WHITE PAPER

DocuSign Security Brochure

Introduction

Security is an essential part of any software-based solution. Few business processes are as securitysensitive as those involving electronic signatures. eSignature transactions routinely contain information that is critical to you, your business, and your customers. This information may include personally identi!able information (PII), pricing details, proprietary business terms, intellectual property, and more.

This is precisely why DocuSign's number one priority is customer security. We lead the industry in defining and delivering the most secure eSignature solution available. DocuSign consistently meets or exceeds the stringent security requirements of even the most security conscious organizations including Fortune 500 companies, the world's largest !nancial institutions, and other global companies.

Executive Summary

In the following pages, we provide an overview of our security approach, which encompasses a number of key areas, including our Security Certi!cations & Tests, as well as our Security Assurance Program.

Security Certifications and Tests

DocuSign's commitment to security begins with our extensive Security Certifications & Tests.

- DocuSign is the only eSignature company that is **ISO 27001 certified** as an information security management system.
- As an **SSAE 16** examined and tested organization, DocuSign complies with the reporting requirements stipulated by the AICPA.
- Our **PCI DSS 2.0** compliance certi!es safe and secure handling of credit card holder information.
- DocuSign's **TRUSTe** certi!cation demonstrates our commitment to protecting customer data.
- DocuSign complies with policies for collection, use and retention of personal data as specified by the **U.S. Department of Commerce Safe Harbor.**

Security Assurance Program

Our dedication to providing the industry's most secure eSignature solution is further demonstrated by the DocuSign Security Assurance Program.
The foundation of DocuSign's Security Assurance Program is built upon our people, processes, platform and participants.

- Our **people**, including a dedicated Chief Security Officer (CSO), prioritize and drive security assurance within DocuSign.
- From internal policies to product development, all business **processes** at DocuSign consider the security of our solution.
- DocuSign's **platform**, extending from the physical infrastructure to the nodes of data transmission, is subject to security scrutiny by internal and external experts.
- To ensure the level of security our customers expect and deserve, external **participants** are considered in all DocuSign security measures.

DocuSign's Security Assurance Program allows us to deliver world-class security to our customers, including confidentiality, integrity, availability, authenticity and non-repudiation.

- DocuSign protects **confidentiality** of customer data at the application level with AES 256 bit encryption.
- DocuSign's unique anti-tampering controls ensure the **integrity** of customers' documents.
- With 99.99% average uptime, **availability** of our customers' data is unmatched by competing solutions.
- DocuSign's robust mechanisms for validating participants in a signing transaction ensure the **authenticity** of all signing parties.
- We offer a number of features designed for **non-repudiation**, including a digital audit trail for every envelope sent with DocuSign.

Security Certifications & Tests

DocuSign meets the highest security standards and offers the industry's most extensive set of certifications & tests, including the following.

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

The standard is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give con!dence to interested parties.

DocuSign is the only eSignature solution that is ISO 27001 certi!ed as an ISMS – a systematic approach to

managing confidential or sensitive corporate information so that it remains secure. This is the highest level of global information security assurance available today.

Follow the link to view our ISO 27001 certification.

The ISO website (www.iso.org) contains more information about the ISO 27001 standard.

SSAE 16 is a statement on standards for attestation engagements put forth by the American Institute of Certi!ed Public Accountants (AICPA) for reporting on design as well as the operating effectiveness of internal controls at service organizations.

DocuSign is SSAE 16 examined and tested yearly across all aspects of our enterprise business and production operations including our datacenters, and has sustained and surpassed all requirements.

A copy of this report is available upon request, subject to non-disclosure agreement.

Further details regarding SSAE 16 may be found on the AICPA website (www.aicpa.org).

PCI DSS 2.0 is a data security standard for organizations handling credit cardholder information that is overseen by the Payment Card Industry Security Standards Council (PCI SSC).

As both a service provider and a merchant, DocuSign places stringent controls around cardholder data and is PCI DSS 2.0 compliant.

Additional information on PCI DSS 2.0 may be found at the PCI SSC website (www.pcisecuritystandards.org).

TRUSTe is a leading global privacy management solutions provider that puts forth a certi!ed privacy protection seal.

DocuSign is TRUSTe certi!ed, and adheres to the terms outlined in our privacy policy to securely and safely handle customer data.

Click on the link to view our TRUSTe certification.

More details on TRUSTe may be found at their website (www.pcisecuritystandards.org).

The U.S. Department of Commerce has developed "safe harbor" frameworks to enhance privacy protection and enable organizations to comply with European and Swiss data protection laws.

DocuSign complies with the U.S. Department of Commerce Safe Harbor policies regarding the collection, use and retention of personal data.

Follow the link to view our U.S. Department of Commerce Safe Harbor compliance.

For information, please visit the U.S. Department of Commerce website (www.commerce.gov).

Security Assurance Program

Our ability to deliver the highest level of security for our customers is centered on our Security Assurance Program.

People

Everyone at DocuSign, from the facilities staff to the executive team, is committed to security excellence.

- A cross-functional team of experts, including a dedicated Chief Security Officer (CSO), is 100% dedicated to security-related activities.
- DocuSign is the only eSignature company with a dedicated CSO since 2010.
- The CSO manages DocuSign's Governance, Risk, and Compliance (GRC) program, the DocuSign Security Council, and a number of security and compliance related meetings detailed in our SSAE 16 report.
- Our dedicated Chief Legal Of!cer (CLO) and Chief Technology Of!cer (CTO) provide customers confidence that DocuSign and its products stay ahead of legal and technology trends.

Processes

DocuSign's business processes, including internal policies, the Software Development Lifecycle (SDLC), and platform monitoring, consider the security of our customer data.

- Taking a top down approach, the Security Council oversees and implements internal security policies such as key encryption access, incident response and data retention.
- Security reviews are part of DocuSign's Software Development Lifecycle (SDLC); which includes the planning, design, implementation, testing, ship, and response phases of the product. We train our engineers to ensure they are coding in a secure manner and conduct regular security audits of the code base.
- DocuSign conducts third-party as well as internal penetration testing. We also have a program for business continuity (BCP) and disaster recovery (DR) testing.
- All prospective employees are subject to background checks, and all employees must pass annual security certification exams.
- DocuSign's commitment to security extends to on-premise policies such as badge access, manned public entrances, and physical access controls.
- For server administration, DocuSign limits access to a minimal number of personnel based on the principle of least privilege and requires multiple layers of secured authentication.

Platform

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

- DocuSign's hardware & infrastructure, including three geo-diverse, SSAE 16 audited datacenters, 365x24x7 on-site security, two-factor authentication for datacenter access, third-party penetration testing, near real-time secure data replication and annual BCP/DR testing, provides customers world- class security and availability.
- The systems & operations that keep our infrastructure secure offer physically and logically separate networks, two-factor encrypted VPN access, near real-time secure data replication, commercial-grade !rewalls and border routers to resist/detect IP-based and Denial of Service (DoS) attacks, and active monitoring and alerting.
- DocuSign's applications & access security is characterized by formal code reviews and vulnerability mitigation by third parties, Advanced Encryption Standard (AES) 256 bit encryption, Key Management & Encryption Program, enterprise-class malware protection, digital audit trail and multiple authentication mechanisms.
- To ensure secure transmission & storage, DocuSign provides a secure, private SSL 256 bit viewing session, anti-tampering controls, signature verification, unalterable capture of signing data, digital certi!cate technology, and customer configurable data retention program.

Participants

External parties are considered players in the security process and are part of DocuSign's security scope.

- DocuSign offers a high level of security assurance to the signers, senders, partners and developers that interact with our system while taking steps to protect ourselves from any threats they might present.
- DocuSign can be securely integrated with external systems through HTTPS SOAP and REST web service API's. We require users to undergo certi!cation before a partner can make an API call in our production accounts, and we enforce the use of an integrator key as well as valid credentials to send API requests.
- DocuSign's dedicated CSO continually engages with the security community, including other security decision makers, government officials and software leadership to stay ahead of emerging trends in the dynamic threat landscape.

This foundation enables our Security Assurance Program to deliver substantial value to our customers, including confidentiality, integrity, availability, authenticity and non-repudiation.

Confidentiality

Our customers' content stays con!dential, including from DocuSign - employees never have access to customer content stored on the DocuSign system.

- DocuSign ensures confidentiality by providing AES 256 bit encryption at the application level for customer documents.
- Our Key Management & Encryption Program is tested and validated by external auditors and documented in our SSAE 16 report.

- Customers specify who can view and sign their encrypted documents over a secure, private SSL 256 bit viewing session.
- DocuSign's robust offering allows signers to authenticate when they sign, including multifactor and two-factor authentication.
- Using SAML (Security Assertion Markup Language), DocuSign offers users the latest features for webbased authentication and authorization including single sign-on (SSO).
- We continually de!ne industry best practices in third-party audits, certi!cations and, and on-site customer reviews.

Integrity

Each document is ensured to be intact and tamper-evident.

- We offer the only eSignature solution that provides strong anti-tampering controls.
  » A visual dashboard monitoring system that alerts across 24 API events.
  » PKI digital certi!cate technology to seal documents.

  » A digital checksum (mathematical hash value) that validates the documents in an envelope have not been tampered with outside of each signing event.

Availability

We are the only eSignature company that performs near real-real time, secure data replication to an ISO 20000 certi!ed, geo-diverse, warm site.

- DocuSign offers three geo-diverse, highly-available datacenters including a disaster recovery facility, which maintains the total data footprint (per stated RPO) and 100% capacity in the event of any single full site failure.
- Our commercial-grade datacenters have diversity across vendors so that in the event of any business disruption critical customer documents remain available.
- DocuSign is dedicated to providing transparent communications to our customers. We send product release notes and communicate maintenance times in advance of changes, and notify customers of performance issues and security alerts immediately upon discovery.
- We regularly post white papers, blog entries, tech/product-notes and other security related documentation to our website.
- Customers can check DocuSign's dedicated Trust Center (trust.docusign.com) to !nd security information and system performance.

Authenticity

Our customers can rely on authenticity of signers – as evidenced by the audit trail and chain of custody offered by our solution.

- DocuSign provides a robust set of mechanisms and options to validate the authenticity of the participants in a signing transaction:
  » Signature veri!cation, unalterable capture of signing parties' names, emails, public IP addresses, signing events (i.e. viewed, signed, etc.), timestamps, signing location (if provided), and completion status.

  » A diverse range of authentication options can be layered based on the need to validate the authenticity of signers, including multifactor and two-factor choices.

Non-Repudiation

Customers' documents are ensured technically, legally, and procedurally unassailable.

- DocuSign is the only eSignature service that provides a variety of unique features for non-repudiation:
  » A digital audit trail for every envelope that captures the name, email address, authentication method, public IP address, envelope action, and timestamp.
  » Application and system logging that provide a digital record of the entities accessing the envelopes.
  » Certifications of completion after all parties have participated in the signing process.

Conclusion

DocuSign's security approach is comprehensive. We meet or exceed national and international security standards and lead the eSignature industry in delivering exceptional document and data security. Our Security Assurance Program further demonstrates our commitment to world-class information security.

We consider our customers' security priority number one. Our security approach encompasses everything from our people and processes to our platform and participants – senders, signers, partners and developers. Our robust strategy allows us to ensure the confidentiality, integrity, authenticity, and nonrepudiation of our customers' documents, and enables us to deliver 99.99% average uptime and availability of our system.

Our security processes are documented and we are audited on interactions of all these components – this all-inclusive approach is why we are the only ISO 27001 certified eSignature company.

Additional Resources

The security we offer our customers extends beyond what has been outlined above. A number of additional resources are available that further demonstrate DocuSign's industry leading security strategy. Follow the links below for more details on our security offerings.

- **Trust Center**

» Trust.Docusign.com

White Papers

» No Hiding in the Cloud

» Best Practices for Electronic Document Management and Security

» Security by Design

» Managing Risk and Building Security in the Cloud

- **Policies**

» Terms of Use

» Privacy Policy

» Use of Cookies