CSC

The SSL Landscape

Certificate management insights for navigating a pivotal transformation

Summary: The SSL landscape is changing—and fragmented management can cost corporations

With shortened secure sockets layer (SSL) certificate renewal life cycles looming, organizations cannot afford to delay a transition to certificate automation. Nor can they afford to compromise the security of their domains with fragmented SSL management.

Domain security is about to enter its most transformative period ever—one that could leave organizations far behind in the protection of their online brands and digital identities. Most notably, the discontinuation of WHOIS email validation earlier this year, and the upcoming reduction in certificate lifetimes and domain control validation (DCV) re-use periods starting in March 2026, will lead to significant changes in how organizations operate.

By 2029, SSL and transport layer security (TLS) certificate life cycles will shrink from 367 days to just 47—meaning organizations accustomed to having roughly a year to renew a certificate will now need to do so nearly eight times a year. In addition, DCV re-use periods will decline from 367 days to only 10 by 2029.

These changes come at a time when low-cost, easy-to-obtain DV certificates dominate the market. Cybercriminals take advantage of these cheap or free certificates to make their fraudulent websites look authentic when they impersonate brands by using the same certificate types, so they can trick customers into clicking malicious links and compromising their data.

Simultaneously, some organizations are putting greater emphasis on security, but our annual "Domain Security Report" highlighted that a large portion of enterprises still have significant domain security risks. Our research found that over two-thirds of all Global 2000 companies have less than half of the recommended security measures implemented.

For this SSL Landscape report, we analyzed use trends and patterns for more than 802,000 digital certificates linked to 2.4 million domains to understand how organizations oversee SSL certificates and how that impacts the integrity assurance of these domains. In our research and personal interactions with corporate leaders, we found organizations are ignoring or delaying the implementation of a strategic response to the shortened SSL certificate life cycles and DCV re-use periods. This report provides an in-depth look at these issues—as well as the needed steps to avoid them.

Too many brands opt for easier-to-obtain certificates

An SSL certificate authenticates the legitimacy and safety of an online brand, validating the credentials of the certificate, and encrypting the connection between a website's server and a user's browser.

There are two key functions of SSL certificates:

- **Security:** Encryption ensures the protection of login credentials, credit card numbers, and other sensitive data.
- **Trust:** Users trust that a site with a certificate is owned by a legitimate entity running the site and data transfer is secured. The level of authentication varies with the validation levels of a certificate.

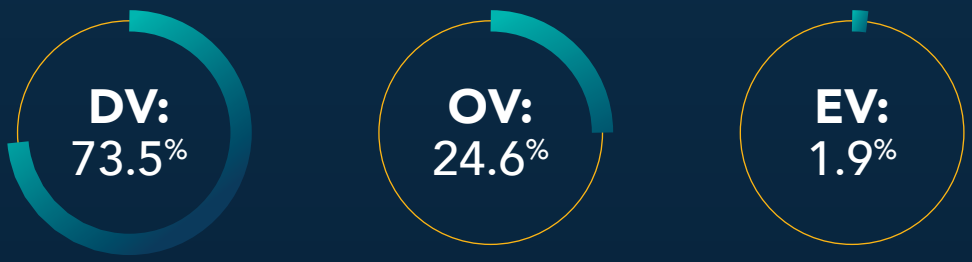
But our research reveals this ideal state of security and trust is more the exception than the norm, with the vast majority of online brands choosing certificate types that are easier to obtain to reduce workload and increase speed.

There are three levels of SSL certificate validation:

- **Domain validation (DV).** These are the lower-cost certificates, and the quickest to get. A DV will only verify that the certificate buyer controls the domain name. Any domain name registrant can obtain an SSL certificate regardless of their intent for the domain name use.
- **Organization validation (OV).** The OV does what the DV does while authenticating certain details about the organization, such as its business registration certificate.
- **Extended validation (EV).** The EV is the most thorough and vigilant of the certificates, amplified by the in-depth vetting of the legal, physical, and operational existence of the organization.

In our research, we found that DVs account for three quarters (73.5%) of certificates, with OVs representing nearly one quarter (24.6%). EVs account for less than 2 percent (1.9%).

Certificate types distribution:



From the distribution, it's unsurprising that DV certificates are the most popular as they're easier and faster to purchase. When companies use vendors offering these low-cost certificates, cybercriminals can leverage the same certificates from the same vendors to legitimize their fraudulent sites and gain user trust with the added hypertext transfer protocol secure (HTTPS). Fraudsters have grown more sophisticated than the instances when spoofed websites would include typos and bad grammar. Malicious actors are very good at disguising themselves, and easy access to DV certificates only boost their ability to pass themselves off as a legit business.

Historically, sites using EV certificates would show a green bar indicator informing visitors the site is secured by an organization that has been thoroughly verified. The green bar indicator is no longer supported in major browsers, which led to a decline in adoption of EV certificates.

This data raises a few questions: Do IT departments have a clear strategy on which certificate is obtained for each type of web asset? Or are they simply acquiring DV certificates because "they're easy and fast?"

Multiple providers results in multiple points of risk

# of providers	% analyzed companies
1	22.4%
2	18.5%
3	16.6%
4	15.8%
5	12.2%
6	7.4%
7	4.1%
8	1.9%
9	1.0%
10 or more	0.3%

Our research shows almost **60% of organizations** use three or more certificate providers, and one organization had as many as 13 providers.

The above chart reveals the vast majority of organizations use multiple certificate providers.

In fact, approximately 60% of businesses use three or more providers, which could lead to major headaches from a management perspective. It may result in a lack of a centralized approach and fragmented, counterproductive processes—the impact of which will be felt exponentially with the shift to shorter life cycles and DCV re-use periods.

Consolidating to a single provider makes certificate renewals—and troubleshooting problems—significantly faster and more efficient. If an SSL-related issue comes up, security team members simply go to one source to resolve it if they're using one provider.

Additionally, working with a single provider reduces risk. Rather than juggling multiple renewal deadlines across different providers, one reliable provider ensures timely renewal notifications. Managing multiple providers may also forfeit cost efficiencies that consolidation with one certificate provider can deliver.

Leading providers are not enterprise class

Top three certificate providers:

Let's Encrypt, Google®, and Amazon®

Combined total: 66% of all analyzed certificates

These three providers supply the majority of DV certificates (89%) used by the analyzed organizations. Their low-cost offerings appeal to companies looking to reduce expenses, but they also make these providers a leading source of certificates for fraudulent domains that CSC's Enforcement Team has taken down. The same accessibility that attracts legitimate companies is equally available to malicious actors.

Top certificate providers for fraudulent domains taken down by CSC:

Google | Let's Encrypt | Cloudflare® | Amazon

Seeking cost savings and speed, organizations choose these consumer-grade providers. However, the providers don't offer the enterprise-class support needed to help companies prepare for upcoming SSL industry changes. This shortsighted approach also creates unnecessary complications with respect to the tighter certificate renewal cycles.

Organizations cannot afford to ignore or delay in preparing for the 47-day windows. If they wait until the last minute, they'll face a staggeringly complex and disruptive transition. They may be unable to cope with the increased frequency of certificate renewals and DCVs. Missed renewals could bring down entire domains and applications—the critical foundations to business operations.

If they plan ahead—and enlist the support of an enterprise-class SSL certificate provider—they'll prevent frantic, expensive scenarios. An established partner will come with a proactive and effective certificate strategy while delivering automation tools to replace time-consuming, manual processes and ensure that expiration outages never happen. With such tools, an agent can request, receive, and install a certificate fully as part of an automated renewal process.

But it takes time to integrate the automation tools into systems. You can't just buy it off the shelf and implement it, because there are nuances involved. For example, existing system components may not be compatible with the tools, which means companies have to replace them. That's why ignoring or de-prioritizing the more rapid renewal cycles will lead to avoidable—and costly—chaos.

Three steps toward optimal automation

In seeking to avoid expiration outages, organizations are increasingly acknowledging they can't manage SSL certificates without automation. They've been attempting to do so manually, tracking pending expirations with spreadsheets, and managing with the current once-a-year renewal rates. But the landscape is set to change, and this is when automation enters the equation.

As indicated, an automated integration isn't a simple feat. Multiple certificate providers and oversights along the way will introduce bottlenecks and complexity. To effectively stay on track, we recommend the following steps:

Standardize—and document—processes.

Team members come and go. Things change. Regardless, certificate management requires standardized practices that remain consistent over time. Before moving forward with automated integration, make sure to develop these practices—and document them so current and future team members will follow them. Include pain points encountered along the way, so team members will be aware of what kind of problems have come up and how they were resolved.

Educate yourself and your teams.

There are many components of automation to comprehend before putting them in play. Partnering with a single, proven certificate provider helps greatly with the learning process as that provider will be well-versed on these components and can educate clients accordingly.

The sole provider can, for example, help clients decide whether to purchase a "big automation solution" or pursue a less expensive and ambitious route. There are IT tools available—some open source and others designed with vendor application programming interfaces (APIs)—that have emerged as alternatives to one large solution. A highly qualified provider allows clients to make informed choices about how to proceed.

Include everything.

Teams will sometimes leave something out of an automated integration initiative. This is a mistake. Piecemeal approaches inevitably leave behind glaring gaps that will hinder a successful integration, so include the full workflow.

Conclusion

Certificates are everywhere, and organizations cannot do without them. Customers only need to see an “unsecure site” pop-up warning to flee to the competition. Yet, most organizations don’t have a good handle of their certificate inventory. With the industry changes planned, organizations are forced to have automation in place, and they need to prepare themselves for it.

The confluence of shortened life cycles and DCV re-use periods brings the foreboding potential for a perfect cyber storm—organizations that delay renewal planning will encounter more costs and risks in attempting to transition. Choosing to consolidate—with a single, proven certificate solutions partner—will result in a smoother, safer transition enhanced by automation.

Learn more about CSC’s flexible suite of digital certificate management solutions that tailors to organizations with diverse needs.

Let's talk 1 800 927 9800 | cscdbs.com

About CSC

CSC is the trusted security and threat intelligence provider of choice for the Forbes Global 2000 and the 100 Best Global Brands (Interbrand®) with focus areas in domain security and management, along with digital brand and fraud protection. As global companies make significant investments in their security posture, our DomainSec℠ platform can help them understand cybersecurity oversights that exist and help them secure their online digital assets and brands. By leveraging CSC's proprietary technology, companies can solidify their security posture to protect against cyber threat vectors targeting their online assets and brand reputation, helping them avoid devastating revenue loss. CSC also provides online brand protection—the combination of online brand monitoring and enforcement activities—with a multidimensional view of various threats outside the firewall targeting specific domains. Fraud protection services that combat phishing in the early stages of attack round out our solutions. Headquartered in Wilmington, Delaware, USA, since 1899, CSC has offices throughout the United States, Canada, Europe, and the Asia-Pacific region. CSC is a global company capable of doing business wherever our clients are—and we accomplish that by employing experts in every business we serve. Visit cscdbs.com.

DBS02132026