

# Expressway MRA에서 GoDaddy Root 마이그레이션이 미치는 영향 이해

## 목차

---

[소개](#)

[배경](#)

[인증서 세부 사항](#)

[이전 루트](#)

[새 루트](#)

[새 중간](#)

[교차 서명 인증서](#)

[인증서 트리\(신규 - 이전\)](#)

[중요 파일](#)

[관련 정보](#)

---

## 소개

이 문서에서는 GoDaddy 루트 인증서를 G2에서 (R1 + R1V1)로 마이그레이션한 효과에 대해 설명합니다.

## 배경

GoDaddy가 기존 루트(G2) 정책에서 새 R1 루트 인증서 체인으로 전환하고 있습니다. 새 인증서는 서버 인증 ECU만 포함해야 합니다.

이 전환은 Good Daddy 인증서를 설치한 고속도로와 기타 에지 제품에 영향을 미칩니다.

루트 전환은 다음과 같은 이유로 발생합니다.

- G2 서명/발급 중간체는 ECU가 나열되지 않으므로 해당 계층이 Chrome Root Program 요구 사항을 준수하지 않습니다. 그 결과 영향받는 G2 중간물질로부터의 발행은 그 일자까지 중단되어야 한다.
- ECU가 없다는 것은 모든 용도가 인증서에 의해 제공된다는 것을 의미합니다.

## 인증서 세부 사항

## 이전 루트

CN: GoDaddy 루트 인증 기관 - G2

2038년 1월 1일 금요일 오전 05:29:59

SN 00

이 기존 루트는 새 루트 R1로 교체됩니다.

## 새 루트

CN = GoDaddy TLS 루트 CA - R1

2040년 8월 24일 금요일 오후 5:29:59

SN 00da62ff9e2619b1257a4809368ee8e3f7

새로운 R1 루트는 다음 섹션에 설명된 대로 새로운 중간체에 서명합니다.

## 새 중간

CN = GoDaddy TLS Intermediate CA DV - R1v1

2040년 8월 24일 금요일 오후 5:29:59

SN 008aaa80515c0bc688c7955d70f27758ac

이전 G2 루트가 있는 OS 신뢰 저장소는 이 목적을 위해 새로운 인증서 체인(R1 + R1V1)을 신뢰하지 않습니다. GoDaddy가 교차 서명 신뢰 경로를 생성했습니다.

새 R1 루트 인증서가 기존 G2 루트 인증서를 신뢰합니다.

## 교차 서명 인증서

CN = GoDaddy TLS 루트 CA - R1

2038년 1월 1일 금요일 오전 05:29:59

SN 0090de6c7fb3b50b3c0617724fc13402ad

올바른 체인이 설치되지 않았거나 Expressway Trust 스토어에 새 체인(R1 + R1v1)만 설치된 경우 MRA IP 전화 등록이 중단됩니다.

Expressway Pcap에 표시된 오류는 IP 전화기에서 오는 알 수 없는 CA입니다. IP 전화 신뢰 저장소에 누락된 CA가 있다고 가정할 수 있습니다.

88xx ip phone 135.x.x.25

172.x.x.34 고속도로

| 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 [RST] Seq=187 Ack=5795 Win=0 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 | 138.587002 | 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       |

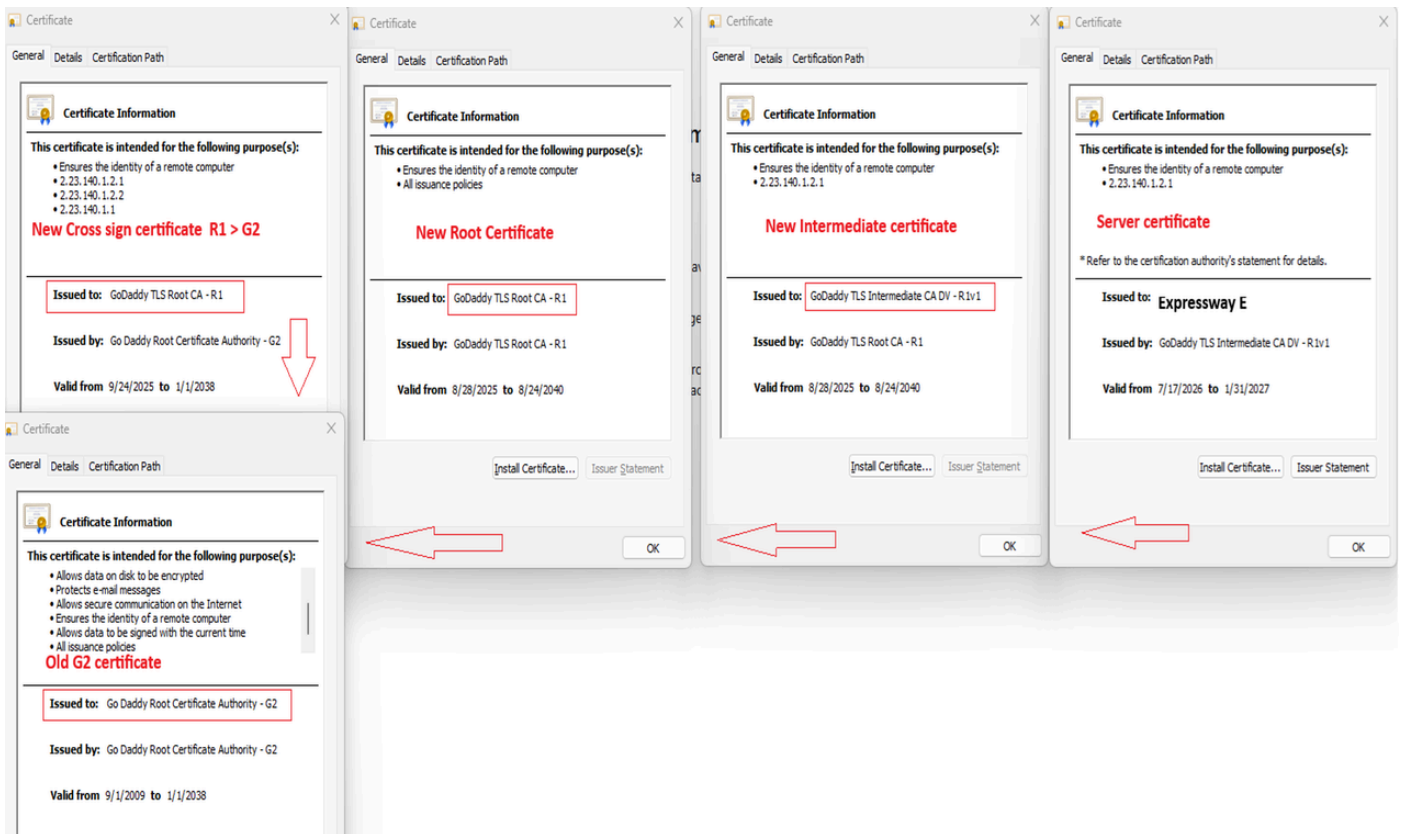
> Frame 3295: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0  
> Ethernet II, Src: PaloAltoNetw\_00:02:40 (00:1b:17:00:02:40), Dst: VMware\_9f:0d:52 (00:50:56:9f:0d:52)  
> Internet Protocol Version 4, Src: 135.x.x.25, Dst: 172.x.x.34  
> Transmission Control Protocol, Src Port: 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)

새 루트 인증서와 교차 서명 인증서의 CN 이름이 CN = GoDaddy TLS Root CA - R1과 같기 때문에 Expressway 트러스트 저장소에서 교차 서명 인증서를 수락하지 않는 경우도 있습니다.

해당하는 경우:

1. 새 루트 R1 인증서 SN 00da62ff9e2619b1257a4809368ee8e3f7을 삭제하지 마십시오.
2. Cross sign certificate SN 0090de6c7fb3b50b3c0617724fc13402ad CN = GoDaddy TLS Root CA - R1을 업로드합니다.

## 인증서 트리(신규 - 이전)



## 중요 파일

리프 인증서는 R1 DV 발급 CA에서 발급되지만, 클라이언트는 게시된 R1→G2 교차 인증서를 사용하여 GoDaddy Class 2 Root - G2에 체인을 구축하여 인증합니다. 저장소의 관련 아티팩트는 G2 트러스트 앵커(gdroot-g2), 상호 인증서(gd\_tls\_root-r1-cross-g2), R1 DV 발급 중간(gd\_tls\_issuing\_dv-r1v1) 및 기본 계층 루트(gd\_tls\_root-r1) certs.godaddy.com입니다. 이 교차 서명 접근 방식을 통해 브라우저는 현재(G2에 고정) 체인의 유효성을 검사할 수 있는 반면, R1 신뢰는 시간이 지남에 따라 전파됩니다.

## 관련 정보

이전 루트에서 새 루트로 전환하는 방법에 대한 자세한 내용은 다음 사이트에 설명되어 있습니다.

- [GoDaddy가 ClientAuth EKU를 제거하고 DV TLS 발급을 위해 R1 루트 계층으로 전환해야 하는 이유는 무엇입니까?](#)

이 문제가 발생하는 경우 인증서를 다운로드할 Godaddy 저장소가 있습니다.

- [GoDaddy 저장소](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.