# 2021年9月30日DST根CA X3證書到期時對 Expressway應執行的操作

### 目錄

<u>簡介</u> <u>採用元件</u> <u>背景資訊</u> <u>問題</u> <u>解決方案</u>

## 簡介

本文檔介紹如何更換設定為於2021年9月30日到期的DST根CA X3。這意味著不信任「IdenTrust DST根CA X3」的較舊裝置將開始收到證書警告,並且TLS協商將中斷。2021年9月30日,較舊的 軟體和裝置信任讓我們加密證書的方式將發生更改。

#### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

Cisco Expressway x12.6

### 背景資訊

- 交叉簽名的CA證書由新的公共CA使用,因此現有裝置可以通過通常可用的現有CA證書信任其 證書。
- 當Let's Encrypt「ISRG Root X1」 CA證書首次於2015年6月頒發時,大多數裝置在其信任儲存 中尚未擁有該證書,因此它們的「ISRG Root X1」 CA證書由自2000年9月30日起已分發的可 靠的「DST Root CA X3」 CA證書交叉簽名。
- 現在大多數裝置都應信任「ISRG根X1」根CA證書,因此我們應能夠輕鬆地更新CA鏈而無需重 新生成伺服器證書。

— 例如,思科在2019年8月之前未將「ISRG根X1」自簽名CA證書新增到我們的intersect信任儲存 捆綁包,但大多數舊裝置仍然可以輕鬆地信任由交叉簽名「ISRG根X1」CA證書頒發的證書,因為 它們都信任「DST根CA X3」根CA證書。

• 這一點非常重要,因為IP電話和CE終端軟體在其嵌入式信任儲存中很可能沒有「ISRG Root X1」自簽名CA證書,因此我們要確保IP電話位於12.7+上,CE終端位於CE9.8.2+或 CE9.9.0+上,以確保他們信任「ISRG Root X1」根CA證書。以下參考連結

https://www.cisco.com/c/dam/en/us/td/docs/voice\_ip\_comm/cuipph/all\_models/ca-list/CA-Trust-List.pdf

https://www.cisco.com/c/en/us/td/docs/voice\_ip\_comm/dx/series/admin/1024/DX00\_BK\_C12F3FF

5\_00\_cisco-dx-series-ag1024/DX00\_BK\_C12F3FF5\_00\_cisco-dx-series-ag1024\_appendix\_01111.html

## 問題

2021年9月30日到期的「IdenTrust DST根CA X3」根,必須替換為「IdenTrust商業根CA 1」

根CA將於2021年9月30日到期

Certificate	×
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s):	-
Proves your identity to a remote computer     Allows data on disk to be encrypted	
Protects email messages     Ensures the identity of a remote computer	
Allows data to be signed with the current time     All issuance policies	
Issued to: DST Root CA X3	-
Issued by: DST Root CA X3	
Valid from 30/09/2000 to 30/09/2021	
	- 1
Issuer <u>S</u> tatemen	t
OK	

Certificate	×
General Details Certification Path	
<u>S</u> how: <all></all>	$\sim$
Field Version Serial number Signature algorithm Signature hash algorithm Signature hash algorithm Valid from Valid from Valid to Subject 30 September 2021 15:01:15	Value V3 44afb080d6a327ba89303986 sha1RSA sha1 DST Root CA X3, Digital Signat 30 September 2000 22:12:19 30 September 2021 15:01:15 DST Root CA X3 Dinital Signat
E	dit Properties <u>C</u> opy to File
	OK

## 解決方案

從Expressway E信任儲存中刪除舊的Acme根CA並更新最新的根證書

下載連結:(複製並貼上)

https://letsencrypt.org/certs/isrgrootx1.pem

https://letsencrypt.org/certs/lets-encrypt-r3.pem

#### 如何更新Expressway伺服器上的根證書

#### 導覽至Maintenance > Security > Trusted CA certificate

# Cisco Expressway-E

Status	> Syste	em > Configuration	on >	Applications >	Users >		Maintenance		
Trust	ed CA ce	rtificate					Upgrade	-	
	Туре		Issue	r		Sub	Logging		ration date
			O=Ter 48e8-	mporary CA f80fac88-( b15c-38a14839ed12	644e-		Smart licensing		
	Certificate		OU=T	emporary CA f80fac88	3-644e-	Mat	Email Notification	ons	11 2023
		CN=T	Temporary CA f80fac88-644e-			Option keys			
	Cortificato		4000-			Mat	Tools >		14 2022
	Certificate			ioVadis Limited CN=0	)uoVadis	IVIAU	Security		Trusted CA certificate
	Certificate		Root	CA 2		Mat	Backup and res	store	Server certificate
	Certificate		O=lde Comn	enTrust, CN=IdenTrust nercial Root CA 1		Mat	Diagnostics >		CRL management
Show a	all (decoded)	Show all (PEM file)	Delete	Select all Unselect al	11		Maintenance m	ode	Client certificate testing
							Language		Certificate-based
Uploa	ad		-				Restart options		autnentication configuration
									Domain certificates
Selec	t the file conta	ining trusted CA certifica	ates		† Brows	e	No file selected.	(i)	Ciphers

### 按一下「Browse」,然後選擇下載的憑證(本檔案上文已提到)。

#### 選擇檔案後點選附加CA證書

CISCO Cisco Expressway-E			his system has 1 ⊨
Status> System> Configuration> Applications> Users> Main	ntenance >		
Trusted CA certificate		You are here: M	laintenance • Secu
Type Issuer		Subject	Expiration date
Certificate O=Temporary CA (80/ac88-644e-48e8-b15c-38a14839ed12, OU=Temporary CA (80/ac88-644e-48e8-b15c-38a1480)	A f80fac88-644e-48e8-b15c-38a14839ed12, CN=Temporary CA f80fac88-644e-48e8-	Matches Issuer	Feb 11 2023
Certificate CN=federation-AD-CA-1		Matches Issuer	Apr 01 2022
Certificate O=QuoVadis Limited, CN=QuoVadis Root CA 2	单 File Upload	**	×
Show all (decoded) Show all (PEM file) Delete Select all Unselect all	$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\clubsuit$ > This PC > Downloads $\checkmark$ $\circlearrowright$ $\checkmark$	Search Downloa	ads
Upload	Organize - New folder	-	• • •
Select the file containing trusted CA certificates	692243340 Name diagnostic_log_c Viotav (2)	Date modifie	ed î
Append CA certificate Reset to default CA certificate	My DATA  X root expire  X root expi	9/27/2021 7 9/27/2021 7	:07 PM :07 PM
Related tasks Activation code onboarding trusted CA certificates	OneDrive - Cisco     Last week (11)     This PC     Y		~ ~ ~
	File name: lets-encrypt-r3 .cer V All I	Files (*.*)	× .
		Open	Cancel

在更新信任儲存中的證書後驗證。

# Cisco Expressway-E

Status	> Syste	em > Configuration >	Applications > Users >	Maintenance >					
Trusted CA certificate       You         Image: File uploaded: CA certificate file uploaded. File contents - Certificates: 1, CRLS: 0.       You									
	Туре	ls 4	ssuer 18e8-b15c-38a14839ed12	Subject	Expiration date	Validity 🔺			
	Certificate	С	CN=federation-AD-CA-1	Matches Issuer	Apr 01 2022	Valid			
	Certificate	C	D=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer	Nov 24 2031	Valid			
	Certificate	C	D=Internet Security Research Group, CN=ISRG Root X1	O=Let's Encrypt, CN=R3	Sep 15 2025	Valid			
	Certificate	C	D=Internet Security Research Group, CN=ISRG Root X1	Matches Issuer	Jun 04 2035	Valid			
Show	all (decoded)	Show all (PEM file) Delete	e Select all Unselect all						

Upload

Select the file containing trusted CA certificates

† Browse... No file selected.

i

Append CA certificate Reset to default CA certificate