CoreStreet
REAL TIME CREDENTIALS

Sistema Distribuito Per Il Controllo Della Validità Dei Certificati Digitali: Prestazioni – Disponibilita' - Costi

Esame delle prestazioni e delle caratteristiche di affidabilità dei sistemi di convalida dei certificati digitali attualmente in uso e presentazione di un sistema distribuito di validazione che serve centinaia di milioni di utenti riducendo i costi di esercizio del 60-80%.

Indice

SISTEMA DISTRIBUITO PER IL CONTROLLO DELLA VALIDITÀ DEI CERTIFICATI DIGITALI: PRESTAZIONI – DISPONIBILITA' - COSTI

Esame delle prestazioni e delle caratteristiche di affidabilità dei sistemi di convalida dei certificati digitali attualmente in uso e presentazione di un sistema distribuito di validazione che serve centinaia di milioni di utenti riducendo i costi di esercizio del 60-80%.

1. Introduzione

Il Governo degli Stati Uniti si sta preparando a estendere su vasta scala le infrastrutture di chiavi pubbliche con attività quali il programma federale di autenticazione elettronica e i vari programmi PKI delle FF.AA e delle agenzie del Dipartimento della Difesa (DoD) quali il Programma KMI [1]; con questi ultimi programmi il numero di utenti è destinato a salire presto da decine a centinaia di milioni. Una volta che l'intera infrastruttura sarà in opera, il numero di applicazioni abilitate con chiave pubblica (PKE) salirà rapidamente per soddisfare la continua richiesta di condurre le transazioni in modo più rapido, più economico e sicuro.

Un fattore critico per il successo di questi programmi sarà costituito dal modo con il quale gli utenti apprezzeranno la prestazione dell'infrastruttura. Gli utenti, infatti, potrebbero rimanere rapidamente delusi dal sistema se le loro applicazioni PKE saranno lente, se saranno costretti ad attendere mentre il sistema esegue i controlli di sicurezza o, peggio, se il sistema diventa indisponibile a causa di una elevato contemporaneo accesso di utenti, un attacco informatico (es. interruzione del servizio) od un guasto fisico che distrugga una parte critica dell'infrastruttura. Scenari come questo possono indurre gli utenti finali a rifiutare l'uso delle loro applicazioni PKE e tornare a lavorare usando mezzi alternativi non sicuri.

Questo documento esamina le prestazioni e le caratteristiche di affidabilità dei sistemi di convalida dei certificati attualmente in uso ed illustra un sistema distribuito di validazione il quale serve centinaia di milioni di utenti e riduce i costi di esercizio del 60-80%.

2. Presentazione del problema della Certificazione

La convalida di un certificato è una funzione che è già stata identificata come avente un impatto significativo sulla prestazioni complessive di una infrastruttura PKI. Poichè la sicurezza di ogni transazione PKI si basa sulle condizioni di validità del momento dei certificati degli utenti collegati, tale stato (valido, revocato o sospeso) deve essere controllato per ogni transazione condotta dagli utenti. Ciò si traduce in un grande volume di operazioni di controllo

[1] Key Management Infrastructure (KMI) è un importante elemento del programma a lungo termine del DoD per concretizzare una strategia di sicurezza delle informazioni su larga scala mediante il vasto impiego di applicazioni con capacità PKI

della validità del certificato. La situazione è ulteriormente complicata dal fatto che la fonte dello stato di validità di ciascun certificato deve essere sicura e, per sistemi su larga scala, a gestione centralizzata.

Allo stato attuale nei programmi PKI federali e del DoD si stanno prendendo in considerazione due possibili sistemi per la verifica della validità dei certificati digitali: le liste di revoca dei certificati (CRL) ed il protocollo di stato di certificato on line (OCSP). E' universalmente riconosciuto che utilizzando il sistema CRL non si possono sostenere milioni di utenti dal momento che tali liste avrebbero le dimensioni di parecchi megabytes; ciò rende il sistema CRL inaccettabile.

Di conseguenza, nella pianificazione e progettazione dei nuovi sistemi PKI si stanno considerando le implicazioni derivanti dall'adozione di sistemi basati sul protocollo di convalida OCSP [2].

Il protocollo OCSP risolve il problema delle dimensioni delle certificazioni presenti nel sistema CRL poiché esso:

- invia solo l'informazione sullo stato del certificato in questione (e non l'intera lista);
- interagisce con l'Autorità di Certificazione (CA) che rilascia le CRL;
- consente una gestione centralizzata dello stato di certificato.

Tuttavia, l'utilizzo di tale sistema comporta un aumento spaventoso del traffico dei dati con critiche ripercussioni ad ogni transazione. Il risultato è il degrado delle prestazioni generali del sistema e la riduzione delle prestazioni dei risponditori di convalida.

Le preoccupazioni riguardanti l'affidabilità e le prestazioni hanno suscitato alcuni quesiti relativi all'impiego dei sistemi con protocollo OCSP:

1) Quanti risponditori OCSP impiegare?
2) Dove mettere i risponditori OCSP?
3) Come meglio sistemare i risponditori OCSP?
4) E, in aggiunta, come può un utente sapere che può fidarsi della risposta che riceve da un risponditore OCSP?

Dal momento che le risposte OCSP sono firmate, ci si deve preoccupare dello stato di sicurezza delle chiavi usate nel processo di firma. La certificazione della firma di un risponditore OCSP non è una cosa semplice (es. chi fornisce la convalida del certificato di firma del risponditore?).

---

[2] L'Online Certificate Status Protocol (OCSP) e' lo standard emergente dell'IETF (Internet Engineering Task Force) destinato al controllo della validita' dei certificati digitali nel corso di una determinata transazione. Prima dell'arrivo di OCSP, i risk manager non avevano a disposizione un sistema per effettuare in modo semplice un duplice controllo sulla validita' di un certificato. OCSP permette invece di condurre queste verifiche in tempo reale, risparmiando tempo e denaro, e fornendo alle attivita' di e-business un sistema piu' rapido, semplice e affidabile per la validazione dei certificati digitali rispetto a quello offerto dal tradizionale scaricamento ed elaborazione delle CRL (Certificate Revocation Lists). Rilasciate dalle Certification Authority (CA), le CRL sono liste di certificati e di possessori non validi.

Le risposte a queste domande dovrebbero basarsi sull'impiego di un'architettura in grado di fornire le migliori prestazioni operative possibili. Dette prestazioni possono essere raggiunte solo se si impiega un sistema ad architettura distribuita il quale consente la convalida dei certificati mediante l'impiego di risponditori ubicati vicini agli utenti senza alcun vincolo ambientale per la loro collocazione. Sfortunatamente, i costi e la complessità dell'architettura distribuita limitano le possibili risposte alle domande di cui sopra; ciò è dovuto al fatto che ciascun server OCSP contiene sia l'informazione di stato di certificato che la chiave privata usata per la firma digitale di ciascun certificato di convalida; le risposte di convalida sono firmate per proteggere la loro integrità il loro transito dal risponditore alle applicazioni dell'utente.

Di conseguenza, ciascun server OCSP deve essere messo in una postazione sicura ed impiegato in maniera sicura da operatori fidati. La sua gestione ed impiego risultano pertanto costosi e complessi paragonabili a quelli, non trascurabili, di messa in opera ed impiego in sicurezza di una infrastruttura CA.

Pertanto, le risposte da dare alle prime tre domande di cui sopra sarebbero:

1) il numero di risponditori da impiegare deve essere limitato;
2) i risponditori devono essere messi in posti sicuri e ad accesso controllato;
3) non c'è una soddisfacente risposta per dove meglio collocare in sicurezza i risponditori anche se si spende molto per proteggerli.

Sintetizzando, le preoccupazione sulla sicurezza portano di nuovo a soluzioni OCSP centralizzate con significativi limiti nelle capacità del sistema di interagire con utenti su vasta scala. In tal modo, prestazioni ed affidabilità del sistema continuano ad essere fortemente penalizzate.

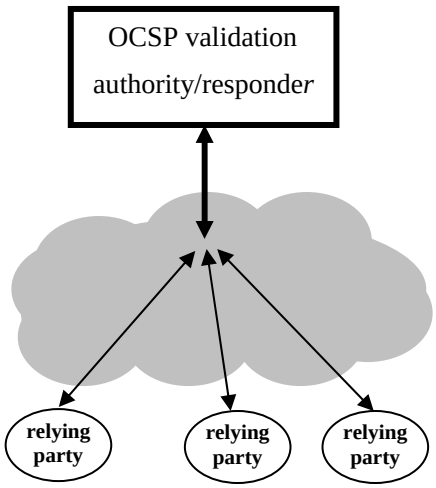

Figura 1 - Architettura OCSP Centralizzata In questa architettura, c'è un'autorità che comunica direttamente con le applicazioni degli utenti per il rilascio dei certificati di validità. Questo sistema centralizzato risulta possedere scarse prestazioni, poca sicurezza e nessuna ridondanza in caso di guasto.

3. Impiego di un'architettura distribuita: un miglioramento decisivo delle prestazioni

Il conseguimento di elevate prestazioni e di alta affidabilità in un ambiente in cui operano milioni di utenti, i quali ottengono informazioni da una o poche fonti, è già stato studiato e

risolto nel mondo commerciale il quale si basa su un'architettura distribuita. La posta elettronica è un buon esempio di architettura distribuita. Un altro esempio è dato dal modo con cui Akamai Technologies Inc. fornisce contenuti web in tutto il mondo.

Akamai ospita contenuti web per oltre 1400 società di e-business d'importanza mondiale su una rete globalmente distribuita di oltre 15.000 servers in 68 Paesi. Si è visto che uno dei fattori prestazionali critici è costituito dal nodo dove le applicazioni Web si interfacciano ad Internet e dalle limitazioni poste dagli apparati di routing e switching i quali costituiscono la spina dorsale dell'Internet". Akamai ha affrontato questo problema spostando il contenuto a cui si deve accede il più vicino possibile agli utenti. I miglioramenti prestazionali ottenuti con questo soluzione sono stati quantificati da Akamai in oltre il 400% [3]. Poiché Akamai non ha le stesse preoccupazioni di sicurezza che devono essere invece insite in un sistema di convalida dei certificati, può essere messo in discussione il fatto che un sistema distribuito possa garantire le migliori prestazioni ed un'elevata affidabilità.

Di seguito sarà illustrato come ciò possa essere raggiunto continuando a soddisfare i requisiti di sicurezza. Prima di tutto saranno esaminate le esigenze in termine di prestazioni.

Una recente analisi indipendente sulle prestazioni di Internet [4] ha concluso che il risultato delle prestazioni, così come percepite dall'utente, crolla non appena la rete diventa congestionata o aumenta la distanza rispetto alla fonte delle informazioni. Nonostante i recenti miglioramenti delle velocità dei processori, l'ottimizzazione dell'impiego del protocollo TCP e la migrazione su linee a velocità 1Mbps o maggiori, le prestazioni della rete sono rimaste costanti a causa del permanere nella rete di fattori di ritardo. Questi ritardi sono causati dal un uso più massiccio della rete e dall'aumentata distanza tra i servers. La figura 2 evidenzia come la percentuale del ritardo nella fornitura di informazioni da un server centrale ad un utente sia cresciuta dal 33% del 1995 al 69% del 1999, con tendenza all'84% nel 2003. La conclusione dello studio è la seguente:

"Non c'è alternativa all'avvicinamento dei contenuti all'utente."

Benché questo studio sia focalizzato sulla consegna di contenuti web a browsers utilizzando Internet piuttosto che alla convalida di certificati mediante applicazioni che usano sistemi di cifratura a chiave pubblica, la conclusione è rilevante anche per questo tipo di sistemi.

---

[3] "A distribuited Infrastructure for e-Business – Real Benefits, Measurable Returns", AKAMAI Technologies, Inc, ©2000"

[4] Sevcik, Peter "Performance Issue facing the World-Wide-Web", Business Communications Review. Volume 29, Number 9.

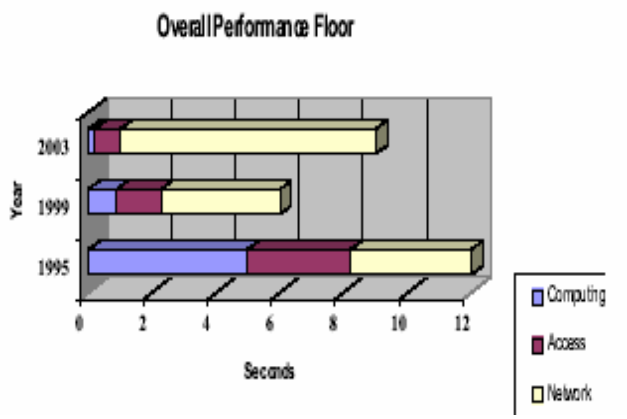

Figura 2 - Aumento del ritardo di rete su Internet Il ritardo nella trasmissione è il fattore di degrado delle prestazioni della rete più notevole e di più rapido incremento.

A seguito di un altro studio [5], Akamai ha apprezzato un miglioramento nella risposta pari al 200% durante improvvisi picchi di traffico utilizzando un'architettura a server distribuiti rispetto alle prestazioni fornite da un'architettura a server centralizzati. (Figura 3).

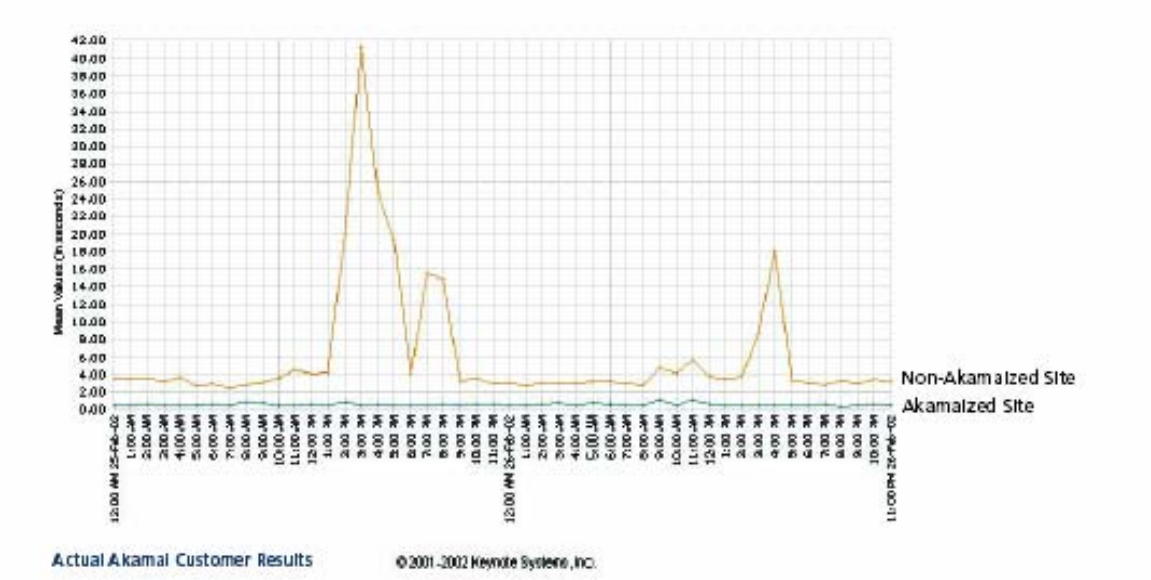

Figura 3 - Ritardi nell'uso della rete con impiego di un'architettura distribuita.

4. La soluzione per un sistema sicuro di convalida dei certificati:

a. Sistema ad architettura distribuita

In un sistema ad architettura distribuita non vi sono vincoli che limitino il numero di risponditori di stato di validità dei certificati né restrizioni circa gli ambienti in cui possono essere sistemati se:

- si predispone la prova di attestazione della validità di ciascun certificato;
- si protegge l'integrità di tali prove così in modo da poterle liberamente distribuire quando necessario.

[5] "Why performance matters", AKAMAI Technologies, Inc, ©2000

La figura 4 mostra un sistema di validazione ad 'architettura distribuita dove un numero significativo di risponditori è stato posizionati vicino alle applicazioni degli utenti senza alcun vincolo nella loro collocazione. Per realizzare ciò, i server non devono contenere informazioni segrete.

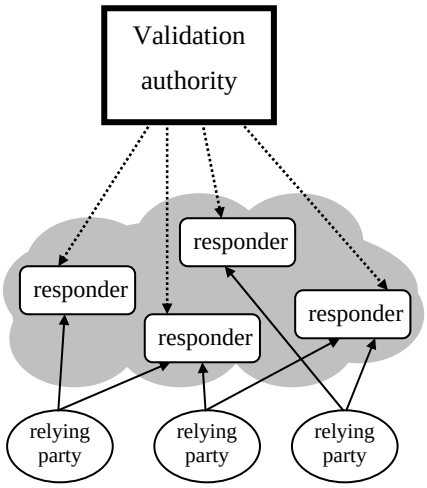

Figura 4 - Architettura OCSP Distribuita. In questa sistema c'è una autorità che controlla il rilascio delle prove di validità e molteplici (illimitati) risponditori, che non contengono dati da mantenere segreti, i quali forniscono le convalide agli utenti.

b. Schema di principio del sistema OCSP ad architettura distribuita

Il principio fondamentale su cui si basa un sistema sicuro di certificazione distribuita è la separazione dei dati di sicurezza sensibili e delle operazioni di sicurezza dal procedimento di consegna dei certificati di validità alle applicazioni degli utenti

In questo sistema, l'autorità di convalida (VA) ritiene tutti i dati sensibili ed effettua tutte le operazioni di sicurezza. Ciò avviene mantenendo una singola autorità di convalida con conseguente alleggerimento delle operazioni di sicurezza e centralizzazione della gestione. Periodicamente, la VA pre-elabora le prove di certificazione individuali, a scadenza limitata, la cui periodicità di pubblicazione (es.ogni ora, quotidianamente, ecc.). è determinata dalle singole politiche di sicurezza L'integrità di queste prove può essere protetta con firma digitale, come avviene nel sistema OCSP tradizionale, oppure usando messaggi di validità (V.Tokens) generati attraverso la tecnica “hashing” che rende la loro integrità auto-validante. Tali certificati possono, quindi, essere liberamente distribuiti, dal momento che essi:

– non richiedono canali di trasmissione sicuri;

– non richiedono sistemi protetti di conservazione.

L'architettura illustrata nella figura 4 evidenzia come i risponditori nel sistema di convalida distribuito non costituiscono un problema per la sicurezza e possono essere sistemati vicino alle applicazioni degli utenti in ambienti non sicuri come un qualsiasi ufficio.

c. Vantaggi del sistema OCSP ad architettura distribuita

I vantaggi del sistema sono numerosi e comprendono:

1) **Scalabilità effettiva**: la possibilità di adattare ed estendere la struttura è assicurata dalla separazione del processo di convalida dalle operazioni di sicurezza associate con il processo di validazione del certificato. Gli ostacoli alla vera scalabilità (risultati, affidabilità, sicurezza e costi) sono stati eliminati.
2) **Affidabilità elevata**: l'elevata affidabilità si ottiene perché le applicazioni degli utenti finali si collegano ad un risponditore locale. Ciò è quello che avviene anche quando si mettono in opera servers di posta elettronica in reti locali per essere più vicini agli utenti ed assicurare una migliore affidabilità.
3) **Prestazioni elevate**: l'architettura di validazione distribuita trae vantaggio dalle lezioni imparate nel mondo commerciale diminuendo la distanza tra l'applicazione dell'utente ed il risponditore eliminando fastidiosi colli di bottiglia ai risponditori, la principale causa di scarse prestazioni.
4) **Disponibilità elevata**: il pericolo di un unico critico fattore di guasto è significativamente ridotto. Gli attacchi multipli volti ad impedire il servizio sono virtualmente eliminati dall'impiego di molteplici risponditori dispersi geograficamente[6]. Gli attacchi fisici alla stessa CA sono altresì inefficaci perché i risponditori continuano ad operare per un certo periodo di tempo il che consentirà di avere un periodo di recupero durante il quale è possibile procedere ad un ripristino on-line della CA (es., se il periodo di validità dei certificati è di 24 ore e vengono rilasciate nuovi certificati ogni 12 ore, ciascun risponditore può continuare a funzionare per almeno 12 ore anche dopo che la CA è stata disabilitata o distrutta. Ciò consente di ripristinarla con copie di back-up prima che gli effetti dell'attacco siano percepiti dall'utenza).
5) **Costo efficacia**: poiché i risponditori non richiedono comunicazioni, collocazioni o modalità operative sicure, il costo associato al loro impiego in forma distribuita su

[6] Il 21 ottobre 2002 un attacco plurimo DoS è stato condotto contro i 13 server DNS che assicurano il transito primario a quasi tutto il traffico Internet. L'attacco, il più massiccio a tutt'oggi, è fallito a causa dell'architettura distribuita dei server di root di Internet, 5 di questi server hanno rilevato l'attacco e sono rimasti disponibili per assicurare il traffico ordinario su Internet durante l'attacco.

vasta scala è basso. In aggiunta, possono essere impiegate piattaforme web server di standard industriale riducendo sensibilmente i costi di messa in opera [7].

6) **Flessibilità e adattabilità:** ciascun risponditore può supportare più di un'autorità certificativa. Ciò permette ad autorità indipendenti di mantenere il controllo completo sul proprio dominio (es. senza lasciare proprie applicazioni o dati ad un'altra autorità) pur condividendo una comune infrastruttura di trasmissione dei certificati.
7) **Capacità di dislocazione elevate:** i risponditori possono essere dislocati nei posti più sperduti del mondo senza che ciò comporti per l'utente un decadimento delle prestazioni dovute a rallentamenti nella rete.
8) **Fattori ambientali:** poiché i risponditori non contengono alcun dato sensibile ai fini della sicurezza, essi possono essere dislocati anche in ambienti dove la minaccia di attcco è reale. L'architettura è anche ideale per scenari suscettibili di varianti repentine dato che è facile ed immediato aggiungere od eliminare risponditori.
9) **Sicurezza elevata:** due fattori di sicurezza sono stati significativamente migliorati rispetto ai sistemi OCSP tradizionali:
   - le richieste di validità dei certificati vanno solo ai risponditori, non all'autorità di validazione. Poiché l'autorità di validazione non consente alcuna comunicazione in entrata dal mondo esterno, la minaccia di un attacco proveniente dall'esterno è virtualmente eliminata;
   - un incremento della struttura di validità per adattarla a bacini di utenza di dimensioni sempre crescenti non richiede una corrispondente ulteriore distribuzione di dati sensibili e di applicazioni sicure. Pertanto ne consegue che la capacità di gestire in sicurezza tali operazioni è fortemente migliorata.

5. La soluzione "Credenziali in tempo reale"

La soluzione "Credenziali in Tempo Reale" (RTC) offre un sistema distribuito di validità dei certificati che può servire alle necessità di centinaia di milioni di utenti con grande affidabilità, alte prestazioni, sicurezza assicurata e minimi costi di messa in opera. L'RTC impiega l'architettura di validazione distribuita descritta nei paragrafi precedenti e supporta sia verifiche di validità a firma digitale che verifiche auto-convalidanti del tipo V-Token.

[7] Vedi l'Appendice B per un confronto dei costi di messa in opera.

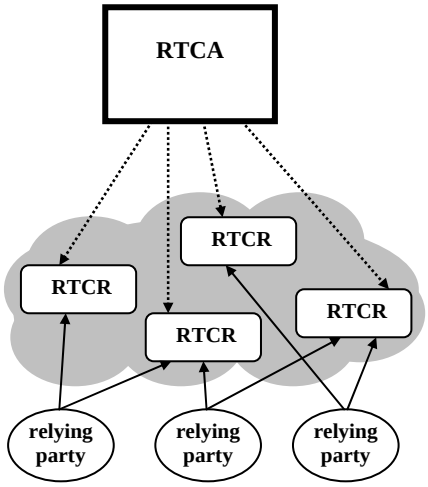

Figura 5 - Architettura RTC Distribuita. Questa soluzione offre scalabilità garantita senza sacrificare prestazioni, affidabilità, sicurezza o costi.

Le conferme di validità sono periodicamente emesse dalla CA (RTCA) e distribuite come files firmati digitalmente (a mezzo di un server intermedio) ai Risponditori RTC (RTCR). Una singola RTCA su piattaforma Intel o Sparc può agevolmente supportare una popolazione di 10 milioni di utenti con conferme quotidiane. Popolazioni più numerose possono essere supportate aggiungendo semplicemente piattaforme RTCA di maggiori dimensioni o aggiuntive. Ciascun risponditore RTC è in grado di ricevere sia una richiesta OCSP che una richiesta V.Token per l'aggiornamento dello stato di un certificato e restituire la risposta appropriata. Dal momento che questa operazione è un semplice riscontro tabellare, la risposta è data in circa 2 millisecondi. Questo è un significativo miglioramento rispetto a un OCSP tradizionale, in cui ogni risposta deve essere firmata prima di essere consegnata all'applicazione dell'utente [8].

a. Ulteriori vantaggi del sistema RTC

Il sistema RTC offre i seguenti ulteriori vantaggi rispetto all'OCSP tradizionale:

1) **Validazione off-line:** poiché le conferme di validità date dal sistema RTC sono inalterabili e non passibili di contraffazione, esse possono essere fornite all'utente da qualsiasi fonte, compresa lo stesso utente. Ciò conferisce, in particolare, grande flessibilità per quelle applicazioni per le quali è difficile o impossibile connettersi in rete. Per esempio, un utente potrebbe acquisire il proprio certificato di validità del giorno utilizzando la sua Carta di Accesso per poi utilizzarla, insieme al suo certificato di convalida, per accedere ad un'applicazione non connessa in rete. L'applicazione può autenticare e convalidare l'utente in locale.

[8] Vedi l'Appendice A per i pertinenti parametri di messa in opera.

2) **Soluzione a minima larghezza di banda:** RTC presenta due soluzioni di convalida che supportano ambienti a bassa larghezza di banda: V.Token e Mini CRL. Ciascun V.Token è lungo solo 20 bytes e ciò lo rende ideale là dove sussistono severe limitazioni di banda nel collegamento tra risponditore ed utente. Il MiniCRL offre un fattore di riduzione dimensionale di 30x rispetto al CRL tradizionale diventando, per questo, ideale dove sussistono severe limitazioni di banda nel collegamento tra la RTCA ed i risponditori RTC.
3) **Gestione dinamica dei privilegi:** le tecnologie del sistema distribuito e quelle del sistema V.Token, per la prima volta, rendono possibile la gestione dinamica di molteplici privilegi associabili ad un singolo certificato senza dover rilasciare nuovamente o modificare tale certificato in nessun caso. Inoltre, la tecnologia RCT consente a questi privilegi di essere gestiti da autorità autonome ed indipendenti.
4) **Autorità di auto-convalida:** uno dei più difficili problemi associati con l'impiego dei risponditori OCSP è il poter rispondere alla domanda "come può un utente sapere se può fidarsi della risposta?" La tecnologia V.Token semplifica questo problema nella misura in cui l'integrità di una V.Token è auto-dimostrata (self evident). Il sistema non utilizza sistemi di firma perciò non ci sono certificati associati a una chiave di firma, da verificare per convalidare l'integrità della risposta.

Qualora se ne rendesse necessario, il sistema RTC avrebbe un solo risponditore (contro decine o centinaia) con una singola chiave di firma e la necessità di un solo certificato da convalidare. Ciò rende il problema molto più facile da risolvere e anche l'uso di "certificati a breve vita" diventa una pratica soluzione.

b. Selezione del formato

I certificati RTC offrono la possibilità di una grande varietà di applicazioni.utilizzando i formati a firma digitale o V.Token.

1) **Certificato sistema OCSP Distribuito –** Questi certificati digitali offrono la massima integrazione grazie alla loro compatibilità con gli standards ed i protocolli esistenti. I certificati RTC sono completamente compatibili con il protocollo OCSP, sono sintatticamente realizzati come risposte OCSP standard e possono essere usati da qualsiasi applicazione di utenti OCSP. A seconda dell'algoritmo di firma, della lunghezza della chiave e dell'eventuale presenza di privilegi, i certificati RTC hanno dimensioni che variano da 150 a 350 bytes e possono essere processati e verificati in meno di 10 millisecondi da qualsiasi computer. Il sistema RTC presenta un'eccellente scalabilità a circa 10 milioni di credenziali indipendenti e centinaia di migliaia di

risponditori.

2) **Certificati V.Token –** Questi certificati assicurano una notevole scalabilità ed ottime prestazioni per ambienti in cui l'ampiezza di banda dell'applicazione client è molto limitata e quando non vi sono esigenze di compatibilità con funzionalità precedenti (i V.Tokens richiedono l'aggiunta di 40 bytes di dati all'estensione “Subject Directory Attribute” del certificato X.509 ed usano software sul client in grado di interpretare i certificati). Grazie all’uso dell'algoritmo hash a una via e dei protocolli utilizzati, i certificati V.Token misurano da 16 a 100 bytes e possono essere generati ed esaminati in meno di un millisecondo. Una soluzione V.Token può facilmente supportare centinaia di milioni di credenziali insieme a decine di migliaia di risponditori. I V.Tokens sono ideali per l'uso con apparecchi portatili collegati in modalità wireless e con sistemi molto diffusi.

3) **MiniCRL –** Questi certificati forniscono grandi scalabilità ed ottime prestazioni per ambienti in cui l'ampiezza di banda di collegamento tra il RTCA ed i risponditori RTC è limitata, come nel caso di canali di comunicazione bordo-terra. Questo sistema è ideale anche per un gran numero di utenti in ambienti a bassa ampiezza di banda. I MiniCRL rappresentano in assoluto la minima dimensione (usano un bit per certificato rilasciato) per convogliare l'informazione di validità di un certificato. La dimensione effettiva è ridotta a circa mezzo bit per certificato, usando le tecniche standard di compressione. Una tecnica di segmentazione è impiegata per mantenere le dimensioni dei dati inviati alle applicazioni client molto piccole. Il sistema MiniCRL usa un plug-in dal lato client per interpretare l'informazione di stato del certificato.

La soluzione RTC assicura affidabilità, scalabilità e sicurezza in modo incomparabile per la gestione di credenziali in ambienti dove la sicurezza degli accessi è un fattore critico qualunque sia il formato usato per i certificati di validità.

6. Conclusioni

Il sistema distribuito di conferma della validità di un certificato non è solo un modo migliore per confermare lo stato di validità dei certificati con l'impiego della PKI; esso rappresenta l'unica soluzione che garantisce scalabilità senza sacrificare le prestazioni, affidabilità, sicurezza e minimi costi. In aggiunta, fornisce soluzioni in situazioni critiche e con impiego di banda limitata che non potrebbero essere effettuate altrimenti.

Appendice A: Parametri di impiego del sistema RTC

La seguente tabella fornisce i principali parametri di impiego per i tre metodi forniti dalla soluzione RTC. Tali parametri sono stati valutati con le seguenti ipotesi:

1) 1 milione di utenti
2) periodo di validità delle prove di validazione: 1 giorno
3) compressione files pari al 50% per files scaricati
4) velocità di trasmissione T1 dall'autorità RTC ai risponditori RTC
5) chiave di firma OCSP = 1024 bit RSA

I tempi sono stati misurati usando un singolo server Intel di fascia media con un acceleratore hardware.

Tabella A: Parametri di impiego per il sistema di validazione RTC

Parametro	OCSP Distribuito	V.Token distribuito	MiniCRL
Requisiti di memorizzazione del RTCA	1 Gbyte	120 Mbytes	120 MBytes
Tempo di elaborazione del RTCA (usando un HSM)	Circa 10 minuti	17 minuti cpu	5 minuti cpu
Dimensione file inviato dalla RTCA ai risponditori RTC	14 Mbytes	17 Mbytes	90 KB
Tempo di download dei risponditori RTC	1.3 minuti	3 minuti	1 secondo
Requisiti di memorizzazione dei risponditori RTC	50 Mbytes	50 Mbytes	30 Mbytes
Dimensione della certificazione inviata al client	2.5 KB	400 bytes	3-4 KB
Tempo di elaborazione per l'applicazione dell'utente	10 millisecondi	1 millisecondo	10 millisecondi

Un tipico server RTCA Sparc con un modulo di sicurezza hardware può generare attestazioni di convalida per 1 milione di certificati in circa 10 minuti e un milione di certificati V.Token in meno di 20 minuti. Un singolo risponditore RTC può fornire più di 1000 risposte al secondo, permettendo di servire milioni di richieste provenienti dagli utenti al giorno. I risponditori RTC possono anche supportare simultaneamente richieste di OCSP Distribuiti, V.Token e MiniCRL. Ciò conferisce la capacità di usare un singolo sistema per mescolare ed utilizzare allo stesso tempo i diversi metodi di certificazione per venire incontro a molteplici e distinte necessità operative.

Appendice B: Analisi dei costi dei metodi di convalida

Una delle principali e vantaggiose caratteristiche del sistema distribuito di convalida RTC è il rapporto costo/efficacia. In questa appendice viene evidenziato il risparmio economico con comparazione dei costi di installazione e i costi ricorrenti delle infrastrutture a parità di livello di servizio fornito con la precisazione che sono stati presi in considerazione solo i costi direttamente legati alle soluzioni architetturali esaminate. Per gli scopi di questo documento "pari livello di servizio" vuol dire impiegare lo stesso numero di risponditori geograficamente collocati per fornire le stesse prestazioni e la stessa affidabilità alle applicazioni degli utenti. Sono messi a confronto due diversi approcci, l'OCSP tradizionale (T-OCSP) e l'OCSP distribuito (D-OCSP). I costi per le infrastrutture necessarie per implementare i certificati di validazione (V.Tokens) e i MiniCRL sono essenzialmente gli stessi del D-OCSP.

Dati di partenza:

– numero di certificati gestiti (milioni)	10
– numero di risponditori installati	10 e 100
– tempo minimo di aggiornamento (periodo di aggiornamento in ore)	2
– tipo di chiave	RSA
– lunghezza della chiave (es. chiave del risponditore OCSP)	1024

Costi stimati dei componenti del sistema OCSP tradizionale:

– sito/hardware risponditore OCSP (include HSM)	$25.000
– impostazioni di sicurezza (una volta/sito)	$50.000
– operazioni di sicurezza (annualità/sito)	$50.000

Costi stimati dei componenti del sistema distribuito:

– hardware RTCA D-OCSP (include HSM)	$113.000
– settaggio di sicurezza del sito RTCA (una volta, singolo sito)	$50.000
– controllo della sicurezza del sito RTCA (annuale, singolo sito)	$50.000
– hardware/sito risponditore RTC (nessun HSM necessario)	$3.000
– quote mensili TI	$1.000

L'installazione del sistema tradizionale OCSP richiede:

– connessione di rete per ciascun risponditore installato per ricevere gli aggiornamenti periodici CRL

- protezione di sicurezza fisica ed elettronica per ciascun risponditore installato (stima)
- operatori fidati che usano controllo di accesso duale (costo stimato)

L'installazione dell'OCSP distribuito richiede:

- una RTCA (il terminale posteriore) che richiede una protezione di sicurezza fisica ed elettronica (il costo è stimato, potrebbe essere collocato con la CA a piccolo o nessun extra costo)
- singolo set di operatori RTCA fidati che usano un controllo di accesso duale (costo stimato)
- connessione di rete tra l'RTCA e ciascun risponditore RTC installato (il D-OCSP richiede velocità TI per oltre 10 milioni di certificati)
- No memorizzazione sicura, postazione od operatore per ciascuno dei risponditori RTC installati
- servers COTS standard per ciascun risponditore RTC.

Calcolo dei costi:

- Costi di set-up per T-OCSP = hardware risponditore + firewall + setup di rete + sicurezza del sito

  = (#Resp) x ($25k + $10k + 2k + $50k)

  = (#Resp) x ($87k)

- Costi di set-up per D-OCSP = hardware RTCA + firewall + fileservers + setup di rete + sicurezza del sito + risponditore (hardware + setup T1)

  = (1) x ($113k + $10k + $10k + $2k + $50k) + (#Resp) x ($3k + $2k)

  =$185.000 + (#Resp) x $ 5.000

- Costi ricorrenti T-OCSP = noleggio linee (per scaricare i CRL) + costi personale di sicurezza

  = (#Resp) x {[#Mbytes/(T1 transfer rate)] x ($T1) + $50k}

  = (#Resp) x {[140 Mbytes/(187.500 bytes /sec)] x ($12k) + $50k}

  = (#Resp) x {(1) x ($12k) + $50k}

  = (#Resp) x ($62k)

- **Costi ricorrenti D-OCSP = noleggio linee + costi personale di sicurezza**

  = (#Resp) x {[#Mbytes/(T1 transfer rate)] x ($TI)} + (1) x ($50k)

  = (#Resp) x {[140 Mbytes/(187.500 bytes /sec)] x ($12k)}+ $50k

  = (#Resp) x {(1) x ($12k) + $50k}

  = (#Resp) x $12k + $ 50k

La Tabella B-1 fornisce un confronto dei costi per un'installazione di 10 risponditori

Elemento di costo	***N. di risponditori***	***T-OCSP***	***D-OCSP***
Costi di set-up per il primo anno	10	$870.000	$235.000
Costi ricorrenti annui		$620.000	$170.000
Risparmi primo anno (setup + ops)		$1.085.000	
Risparmio sui costi ricorrenti		$450.000	
Costi di set-up primo anno	100	$8.700.000	$685.000
Costi ricorrenti annui		$6.200.000	$1.250.000
Risparmi primo anno (setup + ops)		$12.965.000	
Risparmio sui costi ricorrenti		$4.950.000	

Nota 1: Questo confronto è mirato esplicitamente ad evidenziare le differenze di costi nell'impiego con 10 e 100 risponditori. Mentre i costi del T-OCSP crescono linearmente, quelli del D-OCSP crescono molto più lentamente.

Nota 2: Poiché i certificati D-OCSP sono pre-firmati, il tempo di risposta del risponditore all'utente è 20 volte più veloce per il D-OCSP che per il T-OCSP. Tuttavia, di ciò non è stato tenuto in considerazione in questi calcoli. Pertanto, il risparmio è ancora maggiore di quanto mostrato.

E' chiaro, da questo confronto, che il sistema di convalida RTC garantisce la flessibilità richiesta per raggiungere un'elevata affidabilità senza incorrere nelle significative penalizzazioni di costi tipiche del sistema T-OCSP.