Cambiare il provider del servizio di gestione SSL

Smitizzare le preoccupazioni e le aspettative negative sul processo e sulle impostazioni richieste nel passaggio

GLOBALSIGN - LIBRO BIANCO

GlobalSign®

www.globalsign.it

INDICE

INTRODUZIONE

Passare a una nuova Autorità di certificazione per i propri certificati SSL non è un processo semplice, ma non è neanche così complicato come l'Autorità di certificazione attuale sembra voler suggerire. La chiave per realizzare il passaggio con successo e con il minimo sforzo risiede nelle aspettative e nella preparazione, riconoscendo con chiarezza quali sono tutti gli aspetti coinvolti in termini di risorse e costi.

In questo white paper vengono descritte tutte le fasi del processo di passaggio a una nuova Autorità di certificazione, fin dallo stadio iniziale di conoscenza dell'ambiente in essere, passando per la valutazione delle esigenze da soddisfare e la stima dei costi.

FASE 1 – PASSARE IN RASSEGNA CIÒ CHE SI HA

Quando si prende in considerazione il cambio del provider del servizio SSL gestito, il primo passo da compiere consiste nel fare un esame dell'utilizzo attuale di SSL e dell'ambiente operativo in essere. È necessario sapere bene cosa si ha attualmente per poter stabilire delle aspettative ragionevoli sui costi e sul tempo che saranno richiesti per il passaggio.

"Interruzioni del servizio dovute alla scadenza non prevista di un certificato hanno un impatto sulla disponibilità del servizio, sulle prestazioni sottoscritte nello SLA, sull'attendibilità nel brand e sulla fiducia di clienti, partner e su tutti coloro che si affidano all'azienda. Inoltre possono condurre a situazioni di non conformità con le normative in vigore e con altri requisiti".[1]

INVENTARIO DEI CERTIFICATI

Come prima cosa, determinare la posizione dei certificati esistenti così da sapere cosa occorrerà sostituire dopo aver completato il passaggio. Le grandi aziende spesso hanno molti certificati SSL attivi nei loro ambienti operativi. Se durante la transizione non vengono trovati tutti i certificati, questi possono scadere e causare perdite di copertura, possibili interruzioni della rete e problemi di compliance.

L'inventario dei certificati che ne risulterà dipenderà dalla storia degli ordini dell'organizzazione e dal fatto che si utilizzino o meno Autorità di certificazione multiple.

CERTIFICATI DI AUTORITÀ DI CERTIFICAZIONE MULTIPLE

Ci sono diverse ragioni per le quali si possono avere certificati provenienti da più Autorità di certificazione:

- Persone o reparti diversi acquistano certificati separatamente da provider di servizi diversi.
- Fusioni e acquisizioni di organizzazioni che si affidavano ad Autorità di certificazione diverse.

Lavorare con più Autorità di certificazione complica la stesura di un inventario accurato. Fortunatamente è possibile utilizzare appositi strumenti di rilevamento dei certificati per indicizzare la rete e scovare tutti i certificati esistenti, indipendentemente da chi li ha emessi. In questo modo si otterrà un elenco completo a cui fare riferimento nel momento della migrazione a una nuova Autorità di certificazione.

CERTIFICATI DA UN'UNICA AUTORITÀ DI CERTIFICAZIONE

Se si è certi che tutti i certificati SSL esistenti nella propria organizzazione siano stati emessi dalla stessa Autorità di certificazione, scaricare l'elenco di tutti i certificati dall'account relativo a questa CA. In questo modo si potrà disporre di un registro di tutti gli acquisti precedenti, senza doversi affidare all'account precedente per tutto il processo di migrazione.

IDENTIFICAZIONE DEGLI AMMINISTRATORI

Identificare i membri del team che gestiranno il nuovo account. Sarà necessario formare queste persone alla nuova interfaccia grafica. Conteggiare il tempo di formazione nella programmazione complessiva della transizione.

IDENTIFICAZIONE DI SERVER E APPLICAZIONI

Stimare il numero e il tipo di server e di applicazioni su cui sono installati certificati, in modo da sapere esattamente cosa succederà al momento dell'effettivo passaggio. A seconda del tipo di server, ad esempio, può essere necessario effettuare delle sostituzioni manuali di root.

FASE 2 – DETERMINARE LE ESIGENZE DA SODDISFARE

Una volta determinato esattamente su cosa si sta lavorando, è possibile passare a esaminare gli aspetti logistici coinvolti nel passaggio.

Le organizzazioni sono spesso frenate dal cambiare Autorità di certificazione a causa di un'idea sbagliata rispetto a quanto il processo possa essere dispendioso in termini di tempo e fatica. Tuttavia, avere un quadro completo e accurato dell'ambito che sarà coinvolto rende la migrazione più chiara e la mostra per quella che effettivamente è, cioè un'operazione tranquillamente fattibile.

Esaminiamo cosa occorre effettivamente fare per rendere la transizione più semplice e scorrevole possibile.

IMPARARE LA NUOVA INTERFACCIA UTENTE

Occorrerà tenere in considerazione un tempo di formazione nella programmazione delle tempistiche del passaggio. Per questo motivo occorre sapere quanti utenti si avranno e quali saranno i loro ruoli e le loro responsabilità. L'amministratore degli account può richiedere una formazione maggiore rispetto a coloro che saranno responsabili solo di inviare gli ordini.

STABILIRE UNA STRATEGIA DI RINNOVO

Prima di cambiare provider SSL, è opportuno ideare un piano ben preciso per la gestione dei rinnovi dei certificati. Quando si sceglie una nuova Autorità di certificazione, è consigliabile informarsi dettagliatamente sui criteri di sostituzione dei certificati adottati. La nuova Autorità di certificazione deve essere in grado di accettare entrambi i metodi seguenti.

MODELLO BASATO SULLA TRANSIZIONE

Una delle possibilità consiste nell'adottare un approccio al rinnovo basato sui singoli certificati, sostituendoli uno alla volta all'avvicinarsi della loro scadenza. Fare in modo di avere a disposizione rapporti accurati sui certificati e accertarsi che la responsabilità della gestione dei rinnovi sia assegnata al giusto membro del team. Utilizzando questo modello si impiega meno tempo nell'installazione dei certificati durante il periodo iniziale del passaggio, ma occorre prestare estrema attenzione nel monitoraggio delle date di scadenza finché tutti i certificati non sono stati rinnovati con il nuovo account di gestione.

MODELLO BASATO SULLA SOSTITUZIONE RADICALE

Si può anche scegliere di sostituire tutti i certificati in una sola volta. L'adozione di questo approccio richiede un investimento iniziale in termini di tempo e risorse per sostituire tutti i certificati esistenti insieme, ma non ci si dovrà più preoccupare di monitorare i vecchi certificati per il resto della loro vita utile e non sarà più necessario doversi affidare a piattaforme di gestione diverse.

L'Autorità di certificazione scelta avrà certamente modo di compensare il tempo rimanente alla scadenza di un certificato estendendo il periodo di validità di quello nuovo.

"Per usi esterni è preferibile affidarsi ai provider di certificati più affidabili, attendibili e ben conosciuti al pubblico grazie a un brand noto, in particolare quelli orientati ai clienti più sensibili ai rischi". [2]

"Negoziare sul prezzo quando l'infrastruttura PKI sarà utilizzata solo per supportare crittografia SSL/TLS, ma riconoscere i requisiti necessari per gestire i certificati di crittografia sul lungo termine". [2]

USO INTERNO E USO ESTERNO

Le caratteristiche e i livelli di sicurezza dei certificati variano in base all'Autorità di certificazione. Esaminare l'offerta dei certificati della nuova Autorità di certificazione e identificare di quali prodotti si ha bisogno in base alle proprie esigenze di utilizzo.

- Per siti rivolti al pubblico, il certificato SSL fornisce al visitatore la prova che il sito è legittimo ed attendibile. La sicurezza di questi siti deve essere garantita da un certificato di qualità, emesso da un brand con un'ottima reputazione.
- Per siti interni, dove si ha bisogno solo di funzionalità di crittografia, è possibile utilizzare un certificato più spartano.

DETERMINARE L'AMBITO DI UN'EVENTUALE INTEGRAZIONE DELL'API

Se si utilizza l'integrazione dell'interfaccia API con l'Autorità di certificazione attuale, sarà necessario creare un'integrazione simile con la nuova Autorità di certificazione.

La nuova Autorità di certificazione dovrà disporre di adeguata documentazione dell'API e fornire l'assistenza e la guida necessarie durante tutto il processo di migrazione. Conteggiare il tempo di configurazione della nuova API nella programmazione complessiva del progetto.

NON PREOCCUPARSI DELLE LEGGENDE CHE HANNO LO SCOPO DI SCORAGGIARE LE AZIENDE

Spesso le organizzazioni rinunciano a cambiare Autorità di certificazione perché dissuase da una quantità più o meno corposa di percezioni negative. Di seguito elenchiamo quelle più comuni.

"LA DISTRIBUZIONE DI ROOT E ICA È TROPPO DIFFICOLTOSA"

Una delle scuse più comuni per restare con la vecchia Autorità di certificazione è che non si ha intenzione di affrontare lo scomodo processo di distribuzione delle nuove root e ICA dell'Autorità di certificazione. In realtà il processo è abbastanza ordinario, sebbene possa avere un certo impatto sulla pianificazione.

- Se i criteri di gestione dei cambiamenti dell'IT consentono di installare root in qualsiasi momento, è possibile installare le root quando si installa il certificato dell'entità finale. La maggior parte dei vendor forniscono tutti i componenti della catena di certificati necessari come parte del processo di completamento dei certificati dell'entità finale.
- Se il processo di gestione dei cambiamenti è più stringente, la distribuzione dell'ICA può avere un impatto sui tempi programmati per il passaggio. Ad esempio, se ci sono finestre di manutenzione specifiche nelle quali eseguire i cambiamenti dell'IT, può essere necessario pianificare il cambio di Autorità di certificazione in modo da considerare questo aspetto.

Dato che i certificati SSL/TLS sono basati su uno standard comune (X. 509 v3), il processo di richiesta e installazione dei componenti della catena di certificati è *esattamente uguale* tra un vendor a quello successivo.

"L'AGGIORNAMENTO MANUALE DEI PERCORSI OCSP È PROIBITIVO"

Un'altra leggenda molto comune sul passaggio a una nuova Autorità di certificazione è che ciò richiederà la sostituzione manuale dei percorsi CRL e OCSP quando inizierà l'emissione dei certificati da parte della nuova Autorità di certificazione. Se l'organizzazione utilizza solo certificati su server Web, non ci si dovrà preoccupare di questo aspetto.

Ogni certificato SSL emesso deve contenere un collegamento al CRL dell'Autorità di certificazione emittente; non sarà necessario eseguire alcuna operazione in merito a questa questione. Se si hanno istanze non correlate a server Web, allora può essere necessario sostituire manualmente il percorso di revoca. Ecco perché è importante sapere come sono utilizzati i propri certificati.

FASE 3 – STIMA DEI COSTI

Una volta che si conoscono anche sommariamente quali sono gli aspetti coinvolti nel cambio del provider, è possibile passare a valutare i costi.

SPESE IN CONTO CAPITALE (CAPEX)

Tra le spese una-tantum in conto capitale ci possono essere l'acquisto di uno strumento di rilevamento dei certificati, i servizi di gestione dei certificati e il lavoro impiegato nel processo di integrazione dell'API.

STRUMENTO DI RILEVAMENTO DEI CERTIFICATI

Se si hanno certificati provenienti da più Autorità di certificazione può essere preferibile utilizzare uno strumento di rilevamento appositamente ideato per fare l'inventario dell'uso dei certificati. Spesso questo servizio viene offerto gratuitamente insieme ai servizi di gestione certificati illustrati di seguito.

"Nelle organizzazioni che utilizzano un numero di certificati pari o superiore a circa 200 certificati X.509 documentati vi è l'alto rischio di scadenze impreviste e di certificati acquistati ma non distribuiti. Queste organizzazioni devono avviare al più presto un processo di rilevamento formalizzato". [1]

SERVIZI DI GESTIONE DEI CERTIFICATI

L'Autorità di certificazione scelta dovrebbe offrire una piattaforma di tipo SaaS attraverso cui gestire il ciclo di vita dei certificati e che consente agli account manager di ordinare, rinnovare ed emettere certificati, nonché di eseguire altre funzioni di gestione quali la fatturazione e la creazione di rapporti.

Se la propria organizzazione gestisce un gran numero di certificati, adotta una strategia multi-vendor, utilizza certificati autofirmati o è alla ricerca di una maggiore convenienza e automazione nella gestione di certificati SSL, può essere preferibile investire in un software locale aggiuntivo per la gestione delle chiavi. Questi servizi combinano la funzione di inventario con la capacità di fornire certificati, collegandosi direttamente alle API delle principali Autorità di certificazione attraverso "connettori" preconfigurati. È possibile gestire il ciclo di vita dei certificati (ad esempio l'emissione e la sostituzione di certificati) da una singola piattaforma, senza dover accedere al sistema di gestione di ogni singola Autorità di certificazione.

Questi servizi possono inoltre agevolare il rispetto delle normative di conformità (compliance) cercando tutti i certificati presenti nella rete ai fini delle best practice crittografiche, quali ad esempio gli aspetti legati alle dimensioni delle chiave e agli algoritmi di hashing. I servizi possono avvisare l'utente nel caso di certificati che non soddisfano gli standard di sicurezza e facilitarne la sostituzione come parte del servizio offerto.

INTEGRAZIONE DELL'API ESISTENTE

Se si utilizza un'API con l'Autorità di certificazione attuale, tenere conto dei costi di sviluppo necessari per aggiornare il codice al fine di integrare l'API della nuova Autorità di certificazione.

INTEGRAZIONE DELLA NUOVA API

Molte Autorità di certificazione offrono l'integrazione dell'API, grazie alla quale è possibile automatizzare la gestione dei certificati attraverso funzionalità quali:

- Automazione dell'emissione dei certificati
- Ordinamento mediante portali interni

- Gestione di rapporti granulari sull'utilizzazione

Se si desidera automatizzare queste funzionalità, discutere il flusso di lavoro auspicabile e le funzioni desiderate con la nuova Autorità di certificazione. Conteggiare nei costi del primo anno l'eventuale impiego di tempo e risorse per lo sviluppo interno.

SPESE OPERATIVE (OPEX)

Dalla prospettiva operativa quotidiana, è necessario tenere conto del tempo che sarà necessario agli utenti dell'account per familiarizzare con la nuova piattaforma di gestione, inclusa la configurazione di rapporti, la delega delle responsabilità e così via. Il tempo di formazione varierà in base alle responsabilità degli individui.

"Anche se i costi sono uno dei fattori principali, anche qualità del servizio e servizi inclusi nel pacchetto sono aspetti da tenere in considerazione".[3]

"I costi dei certificati dovrebbero pesare per un 70% nella decisione, mentre i fattori tecnici e di fiducia per il restante 30%".[3]

COSTI ANNUALI DEI CERTIFICATI

Nella valutazione di diverse Autorità di certificazione, è consigliabile considerare il costo di singoli prodotti insieme al valore che questi offrono in termini di caratteristiche e funzionalità, inclusi:

- Eventuali costi aggiuntivi per la riemissione o l'installazione di certificati tra più server
- Eventuali servizi aggiuntivi forniti a corredo con il certificato, come ad esempio il monitoraggio di malware e phishing
- La natura del certificato stesso (ad esempio, emesso da root a 2048 bit)

Ogni Autorità di certificazione commercializza i propri certificati in modo differente. Esaminare la linea dei prodotti per accertarsi che il certificato soddisfi le proprie necessità e non includa add-on premium non necessari, come ad esempio SGC (Server Gated Cryptography).

FASE 4 – CONSIDERARE IL PASSAGGIO A GLOBALSIGN

Quando si confrontano diversi provider di SSL gestito, è importante tenere sempre presente che "si sta scegliendo un partner dell'azienda, non un prodotto; questa relazione va ben oltre l'offerta di un prodotto pacchettizzato, poiché si dipenderà da loro per molto tempo dopo l'emissione dei certificati".[4]

Oltre a fornire la sicurezza più elevata e i certificati SSL più ricchi di funzionalità, l'Autorità di certificazione scelta deve essere in grado di:

- Aiutare il cliente con ambienti personalizzati.
- Consigliare il cliente sulle iniziative relative alla sicurezza.
- Creare delle raccomandazioni in base alle esigenze aziendali del cliente.
- Fornire al cliente gli strumenti per verificare che la configurazione dei suoi server Web sia stata ottimizzata per la massima sicurezza.

"La sicurezza non finisce quando si conclude la vendita di una tecnologia. I provider devono offrire un supporto costante su prodotti e servizi che consenta ai loro clienti di massimizzare il valore delle loro soluzioni, incrementandone l'efficacia in un panorama in cui le minacce si evolvono costantemente. GlobalSign è l'Autorità di certificazione che si trova nella posizione migliore per comprendere le esigenze degli amministratori dei siti Web in merito alla configurazione di SSL e alla risoluzione delle questioni legate alla sicurezza".[5]

Le organizzazioni scelgono GlobalSign per il suo impegno nel fornire soluzioni leader per i certificati digitali e per la sua attendibilità come partner di massima fiducia. GlobalSign è una delle più grandi Autorità di certificazione orientate alle aziende e impiega team di specialisti in tutto il mondo per fornire assistenza ai propri clienti. Le sue soluzioni sono costruite attorno alle necessità dei clienti e alle best practice industriali.

IL VANTAGGIO DI SCEGLIERE GLOBALSIGN

GlobalSign investe costantemente nel rendere più sicuri e intuitivi i certificati SSL. La storia dell'azienda è caratterizzata da una leadership continua:

- Ha iniziato a utilizzare root a 2048 bit sin dal 1998, molto tempo prima delle raccomandazioni delle best practice
- È stata la prima nel settore a introdurre servizi di revoca dei certificati in IPv6

L'azienda è costantemente impegnata ad aggiornare la sua piattaforma di gestione e a sviluppare partnership chiave. Le innovazioni e le partnership hanno dato a GlobalSign importanti vantaggi rispetto ad altre Autorità di certificazione.

"Combinando la nostra tecnologia Web avanzata e l'approccio a SSL di GlobalSign, orientato al futuro, i clienti di GlobalSign e i quelli di CloudFlare potranno superare la concorrenza offrendo agli utenti un'esperienza sicura, avanzata e veloce".[6]

PAGINE CARICATE PIÙ VELOCEMENTE

Ogni volta che un browser si connette a un sito sicuro, lo stato del certificato SSL del sito deve essere verificato tramite l'Autorità di certificazione che l'ha emesso. Il tempo impiegato in questo processo (risposta OCSP o recapito CRL) dipende dall'efficienza dell'infrastruttura dell'Autorità di certificazione e dalla posizione dell'utente rispetto all'Autorità di certificazione.

GlobalSign ha una partnership con l'azienda specialista nelle prestazioni delle reti, CloudFlare, per tratte vantaggio dalla sua infrastruttura globale e recapitare richieste di stato dei certificati veloci e affidabili. In questo modo, le risposte OCSP/CRL sono state accelerate da 6 a 10 volte. Un caricamento più veloce delle pagine aiuta a fidelizzare i visitatori e gioca un ruolo importante nel migliorare l'ottimizzazione per i motori di ricerca (SEO).

"Configurare correttamente SSL è un passo importante nello sfruttamento di tutti i vantaggi di questo protocollo di sicurezza. Tuttavia, spesso è difficile per gli amministratori trovare una guida esauriente che lo agevoli nel raggiungimento di questo obiettivo. Il nostro lavoro insieme a GlobalSign consiste nell'affrontare questa necessità e nel rendere Internet un luogo sicuro per tutti". [7]

MAGGIORE DISPONIBILITÀ

La maggior parte delle Autorità di certificazione si affida a un singolo POP (Point Of Presence) del proprio data center per servire le risposte OCSP e recapitare CRL. Se questo va offline si possono verificare importanti interruzioni, con i visitatori esterni che ricevono avvisi di sicurezza e le appliance interne che non possono comunicare. GlobalSign utilizza 23 ubicazioni per i data center, dislocate in tutto il mondo, per evitare tale rischio.

SICUREZZA CONTINUA PER I SITI WEB

SSL di GlobalSign è molto più di un semplice lucchetto. È una soluzione che tiene sicuro il sito Web e lo protegge continuamente.

- Lo strumento di controllo online della configurazione SSL consente di testare un dominio alla ricerca delle oltre trenta problematiche e

vulnerabilità SSL più comuni e fornisce la guida operativa per porvi rimedio.

- Il servizio avvisi di phishing offerto in collaborazione con Netcraft avvisa i responsabili dei siti se questi sono stati designati per azioni di phishing.
- Il monitoraggio del malware offerto in collaborazione con StopTheHacker avvisa i responsabili dei siti in merito a minacce malware conosciute e sconosciute.

"Dopo aver acquistato un certo numero di certificati SSL con il servizio Gestione SSL di GlobalSign, posso dire di aver trovato l'intero processo enormemente più semplice ed efficace rispetto al mio precedente provider di certificati SSL". [8]

GESTIONE DEI CERTIFICATI DELLE AZIENDE

Il servizio Gestione SSL basato su SaaS di GlobalSign gestisce i certificati dell'intera organizzazione. La piattaforma di SSL gestito è stata pensata per aiutare le imprese, anche le più grandi, a ridurre significativamente budget, tempi e costi di gestione associati all'uso di SSL. Grazie alla verifica "one-time", gli amministratori possono emettere su richiesta l'ampia gamma di certificati SSL, dai più economici certificati di crittografia ai certificati EV SSL ad alta garanzia, 24 ore al giorno, 7 giorni su 7, 365 giorni all'anno.

Il servizio può essere personalizzato per soddisfare le esigenze dell'organizzazione, con termini aziendali flessibili quali:

- Licenze di emissione illimitata di certificati.
- Depositi per acquisti in blocco.
- Possibilità di aggiungere utenti, domini e profili illimitati.
- Robusti strumenti di gestione e creazione rapporti.

È possibile integrare il servizio Gestione SSL negli ambienti Microsoft Windows per poter sfruttare la comodità di utilizzare Active Directory per fornire i certificati. L'integrazione supporta l'iscrizione automatica e le installazioni silenti e riduce il tempo e i costi operativi associati all'esecuzione di un'Autorità di certificazione locale.

GESTIONE DEGLI ACCOUNT DEDICATA

Tutti i clienti del servizio Gestione SSL di GlobalSign hanno un Account Manager dedicato, una persona da contattare quando occorre aiuto. Disponibile via telefono, Web ed e-mail, l'Account Manager può assistere nella scelta dei prodotti, fornire assistenza in merito a problematiche nel ciclo di vita dei certificati e discutere delle iniziative di sicurezza che l'organizzazione intende intraprendere.

SICUREZZA OPERATIVA

Le organizzazioni si affidano ai certificati SSL per promuovere la reputazione del brand, aumentare la fiducia degli utenti finali e proteggere le informazioni sensibili dell'organizzazione e dei visitatori del sito. Negli anni, GlobalSign si è guadagnata il riconoscimento e la fiducia del settore:

- GlobalSign è stata una delle prime Autorità di certificazione a utilizzare le ICA e a mantenere una root offline per ridurre al minimo il rischio di esporre l'Autorità di certificazione root agli attacchi. Oggi questa è una best practice di sicurezza ordinaria.
- WebTrust è uno standard di auditing per le Autorità di certificazione che emettono certificati pubblici. GlobalSign ha sempre soddisfatto la conformità dell'auditing WebTrust, conseguita ogni anno sin dal 2001.
- GlobalSign è membro fondatore del CA/B Forum e del CA Security Council.
- È membro sia della Online Trust Alliance che dell'Anti-Phishing Working Group.

Oltre a rispettare le best practice industriali, GlobalSign monitora e protegge la propria infrastruttura con strumenti di sicurezza appropriati e dedicati, raccomandati da consulenti di sicurezza di terze parti.

ELENCO DI CONTROLLO PER IL PASSAGGIO

Di seguito è riportata una raccolta delle considerazioni da fare quando si cambia Autorità di certificazione.

Considerazione	**Perché GlobalSign è la soluzione**
Imparare la nuova interfaccia utente	GlobalSign offre guide e tutorial per gli utenti, disponibili online. Tutti i clienti hanno un Account Manager dedicato da contattare per qualsiasi domanda.
Metodo di rinnovo	GlobalSign accetta sia il modello basato sulla transizione che quello basato sulla sostituzione radicale. Per le organizzazioni che adottano il metodo di sostituzione radicale, GlobalSign aggiunge tutto il tempo rimanente prima della scadenza di un certificato al certificato sostitutivo, in modo da non perdere tempo di vita utile dei certificati precedenti. Le organizzazioni che adottano il metodo di transizione beneficiano della verifica preventiva del dominio, in modo che all'approssimarsi del momento della sostituzione, l'emissione del certificato sia immediata.
Uso interno e uso esterno	GlobalSign è l'Autorità di certificazione che è cresciuta più velocemente in quattro anni, supportando oltre 250 mila domini che si affidano ai suoi certificati SSL, ed è in grado di offrire sia la solida reputazione del brand che ci si aspetta dai siti pubblici e sia la convenienza di opzioni pensate appositamente per l'uso interno.
Costi annuali dei certificati	GlobalSign offre un'ampia gamma di certificati SSL capace di soddisfare qualsiasi utilizzo. Tutti i certificati SSL sono a 2048 bit, possono essere installati su un numero illimitato di server e sono a riemissione gratuita. Si paga solo per ciò che si usa e non è necessario acquistare token o fondi di certificati.
Integrazione dell'API	Che si utilizzi già un'interfaccia API o si abbia l'interesse a integrarne una per la prima volta, gli specialisti di GlobalSign lavoreranno a stretto contatto con voi per garantire che l'integrazione funzioni esattamente come deve.
Sistema di gestione dei certificati	Encryption Director Certificate Manager di Venafi è dotato di un connettore diretto ai servizi dei certificati di GlobalSign.

CONCLUSIONI

Un provider di servizi SSL gestiti dovrebbe offrire più che semplici certificati. La società da scegliere deve offrire tecnologia all'avanguardia, flessibilità nello sviluppo di soluzioni adatte alle proprie esigenze e capacità di consigliare l'organizzazione sui problemi di sicurezza.

GlobalSign ha aiutato decine di organizzazioni a cambiare Autorità di certificazione con successo, incluso il più grande rivenditore degli Stati Uniti. Oltre 250 mila domini sono protetti da GlobalSign e i suoi clienti coprono tutti i mercati verticali, incluso il secondo più grande produttore di automobili e la maggiore compagnia di telecomunicazioni degli Stati Uniti.

Tra le organizzazioni che si affidano a GlobalSign ci sono brand molto noti e di grande attendibilità:

"I prezzi, l'assistenza e la flessibilità del sistema nel complesso e l'approccio alla gestione dei certificati sono straordinari. In ultima analisi, si può dire che GlobalSign rappresenti un approccio gradevole e moderno alla gestione dei certificati SSL. Consiglio vivamente di esaminare la loro offerta".[9]

RICHIESTE RELATIVE ALLA SOLUZIONE DI GESTIONE SSL (MSSL) DI GLOBALSIGN

Per qualsiasi richiesta o domanda relativa al servizio MSSL per la propria azienda, contattare GlobalSign all'indirizzo www.globalsign.it. Saremo lieti di discutere di qualsiasi esigenza o requisiti specifico.

INFORMAZIONI SU GLOBALSIGN

GlobalSign è stata una delle prime Autorità di certificazione e fornisce servizi di credenziali digitali sin dal 1996. Il reparto commerciale è multilingue e gli uffici di assistenza tecnica sono presenti a Londra, Bruxelles, Boston, Tokyo e Shanghai.

GlobalSign ha una storia ragguardevole fatta di grandi investitori, come ING Bank e Vodafone. Oggi GlobalSign fa parte del gruppo GMO Internet Inc., una società per azioni quotata alla prestigiosa Borsa di Tokyo (TSE: 9449), con azionisti del calibro di Yahoo! Japan, Morgan Stanley e Credit Suisse First Boston.

GlobalSign è leader nei servizi per l'attendibilità pubblica, con certificati SSL, Code Signing, identità digitali Adobe CDS, e-mail e autenticazione, soluzioni di identità digitale per aziende, PKI interne e firma root per il Servizio Certificati di Microsoft. I certificati CA trusted root di GlobalSign sono riconosciuti da tutti i sistemi operativi, tutti i maggiori browser per Internet, server Web, client di e-mail e applicazioni Internet, nonché da tutti i dispositivi mobili.

Accreditata per gli standard più elevati

GlobalSign è un'Autorità di certificazione pubblica accreditata da WebTrust ed è membro di Online Trust Alliance, CAB Forum e Anti-Phishing Working Group. Le sue soluzioni core permettono a migliaia di clienti delle aziende di condurre transazioni online protette e di inviare dati in modo sicuro, offrono codice distribuibile a prova di manomissione e sono in grado di collegare le identità a certificati digitali per crittografia di e-mail S/MIME e autenticazione remota a due fattori, come le VPN SSL.

GlobalSign Italia Tél. : +39 02.4070.8276 www.globalsign.it vendita@globalsign.com	**GlobalSign Germania** Tél. : +49 30 8878 9310 www.globalsign.de verkauf@globalsign.com	**GlobalSign Francia** Tél. : +33 1 82 88 01 24 www.globalsign.fr ventes@globalsign.com
GlobalSign Regno Unito Tél. : +44 1622 766766 www.globalsign.co.uk sales@globalsign.com	**GlobalSign Russia** Tél. : +7 (495) 972 46 33 www.globalsign.ru sales@globalsign.com	**GlobalSign Paesi Bassi** Tél. : +31 20 8908021 www.globalsign.nl verkoop@globalsign.com

RIFERIMENTI

1. Gartner, X.509 Certificate Management: Avoiding Downtime and Brand Damage, Eric Ouellet e Vic Wheatman, 4 novembre 2011

2. Gartner, How to Succeed in Revamping Your PKI Program, Brian Lowans ed Eric Ouellet, 4 maggio 2012

3. Gartner, Evaluating SSL Certificates for E-business, Vic Wheatman, 30 agosto 2011

4. Ryan Hurst, CTO di GlobalSign, citato in Salvaging Digital Certificates, Paul Roberts, http://www.darkreading.com/security/application-security/240062664/salvaging-digital-certificates.html

5. Richard Stiennon, celebre autore di soluzioni di sicurezza, speaker e fondatore di IT-Harvest, citato in https://www.globalsign.com/company/press/111512-ssl-configuration-checker-provides-guidance.html

6. Matthew Prince, co-fondatore e CEO di CloudFlare, citato in https://www.globalsign.com/company/press/110112-cloudflare-partnership-accelerates-secure-web-page-load-speed.html

7. Ivan Ristic, Director of Engineering in Qualys, citato in https://www.globalsign.com/company/press/111512-ssl-configuration-checker-provides-guidance.html

8. Richard Sprigg, Dudley Metropolitan Borough Council, citato in https://www.globalsign.com/resources/case-study-dudley-council.pdf

9. Brendan Hourihan, Director of Network and Desktop Support Services, Flagler College, citato in https://www.globalsign.com/resources/case-study-flagler-college-mssl.pdf