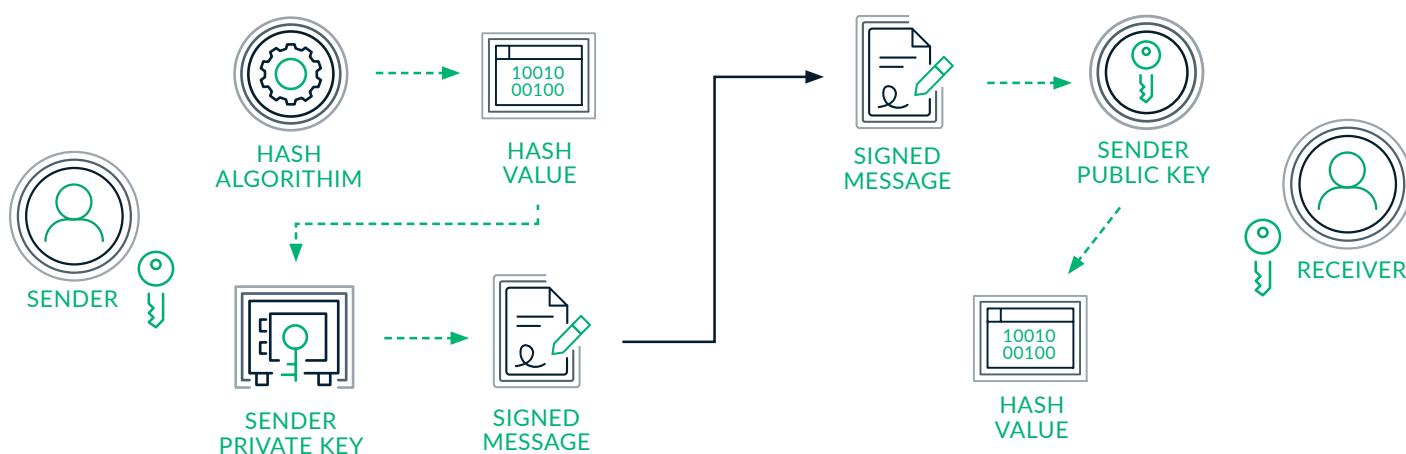
Electronic signatures, commonly referred to as e-signatures, are a broad set of solutions that use an electronic process for accepting a document or transaction with a signature. As documents and communication are increasingly paperless, businesses and consumers worldwide have embraced the speed and convenience of electronic signatures. But there are many different types of electronic signatures, each allowing users to sign documents digitally and offering some degree of identity authentication.

Simple e-signature solutions, such as DocuSign eSignature, are an extremely simple way for signers to represent an electronic version of their physical signature and are commonly used for online or mobile versions of everything from invoices and purchase orders to employment offers to simple contracts. However, while these simple e-signatures are valid in these use cases, they are just representations of a signature.

Digital signatures are the most advanced and secure type of electronic signature and take the secure document exchange a step further than simple e-signatures. Digital signatures provide a way to ensure the integrity, authentication, and non-repudiation of documents. This means that when a document is digitally signed, the recipient can be sure that it has not been altered and that the signer is who they say they are. In addition, digital signatures provide a legally binding way to sign documents, which can be especially useful in cases where there is a dispute. Thus, digital signatures are commonly used to sign enforceable documents, such as government documents, tax filing, and sales or business contracts.

A digital signature cannot be faked as a trusted certificate authority (CA) completes a validation process of the signer before issuing the document signing certificate, as opposed to a simple e-signature where any email address may suffice to be authorized. Once the signer has been validated, a digital signature is then created using public key infrastructure (PKI), the gold standard for authentication and encryption. Leveraging a public and private keypair, the digital signature's private key is used to create the signature and the public key is used to verify the signature.

How Does a Digital Signature Work?



This approach establishes a secure and trusted relationship between the sender and the recipient of a document. When a document is signed with a digital signature, a certificate is also attached to the document. The certificate contains information about the document owner, the certificate issuing authority, and the security features of the document. Furthermore, the certificate provides assurance that the document has not been tampered with and that the signature is genuine. It also enables certificate revocation in case the certificate is compromised.

This contrasts with e-signing in a few important ways. The subtle difference is that with electronic signing tools, the user is trusting the vendor to maintain security of their login credentials and the documents themselves. With a digital signature, the user is in control of the security of their document and authentication is based on the user's private key.

Further, there is a greater level of trust with a digital signature. Because the user is in control of the security of the document, the signature cannot be faked. With e-signing, the user is trusting the vendor to maintain security of their login credentials and the documents themselves. Providers like DocuSign have a robust security infrastructure, but lapses can and do occur.

When it comes to extreme disasters, e-signing tools have the risk that all of the user's login credentials and documents may be lost. On the other hand, a digital signature would still be usable if the document was backed up properly.

More broadly speaking, a centralized repository is vulnerable to a single point of failure. If the e-signing provider goes offline or hacked, for example, all of the documents that have been signed through their system are unavailable. With a digital signature, the document is just a regular file that can be stored anywhere.

Document signing is a critical security control for ensuring the integrity, authentication, and non-repudiation of information. By implementing a robust document signing solution, organizations can protect their documents against tampering and ensure that transactions are executed with certainty and enforceability.

Meeting Today's Cybersecurity Compliance Needs

Compliance and regulatory drivers are also key reasons organizations employ digital signatures. Many compliance standards require documents and signers be validated to ensure legal enforceability. Again, simple e-signatures do not meet these compliance requirements in many use cases, such as government documents, tax filing, and some contracts. This is where digital signatures come in, as they provide an unalterable and time-stamped record of a document's signer, the time of signing, and the document's content itself.

The U.S. Federal E-SIGN Act, for example, requires that electronic contracts be treated the same as traditional contracts. The Consumer Compliance Outlook lists six compliance requirements for electronic signatures, including requirements for notice, authentication, and retention.

Likewise, the eIDAS regulation of the European Union provides similar regulations for digital signatures. eIDAS, which stands for electronic IDentification, Authentication and trust Services, is intended to ensure safe and efficient electronic interactions across the European Union. eIDAS also allows for alternatives to physical presence for identity proofing in the context of issuing qualified certificates, paving the way for remote identity proofing.

Many local governing bodies impose fines for eIDAS violations. In the United Kingdom, for instance, the Information Commissioner's Office can take action if you breach the UK eIDAS Regulation for cross-border transactions with the EU, including fines of £1,000. Failure to comply with an ICO Enforcement Notice, Assessment Notice, or Information Notice can lead to fines of up to £17.5 million, or 4% of your total worldwide annual revenue - whichever is higher.

Additional compliance drivers include the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), and the Payment Card Industry Data Security Standard (PCI DSS). These regulations require businesses to take steps to protect the privacy and security of customer data. Digital signatures provide a way to meet these requirements.

Businesses that exchange documents with partners in the European Union also need to comply with the US-EU Safe Harbor. This framework ensures that personal data is transferred in a way that meets the EU's data protection requirements.

When it comes to cybersecurity and legal enforceability of documents, digital signatures are an essential tool for businesses of all sizes. By using digital signatures, businesses can protect their information while meeting compliance requirements.

Deployment Challenges of Enterprise Document Signing

We've established that digital signatures are a key part of doing business in the 21st century. They enable secure document exchange by ensuring integrity, authentication, and non-repudiation in documents. However, deploying digital signature technology at scale in an enterprise environment is not easy. There are many factors to consider, including compatibility with the many existing user devices, achieving the necessary scale, and deploying affordably.

One challenge is that scalable identity management and authentication across the entire enterprise is difficult. In order to sign a document, the signer's identity needs to be verified and authenticated. This can be a challenge in a large organization with many different signers in many different departments using different systems and devices.

This scalability challenge includes performance scalability, integration scalability, and management scalability.

Performance scalability means that the identity management system can handle the increasing number of transactions as the organization grows. Integration scalability means that the identity management system can be integrated with new applications and systems as they are added to the organization. Management scalability means that digital identity and certificate management systems ensure valid certificates easily and effectively over time as people and devices are continually onboarded and removed.

Another challenge is that signatures must work on whatever device the user is using, whether it's a desktop computer, laptop, tablet, or phone. The user should be able to sign anywhere they are, at home, while traveling, or in the field.

A survey by Owl Labs found that 92% of people expect to work from home at least 1 day per week after the pandemic. As more people work remotely, it's important that they have the ability to sign documents from anywhere. Further, with 87% of businesses relying on their employees to use personal mobile devices to access company apps, it's important that signatures work on any device.

A third challenge is that hardware tokens are costly and difficult to manage. Each token needs to be distributed, managed, supported, and, as necessary, deauthorized. Plus, renewing tokens at scale can be a huge burden on your IT team resources as it is time-consuming to swap out old tokens with new ones. In fact, conservative estimates put a cost figure for physical token deployment at around \$135 per device, with costs increasing for management and support.



92% of
employees
are partially
remote



What Enterprises Should Look for in a Document Signing Solution

As digital transformation continues to change numerous document processes throughout the entire organization and, at the same time, compliance and regulatory requirements increase, organizations must deploy secure document exchange practices that surpass simple electronic signatures. The demand for document signing certificates that secure and validate the identity of signers, as well as the documents being signed, is greater than ever. Yet to overcome the inherent challenges that come with deployment of document signing, organizations need a scalable, easy-to-use, and cost-effective solution. Sectigo Document Signing Certificates offer secure document exchange that satisfies compliance requirements for the entire organization and does so in a single, cloud-based platform that automates the end-to-end lifecycle of the signing certificates as well as all types of digital certificates.

When looking for a document signing solution, enterprises should consider the following:

- **Signee Management**
- **Compliant Certificate Management**
- **Cloud-based Signing Services**

Let's take a closer look at each of these features.

Signee Management

Businesses need to securely sign documents with partners, customers, and employees every day. The challenge is finding a document signing solution that offers the features and functionality needed to make the process as smooth and efficient as possible. One of the most important features to look for is signee management.

Signee management is the ability to authenticate and manage all user identities who will be signing documents. This includes not just the legal department, but also other departments and employees who may need to sign documents from time to time. A good signee management platform should allow businesses to validate signers and easily install document signing certificates on their devices. Further, the platform should also offer easy revocation of certificates when someone leaves the company, for example. This added layer of management gives businesses more control over who can sign documents and when.

Signee management is important because it ensures that only authorized users can sign documents. This helps to protect the integrity of the document and the business's reputation. It also helps to ensure that documents are not signed by unauthorized individuals, which could lead to legal and financial complications.

Compliant Certificate Management

Compliant certificate management is the process of issuing, managing, and verifying digital certificates that meet the compliance requirements of a specific jurisdiction or industry. Compliant certificates are used to ensure the security and validity of digital signatures, and are essential for businesses that need to meet the compliance requirements of the likes of eIDAS trust networks.

Adobe and eIDAS are two of the most well-known trust networks in the world. Adobe is a global authority on digital signatures, and the eIDAS regulations are the gold standard for digital signature regulations in Europe. Enterprises that need to sign documents in a way that is compliant with both Adobe and eIDAS trust networks need a certificate authority that can issue certificates and offer timestamp functionality which meet the stringent requirements of both networks.

Sectigo is the world's largest SSL provider and a leading certificate authority. Sectigo's team of compliance experts who can help enterprises issue certificates that meet the compliance requirements of Adobe and eIDAS trust networks. Sectigo's solutions are fully integrated with Adobe Acrobat and other leading eSignature solutions, and come with 24/7 customer support.

Cloud-based Signing Services

Increasingly, organizations have moved critical business systems to the cloud for greater productivity and increased financial flexibility. Likewise, cloud-based document signing solutions offer a number of advantages over traditional on-premise signing solutions.

Perhaps the most compelling reason to consider a cloud-based signing solution is that it enables employees to sign documents from anywhere. With employees working from home or on the go, it's important that your document signing solution can be accessed from anywhere. A cloud-based document signing solution can do just that, making it easy for employees to sign documents no matter where they are.

Another advantage of a cloud-based document signing solution is that it eliminates the costly requirements to store and manage private keys on-premise. With the additional security controls necessary to properly and securely store private keys, it's reassuring to know that your private keys are securely stored in the cloud within Hardware Security Modules (HSMs) meeting the stringent security requirements of industry regulations. And with centralized key management, it's easy to keep track of who has access to which signing keys.

A cloud-based signing solution also offers flexibility and scalability. As your business grows, you can easily add more users to your signing solution. Additionally, your organization can simply budget as an operational expense, rather than as a major capital cost project associated with building and maintaining on-premise data centers.

Sectigo Document Signing Platform

The Sectigo Document Signing Platform enables secure document exchange by ensuring integrity, authentication, and non-repudiation in documents. The platform is entirely cloud-based, so there is no need for any software installation, and keys are stored in the cloud for easy management and document signing from anywhere in the world. And as a part of Sectigo Certificate Manager (SCM), organizations gain comprehensive certificate lifecycle management of all their digital identities in a single platform that automatically provisions, monitors, and renews digital certificates.



Sectigo Document Signing Certificates provide trusted assurance of authenticity for electronically transmitted documents by confirming the identity of the signer and ensuring the integrity of the document.

Sectigo Document Signing Certificates enable users to digitally sign Adobe® and Microsoft Office® documents. They certificates can be used on any platform that trusts the Sectigo root certificate. Further, visual trust indicators verify the signer's identity and assure recipients of the document's authenticity. Customers can also authenticate documents signed by multiple parties.

When a document is digitally signed, Sectigo Document Signing Certificates are used to create a digital signature. The signature is a unique string of characters that is appended to the document and is used to verify the identity of the signer and the integrity of the document. The signature can only be created using the private key that is associated with the Sectigo Document Signing Certificate.

When a document is received, the signature is verified using the public key that is associated with the Sectigo Document Signing Certificate. This public key is embedded in the certificate and is used to validate the signature. The validation process confirms that the signature was created by the signer and that the document has not been modified since it was signed.

This entire process costs significantly less per user than for hardware-based solutions. Ultimately, this means that Sectigo Document Signing Certificates provide an easy and cost-effective way to ensure the integrity and authenticity of documents.

Conclusion

As digital transformation continues to change numerous document processes throughout the entire organization and, at the same time, compliance and regulatory requirements increase, organizations must deploy secure document exchange practices that surpass simple electronic signatures. The demand for document signing certificates that secure and validate the identity of signers, as well as the documents being signed, is greater than ever. Yet to overcome the inherent challenges that come with deployment of document signing, organizations need a scalable, easy-to-use, and cost-effective solution. Sectigo Document Signing Certificates offer secure document exchange that satisfies compliance requirements for the entire organization and does so in a single, cloud-based platform that automates the end-to-end lifecycle of the signing certificates as well as all types of digital certificates.



About Sectigo

Sectigo is the leading provider of digital certificates and automated Certificate Lifecycle Management (CLM) solutions trusted by the world's largest brands. Its cloud-based universal CLM platform issues and manages the lifecycles of digital certificates issued by Sectigo and other Certificate Authorities (CAs) to secure every human and machine identity across the enterprise. With over 20 years of experience establishing digital trust, Sectigo is one of the longest-standing and largest CAs with more than 700,000 customers, including 36% of the Fortune 1000. For more information, visit www.sectigo.com.