IM и Присутствие и Вопросы и ответы сертификата ECDSA

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Обсуждение команды продукта IM&P ECDSA
Этот параметр говорит RSA выборов IM&P, если это должно выбрать между RSA и ECDSA?
При каких условиях IM Cisco и Присутствие могут передать ECDSA даже при том, что выбран Весь Предпочтительный RSA Шифров?
Если ECDSA имеет более высокий приоритет, он может быть выбран даже при том, что выбран Весь Предпочтительный RSA Шифров?
Можно, очевидно, выбрать, какие шифры имеет высший приоритет. Когда клиент третьей стороны передает Приветственное сообщение с его набором шифров, IM Cisco и Присутствие выбирают самый сильный шифр из этого списка на Сопоставлении Шифра TLS для страницы клиентов третьей стороны что и сервер и поддержка клиентов?
Есть ли какой-либо документ, который разъясняет эти вещи?
Когда CUCM/IMP действует как клиент, предпочтительный параметр RSA всех Шифров только имеет значение?
Это означает, что CUCM/IMP (клиент) передает и RSA и сертификаты ECDSA, но сертификаты RSA могут иметь наивысший приоритет?
На странице справки шифра TLS это говорит, что шифры включены в этот заказ. Это означает, что шифры передаются в том заказе, когда выбрана эта опция?
Когда CUCM/IMP действует как сервер, предпочтительный параметр RSA Всех Шифров не имеет значения. CUCM/IMP в этом случае отвечает Типом сертификата, который имеет наивысший приоритет в Приветственном сообщении клиента?
Если этот параметр обращается только к SIP/CTI, есть ли эквивалентный параметр для TLS подключение с интерфейсами XMPP?

Введение

Этот документ отвечает на вопросы, отнесенные к сертификатам Алгоритма цифровой подписи эллиптической кривой (ECDSA), который работает с IM Cisco и Присутствием (IM&P) устройство.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco Unified Communications Manager (CUCM)

- IM Cisco и присутствие (IMP)
- Session Initiation Protocol (SIP)
- Интеграция CTI
- Шифрование Ривест-Шамир-Адлемена (RSA)
- Алгоритм цифровой подписи эллиптической кривой (ECDSA)
- Расширяемый протокол обмена сообщениями и присутствия (XMPP)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- IM Cisco и присутствие 11.5.1

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

Обсуждение команды продукта IM&P ECDSA

В отношении Transport Layer Security корпоративного параметра (TLS) шифры, выбор по умолчанию является **Всем Предпочтительным RSA Шифров**. Таким образом в отношении шифров TLS параметра, следующие вопросы были подняты с Группой разработчиков IM&P.

Примечание: На все вопросы отвечает и проверяет Группа разработчиков IM&P.

Этот параметр говорит RSA выборов IM&P, если это должно выбрать между RSA и ECDSA?

Да. Этот параметр только для интерфейса SIP/CTI CUCM. Шифрам RSA дают предпочтение по ECDSA.

При каких условиях IM Cisco и Присутствие могут передать ECDSA даже при том, что выбран Весь Предпочтительный RSA Шифров?

Это для предоставления предпочтения к шифрам RSA, но это имеет шифры ECDSA также, но когда клиент инициирует соединение, это передает шифры RSA выше ECDSA.

Если ECDSA имеет более высокий приоритет, он может быть выбран даже при том, что выбран Весь Предпочтительный RSA Шифров?

Да. Этот параметр входит в изображение только, когда CUCM действует как клиент.

Предпочтение дано для заказа, в котором клиент инициирует соединение. Если клиент инициирует соединение с шифрами ECDSA на вершине, то соединение происходит с ECDSA. Если не тогда тогда RSA дают предпочтение.

Можно, очевидно, выбрать, какие шифры имеет высший приоритет. Когда клиент третьей стороны передает Приветственное сообщение с его набором шифров, IM Cisco и Присутствие выбирают самый сильный шифр из этого списка на Сопоставлении Шифра TLS для страницы клиентов третьей стороны что и сервер и поддержка клиентов?

Да. Когда сервер действует как клиент, он передает шифр в заказе, он упомянут в предыдущих вопросах.

Есть ли какой-либо документ, который разъясняет эти вещи?

Да. Существует опция справки, как только вы выбираете ссылку **Шифров TLS** на странице корпоративных параметров, которая сообщает список поддерживаемых шифров.

Когда CUCM/IMP действует как клиент, предпочтительный параметр RSA всех Шифров только имеет значение?

Да.

Это означает, что CUCM/IMP (клиент) передает и RSA и сертификаты ECDSA, но сертификаты RSA могут иметь наивысший приоритет?

Да.

На странице справки шифра TLS это говорит, что шифры включены в этот заказ. Это означает, что шифры передаются в том заказе, когда выбрана эта опция?

Весь предпочтительный RSA шифров

Включает Шифры в следующем порядке:

TLS_ECDHE_RSA с AES256_GCM_SHA384

TLS_ECDHE_ECDSA с AES256_GCM_SHA384

TLS_ECDHE_RSA с AES128_GCM_SHA256

TLS_ECDHE_ECDSA с AES128_GCM_SHA256

TLS_RSA с AES_128_CBC_SHA1

Да.

Когда CUCM/IMP действует как сервер, предпочтительный параметр RSA Всех Шифров не имеет значения. CUCM/IMP в этом случае отвечает Типом сертификата, который имеет наивысший приоритет в Приветственном сообщении клиента?

Да.

Если этот параметр обращается только к SIP/CTI, есть ли эквивалентный параметр для TLS подключение с интерфейсами XMPP?

Нет. Существует усовершенствование функции для XMPP, но это еще не внедрено.