Adobe Document Cloud

Adobe

WHITEPAPER

Überblick über die Sicherheit von Adobe Acrobat Sign.

Oktober 2023

Inhalt.

Sicherheit bei Adobe.

Adobe nimmt die Sicherheit eurer digitalen Inhalte ernst. Bei Adobe sind Sicherheitsmaßnahmen ein fester Bestandteil der Software-Entwicklung, Prozesse und Programme. Sie werden von interdisziplinären Teams konsequent umgesetzt, um etwaigen Zwischenfällen vorzubeugen, diese aufzudecken und angemessen darauf zu reagieren. Darüber hinaus halten wir uns durch Kooperation mit Partnerunternehmen, Forschenden, Sicherheitsinstitutionen und anderen Organisationen über aktuelle Bedrohungen und Schwachstellen auf dem neuesten Stand und integrieren fortlaufend hochentwickelte Sicherheitstechnologien in unsere Produkte und Services.

In diesem Dokument erfahrt ihr, wie Adobe für sichere Adobe Acrobat Sign-Workflows sorgt und eure Daten zuverlässig schützt.

Hinweis: Dieses Dokument beschreibt Funktionen von Acrobat Sign Solutions für Unternehmen und Acrobat Sign Solutions für KMU. Wenn ihr Fragen zur Verfügbarkeit einer bestimmten Funktion von Acrobat Sign habt, wendet euch bitte an euren Adobe-Kontakt.

Über Acrobat Sign.

Mithilfe von Acrobat Sign können Unternehmen herkömmliche Unterschriftsprozesse vollständig digitalisieren – über sämtliche Workflow-Anforderungen hinweg, von einfachen Unterschriften (E-Signaturen) bis hin zu qualifizierten, Cloud-basierten Signaturen. Mit Acrobat Sign lassen sich Dokumente per Browser, Smartphone oder Tablet versenden, unterschreiben, nachverfolgen und Unterschriftsprozesse verwalten. Die Lösung umfasst schlüsselfertige Integrationen und APIs zur Einbindung von Workflows für elektronische Unterschriften in Enterprise-Services, Datensysteme und gängige Cloud-basierte Produktivitäts-Tools wie Microsoft 365.

Acrobat Sign erfüllt zahlreiche gesetzliche Auflagen und Branchenstandards. Dazu gehört auch die Unterstützung von zertifikatbasierten, digitalen Signaturen für Unterschriftsprozesse mit höheren Sicherheitsanforderungen. Die zuverlässige, Cloud-basierte Lösung unterstützt umfangreiche Online-Prozesse für elektronische Unterschriften und bietet unter anderem folgende Funktionen:

- Identitäts-Management, Authentifizierung und Zugriffskontrolle
- Bestätigung der Integrität von Dokumenten
- Überprüfung von elektronischen Unterschriften
- Protokollierung von Einverständniserklärungen oder Eingangsbestätigungen
- Verwaltung von Prüfprotokollen
- Einbindung von elektronischen Unterschriften in wichtige Business-Programme und Enterprise-Systeme

Im Rahmen von verifizierten Standardintegrationen des Cloud Signature Consortium unterstützt Acrobat Sign zudem Cloud-basierte Fernsignaturen mit digitalen Zertifikaten von Vertrauensdiensten. Details zur Rechtsgültigkeit von elektronischen Unterschriften und internationale Vorschriften für elektronische Unterschriften findet ihr im Adobe Trust Center.

Lösungsarchitektur von Acrobat Sign.

Die Architektur von Acrobat Sign ist darauf ausgerichtet, Transaktionen in großem Umfang zu skalieren und zu verarbeiten, ohne dass die Leistung beeinträchtigt wird. Um ein hohes Maß an Verfügbarkeit und Skalierbarkeit zu gewährleisten, werden sämtliche Transaktionsdaten aus Acrobat Sign in mehreren verteilten, redundanten Datenbank-Clustern mit automatischem Failover- und Recovery-System gespeichert.

Mit einem umfassenden Programm für Betriebskontinuität und Disaster Recovery (Business Continuity & Disaster Recovery-Programm, BCDR) gewährleistet Adobe die Bereitstellung und Verfügbarkeit von Acrobat Sign. Das nach ISO 22301 zertifizierte Programm ermöglicht eine bessere Reaktion auf unvorhergesehene Störungen und stellt die minimale Beeinträchtigung durch Ausfälle sowie eine umgehende Wiederherstellung des Betriebs sicher. Weitere Informationen sind im Acrobat Sign BCDR Fact Sheet verfügbar (NDA erforderlich).

Jede logische Ebene der Acrobat Sign-Lösung wird durch mehrere Werkzeuge überwacht, mit denen wiederum Schlüsselindikatoren verfolgt werden, darunter die durchschnittliche Dauer der PDF-Umwandlung oder die Ressourcennutzung.

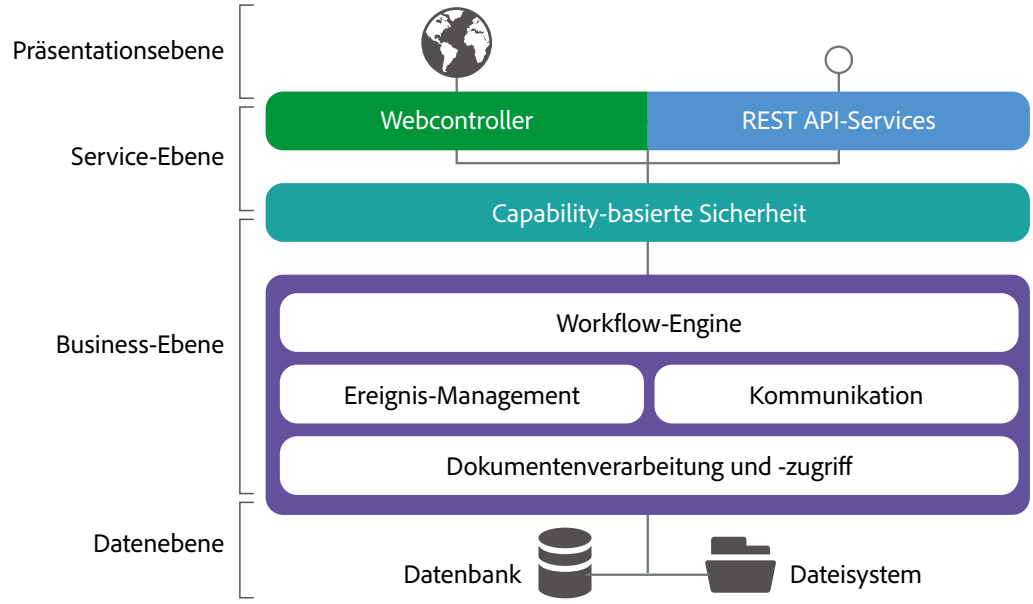

Abb. 1: Lösungsarchitektur von Acrobat Sign

Mit dem Überwachungs-Dashboard kann das technische Betriebs-Team den Zustand des Dienstes im Auge behalten. Wird einer der definierten Schwellenwerte für die Schlüsselindikatoren überschritten, werden die Team-Mitglieder in Echtzeit benachrichtigt. Falls sich ein Problem nicht verhindern lässt, speichert Acrobat Sign umfangreiche Diagnoseprotokolle und forensische Analysen, damit die Ursache schnell behoben und ein Wiederauftreten des Problems vermieden werden kann.

Die folgenden Abschnitte beschreiben die Funktionen der einzelnen Ebenen innerhalb der Lösungsarchitektur von Acrobat Sign.

Präsentationsebene.

Die Präsentationsebene beinhaltet die Web-basierte Benutzeroberfläche (UI) sowie die Funktionen zum Erstellen und Rendern von Dokumenten, die zur Unterzeichnung und Durchführung anderer Workflows versendet werden, z. B. finale PDF-Dokumente mit einem fälschungssicheren Siegel.

Service-Ebene.

Die Service-Ebene umfasst die erforderlichen Kontrollen für die Client- und REST-API-Services. Die Webserver für externe Systeme verarbeiten Browser- und API-Anfragen, während die Mailserver ein- und ausgehenden E-Mail-Verkehr verwalten.

Mithilfe von Lastverteilern verteilen die Webserver komplexe dynamische Anfragen an die Programm-Server von Acrobat Sign auf der Business-Ebene. Die Webserver wenden zudem Filterregeln an, um Angriffe aus dem Web zu verhindern, sowie Firewall-Schutz, um die Zugriffskontrolle zu erhöhen.

Business-Ebene.

Die Business-Ebene von Acrobat Sign erfüllt folgende Funktionen:

- **Workflow-Engine** – Mit der Workflow-Engine werden alle Geschäftsprozesse und Schritte ausgeführt und verwaltet, die für den Unterschriftsprozess notwendig sind. Die Workflow-Engine verwendet eine deklarative XML-basierte Definitionssprache, um die Bedingungen zur Ausführung unternehmensspezifischer Workflows und die Abfolge von Ereignissen zu beschreiben, die erforderlich sind, um einen Unterschrifts- oder Genehmigungsprozess abzuschließen.

- **Capability-basierte Sicherheit** – Mit dieser Sicherheitsmethode wird kontrolliert, welche Ressourcen verfügbar sind und welche Vorgänge im Zusammenhang mit diesen Ressourcen durch authentifizierte Anwenderinnen und Anwender bzw. Programme ausgeführt werden dürfen. Ressourcen umfassen sämtliche Informationen in Form von Dokumenten, Daten, Metadaten, Anwenderdaten, Berichten und APIs.

- **Dokumentenverarbeitung und -zugriff** – Die Dokumenten-Engine bietet zustandslose Funktionen zur Umwandlung verschiedener Dateiformate in PDF, Verschlüsselung und Entschlüsselung von Dateien und Rasterung von Bildern für die Anzeige in einem Webbrowser. Für sämtliche Prozesse zur Dokumentenverarbeitung greift Acrobat Sign auf ein asynchrones, Warteschlangen-basiertes Nachrichtensystem zurück, das über alle Systemressourcen hinweg kommuniziert. Die gesamte Dokumentenverarbeitung und der Zugriff auf den Cloud-Speicherplatz erfolgen im Hintergrund. Das heißt, alle Änderungen innerhalb von Acrobat Sign werden in jedem Schritt des Anwender-Workflows sofort ersichtlich.

- **Ereignis-Management** – Mit den Funktionen für Ereignis-Management wird in jedem Schritt des Workflows ein Prüfprotokoll erstellt und gespeichert, das relevante Informationen zu jedem Dokument und jeder anwendenden Person enthält. In jeder Phase des Workflows erzeugt Acrobat Sign ein Ereignis und sendet über ein asynchrones Nachrichtensystem eine Meldung an die entsprechenden Systemressourcen.

- **Kommunikation** – Acrobat Sign sendet Anwenderbenachrichtigungen über Ereignisse im Zusammenhang mit Unterschriften sowie optional über die Bereitstellung der unterzeichneten und zertifizierten Dokumente am Ende des Unterschriftsprozesses. Um Spamming und Phishing zu vermeiden, ermöglicht Acrobat Sign die Authentifizierung auf Basis von Systemen wie Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC) und Sender Policy Framework (SPF).

Datenebene.

Die Datenebene ist für den Zugriff auf die Transaktionsdatenbank und den Dokumentenspeicher zuständig. Transaktionsdaten, die in der Datenzugriffsebene gespeichert werden, umfassen das ursprüngliche Kundendokument, Zwischenversionen des Dokuments, die während des Unterschriftsprozesses generiert wurden, Metadaten, Anwenderdaten, Ereignisse und das finale unterzeichnete PDF-Dokument, das von Acrobat Sign verarbeitet wurde.

Integration über REST-API-Services.

Acrobat Sign umfasst schlüsselfertige Integrationen für viele Business-Programme, Enterprise-Systeme und Vertrauensdienste. Darüber hinaus bietet Acrobat Sign umfassende REST-APIs für die Anbindung an proprietäre Business-Systeme oder Firmen-Websites über sichere Webservices. Adobe führt eine Liste der Business-Programme und Enterprise-Systeme, die von Acrobat Sign unterstützt werden.

Allgemeiner Datenfluss.

Im Folgenden wird die Interaktion mit Acrobat Sign im Rahmen eines Unterschriftsprozesses beschrieben. Die Schrittfolge entspricht Abbildung 2.

1. **Repository erstellen:** Vor dem ersten Einsatz von Acrobat Sign können auf Anwenderseite eigene, wiederverwendbare Workflow-Definitionen, Bibliotheksvorlagen und Web-Formulare erstellt und im Acrobat Sign-Repository gespeichert werden. Jede Person mit Zugriffsrechten für diese Elemente kann eine Bibliotheksvorlage versenden, einen Workflow initiieren oder ein Web-Formular veröffentlichen, um Unterschriftsprozesse in die Wege zu leiten.

2. **Workflow zusammenstellen:** Um einen Workflow zum Versenden einer Vereinbarung mit Acrobat Sign zu initiieren, werden die Teilnehmenden, die Reihenfolge, in der sie am Prozess teilnehmen, sowie verschiedene Optionen zur genaueren Definition ihrer Teilnahme festgelegt. Der Workflow kann auch über eine schlüsselfertige Integration von Adobe oder über ein kundenspezifisches Programm erfolgen, das mit dem Acrobat Sign-API erstellt wurde. Vereinbarungen können basierend auf einer hochgeladenen Liste mit E-Mail-Adressen an mehrere Personen gleichzeitig verschickt werden.

   Als Nächstes werden die Quelldokumente hochgeladen, die zur Vereinbarung gehören. Acrobat Sign unterstützt den Import von Dokumenten aus dem Cloud-Speicher eines Drittanbieters, aus einem angebundenen Kunden- oder Partnerprogramm, aus einer vorhandenen Bibliotheksvorlage oder vom Anwender-Desktop.

3. **Vereinbarung erstellen:** Ein Dokument, das in Acrobat Sign hochgeladen wurde, wird automatisch als Vereinbarung betrachtet. Wenn es sich um ein Formular mit vordefinierten Feldern auf Basis einer Bibliotheksvorlage handelt, fügt Acrobat Sign diese Felder automatisch in die Vereinbarung ein. Wenn keine Bibliotheksvorlage verwendet wurde, müssen die gewünschten Felder manuell zur Vereinbarung hinzugefügt werden, damit die unterzeichnende Person weiß, an welchen Stellen unterschrieben werden muss.

   Acrobat Sign bietet die Möglichkeit, Unterschriftsfelder an logischen Positionen in der Vereinbarung zu platzieren und Formularfelder zur Angabe von Informationen wie E-Mail-Adresse, Vorname, Name und Titel hinzuzufügen. Dieser Prozess wird als Authoring bezeichnet.

   Jede Vereinbarung muss mindestens ein Unterschriftsfeld enthalten. Das Unterschriftsfeld kann beim Authoring oder automatisch von Acrobat Sign platziert werden. Bei der automatischen Variante wird das Unterschriftsfeld am Ende der Vereinbarung hinzugefügt (wenn genügend Platz vorhanden ist). Alternativ wird die Vereinbarung durch eine zusätzliche Seite zum Unterschreiben ergänzt. Diese Informationen können später exportiert und in nachgelagerten Prozessen verwendet werden.

4. **Link weitergeben:** Sobald das Authoring abgeschlossen ist, wird die Vereinbarung allen Teilnehmenden per E-Mail, Web-Formular oder mithilfe des Acrobat Sign-API in einem benutzerdefinierten Programm bereitgestellt.

5. **Unterschriften einholen:** Je nachdem, welche Parameter die Vereinbarung umfasst, werden Unterzeichnende dazu aufgefordert, ihre Genehmigung zu übermitteln, eine Unterschrift zu leisten und/oder Formularfelder auszufüllen. Die Formularfelder können von der verfassenden Person als optionale Felder oder Pflichtfelder festgelegt und auf verschiedene Weise maskiert oder formatiert werden. Alle Informationen werden zusammen mit dem aktuellen Status der Vereinbarung (Wer hat unterschrieben? Wer muss als Nächstes unterschreiben?) im Acrobat Sign-Datenspeicher in der Cloud gespeichert. In dieser Phase können auch Anhänge erfasst werden.

6. **Unterzeichnete Vereinbarung vorlegen:** Nachdem alle Unterzeichnenden den Workflow zur Unterzeichnung abgeschlossen haben, wird die vollständig ausgefüllte und unterzeichnete Vereinbarung für alle am Unterschriftsprozess Teilnehmenden bereitgestellt und automatisch im Cloud-Speicher von Acrobat Sign gespeichert. Alle Dokumente im Zusammenhang mit dem Unterschriftsprozess können mit den Acrobat Sign-Clients heruntergeladen werden, darunter die unterzeichnete Vereinbarung (zertifizierte PDF-Datei), ein Prüfprotokoll (zertifizierte PDF-Datei) und einen separaten Bericht mit Datenwerten aus Formularfeldern (als CSV-Datei exportierbar). Optional kann die Vereinbarung über Acrobat Sign-APIs oder den Archivierungs-Service eines Partnerunternehmens in ein gewünschtes System verschoben oder kopiert werden.

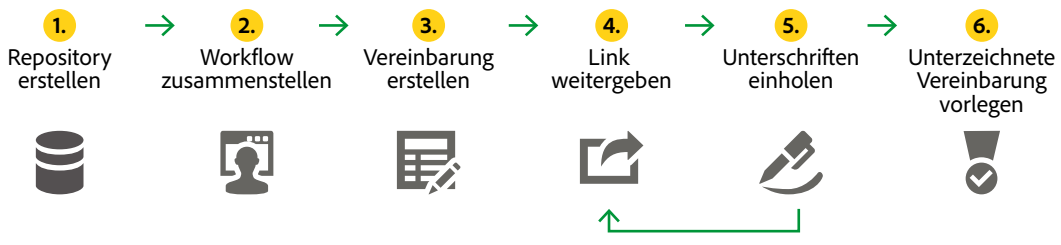

Abb. 2: Datenfluss mit Acrobat Sign

Sicherheitsarchitektur von Acrobat Sign.

Das folgende Diagramm veranschaulicht die Sicherheitsarchitektur von Acrobat Sign, einschließlich Servern für externe Anfragen, Cloud-Servern und Client-Zugriff.

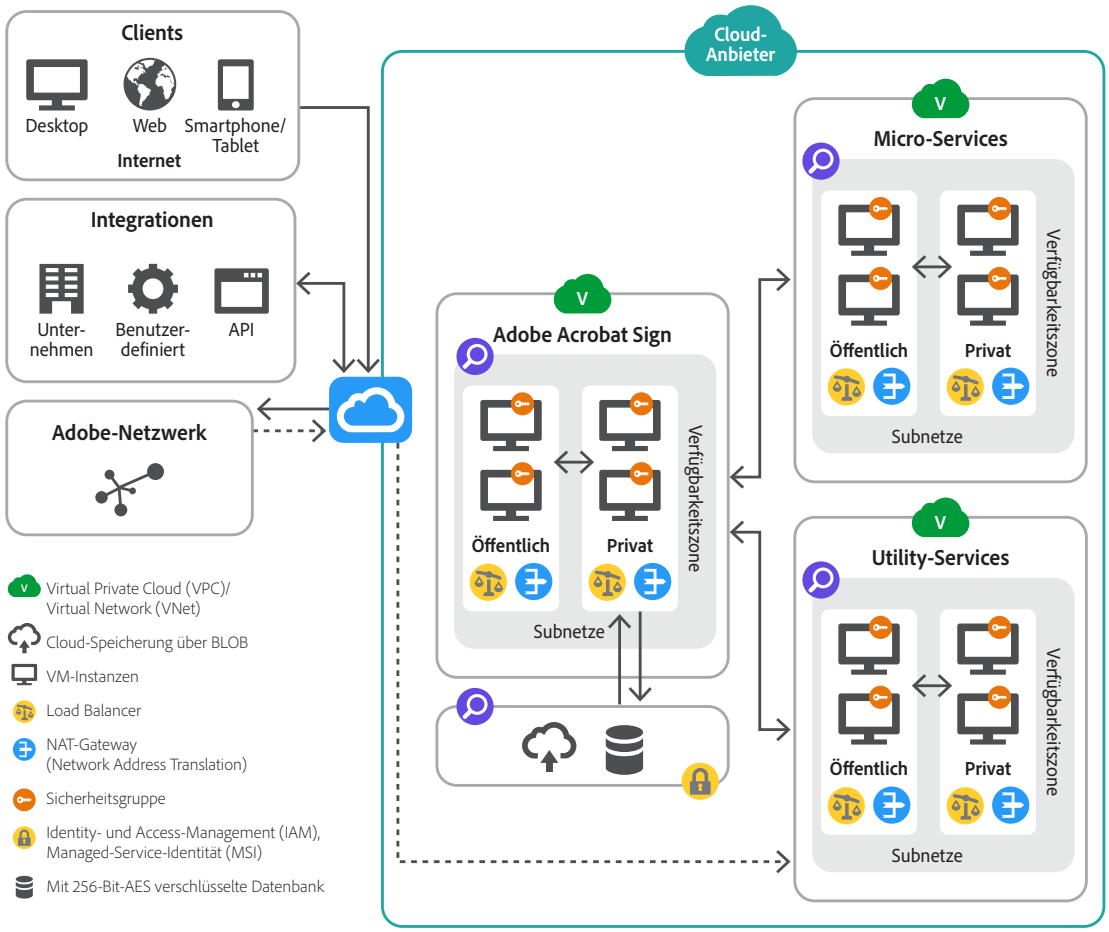

Abb. 3: Sicherheitsarchitektur von Acrobat Sign

Extern erreichbare Server.

Extern erreichbare Server innerhalb der gehosteten Netzwerkarchitektur von Acrobat Sign sind Webserver, die Browser- und API-Anfragen verarbeiten, und Mailserver für den eingehenden und ausgehenden E-Mail-Verkehr. Die Webserver und zugewiesenen Lastverteiler verteilen dynamische Anfragen an die Programm-Server. Die Webserver werden durch Firewalls geschützt, um die Zugriffskontrolle zu erhöhen.

Virtuelle Cloud-Netzwerke.

Die Sicherheitsarchitektur von Acrobat Sign umfasst zudem mehrere virtuelle Cloud-Netzwerke. Bei AWS werden diese Netzwerke als „Virtual Private Cloud" (VPC) bezeichnet, bei Microsoft Azure als „Virtual Network" (VNet).

VPCs/VNets sind logisch isolierte Netzwerke, die von außen nur über stark beschränkte Eingangs- und Ausgangspunkte zugänglich sind. Innerhalb eines VPC/VNet gibt es Subnetze mit einer Reihe von IP-Adressen. Subnetze können entweder privat oder öffentlich sein. Ein öffentliches Subnetz ist mit dem Internet verbunden, ein privates Subnetz nicht. Acrobat Sign verwendet VPCs/VNets wie folgt:

- ein VPC/VNet als Kernelement für zentrale Business-Prozesse mit Acrobat Sign
- ein VPC/VNet für Micro-Services wie die Integration mit dem Cloud Signature Consortium, die Validierung von Signaturen oder das Entfernen von Signaturbildern im Hintergrund
- ein VPCs/VNet für Utility-Services, um die Überwachung von Ereignissen und andere administrative Funktionen zu verwalten

Alle diese Services werden auf skalierbaren, sicheren, virtuellen Cloud-Servern ausgeführt, auf die nur über das gesicherte Subnetz und die Netzwerkbeschränkungen für VPC/VNET zugegriffen werden kann.

Um eine hohe Verfügbarkeit sicherzustellen, werden VPC-/VNet-Instanzen in mehrere redundante Verfügbarkeitszonen unterteilt. Verfügbarkeitszonen werden physisch voneinander isoliert, damit Strom-, Netzwerk- oder sonstige Ausfälle der Infrastruktur in einer Verfügbarkeitszone den Betrieb in anderen Verfügbarkeitszonen nicht beeinträchtigen. Alle Daten werden über alle Verfügbarkeitszonen hinweg repliziert, und innerhalb jeder Verfügbarkeitszone auf mehreren Servern.

Der Netzwerkzugriff innerhalb einer VPC-/VNet-Instanz wird über eine Sicherheitsgruppe geschützt. Wie virtuelle Firewalls ermöglichen Sicherheitsgruppen die genauere Kontrolle des eingehenden und ausgehenden Datenverkehrs von einer VPC-/VNet-Instanz. Auf diese Weise wird sichergestellt, dass nur berechtigte Anwenderinnen und Anwender autorisierte Aktionen ausführen. Die Acrobat Sign-Architektur integriert zusätzlich Sensoren zur Erkennung von Angriffen an kritischen Stellen, um Service-übergreifende Systemintegrität und -sichtbarkeit zu garantieren.

Client-Zugriff.

Der Acrobat Sign-Service ist über verschiedene Client-Endpunkte zugänglich, z. B. Browser, unser REST-API und Mobile Apps. Verbindet sich ein Client mit Acrobat Sign in der jeweiligen Region, erfolgt die Verbindung per Internet-Gateway mit einem bestimmten VPC/VNet. Sämtliche Client-Verbindungen erfolgen über HTTPS mit TLS v1.2 oder höher sowie mindestens 128-Bit-AES-Verschlüsselung.

Datenverschlüsselung.

Acrobat Sign verwendet PCI DSS-geprüfte Verschlüsselungsalgorithmen, um Dateien im Ruhezustand mit 256-Bit-AES zu verschlüsseln. Um die sichere Datenübertragung über HTTPS zu gewährleisten, unterstützt Acrobat Sign das TLS-Protokoll Version 1.2.

Der Zugriff auf Dokumente im Ruhezustand ist nur mit Capability-basierten Berechtigungen über die Datenzugriffsebene in einem privaten Subnetz möglich. Absendende haben zudem die Option, ein Dokument mit einem privaten Kennwort zusätzlich zu schützen.

Verschlüsselungsschlüssel werden in einer sicheren Secrets-Management-Umgebung mit eingeschränktem Zugriff inkl. Multi-Faktor-Authentifizierung gespeichert und verwaltet.

Der E-Mail-Versand aus Acrobat Sign erfolgt normalerweise per SMTPS mit TLS-Verschlüsselung. Dabei kommen Cipher Suites mit einer Schlüssellänge von mindestens 128 Bit zum Einsatz. Da einige wenige E-Mail-Provider TLS-Verschlüsselung nicht unterstützen, werden E-Mails bei Bedarf per unverschlüsseltes SMTP versendet.

Identitäts-Management.

Acrobat Sign setzt rollenbasiertes Identitäts-Management ein, um die Authentifizierung, Autorisierung und Zugriffskontrolle innerhalb des gesamten Acrobat Sign-Systems zu steuern. Die Capability-basierten Sicherheits- und Authentifizierungsprozesse für ein Unternehmen werden von Acrobat Sign-Admins definiert und aktiviert. Acrobat Sign unterstützt die Definition folgender Anwenderrollen:

- **Absender** – Lizenzierte Anwenderinnen und Anwender, die durch ihre Admins die Acrobat Sign-Berechtigungen erhalten haben, um Unterschrifts-Workflows für Dokumente zu erstellen und Dokumente zur Unterzeichnung, Genehmigung oder Ansicht zu versenden.
- **Unterzeichner** – Anwenderinnen und Anwender, die von der absendenden Person Zugriff auf ein bestimmtes Dokument erhalten, um es zu unterzeichnen. Unterzeichnende erhalten standardmäßig von Acrobat Sign eine E-Mail mit einer eindeutigen URL zum Dokument, das unterzeichnet werden soll. Die URL enthält exklusive IDs für die betreffenden Transaktionen.
- **Genehmiger** – Anwenderinnen und Anwender, die von der absendenden Person die Berechtigung erhalten hat, ein bestimmtes Dokument zu genehmigen.
- **Andere** – Verifizierte Anwenderinnen und Anwender, die von der absendenden Person die Berechtigung erhalten haben, ein bestimmtes Dokument oder Prüfprotokoll anzuzeigen.

Lizenzierte Anwenderauthentifizierung.

Acrobat Sign unterstützt mehrere Authentifizierungsmethoden, darunter Ein- und Multi-Faktor-Authentifizierung.

Lizenzierte Anwenderinnen und Anwender melden sich mit einer der folgenden Authentifizierungsmethoden bei Acrobat Sign an:

- **Acrobat Sign ID** – Eine Kombination aus verifizierter E-Mail-Adresse und Kennwort, die für die sichere Anmeldung bei Acrobat Sign verwendet wird.
- **Adobe ID** – Eine Adobe ID ermöglicht den Zugriff auf alle lizenzierten Adobe-Dienste, darunter auch Acrobat Sign.
- **Single Sign-on (SSO)** – Unternehmen, die striktere Zugriffskontrollen benötigen, können SSO über Security Assertion Markup Language (SAML) nutzen, um Acrobat Sign-Anwendende auf Basis ihres internen Identitätssystems zu verwalten.

Admins können die Sicherheitsstufe und Komplexität eines Kennworts festlegen, die Häufigkeit der erlaubten Änderungen, den Vergleich mit früheren Kennwörtern sowie Richtlinien zum Sperren eines Kennworts (beispielsweise eine Frist zur Kennworterneuerung).

Geografischer Standort von ID-Daten.

ID-Daten werden in dem Rechenzentrum gespeichert, das dem jeweiligen geografischen Kundenstandort zugeordnet ist. Für Acrobat Sign-Kundinnen und Kunden, die Adobe Identity Management Services und die Adobe Admin Console zu Anwenderverwaltung verwenden, werden ID-Daten zusätzlich in hochverfügbaren Rechenzentren in Virginia (USA Ost), Oregon (USA West), Irland (EU West) und Singapur repliziert.

Verifizierung der Unterzeichnenden.

Je nachdem, ob es sich um interne oder externe Unterzeichnende handelt, entscheidet sich, welche Art von elektronischer Unterschrift erforderlich ist und welche Methoden zur Authentifizierung der Unterzeichnenden verwendet werden. Da die Mehrheit der Anwenderinnen und Anwender alleinigen Zugriff auf ihr E-Mail-Konto hat, wird bei der Übermittlung eines Dokuments zur Unterzeichnung die erste Stufe der Verifizierung in Acrobat Sign angewendet.

Um die Sicherheit zu erhöhen und Manipulationen vorzubeugen, können zusätzliche Authentifizierungsmethoden wie Anruf, SMS, wissensbasierte Authentifizierung (Knowledge-Based Authentication, KBA), digitale Zertifikate oder die Identitätsprüfung durch ein offizielles Ausweisdokument oder per BankID/eID in den Prozess eingebunden werden. Je nach lokaler Verfügbarkeit ist die Einbindung von weiteren Lösungen für digitale Identitätsprüfung möglich.

Acrobat Sign unterstützt zudem zahlreiche Lösungen von anderen Anbietern mit verifizierter Anbindung an das Acrobat Sign Digital Identity Gateway sowie von Anbietern von Cloud-basierten Unterschriften, die den technischen Standard des Cloud Signature Consortiums (CSC) verwenden.

Weitere Informationen zu den in Acrobat Sign integrierten Lösungen für digitale IDs sind im Adobe Trust Center erhältlich.

Zertifizierung von Dokumenten in Acrobat Sign.

In jeder Phase des Workflows schützt Acrobat Sign das Dokument, um seine Integrität und Authentizität sicherzustellen. Über eine PKI (Public Key Infrastructure) werden finale PDF-Dokumente und Prüfprotokolle mit einer digitalen Signatur zertifiziert, bevor sie an alle Beteiligten verteilt werden.

Die Signatur zur Zertifizierung wird mit einem SHA-256-Hash-Algorithmus erstellt, der einen eindeutigen, verschlüsselten Fingerabdruck aus der finalen unterzeichneten PDF-Datei ermittelt. Die digitale Signatur wird im oberen Bereich des unterzeichneten PDF-Dokuments als blaues Banner mit Zertifizierungs-Badge grafisch dargestellt. Sie verifiziert die Integrität des

Dokuments (siehe Abbildung 4) und bestätigt, dass das Dokument innerhalb von Acrobat Sign generiert wurde. Diese Signatur dient als Beweis dafür, dass das Dokument nicht modifiziert bzw. manipuliert wurde. Das finale zertifizierte PDF-Dokument kann bei Bedarf zusätzlich durch ein Kennwort geschützt werden.

Abb. 4: Zertifizierungsbanner von Acrobat Sign

Um die Schlüssel zum Sperren und Zertifizieren des unterzeichneten PDF-Dokuments zu erzeugen, verwendet Acrobat Sign Zertifikate, die von Vertrauens- und Zeitstempeldiensten ausgegeben werden. Unter bestimmten Umständen können Admins Acrobat Sign so konfigurieren, dass die Signatur zur Zertifizierung anhand eines speziellen Zertifikats erfolgt, das regionale oder spezifische Compliance-Anforderungen voraussetzt. PKI-Schlüssel zur Zertifizierung des finalen PDF-Dokuments werden in Hardware-Sicherheitsmodulen gespeichert, um ein Höchstmaß an Sicherheit und Compliance zu erfüllen.

Hosting und Sicherheit von Acrobat Sign.

Die Service-Infrastruktur von Acrobat Sign wird in Rechenzentren der Kategorie „Tier 4" des American National Standards Institute (ANSI) gehostet und von Amazon Web Services (AWS) und Microsoft Azure verwaltet, unseren bevorzugten Anbietern für Cloud-Hosting. Alle Hosting-Partnerunternehmen führen äußerst strenge Kontrollen in Bezug auf den Zugriff auf Rechenzentren, Fehlertoleranz, Umgebungssicherung und Netzwerksicherheit durch. Nur zugelassene, autorisierte Adobe-Mitarbeitende, Mitarbeitende bei Anbietern von Cloud-Services und Vertragspartner mit einem eingetragenen, anerkannten Unternehmen haben Zugriff auf die gesicherten Standorte.

Weitere Informationen zu den weltweiten Hosting-Standorten sind auf der Seite der Adobe Acrobat Sign-Rechenzentren erhältlich.

Acrobat Sign und Compliance.

Branchenstandards und gesetzliche Vorgaben.

Acrobat Sign ermöglicht verifizierten Unterzeichnenden weltweit die Interaktion mit digitalen Dokumenten von überall und mit jedem Gerät. Die Lösung erfüllt zahlreiche branchenübliche und gesetzliche Standards bzw. kann zu deren Erfüllung entsprechend konfiguriert werden. Kundinnen und Kunden behalten die Kontrolle über ihre Dokumente, Daten und Workflows und können steuern, wie sie lokale oder regionale Vorschriften wie die Datenschutz-Grundverordnung (DSGVO) der EU, den Health Insurance Portability and Accountability Act (HIPAA) der USA oder Title CFR 21 Part 11 der FDA (ebenfalls USA) am besten einhalten. Weitere Informationen zu den Sicherheitsrichtlinien von Adobe findet ihr im Datenschutzzentrum von Adobe.

Mehr über internationale Gesetze zu elektronischen Signaturen sowie die Compliance von Acrobat Sign findet ihr im Adobe Trust Center.

FedRAMP.

Acrobat Sign ist FedRAMP Tailored-konform. Acrobat Sign für Regierungseinrichtungen ist FedRAMP Moderate-konform und wird in der Microsoft Azure Government Community Cloud gehostet. Die Lösung richtet sich ausschließlich an Regierungseinrichtungen der USA sowie deren Vertragspartner in den USA.

Überblick über das Sicherheitsprogramm von Adobe.

Das integrierte Sicherheitsprogramm von Adobe besteht aus fünf Centers of Excellence. Mit neuen und fortschrittlichen Technologien wie Automatisierung, künstlicher Intelligenz und Machine Learning trägt jedes Center kontinuierlich zur Ausführung und Verbesserung der Methoden zur Erkennung und Vermeidung von Risiken bei.

Abb. 5: Fünf Centers of Excellence für Sicherheit

Die Centers of Excellence im Rahmen des Sicherheitsprogramms von Adobe umfassen:

- **Programmsicherheit** – Schutz des Produkt-Codes, Untersuchungen zu Bedrohungen und Implementierung der Ergebnisse aus dem Bug-Bounty-Programm
- **Betriebssicherheit** – Überwachung und Schutz der Systeme, Netzwerke und Cloud-basierten Produktionssysteme von Adobe
- **Unternehmenssicherheit** – Gewährleistung des sicheren Zugriffs auf die Unternehmens-umgebung von Adobe sowie der zuverlässigen Authentifizierung
- **Compliance** – Überwachung unseres Modells für Sicherheits-Governance, der Audit- und Compliance-Programme sowie der Risikoanalyse
- **Problembehandlung** – Rund um die Uhr verfügbares Security Operations Center (SOC) und sofortige Reaktion auf Bedrohungen

Die Centers of Excellence, die sich der Sicherheit unserer Produkte und Services widmen, sind dem Büro des oder der Chief Security Officer (CSO) unterstellt, das sämtliche Maßnahmen zum Schutz unserer Produkte und Services koordiniert und auch das zukünftige Sicherheits-konzept bei Adobe ausarbeitet.

Adobe-Sicherheitsorganisation.

Die Adobe-Sicherheitsorganisation basiert auf transparenter, verantwortlicher und fundierter Entscheidungsfindung und vereint sämtliche Sicherheits-Services in einem einzigen Governance-Modell. Auf Führungsebene arbeiten CSO, Chief Information Officer (CIO) und Chief Privacy Officer (CPO) eng zusammen, um Sicherheitsstrategie und Betrieb im Einklang zu halten.

Zusätzlich zu den oben beschriebenen Centers auf Excellence bezieht Adobe auch Team-Mitglieder aus den Bereichen Recht, Datenschutz, Marketing und PR in die Sicherheits-organisation ein, um Transparenz und Verantwortungsbewusstsein bei sicherheitsbezogenen Entscheidungen zu gewährleisten.

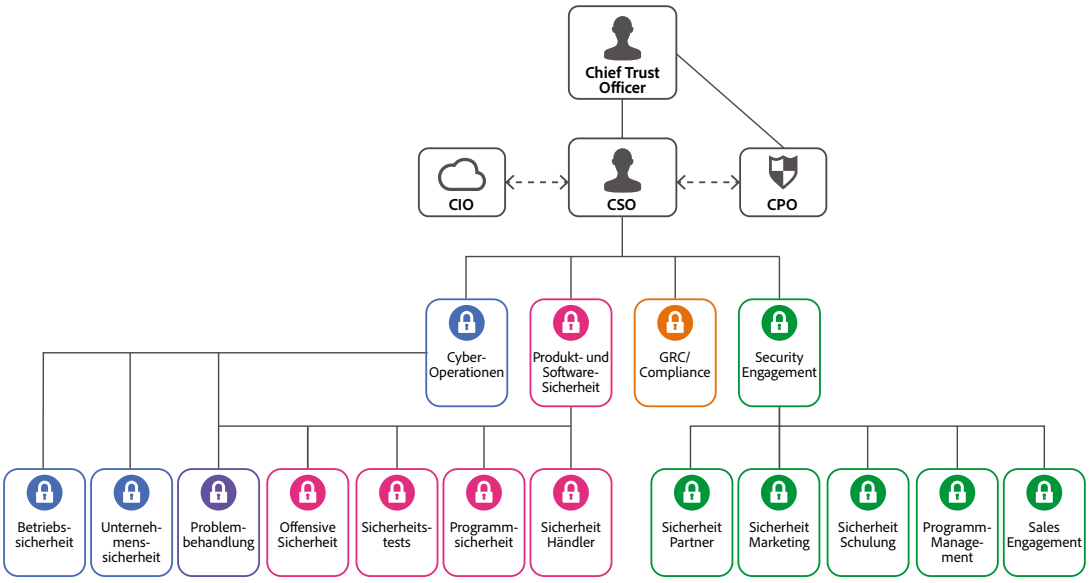

Abb. 6: Adobe-Sicherheitsorganisation

Im Rahmen der unternehmensweiten Sicherheitskultur müssen alle Mitarbeitenden von Adobe jedes Jahr ein Training zum Thema Sicherheit und Datenschutz absolvieren. Dadurch wird gewährleistet, dass alle zum Schutz des Unternehmenseigentums sowie der Daten von Kundinnen und Kunden sowie Mitarbeitenden beitragen. Mitarbeitende in technischen Abteilungen, darunter Software-Entwicklung und technischer Betrieb, werden bei Aufnahme ihrer Beschäftigung automatisch für ein intensives Trainings-Programm angemeldet, das auf ihre jeweiligen Aufgaben zugeschnitten ist.

Ausführliche Informationen zu unserer Sicherheitskultur und den Trainings-Programmen finden sich im englischsprachigen Whitepaper zur Sicherheitskultur von Adobe.

Adobe Secure Product Lifecycle.

Der Adobe Secure Product Lifecycle (SPLC) ist die Grundlage für Sicherheit bei Adobe. SPLC-Maßnahmen kommen während des gesamten Produktzyklus zum Einsatz – von Design und Entwicklung bis zu Qualitätssicherung, Test und Bereitstellung. Das Regelwerk aus mehreren Hundert strengen, auf größtmögliche Sicherheit ausgerichteten Methoden, Prozessen und Werkzeugen gibt klar strukturierte, reproduzierbare Prozesse für die Software-Entwicklung vor, sodass Sicherheit Teil jedes Produkts und jedes Service ist. Das Adobe SPLC wird kontinuierlich weiterentwickelt, um aktuelle Best Practices zu berücksichtigen.

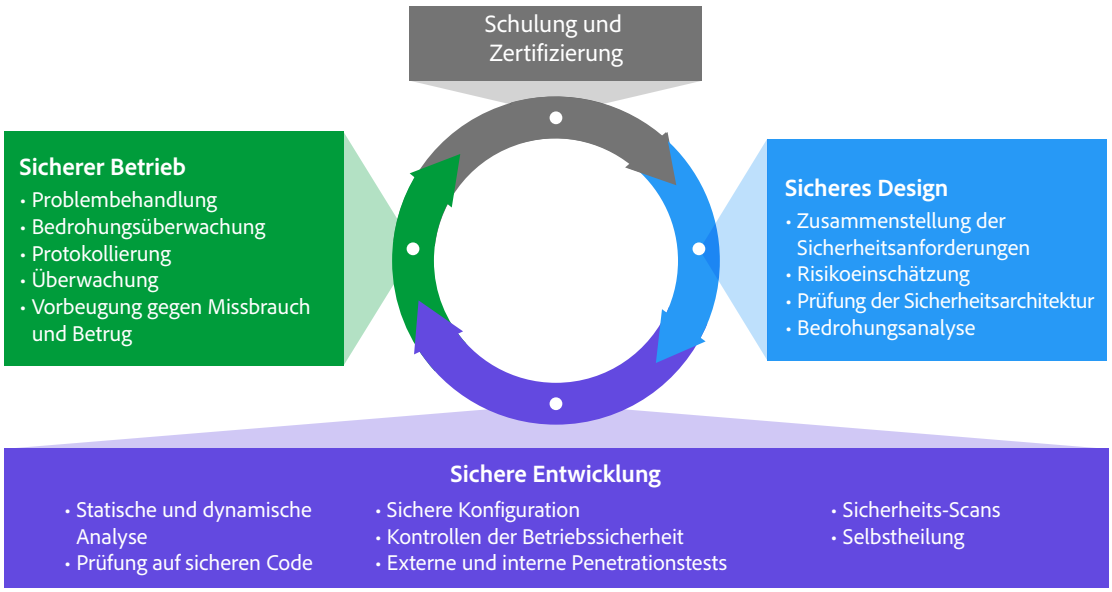

Abb. 7: Adobe Secure Product Lifecycle

Adobe befolgt einen veröffentlichten Standard für den Secure Product Lifecycle, der auf Anfrage eingesehen werden kann. Weitere Informationen über das Adobe SPLC sind dem Überblick über die Programmsicherheit bei Adobe zu entnehmen.

Programmsicherheit bei Adobe.

Das Grundgerüst für die Entwicklung von Adobe-Programmen, die „nativ sicher“ sind, heißt Adobe Application Security Stack. Mit dem Adobe Application Security Stack hat Adobe klare, wiederholbare Prozesse auf Basis fundierter Untersuchungen und Erfahrungen entwickelt. In Kombination mit Automatisierung sorgen diese Prozesse für die konsistente Durchführung von Sicherheitskontrollen. Ziel ist es, die Effizienz während der Entwicklung zu verbessern und das Risiko von Sicherheitslücken zu minimieren. Durch die Verwendung von getesteten und vorab genehmigten, sicheren Coding-Blöcken müssen häufig verwendete Muster und Blöcke nicht neu programmiert werden. So können sich Teams auf andere Aufgaben konzentrieren, mit der Gewissheit, dass der eingesetzte Code sicher ist. Zusammen mit Tests, speziellen Werkzeugen und Überwachungsfunktionen ermöglicht das Adobe Application Security Stack eine standardmäßig sichere Software-Programmierung.

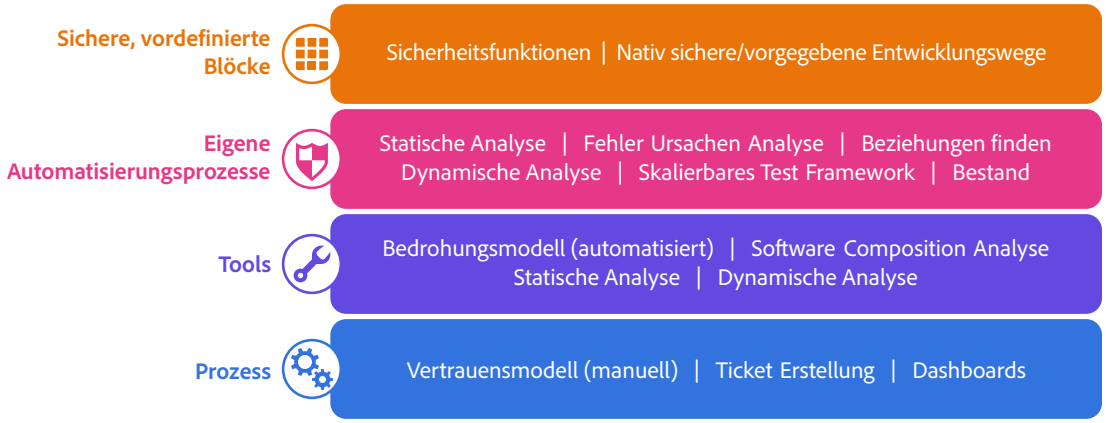

Abb. 8: Adobe Application Security Stack

Adobe befolgt außerdem mehrere veröffentlichte Standards zur Programmsicherheit, darunter arbeitsspezifische Standards für unsere Public Cloud-Infrastruktur auf Basis von Amazon Web Services (AWS) und Microsoft Azure. Diese Standards können auf Anfrage eingesehen werden. Der Überblick über die Programmsicherheit bei Adobe enthält Details zu unseren Maßnahmen und Prozessen zur Gewährleistung der Sicherheit bei Adobe-Produkten.

Betriebssicherheit bei Adobe.

Um sicherzustellen, dass alle Adobe-Produkte und -Services von Anfang an unter Berücksichtigung der Best Practices für Sicherheit entwickelt werden, hat das Team für Betriebssicherheit den Adobe Operational Security Stack (OSS) ins Leben gerufen. Der OSS ist eine Sammlung von Tools, die den Produktentwicklungs-Teams dabei helfen, die Sicherheit zu verbessern und Risiken sowohl für Adobe als auch für Kundinnen und Kunden zu minimieren. Gleichzeitig trägt der OSS dazu bei, dass im gesamten Unternehmen die Governance-Richtlinien wie Compliance und Datenschutz eingehalten werden.

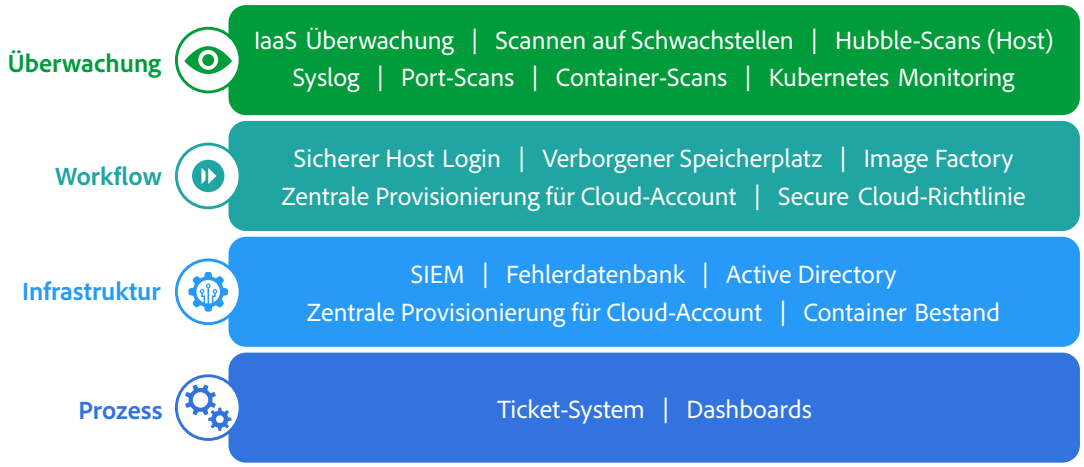

Abb. 9: Adobe Operational Security Stack

Adobe befolgt mehrere veröffentlichte Standards zum Schutz des Cloud-Betriebs, die auf Anfrage eingesehen werden können. Eine detaillierte Beschreibung des Adobe OSS und der in diesem Rahmen eingesetzten Tools findet ihr im englischsprachigen Überblick über die Betriebssicherheit bei Adobe.

Unternehmenssicherheit bei Adobe.

Zusätzlich zu den Maßnahmen zum Schutz unserer Produkte, Services und des Cloud-Hosting-Betriebs setzt Adobe eine Reihe von internen Sicherheitskontrollen unserer internen Netzwerke und Systeme, physischen Standorte sowie Mitarbeitenden und Daten ein.

Nähere Informationen zu unseren Sicherheitsmechanismen und den zugehörigen Standards findet ihr im englischsprachigen Überblick über die Unternehmenssicherheit bei Adobe.

Compliance bei Adobe.

Alle Produkte und Services von Adobe unterliegen dem Adobe Common Controls Framework (CCF). Es umfasst eine Reihe von Sicherheitsmaßnahmen und Compliance-Kontrollen, die in den Produkt-Teams sowie in verschiedenen Teilen der Infrastruktur- und Programm-Teams im Einsatz sind. Adobe setzt auf modernste Automatisierungsprozesse, um Teams auf mögliche Verstöße gegen Richtlinien aufmerksam zu machen und ihnen die schnelle Problemlösung zu ermöglichen.

Adobe-Produkte und -Services erfüllen entweder geltende gesetzliche Vorgaben oder können von Kundinnen und Kunden so genutzt werden, dass sie die jeweiligen gesetzlichen Vorgaben in Bezug auf die Inanspruchnahme von Dienstleistungen erfüllen. Sie behalten die Kontrolle über ihre Dokumente, Daten und Workflows und können steuern, wie sie regionsspezifische Vorgaben (z. B. die Datenschutz-Grundverordnung (DSGVO) der EU) am besten einhalten.

Adobe führt zudem Compliance-Trainings durch und befolgt entsprechende Standards, die auf Anfrage eingesehen werden können. Weitere Informationen zum CCF von Adobe und den wichtigsten Zertifizierungen findet ihr in der Liste der Zertifizierungen, Standards und Vorschriften.

Problembehandlung.

Unser Ziel sind kurze Reaktionszeiten, erfolgreiche Risikominderung und effektive Fehlerbehebung. Im Rahmen des Risiko- und Schwachstellen-Managements überwachen wir die aktuelle Bedrohungslage, tauschen Informationen mit Fachkräften für Sicherheit auf der ganzen Welt aus, beheben Vorfälle innerhalb kürzester Zeit und leiten sämtliche Informationen an unsere Entwicklungs-Teams weiter. So erzielen wir für alle Adobe-Produkte die größtmögliche Sicherheit.

Wir befolgen außerdem interne Standards für den Umgang mit Zwischenfällen und Schwachstellen, die auf Anfrage eingesehen werden können.

Weitere Informationen zu diesem Thema findet ihr im englischsprachigen Whitepaper über den Umgang mit Zwischenfällen bei Adobe.

Betriebliche Kontinuität und Disaster Recovery.

Das Adobe-Programm für betriebliche Kontinuität und Disaster Recovery (Business Continuity and Disaster Recovery, BCDR) setzt sich aus dem Adobe Corporate Business Continuity Plan (BCP) und produktspezifischen Disaster-Recovery-Plänen (DR) zusammen, die gemeinsam die kontinuierliche Verfügbarkeit und Bereitstellung unserer Produkte und Services gewährleisten. Das nach ISO 22301 zertifizierte Programm ermöglicht eine bessere Reaktion auf unvorhergesehene Störungen und stellt die minimale Beeinträchtigung durch Ausfälle sowie eine umgehende Wiederherstellung des Betriebs sicher. Weitere Informationen zum BCDR-Programm von Adobe findet ihr im englischsprachigen Überblick zu Business Continuity und Disaster Recovery bei Adobe.

Fazit.

Das proaktive Sicherheitskonzept und die strikten Verfahren, die in diesem Dokument beschrieben wurden, dienen dem Schutz von Acrobat Sign und eurer vertraulichen Daten. Adobe nimmt die Sicherheit eurer digitalen Inhalte sehr ernst. Die weltweiten Bedrohungen werden fortlaufend beobachtet, um kriminellen Aktivitäten stets einen Schritt voraus zu sein und die Sicherheit der Kundendaten zu gewährleisten.

Weitere Informationen zur Sicherheit bei Adobe findet ihr im Adobe Trust Center.

10/23