Proposta di aggiornamento delle specifiche tecniche per la Posta Elettronica Certificata

(Ver. 1.0)

Francesco Gennai, Marina Buzzi e Luca Ferrucci
ISTI-CNR - Area della ricerca di Pisa

15 Settembre, 2014

1 Introduzione

La Posta elettronica ordinaria non fornisce alcuna garanzia all'utente circa la consegna di un messaggio al destinatario e non integra nativamente meccanismi di sicurezza. Per ovviare a ciò, l'utente può applicare meccanismi basati su chiavi crittografiche nella comunicazione tra utenti finali (end-to-end), al fine di garantire l'integrità e confidenzialità del messaggio oltre che l'autenticazione e non ripudio dell'origine. Di contro, l'utilizzo di tali tecnologie richiede una considerevole conoscenza degli strumenti, degli algoritmi e dei rischi da parte degli utilizzatori e per questo non è, al momento, attuabile su larga scala.

La Posta Elettronica Certificata (PEC) [IETF, 2011] rappresenta una soluzione che cerca un compromesso tra la semplicità d'uso e il grado di sicurezza nella trasmissione di un messaggio. Sintetizzando, la PEC è un sistema di trasmissione di messaggi e allegati con validità legale. Esso notifica le fasi di trasmissione e ricezione di un messaggio di posta, emettendo delle ricevute attestanti la presa in carico , la trasmissione e la consegna nella casella postale del destinatario. L'uso di time-stamp permette di "certificare" la data e l'istante di trasmissione/ricezione. Inoltre, quando il messaggio viene consegnato nella casella del destinatario, il mittente riceve una ricevuta di consegna, o, in alternativa, una ricevuta di mancata consegna che indica le specifiche condizioni.

Attraverso questi meccanismi, la PEC consente di superare le "debolezze" della posta elettronica ordinaria, e si rivela come uno strumento fondamentale in qualsiasi contesto che richieda una valida evidenza di trasmissione e di consegna di un documento elettronico.

A livello mondiale sono stati sviluppati sistemi con funzionalità analoghe alla PEC, ma tra loro **NON** interoperabili. Questo è un grave problema, che ostacola l'utilizzo di comunicazioni certificate tra Paesi diversi.

Uno degli obiettivi di questo studio è effettuare una analisi sulle tecnologie e i processi necessari per l'evoluzione tecnologica della PEC, attraverso la sostituzione di alcuni componenti con nuovi basati su recenti standard IETF.

1.1 PEC: nuove potenzialità dai nuovi standard

In questa sezione vengono analizzate funzionalità della PEC che possono essere migliorate attraverso recenti specifiche tecnologiche provenienti dall'IETF, in particolare la possibilità di applicare le tecnologie relative alla gestione dell'identità digitale ai protocolli di Posta Elettronica e di certificare/identificare domini PEC e providers PEC:

- **Identity Management applicato a protocolli di Posta Elettronica:** Le tecnologie di Identity Management si riferiscono alla gestione delle identità digitali, la loro autenticazione, autorizzazione, ruoli e privilegi all'interno o tra sistemi e confini dell'organizzazione, con l'obiettivo di aumentare la sicurezza e la produttività riducendo costi, tempi di inattività e compiti ripetitivi. Questo problema è comune a tutti i servizi che necessitano di autenticare l'identità dell'utente. Ogni organizzazione attualmente gestisce le identità dei propri utenti autonomamente; con un Identity Management può essere possibile una migrazione verso una gestione centralizzata, con alcuni vantaggi, che non vengono quì riportati. Nel gruppo di lavoro IETF Common Authentication Technology Next Generation (Kitten) sono in fase di sviluppo soluzioni che potrebbero essere di interesse per la PEC.

  In questo documento non viene trattata questa problematica, rimandata ad un approfondimento successivo.

- **Certificazione e identificazione dei PEC providers e dei domini PEC**: Attualmente i PEC providers sono identificati e autorizzati da AGID, che ha il compito istituzionale di controllo e supervisione dei gestori e la verifica del rispetto dei requisiti di legge. Ogni provider PEC ha un certificato x.509v3 [IETF, 2008b] rilasciato da AGID stessa, in veste di Certification Authority (CA). I riferimenti ai PEC providers e i domini PEC da loro gestiti sono, nella soluzione attuale, memorizzati in un file LDIF (LDAP Data Interchange Format) [IETF, 2000], mantenuto su un server LDAP centralizzato. Il formato LDIF è utilizzato per importare ed esportare le informazioni tra Directory Server basati su LDAP, o per descrivere un insieme di cambiamenti da applicare a una Directory.

  Nel seguito, si propone di risolvere il problema della certificazione e identificazione dei domini PEC e dei PEC providers con una soluzione che non faccia uso del file LDIF, in quanto l'uso di un file LDIF introduce le seguenti problematiche:

  - **Scalabilità**: deriva dalla natura centralizzata dell'attuale soluzione. Il file LDIF e il traffico di rete verso il Directory Server LDAP, infatti, cresce in dimensione con l'aumentare del numero di PEC providers, del numero dei domini PEC e dei certificati X.509v3, diventando in breve tempo ingestibile da mantenere, aggiornare e sostenere, anche in termini economici, per un'unica entità.

– **Distribuzione**: Ogni volta che viene aggiunto, cancellato o sostituito un PEC provider, un dominio PEC o un certificato X.509v3, deve essere aggiornato il file LDIF, che deve essere ridistribuito. Questa distribuzione deve essere effettuata nel modo più efficiente possibile rispetto all'uso di un Directory Server LDAP centralizzato.

In questo documento si descrive una proposta di modifica della PEC basata sull'uso del DNS con estensioni sicure, uno strumento ormai standardizzato e ampiamente utilizzato fin dalla sua introduzione da parte dell'IETF nel 2006. Nelle sezioni 1.2 e 1.3 si descrive, in maniera sintetica ma sufficientemente esaustiva per gli scopi di questo documento, lo standard DNS e la sua estensione sicura, DNSSec.

1.2 Domain Name System (DNS): caratteristiche, funzionamento e standard di riferimento

Il DNS è una infrastruttura client server distribuita essenziale per il funzionamento della rete Internet che mantiene la gerarchia dei nomi di dominio e fornisce servizi di traduzione tra i nomi di dominio e gli spazi di indirizzi IP. E' costituito dai Name Server e da un protocollo di comunicazione che definisce un formato standard per la sottomissione e la risposta a query.

Un Name Server memorizza le informazioni suddette sottoforma di record di risorse (Resource Record) DNS, ognuno corrispondente ad un nome a dominio, e risponde a query al suo database, come specificato negli RFC1033 [IETF, 1987a], RFC1034 [IETF, 1987b] e RFC1035 [IETF, 1987c].

La sua organizzazione può essere modellata come una struttura dati ad albero gerarchico rovesciato (con la radice in alto e le foglie in basso). Ogni nodo o foglia nell'albero ha zero o più resource records, che contengono informazioni associate al nome a dominio, come indicato più avanti in questa sezione.

I Name Server sono responsabili di uno o più domini, raggruppati amministrativamente in Zone autoritative, e possono delegare l'autorità su sottodomini ad altri Name Server. Questo meccanismo fornisce un servizio distribuito e tollerante ai guasti, evitando l'uso di un unico database centralizzato.

L'albero è suddiviso in zone con inizio in corrispondenza della zona radice (Root Zone). In figura 1 è possibile vederne un esempio. Nel caso del dominio *www.ietf.org*, il Name Server della zona radice delega un altro Name Server ad essere autoritativo per il dominio *.org*. Quest'ultimo a sua volta delega un altro Name Server ad essere autoritativo per il sottodominio *ietf.org*, fino ad arrivare al dominio foglia.

Ogni record DNS è caratterizzato da un tipo che ne determina le caratteristiche essenziali utili per implementare le sue funzionalità.

Alcuni tipi di record sono:

- **Record A** - definisce la corrispondenza tra un nome ed uno (o più) indirizzi IP. Questo tipo di record implementa la risoluzione dei nomi IP in indirizzi IPv4 (di 32 bit). In particolare, il record A contiene, come

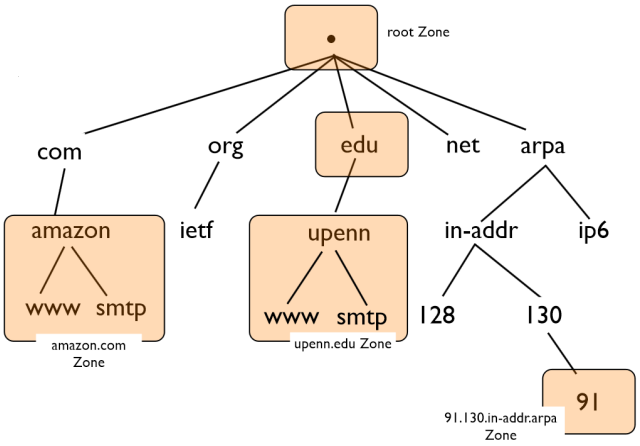

Figure 1: Esempio di un albero DNS

possiamo vedere nell'esempio quì sotto, oltre al nome di dominio, il tipo e la classe, un valore che rappresenta l'indirizzo IPv4 dell'host. Vedi l'RFC1035 [IETF, 1987c].

```
blade3.isti.cnr.it. 86400 IN A 194.119.192.19
```

- **Record MX** - (Mail eXchange) indica i server di posta elettronica per il dominio. In particolare, il record MX contiene, come possiamo vedere nell'esempio quì sotto, oltre al nome di dominio, il tipo e la classe, un valore intero che rappresenta la preferenza e il nome canonico del server di posta che gestisce quel dominio. Vedi l'RFC1035 [IETF, 1987c].

```
isti.cnr.it. 86400 IN MX 10 blade1.isti.cnr.it

isti.cnr.it. 86400 IN MX 10 blade2.isti.cnr.it
```

- **Record CNAME** – E' un alias, cioè un nome alternativo di un certo host, utili per essere raggiungibili dall'esterno con nomi differenti, per es. per servizi diversi. Vedi l'RFC1035 [IETF, 1987c]

- **Record PTR** – E' utilizzato per la risoluzione inversa, ovvero per ottenere il nome di dominio associato a un indirizzo IP. Si utilizzano i record di tipo PTR e un dominio apposito dello spazio dei nomi *in-addr.arpa*. Vedi l'RFC1035 [IETF, 1987c]

.

In figura 2 possiamo vedere un esempio di interrogazione al DNS di un record A, effettuato da un apposito modulo, previsto dallo standard, chiamato

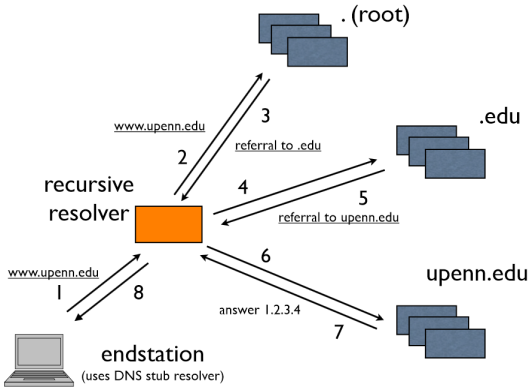

Figure 2: Esempio di risoluzione di una query

Resolver, che si trova sulla macchina client. Nel caso per esempio di query per il dominio *www.upenn.edu*, il Resolver chiede al Name Server di root di risolvere la query. Se questo non ha la risoluzione all'interno della propria cache, risponde dicendo di contattare il Name Server responsabile del dominio *edu*. A questo punto il Resolver sottomette la stessa query al Name Server autoritativo per il dominio *edu*. Questo a sua volta se non ha la risoluzione all'interno della sua cache risponde dicendo di contattare il Name Server responsabile del dominio *uppen.edu*, il quale infine fornisce la risposta al Resolver.

Nell'esempio, la query è costituita da:

- Il campo ID: Identifica un attributo generato dal dispositivo che crea la query DNS. E' copiato dal Name Server nella risposta, cosi che il Resolver possa utilizzarlo confrontando l'ID della richiesta con l'ID della risposta.
- Il campo Query/Response Flag: differenzia le query DNS dalle risposte.
- Il campo opcode può avere i seguenti valori:
  - QUERY: Identifica una query standard
  - IQUERY: Obsoleto
  - STATUS: Notifica lo stato della richiesta al Name Server
  - NOTIFY: Il Name Server primario lo utilizza per notificare al Name Server secondario che la Zona è cambiata
  - UPDATE: Permette ai record DNS di essere aggiunti, cancellati o aggiornati selettivamente
- Il campo AA (Authoritative Answer Flag): indica se il Name Server è autoritativo per la Zona
- Il campo RD (Recursion Desired): Quando è settato in una query, il Resolver richiede che il Name Server gestisca la query ricorsivamente. Il Name Server deve supportare la ricorsione.

- Il campo RA (Recursion Available): indica se il Name Server supporta la ricorsione.
- L'answer section è costituita da:
  - il nome del dominio di cui si è fatta la richiesta
  - il Time To Live (TTL) che indica per quanto l'informazione sarà valida
  - l'etichetta Internet (IN)

Questo standard non protegge da una serie di attacchi informatici, come ad esempio MITM (man in the middle), né garantisce integrità o certezza della provenienza. Queste problematiche sono state risolte con l'introduzione di DNSSec.

1.3 Domain Name System - Security Extensions (DNSSec): caratteristiche, funzionamento e standard di riferimento

DNSSec è un'estensione del DNS standardizzata dall'Internet Engineering Task Force (IETF) che garantisce ai client DNS autenticazione dell'origine dei dati (origin authentication DNS data), autenticazione della non esistenza (authenticated denial of existence), e integrità dei dati (data integrity), ma non disponibilità (availability) o confidenzialità (confidentiality). Tuttavia, una sua implementazione richiede molta attenzione, perché, come per qualsiasi tecnologia di sicurezza, una implementazione non accurata potrebbe causare gravi problemi tecnici e/o operativi.

Lo standard DNS originario è stato ideato per creare un sistema distribuito e scalabile. DNSSec, oltre a questo obiettivo, permette di mantenere la retrocompatibilità con DNS. L'RFC3833 [IETF, 2004] documenta alcune delle minacce conosciute al DNS, risolte da DNSSec.

Il DNSSec è stato progettato per proteggere le applicazioni e i Resolver dall'utilizzo di dati DNS contraffatti o manipolati, come nel caso di attacchi DNS cache poisoning. Tutte le risposte provenienti da Zone DNSSec protette sono digitalmente firmate. Controllando la firma digitale, un Resolver DNS è in grado di verificare se le informazioni sono integre (cioè non modificate e complete, identiche alle informazioni pubblicate dal proprietario della Zona e fornite da un Name Server autoritativo). Anche se la principale preoccupazione è la protezione degli indirizzi IP, DNSSec è in grado di proteggere tutti i dati pubblicati nel DNS. Ad esempio, può essere utilizzato per l'attivazione di altri sistemi di sicurezza che pubblicano i riferimenti a certificati memorizzati nel DNS come Certificate Record (record CERT, RFC4398 [IETF, 2006b]), fingerprint SSH (SSHFP, RFC4255 [IETF, 2006a]), chiavi pubbliche IPSec (IPSECKEY, RFC4025 [IETF, 2005a]), e Trust Anchor TLS (TLSA, RFC6698 [IETF, 2012]).

DNSSec non protegge da attacchi Denial of System (DoS), anche se indirettamente può fornire qualche beneficio.

Altri standard (non DNSSec) vengono utilizzati per proteggere l'invio di grandi masse di dati (bulk data) tra server DNS (come ad esempio un trasferimento di zona DNS).

Le specifiche DNSSec descrivono il protocollo con grande dettaglio. Le originali specifiche (RFC4033 [IETF, 2005b], RFC4034 [IETF, 2005c], RFC4035 [IETF, 2005d]) e successive estensioni (quali l'RFC5155 [IETF, 2008a]) sono state aggiornate dall'RFC6840 [IETF, 2013], che fornisce un insieme di chiarimenti tecnici che sono una preziosa risorsa di riferimento per gli sviluppatori.

I record sono firmati utilizzando la crittografia a chiave pubblica, di cui non parliamo in questo documento. Brevemente si ricorda che consiste in una coppia di chiavi, una privata ed una pubblica, che possono essere utilizzate per autenticazione e/o cifratura. Per l'autenticazione, la chiave pubblica permette di decifrare le informazioni firmate mediante la chiave privata, senza possibilità di risalire a quest'ultima.

DNSSec, per mantenere la retrocompatibilità, integra il DNS con i seguenti nuovi resource record:

- **Record RRSIG** - contiene la segnatura digitale per l'autenticazione di un insieme di resource record. I Resolver DNS validanti verificano la firma con una chiave pubblica, memorizzata in un record DNSKEY.

```
jabber.upenn.edu. IN RRSIG AAAA 5 3 86400 20090719232941(
                                20090619232159 23382 upenn.edu.
                                2...= )
```

  I campi del record hanno i seguenti significati:

  - AAAA: tipo di Record che la segnatura sta firmando
  - 5: tipo di Algoritmo di cifratura
  - 3: etichetta
  - 86400: TTL originale
  - 20090719232941: data di fine validità della segnatura
  - 20090619232159: data di creazione della segnatura
  - 23382: tag della chiave con cui è stata creata la segnatura

- **Record DNSKEY** - contiene la chiave pubblica che un Resolver deve usare per verificare le segnature dei record RRSIG. Viene pubblicato nella zona stessa per poter essere recuperato automaticamente dai Resolver.

  I campi del record hanno i seguenti significati:

  - 256: indica una chiave pubblica che firma l'intera zona
  - 3: indica che la chiave può essere utilizzata solo per firmare la zona DNSSec

```
jabber.upenn.edu. DNSKEY 256 3 5 (
                                A...w
                               ); key id=23382
```

  - 5: algoritmo di segnatura

- **Record DS** - contiene l'hash della chiave pubblica, contenuta in un record DNSKEY, di una zona delegata dalla zona in cui è contenuto il record DS. Serve per costruire una catena di autenticazione che ha inizio da una zona definita, nell'RFC4033 [IETF, 2005b], come Isola di Sicurezza o dalla root zone, se la sua zona è firmata con DNSSec.

  ```
  upenn.edu. 86400 IN DS 8401 5 1 (5248D...606058)
  ```

  I campi del record hanno i seguenti significati:

  - DS: tipo di record
  - 8401: tag della chiave
  - 5: Algoritmo
  - 1: il metodo per calcolare il digest

- **Record NSEC** - Contiene un link al successivo nome di dominio nella Zona e lista i tipi di record che esistono per quel nome di dominio. I Resolver usano i record NSEC per verificare la non-esistenza di un nome e tipo di record come parte del processo di validazione.

```
a.example.com 300 IN NSEC d.example.com. A MX RSIG NSEC
```

I record sono autenticati costruendo una catena di autenticazione a partire da un Trust Anchor di un'Isola di Sicurezza, idealmente la Trust Anchor della root zone. Una Trust Anchor è la chiave pubblica della zona dell'Isola di Sicurezza di cui si può assumere l'affidabilità e autenticità: un Resolver deve memorizzare un Trust Anchor per ogni Isola di Sicurezza che non possiede un DS record, all'interno della Zona delegante, che riferisca la propria chiave pubblica. Per evitare di dover mantenere un numero troppo elevato di Trust Anchor, viene utilizzato un DLV Domain, secondo l'RFC5074 [IETF, 2007b], che contiene un insieme di DLV record che fungono da Trust Anchor. Il DLV record ha esattamente lo stesso formato del DS record, e si indicizza anteponendo il nome del dominio puntato al nome del DLV Domain.

Quando viene usato DNSSec, ogni risposta ad una query contiene un record RRSIG, oltre al tipo di record che è stato richiesto. Il record RRSIG è una firma digitale del set di resource records contenuto nella risposta. La firma digitale viene verificata individuando la chiave pubblica corretta reperita in un

record DNSKEY contenuto nella Zona stessa. Il record NSEC viene utilizzato per fornire la prova crittografica della non-esistenza di qualsiasi resource record; permette di ottenere una forte resistenza contro lo spoofing. Il record DS è pubblicato da una Zona delegante DNSSec ed è utilizzato per autenticare una delle DNSKEY di una Zona delegata, andando a costituire la catena di autenticazione.

Nella prossima sezione viene introdotto uno standard recente, descritto nell'RFC6698 [IETF, 2012], che permette di pubblicare i certificati in standard X.509v3 [IETF, 2008b] all'interno delle Zone DNSSec.

1.3.1 Distribuire i certificati attraverso il DNS

Come detto nella sezione 1.3, la chiave pubblica associata ad un certo dominio è memorizzata all'interno della stessa Zona con vari vantaggi: efficienza nel reperimento della chiave (query DNS), facilità di implementazione, disponibilità di codice open source, e sicurezza, grazie all'esistenza di un'unica catena di autenticazione dalla root al dominio, dato che la chiave di un dominio delegato può essere riferita e autenticata solo dalla chiave del dominio di livello superiore delegante.

Il nuovo scenario che si configura come evoluzione tecnologica futura è DNS-Based Authentication of Named Entities (**DANE**). L'uso della tecnologia da loro introdotta, consente di superare i limiti correnti e in special modo la pubblicazione di certificati X.509v3 per la distribuzione delle chiavi pubbliche associate ai nomi di dominio.

DANE è un gruppo di lavoro IETF che ha l'obiettivo di sviluppare protocolli e tecniche che consentano alle applicazioni Internet di stabilire comunicazioni protette crittograficamente con TLS, DTLS, SMTP, e S/MIME, basate su DNSSec. I nuovi protocolli mirano a definire nuove garanzie e vincoli per il modello tradizionale basato su Public Key Infrastructure, come definito nell'RFC5280 [IETF, 2008b]. Essi potranno anche consentire ai responsabili di un dominio di emettere certificati autonomamente, senza dover più fare riferimento alle CA. Il certificato relativo viene associato al nome di dominio ed è autenticato mediante la catena di autenticazione suddetta.

Il modello basato su CA è fondamentalmente vulnerabile perchè permette ad ogni CA di emettere certificati per ogni dominio. Una singola CA considerata sicura che viene compromessa può rendere insicuro ogni certificato da lei emesso.

L'RFC6698 [IETF, 2012], standardizzato dal gruppo DANE nel 2012 specifica come le informazioni di autenticazione corrispondenti ad un certificato X.509v3 o parti di esso possano essere inserite in una Zona autoritativa DNSsec, introducendo un nuovo tipo di resource record: TLSA.

```
_443._tcp.www.example.com. IN TLSA 0 0 1  d2ab...e971
```

Analizziamo di seguito i parametri del record di tipo TLSA:

- **443**: indica la porta del servizio a cui connettersi
- **tcp**: indica il protocollo di trasporto utilizzato (tcp, udp, ecc...)
- *www.example.com*: indica il nome canonico del server a cui connettersi
- **0**: indica il campo uso che può essere:
  - 0: si usa per specificare la chiave pubblica di un certificato che riferisce una CA.
  - 1: si usa per specificare la chiave pubblica di un certificato che riferisce un'entità foglia. Il certificato deve passare la validazione dell'intera gerarchia mediante PKIX.
  - 2: si usa per specificare la chiave pubblica di un certificato che rappresenta un Trust Anchor per un'Isola di Sicurazza.
  - 3: si usa per specificare la chiave pubblica di un certificato che riferisce un'entità foglia. A differenza del tipo 1, permette all'amministratore di un dominio di emettere un certificato senza richiederlo ad una CA. Non viene controllata l'autenticazione di tutta la catena, ma solo il certificato. Per gli scopi di questo documento, viene usato quest'ultimo tipo di certificato.
- **0**: indica il campo selettore
  - 0: viene effettuato un confronto sull'intero certificato
  - 1: viene effettuato un confronto solo con il SubjectPublicKeyInfo (SPKI) del certificato. L'SPKI, come descritto nell'RFC5280 [IETF, 2008b], rappresenta la parte di un certificato che identifica la chiave pubblica e i suoi attributi (l'algoritmo con cui deve essere utilizzata, il numero di bit, ecc...), ma non la parte che contiene i dati di identificazione dell'entità stessa e della CA. Esso quindi permette di pubblicare un certificato più compatto, eliminandone le parti non necessarie.
- **1**: indica il tipo di confronto:
  - 0: viene effettuato un confronto con l'intero contenuto del certificato
  - 1: viene effettuato un confronto con l'hash SHA-256 del certificato
  - 2: viene effettuato un confronto con l'hash SHA-512 del certificato
- il campo successivo rappresenta il certificato stesso codificato in BASE64

La scadenza contenuta nel certificato estratto dal record TLSA, secondo l'RFC6698 [IETF, 2012], deve essere ignorata, e considerata solo la durata della segnatura del record RRSIG che lo autentica: in sostanza, il certificato è valido solo fino alla scadenza del suo record RRSIG, che quindi ne rappresenta la durata.

La possibile eliminazione della parte che identifica la CA, la sua firma digitale per l'autenticazione del certificato e i dati dell'entità certificata, in caso

di utilizzo di record TLSA con tipo di uso DANE-EE(3), è dovuta al fatto che il record certifica il nome di dominio a cui è associato, ignorando il contenuto del certificato, come riportato in un recente draft rilasciato dal gruppo DANE [group, 2014]. Sebbene questo standard indichi l'uso del record per evitare attacchi di tipo MITM durante l'apertura di una sessione TLS, può essere anche utilizzato per pubblicare certificati per altri usi, come verrà fatto in questo documento.

Nella prossima sezione, verranno introdotti i vari punti di modifica dello standard dell'infrastruttura PEC.

2 Architettura della proposta: punti di modifica dello standard PEC

In questa sezione e nella successiva, viene presentata la proposta di modifica delle specifiche tecniche della PEC, per poter superare le problematiche associate all'uso del file LDIF centralizzato e sulla pubblicazione dei certificati X.509v3, così come descritti nella sezione 1.1. Le modifiche proposte verranno introdotte nella sezione 3 insieme ad un caso di studio.

Si inizia l'esposizione descrivendo il funzionamento logico della PEC, secondo l'RFC6109 [IETF, 2011], indicando i passi in cui sono state introdotte modifiche. In figura 3 è riportato un breve schema, con riferimento allo scambio di un messaggio di PEC correttamente validato.

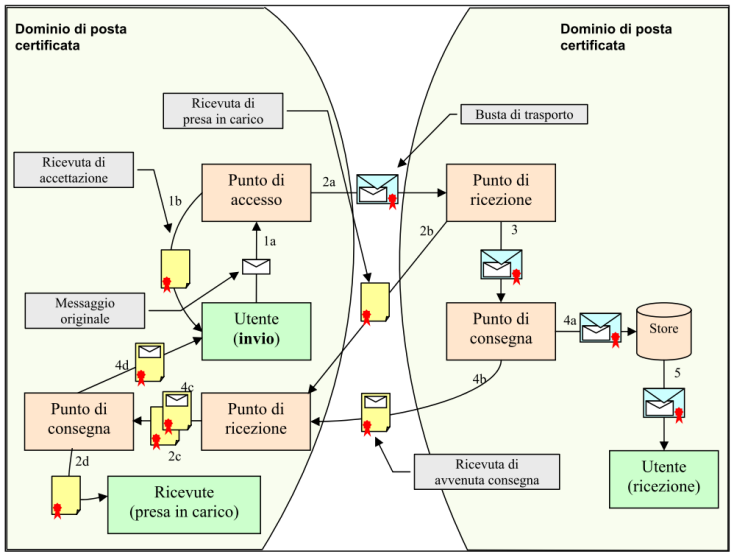

Figure 3: Esempio di scambio di un messaggio PEC correttamente validato

1. L'utente, attraverso un'autenticazione sicura, accede al Punto di Accesso

(**Access Point**) fornito dal PEC provider mittente. Il PEC provider mittente gestisce uno o più domini, che per il D.P.R. n.68/2005 e per il D.Lgl. n.235/2010 possono soltanto contenere caselle email PEC. Questi domini sono appartenenti legalmente a aziende o enti esterni rispetto al PEC provider, e nel documento sono stati e verranno indicati come *domini PEC*.

Il Punto di Accesso effettua le seguenti operazioni:

- Controlla formalmente il formato del messaggio, come indicato nel paragrafo 3.1.1 dell'RFC6109. Questa parte non sarà soggetta a modifiche.
- Controlla le destinazioni del messaggio: cerca di identificare quali sono domini PEC e quali no. Questa parte sarà oggetto di modifiche.
- Genera una Ricevuta di Accettazione per l'utente mittente. La Ricevuta di Accettazione indica al mittente se il suo messaggio è stato accettato dall'infrastruttura PEC. Questa parte non sarà soggetta a modifiche.
- Imbusta il messaggio in una Busta di Trasporto, generata secondo lo standard S/MIMEv3 [IETF, 2010]. Per garantirne la provenienza e l'integrità, il PEC provider genera una coppia di chiavi crittografiche, e firma il messaggio con la chiave privata; la corrispondente chiave pubblica e l'algoritmo di segnatura utilizzato, più i dati di autenticazione sono rilasciati sotto forma di certificato X.509v3 rilasciato da una Certification Authority, come descritto negli RFC2459 e RFC5280 [IETF, 1999],[IETF, 2008b]. Una copia del certificato è aggiunta alla struttura S/MIMEv3 del messaggio. Questa parte non sarà soggetta a modifiche.

2. Il Punto di Accesso invia il messaggio al Punto di Ricezione (**Incoming Point**) del destinatario.

   Il Punto di Ricezione permette:

   - lo scambio di messaggi PEC tra PEC provider
   - l'accesso nell'infrastruttura PEC ai messaggi di posta elettronica ordinaria

   Lo scambio di messaggi avviene tramite una transazione basata sul protocollo SMTP [IETF, 2001]. Gli errori SMTP possono ritardare la ricezione del messaggio nell'infrastruttura PEC non oltre le 24 ore, come riportato nell'RFC6109 [IETF, 2011].

   Il Punto di Ricezione controlla formalmente il formato del messaggio ricevuto e effettua le seguenti operazioni:

   - Se il messaggio in ingresso ha una Busta di Trasporto corretta ed integra come indicato nell'RFC6109 [IETF, 2011], emette una Ricevuta

di Presa in Carico e la invia al PEC provider mittente, altrimenti inserisce il messaggio in una Busta di Anomalia e lo inoltra verso il Punto di Consegna (**Delivery Point**). Questa parte non sarà soggetta a modifiche.

- Se il messaggio in ingresso è una Ricevuta/avviso PEC corretto ed integro, come indicato nell'RFC6109 [IETF, 2011], inoltra la ricevuta/avviso verso il Punto di Consegna. Questa parte non sarà soggetta a modifiche.
- Se il messaggio in ingresso non risponde ai requisiti per una Busta di Trasporto o per una Ricevuta/avviso PEC corretto ed integro, come indicato nell'RFC6109 [IETF, 2011], lo inserisce in una Busta di Anomalia e lo inoltra verso il Punto di Consegna. Questa parte sarà oggetto di modifiche.

Per verificare se la Busta di Trasporto/Ricevuta/avviso è corretta/integra, il Punto di Ricezione compie i seguenti controlli aggiuntivi:

- Verifica se il messaggio è correttamente imbustato in una struttura S/MIMEv3, come definita nell'RFC5751 [IETF, 2010]. Questa parte non sarà soggetta a modifiche.
- Verifica la correttezza e la provenienza della firma del messaggio. Per fare ciò, utilizza il certificato X.509v3 contenuto nel messaggio ricevuto e lo confronta con quello contenuto nel file LDIF. Il certificato deve essere valido, cioè esso non deve essere scaduto o revocato per mezzo di una Certified Revocation List, come indicato nell'RFC5280 [IETF, 2008b] Questa parte sarà oggetto di modifiche.

3. Infine, il Punto di Ricezione passa il messaggio al Punto di Consegna, che si occupa di consegnarlo e inserirlo, senza modifiche, nella mailbox del destinatario. Il Punto di Consegna effettua le seguenti operazioni:

   - Controlla formalmente il formato del messaggio, come indicato nel paragrafo 3.3.1 dell'RFC6109. Questa parte non sarà soggetta a modifiche.
   - Se il messaggio in ingresso è una Busta di Trasporto corretta ed integra come indicato nell'RFC6698 [IETF, 2012], genera una Ricevuta di Avvenuta Consegna per il PEC provider mittente, altrimenti genera una Ricevuta di Non Avvenuta Consegna. Questa parte non sarà soggetta a modifiche.
   - Se il messaggio in ingresso è di posta elettronica ordinaria, è una Ricevuta/avviso PEC corretto ed integro o una Busta di Anomalia, la Ricevuta di Avvenuta Consegna non deve essere emessa. Questa parte non sarà soggetta a modifiche.

Nei punti precedenti, si è indicato dove intervenire nelle procedure standard della infrastruttura di funzionamento della PEC. Nel seguente elenco si riassumono brevemente le problematiche affrontate e i punti di cambiamento:

1. Identificazione e riconoscimento di un PEC provider, sia durante l'invio effettuato dal Punto di Accesso, sia al momento della ricezione di un messaggio. In particolare, occorre un diverso modo di creare, modificare e interrogare la lista dei PEC provider, modificabile solo da AGID ma interrogabile da tutti i PEC provider.

2. Identificazione e riconoscimento di un dominio PEC e del relativo PEC provider, sia durante l'invio effettuato dal Punto di Accesso, sia al momento della ricezione di un messaggio. In particolare, occorre un meccanismo per poter permettere ad ogni PEC provider di poter modificare e pubblicare autonomamente la lista dei propri domini PEC, lasciando ad AGID la possibilità di poter identificare ed intervenire nel caso due o più PEC provider (erroneamente o fraudolentemente) abbiano inserito nella loro lista uno stesso dominio PEC.

3. Pubblicazione, recupero e associazione dei certificati X.509v3 ai PEC provider. Come indicato nell'RFC6109 [IETF, 2011], ogni PEC provider può avere uno o più certificati necessari per firmare i messaggi PEC in uscita. In particolare, occorre un meccanismo per poter permettere ad ogni PEC provider di emettere e pubblicare autonomamente i certificati necessari per la verifica della firma digitale di un messaggio PEC. Il meccanismo usato è quello sviluppato e standardizzato dal DANE group nell'RFC6698 [IETF, 2012], descritto nella sezione 1.3.1.

Come accennato in sezione 1.1, si propone di sfruttare l'infrastruttura DNSSec per risolvere le varie problematiche suddette, in modo da sostituire un meccanismo proprietario e non scalabile con un meccanismo standard e che permette la distribuzione delle informazioni tra i vari attori. Come prerequisito per il funzionamento del metodo descritto nella proposta, viene richiesto che i singoli PEC provider e AGID creino e gestiscano almeno una propria Zona autoritativa DNSSec.

3 Caso di studio: presentazione della proposta e specifiche tecniche

In questa sezione si descrive dettagliatamente la proposta di modifica della PEC, introducendo un caso di studio e gli attori che entrano a far parte di una tipica infrastruttura di Posta Elettronica Certificata. Durante l'esposizione, sono riportate le principali modifiche alle operazioni di funzionamento tipiche della PEC come indicate nella sezione 2, in particolare l'aggiunta, revoca e identificazione sicura di un PEC provider e di un dominio PEC e la gestione dei certificati X.509v3.

Gli attori del caso di studio sono i seguenti:

- **AGID**: rappresenta l'autorità garante e vigilante del rispetto delle regole tecniche della PEC e di altre attività istituzionali. Queste ultime includono ricevere e valutare le domande per i candidati soggetti a svolgere il ruolo di fornitore di PEC (come definito nella circolare CNIPA CR / 49 del 24 novembre 2005), sovrintendere l'attività del PEC provider (mantenimento dei requisiti, livelli di servizio, statistiche di utilizzo), e supervisionare i test di interoperabilità (in base alla circolare CNIPA CR / 51 del 7 dicembre 2006). Gestisce una Zona autoritativa DNSSec, corrispondente al dominio *agid.it*, reso noto a tutti i PEC providers.

- **Pec1, Pec2**: rappresentano due PEC providers. Ognuno di loro gestisce una Zona autoritativa DNSSec, corrispondenti rispettivamente ai domini *pec1.it* e *pec2.it*, che devono contenere **esclusivamente** i resource record che contengono i dati necessari per il corretto funzionamento dell'infrastruttura PEC.

- **Gestito1**: rappresenta l'ente o l'azienda proprietaria di un *dominio PEC*; **Pec1** gestisce il servizio PEC per conto di **Gestito1**. Esso gestisce una Zona autoritativa DNS, corrispondente al dominio *gestito1.it*. Nonostante non sia richiesto l'uso di DNSSec per le Zone autorizzative dei domini PEC perché non soggette al controllo diretto di AGID, ne è comunque consigliabile l'uso laddove siano presenti le necessarie competenze tecniche e amministrative.

In figura 4 si può vedere la Zona autoritativa DNSSec del dominio *agid.it*, creata e mantenuta da AGID, in riferimento al caso di studio. Alcuni record sono stati tagliati perché non importanti per l'esposizione.

Prima di presentare, nelle prossime sezioni, i vari metodi analizzati durante lo studio della proposta di modifica della PEC, vengono quì indicate alcune regole tecniche per il mantenimento delle zone DNSSec:

- Si consiglia di creare due coppie di chiavi per le Zone DNSSec:
  - **Key Signing Key** (KSK): usata per firmare l'insieme dei record DNSKEY. Nell'esempio è rappresentata dal record DNSKEY con l'ID 56208. Può essere creata con un algoritmo di cifratura più forte e può essere rinnovata in tempi lunghi, anche superiori all'anno.
  - **Zone Signing Key** (ZSK): usata per firmare il resto dei record della Zona. Nell'esempio è rappresentata dal record DNSKEY con l'ID 61808. Può essere creata con un algoritmo di cifratura più debole per ragioni di efficienza, ma deve essere rinnovata in tempi più brevi o se compromessa.

- Per poter effettuare l'autenticazione dei record della Zona *agid.it*, che rappresenta un'Isola di Sicurezza, la relativa Trust Anchor, rappresentata dalla KSK, deve essere distribuita ai PEC providers.

```
agid.it.            IN SOA     agid.it. admin.agid.it ( ... )
agid.it.            IN RRSIG   ...
                    .........
agid.it.            IN DNSKEY  256 3 10 (
                               A...f
                               ) ; ZSK; alg = RSASHA512; key id = 61808
agid.it.            IN DNSKEY  257 3 10 (
                               A...V
                               ) ; KSK; alg = RSASHA512; key id = 56208
agid.it.            IN RRSIG   DNSKEY 10 1 86400 (
                               20141003125052 20140903115052 56208 agid.it.
                               I...= )
agid.it.            IN NSEC    pec1.it.agid.it. A NS SOA RRSIG NSEC DNSKEY
agid.it.            IN RRSIG   NSEC 10 1 10800 (
                               20140913153949 20140814143949 61808 agid.it.
                               k...= )
pec1.it.agid.it.    IN DLV     31293 10 2 (
                               934278E4E266FFF2CE2CA91DC97E88ADF0276B98B87F
                               210AB6AA3736A5D93AAF )
pec1.it.agid.it.    IN RRSIG   ...
pec1.it.agid.it.    IN NSEC    pec2.it.agid.it. RRSIG NSEC DLV
pec1.it.agid.it.    IN RRSIG   ...
pec2.it.agid.it.    IN DLV     36612 10 2 (
                               377B76975852294226D196EE40A997A87E68AB03DD45
                               DFD00F614F53CDA7DEDC )
pec2.it.agid.it.    IN RRSIG   ...
pec2.it.agid.it.    IN NSEC    _pec.agid.it. RRSIG NSEC DLV
pec2.it.agid.it.    IN RRSIG   ...
_pec.agid.it        IN TLSA    DANE-EE SPKI Full a....C
_pec.agid.it.       IN RRSIG   TLSA 10 1 10800 (
                               20140913153949 20140914153949 61808 _pec.agid.it.
                               k...= )
_pec.agid.it.       IN NSEC    agid.it. RRSIG NSEC TLSA
_pec.agid.it.       IN RRSIG   ...
```

Figure 4: Master File di esempio del dominio *agid.it*

- Si consiglia di abilitare il rollover automatico della Trust Anchor di AGID da parte dei PEC providers, secondo l'RFC5011 [IETF, 2007a]. In questo modo, nessuno dei PEC providers deve occuparsi di aggiornarla al momento in cui viene sostituita la chiave KSK, semplificando il procedimento.

- Si consiglia di permettere l'uso temporaneo della Zona autoritativa di AGID come dominio DLV per i PEC providers, secondo le specifiche dell'RFC5074 [IETF, 2007b], a causa della scarsità di domini di primo livello firmati; nell'esempio, il dominio *.it* non è firmato con DNSSec. E' richiesto lo scambio, attraverso un canale sicuro, della chiave KSK dei PEC providers con AGID ogni qualvolta essi la rinnovano. Nel caso di studio, i due record DLV alla fine del Master File in figura 4 si riferiscono alle chiavi KSK delle Zone autoritative di **Pec1** e **Pec2**. Questi record non sono necessari se i PEC providers vengono autenticati da un apposito dominio DLV, come ad esempio *dlv.isc.org*, o se il dominio di primo livello viene firmato e viene inserito in esso l'apposito record DS.

3.1 Identificazione di un PEC provider

In questa sezione si descrive la soluzione proposta al problema di identificare se un messaggio PEC integro e corretto è destinato o stato inviato da un PEC provider.

Per poter mantenere e aggiornare un indice dei PEC provider attualmente autorizzati a operare, in sostituzione del metodo attuale basato su un file LDIF che contiene l'elenco dei providers stessi insieme ai domini PEC, si sono vagliati due diversi approcci, descritti nelle sezioni seguenti.

3.1.1 Metodo centralizzato

Nel metodo centralizzato, l'elenco dei PEC providers e dei domini PEC viene inserito all'interno della Zona autoritatiza di AGID per mezzo di appositi record, in modo da poter essere interrogato per mezzo di query DNS.

In questo metodo, per ogni dominio PEC viene creato un record TXT che contiene il nome di dominio del PEC provider che offre il servizio. Ad esempio, in figura 3.1.1, il record TXT associato al nome di dominio *gestito1.it.agid.it* indica che l'entità **Gestito1** è un dominio PEC gestito dal PEC provider **Pec1**. Il record è indicizzabile direttamente, premettendo il nome del dominio PEC al nome di dominio di AGID, come nell'esempio suddetto.

```
                .......
gestito1.it.agid.it.   IN TXT    pec1.it.
gestito1.it.agid.it.   IN RRSIG  ...
gestito1.it.agid.it.   IN NSEC   gestito2.it.agid.it. RRSIG NSEC TXT ...
gestito1.it.agid.it.   IN RRSIG  ...
gestito2.it.agid.it.   IN TXT    pec2.it.
gestito2.it.agid.it.   IN RRSIG  ...
gestito2.it.agid.it.   IN NSEC   agid.it. RRSIG NSEC TXT ...
gestito2.it.agid.it.   IN RRSIG  ...
```

Se l'assenza del record suddetto è validata attraverso l'apposito record NSEC, allora il dominio corrispondente non è PEC.

Per limitare i fenomi di caching, in caso di inserimento o cancellazione del record di un dominio PEC, il corrispondente record RRSIG che lo autentica deve avere durata di validità non superiore ad un giorno, così come per i record NSEC che ne autenticano l'assenza. In questo modo, è possibile ridurre l'inconsistenza tra cache locale ai Resolver e i dati contenuti nella Zona autoritativa ad un massimo del valore consentito per la PEC, come indicato nell'RFC6109 [IETF, 2011], ma si consiglia di tenerlo più basso.

Il metodo centralizzato ha i seguenti pregi e difetti:

1. **Semplicità di gestione**: Permette ad AGID di poter mantenere sempre aggiornato l'elenco dei PEC providers e dei domini PEC, in maniera tempestiva e centralizzata.

   Non è necessaria nessuna modifica per le Zone autoritative dei PEC providers.

2. **Mancanza di scalabilità**: Il Master File della Zona autoritativa di AGID cresce di dimensioni proporzionalmente al crescere del numero di domini PEC e di PEC providers, rendendo il metodo non scalabile. Come conseguenza, si ha anche un aumento del traffico DNS verso i Name Server di AGID, con problemi di prestazioni e di possibile temporanea indisponibilità del servizio DNS.

3. **Inefficienza**: E' necessaria una continua sincronizzazione con i PEC providers per ricevere da loro la lista dei domini PEC da loro gestiti. Questo può comportare un aumento dei costi e dei tempi di gestione della lista centralizzata.

3.1.2 Metodo distribuito

Nel metodo distribuito, gli elenchi dei PEC providers e dei domini PEC sono "virtualmente" distribuiti, in modo da incrementare la scalabilità del sistema.

In questo metodo, ogni PEC provider inserisce nella propria Zona autoritiva un apposito record TXT la cui presenza ne indica la natura di PEC provider. Al fine di evitare che un non-PEC provider possa fraudolentemente indicare se stesso come PEC provider, il contenuto di questo record viene firmato da una chiave privata appositamente creata e mantenuta segreta da AGID. In figura 3.1.2 si può vedere la Zona autoritativa DNSSec del dominio *pec1.it* del PEC provider **Pec1**, dove si può notare la presenza del record suddetto.

Il record contiene il nome del dominio, *pec1.it*, firmato per mezzo della chiave privata suddetta, custodita da AGID. La chiave pubblica è distribuita aggiungendo, nella Zona autoritativa di AGID, un apposito record TLSA contente il corrispondente certificato X.509v3, così come descritto nella sezione 1.3.1.

Per motivi di efficienza, si consiglia di utilizzare una sola coppia di chiavi per tutti i PEC providers. Si consiglia un periodo di validità compreso tra 6 mesi ed un anno. Per il rollover di questa chiave, si veda la sezione 3.3.

```
pec1.it.                IN SOA     pec1.it. admin.pec1.it ( ... )
pec1.it.                IN RRSIG   ...
                        .........
pec1.it.                IN DNSKEY  256 3 10 (
                                   A...f
                                   ) ; ZSK; alg = RSASHA512; key id = 57312
pec1.it.                IN DNSKEY  257 3 10 (
                                   A...V
                                   ) ; KSK; alg = RSASHA512; key id = 32436
pec1.it.                IN RRSIG   DNSKEY 10 1 86400 (
                                   20141207125052 20150101115052 32436 pec1.it.
                                   A...4 )
pec1.it.                IN MX      mx.pec1.it.
pec1.it.                IN RRSIG   ...
pec1.it.                IN TXT     4...d
pec1.it.                IN RRSIG   ...
pec1.it.                IN NSEC    mx.pec1.it.  A NS SOA RRSIG NSEC DNSKEY MX TXT ...
pec1.it.                IN RRSIG   ...
mx.pec1.it.             IN A       www.xxx.yyy.zzz
mx.pec1.it.             IN RRSIG   ...
mx.pec1.it.             IN NSEC    _pec.pec1.it.  A RRSIG NSEC MX ...
mx.pec1.it.             IN RRSIG   ...
_pec.pec1.it.           IN TLSA    DANE-EE SPKI Full a....C
_pec.pec1.it.           IN RRSIG   TLSA 10 1 10800 (
                                   20140913153949 20140814143949 57312 _pec.pec1.it.
                                   k...= )
_pec.pec1.it.           IN NSEC    _pec.pec1.it.  A RRSIG NSEC MX TLSA...
_pec.pec1.it.           IN RRSIG   ...
_25.smtp.mx.pec1.it.    IN TLSA    DANE-EE SPKI Full 5....d
_25.smtp.mx.pec1.it.    IN RRSIG   TLSA 10 1 10800 (
                                   20141001153949 20150401143949 57312 _25.smtp.mx.pec1.it.
                                   k...= )
_25.smtp.mx.pec1.it.    IN NSEC    pec1.it.  A RRSIG NSEC TLSA ...
_25.smtp.mx.pec1.it.    IN RRSIG   ...
```

Figure 5: Master File di esempio del dominio *pec1.it*

L'operazione di revoca dell'autorizzazione ad un PEC provider a operare deve essere, per legge, supervisionata e controllata da AGID, per evitare che un PEC provider continui a fornire il servizio anche se non autorizzato. Per questo motivo essa è particolarmente delicata: essa corrisponde a cancellare, all'interno della Zona del PEC provider revocato, il suddetto record TXT firmato con la chiave di AGID.

Se, fraudolentemente o per un errore involontario, la Zona autoritativa di un PEC provider revocato contiene ancora il record TXT suddetto, valido fino alla scadenza della chiave privata detenuta da AGID, è possibile agire in maniera da prevenire questa possibilità. In particolare, è possibile utilizzare due metodi:

- **Senza Revocation List**

  In questo primo metodo, al momento della revoca di un PEC provider, AGID deve effettuare tempestivamente le seguenti operazioni:

  1. Generare una nuova coppia di chiavi e pubblicare il corrispondente certificato X.509v3 nella sua Zona, sostituendo il precedente record TLSA.
  2. Firmare, con la nuova chiave privata, tutti i record TXT dei PEC provider non revocati e distribuirli.

  I PEC provider devono, tempestivamente, sostituire il proprio record TXT con il nuovo, distribuito da AGID.

  Questo metodo è sconsigliato per le seguenti problematiche:

  – **Difficoltà di pianificazione rollover**: per la natura spesso imprevedibile dell'operazione di revoca (si pensi ad esempio ad una sanzione contro il PEC provider), non è possibile, per AGID, poter pianificare con il necessario anticipo il rollover della chiave e la distribuzione dei nuovi record TXT.

  – **Indisponibilità del servizio PEC**: è possibile che il servizio PEC di un PEC provider sia indisponibile per un certo periodo di tempo. Questo è dovuto al ridotto periodo di tempo disponibile per la distribuzione dei record TXT e la sostituzione degli stessi nelle Zone autoritative dei PEC providers per il rollover improvviso di una chiave. Il tempo di indisponibilità è rapportato alla differenza tra la fine di validità della vecchia chiave e il recupero del nuovo record TXT da parte dei Resolver.

- **Revocation List**

  In questo secondo metodo, AGID deve creare all'interno della sua Zona autoritativa, una lista di PEC provider revocati, simile ad una Revocation List usata, ad esempio, per gestire la revoca dei certificati X.509v3 come descritto nell'RFC3279 [IETF, 2002].

Al momento della revoca di un PEC provider, AGID deve effettuare le seguenti operazioni:

- Inserire, nella propria Zona autoritativa, un apposito record TXT, con nome di dominio creato come nel metodo centralizzato, la cui presenza indica che il PEC provider corrispondente è stato revocato.

  Il contenuto del record viene lasciato vuoto e riservato per usi futuri.

- Cancellare i record inseriti nella Revocation List al momento del rollover della chiave conservata da AGID per firmare i record TXT dei PEC providers.

  Per il rollover della chiave, si consiglia un periodo di validità compreso tra 6 mesi ed un anno.

Per limitare i fenomi di caching, in caso di inserimento o cancellazione del record di revoca di un PEC provider, il corrispondente record RRSIG che lo autentica deve avere durata di validità non superiore ad un giorno, così come per i record NSEC che ne autenticano l'assenza. In questo modo, è possibile ridurre l'inconsistenza tra cache locale ai Resolver e i dati contenuti nella Zona autoritativa ad un massimo del valore consentito per la PEC, come indicato nell'RFC6109 [IETF, 2011], ma si consiglia di tenerlo più basso.

Per esemplificare questo metodo, supponiamo che, nel caso di studio, venga revocato il PEC provider **Pec1**. AGID deve inserire i seguenti record nella sua Zona autoritativa:

```
                .......
_pec.agid.it. IN TLSA DANE-EE SPKI Full a....C
_pec.agid.it. IN RRSIG TLSA 10 1 86400 (
                                 20140924153949 20140925153949 61808 _pec.agid.it.
                                 k...= )
_pec.agid.it. IN pec1.agid.it. NSEC TLSA RRSIG ...
_pec.agit.it. IN RRSIG ...
pec1.agid.it. IN TXT ...
pec1.agid.it. IN RRSIG TXT 10 1 86400 (
                                 20141010153949 20141011153949 61808 _pec.agid.it.
                                 k...= )
pec1.agid.it. IN agid.it.  NSEC TXT RRSIG ...
pec1.agit.it. IN RRSIG ...
```

Questo metodo è consigliato per i seguenti motivi:

- **Possibilità di pianificazione rollover**: è possibile, per AGID, poter pianificare con il necessario anticipo il rollover della chiave e la distribuzione dei nuovi record TXT, operazioni che, all'aumentare del numero dei PEC providers, risultano onerose in tempo necessario ad eseguirle.

- **Scalabilità**: la dimensione del Master File della Zona autoritativa di AGID è scalabile con l'aumentare del numero dei PEC providers. Infatti

la lista dei PEC providers revocati, cancellata periodicamente al momento del rollover della chiave, ha dimensione indipendente dal numero di PEC providers.

Per esemplificare meglio come funziona questo secondo metodo, si supponga, ad esempio, che **Pec2** riceva una email proveniente dal dominio PEC **gestito1.it**, gestito dal PEC provider **Pec1**e imbustata correttamente secondo le regole della PEC. Per verificare se **Pec1** è un PEC provider, il Punto di Accesso di **Pec2** deve effettuare le seguenti operazioni:

1. Controllare se esiste il record TXT corrispondente al nome di dominio *pec1.it* tramite un'apposita query al DNS. Il Name Server di Pec1 è autoritativo per rispondere a questa query.

2. In caso di risposta affermativa validata al punto 1, deve recuperare, con un'apposita query, la chiave pubblica necessaria a decifrare il record TXT dalla Zona autoritativa di AGID. Essa è rappresentata dal record di tipo TLSA corrispondente al nome di dominio *_pec.agid.it*. In parallelo, deve controllare, tramite un'apposita query, se esiste un record TXT corrispondente al nome di dominio *pec1.agid.it* nella Revocation List mantenuta da AGID.

3. In caso di risposta affermativa validata alla prima query del punto 2, e di risposta negativa alla seconda query, validata tramite l'apposito record NSEC, deve usare il certificato recuperato dal dominio di AGID per decifrare il contenuto del record TXT recuperato dalla Zona autoritativa di **Pec1**.

4. Se il contenuto del record TXT recuperato dalla Zona autoritativa di **Pec1** è correttamente decifrato con la chiave pubblica recuperata dal dominio di AGID, e corrisponde alla stringa **pec1.it**, allora può riconoscere **Pec1** come PEC provider.

5. Se il record TXT di **Pec1** è validato come non esistente con apposito record NSEC o la decifratura effettuata con la chiave pubblica non è valida o ottengo un nome diverso da **pec1.it**, allora deve considerare il messaggio come ricevuto da un non-PEC provider e deve consegnarlo in una Busta di Anomalia al destinatario, come indicato nella sezione 2.2.2 dell'RFC6109 [IETF, 2011].

6. In caso di risposta affermativa validata alla seconda query del punto 2, allora deve considerare il messaggio viene considerato come ricevuto da un non-PEC provider e agire come nel punto 5.

7. Se capita una delle problematiche indicate nel seguente elenco, il Punto di Accesso deve trattarle come errori temporanei o transitori:

   (a) il record TLSA corrispondente alla chiave pubblica di AGID usata per firmare i record TXT dei Pec providers è validato come non esistente con apposito record NSEC

(b) uno dei record in una delle Zone autoritative di AGID o di **Pec1** non è correttamente validato (potrebbe rappresentare un possibile attacco alla Zona DNSSec)

(c) non si riceve risposta ad una delle query entro un apposito timeout (rete sovraccarica, Name Servers non raggiungibili, ecc...),

Viene definito un tempo massimo ((inferiore al tempo di 24 ore definito per i possibili errori SMTP nell'RFC6109 [IETF, 2011]) entro il quale, se l'errore non è risolto, è possibile scegliere tra due possibili soluzioni:

- Consegnare il messaggio in una Busta di Anomalia considerando il dominio come non-PEC, come nel punto 5.
- Inviare a **Pec1** una ricevuta di non avvenuta consegna dal Delivery Point di **Pec2**. La gestione degli errori verrà approfondita durante lo studio di fattibilità.

Il metodo distribuito con Revocation List ha i seguenti pregi e difetti:

1. **Maggiore complessità di gestione**

   AGID deve effettuare regolarmente la seguente serie di operazioni:

   - Generare una coppia di chiavi per la firma dei record TXT di identificazione dei PEC providers
   - Pubblicare il record TLSA contenente il certificato X.509v3 della chiave pubblica nella sua Zona autoritativa
   - Fare il rollover della chiave suddetta, firmare i record TXT dei PEC provider autorizzati e distribuirli.
   - Mantenere la Revocation List

   Ognuna di queste operazioni comporta un costo in termini di tempo, di competenza e di rispetto di precisi vincoli temporali, per poter mantenere funzionante l'infrastruttura PEC.

2. **Maggior traffico DNS**: l'algoritmo di verifica dell'identità di un PEC provider è più complesso e richiede un numero di query maggiore rispetto al metodo centralizzato.

   Il traffico è comunque distribuito tra AGID e i PEC providers.

3. **Scalabilità**: La dimensione del Master File della Zona autoritativa di AGID non cresce di dimensioni proporzionalmente al numero di PEC providers. Essa deve solo mantenere le seguenti informazioni nella sua Zona:

   - Un record TLSA corrispondente alla chiave pubblica usata per decifare i record TXT necessari per identificare i PEC providers

- I record TXT della Revocation List dei PEC providers

I PEC provider devono solo mantenere aggiornato il record TXT firmato da AGID.

4. **Efficienza**: Non è necessaria una continua sincronizzazione con i PEC providers per ricevere da loro la lista aggiornata dei domini PEC da loro gestiti. Con questo metodo, la lista dei domini PEC è mantenuta e gestita da ogni PEC provider autonomamente.

   L'interazione tra PEC providers ed AGID è ridotta alla distribuzione dei record TXT firmati, durante il rollover della chiave. E' comunque possibile automatizzare questa operazione, ad esempio pubblicando la stringa firmata su una pagina web apposita, da cui ogni PEC provider può recuperarla attraverso una sessione sicura.

In questa proposta si è scelto di utilizzare il metodo distribuito con Revocation List, visto i benefici di scalabilità, ad un costo tollerabile in aumento della complessità di mantenimento e gestione dell'infrastruttura DNSSec e di traffico DNS.

3.2 Identificazione di un dominio PEC

In questa sezione si descrive la soluzione proposta al problema di identificare se un messaggio PEC integro e corretto è destinato o stato inviato da un dominio PEC e di recuperare il nome del PEC provider che ne gestisce il servizio. Questa soluzione si integra con quella per identificare un PEC provider descritta in sezione 3.1, andando a risolvere le problematiche riportate in sezione 1.1.

Il metodo utilizzato è identico al metodo distribuito con Revocation List descritto in sezione 3.1.2.

Ogni PEC provider deve creare **autonomamente** la propria coppia di chiavi necessarie per firmare e decifrare i record TXT utilizzati per identificare **esclusivamente** i domini PEC da lui gestiti. Il record TXT contiene la stringa firmata con la chiave privata del PEC provider gestore ed il nome di dominio di quest'ultimo: questo permette di poter identificare il dominio del PEC provider gestore univocamente.

In più deve mantenere la Revocation List dei domini PEC che, rispetto all'ultimo rollover della suddetta coppia di chiavi, non sono più gestiti da lui.

Per esemplificare meglio come funziona questo metodo, si supponga che **Pec2** riceva una email proveniente dal dominio PEC *gestito1.it*, gestito dal PEC provider **Pec1** e imbustata correttamente secondo le regole della PEC. Per verificare se **gestito1.it** è un dominio PEC, e quale sia il suo PEC provider, il Punto di Accesso di **Pec2** deve effettuare le stesse operazioni descritte in sezione 3.1.2. Si deve però tenere in considerazione che, come possiamo notare in figura 6, dove si può vedere la Zona autoritativa del dominio *gestito1.it*, la Zona del dominio PEC **non è DNSSec**.

```
gestito1.it.   IN SOA    gestito1.it. admin.gestito1.it ( ... )
      .........
gestito1.it.   IN MX mx.pec1.it.
gestito1.it.   IN TXT A...8 pec1.it
```

Figure 6: Master File di esempio del dominio *gestito1.it*

Rispetto al metodo discusso in sezione 3.1, in questo caso si deve tenere conto delle problematiche dovute all'uso di un dominio DNS non sicuro da parte del dominio PEC. In particolare i due punti seguenti:

- Si devono analizzare le conseguenze dei possibili attacchi informatici al dominio *gestito1.it*, di tipo DNS spoofing, cache poisoning, MITM o altri. Il grado di sicurezza mantenuto dalle modifiche proposte in questo documento non deve essere inferiore al grado di sicurezza dell'attuale infrastruttura PEC.
- Si deve poter garantire la sicurezza che due o più PEC providers non possano indicare se stessi, senza possibilità di controllo o di identificazione da parte di AGID, come gestori di uno stesso dominio PEC.

Nel seguito di questa sezione trattiamo dettagliatamente i due punti suddetti, iniziando ad analizzare alcuni dei possibili attacchi al dominio PEC **gestito1.it**, in particolare ai record MX e TXT da lui pubblicati, recuperati dal PEC provider **Pec2** per poter identificare il dominio PEC ed il PEC provider che ne gestisce il servizio, Si supponga che **Pec2** debba inviare, per conto di **Gestito2**, un messaggio PEC con destinatario appartenente al dominio *gestito1.it*:

- **Sostituzione o cancellazione del record TXT**

  Questo record è firmato dal PEC provider **Pec1**, che gestisce il servizio di PEC per il dominio PEC **Gestito1**. Esso può essere sostituito o cancellato da uno degli attacchi suddetti. E' possibile uno dei casi seguenti:

  - **Cancellazione del record TXT**: in questo caso, per sicurezza (in caso sia in azione un attacco), si deve considerare **Gestito1** come un dominio non-PEC.
  - **Sostituzione del record TXT**: in questo caso, **Pec2** deve recuperare, dalla Zona autoritativa del PEC provider **Pec1** indicato nel record TXT di **Gestito1**, il record TLSA contenente la chiave pubblica per validare quest'ultimo.

    Sono possibili diversi scenari:

    1. **Inesistenza del record TLSA**: in questo caso, per sicurezza (in caso sia in azione un attacco), si deve considerare **Gestito1** come un dominio non-PEC.

2. **Mancata validazione del record TXT**: se la chiave pubblica recuperata non valida correttamente il record TXT di **Gestito1**, si procede come nel punto 1.
3. **Il dominio di Pec1 non è DNSSec**: in questo caso, **Pec1** è considerato un provider non-PEC. Si procede come nel punto 1.
4. **Pec1 non è PEC provider**: se **Pec1**, eseguendo l'algoritmo di identificazione descritto nella sezione 3.1, non è riconosciuto come PEC provider, si procede come nel punto 1.

In ognuno degli scenari suddetti, è possibile riconoscere un attacco al record TXT da parte di un'entità che non è un PEC provider. Considerando il dominio di **Gestito1** come non-PEC, si inibisce l'accesso all'infrastruttura PEC.

Se invece il record TXT di **Gestito1** è correttamente validato e **Pec1** è riconosciuto come PEC provider eseguendo l'algoritmo di identificazione descritto nella sezione 3.1, si può ancora identificare un possibile comportamento fraudolento, rappresentato da un tentativo di sostituzione nella fornitura del servizio PEC per conto di **Gestito1** da parte di **Pec1** ai danni di un altro PEC provider, effettuando un controllo incrociato con il record MX contenuto nella Zona autoritativa di **Gestito1**. Il controllo incrociato è effettuato da **Pec2** eseguendo le seguenti operazioni:

1. Controlla se esiste un record di tipo A che mappi il nome di dominio del server di posta indicato nel record MX, nell'esempio *mx.pec1.it*, nella Zona autoritativa del PEC provider. Nell'esempio, guardando la figura 3.1.2, è possibile notare la presenza del record suddetto.
2. Se il record MX non è presente, ma è presente un record CNAME, **Pec2** ripete il controllo suddetto dopo aver recuperato il record MX nella Zona autoritativa corrispondente al nome di dominio contenuto nel record CNAME.
   Se viene trovato un nuovo CNAME, si prosegue fino a trovare un record MX. Successivamente, si effettua il controllo al punto 1.
3. Se il record A descritto nel punto 1 è validato come non esistente con apposito record NSEC, o il record MX punta ad un dominio diverso da quello del PEC provider indicato nel record TXT, per sicurezza (in caso sia in azione un attacco), si deve considerare **Gestito1** come un dominio non-PEC.
4. Se il record A descritto nel punto 1 è presente nella Zona autoritativa del PEC provider**Pec1**, come nel nostro esempio, ed è correttamente validata la sua segnatura, il dominio **Gestito1** deve essere considerato PEC.

Questo controllo incrociato aumenta la sicurezza della proposta descritta in questo documento, rispetto al metodo precedente basato sull'uso del file LDIF: questo controllo è infatti basato sull'autenticità

e integrità dei dati contenuti nella Zona autoritativa del PEC provider, in questo caso **Pec1**, ottenibile grazie all'utilizzo dello standard DNSSec.

- **Sostituzione o cancellazione del record MX**

  Questo record punta al server di posta del PEC provider gestore. Esso può essere sostituito o cancellato da uno degli attacchi suddetti. Supponiamo che esista e sia unico il record TXT firmato dal PEC provider gestore, e che sia possibile correttamente validarlo, altrimenti i casi possibili sono trattati nella sezione precedente relativa alla sostituzione o cancellazione del record TXT.

  E' possibile uno dei casi seguenti:

  1. **Cancellazione del record MX**: in questo caso, per impossibilità di identificare il server di posta del PEC provider, si deve considerare **Gestito1** come un dominio non-PEC.
  2. **Sostituzione del record MX**: in questo caso, si effettua il controllo incrociato indicato nella sezione precedente.

- **Aggiunta di uno o più record TXT**

  In caso di presenza di uno o più record TXT, sono possibili vari comportamenti:

  - Se uno dei record TXT è autenticabile da un provider riconosciuto correttamente come PEC eseguendo l'algoritmo descritto in sezione 3.1, e non lo ha inserito nella sua Revocation List, si può scegliere se tra due opzioni possibili:
    - considerare il dominio PEC come gestito da questo PEC provider, e considerare gli altri record TXT come errori o tentativi di attacco identificati. Questa scelta non è consigliata, per mantenere un approccio conservativo alla sicurezza.
    - considerare la presenza di più record come un errore o un tentativo di attacco e, per sicurezza, considerare il dominio come un dominio non-PEC.
  - Se nessuno dei record TXT è autenticabile da un provider riconosciuto correttamente come PEC eseguendo l'algoritmo descritto in sezione 3.1, o tutti i PEC provider iconosciuti correttamente lo hanno inserito nella loro Revocation List, allora per sicurezza (in caso sia in azione un attacco), si deve considerare il dominio come un dominio non-PEC.
  - Se più di uno dei record TXT è autenticabile da un provider riconosciuto correttamente come PEC eseguendo l'algoritmo descritto in sezione 3.1, e più di uno dei PEC provider non ha il dominio PEC inserito nella sua Revocation List, allora per sicurezza (in caso sia in azione un attacco), si deve considerare il dominio come un dominio non-PEC.

– La presenza di più record TXT potrebbe indicare il rollover della chiave del PEC provider gestore, e quindi non costituire un attacco. **Pec1** può riconoscere questa eventualità controllando se i record TXT si riferiscono allo stesso PEC provider e se la Zona autoritativa del PEC provider contiene due record TLSA che validano entrambi i record TXT. Se questo controllo non va a buon fine, per sicurezza (in caso sia in azione un attacco), si deve considerare il dominio come un dominio non-PEC.

La possibilità di due diversi PEC providers di poter indicare (erroneamente o fraudolentemente) uno stesso dominio PEC come da loro gestito viene prevenuta facilmente da questo metodo, grazie alla presenz0a, nel dominio PEC, del record TXT firmato da un solo PEC provider, quello che fornisce il servizio PEC al dominio: questo record è inserito da **Gestito1** e recuperabile solo dalla Zona autoritativa del dominio PEC, e non è modificabile dai PEC providers.

Si hanno però due casi possibili di eccezione:

- in caso di attacco informatico (DNS spoofing, MITM, ecc...), da parte di uno dei PEC provider, della Zona autoritativa del dominio PEC, andandosi a sostituire al PEC provider gestore autorizzato dal dominio PEC.

  Si può notare come l'attacco deve essere portato sia al record TXT che al record MX contenuti nella Zona autoritativa del dominio PEC. Questo, insieme alle competenze tecnologiche necessarie, rende la probabilità di attacco da parte di un PEC provider molto bassa, tenendo in considerazione le possibili sanzioni amministrative in caso di identificazione dell'attacco.

- in caso un PEC provider sia, oltre che fornitore del servizio PEC, anche fornitore del servizio DNS per conto del dominio PEC. Esso può esercitare resistenza nel cambiare i record MX e TXT nella Zona autoritativa del dominio PEC con quelli di un nuovo PEC provider gestore, in caso di migrazione del servizio da un PEC provider ad un altro.

  Questa problematica è attualmente sensibilmente diffusa, e verrà affrontata durante lo studio di fattibilità.

Tutti gli altri tipi di attacchi al dominio non DNSSec *gestito1.it* hanno lo stesso livello di sicurezza del metodo attuale basato sull'uso del file LDIF.

3.3 Pubblicazione dei certificati X.509v3 e rollover delle chiavi

In questa sezione si descrive la soluzione proposta al problema di quale metodo utilizzare per pubblicare, recuperare e associare automaticamente i certificati X.509v3 utilizzati dai PEC provider per firmare o autenticare la provenienza delle email PEC per conto dei domini PEC.

Lo stesso metodo è usato per pubblicare la chiave pubblica utilizzata per autenticare i record TXT necessari per identificare i PEC provider e i domini PEC.

Il metodo usato è simile a quello sviluppato e standardizzato dal DANE group nell'RFC6698 [IETF, 2012], descritto nella sezione 1.3.

In questo metodo, per poter decentralizzare la gestione dei certificati X.509v3 associati ai PEC provider, ognuno di loro inserisce nella propria Zona autoritativa un record TLSA per ogni certificato a lui associato, in modo che possa essere facilmente recuperato attraverso un'apposita query.

Il seguente esempio mostra il record TLSA di un certificato emesso da **Pec1** e pubblicato nella propria Zona autoritativa, come visibile in figura 3.1.2:

```
                              ...
_25.smtp.mx.pec1.it.    IN TLSA  DANE-EE SPKI Full 5....d
_25.smtp.mx.pec1.it.    IN RRSIG TLSA 10 1 10800 (
                                 20141001153949 20150401143949 57312 _25.smtp.mx.pec1.it.
                                 k...= )
                              ...
```

In questa proposta, devono essere utilizzati i seguenti parametri per i record TLSA contenenti i certificati X.509v3 e la chiave pubblica necessaria per firmare i record TXT rilasciati ai domini PEC gestiti dal PEC provider **Pec1**:

- Il nome di dominio associato al certificato contenuto nel record è creato concatenando la porta SMTP del server di posta di **Pec1** (25) al nome del protocollo (SMTP) ed al nome canonico del server di posta stesso (*mx.pec1.it*). Come riportato in un recente draft rilasciato dal gruppo DANE [group, 2014], il nome dell'entità autenticata (**Pec1**) contenuto nel certificato viene ignorato, risolvendo eventuali discrepanze.

- Il campo *uso* deve contenere il valore **DANE-EE**(3), che indica che la normale catena di trusting, necessaria per autenticare il certificato X.509v3, non deve essere controllata. Questo permette al PEC provider di emettere e revocare autonomamente un certificato, superando il modello basato sulle CA.

- Il campo *selettore* deve contenere il valore **SPKI**(1), in modo da ridurre la dimensione del certificato ed ottenere un record più compatto, risparmiando spazio ed evitando problemi di troncamento nelle risposte alle query e riducendo il traffico DNS.

- Il campo *tipo di confronto* deve contenere il valore **Full**(0), per indicare che il campo successivo rappresenta l'intero certificato, o la sua parte SPKI, e non soltanto un hash dello stesso.

L'impostazione *tipo di confronto* viene impostata a **Full** per poter evitare di utilizzare il certificato X.509v3 che viene aggiunto in alla struttura S/MIMEv3 di un messaggio PEC, come indicato nell'RFC6109 [IETF, 2011], durante la fase di verifica e validazione dell'origine: la priorità è data al certificato recuperato nel record TLSA. In futuro si consiglia di lasciare come opzionale la presenza di questo certificato nel messaggio PEC, mantenuto per retrocompatibilità con

l'attuale metodo basato sul file LDIF, in modo da poter ridurre, dove possibile, la dimensione del messaggio e quindi il traffico SMTP.

Per limitare i fenomi di caching, in caso di revoca di un certificato X.509v3, ad esempio in conseguenza alla compromissione della chiave, il corrispondente record RRSIG che lo autentica deve avere durata di validità non superiore ad un giorno, così come per i record NSEC che ne autenticano l'assenza. In questo modo, è possibile ridurre l'inconsistenza tra cache locale ai Resolver e i dati contenuti nella Zona autoritativa ad un massimo del valore consentito per la PEC, come indicato nell'RFC6109 [IETF, 2011].

Il rollover dei certificati X.509v3 pubblicati tramite record TLSA, viene effettuato seguendo lo stesso algoritmo descritto nell'RFC5011 [IETF, 2007a] per il rollover automatico dei Trust Anchor, riassunto nei seguenti punti:

- **Creazione nuovo certificato**: con sufficiente anticipo prima della scadenza del certificato pubblicato, viene emesso un nuovo certificato X.509v3, ridotto alla sola parte SPKI, descritta nell'RFC5280 [IETF, 2008b]. I parametri del record TLSA, a eccezione del campo rappresentante la codifica del certificato, non devono cambiare.

- **Pubblicazione**: Il nuovo record TLSA relativo al nuovo certificato emesso deve essere inserito nella propria Zona autoritativa in modo tale che la data di inizio validità del record RRSIG che lo autentica sia di poco precedente alla data di fine validità del record RRSIG che autentica il vecchio record TLSA. Questo permette di attendere fino a quando tutte le cache dei Resolver hanno invalidato il precedente record TLSA.

- **Rimozione record precedente**: Allo scadere della validità del vecchio record TLSA, esso deve essere rimosso dalla Zona autoritativa in cui era stato pubblicato.

Il rollover dei record TXT usati per l'autenticazione dei PEC providers e dei domini PEC utilizza lo stesso algoritmo suddetto.

4 Punti di forza e debolezza della proposta

In questa sezione si riassumono i punti di forza e di debolezza del metodo descritto in questa proposta.

Innanzitutto, si nota come gli obiettivi prefissati nella sezione 1 sono stati raggiunti, risolvendo le problematiche riportate in sezione 1.1:

- **Adozione nuova proposta graduale**:Il nuovo metodo proposto spostao le funzionalità prima accentrate nel file LDIF all'interno dell'infrastruttura DNS e distribuendo le responsabilità amministrative e tecniche tra i vari attori, senza punti di centralizzazione. E'inoltre possibile una sua applicazione graduale: qualora l'infrastruttura DNSSec sia temporaneamente o permanentemente non utilizzabile, un PEC provider può continuare ad

usare il vecchio file LDIF in attesa di un completo adeguamento da parte di tutti i PEC providers.

Se un PEC provider implementa il nuovo metodo, il suo uso ha comunque priorità rispetto al metodo basato sul file LDIF per evitare eventuali discrepanze.

- **Gestione distribuita e autonoma dei certificati X.509v3**: questo ha permesso di scaricare AGID delle problematiche relavite alla emissione, revoca ed aggiornamento dei certificati X.509v3 dei PEC providers.
- **Interoperabilita**: l'interoperabilità con i provider di posta elettronica ordinaria è garantita dalla retrocompatibilità di DNSSec, che può inviare risposte prive dei record di segnatura alle query sottomesse dai Resolver non validanti.
- **Aderenza agli standard internazionali**: attraverso l'uso di standard internazionali riconosciuti, come il DNSSec e DANE [IETF, 2012], è ora aperta una strada per poter rendere la PEC interoperabile anche con altre infrastrutture CEM.
- **Limitato numero di cambiamenti nell'infrastruttura**
  - Nessuna modifica necessaria ai client degli utenti.
  - Nessuna modifica necessaria al formato dei messaggi PEC e delle ricevute.
  - Nessuna modifica necessaria al software di gestione della posta elettronica
  - Modifiche minimali al software di gestione della PEC, limitate alle operazioni di recupero dei certificati X.509v3 e di identificazione dei PEC provider e dei domini PEC
  - Requisito nell'uso del DNSSec limitato ai domini di AGID e dei PEC providers
- **Scalabilità**: il numero dei PEC providers o dei domini PEC non influisce sulla dimensione delle varie Zone autoritative, grazie all'adozione di un metodo distribuito basato su Revocation List.
- **Sicurezza**: i livelli di sicurezza contro gli attacchi informatici, e il livello di controllo sull'infrastruttura da parte di AGID sono equivalenti o in alcuni casi superiori a quelli precedenti, con l'eccezione delle due problematiche descritte alla fine della sezione 3.2.

  I vantaggi in termini di autenticazione dell'origine dei dati, autenticazione della non esistenza, integrità e protezione da svariate tipologie di attacchi informati, dati dall'uso dell'infrastruttura DNSSec, hanno permesso di mantenere un livello di sicurezza equivalente almeno al metodo basato sull'uso del file LDIF, permettendo ad AGID di identificare tempestivamente le responsabilità dei PEC provider sul contenuto e la correttezza delle loro Zone autoritative.

Si devono però indicare i seguenti punti di debolezza ed alcune delle problematiche ancora aperte:

- **Complessità di gestione**: l'uso del DNSSec porta ad una maggiore complessità di gestione delle Zone autoritative, in termini di competenza, strumenti e tempo per la gestione delle procedure, in particolare per i PEC providers, che ora hanno un maggior ruolo attivo nel funzionamento dell'infrastruttura, e per i domini PEC, che devono porre attenzione al mantenimento e rollover dei record TXT firmati dal PEC provider gestore.

  Nelle tabelle 4 e 4 sono riportate, ad alto livello le operazioni eseguite dai vari attori rispettivamente nel metodo con uso del file LDIF e nel metodo distribuito con Revocation List, in modo da poterli comparare.

- **Canali sicuri**: vi è la necessità di proteggere il canale tra i Resolver (non validanti) e i Name Server DNSSec, per evitare attacchi di tipo MITM. E' consigliato l'uso di Resolver validanti da parte dei PEC provider.

  I canali utilizzati per distribuire i file TXT firmati da AGID o dai PEC provider devono essere sicuri per poter evitare, anche in questo caso, attacchi di tipo MITM.

- **Maggior traffico DNS**: l'uso del DNSSec e del metodo distribuito con Revocation List comporta un inevitabile aumento del traffico DNS verso i domini di AGID e dei PEC provider.

References

[group, 2014] group, D. (2014). Smtp security via opportunistic dane tls - draft-ietf-dane-smtp-with-dane-12. https://tools.ietf.org/html/draft-ietf-dane-smtp-with-dane-12.

[IETF, 1987a] IETF (1987a). Rfc1033 - domain administrators operations guide. https://www.ietf.org/rfc/rfc1033.txt.

[IETF, 1987b] IETF (1987b). Rfc1034 - domain names - concepts and facilities. https://www.ietf.org/rfc/rfc1034.txt.

[IETF, 1987c] IETF (1987c). Rfc1035 - domain names - implementation and specification. https://www.ietf.org/rfc/rfc1035.txt.

[IETF, 1999] IETF (1999). Rfc2459 - internet x.509 public key infrastructure certificate and crl profile. https://www.ietf.org/rfc/rfc2459.txt.

[IETF, 2000] IETF (2000). Rfc2849 - the ldap data interchange format (ldif) - technical specification. https://www.ietf.org/rfc/rfc2849.txt.

[IETF, 2001] IETF (2001). Rfc2821 - simple mail transfer protocol. https://www.ietf.org/rfc/rfc2821.txt.

[IETF, 2002] IETF (2002). Rfc3279 - algorithms and identifiers for the internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. https://www.ietf.org/rfc/rfc3279.txt.

[IETF, 2004] IETF (2004). Rfc3833 - threat analysis of the domain name system (dns). https://www.ietf.org/rfc/rfc3833.txt.

[IETF, 2005a] IETF (2005a). Rfc4025 - a method for storing ipsec keying material in dns. https://www.ietf.org/rfc/rfc4025.txt.

[IETF, 2005b] IETF (2005b). Rfc4033 - dns security introduction and requirements. https://www.ietf.org/rfc/rfc4033.txt.

[IETF, 2005c] IETF (2005c). Rfc4034 - resource records for the dns security extensions. https://www.ietf.org/rfc/rfc4034.txt.

[IETF, 2005d] IETF (2005d). Rfc4035 - protocol modifications for the dns security extensions. https://www.ietf.org/rfc/rfc4035.txt.

[IETF, 2006a] IETF (2006a). Rfc4255 - using dns to securely publish secure shell (ssh) key fingerprints. https://www.ietf.org/rfc/rfc4255.txt.

[IETF, 2006b] IETF (2006b). Rfc4398 - storing certificates in the domain name system (dns). https://www.ietf.org/rfc/rfc4398.txt.

[IETF, 2007a] IETF (2007a). Rfc5011 - automated updates of dns security (dnssec) trust anchors. https://www.ietf.org/rfc/rfc5011.txt.

[IETF, 2007b] IETF (2007b). Rfc5074 - dnssec lookaside validation (dlv). https://www.ietf.org/rfc/rfc5074.txt.

[IETF, 2008a] IETF (2008a). Rfc5155 - dns security (dnssec) hashed authenticated denial of existence. https://www.ietf.org/rfc/rfc5155.txt.

[IETF, 2008b] IETF (2008b). Rfc5280 - internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. https://www.ietf.org/rfc/rfc5280.txt.

[IETF, 2010] IETF (2010). Rfc5751 - secure/multipurpose internet mail extensions (s/mime) version 3.2: Message specification. https://www.ietf.org/rfc/rfc5751.txt.

[IETF, 2011] IETF (2011). Rfc6109 - la posta elettronica certificata - italian certified electronic mail. http://tools.ietf.org/html/rfc6109.

[IETF, 2012] IETF (2012). Rfc6698 - the dns-based authentication of named entities (dane) transport layer security (tls) protocol: Tlsa. https://www.ietf.org/rfc/rfc6698.txt.

[IETF, 2013] IETF (2013). Rfc6840 - clarifications and implementation notes for dns security (dnssec). https://www.ietf.org/rfc/rfc6840.txt.

AGID	PEC provider	Dominio PEC
Mantiene lista di Provider e domini PEC (file LDIF).	Invia il proprio file LDIF ad AGID ad ogni aggiornamento dei propri domini PEC	Configura MX record nella propria zona DNS
	Scarica il file LDIF aggiornato giornalmente	Configura i client di posta per accedere al mailserver del PEC provider
Emette/revoca certificati per i PEC provider (chiave pubblica nel server LDIF)	Riceve il proprio certificato da AGID e lo inserisce nel proprio file LDIF	

Table 1: Operazioni eseguite dai vari attori nel metodo con uso del file LDIF

AGID	PEC provider	Dominio PEC
Crea una zona DNSSec • Mantiene una Revocation List(RL) dei PEC provider • Genera una coppia di chiavi • Firma con la chiave privata i record che certificano i PEC provider • Azzera la RL dei PEC provider revocati ad ogni aggiornamento della chiave • Distribuisce i record firmati a tutti i PEC provider • Inserisce la chiave pubblica nella propria zona	Crea una zona DNSSec • Mantiene una Revocation List dei domini PEC • Genera una coppia di chiavi • Firma con la chiave privata generata i record che certificano i domini PEC • Azzera la RL dei domini PEC revocati ad ogni aggiornamento della chiave • Distribuisce i record firmati a tutti i domini PEC • Inserisce la chiave pubblica nella propria zona Gestisce i propri certificati Inserisce nella sua zona il record firmato da AGID	Crea una zona DNS Inserisce nella propria zona il record firmato dal PEC provider Configura MX record nella propria zona Configura i client di posta per accedere al mail server del PEC provider

Table 2: Operazioni eseguite dai vari attori nel metodo con uso del DNSSec