IM and Presence and ECDSA certificate Questions and Answers

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[IM&P Product Team Discussion on ECDSA](#)
[Does this parameter tells IM&P picks RSA if it has to choose between RSA and ECDSA?](#)
[Under what conditions can Cisco IM and Presence send ECDSA even though All Ciphers RSA Preferred is selected?](#)
[If ECDSA has higher priority, can it be chosen even though All Ciphers RSA Preferred is selected?](#)
[One can obviously select which ciphers has the top priority. When a 3rd party client sends a Hello message with its cipher suite, does Cisco IM and Presence chooses the strongest cipher from this list on the TLS Cipher Mapping for 3rd party clients page that both the server and client support?](#)
[Is there any document that clarifies these things?](#)
[All Ciphers RSA Preferred parameter only matters when CUCM/IMP is acting as a client?](#)
[Does it mean that CUCM/IMP (client) sends both RSA and ECDSA certificates but RSA certificates can have highest priority?](#)
[On TLS cipher help page it says that ciphers are included in this order. Does that mean that ciphers are sent in that order when this option is selected?](#)
[The All Ciphers RSA Preferred parameter doesn't matter when CUCM/IMP acts as a server. The CUCM/IMP in that case responds with a certificate type that has the highest priority in the client's Hello message?](#)
[If this parameter refers only to SIP/CTI, is there an equivalent parameter for TLS connections with XMPP interfaces?](#)

Introduction

This document answers questions related to the Elliptic Curve Digital Signature Algorithm (ECDSA) certificates that works with the Cisco IM and Presence (IM&P) appliance.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Communications Manager (CUCM)
- Cisco IM and Presence (IMP)
- Session Initiation Protocol (SIP)
- Computer Telephony Integration (CTI)
- Rivest-Shamir-Adleman (RSA) Encryption

- Elliptic Curve Digital Signature Algorithm (ECDSA)
- Extensible Messaging and Presence Protocol (XMPP)

Components Used

The information in this document is based on these software and hardware versions:

- 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. If your network is live, ensure that you understand the potential impact of any command.

IM&P Product Team Discussion on ECDSA

In reference to the enterprise parameter Transport Layer Security (TLS) ciphers, the default selection is **All Ciphers RSA Preferred**. So in reference to parameter TLS ciphers, the following questions were raised with the IM&P Engineering team.

> **Note**: All questions are answered and verified by the IM&P Engineering Team.

Does this parameter tells IM&P picks RSA if it has to choose between RSA and ECDSA?

Yes. This parameter is only for CUCM SIP/CTI interface. RSA ciphers is given preference over ECDSA.

Under what conditions can Cisco IM and Presence send ECDSA even though All Ciphers RSA Preferred is selected?

It is for giving preference to RSA ciphers but it has ECDSA ciphers as well, but when client initiates a connection it sends RSA ciphers above ECDSA.

If ECDSA has higher priority, can it be chosen even though All Ciphers RSA Preferred is selected?

Yes. This parameter comes into the picture only when CUCM acts as a client. The preference is given to order in which the client initiates the connection. If the client initiates a connection with ECDSA ciphers on the top, then the connection happens with ECDSA. If not then then RSA is given preference.

One can obviously select which ciphers has the top priority. When a 3rd party client sends a Hello message with its cipher suite, does Cisco IM and Presence chooses the

strongest cipher from this list on the TLS Cipher Mapping for 3rd party clients page that both the server and client support?

Yes. When server acts as a client it sends the cipher in the order it is mentioned in the previous questions.

Is there any document that clarifies these things?

Yes. There is a help option as soon as you select the **TLS Ciphers** link on the enterprise parameters page which states the list of the ciphers supported.

All Ciphers RSA Preferred parameter only matters when CUCM/IMP is acting as a client?

Yes.

Does it mean that CUCM/IMP (client) sends both RSA and ECDSA certificates but RSA certificates can have highest priority?

Yes.

On TLS cipher help page it says that ciphers are included in this order. Does that mean that ciphers are sent in that order when this option is selected?

All Ciphers RSA Preferred

Includes Ciphers in the following order:

TLS_ECDHE_RSA with AES256_GCM_SHA384

TLS_ECDHE_ECDSA with AES256_GCM_SHA384

TLS_ECDHE_RSA with AES128_GCM_SHA256

TLS_ECDHE_ECDSA with AES128_GCM_SHA256

TLS_RSA with AES_128_CBC_SHA1

Yes.

The All Ciphers RSA Preferred parameter doesn't matter when CUCM/IMP acts as a server. The CUCM/IMP in that case responds with a certificate type that has the highest priority in the client’s Hello message?

Yes.

If this parameter refers only to SIP/CTI, is there an equivalent parameter for TLS connections with XMPP interfaces?

No. There is a feature enhancement for XMPP, but it is not yet implemented.