

Comprendre l'effet de la migration de racine GoDaddy sur Expressway MRA

Table des matières

[Introduction](#)

[Informations générales](#)

[Caractéristiques du certificat](#)

[Ancienne racine](#)

[CN : Autorité de certification racine GoDaddy - G2](#)

[Nouvelle racine](#)

[CN = Autorité de certification racine GoDaddy TLS - R1](#)

[Nouvel intermédiaire](#)

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

[Certificat De Signes Croisés](#)

[CN = Autorité de certification racine GoDaddy TLS - R1](#)

[Arborescence de certificats \(nouveau à ancien\)](#)

[Fichiers importants](#)

[Informations connexes](#)

Introduction

Ce document décrit l'effet de la migration du certificat racine GoDaddy de G2 vers (R1 + R1V1).

Informations générales

GoDaddy passe de l'ancienne stratégie racine (G2) à la nouvelle chaîne de certificats racine de R1. Les nouveaux certificats doivent inclure uniquement l'EKU d'authentification du serveur.

Cette transition affecte les autoroutes et autres produits de périphérie qui ont installé des certificats GoDaddy.

La transition des racines se produit en raison de :

- Les intermédiaires de signature/émission G2 n'ont pas d'EKU répertorié, ce qui rend cette hiérarchie non conforme à l'exigence du programme racine Chrome. Par conséquent, l'émission par les intermédiaires G2 touchés doit cesser à cette date.
- Pas d'UER signifie que tous les usages sont servis par un certificat.

Caractéristiques du certificat

Ancienne racine

CN : Autorité de certification racine GoDaddy - G2

Expiration Vendredi 1er janvier 2038 5:29:59

SN 00

Cette ancienne racine est remplacée par la nouvelle racine R1.

Nouvelle racine

CN = Autorité de certification racine GoDaddy TLS - R1

Expiration Vendredi, 24 août 2040 17:29:59

SN 00da62ff9e2619b1257a4809368ee8e3f7

La nouvelle racine R1 signe le nouvel intermédiaire comme indiqué dans les sections suivantes.

Nouvel intermédiaire

CN = GoDaddy TLS Intermediate CA DV - R1v1

Expiration Vendredi, 24 août 2040 17:29:59

SN 008aaa80515c0bc688c7955d70f27758ac

Les magasins d'approbation du système d'exploitation qui ont une ancienne racine G2 ne feront pas confiance à une nouvelle chaîne de certificats (R1 + R1V1) à cet effet GoDaddy a créé un chemin d'approbation entre les signes croisés, où

Le nouveau certificat racine R1 approuve l'ancien certificat racine G2.

Certificat De Signes Croisés

CN = Autorité de certification racine GoDaddy TLS - R1

Expiration vendredi 1janvier 1, 2038 5:29:59

SN 0090de6c7fb3b50b3c0617724fc13402ad

Si la chaîne installée n'est pas correcte ou si la nouvelle chaîne (R1 + R1v1) est uniquement installée dans le magasin Expressway Trust, l'enregistrement du téléphone IP MRA est bloqué.

L'erreur détectée dans expressway pcap est une CA inconnue provenant d'un téléphone IP. Vous pouvez supposer qu'il manque une autorité de certification dans le magasin de confiance de téléphone IP.

téléphone ip 88xx 135.x.x.25

Expressway 172.x.x.34

The image shows a Wireshark packet capture of a TLS handshake. The packet list on the left shows several packets, with packet 3295 highlighted in red. The packet details pane on the right shows the structure of packet 3295, which is a TLS alert. The alert is of level 'Fatal' and description 'Unknown CA'. The content type is 'Alert (21)' and the version is 'TLS 1.2 (0x0303)'. The packet is sent from source IP 135.579359 to destination IP 172.1425360.

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 [SNI= 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
3317	140.753164	1	1	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: 135.579359, Dst: 172.1425360
> Transmission Control Protocol, Src Port: 50988, Dst Port: 8443, Seq: 180, 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)

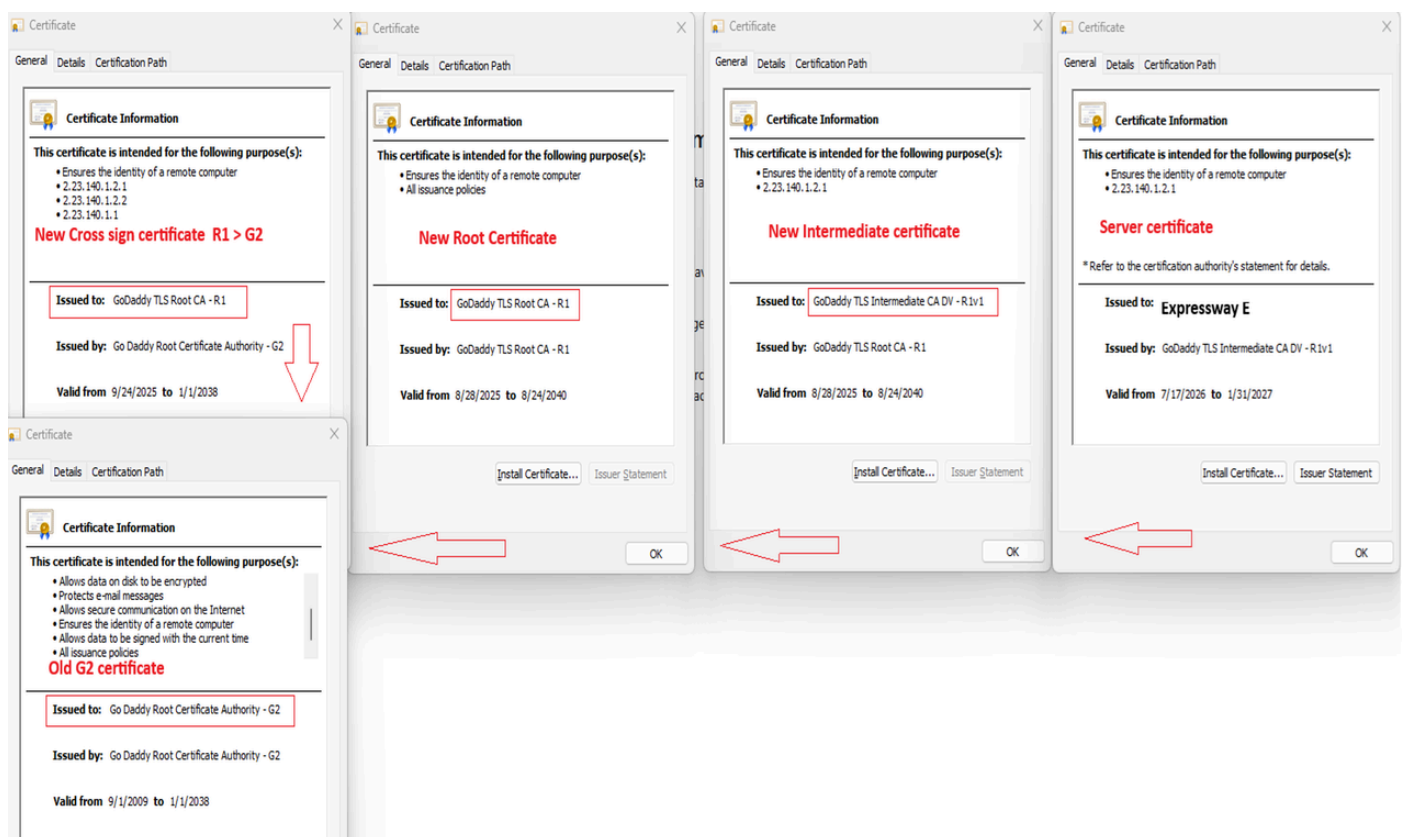
Il y a également une situation où le magasin de confiance Expressway n'accepte pas le certificat de croix de signe parce que le nouveau certificat racine et le nouveau certificat de croix de signe

ont le même nom CN, comme dans CN = GoDaddy TLS Root CA - R1.

Si c'est le cas :

1. SUPPRIMEZ le nouveau certificat racine R1 SN 00da62ff9e2619b1257a4809368ee8e3f7.
2. Téléchargez le certificat Cross sign SN 0090de6c7fb3b50b3c0617724fc13402ad CN = GoDaddy TLS Root CA - R1.

Arborescence de certificats (nouveau à ancien)



Fichiers importants

Le certificat leaf est émis sous l'autorité de certification émettrice de la DV de R1, mais les clients le valident en créant une chaîne à GoDaddy Class 2 Root - G2 à l'aide du certificat croisé R1 → G2 publié. Les artefacts pertinents dans le référentiel sont l'ancre de confiance G2 (gdroot-g2), le certificat croisé (gd_tls_root-r1-cross-g2), l'intermédiaire d'émission de DV R1 (gd_tls_emission_dv-r1v1) et la racine de hiérarchie native (gd_tls_root-r1) certs.godaddy.com. Cette approche de signe croisé permet aux navigateurs de valider la chaîne aujourd'hui (ancrage au niveau de G2), tandis que la confiance de R1 se propage au fil du temps.

Informations connexes

Les détails sur la transition de l'ancienne racine à la nouvelle racine sont documentés ici :

[Pourquoi GoDaddy supprime ClientAuth ECU et effectue la transition vers la hiérarchie racine de R1 pour l'émission DV TLS ?](#)

Si vous rencontrez ce problème, [voici](#) le référentiel Godaddy pour télécharger le certificat.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.