Automazione PKI aziendale

WHITEPAPER DI SECTIGO

SECTIGO®

Le aziende hanno bisogno di una soluzione di autenticazione per soddisfare requisiti sempre più complessi

Le esigenze di autenticazione aziendale stanno diventando sempre più complesse. Applicazioni e dati in esecuzione in più ambienti cloud, una forza lavoro distribuita e dispositivi connessi innovativi si intersecano in modi che richiedono un forte approccio all'identità digitale per proteggersi dalle minacce in continua evoluzione.

Le aziende si affidano ai certificati PKI come gold standard per garantire l'identità e come parte fondamentale di un'architettura Zero Trust e senza password per utenti, dispositivi, server e identità delle applicazioni.

Sebbene non esista una soluzione di autenticazione e crittografia più forte e più facile da usare dell'identità digitale fornita da PKI, la sfida per le squadre IT impegnate è che la distribuzione e la gestione manuale dei certificati richiede tempo e può creare interruzioni del servizio non necessarie. Indipendentemente dal fatto che un'azienda distribuisca un singolo certificato SSL per un server Web o gestisca milioni di certificati su tutti i dispositivi in rete e le identità utente, il processo end-to-end di emissione, configurazione e distribuzione dei certificati può richiedere ore per certificato. La gestione manuale dei certificati espone inoltre le aziende a un rischio significativo che i certificati vengano dimenticati fino alla scadenza e che siano esposti a lacune nella proprietà, con conseguenti interruzioni improvvise dei sistemi aziendali fondamentali.

Costo finanziario della gestione manuale dei certificati

Poiché gli ambienti già complessi si espandono per includere dispositivi mobili, infrastruttura cloud, DevOps, Internet delle cose e altro, il costo finanziario per gestire in modo efficace i certificati PKI è aumentato notevolmente.

L'investimento per la sicurezza più efficace è quello per la sicurezza che può essere facilmente implementata e facilmente utilizzata dai dipendenti. Tuttavia, le soluzioni di sicurezza come le password spesso impongono ai singoli utenti di ricordare, aggiornare e gestire la propria sicurezza. Inoltre, le squadre IT sono sommerse da lunghe richieste di reimpostazione delle password e addestrano i dipendenti a non cedere le password a sofisticati schemi di phishing. Ad esempio, se i dipendenti non possono crittografare/decrittografare sul proprio dispositivo mobile, ignoreranno semplicemente la crittografia della posta elettronica.

Inoltre, i tuoi clienti e gli utenti interni si affidano a sistemi aziendali critici per essere sempre attivi. I certificati scaduti hanno già causato numerose interruzioni di siti Web e servizi di alto profilo, con conseguente perdita di entrate per miliardi di dollari, sanzioni contrattuali e azioni legali, nonché la significativa perdita di reputazione del marchio.

Una gestione insufficiente dei certificati può anche mettere le aziende a rischio di non conformità ai mandati normativi. Per proteggersi dal furto di informazioni, regolamenti come HIPAA/HITECH, GDPR e le regole di acquisizione del governo federale degli Stati Uniti (DFARS) richiedono la crittografia dei dati per mitigare o ridurre al minimo le conseguenze di una violazione o divulgazione accidentale. Il mancato rispetto dei requisiti di conformità può comportare sanzioni sostanziali. Inoltre, il GDPR impone che le multe non si basino solo sulla portata di una singola violazione, ma anche sul livello di negligenza. Quindi, mettere una forte protezione sui tuoi sistemi e dispositivi non solo aiuta a ridurre il rischio di una violazione in sé, ma aiuta a ridurre l'importo della multa in caso di violazione.

I costi di amministrazione si sommano rapidamente

La gestione dei certificati può essere percepita come un'attività semplice e quotidiana per un amministratore IT o Web, ma garantire che i certificati siano validi uno alla volta è costoso. L'utilizzo di processi manuali per rilevare, installare, monitorare e rinnovare tutti i certificati PKI in un'organizzazione è laborioso e tecnicamente impegnativo.

Ad esempio, anche un'installazione manuale minima di un certificato SSL con un singolo dominio web comporta più passaggi e può facilmente aggiungere fino a oltre 50 $ per server Web. La Figura 1 illustra ogni passaggio che un amministratore Web deve eseguire per installare correttamente un singolo certificato SSL. Per un'organizzazione con 2.000 server Web, è necessaria una persona che lavori a tempo pieno per sostituire i certificati prima della scadenza.

Figura 1 – Passaggi necessari per installare manualmente i certificati SSL

Passaggi	Tempo
Selezione/acquisto di certificati SSL	Da minuti a ore
Accesso SSH al server Web	< 2 minuti - ricerca dell'indirizzo e delle credenziali del server.
Immissione di una serie di comandi per ottenere la convalida del controllo del dominio (per nuovi domini)	Da minuti a ore - leggere la documentazione, digitare i comandi appropriati. I forum di amministrazione Web sono pieni di domande e risposte e risoluzione dei problemi, suggerendo che molti hanno problemi con questo passaggio.
Richiesta di emissione del certificato e download	Fino a 5-10 minuti: leggere la documentazione, digitare i comandi appropriati.
Copia dei file del certificato nel percorso del file del server appropriato (varia in base al server Web)	<2 minuti - ricerca della posizione del file del server, digitare i comandi appropriati.
Modifica del file di configurazione del server Web per consentirgli di utilizzare il certificato SSL e pubblicare https	Da minuti a ore - leggere la documentazione, digitare i comandi appropriati, salvare i file. I forum di amministrazione Web sono pieni di domande e risposte e risoluzione dei problemi, suggerendo che molti hanno problemi con questo passaggio.
Aggiornamento//Riavvio del server Web per riconoscere la configurazione	<1 minuto
Test Tutti i passaggi precedenti devono essere eseguiti con precisione. In caso contrario, il tempo e gli sforzi umani vengono sprecati e i sistemi aziendali fondamentali verranno messi fuori servizio.	Da minuti a ore: se non vengono visualizzati messaggi di errore, il test sarà rapido. La risposta ai messaggi di errore richiederà una nuova modifica del file di configurazione del server Web.

L'evoluzione crittografica crea nuove sfide per la sicurezza aziendale

Ora le aziende devono affrontare un'altra nuova minaccia alla sicurezza con l'evoluzione della crittografia. Entro pochi anni, il calcolo quantistico renderà inutili gli attuali algoritmi di crittografia RSA ed ECC da cui dipendono i nostri sistemi digitali. Mentre il NIST e le autorità di certificazione come i Quantum Labs di Sectigo stanno sviluppando certificati X.509 sicuri per il quantum che utilizzano algoritmi di crittografia per sopportare al calcolo quantistico, è chiaro che le aziende dovranno adottare famiglie di crittografia completamente nuove con una velocità senza precedenti.

Per un'azienda che ha 10.000 certificati installati manualmente tra utenti, server, dispositivi e applicazioni, ci vorrebbero fino a cinque persone per un anno per trovare e sostituire tutti i certificati. Prima che abbia finito, il malintenzionato sfrutterà la debole crittografia per impersonare il legittimo proprietario o decrittografare le informazioni sensibili.

L'azienda moderna ha bisogno di soluzioni automatizzate

Con le insidie e le ramificazioni finanziarie inerenti alla gestione manuale dei certificati PKI, il ritorno sull'investimento per la gestione automatizzata del ciclo di vita dei certificati è chiaro. I professionisti IT devono ripensare la loro strategia di gestione del ciclo di vita dei certificati. In particolare, poiché le aziende entrano nel mercato più rapidamente con i nuovi servizi abilitati da DevOps, le organizzazioni necessitano di una soluzione automatizzata che garantisca la corretta configurazione e implementazione dei certificati senza intervento umano. Questa automazione non solo elimina le interruzioni del servizio, ma consente ai reparti IT di controllare i costi operativi e lanciare i servizi sul mercato più rapidamente.

Recentemente, PKI si è evoluto per diventare ancora più versatile. Interoperabilità, tempo di attività elevato e gestione sono ancora vantaggi chiave. Ma le soluzioni PKI di oggi sono anche funzionalmente in grado di migliorare l'amministrazione e la gestione del ciclo di vita dei certificati attraverso:

Automazione

Accelera la distribuzione dei certificati eliminando costi ed errori

Scalabilità

Gestione della numerazione dei certificati in centinaia, migliaia o addirittura milioni

Cripto-agilità

Aggiornamento della sicurezza crittografica e revoca e sostituzione dei certificati a rischio con certificati quantistici sicuri molto rapidamente, in risposta a minacce nuove o mutevoli

Visibilità

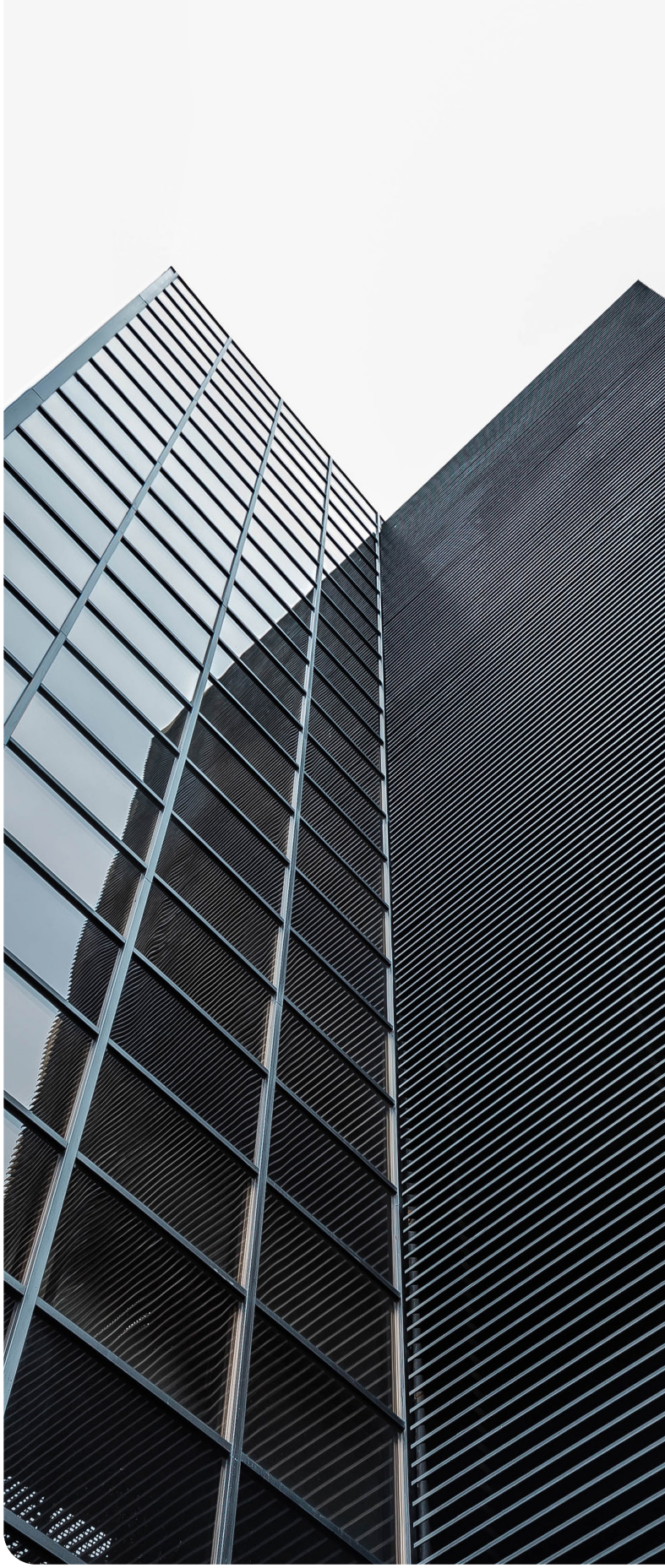
Visualizzazione dello stato del certificato con un unico pannello di controllo su tutti gli utenti, dispositivi, server e applicazioni

Risparmia tempo e mantieni il controllo con Sectigo PKI Automation

Dati i diversi sistemi, applicazioni e dispositivi che utilizzano certificati digitali, le squadre IT spesso gestiscono servizi di automazione distinti di molti fornitori diversi, con interfacce utente e qualità del supporto diversi. Un unico dashboard di gestione dei certificati che automatizza il rilevamento, la distribuzione e la gestione del ciclo di vita in tutti i casi d'uso e le piattaforme dei fornitori crea l'efficienza promessa dall'automazione. E le squadre IT mantengono ancora il controllo delle definizioni e delle regole di configurazione in modo che i passaggi di automazione vengano eseguiti correttamente.

Sectigo fornisce soluzioni di automazione dei certificati che consentono alle aziende di essere agili ed efficienti e di mantenere il controllo di tutti i certificati nel loro ambiente. Sectigo supporta l'installazione, la revoca e il rinnovo automatizzati di certificati SSL/TLS e non SSL tramite protocolli standard di settore, API e integrazioni di terze parti.

Inoltre, con Sectigo, non ti imbatterai mai in un limite di volume del certificato, come potresti fare con le alternative open source. Le soluzioni di automazione di Sectigo consentono al tuo team di sicurezza di applicare facilmente criteri di sicurezza crittografici; proteggere le comunicazioni, prevenire la perdita di dati tramite accesso non autorizzato e sistemi, applicazioni e dispositivi a prova di futuro in tutta l'azienda.



Gestione automatizzata dei certificati SSL/TLS

Per i certificati SSL/TLS, Sectigo fornisce una gestione certificata automatizzata attraverso:

- **Supporto per il protocollo ACME (Automated Certificate Management Environment):** Sectigo Certificate Manager supporta il protocollo ACME, consentendo di automatizzare l'emissione, l'installazione e la revoca dei certificati per un'ampia gamma di server Web e i load balancers. Il protocollo ACME richiede pochissimo tempo alle squadre IT per configurare ed eseguire l'automazione della gestione dei certificati, rendendolo un componente sempre più adottato della sicurezza aziendale.

Sectigo supporta i tipi di certificato SSL privato DV, OV, EV e tramite ACME e fornisce il controllo completo agli amministratori IT. Sectigo fornisce il server ACME e lavora con client conformi ad ACME, incluso Certbot della Electronic Frontier Foundation (di cui Sectigo è sponsor). Vedere la Figura 2 per il funzionamento dell'autenticazione del certificato utilizzando ACME.

Come funziona il protocollo ACME per la gestione automatizzata dei certificati PKI

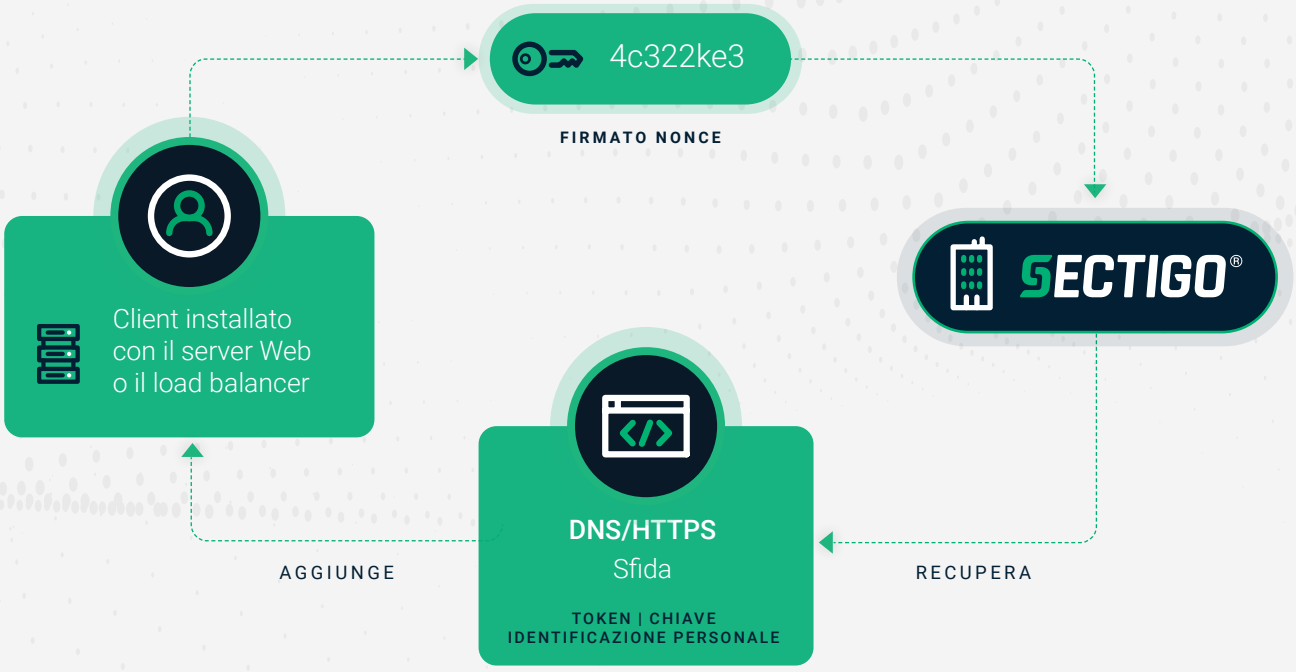


Figura 2 – Processo di autenticazione utilizzando il protocollo ACME

Gestione automatizzata dei certificati SSL/TLS

- **REST API:** in alcuni casi, le aziende preferiscono integrare le applicazioni con Sectigo utilizzando REST API di Sectigo. Sebbene ciò richieda uno sviluppo aggiuntivo sul lato dell'applicazione, consente di sfruttare la gestione dei certificati e personalizzare il flusso di lavoro.

  Inoltre, tramite REST API, Sectigo ha integrazioni dirette con tutti i principali ambienti di containerizzazione e strumenti di automazione, come Docker, Chef, Ansible, Salt Stack, Terraform, Puppet e Jenkins. Includiamo anche meccanismi per incorporare PKI nell'elaborazione di integrazione continua e distribuzione continua (CI/CD), strutture orchestrate come Kubernetes e cassette di sicurezza delle chiavi di terze parti come HashiCorp's Vault.

- **Agent di installazione automatizzata presso il locale del cliente:** utilizzando Network Agent di Sectigo, puoi automatizzare la gestione dei certificati per una varietà di sistemi, inclusi i server Web Apache, Tomcat, IIS e F5. Il Network Agent dei locali del cliente è integrato con Sectigo Certificate Manager per programmare l'emissione, l'installazione e il rinnovo dei certificati.
- **Integrazione con fornitori di terze parti:** Sectigo si integra direttamente con i principali fornitori di terze parti per aiutare i clienti a ottenere la completa automazione dei certificati utilizzando tecnologie popolari già in uso negli ambienti IT, come il load balancer Big-IP di F5, il controller di distribuzione delle applicazioni ADC di Citrix e la piattaforma del flusso di lavoro IT di ServiceNow.

  Vedere la Figura 3 per un elenco delle piattaforme e delle tecnologie attualmente supportate.

Figura 3 – Soluzioni di automazione attualmente supportate per certificati SSL/TLS

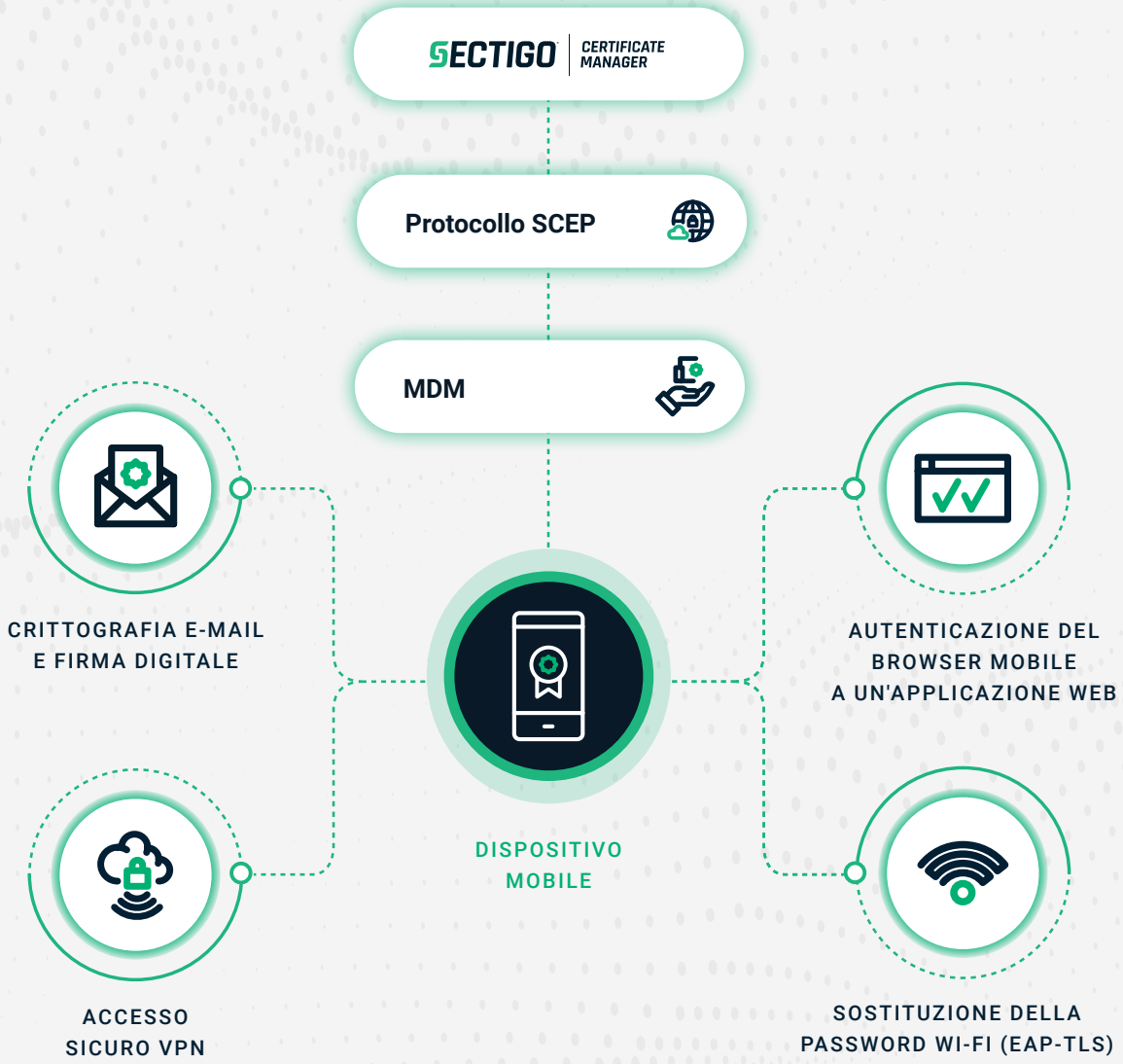
Server Web/Attrezzatura di rete/Strumenti DevOps		Scelta del cliente			
Tipo	**Piattaforma**	**Sectigo Installation Agent**	**ACME**	**Sectigo REST API**	**Integrazione personalizzata**
Server Web	Apache HTTP Server	Sì	Sì	Disponibile	
	Apache Tomcat	Sì	Sì	Disponibile	
	IIS	Sì	Sì	Disponibile	
	NGINX		Sì	Disponibile	
	Altri server Web supportati da Certbot		Sì	Disponibile	
Load Balancer	F5	Sì	Sì	Disponibile	Sì
	Citrix ADC (precedentemente NetScaler)		Sì	Disponibile	Sì
Gestione dei servizi IT	ServiceNow			Disponibile	Sì
Strumenti DevOps	Ansible			Disponibile	
	AWS ELB		Sì	Disponibile	
	Chef			Disponibile	
	Docker			Disponibile	
	HashiCorp Vault			Disponibile	
	Jenkins			Disponibile	
	Kubernetes		Sì	Disponibile	
	Puppet			Disponibile	
	SaltStack			Disponibile	
	Terraform			Disponibile	

Automatizzazione dell'installazione di certificati non SSL

Molti sistemi, applicazioni e dispositivi utilizzano certificati non SSL, ad esempio i certificati di identità per dispositivi mobili. Per l'installazione di certificati non SSL, Sectigo fornisce:

- **Iscrizione al protocollo Secure Transport (EST):** Sectigo supporta il protocollo EST, che viene utilizzato per la gestione delle apparecchiature di rete di molti fornitori. In effetti, numerosi fornitori hanno il supporto EST già integrato. EST è anche popolare negli ambienti Internet delle cose (Internet of Things) (IoT) data l'efficienza del protocollo e il supporto delle chiavi ECC (Elliptic Curve Cryptography). Sectigo offre un client EST commerciale e supporta anche i numerosi client EST open source disponibili.
- **Protocollo di registrazione del certificato semplice (SCEP) (Simple Certificate Enrollment Protocol):** SCEP esiste da quasi due decenni e ha acquisito un notevole interesse presso le aziende. Poiché il protocollo SCEP non prevede costi di licenza e richiede pochissimo tempo per la configurazione e l'esecuzione da parte delle squadre IT, è diventato un componente quasi onnipresente della sicurezza aziendale. I sistemi di gestione dei dispositivi mobili (MDM) (Mobile Device Management) come Microsoft Intune e AirWatch utilizzano SCEP per la registrazione dei certificati PKI. Ciò consente ai dispositivi mobili di sostituire la password Wi-Fi e di autenticarsi per VPN. La maggior parte delle apparecchiature di rete, inclusi router, load balancers, hub Wi-Fi, dispositivi VPN e firewall, supportano anche il protocollo SCEP per la registrazione dei certificati.

Figura 4 – SCM utilizza SCEP per passare i certificati all'MDM che li installa nel dispositivo mobile



Nell'ambiente Sectigo, SCEP può essere utilizzato per registrare certificati in Linux, MacOS e altri sistemi operativi.

- **Microsoft Agent:** un server Sectigo Proxy può trovarsi tra il desktop Microsoft e il servizio certificati Active Directory. Intercetta le richieste di certificato effettuate tramite il protocollo di Windows WCCE (Windows Client Certificate Enrollment Protocol - Protocollo di registrazione del certificato client Windows) e fornisce automaticamente il certificato al desktop senza alcun intervento da parte dei dipendenti.
- **Sectigo Mobile Certificate Manager (MCM):** Sectigo MCM emette e gestisce certificati e chiavi su dispositivi mobili iOS, Chrome OS e Android con un intervento minimo o nullo da parte dell'utente. Supporta tutti i tipi di certificato ed è interoperabile con tutti i principali dispositivi, sistemi operativi e protocolli di registrazione. Sectigo utilizza un MDM integrato nel nostro Certificate Manager o un approccio di portale web self-service, a seconda delle esigenze del cliente.

Automatizzazione dell'installazione dei certificati emessi da ADCS

Utilizzando il servizio di certificazione Active Directory (ADCS) di Microsoft, gli amministratori IT possono ordinare a tutti i desktop e i server di registrare e rinnovare automaticamente i certificati emessi dai servizi di certificazione di Active Directory. Ma questa automazione si applica solo alle applicazioni che utilizzano un sistema operativo Windows. Le aziende odierne dispongono di dispositivi che non utilizzano i sistemi operativi Microsoft, il che significa che l'amministratore e il dipendente condividono l'onere di rinnovare e installare manualmente i certificati per qualsiasi applicazione o dispositivo non Microsoft. Per questi certificati, gli amministratori spesso impiegano un metodo soggetto a errori utilizzando fogli di calcolo per tenere traccia manualmente di quando sono stati emessi i certificati, dove sono stati installati, la loro forza crittografica, quando scadono e chi ne è responsabile.

Sectigo offre queste opzioni:

- Continuare a utilizzare ADCS come CA principale, definire Sectigo come CA che emette i certificati e installa automaticamente i certificati nel dispositivo o nell'applicazione. L'azienda non ha bisogno di incorporare nuovamente la CA radice.
- Continuare a utilizzare ADCS come CA che emette i certificati. Il gestore dei certificati Sectigo rileverà i certificati emessi da ADCS, riferirà sugli attributi/proprietà dei certificati e invierà notifiche prima della scadenza.
- Sostituire sia la radice ADCS che la CA emittente con la CA Sectigo. Ciò elimina il costo di gestione di ADCS, automatizzando completamente l'emissione e l'installazione dei certificati.

ADCS non può installare automaticamente i certificati per molti casi d'uso aziendali comuni, tra cui:

- Server Web
- Dispositivi mobili Apple, Android, Chromebook, senza un sistema di gestione dei dispositivi mobili
- Azure key vault
- Identità di persone o dispositivi non presenti in Microsoft Active Directory
- Load balancers
- Attrezzatura di rete
- Firma codice
- Container DevOps
- Autenticazione degli amministratori di server che utilizzano SSH
- Garanzia affidabilità pubblica/Estensioni multiuso della mail Internet (S/MIME)
- Firma di documenti attendibile da Adobe Reader, Adobe Sign
- Dispositivi Internet delle cose
- Possibilità di fornire la stessa cronologia della chiave di crittografia a tutti i dispositivi di proprietà dello stesso utente

Sectigo Certificate Manager potenzia gli ADCS automatizzando l'installazione dei certificati, eliminando la necessità di una gestione manuale costosa e soggetta a errori. Certificate Manager garantisce che i certificati aziendali siano gestiti correttamente e non scadano inaspettatamente.

Conclusione: Ottieni la tranquillità automatizzando PKI con Sectigo

PKI è la migliore tecnologia per eliminare le password e garantire che solo i dispositivi e gli utenti autorizzati accedano ai sistemi aziendali.

Sectigo ha aperto la strada a SSL e alle tecnologie correlate ed è ora leader mondiale nella PKI. Sectigo continua a investire in nuove tecnologie, standard e soluzioni per rimanere all'avanguardia della sicurezza e proteggere la tua azienda dalle minacce digitali.

Con Sectigo, ottieni di più:

Scelta

Con la filosofia di base di Sectigo sull'interoperabilità e l'uso di standard aperti come ACME, SCEP ed EST come nostra base, puoi essere certo che avrai un ampio grado di scelta e controllo sulla tua soluzione PKI. E se qualcosa dovesse andare storto, hai un unico punto di contatto 24 ore su 24, 7 giorni su 7.

Facilità d'uso

A differenza di altre società, Sectigo è concentrata sull'identità digitale, sia come CA pubblica che come fornitore leader di PKI privata. Sfruttando la nostra automazione della distribuzione dei certificati e le tecnologie di gestione/report di un unico pannello di controllo per centralizzare e semplificare le attività noiose associate alla gestione del ciclo di vita dei certificati, sarai in grado di liberare il tuo team per concentrarti su attività di valore più elevato.

Valore

Secondo il modello di licenza Sectigo, non addebitiamo per emissione, ma piuttosto per utilizzo. I certificati che non sono più in uso (ad esempio, quando qualcuno lascia la tua azienda) possono essere trasferiti.

Pronti per il futuro

Sectigo è la principale CA commerciale del mondo e investiamo costantemente in nuove tecnologie e soluzioni. Quando collabori con noi, puoi stare certo che la tua azienda rimarrà all'avanguardia della crittografia man mano che le tue esigenze cambiano e crescono. Le nostre tecnologie automatizzate garantiranno l'agilità crittografica per adattarsi ai progressi nelle tecniche informatiche e crittografiche che richiedono aggiornamenti agli algoritmi di hashing e crittografia.

Tranquillità

Tutto ciò porta a una maggiore tranquillità. Sectigo è conforme a WebTrust e SOC 3, e le nostre connessioni con CA/Browser Forum ed enti governativi selezionati ci aiutano a garantire che riceviamo avvisi tempestivi sui problemi di sicurezza PKI. Inoltre, il nostro approccio open source aiuta a ridurre le vulnerabilità della sicurezza. Con le dimensioni, la scalabilità, la leadership e il continuo investimento di Sectigo in PKI, non esiste partner migliore per proteggere le fondamenta della tua infrastruttura digitale.

Sectigo è un leader tecnologico nella sicurezza informatica che fornisce soluzioni di identità digitale, inclusi certificati TLS/SSL, sicurezza web, DevOps, IoT e gestione PKI di livello aziendale. In qualità di autorità di certificazione commerciale più grande del mondo, con oltre 700.000 clienti in tutto il mondo e 20 anni di esperienza nella fornitura di soluzioni di fiducia online, Sectigo fornisce comprovate soluzioni di fiducia pubbliche e private per la protezione di server Web, identità digitali, dispositivi connessi e applicazioni. Riconosciuta per le sue innovazioni pluripremiate e il migliore supporto globale ai clienti, Sectigo fornisce le tecnologie necessarie per proteggere i panorami digitali di oggi e di domani.

Per maggiori informazioni, visitare www.sectigo.com e seguire @SectigoHQ