Whitepaper

Sicherheit und Datenschutz in Cisco Spark

Version 1.0 (Juni 2016)

Cisco® Spark ist eine Cloud Collaboration-Plattform mit Messaging-, Anruf- und Meeting-Funktionen. Die Cisco Spark® App dient als Front-End zur Verbindung mit dieser Plattform und bietet daher umfassende Funktionen für die Zusammenarbeit in Teams. Benutzer können Nachrichten senden, Dateien teilen und sich mit anderen Teams treffen – alles an einem Ort.

Dieses Whitepaper gibt einen Überblick über einige der Sicherheitsmechanismen der Cisco Spark Cloud und von Cisco Spark Messaging.

Die hier beschriebenen Cisco Produkte, Services und Funktionen befinden sich derzeit in unterschiedlichen Phasen der Entwicklung. Während einige dieser Cisco Produkte, Services und Funktionen aktuell verfügbar sind, befinden sich andere noch in der Entwicklung oder Planung. Zusätzliche Informationen finden Sie unter www.cisco.com.

Cisco übernimmt keinerlei Haftung für die verspätete oder unterbliebene Bereitstellung der in diesem Dokument genannten Produkte, Services oder Funktionen.

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

Herausforderungen bezüglich Sicherheit und Datenschutz bei der Cloud Collaboration

Einer der wichtigsten Vorteile für Unternehmen, die Cloud-Services in Anspruch nehmen, ist die Möglichkeit, Funktionen so schnell zu nutzen, wie der Anbieter sie bereitstellt. In vielen Fällen ist das Mehrwertangebot der Cloud-Provider jedoch nur durch vollständigen Zugriff auf alle Benutzerdaten und -inhalte möglich. Bei Collaboration-Anwendungen greifen die meisten Cloud-Provider direkt auf Nachrichten, Anrufe und auch Meeting-Inhalte zu, um Funktionen wie Nachrichtensuche, Transkodierung von Inhalten oder Integration mit Anwendungen von Drittanbietern anzubieten. Andererseits sind moderne Verbraucher-Collaboration-Services darauf ausgerichtet, die Privatsphäre der Verbraucher zu schützen, indem sie End-to-End-Verschlüsselung auf Kosten von Mehrwertfunktionen anbieten.

Cisco Spark bietet eine Cloud Collaboration-Plattform mit End-to-End-Verschlüsselung sowie die Möglichkeit zur Integration von Mehrwertangeboten von Cisco oder Drittanbietern. Die Plattform verfügt daher über eine offene Architektur zur sicheren Bereitstellung der Schlüsselinformationen und erlaubt es Unternehmen so die exklusive Kontrolle über eben diese Schlüsselinformationen zu behalten und damit die Vertraulichkeit der Daten zu gewährleisten. Inhalte werden bereits direkt auf dem Benutzer-Client verschlüsselt und bleiben es bis zum Erhalt durch den Empfänger, wodurch keine zwischengelagerte Instanz oder der Cloud-Anbieter selbst ohne die ausdrückliche Genehmigung des Unternehmens Zugriff auf die Schlüsselinformationen oder die damit verschlüsselten Inhalte erlangen kann.

Durch den Zugriff auf diese Schlüssel stehen Ihnen zusätzliche Funktionen zur Verfügung. Gleichzeitig sorgen wir für eine End-to-End-Verschlüsselung in der gesamten Architektur von Spark, wodurch viele der Mehrwertfunktionen nur über verschlüsselte Daten laufen. Durch die Nutzung innovativer Konzepte zur Nachrichtenindizierung, Berechtigungsverwaltung, Authentifizierung, sowie Verschlüsselung- und Bereitstellungsmodellen unterstützt Cisco Spark daher Funktionen wie die globale Suche von Inhalten, ohne dass diese zuvor in der Cisco Spark Cloud entschlüsselt wurden.

Die meisten Cloud-Service-Provider belegen die Sicherheit ihrer Angebote durch eine verschlüsselte Übertragung der Daten zwischen Endbenutzergeräten und den jeweiligen Servern oder zwischen den eigenen Rechenzentren. Damit sind die Daten aber nicht vor einem Zugriff durch den Service-Provider selbst geschützt. Alle Verbindungen zu und von der Spark-Cloud werden bei der Übertragung verschlüsselt. Wir gehen aber noch einen Schritt weiter und stellen sicher, dass wir nur Benutzerinhalte sehen, zu denen uns ausdrücklich Zugriff gewährt wurde.

Unser Versprechen, einen sicheren und zuverlässigen Service bereitzustellen beschränkt sich dabei nicht allein auf den Schutz von Benutzerinhalten. Spark schützt alle Benutzer- und Nutzungsdaten mit einer Kombination aus Datenschutzmechanismen und Funktionen wie *Identitätsverschleierung*[1], Wahlfreiheit und Transparenz. Wie bei der End-to-End-Verschlüsselung haben wir diese Schutzmechanismen von Anfang an in den Service integriert.

End-to-End-Verschlüsselung von Inhalten

Eine Kernkomponente der End-to-End-Verschlüsselung in der Cisco Spark-Cloud bildet der sogenannte Key Management Server (KMS). Der KMS ist verantwortlich für das Erstellen, Speichern und Autorisieren sowie die Bereitstellung der Schlüsselinformationen, die dann von den Spark-Clients zum Ver- und Entschlüsseln von Nachrichten und Dateien verwenden werden. Die End-to-End-Verschlüsselung in Spark wird durch die architektonische und operative Trennung zwischen dem KMS und der übrigen Spark-Cloud ermöglicht. Sie befinden sich praktisch in unterschiedlichen Bereichen bzw. Vertrauensdomänen in der Cloud: Der KMS befindet sich im „*Security-Realm*“ während alle anderen Komponenten von Spark sich im *Core* befinden.

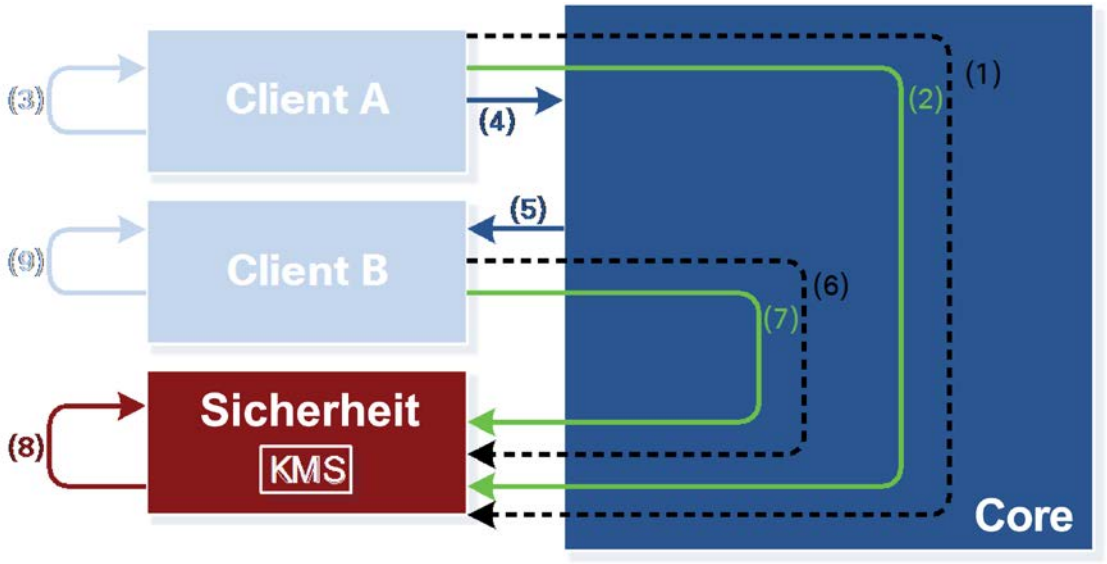
[1] Siehe Abschnitt zur Identitätsverschleierung

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

Die Kommunikation mit dem KMS durchläuft die Cisco Spark-Cloud, ist aber ebenfalls durchgängig verschlüsselt und kann daher nicht vom Core gelesen werden. Zudem wird sie mit einem Zugriffs-Token authentifiziert, das an keiner anderen Stelle in der Cisco Spark-Cloud verwendet werden kann. Dieses Modell gewährleistet einen angemessenen Zugriff auf Verschlüsselungsschlüssel und garantiert gleichzeitig, dass keine Core-Servicekomponenten auf diese Kommunikation oder die im KMS gespeicherten Schlüssel zugreifen können. Die Services im Security-Realm werden bei Cisco auf einer separaten Infrastruktur in einem separaten Tenant betrieben. Unternehmen mit besonders hohen Sicherheitsanforderungen können die Security-Realm-Services, einschließlich des KMS, alternativ am eigenen Standort bereitstellen. Details hierzu finden Sie im nächsten Abschnitt.

Wenn ein Spark-Benutzer Inhalte zu einem Spark-Raum senden möchte, muss der Client des Benutzers zuerst einen sicheren Kanal zum KMS herstellen, wie in **(1)** in Abbildung 1 dargestellt. Um einen gemeinsamen geheimen Schlüssel für einen sicheren Kanal zwischen Client und KMS herzustellen, führen der Client und der KMS einen authentifizierten flüchtigen Elliptic Curve Diffie-Hellman-Schlüsselaustausch (ECDH) durch. Durch diesen Austausch wird ein symmetrischer gemeinsamer Schlüssel erzeugt, der für eine sichere Nachrichtenübermittlung verwendet werden kann.

Abbildung 1: Client-KMS-Kommunikation in Cisco Spark



Für diesen Kanal ist eine Authentifizierung erforderlich, um sicherzustellen, dass es für Cisco oder eine andere Drittpartei nicht möglich ist, Informationen und Schlüssel, die auf diesem Kanal übertragen werden, einzusehen, zu ändern oder als Man-in-the-Middle zu agieren. Der Authentifizierungsmechanismus nutzt ein Public-Key-Infrastruktur-Zertifikat auf dem KMS, in dem das Zertifikat einen Common Name (CN) oder Subject Alternative Name (SAN), der dem Domänennamen des Unternehmens entspricht, enthält. Clients verschlüsseln ihre Hälfte des ECDH-Austauschs zum KMS über den öffentlichen Teil des KMS-Serverzertifikats. ECDH-Antworten vom KMS werden mithilfe des privaten Teils des KMS-Serverzertifikats gekennzeichnet[2]. Dies ist insofern eine geringfügige Veränderung am ECDHE-RSA-Mechanismus, als dass der Client die Verschlüsselung mit dem öffentlichen Zertifikat des Servers durchführt und nicht mit seinem eigenen Schlüssel, wodurch Clients keine Zertifikate benötigen. Dies bedeutet jedoch auch, dass die Clients in der Lage sein müssen, das Zertifikat des

[2] Clients werden über ihr KMS-Authentisierungs-Token authentifiziert, siehe hierzu den Abschnitt zur Raumautorisierung unten.

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

KMS zu authentifizieren. Hierfür müssen KMS-Zertifikate entweder eine öffentliche Zertifizierungsstelle (CA, Certificate Authority) nutzen, die sowohl auf Desktops als auch auf mobilen Geräten weit verbreitet ist, oder Unternehmen müssen in der Lage sein, ihr privates CA-Stammzertifikat an die Endgeräte zu übermitteln, über die ihre Benutzer auf Cisco Spark zugreifen. Die Übertragung von privaten CA-Zertifikaten an Clients wird nicht von Cisco Spark ausgeführt, die Cisco Spark-Clients können jedoch jedes vertrauenswürdige Zertifikat nutzen, dass sich im Trusted Certificate Store des Client befindet.

Sobald der Client und der KMS sich auf einen symmetrischen Schlüssel über den authentifizierten ECDH-Mechanismus geeinigt haben, nutzt der Client diesen Kanal, um neue Schlüsselinformationen anzufordern. Dieser wird dann verwendet um den für einen einzelnen Spark-Raum bestimmten Inhalt sowie dessen Teilnehmer, wie in **(2)** dargestellt, zu verschlüsseln. Dieser Schlüssel wird Konversationsschlüssel genannt.

Nachdem der Benutzer eine Nachricht verfasst hat, verschlüsselt der Client die Nachricht mit dem Konversationsschlüssel **(3)**, kennzeichnet sie mit der Raum-ID des Zielraums und sendet sie zum Core **(4)**. Der Core erhält eine Nachricht in verschlüsselter Form. Der Core verfügt nicht über den Konversationsschlüssel, sodass er die Nachricht nicht entschlüsseln kann. Der Core überprüft die Liste der Benutzer, die mit der Raum-ID verbunden sind, welche in den Metadaten einer Nachricht angegeben ist, und sendet den anderen Benutzern im Raum **(5)** die verschlüsselte Nachricht. Zusätzlich wird die Nachricht in verschlüsselter Form, unter Referenz zum jeweiligen Raum, in der Nachrichtendatenbank des Core gespeichert.

Die Nachricht bleibt verschlüsselt, wenn sie von den Clients der anderen Benutzer empfangen wird. Die Clients der anderen Benutzer kontaktieren ihren KMS, um den Konversationsschlüssel zu erhalten und damit die Nachricht entschlüsseln zu können **(6, 7)**. Dabei ist der Austausch zwischen den Empfängern **(6)** und dem zugehörigen KMS identisch mit dem ersten Austausch **(1)**. Der KMS authentifiziert jeden Benutzer, um die Zugriffsberechtigung für den Konversationsschlüssel anhand des zugeordneten Raums zu überprüfen **(8)**. Der KMS verteilt den Konversationsschlüssel an die Empfänger und ermöglicht ihnen, die Nachricht damit zu entschlüsseln und zu lesen **(9)**.

Es ist wichtig, zu beachten, dass zwei verschiedene Verschlüsselungsebenen in den oben aufgeführten Abläufen verwendet werden: Hop-by-Hop und End-to-End. Wie oben beschrieben werden Benutzerinhalte und die Interaktion zwischen Client und KMS mithilfe von symmetrischer Verschlüsselung mit raumspezifischen Konversationsschlüsseln für Benutzerinhalte sowie flüchtigen Schlüsseln für Client-KMS-Inhalte durchgängig verschlüsselt. Derzeit ist der in Spark verwendete Codierungsschlüssel AES256-GCM. Bei der Übermittlung durchgängig verschlüsselter Inhalte von Client zu Server, von Server zu Server und vom Server zurück zu anderen Clients werden sie zusätzlich durch Hop-by-Hop-Verschlüsselung geschützt. Hop-by-Hop-Verschlüsselung verwendet das Transport Layer Security (TLS)-Protokoll, dasselbe Protokoll, das ein Webbrowser bei der Kommunikation mit einer Bank oder einem Online-Einzelhändler verwendet. Für die End-to-End- und Hop-by-Hop-Verschlüsselung werden die derzeit besten Verschlüsselungsmethoden eingesetzt. Zudem wurde Spark nach einem Konzept entwickelt, das als Algorithmusflexibilität bekannt ist. Algorithmusflexibilität ermöglicht die schnelle Einführung neuer Verschlüsselungsmechanismen. Denn auch die aktuell zuverlässigsten Methoden können veralten und durch neue Branchenempfehlungen ersetzt werden.

Die oben genannten benutzergenerierten Inhalte umfassen dabei alle Nachrichten, Raumnamen und Dateien, die auf Spark geteilt werden.

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

Konversationsschlüssel-URIs

Konversationsschlüssel werden durch eindeutige und einheitliche Bezeichner für Ressourcen (URI, Uniform Resource Identifiers) identifiziert und referenziert. Wenn durchgängig verschlüsselte Inhalte von einem Client zur Spark-Cloud gesendet werden, enthält der Header die Schlüssel-URI. Die URI liefert Details dazu, welcher KMS den Schlüssel generiert hat und wo dieser abgerufen werden kann – vorausgesetzt der Anfrager durchläuft die Authentifizierungs- und Autorisierungsprüfungen erfolgreich.

Mehrere Konversationsschlüssel und Schlüsselrotation

Es ist zu jeder Zeit mindestens ein Konversationsschlüssel pro Client vorhanden, der Inhalte an einen Spark-Raum bereitstellt. Wenn beispielsweise Andrea in einem Spark-Raum sowohl von ihrem Mobilgerät als auch von ihrem Laptop aus Inhalte bereitstellt und Jan im selben Raum von seinem Laptop ebenfalls Inhalte bereitstellt, während er auf seinem Mobilgerät Inhalte lediglich anzeigt, sind drei (3) symmetrische Konversationsschlüssel im Raum aktiv: einer für Andreas Mobilgerät, ein weiterer für ihren Laptop sowie einer für Jans Laptop.

Die Konversationsschlüssel werden deaktiviert, wenn Benutzer Räume verlassen, egal ob freiwillig oder zwangsweise. Wenn Clients bemerken, dass ein Benutzer den Raum verlässt (siehe „Transparente Autorisierung“ unten), muss der Client den Konversationsschlüssel rotieren, bevor weitere Inhalte im Raum bereitgestellt werden können. Die Spark-Cloud erzwingt dieses Verhalten. Symmetrische Client-KMS-Schlüssel rotieren ebenfalls regelmäßig.

Raumautorisierung

Wenn Benutzer andere Benutzer zu Räumen hinzufügen oder aus diesen löschen, muss der Client des Benutzers sicherstellen, dass sowohl Spark als auch der KMS des Benutzers die Veränderungen bezüglich der Raumautorisierung registriert haben. Der Client erzeugt eine Autorisierungsnachricht, um Spark und den KMS über diese Änderungen zu informieren. Die Autorisierungsnachricht beinhaltet zwei untergeordnete Nachrichten:

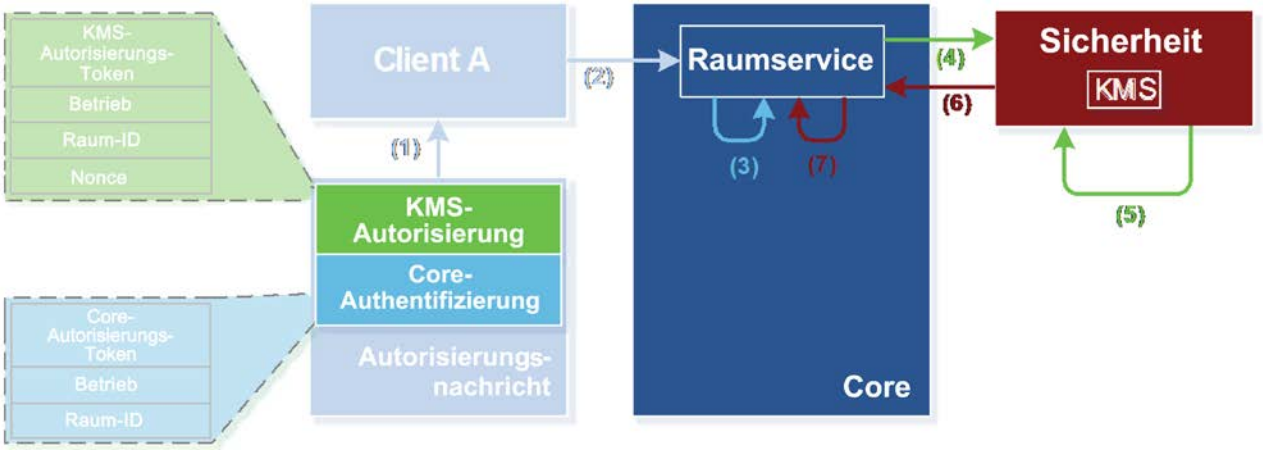
- Die erste Nachricht ist ein Autorisierungsänderungsblock, der das Authentisierungs-Token[3] des Clients für den Core, den Vorgang des Hinzufügens/Entfernens und die eindeutige Raumkennung für diesen Vorgang enthält.
- Die zweite Nachricht ist ein verschlüsselter Autorisierungsänderungsblock, der das KMS-Authentifizierungs-Token, den Vorgang des Hinzufügens/Entfernens und die eindeutige Raumkennung für diesen Vorgang und eine Nonce (einen zufällig generierten, einmalig genutzten Datenblock) enthält.

Die untergeordnete Nachricht wird mithilfe des vorübergehenden symmetrischen Schlüssels verschlüsselt, der zuvor zwischen dem Client und dem KMS während der Konversationsschlüsselabfrage übertragen wird. Dabei muss beachtet werden, dass die verschlüsselte untergeordnete Nachricht das KMS-Authentifizierungs-Token verwendet, während die für den Core bestimmte untergeordnete Nachricht das Core-Authentifizierungs-Token verwendet. Diese Verwendung eindeutiger Authentisierungs-Tokens zusammen mit der zusätzlichen Verschlüsselungsebene beim Änderungsvorgang des KMS verhindert, dass der Core die Identität des Client vortäuschen kann, was andernfalls dazu führen würde, dass der Core falsche Autorisierungsanfragen an den KMS senden könnte.

[3] Alle Token sind OAuth-Inhaber-Token.

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

Abbildung 2: Erstellung der zweiteiligen Autorisierungsnachricht



- Nachdem der Client die zweiteilige Autorisierungsnachricht **(1)** in Abbildung 2 erzeugt hat, sendet der Client die Nachricht über TLS an den Raumservice **(2)**.
- Der Raumservice validiert **(3)** die untergeordnete Core-Nachricht, einschließlich des Core-Authentifizierungs-Token, und überprüft, ob der Anfrager für Änderungen am in der Raum-ID angegebenen Raum autorisiert ist.
- Wenn alles in Ordnung ist, leitet der Raumservice die verschlüsselte untergeordnete Nachricht zusammen mit der in der untergeordneten Core-Nachricht enthaltenen Raum-ID und der Benutzer-ID aus dem Core-Authentifizierungs-Token an den KMS des Benutzers weiter **(4)**.
- Durch die Einbeziehung der Raum-ID in der Kommunikation und der ID des authentifizierten Benutzers kann der KMS überprüfen, ob die Raumserviceanfrage und die KMS-Anfrage zur Authentifizierung und Autorisierung übereinstimmen. Der KMS entschlüsselt die empfangene Nachricht, validiert das KMS-Authentifizierungs-Token und stellt sicher, dass der anfragende Benutzer berechtigt ist, Änderungen am angegebenen Raum **(5)** vorzunehmen.
- Wenn alles in Ordnung ist, führt der KMS den angeforderten Vorgang durch und gibt den Erfolg an den Raumservice **(6)** zurück. Nach Eingang der Erfolgsmeldung des KMS bezüglich der Durchführung des Vorgangs, wird die eigentliche Änderung durchgeführt **(7)**.

Ein Vorteil dieses Ansatzes ist, dass er die Prinzipien des Fate-Sharings befolgt. Bei Client-Anfragen zum Hinzufügen oder Entfernen eines Benutzers wird dieser sowohl auf dem Core als auch dem KMS oder auf keinem von beiden hinzugefügt oder entfernt; eine Eigenschaft, die in der Regel als *Atomizität* bezeichnet wird, d. h. die beiden Vorgänge in keinem Fall unabhängig voneinander erfolgen. Dies gewährleistet, dass der Core und der KMS synchron bleiben, während gleichzeitig von den Sicherheitsvorteilen profitiert werden kann, die durch die Core-gesteuerte Autorisierung für die verschlüsselten Inhalte und die KMS-gesteuerten Autorisierung von Schlüsseln zur eigentlichen Entschlüsselung der Inhalte entstehen.

Transparente Autorisierung

Die Liste der autorisierten Benutzer für einen bestimmten Spark-Raum wird allen anderen autorisierten Benutzern des Raums im Spark-Client angezeigt. Neben der Liste der autorisierten Benutzer werden im Raum Beitritt, Verlassen sowie das Entfernen von Benutzern zusammen mit den eigentlichen Inhalten des Raums angezeigt. Diese Inline-Nachrichten machen den Mitgliedern eines Raums deutlich, wer von wem hinzugefügt oder aus einem Raum entfernt wurde. Verlässt ein Mitarbeiter das Unternehmen, erzwingt Spark das Verlassen aller Räume, auf die der Mitarbeiter Zugriff hatte. Dies verdeutlicht den verbleibenden Raumteilnehmern, dass der Mitarbeiter nicht

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

mehr länger auf die vorhandenen oder zukünftigen Rauminhalte zugreifen kann, und führt dazu, dass alle anderen Teilnehmer ihre Konversationsschlüssel rotieren müssen.

Schlüsselzugriff von Funktionen

In der aktuellen Form sind einige Funktionen nur verfügbar, wenn Cisco Zugriff auf die Schlüssel erhält. Dazu zählt z. B. die Transkodierung von Dokumenten, ein Hintergrundprozess, der viele Dateitypen, wie z. B. Microsoft Office-Dokumente, in Bildformate konvertiert, um sicherzustellen, dass Web- und Mobilgeräte Formate schnell anzeigen können, die von der jeweiligen Plattform nicht unterstützt werden. Funktionen, die einen Schlüsselzugriff erfordern, fordern die Schlüssel vom Unternehmens-KMS auf die gleiche Weise wie alle anderen Benutzer-Clients an. Dies geschieht jedoch über ein maschinelles Konto, das vom Unternehmensadministrator speziell für den Zugriff auf bestimmte Schlüssel im Unternehmens-KMS autorisiert wurde. Maschinelle Konten funktionieren wie Benutzerkonten, aber während Benutzerkonten ein Benutzername und ein Passwort zugeordnet ist, ist maschinellen Konten eine maschinelle ID und ein maschineller Schlüssel für die Maschine-Maschine (M2M)-Authentifizierung zugeordnet.

Wir wissen, dass einige Kunden sich möglicherweise nicht wohl dabei fühlen, wenn Cisco Zugriff auf wichtige Dokumente in den Spark-Räumen hat. Aus diesem Grund gibt Spark Kunden immer die Möglichkeit, bestimmte Funktionen, die Schlüsselzugriff für das gesamte Unternehmen benötigen, zu deaktivieren. Wenn diese Funktionen deaktiviert werden, wird auch die Autorisierung für das dazugehörige maschinelle Konto im Unternehmens-KMS deaktiviert. Somit wird sichergestellt, dass auf den Schlüssel nicht mehr zugegriffen werden kann. Werden Dokumente oder Inhalte in einen Raum hochgeladen, der auch Teilnehmer aus einem anderen Unternehmen enthält, kann dies weiterhin zum Cloud-Zugriff auf Inhalte führen, wenn das andere Unternehmen einen Cloud-KMS oder andere Funktionen nutzt, die den Zugriff auf Schlüssel erfordern.

Eine vollständige Liste der Funktionen, die derzeit Schlüsselzugriff erfordern, zusammen mit Anweisungen zu deren Deaktivierung, ist im Cisco Cloud Collaboration Management-Portal erhältlich. Der Abschnitt zu Integration und Erweiterbarkeit beschreibt, wie Drittparteien der Cisco Spark-Plattform neue Funktionen hinzufügen können.

Bereitstellungsoptionen im Security-Realm

Sie wissen jetzt wie Cisco die End-to-End-Verschlüsselung in die Fabric von Spark integriert hat und dabei auf die Trennung des Security-Realm vom Rest der Cisco Spark Cloud setzt. Für Kunden, die aufgrund besonderer Anforderungen sicherstellen möchten, dass Cisco als Cloud-Service-Provider keinerlei Zugriff auf ihre Inhalte hat, gibt es die Möglichkeit, einen Teil der Dienste des Security-Realm auszulagern – darunter auch den KMS.

Der Kunde hat daher die Wahl, diese Services des Security-Realm durch Cisco hosten zu lassen oder sie im eigenen Rechenzentrum bereitzustellen. Cisco stellt allen Unternehmenskunden, die dies zur Überprüfung unseres Versprechens wünschen, nicht nur kommerziell verfügbare Versionen aller Services, sondern auch Quellcode für Security-Realm-Services, wie dem KMS, zur Verfügung. Zusätzlich nutzen alle Services im Security-Realm branchenübliche Protokolle wie JSON über HTTPS. Darüber hinaus arbeitet Cisco aktiv an der Standardisierung der Schlüsselverwaltungstechniken, die von Cisco Spark verwendet werden, damit Services von Cisco zukünftig bei Bedarf auch durch kommerzielle und Open-Source-Lösungen von Drittanbietern ersetzt werden können. Gut dokumentierte, standardkonforme Schnittstellen sorgen dafür, dass Kunden, die großen Wert auf Vertraulichkeit legen oder eine starke Anpassung benötigen, die Freiheit haben, mit der Zeit auch ihre eigenen Implementierungen dieser Services zu erstellen.

Wird der Security-Realm in der aktuell verfügbaren Version außerhalb der Cisco Spark-Cloud gehostet, betreibt Cisco die Software gemeinsam mit dem Kunden oder Partner In diesem gemeinsamen Modell hat Cisco Zugriff auf Protokolle sowie Analysen und liefert Upgrades. Protokolle enthalten niemals Schlüssel oder persönlich identifizierbare Informationen. Auf die gleiche Weise werden auch Metriken gesammelt, durch die Cisco die

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

Server-Leistung nachvollziehen kann. Der Kunde oder der Partner verwaltet die Hardwarebereitstellung sowie die gesamte Servicebereitstellung und -konfiguration.

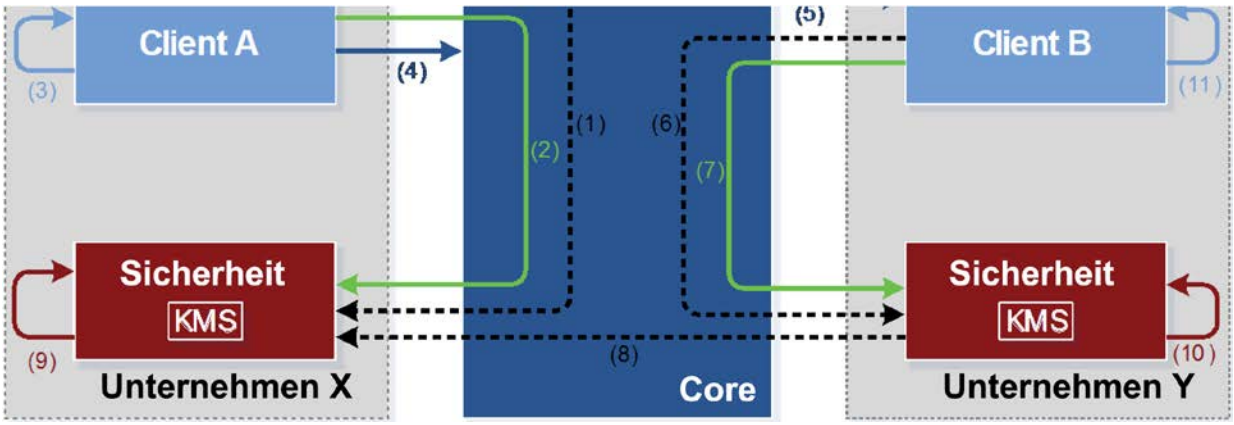
Sobald alle Administrationsprozesse und die notwendigen Schnittstellen vollständig entwickelt sind, wird der Security-Realm in einem vollständig von einem Partner oder dem Unternehmen gehosteten und betriebenen Modell verfügbar sein. Bei diesem Modell betreibt Cisco auch weiterhin die Services in anderen Bereichen. Der Security-Realm wird jedoch vollständig von einem Cisco Partner in der Infrastruktur des Partners oder vom Unternehmen des Kunden in der eigenen Infrastruktur oder beim bevorzugten Cloud-Provider betrieben. Damit liegt dann die vollständige betriebliche Kontrolle über den KMS, den Search-Indexer, die verbundenen Datenbanken und alle weiteren Security-Realm-Services in den Händen des Partners bzw. des Unternehmens.

Weitere Informationen zu den Bemühungen von Cisco zur Standardisierung der KMS-Architektur finden Sie unter http://cs.co/keymanagement.

Key Management Server (KMS)-Verbund

Benutzer in Cisco Spark sind immer nur einem einzigen Unternehmen zugeordnet und jedes Unternehmen kann theoretisch einen eigenen KMS betreiben. Wenn Cisco Spark-Benutzer, die unterschiedlichen Unternehmen angehören, kommunizieren, müssen die Konversationsschlüssel dennoch von einem Benutzer an den anderen übermittelt werden. Um dies zu erreichen, nutzt Cisco einen Prozess, der als Federation bekannt ist. Viele der Schritte in einer Federation sind mit den Schritten im Abschnitt zur End-to-End-Verschlüsselung von Inhalten (oben) identisch. Es gibt jedoch einen entscheidenden Unterschied: Jeder Client kommuniziert nur mit einem verbundenen KMS, und in einem zusätzlichen Schritt kommunizieren die beiden KMS miteinander, um ihrerseits Schlüssel auszutauschen. Anders als bei herkömmlichen Konzepten von Federation erfordert der KMS-Verbund keine Konfiguration oder Einrichtung durch den Kunden oder Partner. Der Gesamtservice ist weiterhin ein Cloud-Modell, in dem jeder Benutzer mit anderen Benutzern weltweit kommunizieren kann.

Abbildung 3: Unternehmensübergreifende Kommunikation mit Spark



- Wenn ein Spark-Benutzer Inhalte zu einem Spark-Raum senden möchte, muss der Client des Benutzers (Client A) zuerst, wie in **(1)** in Abbildung 3 dargestellt, einen sicheren Kanal zwischen sich und dem zuständigen KMS (Unternehmen X) herstellen und daraufhin einen Konversationsschlüssel anfordern **(2)**. Wie zuvor erfolgt dies über einen sicheren Kanal **(1)** mithilfe eines authentifizierten vorübergehenden ECDH-Austauschs.
- Client A verschlüsselt daraufhin **(3)** den Inhalt mittels symmetrischer Verschlüsselung sowie dem Konversationsschlüssel und sendet ihn an die Spark-Cloud **(4)**.

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

- Die Spark-Cloud überprüft die Liste der Benutzer, die mit der in den Metadaten der Nachricht angegebenen Raum-ID verbunden sind (in diesem Fall ein Benutzer im Unternehmen Y), und Spark sendet die verschlüsselte Nachricht an den Client des Empfängers **(5)**. Die Nachricht ist noch verschlüsselt, wenn Client B sie erhält.
- Client B kontaktiert den KMS des Unternehmens Y, um einen Konversationsschlüssel für die empfangene Nachricht zu erhalten **(6, 7)**. Wenn der KMS des Unternehmens Y diese Anfrage erhält, überprüft er die URI des Konversationsschlüssels und stellt fest, dass der Schlüssel in einem Remote-KMS vorhanden ist. Daher stellt der KMS des Unternehmens Y einen wechselseitigen TLS-Kanal über den Core zum ursprünglichen KMS in Unternehmen X her **(8)**, um den Schlüssel anzufordern.
- Dieser wechselseitige TLS-Kanal wird über das jedem Unternehmens-KMS zugeordnete PKI-Zertifikat authentifiziert. Die PKI-Zertifikate müssen durch eine CA ausgestellt sein, die keine untergeordneten CA oder Zwischenzertifikate ausstellt.

Eine vollständige Liste der Zertifizierungsstellen finden Sie im Cisco Cloud Collaboration Management-Portal.

Diese Verbindung führt, wie alle Verbindungen in Spark, durch den Core, um Firewall-Anforderungen und die Anzahl der Gegenstellen zu minimieren. Sie wurde jedoch ebenfalls durchgängig verschlüsselt und ist somit für den Core nicht einsehbar – wie auch jede andere Kommunikation in Spark. Wenn der KMS des Unternehmens X diese Anfrage empfängt, überprüft er die Autorisierungsliste der Benutzer, die dem Spark-Raum zugeordnet sind, und findet dann heraus, dass tatsächlich ein Benutzer im Unternehmen Y über eine Autorisierung für den Zugriff auf diesen Raum verfügt.

Da der KMS des Unternehmens X nur für die Benutzer, die dem Unternehmen X zugeordnet sind, sichtbar ist, kann er keine Benutzer von Unternehmen Y authentifizieren. Deshalb muss er dem vom KMS des Unternehmens Y bereitgestellten PKI-Zertifikat vertrauen, um die abfragende Identität des KMS zum Unternehmen Y zuzuordnen.

- Der KMS des Unternehmens X überprüft, ob mindestens ein Benutzer von Unternehmen Y ein gültiger Teilnehmer im Raum ist, um die Schlüsselanforderung zu autorisieren**(9)**.
- Sobald der abfragende Unternehmens-KMS authentifiziert und die Autorisierungsprüfung ausgeführt wurde, gibt der KMS des Unternehmens X den angeforderten Konversationsschlüssel an den KMS des Unternehmens Y über den wechselseitigen TLS-Kanal zurück.
- Der KMS des Unternehmens Y speichert den Schlüssel in der lokalen Datenbank zwischen und führt dann eine Autorisierungsprüfung durch, um sicherzustellen, dass der anfordernde Client zu einem Benutzer gehört, der berechtigt ist, auf diesen Schlüssel zuzugreifen **(10)**.
- Sobald die Autorisierung erfolgreich war, übermittelt der KMS des Unternehmens Y den Konversationsschlüssel an Client B, sodass Client B die Nachricht entschlüsseln und lesen kann **(11)**.

Wenn ein einem Unternehmen zugeordneter Benutzer mit einem nicht zu einem Unternehmen zugeordneten Benutzer (zum Beispiel einem Fremium-Benutzer) kommunizieren möchte, läuft der Austausch gleichermaßen ab, mit dem einzigen Unterschied, dass einer der beiden betroffenen KMS von Cisco betrieben und verwaltet wird.

Nachvollziehbarkeit

Die Protokolle, die von Cisco Spark verwendet werden, einschließlich denen für die Schlüsselverwaltung, sind entweder bestehende Standards oder ausstehende Standards gemäß IETF oder W3C, wie in diesem Dokument angegeben. Diese Protokolle gewährleisten, wenn sie korrekt implementiert werden, die End-to-End-Sicherheit von Unternehmensinhalten. Während die Protokollebene vom Kunden einfach per Packet-Inspection überprüft werden kann, sind die internen Vorgänge der Security-Realm-Services nicht so einfach zu beobachten. Um dieses Blackbox-Problem zu beheben, können die Security-Realm-Services Prüfprotokolle erstellen, die mit der

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

Client-Nutzung und dem ausdrücklich gewährten Cloud-Zugriff verglichen werden können, um zu überprüfen, ob das System wie erwartet funktioniert. Darüber hinaus bietet Cisco jedem Unternehmenskunden Zugriff auf den Quellcode für die im Security-Realm enthaltenen Komponenten, um eine Inspektion, Kompilierung sowie einen binären Vergleich derselben Komponenten, die in binärer Form für die Bereitstellung zur Verfügung stehen, zu ermöglichen.

Echtzeit-Medienverschlüsselung

Alle Medien in Cisco Spark, darunter Sprache, Video und Desktop-Freigabe, werden mit dem Secure Real-Time Transport Protocol übertragen (SRTP, definiert in RFC 3711). Derzeit *entschlüsselt die Cisco Spark Cloud Echtzeitmedien für Mischung, Verteilung und PSTN-Trunking (Public Switched Telephone Network) und -Demarkation.*

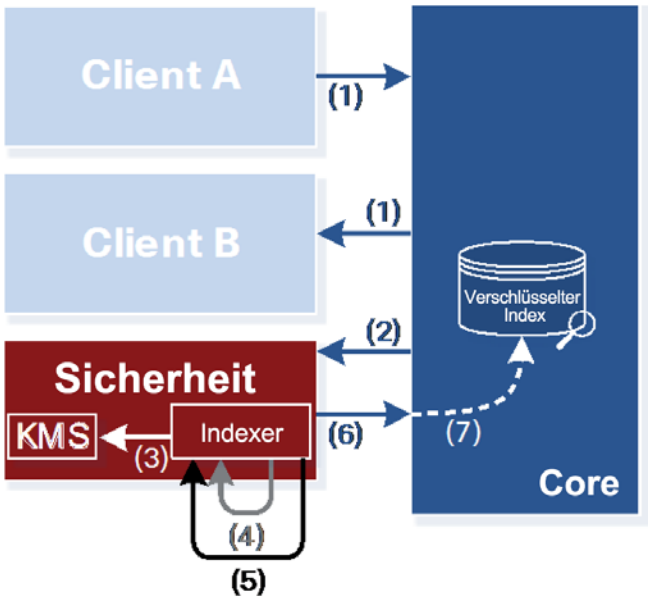
Um die Sicherheit des SRTP in Zukunft weiter zu steigern, engagiert sich Cisco zudem in der neuen PERC-Arbeitsgruppe (Privacy Enhanced RTP Conferencing) der IETF. Das Ziel von PERC besteht darin, Medien durchgängig zu verschlüsseln, wobei Hop-by-Hop-Authentifizierung auch weiterhin möglich bleiben soll. Mit Etablierung des neuen Standards nutzt Cisco Spark diese Verbesserung der Verschlüsselung von Echtzeitmedien, damit Schlüssel für die Verschlüsselung von Echtzeitmedien vom KMS unterstützt werden und die Cisco Spark Cloud PERC-kompatible Kommunikation nicht mehr entschlüsselt. PERC hat keine Auswirkungen auf die Entschlüsselung von PSTN-Anrufen, die für die absehbare Zukunft eine Cloud-Entschlüsselung durch den PSTN-Provider erfordern. Weitere Informationen zu PERC finden Sie unter https://datatracker.ietf.org/wg/perc.

Verschlüsselte Suche: sicher und schnell

Da der Spark Core Inhalte niemals unverschlüsselt sieht, könnte man annehmen, dass eine Nachrichtensuche in der Cloud nicht möglich sei. Cisco hat jedoch ein äußerst innovatives Verfahren entwickelt, das eine globale Nachrichtensuche ermöglicht, ohne dass im Core von Cisco Spark Entschlüsselungsfunktionen benötigt werden.

Dies geschieht mithilfe einer zusätzlichen Komponente im Security-Realm: dem Indexer. Genauso wie beim KMS besteht auch beim Indexer eine architektonische und operative Trennung vom Core. Dabei ist der Indexer jedoch fest mit dem KMS verknüpft. Er spielt eine entscheidende Rolle beim Aufbau und bei der Abfrage des Suchindex, also bei zwei grundlegenden Aufgaben, die zur Unterstützung einer globalen Nachrichtensuche nötig sind.

Abbildung 4: Reihenfolge der Nachrichtenindizierung



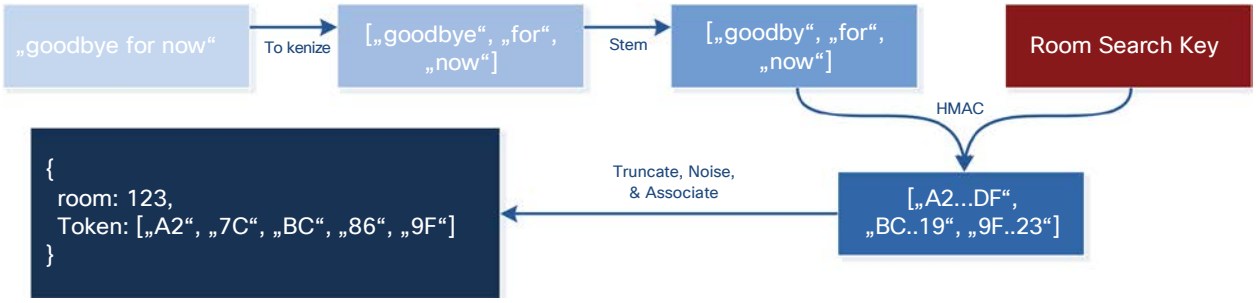
© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

Aufbau des Suchindex

Der erste Schritt besteht im Aufbau des Suchindex.

- Jedes Mal, wenn ein Benutzer in Spark eine Nachricht sendet, **(1)** wird die Nachricht in ihrer von Ende zu Ende verschlüsselten Form an den Indexer gesendet, wie in Abbildung 4 **(2)** gezeigt. Der Indexer fragt dann vom KMS den für die Entschlüsselung der Nachricht erforderlichen Konversationsschlüssel ab. Der Indexer ist ein SparkBot[4], der per Unternehmensrichtlinie in jedem Raum eingeladen ist, um bei Suchvorgängen zu helfen.
- Der KMS übergibt dem Indexer den passenden Konversationsschlüssel, da der Indexer ein aktiver Teilnehmer des Raumes ist, der zur Entschlüsselung der Ressourcen des Raumes berechtigt ist **(3)**.
- Der Indexer entschlüsselt die Nachricht und trennt sie in die einzelnen Wörter auf, aus der sie besteht **(4)**.
- Der Indexer wendet dann einen kryptografischen Einweg-Hash auf jedes Wort oder jeden Wortstamm an. Dabei handelt es sich um einen speziellen Suchschlüssel, der im KMS gespeichert und für Raum[5] **(5)** spezifisch ist. Beispielsweise würde „goodbye for now“ in „goodbye“, „for“ und „now“ aufgeteilt und jedes Wort mit einem Hash versehen. Das Ergebnis ist eine Liste von mit Hash versehenden Wörtern, die alle zu dem Raum gehören, in dem die Nachricht gepostet wurde. Die Hashes sind im Grunde eine Einwegverschlüsselung – ein bestimmter Hash kann nicht in das Wort der ursprünglichen Nachricht zurück geändert werden. Der Indexer fügt dieser Liste einige zufällige Hashes mit „Rauschen“ hinzu, um sicherzustellen, dass die Nachrichten des Raumes nicht durch eine Häufigkeitsanalyse entschlüsselt werden können. (Da Wörter wie „and“ und „the“ im Englischen häufig auftreten, stellt das Hinzufügen von Rauschen sicher, dass die Hashes im Raum nicht dieselbe Häufigkeitsverteilung aufweisen.)
- Im abschließenden Schritt sendet der Indexer diese Liste mit Hashes an die Spark Cloud **(6)**, wo sie im Suchindex verschlüsselt gespeichert werden **(7)**. Hierdurch verfügt Spark Cloud über einen verschlüsselten Index aller Worte in allen Nachrichten, die den Räumen zugeordnet sind, und der von der Spark Cloud nicht entschlüsselt werden kann.

Abbildung 5: Ablaufdiagramm des Nachrichtenindex



Abfrage des Suchindex

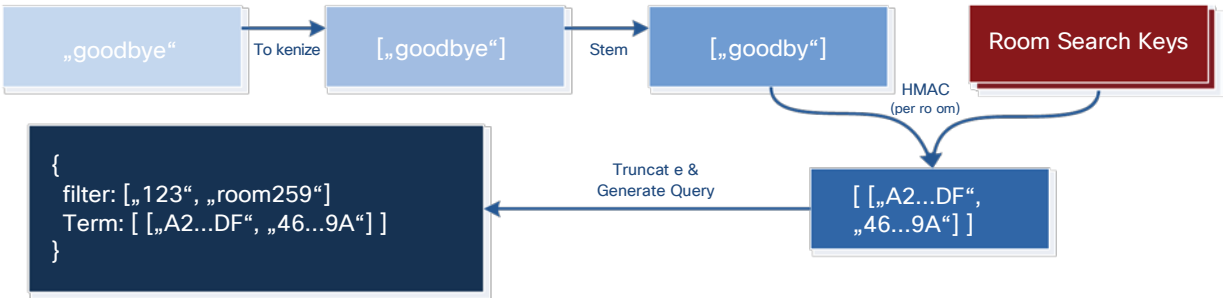
Wenn ein Benutzer eine Suche durchführt, interagiert der Client mit dem Indexer, als ob der Benutzer eine private Konversation mit dem Indexer hätte. Das bedeutet, dass die gesamte zuvor für Konversationen unter Benutzern beschriebene End-to-End-Verschlüsselung auch für die Abfragen des Indexers durch den Benutzer verwendet wird.

[4] Siehe *Integrationen und Erweiterbarkeit* weiter unten.
[5] Verwendet auf 80 Bit gekürzte SHA-256-HMACs.

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

Zudem wird die Suchanfrage zuerst auf dem Client des Benutzers mit einem End-to-End-Schlüssel verschlüsselt, der speziell zur Verschlüsselung der Kommunikation zwischen dem Client des Benutzers und dem Indexer dient. Jeder Benutzer ist einem spezifischen Indexer zugeordnet. Der Client des Benutzers sendet die verschlüsselte Abfrage an die Spark Cloud, die die verschlüsselte Abfrage zum Indexer zusammen mit der Liste der Räume weiterleitet, für die der Benutzer eine Zugriffsberechtigung hat. Die Spark Cloud kann die Suchanfrage nicht entschlüsseln, da sie mit einem Schlüssel verschlüsselt ist, auf den sie nicht zugreifen kann. Hierbei handelt es sich um den End-to-End-Konversationsschlüssel für die Konversation dieses bestimmten Clients mit dem Indexer.

Abbildung 6: Ablaufdiagramm der Suche



Der Indexer führt dann dieselben Schritte wie bei der Erstellung des Suchindex aus: Er teilt die Abfrage in Worte und Wortstämme auf und versieht sie dann jeweils mit dem Suchschlüssel der Räume, zu denen der Benutzer Zugriff hat, mit einem Hash. Wenn also ein Benutzer, der 10 Räumen zugeordnet ist, eine Suchanfrage mit zwei Wörtern eingibt, generiert der Indexer mindestens 20 mit Hash versehene Suchbegriffe und möglicherweise zahlreiche mehr. Dies hängt davon ab, wie viele Wortstämme die jeweiligen Wörter haben. Der Indexer sendet dann diese Liste der mit Hash versehenen Suchbegriffe an die Spark Cloud.

Der Spark Core kann dann den Suchindex nach Übereinstimmungen durchsuchen. Wenn er im Suchindex Räume findet, die einem der vom Indexer empfangenen Hashes zugeordnet sind, erstellt er eine Liste, die an den Client des Benutzers zurückgesendet wird. Dieser kombiniert die Ergebnisse mit den zugeordneten Konversationsschlüsseln, die er entweder aus seinem Cache oder vom KMS abruft, und zeigt dann die Suchergebnisse dem Benutzer an.

Das Beste beider Welten

Die Suchfunktion in Spark ist mit keinerlei Beeinträchtigungen in Bezug auf Sicherheit oder Benutzer. Obwohl eine einzige Suche die Generierung und den Vergleich von mehreren Tausend mit Hash versehender Suchbegriffe umfassen kann, ist die Suche mit Spark genauso schnell wie bei gängigen Internet-Suchmaschinen.

Integrationen und Erweiterbarkeit

Die Cisco Spark und die Spark Cloud bieten zwar bereits herausragende Funktionen für die Zusammenarbeit, unsere Partner und Kunden legen jedoch Wert darauf, dass sie unsere Angebote anpassen und erweitern können. Dazu bieten wir APIs, die einfach zu erlernen und zu verwenden sind. Entwickler möchten, dass APIs umfassend und dennoch einfach sind, damit sie sich auf ihre eigene Anwendungen statt auf die Komplexität einer Plattform konzentrieren können. Wir haben erhebliche Anstrengungen unternommen, um unsere APIs intuitiv zu gestalten und die Komplexität der zugrunde liegenden Plattform zu entfernen.

Obwohl der Core von Cisco Spark Cloud niemals Zugriff auf Inhalte hat, ist uns bewusst, dass Entwickler, Partner und Kunden die Plattform auf Arten und Weisen erweitern wollen, für die ein Zugriff auf Inhalte erforderlich ist. Daher befinden sich Erweiterungen der Cisco Spark Cloud außerhalb des Core und müssen explizit von einem Kunden oder Benutzer aktiviert werden. Da sie sich außerhalb der Cisco Spark Cloud befinden, können Kunden wählen, wo sie ihre Plattformerweiterungen implementieren möchten, von wem sie verwaltet werden sollen und auf

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

welche Ressourcen sie Zugriff haben sollen. Integrationen und Erweiterungen für Cisco Spark benötigen auf dieselbe Weise Zugriff auf Verschlüsselungsschlüssel, wie im Abschnitt „Schlüsselzugriff von Funktionen“ beschrieben.

Cisco Spark definiert aktuell drei Kategorien von Integrationen: Bots, Apps und Webhooks. Wir gehen aber davon aus, dass Kunden und Drittanbieter die Plattform noch um äußerst Innovative Funktionen erweitern werden. Weitere Informationen zu den APIs für Cisco Spark finden Sie unter https://developer.ciscospark.com.

Bots

Bots stellen erweiterte Funktionen für das gesamte Unternehmen wie beispielsweise einen Dienst für die Anrufaufzeichnung zur Verfügung. Bots müssen die Räume, auf die sie Zugriff benötigen, entweder selber erstellen oder in diese eingeladen werden. Einladungen in einen Raum können durch eine Unternehmensrichtlinie oder einen Benutzer erfolgen, der sich bereits im Raum befindet.

Apps

Apps erweitern das Funktionsspektrum für Einzelnutzer und fungieren beispielsweise als persönlicher Assistent oder Dokumentenübersetzer. In vielerlei Hinsicht kann eine App als ein von der Cloud oder vom Server gehosteter Client ohne Benutzeroberfläche betrachtet werden. Apps haben Zugriff auf alle Räume, auf die der zugeordnete Benutzer Zugriff hat. Die App kann aber auch nutzerseitig aus bestimmten Räumen ausgeschlossen werden.

Webhooks

Webhooks bieten per Einzel-URL Zugriff auf vereinfachte Core-Funktionen, wie das Posten von Inhalten in einem Raum oder Benachrichtigungen über neue Inhalte. Webhooks können sich insofern ähnlich wie Bots und Apps verhalten, als sie wie ein Bot über eine eigene Identität verfügen oder wie eine App die Identität eines Benutzers mitverwenden können. Webhooks erzielen die Einfachheit von Einzel-URLs, indem sie langlebige OAuth2-Zugriffstoken mit beschränktem Geltungsbereich in den URL-Abfrage-String einbetten und die gesamte Ver- und Entschlüsselung der Inhalte innerhalb des Webhook-Workers ausführen. In jedem Fall ist der Geltungsbereich von Webhooks auf eine einzelne Ressource (z. B. einen Raum) begrenzt. Diese Einschränkungen des Geltungsbereichs für den Zugriff werden konfiguriert und festgeschrieben, wenn ein Webhook hinzugefügt wird.

Wahlfreiheit für Unternehmen und Benutzer

Cisco hat den Anspruch, Spark zu einer der führenden Lösungen der Branche zu machen. Wahlfreiheit für Kunden ist der Schlüssel zum Erfolg dieses Hybridmodells. Kunden können wählen, ob sie nur den Core verwenden oder den Core mit Bots, Apps und Webhooks erweitern. Unternehmen können eine Richtlinie definieren, die spezifische Bots und Apps ermöglicht, und Benutzer können im Rahmen dieser Richtlinie Apps auswählen. Die Plattform von Cisco Spark wurde um gut dokumentierte und standardbasierte APIs herum entwickelt. Hierdurch können Komponenten außerhalb des Core (einschließlich Bots, Apps und Webhooks) von Drittanbietern bezogen oder selber erstellt werden.

Certificate Pinning

Die Kommunikation des Spark-Client mit dem Core erfolgt über eine TLS-verschlüsselte Verbindung. Clients verwenden eine als *Certificate Pinning* bezeichnete Technik, um sicherzustellen, dass die Kommunikation während der Übertragung nicht abgefangen, mitgelesen oder verändert wird. Cisco bindet Serverzertifikate an einige wenige Root-CAs, die sich dazu verpflichtet haben, keine Zwischenzertifikate auszustellen – und zwar sowohl im Certification Practice Statement des Ausstellers als auch durch die Aufnahme des Felds „pathLenConstraint“ mit der Einstellung null (0) in die Erweiterung „BasicConstraints“ im Stammzertifikat, um anzuzeigen, dass dem ausgestellten Zertifikat in einem Zertifizierungspfad keine CA-Zertifikate folgen dürfen.

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

Datenschutz

Unser Versprechen, einen sicheren und zuverlässigen Service bereitzustellen beschränkt sich dabei nicht allein auf den Schutz von Benutzerinhalten. Spark schützt alle Benutzer- und Nutzungsdaten mit einer Kombination aus Datenschutz-Tools und Merkmalen wie Identitätsverschleierung, fein abgestuften Administratorrollen, Wahlfreiheit für Unternehmen und Benutzer sowie Transparenz. Wie bei der End-to-End-Verschlüsselung haben wir diese Schutzmechanismen von Anfang an in den Service integriert.

Identitätsverschleierung

Für Collaboration-Services ist ein umfassendes Konzept für den Umgang mit Benutzeridentitäten entscheidend. Benutzer möchten sich schnell mit Mitgliedern ihrer Teams verbinden, andere Benutzer nach Name, E-Mail-Adresse oder Telefonnummer suchen und deren Identität anhand von Profilfotos bestätigen können. Gleichzeitig können Informationen zur Benutzeridentität sowohl aus Sicht des Benutzers als auch aus Sicht des Unternehmens sicherheitsempfindlich sein. Ihre Offenlegung ausschließlich auf Kontexte zu beschränken, in denen diese erforderlich ist, ist ein grundlegendes Prinzip von Spark.

Um die Offenlegung von Informationen zur Benutzeridentität einzuschränken unterscheiden wir in der Spark Cloud zwischen der „echten“ und der „verschleierten“ Identität. Die Daten, die wir im Rahmen der Benutzerregistrierung erfassen (Benutzername, E-Mail-Adresse, Telefonnummer usw.), gelten als „echte Identität“ und werden im Profil des Benutzers in einer Komponente von Spark Cloud mit dem Namen „Common Identity“ gespeichert. Für jeden Benutzer generieren wir auch einen zufälligen UUID (Universally Unique Identifier) mit 128 Bit, der als verschleierte Identität des Benutzers dient. Entsprechend verwenden wir für Unternehmen eine per Zufallsgenerator erstellte „Unternehmens-ID“ mit 128 Bit als verschleierte Identität des jeweiligen Unternehmens. Innerhalb des Spark-Service verwenden wir verschleierte Identität wo immer möglich. Dies umfasst Folgendes:

- **Nachrichten-Routing:** Alle Nachrichten werden in Spark ausschließlich auf Grundlage der verschleierten Identität vom Absender an den Empfänger geroutet. Alle Cloud-internen Abfragen, die sich auf einzelne Benutzer beziehen, basieren ebenfalls auf der verschleierten Identität. Dies gilt beispielsweise für sämtliche oben beschriebenen Interaktionen zwischen dem KMS und dem Indexer.
- **Serverseitige Protokollierung:** Alle Protokolle, die von Anwendungskomponenten von der Spark Cloud zu Zwecken der Fehlerbehebung generiert werden, verwenden die verschleierte Identität.
- **Analytik:** Spark arbeitet mit einem DevOps-Modell und unser Entwicklungsteam entscheidet mithilfe von Analysen der Leistungs- und Nutzungsdaten darüber, wie der Service verbessert werden kann. Das Team trifft diese Entscheidungen anhand von Analysen der Nutzungsprotokolle von Spark, die die verschleierte Identität verwenden.

Wenn es aber erforderlich ist, die Identität eines Benutzers oder Unternehmens in einem Spark-Client, dem Cisco Cloud Collaboration Management-Portal oder einer Integration eines Drittanbieters wiederzugeben, gibt es für autorisierte Clients und Cloud-Servicekomponenten selbstverständlich eine Möglichkeit zum Zugriff auf die echte Identität. Immer wenn ein Spark-Client, eine Cloud-Komponente, eine App oder ein Bot diesen Zugriff benötigt, erfolgt eine Authentifizierung bei der Komponente Common Identity, die Informationen über die echte Identität nur autorisierten Anforderern bereitstellt.

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

Feinstufig festlegbare Administratorrollen

Jeder Kunde und Partner mit Spark hat Zugriff auf das Cisco Cloud Collaboration Management-Portal, das umfassendes Management ermöglicht. Zur Verfügung stehen Testfunktionen, Erwerb, Kontenkonfiguration, Konteneinstellungen, Unterstützung bei der Einführung, Kundensupport und API-Nutzung durch Entwickler. Da uns bewusst ist, dass es für diese Funktionen erforderlich sein kann, auf vertrauliche Information über Benutzer und Konten, Produktnutzung und Konfigurationsdaten zuzugreifen, haben wir das Portal so gestaltet, dass es diverse verschiedene Administratorrollen mit Zugriff auf unterschiedliche Teilmengen der Informationen unterstützt. Beispielsweise können Administratoren für den Support auf Benutzerinformationen und Supportprotokolle zugreifen, während der Zugriff von Partner-Administratoren für den Vertrieb stärker beschränkt und auf das Zusammentragen von Nutzungsberichten sowie das Management Servicetests konzentriert ist. Volladministratoren haben Zugriff auf alle Funktionen des Portals und können anderen Administratoren in ihren Unternehmen die entsprechenden Rollen zuordnen.

Wir bieten diese Rollen Partnern und Kunden an, aber wir nutzen sie auch selbst, um den Zugriff ausschließlich auf die Cisco Administratoren zu begrenzen, die ihn benötigen. Während unsere Administratoren und Techniker im Bereich Support auf Supportprotokolle und Benutzerinformationen zugreifen können, um Kunden und Partnern bei der Fehlerbehebung unterstützen zu können, haben unsere Mitarbeiter in den Bereichen Vertrieb und Kundenbetreuung in Verbindung mit der Rolle des Administrators im Bereich Vertrieb nur begrenzten Zugriff.

Wahlfreiheit für Unternehmen und Benutzer

Spark bietet Benutzern und Unternehmen verschiedene Optionen beim Datenschutz, ohne dass dabei komplizierte Konfigurationsschnittstellen erforderlich sind. Zu den Optionen für Unternehmensadministratoren gehören:

- **Single Sign-On (SSO):** Administratoren können Spark für die Arbeit mit ihren vorhandenen SSO-Lösungen konfigurieren. Wir unterstützen Identitäts-Provider, die SAML 2.0 (Security Assertion Markup Language) und OAuth 2.0 verwenden.
- **Verzeichnissynchronisierung:** Administratoren können Änderungen des Lebenszyklus von Mitarbeitern in Spark in Echtzeit wiedergeben lassen, wenn sie Microsoft Active Directory verwenden.
- **Datenweitergabe an Cisco Partner:** Unternehmen können wählen, ob sie Daten zur Servicequalität und Projektdaten an ihre Cisco Partner weitergeben möchten, um ein höheres Maß an Partnersupport zu ermöglichen.

Zu den Optionen für Benutzer gehören:

- **Geräteberechtigungen:** Abhängig davon, auf welcher mobilen oder Browser-Plattform der Benutzer Spark ausführt, fordert Spark verschiedene Geräteberechtigungen für beispielsweise Telefon, Mikrofon, Kamera, Audioaufzeichnung, Bildschirmfreigabe, Kalender, Kontakte, Dateien und Fotos sowie Push-Benachrichtigungen an. Bei den meisten Plattformen ist hierfür eine ausdrückliche Genehmigung erforderlich, die der Benutzer jederzeit widerrufen kann.
- **Proximity-Funktionen:** Auf Mobilgeräten können Spark-Clients sich automatisch mit Cisco Sprach- und Video-Endpunkten verbinden, indem sie nach Ultraschallsignalen suchen, wenn der Spark-Client aktiv ist. Da hierfür das Mikrofon des Geräts verwendet werden muss, können Benutzer diese Funktion nach Wunsch deaktivieren.
- **Profilfotos:** Profilfotos sind für die Verwendung von Spark nicht erforderlich.

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

- **Anzeigen für externe Teilnehmer:** Cisco Spark-Clients zeigen den Benutzern mit visuellen Anzeigen deutlich an, wenn sich in einem Raum Teilnehmer befinden, die nicht ihrem Unternehmen angehören.
- **Kontrolle durch Raummoderatoren:** Benutzer können Räume moderieren, was die Ernennung ausgewählter Teilnehmer zu Moderatoren ermöglicht, die die exklusive Kontrolle über den Namen und die Teilnehmerliste des Raumes haben.

Transparenz

Wir möchten dass unsere Benutzer und Kunden verstehen, welche Optionen sie haben und wie wir die Daten, die sie Cisco anvertrauen, verwalten und schützen. Um dieses zu ermöglichen, verwenden wir ein mehrschichtiges Modell für die Transparenz. Wir stellen kurze Offenlegungen bereit, die Benutzer bei Echtzeitentscheidungen innerhalb des Spark-Client unterstützen. Weitere Informationen finden Sie auf unseren Supportseiten, die wir regelmäßig aktualisieren. Und für alle Informationen dazu, welche Daten wir erfassen, wie wir sie verwenden und wie wir sie schützen, verweisen wir auf die Cisco Online-Datenschutzerklärung mit einer speziellen Ergänzung für den Datenschutz in Spark.

Sicherheit von Plattform und Services

Zusätzlich zum Cisco Secure Development Lifecycle führt Cisco Spark häufige interne und externe, Whitebox-, Blackbox- und Penetrationstests für die Spark-Plattform und -Services durch. Weitere Informationen zum Cisco Secure Development Lifecycle finden Sie unter: https://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle.html

Incident-Management und Sicherheitsrichtlinien

Cisco Product Security Incident Response

Das Cisco Product Security Incident Response Team (PSIRT) ist für die Bearbeitung von Sicherheitsvorfällen bei Cisco Produkten verantwortlich. Das Cisco PSIRT-Team ist ein dediziertes globales Team, das den Eingang, die Untersuchung und die Veröffentlichung von Informationen zu Sicherheitslücken bei Cisco Produkten und Netzwerken verwaltet. Cisco PSIRT arbeitet rund um die Uhr mit Cisco Kunden, unabhängigen Security-Experten, Beratern, Branchenunternehmen und anderen Anbietern zusammen, um potenzielle Sicherheitsprobleme bei Cisco Produkten und Netzwerken zu identifizieren.

Berichterstellung und Support bei einer mutmaßlichen Sicherheitslücke

Einzelpersonen oder Unternehmen, die bei einem Produkt auf ein Sicherheitsproblem stoßen, wird unbedingt empfohlen, sich mit Cisco PSIRT in Verbindung zu setzen. Berichte von unabhängigen Experten, Branchenunternehmen, Anbietern, Kunden und anderen Quellen, die sich mit der Produkt- oder Netzwerksicherheit beschäftigen, sind bei Cisco stets willkommen. Wenden Sie sich über eine der folgenden Möglichkeiten an Cisco PSIRT:

	Notfall-Support
Telefon	+1 877 228 7302 (innerhalb von Nordamerika gebührenfrei); +1 408 525 6532 (internationale Direktwahl)
Erreichbarkeit	Rund um die Uhr, 7 Tage die Woche
	Support bei weniger dringenden Problemen
E-Mail	psirt@cisco.com
Erreichbarkeit	Support-Anfragen per E-Mail werden in der Regel innerhalb von 48 Stunden bestätigt.

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

Weitere Informationen finden Sie unter http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Transparenz und Strafverfolgungsanfragen bezüglich Kundendaten

Cisco verpflichtet sich zur Veröffentlichung von Daten bei Anfragen oder Forderungen bezüglich Kundendaten von Strafverfolgungsbehörden und Sicherheitsbehörden weltweit. Wir veröffentlichen diese Daten zweimal jährlich (die Berichtszeiträume umfassen Januar bis Juni bzw. Juli bis Dezember). Wie andere Technologieanbieter auch veröffentlichen wir diese Daten sechs Monate nach dem Ende eines bestimmten Berichtszeitraums gemäß den zeitlichen Einschränkungen dieser Berichte. Weitere Informationen finden Sie unter http://www.cisco.com/web/about/doing_business/trust-center/transparency-report.html

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter **http://www.cisco.com/go/offices**.

Cisco und das Cisco Logo sind Marken bzw. eingetragene Marken von Cisco Systems, Inc. und/oder Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Cisco Marken finden Sie unter www.cisco.com/go/trademarks. Die genannten Marken anderer Anbieter sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1110R)

COLLAB-SPARK-0616

© 2016 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.