DocuSign

DocuSign Security Brief

Introduction

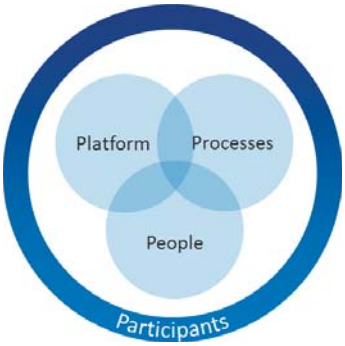
Security is an essential part of any software-based solution, but few business processes are as security sensitive as those involving electronic signatures.

When transactions contain highly sensitive information, like personally identifiable information, pricing details, proprietary business terms, intellectual property, and more, you can't afford to take risks. That's why DocuSign emphasizes security and always-on availability in everything that we do. Protecting customers is DocuSign's number one priority, and our comprehensive approach addresses the security, privacy, compliance, and validity of your DocuSign transactions.

It's a big reason why DocuSign is the most widely used eSignature solution in the world, serving over 85 million users across 188 countries. DocuSign consistently meets or exceeds the stringent security requirements of even the most security conscious organizations, including Fortune 500 companies, the world's largest financial institutions, and other global companies.

In the following pages, we provide an overview of our security approach, which encompasses a number of key areas: our security assurance program, certifications, and tests.

DocuSign Security Assurance Program



Our dedication to deliver the highest level of security possible for our customers is centered on our security assurance program, which aligns our people, processes, and platform to address the overall security, privacy, and validity of your eSignature transactions.

People

Security at DocuSign is everyone's job. We invest in training and awareness to ensure that security stays top of mind for all of our employees.

- ✓ A cross-functional team of experts with deep banking experience that's 100-percent dedicated to security-related activities
- ✓ A security council that oversees risk management strategy and implementation across the organization
- ✓ Background checks for all prospective employees and suppliers
- ✓ A dedicated chief information security officer (CISO) who manages security operations and continuously engages with the security community to ensure DocuSign stays ahead of emerging trends in the dynamic threat landscape
- ✓ Annual security training for all employees
- ✓ Training for engineers to ensure coding is done securely, with regular security audits of the code base

DocuSign

DocuSign Security Brief

Processes

DocuSign's business processes, including internal policies, software development, and platform monitoring, take into consideration the security of our customer data.

- ✓ On-premise security policies, such as badge access, manned public entrances, and physical access controls
- ✓ Access limited to a minimal number of personnel based on the least-privilege principle, with multiple layers of secured authentication required for all critical systems
- ✓ Active monitoring and alerting
- ✓ Security reviews within the DocuSign SDLC, including the planning, design, implementation testing, shipping, and response phases
- ✓ Formal code reviews and vulnerability mitigation by third parties for applications and access security
- ✓ Testing and validation of DocuSign's key management and encryption program by external auditors and documented in our SSAE 16 report

Platform

DocuSign's secure platform encompasses hardware and infrastructure, systems and operations, applications and access, and transmission and storage.

- ✓ Commercial-grade datacenters with diversity across vendors, so that critical customer documents remain available in the event of any business disruption
- ✓ Carrier-grade architecture featuring simultaneously active and redundant systems that allow the overall system to survive full-site outages and be "always on"
- ✓ Secure, near real-time data replication
- ✓ Physically and logically separated networks for systems and operations
- ✓ Malware protection
- ✓ Commercial-grade firewalls and border routers to resist/detect IP-based and denial-of-service attacks
- ✓ Multiple authentication options for signers
- ✓ Anti-tampering controls
- ✓ Digital certificate technology
- ✓ Two-factor encrypted VPN access

A Holistic Approach

DocuSign doesn't just look at security in a vacuum. We consider all areas that keep your sensitive transactions protected, including privacy and compliance with laws and regulations globally. Customer content stays confidential—not even DocuSign employees have access to customer secret data. Moreover, DocuSign's features ensure the enforceability and non-repudiation of our customers' documents.

- ✓ AES 256-bit encryption at the application level for customer documents to ensure confidentiality
- ✓ Access and transfer of data to/from DocuSign via HTTPS
- ✓ Use of Security Assertion Markup Language (SAML), giving users the latest capabilities for Web-based authentication and authorization, including single sign-on
- ✓ Ability for signers to authenticate when they sign, including multifactor and two-factor authentication
- ✓ A digital checksum (mathematical hash value) that validates documents haven't been tampered with outside of each signing event
- ✓ Certificates of completion after all parties have participated in the signing process
- ✓ Signature verification and unalterable capture of signing parties' names, emails, public IP addresses, signing events, timestamps, signing location (if provided), and completion status
- ✓ A digital audit trail for every envelope that captures the name, email address, authentication method, public IP address, envelope action, and timestamp

DocuSign Security Brief

Security Certifications and Tests

DocuSign makes significant investments in enterprise security and operations, and we undergo rigorous scrutiny by third-party auditors to assess and validate the security measures we have in place.

- ✓ Consistently meets or exceeds national and international security standards
- ✓ Continual leadership in defining industry best practices for third-party audits, certifications, and onsite customer reviews
- ✓ Compliance with applicable laws, regulations, and industry standards around the world, governing digital transactions and electronic signatures
- ✓ Dedicated chief legal officer and chief technology officer that ensure DocuSign and our products align with the latest legal and technology trends
- ✓ Ability to comply with specialized industry regulations, such as HIPAA, 21 CFR Part 11, and specified rules from the FTC, FHA, IRS, and FINRA

ISO 27001:2013

ISO 27001:2013 is an information security management system (ISMS) standard published by the International Organization for Standardization (ISO).

It's the highest level of global information security assurance available today and provides customers assurance that DocuSign meets stringent international standards on security.

DocuSign is ISO 27001:2013 certified as an ISMS—a systematic approach to managing confidential or sensitive corporate information, so that it remains secure.

View DocuSign's ISO 27001:2013 certification, and visit the ISO website for more information about the standard.

SSAE 16, SOC 1 Type 2, SOC 2 Type 2

Issued by the American Institute of Certified Public Accountants (AICPA), SSAE 16 reports on the design and operating effectiveness of internal controls at service organizations.

DocuSign is SSAE 16 examined and tested yearly across all aspects of our enterprise business, including our datacenters, and has sustained and surpassed all requirements. SOC 2 specifically indicates that DocuSign's technology meets the criteria for security, availability, and confidentiality, and is:

- **Protected** against unauthorized physical and logical access
- **Available** for operation and use as information systems, designated as confidential and protected

Further details regarding SSAE 16 may be found on the AICPA website.

xDTM Standard, Version 1.0

The first standard of its kind to focus on Digital Transaction Management (DTM), the xDTM Standard was developed to raise the bar on quality and promote more trust and confidence in conducting business transactions online. The Standard ensures that digital transactions are protected yet accessible—regardless of where parties reside or the devices used.

DocuSign is certified compliant with the xDTM Standard, version 1.0. For more information, visit www.xdtm.org.

PCI DSS 3.1

Overseen by the Payment Card Industry Security Standards Council (PCI SSC), PCI DSS 3.1 is a data security standard for organizations handling credit card holder information. As both a service provider and a merchant, DocuSign places stringent controls around cardholder data and is PCI DSS 3.1 compliant.

Additional information on PCI DSS 3.1 may be found at www.pcisecuritystandards.org.

CloudTrust

With Skyhigh's CloudTrust program, DocuSign fully satisfies the most stringent requirements for data protection, identity verification, and security controls, based on detailed criteria developed in conjunction with the Cloud Security Alliance.

Learn more about the program on the Skyhigh Networks website.

Conclusion

We're committed to fiercely protecting the data our customers entrust to us. It's why we weave security into every aspect of our organization through the security assurance program, focusing on people, processes, and technology. This is evidenced by our investment in meeting or exceeding national and international security standards, including certification for ISO 27001:2013.

Our customers demand and expect thorough protection of their most sensitive transactions, and that's the stance we take in delivering exceptional document and data security. Security is top of mind for them, and it's our priority as the leader in eSignature solutions.

Additional Resources

The security we offer our customers extends beyond what's outlined in this document. A number of additional resources are available that further demonstrate DocuSign's industry-leading security strategy.

Follow the links below for more details on how we approach and deliver security.

Trust Center: trust.docusign.com

DocuSign Partner Ecosystem Integrations

Policies
- Terms of Use
- Privacy Policy
- Use of Cookies

About DocuSign

DocuSign is changing how business gets done. DocuSign empowers anyone to transact anytime, anywhere, on any device with trust and confidence. Organizations of every size, industry, and geography accelerate contracts, approvals, and workflows with DocuSign's DTM platform and eSignature solution. DocuSign keeps life and business moving forward.

For U.S. inquiries:
toll free +1 866 219 4318 | docusign.com

For EMEA inquiries:
phone +44 203 714 4800 | emea@docusign.com | docusign.co.uk

For APAC inquiries:
phone +1 800 255 982 | docusign.com/au

For LATAM inquiries:
phone +55 11 3330 1000 | docyousign.com/br

For more information
To learn more about how DocuSign can help you streamline multi-document agreements, contact your account executive or email sales@docusign.com.