

Auswirkungen der GoDaddy-Root-Migration auf Expressway MRA

Inhalt

[Einleitung](#)

[Hintergrund](#)

[Zertifikatsspezifikationen](#)

[Alte Wurzel](#)

[Neuer Stamm](#)

[Neue Zwischenprodukte](#)

[Zertifikat für Kreuzzeichen](#)

[Zertifikatsstruktur \(Neu in alt\)](#)

[Wichtige Dateien](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Auswirkungen der Migration des GoDaddy-Stammzertifikats von G2 nach (R1 + R1V1) beschrieben.

Hintergrund

GoDaddy wechselt von der alten Root-Richtlinie (G2) zur neuen R1-Stammzertifikatkette. Neue Zertifikate dürfen nur die EKU für die Serverauthentifizierung enthalten.

Dieser Übergang betrifft Schnellstraßen und andere Edge-Produkte, die Good-Daddy-Zertifikate installiert haben.

Der Übergang der Wurzeln erfolgt aufgrund von:

- G2-Signierungs-/Ausstellungsvermittler haben keine EKU aufgelistet, was diese Hierarchie aus der Übereinstimmung mit der Chrome Root Program-Anforderung macht. Daher muss die Ausgabe von den betroffenen G2-Zwischenprodukten bis zu diesem Datum eingestellt werden.
- Keine EKU bedeutet, dass alle Zwecke mit einem Zertifikat bedient werden.

Zertifikatsspezifikationen

Alte Wurzel

KN GoDaddy Root Certificate Authority - G2

Ablauf Freitag, .Januar 1..2038 05:29:59

SN 00

Dieser alte Root wird durch den neuen Root R1 ersetzt.

Neuer Stamm

CN = GoDaddy TLS-Stammzertifizierungsstelle - R1

Ablauf Freitag, .August 24..2040 17:29:59

SN 00da62ff9e2619b1257a4809368ee8e3f7

Der neue R1-Root signiert das neue Zwischenprodukt, wie in den nächsten Abschnitten beschrieben.

Neue Zwischenprodukte

CN = GoDaddy TLS Intermediate CA DV - R1v1

Ablauf Freitag, .August 24..2040 17:29:59

SN 008aaa80515c0bc688c7955d70f27758ac

OS Trust Stores, die alte G2 Root haben, werden nicht vertrauen neue Kette von Zertifikaten (R1 + R1V1) für diesen Zweck GoDaddy hat einen Cross - Sign - Trust - Pfad, wo

Das neue R1-Stammzertifikat vertraut dem alten G2-Stammzertifikat.

Zertifikat für Kreuzzeichen

CN = GoDaddy TLS-Stammzertifizierungsstelle - R1

Ablauf am Freitag, . . 1. .2038 05:29:59

SN 0090de6c7fb3b50b3c0617724fc13402ad

Wenn Sie keine richtige Kette installiert haben oder nur eine neue Kette (R1 + R1v1) im Expressway Trust Store installiert ist, wird die MRA IP-Telefonregistrierung beendet.

Der Fehler, der auf der Schnellstraße Pcap festgestellt wurde, ist eine unbekannte Zertifizierungsstelle, die von einem IP-Telefon stammt. Sie können davon ausgehen, dass im Vertrauensspeicher des IP-Telefons eine Zertifizierungsstelle fehlt.

88xx IP-Telefon 135.x.x.25

172.x.x.34 Schnellstraße

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 [SN] [f.org]
3286	138.548081	1	5	1	1,25	TCP 66 8443 → 50988 [ACK] Seq=1 Ack=180 Win=65536 Len=0 TSval=2071425344 TSecr=4294941909
3287	138.548482	1	5	1	1,25	TLSv1.. 2962 Server Hello
3288	138.548504	1	5	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	5	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 [FIN, ACK] Seq=5795 Ack=187 Win=65536 Len=0 TSval=2071425376 TSecr=4294941912
3297	138.579558	1	5	1	4	TCP 66 50988 → 8443 [RST, ACK] Seq=187 Ack=5795 Win=26184 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
3317	140.752164	1	5	1	4	TCP 74 8443 → 50989 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2071427548 TSecr=0

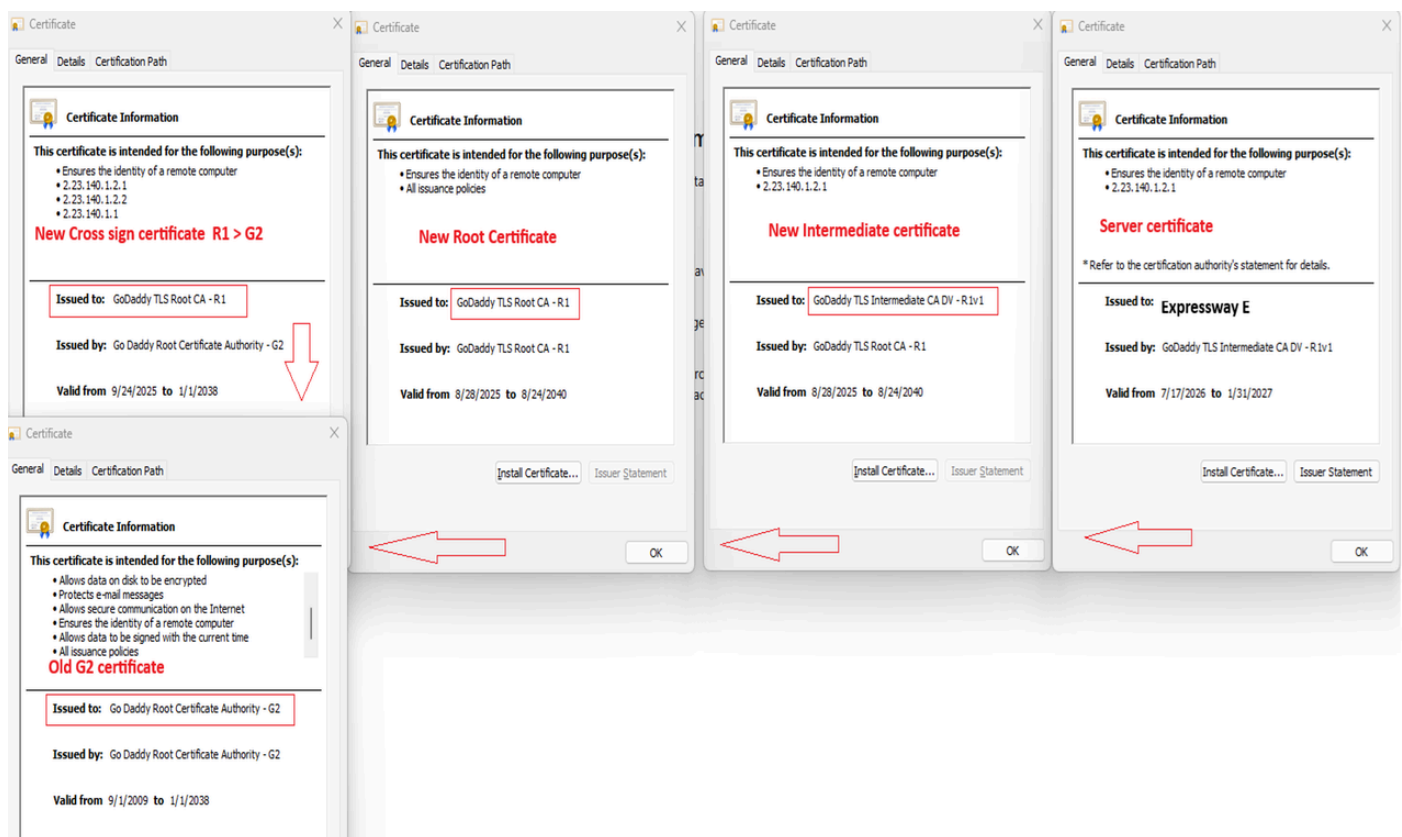
> Frame 3295: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
> Ethernet II, Src: PaloAltoNetw_00:02:40 (00:1b:17:00:02:40), Dst: VMware_9f:0d:52 (00:50:56:9f:0d:52)
> Internet Protocol Version 4, Src: 135.x.x.25, Dst: 172.x.x.34
> Transmission Control Protocol, Src Port: 50988, Dst Port: 8443, Seq: 187, Ack: 5795, Len: 7
v Transport Layer Security
v TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Unknown CA)
Content Type: Alert (21)
Version: TLS 1.2 (0x0303)

Es gibt auch eine Situation, in der der Expressway-Vertrauensspeicher das Zertifikat mit Kreuzzeichen nicht akzeptiert, da das neue Stammzertifikat und das Zertifikat mit Kreuzzeichen denselben CN-Namen haben, wie in CN = GoDaddy TLS Root CA - R1.

Wenn dies der Fall ist:

1. Löschen Sie nicht New Root R1 Zertifikat SN 00da62ff9e2619b1257a4809368ee8e3f7.
2. Kreuzsignaturzertifikat hochladen SN 0090de6c7fb3b50b3c0617724fc13402ad CN = GoDaddy TLS Root CA - R1.

Zertifikatsstruktur (Neu in alt)



Wichtige Dateien

Das Leaf-Zertifikat wird unter der R1 DV ausstellenden CA ausgestellt, aber die Clients validieren es, indem sie eine Kette zu GoDaddy Class 2 Root - G2 aufbauen, die das veröffentlichte R1→G2-Kreuzzertifikat verwendet. Die relevanten Artefakte im Repository sind der G2-Vertrauensanker (gdroot-g2), das Kreuzzertifikat (gd_tls_root-r1-cross-g2), die R1 DV-ausstellende Zwischenstation (gd_tls_Issuing_dv-r1v1) und die native Hierarchie-Root. (gd_tls_root-r1) certs.godaddy.com. Bei diesem Cross-Sign-Ansatz können Browser die Kette heute validieren (Verankerung am G2), während sich die R1-Vertrauensstellung im Laufe der Zeit ausbreitet.

Zugehörige Informationen

Details zum Übergang vom alten Root zum neuen Root sind hier dokumentiert:

- [Warum entfernt GoDaddy die ClientAuth EKU und wechselt zur R1-Root-Hierarchie für die DV TLS-Ausgabe?](#)

Falls Sie dieses Problem haben, hier ist das Godaddy-Repository zum Herunterladen des Zertifikats:

- [GoDaddy-Repository](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.