

了解GoDaddy根迁移对Expressway MRA的影响

目录

[简介](#)

[背景信息](#)

[证书具体信息](#)

[旧根](#)

[CN:GoDaddy根证书颁发机构 — G2](#)

[新根](#)

[CN = GoDaddy TLS根CA - R1](#)

[新的中间产品](#)

[CN = GoDaddy TLS中间CA DV - R1v1](#)

[交叉签名证书](#)

[CN = GoDaddy TLS根CA - R1](#)

[证书树 \(新到旧\)](#)

[重要文件](#)

[相关信息](#)

简介

本文档介绍将GoDaddy根证书从G2迁移到(R1 + R1V1)的效果。

背景信息

GoDaddy正在从旧根(G2)策略过渡到新的R1根证书链。新证书必须仅包含服务器身份验证EKU。

此过渡影响expressway和已安装GoDaddy证书的其他边缘产品。

根过渡发生的原因包括：

- G2签名/发布中间件未列出任何EKU，这使得该层次结构不符合Chrome根计划要求。因此，受影响的G2中间体的发行必须在该日期前停止。
- 没有EKU意味着所有用途都通过证书提供。

证书具体信息

旧根

CN:GoDaddy根证书颁发机构 — G2

2038年1月1日星期五5:29:59

SN 00

这个旧的根桥被新的根R1所取代。

新根

CN = GoDaddy TLS根CA - R1

2040年8月24日星期五5:29:59

SN 00da62ff9e2619b1257a4809368ee8e3f7

新的R1根桥接符新中间设备，如下一节所述。

新的中间产品

CN = GoDaddy TLS中间CA DV - R1v1

2040年8月24日星期五5:29:59

SN 008aaa80515c0bc688c7955d70f27758ac

具有旧G2根的OS信任存储区不会信任新的证书链(R1 + R1V1)，为此，GoDaddy已创建交叉符号信任路径，其中

新的R1根证书信任旧的G2根证书。

交叉签名证书

CN = GoDaddy TLS根CA - R1

2038年1月1日星期五5:29:59

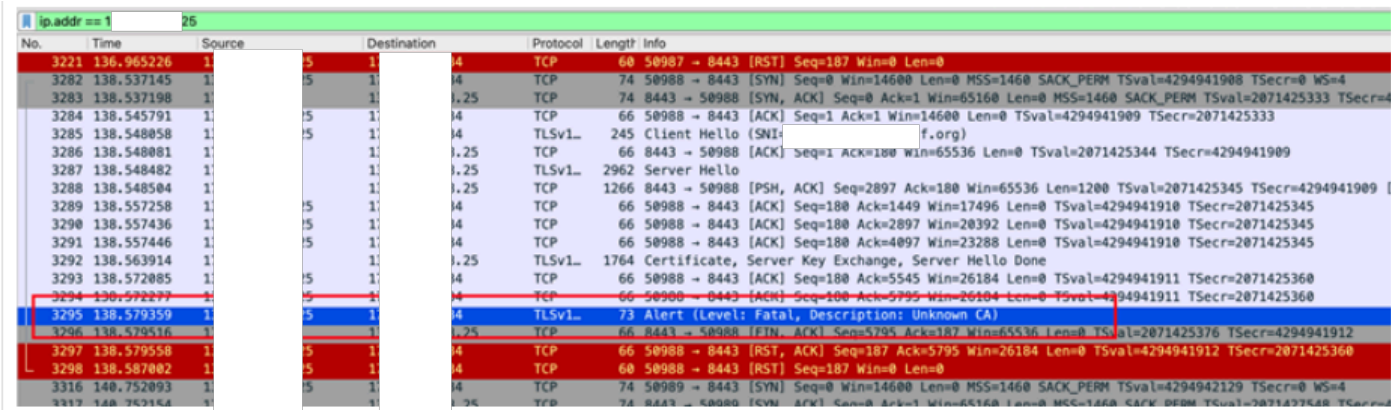
SN 0090de6c7fb3b50b3c0617724fc13402ad

如果您没有安装正确的链，或者您在Expressway Trust商店中仅安装新的链(R1 + R1v1)，则MRA IP电话注册会暂停。

在expressway pcap中看到的错误是来自IP电话的未知CA。您可以假设IP电话信任库上缺少CA。

88xx ip电话135.x.x.25

172.x.x.34高速公路



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	4	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	4	TLSv1.2 245 Client Hello [SNI= f.org]
3286	138.548081	1	5	1	1,25	TCP 66 8443 → 50988 [ACK] Seq=1 Ack=180 Win=65536 Len=0 TSval=2071425344 TSecr=4294941909
3287	138.548482	1	5	1	1,25	TLSv1.2 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	TLSv1.2 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	TLSv1.2 73 Alert (Level: Fatal, Description: Unknown CA)
3296	138.579516	1	5	1	1,25	TCP 66 8443 → 50988 [PSH, 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	138.587002	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	140.752154	1	5	1	4	TCP 74 8443 → 50989 [SYN, 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: 135.537198, Dst: 172.140.752093

> 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)

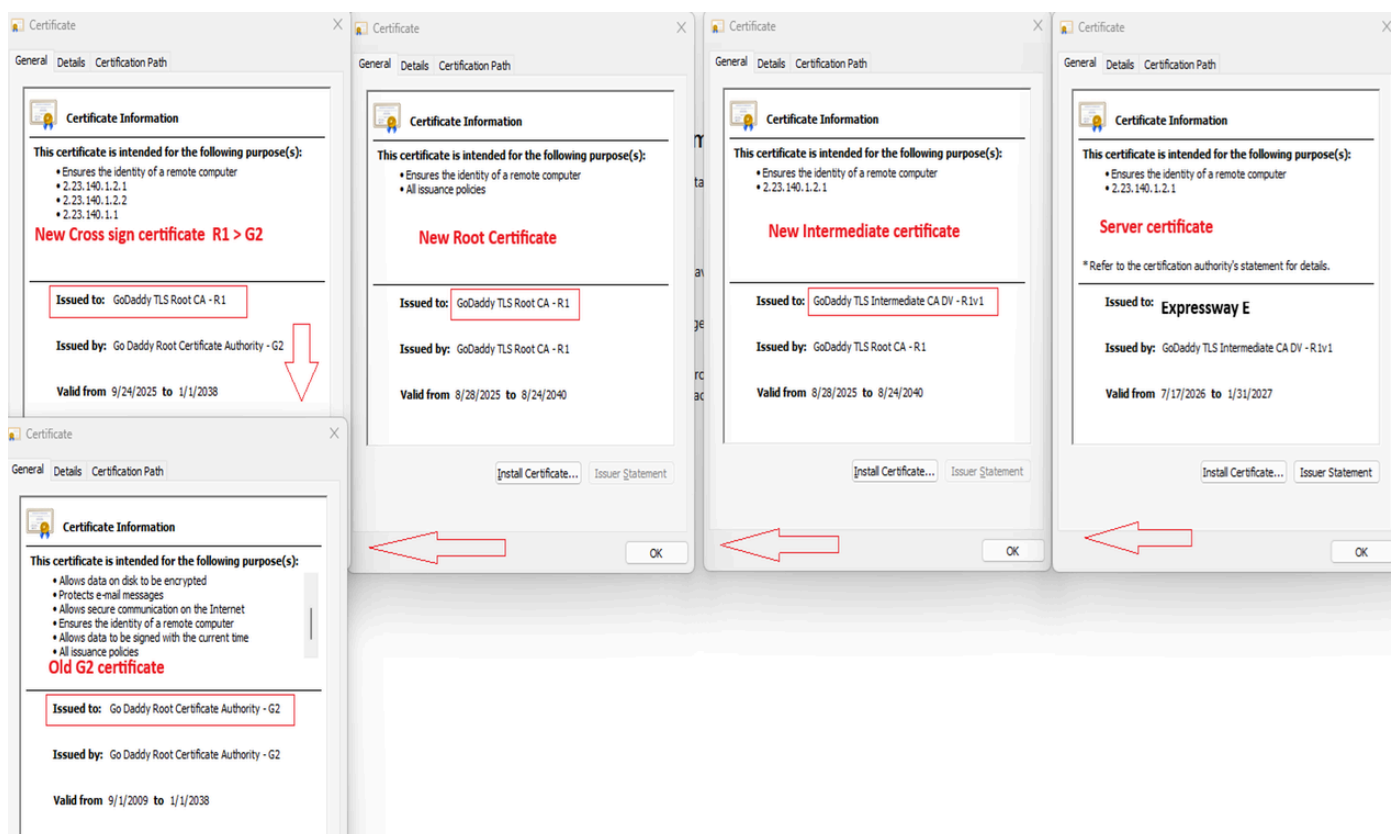
 Version: TLS 1.2 (0x0303)

此外，Expressway信任存储也不接受交叉签名证书，因为新的根证书和交叉签名证书具有相同的CN名称，如CN = GoDaddy TLS Root CA - R1。

如果情况如此：

- 1.删除新的根R1证书SN 00da62ff9e2619b1257a4809368ee8e3f7。
- 2.上传交叉签名证书SN 0090de6c7fb3b50b3c0617724fc13402ad CN = GoDaddy TLS根CA - R1。

证书树（新到旧）



重要文件

枝叶证书根据R1 DV颁发CA颁发，但客户端使用已发布的R1 → G2交叉证书建立到GoDaddy 2类根— G2的链来对其进行验证。存储库中的相关对象是G2信任锚点(gdroot-g2)、交叉证书(gd_tls_root-r1-cross-g2)、R1 DV发布中间件(gd_tls_issuing_dv-r1v1)和本地层次结构根(gd_tls_root-r1)certs.godaddy.com。这种交叉符号方法允许浏览器验证当前链（在G2上锚定），而R1信任会随着时间推移而传播。

相关信息

从旧根到新根的转换详细信息记录如下：

[为什么GoDaddy删除ClientAuth EKU并过渡到R1根层次结构以进行DV TLS颁发？](#)

如果遇到此问题，请点击此处[下载Godaddy](#)存储库。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。