Expressway für Client-Authentifizierung vorbereiten EKU Sunset in öffentlichen Zertifizierungsstellenzertifikaten

Inhalt

- Einleitung
- Backgroup-Informationen
- Problemdefinition
  - Änderung der Chrome-Stammprogrammrichtlinie
  - Wichtige Richtlinienanforderungen
  - Öffentliche Zertifizierungsstelle - Reaktionszeit
  - Zugehörige Cisco Dokumentation
- Auswirkungen auf die Expressway-Lösung
  - Betroffene Produkte
  - Doppelrolle des Expressway
- Spezifische Anwendungsfälle
- Empfehlungen
  - Aktuelle Zertifikate überwachen (ERSTER SCHRITT OBLIGATORISCH)
  - Kurzfristige Lösungen (vor Juni 2026)
  - Option 1: Wechseln zu öffentlichen Stammzertifizierungsstellen mit kombinierten EKU-Zertifikaten
  - Option 2: Verlängerung der aktuellen Zertifikate, um ihre Gültigkeit zu verlängern
    - Erneuerungsstrategie
    - Besondere Überlegungen fürLet'sEncrypt-Zertifikate
    - Aktionen zum Verschlüsseln von Benutzern
  - Option 3: Evaluierung und Migration zu alternativen Zertifizierungsstellenanbietern
    - Privater PKI-Ansatz
    - Langfristige Lösung (Software-Upgrades erforderlich)
    - Cisco Expressway X15.4 - Lösungsdetails (Februar 2026)
    - Cisco Expressway X15.5 - Lösungsdetails (Mai 2026)
- Entscheidungsablauf
- Häufig gestellte Fragen
  - Allgemeine Fragen
  - Verschlüsseln wir spezifische
  - Fragen zum Upgrade
  - MRA-spezifisch (Mobiler und Remote-Zugriff)
  - Zertifikatsverwaltung
  - Fragen zum Zeitplan
- Zusätzliche Ressourcen
  - Cisco Dokumentation
  - Externe Referenzen

Ressourcen der Zertifizierungsstelle

Schlussfolgerung

Wichtigste Punkte

Einleitung

In diesem Dokument werden Änderungen der Chrome-Stammprogrammrichtlinie für Cisco Expressway und die Clientauthentifizierungs-EKU nach dem 26. Juni in öffentlichen Zertifizierungsstellenzertifikaten beschrieben.

Backgroup-Informationen

Digitale Zertifikate sind von vertrauenswürdigen Zertifizierungsstellen (Certificate Authorities, CAs) ausgestellte elektronische Zertifikate, die die Kommunikation zwischen Servern und Clients durch die Gewährleistung von Authentifizierung, Datenintegrität und Vertraulichkeit schützen. Diese Zertifikate enthalten Extended Key Usage (EKU)-Felder, die ihren Zweck definieren:

- Serverauthentifizierungs-EKU (id-kp-serverAuth): Wird verwendet, wenn ein Server sein Zertifikat zum Identitätsnachweis vorlegt
- Clientauthentifizierungs-EKU (id-kp-clientAuth): Verwendung für gegenseitige TLS-Verbindungen (mTLS), bei denen sich beide Parteien gegenseitig authentifizieren

Bisher konnte ein einzelnes Zertifikat sowohl Server- als auch Clientauthentifizierungs-EKUs enthalten, sodass es für zwei Zwecke verwendet werden konnte. Dies ist besonders wichtig für Produkte wie Cisco Expressway, die in verschiedenen Verbindungsszenarien sowohl als Server als auch als Client fungieren.

Problemdefinition

Änderung der Chrome-Stammprogrammrichtlinie

Ab Juni 2026 schränkt die Chrome Root Program Policy die im Chrome Root Store enthaltenen Zertifikate der Root Certificate Authority (CA) ein, wobei die Mehrzweck-Roots schrittweise abgeschafft werden, um alle Public-Key Infrastructure (PKI)-Hierarchien so auszurichten, dass sie nur für Anwendungsfälle der TLS-Serverauthentifizierung verwendet werden.

Wichtige Richtlinienanforderungen

- Öffentliche Stammzertifizierungsstellen müssen nur die erweiterte Schlüsselverwendung (Extended Key Usage, EKU) für die Serverauthentifizierung (id-kp-serverAuth) geltend machen
- Zertifikate müssen NUR Serverauthentifizierungs-EKU enthalten, um die Vertrauenswürdigkeit vom Google Chrome-Browser aus aufrechtzuerhalten
- Das Einschließen von Clientauthentifizierungs-EKU in diese Zertifikate ist nicht zulässig.

- Stammzertifizierungsstellen, die weiterhin Zertifikate mit der Clientauthentifizierungs-EKU ausstellen, werden schließlich aus dem Chrome-Stammspeicher entfernt
- Keine gemischten Stammzertifizierungsstellen mehr für TLS-Zertifikate für öffentliche Server
- Durchsetzungszeitleiste: Juni 2026

Öffentliche Zertifizierungsstelle - Reaktionszeit

- Oktober 2025: Viele öffentliche Zertifizierungsstellen (DigiCert, Sectigo, SSL) begannen standardmäßig mit der Ausgabe von Zertifikaten nur für Server.
- 11. Februar 2026: Let's Encrypt stoppt die Ausstellung von Zertifikaten mit Client Authentication EKU unter Verwendung des klassischen ACME-Profils
- Mai 2026: Öffentliche Zertifizierungsstellen-Server stellen keine Client Authentication/EKU-Zertifizierungen mehr aus
- Juni 2026: Chrome Root-Programm-Richtlinie wird voll wirksam

---

Anmerkung: Diese Richtlinie gilt nur für Zertifikate, die von öffentlichen Zertifizierungsstellen ausgestellt wurden. Private PKI und selbstsignierte Zertifikate sind von dieser Richtlinie nicht betroffen.

Zugehörige Cisco Dokumentation

- Cisco Bug-ID: CSCwr73373- Unterstützung für separaten Server und Client-Zertifikat für Expressway
- Problemhinweis: FN74362
- Chrome-Root-Programmrichtlinie: Dokumentation der Chrome-Root-Programmrichtlinie

Auswirkungen auf die Expressway-Lösung

Betroffene Produkte

Gemäß Problemhinweis FN74362 sind alle Cisco Expressway-Versionen betroffen:

Produkt	Betroffene Versionen	Auswirkungen
Expressway Core und Edge	X14 (Alle Versionen)	X14.0.0 bis X14.3.7 - Alle Versionen betroffen
Expressway Core und Edge	X15 (Versionen vor X15.4)	X15.0.0 bis X15.3.2 - Alle Versionen betroffen

Doppelrolle des Expressway

Cisco Expressway-Produkte (Expressway-C und Expressway-E) fungieren in verschiedenen Verbindungsszenarien sowohl als Server als auch als Client und erfordern Zertifikate mit Server- und Client-Authentifizierungs-EKUs.

Expressway E als Server (Server-Authentifizierungs-EKU erforderlich):

- HTTPS-Browserzugriff
- SIP-UC-Traversal-Verbindungen
- WebEx Edge Audio/MRA-Konnektivität

Expressway E als Client (Client-Authentifizierungs-EKU erforderlich):

- B2B-Kommunikation
- MRA-Verbindungen (Mobile und Remote Access)
- XMPP-Federation
- SIP Neighbor Zone/CMS-Verbindungen
- Interaktionen mit externen Stellen
- Verbindung zur Cisco Cloud (MRA-Onboarding)

Spezifische Anwendungsfälle

Das von einer öffentlichen Zertifizierungsstelle signierte Zertifikat mit der Clientauthentifizierungs-EKU, das derzeit für mTLS-Verbindungen in Cisco Expressway verwendet wird, ist das Expressway Server Certificate. Dieses Zertifikat wird für die folgenden mTLS-Verbindungen verwendet:

1. SIP B2B-Anruf über mTLS - Expressway E wird abhängig vom sitzungsinitiierten Standort zu Client oder Server über mTLS-Verbindung
2. SIP-IMP-Federation über mTLS - Expressway E wird abhängig vom sitzungsinitiierten Standort zu Client oder Server auf mTLS-Verbindung
3. UC Traversal Zone - Expressway C präsentiert Client-Authentifizierung EKU
4. Traversal Zone mit mTLS-Konfiguration - Expressway C präsentiert Client-Authentifizierung EKU
5. SIP Neighbor Zone mit mTLS-Konfiguration - Expressway wird Client oder Server auf einer mTLS-Verbindung, abhängig vom durch eine Sitzung initiierten Standort, einschließlich Verbindungen mit:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Unity
- Cisco Unified Border Element (CUBE)
- Cisco Meeting Server (CMS)
- Verbindung zur Cisco Cloud - MRA-Onboarding (Expressway initiiert die Verbindung zur Cisco Cloud und präsentiert Client Authentication EKU)

Empfehlungen

Aktuelle Zertifikate überwachen (ERSTER SCHRITT OBLIGATORISCH)

Problemhinweis FN74362, bevor Workaround- und Lösungsoptionen in Betracht gezogen werden:

- Erstellen eines Inventars aller öffentlichen TLS-Zertifikate, um zu ermitteln, welche Zertifikate die Clientauthentifizierungs-EKU enthalten
- Sichern Sie Ihre Cisco Expressway-Instanz, oder kopieren Sie das signierte Zertifikat und den privaten Schlüssel manuell.
- Verwendung von Dokumentenzertifikaten: Ermitteln, welche Zertifikate für mTLS-Verbindungen verwendet werden
- CA- und Stamminformationen überprüfen: Dokumentieren Sie, welche Zertifizierungsstelle und welcher Stamm die einzelnen Zertifikate ausgestellt hat.
- Ablaufdatum überprüfen: Strategische Planung von Vertragsverlängerungen vor der Durchsetzung von Richtlinien

Kurzfristige Lösungen (vor Juni 2026)

Administratoren können aus einer der folgenden Workaround-Optionen wählen:

Option 1: Wechseln zu öffentlichen Stammzertifizierungsstellen mit kombinierten EKU-Zertifikaten

Einige Public Root-CAs (wie DigiCert und IdenTrust) stellen Zertifikate mit kombinierter EKU von einem alternativen Root aus aus aus, die nicht in den Chrome-Browser-Vertrauensspeicher aufgenommen werden können.

Beispiele für öffentliche Stammzertifizierungsstellen und EKU-Typen (gemäß FN74362):

CA-Anbieter	EKU-Typ	Stamm-CA	Issuing/Sub-CA
IdenTrust	clientAuth + serverAuth	IdenTrust Stammzertifizierungsstelle für den öffentlichen Sektor 1	IdenTrust Public Sector Server CA 1
DigiCert	clientAuth + serverAuth	DigiCert Assured ID Root G2	DigiCert Assured ID CA G2

Voraussetzungen für diesen Ansatz:

- Wenden Sie sich an Ihren Zertifizierungsstellenanbieter, um die Verfügbarkeit solcher Zertifikate zu überprüfen.
- Stellen Sie vor der Bereitstellung von Zertifikaten sicher, dass sowohl der Server, der

das Zertifikat präsentiert, als auch alle Clients, die es verwenden, der entsprechenden Stammzertifizierungsstelle vertrauen.
- Tauschen Stammzertifikatinformationen mit Kommunikations-Peers aus.
- Auf diese Weise können Software-Upgrades vermieden werden.

Verweise auf die Zertifikatsverwaltung:

- Cisco Expressway Certificate Creation and Use Deployment Guide (X14.0)
- Cisco Expressway Certificate Creation and Use Deployment Guide (X15.0)

Option 2: Verlängerung der aktuellen Zertifikate, um ihre Gültigkeit zu verlängern

Zertifikate, die von öffentlichen Stammzertifizierungsstellen vor Mai 2026 ausgestellt wurden und über eine EKU für die Server- und Clientauthentifizierung verfügen, werden bis zum Ablauf ihrer Laufzeit weiterhin anerkannt.

Erneuerungsstrategie

Allgemeine Empfehlungen:

- Erneuern Sie kombinierte EKU-Zertifikate, bevor die Richtlinie außer Kraft gesetzt wird.
- Beabsichtigen Sie, die Zertifikate vor dem 15. März 2026 zu verlängern, um ihre maximale Gültigkeit zu erreichen.
- Nach diesem Datum sind von öffentlichen Zertifizierungsstellen ausgestellte Zertifikate nur noch 200 Tage gültig.
- Cisco empfiehlt dringend, Ihre Zertifikate vor diesem Datum zu verlängern, wenn Sie diese Option nutzen möchten.
- Die Richtlinien für öffentliche Zertifizierungsstellen und die Implementierungsdaten können variieren.
- Einige öffentliche Zertifizierungsstellen haben die Ausstellung kombinierter EKU-Zertifikate gestoppt und können standardmäßig keines bereitstellen.
- Wenn Sie ein Zertifikat mit einer kombinierten EKU generieren möchten, arbeiten Sie mit Ihrer Zertifizierungsstelle zusammen, und verwenden Sie ein von öffentlichen Zertifizierungsstellen bereitgestelltes Sonderprofil.

Besondere Überlegungen für das Verschlüsseln von Zertifikaten

Gemäß FN74362, wenn Sie Zertifikate verschlüsseln:

- Expressway verwendet derzeit ein klassisches ACME-Profil, das fest codiert ist und von den Benutzern nicht geändert werden kann.
- Dieses klassische ACME-Profil wird derzeit zum Anfordern von Zertifikaten verwendet, die sowohl Server- als auch Client-Authentifizierungs-EKUs enthalten.
- Ab dem 11. Februar 2026 enthalten Zertifikatanforderungen, die dieses Profil verwenden, die Clientauthentifizierungs-EKU nicht mehr in Zertifikaten, die von Let's

Encrypt generiert wurden
- Weitere Informationen finden Sie unter Ending TLS Client Authentication Certificate Support in 2026 - Let's Encrypt

Aktionen zum Verschlüsseln von Benutzern

- Erneuern Sie Zertifikate vor dem 11. Februar 2026 - idealerweise so nahe wie möglich an diesem Datum, um die 90-tägige Gültigkeitsdauer zu maximieren.
- Deaktivieren Sie den automatischen ACME-Scheduler, um zu verhindern, dass Zertifikate nach dem 11. Februar 2026 automatisch erneuert werden.
- Dadurch wird verhindert, dass Zertifikate versehentlich mit Versionen überschrieben werden, die nur die Serverauthentifizierungs-EKU enthalten.
- Wenn Sie Ihren Vertrag nicht vor dem 11. Februar 2026 verlängern, wenden Sie sich an Cisco TAC, um Support zu erhalten.

Option 3: Evaluierung und Migration zu alternativen Zertifizierungsstellenanbietern

Diese Option gilt nur für: Expressway C; NICHT für Expressway E.

Privater PKI-Ansatz

- Bewertung der Machbarkeit eines Übergangs zu einer privaten PKI
- Richten Sie eine private Zertifizierungsstelle ein, um einzelne Zertifikate mit kombinierten EKUs (Server- und Clientzertifikate mit den erforderlichen EKUs) auszustellen.
- Wenn Sie ein privates CA-signiertes Zertifikat ausstellen, müssen Sie dem Peer Stammzertifikatinformationen zur Verfügung stellen.
- Bevor Sie ein Zertifikat ausstellen oder bereitstellen, stellen Sie sicher, dass sowohl der Server, der das Zertifikat präsentiert, als auch alle Clients, die es nutzen, der entsprechenden Stammzertifizierungsstelle vertrauen.
- Private CAs unterliegen nicht den Richtlinien des Chrome Root-Programms
- Bietet langfristige Kontrolle über Zertifikatrichtlinien

⚠ Vorsicht: Diese Option eignet sich nicht für Expressway-E, für das öffentliche Zertifizierungsstellenzertifikate für Dienste mit externer Ausrichtung und Browser-Vertrauensstellung erforderlich sind.

Langfristige Lösung (Software-Upgrades erforderlich)

Gemäß Problemhinweis FN74362 implementiert Cisco Produkterweiterungen in festen Versionen, um dieses Problem umfassend anzugehen.

Fester Veröffentlichungsplan:

Produkt	Betroffene Version	Feste Version	Zweck der Fehlerbehebung	Verfügbarkeit
Cisco Expressway	X14.x (Alle Versionen) X15.x (älter als X15.4)	X15,4	Intermittierende Lösung: Ermöglicht das zusätzliche Hochladen eines signierten ServerAuth EKU-Zertifikats auf den Expressway E und die Anpassung der Zertifikatsverifizierung für das MRA-SIP-Signal zwischen Expressway E und Expressway C	Februar 2026
Cisco Expressway	X14.x (Alle Versionen) X15.x (älter als X15.5)	X15,5	Umfassende Lösung: Bietet eine verbesserte Benutzeroberfläche zum Trennen von Client- und Serverzertifikaten und bietet Administratoren Optionen zum Deaktivieren der EKU-Prüfung	Mai 2026

Anmerkung: Sowohl Cisco Expressway E als auch Expressway C müssen auf dieselbe Version aktualisiert werden.

Cisco Expressway X15.4 - Lösungsdetails (Februar 2026)

Zweck: Intermittierende Lösung zur ausschließlichen Aufnahme von Zertifikaten mit ServerAuth EKU und zur Aktivierung von MRA-Registrierungen

Die wichtigsten Verbesserungen:

- Entfernt die Beschränkung für das Hochladen von Zertifikaten
- Ermöglicht Administratoren das Hochladen von Zertifikaten mit nur Server Authentication EKU über die Web-GUI auf Expressway E
- Früher hat Expressway nur Server-Zertifikate abgelehnt.
- Passt die Zertifikatsüberprüfung für MRA an
- Ändert die Zertifikatsverifizierung für die SIP-Signalisierung zwischen Expressway-E und Expressway-C in MRA-Lösungen
- Ermöglicht die Annahme von Zertifikaten nur für Server von Drittanbieteranwendungen

Upgrade auf X15.4 möglich:

- wenn Sie neue oder vorhandene Expressway-E für MRA mit rein serversignierten

Zertifikaten bereitstellen.
- Wenn Sie nach dem 11. Februar 2026 ACME-Zertifikate (Let's Encrypt) verwenden.
- Vorhandene Bereitstellungen, die signierte Zertifikate aktualisieren müssen, die nur die Serverauthentifizierungs-EKU enthalten.
- wenn bei mTLS-Verbindungen zertifikatbezogene Authentifizierungsprobleme auftreten.

Wichtige Anforderungen für X15.4:

- Sowohl Expressway-E als auch Expressway-C müssen auf X15.4 aktualisiert werden
- Planen Sie Upgrades während des Wartungsfensters, um Serviceunterbrechungen zu minimieren.

Einschränkungen von X15.4 sind:

- Hierbei handelt es sich um eine Lösung, die nur gelegentlich eingesetzt wird und unmittelbare Kompatibilitätsprobleme behebt.
- Bietet keine vollständige Unterstützung für zwei Zertifikate
- Keine Serviceparameter zum Deaktivieren der EKU-Prüfung enthalten
- mTLS-Verbindungen können je nach vom Sitzungsstandort initiiertem Standort fehlschlagen.

Cisco Expressway X15.5 - Lösungsdetails (Mai 2026)

Zweck: Umfassende Lösung zur Erfüllung der Anforderungen des globalen Google Chrome Root-Programms

Wichtigste Produktverbesserungen:

- Trennung von Client- und Serverzertifikaten
- Ermöglicht die Unterstützung von zwei separaten Zertifikaten auf derselben Schnittstelle.
- Expressway-Zertifikate mit separater EKU für die Serverauthentifizierung und EKU für die Clientauthentifizierung
- Erleichtert korrekte mTLS-Verbindungen mit separaten Zertifikatrollen
- Verbesserungen für Benutzeroberfläche und Backend
- Neue Zertifikats-Management-Schnittstellen für die individuelle Verwaltung beider Zertifikate
- EKU-Validierung für die Clientauthentifizierung während des Zertifikats-Uploads, um versehentliche MTLS-Verbindungsverluste zu vermeiden
- Administratoren können Server- und Client-Zertifikate separat hochladen und verwalten.
- Optionen zum Deaktivieren der EKU-Prüfung für die Clientauthentifizierung
- Serviceparameter, mit dem Administratoren die EKU-Prüfung für die Client-Authentifizierung entsprechend den individuellen Unternehmensanforderungen deaktivieren können
- Ermöglicht Cisco Expressway, die EKU vom Remote-Peer (Client) zu ignorieren, der eine Verbindung nur mit EKU-Zertifikaten für die Serverauthentifizierung anfordert.
- Wenn kein EKU-Zertifikat für die Clientauthentifizierung vorhanden ist, kann Expressway

das EKU-only-Zertifikat für die Serverauthentifizierung als Clientzertifikat (erneut) verwenden.

Anmerkung: In diesem Fall muss der Remote-Peer auch ein ähnliches EKU-Modell für die Ignore Client Authentication unterstützen.

Entscheidungsablauf

START: Verwenden Sie auf Expressway Zertifikate für öffentliche Zertifizierungsstellen?

│

├─ NEIN: Private PKI oder selbstsigniert

│ └─ Keine Aktion erforderlich - Nicht von Richtlinie betroffen

│

└─ JA: Verwendete öffentliche Zertifizierungsstellenzertifikate

  │

  ├─ Werden sie für mTLS-Verbindungen verwendet? (Anwendungsfälle im Abschnitt "Spezifische betroffene Anwendungsfälle" überprüfen)

  │ │

  │ ├─ NEIN: Nur Serverauthentifizierung

  │ │ └─ Minimale Auswirkungen - Überwachung auf zukünftige Änderungen

  │ │

  │ └─ JA: mTLS-Verbindungen mit Client Auth EKU

  │ │

  │ └─ Wählen Sie IHREN Ansatz:

  │ │

  │ ├─ Option A: Zu alternativer Root-CA wechseln

  │ │ ├─ CA-Anbieter für kombinierte EKU von alternativer Root kontaktieren

  │ │ ├─ Stellen Sie sicher, dass alle Peers dem neuen Root vertrauen

│ │ └─ Sofortiges Software-Upgrade nicht erforderlich

│ │

│ ├─ Option B: Verlängerung von Zertifikaten vor Ablauf der Frist

│ │ ├─ Wenn wir verschlüsseln: Verlängern Sie Ihren Vertrag vor dem 11. Februar 2026

│ │ │ └─ Deaktivieren Sie den ACME-Scheduler nach der Verlängerung.

│ │ ├─ Maximale Gültigkeit: Verlängern Sie Ihren Vertrag vor dem 15. März 2026

│ │ └─ Kaufzeit bis zum Ablauf des Zertifikats

│ │

│ ├─ Option C: Migration zu privater PKI (nur Expressway-C)

│ │ ├─ Einrichtung einer privaten Zertifizierungsstelleninfrastruktur

│ │ ├─ Gemeinsame EKU-Zertifikate ausstellen

│ │ ├─ Verteilen des Stammverzeichnisses an alle Peers

│ │ └─ Langzeitkontrolle, NICHT für Expressway-E

│ │

│ └─ Option D: Software-Upgrade planen

│ ├─ Dringender Bedarf? → Upgrade auf X15.4 (Februar 2026)

│ └─ Umfassende Lösung → Upgrade auf X15.5 (Mai 2026)

│ └─ Erhalten Sie dann separate Server-/Client-Zertifikate.

Häufig gestellte Fragen

Allgemeine Fragen

F: Muss ich mir darüber Gedanken machen, wenn ich eine private PKI verwende?

A : Nein. Diese Richtlinie wirkt sich nur auf Zertifikate aus, die von öffentlichen Stammzertifizierungsstellen ausgestellt wurden. Private PKI und selbstsignierte Zertifikate sind nicht betroffen.

F: Was geschieht, wenn ich keine mTLS-Verbindungen verwende?

A: Wenn Sie nur Standard-TLS (Serverauthentifizierung) verwenden, sind Sie von dieser Richtlinie

nicht betroffen. Ihre Serverzertifikate funktionieren weiterhin. Überprüfen Sie Ihre Anwendungsfälle jedoch anhand der Liste im Abschnitt "Spezifische betroffene Anwendungsfälle", da einige der Anwendungsfälle standardmäßig mTLS verwenden.

F: Funktionieren meine HTTPS-Standardwebverbindungen zu Expressway nicht mehr?

Antwort: Nein. Standard-TLS-Verbindungen sind davon nicht betroffen. Der Webbrowserzugriff auf Expressway funktioniert auch mit rein serverbasierten EKU-Zertifikaten normal.

F: Kann ich meine vorhandenen Zertifikate weiterhin verwenden?

A : Ja, vorhandene Zertifikate mit kombinierter EKU bleiben bis zu ihrem Ablauf gültig. Das Problem tritt auf, wenn eine Verlängerung erforderlich ist. Sie funktionieren sowohl für TLS- als auch für mTLS-Verbindungen bis zum Ablauf.

F: Woher weiß ich, ob ich mTLS oder Standard-TLS verwende?

A : Abschnitt "Spezifische Fälle betroffener Verwendung".

F. Was kann ich jetzt tun?

A: Cisco empfiehlt dringend folgende Sofortmaßnahmen:

- Prüfung Ihrer Zertifikate

  Identifizieren der für mTLS verwendeten öffentlichen TLS-Zertifikate

- Frühzeitige Verlängerung von Zertifikaten

  Verlängern Sie Ihren Vertrag vor dem 15. März 2026, um Ihre Gültigkeit zu maximieren.

- ACME-Automatisierung steuern

  Deaktivieren Sie automatische Verlängerungen, die unerwartet Zertifikate ersetzen können.

- Koordination mit Ihrem CA

  Einige Zertifizierungsstellen bieten temporäre oder alternative Zertifikatprofile.

F: Ist CUCM SU3(a) kompatibel mit X15.4 und X15.5

A : Ja

F: Besteht eine Sicherheitslücke beim Deaktivieren der Client EKU-Prüfung in Cisco Expressway E (mit X15.5-Version)?

A: Das Zertifikat überprüft noch CN/SAN, um zu überprüfen, ob die Verbindungsquelle gültig ist, nur die EKU-Validierung umgehen (Zertifikat für den Zweck der Client-Rolle), die standardmäßig enthalten war, bis Google Sicherheitsbedenken aufwirft, daher darf kein Sicherheitsproblem im Vergleich zu früher vorliegen.

Verschlüsseln wir spezifische

F: Ich verwende Let's Encrypt with ACME auf Expressway. Was kann ich tun?

A :

1. Erneuern Sie Ihr Zertifikat vor dem 11. Februar 2026 (so bald wie möglich)
2. Deaktivieren Sie den automatischen ACME-Scheduler unmittelbar nach der Verlängerung.
3. Planen eines Upgrades auf X15.5 für eine langfristige Lösung

F: Kann ich das ACME-Profil ändern, um weiterhin kombinierte EKU-Zertifikate zu erhalten?

A : Nein. Aktuell verwendet Expressway ein fest codiertes "klassisches" ACME-Profil, das von Benutzern nicht geändert werden kann. Wenden Sie sich an das Cisco TAC, um Unterstützung für ACME-Zertifikatprofile zu erhalten.

Fragen zum Upgrade

F: Muss ich sowohl Expressway-E als auch Expressway-C aktualisieren?

A : Ja, absolut. Für den ordnungsgemäßen Betrieb müssen beide auf dieselbe Version (X15.4 oder X15.5) aktualisiert werden.

F: Kann ich ein Upgrade auf X15.4 durchführen oder auf X15.5 warten?

A :

- Upgrade auf X15.4, wenn Sie dringende Probleme haben oder jetzt nur Server-Zertifikate akzeptieren müssen
- Warten Sie nach Möglichkeit auf X15.5 (Mai 2026) für die umfassende Lösung mit Unterstützung für zwei Zertifikate.

F: Meine Clusterreplikation ist nach der Zertifikatverlängerung unterbrochen. Was ist passiert?

A: Wahrscheinlich hat Ihr neues Zertifikat nur die EKU für die Serverauthentifizierung, aber:

- Bei einer Version vor X15.4 mit TLS Verify = Durchsetzen: Cluster-Peers können keine mTLS-Verbindungen ohne Clientauthentifizierungs-EKU herstellen.
- Lösungsoptionen (eine oder mehrere):

  TLS-Überprüfungsmodus auf "Permissive" (weniger sicher) setzen

  Abrufen von Zertifikaten mit kombinierter EKU vom alternativen Zertifizierungsstellen-Root

  Upgrade auf X15.4 oder höher unter Umgehung der Client Auth EKU-Verifizierung für ClusterDB

F: Kann ich nach dem Upgrade auf X15.4 den Erzwingungsmodus mit rein serverbasierten Zertifikaten in meinem Cluster verwenden?

A: Ja. Ab X15.4 umgeht Expressway die Client Auth EKU-Verifizierung für mTLS ClusterDB-Verbindungen. Daher kann die TLS-Überprüfung auf "Erzwingen" gesetzt werden, auch wenn ein oder mehrere Clusterknoten nur über die Server-Auth-EKU verfügen.

F: Warum kann ich mein Zertifikat nicht über die Expressway-Web-GUI hochladen?

A: Vor X15.4 erzwingt die Web-GUI eine hartcodierte Validierung, für die Zertifikate mit Clientauthentifizierungs-EKU erforderlich sind. Wenn Ihr Zertifikat nur über die Serverauthentifizierungs-EKU verfügt, haben Sie zwei Möglichkeiten:

- Verwenden Sie SCP (Secure Copy Protocol), um das Zertifikat direkt auf den Server hochzuladen (/persistente/Zertifikate).
- Upgrade auf X15.4 oder höher (nur Expressway-E), wodurch diese Einschränkung aufgehoben wird

F: Nach dem Upgrade auf X15.4 kann ich immer noch keine Server-Only-Zertifikate auf Expressway-E hochladen

A: Stellen Sie nach dem Upgrade sicher, dass dieser Befehl aktiviert ist.

xConfiguration XCP TLS-Zertifikat CVS EnableServerEkuUpload: On

F: Ich habe ein Upgrade auf X15.4 durchgeführt. Kann ich jetzt auf Expressway-E und Expressway-C nur Server-Zertifikate hochladen?

A: Nein. X15.4 beseitigt nur die Upload-Einschränkung für Expressway-E. Expressway-C benötigt weiterhin kombinierte EKU-Zertifikate für den Upload über die Web-GUI. Dies liegt daran, dass Expressway-C häufig als TLS-Client in UC-Überbrückungszonen fungiert und Clientauthentifizierungs-EKU erfordert. Stellen Sie sicher, dass Sie diesen Befehl auf Expressway-E ausführen. Dieser Befehl wird auf Expressway-C nicht ausgeführt.

xConfiguration XCP TLS-Zertifikat CVS EnableServerEkuUpload: On

F: Ich kann die Smart License nach der Erneuerung des Zertifikats nicht registrieren. Warum ist das so?

A : Fehler bei der Smart Licensing-Lizenz nach der Zertifikatverlängerung hat normalerweise KEINEN Bezug zu EKU:

- Überprüfen Sie, ob Expressway tools.cisco.com (CSSM) erreichen kann.
- Überprüfung, ob Firewall-Regeln ausgehenden HTTPS-Verkehr zulassen (Port 443)
- Überprüfen Sie, ob die Proxykonfiguration korrekt ist (bei Verwendung des HTTP-Proxys).
- Überprüfen, ob das CSSM-Serverzertifikat im Expressway-Vertrauensspeicher vertrauenswürdig ist
- Die Smart Licensing-Funktion erfordert keine ClientAuth, daher wirkt sich diese Richtlinienänderung nicht darauf aus.

MRA-spezifisch (Mobiler und Remote-Zugriff)

F: Ist für MRA eine Clientauthentifizierungs-EKU auf Expressway-E erforderlich?

A: Das hängt von der Expressway-Version ab:

- Vor x15.4: Ja, indirekt erforderlich

  Während der MRA-SIP-Signalisierung sendet Expressway-E sein signiertes Zertifikat in einer SIP SERVICE-Nachricht an Expressway-C

  Expressway-C validiert das Zertifikat und erfordert EKUs für Client-Authentifizierung und Serverauthentifizierung.

  Ohne kombinierte EKU schlägt die MRA-SIP-Registrierung fehl

- X15.4 und höher: Nein

  Expressway-C validiert Client Authentication EKU nicht mehr in der SIP SERVICE-Nachricht

  Expressway-E benötigt nur Server Authentication EKU für MRA

  UC Traversal Zone arbeitet unidirektional (Expressway-C validiert nur Expressway-E-Serverzertifikat)

F: Warum meine Nachbarzonen nach dem Hochladen desServer-Authentifizierungs-EKU für ExpressBayX15.4

A : Wenn Sie den TLS-Verifizierungsmodus auf "on" (Ein) setzen, ist eine Clientauthentifizierungs-EKU erforderlich. Sie können die TLS-Verifizierung daher in der Konfiguration der Nachbarzone deaktivieren.

F: Welche Zertifikate werden benötigt, damit MRA ordnungsgemäß funktioniert?

A : Für eine typische MRA-Bereitstellung:

Komponente	Zertifikatanforderungen	EKU erforderlich	Hinweise
Expressway-E (vor X15.4)	ServerAuth + ClientAuth	Beide	Zur SIP-SERVICE-Validierung durch Exp-C
Expressway-E (X15.4+)	Nur ServerAuth	Nur Server	Client-EKU-Prüfung umgangen
Schnellstraße C	clientAuth + serverAuth	Beide	Fungiert immer als Client bei UC-Traversal

UC-Überbrückungszone	Unidirektionale Validierung	Exp-E: serverAuth Exp-C: clientAuth	Exp-C validiert Exp-E-Serverzertifikat

F: Mein MRA funktionierte einwandfrei, aber nachdem ich mein Expressway-E-Zertifikat mit nur einer Server-EKU erneuert hatte, schlägt die SIP-Registrierung fehl.

A: Wenn Sie eine Version vor X15.4 ausführen, benötigt die MRA-SIP-Signalisierung Expressway-E, um Server- und Client-Authentifizierungs-EKUs in der SIP SERVICE-Nachricht anzuzeigen. Ihre Optionen:

- Erhalten Sie ein Zertifikat mit kombinierter EKU
- Wechseln Sie zu einem alternativen Zertifizierungsstellen-Root, der die kombinierte EKU ausgibt
- Upgrade von Expressway-E und Expressway-C auf X15.4 oder höher (empfohlen)

Zertifikatsverwaltung

F: Wie erhalte ich ein Zertifikat mit kombinierter EKU von DigiCert oder IdenTrust?

A : Wenden Sie sich an Ihren Zertifizierungsstellenanbieter, und fordern Sie ein Zertifikat vom alternativen Stammverzeichnis an, das noch immer die kombinierte EKU ausstellt.

F: Meine Zertifizierungsstelle gibt an, dass sie nur Serverzertifikate bereitstellen kann. Was kann ich tun?

A : Sie haben mehrere Möglichkeiten:

- Auf alternative Wurzeln prüfen: Fragen Sie Ihre Zertifizierungsstelle, ob sie alternative Wurzeln haben, die eine kombinierte EKU auslösen (wie DigiCert Assured ID oder IdenTrust Public Sector).
- Switch-CA-Anbieter: Suchen Sie nach CAs, die kombinierte EKU von nicht-Chrome-vertrauenswürdigen Wurzeln anbieten.
- Private PKI verwenden: Einrichten einer internen Zertifizierungsstelle für kombinierte EKU-Zertifikate (nur Expressway-C-Bereitstellungen)
- Upgrade auf X15.4: Intermittierende Lösung zur Aufnahme von Zertifikaten nur mit ServerAuth EKU und zur Aktivierung von MRA-Registrierungen
- Upgrade auf X15.5, sobald verfügbar: Planen Sie eine Architektur mit zwei Zertifikaten, in der nur Server-Zertifikate zulässig sind, und eine umfassende Lösung, um die Anforderungen des globalen Google Chrome-Root-Programms zu erfüllen.

Fragen zum Zeitplan

F: Was passiert am 15. Juni 2026?

A : Chrome beendet das Vertrauen in öffentliche TLS-Zertifikate, die sowohl Server- als auch Clientauthentifizierungs-EKUs enthalten. Dienste, die solche Zertifikate verwenden, können fehlschlagen.

F: Warum muss ich die Lizenz vor dem 15. März 2026 verlängern?

A : Nach dem 15. März 2026 verkürzt sich die Gültigkeitsdauer der Zertifikate von 398 auf 200 Tage. Wenn Sie das Zertifikat vor diesem Datum verlängern, haben Sie die maximale Lebensdauer.

Frage: Bis zu welchem Termin müssen Maßnahmen ergriffen werden?

A : Es gibt mehrere Fristen:

- 11. Februar 2026: Let's Encrypt stoppt kombinierte EKU über klassischen ACME
- 15. März 2026: Die Gültigkeit des Zertifikats wird auf 200 Tage reduziert.
- Mai 2026: Die meisten öffentlichen Zertifizierungsstellen geben kombinierte EKU nicht mehr vollständig aus.
- Juni 2026: Chrome-Richtlinie vollständig durchgesetzt

Zusätzliche Ressourcen

Cisco Dokumentation

- Problemhinweis FN74362: Auswirkungen von Cisco Expressway auf die sichere Kommunikation aufgrund bevorstehender Änderungen an TLS-Zertifikaten
- Cisco Bug-ID CSCwr73373: Unterstützung für separaten Server und Client Zertifikat für Expressway

Externe Referenzen

- Richtlinie für Chrome-Stammprogramm
- Verschlüsseln wir: Unterstützung für TLS-Clientauthentifizierungszertifikate wird 2026 beendet
- Grundlegende Anforderungen für CA/Browser-Forum

Ressourcen der Zertifizierungsstelle

- DigiCert-Support-Portal
- IdenTrust-Zertifikatdienste
- Verschlüsseln wir das Community-Forum
- Sectigo Wissensdatenbank

Schlussfolgerung

Die Einstellung der EKU für die Client-Authentifizierung in öffentlichen Zertifizierungsstellenzertifikaten stellt eine erhebliche Änderung der Sicherheitsrichtlinien dar, die sich auf Cisco Expressway-Bereitstellungen mit mTLS-Verbindungen auswirkt. Obwohl es sich hierbei um eine branchenweite Änderung handelt, ist die Auswirkungsbewertung ENTSCHEIDEND (CRITICAL) nach der Problembeschreibung FN74362, und es sind sofortige Maßnahmen erforderlich, um Serviceunterbrechungen zu vermeiden.

Wichtigste Punkte

- Dies betrifft ALLE Expressway-Versionen (X14 und X15 vor X15.4)
- Auditieren Sie Ihre Zertifikate JETZT - Dies ist der obligatorische erste Schritt.
- Es stehen mehrere Workarounds zur Verfügung - Wählen Sie die für Ihre Umgebung am besten geeignete Lösung.
- Software-Upgrades sind für langfristige Lösung erforderlich - Planung für X15.5
- Sowohl Expressway-E als auch Expressway-C müssen gemeinsam aufgerüstet werden
- Let's Encrypt-Benutzer haben die früheste Frist - 11. Februar 2026

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.