

Expressway MRAでのGoDaddyルート移行の影響について

内容

[はじめに](#)

[バックグラウンド情報](#)

[証明書の詳細](#)

[古いルート](#)

[CN:GoDaddyルート認証局 - G2](#)

[新しいルート](#)

[CN = GoDaddy TLSルートCA - R1](#)

[新しい中間](#)

[CN = GoDaddy TLS中間CA DV - R1v1](#)

[クロス署名証明書](#)

[CN = GoDaddy TLSルートCA - R1](#)

[証明書ツリー \(新規から旧へ\)](#)

[重要なファイル](#)

[関連情報](#)

はじめに

このドキュメントでは、GoDaddyルート証明書をG2から(R1 + R1V1)に移行した結果について説明します。

バックグラウンド情報

GoDaddyは古いルート(G2)ポリシーから新しいR1ルート証明書チェーンに移行します。新しい証明書には、サーバ認証EKUのみを含める必要があります。

この移行は、GoDaddy証明書をインストールしたExpresswayおよびその他のエッジ製品に影響を与えます。

ルートの移行は、次の理由で行われます。

- G2署名・発行中間機関はEKUリストを持たないため、この階層はChromeルートプログラム要件に準拠していません。その結果、影響を受けたG2中間国からの発行は、同日までに停止しなければならない。

- ECUは、すべての目的が証明書によって提供されることを意味しません。

証明書の詳細

古いルート

CN:GoDaddyルート認証局 – G2

有効期限2038年1月1日金曜日午前5:29:59

シリアル00

この古いルートは、新しいルートR1に置き換えられます。

新しいルート

CN = GoDaddy TLSルートCA - R1

有効期限2040年8月24日 (金午後5:29:59)

SN 00da62ff9e2619b1257a4809368ee8e3f7

次のセクションで概説するように、新しいR1ルートが新しい中間ルートに署名します。

新しい中間

CN = GoDaddy TLS中間CA DV - R1v1

有効期限2040年8月24日 (金午後5:29:59)

SN 008aaa80515c0bc688c7955d70f27758ac

古いG2ルートを持つOS信頼ストアは、この目的のために新しい証明書チェーン(R1 + R1V1)を信頼しません。GoDaddyはクロス署名の信頼パスを作成しました。

新しいR1ルート証明書は、古いG2ルート証明書を信頼します。

クロス署名証明書

CN = GoDaddy TLSルートCA - R1

有効期限：2038年1月1日（金）午前5:29:59

SN 0090de6c7fb3b50b3c0617724fc13402ad

正しいチェーンがインストールされていない場合、またはExpressway信頼ストアに新しいチェーン(R1 + R1v1)のみがインストールされている場合、MRA IP電話の登録は停止します。

Expressway pcapに表示されるエラーは、IP Phoneからの不明なCAです。IP Phone信頼ストアにCAが存在しないと仮定できます。

88xx ip phone 135.x.x.25

172.x.x.34 Expressway

No.	Time	Source	Destination	Protocol	Length	Info
3221	136.965226	1	5	1	60	TCP 50987 → 8443 [RST] Seq=187 Win=0 Len=0
3282	138.537145	1	5	1	74	TCP 50988 → 8443 [SYN] Seq=0 Win=1460 Len=0 MSS=1460 SACK_PERM TSval=4294941908 TSecr=0 WS=4
3283	138.537198	1	5	1	74	TCP 8443 → 50988 [SYN, ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=1460 SACK_PERM TSval=2071425333 TSecr=4
3284	138.545791	1	5	1	66	TCP 50988 → 8443 [ACK] Seq=1 Ack=1 Win=1460 Len=0 TSval=4294941909 TSecr=2071425333
3285	138.548058	1	5	1	245	TLSv1.. Client Hello (SN=[f.org])
3286	138.548081	1	5	1	66	TCP 8443 → 50988 [ACK] Seq=1 Ack=180 Win=65536 Len=0 TSval=2071425344 TSecr=4294941909
3287	138.548482	1	5	1	2962	TLSv1.. Server Hello
3288	138.548504	1	5	1	1266	TCP 8443 → 50988 [PSH, ACK] Seq=2897 Ack=180 Win=65536 Len=1200 TSval=2071425345 TSecr=4294941909
3289	138.557258	1	5	1	66	TCP 50988 → 8443 [ACK] Seq=180 Ack=1449 Win=17496 Len=0 TSval=4294941910 TSecr=2071425345
3290	138.557436	1	5	1	66	TCP 50988 → 8443 [ACK] Seq=180 Ack=2897 Win=20392 Len=0 TSval=4294941910 TSecr=2071425345
3291	138.557446	1	5	1	66	TCP 50988 → 8443 [ACK] Seq=180 Ack=4097 Win=23288 Len=0 TSval=4294941910 TSecr=2071425345
3292	138.563914	1	5	1	1764	TLSv1.. Certificate, Server Key Exchange, Server Hello Done
3293	138.572085	1	5	1	66	TCP 50988 → 8443 [ACK] Seq=180 Ack=5545 Win=26184 Len=0 TSval=4294941911 TSecr=2071425360
3294	138.572277	1	5	1	66	TCP 50988 → 8443 [ACK] Seq=180 Ack=5795 Win=26184 Len=0 TSval=4294941911 TSecr=2071425360
3295	138.579359	1	5	1	73	TLSv1.. Alert (Level: Fatal, Description: Unknown CA)
3296	138.579516	1	5	1	66	TCP 8443 → 50988 [FIN, ACK] Seq=5795 Ack=187 Win=65536 Len=0 TSval=2071425376 TSecr=4294941912
3297	138.579558	1	5	1	66	TCP 50988 → 8443 [RST, ACK] Seq=187 Ack=5795 Win=26184 Len=0 TSval=4294941912 TSecr=2071425360
3298	138.587002	1	5	1	60	TCP 50988 → 8443 [RST] Seq=187 Win=0 Len=0
3316	140.752093	1	5	1	74	TCP 50989 → 8443 [SYN] Seq=0 Win=1460 Len=0 MSS=1460 SACK_PERM TSval=4294942129 TSecr=0 WS=4
3317	140.763154	1	5	1	74	TCP 8443 → 50989 [SYN, ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=1460 SACK_PERM TSval=2071427548 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.x.x.34, 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)

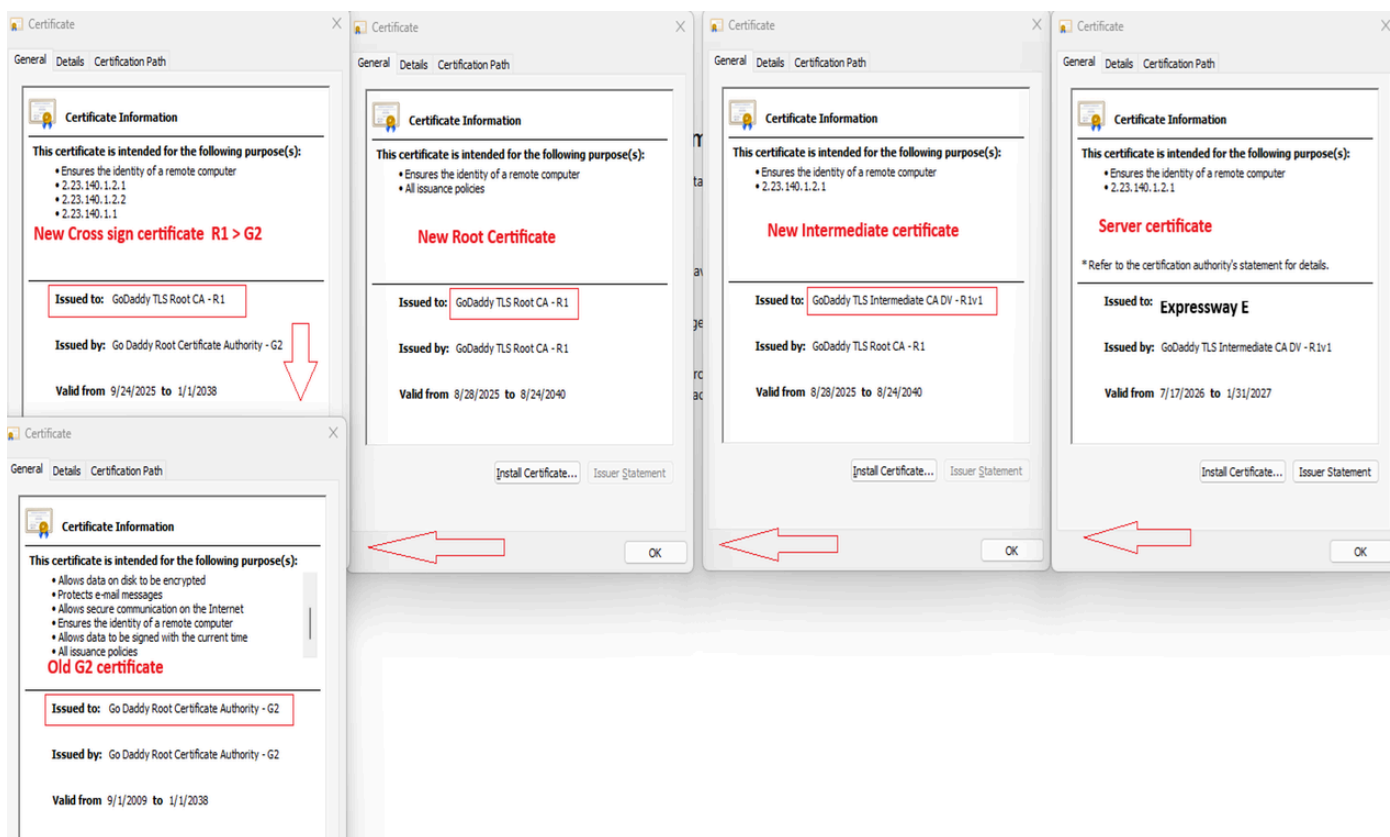
> Version: TLS 1.2 (0x0303)

また、新しいルート証明書とクロスサイン証明書がCN = GoDaddy TLSルートCA - R1のように同じCN名を持つため、Expressway信頼ストアがクロスサイン証明書を受け入れない場合もあります。

この場合、次のようになります。

1. 新しいルートR1証明書SN 00da62ff9e2619b1257a4809368ee8e3f7を削除します。
2. クロスサイン証明書SN 0090de6c7fb3b50b3c0617724fc13402ad CN = GoDaddy TLSルートCA - R1をアップロードします。

証明書ツリー (新規から旧へ)



重要なファイル

リーフ証明書はR1 DV発行側CAで発行されますが、クライアントは、公開されたR1 → G2クロス証明書を使用してGoDaddyクラス2ルート - G2へのチェーンを構築することで、リーフ証明書を検証します。リポジトリ内の該当するアーティファクトは、G2トラストアンカー(gdroot-g2)、クロス証明書(gd_tls_root-r1-cross-g2)、R1 DV発行中間(gd_tls_issuing_dv-r1v1)、およびネイティブ階層ルート(gd_tls_root-r1)certs.godaddy.comです。このクロスサインアプローチにより、ブラウザは現在のチェーンを検証し (G2にアンカー) 、R1信頼は時間の経過とともに伝播します。

関連情報

古いルートから新しいルートへの移行に関する詳細は、次のドキュメントに記載されています。

[GoDaddyはなぜClientAuth ECUを削除し、DV TLS発行のR1ルート階層に移行するのですか。](#)

この問題が発生した場合は、[こちら](#)が証明書をダウンロードするGodaddyリポジトリです。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。