Infrastruttura IGPEC

Documentazione tecnica

Sistema Pubblico di Connettività

Scopo del Documento:

Lo scopo del presente documento è descrivere l'infrastruttura del servizio di Indice dei Gestori di PEC.

Sommario

0. GENERALITA'

0.1 Applicabilità

Il presente documento si applica all'infrastruttura preposta all'erogazione del servizio di Indice dei gestori di PEC.

0.2 Assunzioni

Non applicabile.

0.3 Riferimenti

Identificativo	Titolo/Descrizione
DPCM	D.P.C.M del 31 Ottobre 2000
Regole Tecniche	Posta Certificata – Allegato Tecnico CNIPA

0.4 Definizione ed Acronimi

Definizione / Acronimo	Descrizione
SPC	Sistema Pubblico di Connettività
PEC	Posta Elettronica Certificata
IGPEC	Indice dei Gestori di PEC
IANA	Internet Assigned Numbers Authority
DigitPA	Ente nazionale per la digitalizzazione della Pubblica Amministrazione
PEM	Privacy Enhanced Mail

1. Generalità sul servizio di Indice dei Gestori di PEC

La caratteristica saliente del modello di funzionamento della PEC prevede la presenza di più gestori del servizio che operano in modo paritetico. Questo modello federato è sicuramente più potente e flessibile rispetto a modelli di erogazione centralizzati ma richiede, per un corretto funzionamento, la realizzazione di ulteriori servizi che si integrino in tale modello.

In particolare la comunità dei gestori di PEC deve riconoscere in modo univoco l'appartenenza di un dominio al sistema di PEC. Come definito nelle Linee Guida "… il servizio di PEC rende disponibili tutte le sue funzionalità nel caso in cui sia il mittente sia il destinatario, fanno riferimento a un proprio gestore del servizio, eventualmente coincidente, presente nell'indice dei Gestori di PEC".

Inoltre, la presenza di un numero apprezzabile di Gestori del servizio e di fornitori di soluzioni software in congiunzione con l'indispensabile aggiornamento delle regole della PEC e il contesto normativo e tecnologico in continua evoluzione, rende indispensabile un servizio che verifichi l'interoperabilità dei Gestori/soluzioni con una piattaforma di riferimento.

Nel seguito del documento sarà illustrata l'implementazione del servizio nelle sue componenti.

Da un punto di vista funzionale, il servizio "Indice dei Gestori di Posta Elettronica Certificata" è suddiviso nelle seguenti componenti:

- Servizio di directory LDAP;
- Web server;
- Servizio di gestione dell'Indice.

La prima componente realizza la base dati, vera e propria, dell'Indice dei Gestori di PEC, non accessibile dall'esterno. All'interno di questa base dati, sono inseriti i dati riguardanti i provider, le informazioni relative ai domini di Posta Certificata gestiti ed infine i certificati digitali utilizzati per firmare i messaggi di PEC.

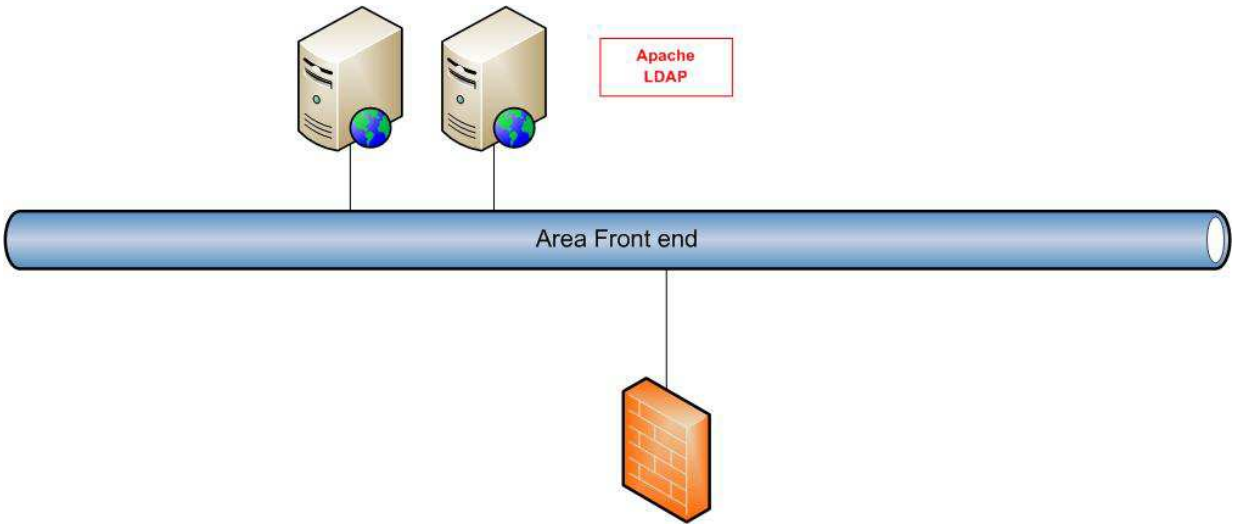
Il web server, invece, permette il download delle informazioni contenute nell'indice ai fini della duplicazione dell'Indice stesso presso gli altri provider. Attraverso il web server, infatti, le informazioni presenti nella base dati possono essere accedute da un qualsiasi browser web attraverso il protocollo HTTPS, previa autenticazione mediante certificato di accesso rilasciato dal DigitPA

Il servizio di gestione dell'Indice, infine, rappresenta la codifica di tutti i processi che riguardano le operazioni di:

- Verifica della aderenza di un provider agli standard;
- Inserimento/cancellazione dei provider dall'Indice;
- Aggiornamento delle informazioni di un provider;

1.1 Dettaglio infrastruttura e storage

L'infrastruttura realizzata consiste di due server paritetici configurati in cluster in modalità hot-standby attraverso il prodotto heartbeat.



Entrambi i nodi sono configurati in maniera speculare ed ospitano i servizi web ed ldap necessari al funzionamento dell'Indice.

L'allineamento dei due sistemi avviene contestualmente all'esecuzione della procedura di aggiornamento dei dati: un batch, terminate le operazioni di aggiornamento, si occupa di trasferire dal nodo attivo al nodo passivo i data file di LDAP ed il file ldif firmato che pubblica le informazioni dell'indice.

Il sistema, tenuto conto del particolare carico di lavoro e delle dimensioni dei dati, non prevede l'impiego di un sottosistema storage esterno.

Le occupazioni di spazio sui dischi interni dei due sistemi, al momento della stesura del presente documento, sono le seguenti:

Database LDAP: 200Mb circa

Sito web (comprensivo di procedura di aggiornamento, configurazioni e log giornaliero dell'applicazione): 4Gb circa

1.2 Dettaglio principali sofwtare installati

Di seguito il riepilogo dei sofware necessari per l'erogazione del servizio.

Prodotto	Versione
Apache httpd server	2.2.3-X
Openldap	2.3.43-X
Heartbeat	2.1.3-X
Perl	5.8.8-X
Openssl / Openssl-perl	0.9.8e-X

2. Realizzazione del Directory Server

In questo paragrafo è illustrata la realizzazione del servizio di Directory LDAP dell'Indice dei Gestori di PEC, fornendo le indicazioni sullo schema del directory, unitamente ai dettagli di installazione e di configurazione del software applicativo utilizzato dalla componente.

2.1 Definizione dello schema

Lo schema del directory server può essere definito come l'insieme delle definizioni dei tipi (o classi) di oggetti (objectclass) e, dei tipi di informazioni su tali oggetti che è possibile memorizzare al suo interno.

In questo paragrafo viene fornita la definizione dello schema del servizio di directory per l'Indice dei Gestori della PEC per il quale non viene utilizzato alcuna objectclass o attributo standard definito nella RFC 2256, poiché non applicabili allo schema adottato. Di seguito verrà fornita una descrizione delle estensioni allo schema e per ciascuna Objectclass o attributo, saranno riportati gli identificativi OID (Object IDentifier) come da RFC.

Di seguito riportiamo delle tabelle che definiscono gli attributi e le classi di oggetti necessari a definire lo schema così come definito nel documento delle "Regole Tecniche della PEC": per ciascun'estensione è necessario definire un OID univoco, sulla base della numerazione messa a disposizione dallo IANA al CNIPA.

2.2 Attributi

Per ciascun attributo definiamo il nome, la descrizione, l'OID, il tipo (cis=Case Insensitive String; css=Case Sensitive String; dn=Distinguish Name) e se è richiesto che questo sia unico per ciascun oggetto.

Nome Attributo	Descrizione	OID	Tipo	Unico
providerCertificateHash	Rappresentazione esadecimale (40 caratteri) dell'hash in formato SHA1 del certificato usato dal gestore per la firma delle ricevute e delle buste	16572.2.2.1	cis	Si
provider Certificate	Certificato X.509 in formato binario ASN.1 DER	16572.2.2.2	cis	No
providerName	Nome del gestore di posta certificata	16572.2.2.3	cis	Si
mailReceipt	E-mail a cui inviare le ricevute di presa in carico	16572.2.2.4	cis	Si
managedDomains	Domini gestiti dal gestore di posta certificata	16572.2.2.5	cis	No
LDIFLocationURL	URL (HTTP) del file LDIF che definisce la entry	16572.2.2.6	css	Si
providerUnit	Nome dell'ambiente operativo secondario	16572.2.2.7	cis	Si

2.3 Objectclass

Per ciascuna objectclass da definire, andiamo a specificare il nome, la objectclass superiore nonchè gli attributi richiesti e quelli consentiti, per i suoi oggetti.

Dalla tabella escludiamo, per semplicità, gli attributi ereditati dalla objectclass superiore.

Per l'identificativo di ciascuna objectclass si utilizza una numerazione progressiva sulla base di quella assegnata dallo IANA al DigitPA.

Nome Objectclass	Objectclass superiore	OID	Attributi richiesti	Attributi consentiti
LDIFLocationURLObject	top	16572.2.1.1		LDIFLocationURL
provider	top	16572.2.1.2	providerCertificateHash providerCertificate providerName mailReceipt managedDomains	Description, providerUnit, LDIFLocationURL

2.4 Realizzazione directory server LDAP

Il directory server costituisce la base dati vera e propria dell'iGPEC; la soluzione proposta prevede l'utilizzo del software openLDAP, distribuito con la piattaforma linux RedHat ed installato su due sistemi distinti.

L'alta affidabilità della componente, è demandata al software di clustering heartbeat mentre la consistenza dei dati tra i due host che svolgono il servizio è demandata alle operazioni di fermo e copia a freddo dei datafile di openldap durante le operazioni di aggiornamento dell'indice. La ridondanza sui dischi, invece, è gestita a livello hardware dal controller RAID dei sistemi che ospitano il servizio.

2.4.1 Schema del Directory

Per gli attributi la sintassi come da RFC 2252 è la seguente:

```
attributetype ( 16572.2.2.1
        NAME 'providerCertificateHash'
        DESC 'Hash SHA1 del certificato X.509 in formato
esadecimale'
        EQUALITY caseIgnoreIA5Match
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{40} )

attributetype ( 16572.2.2.2
        NAME 'providerCertificate'
        DESC 'Certificato X.509 in formato binario ASN.1 DER'
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.8 )

attributetype ( 16572.2.2.3
        NAME 'providerName'
        DESC 'Nome del gestore di posta certificata'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768}
        SINGLE-VALUE )

attributetype ( 16572.2.2.4
        NAME 'mailReceipt'
        DESC 'E-mail a cui inviare le ricevute di presa in
carico'
        EQUALITY caseIgnoreIA5Match
        SUBSTR caseIgnoreIA5SubstringsMatch
```

```
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{256}
        SINGLE-VALUE )

attributetype ( 16572.2.2.5
        NAME 'managedDomains'
        DESC 'Domini gestiti dal gestore di posta certificata'
        EQUALITY caseIgnoreIA5Match
        SUBSTR caseIgnoreIA5SubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

attributetype ( 16572.2.2.6
        NAME 'LDIFLocationURL'
        DESC 'URL (HTTP) del file LDIF che definisce la entry'
        EQUALITY caseExactMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )

attributetype ( 16572.2.2.7
        NAME 'providerUnit'
        DESC 'Nome dell'ambiente operativo secondario'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768}
        SINGLE-VALUE )

objectclass ( 16572.2.1.1
        NAME 'LDIFLocationURLObject'
        DESC   'Classe   per   inserimento   di   un   attributo
LDIFLocationURL'
        MAY ( LDIFLocationURL )
        SUP top AUXILIARY )

objectclass ( 16572.2.1.2
        NAME 'provider'
        DESC 'Gestore di posta certificata'
        SUP top
        MUST    ( providerCertificateHash $
                  providerCertificate $
                  providerName $
                  mailReceipt $
                  managedDomains)
        MAY     ( description $
                  LDIFLocationURL $
                  providerUnit) )
```

Tale sintassi, può essere utilizzata direttamente per OpenLDAP. Le definizioni vanno salvate all'interno di un file "pcert.schema" che dovrà successivamente essere indicato come estensione dello schema standard mediante la direttiva "include" nel file di configurazione del prodotto, che sarà descritto nei paragrafi successivi.

2.4.2 Creazione Indici

Un indice per il directory server è una partizione del suo database, la cui chiave di ricerca principale è un dato attributo: la creazione di indici evita che la ricerca di entry caratterizzate da un valore specifico di un certo attributo sia effettuata in modo sequenziale su tutto il db.

Ai fini dell'oggetto che si va ad implementare, si ritiene indispensabile andare ad indicizzare gli attributi secondo i criteri presentati nella tabella che segue

Attributo	Equality (attr=val)	Presence (attr=*)	Substring (attr=*string*)
providername	x		
managedDomains	x	x	x
providerCertificateHash	x	x	x
ldifLocationUrl	x		x

In questo modo, il tempo di ricerca per query che riguardano i nomi dei provider, i domini gestiti e le URL da cui scaricare i files LDIF, si abbassanno.

2.4.3 Configurazione OpenLDAP

Il prodotto OpenLDAP viene installato unitamente al software di base.

La configurazione del servizio si effettua editando il file "`/etc/openldap/slapd.conf`"; inserendo le seguenti direttive:

```
include         /etc/openldap/schema/pcert.schema
suffix            "o=postacert"
rootdn          "cn=Directory Manager,c=it"
rootpw          <password>
...
access to *
             by dn="cn=Directory Manager,c=it" write
             by * read
```

La direttiva "suffix" definisce la radice del directory server: "o=postacert" è la radice su cui si innestano i rami relativi ai dati dei gestori di PEC.

Le direttive "rootdn" e "rootpw" definiscono rispettivamente l'identificazione e la password di accesso dell'amministratore del directory server: l'unica utenza con privilegi illimitati di lettura e scrittura.

Il file "/etc/openldap/schema/pcert.schema" definito mediante la direttiva "include", infine, contiene lo schema esteso dell'Indice. Si tratta di un file di testo che contiene la definizione di attributi ed objectclasses secondo la sintassi stabilita da RFC 2252 e riportata in precedenza.

2.4.4 Inizializzazione del DB

Prima di attivare il demone di OpenLDAP è necessario inizializzare il suo database.

Tipicamente si crea un file LDIF contenente le informazioni minime per tutte le direttive "suffix" presenti nel file di configurazione; ad esempio:

```
dn: o=postacert
objectClass: top
objectClass: organization
objectClass: LDIFLocationURLObject
o: postacert
```

```
description: Base root per l'indice dei gestori di posta
   certificata
LDIFLocationURL: https://igpec.ctrupa.it/igpec.ldif
```

Supponiamo che tale file venga chiamato “/tmp/init.ldif”; i comandi per inizializzare il database sono i seguenti:

```
# rm -f /var/lib/ldap/*
# slapadd -v -f /etc/openldap/slapd.conf -l /tmp/init.ldif
```

Successivamente, la proprietà dei files del database appena creato va data all’utente “ldap”, con il comando che segue:

```
# chown -R ldap:ldap /var/lib/ldap/*
```

A questo punto OpenLDAP può essere attivato e si possono iniziare le operazioni di caricamento dei dati.

3. Realizzazione del web server

L'interfaccia web consente la consultazione dei dati presenti nell'IGPEC, finalizzata al download dell'indice stesso da parte dei provider che partecipano.

La soluzione prevede l'utilizzo di Apache Web Server installato su kernel Linux sulle stesse macchine che erogano il servizio di directory LDAP.

L'alta affidabilità, come nell'altro caso è garantita dal software di clustering heartbeat.

Per quanto riguarda la configurazione del demone httpd di Apache web server, occorre editare i files "/etc/httd/conf/httpd.conf" e "/etc/httd/conf/ssl.conf".

Il principio guida della configurazione è quello di inserire tutta la configurazione del web in un "virtual host" corrispondente al nome dns "igpec.cnipa.it".

```
<VirtualHost 0.0.0.0:443>
ServerName igpec.cnipa.it
DocumentRoot /IGPEC/igpec.cnipa.it
DirectoryIndex index.html index.php
CustomLog logs/igpec.cnipa.it_ssl_access_log common-ssl
ErrorLog logs/igpec.cnipa.it_ssl_error_log
LogLevel info
SSLEngine on
SSLProtocol all -SSLv2
SSLCipherSuite
ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW
SSLCertificateFile /IGPEC/certificati/public/igpec-web.crt
SSLCertificateKeyFile /IGPEC/certificati/private/igpec-web.key
SSLCACertificatePath /IGPEC/certificati/public/trusted
SSLVerifyClient require
SSLVerifyDepth 5
<Directory /IGPEC/igpec.cnipa.it>
  SSLRequireSSL
  SSLRequire \
  %{SSL_CLIENT_S_DN}        eq        "/C=IT/O=EDS        Pubblica
Amministrazione/CN=www.edspa.it" or \
  %{SSL_CLIENT_S_DN}    eq    "/C=IT/O=HP    Enterprise    Services
Italia/CN=Posta Elettronica Certificata" or \

...

</Directory>

</VirtualHost>
```

Molto importanti sono le righe della configurazione che stabiliscono l'accesso al file contenente l'indice dei gestori. A tale fine viene controllato:

- la validità del certificato (la sua scadenza)
- la CA emittente
- il DN del certificato che deve avere corrispondenza in una delle righe della direttiva SSLRequire illustrate sopra.

3.1.1 Rotazione dei log di Apache

Giornalmente, a mezzanotte, il file di log degli accessi deve essere ruotato mediante una procedura in crontab.

Tale procedura provvede a congelare il file di log del giorno ed a rinominarlo in “webipaN_DD_MM_YYYY.log”, dove N è l’id del sistema, DD è il giorno, MM è il mese e YYYY è l’anno.

Giornalmente i log ruotati vengono salvati su nastro con retention corrispondente ai termini previsti dalla legge per la conservazione di questo tipo di dato.

I certificato del Web Server è fornito dal Responsabile dell’Indice.

4. Servizio di Gestione

Nel processo di gestione dell'indice sono coinvolti diversi attori con ruoli diversificati rispetto a compiti specifici quali:

- Accreditamento di un provider;
- Aggiornamento dei dati di un provider.
- Download e consultazione dell'Indice;
- Cancellazione di un provider

I principali attori coinvolti nella gestione dell'indice possono essere riassunti dalle seguenti figure.

Responsabile igPEC. Ha il compito di raccogliere le richieste dei candidati all'accreditamento nell'indice dei gestori e di comunicarle al Gestore dell'Indice. Tale figura/funzione dove essere svolta dal DigitPA.

Provider di PEC. Generico provider internet che offre un servizio di Posta Elettronica Certificata così come descritto dalla normativa.

Gestore igPEC. Ha il compito di:

1. Verificare la rispondenza dei provider di Posta Certificata ai requisiti imposti dalla normativa. Tale verifica controlla l'aderenza del singolo progetto alle "regole tecniche" e prevede un certo numero di test di interoperabilità con i sistemi del provider.
2. Comunicare l'esito dei test di Interoperabilità al Responsabile dell'Indice, il quale, a fronte di un esito positivo delle verifiche può richiedere l'inserimento del provider.
3. Inserire nell'indice, su richiesta del Responsabile dell'Indice, i dati di un provider di PEC.

Il Gestore dell'Indice è inoltre responsabile delle operazioni di aggiornamento periodico della base dati, delle operazioni di verifica sintattica e semantica dei dati contenuti nell'Indice e delle operazioni di manutenzione periodica dello stesso.

Tutte le comunicazioni di Accreditamento e Accesso che il Responsabile dell'indice invierà al Gestore dell'Indice dovranno essere effettuate in formato cartaceo, su carta intesta oppure tramite PEC.

4.1 Accreditamento di un Provider

4.1.1 Inserimento

La procedura prevista per l'accreditamento di un provider presso l'indice prevede i seguenti passi:

1. Il Responsabile dell'Indice invia al Gestore dell'Indice la richiesta di accreditamento del provider. Tale richiesta conterrà le seguenti informazioni:
    1. Nome univoco del provider;
    2. Referente per la gestione dei contatti diretti con il provider;
    3. URL da cui scaricare il file LDIF per l'inserimento nell'Indice dei Gestori;
2. In seguito alla richiesta del Responsabile dell'Indice, il Gestore dell'Indice provvederà al caricamento dei contenuti del file LDIF nella base dati e a notificare al Responsabile dell'Indice l'avvenuto accreditamento.
3. In caso di difformità a livello sintattico o di contenuti, il Gestore dell'Indice richiederà al provider di effettuare le correzioni del caso.

4.1.2 Aggiornamento

I dati contenuti nell'Indice dei Gestori sono aggiornati mediante batch automatico schedulato sei volte al giorno.
In caso di errori sintattici o di coerenza in fase di aggiornamento, il Gestore dell'Indice informerà il Provider interessato e il Responsabile dell'Indice.
La comunicazione sarà effettuata utilizzando il contatto indicato nel fax di richiesta (generalmente la email del referente).

4.1.3 Cancellazione

La cancellazione di un provider è a carico del Gestore dell'Indice che, su richiesta del Responsabile dell'Indice, previo backup, rimuove i dati contenuti nell'indice, eliminando il provider dalla procedura di aggiornamento automatico.

4.1.4 Controlli Sintattici

L'accreditamento e l'aggiornamento di un provider prevede una serie di controlli formali dettati dalle "*Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata*" paragrafo 7.5 "*Schema indice dei gestori di posta certificata"* disponibili sul sito del Responsabile dell'Indice http://www.digitpa.gov.it/pec .

Una volta scaricato il file LDIF firmato (p7m) e verificata la firma sono controllati:

providerName: deve coincidere con la denominazione specificata in fase di accreditameto.

providerCertificate e providerCertificateHash: ciascun providerCertificate deve avere un providerCertificateHash associato (*Rappresentazione esadecimale di 40 caratteri dell'hash in formato SHA1 del certificato usato dal gestore per la firma delle ricevute e delle buste*)

managedDomains: la lista dei managedDomains non ammette duplicati.

mailReceipt: il campo deve rispettare la rfc822 ed il dominio deve avere un record MX.

LDIFLocationURL: deve essere definito e non deve essere presente in una providerUnit.

Tutti i controlli sopra indicati sono bloccanti, quindi la non conformità rispetto a una di queste norme interrompe l'accreditamento o l'aggiornamento del provider, segnalando l'anomalia via posta elettronica, sia al Referente del Gestore di PEC che al Responsabile dell'Indice. Il record LDAP del provider non sarà modificato, quindi nella successiva fase di pubblicazione dell'Indice saranno utilizzate le informazioni acquisite nell'ultimo aggiornamento del Gestore PEC andato a buon fine. Sarà cura del Referente del Gestore correggere il file che sarà quindi processato al successivo aggiornamento dell'Indice.

Al campo managedDomains è applicato un ulteriore controllo che verifica la registrazione del dominio e la presenza di un record MX associato. Qualora ci fossero dei domini non rispettino queste regole, la procedura non sarà interrotta e superati tutti i precedenti controllo il provider verrà accreditato o aggiornato. Al Referente del Gestore di PEC e al Responsabile dell'indice sarà inviata una mail riportante l'anomalia.

A causa dell'elevato numero di domini (circa duecentomila) la procedura è stata modificata in modo da verificare esclusivamente i domini non ancora verificati, questo significa che una volta che un dominio è stato verificato, non sarà più controllato.

4.1.5 Gestione dei domini duplicati

Quando un dominio passa da un gestore ad un altro c'è la possibilità che il Gestore subentrante non possa essere in grado di aggiornare il proprio provider all'interno dell'Indice. Le cause possono essere due:

1. Il Gestore cedente non ha rimosso il dominio dalla sua lista dei managedDomains
2. L'aggiornamento del Gestore subentrante è eseguito prima del Gestore cedente.

Nel primo caso sarà cura del Gestore subentrante e del Responsabile dell'Indice prendere contatto con il gestore cedente per la rimozione del dominio.
Nel secondo caso, qualora il Gestore di PEC o il Responsabile dell'Indice ne facciano richiesta, sarà possibile azzerare il tempo di "migrazione" del dominio (che altrimenti potrebbe richiedere 2 aggiornamenti dell'indice e quindi almeno 8 ore) modificando il file di configurazione in modo che il Gestore subentrante venga eseguito dopo il Gestore cedente.
L'applicazione, legge in maniera sequenziale il file di configurazione "/IGPEC/providers.conf" e in base a questo ordine processa i provider uno alla volta. Sarà quindi possibile spostare il Gestore subentrante in una riga successiva il Gestore cedente (o viceversa).

4.2 Accesso all'indice

4.2.1 Inserimento

La procedura prevista per l'accesso al download dell'indice prevede i seguenti passi:

1. Il Responsabile dell'Indice invia al Gestore dell'Indice la richiesta di accesso contenente:
   a. il certificato pubblico da autorizzare;
   b. la catena dei certificati delle Certification Autority che lo hanno firmato (può essere omesso qualora siano già stati inviti in un precedente accreditamento)
2. Il Gestore dell'Indice andrà ad aggiungere nella configurazione dei Web e provvederà al loro riavvio.

4.2.2 Aggiornamento

La procedura di aggiornamento è prevista solo nel caso in cui il "subjet" del certificato cambi oppure cambi uno dei certificati delle CA che lo hanno firmato.

Il Responsabile dell'Indice invia al Gestore dell'Indice invierà l'utenza da aggiornare e quest'ultimo provvederà alla mofica dell'autorizzazioni in maniera analoga al precedente paragrafo.

4.2.3 Cancellazione

Il Responsabile dell'Indice invia al Gestore l'utenza da revocare e/o le eventuali CA da rimuovere dall'elenco delle CA autorizzare. Il Gestore provvederà alla rimozione dell'utenza dal file di configurazione del web server e/o la rimozione del file contenente il certificato della CA da rimuovere e a riavviare il web server.

5. Batch

5.1 Aggiornamento dell'indice

L'aggiornamento dell'Indice come indicato in precedenza è schedulato con cadenza di 4 ore a partire dalle 00:30 tramite "crontab"

```
30 */4 * * * root /IGPEC/igpec-update.pl > /IGPEC/logs/igpec.log 2>&1
```

La procedura è un batch Perl, che utilizza i seguenti moduli:

- `Crypt::SSLeay`
- `Data::Validate::Domain`
- `Digest::SHA1`
- `Email::Valid`
- `LWP::UserAgent`
- `Mail::Sendmail`
- `Net::DNS`
- `Net::LDAP`
- `Net::LDAP::Entry`
- `Net::LDAP::LDIF`
- `Net::LDAP::Schema`
- `Tie::DNS`
- `List::MoreUtils`

La procedura è suddivisibile in due fasi:

1. Download e Verifica:
   - Scaricare il file ldif firmato di ciascun provider
   - Verificare la corretta firma del file
   - Verificare la corretta formattazione del file ldif
   - Validazione dei dati rispetto alle Norme Tecniche
2. Caricamento e Pubblicazione:
   - Aggiornamento dei dati di ciascun Gestore (qualora fossero cambiati)[1]
   - Pubblicazione e firma dell'Indice dei Gestori

[1] Non essendo prevista la pubblicazione di LDIF incrementali, l'aggiornamento di un provider è di fatto la sua cancellazione e creazione.

La fase di caricamento, e quindi modifica della base dati, è vincolata al superamento di tutte le verifiche sintattiche e formali (dettagliate nel paragrafo 4.1.4).

Di particolare criticità è la fase di Aggiornamento, vincolato dal formato, la procedura ha l'obbligo di cancellare il vecchio "record". A protezione di eventuali errori, la procedura esegue un backup del Gestore e qualora il caricamento non vada a buon fine provvede al suo ripristino. Generalizzando, la procedura non effettua nessuna modifica al Gestore in presenza di qualsiasi errore.

Il batch è schedulato esclusivamente su uno dei due nodi del cluster (definito nodo attivo) e la sua abilitazione o rimozione e gestita interamente dal cluster in maniera da garantire l'esecuzione su un solo nodo del cluster.

I file di configurazione sono:

1) /IGPEC/provider.conf contenente l'elenco di tutte le informazione relative ai Gestori PEC
2) /IGPEC/ldap.conf che oltre a contere le informazione relative all'autenticazione del server ldap contiene anche le variabili utilizzate dal batch relative ai certificati e alle notifiche.

5.2 Backup

Il Backup dell'Indice come per l'aggiornamento è schedulato con cadenza di 4 a partire dalle 00:00 tramite "crontab" la sua schedulazione è gestita in maniera analaga al batch di aggiornamento.

```
0 */4 * * * root /IGPEC/igpec-backup.sh > /IGPEC/logs/igpec.log 2>&1
```

5.3 Sincronizzazione della base dati LDAP

La sincronizzazione del nodo passivo è effettuata copia dei datafile sul nodo passivo. La procedura è schedulata 5 minuti dopo l'avvio della procedura di aggiornamento, e la sua schedulazione è gestita dal cluster.

```
35 */4 * * * root /IGPEC/IGPECsyncLDAP.sh >> /IGPEC/logs/igpec.log 2>&1
```

5.4 Sincronizzazione file system

La sincronizzazione del nodo passivo è effettuata tramite rsync dal nodo passivo stesso.

Come in precedenza è il cluster che si occupa della schedulazione del batch di sincronizzazione.

```
*/10 * * * * root /IGPEC/IGPECsync.sh > /IGPEC/logs/igpec.log 2>&1
```

6. Procedure e comandi

6.1 Abilitazione Accesso

Estrarre il subject dal certificato ricevuto

```
#openssl x509 -noout -subject -in certificato.pem
```

La stringa ottenuta è del tipo:

subject=

/C=IT/O=POSTECOM S.P.A. - GRUPPO POSTE ITALIANE/CN=POSTECERT CLIENT LDIF

Su entrambi i sistemi copiare il subject ottenuto con il comando precedente, nel file /etc/httpd/conf.d/ssl.conf (previo backup del file di configurazione ssl.conf) nella sezione

```
<Directory /IGPEC/igpec.cnipa.it>
 SSLRequireSSL
 SSLRequire
```

In particolare, inserire in coda alle stringhe già esistenti, questo tipo di stringa:

%{SSL_CLIENT_S_DN} eq "/C=IT/O=POSTECOM S.P.A. - GRUPPO POSTE ITALIANE/CN=POSTECERT CLIENT LDIF"

Inoltre, alla fine della stringa precedente a quella appena inserita, occorre aggiungere "or \".

Su entrambi i sistemi ricaricare il file di configurazione di Apache con il seguente comando:

```
#/etc/init.d/httpd reload
```

6.1 Accreditamento di un Provider

Le operazioni di accreditamento vanno eseguite sul nodo attivo del cluster. I file che si andranno a modificare, infatti, sono automaticamente trasferiti sull'altro server mediante la sincronizzazione schedulata in crontab.

Sul server su cui è attivo il servizio ldap, editare il file /IGPEC/providers.conf ed inserire i seguenti campi, separati da "::" , in modo sequenziale:

1. Progressivo
2. Nome del provider[2]
3. indirizzo e-mail del referente (se più di uno utilizzare la virgola come separatore)
4. URL da cui scaricare il file .p7m

Esempio:

00022:: ...
00023:: ...
00024::ACME::taddeo@looneytunes.it::https://acme.looneytunes.it/pec/bugsbunny.ldif.p7m

[2] il nome del provider è indicato sul fax, ma esso deve essere identico al campo "ProviderName" contenuto nel DN del file ldif, pertanto è consigliabile verificare tale campo collegandosi, tramite browser, alla URL indicata nel fax, e in caso di anomalie contattare il Responsabile dell'Indice.

6.2 Comandi utili

Verifica la firma
```
# openssl smime -verify -in file.p7m -inform DER -CAfile CA.crt
```

Verifica la firma ed estrae il file
```
# openssl smime -verify -in file.p7m -inform DER -CAfile CA.crt -out file
```

Verifica la firma ed estrae il file ed il certificato firmante
```
# openssl smime -verify -in file.p7m -inform DER -CAfile CA.crt -out
file -signer certificato_da_estrarre
```

Estrae esclusivamente il certificato dal p7m
```
# openssl smime -verify -in file.p7m -inform DER -noverify -signer
certificato_da_estrarre
```

Legge il contenuto di un certificato
```
# openssl x509 -noout -text -in certificato
```

Legge il subject di un certificato
```
# openssl x509 -noout -subject -in certificato
```

Legge il contenuto di un csr
```
# openssl req -noout -text -in richiesta
```

Firma un file
```
# openssl smime -sign -signer certificato_pubblico_firmante -inkey
chiave_privata_firmante -outform DER -in file_da_firmare -binary
-nodetach -out file_da_firmare.p7m
```

Esporta chiave pubblica e certificato in formato pkcs12 (utile per portarli su MS)
```
# openssl pkcs12 -export -in certificato -inkey chiaveprivata -name
"NOME" -certfile certificatoCA -out certificatoechiave.p12
```

Calcola l'hash sha1 del certificato in caso di aggiunta o rinnovo dello stesso (converte il certificato da PEM in DER e poi calcola l'hash sha1)
```
# openssl x509 -in certificato -inform PEM -outform DER | sha1sum
```

Download dei file in SSL (senza verificare il certificato del server)
```
# curl -x 213.175.2.5:8080 https://url/file.p7m -k > file.p7m
```

Download dei file in SSL (verificando il certificato del server)
```
# curl -x 213.175.2.5:8080 https://url/file.p7m -k --cacert
certificato_della_ca > file.p7m
```

Converte un certificato da DER in PEM
```
# openssl x509 -in cert.der -inform DER -out cert.pem -outform PEM
```

Query ldap per visualizzare il file IGPEC
```
# /opt/sysnet/ldap/bin/ldapsearch -x -LLL -h 127.0.0.1 -p 389 -b o=postacert
```