

Entender o efeito da migração de raiz GoDaddy no MRA do Expressway

Contents

[Introdução](#)

[Informações de Apoio](#)

[Especificações do certificado](#)

[Raiz Antiga](#)

[CN: Autoridade de Certificação Raiz GoDaddy - G2](#)

[Nova Raiz](#)

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

[Novo intermediário](#)

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

[Assinatura cruzada de certificado](#)

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

[Árvore de Certificados \(Nova para Antiga\)](#)

[Arquivos importantes](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o efeito da migração do certificado raiz GoDaddy de G2 para (R1 + R1V1).

Informações de Apoio

GoDaddy está fazendo a transição da política de Raiz Antiga (G2) para a nova cadeia de certificados raiz de R1. Os novos certificados devem incluir somente o ECU de Autenticação de Servidor.

Essa transição afeta as vias expressas e outros produtos de borda que instalaram certificados GoDaddy.

A transição de raízes ocorre devido a:

- Os intermediários de assinatura/emissão G2 não têm nenhum ECU listado, o que torna essa hierarquia fora do cumprimento do requisito do programa raiz do Chrome.

Consequentemente, a emissão dos intermediários G2 afetados deve cessar nessa data.

- Nenhuma ECU significa que todas as finalidades são servidas por certificado.

Especificações do certificado

Raiz Antiga

CN: Autoridade de Certificação Raiz GoDaddy - G2

Vencimento sexta-feira, 1 de janeiro de 1, 2038 05:29:59

SN 00

Essa raiz antiga é substituída pela nova raiz R1.

Nova Raiz

CN = CA raiz TLS GoDaddy - R1

Vencimento sexta-feira, 24 de agosto de 2004, 2040 17:29:59

SN 00da62ff9e2619b1257a4809368ee8e3f7

A nova raiz de R1 assina o novo intermediário conforme descrito nas próximas seções.

Novo intermediário

CN = GoDaddy TLS Intermediate CA DV - R1v1

Vencimento sexta-feira, 24 de agosto de 2004, 2040 17:29:59

SN 008aaa80515c0bc688c7955d70f27758ac

As lojas de confiança do SO que têm raiz G2 antiga não confiarão em uma nova cadeia de

certificados (R1 + R1V1) para essa finalidade. O GoDaddy criou um caminho de confiança de sinal cruzado, onde

o novo certificado raiz R1 confia no antigo certificado raiz G2.

Assinatura cruzada de certificado

CN = CA raiz TLS GoDaddy - R1

Vencimento sexta-feira, 1 de janeiro de 1, 2038 05:29:59

SN 0090de6c7fb3b50b3c0617724fc13402ad

Se você não tiver a cadeia correta instalada ou se tiver apenas uma nova cadeia (R1 + R1v1) instalada no armazenamento Expressway Trust, o registro do telefone IP MRA será interrompido.

O erro visto no pcap do expressway é uma CA desconhecida proveniente de um telefone IP. Você pode supor que há uma CA ausente no armazenamento confiável do telefone IP.

telefone ip 88xx 135.x.x.25

Expressway 172.x.x.34

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	1,25	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	1,25	TCP 66 8443 → 50988 [ACK] Seq=1 Ack=180 Win=65536 Len=0 TSval=2071425344 TSecr=4294941909
3286	138.548081	1	5	1	1,25	TLSv1_ 2962 Client Hello [SN] [f.org]
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	138.587082	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	140.763162	1	5	1	4	TCP 74 8443 → 50988 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3081437648 TSecr=0

> Frame 3295: 73 bytes captured 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: 135.172.255.34

> 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)

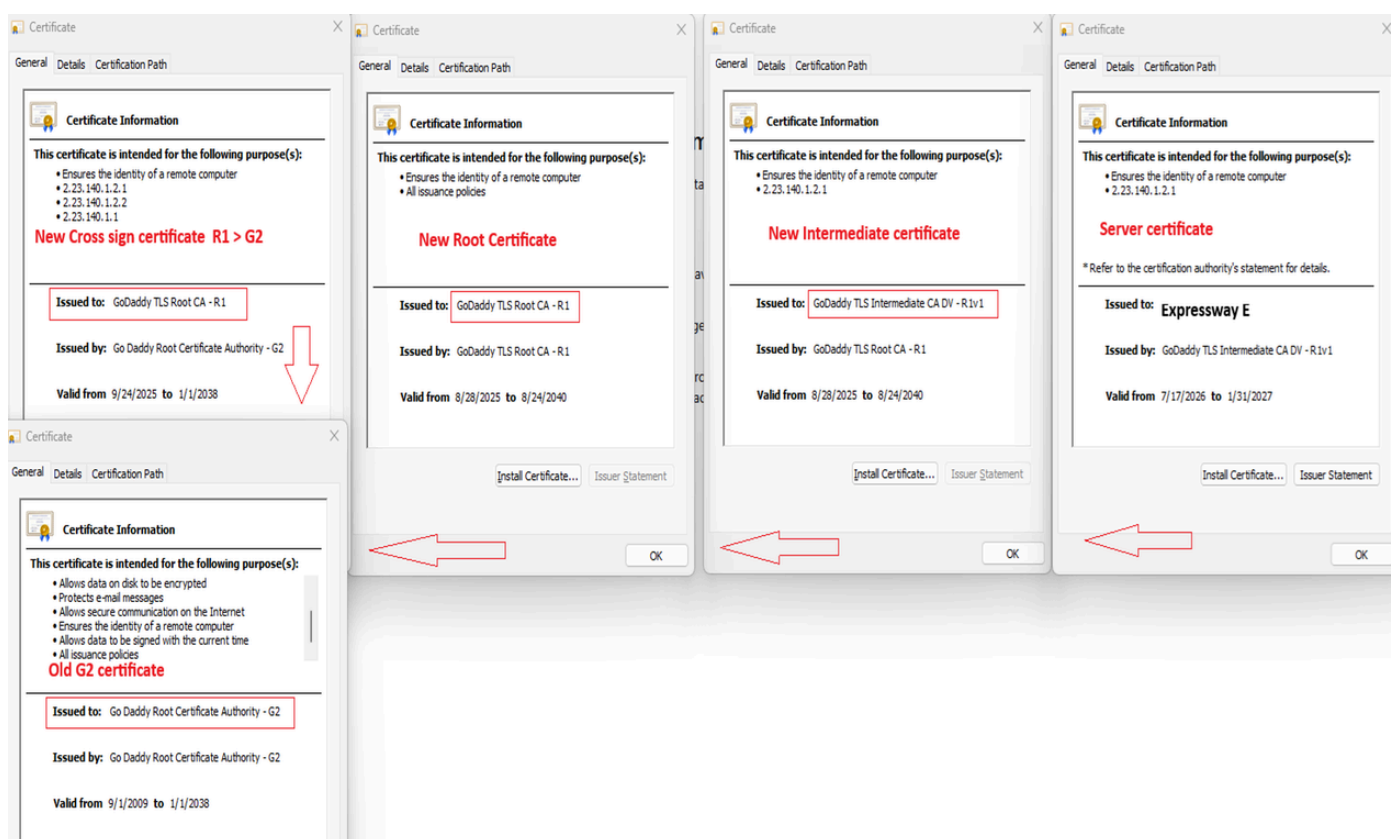
 Version: TLS 1.2 (0x0303)

Há também uma situação em que o armazenamento de confiança do Expressway não aceita o certificado de assinatura cruzada porque o novo certificado raiz e o certificado de assinatura cruzada têm o mesmo nome CN, como em CN = GoDaddy TLS Root CA - R1.

Se for esse o caso:

1. DELETE Novo certificado R1 Raiz SN 00da62ff9e2619b1257a4809368ee8e3f7.
2. Carregar Certificado de assinatura cruzada SN 0090de6c7fb3b50b3c0617724fc13402ad CN = GoDaddy TLS Root CA - R1.

Árvore de Certificados (Nova para Antiga)



Arquivos importantes

O certificado leaf é emitido sob a CA emissora do DV de R1, mas os clientes o validam criando uma cadeia para Raiz GoDaddy Classe 2 - G2 usando o certificado cruzado R1 → G2 publicado. Os artefatos relevantes no repositório são a âncora de confiança G2 (gdroot-g2), o certificado cruzado (gd_tls_root-r1-cross-g2), o DV de R1 que emite intermediário (gd_tls_issuing_dv-r1v1) e a raiz de hierarquia nativa (gd_tls_root-r1) certs.godaddy.com. Essa abordagem de sinal cruzado permite que os navegadores validem a cadeia hoje (ancorando em G2), enquanto a confiança em

R1 se propaga ao longo do tempo.

Informações Relacionadas

Detalhes sobre a transição da raiz antiga para a nova raiz estão documentados aqui:

[Por que GoDaddy está removendo a ECU ClientAuth e fazendo a transição para a hierarquia raiz R1 para emissão de DV TLS?](#)

No caso de você encontrar este problema, [aqui](#) é o repositório Godaddy para baixar o certificado.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.