Expressway voorbereiden voor Client Auth EKU-zonsondergang in openbare CA-certificaten

Inhoud

Inleiding

Dit document beschrijft wijzigingen in het Chrome-hoofdprogrammabeleid voor Cisco Expressway en EKU-clientverificatie in openbare CA-certificaten na 6/26.

achtergrondgroepinformatie

Digitale certificaten zijn elektronische referenties die worden uitgegeven door vertrouwde certificeringsinstanties (CA's) die de communicatie tussen servers en clients beveiligen door authenticatie, gegevensintegriteit en vertrouwelijkheid te waarborgen. Deze certificaten bevatten EKU-velden (Extended Key Usage) die hun doel definiëren:

- Server Authentication EKU (id-kp-serverAuth): Gebruikt wanneer een server zijn certificaat presenteert om zijn identiteit te bewijzen
- Client Authentication EKU (id-kp-clientAuth): Gebruikt in wederzijdse TLS (mTLS) verbindingen waar beide partijen elkaar authenticeren

Traditioneel kan een enkel certificaat zowel server- als clientverificatie-EKU's bevatten, waardoor het voor twee doeleinden kan worden gebruikt. Dit is vooral belangrijk voor producten zoals Cisco Expressway die zowel als server als client fungeren in verschillende verbindingsscenario's.

probleemdefinitie

Wijziging van het rootprogramma van Chrome

Met ingang van juni 2026 beperkt het Chrome Root Program Policy Root Certificate Authority (CA) -certificaten die zijn opgenomen in de Chrome Root Store, waardoor multifunctionele roots worden uitgefaseerd om alle public-key infrastructure (PKI) -hiërarchieën uit te lijnen om alleen TLS-serverauthenticatie te gebruiken.

Belangrijkste beleidsvereisten

- Public Root CA's moeten EKU (Extended Key Usage) ALLEEN voor serververificatie (id-kp-serverAuth) bevestigen
- Certificaten moeten ALLEEN Server Authentication EKU bevatten om het vertrouwen van de Google Chrome-browser te behouden
- Het opnemen van Client Authentication EKU in deze certificaten is verboden
- Root-CA's die certificaten blijven uitgeven met Client Authentication EKU worden uiteindelijk verwijderd uit de Chrome Root Store
- Geen root-CA's voor gemengd gebruik meer voor TLS-certificaten voor openbare servers
- Tijdschema voor handhaving: juni 2026

Openbare CA-responstijdlijn

- Oktober 2025: Veel publieke CA's (DigiCert, Sectigo, SSL) zijn standaard begonnen met het uitgeven van alleen-servercertificaten
- 11 februari 2026: Let's Encrypt stopt met het uitgeven van certificaten met Client Authentication EKU met behulp van het klassieke ACME-profiel
- Mei 2026: Openbare CA-servers geven geen EKU-certificeringen voor clientverificatie meer uit
- Juni 2026: Chrome Root Program Policy wordt volledig effectief

---

Opmerking: dit beleid is alleen van toepassing op certificaten die zijn uitgegeven door openbare CA's. Particuliere PKI en zelf ondertekende certificaten worden niet beïnvloed door dit beleid.

Gerelateerde Cisco-documentatie

- Cisco bug ID: CSCwr73373- Ondersteuning voor afzonderlijke server- en clientcertificaat voor Expressway
- Bericht ter plaatse: FN74362
- Hoofdprogrammabeleid van Chrome: Hoofdprogrammabeleidsdocumentatie van Chrome

Hoe het de Expressway-oplossing beïnvloedt

Betrokken producten

Volgens Field Notice FN74362 worden alle Cisco Expressway-versies beïnvloed:

Product	Betrokken vrijkomingen	Impact
Expressway Core en Edge	X14 (alle versies)	X14.0.0 tot en met X14.3.7 - Alle releases worden beïnvloed
Expressway Core en Edge	X15 (versies vóór X15.4)	X15.0.0 tot en met X15.3.2 - Alle releases worden beïnvloed

Dubbele rol van de snelweg

Cisco Expressway-producten (Expressway-C en Expressway-E) fungeren zowel als server als

client in verschillende verbindingsscenario's, waarbij certificaten met zowel server- als clientverificatie-EKU's vereist zijn.

Expressway E als server (serververificatie EKU vereist):

- HTTPS-browsertoegang
- SIP UC-traversale verbindingen
- Webex Edge Audio/MRA-connectiviteit

Expressway E als client (clientverificatie EKU vereist):

- B2B-communicatie
- MRA-verbindingen (Mobile en Remote Access)
- XMPP-federatie
- SIP Neighbor Zone/CMS-verbindingen
- Interacties met externe entiteiten
- Verbinding met Cisco Cloud (MRA Onboarding)

Specifieke getroffen gebruiksgevallen

Het Public CA-signed certificaat met Client Authentication EKU dat momenteel wordt gebruikt voor mTLS-verbindingen in Cisco Expressway is het Expressway Server-certificaat. Dit certificaat wordt gebruikt voor de volgende mTLS-verbindingen:

1. SIP B2B-aanroep via mTLS - Expressway E wordt client of server op mTLS-verbinding, afhankelijk van de site die met de sessie is gestart
2. SIP IMP Federation over mTLS - Expressway E wordt client of server op mTLS-verbinding, afhankelijk van de site die met de sessie is gestart
3. UC Traversal Zone - Expressway C presenteert Client Authentication EKU
4. Traversal Zone met mTLS-configuratie - Expressway C presenteert Client Authentication EKU
5. SIP Neighbor Zone met mTLS-configuratie - Expressway wordt client of server met mTLS-verbinding, afhankelijk van de site die met de sessie is gestart, inclusief verbindingen met:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Unity
- Cisco Unified Border Element (CUBE)
- Cisco Meeting Server (CMS)
- Verbinding met Cisco Cloud - MRA Onboarding (Expressway initieert de verbinding met Cisco Cloud en presenteert Client Authentication EKU)

Aanbevelingen

Controle van lopende certificaten (VERPLICHTE EERSTE STAP)

Per Field Notice FN74362, alvorens workaround- en oplossingsopties te overwegen:

- Maak een inventarisatie van alle openbare TLS-certificaten om te bepalen welke certificaten de Client Authentication EKU bevatten
- Maak een back-up van uw Cisco Expressway-exemplaar of kopieer het ondertekende certificaat en de privésleutel handmatig
- Gebruik van documentcertificaat: identificeren welke certificaten worden gebruikt voor mTLS-verbindingen
- CA- en root-informatie verifiëren: documenteren welke CA en root elk certificaat hebben uitgegeven
- Vervaldatums controleren: Plan verlengingen strategisch vóór beleidshandhaving

Kortetermijnoplossingen (vóór juni 2026)

Beheerders kunnen kiezen uit een van de volgende opties:

Optie 1: Switch naar Public Root CA's die gecombineerde EKU-certificaten leveren

Sommige Public Root CA's (zoals DigiCert en IdenTrust) geven certificaten uit met gecombineerde EKU van een alternatieve root, die niet kan worden opgenomen in de Chrome-browservertrouwenswinkel.

Voorbeelden van Public Root CA's en EKU-typen (volgens FN74362):

CA-leverancier	EKU-type	Root CA	Uitgevende instantie/subinstantie
IdenTrust	clientAuth + serverAuth	IDenTrust-basisoplossing voor de publieke sector CA 1	IDenTrust Public Sector Server CA 1
DigiCert	clientAuth + serverAuth	DigiCert Assured ID Root G2	DigiCert verzekerde ID CA G2

Voorwaarden voor deze aanpak:

- Coördineer met uw CA-provider om de beschikbaarheid van dergelijke certificaten te controleren.
- Voordat u certificaten implementeert, moet u ervoor zorgen dat zowel de server die het certificaat presenteert als alle clients die het certificaat gebruiken, vertrouwen op de corresponderende basiscertificeringsinstantie.
- Informatie over basiscertificaten uitwisselen met communicatieve peers.
- Met deze aanpak wordt voorkomen dat software-upgrades onmiddellijk nodig zijn.

Referenties certificaatbeheer:

- Gids voor het maken en gebruiken van Cisco Expressway-certificaten (X14.0)
- Gids voor het maken en gebruiken van Cisco Expressway-certificaten (X15.0)

Optie 2: Huidige certificaten verlengen om hun geldigheid te verlengen

Certificaten die vóór mei 2026 zijn uitgegeven door Public Root CA's en die zowel server- als clientverificatie-EKU hebben, worden nog steeds gehonoreerd totdat hun termijn afloopt.

vernieuwingsstrategie

Algemene aanbevelingen zijn:

- Gecombineerde EKU-certificaten vernieuwen voordat het beleid wordt gewijzigd
- Voor de maximale geldigheid van het certificaat, plan om certificaten te vernieuwen vóór 15 maart 2026.
- Na deze datum zijn openbare CA-uitgegeven certificaten slechts 200 dagen geldig.
- Cisco raadt u ten zeerste aan om uw certificaten vóór deze datum te verlengen als u deze optie wilt volgen.
- Het beleid en de implementatiedata van openbare CA's kunnen variëren.
- Sommige publieke CA's zijn gestopt met het uitgeven van gecombineerde EKU-certificaten en kunnen er standaard geen verstrekken.
- Om een certificaat te genereren met een gecombineerde EKU, werkt u samen met uw CA-autoriteit en gebruikt u een speciaal profiel dat wordt verstrekt door openbare CA's.

Speciale overwegingen voor Let's Encrypt-certificaten

Per FN74362, als u Let's Encrypt-certificaten gebruikt:

- Momenteel gebruikt Expressway een klassiek ACME-profiel dat hardcoded is en niet door gebruikers kan worden gewijzigd
- Dit klassieke ACME-profiel wordt momenteel gebruikt voor het aanvragen van certificaten die zowel server- als clientverificatie-EKU's bevatten
- Vanaf 11 februari 2026 nemen certificaataanvragen met dit profiel de Client Authentication EKU niet langer op in certificaten die door Let's Encrypt zijn gegenereerd
- Zie Ondersteuning voor TLS-clientverificatiecertificaten beëindigen in 2026 - Laten we coderen voor meer informatie

Actie-items voor het coderen van gebruikers

- Verleng certificaten vóór 11 februari 2026 - idealiter zo dicht mogelijk bij deze datum om de geldigheidsduur van 90 dagen te maximaliseren.
- Schakel de automatische planning van de ACME uit om te voorkomen dat certificaten na 11 februari 2026 automatisch worden verlengd.
- Deze actie helpt te voorkomen dat certificaten per ongeluk worden overschreven met versies die alleen de serververificatie EKU bevatten.
- Als u niet voor 11 februari 2026 verlengt, neem dan contact op met Cisco TAC voor ondersteuning.

Optie 3: Evalueren en migreren naar alternatieve CA-providers

Deze optie is alleen van toepassing op: Expressway C; NIET van toepassing op Expressway E.

Private PKI-benadering

- Evalueer de haalbaarheid van de overgang naar private PKI
- Een eigen CA instellen voor het uitgeven van afzonderlijke certificaten met gecombineerde EKU (server- en clientcertificaten met de vereiste EKU's)
- Bij het uitgeven van een privé CA-ondertekend certificaat, moet u rootcertificaatinformatie delen met de peer.
- Voordat u een certificaat afgeeft of implementeert, moet u ervoor zorgen dat zowel de server die het certificaat presenteert als alle clients die het certificaat gebruiken, vertrouwen op de corresponderende basiscertificeringsinstantie.
- Particuliere CA's zijn niet onderworpen aan het hoofdprogrammabeleid van Chrome
- Biedt langetermijncontrole over certificaatbeleid

⚠ Let op: deze optie is niet haalbaar voor Expressway-E, waarvoor openbare CA-certificaten vereist zijn voor externe services en browservertrouwen.

Oplossing voor de lange termijn (software-upgrades vereist)

Volgens Field Notice FN74362 implementeert Cisco productverbeteringen in vaste releases om dit probleem volledig aan te pakken.

Vaste releaseschema:

Product	Betrokken release	vaste afgifte	Doel van Fix	Beschikbaarheid
Cisco Expressway	X14.x (alle versies) X15.x (eerder dan X15.4)	X15,4	Intermitterende oplossing: maakt extra upload mogelijk van ServerAuth EKU-certificaat op Expressway E en aanpassing van certificaatverificatie voor MRA SIP-signaal tussen Expressway E en Expressway C	februari 2026
Cisco Expressway	X14.x (alle versies) X15.x (eerder dan X15.5)	X15,5	Uitgebreide oplossing: biedt UI-verbetering voor het scheiden van client- en servercertificaten en biedt beheerders opties om EKU-controle uit te schakelen	mei 2026

Opmerking: zowel Cisco Expressway E als Expressway C moeten worden bijgewerkt naar dezelfde versie.

Cisco Expressway X15.4-oplossing — Gegevens (februari 2026)

Doel: Intermitterende oplossing voor certificaten met alleen ServerAuth EKU en voor MRA-registraties

Belangrijke verbeteringen zijn:

- Verwijdert beperking voor het uploaden van certificaten
- Hiermee kunnen beheerders certificaten uploaden met alleen Server Authentication EKU via Web GUI op Expressway E
- Eerder verwierp Expressway alleen certificaten voor servers
- Aanpassing certificaatverificatie voor MRA
- Wijzigt certificaatverificatie voor SIP-signalering tussen Expressway-E en Expressway-C in MRA-oplossingen
- Biedt acceptatie van alleen-servercertificaten van toepassingen van derden

Wie kan upgraden naar X15.4:

- als u nieuwe Expressway-E implementeert of bestaande Expressway-E opnieuw implementeert voor MRA met alleen door de server ondertekende certificaten.
- Als u ACME (Let's Encrypt)-certificaten gebruikt na 11 februari 2026.
- Bestaande implementaties waarvoor ondertekende certificaten moeten worden bijgewerkt die alleen serververificatie-EKU bevatten.
- als u problemen ondervindt met certificaatgerelateerde verificatie in mTLS-verbindingen

Belangrijke vereisten voor X15.4:

- Zowel de Expressway-E als de Expressway-C moeten worden bijgewerkt naar X15.4
- Upgrade plannen tijdens onderhoudsfase om onderbreking van de service tot een minimum te beperken

Beperkingen van X15.4 zijn:

- Dit is een intermitterende oplossing die onmiddellijke compatibiliteitsproblemen aanpakt
- Biedt geen volledige ondersteuning voor dubbele certificaten
- Bevat geen serviceparameter om EKU-controle uit te schakelen
- mTLS-verbindingen kunnen mislukken, afhankelijk van de site die met de sessie is gestart

Details Cisco Expressway X15.5-oplossing (mei 2026)

Doel: Uitgebreide oplossing om te voldoen aan de wereldwijde vereisten van het Google Chrome Root Program

Belangrijkste productverbeteringen:

- Segregatie van client- en servercertificaten
- Biedt ondersteuning voor twee afzonderlijke certificaten op dezelfde interface
- Expressway-certificaten met aparte serververificatie EKU en clientverificatie EKU
- Vergemakkelijkt de juiste mTLS-verbindingen met gescheiden certificaatrollen
- UI- en backend-verbeteringen
- Nieuwe interfaces voor certificaatbeheer voor individueel beheer van beide certificaten
- Client Authentication EKU-validatie tijdens het uploaden van het certificaat om te voorkomen dat de MTLS-verbinding per ongeluk vervalt
- Beheerders kunnen server- en clientcertificaten afzonderlijk uploaden en beheren
- Opties voor het uitschakelen van Client Authentication EKU Check
- Serviceparameters waarmee beheerders de EKU-controle voor clientverificatie kunnen uitschakelen op basis van individuele bedrijfsvereisten
- Hiermee kan Cisco Expressway EKU negeren van de externe peer (client) die een verbinding aanvraagt met alleen EKU-certificaten voor serververificatie
- Bij afwezigheid van een Client Authentication EKU certificaat, staat Expressway toe om het Server Authentication EKU-only certificaat te (her)gebruiken als een Client certificaat

---

Opmerking: In dit geval moet de externe peer ook een vergelijkbaar Ignore Client Authentication EKU-model ondersteunen

---

beslissingsboom

Start: Gebruikt u openbare CA-certificaten op Expressway?

│

├: Privé-PKI of zelfondertekend

│ └Geen actie vereist - Niet beïnvloed door beleid

│

└ YES: Openbare CA-certificaten in gebruik

  │

  ├Worden ze gebruikt voor mTLS-verbindingen? (Zie de sectie Use Cases in Specific Affected Use Cases)

  │ │

  │ ├NEE: Alleen serververificatie

│ │ └ Minimale impact - Monitor voor toekomstige veranderingen

│ │

│ └: mTLS-verbindingen met Client Auth EKU

│ │

│ └ KIES UW AANPAK:

│ │

│ ├ Optie A: Switch naar alternatieve basiscertificeringsinstantie

│ │├Neem contact op met CA-provider voor gecombineerde EKU van alternatieve root

│ │├ Zorg ervoor dat alle peers nieuwe root vertrouwen

│ │ └Geen onmiddellijke software-upgrade nodig

│ │

│ ├ optie B: certificaten vóór de uiterste termijnen vernieuwen

│ │ ├Als laten we versleutelen: Vernieuwen voor 11 februari 2026

│ │ │ └ ^ Schakel ACME-planner uit na verlenging

│ │├Voor maximale geldigheid: Verleng vóór 15 mrt 2026

│ │ └ Koopt tijd tot vervaldatum certificaat

│ │

│ ├ optie C: Migreren naar privé-PKI (alleen Expressway-C)

│ │├Een particuliere CA-infrastructuur opzetten

│ │ ├Geef gecombineerde EKU-certificaten af

│ │├Distribueer root naar alle peers

│ │ └, NIET voor Expressway-E

│ │

│ └ optie D: Software-upgrade plannen

│ ├? Dringende noodzaak? → Upgrade naar X15.4 (februari 2026)

│ └ Comprehensive solution → Upgrade naar X15.5 (mei 2026)

│ └, verkrijg vervolgens afzonderlijke server-/clientcertificaten

Veelgestelde vragen (FAQ)

Algemene vragen

V: Moet ik me hier zorgen over maken als ik privé-PKI gebruik?

A: Nee. Dit beleid is alleen van invloed op certificaten die zijn uitgegeven door Public Root CA's. Particuliere PKI en zelf ondertekende certificaten worden niet beïnvloed.

V: Wat als ik geen mTLS-verbindingen gebruik?

A: Als u alleen standaard TLS (serververificatie) gebruikt, wordt dit beleid niet van toepassing op u. Certificaten die alleen op de server worden gebruikt, blijven werken. Controleer uw use cases echter aan de hand van de lijst in het gedeelte Specifieke getroffen gebruiksgevallen, omdat in sommige gevallen standaard mTLS wordt gebruikt.

V: Werkt mijn standaard HTTPS-webverbinding met Expressway niet meer?

A: Nee. Standaard TLS-verbindingen worden niet beïnvloed. De toegang tot Expressway via de webbrowser blijft normaal werken, zelfs met EKU-certificaten die alleen voor servers zijn bedoeld.

V: Kan ik mijn bestaande certificaten blijven gebruiken?

A: Ja, bestaande certificaten met gecombineerde EKU blijven geldig totdat ze verlopen. Het probleem doet zich voor wanneer u moet vernieuwen. Ze werken voor zowel TLS- als mTLS-verbindingen tot het verstrijken.

V: Hoe weet ik of ik mTLS of standaard TLS gebruik?

A: Specifieke casesectie betreffende gebruik bekijken.

Q: Wat kan ik nu doen?

A: Cisco beveelt deze onmiddellijke acties ten zeerste aan:

- Controle van uw certificaten

  Openbare TLS-certificaten identificeren die voor mTLS worden gebruikt

- Certificaten vroegtijdig vernieuwen

  Verlengen voor 15 maart 2026 om de geldigheid te maximaliseren

- ACME-automatisering beheren

  Geautomatiseerde vernieuwingen uitschakelen die certificaten onverwacht kunnen vervangen

- Coördineren met je CA

  Sommige CA's bieden tijdelijke of alternatieve certificaatprofielen

V: Is CUCM SU3(a) compatibel met X15.4 en X15.5

A: Ja

V: Is er een beveiligingsprobleem met het uitschakelen van Client EKU-controle in Cisco Expressway E (met X15.5-release)?

A: Certificaat controleert nog steeds de CN/SAN om te controleren of de verbindingsbron geldig is, omzeilt alleen de EKU-validatie (certificaat voor clientroldoeleinden) die standaard is opgenomen totdat Google beveiligingsproblemen opwerpt, en mag daarom geen beveiligingsproblemen hebben in vergelijking met voorheen.

Laten we specifiek versleutelen

V: Ik gebruik Let's Encrypt met ACME op Expressway. Wat kan ik doen?

A :

1. Vernieuw je certificaat voor 11 februari 2026 (zo dicht mogelijk bij die datum)
2. Schakel de automatische ACME-planner onmiddellijk na verlenging uit
3. Upgrade naar X15.5 voor langetermijnoplossing

V: Kan ik het ACME-profiel wijzigen om gecombineerde EKU-certificaten te blijven ontvangen?

A: Nee. Momenteel gebruikt Expressway een hardcoded "klassiek" ACME-profiel dat niet door gebruikers kan worden gewijzigd. Neem contact op met Cisco TAC voor ondersteuning van het ACME-certificaatprofiel.

Upgradevragen

V: Moet ik zowel de Expressway-E als de Expressway-C upgraden?

A: Ja, absoluut. Beide moeten worden bijgewerkt naar dezelfde versie (X15.4 of X15.5) voor een goede werking.

V: kan ik upgraden naar X15.4 of wachten op X15.5?

A :

- Upgrade naar X15.4 als u dringende problemen hebt of als u nu alleen-servercertificaten wilt accepteren
- Wacht indien mogelijk op X15.5 (mei 2026) voor de uitgebreide oplossing met ondersteuning voor dubbele certificaten

V: Mijn clusterreplicatie is verbroken na verlenging van het certificaat. Wat is er gebeurd?

A: Hoogstwaarschijnlijk heeft uw nieuwe certificaat alleen serververificatie EKU, maar:

- Als op versie vóór X15.4 met TLS Verify = Afdwingen: clusterpeers kunnen geen mTLS-verbindingen maken zonder Client Authentication EKU
- Oplossingsopties (beide):

  TLS-verificatiemodus instellen op "Toegestaan" (minder veilig)

  Certificaten verkrijgen met gecombineerde EKU van alternatieve CA-hoofdmap

  Upgrade naar X15.4 of hoger, waardoor verificatie van Client Auth EKU voor ClusterDB wordt omzeild

V: Kan ik na een upgrade naar X15.4 de afdwingingsmodus gebruiken met alleen-servercertificaten in mijn cluster?

A: Ja. Vanaf X15.4 omzeilt Expressway de verificatie van Client Auth EKU voor mTLS ClusterDB-verbindingen. Daarom kan TLS Verify worden ingesteld op "Afdwingen", zelfs als een of meer clusternodes alleen Server Auth EKU hebben.

V: Waarom kan ik mijn certificaat niet uploaden via de Expressway Web GUI?

A: Vóór X15.4, de Web GUI handhaaft een hardcoded validatie die certificaten vereist om Client Authentication EKU hebben. Als uw certificaat alleen Server Authentication EKU heeft, hebt u twee opties:

- Gebruik SCP (Secure Copy Protocol) om het certificaat rechtstreeks naar de server te uploaden (map/persistent/Certs)
- Upgrade naar X15.4 of hoger (alleen Expressway-E), waardoor deze beperking wordt verwijderd

V: Na een upgrade naar X15.4 kan ik nog steeds geen certificaten voor alleen servers uploaden naar Expressway-E

A: Controleer of deze opdracht is ingeschakeld nadat u een upgrade hebt uitgevoerd

xConfiguration XCP TLS Certificate CVS EnableServerEkuUpload: On

V: Ik heb een upgrade uitgevoerd naar X15.4. Kan ik nu alleen-servercertificaten uploaden op zowel Expressway-E als Expressway-C?

A: Nee. X15.4 verwijdert alleen de uploadbeperking voor Expressway-E. Expressway-C vereist nog steeds gecombineerde EKU-certificaten voor uploaden via Web GUI. Dit komt omdat Expressway-C vaak fungeert als een TLS-client in UC Traversal Zones en vereist Client Authentication EKU. Zorg ervoor dat u deze opdracht uitvoert op Expressway-E. Deze opdracht wordt niet uitgevoerd op Expressway-C

xConfiguration XCP TLS Certificate CVS EnableServerEkuUpload: On

V: Ik kan Smart License niet registreren na verlenging van het certificaat. Waarom?

A: Slimme licentiestoring na certificaatvernieuwing is meestal NIET gerelateerd aan EKU:

- Controleer of Expressway tools.cisco.com (CSSM) kan bereiken
- Controleren of firewallregels HTTPS-uitgaand verkeer toestaan (poort 443)
- Controleer of de proxyconfiguratie correct is (bij gebruik van HTTP-proxy)
- Controleren of het CSSM-servercertificaat vertrouwd is in het Expressway-vertrouwensarchief
- Voor Smart Licensing is geen clientAuth vereist, dus deze beleidswijziging heeft geen invloed

MRA (Mobile and Remote Access) Specific

V: Vereist MRA Client Authentication EKU op Expressway-E?

A: Het hangt af van de Expressway-versie:

- Vóór X15.4: Ja, indirect vereist

  Tijdens MRA SIP-signalering verzendt Expressway-E zijn ondertekende certificaat in een SIP SERVICE-bericht naar Expressway-C

  Expressway-C valideert het certificaat en vereist zowel Client Authentication als Server Authentication EKU's

  Zonder gecombineerde EKU mislukt MRA SIP-registratie

- X15.4 en hoger: Nee

  Expressway-C valideert Client Authentication EKU niet langer in het SIP SERVICE-bericht

  Expressway-E heeft alleen Server Authentication EKU nodig voor MRA

  UC Traversal Zone werkt unidirectioneel (Expressway-C valideert alleen Expressway-E-servercertificaat)

V: Waarom mijn buurzones falen na het uploaden van deSerververificatie EKU op Expresswayx15.4

A: Als u de TLS-verificatiemodus instelt op "aan", moet u een EKU voor clientverificatie hebben. U kunt de TLS-verificatie uitschakelen in de configuratie van de buurzone

V: Welke certificaten zijn nodig om MRA goed te laten werken?

A: Voor een typische MRA-implementatie:

component	Certificaatvereisten	EKU vereist	Opmerkingen
Expressway-E (vóór	serverAuth +	Beide	Voor SIP SERVICE-validatie

X15.4)	clientAuth		door Exp-C
Expressway-E (X15.4+)	Alleen serverAuth	Alleen server	Client-EKU-controle overgeslagen
snelweg-C	clientAuth + serverAuth	Beide	Altijd als klant optreden in UC Traversal
UC-dwarszone	Unidirectionele validatie	Exp-E: serverAuth Exp-C: clientAuth	Exp-C valideert Exp-E-servercert

Vraag: Mijn MRA werkte prima, maar na het vernieuwen van mijn Expressway-E-certificaat met EKU alleen voor servers, mislukt de SIP-registratie. Wat is er mis?

A: Als u een versie vóór X15.4 uitvoert, vereist MRA SIP-signalering dat Expressway-E zowel server- als clientverificatie-EKU's in het SIP-SERVICEbericht moet weergeven. Uw opties:

- Verkrijgen van een certificaat met gecombineerde EKU
- Switch naar een alternatieve CA-hoofdmap die gecombineerde EKU's uitgeeft
- Upgrade zowel Expressway-E als Expressway-C naar X15.4 of hoger (aanbevolen)

certificaatbeheer

V: Hoe krijg ik een certificaat met gecombineerde EKU van DigiCert of IdenTrust?

A: Neem contact op met uw CA-provider en vraag een certificaat aan bij hun alternatieve root die nog steeds gecombineerde EKU's uitgeeft.

V: Mijn CA zegt dat ze alleen certificaten voor servers kunnen leveren. Wat kan ik doen?

A: Je hebt verschillende opties:

- Vraag uw CA of ze alternatieve roots hebben die gecombineerde EKU uitgeven (zoals DigiCert Assured ID of IdenTrust Public Sector)
- Switch CA-providers: zoek naar CA's die gecombineerde EKU aanbieden van niet-Chrome-vertrouwde roots
- Private PKI gebruiken: interne CA instellen voor gecombineerde EKU-certificaten (alleen Expressway-C-implementaties)
- Upgrade naar X15.4: Intermitterende oplossing voor certificaten met alleen ServerAuth EKU en MRA-registraties
- Upgrade naar X15.5 zodra deze beschikbaar is: plan voor architectuur met twee certificaten waarbij alleen servercertificaten acceptabel zijn en uitgebreide oplossing om te voldoen aan

de wereldwijde vereisten van het Google Chrome Root Program

Tijdlijnvragen

V: Wat gebeurt er op 15 juni 2026?

A: Chrome stopt met het vertrouwen op openbare TLS-certificaten die zowel Server- als Client Authentication EKU's bevatten. Diensten die dergelijke certificaten gebruiken, kunnen mislukken.

V: Waarom moet ik voor 15 maart 2026 vernieuwen?

A: Na 15 maart 2026 wordt de geldigheid van het certificaat teruggebracht van 398 dagen naar 200 dagen. Verlenging vóór deze datum geeft u een maximale levensduur van het certificaat.

V: Wat is de deadline voor actie?

A: Er zijn meerdere deadlines:

- 11 februari 2026: Let's Encrypt stopt gecombineerde EKU via klassieke ACME
- 15 maart 2026: Geldigheid certificaat teruggebracht tot 200 dagen
- Mei 2026: De meeste openbare CA's stoppen volledig met de uitgifte van gecombineerde EKU
- Juni 2026: Chrome-beleid volledig gehandhaafd

Aanvullende bronnen

Cisco-documentatie

- FN74362: Cisco Expressway Impact op beveiligde communicatie vanwege aankomende wijzigingen in TLS-certificaten
- Cisco bug ID CSCwr73373: Ondersteuning voor afzonderlijke server- en clientcertificaat voor Expressway

Externe verwijzingen

- Chrome Root Program-beleid
- Let's Encrypt: ondersteuning voor TLS-clientverificatiecertificaten beëindigen in 2026
- Basisvereisten CA/Browser Forum

Middelen van de certificaatautoriteit

- DigiCert-ondersteuningsportaal
- IDenTrust-certificaatservices
- Laten we het communityforum versleutelen
- Sectigo Knowledge Base

Conclusie

De onderinstelling van Client Authentication EKU in openbare CA-certificaten vertegenwoordigt een belangrijke verschuiving in het beveiligingsbeleid die van invloed is op Cisco Expressway-implementaties met behulp van mTLS-verbindingen. Hoewel dit een verandering in de hele sector is, is de impactbeoordeling KRITIEK volgens Field Notice FN74362, en onmiddellijke actie is vereist om onderbrekingen van de service te voorkomen.

Belangrijkste afhaalrestaurants

- Dit is van invloed op ALLE Expressway-versies (X14 en X15 vóór X15.4)
- Controleer uw certificaten NU - Dit is de verplichte eerste stap
- Meerdere oplossingen zijn beschikbaar - Kies de beste oplossing voor uw omgeving
- Software-upgrades zijn vereist voor langetermijnoplossingen - Plan voor X15.5
- Zowel Expressway-E als Expressway-C moeten samen worden opgewaardeerd
- Let's Encrypt-gebruikers hebben de vroegste deadline - 11 februari 2026

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.