

瞭解GoDaddy根遷移對Expressway MRA的影響

目錄

[簡介](#)

[背景資訊](#)

[證書說明](#)

[舊根](#)

[CN:GoDaddy根證書頒發機構 — G2](#)

[新根](#)

[CN = GoDaddy TLS根CA - R1](#)

[新的中間產品](#)

[CN = GoDaddy TLS中間CA DV - R1v1](#)

[交叉簽名證書](#)

[CN = GoDaddy TLS根CA - R1](#)

[證書樹 \(從新到舊\)](#)

[重要檔案](#)

[相關資訊](#)

簡介

本文檔介紹將GoDaddy根證書從G2遷移到(R1 + R1V1)的效果。

背景資訊

GoDaddy正在從舊根(G2)策略過渡到新的R1根證書鏈。新證書必須僅包括伺服器身份驗證EKU。

此過渡影響已安裝GoDaddy證書的expressway和其他邊緣產品。

根過渡發生的原因包括：

- G2簽名/發行中介軟體未列出任何EKU，這使得該層次結構不符合Chrome根程式要求。因此，受影響的G2中間體的發行必須在該日期前停止。
- No EKU表示所有目的都通過證書提供。

證書說明

舊根

CN:GoDaddy根證書頒發機構 — G2

2038年1月1日25:29:59到期

SN 00

這個舊的根目錄被新的根R1取代。

新根

CN = GoDaddy TLS根CA - R1

2040年8月24日周五下午5:29:59

SN 00da62ff9e2619b1257a4809368ee8e3f7

新的R1根目錄對下一節中介紹的新中間節點進行簽名。

新的中間產品

CN = GoDaddy TLS中間CA DV - R1v1

2040年8月24日周五下午5:29:59

SN 008aaa80515c0bc688c7955d70f27758ac

具有舊G2根的OS信任儲存將不信任新的證書鏈(R1 + R1V1)為此目的GoDaddy已建立交叉簽名信任路徑，其中

新的R1根證書信任舊的G2根證書。

交叉簽名證書

CN = GoDaddy TLS根CA - R1

2038年1月1日星期五5:29:59

SN 0090de6c7fb3b50b3c0617724fc13402ad

如果您沒有安裝正確的鏈條，或者您在Expressway信任商店上只安裝新的鏈條(R1 + R1v1)，則MRA IP電話註冊會暫停。

在expressway pcap中出現的錯誤是來自IP電話的未知CA。您可以假設IP電話信任儲存中缺少一個CA。

88xx ip電話135.x.x.25

172.x.x.34高速公路

No.	Time	Source	Destination	Protocol	Length	Info
3221	136.965226	1	5	1	4	TCP 60 50987 → 8443 [RST] Seq=187 Win=0 Len=0
3282	138.537145	1	5	1	4	TCP 74 50988 → 8443 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM TSval=4294941908 TSecr=0 WS=4
3283	138.537198	1	5	1	4	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	4	TCP 66 50988 → 8443 [ACK] Seq=1 Ack=1 Win=14600 Len=0 TSval=4294941909 TSecr=2071425333
3285	138.548058	1	5	1	4	TLSv1_ 245 Client Hello [SNI= f.org)
3286	138.548081	1	1	1	1,25	TCP 66 8443 → 50988 [ACK] Seq=1 Ack=180 Win=65536 Len=0 TSval=2071425344 TSecr=4294941909
3287	138.548482	1	1	1	1,25	TLSv1_ 2962 Server Hello
3288	138.548504	1	1	1	1,25	TCP 1266 8443 → 50988 [PSH, ACK] Seq=2897 Ack=180 Win=65536 Len=1200 TSval=2071425345 TSecr=4294941909
3289	138.557258	1	5	1	4	TCP 66 50988 → 8443 [ACK] Seq=180 Ack=1449 Win=17496 Len=0 TSval=4294941910 TSecr=2071425345
3290	138.557436	1	5	1	4	TCP 66 50988 → 8443 [ACK] Seq=180 Ack=2897 Win=20392 Len=0 TSval=4294941910 TSecr=2071425345
3291	138.557446	1	5	1	4	TCP 66 50988 → 8443 [ACK] Seq=180 Ack=4097 Win=23288 Len=0 TSval=4294941910 TSecr=2071425345
3292	138.563914	1	1	1	1,25	TLSv1_ 1764 Certificate, Server Key Exchange, Server Hello Done
3293	138.572085	1	5	1	4	TCP 66 50988 → 8443 [ACK] Seq=180 Ack=5545 Win=26184 Len=0 TSval=4294941911 TSecr=2071425360
3294	138.572277	1	5	1	4	TCP 66 50988 → 8443 [ACK] Seq=180 Ack=5795 Win=26184 Len=0 TSval=4294941911 TSecr=2071425360
3295	138.579359	1	5	1	4	TLSv1_ 73 Alert (Level: Fatal, Description: Unknown CA)
3296	138.579516	1	5	1	1,25	TCP 66 8443 → 50988 [RST, ACK] Seq=187 Ack=5795 Win=0 Len=0 TSval=2071425376 TSecr=4294941912
3297	138.579558	1	5	1	4	TCP 66 50988 → 8443 [RST, ACK] Seq=187 Ack=5795 Win=0 Len=0 TSval=4294941912 TSecr=2071425360
3298	138.587002	1	5	1	4	TCP 60 50988 → 8443 [RST] Seq=187 Win=0 Len=0
3316	140.752093	1	5	1	4	TCP 74 50989 → 8443 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM TSval=4294942129 TSecr=0 WS=4

> 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: 135.172.140.34, Dst: 172.16.17.25

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

> Transport Layer Security

 < TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Unknown CA)

 Content Type: Alert (21)

 Version: TLS 1.2 (0x0303)

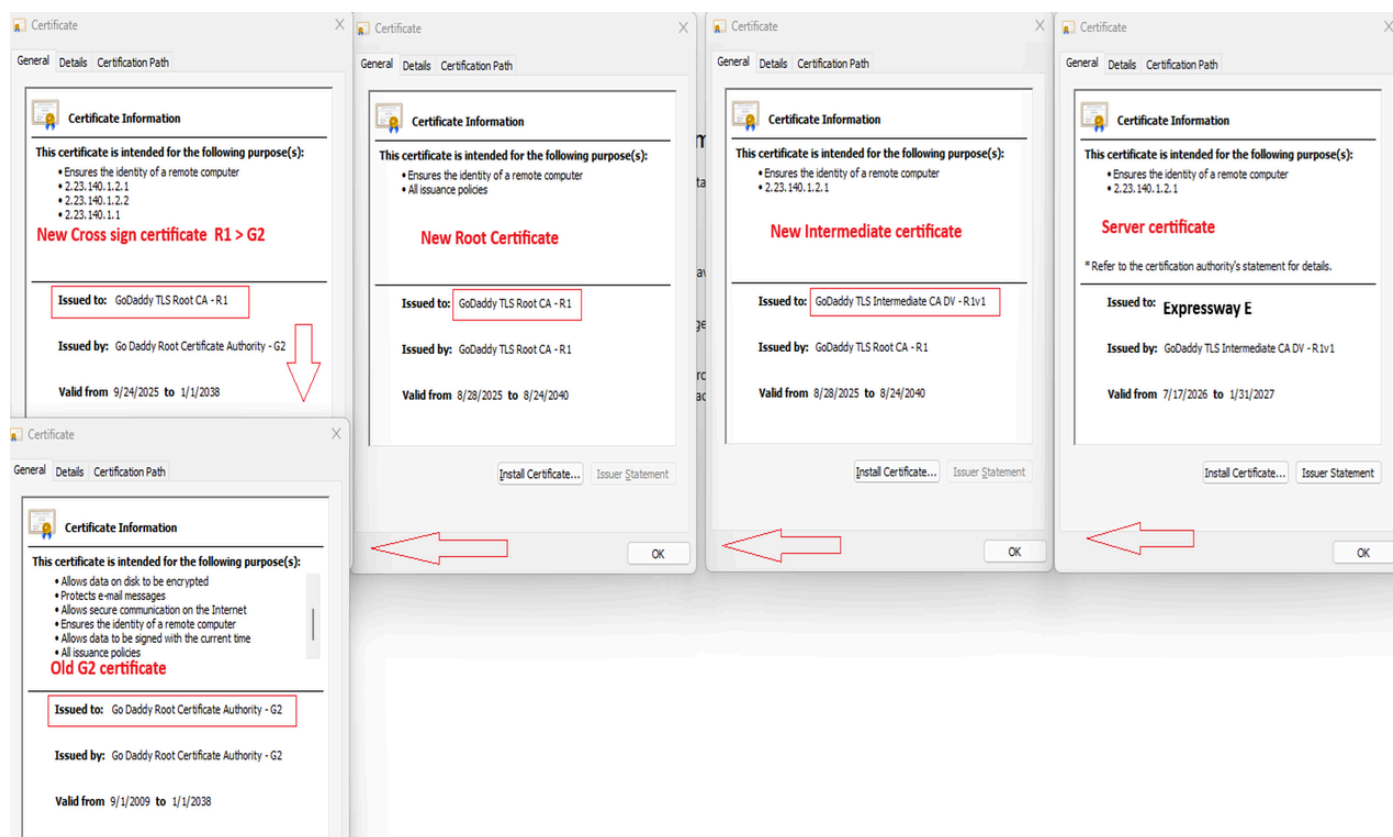
此外，還存在Expressway信任儲存不接受交叉簽名證書的情況，因為新的根證書和交叉簽名證書具有相同的CN名稱，如CN = GoDaddy TLS根CA - R1。

如果情況如此：

1.刪除新的根R1證書SN 00da62ff9e2619b1257a4809368ee8e3f7。

2.上傳交叉簽名證書SN 0090de6c7fb3b50b3c0617724fc13402ad CN = GoDaddy TLS根CA - R1。

證書樹（從新到舊）



重要檔案

枝葉證書在R1 DV頒發CA下頒發，但客戶端使用發佈的R1 → G2交叉證書建立到GoDaddy 2類Root - G2的鏈來驗證它。儲存庫中的相關對象是G2信任錨點(gdroot-g2)、交叉證書(gd_tls_root-r1-cross-g2)、R1 DV發行中間體(gd_tls_issuing_dv-r1v1)和本地層次結構根(gd_tls_root-r1)certs.godaddy.com。這種交叉符號方法允許瀏覽器驗證當前鏈（在G2錨定），而R1信任會隨著時間推移而傳播。

相關資訊

從舊根到新根的轉換詳細資訊記錄如下：

[為什麼GoDaddy正在刪除ClientAuth ECU並過渡到R1根層次結構以進行DV TLS發佈？](#)

如果您遇到此問題，請[此處](#)為用於下載證書的Godaddy儲存庫。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。