パブリックCA証明書でのクライアント認証EKUのサンセットに対するExpresswayの準備

内容

はじめに

このドキュメントでは、6/26以降のパブリックCA証明書でのCisco Expresswayとクライアント認証EKUのサンセットに関するChromeルートプログラムポリシーの変更について説明します。

バックグループ情報

デジタル証明書は、信頼できる認証局(CA)によって発行される電子証明書で、認証、データの整合性、機密性を確保することによってサーバとクライアント間の通信を保護します。これらの証明書には、その目的を定義する拡張キー使用法(EKU)フィールドが含まれています。

- サーバ認証EKU(id-kp-serverAuth)：サーバが身元を証明するために証明書を提示するときに使用されます。
- クライアント認証EKU(id-kp-clientAuth)：双方が互いを認証する相互TLS(mTLS)接続で使用されます。

従来、1つの証明書にサーバ認証とクライアント認証の両方のEKUを含めることができるため、二重目的で使用できます。これは、異なる接続シナリオでサーバとクライアントの両方として機能するCisco Expresswayなどの製品にとって特に重要です。

問題の定義

Chromeルートプログラムポリシーの変更

2026年6月より、Chromeルートプログラムポリシーは、Chromeルートストアに含まれるルート認証局(CA)証明書を制限し、多用途ルートを段階的に廃止して、すべての公開キーインフラストラクチャ(PKI)階層を調整し、TLSサーバ認証のユースケースのみを提供します。

主要なポリシー要件

- パブリックルートCAは、サーバー認証(id-kp-serverAuth)に対してのみ拡張キー使用法(EKU)をアサートする必要があります
- Google Chromeブラウザからの信頼を維持するには、証明書にサーバ認証EKUのみが含まれている必要があります
- これらの証明書にクライアント認証EKUを含めることは禁止されています
- クライアント認証EKUを使用して証明書を発行し続けるルートCAは、最終的にChromeルートストアから削除されます
- パブリックサーバのTLS証明書に使用するルートCAが混在することがなくなりました。
- 実施スケジュール:2026年6月

パブリックCA応答のタイムライン

- 2025年10月：多くのパブリックCA(DigiCert、Sectigo、SSL)が、デフォルトでサーバ

専用証明書の発行を開始しました
- 2026年2月11日：Let's Encryptは、classic ACMEプロファイルを使用したクライアント認証EKUを含む証明書の発行を停止します。
- 2026年5月：パブリックCAサーバがClient Authentication EKU証明書の発行を停止
- 2026年6月：Chromeルートプログラムポリシーが完全に発効

注：このポリシーは、パブリックCAによって発行された証明書にのみ適用されます。プライベートPKIおよび自己署名証明書は、このポリシーの影響を受けません。

シスコの関連資料

- Cisco Bug ID:CSCwr73373- Expressway用の個別のサーバ証明書とクライアント証明書のサポート
- フィールド通知: FN74362
- Chromeルートプログラムポリシー：Chromeルートプログラムポリシードキュメント

Expresswayソリューションへの影響

該当製品

Field Notice FN74362によると、すべてのCisco Expresswayバージョンが該当します。

製品	該当するリリース	影響
Expressway CoreおよびEdge	X14（すべてのバージョン）	X14.0.0からX14.3.7 – 該当するすべてのリリース
Expressway CoreおよびEdge	X15（X15.4より前のバージョン）	X15.0.0からX15.3.2 – 該当するすべてのリリース

Expresswayのデュアルロール

Cisco Expressway製品（Expressway-CおよびExpressway-E）は、さまざまな接続シナリオでサーバとクライアントの両方として機能し、サーバ認証EKUとクライアント認証EKUの両方で証明書を必要とします。

サーバとしてのExpressway E（サーバ認証EKUが必要）:

- HTTPSブラウザアクセス
- SIP UCトラバーサル接続
- Webex Edge音声/MRA接続

クライアントとしてのExpressway E（クライアント認証EKUが必要）：

- B2B通信
- MRA（モバイルおよびリモートアクセス）接続
- XMPPフェデレーション
- SIPネイバーゾーン/CMS接続
- 外部エンティティとの相互作用
- シスコクラウドへの接続（MRAオンボーディング）

影響を受ける具体的な使用例

Cisco ExpresswayでのmTLS接続に現在使用されているクライアント認証EKUを含むパブリックCA署名付き証明書は、Expresswayサーバ証明書です。この証明書は、次のmTLS接続に使用されます。

1. mTLSを介したSIP B2Bコール：Expressway Eが、セッションが開始されたサイトに応じて、mTLS接続でクライアントまたはサーバになる
2. mTLS経由のSIP IMPフェデレーション：Expressway Eは、セッションが開始されたサイトに応じて、mTLS接続でクライアントまたはサーバになります
3. UCトラバーサルゾーン：Expressway Cがクライアント認証EKUを提示
4. mTLS設定によるトラバーサルゾーン：Expressway Cがクライアント認証EKUを提示
5. mTLS設定を使用したSIPネイバーゾーン：Expresswayは、セッションが開始したサイトに応じて、次のものを含め、mTLS接続上のクライアントまたはサーバになります。

- Cisco Unified Communications Manager（Unified CM）
- Cisco Unity
- Cisco Unified Border Element（CUBE）
- Cisco Meeting Server(CMS)
- シスコクラウドへの接続 – MRAオンボーディング（Expresswayがシスコクラウドへの接続を開始し、クライアント認証EKUを提示します）

推奨事項

現在の証明書の監査（必須の最初の手順）

Field Notice FN74362に従い、回避策とソリューションオプションを検討する前に次の手順を実行してください。

- すべてのパブリックTLS証明書のインベントリを準備し、クライアント認証EKUを含む証明書を特定します
- Cisco Expresswayインスタンスのバックアップを作成するか、署名付き証明書と秘密キーを手動でコピーします
- 証明書の使用法の文書化：mTLS接続に使用される証明書を特定します。
- CAおよびルート情報の確認：各証明書を発行したCAおよびルートを文書化します。
- 有効期限の確認：ポリシー適用前に計画的に更新を計画

短期的な回避策（2026年6月より前）

管理者は、次のいずれかの回避策を選択できます。

オプション1：結合されたEKU証明書を提供するパブリックルートCAに切り替える

一部のパブリックルートCA(DigiCertやIdentrustなど)は、代替ルートからの結合EKUを含む証明書を発行します。これは、Chromeブラウザの信頼ストアに含めることはできません。

パブリックルートCAおよびEKUタイプの例(FN74362ごと):

CAベンダー	EKUタイプ	ルートCA	発行側/下位CA
Identrust	clientAuth +サーバ認証	Identrustパブリックセクタルートca 1	Identrust Public Sector Server CA 1
デジタル証明書	clientAuth +サーバ認証	DigiCert Assured ID Root G2	DigiCert Assured ID CA G2

このアプローチの前提条件：

- CAプロバイダーと連携して、そのような証明書が使用可能かどうかを確認します。
- 証明書を展開する前に、証明書を提示するサーバと、証明書を使用するすべてのクライアントの両方が、対応するルートCAを信頼していることを確認してください。
- 通信ピアとルート証明書情報を交換する。
- このアプローチにより、ソフトウェアを即座にアップグレードする必要がなくなります。

証明書管理参照：

- Cisco Expressway証明書の作成および使用展開ガイド(X14.0)
- Cisco Expressway証明書の作成および使用展開ガイド(X15.0)

オプション2：現在の証明書を更新して有効期間を延長する

2026年5月より前に公開ルートCAによって発行され、サーバ認証とクライアント認証の両方のEKUを持つ証明書は、その期間が満了するまで保持されます。

更新戦略

一般的な推奨事項は次のとおりです。

- ポリシーのサンセットが発生する前に結合されたEKU証明書を更新する
- 証明書の有効性を最大にするために、2026年3月15日より前に証明書を更新する予定です。
- この日付を過ぎると、パブリックCA発行の証明書は200日間だけ有効になります。
- このオプションを使用する場合は、証明書をこの日付より前に更新することを強くお勧めします。
- パブリックCAポリシーと実装の日付は異なる場合があります。
- 一部のパブリックCAは結合EKU証明書の発行を停止しており、デフォルトでは提供できません。
- EKUを組み合わせた証明書を生成するには、CA認証局と連携し、パブリックCAによって提供される特別なプロファイルを使用します。

証明書の暗号化に関する特別な考慮事項

FN74362によると、証明書を暗号化してみましょう：

- 現在、Expresswayはハードコードされた従来のACMEプロファイルを使用し、ユーザは変更できません
- この従来のACMEプロファイルは、現在、サーバ認証EKUとクライアント認証EKUの両方を含む証明書を要求するために使用されています
- 2026年2月11日以降、このプロファイルを使用する証明書要求では、Let's Encryptによって生成された証明書にクライアント認証EKUが含まれなくなりました
- 詳細については、「2026年のTLSクライアント認証証明書サポートの終了 – 暗号化しましょう」を参照してください。

ユーザーを暗号化するためのアクションアイテム

- 2026年2月11日より前に証明書を更新する- 90日の有効期間を最大限にするために、できるだけ日付に近づけることが理想的です。
- 2026年2月11日以降に証明書が自動的に更新されないようにするには、ACME自動スケジューラを無効にします。
- このアクションにより、サーバ認証EKUのみを含むバージョンで証明書が誤って上書きされるのを回避できます。
- 2026年2月11日より前に更新しない場合は、Cisco TACにサポートを依頼してください。

オプション3：代替CAプロバイダーの評価と移行

このオプションは、Expressway Cのみに適用され、Expressway Eには適用されません。

プライベートPKIアプローチ

- プライベートPKIへの移行の実現可能性を評価する
- EKUを組み合わせた単一の証明書（必要なEKUを持つサーバ証明書とクライアント証明書）を発行するようにプライベートCAを設定する

- プライベートCA署名付き証明書を発行する場合、ルート証明書情報をピアと共有する必要があります。
- 証明書を発行または展開する前に、証明書を提示するサーバと、証明書を使用するすべてのクライアントの両方が、対応するルートCAを信頼していることを確認してください。
- プライベートCAは、Chromeルートプログラムポリシーの対象ではありません
- 証明書ポリシーの長期的な制御を提供する

⚠ 注意：このオプションは、外部向けサービスとブラウザの信頼にパブリックCA証明書が必要なExpressway-Eには適用できません。

長期的なソリューション（ソフトウェアのアップグレードが必要）

Field Notice FN74362によると、シスコはこの問題に包括的に対処するために、修正済みリリースで製品の機能拡張を行っています。

修正済みリリーススケジュール：

製品	影響を受けるリリース	修正済みリリース	修正の目的	アベイラビリティ
Cisco Expressway	X14.x（すべてのリリース） X15.x（X15.4より前）	X15.4	断続的な解決策：Expressway E上でのServerAuth EKU専用署名付き証明書の追加アップロード、およびExpressway EとExpressway C間のMRA SIP信号用の証明書検証の調整を可能にします。	2026年2月
Cisco Expressway	X14.x（すべてのリリース） X15.x（X15.5より前）	X15.5	包括的なソリューション：クライアント証明書とサーバ証明書を分離するためのUI拡張機能を提供し、EKUチェックを無効にするためのオプションを管理者に提供します。	May 2026

✎ 注:Cisco Expressway EとExpressway Cの両方を同じバージョンにアップグレードする必要があります。

Cisco Expressway X15.4ソリューションの詳細（2026年2月）

目的:ServerAuth EKUのみで証明書に対応し、MRA登録を有効にする断続的なソリューション

主な機能拡張は次のとおりです。

- 証明書のアップロードに関する制限を排除
- 管理者はExpressway EのWeb GUIからサーバ認証EKUのみを使用して証明書をアップロードできます。
- 以前は、Expresswayはサーバのみの証明書を拒否していました
- MRAの証明書検証を調整します。
- MRAソリューションのExpressway-EとExpressway-C間のSIPシグナリングの証明書検証を変更する
- サードパーティアプリケーションからのサーバ専用証明書の受け入れを許可

X15.4へのアップグレードが可能な担当者：

- 新規または既存のExpressway-E for MRAをサーバ専用署名証明書を使用して再導入する場合:
- 2026年2月11日以降にACME(Let's Encrypt)証明書を使用する場合。
- サーバ認証EKUのみを含む署名付き証明書のアップグレードが必要な既存の導入。
- mtls接続で証明書関連の認証の問題が発生する場合

X15.4の重要な要件

- Expressway-EとExpressway-Cの両方をX15.4にアップグレードする必要があります。
- メンテナンス時間帯にアップグレードを計画して、サービスの中断を最小限に抑える

X15.4には次のような制限があります。

- これは、互換性に関する差し迫った問題に対処する断続的なソリューションです
- 完全なデュアル証明書サポートは提供されない
- EKUチェックを無効にするサービスパラメータは含まれていません
- mTLS接続は、セッションが開始されたサイトによっては失敗する可能性があります

Cisco Expressway X15.5ソリューションの詳細（2026年5月）

目的：グローバルなGoogle Chromeルートプログラムの要件を満たす包括的なソリューション

製品の主な機能強化：

- クライアント証明書とサーバ証明書の分離
- 同じインターフェイス上で2つの異なる証明書のサポートを有効にします
- 個別のサーバ認証EKUとクライアント認証EKUを持つExpressway証明書
- 分離された証明書ロールにより、適切なmTLS接続を促進
- UIおよびバックエンドの機能拡張
- 両方の証明書を個別に管理するための新しい証明書管理インターフェイス
- 証明書のアップロード中のクライアント認証EKU検証により、MTLS接続の偶発的なドロップを回避
- 管理者は、サーバ証明書とクライアント証明書を個別にアップロードおよび管理できます

- クライアント認証EKUチェックを無効にするオプション
- 個々のエンタープライズ要件に従って、管理者がクライアント認証EKUチェックを無効にできるサービスパラメータ
- Cisco Expresswayがリモートピア（クライアント）からのEKUを無視して、サーバ認証EKU証明書のみの接続を要求できるようにします。
- クライアント認証EKU証明書がない場合、は、Expresswayでサーバ認証EKU専用証明書をクライアント証明書として使用（再）できるようにします

注：この場合、リモートピアでも同様のIgnore Client Authentication(MCP)EKUモデルをサポートする必要があります

デシジョンツリー

開始：ExpresswayでパブリックCA証明書を使用しますか。

|

├─いいえ：プライベートPKIまたは自己署名

| └─対処の必要なし – ポリシーの影響を受けない

|

└─はい：パブリックCA証明書が使用されています

|

├─ mTLS接続に使用されますか。（影響を受ける特定のユースケースのセクションでユースケースを確認する）

| |

| ├─ NO：サーバ認証のみ

| | └─影響は最小限 – 将来の変更を監視

| |

| └─はい：クライアント認証EKUを使用したmTLS接続

| |

| └─アプローチの選択：

| |

| ├─オプションA：代替ルートCAへの切り替え

| | ├─代替ルートからの結合EKUについてCAプロバイダーに問い合わせてください

| | ├─すべてのピアが新しいルートを信頼することを確認します

| | └─ソフトウェアの即時アップグレードは不要です

| |

| ├─オプションB：期限前の証明書の更新

| | | ├─暗号化する場合： 2026年2月11日までに更新

| | | └─更新後にACMEスケジューラを無効にする

| | | ├─有効期間の延長： 2026年3月15日までに更新

| | └─証明書が期限切れになるまで時間を購入します

| |

| ├─オプションC：プライベートPKIへの移行（Expressway-Cのみ）

| | ├─プライベートCAインフラストラクチャのセットアップ

| | ├─組み合わせたEKU証明書を発行します

| | ├─ルートをすべてのピアに配布します

| | └─長期制御、Expressway-Eは除く

| |

| └─オプションD：ソフトウェアアップグレードの計画

|緊急├─必要な場合→ X15.4へのアップグレード（2026年2月）

| └─ Comprehensive solution → X15.5へのアップグレード（2026年5月）

| └─その後、個別のサーバ/クライアント証明書を取得します

よく寄せられる質問（FAQ）

一般的な質問

Q：プライベートPKIを使用する場合、この点について懸念する必要がありますか。

A：いいえ。このポリシーは、パブリックルートCAによって発行された証明書にのみ影響します

。プライベートPKIおよび自己署名証明書には影響しません。

Q: mTLS接続を使用しない場合はどうなりますか。

A：標準TLS（サーバ認証）のみを使用する場合は、このポリシーの影響を受けません。 サーバーのみの証明書は引き続き機能します。ただし、一部のユースケースはデフォルトでmTLSを使用するため、「影響を受ける特定のユースケース」セクションのリストに照らしてユースケースを確認します。

Q: Expresswayへの標準のHTTPS Web接続は機能しなくなりますか。

A：いいえ。標準TLS接続は影響を受けません。 ExpresswayへのWebブラウザアクセスは、サーバのみのEKU証明書でも正常に動作し続けます。

Q：既存の証明書を引き続き使用できますか。

A：はい。結合EKUを含む既存の証明書は、有効期限が切れるまで有効です。この問題は、更新が必要になったときに発生します。有効期限が切れるまで、TLS接続とmTLS接続の両方に対して機能します。

Q:mTLSまたは標準TLSのどちらを使用しているかを確認するには、どうすればよいのですか。

A:影響を受ける特定の使用の事例を確認してください。

Q.現在、何ができますか？

A：シスコでは、次の措置を即時に講じることを強く推奨します。

- 証明書の監査

  mTLSに使用されるパブリックTLS証明書の特定

- 証明書を早期に更新する

  有効期間を最大化するため、2026年3月15日前に更新

- 制御ACME自動化

  証明書が予期せず置き換えられる自動更新を無効にする

- CAとの調整

  一部のCAは、一時的または代替の証明書プロファイルを提供します

Q: CUCM SU3(a)は、X15.4およびX15.5と互換性がありますか。

A：はい

Q:Cisco Expressway EでクライアントEKUチェックを無効にすると（X15.5リリースで）、セキュリティの脆弱性が生じますか。

A：引き続き証明書でCN/SANをチェックし、接続ソースが有効であることを確認します。

Googleがセキュリティ上の問題を提起するまで、デフォルトで含まれているEKU検証（クライアントロール用の証明書）のみをバイパスします。そのため、以前と比較してセキュリティの問題が発生することはありません。

特定の暗号化

Q: ExpresswayでLet's Encrypt with ACMEを使用しています。どうしたらよいですか。

A：

1. 2026年2月11日より前に証明書を更新してください（可能な限り更新日に近い日付に更新してください）
2. 更新直後のACME自動スケジューラの無効化
3. 長期的なソリューションとしてX15.5へのアップグレードを計画

Q：結合されたEKU証明書の取得を続行するようにACMEプロファイルを変更できますか。

A：いいえ。現在、Expresswayではハードコードされた「クラシック」ACMEプロファイルが使用されていますが、ユーザはこれを変更できません。ACME証明書プロファイルのサポートについては、Cisco TACにお問い合わせください。

アップグレードの質問

Q: Expressway-EとExpressway-Cの両方をアップグレードする必要がありますか。

A：はい、そのとおりです。正常に動作させるには、両方を同じバージョン（X15.4またはX15.5）にアップグレードする必要があります。

Q: X15.4にアップグレードできますか、それともX15.5まで待つことができますか。

A：

- 緊急の問題がある場合、またはサーバ専用証明書をすぐに受け入れる必要がある場合は、X15.4にアップグレードします
- 可能であれば、デュアル証明書をサポートする包括的なソリューションのX15.5（2026年5月）を待ちます

Q：証明書の更新後にクラスタの複製が中断されます。何が起こったの？

A：新しい証明書のEKUはサーバ認証のみである可能性が高いですが、次の点が異なります。

- X15.4より前のバージョンでTLS検証を使用している場合=適用：クライアント認証EKUを使用しないと、クラスタピアはmTLS接続を確立できません
- ソリューションオプション（いずれか）:

  TLS検証モードを「Permissive」（安全性が低い）に設定する

  代替CAルートからの結合EKUを含む証明書の取得

  X15.4以降にアップグレードし、ClusterDBのクライアント認証EKU検証をバイパス

Q: X15.4にアップグレードした後、クラスタ内でサーバ専用証明書を使用してEnforcingモードを使用できますか。

A:はい。 X15.4以降、ExpresswayはmTLS ClusterDB接続のクライアント認証EKU検証をバイパスします。したがって、1つ以上のクラスターノードにサーバー認証EKUしかない場合でも、TLS検証を[強制]に設定できます。

Q: ExpresswayのWeb GUIから証明書をアップロードできないのはなぜですか。

A: X15.4より前のバージョンでは、Web GUIによって、証明書にクライアント認証EKUを含める必要がある、ハードコードされた検証が適用されます。証明書にサーバ認証EKUしかない場合は、次の2つのオプションがあります。

- SCP(Secure Copy Protocol)を使用して、証明書をサーバ（/persistent/Certsフォルダ）に直接アップロードします。
- X15.4以降にアップグレードします（Expressway-Eのみ）。これにより、この制限が排除されます

Q: X15.4へのアップグレード後も、サーバ専用証明書をExpressway-Eにアップロードできません

A:アップグレードが完了したら、次のコマンドが有効になっていることを確認してください

xConfiguration XCP TLS Certificate CVS EnableServerEkuUpload：オン

Q: X15.4にアップグレードしました。Expressway-EとExpressway-Cの両方でサーバ専用証明書をアップロードできますか。

A:いいえ。X15.4では、Expressway-Eのアップロード制限のみが削除されます。 Expressway-Cでは、Web GUIを使用してアップロードするために結合されたEKU証明書が引き続き必要です。これは、Expressway-CがUCトラバーサルゾーンでTLSクライアントとして機能することが多く、クライアント認証EKUを必要とするためです。 Expressway-Eでこのコマンドが実行されていることを確認します。このコマンドはExpressway-Cでは実行されません

xConfiguration XCP TLS Certificate CVS EnableServerEkuUpload：オン

Q：証明書の更新後にスマートライセンスを登録できません。これは、なぜですか。

A：証明書の更新後のスマートライセンスの失敗は、通常はEKUとは関係ありません。

- Expresswayがtools.cisco.com(CSSM)に到達できるかどうかを確認します。
- ファイアウォール規則でHTTPS送信（ポート443）が許可されていることを確認します。
- プロキシ設定が正しいかどうかを確認します（HTTPプロキシを使用している場合）
- CSSMサーバ証明書がExpressway信頼ストアで信頼されていることを確認します。
- Smart LicensingではclientAuthは必要ないため、このポリシー変更による影響はありません

MRA（モバイルおよびリモートアクセス）固有

Q: MRAでは、Expressway-E上でクライアント認証EKUが必要ですか。

A: Expresswayのバージョンによって異なります。

- X15.4より前：はい、間接的に必要

  MRA SIPシグナリング中、Expressway-Eは署名付き証明書をSIP SERVICEメッセージでExpressway-Cに送信します

  Expressway-Cが証明書を検証し、クライアント認証とサーバ認証の両方のEKUが必要です

  統合EKUがないと、MRA SIP登録が失敗します

- X15.4以降：いいえ

  Expressway-CはSIP SERVICEメッセージ内のクライアント認証EKUを検証しなくなりました

  Expressway-Eに必要なのは、MRA用のサーバ認証EKUだけです

  UCトラバーサルゾーンは単方向で動作する（Expressway-CはExpressway-Eサーバ証明書のみを検証）

Q：ネイバーゾーンがExpresswayx15.4のサーバ認証EKU

A: TLS検証モードを「on」に設定した場合、クライアント認証EKUが必要になります。 そのため、ネイバーゾーン設定でTLS検証を無効にすることができます

Q:MRAが正しく動作するには、どのような証明書が必要ですか。

A：一般的なMRA導入の場合：

コンポーネント	証明書の要件	EKUが必要です	注意事項
Expressway-E（X15.4より前）	サーバ認証+ clientAuth	両方	Exp-CによるSIP SERVICE検証の場合
Expressway-E(X15.4+)	serverAuthのみ	サーバのみ	クライアントEKUチェックがバイパスされました
Expressway-C	clientAuth +サーバ認証	両方	UCトラバーサルで常にクライアントとして動作
UCトラバーサルゾーン	単一方向の検証	Exp-E:serverAuth	Exp-CがExp-Eサーバ証明書を検証

		Exp-C:clientAuth	

Q:MRAは正常に動作していましたが、サーバのみのEKUでExpressway-E証明書を更新した後、SIP登録が失敗します。 何が問題でしょうか。

A: X15.4より前のバージョンを実行している場合、MRA SIPシグナリングでは、Expressway-EがSIP SERVICEメッセージにサーバ認証とクライアント認証のEKUを両方とも含める必要があります。オプション：

- EKUを組み合わせた証明書の取得
- 結合EKUを発行する代替CAルートに切り替えます
- Expressway-EとExpressway-Cの両方をX15.4以降にアップグレードする（推奨）

証明書の管理

Q:EKUを組み合わせた証明書をDigiCertまたはIdentrustから取得するにはどうすればよいですか。

A:CAプロバイダーに連絡して、結合EKUを引き続き発行する代替ルートの証明書を要求してください。

Q：使用しているCAで、サーバのみの証明書しか提供できないと言われています。どうしたらよいですか。

A：次のオプションがあります。

- 代替ルートの確認：複合EKUを発行する代替ルート(DigiCert Assured IDやIdentrust Public Sectorなど)があるかどうかをCAに確認します。
- スイッチCAプロバイダー：Chrome以外の信頼されたルートからの統合EKUを提供するCAを探す
- プライベートPKIの使用：組み合わされたEKU証明書の内部CAを設定します（Expressway-C導入のみ）。
- X15.4へのアップグレード：ServerAuth EKUのみの証明書に対応し、MRA登録を有効にする断続的なソリューション
- X15.5へのアップグレードが利用可能になったら：サーバのみの証明書が許容されるデュアル証明書アーキテクチャを計画し、グローバルなGoogle Chromeルートプログラムの要件を満たす包括的なソリューション

スケジュールに関する質問

Q:2026年6月15日はどうなりますか。

A: Chromeは、サーバとクライアントの両方の認証EKUを含むパブリックTLS証明書の信頼を停止します。このような証明書を使用するサービスは失敗する可能性があります。

Q：なぜ2026年3月15日より前に更新する必要があるのですか。

A:2026年3月15日以降、証明書の有効期間は398日から200日に短縮されます。この日付より前に更新すると、証明書の有効期間が最大になります。

Q：アクションの期限はいつですか？

A：複数の期限があります。

- 2026年2月11日：Let's Encryptが従来のACMEを介したEKUの結合を停止する
- 2026年3月15日：証明書の有効期間を200日に短縮
- 2026年5月：ほとんどのパブリックCAが複合EKUの発行を完全に停止
- 2026年6月：Chromeポリシーの完全適用

関連情報

シスコのドキュメント

- Field Notice FN74362：今後のTLS証明書の変更によるCisco Expresswayのセキュア通信への影響
- Cisco Bug ID CSCwr73373:Expressway用の個別のサーバおよびクライアント証明書のサポート

外部参照

- Chromeルートプログラムポリシー
- 暗号化しましょう： 2026年のTLSクライアント認証証明書サポートの終了
- CA/ブラウザフォーラムのベースライン要件

認証局のリソース

- DigiCertサポートポータル
- Identrust証明書サービス
- コミュニティフォーラムを暗号化しましょう
- Sectigoナレッジベース

結論

パブリックCA証明書でのクライアント認証EKUのサンセット設定は、mTLS接続を使用したCisco Expresswayの導入に影響を与える重要なセキュリティポリシーシフトを表します。これは業界全体に及ぶ変更ですが、Field Notice FN74362に従えばインパクトレーティングは非常に重要であり、サービスの中断を防ぐための迅速な対応が必要です。

重要なポイント

- これは、すべてのExpresswayバージョン（X15.4より前のX14およびX15）に影響します。
- Audit your certificates NOW：これは必須の最初のステップです
- 複数の回避策が利用可能 – 環境に最適な回避策を選択
- 長期的なソリューションのソフトウェアアップグレードが必要- X15.5の計画
- Expressway-EとExpressway-Cの両方を同時にアップグレードする必要がある
- 最も早い期限をユーザーに暗号化しましょう- 2026年2月11日

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。