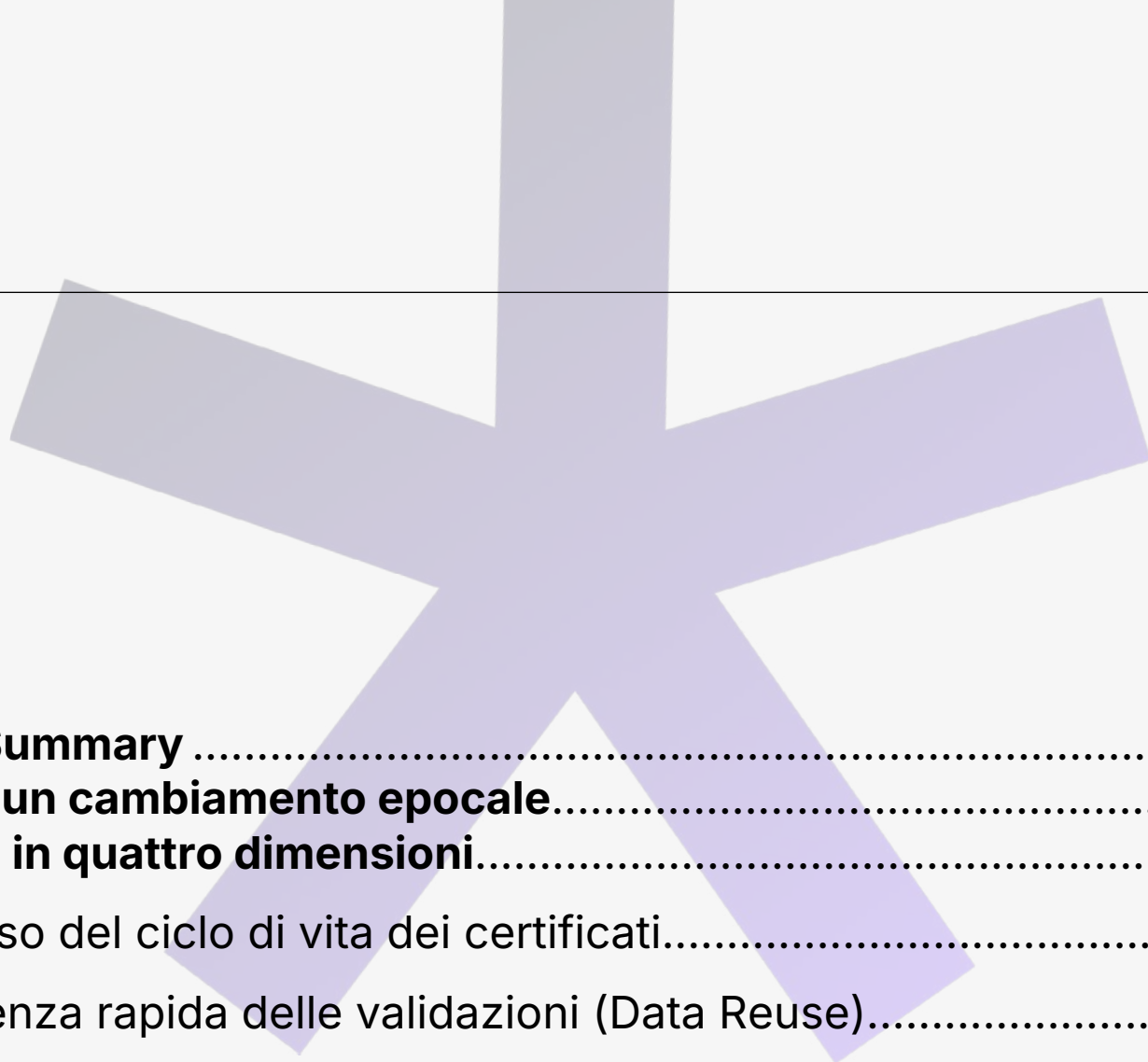




Certificati TLS: dalla gestione manuale all'automazione obbligatoria

Comprendere il nuovo standard del CA/Browser Forum e prepararsi al cambiamento nella gestione dei certificati TLS pubblici

Un whitepaper a cura di Angelo Maturi, Mateus Pavei Menegon e Fabio Sanna



Executive Summary	3
Il contesto: un cambiamento epocale.....	3
Il problema in quattro dimensioni.....	4
1. Collasso del ciclo di vita dei certificati.....	4
2. Scadenza rapida delle validazioni (Data Reuse).....	4
3. Complessità nella validazione dei domini (DCV) e DNSSEC.....	4
4. Obblighi legali stringenti.....	4
Le tappe del cambiamento.....	4
Tabella.....	4
Cosa significa per l'organizzazione.....	5
Il nostro approccio: dall'assessment al servizio continuo.....	6
Tabella.....	6
Perché agire ora.....	6

Executive Summary

Il CA/Browser Forum — il consorzio che stabilisce gli standard di sicurezza per i certificati TLS pubblici riconosciuti dai browser — ha avviato un cambiamento strutturale nella gestione del ciclo di vita dei certificati. Entro il 2029, la validità massima di un certificato pubblico scenderà da 398 a soli 47 giorni, e il periodo in cui un'autorità di certificazione può riutilizzare la validazione di un dominio si ridurrà fino a 10 giorni.

Per le organizzazioni che gestiscono certificati TLS su larga scala — banche, e-commerce, pubblica amministrazione, service provider — questo significa che un processo storicamente occasionale (rinnovare un certificato ogni uno o due anni) diventa un'attività operativa continua, ad alta cadenza e ad alto rischio se gestita manualmente. Questo documento descrive il contesto normativo, gli impatti concreti per le organizzazioni e l'approccio che Sorint. lab propone per trasformare questo obbligo in un processo automatizzato, affidabile e conforme.

Il contesto: un cambiamento epocale

Per anni, la gestione dei certificati TLS pubblici è stata un'attività a bassa frequenza: si acquistava un certificato, lo si installava, e ci si ricordava di rinnovarlo dopo uno o due anni. Il CA/Browser Forum — che riunisce le principali autorità di certificazione e i produttori di browser — ha progressivamente ridotto questa finestra temporale, con l'obiettivo dichiarato di limitare la superficie di rischio legata a chiavi compromesse, configurazioni obsolete e domini non più controllati dal legittimo proprietario.

Il risultato è un percorso di riduzione già in corso e destinato ad accelerare: dai 398 giorni storici si è passati a 200 giorni nel marzo 2026, si scenderà a 100 giorni nel 2027, fino ad arrivare a soli 47 giorni nel marzo 2029. Parallelamente, anche il periodo in cui una CA può riutilizzare la validazione di un dominio (Domain Control Validation, DCV) si riduce, fino a un minimo di 10 giorni.

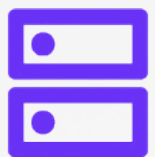
In sintesi: un processo che oggi si ripete una o due volte l'anno, nel 2029 dovrà ripetersi quasi ogni settimana — su ogni singolo certificato pubblico dell'organizzazione.

Il problema in quattro dimensioni



1. Collasso del ciclo di vita dei certificati

La validità massima dei certificati pubblici si riduce drasticamente, arrivando a soli 47 giorni entro marzo 2029. Un'organizzazione con centinaia o migliaia di certificati non può più gestire i rinnovi con processi manuali senza esporsi a un rischio concreto di interruzione dei servizi.



3. Complessità nella validazione dei domini (DCV) e DNSSEC

Molti metodi storici di validazione — via email, telefono o WHOIS — sono stati deprecati dal CA/Browser Forum. Le infrastrutture DNS aziendali devono inoltre supportare correttamente DNSSEC e i record CAA, requisiti spesso non presidiati con la stessa attenzione riservata ai certificati stessi.



2. Scadenza rapida delle validazioni (Data Reuse)

Il periodo in cui una CA può riutilizzare la validazione di un dominio, senza doverlo riverificare, scenderà progressivamente fino a soli 10 giorni entro il 2029. Ogni rinnovo richiederà quindi una nuova validazione, moltiplicando il carico operativo.



4. Obblighi legali stringenti

Attraverso il Subscriber Agreement sottoscritto con la CA, l'azienda è legalmente responsabile della protezione della chiave privata, del non utilizzo di chiavi crittograficamente deboli (vulnerabilità note come Debian o ROCA) e dell'obbligo di richiedere la revoca immediata — entro 24 ore — in caso di compromissione o di dati inesatti.

Le tappe del cambiamento

La tabella seguente riassume la roadmap normativa già definita dal CA/Browser Forum. Ogni tappa dimezza, o quasi, la finestra temporale a disposizione per gestire ciascun certificato.

Data di entrata in vigore	Durata massima del certificato	Riutilizzo massimo della validazione	Stato
Prima del 15 Marzo 2026	398 giorni	398 giorni	Superato
15 Marzo 2026	200 giorni	200 giorni	In vigore
15 Marzo 2027	100 giorni	100 giorni	Futuro
15 Marzo 2029	47 giorni	10 giorni	Traguardo finale

Oggi ci troviamo nella finestra dei 200 giorni, in vigore dal 15 marzo 2026. Le organizzazioni che iniziano oggi un percorso di automazione arrivano preparate a ogni tappa successiva; chi rimanda, dovrà gestire in emergenza una finestra sempre più stretta.

Cosa significa per l'organizzazione

L'impatto di questo cambiamento non è solo tecnico: coinvolge più funzioni aziendali, ciascuna con responsabilità specifiche. Gli IT Operations e i System & Network Administrator devono implementare protocolli di automazione (come ACME) e gestire rinnovi continui senza causare interruzioni di servizio. I DNS & Domain Administrator devono garantire che l'infrastruttura DNS supporti correttamente la validazione dei domini e la gestione dei record CAA. Il CISO e i team di sicurezza devono presidiare la protezione delle chiavi private e predisporre piani di Incident Response capaci di rispondere a una revoca entro 24 ore.

Il rischio principale non è teorico: un rinnovo mancato anche di un solo giorno, in un ciclo di vita a 47 giorni, si traduce in un'interruzione visibile dei servizi esposti al pubblico — con impatti diretti su operatività, fiducia dei clienti e, in molti settori, conformità normativa.

Il nostro approccio: dall'assessment al servizio continuo

Sorint.lab affronta questo cambiamento con un modello di servizio strutturato in quattro fasi, pensato per accompagnare l'organizzazione dalla fotografia dello stato attuale fino a un presidio continuo e automatizzato del ciclo di vita dei certificati.

1 · Assessment

Censimento di tutti i certificati TLS pubblici in uso, analisi dei metodi di validazione attuali e valutazione della solidità crittografica delle chiavi private.

2 · Solution Design

Progettazione dell'architettura di automazione (es. protocollo ACME) per il ciclo di vita a 47 giorni, definizione dei processi interni e pianificazione degli aggiornamenti DNS/DNSSEC.

3 · Implementation

Integrazione e configurazione dei client ACME su server, load balancer e firewall; creazione sicura delle chiavi direttamente sugli endpoint finali.

4 · Servizio Continuo (CIS)

Monitoraggio h24 dello stato dei certificati, gestione di incidenti e revoche entro 24 ore, adeguamento costante ai cambiamenti introdotti dal CA/Browser Forum.

L'approccio è deliberatamente agnostico rispetto alla tecnologia: a seconda del contesto del cliente, valutiamo insieme la soluzione più adatta, che si tratti di una piattaforma enterprise (come Venafi, Keyfactor, AppViewX o DigiCert/Sectigo) o di una soluzione open source (come cert-manager, HashiCorp Vault o UCM). L'obiettivo non è vendere uno strumento, ma garantire continuità di servizio e conformità normativa nel tempo.

Perché agire ora

Chi non avvia oggi un percorso di automazione dovrà comunque farlo entro pochi anni, ma in condizioni più urgenti e con margini di errore ridotti. Avviare un assessment ora consente di affrontare il cambiamento con gradualità, testando l'approccio su un perimetro limitato prima che la finestra dei 47 giorni diventi la norma.

Il rischio non è "se" un rinnovo verrà mancato, ma "quando" — a meno che il processo non sia automatizzato.

Un white paper a cura di:



Angelo Maturi

Head of CIO Initiative HUB

E-mail:
amaturi@sorint.com



Mateus Pavei Menegon

DevOps Engineer

E-mail:
mpavei@sorint.com



Fabio Sanna

DevOps Architect

E-mail:
fabio.sanna@sorint.com

Per ulteriori dettagli o approfondimenti scrivici a:
welisten@sorint.com



[LinkedIn](#) | [Facebook](#) | [YouTube](#) | [Instagram](#) | [GitHub](#)

BUILDING GREAT TECHNOLOGY
www.sorint.com