

ىلع GoDaddy رذج ليحرت ريثأت مهف Expressway MRA

تايوتحملا

[قم دقمل](#)

[قيساس تامولعم](#)

[قداهش لئافصاوم](#)

[مي دق رذج](#)

[GoDaddy - G2 رذج قداهش قسيه ننايس](#)

[دي رذج](#)

[CN = GoFather TLS Root CA - R1](#)

[دي دجل طيسولا](#)

[CN = GoFather TLS Intermediate CA DV - R1v1](#)

[قداهش لئافصاوم](#)

[CN = GoFather TLS Root CA - R1](#)

[\(قم دق رذج\) قداهش لئافصاوم](#)

[قداهش لئافصاوم](#)

[قداهش لئافصاوم](#)

قم دقمل

(R1 + R1V1) ىل G2 نم GoDaddy رذج قداهش ليحرت ريثأت دن تسمل اذه فصلي

قيساس تامولعم

R1 رذجل تاداهش قلسلس ىل (G2) مي دقل رذجل قساي س نم لاق تنالاب GoDaddy موقلي
طقف مداخل قداصل EKU قداهش لئافصاوم نمضت نأ بجي. قداهش لئافصاوم

تاداهش تي بئبئب تماق يئال ىرخال قداهش لئافصاوم Expressway ىل لاق تنالاب اذه رثوي
GoDaddy.

بب سب روجل لاق تنالاب شدي

- EKU تادحو نم ي G2 قئفل نم رادصلال/عيقوتلاب نوموقي نيذل اعطسولا ىدل دجوي ال
Chrome جم انرب تابل طتمل لاثتمال قاطن جراخ يمرهال لسلسلئال اذه لعجي امم، قجر دمل
ني ررضتمل ني ررضعل اعومجم اعطسو نم رادصلال ققوت ي نأ بجي، كذل قجي تنو.
Root. خيراتل كذل لولحب

• .ةداهشب اهميدقت متي ضارغألا عي مج نأ ينع ي EKU ال

ةداهشلا تافصاوم

ميدق رذج

GoDaddy - G2 رذج ةداهش ةئييه :نإ يس

ص 5:29:59 2038 ، 1 يناثلا نوناك 1 ،ةعمجل ءاهتنا

SN 00

R1. دي دجل رذجلاب ميدقلا رذجل اذه لادبتسا متي

دي دج رذج

CN = GoFather TLS Root CA - R1

م 5:29:59 2040 ، 24 س طسغأ ،ةعمجل ءاهتنا

SN 00da62ff9e2619b1257a4809368ee8e3f7

.ةيلاتلا ماسقألا ي ف ني بمل وحنلا ىلع دي دجل طيسولا ىلع R1 مداخلل دي دجل رذجل ع قوي

دي دجل طيسولا

CN = GoFather TLS Intermediate CA DV - R1v1

م 5:29:59 2040 ، 24 س طسغأ ،ةعمجل ءاهتنا

SN 008aaa80515c0bc688c7955d70f27758ac

نم ةدي دج ةلسلس ي ف قثت نل ،ميدق G2 رذج اهل يتلا ليغشتلا ةمظنأ ةقث نزاخم
ثيح ،عيقوت - ربع ةقثلا راسم ءاشنإب GoDaddy ماق ضرغل اذهل (R1 + R1V1) تاداهشلا

ةميدق ال G2 رذج ةداهش ىلع ةديدجل R1 رذج ةداهش دمتعت

ةعطاقتم ال ةمالع ال ةداهش

CN = GoFather TLS Root CA - R1

ص 2038 5:29:59، 1 يناتل نوناك 1، ةعمجل ةيحلصل ءاهتنا

SN 0090de6c7fb3b50b3c0617724fc13402ad

مت يتي ال (R1 + R1v1) ةديدجل ةلسلسل نأ وأ، ءحيحص ةلسلسل تيبتت متي مل اذا
MRA IP فتاه ليحست كاشك، Expressway Trust، نرجم ىلع طقف اهتيبتت

لوكتورب فتاه نم مداق فورعم ريغ قدصم عجرم وه Expressway PCAP يه رهظي يذلا أطخل
IP فتاه ةقث نرجم ىلع دوقفم قدصم عجرم دوجو ضارثفا كنكمي. تنرتنإل

88xx IP 135.x.25 تنرتنإل لوكتورب فتاه

172.x.x.34 Expressway

No.	Time	Source	Destination	Protocol	Length	Info
3221	136.965226	1	5	1	64	TCP 60 50987 → 8443 [RST] Seq=187 Win=0 Len=0
3282	138.537145	1	5	1	64	TCP 74 50988 → 8443 [SYN] Seq=0 Win=1460 Len=0 MSS=1460 SACK_PERM TSval=4294941908 TSecr=0 WS=4
3283	138.537198	1	5	1	64	TCP 74 8443 → 50988 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2071425333 TSecr=4
3284	138.545791	1	5	1	64	TCP 66 50988 → 8443 [ACK] Seq=1 Ack=1 Win=1460 Len=0 TSval=4294941909 TSecr=2071425333
3285	138.548058	1	5	1	64	TLSv1.. 245 Client Hello [SN] f.org)
3286	138.548081	1	5	1	64	TCP 66 8443 → 50988 [ACK] Seq=1 Ack=180 Win=65536 Len=0 TSval=2071425344 TSecr=4294941909
3287	138.548482	1	5	1	64	TLSv1.. 2962 Server Hello
3288	138.548504	1	5	1	64	TCP 1266 8443 → 50988 [PSH, ACK] Seq=2897 Ack=180 Win=65536 Len=1200 TSval=2071425345 TSecr=4294941909
3289	138.557258	1	5	1	64	TCP 66 50988 → 8443 [ACK] Seq=180 Ack=1449 Win=17496 Len=0 TSval=4294941910 TSecr=2071425345
3290	138.557436	1	5	1	64	TCP 66 50988 → 8443 [ACK] Seq=180 Ack=2897 Win=20392 Len=0 TSval=4294941910 TSecr=2071425345
3291	138.557446	1	5	1	64	TCP 66 50988 → 8443 [ACK] Seq=180 Ack=4097 Win=23288 Len=0 TSval=4294941910 TSecr=2071425345
3292	138.563914	1	5	1	64	TLSv1.. 1764 Certificate, Server Key Exchange, Server Hello Done
3293	138.572085	1	5	1	64	TCP 66 50988 → 8443 [ACK] Seq=180 Ack=5545 Win=26184 Len=0 TSval=4294941911 TSecr=2071425360
3294	138.572277	1	5	1	64	TCP 66 50988 → 8443 [ACK] Seq=180 Ack=5795 Win=26184 Len=0 TSval=4294941911 TSecr=2071425360
3295	138.579359	1	5	1	64	TLSv1.. 73 Alert (Level: Fatal, Description: Unknown CA)
3296	138.579516	1	5	1	64	TCP 66 8443 → 50988 [FIN, ACK] Seq=5795 Ack=187 Win=65536 Len=0 TSval=2071425376 TSecr=4294941912
3297	138.579558	1	5	1	64	TCP 66 50988 → 8443 [RST, ACK] Seq=187 Ack=5795 Win=26184 Len=0 TSval=4294941912 TSecr=2071425360
3298	138.587002	1	5	1	64	TCP 60 50988 → 8443 [RST] Seq=187 Win=0 Len=0
3316	140.752093	1	5	1	64	TCP 74 50989 → 8443 [SYN] Seq=0 Win=1460 Len=0 MSS=1460 SACK_PERM TSval=4294942129 TSecr=0 WS=4
3317	140.763154	1	5	1	64	TCP 74 8443 → 50989 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2071427548 TSecr=0

> Frame 3295: 73 bytes captured on wire (584 bits), 73 bytes captured (584 bits)

> Ethernet II, Src: PaloAltoNetw_00:02:40 (00:1b:17:00:02:40), Dst: VMware_9f:0d:52 (00:50:56:9f:0d:52)

> Internet Protocol Version 4, Src: 135.25.34

> Transmission Control Protocol, Src Port: 50988, Dst Port: 8443, Seq: 180, Ack: 5795, Len: 7

> Transport Layer Security

- TLV1.2 Record Layer: Alert (Level: Fatal, Description: Unknown CA)

Content Type: Alert (21)
Version: TLS 1.2 (0x0303)

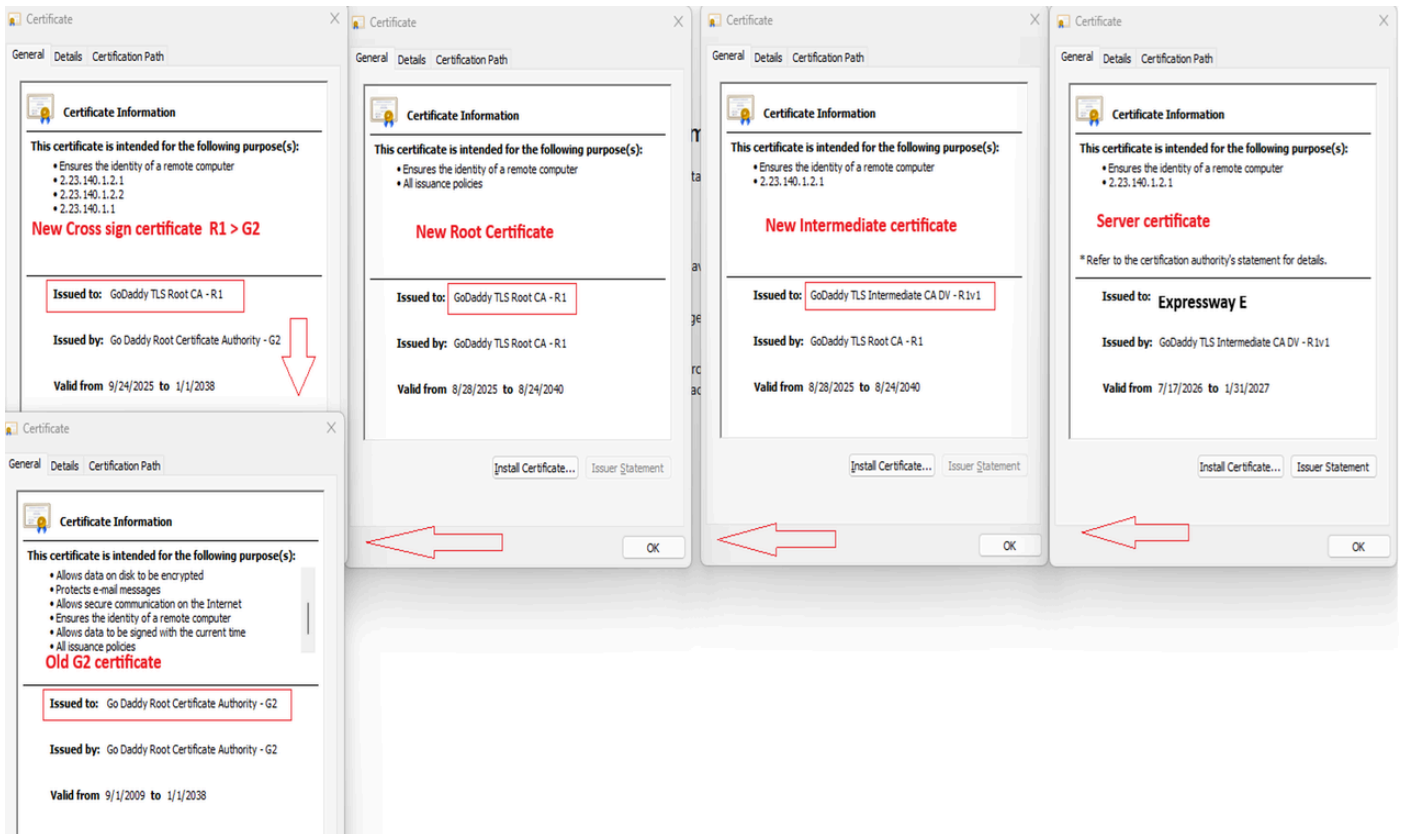
ةداهش نأل ةيلدابتل ةمالع ال ةداهش Expressway ةقث نرجم لبقي ال شيح ةلاح اضيأ كانه
رذج ال CN = GoDaddy TLS Root CA - R1، مساسفن اهل ةيلدابتل ةمالع ال ةداهش و ةديدجل رذج ال
CA - R1.

لإحالة هذه ناك اذا:

1. R1 Root R1 SN 00da62ff9e2619b1257a4809368ee8e3f7. عداش فذخا .

2. SN 0090de6c7fb3b50b3c0617724fc13402ad CN = GoDaddy TLS Root CA - R1. عداش لي ماحت .

(عميدق لى إديج) عداش لى عرجش



عماله تافل مالا

عالم عمل نكلو ، R1 DV رادصاب صاخلا (CA) قدصملا عجرملا بجومب قاروالا عداش رادصاب ماتي مادختساب G2 - GoDaddy Class 2 Root عداش لى سلس عاشن لالخنم اهيلع نووقدصي يه عدوتسملا يف ةدوجوملا ةلصللا تاذا عونصملاو . ةروشنملا R1 → G2 ةعطاقتملا عداشلا طيسولا رادصابلاو ، (gd_tls_root-r1-cross-g2) ةعطاقتملا عداشلاو ، G2 (gdroot-g2) ةقث ةاسرم certs.godadi.com (gd_tls_root-r1) يلصلالا يمرهلا جردتلا رذجو ، R1 DV (gd_tls_issuing_dv-r1v1) ةحص نم ققحتلا ةيناكملا تاضرعتسملا ةكرتشملا تامالعل لىل عمئاقلا جهنلا اذه حيتي رورم عم R1 يف ةقثلا رشن ماتي امنيب ، (G2) يف اهتيتبثت ماتي يتلا) مويللا ةلسلسلا تقولا .

ةلص تاذا تامولعم

انه ديدجل رذجل الى ميقلا رذجل نم لاقتنال لىصافت قيثوت متي

[R1 رذجل يمره لىلست الى لىل لاقتنال او ClientAuth EKU ةلازاب GoDaddy موقى اذامل DV TLS؟ رادصل](#)

ةداهشل لىزنتل Godaddy عدوتسم وه [اه](#)، ةلكشملا هذه ةهجاوم ةلاح يف

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا