

Understand Effect of GoDaddy Root Migration on Expressway MRA

Contents

[Introduction](#)

[Background Information](#)

[Certificate Specifics](#)

[Old Root](#)

[CN: GoDaddy Root Certificate Authority - G2](#)

[New Root](#)

[CN = GoDaddy TLS Root CA – R1](#)

[New Intermediate](#)

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

[Cross Sign Certificate](#)

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

[Certificate Tree \(New to Old\)](#)

[Important Files](#)

[Related Information](#)

Introduction

This document describes the effect of migrating the GoDaddy root certificate from G2 to (R1 + R1V1).

Background Information

GoDaddy is transitioning from the Old Root (G2) policy to the new R1 root certificate chain. New certificates must include only the Server Authentication EKU.

This transition affects expressways and other edge products who have installed GoDaddy certificates.

The roots transition takes place due to:

- G2 signing/issuing intermediates do not have any EKU listed, which makes that hierarchy out of compliance with the Chrome Root Program requirement. As a result, issuance from the affected G2 intermediates must stop by that date.
- No EKU means all purposes are served by certificate.

Certificate Specifics

Old Root

CN: GoDaddy Root Certificate Authority - G2

Expiry Friday, January 1, 2038 5:29:59 AM

SN 00

This old root is replaced by the new root R1.

New Root

CN = GoDaddy TLS Root CA – R1

Expiry Friday, August 24, 2040 5:29:59 PM

SN 00da62ff9e2619b1257a4809368ee8e3f7

The new R1 root signs the new intermediate as outlined in the next sections.

New Intermediate

CN = GoDaddy TLS Intermediate CA DV - R1v1

Expiry Friday, August 24, 2040 5:29:59 PM

SN 008aaa80515c0bc688c7955d70f27758ac

OS trust stores which have old G2 root, will not trust new chain of certs (R1 + R1V1) for this purpose
GoDaddy has created a cross – sign trust path, where

new R1 root certificate trusts old G2 root certificate.

Cross Sign Certificate

CN = GoDaddy TLS Root CA - R1

Expiry Friday, January 1, 2038 5:29:59 AM

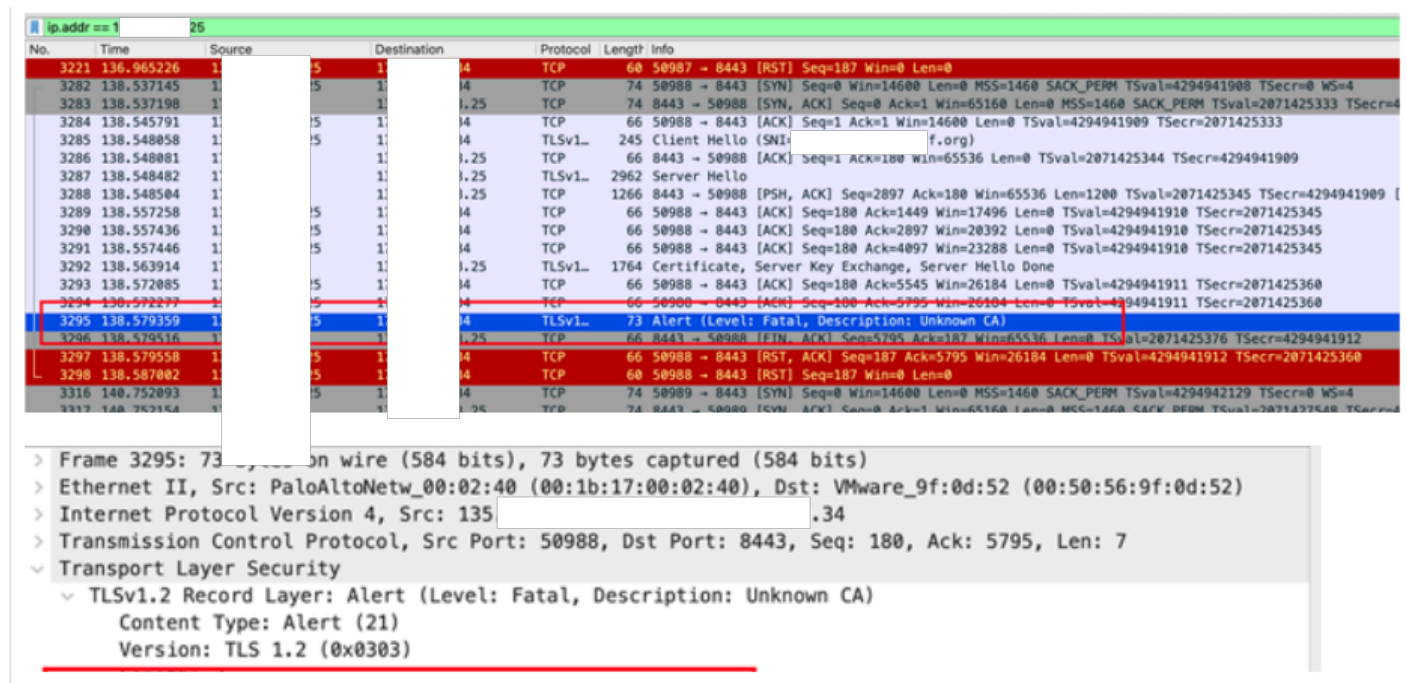
SN 0090de6c7fb3b50b3c0617724fc13402ad

If you do not have correct chain installed, or you only have new chain (R1 + R1v1) installed on Expressway Trust store, MRA IP phone registration stalls.

The error seen in expressway pcap is an unknown CA coming from an IP phone. You can assume there is a missing CA on the IP phone trust store.

88xx ip phone 135.x.x.25

172.x.x.34 Expressway



No.	Time	Source	Destination	Protocol	Length	Info
3221	136.965226	1	1	TCP	60	50987 → 8443 [RST] Seq=187 Win=0 Len=0
3282	138.537145	1	1	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	1	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	1	TCP	66	50988 → 8443 [ACK] Seq=1 Ack=1 Win=14600 Len=0 TSval=4294941909 TSecr=2071425333
3285	138.548058	1	1	TLSv1..	245	Client Hello (SN=[f.org])
3286	138.548081	1	1	TCP	66	8443 → 50988 [ACK] Seq=1 Ack=180 Win=65536 Len=0 TSval=2071425344 TSecr=4294941909
3287	138.548482	1	1	TLSv1..	2962	Server Hello
3288	138.548504	1	1	TCP	1266	8443 → 50988 [PSH, ACK] Seq=2897 Ack=180 Win=65536 Len=1200 TSval=2071425345 TSecr=4294941909
3289	138.557258	1	1	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=1449 Win=17496 Len=0 TSval=4294941910 TSecr=2071425345
3290	138.557436	1	1	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=2897 Win=20392 Len=0 TSval=4294941910 TSecr=2071425345
3291	138.557446	1	1	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=4097 Win=23288 Len=0 TSval=4294941910 TSecr=2071425345
3292	138.563914	1	1	TLSv1..	1764	Certificate, Server Key Exchange, Server Hello Done
3293	138.572085	1	1	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=5545 Win=26184 Len=0 TSval=4294941911 TSecr=2071425360
3294	138.572277	1	1	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=5795 Win=26184 Len=0 TSval=4294941911 TSecr=2071425360
3295	138.579359	1	1	TLSv1..	73	Alert (Level: Fatal, Description: Unknown CA)
3296	138.579516	1	1	TCP	66	8443 → 50988 [FIN, ACK] Seq=5795 Ack=187 Win=65536 Len=0 TSval=2071425376 TSecr=4294941912
3297	138.579558	1	1	TCP	66	50988 → 8443 [RST, ACK] Seq=187 Ack=5795 Win=26184 Len=0 TSval=4294941912 TSecr=2071425360
3298	138.587002	1	1	TCP	60	50988 → 8443 [RST] Seq=187 Win=0 Len=0
3316	140.752093	1	1	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 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: 180, Ack: 5795, Len: 7

> Transport Layer Security

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

 Content Type: Alert (21)

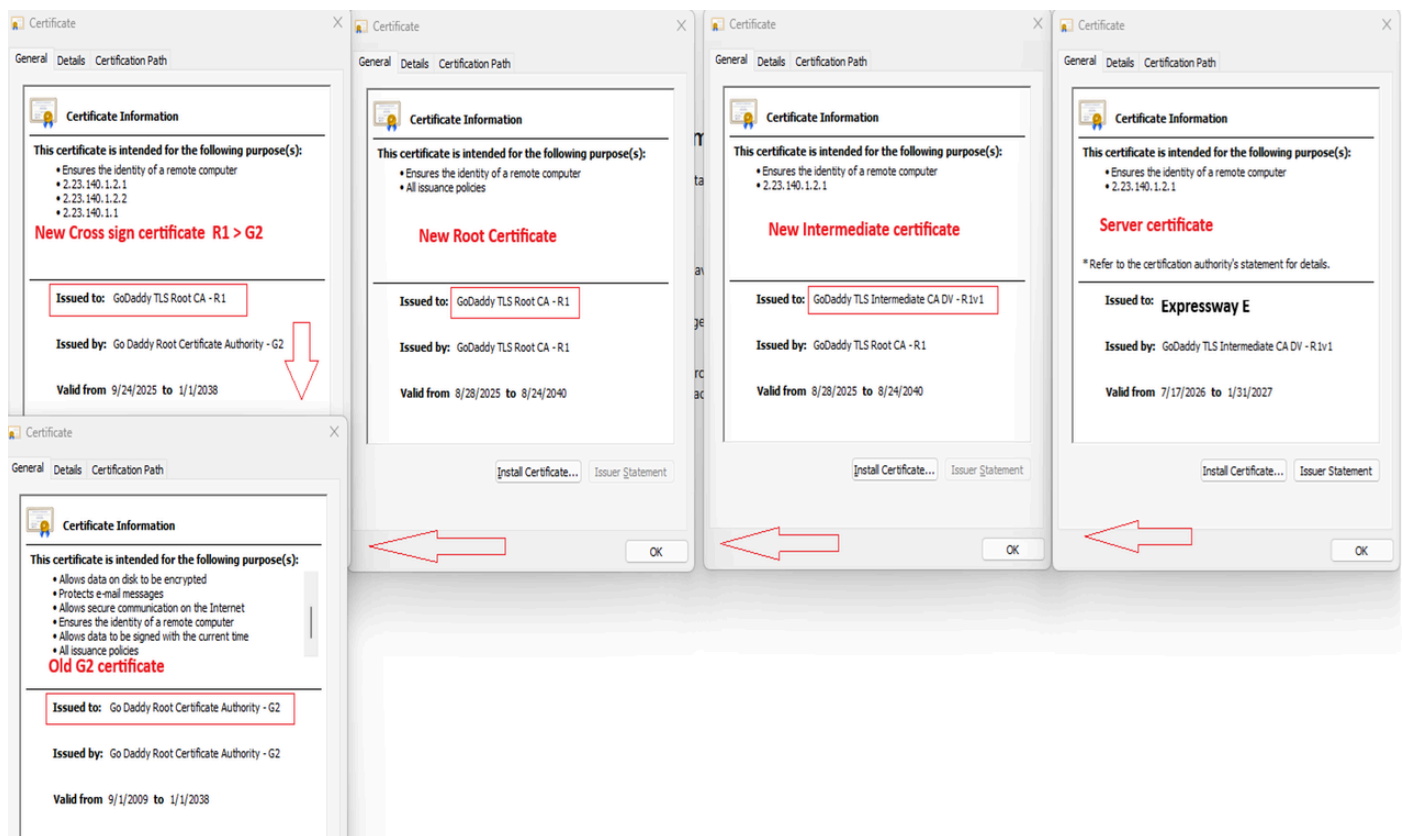
 Version: TLS 1.2 (0x0303)

There is also a situation where the Expressway trust store does not accept the cross-sign certificate because the new root certificate and cross sign certificate have same CN name, as in CN = GoDaddy TLS Root CA - R1.

If this is the case:

1. DELETE New Root R1 certificate SN 00da62ff9e2619b1257a4809368ee8e3f7.
2. Upload Cross sign certificate SN 0090de6c7fb3b50b3c0617724fc13402ad CN = GoDaddy TLS Root CA - R1.

Certificate Tree (New to Old)



Important Files

The leaf certificate is issued under the R1 DV issuing CA, but clients validate it by building a chain to GoDaddy Class 2 Root – G2 using the published R1 → G2 cross certificate. The relevant artifacts in the repository are the G2 trust anchor (gdroot-g2), the cross certificate (gd_tls_root-r1-cross-g2), the R1 DV issuing intermediate (gd_tls_issuing_dv-r1v1), and the native hierarchy root (gd_tls_root-r1) **certs.godaddy.com**. This cross-sign approach allows browsers to validate the chain today (anchoring at G2), while R1 trust propagates over time.

Related Information

Details on transitioning from the old root to new root are documented here:

[Why is GoDaddy removing ClientAuth EKU and transitioning to the R1 root hierarchy for DV TLS issuance?](#)

In case you encounter this issue, [here](#) is the Godaddy repository to download certificate.