Funkcje bezpieczeństwa i ochrona prywatności w rozwiązaniu Cisco Spark

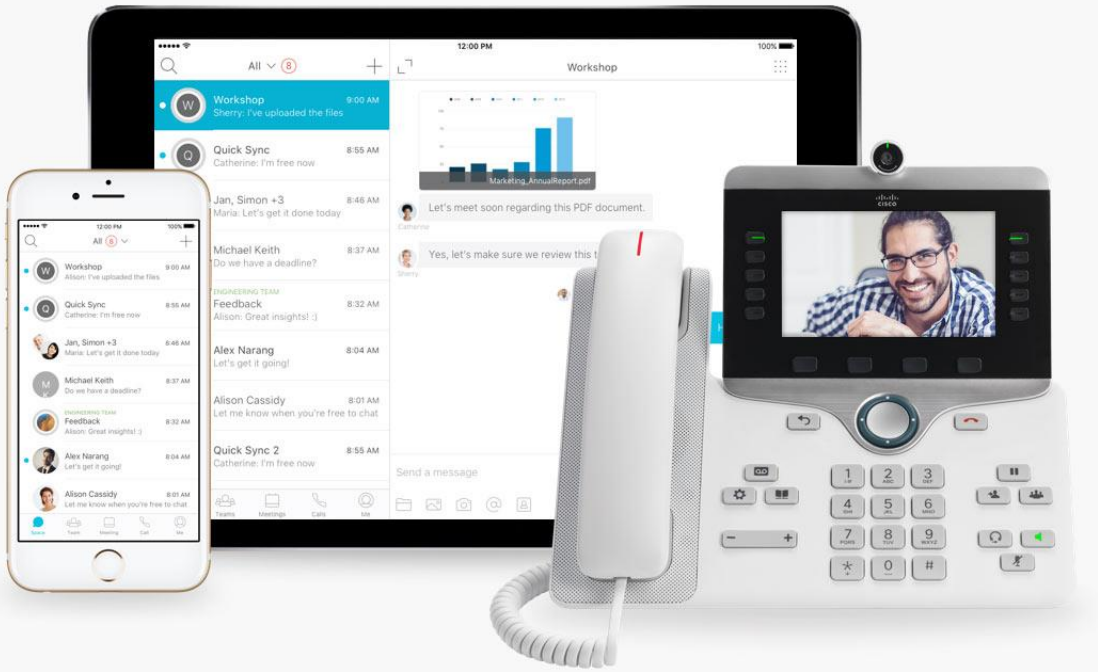
Cisco® Spark to platforma współpracy działająca w chmurze, która zapewnia funkcje przesyłania wiadomości, telefoniczne i konferencyjne. W ramach rozwiązania Cisco Spark® dostępna jest aplikacja kliencka, która łączy się z tą platformą i zapewnia kompleksowy zestaw narzędzi wspomagających pracę zespołową. Użytkownicy mogą wysyłać widomości, dzielić się plikami i spotykać z innymi zespołami, wszystko z poziomu jednego rozwiązania.

W niniejszym dokumencie opisano funkcje bezpieczeństwa i ochrony prywatności rozwiązań Cisco Spark Cloud i Cisco Spark Messaging.

Produkty, usługi i funkcje firmy Cisco opisane w niniejszym dokumencie znajdują się na różnych stadiach rozwoju. Część z nich jest aktualnie dostępnych, inne mogą znajdować się w fazie rozwojowej lub być planowane w przyszłości. Dodatkowe informacje można znaleźć na stronie: www.cisco.com.

Firma Cisco nie ponosi odpowiedzialności za opóźnienia lub uchybienia w dostarczaniu produktów, usług lub funkcji określonych w niniejszym dokumencie.

Spis treści



Wyzwania związane z bezpieczeństwem i prywatnością spotykane w rozwiązaniach do współpracy działających w chmurze

Jedną z kluczowych korzyści oferowanych przedsiębiorstwom korzystającym z usług działających w chmurze jest możliwość praktycznie natychmiastowego korzystania z najnowszych wartościowych funkcji i funkcjonalności wdrożonych przez dostawcę usługi. Ale w przypadku wielu dostawców tzw. usług Cloud te wartościowe funkcjonalności często wiążą się z posiadaniem pełnego dostępu do zasobów i danych użytkownika. W przypadku aplikacji służących do współpracy zespołowej większość dostawców usług cloud ma bezpośredni dostęp do wiadomości, połączeń i treści prezentowanych na spotkaniach, dzięki czemu mogą zaoferować funkcjonalności takie jak wyszukiwanie widomości, transkodowanie treści czy integracja z aplikacjami innych producentów. Z kolei nowoczesne konsumenckie usługi do współpracy pracowników są nastawione na ochronę prywatności danych oferując pełne szyfrowanie komunikacji (ang. end-to-end) kosztem dodatkowych funkcjonalności.

Rozwiązanie Cisco Spark łączy najlepsze elementy z tych dwóch światów: w pełni szyfrowaną platformę do współpracy w chmurze oraz możliwość wyboru integracji z produktami Cisco i innymi aplikacjami. Cisco Spark wykorzystuje otwartą architekturę dla bezpiecznej dystrybucji kluczy szyfrujących, pozwalając przedsiębiorstwom na uzyskanie wyłącznej kontroli nad procesem zarządzania posiadanymi kluczami szyfrującymi oraz poufnością ich danych. Oznacza to, że treści są szyfrowane na poziomie aplikacji klienckiej użytkownika i pozostają zaszyfrowane dopóki nie dotrą do odbiorcy, bez udziału elementów pośredniczących mających dostęp do kluczy deszyfrujących treść, chyba że przedsiębiorstwo jednoznacznie wyrazi zgodę na udzielenie takiego dostępu.

Pomimo tego, że przyznając bezpośredni dostęp do kluczy mogą Państwo uzyskać dodatkowe funkcjonalności, wbudowaliśmy także pełne szyfrowanie w samą strukturę rozwiązania Spark, co oznacza, że wiele wartościowych funkcji i funkcjonalności operuje w oparciu o szyfrowane dane. Stosując innowacyjne indeksowanie wiadomości, modele pozwoleń, przepływy uwierzytelnień,

szyfrowanie oraz modele wdrożeń, Spark wspiera funkcje takie jak globalne wyszukiwanie treści, które nie są deszyfrowane w chmurze Cisco Spark.

Większość dostawców usług cloud twierdzi, że ich rozwiązania są bezpieczne, ponieważ szyfrują dane przesyłane pomiędzy urządzeniami użytkowników a swoimi serwerami, lub pomiędzy ich własnymi centrami danych. Ale szyfrowanie w trakcie przesyłania danych nie pozwala chronić danych użytkownika przed ich ujawnieniem dostawcy usług cloud. Wszystkie połączenia z i do chmury Spark są szyfrowane w trakcie przesyłania danych – ale oferujemy znaczenie więcej, ponieważ mamy dostęp do treści użytkownika, tylko gdy uzyskaliśmy jego wyraźną zgodę.

Nasze zobowiązanie do dostarczania godnej zaufania oferty usług nie ogranicza się do ochrony treści użytkownika. Spark zabezpiecza wszystkie dane o użytkownikach stosując połączenie narzędzi do ochrony prywatności i funkcje, które obejmują zaciemnianie tożsamości[1], możliwość wyboru oraz przejrzystość. Podobnie jak w przypadku pełnego szyfrowania, wbudowaliśmy te elementy u podstaw naszej usługi.

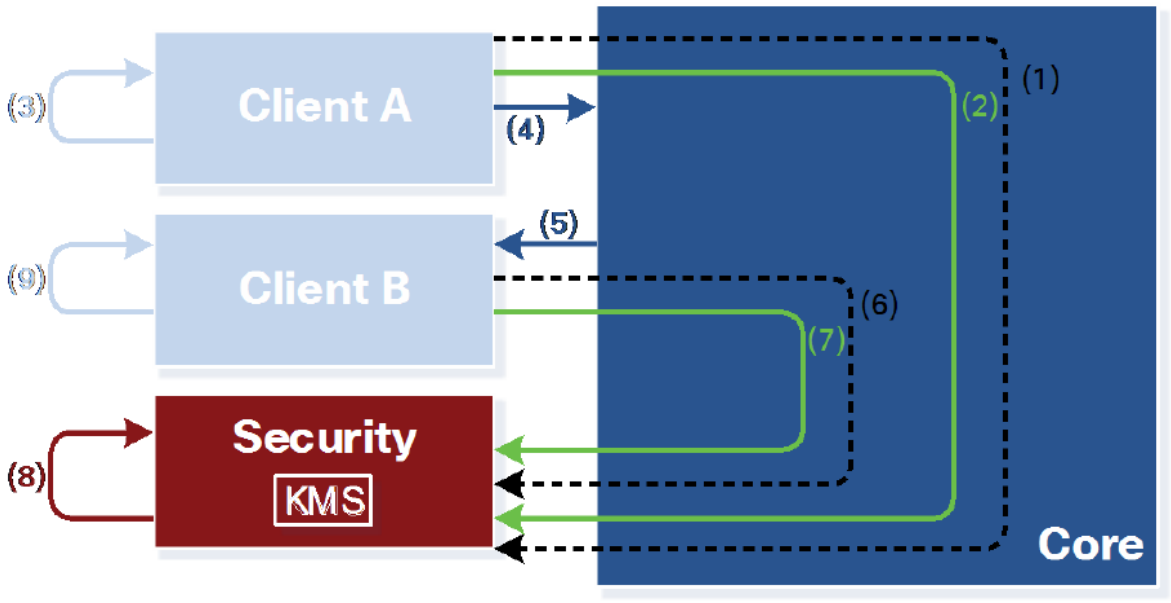
[1] Więcej informacji w rozdziale „Zaciemnianie tożsamości”.

Pełne szyfrowanie treści (ang. end-to-end)

Podstawowym elementem pełnego procesu szyfrowania treści w rozwiązaniu Cisco Spark Cloud jest serwer zarządzania kluczami KMS (Key Management Server). Serwer KMS jest odpowiedzialny za tworzenie, zapisywanie i autoryzowanie kluczy szyfrujących oraz zapewnianie do nich dostępu. Są one stosowane przez aplikacje klienckie Spark do szyfrowania i deszyfrowania wiadomości oraz plików. Pełne szyfrowanie jest możliwe w ramach Spark z uwagi na architekturalny i operacyjny rozdział pomiędzy KMS a pozostałymi usługami Spark Cloud. Należy je traktować jak by znajdowały się w odrębnych domenach w chmurze: KMS znajduje się w tzw. domenie bezpieczeństwa (ang. Security Realm), a wszystkie pozostałe usługi składające się na Spark są umieszczone w rdzeniu (ang. Core).

Komunikacja z KMS przechodzi przez Cisco Spark Cloud, ale jest także w pełni szyfrowana, tym samym nie może być odczytana przez rdzeń i jest uwierzytelniana przy pomocy tokenów dostępu (ang. access token) nie używanych nigdzie indziej w ramach Cisco Spark Cloud. Ten model zapewnia odpowiedni dostęp do kluczy szyfrujących, jednocześnie gwarantując, że żadne usługi rdzeniowe nie mają dostępu do tej komunikacji lub kluczy przechowywanych przez KMS. W rozwiązaniu Cisco usługi znajdujące się w domenie bezpieczeństwa działają w ramach odrębnej infrastruktury jako oddzielny użytkownik chmury. Przedsiębiorstwa zwracające szczególną uwagę na kwestie bezpieczeństwa mogą wybrać wdrożenie usług domeny bezpieczeństwa wraz z KMS, w ich lokalnych sieciach, szczegóły są opisane w następnym rozdziale.

W momencie, gdy użytkownik Spark chce wysłać jakieś treści do pomieszczenia, w którym działa rozwiązanie Spark, wówczas aplikacja kliencka tego użytkownika musi w pierwszej kolejności ustanowić bezpieczny kanał połączeniowy z KMS – relacja (1) na Rys. 1. Aby ustanowić współdzielony klucz dla bezpiecznego kanału połączeniowego pomiędzy Klientem a KMS, Klient i KMS korzystają z mechanizmu wymiany kluczy efemerycznych ECDH (Elliptic Curve Diffie– Hellman). W wyniku tego procesu powstaje symetryczny współdzielony klucz, który może być stosowany do bezpiecznej wymiany wiadomości.



Rys. 1. Komunikacja pomiędzy klientem a KMS w ramach Cisco Spark

Uwierzytelnianie w ramach tego kanału jest konieczne, by mieć pewność, że ani Cisco ani inny podmiot nie może podglądać lub modyfikować informacji i kluczy, które są przesyłane tym kanałem i stanowi również ochronę przed działaniami typu man-in-the-middle. Mechanizm uwierzytelniania wykorzystuje certyfikat infrastruktury klucza publicznego PKI w KMS, zawierający wpisy CN (Common Name) lub SAN (Subject Alternative Names) odpowiadające nazwie domeny organizacji. Klienci szyfrują swoją połowę klucza ECDH do komunikacji z KMS stosując publiczną część certyfikatu serwera KMS. Odpowiedzi ECDH z KMS są podpisane przy pomocy prywatnej części certyfikatu serwera KMS2. Jest to niewielka modyfikacja w stosunku do mechanizmu ECDHE-RSA, gdzie klient przeprowadza szyfrowanie z wykorzystaniem publicznego certyfikatu serwera, zamiast podpisywać się własnym kluczem, co oznacza, że klienci nie potrzebują certyfikatów. Jednakże oznacza to oczywiście, że klienci muszą mieć możliwości uwierzytelnienia certyfikatu KMS. Aby to zrealizować, certyfikaty KMS muszą albo wykorzystać publiczne urzędy certyfikacji CA (ang. Certificate Authority), które są szeroko stosowane na komputerach osobistych i urządzeniach mobilnych, albo przedsiębiorstwa muszą mieć możliwość wysyłania ich prywatnego głównego certyfikatu CA do urządzeń końcowych, które będą stosowane przez ich użytkowników do komunikacji z Cisco Spark. Kierowanie prywatnych certyfikatów CA do klientów nie jest obsługiwane przez Cisco Spark, ale klienci Cisco Spark wykorzystują dowolny certyfikat, który znajduje się w ich bazie zaufanych certyfikatów.

Gdy Klient i KMS uzgodnili symetryczny klucz przy pomocy uwierzytelnionego mechanizmu ECDH, wówczas Klient wykorzystuje ten kanał by wnioskować o nowy klucz szyfrujący przeznaczony specjalnie do szyfrowania treści kierowanych do danego pomieszczenia z aplikacją Spark oraz osób w nim przebywającym, relacja (2) na powyższym rysunku. Ten klucz jest określany jak tzw. klucz konwersacji (ang. conversation key).

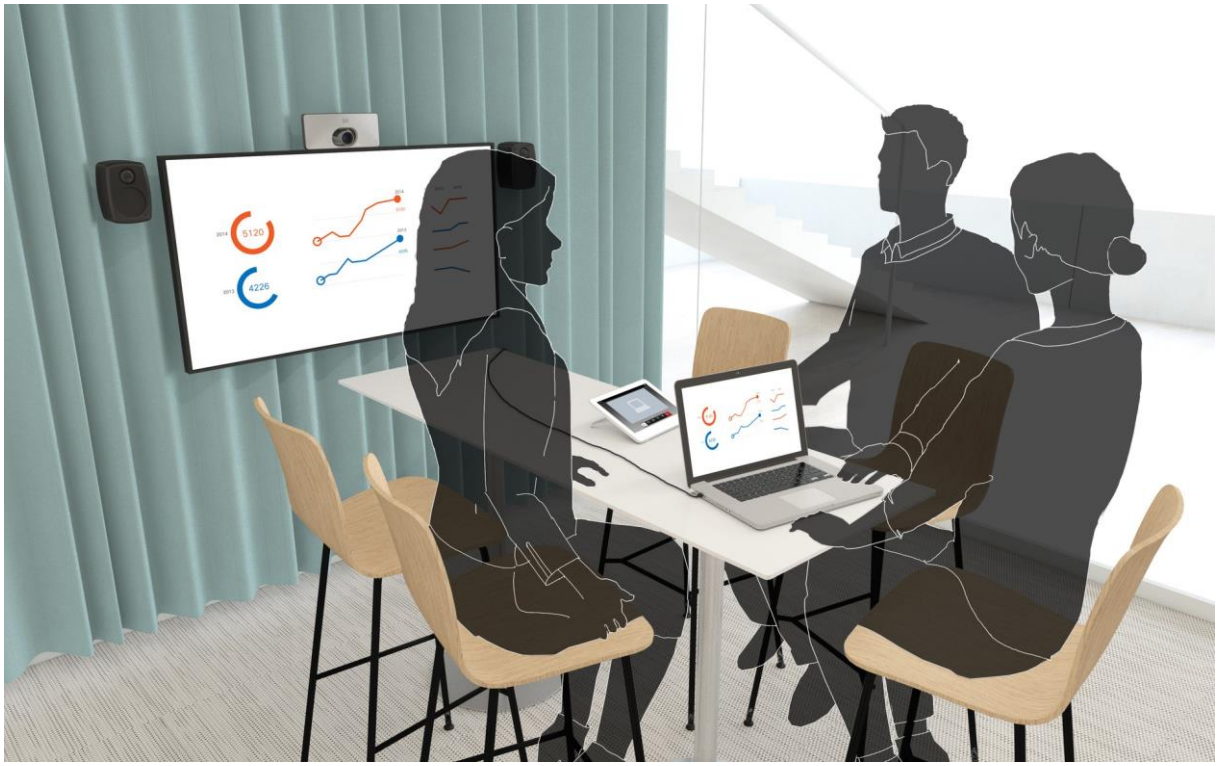
Po napisaniu wiadomości przez użytkownika jego aplikacja kliencka szyfruje ją za pomocą klucza konwersacji, (3) na powyższym rysunku, nadaje jej ID pomieszczenia docelowego i wysyła do rdzenia, relacja oznaczona jako (4). Rdzeń otrzymuje wiadomość w zaszyfrowanej postaci. Rdzeń nie posiada klucza konwersacji, przez co nie może odszyfrować treści wiadomości. Rdzeń sprawdza listę użytkowników powiązanych z ID danego pomieszczenia określonym w metadanych wiadomości, a następnie wysyła zaszyfrowaną wiadomość do pozostałych

użytkowników w pomieszczeniu (5). Co więcej, wiadomość, w swojej zaszyfrowanej postaci, jest zapisywana w specjalnej bazie danych w rdzeniu, powiązanej z odpowiednim pokojem.

Wiadomość nadal jest zaszyfrowana, gdy otrzymuje ją aplikacja kliencka innego użytkownika. Aplikacje klienckie innych użytkowników kontaktują się ze swoim KMS by otrzymać klucz konwersacji pozwalający na odszyfrowanie zawartości (6,7). Wymiana zawartości pomiędzy odbiorcami (6), a ich powiązanym KMS jest taka sama jak przy pierwszej wymianie kluczy (1). KMS uwierzytelnia każdego użytkownika by sprawdzić pozwolenia dostępu do klucza konwersacji z racji przebywania w powiązanym pomieszczeniu (8). KMS dystrybuuje klucz konwersacji do odbiorców, pozwalając im na odszyfrowywanie i odczytanie wiadomości (9).

Należy pamiętać, że w przepływach opisanych powyżej są stosowane dwie różne metody szyfrowania: hop-by-hop i pełna (end-to-end). Jak opisano powyżej, treści użytkownika oraz interakcja klient-KMS są szyfrowane w pełni - przy wykorzystaniu symetrycznego szyfrowania i charakterystycznych dla pomieszczeń kluczy konwersacji dla obsługi treści użytkownika oraz kluczy efemerycznych („tymczasowych") dla obsługi komunikacji klient-KMS. Obecnie stosowany w Spark symetryczny szyfr to AES256-CGM. Ponieważ w pełni zaszyfrowane treści są przesyłane z klienta do serwera, z serwera do serwera oraz z serwera do innych klientów, są one dodatkowo chronione przy pomocy szyfrowania hop-by-hop. Szyfrowanie hop-by-hop wykorzystuje protokół TLS (Transport Layer Security), czyli ten sam który jest wykorzystywany przez przeglądarkę internetową kiedy łączymy się ze stroną banku lub sklepu internetowego. Choć metody szyfrowania pełna i hop-by-hop są obecnie uważane za najlepsze, Spark został zbudowany w ramach koncepcji określanej jako Algorithm Agility, pozwalającej na wymianę algorytmu w trakcie pracy. Funkcja Algorithm Agility pozwala na szybkie zastosowanie nowych mechanizmów szyfrowania, w momencie gdy obecnie najsilniejsze metody staną się przestarzałe i pojawią się nowe zalecenia branżowe je zastępujące.

Wygenerowane przez użytkownika treści, do których odnoszono się powyżej, obejmują każdą wiadomość, nazwę pomieszczenia i pliki współdzielone w ramach Spark.



[2] Klienci są uwierzytelniani za pomocą posiadanych tokenów KMS, jak opisano w rozdziale dotyczącym Autoryzacji pomieszczenia poniżej

Identyfikatory URI kluczy konwersacji

Klucze konwersacji są identyfikowane i można się do nich odwoływać poprzez unikalne ujednolicone identyfikatory zasobów URI. Gdy w pełni szyfrowane treści są wysyłane od Klienta do Spark Cloud, nagłówek zawiera identyfikator URI klucza. Identyfikator URI zawiera informacje o serwerze KMS, który wygenerował klucz oraz lokalizację, która może być wykorzystana do pobrania klucza – zakładając, że element wnioskujący o klucz jest odpowiednio uwierzytelniony i autoryzowany.

Obsługa wielu kluczy konwersacyjnych i ich wymiana

Zawsze istnieje co najmniej jeden Klucz konwersacji przypadający na klienta, który przesyła treści do Spark Room. Przykładowo, jeżeli Alice przesyła treści do Spark Room ze swojego urządzenia mobilnego oraz laptopa, a Bob przesyła dane do tego samego pomieszczenia z poziomu swojego laptopa, jednocześnie przeglądając treści na swoim urządzeniu mobilnym, wówczas w ramach danego pomieszczenia będą aktywne 3 symetryczne klucze konwersacji: jeden dla mobilnego urządzenia Alice, jeden dla jej laptopa i jeden dla laptopa Boba.

Klucze konwersacji są wymieniane w sytuacji, gdy użytkownik opuszcza określone pomieszczenia, własnowolnie lub siłowo (wyrzucony z sesji). Kiedy klienci dowiedzą się o takim użytkowniku (rozdział Widoczność autoryzowanych użytkowników), wówczas każdy klient musi wymienić klucz konwersacji (ang. key rotation), aby móc dalej przesyłać treści do danego pomieszczenia. Spark Cloud egzekwuje to zachowanie. Symetryczne klucze Klient-KMS również są wymieniane co pewien czas.

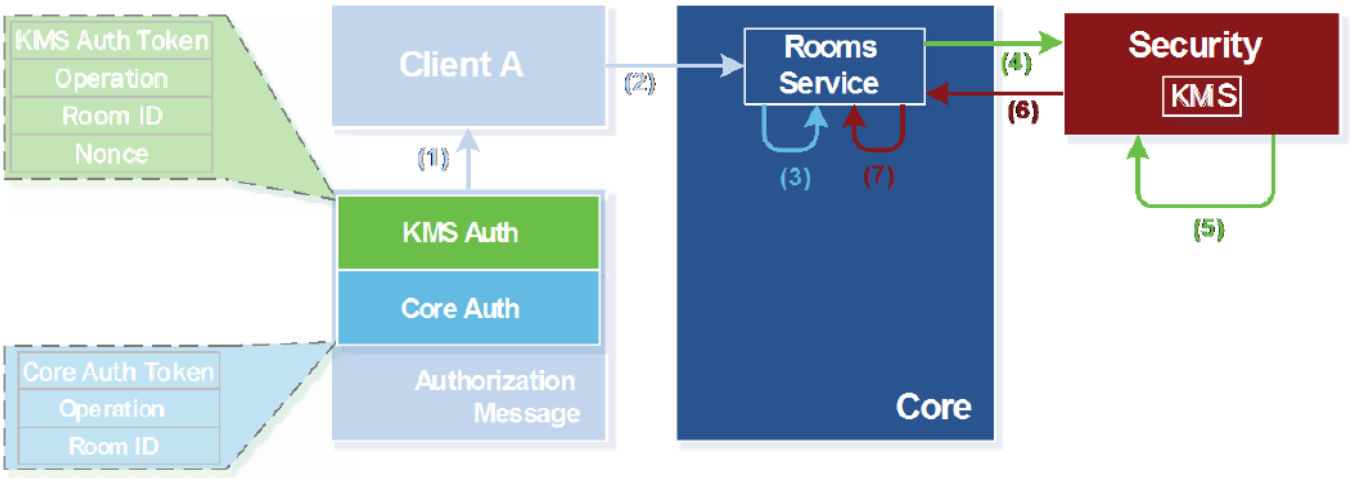
Autoryzacja pokoi spotkań

Gdy użytkownicy dodają lub usuwają kolejnych użytkowników spotkania, aplikacja kliencka użytkownika musi mieć pewność, że zarówno Spark jak i serwer KMS użytkownika wiedzą o zmianach jakie nastąpiły w autoryzacji dostępu do danego pokoju spotkań. Klient generuje komunikat autoryzacyjny AM (Authorization Message) by powiadomić Spark i KMS o zaistniałych zmianach. Komunikat AM składa się z dwóch odrębnych wiadomości (tzw. sub-komunikatów):

- Pierwsza dotyczy zmiany autoryzacji i zawiera token uwierzytelniający klienta[3] przeznaczony dla rdzenia, operację dodaj/usuń oraz unikalny identyfikator pomieszczenia, którego dotyczy dana operacja.
- Druga to szyfrowana zmiana autoryzacji, która zawiera token uwierzytelniający KMS, operację dodaj/usuń, unikalny identyfikator pomieszczenia, którego dotyczy dana operacja, oraz unikatową wartość nonce (losowy blok danych jednorazowego użytku).

Sub-komunikat jest szyfrowany przy użyciu efemerycznego („tymczasowego”) symetrycznego klucza wcześniej uzgodnionego pomiędzy aplikacją kliencką a KMS w procesie uzyskiwania Klucza konwersacji. Warto podkreślić, że szyfrowany sub-komunikat przeznaczony dla KMS

wykorzystuje token uwierzytelniający KMS, natomiast sub-komunikat przeznaczony dla rdzenia stosuje token uwierzytelniający rdzenia. Stosowanie odrębnych tokenów uwierzytelniających, wraz z dodatkową warstwą szyfrowania dla operacji zmiany KMS, uniemożliwia podszywanie się pod klienta przez rdzeń, co umożliwiłoby fałszowanie wniosków autoryzacyjnych kierowanych do KMS.



Rys. 2. Generowanie dwuczęściowego komunikatu autoryzacji.

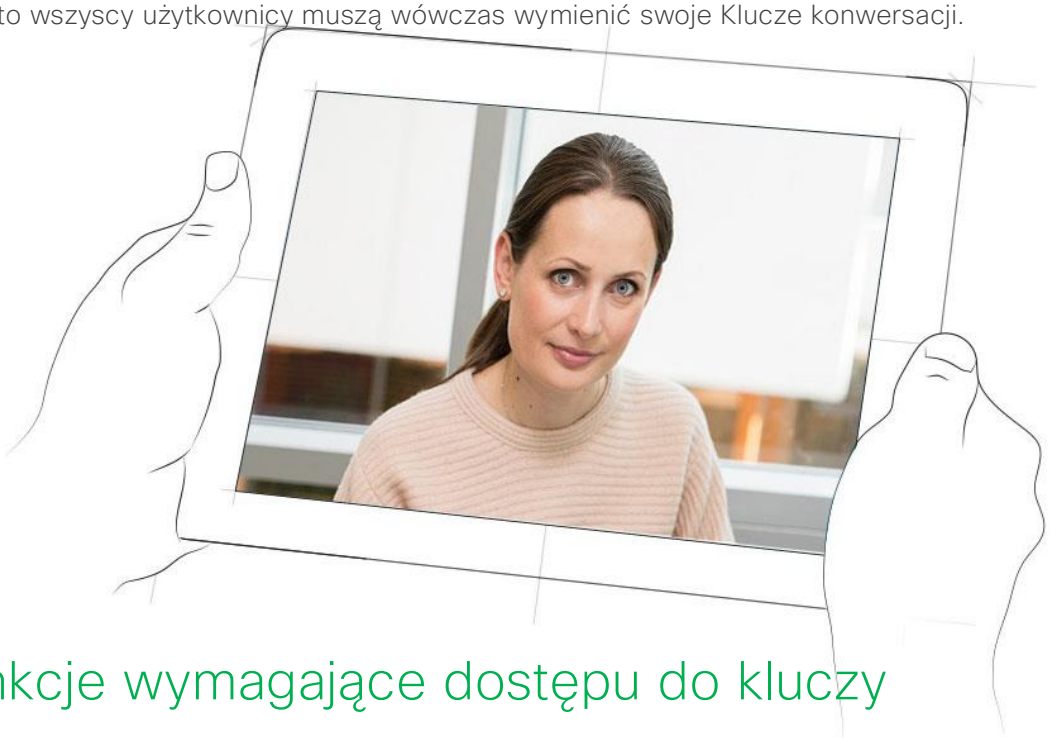
- Gdy klient wygenerował dwuczęściowy komunikat AM, relacja (1) na rys. 2, wysyła następnie tą wiadomość do obsługi pokoi (ang. Rooms Service) zlokalizowanej w rdzeniu poprzez TLS (2).
- Rooms Service potwierdza treść (3) sub-komunikatu przeznaczonego dla rdzenia, w tym token uwierzytelniający rdzenia i sprawdza czy wnioskujący użytkownik posiada upoważnienie do wprowadzania zmian w pokoju identyfikowanym przez dane RoomID.
- Jeżeli weryfikacja przebiegnie prawidłowo, Rooms Service przekazuje zaszyfrowany sub-komunikat do serwera KMS użytkownika (4) wraz z Room ID zawartym w sub-komunikacie rdzenia oraz ID użytkownika odkodowanym z tokenu uwierzytelniającego rdzenia.
- Zastosowanie tekstu jawnego w postaci Room ID oraz ID uwierzytelnionego użytkownika pozwala KMS na sprawdzenie czy wniosek Rooms Service odpowiada wnioskowi KMS w kwestii uwierzytelniania i autoryzacji. KMS odszyfrowuje otrzymaną wiadomość, potwierdza token uwierzytelniający KMS i zapewnia, że wnioskujący użytkownik jest upoważniony do wprowadzania zmian w danym pokoju (5).
- Jeżeli wszystko jest prawidłowo, KMS wykonuje żądaną operację i informuje o jej pomyślnym wykonaniu Rooms Service (6). Po otrzymaniu tej wiadomości od KMS, Rooms Service realizuje operację z wykorzystaniem tekstu jawnego (7).

Zaletą tego podejścia, jest wymiana informacji. Żądania klienta dotyczące dodania lub usunięcia użytkownika z danego pokoju powodują, że użytkownik będzie dodany lub usunięty jednocześnie z rdzenia i KM, ta cecha jest określana jako tzw. niepodzielność oznaczająca, że dwie operacje stanowią łącznie nierozłączny i nieredukowalny zestaw działań. Daje to pewność, że rdzeń i KMS są ze sobą zsynchronizowane jednocześnie zapewniając korzyści na polu bezpieczeństwa szyfrowanych treści związanych z autoryzacją kontrolowaną przez rdzeń, a także większe bezpieczeństwo kluczy stosowanych do odszyfrowania treści dzięki autoryzacji kontrolowanej przez KMS.

[3] Wszystkie tokeny są typu OAuth Bearer.

Widoczność autoryzowanych użytkowników

Lista użytkowników autoryzowanych do korzystania z danego pokoju Spark Room jest widoczna dla wszystkich innych autoryzowanych użytkowników tego pomieszczenia z poziomu aplikacji klienckich Spark. Oprócz listy autoryzowanych użytkowników, wyświetlane są informacje o aktywności związanej z dołączaniem i opuszczaniem spotkania przez użytkowników (w tym o użytkownikach wyrzuconych z sesji). Dzięki temu, że te informacje są aktualizowane na bieżąco, osoby przebywające w wirtualnym pomieszczeniu wiedzą kto został dodany lub usunięty z sesji i przez kogo. W momencie, gdy użytkownik opuszcza daną organizację (zwolnił się lub został zwolniony) Spark sprawi, że zostanie on wypisany ze wszystkich pokoi do jakich był przypisany. Tym samym, pozostali uczestnicy pokoju wiedzą, że ten pracownik nie ma już dostępu ani do dotychczasowych ani do przyszłych treści współdzielonych w danymi wirtualnym pomieszczeniu, ponadto wszyscy użytkownicy muszą wówczas wymienić swoje Klucze konwersacji.



Funkcje wymagające dostępu do kluczy

Należy zwrócić uwagę, że niektóre funkcje są dostępne jeśli Cisco ma przyznany dostęp do kluczy. Jedną z takich funkcji jest Transkodowanie dokumentów (ang. Document Transcoding), które jest procesem działającym w tle konwertującym wiele typów plików, jak np. dokumenty MS Office do formatu obrazów. W ten sposób urządzenia mobilne i aplikacje webowe mogą szybko wyświetlać zawartość, która często nie jest natywnie obsługiwana przez platformy odbiorców. Funkcje, których działanie wymaga dostępu do kluczy, wnioskują o przyznanie klucza w serwerze KMS w ten sam sposób jak inne aplikacje klienckie użytkownika, ale realizują to w ramach konta maszyny, które posiada autoryzację dostępu do określonych kluczy w korporacyjnym KMS. Konta maszyn są podobne do kont użytkowników, ale podczas gdy konta użytkowników są powiązane z nazwą użytkownika i hasłem, konta maszyn są powiązane z ID i kluczem maszyny, i stosowane do uwierzytelniania typu machine-to-machine (M2M).

Zdajemy sobie sprawę, że niektórzy klienci mogą nie życzyć sobie, aby Cisco miało dostęp do dokumentów udostępnianych w wirtualnych pokojach spotkań Spark Room. Z tego powodu, Spark oferuje możliwości wyłączenia wszystkich funkcji, które wymagają klucza dostępu do zasobów przedsiębiorstwa. Wyłączenie tych funkcji anuluje autoryzację w KMS dla konta maszyny z nimi związanego, a tym samym zapewnia, że nikt z poza organizacji nie ma dostępu do klucza. Warto jednak odnotować, że gdy użytkownik firmy przesyła dokumenty lub inne treści

do danego pokoju, do którego przypisane są także osoby z innej firmy, wówczas dane mogą być nadal dostępne z poziomu chmury, ponieważ ta druga firma może korzystać z usługi KMS zlokalizowanej w chmurze lub funkcji, które wymagają dostępu do kluczy.

W celu uzyskania informacji o pełnej liście funkcji, które wymagają dostępu do klucza, wraz z instrukcjami jak je wyłączyć, prosimy odnieść się do portalu Cisco Cloud Collaboration Management Portal. Rozdział „Integracje i rozszerzenia" przedstawia w jaki sposób podmioty trzecie mogą dodawać nowe funkcje do platformy Cisco Spark.

Możliwości wdrożenia domeny bezpieczeństwa (Secuirty Realm)

Zapoznali się Państwo ze sposobem w jaki Cisco wbudowało pełne szyfrowanie w strukturę rozwiązania Spark, co wiąże się z rozdzieleniem domeny bezpieczeństwa (Security Realm) od pozostałej części Cisco Spark Cloud. W przypadku klientów, którzy wymagają jeszcze większej gwarancji, że Cisco, jako dostawca usług cloud, nie ma dostępu do ich zasobów, Cisco oferuje elastyczność wdrożenia usług dostępnych w domenie bezpieczeństwa – w tym w serwerze KMS.

Klienci mają możliwość stosowania usług Security Realm hostowanych przez Cisco lub mogą je wdrożyć lokalnie. Cisco zapewni komercyjnie dostępne wersje każdej usługi, ale również przekaże kod źródłowy dla usług Security Realm, takich jak KMS, każdemu klientowi korporacyjnemu, który ich wymaga dla potwierdzenia naszych zapewnień. Ponadto, wszystkie usługi dostępne w ramach Security Realm wykorzystują i zapewniają standardowe w branży protokoły takie jak JSON over RESTful HTTPS. Cisco pracuje także aktywnie nad tym, aby ustandaryzować najważniejsze stosowane przez Cisco Spark techniki zarządzania, co pozwoli na stosowanie w przyszłości również funkcji open-source i komercyjnych innych producentów, zamiast usług proponowanych przez Cisco. Właściwie udokumentowane i zgodne ze standardami interfejsy oznaczają, że organizacje bardzo wrażliwe na kwestie bezpieczeństwa lub wymagające dużych możliwości dostosowania rozwiązania mogą dowolnie tworzyć własne implementacje tych usług.

Obecnie, gdy domena Secuirty Realm jest hostowana poza Cisco Spark Cloud, Cisco będzie wspólnie z klientem lub partnerem obsługiwać oprogramowanie. W tym połączonym modelu współpracy, Cisco posiada dostęp do logów, analityki i dostarcza aktualizacje. Logi nigdy nie zawierają kluczy czy danych osobowych. Podobnie jest w przypadku danych pomiarowych, które są odpowiednio zagregowane i służą Cisco do oceny wydajności serwera. Natomiast klient lub partner zarządzają sprzętową stroną wdrożenia oraz ogólnym świadczeniem i konfiguracją usługi.

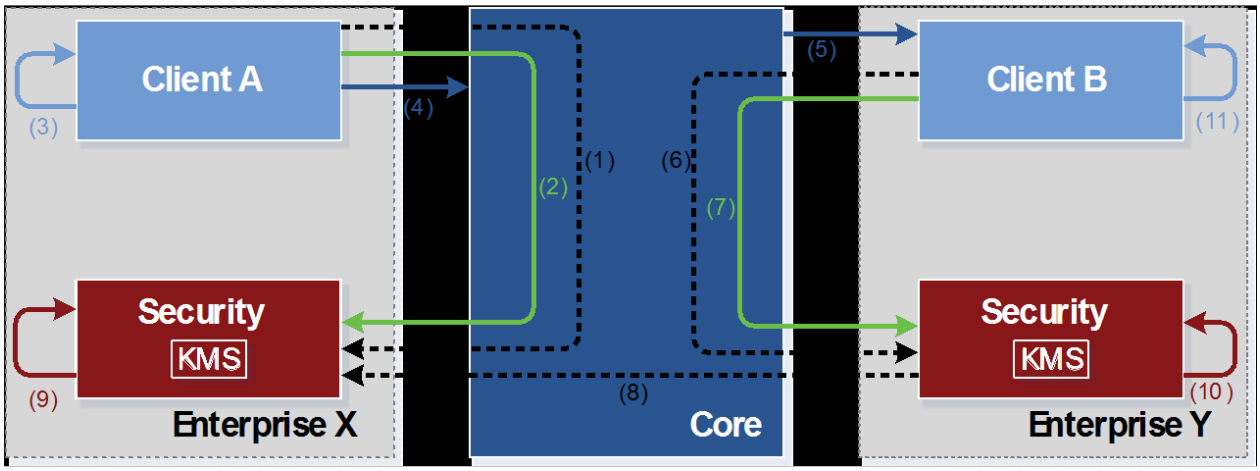
W momencie, gdy przepływy i interfejsy administracyjne przybiorą swoją ostateczną formę i będą stabilne, domena Security Realm będzie dostępna w ramach modelu w pełni zarządzanego i utrzymywanego przez partnera lub dane przedsiębiorstwo. W takim modelu, Cisco nadal świadczy usługi w innych domenach, ale domena bezpieczeństwa jest w całości obsługiwana przez partnera Cisco w ramach jego lokalnej infrastruktury lub przez przedsiębiorstwo w ramach jego infrastruktury lub przy udziale wybranego dostawcy usług cloud. W takim podejściu, partner lub przedsiębiorstwo będą mieć pełną operacyjną kontrolę nad serwerem KMS, systemem indeksowania Search Indexer, powiązanymi bazami danych oraz wszystkimi innymi usługami dostępnymi w ramach domeny bezpieczeństwa Security Realm.

Więcej informacji o działaniach Cisco na rzecz standaryzacji architektury KMS można znaleźć na stronie: http://cs.co/keymanagement.

Proces KMS (Key Management Server) Federation

Użytkownicy Cisco Spark są powiązani wyłącznie z jednym przedsiębiorstwem, a każde przedsiębiorstwo ma swój własny serwer KMS. Kiedy użytkownicy Cisco Spark z różnych przedsiębiorstw komunikują się ze sobą, wówczas klucze konwersacji muszą być przekazywane pomiędzy tymi użytkownikami. W tym celu Cisco Spark wykorzystuje proces określany jako Federation. Większość kroków w tym procesie jest identycznych jak opisane we wcześniejszym rozdziale pt. Pełne szyfrowanie treści. Główna różnica polega na tym, że każdy Klient komunikuje się wyłączenie z powiązanym z nim serwerem KMS oraz wprowadzonym dodatkowym, w którym dwa serwery KMS komunikują się ze sobą celem wymiany kluczy. W przeciwieństwie do tradycyjnych tego typu procesów, KMS Federation nie wymaga żadnej konfiguracji ze strony klienta lub partnera. Ogólnie rzecz biorąc usługa działa w modelu cloud – w którym każdy użytkownik może komunikować z dowolnym innym użytkownikiem na świecie.

- Jak już wcześniej omówiono, kiedy użytkownik Spark chce wysłać jakieś treści do pokoju Spark Room, wówczas aplikacja kliencka użytkownika (Client A/ Klient A) musi najpierw ustanowić bezpieczny kanał połączeniowy z powiązanym serwerem KMS (Enterprise X/ Przedsiębiorstwo X), jak pokazano na rys. 3 (relacja (1)) a następnie wnioskować o Klucz konwersacji (2). Jak poprzednio, jest to realizowane poprzez bezpieczny kanał połączeniowy (1) z wykorzystaniem efemerycznej wymiany uwierzytelnionych kluczy ECDH.
- Klient A następnie szyfruje (3) przesyłane treści stosując metodę symetryczną i Klucz konwersacji i wysyła je do Spark Cloud (4).
- Spark Cloud sprawdza listę użytkowników przypisanych do ID pokoju określonego w metadanych komunikatu (w tym przypadku użytkownik w przedsiębiorstwie Y), a Spark wysyła zaszyfrowaną wiadomość do klientów odbiorcy (5). Wiadomość pozostaje zaszyfrowana w momencie jej otrzymania przez Klienta B (Client B).



Rys 3. Komunikacja pomiędzy przedsiębiorstwami w ramach Spark.

- Klient B kontaktuje się z serwerem KMS Przedsiębiorstwa Y, aby zyskać Klucz konwersacji dla otrzymanej wiadomości (6,7). Gdy serwer KMS Przedsiębiorstwa Y otrzymuje takie żądanie, sprawdza identyfikator URI Klucza konwersacji i określa czy Klucz istnieje w odległym KMS. Jeżeli tak, serwer KMS Przedsiębiorstwa Y ustanawia kanał połączeniowy TLS, przechodzący przez rdzeń, z serwerem KMS w Przedsiębiorstwie X (8) w celu uzyskania Klucza.

- Ten wspólny kanał połączeniowy TLS jest uwierzytelniany przy pomocy certyfikatów PKI powiązanych z serwerami KMS każdego z przedsiębiorstw, przy czym certyfikaty PKI muszą być wydane przez urząd certyfikacji CA, który nie nada certyfikatów tymczasowych lub przez pośredni urząd certyfikacji.

Pełna lista urzędów certyfikacji CA jest dostępna na portalu Cisco Cloud Collaboration Management Portal.

To połączenie, podobnie jak wszystkie połączenia w ramach Spark, jest przesyłane przez Rdzeń w celu minimalizacji wymagań wobec firewalla oraz zdalnych urządzeń. Jednakże, jest w pełni szyfrowane i niewidoczne dla Rdzenia – tak jak inna komunikacja w ramach Spark. Kiedy serwer KMS przedsiębiorstwa X otrzymuje takie żądanie, sprawdza autoryzowaną listę użytkowników przypisanych do pokoju Spark Room i dowiaduje się, że użytkownik w Przedsiębiorstwie Y rzeczywiście jest upoważniony do dostępu do danego pokoju.

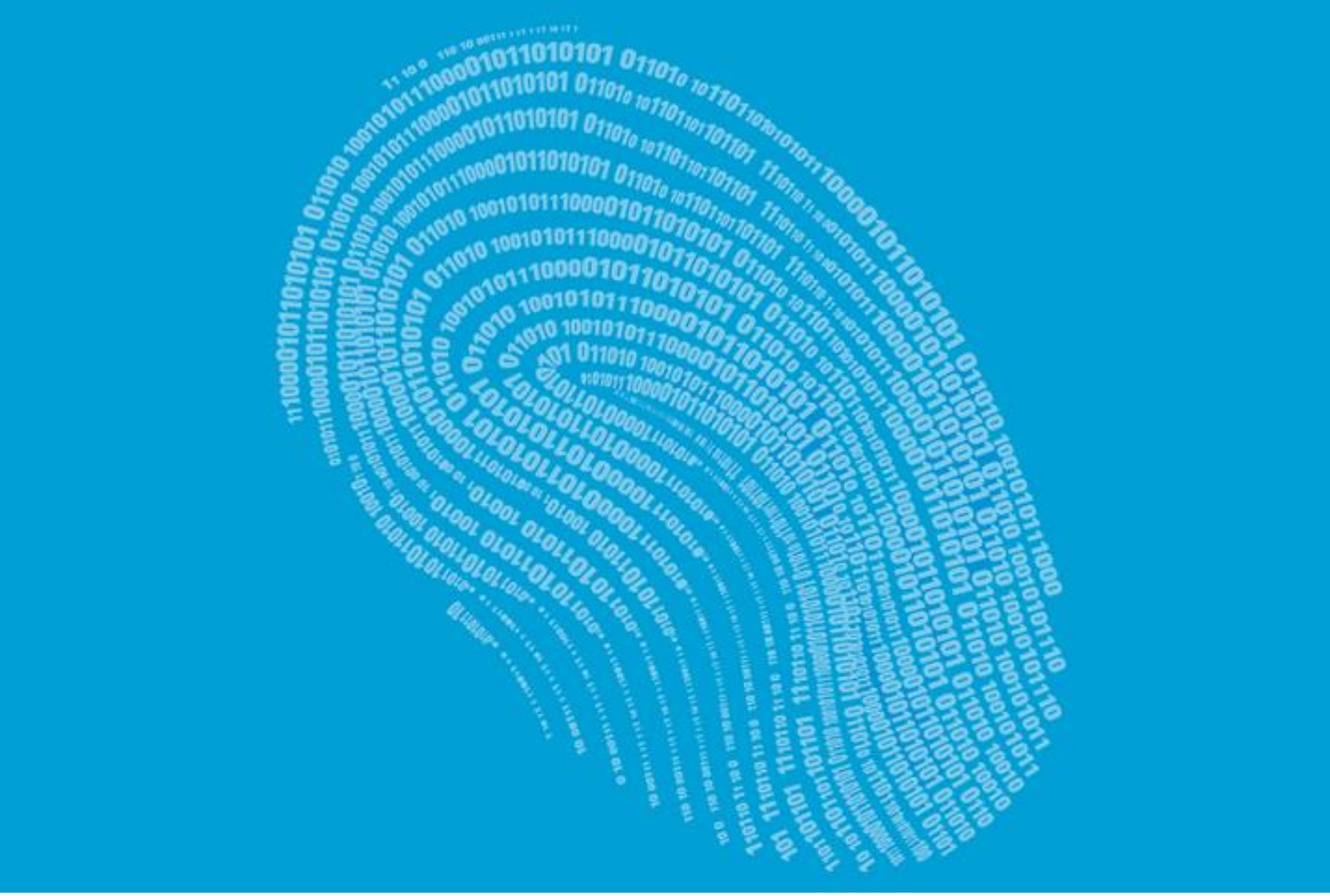
Ponieważ serwer KMS Przedsiębiorstwa X może widzieć tylko użytkowników z Przedsiębiorstwa X, nie może uwierzytelniać użytkowników Przedsiębiorstwa Y. Tym samym, musi polegać na certyfikacie PKI otrzymanym od serwera KMS Przedsiębiorstwa Y w celu ustalenia, że dana tożsamość KMS należy do Przedsiębiorstwa Y.

- Serwer KMS Przedsiębiorstwa X sprawdza czy co najmniej jeden użytkownik w Przedsiębiorstwie Y jest upoważnionym członkiem danego pokoju, w celu autoryzacji wniosku o przyznanie klucza (9).
- Po uwierzytelnianiu i autoryzacji serwera KMS należącego do przedsiębiorstwa wysyłającego zapytanie, serwer KMS Przedsiębiorstwa X przesyła Klucz konwersacji do serwera KMS Przedsiębiorstwa Y poprzez wspólny kanał połączeniowy TLS.
- Serwer KMS Przedsiębiorstwa Y przechowuje klucz w swojej lokalnej bazie danych a następnie przeprowadza proces weryfikacji autoryzacji, w celu upewnienia się, że wnioskująca aplikacja kliencka należy do użytkownika, który jest upoważniony do dostępu do tego klucza (10).
- Po autoryzacji serwer KMS Przedsiębiorstwa Y przesyła Klucz konwersacji do Klienta B, dzięki czemu może on odszyfrować i odczytać wiadomość (11).

W przypadku, gdy użytkownik danego przedsiębiorstwa komunikuje się z kimś z zewnątrz organizacji, realizowany jest taki sam proces, z tą różnicą, że jeden z dwóch serwerów KMS uczestniczących w komunikacji jest obsługiwany i zarządzany przez Cisco.

Możliwości weryfikacji kodu i usług

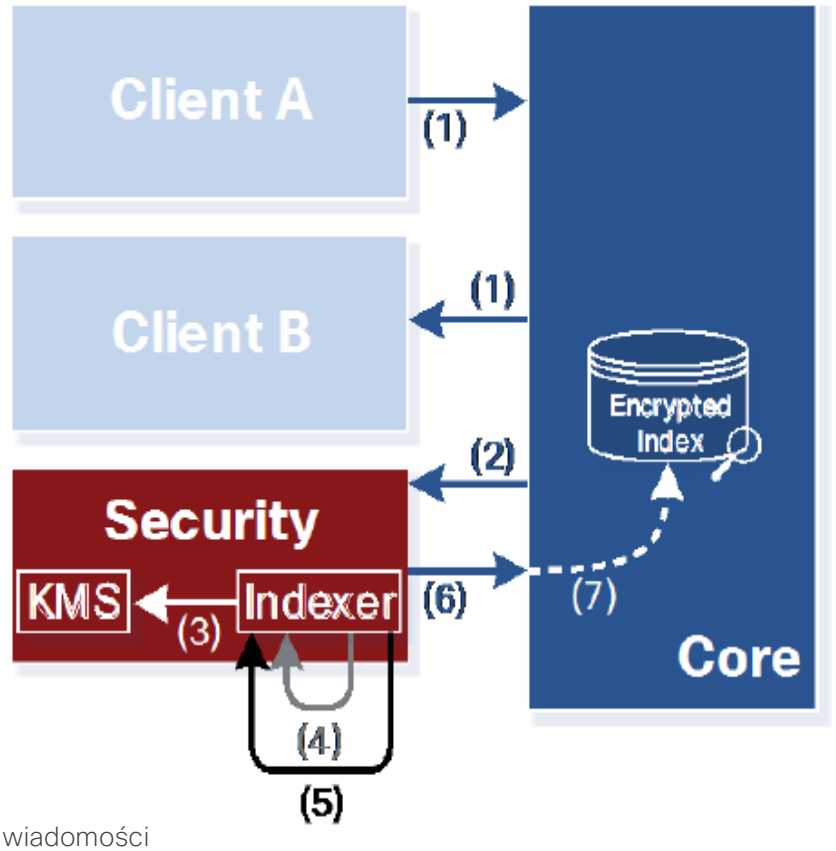
Protokoły stosowane przez Cisco Spark, w tym te stosowane do zarządzania kluczami, to albo istniejące standardy albo standardy oczekujące na zatwierdzenie przez IETF lub W3C. Te protokoły, przy prawidłowej implementacji, zapewniają pełne bezpieczeństwo zasobów przedsiębiorstwa. Poziom protokołów jest łatwy do sprawdzenia przez klienta dzięki mechanizmowi inspekcji pakietów, natomiast wewnętrzne procesy zaufanych usług w ramach domeny Security Realm nie są już tak łatwe do obserwacji. W celu obejścia tego problemu, usługi Security Realm mogą zapewniać logi kontroli, które mogą być oceniane pod kątem wykorzystania usługi przez aplikacje klienckie oraz przyznanego dostępu do chmury – w ten sposób można sprawdzić, czy system działa prawidłowo. Co więcej, Cisco zapewni każdemu klientowi korporacyjnemu dostęp do kodu źródłowego elementów wchodzących w skład domeny Security Realm, w celu sprawdzenia, zestawienia i porównania binarnie z tymi samymi elementami (w postaci binarnej), które mają być wdrożone w środowisku organizacji.



Szyfrowanie treści multimedialnych w czasie rzeczywistym

Wszelkie treści multimedialne w Cisco Spark, takie jak głos, wideo czy współdzielona zawartość pulpitów są przesyłane przy wykorzystaniu protokołu SRTP (Secure Real-Time Transport Protocol, RFC 3711). Obecnie, Cisco Spark Cloud odszyfrowuje multimedia przesyłane w czasie rzeczywistym dla potrzeb mieszania, dystrybucji, trunkingu i rozgraniczania wymaganych przez sieci telefoniczne PSTN (Public Switched Telephone Network).

Aby w przyszłości jeszcze bardziej zwiększyć bezpieczeństwo protokołu SRTP, Cisco jest także jednym z aktywnych członków nowej grupy roboczej PERC (Privacy Enhanced RTP Conferencing) w ramach IETF. Celem prac grupy PERC jest możliwość pełnego szyfrowania treści multimedialnych, przy zachowaniu uwierzytelniania na zasadzie hop-by-hop. Gdy ten nowy standard dojrzeje, Cisco Spark będzie korzystać z tego udoskonalenia procesu szyfrowania danych multimedialnych w czasie rzeczywistym, w taki sposób, że klucze szyfrujące dla przesyłanych danych będą obsługiwane przez serwer KMS a Cisco Spark Cloud nie będzie już deszyfrować komunikacji kompatybilnej z PERC. PERC nie wpłynie na deszyfrowanie połączeń PSTN, które w najbliższej przyszłości będą wymagać deszyfrowania w chmurze przez dostawcę usług PSTN. Więcej informacji o pracach PERC na stronie: https://datatracker.ietf.org/wg/perc.



Rys. 4. Proces indeksowania wiadomości

Szyfrowane wyszukiwania: szybkie i bezpieczne

Ponieważ rozwiązanie Spark Cloud nie ma możliwości podglądu całej zawartości komunikacji, można się spodziewać, że wyszukiwanie wiadomości w chmurze będzie niemożliwe. Ale Cisco opracowało innowacyjny sposób globalnego wyszukiwania wiadomości bez konieczności ich odszyfrowywania przez Rdzeń Cisco Spark.

Zrealizowaliśmy to przez dodanie kolejnego komponentu do domeny Security Realm odpowiedzialnego za indeksowanie, tzw. Indexera. Podobnie jak serwer KMS, Indexer jest architektonicznie i operacyjnie oddzielony od Rdzenia, ale ściśle powiązany z serwerem KMS. Odgrywa kluczową rolę przy realizacji dwóch podstawowych zadań niezbędnych do obsługi procesu globalnego wyszukiwania wiadomości: tworzy i odpytuje indeks wyszukiwania.

Tworzenie indeksu wyszukiwania

Pierwszym krokiem jest budowa indeksu wyszukiwania.

- Za każdym razem, gdy użytkownik przesyła wiadomość w ramach rozwiązania Spark (1), jest ona przesyłana do Indexera w pełni zaszyfrowanej postaci, jak pokazano na rys 4 – relacja (2). Indexer następnie odpytuje serwer KMS o klucz konwersacji niezbędny do odszyfrowania wiadomości. Indexer to tzw. Spark Bot4, który jest członkiem każdego wirtualnego pokoju

spotkań, na podstawie właściwej polityki przedsiębiorstwa, co zwiększa efektywność wyszukiwań.

• Serwer KMS przekazuje właściwy klucz konwersacji Indexerowi, ponieważ ten element jest aktywnym uczestnikiem każdego pokoju i posiada upoważnienie do odszyfrowywania treści udostępnianych w poszczególnych pokojach (3).

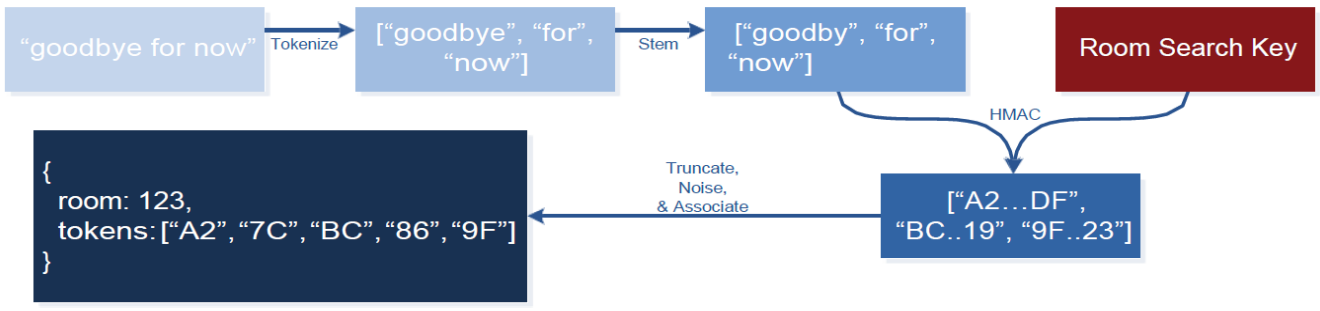
• Indexer odszyfrowuje wiadomości i rozkłada je na poszczególne słowa składowe (4).

• Następnie Indexer stosuje kryptograficzny jednostronny hash do każdego słowa lub rdzenia każdego słowa, stosując specjalny, charakterystyczny dla danego pokoju klucz wyszukiwania przechowywany w serwerze KMS5 (5). Przykładowo, wyrażenie „goodbye for now" zostanie rozbite na słowa „goodbye", „for" i „now", z których każde zostanie zahaszowane. Rezultatem jest lista zahaszowanych słów, które są przypisane do pokoju, w którym opublikowano daną wiadomość. Hasze szyfrują tekst jednostronnie, nie ma możliwości odwrócenia tego procesu i odczytania oryginalnego wyrazu. Indexer dodaje do tej listy słów pewne losowe hasze co zapewnia, że wiadomości nie mogą zostać odczytane przy zastosowaniu analiz częstotliwości występowania znaków (ponieważ np. słowa takie jak „and" oraz „the" często pojawiają się w języku angielskim, dodanie losowych wartości zapewnia, że da się w takim wypadku określić pewnej prawidłowości występowania znaków).

• Na koniec Indexer wysyła tą listę haszów do Spark Cloud (6), gdzie są przechowywane w zaszyfrowanej postaci w indeksie wyszukiwania (7). W rezultacie, Spark Cloud posiada indeks wszystkich słów każdej wiadomości powiązanej z danymi pokojami, w zaszyfrowanej postaci, która nie może być odszyfrowana przez Spark Cloud.

[4] Więcej informacji w rozdziale Integracje i możliwości rozbudowy w dalszej części dokumentu.

[5] Wykorzystuje kod 256 HMAC skrócony do 80 bitów.

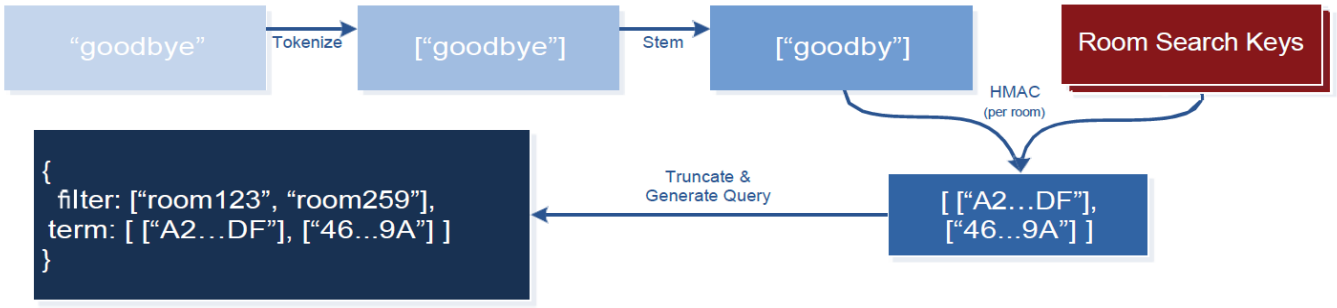


Rys. 5. Przepływ danych związany z indeksowaniem wiadomości

Wysyłanie zapytań do indeksu wyszukiwania

Kiedy użytkownik przeprowadza wyszukiwanie, jego aplikacja kliencka współpracuje z Indexerem, w jego imieniu. Oznacza to, że cały proces pełnego szyfrowania wiadomości, opisany wcześniej dla komunikacji pomiędzy użytkownikami, jest stosowany do obsługi zapytań kierowanych przez użytkowników do Indexera.

Rozwijając tą kwestie, zapytanie wyszukiwania jest najpierw szyfrowane przez aplikację kliencką użytkownika za pomocą klucza szyfrującego end-to-end służącego szyfrowaniu komunikacji pomiędzy tą aplikacją a Indexerem. Każdy użytkownik jest powiązany z określonym Indexerem. Aplikacja kliencka użytkownika wysyła zaszyfrowane zapytanie do Spark Cloud, które z kolei przekazuje je do Indexera wraz z listą pokoi, do których użytkownik ma autoryzowany dostęp. Spark Cloud nie może odszyfrowywać zapytania wyszukiwania, ponieważ jest ono zaszyfrowane za pomocą klucza, do którego nie ma dostępu – czyli klucza konwersacji dla tej konkretnej komunikacji aplikacji klienckiej z Indexerem.

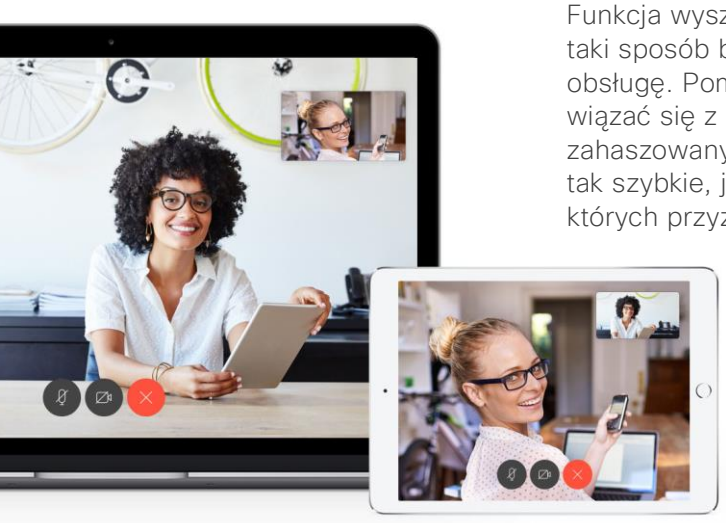


Rys. 6. Przepływ danych związany z wyszukiwaniem wyrazu

Indexer następnie realizuje te same kroki, jak wtedy gdy tworzył indeks wyszukiwania: rozkłada zapytania na poszczególne słowa i rdzenie słów, a następnie haszuje je za pomocą klucza wyszukiwania charakterystycznego dla każdego pokoju, do którego dostęp ma użytkownik. Oznacza to, że jeżeli użytkownik przypisany do 10 typów pokoi wpisze frazę wyszukiwania składającą się z dwóch słów, wówczas Indexer wygeneruje co najmniej 20 zahaszowanych zapytań, a możliwe, że nawet wiele więcej zależnie od tego, ile rdzeni ma każde słowo. Indexer następnie wysyła tą listę zahaszowanych zapytań do Spark Cloud.

Spark Core następnie przeszukuje indeks wyszukiwania w celu określenia dopasowania (jeżeli istnieją). Gdy znajdzie pokoje w indeksie wyszukiwania, które są powiązane z dowolnym haszem otrzymanym od Indexera tworzy listę, która ma być odesłana do aplikacji klienckiej użytkownika. Lista łączy uzyskane wyniki wyszukiwania z określonymi kluczami konwersacji, pozyskanymi z pamięci podręcznej aplikacji lub pobranymi z serwera KMS. Następnie wyniki wyszukiwania prezentowane są użytkownikowi.

Wszystko co najlepsze w ramach jednego rozwiązania



Funkcja wyszukiwania dostępna w Spark została opracowana w taki sposób by zapewniać wysoki poziom bezpieczeństwa i łatwą obsługę. Pomimo faktu, że nawet pojedyncze wyszukiwanie może wiązać się z generowaniem i porównywaniem tysięcy zahaszowanych wyrażeń, działanie funkcji wyszukiwania Spark jest tak szybkie, jak popularnych wyszukiwarek internetowych, do których przyzwyczajeni są użytkownicy.

Integracje i rozszerzenia

Pomimo, że platforma Cisco Spark Cloud oferuje fantastyczne możliwości, podobnie jak nasze doskonałe narzędzie do współpracy Cisco Spark, zdajemy sobie sprawę, że partnerzy i klienci potrzebują możliwości dostosowania i rozbudowy naszej oferty. Naszym celem jest, aby interfejsy API były łatwe do opanowania i obsługi. Programiści oczekują interfejsów API oferujących szerokie możliwości a przy tym prostych w obsłudze, tak aby mogli się skoncentrować na swoich własnych aplikacjach a nie na skomplikowanej platformie. Dołożyliśmy wszelkich starań, aby nasze interfejsy API były przejrzyste, pozbawione złożoności stojącej za nimi platformy.

Choć Rdzeń rozwiązania Cisco Spark Cloud nie posiada możliwości dostępu do przesyłanych treści, wiemy, że programiści, partnerzy i klienci, będą chcieli rozszerzać możliwości platformy w sposób, który często wymaga właśnie dostępu do takiej chronionej zawartości. W tym celu, wszystkie rozszerzenia do Cisco Spark Cloud umieszczone poza rdzeniem, muszą być świadomie aktywowane przez klienta lub użytkownika. Ponieważ funkcjonują one poza Cisco Spark Cloud, klienci mogą wybrać miejsce gdzie mają być wdrożone te rozszerzania platformy, przez kogo mają być zarządzane i do jakich zasobów mają mieć dostęp. Integracje i rozszerzenia Cisco Spark wymagają dostępu do kluczy szyfrujących, na takiej samej zasadzie jak opisane w rozdziale „Funkcje wymagające dostępu do kluczy”.

Cisco Spark obecnie identyfikuje trzy kategorie integracji – Boty, Aplikacje i Webhooks. Jednakże jesteśmy przekonani, że nasi klienci i inne podmioty będą rozbudowywać tą platformę na wiele różnych interesujących sposobów, których nie mogliśmy przewidzieć tworząc te podstawowe kategorie. Więcej informacji o interfejsach API Cisco Spark Cloud można znaleźć na stronie: https://developer.ciscospark.com.

Boty

Boty zapewniają rozszerzone funkcjonalności dla całej organizacji, np. usługę nagrywania połączeń. Boty muszą same tworzyć pokoje, w których mają działać lub muszą być do nich przypisywane. Umieszczenie bota w pokoju może następować w oparciu o odpowiednią politykę korporacyjną lub może on być dodany przez użytkownika przypisanego do danego pomieszczenia.

Aplikacje

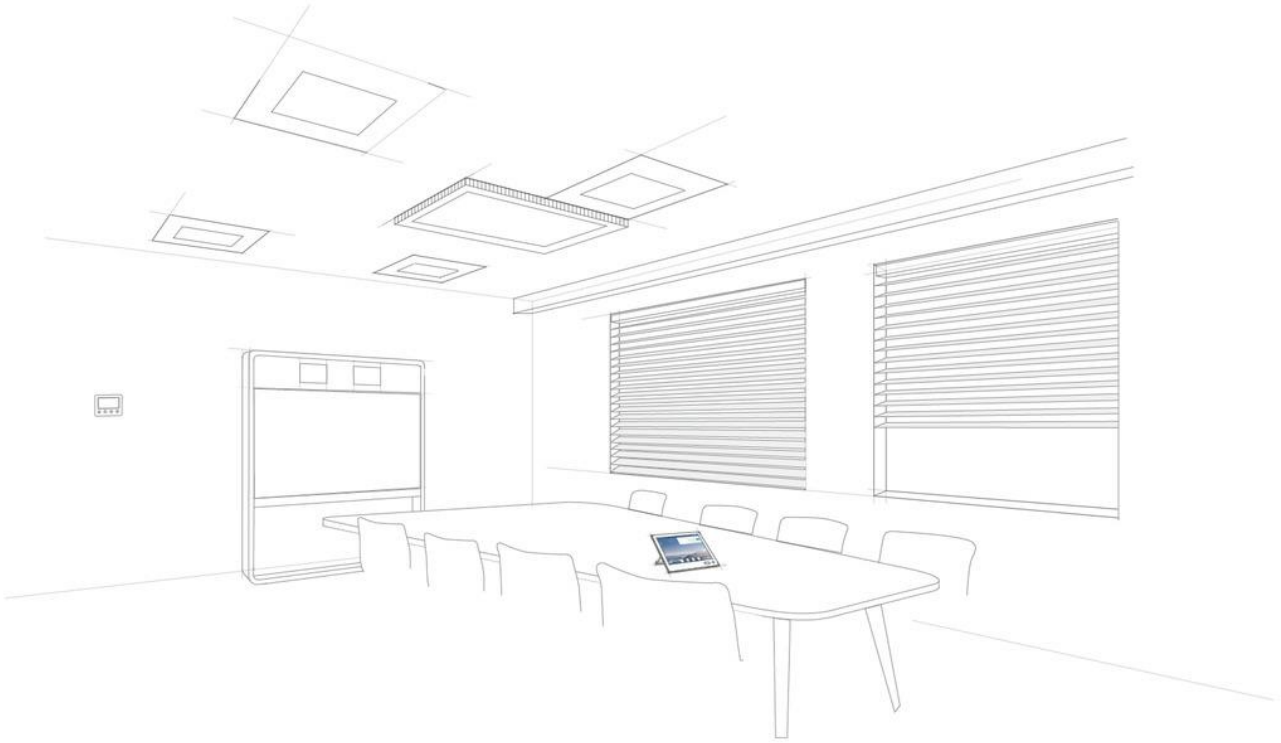
Aplikacje zapewniają dodatkowe funkcje poszczególnym użytkownikom, np. osobisty asystent czy tłumaczenie dokumentów. Pod wieloma względami, Aplikacje mogą być traktowanie jako aplikacje klienckie utrzymywane na serwerze lub w chmurze pozbawione interfejsu użytkownika. Aplikacje mają dostęp do wszystkich pokoi, do których dostęp ma powiązany z nimi użytkownik, aczkolwiek może on wykluczyć je z wybranych pomieszczeń.

Webhooks

Webhooks zapewniają dostęp z poziomu jednego URL do uproszczonych funkcji Rdzenia, takich jak publikowanie treści w pokoju lub powiadamianie o nowych treściach. Webhooks mogą zachowywać się podobnie do Botów i Aplikacji, tzn. mogą mieć swoją własną tożsamość jak Boty lub opierać się na tożsamości użytkownika jak Aplikacje. Webhooks oferują prostotę pojedynczego URL przez osadzenie ograniczonych w zakresie i długotrwałych tokenów dostępu OAuth2 w zapytaniu URL i realizują szyfrowanie i deszyfrowania treści w ramach procesów (worker) Webhook. W każdym przypadku, Webhooks są ograniczone w zakresie do pojedynczego zasobu (np. pokoju). Te ograniczania zakresu dostępu są konfigurowane i ustalane w momencie dodawania elementu Webhook.

Wybór należy do przedsiębiorstwa i użytkownika

Chociaż uważamy, że poziom bezpieczeństwa oferowany przez Cisco Spark Cloud nie ma sobie równych na rynku, to uznajemy, że każdy klient Cisco ma różne wymagania co do bezpieczeństwa. To od decyzji klienta zależy sposób funkcjonowania tego hybrydowego modelu użytkowania. Klienci mogą zdecydować się na korzystanie wyłącznie z Rdzenia (Core) lub rozszerzyć go o Boty, Aplikacje i Webhooks. Przedsiębiorstwa mogą określić politykę korporacyjną zezwalającą na stosowanie danych Aplikacji i Botów, a użytkownicy mogą podejmować decyzje o Aplikacjach w ramach tej polityki. Platforma Cisco Spark została opracowana z uwzględnieniem dobrze udokumentowanych, opartych na standardach interfejsach API, co oznacza, że elementy osadzone poza Rdzeniem (w tym Boty, Aplikacje, Webhooks) mogą być tworzone samodzielnie lub przez inne podmioty.



Certificate Pinning – przypinanie certyfikatów

Komunikacja Klienta Spark z Rdzeniem jest realizowana przez szyfrowane połączenie TLS. Klienci stosują technikę określaną jako przypinanie certyfikatów (ang. certificate pinning) w celu zapewnienia, że komunikacja nie została przechwycona, odczytana lub zmodyfikowana w trakcie przesyłania. Cisco „przypina" certyfikaty serwera do kilku głównych urzędów certyfikacji CA, które zobowiązały się do niewydawania pośrednich certyfikatów zarówno w ramach Kodeksu Postępowania Certyfikacyjnego, jak i przez ustawienie wartości pola „pathLenConstraint" (w sekcji podstawowych ograniczeń – BasicConstraints) głównego certyfikatu na zero (0), co wskazuje, że żadne certyfikaty CA nie mogą następować po danym Certyfikacie.

Ochrona prywatności danych

Nasze zaangażowanie w dostarczanie godnej zaufania oferty usług nie ogranicza się do ochrony treści użytkownika. W przypadku Spark dane o użytkownikach i wykorzystaniu są zabezpieczane przez połączenie narzędzi i funkcji do ochrony prywatności, które obejmują zaciemnianie tożsamości, szczegółowe role administracyjne, możliwość wyboru przez organizację i użytkownika oraz przejrzystość. Podobnie jak w przypadku pełnego szyfrowania, te elementy są bazą Cisco Spark.

Zaciemniona tożsamość

Szerokie podejście do kwestii związanych z tożsamością użytkowników ma krytyczne znaczenie dla usług służących współpracy zespołowej. Użytkownicy chcą mieć możliwość szybkiej komunikacji z osobami ze swoich zespołów; potrzebują możliwości wyszukiwania użytkowników po nazwie, adresie mailowym lub numerze telefonu; chcą potwierdzać tożsamość wizualnie za pomocą zdjęć profilowych. Jednocześnie, informacje o tożsamości użytkownika mogą być wrażliwe zarówno z perspektywy użytkownika jak i przedsiębiorstwa. Ograniczanie ekspozycji tożsamości użytkowników tylko do zakresu w jakim jest to konieczne to istotne założenie rozwiązania Spark.

Aby ograniczyć ekspozycję informacji o tożsamości użytkownika, w Spark Cloud wyodrębniamy tzw. „rzeczywistą" i „zaciemnioną" (ang. obfuscated) tożsamość. Dane zbierane podczas rejestracji użytkownika w Spark – nazwa użytkownika, adres mailowy, numer telefon, itp., to „rzeczywista tożsamość" i są one przechowywane w profilu użytkownika w elemencie rozwiązania Spark Cloud określanym jako Common Identity. Dodatkowo, dla każdego użytkownika jest generowany losowy 128-bitowy unikalny identyfikator UUID (Universally Unique Identifier), który stanowi „zaciemnioną tożsamość" użytkownika. Również w przypadku przedsiębiorstw stosujemy losowe 128-bitowe ID organizacji, stanowiące jej zaciemnioną tożsamość. W usłudze Spark zaciemniona tożsamość jest stosowana wszędzie, gdzie to możliwe, w tym:

- Przesyłanie wiadomości: Wszystkie wiadomości w Spark są przesyłane od nadawcy do odbiorcy wyłączanie w oparciu o zaciemnioną tożsamość. Również wszelkie zapytania wewnątrz chmury dotyczące poszczególnych użytkowników opierają się na zaciemnionej tożsamości, np. cała interakcja serwera KMS z Indexerem opisana powyżej.
- Logi serwera: Wszystkie logi wygenerowane przez komponenty aplikacji Spark Cloud dla potrzeb procesu rozwiązywania problemów wykorzystują zaciemnioną tożsamość.
- Analityka: Spark wykorzystuje metodykę DevOps a nasz zespół rozwojowy podejmuje decyzje o wprowadzeniu zmian w usłudze analizując dane o wydajności i wykorzystaniu. Dane o wykorzystaniu Spark opierają się na zaciemnionej tożsamości.

Oczywiście, gdy konieczne jest odtworzenie tożsamości użytkownika lub przedsiębiorstwa w aplikacji klienckiej Spark, portalu Cisco Cloud Collaboration Management Portal lub integracji innego producenta, autoryzowani klienci i elementy usługi cloud mogą mieć dostęp do rzeczywistej tożsamości. Jeżeli dowolna aplikacja kliencka Spark, element usługi cloud, Aplikacja lub Bot potrzebuje dostępu do rzeczywistej tożsamości uwierzytelnia się w ramach elementu Common Identity, które udostępnia tego typu dane tylko autoryzowanym wnioskodawcom.

Szczegółowo określone role administracyjne

Każdy partner i klient Spark posiada dostęp do portalu Cisco Cloud Collaboration Management Portal, który zapewnia szeroki zakres usług zarządzania, w tym wersje próbne, zakupy, konfiguracja konta, wdrażanie, usługi wsparcia oraz interfejsy API. Ponieważ zdajemy sobie sprawę, że te funkcje mogą wiązać się z dostępem do wrażliwych informacji o użytkownikach i kontach, wykorzystaniu produktów oraz konfiguracji, stworzyliśmy portal wspierający wiele różnych roli administracyjnych i zapewniający dostęp do różnych zestawów informacji. Przykładowo, administratorzy odpowiedzialni za usługi wsparcia mogą mieć dostęp do informacji o użytkownikach i logów wsparcia, natomiast dostęp administratora nadzorującego sprzedaż partnera jest bardziej ograniczony i skupiony na zagregowanych raportach wykorzystania i monitorowaniu usług. Administratorzy systemu mają dostęp do wszystkich funkcji portalu i mogą przypisywać odpowiednie role innym administratorom w ich organizacji.

Oferujemy powyżej wymienione role naszym partnerom i klientom, ale również sami z nich korzystamy ograniczając dostęp tylko do wybranych administratorów Cisco. Podczas, gdy nasi administratorzy i inżynierowie odpowiedzialni za usługi wsparcia mogą mieć dostęp do logów wsparcia i informacji o użytkownikach w celu rozwiązywania zgłaszanych przez partnerów i klientów problemów, to nasz personel zajmujący się sprzedażą i relacjami z klientami ma tylko ograniczony dostęp do tych danych wynikający z przypisanej im roli.

Możliwości wyboru dostępne dla organizacji i użytkownika

Spark daje użytkownikom i przedsiębiorstwom możliwość wyboru metod ochrony prywatności z poziomu prostego w obsłudze interfejsu konfiguracyjnego. Możliwości dostępne dla administratorów systemu:

- Uwierzytelnianie Single Sign-On (SSO): Administratorzy mogą tak skonfigurować aplikację Spark, by współpracowała z ich istniejącymi rozwiązaniami SSO. Obsługujemy zewnętrzne rozwiązania wykorzystujące technologie Security Assertion Markup Language (SAML) 2.0 i OAuth 2.0.
- Synchronizacja z usługami katalogowymi: Administratorzy mogą w czasie rzeczywistym odwzorowywać w Spark role pracowników danej organizacji dzięki współpracy z Microsoft Active Directory.
- Współdzielenie danych z partnerem Cisco: Przedsiębiorstwa mogą wybrać czy udostępniać dane o QoS i wykorzystaniu ze swoimi partnerami Cisco by zapewnić wyższy poziom wsparcia partnerów.

Możliwości wyboru dostępne dla użytkownika:

- Uprawnienia do wykorzystania funkcji urządzenia: Zależnie od przeglądarki lub urządzenia mobilnego, z poziomu których użytkownik obsługuje aplikację, Spark będzie żądał szeregu uprawnień dotyczących wykorzystania funkcji urządzenia, w tym telefonu, mikrofonu, kamery, nagrywania dźwięku, udostępniania ekranu, kalendarza, kontaktów, plików i zdjęć oraz wiadomości push. Na większości platform, wymaga to wyraźnej zgody użytkownika, która w każdej chwili może być przez niego cofnięta.
- Komunikacja zbliżeniowa: W przypadku urządzeń mobilnych, klienci Spark mogą automatycznie łączyć się urządzeniami głosowymi i wideo Cisco przez nasłuchiwanie sygnałów ultradźwiękowych, gdy klient Spark jest aktywny. Ponieważ wymaga to wykorzystania mikrofonu urządzenia, użytkownicy mogą w razie potrzeby wyłączyć tą funkcję.
- Zdjęcia profilowe: Zdjęcia profilowe nie są wymagane by korzystać ze Spark.
- Informowanie o osobach z poza organizacji: Klienci Cisco Spark sygnalizują użytkownikom w sposób wizualny, że w danym pokoju znajdują się osoby z poza ich organizacji.
- Moderowanie pokoju: Użytkownicy mogą moderować pokoje, pozwalając wybranym uczestnikom spotkania na pełnienie roli moderatorów posiadających wyłączną kontrolę nad pokojem i listą uczestników spotkania.

Przejrzystość

Chcemy, aby nasi użytkownicy i klienci mieli świadomość swoich wyborów i wiedzieli w jaki sposób obsługujemy i chronimy dane jakie nam powierzyli. W tym celu wykorzystujemy wielowarstwowy model przejrzystości. Dostarczamy wystarczające informacje, które pomagają użytkownikom w bieżącym podejmowaniu decyzji w ramach aplikacji klienckiej Spark. Dodatkowe informacje są dostępne na naszych stronach wsparcia, które regularnie

aktualizujemy. Natomiast szczegółowe informacje o zbieranych przez nas danych, sposobach ich wykorzystania i zabezpieczania są określone w dokumencie Cisco Online Privacy Statement i dedykowanym załączniku dotyczącym Spark.

Bezpieczeństwo platformy i usług

Oprócz procesu Cisco Secure Development Lifecycle, Cisco Spark przeprowadza okresowo wewnętrzne i zewnętrze testy penetracyjne (White-Box i Black-Box) platformy i usług Spark. Więcej informacji o procesie Cisco Secure Development Lifecycle jest dostępnych na stronie:

https://www.cisco.com/c/en/us/about/security-center/security- programs/secure-development-lifecycle.html

Zarządzanie incydentami i korporacyjne polityki bezpieczeństwa

Zespół Cisco Product Security Incident Response Team (PSIRT)

Zespół PSIRT jest odpowiedzialny za reagowanie na incydenty bezpieczeństwa związane z produktami Cisco. Cisco PSIRT to dedykowany globalny zespół, który obsługuje, bada i publikuje informacje o lukach bezpieczeństwa związanych z sieciami i produktami Cisco. Zespół Cisco PSIRT pozostaje w ciągłej gotowości i 24 godziny na dobę współpracuje z klientami Cisco, niezależnymi analitykami bezpieczeństwa, konsultantami, organizacjami branżowymi oraz innymi dostawcami by identyfikować możliwe zagrożenia bezpieczeństwa dotyczące produktów i sieci Cisco.

Jawność i wnioski organów ścigania dotyczące danych należących do klientów

Cisco jest zobowiązane do publikowania danych dotyczących wniosków i zapytań o udostępnienie danych klienta zgłaszanych przez organy ścigania i narodowe agencje bezpieczeństwa z całego świata. Będziemy publikować tego typu dane dwa razy w roku (za okres sprawozdawczy: styczeń-czerwiec i lipiec-grudzień). Podobnie jak inne firmy technologiczne publikujemy te dane 6 miesięcy po zakończeniu danego okresu sprawozdawczego zgodnie z ograniczeniami czasowymi takich raportów. Więcej informacji można znaleźć na stronie: http://www.cisco.com/web/about/doing_business/trust-center/transparency-report.html

Zgłaszanie lub uzyskiwanie wsparcia dla problemów dotyczących bezpieczeństwa

Poszczególni użytkownicy lub organizacje, którzy dostrzegli problemy z bezpieczeństwem produktu, są usilnie zachęcani do kontaktu z zespołem Cisco PSIRT. Cisco chętnie przyjmuje raporty od niezależnych analityków, organizacji branżowych, dostawców, klientów i innych źródeł zajmujących się bezpieczeństwem sieci lub produktów. Prosimy o kontakt z Cisco PSIRT za pomocą jednej z poniższych metod:

W pilnych sprawach

Telefon +1 408 525 6532 (połączenia międzynarodowe)

24 godziny na dobę, 7 dni w tygodniu

Standardowa obsługa

Email psirt@cisco.com

Wnioski otrzymane drogą mailową są zazwyczaj potwierdzane w ciągu 48 godzin.

Więcej informacji na stronie:
http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html