Buone Pratiche per l'utilizzo dei Certificati SSL (TLS publicly-trusted)

Somario

1. Automazione
2. Infrastrutture critiche
3. Certificati ad uso interno
4. Certificate pinning

Riferimenti

[1] https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/#613-delayed-revocation
[2] https://googlechrome.github.io/chromerootprogram/

Automazione

L'automazione della gestione dei certificati SSL, attraverso protocolli come ACME, è diventata una necessità tecnica e operativa fondamentale per qualsiasi organizzazione. Questa non è solo una best practice consigliata, ma l'unica pratica sostenibile all'evoluzione normativa dell'ecosistema PKI pubblico.

Il CA/B Forum (Certification Authority/Browser Forum) ha formalizzato una ***validity reduction schedule*** che ridurrà progressivamente la durata massima dei certificati SSL publicly-trusted. Mentre fino a pochi anni fa i certificati potevano avere una validità fino a 3 anni, oggi siamo a 398 giorni, e da metà marzo 2026 la validità massima scenderà a 200 giorni. La roadmap prevede poi riduzioni ulteriori a 100 giorni e poi a 47 giorni rispettivamente al 15 marzo 2027 e 15 marzo 2029. Questa decisione risponde anche ad **esigenze di sicurezza:** certificati più brevi riducono la finestra temporale in cui chiavi compromesse possono essere sfruttate dagli hacker e incentivano le aziende a mantenere aggiornati i propri inventari dei certificati.

Il Root Store Programs dei browser vendors, hanno adottato requisiti sempre più stringenti. Nessuna Certification Autority trusted può sottrarsi a queste direttive senza rischiare la rimozione dai Root Store dei vari browser vendors, il che significa che **ogni organizzazione che usa certificati SSL** dovrà necessariamente **adattarsi alle nuove politiche** di gestione dei certificati.

Nel futuro scenario regolamentare, la gestione manuale dei certificati diventerà rapidamente insostenibile. Per esempio, un'organizzazione con 100 siti web che oggi rinnova certificati annuali deve gestire 100 rinnovi all'anno. Con certificati di 100 giorni, gli stessi siti web richiederebbero 400 rinnovi annuali. Con certificati di 45 giorni, 800 operazioni di rinnovo. Ogni rinnovo manuale comporta generazione di CSR, validazione del dominio, download, installazione, e verifica del certificato. La probabilità di errore umano e downtime aumenterà proporzionalmente.

Automazione con ACME

L'automazione attraverso **ACME** risolve già da oggi questi problemi operativi g**estendo l'intero ciclo di vita del certificato**: richiesta, validazione del dominio, emissione, installazione e rinnovo. La validazione avviene programmaticamente, eliminando ogni intervento manuale. Il rinnovo automatico garantisce inoltre che i certificati vengano sostituiti prima della scadenza, tipicamente con un margine di sicurezza 30 giorni dalla scadenza. Infine, l'installazione automatica dei certificati - supportata da diversi client ACME - consente all'organizzazione di evitare qualsiasi operazione manuale.

I vantaggi operativi sono tangibili. L'automazione riduce drasticamente il carico di lavoro, elimina errori umani, garantisce la conformità nel continuo e migliora la sicurezza con certificati di durata minore. Dal punto di vista economico, l'investimento iniziale per adottare e configurare ACME verrà rapidamente ammortizzato nel tempo. Il costo (talvolta "nascosto") dei processi manuali, in termini di tempo del personale e rischio di downtime, supera largamente il costo di implementazione di ACME. Un singolo incidente causato da un certificato scaduto può costare più dell'intero progetto di automazione.

L'ecosistema di strumenti disponibili per ACME è maturo: Certbot, Win-ACME, Posh-ACME, acme.sh, e numerosi altri client ACME di pubblico dominio, pronti all'uso e senza costi, semplificano l'integrazione. Le organizzazioni possono iniziare con progetti pilota su sistemi non critici, acquisire esperienza, e poi espandere gradualmente la tecnologia agli ambienti di produzione.

È fondamentale comprendere che questa transizione non è opzionale o procrastinabile ma un preciso **obbligo normativo**. La validity reduction schedule è già stata calendarizzata e verrà implementata indipendentemente dalla preparazione delle organizzazioni che usano i certificati SSL. Le Certification Authority non potranno emettere certificati con validità superiore ai limiti imposti dai regolamenti, e i browser rifiuteranno i certificati la cui validità eccede quanto previsto dai vincoli normativi. Le organizzazioni che non si adegueranno si troveranno ben presto a gestire emergenze operative con conseguenze potenzialmente gravi per la continuità dei propri servizi ed innalzamento dei costi.

La nostra raccomandazione è quella di avviare immediatamente un progetto che include:

- la predisposizione di un inventario completo dei certificati esistenti all'interno dell'organizzazione,
- l'identificazione dei sistemi che possono beneficiare di automazione,
- la selezione di strumenti appropriati, la formazione del team tecnico,
- l'implementazione graduale di ACME.

Il tempo investito oggi nell'automazione eviterà crisi operative ed incidenti domani.

Infrastrutture critiche

Actalis sconsiglia vivamente l'utilizzo di certificati SSL (TLS publicly-trusted) per le infrastrutture critiche negli ambiti della Sanità, Energia, Trasporti, Servizi finanziari, Telecomunicazioni, Gestione delle risorse idriche e nella Pubblica Amministrazione.

Il motivo è di natura operativa e di continuità del servizio: le Certification Authority (CA) pubbliche sono vincolate da normative stringenti che le obbligano, in circostanze particolari, a revocare i certificati entro 5 giorni lavorativi, o addirittura entro 24. Una revoca improvvisa e/o imprevista renderebbe immediatamente inaccessibili tutti i servizi che utilizzano tali certificati, causando:

- **Interruzioni critiche dei servizi** con potenziali conseguenze sulla salute e sicurezza dei cittadini
- **Perdite economiche significative** per organizzazioni e utenti, anche a causa di potenziali rischi sanzionatori
- **Disagi operativi gravi** per l'erogazione di servizi essenziali
- **Rischi per l'incolumità pubblica** nei settori più sensibili come sanità e trasporti
- **Impatti reputazionali** importanti verso le terze parti.

Per tutte queste ragioni, le infrastrutture critiche dovrebbero preferire certificati privati, emessi da Certification Authority private, che garantiscono pieno controllo sui tempi e sulle modalità di gestione del ciclo di vita dei certificati.

Si deve notare infatti che, nelle circostanze che lo richiedono, la **Certification Authority ha l'obbligo** di revocare i certificati indipendentemente dal fatto che tali certificati siano utilizzati nell'ambito di infrastrutture critiche.

Certificati ad uso interno

L'uso di certificati SSL "publicly-trusted" per i propri **servizi interni**, come siti intranet o applicazioni che non interagiscono direttamente con utenti esterni della rete Internet pubblica, è **fortemente sconsigliato** in quanto presenta diversi **problemi significativi:**

- **Requisiti di validazione del dominio:** le Certification Authority pubbliche devono verificare il tuo controllo del dominio. Per servizi interni con nomi come intranet.local o indirizzi IP privati (192.168.x.x, 10.x.x.x), questa validazione è impossibile. Si dovrebbero usare domini pubblici realmente posseduti, esponendo informazioni potenzialmente sensibili sulla propria infrastruttura.

- **Esposizione nei Certificate Transparency Logs**: tutti i certificati emessi da Certification Authority pubbliche vengono registrati obbligatoriamente nei CT Logs pubblici. Questo rivela i nomi dei propri server interni, i dettagli sulla tua architettura di rete, potenziali obiettivi per attaccanti, e queste sono informazioni che rimangono permanentemente accessibili.
- **Vincoli operativi**: le Certification Authority pubbliche impongono una validità massima in progressiva riduzione (ad oggi 398 giorni, ma dal marzo 2026 saranno 200 giorni e poi a calare negli anni seguenti), richiedendo dunque rinnovi frequenti; la revoca dei certificati è obbligatoria in caso di compromissione della chiave privata o di qualsiasi "difetto" (rispetto a quanto prescritto dai requisiti del CAB Forum) nel profilo dei certificato. Vi sono inoltre limitazioni sui nomi di dominio ammissibili.
- **Problemi di sicurezza e segmentazione**: mescolando certificati pubblici e privati, si riduce la separazione tra perimetro esterno e interno; gli incidenti di sicurezza interni vengono esposti pubblicamente attraverso i CT Logs, la revoca tramite CRL/OCSP potrebbe non funzionare sulle reti interne isolate dalla internet pubblica.

L'esigenza di abilitare il protocollo SSL sui propri siti ad uso interno si può facilmente soddisfare attraverso una **Certification Authority privata** che può essere realizzata con svariate tecnologie anche gratuite.

Certificate pinning

Il Certificate Pinning è una tecnica di sicurezza in cui all'interno di un'applicazione client (tipicamente un'app per Android o iOS) viene "cablato" uno specifico certificato TLS (detto *pin*) appartenente al web server di destinazione. Oppure viene "cablato" il certificato della CA emittente. Invece di accettare qualsiasi certificato emesso sotto una Root CA attendibile, il client procede con la connessione SSL/TLS solo se il certificato TLS presentato dal server (oppure il certificato della CA emittente) corrispondono allo specifico pin. Questo meccanismo è stato originariamente ideato per contrastare gli attacchi Man-in-the-Middle (MITM), in particolare quelli derivanti dalla compromissione delle Certification Authority (si ricordi il caso emblematico della DigiNotar[SD1]).

Se correttamente implementato e gestito, questo meccanismo è certamente utile; tuttavia, esso comporta anche degli svantaggi che devono essere ben considerati e che, in definitiva, superano i benefici. In breve, il Certificate Pinning **dovrebbe essere generalmente evitato** perché introduce complessità e rischi operativi significativi.

L'implementazione del Certificate Pinning è notoriamente rischiosa e soggetta a errori. Inoltre, comporta un considerevole **overhead di manutenzione** e una **flessibilità ridotta**, poiché qualsiasi modifica al

certificato del server (ad esempio, il rinnovo che, dopo un certo tempo, è comunque indispensabile) o della Certification Authority emittente (anch'essa di durata limitata e soggetta a revoca) richiede l'aggiornamento dell'applicazione client con il nuovo pin. Il mancato o non tempestivo aggiornamento può causare interruzioni del servizio o problemi di connessione per gli utenti delle app interessate.
In particolare, il pinning dei certificati **compromette la capacità di rispondere a problemi di certificato con breve preavviso**, soprattutto se si considerano tutti i requisiti del CA/Browser Forum che tutte le Certification Authority trusted sono tenute a rispettare rigorosamente.

Tali requisiti, infatti, impongono alle Certification Authority la **revoca dei certificati entro un tempo brevissimo i**n determinati scenari. Ad esempio, se viene rilevato che un certificato contiene dati identificativi errati, ogni Certification Authority ha l'obbligo di revocarlo entro **5 giorni.** In altri casi (per es. compromissione della chiave privata o altri motivi di sicurezza), la revoca deve essere fatta **entro 24 ore**.

Se una organizzazione ha "cablato" (pinned) un certificato soggetto a questo tipo di revoca, dovrà distribuire gli aggiornamenti a tutte le app entro lo stesso lasso di tempo, molto breve, per includere il certificato sostitutivo. Questo conflitto intrinseco, in cui le modifiche rapide e obbligatorie dei certificati si scontrano con il complesso processo di aggiornamento delle applicazioni client bloccate, è la ragione tecnica principale per cui il certificate pinning **comporta più rischi che benefici** nella gran parte degli scenari più comuni.