Livre blanc

Cisco Spark : sécurité et confidentialité

Version 1.0 (juin 2016)

Cisco® Spark est une plate-forme de collaboration cloud qui propose des fonctionnalités de messagerie, d'appels vocaux et d'organisation de réunions. L'application Cisco Spark® est une logiciel qui permet de se connecter à cette plate-forme et ainsi de profiter d'un outil complet pour le travail d'équipe. Les utilisateurs peuvent envoyer des messages, partager des fichiers et rencontrer diverses équipes, tout cela dans une même interface.

Ce livre blanc présente les fonctionnalités de sécurité et de protection de la confidentialité pour le cloud Cisco Spark et la messagerie Cisco Spark.

Les produits, les services et les fonctionnalités Cisco décrits dans ce document sont à divers stades de développement. Si certains de ces produits, services et fonctionnalités sont déjà disponibles, d'autres sont en cours de développement ou à venir. Pour plus d'informations, rendez-vous sur www.cisco.com.

Cisco ne pourra être tenu responsable d'un retard dans la livraison ou d'une incapacité à livrer les produits, les services ou les fonctionnalités présentés dans ce document.

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Les défis liés à la sécurité et à la confidentialité de la collaboration dans le cloud 3
Chiffrement total des contenus 3
URI des clés de conversation 5
Clés de conversation multiples et changements de clés 5
Autorisation d'accès aux salles 6
Visibilité sur les autorisations 7
Fonctions nécessitant un accès aux clés 7
Options de déploiement du domaine de sécurité 8
Fédération des serveurs de gestion des clés (KMS) 8
Vérifiabilité 10
Chiffrement en temps réel 10
Recherche chiffrée : sécurité et rapidité 11
Construire l'index de recherche 11
Interroger l'index de recherche 12
Un compromis optimal 13
Intégrations et évolutivité 13
Robots 13
Applications 13
Webhooks 13
Plusieurs options pour les utilisateurs et les entreprises 14
Association de certificat 14
Confidentialité des données 14
Identité masquée 14
Gestion granulaire des rôles d'administrateurs 15
Plusieurs options pour les utilisateurs et les entreprises 15
Transparence 16
Sécurité de la plate-forme et des services 16
Gestion des incidents et politiques de sécurité internes 16
Traitement des incidents de sécurité des produits Cisco 16
Signaler un risque pour la sécurité et obtenir une assistance 16
Transparence et demandes d'accès aux données des clients par les services de police 17

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Les défis liés à la sécurité et à la confidentialité de la collaboration dans le cloud

Pour les entreprises, l'un des principaux bénéfices des services cloud est de pouvoir tirer parti des nouvelles fonctionnalités dès qu'elles sont déployées par le fournisseur. Mais souvent, lorsqu'un fournisseur cloud développe les fonctionnalités d'un service, il a accès à l'ensemble des données et contenus des utilisateurs. En effet, pour les applications de collaboration, la plupart des fournisseurs cloud doivent accéder directement à vos messages, à vos appels et au contenu de vos réunions pour pouvoir vous offrir des fonctions telles que la recherche de messages, le transcodage des contenus ou l'intégration dans une application tierce. Par opposition, les services de collaboration de nouvelle génération tendent à renforcer la protection de la confidentialité des données des utilisateurs en proposant un chiffrement total des contenus, aux dépens des nouvelles fonctionnalités.

Cisco Spark vous offre un compromis optimal : une plate-forme de collaboration cloud offrant un chiffrement total des données, tout en permettant aux entreprises de choisir les nouvelles fonctionnalités Cisco ou tierces qu'elles souhaitent intégrer. Pour assurer la distribution sécurisée des clés de chiffrement, Cisco Spark utilise une architecture ouverte, permettant aux entreprises de bénéficier d'un contrôle total sur la gestion de leurs clés de chiffrement et de la confidentialité de leurs données. Ainsi, le contenu est chiffré sur le client de l'utilisateur et reste chiffré jusqu'à ce qu'il soit reçu par le destinataire. Aucun intermédiaire n'a accès à la clé de déchiffrement, sauf si l'entreprise en décide autrement.

Pour profiter de fonctionnalités supplémentaires, vous devez explicitement leur accorder l'accès aux clés. Or, comme nous intégrons le chiffrement total des contenus dans la plate-forme Spark, la plupart des nouvelles fonctionnalités traitent des données chiffrées. Grâce à plusieurs innovations en matière d'indexation de la messagerie, de modèles de permission, de flux d'authentification, de chiffrement et de modèles de déploiement, la solution prend en charge des fonctionnalités telles que la recherche globale de contenus chiffrés dans le cloud Spark.

La plupart des fournisseurs de services cloud prétendent proposer des services sécurisés simplement en chiffrant les données en cours d'acheminement entre les appareils des utilisateurs et leurs serveurs ou leurs propres data centers. Mais ce n'est pas suffisant pour empêcher le fournisseur lui-même d'y avoir accès. C'est pourquoi nous sommes allés plus loin avec Spark : non seulement toutes les connexions vers et depuis le cloud Spark sont chiffrées, mais nous n'avons accès aux contenus de l'utilisateur que lorsque ce dernier nous y a explicitement autorisés.

Notre engagement à fournir un service fiable n'est pas limité à la protection des contenus de l'utilisateur. Spark protège toutes les données des utilisateurs et celles relatives à l'utilisation du système à l'aide d'une combinaison d'outils et de fonctionnalités de protection de la confidentialité, notamment *le concept d'identité masquée*[1], un choix d'options pour les utilisateurs et les entreprises, et la transparence. Comme pour le chiffrement total, ces protections sont intégrées au service dès le départ.

Chiffrement total des contenus

Le chiffrement total des contenus dans le cloud Cisco Spark est rendu possible grâce à un composant essentiel : le serveur de gestion des clés (KMS). Le KMS permet de créer, de stocker et d'autoriser les clés de chiffrement que les clients Spark utilisent pour chiffrer et déchiffrer les messages et les fichiers, et d'y accéder. C'est grâce à la séparation architecturale et opérationnelle entre le KMS et le reste du cloud Spark que le chiffrement total des données est possible. C'est comme s'ils appartenaient à deux domaines de confiance distincts dans le cloud : le KMS appartient au *Domaine de sécurité* et tous les autres services composant Spark sont dans le *Domaine central.*

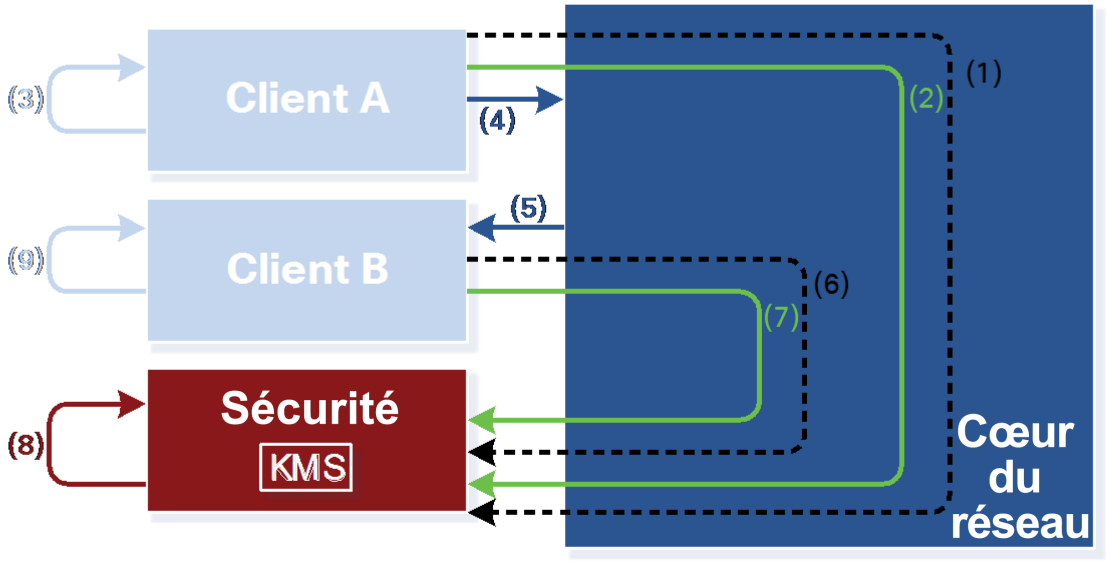
[1] Voir la rubrique Identité masquée

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Les communications via le KMS sont acheminées dans le cloud Cisco Spark et sont totalement chiffrées. Ainsi, elles ne peuvent pas être lues par les composants du domaine central et doivent être authentifiées par un token d'accès unique dans le cloud Cisco Spark. Grâce à ce modèle, nous renforçons la sécurité autour de l'accès aux clés de chiffrement, tout en garantissant qu'aucun composant des services du domaine central ne puisse accéder aux communications ou aux clés stockées sur le KMS. Lorsqu'ils sont exécutés par Cisco, les services du domaine de sécurité fonctionnent sur une infrastructure séparée, dans un compte locataire différent. Les entreprises clientes soucieuses de leur sécurité peuvent choisir de déployer les services du domaine de sécurité, parmi lesquels le KMS, dans leurs locaux. La prochaine rubrique en propose une description détaillée.

Lorsqu'un utilisateur de Spark souhaite envoyer du contenu vers une salle de réunion Spark, son système client doit d'abord établir un canal sécurisé entre son appareil et le KMS, comme illustré en **(1)** sur la Figure 1. Pour établir une clé secrète partagée et créer un canal sécurisé entre le client et le KMS, ces derniers procèdent à un échange temporaire de clés Diffie-Hellman basé sur les courbes elliptiques (ECDH). Cet échange permet de produire une clé partagée symétrique qui peut être utilisée pour échanger des messages en toute sécurité.

Figure 1 : Communication entre le client et le KMS dans Cisco Spark



L'authentification est requise sur ce canal afin de garantir que ni Cisco ni un tiers ne puisse voir ou modifier les informations et les clés acheminées par ce canal, ou ne puisse servir d'intermédiaire. Pour l'authentification, un certificat PKI (infrastructure à clé publique) est utilisé. Il contient un nom commun (CN) ou d'autres noms d'objet (SAN) correspondant au nom de domaine de l'entreprise. Les clients chiffrent leur moitié de l'échange ECDH vers le KMS grâce à la partie publique du certificat du serveur KMS. Les réponses ECDH du KMS sont signées grâce à la partie privée du certificat du serveur KMS.[2] Ce fonctionnement est légèrement différent du mécanisme ECDHE-RSA. En effet, ici les clients procèdent au chiffrement à l'aide du certificat public du serveur au lieu de signer en utilisant leur propre clé. Les clients n'ont donc plus besoin de certificat. Toutefois, ils doivent être capables d'authentifier le certificat KMS. Pour ce faire, les certificats KMS doivent avoir recours à une autorité de certification (CA) publique reconnue par les terminaux de bureau et mobiles, ou alors l'entreprise doit pouvoir envoyer son certificat CA racine privé aux terminaux que les utilisateurs utilisent pour accéder à Cisco Spark.

[2] Les clients sont authentifiés grâce à leur token d'authentification KMS, comme décrit ci-après dans la rubrique relative à l'Autorisation d'accès aux salles.

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Cisco Spark ne prend pas en charge l'envoi de certificats CA privés aux clients, mais les clients Cisco Spark utilisent un certificat issu du catalogue de certificats de confiance du client.

Une fois que le client et le KMS se sont mis d'accord sur une clé symétrique via le mécanisme ECDH authentifié, le client utilise ce canal pour demander une nouvelle clé de chiffrement afin de chiffrer le contenu destiné à une salle de réunion Spark et aux participants présents dans cette salle, comme illustré en **(2)**. Il s'agit d'une clé de conversation.

Une fois que l'utilisateur a écrit son message, le client le chiffre avec la clé de conversation **(3)**, l'identifie avec l'ID de la salle de destination et l'envoie au domaine central de Spark **(4)**. Le domaine central reçoit le message sous forme chiffrée. Toutefois, il ne dispose pas de la clé de conversation et ne peut donc pas déchiffrer le message. Le domaine central contrôle la liste des utilisateurs associés à l'ID de la salle spécifié dans les métadonnées du message, puis envoie le message chiffré aux autres utilisateurs de la salle **(5)**. De plus, le message est stocké sous sa forme chiffrée dans la base de données des messages du domaine central, sous le numéro de salle approprié.

Le message est toujours chiffré lorsque les autres clients des utilisateurs le reçoivent. Il ne leur reste plus qu'à contacter leur KMS pour obtenir la clé de conversation et déchiffrer le message **(6, 7)**. L'échange entre les destinataires du contenu **(6)** et leur KMS s'effectue de manière identique à l'échange initial entre l'auteur du message et le KMS **(1)**. Le KMS authentifie chaque utilisateur pour vérifier qu'ils se trouvent dans la salle concernée et sont donc autorisés à accéder à la clé de conversation **(8)**. Le KMS distribue ensuite la clé de conversation aux destinataires, leur permettant ainsi de déchiffrer et de lire le message **(9)**.

Deux couches de chiffrement différentes sont donc appliquées dans les processus décrits ci-dessus : un chiffrement à chaque étape du transfert et un chiffrement global. Comme nous l'avons expliqué, le contenu envoyé par l'utilisateur et l'échange client-KMS sont totalement chiffrés : un chiffrement symétrique est appliqué au contenu de l'utilisateur via les clés de conversation spécifiques à chaque salle de réunion, et des clés temporaires sont appliquées à l'échange client-KMS. Le mode de chiffrement symétrique utilisé actuellement par Spark est AES256-GCM. Lorsque le contenu totalement chiffré est transmis du client au serveur, du serveur au serveur et du serveur aux autres clients, sa sécurité est renforcée par un chiffrement à chaque étape du transfert. Pour le chiffrement à chaque étape du transfert, c'est le protocole TLS (Transport Layer Security) qui est utilisé. Il s'agit du même protocole utilisé par les navigateurs pour communiquer avec les banques ou les sites de commerce en ligne. Même si les méthodes utilisées pour le chiffrement total et le chiffrement à chaque étape du transfert sont les meilleures disponibles sur le marché, Spark repose sur le concept d'agilité des algorithmes. Ce concept permet d'adopter rapidement de nouveaux mécanismes de chiffrement, les méthodes de chiffrement les plus efficaces disponibles à ce jour devenant obsolètes et étant remplacées par de nouvelles recommandations du secteur.

Le « contenu généré par l'utilisateur » inclut tous les messages, noms de salle et fichiers partagés sur Spark.

URI des clés de conversation

Les clés de conversation sont identifiées et référencées par un URI (Uniform Resource Identifier). Lorsqu'un contenu chiffré est envoyé d'un client vers le cloud Spark, l'URI de la clé est précisé dans l'en-tête du message. Si l'utilisateur passe les contrôles d'authentification et d'autorisation, l'URI lui fournit différentes informations, notamment par quel KMS la clé a été générée et son emplacement.

Clés de conversation multiples et changements de clés

Une clé de conversation est attribuée au minimum à chaque client qui envoie du contenu vers une salle Spark. Par exemple, si Alice envoie du contenu vers une salle Spark depuis son terminal mobile et son ordinateur portable, et que Bob envoie du contenu vers la même salle depuis son ordinateur portable, tout en visionnant un autre contenu

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

sur son terminal mobile, trois (3) clés symétriques de conversation sont actives dans la même salle : une pour le terminal mobile d'Alice, une pour son ordinateur portable et une pour l'ordinateur portable de Bob.

Lorsqu'un utilisateur quitte une salle volontairement ou de façon contrainte, les clés de conversation sont modifiées. Dès qu'un système client apprend qu'un utilisateur quitte une salle (voir la section Visibilité sur les autorisations ci-dessous), il doit modifier les clés de conversation de la salle avant d'y envoyer de nouveaux contenus. Ce processus est obligatoire dans le cloud Spark. Les clés symétriques client-KMS changent également à intervalles réguliers.

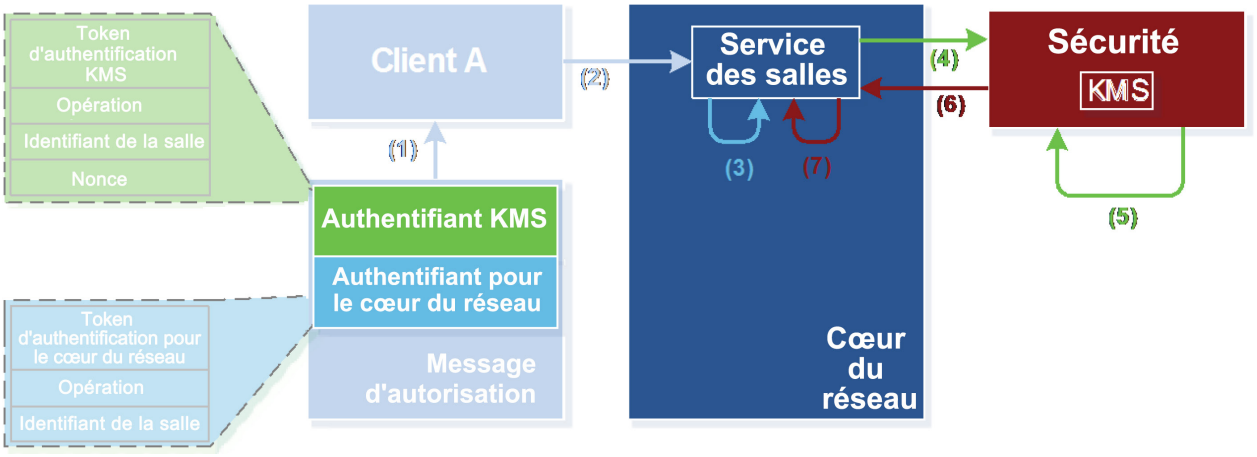
Autorisation d'accès aux salles

Lorsqu'un utilisateur autorise ou supprime l'accès aux salles à d'autres utilisateurs, son système client doit s'assurer que l'information est transmise à Spark et à son serveur KMS. Il génère donc un message d'autorisation pour signaler ces modifications à Spark et au KMS. Ce message d'autorisation est composé de deux sous-messages :

- Le premier contient les informations relatives à la modification, dont le token d'authentification[3] du client pour le domaine central, le type d'opération (ajout/suppression) et l'ID unique de la salle concernée.
- Le second contient les informations chiffrées relatives à la modification, dont le token d'identification du KMS, le type d'opération (ajout/suppression), l'ID unique de la salle concernée et un *nonce* (une suite de données aléatoire à usage unique).

Le sous-message est chiffré à l'aide d'une clé symétrique temporaire négociée entre le client et le KMS au moment de la récupération de la clé de conversation. Rappelons que le sous-message chiffré utilise le token d'identification du KMS, alors que le sous-message destiné au domaine central utilise le code d'identification du domaine central. Grâce à l'utilisation de différents tokens ainsi qu'au chiffrement supplémentaire appliqué à l'opération de modification du KMS, le domaine central ne peut pas se faire passer pour le client et falsifier des demandes d'autorisation envoyées au KMS.

Figure 2 : Génération d'un message d'autorisation en deux parties



[3] Tous les tokens sont des tokens OAuth.

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

- Une fois que le client a généré un message d'autorisation en deux parties **(1)**, comme illustré sur la Figure 2, il l'envoie au service de gestion des salles dans le domaine central de Spark via le protocole TLS **(2)**.
- Le service de gestion des salles valide **(3)** le sous-message du domaine central, notamment le token d'authentification du domaine central, et vérifie que le demandeur est autorisé à apporter des modifications à la salle correspondant à l'ID spécifié.
- Si tout est correct, le service de gestion des salles transmet le sous-message chiffré au KMS de l'utilisateur **(4)**, ainsi que l'ID de la salle contenu dans le sous-message du domaine central et l'ID de l'utilisateur déchiffré grâce au token d'authentification du domaine central.
- L'ID de la salle et l'ID de l'utilisateur authentifié permettent au KMS de vérifier que la demande d'autorisation et d'authentification du service de gestion des salles correspond à la demande KMS. Le KMS déchiffre le message reçu, valide le token d'authentification KMS et s'assure que l'utilisateur demandeur est autorisé à apporter des modifications à la salle **(5)**.
- Si tout est correct, le KMS effectue l'opération demandée et envoie un message au service de gestion des salles dès qu'elle est terminée **(6)**. Dès qu'il reçoit ce message, le service de gestion des salles exécute l'opération **(7)**.

Grâce à cette méthode, les deux opérations sont liées. Lorsqu'un client demande d'ajouter ou de supprimer un utilisateur d'une salle, ce dernier est ajouté ou supprimé à la fois sur le domaine central et le KMS ou sur aucun des deux. Ainsi, ces deux opérations forment un ensemble indivisible et irréductible : c'est ce que l'on appelle l'*atomicité*. Cela permet de garantir que le domaine central et le KMS restent synchronisés, tout en renforçant la sécurité puisque le domaine central garde le contrôle sur l'accès au contenu chiffré et le KMS contrôle l'accès aux clés nécessaire pour le déchiffrer.

Visibilité sur les autorisations

Chaque utilisateur autorisé à accéder à une salle Spark peut voir la liste de tous les autres utilisateurs autorisés à accéder à la salle, depuis son client Spark. De plus, la salle affiche le nom des utilisateurs qui la rejoignent, en sont sortis ou en ont été expulsés. Ainsi, les membres d'une salle savent qui a été ajouté ou supprimé, et par qui. Si un employé quitte l'entreprise, après avoir démissionné ou à la fin de son contrat par exemple, Spark le supprime des salles auxquelles il avait accès. Cela permet aux participants restants de savoir qu'il n'a plus accès aux contenus actuels ou futurs de la salle et les oblige à modifier leurs clés de conversation.

Fonctions nécessitant un accès aux clés

Actuellement, certaines fonctionnalités ne sont disponibles que si Cisco peut accéder aux clés. C'est le cas, par exemple, de la fonction de transcodage des documents, un processus back-end qui convertit divers types de fichiers, notamment les documents Microsoft Office, en images afin de s'assurer que les appareils web et mobiles puissent rapidement afficher les formats qui ne sont pas pris en charge de manière native sur la plate-forme du destinataire. Les fonctionnalités nécessitant un accès aux clés en font la demande auprès du KMS de l'entreprise, de la même manière que tous les autres clients, sauf qu'elles passent par un compte machine que l'administrateur de l'entreprise a autorisé à accéder à des clés spécifiques du KMS. Les comptes machines sont semblables aux comptes d'utilisateurs, sauf qu'au lieu d'être associés à un nom d'utilisateur et à un mot de passe, ils sont associés à un ID machine et à une clé machine, et sont utilisés pour l'authentification M2M (machine-to-machine).

Il est possible que certains clients ne souhaitent pas que Cisco ait accès aux clés des documents partagés dans les salles Spark. C'est pourquoi Spark permet aux entreprises clientes de désactiver à tout moment toute fonction nécessitant un accès aux clés, à l'échelle de l'entreprise. En désactivant ces fonctions, les comptes machines

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

associés ne disposent plus de l'autorisation nécessaire pour accéder aux clés sur le KMS de l'entreprise. Toutefois, si un utilisateur charge des documents ou du contenu dans une salle à laquelle ont accès des participants d'une autre entreprise, il est possible d'accéder à ce contenu via le cloud si l'autre entreprise utilise un KMS cloud ou des fonctions qui nécessitent un accès aux clés.

Pour connaître la liste complète des fonctionnalités qui nécessitent un accès aux clés ainsi que les instructions à suivre pour les désactiver, consultez le portail Cisco de gestion des solutions de collaboration cloud. Les rubriques Intégrations et Extensibilité expliquent comment ajouter de nouvelles fonctionnalités à la plate-forme Cisco Spark.

Options de déploiement du domaine de sécurité

Nous avons vu comment Cisco assure un chiffrement total dans le fabric Spark, reposant sur la séparation entre le domaine de sécurité et le reste du cloud Cisco Spark. Si certains clients souhaitent renforcer la protection de leurs contenus et s'assurer que Cisco en tant que fournisseur de services cloud ne puisse pas y accéder, nous leur proposons des modes de déploiement flexibles pour les services contenus dans le domaine de sécurité, notamment le KMS.

Nos clients ont la possibilité d'utiliser les services du domaine de sécurité hébergés par Cisco ou de déployer ces services sur leur site. Pour chaque service, nous fournissons une version disponible dans le commerce, mais aussi un code source pour les services du domaine de sécurité, tels que le KMS, à toutes les entreprises clientes qui le demandent. En outre, tous les services du domaine de sécurité utilisent et fournissent des protocoles standard du secteur, tels que JSON over RESTful HTTPS. Enfin, nous travaillons activement à standardiser les techniques de gestion des clés utilisées par Cisco Spark afin de permettre à de futures solutions commerciales et open source tierces de remplacer les services Cisco. Les interfaces étant bien documentées et normalisées, les clients pour lesquels la confidentialité est particulièrement importante ou qui souhaitent profiter d'un service hautement personnalisé sont également libres d'adapter nos services à leurs besoins.

À l'heure actuelle, lorsque le domaine de sécurité est hébergé en dehors du cloud Cisco Spark, nous utilisons le logiciel en collaboration avec le client ou le partenaire. Nous avons ainsi accès aux journaux et aux analyses, et pouvons fournir des mises à niveau. Les journaux ne contiennent pas de clés ou d'informations nominatives. De même, des données sont collectées afin d'informer Cisco sur les performances du serveur. Le client ou le partenaire gère le déploiement du matériel ainsi que la configuration et le provisionnement global du service.

Lorsque les interfaces et processus d'administration sont finalisés et stables, le domaine de sécurité est disponible dans un modèle entièrement hébergé et géré par le partenaire ou l'entreprise. Ainsi, nous continuons d'exploiter les services dans les autres domaines, mais le domaine de sécurité est entièrement exploité dans l'infrastructure sur site d'un partenaire Cisco, ou dans l'infrastructure de l'entreprise ou du fournisseur cloud de son choix. Lorsque c'est possible, le partenaire ou l'entreprise dispose d'un contrôle opérationnel total sur le moteur d'indexation de recherche du KMS, sur les bases de données associées et sur tous les autres services du domaine de sécurité.

Pour plus d'informations sur les efforts déployés par Cisco pour standardiser l'architecture KMS, rendez-vous sur www.cs.co/keymanagement.

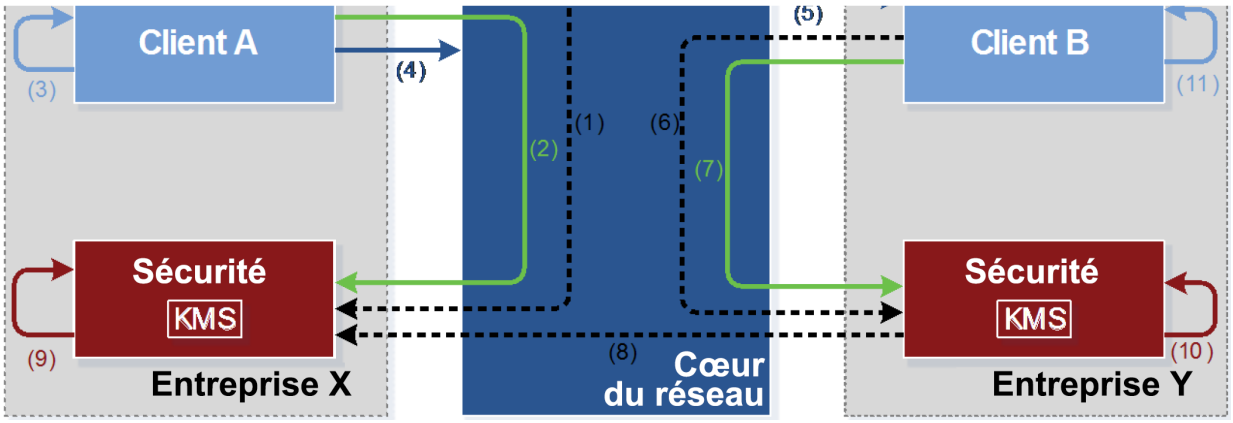
Fédération des serveurs de gestion des clés (KMS)

Dans Cisco Spark, les utilisateurs ne sont associés qu'à une seule entreprise et chaque entreprise peut disposer de son propre KMS. Lorsque des utilisateurs associés à des entreprises différentes communiquent, ils doivent pouvoir se transmettre les clés de conversation. Pour ce faire, Cisco Spark utilise un processus de « fédération ». La plupart des étapes du processus de fédération sont identiques à celles décrites dans la rubrique Chiffrement total

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

des contenus ci-dessus. Toutefois, ici chaque client communique uniquement avec son KMS et les deux KMS doivent communiquer entre eux pour partager les clés. Contrairement aux modèles classiques de fédération, la fédération KMS ne nécessite aucune configuration ou installation de la part du client ou du partenaire. Ce service correspond globalement à un modèle de cloud, qui permet à chaque utilisateur de communiquer avec d'autres utilisateurs à travers le monde.

Figure 3 : Communications Spark d'une entreprise à l'autre.



- Comme nous l'avons vu précédemment, lorsqu'un utilisateur souhaite envoyer du contenu vers une salle Spark, le client de l'utilisateur (Client A) doit d'abord établir un canal sécurisé entre son appareil et le KMS associé (Entreprise X), comme illustré en **(1)** sur la Figure 3, puis faire une demande de clé de conversation **(2)**. Cette opération s'effectue sur un canal sécurisé établi **(1)** via un échange ECDH temporaire authentifié.
- Ensuite, le Client A chiffre **(3)** le contenu à l'aide d'un mode de chiffrement symétrique et de la clé de conversation, et l'envoie vers le cloud Spark **(4)**.
- Le cloud Spark contrôle la liste des utilisateurs associés à l'ID de la salle spécifié dans les métadonnées du message (dans ce cas, un utilisateur de l'Entreprise Y) et Spark envoie le message chiffré aux clients destinataires **(5)**. Le message est toujours chiffré lorsque le Client B le reçoit.
- Le Client B contacte le KMS de l'Entreprise Y pour obtenir une clé de conversation pour le message reçu **(6, 7)**. Lorsque le KMS de l'Entreprise Y reçoit cette requête, il contrôle l'URI de la clé de conversation et vérifie si elle existe sur un KMS distant. Enfin, le KMS de l'Entreprise Y établit un canal TLS mutuel entre le domaine central et le KMS d'origine de l'Entreprise X **(8)** afin de faire la demande de clé.
- Ce canal TLS mutuel est authentifié à l'aide du certificat PKI associé au KMS de chaque entreprise. Les certificats PKI doivent être émis par une autorité de certification (CA) qui ne délivre pas de certificats CA subordonnés ni de certificats intermédiaires.

Pour connaître la liste des autorités de certification, consultez le portail de gestion des solutions de collaboration cloud de Cisco.

Cette connexion, comme toutes les connexions Spark, passe par le domaine central pour réduire les besoins en pare-feu et le recours à des systèmes homologues distants. Elle est cependant entièrement chiffrée et invisible pour le domaine central, comme toutes les communications dans Spark. Lorsque le KMS de l'Enterprise X accepte cette requête, il vérifie dans la liste d'autorisations les utilisateurs associés à la salle Spark et constate qu'un utilisateur de l'Enterprise Y a l'autorisation d'accéder à la salle.

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Comme le KMS de l'Entreprise X bénéficie uniquement d'une visibilité sur les utilisateurs associés à l'Entreprise X, il ne peut pas authentifier les utilisateurs de l'Entreprise Y. Par conséquent, il doit s'appuyer sur le certificat PKI fourni par le KMS de l'Entreprise Y pour établir que le KMS à l'origine de la requête appartient bien à l'Entreprise Y.

- Le KMS de l'Enterprise X vérifie qu'au moins un utilisateur de l'Entreprise Y est un participant valide de la salle pour autoriser la demande de clé **(9)**.
- Une fois que le KMS à l'origine de la requête a été authentifié et que l'autorisation a été vérifiée, le KMS de l'Entreprise X renvoie la clé de conversation demandée au KMS de l'Entreprise Y via le canal TLS mutuel.
- Le KMS de l'Entreprise Y met la clé en cache dans sa base de données locale puis vérifie l'autorisation pour s'assurer que le client à l'origine de la requête appartient à un utilisateur autorisé à accéder à cette clé **(10)**.
- Une fois l'autorisation reçue, le KMS de l'Entreprise Y distribue la clé de conversation au Client B, lui permettant ainsi de déchiffrer et de lire le message **(11)**.

Dans le cas d'un utilisateur associé à une entreprise communiquant avec un utilisateur non associé à une entreprise, le même échange se produit, la seule différence étant qu'un des deux KMS est exploité et géré par Cisco.

Vérifiabilité

Les protocoles utilisés par Cisco Spark, y compris ceux pour la gestion des clés, correspondent à des standards IETF ou W3C existants ou en attente de validation, comme indiqué dans ce document. Ces protocoles, lorsqu'ils sont mis en œuvre correctement, garantissent la sécurité intégrale des contenus de l'entreprise. Même si le client peut facilement vérifier le niveau de protocole par le biais d'une inspection des paquets, le fonctionnement interne des services du domaine de sécurité n'est pas aussi facile à examiner. Afin de résoudre ce problème d'opacité, les services du domaine de sécurité peuvent fournir des journaux d'audit, que vous pouvez comparer aux données d'utilisation du client et aux accès aux services cloud explicitement autorisés pour vérifier que le système fonctionne comme prévu. En outre, Cisco donne aux entreprises clientes l'accès au code source des composants du domaine de sécurité afin de leur permettre de les inspecter, de les compiler et de les comparer avec les mêmes composants proposés sous forme binaire pour le déploiement.

Chiffrement en temps réel

Tous les supports médias pris en charge par Cisco Spark, comme la voix, la vidéo et le partage de bureau utilisent le protocole SRTP (Secure Real-Time Transport, comme défini dans RFC 3711). À l'heure actuelle, *le cloud Cisco Spark déchiffre ces supports médias en temps réel à des fins de combinaison, de distribution, de démarcation et de trunking RTPC (Réseau téléphonique public commuté).*

Pour continuer à améliorer la sécurité du protocole SRTP, Cisco est également l'un des acteurs majeurs du nouveau groupe de travail PERC (Privacy Enhanced RTP Conferencing) de l'IETF. L'objectif du groupe PERC est de créer des supports médias totalement chiffrés qui peuvent néanmoins être authentifiés à chaque étape. À mesure que ce nouveau standard se développera, Cisco Spark utilisera ce nouveau mode de chiffrement en temps réel : les clés de chiffrement en temps réel reposeront sur le KMS, et le cloud Cisco Spark ne déchiffrera plus les communications compatibles avec les processus PERC. Les processus PERC n'affecteront pas le déchiffrement des appels RTPC, qui nécessite un mode de déchiffrement dans le cloud par le fournisseur RTPC. Pour plus d'informations sur le groupe de travail PERC, consultez https://datatracker.ietf.org/wg/perc.

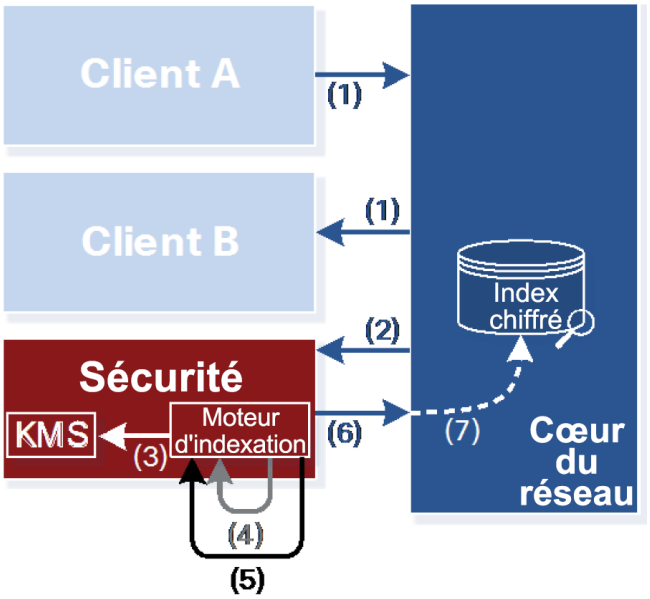
© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Recherche chiffrée : sécurité et rapidité

Comme le domaine central de Spark ne lit jamais de contenu en clair, on pourrait penser que la recherche dans les messages du cloud est impossible. Mais nous avons mis au point une façon innovante d'effectuer des recherches globales dans les messages sans que le domaine central de Cisco Spark n'ait de capacité de déchiffrement.

Pour cela, nous avons ajouté un autre composant au domaine de sécurité : le moteur d'indexation. Comme le KMS, le moteur d'indexation est séparé du domaine central tant au niveau architectural qu'opérationnel, mais il est étroitement lié au KMS. Il joue un rôle essentiel dans les deux tâches principales requises pour effectuer une recherche globale dans les messages : construire et interroger le moteur d'indexation.

Figure 4 : Séquence d'indexation des messages



Construire l'index de recherche

La première étape consiste à construire l'index de recherche.

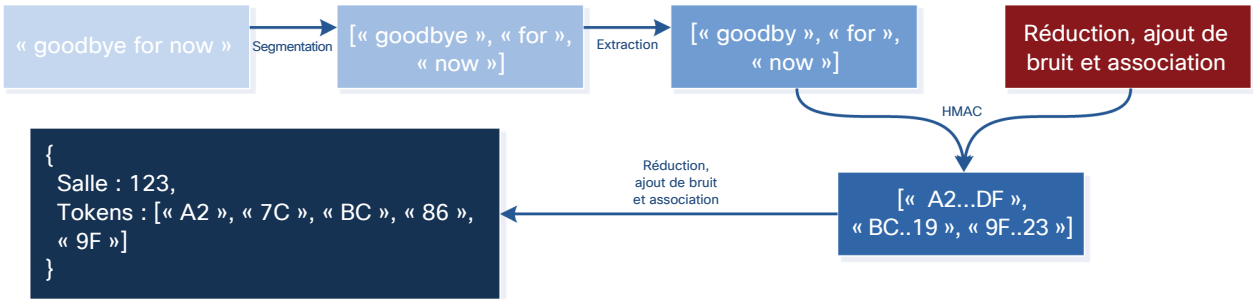
- Chaque fois qu'un utilisateur envoie un message dans Spark **(1)**, le message est envoyé au moteur d'indexation sous forme totalement chiffrée, comme illustré en **(2)** dans la Figure 4. Le moteur d'indexation interroge ensuite le KMS pour obtenir la clé de conversation requise pour déchiffrer le message. Le moteur d'indexation est un Spark Bot[4] ; il est invité dans chaque salle par le biais de la politique de l'entreprise pour aider à la recherche.
- KMS fournit la bonne clé de conversation au moteur d'indexation, car ce dernier est un participant actif de la salle et il est autorisé à déchiffrer les ressources de la salle **(3)**.
- Le moteur d'indexation déchiffre le message et le divise selon chaque mot qui le compose **(4).**
- Le moteur d'indexation applique alors un hachage unidirectionnel cryptographique à chaque mot, ou à ses racines, à l'aide d'une clé de recherche spécifique à la salle5[5] et enregistrée dans le KMS **(5)**. Par exemple, « à plus tard » est divisé en « à », « plus » et « tard », et chaque mot est haché. On obtient alors une liste de mots hachés qui appartiennent tous à la salle où le message a été publié. Les hachages sont en fait un chiffrement unidirectionnel : un hachage particulier ne peut pas être restauré pour reconstituer le message d'origine. Le moteur d'indexation ajoute à la liste des hachages aléatoires de type « bruit » pour garantir que les messages de la salle ne pourront pas être restaurés via une analyse de fréquence. (Les mots comme « et » et « le » apparaissant fréquemment dans la langue française, ajouter du bruit garantit que les hachages de la salle ne suivent pas la même distribution de fréquence.)
- Lors de la dernière étape, le moteur d'indexation envoie cette liste de hachages au cloud Spark **(6)**, qui la stocke dans l'index de recherche sous forme chiffrée **(7)**. Le cloud Spark dispose alors d'un index comprenant chaque mot de chaque message associé aux salles, sous une forme chiffrée qu'il ne peut pas déchiffrer.

[4] Voir *Intégrations et évolutivité*, ci-dessous.

[5] Utilise des HMAC SHA-256 tronqués à 80 bits.

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Figure 5 : Flux de données de l'index de messagerie

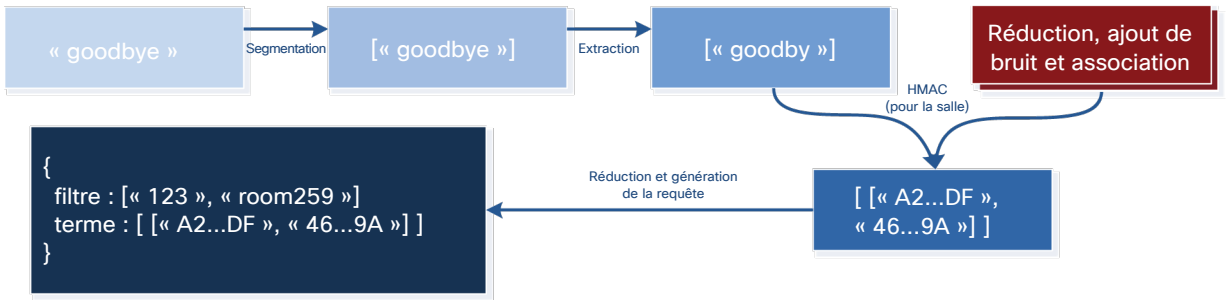


Interroger l'index de recherche

Lorsqu'un utilisateur effectue une recherche, le client interagit avec le moteur d'indexation comme si l'utilisateur et lui avaient une conversation individuelle. Cela signifie que le chiffrement total décrit précédemment pour les conversations entre utilisateurs est aussi utilisé pour les requêtes envoyées par l'utilisateur au moteur d'indexation.

De plus, la requête de recherche est d'abord chiffrée sur le client de l'utilisateur à l'aide d'une clé de chiffrement total conçue spécifiquement pour chiffrer les communications entre le client d'un utilisateur et le moteur d'indexation. Chaque utilisateur est associé à un moteur d'indexation spécifique. Le client de l'utilisateur envoie la requête chiffrée au cloud Spark, qui la transfère au moteur d'indexation avec la liste des salles auxquelles l'utilisateur est autorisé à accéder. Le cloud Spark ne peut pas déchiffrer la requête de recherche, car elle est chiffrée avec une clé à laquelle il n'a pas accès, c'est-à-dire la clé de chiffrement total de cette conversation particulière du client avec le moteur d'indexation.

Figure 6 : Flux de données de recherche



Le moteur d'indexation effectue ensuite les mêmes étapes que lors de la construction de l'index de recherche : il divise la requête en mots et en racines de mots, puis les hache à l'aide de la clé de recherche de la salle, et ce pour chaque salle auxquelles l'utilisateur a accès. Ainsi, si un utilisateur qui appartient à 10 salles saisit une requête composée de deux mots, le moteur d'indexation générera un minimum de 20 termes de recherche hachés, et potentiellement bien plus selon le nombre de racines que possède chaque mot. Le moteur d'indexation envoie ensuite cette liste de termes de recherche hachés au cloud Spark.

Le domaine central de Spark recherche ensuite des correspondances dans l'index de recherche. À mesure qu'il y trouve des salles associées aux hachages reçus par le moteur d'indexation, il établit une liste qu'il renvoie au client de l'utilisateur. Ce client recoupe les résultats avec les clés de conversation associées, présentes dans sa mémoire cache ou extraites du KMS, et affiche les résultats de la recherche pour l'utilisateur.

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Un compromis optimal

Nous avons développé la fonctionnalité de recherche de Spark sans compromettre la sécurité ni l'expérience de l'utilisateur. Bien qu'une seule recherche puisse générer et comparer des milliers de termes de recherche hachés, la recherche sur Spark est aussi rapide que ce à quoi les utilisateurs sont habitués dans les moteurs de recherche en ligne.

Intégrations et évolutivité

Même si le cloud Cisco Spark constitue une excellente plate-forme ainsi qu'un outil collaboratif d'une grande efficacité, nous savons que nos partenaires et nos clients aiment personnaliser et enrichir nos solutions. Notre objectif est de rendre nos API faciles à prendre en main et à utiliser. Les développeurs ont besoin d'API complètes, mais néanmoins simples, pour pouvoir se concentrer sur leurs propres applications plutôt que sur la complexité d'une plate-forme. Nous avons fait d'innombrables efforts pour rendre nos API aussi élégantes que possible et dissimuler les complexités de la plate-forme sous-jacente.

Nous sommes conscients que les développeurs, les partenaires et les clients voudront enrichir la plate-forme de nouvelles fonctionnalités nécessitant l'accès au contenu, alors même que le domaine central du cloud Cisco Spark ne peut pas y accéder. C'est pourquoi les extensions du cloud Cisco Spark se trouvent en dehors du domaine central et doivent être explicitement activées par un client ou un utilisateur. Les clients peuvent ainsi choisir où déployer leurs extensions de plate-forme, les utilisateurs qui les gèrent et les ressources auxquelles elles ont accès. Les intégrations et les extensions de Cisco Spark requièrent l'accès aux clés de chiffrement, comme indiqué dans la section Fonctions nécessitant un accès aux clés.

Trois catégories d'intégrations sont actuellement possibles : l'intégration avec les robots, les applications ou les webhooks. Mais nos clients et les développeurs tiers enrichiront sans doute la plate-forme de fonctionnalités innovantes que nous n'avons pas prévues nous-mêmes. Pour plus d'informations sur les API cloud Cisco Spark, consultez https://developer.ciscospark.com.

Robots

Les robots offrent des fonctionnalités supplémentaires aux entreprises, par exemple un service d'enregistrement des appels. Les robots doivent créer des salles ou être invités dans les salles auxquelles ils ont besoin d'accéder. Les invitations à rejoindre une salle peuvent provenir de la politique de l'entreprise ou d'un utilisateur qui se trouve déjà dans la salle.

Applications

Les applications offrent des fonctionnalités supplémentaires aux utilisateurs, par exemple un assistant personnel ou une traduction de document. À bien des égards, une application peut être considérée comme un client hébergé dans le cloud ou sur un serveur, mais sans interface utilisateur. Les applications ont accès à toutes les salles auxquelles l'utilisateur associé a accès, mais ce dernier peut exclure l'application de salles spécifiques.

Webhooks

Les webhooks fournissent un accès par URL unique à des fonctionnalités du domaine central de Spark, comme la publication de contenu dans une salle ou l'envoi de notifications relatives aux nouveaux contenus. Les webhooks se comportent comme les robots et les applications : ils peuvent avoir leur propre identité, comme un robot, ou utiliser l'identité d'un utilisateur, comme une application. Leur fonctionnement par URL unique est rendu possible par l'intégration de tokens d'accès OAuth2 à longue durée de validité et à portée limitée dans la chaîne de requête de l'URL, et par l'exécution de l'ensemble du chiffrement et du déchiffrement des contenus dans le webhook.

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Dans les deux cas, la portée des webhooks est limitée à une ressource unique (par exemple, une salle) ; ces limitations d'accès sont configurées et sécurisées lors de leur ajout.

Plusieurs options pour les utilisateurs et les entreprises

Nous pensons que la sécurité du cloud Cisco Spark est la meilleure du secteur, mais nous savons aussi que chaque client Cisco a ses propres exigences de sécurité. Le choix offert aux clients est essentiel au fonctionnement de ce modèle hybride. Ils peuvent choisir d'utiliser uniquement le domaine central ou de l'enrichir avec des robots, des applications et des webhooks. Les entreprises peuvent définir une politique autorisant des robots et des applications spécifiques. Les utilisateurs peuvent faire des choix concernant des applications respectant cette politique d'entreprise. La plate-forme Cisco Spark est conçue sur la base d'API bien documentées et standardisées, ce qui signifie que les composants situés hors du domaine central (robots, applications et webhooks) peuvent être obtenus auprès de tiers ou développés par les entreprises.

Association de certificat

Les communications Spark entre le client et le domaine central se font via une connexion TLS chiffrée. Les clients utilisent la technique dite de l'*association de certificat* pour garantir que les communications ne sont pas interceptées, lues ou modifiées en cours d'acheminement. Cisco associe les certificats à certaines autorités CA racines qui s'engagent à ne pas produire de certificats intermédiaires de deux façons : via la déclaration CPS (Déclaration des pratiques de certification) du fournisseur et en faisant en sorte que le certificat racine contienne un champ « pathLenConstraint » défini sur zéro (0) dans l'extension BasicConstraints pour indiquer qu'aucun certificat CA ne suivra le certificat d'émission dans le chemin de certification.

Confidentialité des données

Notre engagement à fournir un service fiable n'est pas limité à la protection des contenus des utilisateurs. Dans Spark, les données sur les utilisateurs et l'utilisation du système sont protégées à l'aide d'une combinaison d'outils de confidentialité et de fonctionnalités incluant l'identité masquée, la gestion granulaire des rôles d'administrateurs, le choix d'options pour les utilisateurs et les entreprises, et la transparence. Ces protections sont entièrement intégrées dans le service dès le départ, comme l'est le chiffrement total.

Identité masquée

Les services de collaboration reposent sur un concept central d'identité de l'utilisateur. Les utilisateurs veulent communiquer rapidement avec leurs équipes, rechercher d'autres utilisateurs par nom, e-mail ou numéro de téléphone et vérifier leur identité avec une photo de profil. Cependant, les informations sur leur identité peuvent se révéler sensibles, du point de vue de l'utilisateur et de l'entreprise. Révéler uniquement les informations sur l'identité dans les contextes où c'est nécessaire est un des principes fondamentaux de Spark.

Pour limiter l'exposition des informations sur l'identité des utilisateurs, nous faisons la distinction entre identité « véritable » et « masquée » dans le cloud Spark. Les données que nous collectons dans le cadre d'une inscription sur Spark (nom d'utilisateur, e-mail, téléphone, etc.) sont considérées comme l'identité « véritable » de l'utilisateur et stockées dans son profil via un composant du cloud Spark appelé Common Identity. Pour chaque utilisateur, nous générons également un identifiant universel unique (UUID) aléatoire de 128 bits, qui constitue son identité masquée. De même, pour les entreprises, nous générons un identifiant d'entreprise (ID) aléatoire de 128 bits qui constitue leur identité masquée. Nous utilisons l'identité masquée partout dans les services Spark, notamment pour les fonctionnalités suivantes :

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

- **Le routage des messages :** tous les messages envoyés via Spark sont acheminés de l'expéditeur au destinataire sur la base d'une identité masquée. Toutes les requêtes internes au cloud et liées à des utilisateurs recourent également à l'identité masquée. C'est le cas de toutes les interactions entre le KMS et le moteur d'indexation décrites ci-dessus.
- **La journalisation côté serveur :** tous les journaux générés par les composants de l'application cloud Spark à des fins de dépannage utilisent l'identité masquée.
- **L'analytique :** Spark fonctionne sur un modèle DevOps ; notre équipe de développement prend des décisions sur la façon d'améliorer le service en analysant les données relatives aux performances et à l'utilisation. L'équipe base ses décisions sur l'analyse des enregistrements de l'utilisation de Spark, dans lesquels l'identité de chacun est masquée.

Les clients et les composants du service cloud qui y sont autorisés peuvent néanmoins accéder à la véritable identité d'un utilisateur ou d'une entreprise lorsque celle-ci doit être restituée dans un client Spark, dans le portail Cisco de gestion des solutions de collaboration cloud ou lors d'une intégration avec un système tiers. Dès qu'un client Spark, un composant cloud, une application ou un robot a besoin d'accéder à une identité véritable, il est authentifié auprès de Common Identity, qui communique ces informations uniquement aux utilisateurs autorisés.

Gestion granulaire des rôles d'administrateurs

Chaque client et partenaire Spark a accès au portail Cisco de gestion des solutions de collaboration cloud, qui offre une gestion globale du service comprenant les essais, l'achat, la configuration de comptes, l'adoption, l'assistance aux clients et l'utilisation d'API de développeurs. Nous savons que ces fonctionnalités peuvent impliquer l'accès à des informations sensibles concernant les utilisateurs, les comptes, l'utilisation du produit et les données de configuration. C'est pourquoi nous avons créé le portail de façon à prendre en charge différents rôles d'administrateurs ayant accès à différents sous-ensembles de données. Par exemple, les administrateurs d'assistance peuvent accéder aux informations sur les utilisateurs et aux journaux d'assistance, tandis que les administrateurs commerciaux de nos partenaires sont limités aux rapports d'utilisation agrégés et à la gestion des essais de service. Les administrateurs globaux ont accès à toutes les fonctionnalités du portail et peuvent attribuer les rôles adéquats aux autres administrateurs de leur entreprise.

Nous proposons ces rôles aux partenaires et aux clients, et nous les utilisons également pour autoriser uniquement les administrateurs Cisco qui en ont réellement besoin à accéder aux données. Nos administrateurs et ingénieurs d'assistance peuvent accéder aux journaux d'assistance et aux informations sur les utilisateurs pour aider les clients et les partenaires lors d'un dépannage, tandis que nos équipes en charge des ventes et de la réussite client disposent du rôle d'administrateur des ventes avec un accès limité.

Plusieurs options pour les utilisateurs et les entreprises

Spark est conçue pour permettre aux utilisateurs et aux entreprises de paramétrer la confidentialité sans avoir à appréhender une interface complexe. Parmi les options disponibles pour les administrateurs de l'entreprise :

- **La connexion unique (SSO) :** les administrateurs peuvent configurer Spark pour l'utiliser avec leurs solutions SSO. Nous prenons en charge les fournisseurs d'identité utilisant le langage SAML 2.0 (Security Assertion Markup Langage) et OAuth 2.0.
- **La synchronisation des répertoires :** les administrateurs qui utilisent Microsoft Active Directory peuvent faire apparaître en temps réel dans Spark les changements apportés au cycle de vie des employés.
- **Le partage des données avec un partenaire Cisco :** les entreprises peuvent choisir de partager les données sur la qualité de service et sur l'engagement avec leurs partenaires Cisco afin de renforcer l'assistance reçue.

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Parmi les options disponibles pour les utilisateurs :

- **Les autorisations pour les appareils :** en fonction du navigateur ou du terminal mobile sur lequel l'utilisateur exécute Spark, le client demande différentes autorisations portant sur le téléphone, le microphone, la caméra, l'enregistrement audio, le partage d'écran, le calendrier, les contacts, les fichiers et les photos, et les notifications Push. Sur la plupart des plates-formes, cette autorisation doit être explicitement accordée par l'utilisateur, qui peut la révoquer à tout moment.
- **Les fonctionnalités de proximité :** sur les terminaux mobiles, les clients Spark actifs peuvent s'associer automatiquement à des terminaux vidéo et audio en détectant les signaux ultrasons. Cette fonctionnalité requiert l'utilisation du microphone du terminal, mais les utilisateurs peuvent la désactiver s'ils le souhaitent.
- **Les photos de profil :** les photos de profil ne sont pas obligatoires pour utiliser Spark.
- **Les indicateurs de participants externes :** les clients de Cisco Spark peuvent indiquer visuellement quand une salle contient des participants qui ne font pas partie de leur entreprise.
- **Les fonctions de modération en salle :** les utilisateurs peuvent modérer les salles et donner à certains participants les droits de modérateur disposant d'un contrôle exclusif sur le nom de la salle et la liste de ses participants.

Transparence

Nous souhaitons que nos utilisateurs et nos clients comprennent les options qui leur sont proposées et la façon dont nous gérons et protégeons les données qu'ils nous confient. Nous utilisons un modèle de transparence hiérarchisé pour y parvenir. Nos courtes publications aident les utilisateurs à prendre des décisions en temps réel depuis le client Spark lui-même. Des détails supplémentaires sont disponibles dans nos pages d'assistance, que nous mettons à jour régulièrement. La déclaration de confidentialité de Cisco en ligne contient un supplément sur la confidentialité dans Spark, détaillant les informations que nous collectons, la façon dont nous les utilisons et la façon dont nous les protégeons.

Sécurité de la plate-forme et des services

En plus de suivre le cycle de développement sécurisé de Cisco, Cisco Spark exécute des tests de pénétration internes et externes fréquents, en boîte blanche et en boîte noire, sur la plate-forme et les services Spark. Vous trouverez plus d'informations sur le cycle de développement sécurisé Cisco à l'adresse www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle.html

Gestion des incidents et politiques de sécurité internes

Traitement des incidents de sécurité des produits Cisco

L'équipe PSIRT est chargée de répondre aux incidents de sécurité impliquant des produits Cisco. L'équipe PSIRT est une équipe mondiale en charge de collecter, d'analyser et de publier les informations sur les vulnérabilités de sécurité relatives aux produits et aux réseaux Cisco. L'équipe d'intervention PSIRT travaille 24 heures sur 24 à identifier les vulnérabilités potentielles des produits et réseaux Cisco, en collaboration avec nos clients, des centres de recherche indépendants, des consultants et d'autres entreprises du secteur.

Signaler un risque pour la sécurité et obtenir une assistance

Nous encourageons vivement les particuliers et les professionnels confrontés à un problème de sécurité sur un produit à le signaler à l'équipe PSIRT de Cisco. Tous les signalements sont les bienvenus, qu'ils proviennent de chercheurs indépendants, d'entreprises du secteur, de fournisseurs tiers, de clients ou de toute autre source concernée par la sécurité des produits et des réseaux. L'équipe PSIRT peut être contactée de deux façons :

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

	Assistance d'urgence
Téléphone	+1 877 228 7302 (numéro vert en Amérique du Nord) ; +1 408 525 6532 (numérotation internationale)
Heures	24 heures sur 24, 7 jours sur 7
	Assistance non urgente
E-mail	psirt@cisco.com
Heures	Les demandes d'assistance reçues par e-mail sont généralement traitées sous 48 heures.

Vous trouverez plus d'informations à l'adresse www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Transparence et demandes d'accès aux données des clients par les services de police

Cisco s'engage à publier les informations sur les demandes d'accès aux données de ses clients émanant des services de police et de sécurité nationale du monde entier. Nous publions ces données deux fois par an (couvrant ainsi une période allant de janvier à juin et de juillet à décembre). Comme les autres entreprises technologiques, nous publions ces informations six mois après la fin de l'accès aux données, conformément aux règles applicables en la matière. Vous trouverez plus d'informations à l'adresse www.cisco.com/web/about/doing_business/trust-center/transparency-report.html

Siège social aux États-Unis
Cisco Systems, Inc.
San José. CA

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site web de Cisco, à l'adresse : **http://www.cisco.com/go/offices**.

Cisco et le logo Cisco sont des marques commerciales ou des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques commerciales Cisco, visitez le site : www.cisco.com/go/trademarks. Les autres marques mentionnées dans les présentes sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat commercial entre Cisco et d'autres entreprises. (1110R)

COLLAB-SPARK-0616

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.