cpl.thalesgroup.com

THALES
Building a future we can all trust

Schlüsselverwaltungslösungen der CipherTrust Data Security Platform für Google

Die zahlreichen Kooperationen von Thales mit Google erleichtern es Unternehmen, sensible Daten sicher zwischen öffentlichen Clouds sowie hybriden und privaten IT-Infrastrukturen zu migrieren. Thales und Google bieten eine Vielzahl von Funktionen, die es Sicherheitsteams ermöglichen, ihre kryptographischen Schlüssel selbst zu besitzen und zu kontrollieren, um vor dem aktuellen Hintergrund einer räumlich weit verteilten Belegschaft die immer strikter werdenden gesetzlichen Anforderungen zu erfüllen.

Überblick über die Lösungen zum Besitz und zur Kontrolle von kryptographischen Schlüsseln von Google

Die Google Cloud Platform (GCP) bietet eine Reihe von kundenkontrollierten Mechanismen für die Schlüsselverwaltung. Um die Verschlüsselung von Data-at-Rest zu ermöglichen und Schlüssel außerhalb der Google-Infrastruktur zu verwalten, bietet Google Cloud vom Kunden verwaltete kryptographische Schlüssel (Customer-Managed Encryption Keys – CMEK) sowie externe Schlüsselverwaltung (External Key Management – EKM) an. Für die Verschlüsselung von Data in Use mit Schlüsseln, die im Prozessor verbleiben und für Google nicht verfügbar sind, bietet Google Confidential Computing. Google Ubiquitous Data Encryption nutzt die Erweiterungen in EKM. Und die Google Cloud VMware Engine nutzt das Key Management Interoperability Protocol (KMIP), um sowohl virtuelle Maschinen zu verschlüsseln als auch selbstverschlüsselnde Laufwerke in VMware VSAN zu verwalten. Google Workspace bietet eine client-seitige Verschlüsselung, die Inhalte schützt und gleichzeitig dem Kunden die Kontrolle über die kryptographischen Schlüssel der Daten ermöglicht. Verschiedene Lösungen der CipherTrust Data Security Platform von Thales verwalten die kryptographischen Schlüssel für die unterschiedlichen, vom Kunden kontrollierten Schlüsselverwaltungsmechanismen der GCP.

CipherTrust Data Security Platform

Die CipherTrust Data Security Platform von Thales ermöglicht es Benutzern, Daten auf der Google Cloud Platform, in Google Workspace, anderen Clouds sowie on-premises, einschließlich in hybriden Cloud-Umgebungen, zu entdecken, zu schützen und zu kontrollieren. Das Herzstück der Plattform ist der CipherTrust Manager, eine umfassenden, zentrale Lösung zur Verwaltung von Schlüsseln und der Richtlinien zum Datenschutz, einschließlich eines branchenführenden KMIP-Servers.Der CipherTrust Cloud Key Manager verwaltet Schlüssel für die Multi-Cloud über ihren gesamten Lebenszyklus mit umfassender Google-Unterstützung. CipherTrust Data Discovery and Classification kann sowohl Google Drive als auch Gmail scannen und ermöglicht es, CipherTrust Transparent Encryption auf Google Cloud Platform Infrastructure as a Service (IaaS) und Lösungen wie CipherTrust Tokenization auf cloud-native Lösungen zu übertragen, die auf GCP bereitgestellt werden.

KMIP-Lösungen der Google Cloud Platform

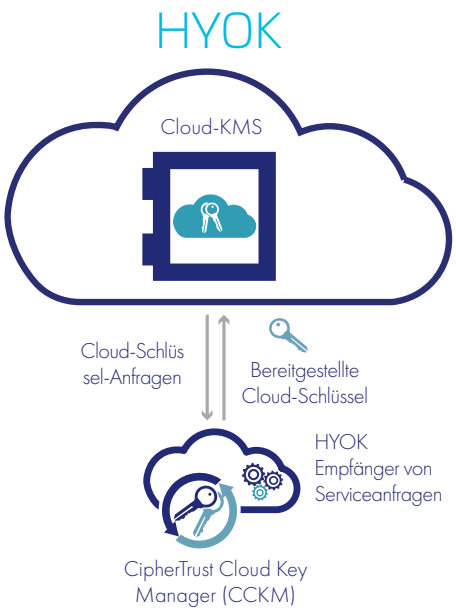
VMware vSphere VM Encryption ermöglicht die Verschlüsselung virtueller Maschinen. VM Encryption schützt die Dateien virtueller Maschinen, virtuelle Festplattendateien und Core-Dump-Dateien, indem In- und Output der virtuellen Maschine vor der Speicherung auf der Festplatte verschlüsselt werden. VMware vSAN bündelt Server-attached Storage, um einen stabilen und verschlüsselten gemeinsamen Datenspeicher bereitzustellen, der für alle virtualisierten Workloads, einschließlich geschäftskritischer Anwendungen, geeignet ist.

Sowohl vSphere VM Encryption als auch vSAN nutzen das Key Management Interoperability Protocol (KMIP) für die Schlüsselverwaltung und die Aufbewahrung von Schlüsseln, sodass beide Lösungen den KMIP-Server im CipherTrust Manager für das vollständige Key Lifecycle Management und Rollentrennung einsetzen können.

Google unterstützt den VMware Stack in Google Cloud mit der Google Cloud VMware Engine (GCVE). Jetzt können Anwendungen und Arbeitslasten, die für die Ausführung innerhalb von VMware entwickelt wurden, zusammen mit der KMIP-Unterstützung des CipherTrust Manager nahtlos in die Cloud migriert werden.

Externe Schlüsselverwaltung

Google Cloud Platform External Key Management (EKM) ist eine führende „Hold Your Own Key"-Implementierung (HYOK), für die der CipherTrust Cloud Key Manager (CCKM) als EKM-Service oder EKMS fungiert. EKM unterstützt immer mehr Dienste der Google Cloud Platform, die Sie hier einsehen können. HYOK mit EKM ermöglicht standardmäßig den Besitz von Kundenschlüsseln mit Widerruf, da Schlüssel in Google Cloud nur vorübergehend existieren. Leistungsstarke Zugriffskontrollen basieren auf der Gewährung granularen Zugriffs (Key Access Justification – KAJ) auf Schlüssel für jedes Google Cloud-Projekt, bevor diese verwendet werden können.



Ubiquitous Data Encryption

Die Ubiquitous Data Encryption (UDE) von Google beinhaltet zwei wichtige Innovationen im Bereich der Computersicherheit. Der CipherTrust Cloud Key Manager unterstützt sowohl Confidential Computing als auch Split Trust.

Confidential Computing im Kontext der UDE nutzt hardwaregesicherte Google Cloud Platform Compute Engines, die sichere Garantien für den Schutz von Data in Use bieten. Ein entscheidender Aspekt von Confidential Computing ist die sogenannte Bescheinigung (Attestation) – die Möglichkeit, zu überprüfen, ob eine entfernte Umgebung geschützt und für die Übermittlung sensibler Daten und/oder Schlüssel geeignet ist. Im Zusammenhang mit UDE ermöglicht die Bescheinigung die Fernüberprüfung, dass bestimmte Compute-Instanzen der Google Cloud Platform mit hardwaregesichertem Confidential-Computing-Schutz betrieben werden.

Zur Unterstützung einer vertraulichen Datenverarbeitung kann der CipherTrust Cloud Key Manager die Bescheinigungen überprüfen. Die Regeln für den Zugriff auf Schlüssel enthalten nun Anforderungen für vertrauliche Datenverarbeitung – in diesem Fall werden Anfragen für den Zugriff auf Schlüssel nur akzeptiert, wenn eine überprüfbare Bescheinigung über eine vertrauliche Datenverarbeitungsumgebung vorgelegt wird.

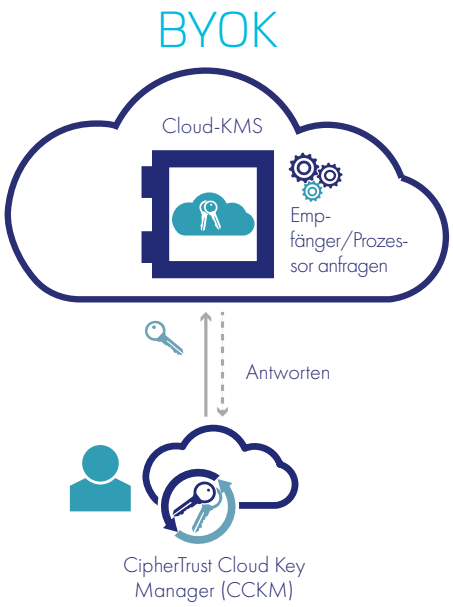
Als Komponente von UDE, erhöht **Split Trust** das Vertrauen, indem es sich für das Wrapping eines kompletten Schlüssels nicht auf eine einzige Quelle verlässt. Stattdessen kann der DEK aufgeteilt und jedes Fragment an mehrere Wrapping-Dienste gesendet werden. Split Trust erhöht das Vertrauen in die Cloud, indem es sicherstellt, dass weder Google noch ein Host, eine Anwendung oder ein Benutzer mit Zugriff auf den CipherTrust Cloud Key Manager einseitig Kundendaten entschlüsseln können. Der CipherTrust Cloud Key Manager bietet volle Unterstützung für Split Trust.

Split Trust erfüllt das Konzept der Ubiquitous Data Encryption:

- Data in Use werden mit einer Speicherverschlüsselung verschlüsselt, die von vertraulicher Computerhardware bereitgestellt wird
- Data in Motion werden während der Übertragung verschlüsselt
- Data at Rest werden mit der zusätzlichen Leistung der kryptographischen Schlüssel von Split Trust verschlüsselt

Vom Kunden verwaltete kryptographische Schlüssel

Kunden, die einen Bring-Your-Own-Key-Mechanismus bevorzugen, können Google Customer-Managed Encryption Keys verwenden. Sie unterstützen eine Vielzahl von Google-Cloud-Platform-Diensten, die hier eingesehen werden können.



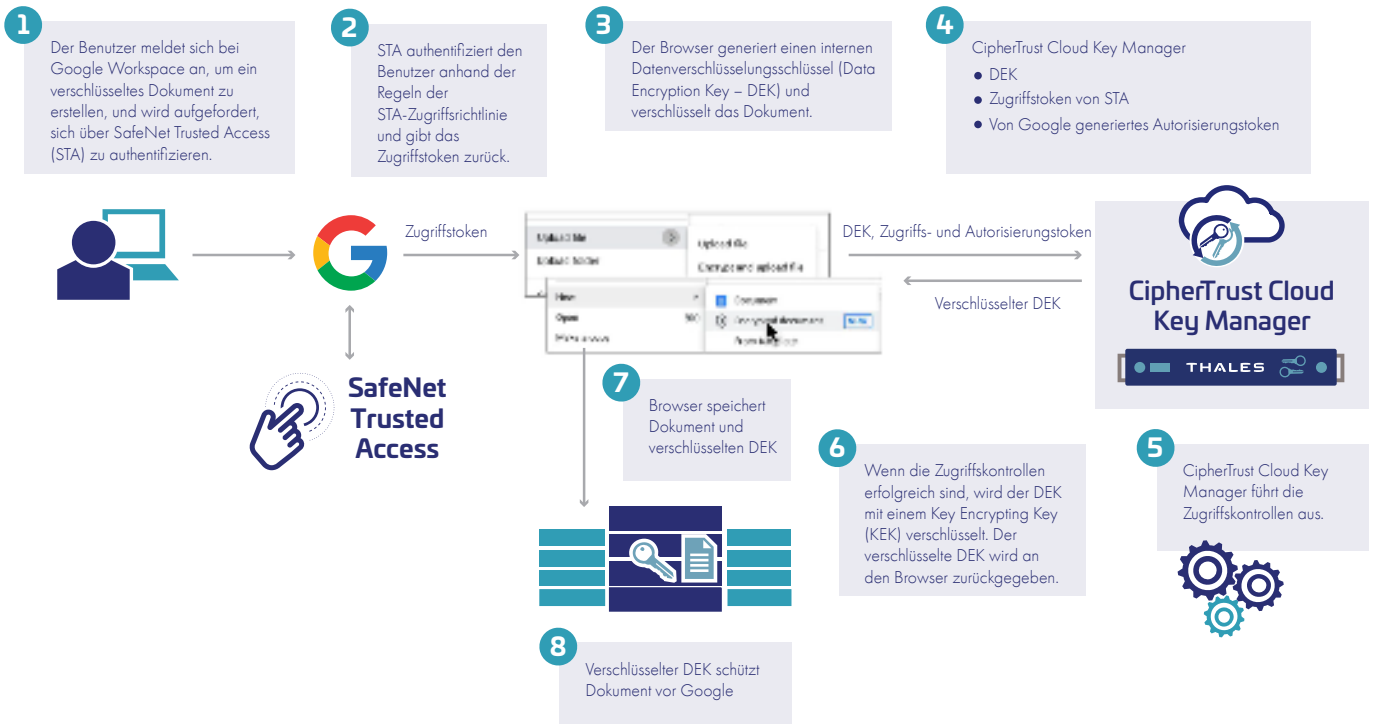


Abb 1.: Workflow der Authentifizierung und Verschlüsselung

Client-seitige Verschlüsselung von Google Workspace

Die client-seitige Verschlüsselung von Google Workspace verschlüsselt die Workspace-Inhalte im Browser des Benutzers mit einem vom Browser erstellten DEK. Gemäß dem Konzept der „Shared Security" (verteilte Sicherheit) empfiehlt Google seinen Kunden den Einsatz einer externen Schlüsselverwaltung (EKM) und eines Identitätsproviders (IDP), um sicherzustellen, dass nur autorisierte und authentifizierte Personen auf geschützte Dokumente zugreifen können. Die EKM ist der CipherTrust Cloud Key Manager. Nach Erhalt einer Wrapping- oder Unwrapping-Anfrage, die den DEK, ein Authentifizierungs-Token von einem von CCKM unterstützten IDP und ein Autorisierungstoken von Google Workspace enthält, stellt der CCKM sicher, dass die Anfrage von einem legitimen Anfrager stammt und gültig ist. Anschließend führt der CCKM den Wrapping- oder Unwrapping-Vorgang durch und sichert den Zugriff auf Google Drive, Gmail, Google Calendar oder Anrufe über Google Meet für verifizierte Benutzer und deren Rolle (z. B. nur lesen, lesen und schreiben).

Kunden, die die client-seitige Verschlüsselung von Google Workspace nutzen, können mit der integrierten End-to-End-Lösung von Thales, die kryptographische Schlüssel getrennt von ihren sensiblen Daten in der Cloud kontrolliert und Identitäten schützt, eine höhere Sicherheit und einen geringeren Bereitstellungsaufwand erreichen. In Kombination mit SafeNet Trusted Access (STA) bietet der CipherTrust Cloud Key Manager Kunden Schlüsselverwaltung und eine unabhängige IDP-Lösung von einem einzigen Anbieter, die mit einer reibungslosen Bereitstellung und einer überragenden Benutzererfahrung zum Erreichen der Geschäftsziele beitragen.

Google und die CipherTrust Data Security Platform von Thales

Die Lösungen zur Schlüsselverwaltung von Thales werden mit den Innovationen von Google Cloud Platform und Google Workspace rasch erweitert. Und die Lösungen von Thales für die Erkennung, den Schutz und die Kontrolle von Daten in der CipherTrust Data Security Platform können die Sicherheit der Google Cloud Platform und anderer Multi- und Hybrid-Cloud-Lösungen sowohl für IaaS- als auch für cloud-native Computing-Umgebungen verbessern.

Über Thales

Die Menschen, denen Sie den Schutz Ihrer Daten anvertrauen, vertrauen beim Datenschutz auf Thales. Beim Thema Datensicherheit stehen Unternehmen immer häufiger vor entscheidenden Momenten. Egal, ob es darum geht, eine Verschlüsselungsstrategie zu entwickeln, Ihre Daten in die Cloud zu übertragen oder Compliance-Anforderungen zu erfüllen – Sie können sich bei der Sicherung Ihrer digitalen Transformation auf Thales verlassen.

Entscheidende Technologie für entscheidende Momente.