Questions et réponses sur le certificat IM and Presence et ECDSA

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Discussion de l'équipe produit IM&P sur l'ECDSA](#)
[Ce paramètre indique-t-il que IM&P choisit RSA s'il doit choisir entre RSA et ECDSA ?](#)
[Dans quelles conditions Cisco IM and Presence peut-il envoyer l'ECDSA même si All Ciphers RSA Preferred est sélectionné ?](#)
[Si l'ECDSA a une priorité plus élevée, peut-elle être choisie même si All Ciphers RSA Preferred est sélectionné ?](#)
[Il est évident que l'on peut sélectionner les algorithmes de chiffrement ayant la priorité la plus élevée. Lorsqu'un client tiers envoie un message Hello avec sa suite de chiffrement, Cisco IM and Presence choisit-il le chiffrement le plus fort dans cette liste de la page TLS Cipher Mapping for 3rd party clients que le serveur et le client prennent en charge ?](#)
[Y a-t-il un document qui clarifie ces choses ?](#)
[Tous les paramètres RSA Preferred de Ciphers sont importants uniquement lorsque CUCM/IMP agit en tant que client ?](#)
[Cela signifie-t-il que CUCM/IMP (client) envoie des certificats RSA et ECDSA, mais que les certificats RSA peuvent avoir la priorité la plus élevée ?](#)
[Sur la page d'aide du chiffrement TLS, il est indiqué que les chiffrement sont inclus dans cette commande. Cela signifie-t-il que les chiffrements sont envoyés dans cet ordre lorsque cette option est sélectionnée ?](#)
[Le paramètre All Ciphers RSA Preferred n'a pas d'importance lorsque CUCM/IMP agit en tant que serveur. Dans ce cas, CUCM/IMP répond avec un type de certificat qui a la priorité la plus élevée dans le message Hello du client ?](#)
[Si ce paramètre fait uniquement référence à SIP/CTI, existe-t-il un paramètre équivalent pour les connexions TLS avec des interfaces XMPP ?](#)

Introduction

Ce document répond aux questions relatives aux certificats ECDSA (Elliptic Curve Digital Signature Algorithm) qui fonctionnent avec l'appareil de messagerie instantanée et de présence Cisco (IM&P).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestionnaire de communications unifiées de Cisco (version CUCM)
- Cisco IM and Presence (IMP)
- Session Initiation Protocol (SIP)
- Intégration de la téléphonie informatique (CTI)
- Cryptage RSA (Rivest-Shamir-Adleman)
- Algorithme de signature numérique de courbe elliptique (ECDSA)
- eXtensible Messaging and Presence Protocol (XMPP)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Messagerie instantanée et présence Cisco 11.5.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Discussion de l'équipe produit IM&P sur l'ECDSA

En référence au paramètre d'entreprise Chiffres TLS (Transport Layer Security), la sélection par défaut est **All Ciphers RSA Preferred**. Par conséquent, en ce qui concerne les chiffrements de paramètres TLS, les questions suivantes ont été posées à l'équipe d'ingénierie de GI&P.

> **Note**: Toutes les questions sont répondues et vérifiées par l'équipe d'ingénierie de la GI-P.

Ce paramètre indique-t-il que IM&P choisit RSA s'il doit choisir entre RSA et ECDSA ?

Oui. Ce paramètre est uniquement pour l'interface SIP/CTI de CUCM. Les algorithmes de chiffrement RSA sont privilégiés par rapport aux algorithmes ECDSA.

Dans quelles conditions Cisco IM and Presence peut-il envoyer l'ECDSA même si All Ciphers RSA Preferred est sélectionné ?

Il s'agit de donner la préférence aux chiffrement RSA, mais il possède également des chiffrement ECDSA, mais lorsque le client initie une connexion, il envoie des chiffrement RSA au-dessus de l'ECDSA.

Si l'ECDSA a une priorité plus élevée, peut-elle être choisie même si All Ciphers RSA Preferred est sélectionné ?

Oui. Ce paramètre n'entre dans l'image que lorsque CUCM agit en tant que client. La préférence est donnée à l'ordre dans lequel le client initie la connexion. Si le client initie une connexion avec les chiffrement ECDSA en haut, la connexion se produit avec ECDSA. Si ce n'est pas le cas, RSA

est privilégié.

Il est évident que l'on peut sélectionner les algorithmes de chiffrement ayant la priorité la plus élevée. Lorsqu'un client tiers envoie un message Hello avec sa suite de chiffrement, Cisco IM and Presence choisit-il le chiffrement le plus fort de cette liste sur la page Mappage de chiffrement TLS pour les clients tiers que le serveur et le client prennent en charge ?

Oui. Lorsque le serveur agit en tant que client, il envoie le chiffre dans l'ordre indiqué dans les questions précédentes.

Y a-t-il un document qui clarifie ces choses ?

Oui. Une option d'aide est disponible dès que vous sélectionnez le lien **TLS Ciphers** sur la page des paramètres d'entreprise qui indique la liste des chiffrements pris en charge.

Tous les paramètres RSA Preferred de Ciphers sont importants uniquement lorsque CUCM/IMP agit en tant que client ?

Oui.

Cela signifie-t-il que CUCM/IMP (client) envoie des certificats RSA et ECDSA, mais que les certificats RSA peuvent avoir la priorité la plus élevée ?

Oui.

Sur la page d'aide du chiffrement TLS, il est indiqué que les chiffrement sont inclus dans cette commande. Cela signifie-t-il que les chiffrements sont envoyés dans cet ordre lorsque cette option est sélectionnée ?

Tous les chiffrement RSA favoris

Comprend les Chiffres dans l'ordre suivant :

TLS_ECDHE_RSA avec AES256_GCM_SHA384

TLS_ECDHE_ECDSA avec AES256_GCM_SHA384

TLS_ECDHE_RSA avec AES128_GCM_SHA256

TLS_ECDHE_ECDSA avec AES128_GCM_SHA256

TLS_RSA avec AES_128_CBC_SHA1

Oui.

Le paramètre All Ciphers RSA Preferred n'a pas d'importance lorsque CUCM/IMP agit en tant que serveur. Dans ce cas, CUCM/IMP répond avec un type de certificat qui a la priorité la plus élevée dans le message Hello du client ?

Oui.

Si ce paramètre fait uniquement référence à SIP/CTI, existe-t-il un paramètre équivalent pour les connexions TLS avec des interfaces XMPP ?

Non. Il existe une amélioration de fonctionnalité pour XMPP, mais elle n'est pas encore implémentée.