Consiglio Nazionale delle Ricerche

MessageVerify: un sistema per la verifica automatica della firma digitale

M. Buzzi, F. Gennai

IIT TR-02/2002

Technical report

Marzo 2002

Istituto di Informatica e Telematica

Abstract

La firma digitale associata a messaggi di Posta Elettronica garantisce: l'autenticazione del mittente, l'integrità del messaggio, e il non ripudio dell'origine.

L'operazione di validazione della firma è una operazione piuttosto critica affidata all'intervento manuale dell'interlocutore: di solito la funzione di verifica viene effettuata dal client di Posta Elettronica che avvisa l'utente sia in caso di errori (ad es. la verifica ha avuto esito negativo) sia di warning (ad es. l'indirizzo di e-mail del mittente non compare nel certificato). Vista però come "chiave" per l'autorizzazione all'utilizzo di un certo servizio, allora il concetto di validazione della firma può essere spostato su sistemi automatici capaci di processare un elevato numero di messaggi nell'unità di tempo. Questo rapporto tecnico descrive l'architettura e le funzionalità di un sistema per la verifica automatica (via server) della firma digitale associata a messaggi di Posta Elettronica. L'ultima parte del documento descrive le estensioni funzionali apportate al sistema per includere la generazione della firma e l'inoltro di "web form" digitalmente firmati.

Indice

Introduzione

In questo report sono descritte l'architettura e le funzionalità di un sistema per la verifica automatica (via server) della firma digitale associata a messaggi di Posta Elettronica. E' chiaro che la funzionalità di verifica automatica della firma digitale associata a messaggi di Posta Elettronica è applicabile solo in particolari contesti ove non esista una relazione semantica tra il mittente ed il contenuto del messaggio, che solo il destinatario sia in grado di capire.

Nel caso specifico, il sistema è stato progettato per semplificare il servizio di registrazione di nomi a dominio sotto il Top Level Domain .IT, effettuato dalla Registration Authority (RA) Italiana [1], [2], [3]. In questo contesto, la verifica di un messaggio è utilizzata come chiave di accesso per la registrazione di nomi a dominio (*domain names)*. I messaggi ricevuti sono sostanzialmente dei moduli elettronici che contengono i parametri necessari per la registrazione del servizio (nel nostro caso un form di registrazione per un dominio). I dati inviati sono conformi ad una specifica sintassi (per es. keyword:valore) che ne facilita l'elaborazione automatica. Contenuti differenti, se ricevuti, sono rifiutati.

Il sistema sviluppato, chiamato MsgVerify (MV), è stato progettato per interporsi, come interfaccia trasparente, tra la ricezione di messaggi di richiesta di un servizio e il pre-esistente software per l'elaborazione automatica del loro contenuto. Se il processo di verifica ha successo, la richiesta è accettata ed elaborata, altrimenti è rigettata ed una notifica automatica viene inviata al mittente. Un requisito basilare per la progettazione del sistema era perciò la trasparenza della soluzione, in modo che la RA potesse utilizzare senza alcuna modifica il software di elaborazione automatica già disponibile.

Il punto fondamentale nella progettazione del sistema era capire in che modo automatizzare il processo di verifica. Questa parte ha richiesto uno studio dell'applicazione della tecnologia di crittografia a chiave pubblica nei sistemi di Posta Elettronica. In particolare abbiamo studiato i meccanismi da applicare per interpretare la firma digitale nei messaggi in ingresso al sistema. Il processo di verifica può essere decomposto in due parti:

- Individuazione all'interno del messaggio delle parti MIME contenenti i dati protetti. L'RFC 1847 (S-MIME) [4] specifica come applicare servizi di sicurezza alle parti

MIME del body del messaggio. S-MIME aggiunge due nuovi content type: Multipart/Signed e Multipart/Encrypted, entrambi contenenti due body: una per i dati protetti e l'altra per le informazioni di controllo necessarie per rimuovere le protezioni. L'RFC 2630 descrive la sintassi (Cryptographic Message Syntax) utilizzata per generare il digest, firmare o cifrare messaggi, etc. [5]. Infine l'RFC 2633 [6] definisce il MIME type application/pkcs7-signature utilizzato per trasportare messaggi S/MIME digitalmente firmati e spiega dettagliatamente i requisiti e le specifiche a cui gli agenti che ricevono i messaggi (receiving agents) devono attenersi per manipolarli correttamente.

- Corretta applicazione del processo di verifica alle parti MIME estratte. Per effettuare questo processo sono necessari meccanismi per il recupero e la validazione di certificati. L'RFC 2632 [7] specifica le regole di base che gli agenti devono applicare per verificare correttamente un messaggio digitalmente firmato. In aggiunta, l'Internet Draft (I-D) "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile" (che aggiorna l'RFC 2459), descrive il formato (e la semantica) dei Certificati e delle Certificate Revocation List (CRL) e le procedure per l'elaborazione dei cammini di certificazione (certification path) in ambiente Internet [8]. Questo I-D dà una cornice in cui gestire certificati e CRL.

Era inoltre necessario studiare un altro punto basilare: in quale modo effettuare le funzioni svolte dell'utente nell'interazione con il client di Posta Elettronica. Nella verifica della firma digitale via client, infatti l'utente interagisce con il software di Posta Elettronica in varie occasioni, come ad esempio per caricare il certificato di una CA nel database delle Trusted CA (cioè delle Certification Authority di sua fiducia). Tali funzionalità nel sistema MessageVerify vengono trasferite dall'utente (destinatario) ad un amministratore del sistema che può effettuare le stesse operazioni via web.

Nei prossimi paragrafi è illustrata l'architettura del sistema e viene descritto il funzionamento del sistema.

Ambiente operativo

Descriviamo innanzitutto l'ambiente operativo. Il sistema gira su uno SCSI cluster costituito da 2 sistemi AlphaServer 800 (500 Mhz) con sistema operativo OpenVMS che condividono un disk array da 90 GB in configurazione RAID5. Sul cluster sono attivi il

sistema di Posta Elettronica commerciale PMDF [9] e il server HTTP OSU-Web (Ohio State University Web Server) [10] di pubblico dominio.

Il sistema MessageVerify è stato realizzato in linguaggio DCL (Data Command Language) utilizzando le librerie crittografiche di pubblico dominio OpenSSL [11]. Queste librerie offrono le API (Application Programming Interfaces) per lo sviluppo di applicazioni crittografiche, nonché gli strumenti crittografici da utilizzare a linea di comando. Utilizzando questi strumenti il sistema effettua i seguenti controlli: verifica della firma, verifica dei percorsi validi fino a una CA affidabile, verifica dell'accessibilità della CRL, verifica della validità di una CRL, verifica della scadenza e della revoca di certificato.

Architettura

Per semplificare la comprensione del sistema possiamo schematizzare l'intero processo in più passi:

a) L'utente invia il messaggio firmato a un mailbox configurato per l'elaborazione automatica del contenuto del messaggio;
b) All'ingresso del sistema al messaggio viene assegnato un identificatore univoco;
c) Viene verificata la firma;
d) Se la firma è verificata con successo, la parte firmata è estratta e inviata alle successive fasi;
e) Se la verifica fallisce con un errore temporaneo (p. es. CRL non disponibile) il messaggio viene accodato per successivi tentativi (fino al raggiungimento di una soglia prefissata).
f) Se la verifica fallisce con un errore permanente (per es. messaggio non firmato), viene inviata una notifica di errore al mittente e all'amministratore locale.

Il sistema è composto da componenti software (uno o più moduli eseguibili) con diverse funzionalità. I moduli possono essere eseguiti in parallelo su un qualsiasi nodo di un cluster. La figura 1 mostra lo schema logico del sistema MsgVerify (MV).

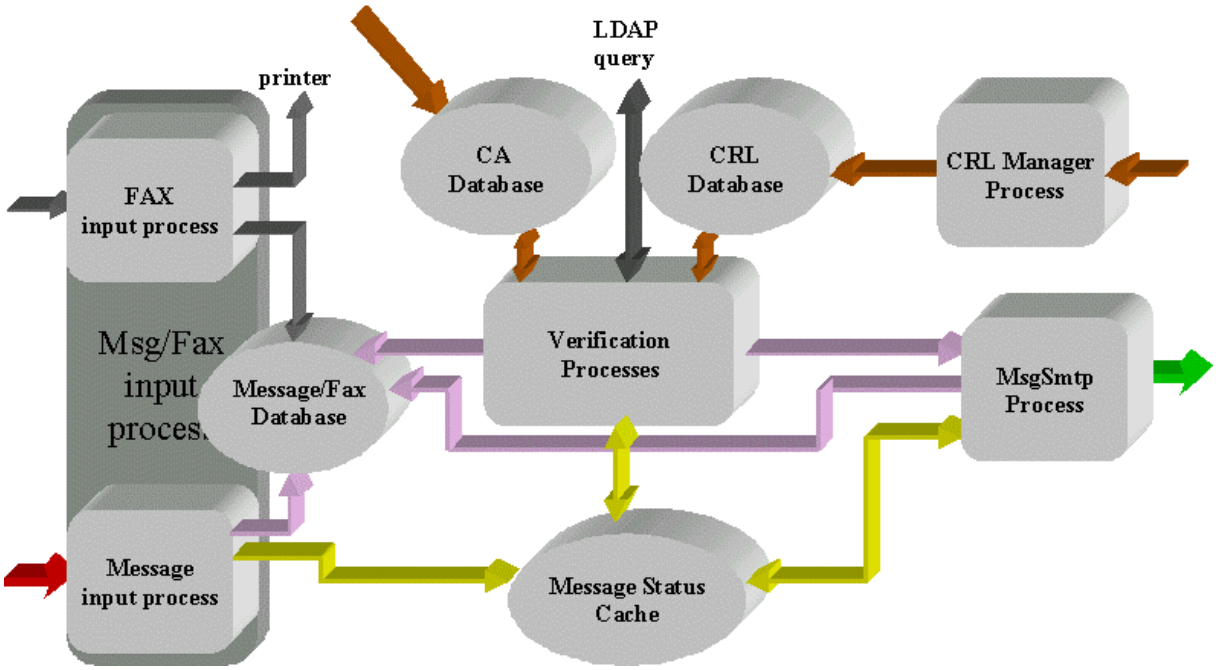

Fig.1 - schema logico del sistema MV

Il sistema è composto da database, moduli specializzati e interfacce CGI per la gestione e il controllo del sistema via web. In Figura 1 i processi (moduli in esecuzione) sono rappresentati con triangoli ed i database con ellissi.

I moduli svolgono le seguenti funzioni:

- Ingresso del messaggio nel sistema e pre-processing (MsgVerify_Deliver)
- Verifica della firma digitale associata al messaggio (Verification Process)
- Trasmissione messaggi verificati verso la RA (MsgSmtp Process)
- Aggiornamento CRL (CRL Manager Process)

Le interfaccie web (moduli CGI) consentono di effettuare operazioni di:

- accesso all'archivio messaggi/fax
- gestione e controllo del sistema

I database utilizzati dal sistema sono quattro:

- **Archivio messaggi/fax**. Il *Message database* include anche richieste ricevute via fax, memorizzate come file postscript (*Message/Fax Database*). Un identificatore globale viene assegnato ad ogni messaggio o fax che entra nel sistema, mantenendo la sequenza temporale delle richieste; questo è veramente importante per risolvere collisioni su richieste dello stesso nome a dominio.

- **Database dei certificati delle Trusted CA**. I certificati delle CA di fiducia (trusted CAs) possono essere aggiunte al (o rimosse dal) *CA Database* dall'amministratore del sistema. Naturalmente il sistema realizzato è in grado di utilizzare certificati emessi da qualsiasi CA, previo caricamento del certificato/i della CA root ed eventuali subCA nel database del sistema.
- **Database delle CRL**. Le CRL sono automaticamente scaricate (utilizzando il campo Certificate's *CRL Distribution Point*) dal processo *CRL Manager* che aggiorna il database delle CRL locale (*CRL Database*). LDAP query sono naturalmente possibili, ma non ancora implementate.
- **Message Status Cache**. Il *Message Status Cache* è utilizzato per migliorare l'efficienza ed anche per mantenere separate le informazioni relative ai processi da quelle dei messaggi/fax: esso mantiene informazioni temporanee sullo stato del messaggio, durante il suo tempo di vita all'interno del sistema.

Lo scheletro dell'intero sistema è costituito da tre moduli principali: MSGVERIFY_DELIVER, MSGVERIFY e MSGTOSMTP. Le altre componenti sono di supporto, come i moduli LOAD_CA_CERT e CRL_MANAGER. Nel seguito descriviamo nel dettaglio le funzionalità dei moduli.

Modulo MSGVERIFY_DELIVER

MSGVERIFY_DELIVER è il modulo di immissione dei messaggi nel sistema MsgVerify/fax-RA. Le sue funzioni primarie sono:

- pre-processing dei messaggi per estrarre dati necessari alle successive elaborazioni.
- sincronizzazione del generatore di identificatore univoco tra sistema MsgVerify e il sistema fax-RA.
- archiviazione del messaggio nel suo formato originale.
- accodamento del messaggio alla coda di ingresso.
- scheduling del successivo modulo di elaborazione (MSGVERIFY).

Il modulo viene automaticamente schedulato all'arrivo di un messaggio.

Modulo MSGVERIFY

Questo modulo costituisce il cuore del sistema MsgVerify. Ha il compito di effettuare la verifica di validità della firma e di gestire i vari stati del singolo messaggio e dell'intero sistema, derivanti da questa attività.

I dati in ingresso al modulo sono rappresentati dal flusso dei messaggi di cui occorre verificare la validità della firma, dall'archivio integrato Messaggi/fax, dal database delle Certification Authority Trusted, dal database delle Certificate Revocation Lists e dal cache database.

I dati in uscita dal modulo sono rappresentati dal flusso dei messaggi elaborati, dall'archivio integrato Messaggi/Fax e dal cache database.

Il processo di verifica aggiunge quattro campi all'header del messaggio, che specificano rispettivamente: il *Distinguished Name* di chi ha emesso il certificato (*Certificate Issuer Distinguished Name)*, il *Distinguished Name* del possessore del certificato *(Certificate Subject Distinguished Name),* il numero di serie del certificato (*Certificate Serial Number*) e la concatenazione tra il codice di ritorno del processo di verifica e l'identificatore globale del messaggio (X-MVcertissuer:, X-MVcertsubject:, X-MVserialnumber, X-MVglobalid:). In tal modo il messaggio archiviato mantiene informazioni sull'esito dell'operazione di verifica.

Il modulo genera ed invia messaggi di notifica relativi all'esito delle proprie azioni.

Modulo MSGTOSMTP

Il modulo MSGTOSMTP ha il compito di comporre il messaggio finale, escludendo la parte MIME che contiene la firma e di inoltrarlo verso i sistemi della Registration Authority.

Modulo LOAD_CA_CERT

Con questo modulo è possibile gestire il database delle trusted CA utilizzando una semplice interfaccia web.

Il caricamento del certificato di una CA può avvenire attraverso due diverse funzioni:

- sessione HTTP verso il server web della CA dove il certificato è pubblicato.
- upload dal disco del client dell'amministratore.

Modulo CRL_MANAGER

Questo modulo automatizza la gestione del database delle CRL.

Il modulo apre una connessione con il server web di ciascuna CA ad intervalli di tempo prefissati dall'amministratore e tenta di effettuare il download della CRL aggiornando il database locale. I risultati sono mantenuti in un dettagliato file di log delle varie sessioni.

Il modulo stesso provvede a notificare all'amministratore eventuali errori o l'approssimarsi della data di scadenza di una CRL.

Sincronizzazione dei processi

L'intero sistema è architettato per funzionare in ambiente cluster, dove il modulo MSGVERIFY può essere in esecuzione simultanea su diversi nodi.

Questa opzione rende il sistema altamente scalabile, ma richiede una sincronizzazione tra i processi operanti su nodi diversi.

In particolare il sistema deve garantire che i messaggi la cui verifica ha avuto successo siano inoltrati verso l'uscita nello stesso ordine che avevano all'ingresso del sistema.

E' anche necessario tenere traccia dello stato di ciascun messaggio che per varie cause con carattere di temporaneità permane per un certo tempo all'interno del sistema (intervalli di generazione notifiche al mittente, cause di precedenti malfunzionamenti, etc.).

Per ottimizzare la gestione delle funzioni di cui sopra il sistema MsgVerify utilizza un cache database in cui sono memorizzate varie informazioni per ciascun messaggio che si trova nella fase di "transito" all'interno del sistema.

Il cache database è scritto/letto/aggiornato dalla maggioranza dei moduli del sistema MsgVerify:

- Il modulo MSGVERIFY_DELIVER ha il compito di creare una entry per ogni nuovo messaggio che immette nel sistema.
- Il modulo MSGVERIFY legge/aggiorna tale entry in base ai risultati delle proprie azioni compiute sul messaggio. Nel caso una delle azioni fallisca con un errore di carattere temporaneo, la entry è rimossa e una notifica di errore viene inviata al mittente e all'amministratore del sistema.
- Nel caso la verifica firma del messaggio termini con successo, il cache database è aggiornato e il modulo MSGTOSMTP è schedulato per le elaborazioni successive.

- Il modulo MSGTOSMTP accede al cache database per selezionare i messaggi che possono essere inoltrati verso l'uscita del sistema. Il modulo MSGTOSMTP provvede a rimuovere dal cache database le entry dei messaggi il cui invio ha avuto successo.

Eventuali errori sono segnalati all'amministratore.

Notifiche

I risultato di diverse azioni viene notificato al mittente del messaggio e all'amministratore del sistema. I messaggi di notifica vengono generati a conclusione delle diverse azioni, e sono suddivisibili in tre principali classi, in dipendenza dal loro esito:

- errore permanente.
- errore temporaneo.
- successo.

La struttura di un messaggio di notifica consente l'adozione di procedure di elaborazione automatiche. Il messaggio trasporta comunque una descrizione relativa alla notifica stessa.

Le interfacce web

L'interfaccia richiede un accesso controllato da user/password che autorizza due tipi di accesso:

- normale, per gli operatori - consente l'accesso via web all'archivio messaggi/fax (Messages/Faxes selection);
- privilegiato, per l'amministratore - consente di accedere alle funzioni di configurazione (fig. 2). In particolare l'accesso privilegiato abilita l'amministratore ad eseguire le seguenti funzioni:
  - aggiungere o rimuovere certificati di CA;
  - gestire il database dei certificati delle CA, ed in particolare visualizzare i campi presenti nei certificati;
  - visualizzare il log del processo di gestione delle CRL in formato compatto o esteso;
  - configurare il sistema;
  - monitorare il sistema (processi).

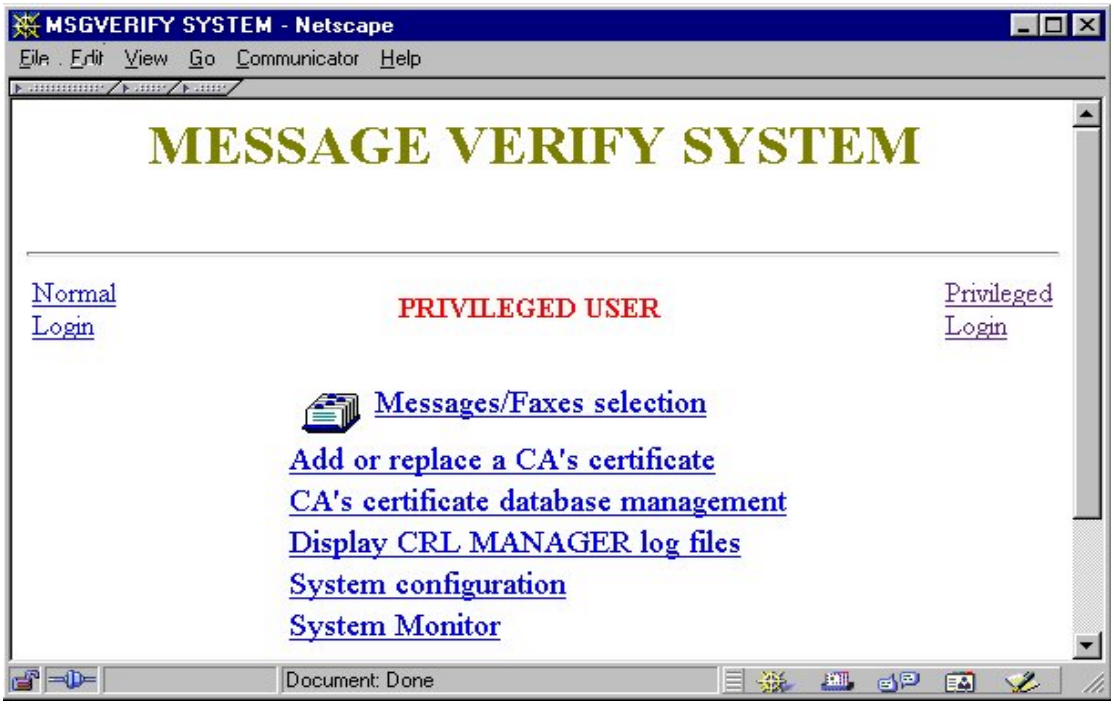

Fig. 2 - Interfaccia del sistema Message Verify

Accesso all'archivio messaggi/fax

Le interfacce web forniscono l'accesso all'archivio messaggi/fax, utile sia in fase di modifica/cancellazione domini sia per il servizio di help desk nella la risoluzione di specifici problemi evidenziati dall'utenza. Esse permettono di effettuare funzioni di utilità come la ricerca di elementi (per identificatore, data, etc.), la visualizzazione o re-printing di fax e messaggi, la visualizzazione di eventuali problemi verificatesi nella verifica della firma digitale, etc. Per maggiori dettagli sul sistema fax della RA si rimanda a [12], [13].

La figura 3 mostra l'interfaccia di accesso al database fax/messaggi in cui i dati sono stati mascherati. Sono possibili ricerche per data o per identificatore univoco del msg/fax.

Configurazione del sistema

Come accennato nei paragrafi precedenti, il sistema "Message Verify" (MV) è totalmente configurabile e monitorabile via web. La figura 4 mostra una porzione dell'interfaccia di configurazione del sistema. Come si può vedere dalla figura il sistema è stato reso il più possibile flessibile, in modo da adattarsi velocemente a cambiamenti nella policy dell'organizzazione.

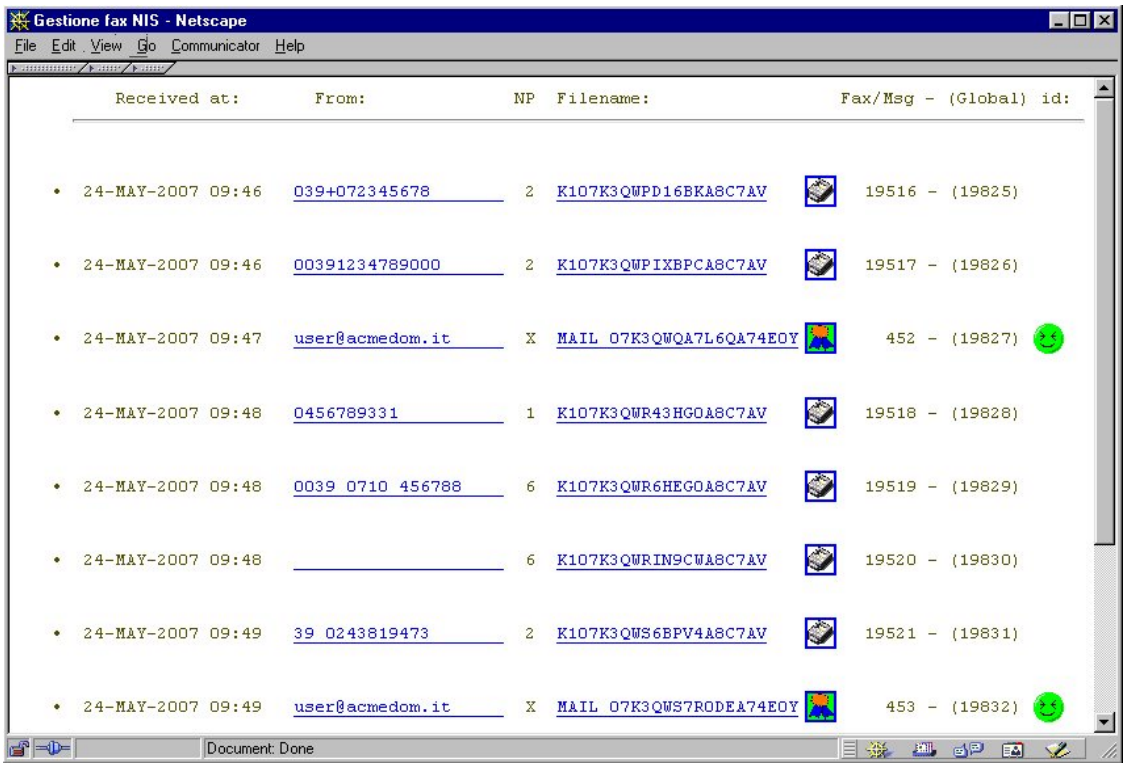

Fig. 3 - Browsing del database messaggi/fax

Nel seguito sono descritti tutti i parametri di configurazione del sistema. La Figura 4 mostra una parte dell'interfaccia di configurazione.

- *Autoforwarding* (Yes/No). Indica se i messaggi devono essere forwardati o no verso una certa destinazione.
- *Destination address*. Se il parametro Autoforwarding è YES, specifica l'indirizzo e-mail di destinazione.
- *Alternate destination address*. Specifica un indirizzo e-mail di destinazione alternativo.
- *Operator addresses*. Indirizzo/i e-mail (di operatore/i) per le comunicazioni di sistema.
- *Alternate Operator address*. Specifica un indirizzo e-mail di operatore alternativo.
- *Success envelop from*. Indirizzo che il sistema inserisce nel campo from dell'envelop del messaggio generato ed inoltrato verso le successive fasi del processo di registrazione (in caso di successo dell'operazione di verifica).
- *Delivery Method*. Determina il comportamento di default del sistema in caso di un errore temporaneo relativo ad una certa CA (come ad es. CRL scaduta).

L'amministratore può scegliere una tra le seguenti opzioni, in accordo alla policy scelta dall'organizzazione:

- **P** - invia il messaggio originario all'Operatore (all'indirizzo e-mail specificato dal parametro *Operator Addresses*) e continua a processare i messaggi successivi.
- **S** - Solo i messaggi firmati con certificati emessi dalla CA in oggetto vengono ri-processati ad intervalli fissi (vedi parametro *Message Verify job execution interva*l) in attesa che il problema sia risolto, mentre i rimanenti continuano ad essere processati.
- **A** - Tutti i messaggi vengono riprocessati ad intervalli fissi (vedi parametro *Message Verify job execution interval*) in attesa che il problema sia risolto.
- **U** - Continuazione incondizionata del sistema. I messaggi verificati con successo sono inviati immediatamente al successivo passo di elaborazione, anche se fallimenti temporanei dell'operazione di verifica potrebbero ritardarne altri.

- *Number of entries displayed in the CRL log file*. Numero di entry visualizzate nel file di log relativo al downloading delle CRL.
- *CRL master job execution interval*. Tempo di esecuzione del Modulo che effettua il download delle CRL (CRL_Manager).
- *CRL Maximum extension time*. Tempo massimo di estensione di una CRL. Pone un limite superiore al valore che l'amministratore può specificare nell'interfaccia di gestione del database delle CA (CA certificate database Management).
- *Message Verify job execution interval*. Intervallo di esecuzione del Modulo Message Verify.
- *Minimum notification interval*. Intervallo tra due notifiche di errore per lo stesso messaggio.
- *Maximum retry interval*. Tempo massimo per cui un messaggio non verificabile è trattenuto in coda, prima che l'errore venga considerato permanente.
- *Monitor retry interval*. Specifica l'intervallo di refresh delle interfacce web di monitoring del sistema MV.
- *Address for CRL notification*. Indirizzo e-mail dove inviare notifiche relative a operazioni su CRL.

- *CRL notification days*. Numero di giorni per cui saranno inviate le notifiche relative a operazioni su CRL.

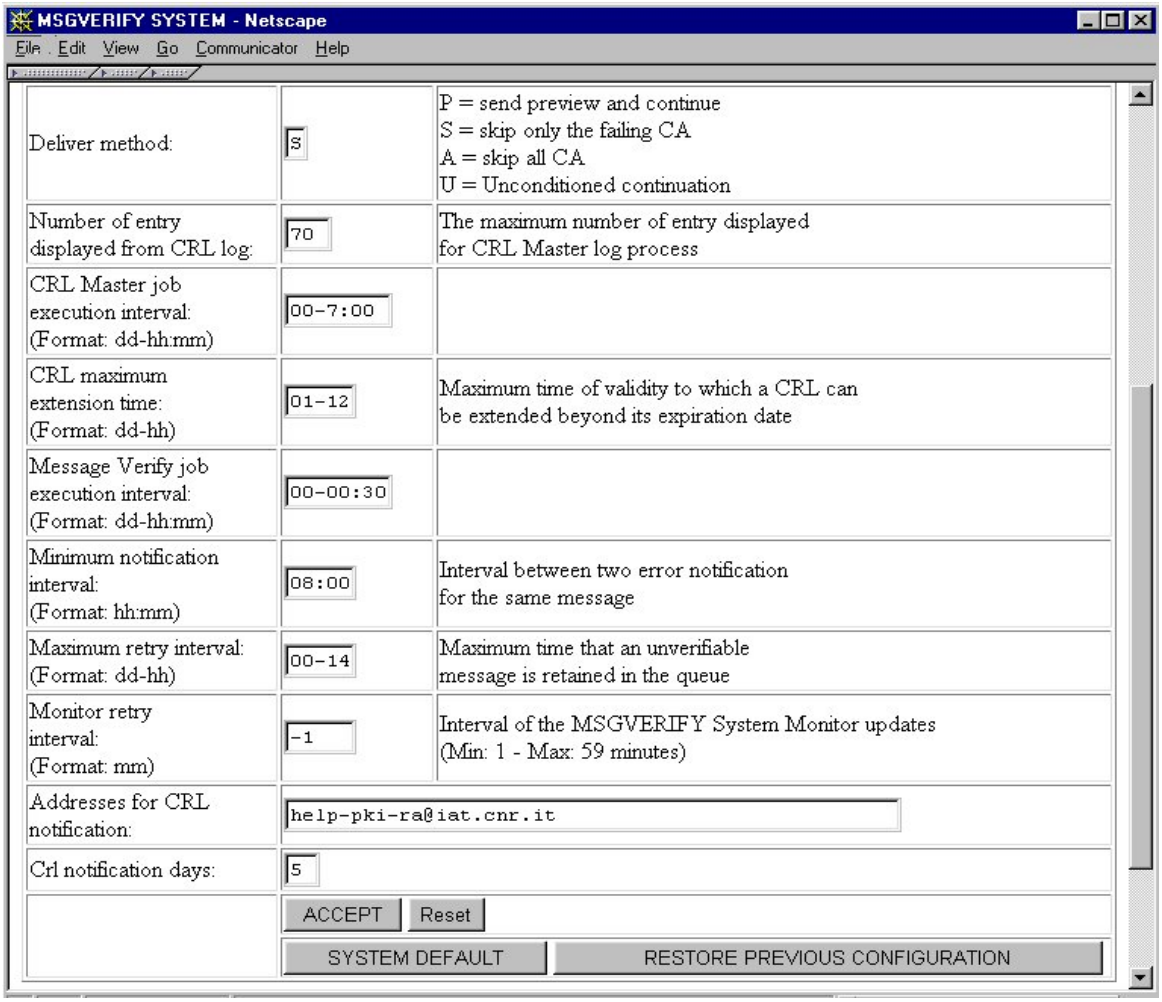

Fig. 4 - Interfaccia di configurazione del sistema Message Verify

L'interfaccia di configurazione offre la possibilità di salvare la nuova configurazione (push button *accept*), ripristinare i valori di default del sistema (push button *system default*), o la configurazione precedente (push button *restore previous configuration*).

Performance

Per verificare le performance del sistema, prima della sua messa in funzione, è stato effettuato un test effettuato sull'invio automatico di 2000 messaggi firmati. I risultati sono mostrati nella tabella 1. Le attività del sistema sono state suddivise in due parti: la verifica e il delivery del messaggio verso il software di elaborazione automatica. Nella terminologia del sistema operativo, viene definito job una unità di lavoro che può

comprendere l'esecuzione di uno o più moduli. Nel caso in oggetto il job include tutte le elaborazioni effettuate sul messaggio dall'ingresso nel sistema fino alla sua uscita (delivery).

	6 Job (3 x nodo)	2 Job (1 x nodo)	1 Job
Processo verifica	45 min	59 min	2h 6min
Processo delivery	1h 16 min	1h 4 min	2h 6min
Totale	*1h 16 min*	*1h 4 min*	*2h 6min*

Tab. 1 - Tempi di esecuzione del test

I risultati evidenziano come le migliori prestazioni si ottengano attivando un singolo job su ognuno dei due nodi del cluster. Attivare più esecuzioni parallele sullo stesso nodo non produce ulteriori vantaggi, ma anzi comporta un leggero aumento nel tempo totale di esecuzione, probabilmente implicato dalla competizione dei processi nell'accesso alle risorse.

Estensione del sistema

Per completare le funzionalità di verifica automatica, il sistema MsgVerify è stato esteso con l'aggiunta del modulo "Signing Form Module" per la generazione della firma e l'inoltro di "web form" digitalmente firmati [14].

Con il browser Netscape (4.04 e superiori) è possibile apporre la firma digitale ad un "web form". A partire da tale versione infatti Netscape include un "metodo" JavaScript (crypto.sign.Text) per la firma digitale di una stringa di testo da parte dell'utente.

Conformemente alla PKCS7 [15] e alla "Cryptographic Message Syntax" (che in parte estende la PKCS7), Netscape utilizza la modalità "external signature". Il risultato è che la struttura "signed-data" non conterrà il testo originale, che dovrà essere trattato separatamente.

Modulo Signing Form

Il modulo, totalmente integrato nel sistema MsgVerify, introduce e controlla le seguenti funzioni:

Lato client (web browser):

- compilazione di un "web form" per la richiesta di registrazione dominio;
- firma digitale del "web form" da parte dell'utente.

Lato server (HTTP server):

- verifica validità firma del "web form";

- accesso al database della CA trusted del sistema MsgVerify;
- controllo scadenza e validità certificato (accesso al database della CRL);
- sincronizzazione con il generatore di identificatore univoco Messaggi/Fax;
- accodamento della richiesta al modulo "MV:MSGTOSMTP" (per inoltro a domain@nic.it);
- archiviazione della richiesta nel database integrato Messaggi/Fax;
- in caso di esito positivo: immediata notifica su pagina web dell'identificativo univoco (globalid) assegnato alla richiesta di registrazione dominio;
- in caso di errore: immediata notifica tramite pagina web.

Da un punto di vista della logica di funzionamento vanno notate alcune caratteristiche rilevanti:

a) *Generazione identificatore univoco*.

La sincronizzazione dell'identificativo univoco tra Messaggi, Fax e richieste via Web, ha richiesto una riscrittura dell'algoritmo di allocazione dei generatori di identificatori (msgid, faxid e globalid).

L'accesso via web ha infatti introdotto un diverso meccanismo di interazione con i generatori di identificatori (id.) laddove si richiede una risposta ad una richiesta nell'arco di pochi secondi e si possono avere numerose richieste in contemporanea.

Per i processi di consegna dei messaggi e dei fax il tempo di risposta nell'allocazione del generatore di id è meno critico e la stessa allocazione può essere gestita con modalità più semplici che garantiscano la disponibilità della risorsa "generatore di id." ad ogni richiesta (nessun conflitto di accesso sulla risorsa). Per contro per i processi "non interattivi" di consegna messaggi e fax è più critico gestire il caso in cui la risorsa non sia allocabile in un ragionevole "resource allocation timeout".

Il nuovo algoritmo è ora in grado di gestire qualsiasi livello di conflitto di accesso sui generatori di id, tenendo conto del fatto, che a fronte di un conflitto nella allocazione risorsa è più semplice e corretto generare un messaggio di errore verso l'utente interattivo (accesso da web) piuttosto che penalizzare i processi di accodamento messaggi e/o fax.

Sulla base di tali considerazioni, l'algoritmo è tale da privilegiare le richieste di allocazione provenienti dai processi messaggi/fax mediante un meccanismo di

"interrupt" verso il processo concorrente CGI/HTTP (gestione delle richieste provenienti da utenti interattivi – "web form").

b) *Database*.

Il modulo di verifica della firma del "Signing Form Module" ("SF verification process module") utilizza le stesse routine del "MV verification process module".

Ne consegue:

- la condivisione dei database:
  - trusted CA database
  - CRL database
- il rispetto delle stesse politiche di gestione impostate dall'amministratore del "MsgVerify system": identificazione delle CA trusted, CRL extension time, frequenza aggiornamento database delle CRL, esclusione CRL, etc.

c) *Generazione ed inoltro richiesta registrazione dominio*.

La richiesta di registrazione dominio viene accodata, sottoforma di messaggio, al modulo del sistema MsgVerify "MV:MSGTOSMTP", che ha il compito di inoltrare tutte le richieste a domain@nic.it, rispettando strettamente l'ordine con cui queste si erano presentate all'ingresso del sistema MsgVerify. Questo significa ottenere una sequenza di inoltro ordinata delle richieste giunte via fax, messaggio o web (se via "Signing Form Module").

Le notifiche relative alle varie fasi saranno inviate all'indirizzo specificato nel campo "Notifyto" all'atto della compilazione del web form.

d) *Alta disponibilità del sistema*.

Il sistema è installato in ambiente cluster. La gestione del conflitto di accesso alle risorse, come i "generatori di id", è fatta a livello di cluster: i processi, anche appartenenti a nodi diversi, controllano e risolvono i conflitti di accesso alle risorse tra loro condivise.

Il carico dei due nodi è bilanciato in modo dinamico e qualsiasi intervento operativo, compreso installazione di nuovo software di base (ad es. nuova versione sistema operativo) o applicativo, o upgrade dei nodi (ad es. sostituzione con server di maggior potenza) non comporta alcuna interruzione del servizio.

Conclusioni

Il sistema è stato sviluppato per permettere la verifica automatica della firma digitale di un flusso di messaggi destinati a ulteriori elaborazioni automatiche. Il contesto di sviluppo e sperimentazione del sistema è stata la Registration Authority italiana. La sperimentazione è stata effettuta su un insieme ristretto di Maintainer al fine di testare ed eventualmente mettere a punto il sistema.

La sperimentazione del sistema, ha manifestato numerosi vantaggi:

- Efficienza nel servizio;
- Miglioramento nella qualità del servizio: la firma digitale fornisce un metodo di autenticazione forte, rispetto ai tradizionali meccanismi di user e password (autenticazione debole).
- Trasparenza del servizio per gli operatori - non è richiesta alcuna formazione;
- Affidabilità nel processo di verifica della firma digitale e nella archiviazione dei dati;
- Basso costo.

Il sistema è attivo da diversi mesi durante i quali non sono stati rilevati particolari problemi.

Bibliografia

[1] Registration Authority Italiana - http://www.nic.it/
[2] Francesco Gennai, Marina Buzzi. Integrating security services with the automatic processing of e-mail content. TERENA Networking Conference 2001, 14 - 17 May 2001, Antalya (Turkey).
[3] Francesco Gennai, Marina Buzzi. Posta Elettronica e sicurezza: una applicazione. XXXIX Congresso AICA - Como 19-22 settembre 2001.
[4] J. Galvin, S. Murphy, S. Crocker N. Freed - RFC 1847. Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted. http://www.imc.org/rfc1847, October 1995.
[5] R. Housley. RFC 2630: Cryptographic Message Syntax, http://www.imc.org/rfc2630, June 1999.
[6] R B. Ramsdell - RFC 2633: S/MIME Version 3 Message Specification. http://www.imc.org/rfc2633, June 1999.
[7] B. Ramsdell. RFC 2632: S/MIME Version 3 Certificate Handling. http://www.imc.org/rfc2632, June1999.
[8] Housley,W. Ford, W. Polk, D. Solo - I-D: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, http://search.ietf.org/internet-drafts/draft-ietf-pkix-new-part1-12.txt - January 2002.
[9] PMDF - http://www.process.com/.
[10] David Jones. OSU HTTP Server http://www.er6.eng.ohio-state.edu/www/doc/serverinfo.html.
[11] The OpenSSL Project - http://www.openssl.org/.
[12] Francesco Gennai. Il sistema fax della Registration Authority. IAT-B4-2001-014. 12 Novembre 2001.
[13] Francesco Gennai. Guida rapida all'utilizzo del sistema fax-RA. IAT-B4-2001-018, - 1 Dicembre 2001.
[14] Francesco Gennai. Descrizione Signing Form Module MV:SIGNFORM, Aprile 2001.
[15] B. Kaliski, Request for Comments: 2315. - March 1998. ftp://ftp.isi.edu/in-notes/rfc2315.txt.