BLUEBITS
The Level Of Trust

GlobalSign OVmTLS

Chứng chỉ số chuyên dụng cho cơ chế xác thực hai chiều/xác thực máy khách

Định danh tin cậy cho hệ thống tài chính, ngân hàng và doanh nghiệp

Chính sách Chrome Root Program thay đổi gì ?

Từ ngày **27/07/2026**, các chứng thư SSL/TLS công khai trên Google Chrome chỉ còn được tin cậy với:

- Server Authentication
- Client Authentication

Nếu không tuân thủ tách chức năng Client Authentication khỏi Web PKI, chứng thư sẽ không còn được trình duyệt Chrome tin cậy.

Google muốn:

Giảm phạm vi rủi ro:
1 root CA chỉ được trust cho một mục đích (Server authen), một địa điểm (trình duyệt)

Browser không chịu trách nhiệm:
Enteprise PKI – các kết nối API, workload, IoT... là việc nội bộ của doanh nghiệp

Browser không kiểm soát được rủi ro của DN:
Google không nên là bên tin cậy để doanh nghiệp tham chiếu

Nguyên tắc đặc quyền tối thiểu:
Một certificate chỉ nên có đúng chức năng nó cần.

Ý nghĩa: Google không quy định mTLS certificate nào chạy trên Google Chrome. Google quy định chứng chỉ muốn chạy được trên Google Chrome không được mang tính năng mTLS

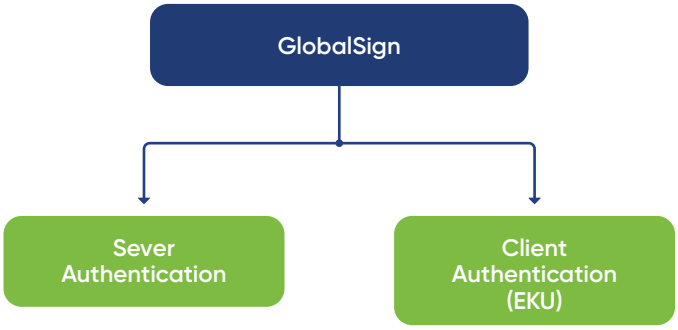
TÁC ĐỘNG VỚI CHỨNG CHỈ HIỆN TẠI

KHÔNG CÓ THAY ĐỔI

Các chứng chỉ đang sử dụng ở dạng GlobalSign Root R3:

- Tiếp tục hoạt động bình thường
- Tiếp tục có hiệu lực cho đến hết thời hạn
- Nếu có Client Authentication EKU thì tính năng này không bị ảnh hưởng

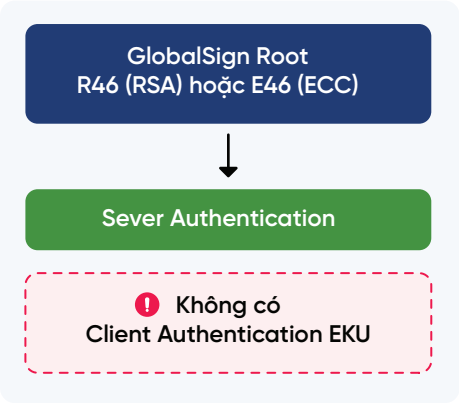
HIỆN NAY



Không cần thay đổi hay cấp lại chứng chỉ trước khi hết hạn.

KHI GIA HẠN CHỨNG CHỈ (MẶC ĐỊNH)

Sau ngày **27/07/2026**, khi chứng chỉ được gia hạn hoặc cấp mới theo quy trình thông thường:



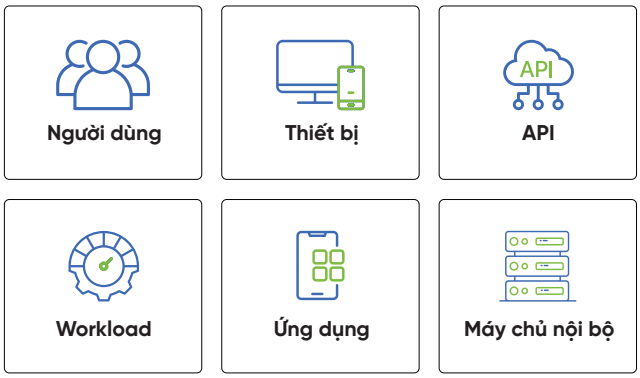
Các chứng chỉ này:

- Phù hợp cho Website HTTPS thông thường
- Không còn hỗ trợ Client Authentication EKU
- Không thể sử dụng cho các hệ thống yêu cầu mTLS hoặc xác thực máy khách

GlobalSign có phải pháp nếu hệ thống tiếp tục cần Client Authentication

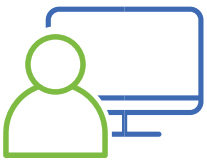
GLOBALSIGN OVmTLS

GlobalSign OVmTLS là một PKI chuyên dùng nhằm đáp ứng định hướng của Chính sách của chương trình Chrome Root. Khác với các chứng chỉ SSL/TLS công khai, GlobalSign OVmTLS tập trung vào việc xây dựng định danh số cho:



Các chứng chỉ này không hướng tới mục tiêu xác thực Website HTTPS trên Internet mà phục vụ các môi trường doanh nghiệp và hệ thống nội bộ.

VÌ SAO LỰA CHỌN GLOBALSIGN OVmTLS?



Chuyên biệt cho Client Authentication

Được thiết kế để phục vụ xác thực người dùng, thiết bị và ứng dụng thay vì Website công cộng.

Phân tách môi trường quản trị

Cho phép doanh nghiệp quản lý riêng hệ thống chứng chỉ phục vụ mTLS và hệ thống chứng chỉ Website.

Sẵn sàng cho Zero Trust

Đáp ứng nhu cầu định danh số cho Machine Identity trong các mô hình bảo mật hiện đại.

Đồng hành cùng xu hướng Web PKI

Phù hợp với định hướng loại bỏ Client Authentication khỏi các chứng chỉ SSL/TLS công khai.

SO SÁNH NHANH

Tiêu chí	SSL/TLS Public	GlobalSign R3 for mTLS
Website HTTPS	✓	Không khuyến nghị
Client Authentication	! (Theo lộ trình mới)	✓
Mutual TLS	!	✓
Device Identity	!	✓
API Authentication	✓ Giới hạn	✓
Zero Trust	Hạn chế	✓

VỀ BLUEBITS

Bluebits là đối tác Golden Partner của GlobalSign tại Việt Nam với hơn 18 năm kinh nghiệm triển khai các giải pháp PKI và Certificate Lifecycle Management.

CHÚNG TÔI CUNG CẤP

- Tư vấn kiến trúc PKI
- Tư vấn triển khai mTLS
- Cấp phát chứng chỉ GlobalSign OVmTLS
- Tích hợp với hệ thống hiện hữu
- Triển khai Certificate Lifecycle Management (CLM)
- Hỗ trợ vận hành và đào tạo

LIÊN HỆ TƯ VẤN

bluebits@bluebit.vn
www.bluebit.vn