DocuSign®

The Global Standard for
Digital Transaction Management™

Security at DocuSign

Kathy Ahuja, *Senior Director of Compliance, DocuSign*

February 8, 2017

DocuSign is the fastest most secure way to make every agreement and approval digital, so you can keep life and business moving forward.

DocuSign®

Security Is a Top Concern

FORRESTER®

2015 Forrester Digital Transaction Management (DTM) survey reveals:

81% of respondents state "Security" as **top concern** when considering adopting and growing a DTM solution*

The DocuSign Difference

Why Customers Choose DocuSign

Choice

Works with applications, services, and devices you already use.

Experience

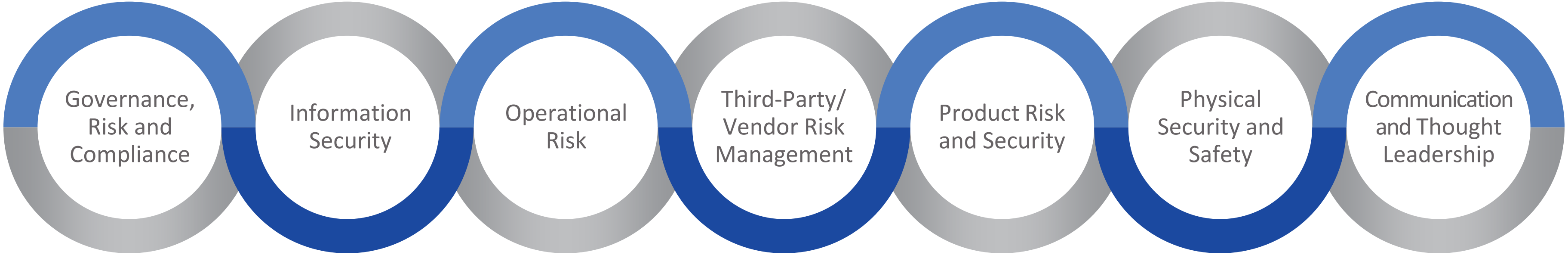
Simple to use, implement, and manage, driving immediate user adoption.

Trust

The most reliable and globally trusted service for digital transactions.

World Class Security

Delivering World-Class Risk Mitigation and Security


Governance, Risk and Compliance
Information Security
Operational Risk
Third-Party/ Vendor Risk Management
Product Risk and Security
Physical Security and Safety
Communication and Thought Leadership

DocuSign: Highest and Broadest Set of Security Certifications

IS 580155

- Global Security Gold Standard: ISO 27001:2013
- Defines an (ISMS) Information Security Management System
- Requires Business Continuity

- Security Framework
- Testing of Controls
- Effectiveness Measured
- Reliability of Service

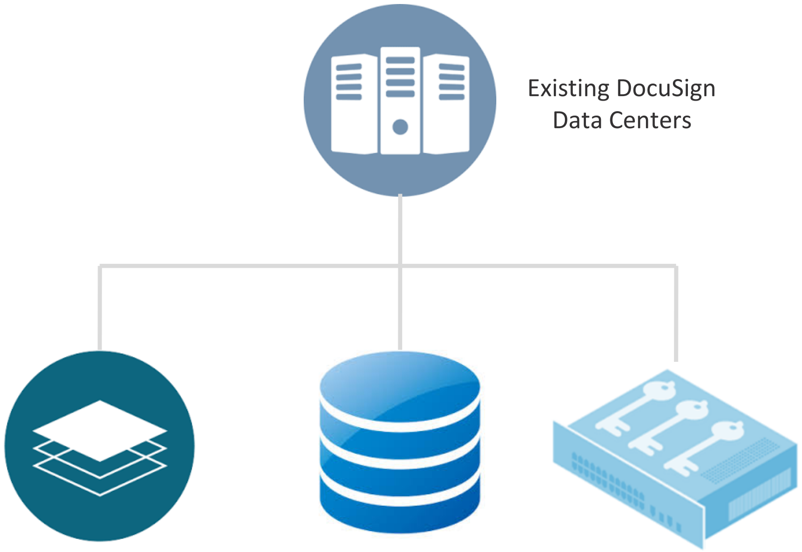
- Protection of Data
- General Computing Controls Focus
- Comprehensive Scope (Level-3 Merchant, Level-1 Service Provider)

- Data Privacy
- Collection of Data
- Use of Data
- Data Requirements

- Data Protection, Identity Verification, Service Security, Business Practices, and Legal Protection for Cloud Services
- Based on Criteria Developed with Cloud Security Alliance (CSA)

Coming Soon: FedRamp

Path to Authorization



Existing DocuSign Data Centers

Multi-Tenant Platform

Dedicated Storage Appliance

Dedicated Security Appliance

In Process

DocuSign Sponsored by Federal Communications Commission (FCC) for FedRAMP Authorization – 10/17/2016

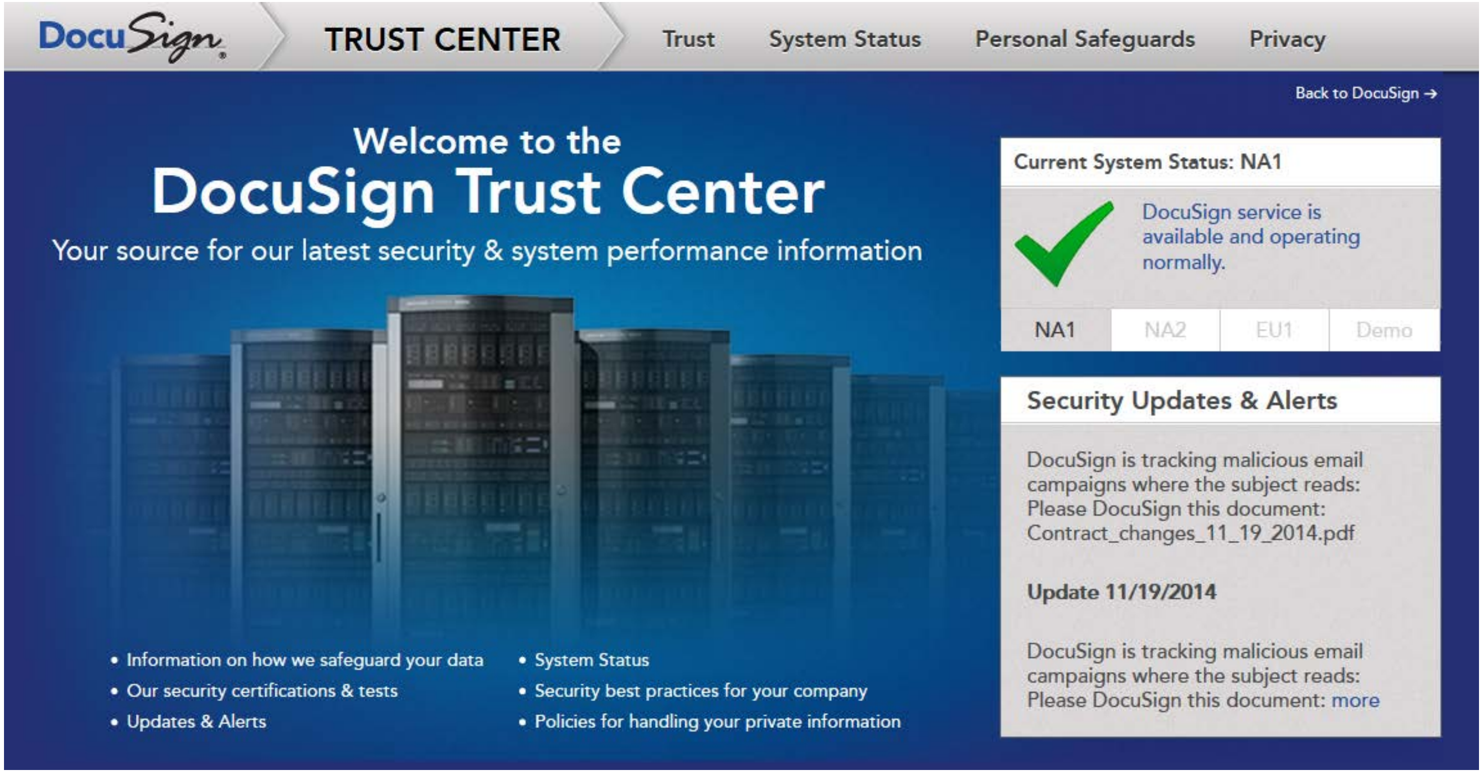
3PAO Audit

DocuSign's System Security Plan (SSP) and Develop Security Assessment Report (SAR) – 11/14/2016

Authorization

Authority to Operate (ATO) Issued by FCC Anticipated Early 2017

DocuSign Trust Center: Keeping Customers Informed



Welcome to the

DocuSign Trust Center

Your source for our latest security & system performance information

- Information on how we safeguard your data
- Our security certifications & tests
- Updates & Alerts
- System Status
- Security best practices for your company
- Policies for handling your private information

Current System Status: NA1

✓ DocuSign service is available and operating normally.

Security Updates & Alerts

DocuSign is tracking malicious email campaigns where the subject reads: Please DocuSign this document: Contract_changes_11_19_2014.pdf

Update 11/19/2014

DocuSign is tracking malicious email campaigns where the subject reads: Please DocuSign this document: more

Raising the Quality Bar Together

xDTM

STANDARD

The Transaction Management Standard for an Open Digital World

Security *Privacy* *Compliance* *Enforceability* *Availability* *Scalability* *Universality* *Interoperability*

xDTM Standard Governing Board

Stanford Hospital & Clinics CIO	NIST Former Director	FedEx President FedEx Office, CIO	hp CISO	Lucile Packard Children's Hospital Stanford Chief Medical Information Officer	NBCUniversal CISO
Buckley Sandler LLP Partner	Purdue University VP IT & System CIO	intel Vice President	DocuSign CRO	Mandiant Founder	Security Innovation Network Chairman
VISA Senior Vice President	Commonwealth of Kentucky Auditor	Microsoft CISO	Lookout CTO/Founder	United States Postal Service CIO	Brown-Forman CISO

DocuSign

A Dedicated Team Focused on Risk and Security

A team of 30+ people and growing that includes bank security specialists

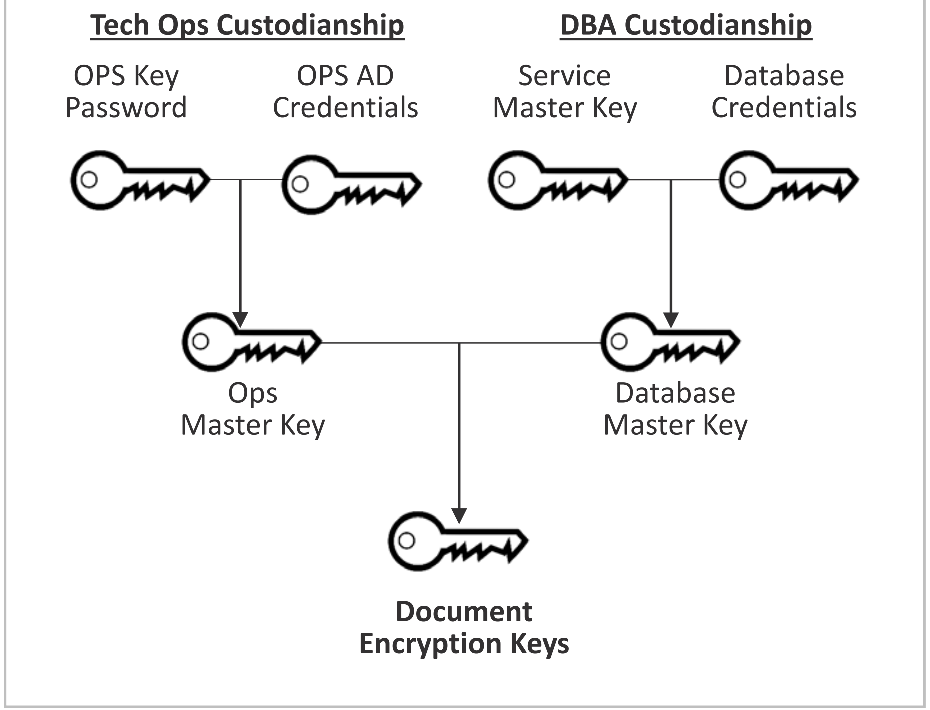
Over 100 years of combined security experience

Headed by DocuSign Legal, with accountability to the CEO and Board of Directors

A charter to oversee and manage risk, audit, information security, and physical security, and participate in the xDTM organization

Only Customers Can Access Customer Data

Multi-Layered Protection of Encryption Keys



☑ **All customer data is encrypted at all times**

☑ DocuSign enforces **strict segregation and rotation of key custodianship duties** to ensure security is never compromised

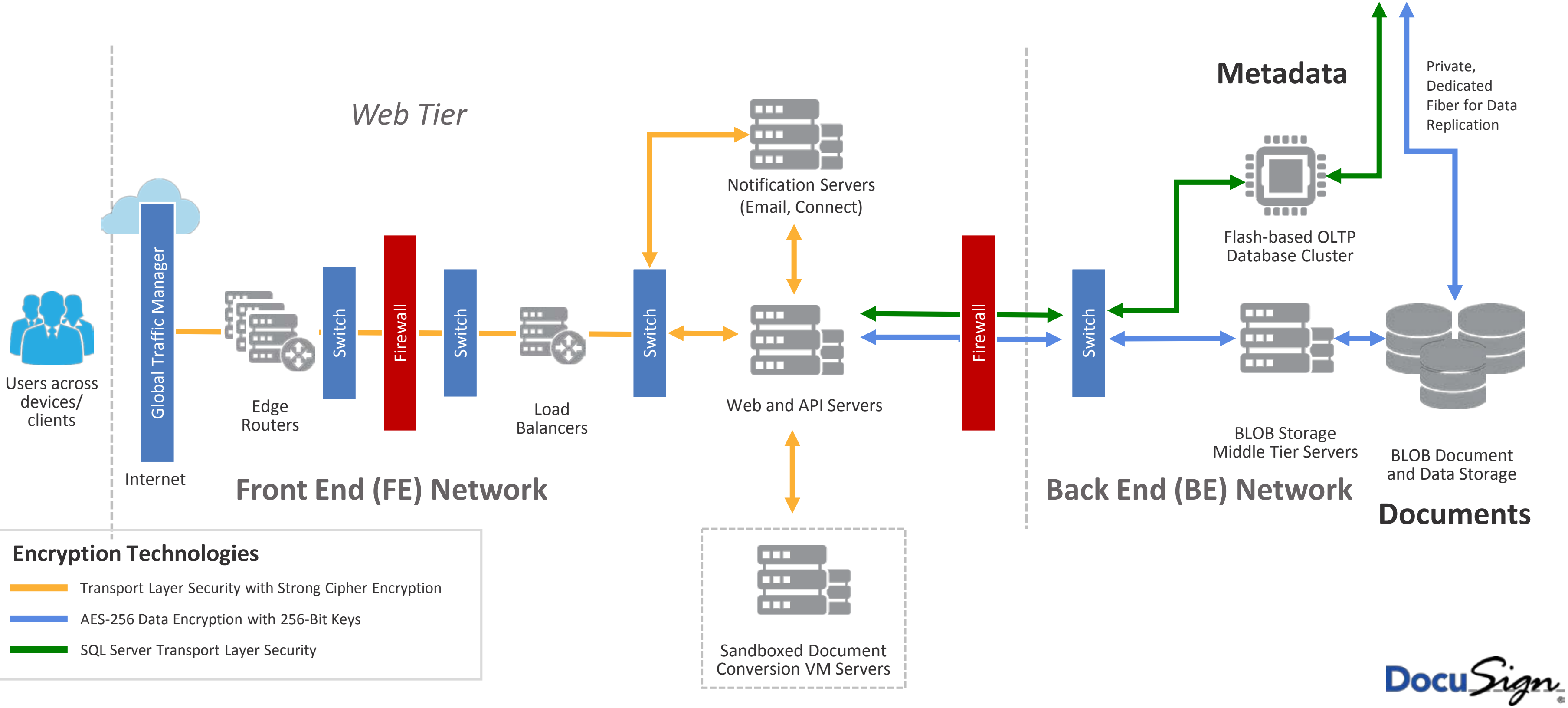
- 4 sets of independently held keys are needed to decrypt the document
- Keys are rotated regularly

☑ **Customer data can only be retrieved by the customer**; even the most privileged DocuSign employee cannot access customer data

DocuSign

DocuSign Network Architecture

- Customer data is **encrypted at all times** using state-of-the-art encryption technology



Web Tier

Metadata

Private, Dedicated Fiber for Data Replication

Users across devices/ clients

Global Traffic Manager

Internet

Edge Routers

Switch

Firewall

Switch

Load Balancers

Switch

Notification Servers (Email, Connect)

Web and API Servers

Sandboxed Document Conversion VM Servers

Firewall

Switch

Flash-based OLTP Database Cluster

BLOB Storage Middle Tier Servers

BLOB Document and Data Storage

Front End (FE) Network

Back End (BE) Network

Documents

Encryption Technologies

🟧	Transport Layer Security with Strong Cipher Encryption
🟦	AES-256 Data Encryption with 256-Bit Keys
🟩	SQL Server Transport Layer Security

Unparalleled Availability

DocuSign

Unparalleled Availability and Resilient Performance

Never worry about system availability or disaster recovery again

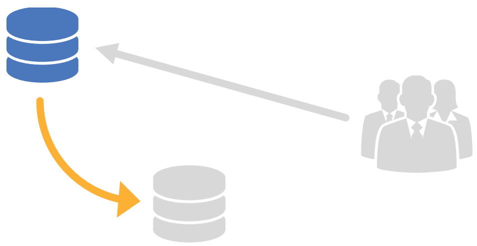
- Carrier grade architecture
- Real-time replicating, active DocuSign sites
- Massively redundant distributed data (9 copies across 3 sites in North American or the EU)
- Fusion IO-powered, flash memory-based OLTP subsystem
- Global load balancing and traffic management with session-based site failover
- Choice of data residency within North America or the EU

✓ Zero maintenance downtime
✓ Zero data loss in a disaster for maximum peace-of-mind
✓ Consistently high performance, even at peak load

Pictured: Active-Active-Active Architecture

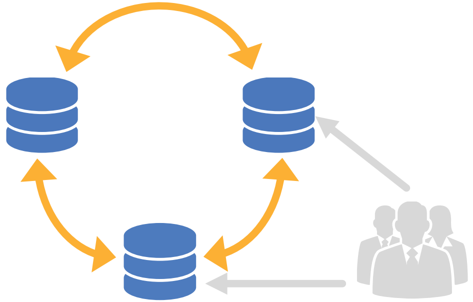
DocuSign’s Carrier Grade Architecture Is Unprecedented in SaaS

Industry Average



Annual Maintenance	**Days?**
Maximum Data Loss	**24 Hours?**
Recovery Time	**Days??**
Data Copies	**2**

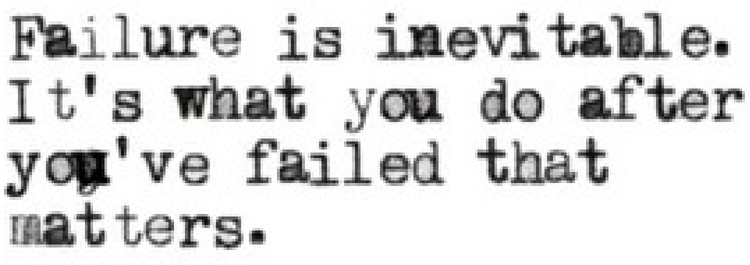
DocuSign Carrier Grade Architecture



Annual Maintenance	**0 Hours**
Maximum Data Loss	**0 Hours**
Recovery Time	**0.5 Hours**
Data Copies	**9**

DocuSign

We Build a Robust Product by Stress Testing Every Failure Scenario



Failure is inevitable. It's what you do after you've failed that matters.

DocuSign Testing Principles

Make everything fail

- Disk, server, network, dependent infrastructure

Add a lot of stress

- >5000 hours storage stress
- >1,000,000 failure injection cases executed

Get Creative in Failure Scenarios

- Hundreds of executed scenarios

DocuSign®