

ةيروفلا ةلسارملا لوح تاباج او ةلئسا ECDSA تاداهش و روضحلاو

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتلا](#)

[تابلطتلا](#)

[ةمدختسمل تانوكملا](#)

[ECDSA لىلج IM&P تاجت نم قيرف ةشقانم](#)

[ECDSA و RSA نيب رايختالا اهليلع نيغت ي ناك اذا RSA رايخت IM&P نأ ةملعملما هذه ملعت له ريفشلتلا عيمج ديدحت مت ولو ىتح ECDSA Presence و Cisco IM لسري نأ نكمي فورظ ي ا يف RSA هلضفي يذلا](#)

[هلضفملا ريفشلتلا عيمج ديدحت عم ىتح هرايختا نكمي له ، لىلج ةيولوا هي دل ECDSA ناك اذا RSA؟](#)

[ههج نم ليمع لسري ام دنع . ايلعل ةيولوا اهل يتلا تارفشملما ديدحت حوضوب عرملل نكمي Presence و Cisco IM موق ي له ، هب ةصاخلا ريفشلتلا ةومجم مادختساب Hello ةلاس رةي جراخ تاهجلا ءالمعل TLS ريفشلت نيغت ةحفص لىلج ةمئاقلا هذه نم ريفشلت يوقا رايختاب ليمعمل او مداخلا نم لك معد ي يتلا ةي جراخلا](#)

[؟ رومألا هذه حضوت ةقيثو نم له](#)

[؟ ليمعك CUCM/IMP لمعي ام دنع طقف ةمهم RSA All Ciphers ل ةلضفملا ةملعملما نوكت له نكمي RSA تاداهش نكلو ECDSA و RSA تاداهش لسري \(ليمعلما\) CUCM/IMP نأ كلذ ينع ي له ؟ ةيولوا لىلج اهل نوكت نأ](#)

[كلذ ينع ي له . بيترتلا اذهب تاعفشملما نيضت مت ي ، TLS ريفشلت تاميلعت ةحفص ي ف رايخلا اذه ديدحت دنع بيترتلا اذهب اهل لسرا مت ي تارفشملما نأ](#)

[بيجتسي . مداخك CUCM/IMP لمعي ام دنع مهت ال ريفشلتلا ةفاكل RSA ةلضفملا ةملعملما ليمعملاب ةصاخلا Hello ةلاس ر ي ةيولوا لىلج اهل ةداهش عونب ةلاخلا هذه ي ف CUCM/IMP TLS تالاصتال ةئفاكم ةملعم كانه له ، SIP/CTI لىلج طقف ريفشلت ةملعملما هذه تناك اذا XMPP؟ تاهجاوب](#)

ةمدقملا

ىنح نملل يمقرلا عيقوتلا ةيمزراوخ تاداهشب ةقلعتملا ةلئسألا لىلج دننتملا اذه بيحي Cisco IM and Presence (IM&P) زاهج عم لمعت يتلا (ECDSA) يواضيبلا

ةيساسألا تابلطتلا

تابلطتلا

ةيلالتلا عيضاوملاب ةفرعم كيدل نوكت نأ Cisco ي صوت:

- Cisco Unified Communications Manager (CUCM) جم انرب
- Cisco نم (IMP) روضحلاو ةيروفلا ةلسارملا
- (SIP) لمع ةسلج ادب لوكتورب
- (CTI) رتوي بمكلا زاهج يفتاهلا لاصتالا جم د

- Rivest-Shamir-Adleman (RSA) ريفش ت
- ECDSA) يواضيب لى نى نى م ل ل ي م ق ر ل ل ع ي ق و ت ل ل ا ة ي م ز ر ا و خ
- XMPP) ع س و ت ل ل ة ل ب ا ق ل ل ة ل س ا ر م ل ل ا و د ج ا و ت ل ل ل و ك و ت و ر ب

ةمدختس م ل ا ت ا ن و ك م ل ا

ةي ل ا ت ل ل ا ة ي د ا م ل ل ا ت ا ن و ك م ل ل ا و ج م ا ر ب ل ل ا ت ا ر ا د ص ا ل ل ا د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا د ن ت س ت

- Cisco IM and Presence 11.5.1

ة ص ا خ ة ي ل م ع م ة ئ ي ب ي ف ة د و ج و م ل ا ة ز ه ج ا ل ا ن م د ن ت س م ل ا ا ذ ه ي ف ة د ر a و ل ا T ا م و ل ع م ل ا ء ا ش ن ا م ت ت ن ا ك ا ذ ا . (ي ض ا ر ت ف ا) ح و س م م ن ي و ك ت ب د ن ت س م ل ا ا ذ ه ي ف ة م د خ ت س م ل ا ة ز ه ج ا ل ا ع ي م ج ت ا د ب ر م ا ي ا ل ل م ت ح م ل ا ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ل ي غ ش ت ل ا د ي ق ك ت ك ب ش

ECDSA لى ل ع IM&P ت ا ج ت ن م ق ي ر ف ة ش ق ا ن م

د ي د ح ت ل ل ن و ك ي ، ة س س و م ل ا ب ة ص ا خ ل ا (TLS) ت ا م ل ع م ل ا ل ق ن ة ق ب ط ن ا م ا ت ا ر ف ش ل ل ا ة ر ا ش ا ل ا ي ف ن ا ف ، ة م ل ع م ل ل TLS ة ر ف ش ل ل ا ة ر ا ش ا ل ا ب ا ذ ا . All Ciphers RSA ل ل ل ض ف م ل a و ه ي ض ا ر ت ف a ل ا IM&P. ة س د ن ه ق ي ر ف ع م ت ر ي ث ا ة ي ل ا ت ل ل ة ل ئ س ا ل a

ة ك ر ش ل ل ع ب ا ت ل ل ا ي س د ن ه ل ا ق ي ر ف ل l ا ه ن م ق ق ح ت ي و ا ه ي ل ع ب ي ج ي ة ل ئ س a ل ا ع ي م ج : ة ط ح a ل م IM&P.

ن ي ع ت ي ن ا ك ا ذ ا RSA ر ا ت خ ت IM&P ن ا ة م ل ع م ل a ه ذ ه م ل ع ت ل ه RSA و ECDSA ن ي ب ر ا ي ت خ a ل a ه ي ل ع

ل ع ة ي ل ض ف a ل a RSA ر ي ف ش ت ي ط ع ت . ط ق ف CUCM SIP/CTI ة ه ج ا و ب ة ص ا خ ة م ل ع م ل a ه ذ ه . م ع ن ECDSA.

ل ي ت ح ECDSA و Cisco IM و Presence ل س ر ي ن ا ن ك م ي ف و ر ط ي ا ي ف RSA ه ل ض ف ي ي ذ ل ا ر ي ف ش ت ل a ع ي م ج د ي د ح ت م ت و ل و

ن ك ل و ، ا ض ي ا ECDSA ت ا ر ف ش ل ل ع ي و ت ح ي ه ن ك ل و RSA ت ا ر ف ش ل ل ة ي ل ض ف a ل a ء ا ط ع ا ل ا ذ ه ن و ك ي و ECDSA ق و ف RSA ت ا ر ف ش ل ل س ر ي ه ن ا ف ل ا ص ت a ء د ب ب ل ي م ع ل a م و ق ي ا م د ن ع

ع م ل ي ت ح ه ر ا ي ت خ ا ن ك م ي ل ه ، ل ع ا ة ي و ل و ا ه ي د ل ECDSA ن ا ك ا ذ ا RSA ل ل ض ف م ل a ر ي ف ش ت ل a ع ي م ج د ي د ح ت

ة ي ل ض ف a ل a ي ط ع ت . ل ي م ع ك CUCM ل م ع ي ا م د ن ع a ل ا ة ر و ص ل a ي ف ة م ل ع م ل a ه ذ ه ر ه ط ت a ل . م ع ن ل ا ص ت a ء د ب ب ل ي م ع ل a م ا ق a ذ a . ل ا ص ت a ل ا ة ئ ي ه ت ب ه ل a ل خ ن م ل ي م ع ل a م و ق ي ي ذ ل a ب ي ت ر ت ل ل ن و ك ي ف ، ك ل ذ ك ر م a ل ن ك ي م ل a ذ a و . ECDSA ب ل ا ص ت a ل ا ش د ح ي ف ، ل ع a ل a ي ف ECDSA ت a ر ف ش ب ة ي ل ض ف a ل a و ه RSA.

ة ي و ل و a ل a ه ل ي ت ل a ت a ر ف ش م ل a د ي د ح ت ح و ض و ب ع ر م ل ل ن ك م ي ع م Hello ة ل س ر ة ي ج ر ا خ ة ه ج ن م ل ي م ع ل س ر ي ا م د ن ع . ا ي ل ع ل a

Cisco IM و Presence موقوي له ، هب ةصاخلا ريفشتلا ةعومجم ريفشت نييعت ىلع ةمئاقلا هذه نم ريفشت ىوقا رايثخاب مداخل اهم عدي يتلا ةيجراخلا تاهجلا ءالمع ةحفصل TLS ليمعلاو؟

ةلئسأل ي ف روكذملا بيترتلاب ريفشتلا لسري هناف ليمعك مداخل لمعي امذن ع .معن ةقباسلا

رومألا هذه حضوت ةقويثو نم له

ةسسؤملا تاملعم ةحفص ي ف TLS تارفش طابترا ديحت درجمب تاميلعت رايخ كانه .معن ةمومدملا تارفشلا ةمئاق ركذت يتلا

طاقف ةمهم RSA All Ciphers ل ةلضفملا ةملعمل نوكت له ليمعك CUCM/IMP لمعي امذن ع

معن .

و RSA تاداهش لسري (ليمعلا) CUCM/IMP نأ كلذ ينعي له ةيولوا ىلعا هل نوكت نأ نكمي RSA تاداهش نكلو ECDSA

معن .

تاعفشملا ني مضت متي ، TLS ريفشت تاميلعت ةحفص ي ف اذهب اهلا سرا متي تارفشملا نأ كلذ ينعي له .بيترتلا اذهب رايخلا اذه ديحت دن ع بيترتلا

RSA لضملا ريفشتلا عيجم

يلائلا بيترتلاب تارفشلا نمضتي

TLS_ECDHE_RSA مع AES256_GCM_SHA384

TLS_ECDHE_ECDSA مع AES256_GCM_SHA384

TLS_ECDHE_RSA مع AES128_GCM_SHA256

TLS_ECDHE_ECDSA مع AES128_GCM_SHA256

TLS_RSA مع AES_128_CBC_SHA1

معن .

لمعني امدن مع مهت ال ريفش تال ة فاكل RSA ة لصف م ل ة عمل عمل
عونب ة لال هذه في CUCM/IMP بيجتسي .مداخك CUCM/IMP
لمعملاب ة صاخلا Hello ة لاسر في ة ولوا لعل ة داهش

معن.

عمل عمل كانه له ، SIP/CTI لى لطق ريفش ت عمل عمل هذه تناك اذا
XMPP تاهجاوب TLS تال اصتال ة فاكل م

دعب هذيفنت متي مل هنكلو ، XMPP ة زم ل نيسحت كانه .ال

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئى. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد عوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلأل يزيلچنلإل دن تسمل