# IM和在线状态和ECDSA证书问题和解答

## 目录



## 简介

与思科IM和在线状态的本文应答与椭圆曲线数字签名算法(ECDSA)证书涉及的问题(IM&P)设备一起使用。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- Cisco Unified Communications Manager (CUCM)
- 思科IM和在线状态(IMP)
- 会话初始化协议(SIP)
- 计算机电话集成(CTI)
- Rivest Shamir Adelman (RSA)加密
- 椭圆曲线数字签名算法(ECDSA)
- 可扩展消息传送和在线状态协议(XMPP)

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科IM和在线状态11.5.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请保证您了解所有命令潜在影响。

## IM&P在ECDSA的产品小组讨论

关于企业参数传输层安全(TLS)密码器，默认选项是**首选的所有密码器RSA**。因此关于参数TLS加密，以下问题上升了与IM&P工程组。

**注意**：所有问题由IM&P工程组应答并且验证。

## 如果必须选择在RSA和ECDSA之间，此参数告诉IM&P选择RSA？

可以。此参数仅是为CUCM SIP/CTI接口。 RSA密码器给在ECDSA的首选。

## 在思科能IM和在线状态发送什么情况下ECDSA，即使所有密码器RSA首选的选择？

它是为给首选对RSA密码器，但是有ECDSA密码器，但是，当客户端首次连接时它发送在ECDSA上的RSA密码器。

## 如果ECDSA有更加高优先级，能选择，即使所有密码器RSA首选的选择？

可以。只有当CUCM作为客户端时，此参数进入图片。首选在哪些给预定客户端首次连接。 如果客户端启动与ECDSA的一连接在上面加密，则连接发生与ECDSA。如果RSA然后不然后给首选。

## 一能明显地选择哪些密码器有最优先考虑的事。当第三方客户端传送与其密码器套件时的一个Hello消息， Cisco IM和在线状态从在TLS的此列表选择最强的密码器加密第三方服务器和客户端支持的客户端页的映射？

可以。当服务器作为客户端时发送密码器按在上一个问题被提及的顺序。

## 有没有澄清这些事的任何文档？

可以。有Help选项，当您在陈述支持的密码器列表的企业参数页选择**TLS密码器**连接。

## 当CUCM/IMP作为客户端时，所有密码器RSA更喜欢仅参数事态

## ？

可以。

## 它意味着CUCM/IMP (客户端)发送RSA和ECDSA证书，但是RSA证书能有最高优先级？

可以。

## 在Help页TLS的密码器上它说密码器按此顺序包括。该意味着密码器按该顺序发送，当此选项选择时？

首选的所有密码器RSA

在下列顺序包括密码器：

与AES256_GCM_SHA384的TLS_ECDHE_RSA

与AES256_GCM_SHA384的TLS_ECDHE_ECDSA

与AES128_GCM_SHA256的TLS_ECDHE_RSA

与AES128_GCM_SHA256的TLS_ECDHE_ECDSA

与AES_128_CBC_SHA1的TLS_RSA

可以。

## 当CUCM/IMP作为服务器，所有密码器RSA首选参数不重要。CUCM/IMP在那种情况下回应有最高优先级在客户端的Hello消息的证书类型？

可以。

## 如果此参数仅参考SIP/CTI，有没有TLS连接的等同的参数与XMPP接口？

不能。有XMPP的一种功能增强，但是没有实现。