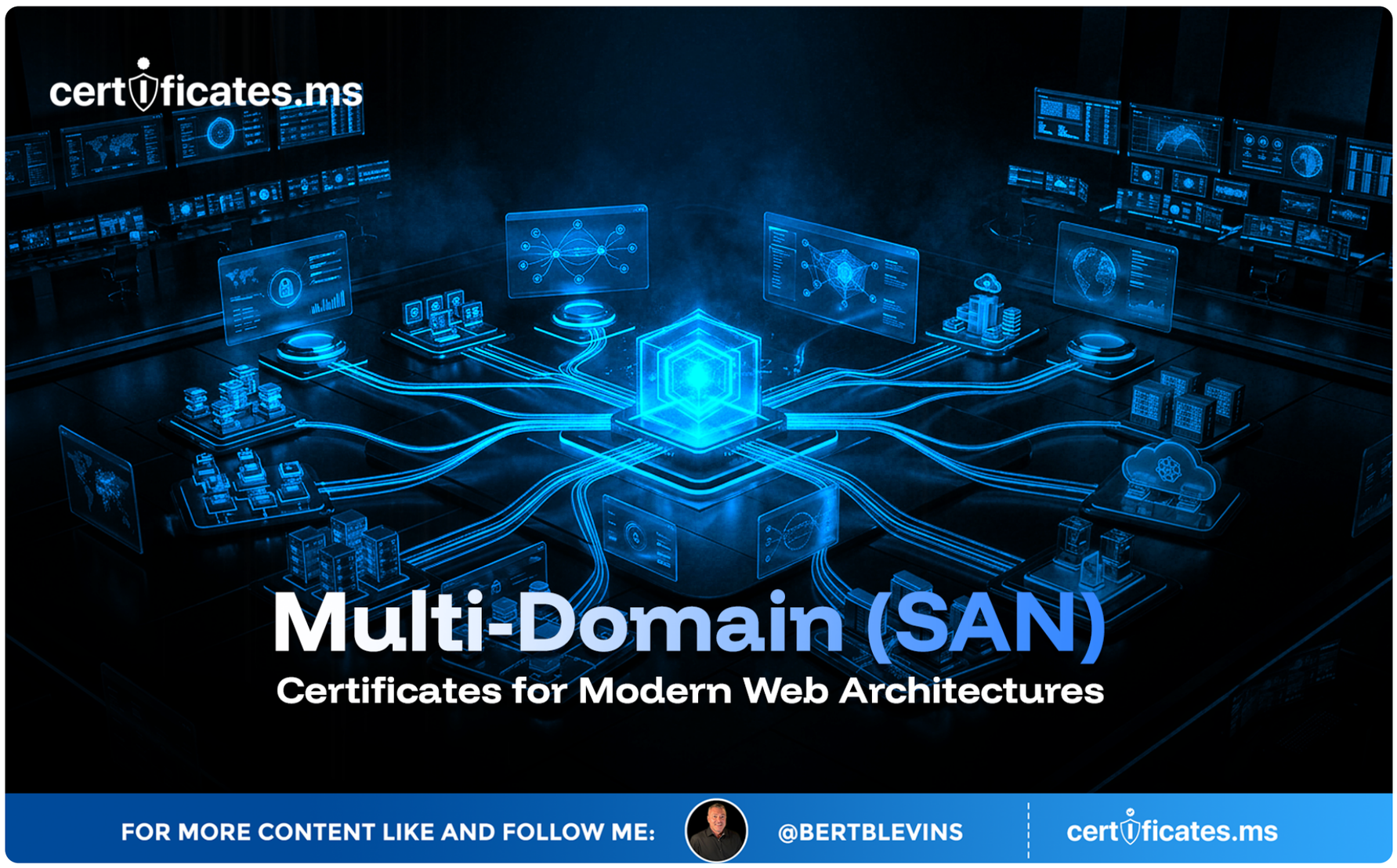
Multi-Domain (SAN) Certificates for Modern Web Architectures



Modern applications rarely live on a single domain anymore. A typical product might span a main website, a separate API domain, a customer portal, and several regional or brand variations, each needing certificate coverage. Multi-domain certificates, built around the Subject Alternative Name extension, exist specifically to handle this reality cleanly. This article covers how they work and where they fit into modern web architecture.

What a SAN Certificate Actually Does

A Subject Alternative Name certificate, commonly called a SAN or multi-domain certificate, lists multiple distinct hostnames within a single certificate, each one independently validated during issuance. Unlike a wildcard, which covers an entire pattern of subdomains under one parent domain, a SAN certificate explicitly names each specific hostname it covers, which can span entirely different domains, not just subdomains of the same root, giving it considerably more flexibility for organizations managing a diverse portfolio of properties.

Why Modern Architectures Favor This Approach

Contemporary web architectures frequently separate concerns across multiple domains for legitimate technical and organizational reasons: a dedicated API domain separate from the main site, distinct domains per brand or regional market, and separate domains for content delivery versus the primary application. Managing a separate certificate for each of these domains individually multiplies the number of renewal events an operations team has to track. A single SAN certificate covering the full set consolidates that management overhead into one certificate, one renewal schedule, and one installation point, while still validating each domain independently rather than relying on a wildcard pattern that might not fit the actual domain structure.

Practical Limits Worth Knowing

Most CAs impose a maximum number of Subject Alternative Names permitted on a single certificate, commonly in the range of one hundred, though this varies by CA and certificate product. Every domain listed still needs to pass its own validation during issuance, meaning adding a new domain to an existing SAN certificate typically requires reissuing the entire certificate with the updated domain list, rather than simply appending to an existing one without any further validation. Organizations managing certificates with many SAN entries also need robust processes for tracking exactly which domains are covered, since a certificate with dozens of hostnames can become difficult to reason about without good documentation and tooling.

SAN Certificates and Load Balanced, Multi-Region Deployments

Multi-domain certificates pair naturally with load-balanced architectures spanning multiple regions or cloud providers, since the same certificate, and the same private key, can be deployed consistently across every region's load balancer, provided the underlying key material is distributed and protected securely across all of them. This consolidation simplifies operations for globally distributed applications considerably, though it reintroduces the same concentrated-risk consideration that applies to wildcard certificates: a single compromised key now affects every domain and every region relying on it.

Choosing Between SAN, Wildcard, and Single-Domain Certificates

The right choice depends on the actual domain structure being protected. A predictable, single-level subdomain pattern under one parent domain often fits a wildcard well. A diverse set of specific, named domains, potentially spanning multiple root domains entirely, fits a SAN certificate better. A single, isolated, high-risk domain may still be best served by its own dedicated certificate, kept entirely separate from anything else, so a compromise anywhere else in the organization's certificate estate cannot affect it.

SAN Certificates for AI Product Suites

Organizations offering a suite of AI-powered products, often spanning a marketing site, a dedicated API domain for developers, a customer-facing application domain, and sometimes a separate domain for AI agent or webhook callbacks, are a natural fit for SAN certificates, consolidating what could otherwise be four or five separately managed certificates into one coordinated renewal process, provided the security posture and risk tolerance across those domains is genuinely comparable enough to justify sharing a single certificate and key.

The Countdown Is Already Running: 200 Days, 100 Days, 47 Days

Every certificate conversation in 2026 eventually arrives at the same clock, and it is worth closing on it here. The CA/Browser Forum's Ballot SC-081v3 is not a proposal under discussion; it is an approved, already-in-motion schedule. Maximum public TLS certificate lifetimes fall from 398 days to 200 days on March 15, 2026. They fall again to 100 days on March 15, 2027. By March 15, 2029, they drop to just 47 days, with domain validation itself needing to be re-proven roughly every 10 days.

01

Translate that into operational terms and the picture gets stark quickly. An organization currently renewing certificates a few times a year will be handling renewal events on the order of every couple of weeks by the end of this countdown, across every endpoint it operates. Manual tracking, calendar reminders, and a spreadsheet somebody checks once a month will not survive contact with that cadence. What has always been an occasional chore is becoming a continuous, automated operation, whether an organization plans for it or not.

02

Multi-domain certificates carry the same public lifetime rules as any other certificate below, and because a single SAN certificate often anchors several parts of a modern architecture at once, keeping its renewal fully automated becomes increasingly important as that renewal window shrinks toward 47 days.

03

The 200-day, 100-day, and 47-day milestones are not distant hypotheticals; the first has already arrived. Organizations that build the automation loop now, generating keys, vaulting them securely, brokering issuance across Certificate Authorities through APIs, and rebinding certificates to live endpoints without manual intervention, will meet each deadline without disruption. Organizations that wait will be rebuilding their certificate operations under deadline pressure, with far less room for error and far less time to get it right. The countdown is the call to action. The only real decision left is whether to automate on your own schedule, or on the CA/Browser Forum's.