

Preguntas y respuestas sobre el certificado de IM and Presence y ECDSA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Debate del equipo de productos de IM&P sobre ECDSA](#)

[¿Este parámetro indica a IM&P que selecciona RSA si tiene que elegir entre RSA y ECDSA?](#)

[¿En qué condiciones puede Cisco IM and Presence enviar ECDSA aunque se hayan seleccionado Todos los cifradores RSA preferidos?](#)

[Si ECDSA tiene una prioridad más alta, ¿se puede elegir aunque se haya seleccionado Todos los cifradores RSA Preferred?](#)

[Obviamente, se puede seleccionar qué cifras tienen la prioridad más alta. Cuando un cliente de terceros envía un mensaje Hello con su paquete de cifrado, ¿Cisco IM and Presence elige el cifrado más sólido de esta lista en la página de asignación de cifrado TLS para clientes de terceros que admite tanto el servidor como el cliente?](#)

[¿Hay algún documento que aclare estas cosas?](#)

[¿Todos los parámetros preferidos RSA de los Cifers sólo importan cuando CUCM/IMP actúa como cliente?](#)

[¿Significa esto que CUCM/IMP \(cliente\) envía los certificados RSA y ECDSA, pero los certificados RSA pueden tener la prioridad más alta?](#)

[En la página de ayuda del cifrado TLS se indica que los cifrados se incluyen en este pedido.](#)

[¿Significa esto que los cifrados se envían en ese orden cuando se selecciona esta opción?](#)

[El parámetro All Ciphers RSA Preferred no importa cuando CUCM/IMP actúa como servidor. En ese caso, CUCM/IMP responde con un tipo de certificado que tiene la prioridad más alta en el mensaje Hello del cliente?](#)

[Si este parámetro se refiere solamente a SIP/CTI, ¿hay un parámetro equivalente para las conexiones TLS con interfaces XMPP?](#)

Introducción

Este documento responde a preguntas relacionadas con los certificados del algoritmo de firma digital de curva elíptica (ECDSA) que funcionan con el dispositivo Cisco IM and Presence (IM&P).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Communications Manager (CUCM)
- Cisco IM and Presence (IMP)

- Protocolo de inicio de sesión (SIP)
- Computer Telephony Integration (CTI)
- Cifrado Rivest-Shamir-Adleman (RSA)
- Algoritmo de firma digital de curva elíptica (ECDSA)
- Protocolo extensible de mensajería y comunicación de presencia (XMPP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IM and Presence 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Debate del equipo de productos de IM&P sobre ECDSA

En referencia a los cifrados de seguridad de la capa de transporte (TLS) del parámetro empresarial, la selección predeterminada es **Todos los cifradores RSA preferidos**. Por lo tanto, en referencia a los parámetros de los cifradores TLS, se plantearon las siguientes preguntas al equipo de ingeniería de IM&P.

Nota: El equipo de ingeniería de IM&P responde y verifica todas las preguntas.

¿Este parámetro indica a IM&P que selecciona RSA si tiene que elegir entre RSA y ECDSA?

Yes. Este parámetro es sólo para la interfaz CUCM SIP/CTI. Se da preferencia a los cifrados RSA sobre el ECDSA.

¿En qué condiciones puede Cisco IM and Presence enviar ECDSA aunque se hayan seleccionado Todos los cifradores RSA preferidos?

Es para dar preferencia a los cifrados RSA pero también tiene cifrados ECDSA, pero cuando el cliente inicia una conexión envía cifrados RSA por encima de ECDSA.

Si ECDSA tiene una prioridad más alta, ¿se puede elegir aunque se haya seleccionado Todos los cifradores RSA Preferred?

Yes. Este parámetro entra en la imagen sólo cuando CUCM actúa como cliente. Se da preferencia al orden en el que el cliente inicia la conexión. Si el cliente inicia una conexión con los cifrados ECDSA en la parte superior, entonces la conexión ocurre con ECDSA. Si no es así, se da preferencia a RSA.

Obviamente, se puede seleccionar qué cifras tienen la prioridad más alta. Cuando un cliente de terceros envía un mensaje Hello con su conjunto de cifrado, ¿Cisco IM and Presence elige el cifrado más fuerte de esta lista en la página de asignación del cifrado TLS para clientes de terceros que tanto el servidor como el cliente admiten?

Yes. Cuando el servidor actúa como cliente, envía el cifrado en el orden en que se menciona en las preguntas anteriores.

¿Hay algún documento que aclare estas cosas?

Yes. Hay una opción de ayuda tan pronto como se selecciona el enlace **Cifradores TLS** en la página de parámetros empresariales que indica la lista de los cifrados admitidos.

¿Todos los parámetros preferidos RSA de los Cifers sólo importan cuando CUCM/IMP actúa como cliente?

Yes.

¿Significa esto que CUCM/IMP (cliente) envía los certificados RSA y ECDSA, pero los certificados RSA pueden tener la prioridad más alta?

Yes.

En la página de ayuda del cifrado TLS se indica que los cifrados se incluyen en este pedido. ¿Significa esto que los cifrados se envían en ese orden cuando se selecciona esta opción?

Todos los cifrados preferidos por RSA

Incluye los cifrados en el siguiente orden:

TLS_ECDHE_RSA con AES256_GCM_SHA384

TLS_ECDHE_ECDSA con AES256_GCM_SHA384

TLS_ECDHE_RSA con AES128_GCM_SHA256

TLS_ECDHE_ECDSA con AES128_GCM_SHA256

TLS_RSA con AES_128_CBC_SHA1

Yes.

El parámetro All Ciphers RSA Preferred no importa cuando CUCM/IMP actúa como servidor. En ese caso, CUCM/IMP responde con un tipo de certificado que tiene la prioridad más alta en el mensaje Hello del cliente?

Yes.

Si este parámetro se refiere solamente a SIP/CTI, ¿hay un parámetro equivalente para las conexiones TLS con interfaces XMPP?

No. Hay una mejora de la función para XMPP, pero todavía no se ha implementado.