

Het effect van GoDaddy Root Migration op Expressway MRA

Inhoud

[Inleiding](#)

[Achtergrond](#)

[Certificaatspecificaties](#)

[oude wortel](#)

[Nieuwe wortel](#)

[nieuw tussenproduct](#)

[kruisondertekeningcertificaat](#)

[Certificaatstructuur \(nieuw naar oud\)](#)

[Belangrijke bestanden](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft het effect van de migratie van het GoDaddy-basiscertificaat van G2 naar (R1 + R1V1).

Achtergrond

GoDaddy gaat over van het Old Root (G2) beleid naar de nieuwe R1 root certificaatketen. Nieuwe certificaten mogen alleen de ECU voor serververificatie bevatten.

Deze overgang heeft invloed op snelwegen en andere edge-producten die Good Daddy-certificaten hebben geïnstalleerd.

De overgang van de wortels vindt plaats door:

- G2 ondertekening / afgifte tussenproducten hebben geen ECU vermeld, waardoor die hiërarchie niet voldoet aan de eis van het Chrome Root Program. Als gevolg daarvan moet de uitgifte door de betrokken G2-intermediairs op die datum stoppen.
- Geen ECU betekent dat alle doeleinden worden bediend door een certificaat.

Certificaatspecificaties

oude wortel

CN: GoDaddy Root Certificate Authority - G2

Vervaldatum vrijdag januari 1, 2038 05:29:59

SN 00

Deze oude wortel wordt vervangen door de nieuwe wortel R1.

Nieuwe wortel

CN = GoDaddy TLS Root CA – R1

Vervaldatum vrijdag augustus 24, 2040 17:29:59

SN 00da62ff9e2619b1257a4809368ee8e3f7

De nieuwe R1-wortel tekent het nieuwe tussenproduct zoals beschreven in de volgende secties.

nieuw tussenproduct

CN = GoDaddy TLS Intermediate CA DV - R1v1

Vervaldatum vrijdag augustus 24, 2040 17:29:59

SN 008aaa80515c0bc688c7955d70f27758ac

Vertrouwenswinkels voor besturingssystemen die oude G2-hoofdmap hebben, vertrouwen hiervoor geen nieuwe keten van certs (R1 + R1V1) GoDaddy heeft een cross-sign-vertrouwenspad gemaakt, waarbij

nieuw R1-basiscertificaat vertrouwt op oud G2-basiscertificaat.

kruisondertekeningscertificaat

CN = GoDaddy TLS Root CA - R1

Vervaldatum vrijdag januari 1, 2038 05:29:59

SN 0090de6c7fb3b50b3c0617724fc13402ad

Als u niet de juiste keten hebt geïnstalleerd, of als u alleen een nieuwe keten (R1 + R1v1) hebt geïnstalleerd in de Expressway Trust-winkel, worden MRA IP-telefoonregistratiekraampjes geïnstalleerd.

De fout die wordt gezien in expressway Pcap is een onbekende CA die afkomstig is van een IP-telefoon. U kunt ervan uitgaan dat er een ontbrekende CA in de IP-telefoonvertrouwenswinkel is.

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

172.x.x.34 snelweg

The image shows a Wireshark packet capture of a TLS connection. The top pane displays a list of packets. Packet 3295 is highlighted, showing a TLS alert (Level: Fatal, Description: Unknown CA) from 135.x.x.25 to 172.x.x.34. The bottom pane shows the details of this packet, including the Ethernet II header, Internet Protocol Version 4 header, Transmission Control Protocol header, and Transport Layer Security (TLS) record layer. The TLS alert is shown as a fatal alert with the description 'Unknown CA'.

No.	Time	Source	Destination	Protocol	Length	Info
3221	136.965226	1	5	TCP	60	50987 → 8443 [RST] Seq=187 Win=0 Len=0
3282	138.537145	1	5	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	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	TCP	66	50988 → 8443 [ACK] Seq=1 Ack=1 Win=14600 Len=0 TSval=4294941909 TSecr=2071425333
3285	138.548058	1	5	TLSv1..	245	Client Hello [SN] [f.org]
3286	138.548081	1	5	TCP	66	8443 → 50988 [ACK] Seq=1 Ack=180 Win=65536 Len=0 TSval=2071425344 TSecr=4294941909
3287	138.548482	1	5	TLSv1..	2962	Server Hello
3288	138.548504	1	5	TCP	1266	8443 → 50988 [PSH, ACK] Seq=2897 Ack=180 Win=65536 Len=1200 TSval=2071425345 TSecr=4294941909
3289	138.557258	1	5	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=1449 Win=17496 Len=0 TSval=4294941910 TSecr=2071425345
3290	138.557436	1	5	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=2897 Win=20392 Len=0 TSval=4294941910 TSecr=2071425345
3291	138.557446	1	5	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=4097 Win=23288 Len=0 TSval=4294941910 TSecr=2071425345
3292	138.563914	1	5	TLSv1..	1764	Certificate, Server Key Exchange, Server Hello Done
3293	138.572085	1	5	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=5545 Win=26184 Len=0 TSval=4294941911 TSecr=2071425360
3294	138.572277	1	5	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=5795 Win=26184 Len=0 TSval=4294941911 TSecr=2071425360
3295	138.579359	1	5	TLSv1..	73	Alert (Level: Fatal, Description: Unknown CA)
3296	138.579516	1	5	TCP	66	8443 → 50988 [FIN, ACK] Seq=5795 Ack=187 Win=65536 Len=0 TSval=2071425376 TSecr=4294941912
3297	138.579558	1	5	TCP	66	50988 → 8443 [RST, ACK] Seq=187 Ack=5795 Win=26184 Len=0 TSval=4294941912 TSecr=2071425360
3298	138.587082	1	5	TCP	60	50988 → 8443 [RST] Seq=187 Win=0 Len=0
3316	140.752093	1	5	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	TCP	74	8443 → 50989 [ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2071427548 TSecr=0

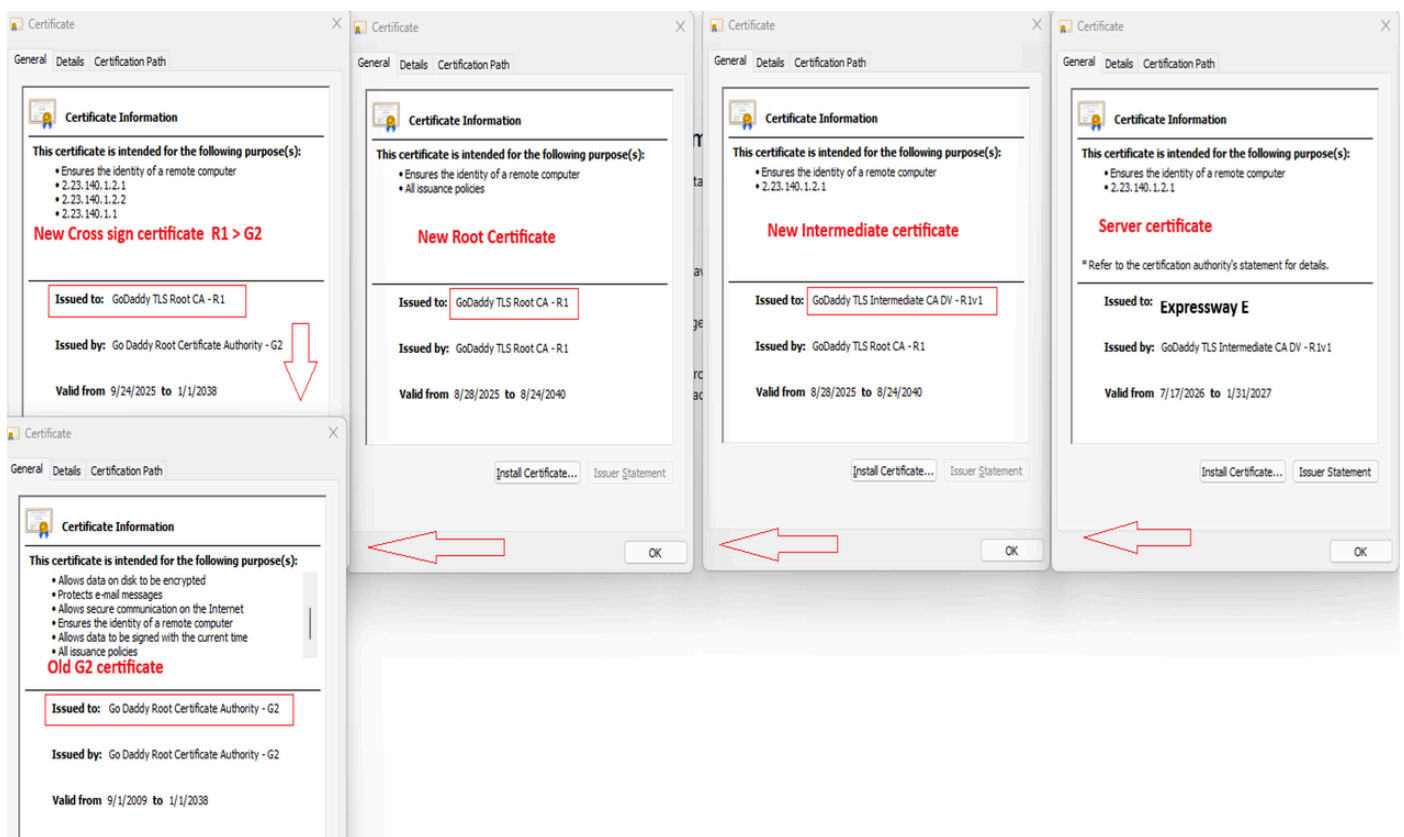
Frame 3295: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
> Ethernet II, Src: PaloAltoNetw_00:02:40 (00:1b:17:00:02:40), Dst: VMware_9f:0d:52 (00:50:56:9f:0d:52)
> Internet Protocol Version 4, Src: 135.x.x.25, Dst: 172.x.x.34
> Transmission Control Protocol, Src Port: 50988, Dst Port: 8443,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

Er is ook een situatie waarin de Expressway trust store het kruisondertekeningscertificaat niet accepteert omdat het nieuwe basiscertificaat en kruisondertekeningscertificaat dezelfde CN-naam hebben, zoals in CN = GoDaddy TLS Root CA - R1.

Indien dit het geval is:

1. Verwijder Nieuw Root R1-certificaat SN 00da62ff9e2619b1257a4809368ee8e3f7 niet.
2. Upload kruisondertekeningscertificaat SN 0090de6c7fb3b50b3c0617724fc13402ad CN = GoDaddy TLS Root CA - R1.

Certificaatstructuur (nieuw naar oud)



Belangrijke bestanden

Het leaf certificaat wordt uitgegeven onder de R1 DV uitgifte CA, maar klanten valideren het door het bouwen van een keten naar GoDaddy Klasse 2 Root – G2 met behulp van de gepubliceerde R1 → G2 cross certificaat. De relevante artefacten in de repository zijn het G2-vertrouwensanker (gdroot-g2), het kruiscertificaat (gd_tls_root-r1-cross-g2), het R1 DV-uitgevende intermediair (gd_tls_issuing_dv-r1v1) en de hoofdhiërarchiewortel (gd_tls_root-r1) certs.godaddy.com. Deze cross-sign benadering stelt browsers in staat om de keten vandaag te valideren (verankering bij G2), terwijl R1-vertrouwen zich in de loop van de tijd verspreidt.

Gerelateerde informatie

Details over de overgang van de oude root naar de nieuwe root zijn hier gedocumenteerd:

- [Waarom verwijdt GoDaddy ClientAuth ECU en schakelt over naar de R1-roothierarchie voor de uitgifte van DV TLS?](#)

In het geval dat u dit probleem tegenkomt, is hier de Godaddy-repository om het certificaat te downloaden:

- [GoDaddy-opslagplaats](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.