Validità del certificato SSL ridotta a 199 giorni: ecco cosa devi sapere.

A partire **dal 24 febbraio 2026**, tutte le Autorità di Certificazione (CA) inizieranno a rilasciare **certificati TLS/SSL con una validità massima di 199 giorni**, rispetto agli attuali 397 giorni.

Non si tratta **di una decisione specifica di un fornitore**, bensì di un **requisito a livello di settore,** imposto dai **requisiti di base aggiornati del CA/Browser Forum**. L'obiettivo principale è rafforzare la sicurezza generale di Internet riducendo il periodo di esposizione dei certificati compromessi e consentendo una più rapida adozione di nuovi standard crittografici man mano che le minacce si evolvono.

Perché la durata dei certificati si sta accorciando

Periodi di validità dei certificati più brevi offrono numerosi vantaggi in termini di sicurezza e operatività:

- Rischio ridotto in caso di compromissione della chiave privata
- Risposta più rapida alle vulnerabilità e alle obsolescenze crittografiche.
- Migliore allineamento con la moderna gestione automatizzata dei certificati.

Questa modifica segue lo stesso approccio incentrato sulla sicurezza che in precedenza ha portato alla riduzione dei certificati da pluriennali a annuali.

Date limite in California

Le diverse autorità di certificazione applicheranno la nuova validità massima di 199 giorni in date diverse:

- **DigiCert** – 24 febbraio 2026

- **Settigine** – 14 marzo 2026

Dopo tali date, qualsiasi certificato di nuova emissione o riemesso sarà soggetto al limite di 199 giorni.

Come gestire i certificati SSL più brevi: due approcci possibili

Con la riduzione della durata di validità dei certificati, esistono due modi pratici per gestire i rinnovi e le riemissioni.

Opzione 1 – Riemissione manuale

Puoi continuare ad acquistare certificati SSL esattamente come fai oggi (ad esempio, prodotti con validità di 1 o 2 anni). Tuttavia, dovrai **riemettere e reinstallare il certificato all'incirca ogni sei mesi** .

Punti chiave:

- Nessun costo aggiuntivo per le riemissioni.
- Richiede attenzione operativa
- Le notifiche di riemissione devono essere abilitate nel tuo account per evitare interruzioni del servizio

Questo approccio è adatto ad ambienti con volumi di lavoro ridotti o a organizzazioni con procedure manuali consolidate.

Opzione 2 – Passare all'automazione dei certificati (consigliata)

L'automazione elimina l'onere operativo delle frequenti riemissioni e annulla virtualmente il rischio di scadenza dei certificati.

Nelle prossime settimane, **WhiteReady** introdurrà diverse opzioni di automazione, tra cui:

- **Abbonamento SSL** con installazione automatica per Apache, NGINX e Microsoft IIS
- **Certificati SSL basati su ACME** per emissione e rinnovo completamente automatizzati

- **Supporto per la riemissione automatica dei** certificati SSL per le integrazioni AutoInstall con cPanel, Plesk e DirectAdmin.

Una volta configurati, i certificati vengono riemessi, installati e rinnovati automaticamente, senza intervento manuale.

Preparatevi ora all'era SSL di 199 giorni.

Il passaggio a certificati TLS di durata inferiore è inevitabile ed è già in programma. Le organizzazioni che si preparano, soprattutto adottando l'automazione, beneficeranno di una maggiore sicurezza, di un rischio ridotto di interruzioni del servizio e di minori costi operativi.

Se hai bisogno di assistenza per scegliere la soluzione SSL più adatta o per abilitare l'automazione, il team di WhiteReady è pronto ad aiutarti a prepararti con largo anticipo rispetto alle scadenze del 2026.

Revision #1
Created 6 August 2026 19:01:06 by Franco Abitante
Updated 6 August 2026 19:02:38 by Franco Abitante