Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"
Consiglio Nazionale delle Ricerche

ISTI Technical Reports

Analisi di particolari condizioni di insicurezza della REM (Registered EMail)

Loredana Martusciello, CNR-IIT, Pisa, Italy
Francesco Gennai, CNR-ISTI, Pisa, Italy
Marina Buzzi, CNR-IIT, Pisa, Italy

ISTI-TR-2022/003

Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"
Consiglio Nazionale delle Ricerche

Analisi di particolari condizioni di insicurezza della REM (Registered EMail)

Martusciello L.; Gennai F.; Buzzi M.

ISTI-TR-2022/003

Abstract

Descrizione di una potenziale problematica di sicurezza nel funzionamento della REM (Registered Electronic Mail) e le relative deduzioni.

REM, Registered email, Posta Elettronica Certificata, PEC, Sicurezza, Certified Electronic Email, Agid, Trusted List, MITM, MOTM, SMTP, MX, record MX, ETSI, 319 532-4, ETSI EN 319 532-4, 532-4

Citation

Martusciello L.; Gennai F.; Buzzi M. *Analisi di particolari condizioni di insicurezza della REM (Registered EMail)* ISTI Technical Reports 2022/003. DOI: 10.32079/ISTI-TR-2022/003

Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"
Area della Ricerca CNR di Pisa
Via G. Moruzzi 1
56124 Pisa Italy
http://www.isti.cnr.it

Analisi di particolari condizioni di insicurezza della REM (Registered EMail)

Loredana Martusciello (IIT-CNR)
Francesco Gennai (ISTI-CNR)
Marina Buzzi (IIT-CNR)

Marzo 2022

Indice

Introduzione

In questo documento viene descritta una potenziale problematica di sicurezza nel funzionamento della REM (Registered Electronic Mail) [1] e le relative deduzioni.

Nel seguito sono descritte sinteticamente le azioni che compie un qualsiasi provider (anche non REM) per inviare la posta ad un qualsiasi dominio Internet (in questo esempio dom1.it).

1) interroga il DNS per ottenere il record MX [2]

```
dom1.it  IN  MX 10  email.genericproviderx.it.
```

2) estrae il nome email.genericproviderx.it, che è il nome del server SMTP del provider remoto verso cui aprire la sessione SMTP per la trasmissione della email indirizzata a dom1.it
3) apre la sessione SMTP verso il server email.genericproviderx.it
4) se il server email.genericproviderx.it, nella risposta che dà al server mittente, annuncia l'estensione STARTTLS [3] significa che è in grado di accettare una sessione SMTP-TLS.
É da notare che, fin qui, la comunicazione tra il server mittente e il destinatario è avvenuta in chiaro.
5) a questo punto, il server mittente, se supporta TLS, può far partire l'*handshacking* dei certificati, quindi la sessione SMTP su TLS, questo modo di attivare il TLS è chiamato *opportunistic TLS*[1] [4]

Questo schema di funzionamento, ad oggi il più diffuso in Internet, non prevede che i due server ai capi della sessione SMTP-TLS si debbano identificare. L'uso dei certificati è finalizzato solo allo scambio delle rispettive chiavi pubbliche da utilizzare nell'*encrypt* della sessione, da qui l'ampio utilizzo, comunque corretto, di certificati *self-signed*, che non sono utilizzabili per l'identificazione dell'organizzazione che li utilizza.
Questo schema di funzionamento è di facile attacco di tipo MOTM (Monkey-In-The-Middle), anche conosciuto come MITM (Man-In-The-Middle)[2]. Infatti, è sufficiente che un hacker intercetti la prima risposta in chiaro che il server SMTP destinatario

[1] https://en.wikipedia.org/wiki/Opportunistic_TLS
[2] https://en.wikipedia.org/wiki/Man-in-the-middle_attack
In cryptography and computer security, a man-in-the-middle, monster-in-the-middle, machine-in-the-middle, monkey-in-the-middle, […]

invia al client SMTP (mittente), rimuovendo dalla stessa la keyword STARTTLS, per far credere al server mittente che il server destinatario non supporta il TLS.
Esempio di una normale sessione SMTP, estratto da:
https://en.wikipedia.org/wiki/Opportunistic_TLS
Dove S: = server SMTP, C: = client SMTP

```
S: <waits for connection on TCP port 25>
C: <opens connection>
S: 220 mail.example.org ESMTP service ready
C: EHLO client.example.org
S: 250-mail.example.org offers a warm hug of welcome
S: 250 STARTTLS
C: STARTTLS
S: 220 Go ahead
C: <starts TLS negotiation>
C & S: <negotiate a TLS session>
C & S: <check result of negotiation>
C: EHLO client.example.org
. . .
```

In questo esempio, l'attacco MOTM consiste nel rimuovere la riga S: 250 STARTTLS dalle sequenze di dati inviati al client.
A questo punto, il sistema mittente (client SMTP) è obbligato ad aprire una sessione in chiaro. Il sistema di destinazione (server SMTP), ricevendo la sessione in chiaro, la accetterà presupponendo che il server mittente non supporti TLS.
Un altro tipo di attacco, che porta ad un risultato analogo al precedente, consiste nell'intercettare la query al DNS che il client SMTP deve fare, per ottenere l'MX record contenente il nome del server destinatario verso cui aprire una sessione SMTP.
La comunicazione con il DNS (query e relativa risposta) avviene in chiaro sulla rete, la risposta può, perciò, essere intercettata da un hacker, inserendo nell'MX record il nome di un server email sotto il suo controllo. Il client SMTP, ignaro di questa modifica, aprirà la sessione SMTP verso tale server per l'invio delle email che erano destinate altrove. Il server dell'hacker potrà, a sua volta, inviarle all'effettivo server di destinazione.
In entrambi gli esempi qui riportati, le azioni di *hacking* risultano invisibili ai capi della comunicazione. Nel primo caso è abbastanza evidente, poiché l'email giunge comunque al server di destinazione. Nel secondo caso, il server dell'hacker può semplicemente inoltrare l'email catturata verso la sua effettiva destinazione.
Per ovviare alle criticità citate nelle note precedenti (identificazione del server e garanzia che la sessione sia TLS), sono state definite dall'IETF[3] due diverse soluzioni:

[3] https://www.ietf.org/

DNS-based Authentication of Named Entities (DANE)[4] [5] [6] e SMTP MTA Strict Transport Security (MTA-STS)[5] [7]. DANE ha come prerequisito DNSSEC[6], ma la lentezza della diffusione di DNSSEC [8] ha causato difficoltà nella sua diffusione. Anche per questo motivo è stato proposto MTA-STS, che non utilizza DNSSEC.
La versione base di MTA-STS presenta alcune criticità (descritte nella stessa RFC 8461), che potrebbero essere contrastate grazie alla possibilità di utilizzare le estensioni previste dallo standard.

Veniamo adesso a quanto si trova nelle specifiche tecniche della REM in merito alle criticità relative all'individuazione dei server SMTP di destinazione e alle garanzie che venga utilizzato il TLS nella sessione SMTP.

Background

Per attivare un dominio Internet come dominio di posta REM occorre individuare un provider REM e, conseguentemente, configurare il name server per indirizzare la posta verso il server REM del provider individuato. In pratica si tratta di inserire nel name server autoritativo per la zona del DNS cui appartiene il dominio Internet, un opportuno record MX. Questo indirizzamento, avviene, con il meccanismo descritto nell'introduzione.
Il name server del dominio di posta REM può essere gestito da un'organizzazione (ma anche individualmente, nel caso di domini personali) che non ha alcuna relazione con il Provider REM prescelto. In questo caso le policy di gestione del name server sono al di fuori della REM, comunque non facilmente controllabili.

Le descrizioni dei passi che andiamo a rivedere nei seguenti paragrafi sono, in parte, semplificate per concentrarsi principalmente sulla loro la semantica.
Rivediamo alcuni passi introdotti all'inizio: questa volta è un provider REM ad essere coinvolto nell'invio al dominio dom1.it.
Il Provider REM ha appena ricevuto, da un proprio utente, una email da inviare a mailbox1@dom1.it.
In questa fase, il Provider REM non sa ancora se il dominio dom1.it è un dominio REM o un normale dominio esterno alla REM.

[4] https://datatracker.ietf.org/doc/html/rfc7671
[5] https://datatracker.ietf.org/doc/html/rfc8461
[6] https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions

Per sapere se il dominio è REM o NON-REM deve effettuare alcune query al DNS e alcune verifiche che vedremo di seguito in dettaglio.
Compone comunque il *Dispatch* per poi accodarlo verso l'inoltro al server remoto.

1X) il Provider interroga il DNS per ottenere il record MX.
Il name server, amministrato dall'organizzazione (o dall'individuo) titolare della Zona DNS dom1.it darà la seguente risposta (esempio).

```
dom1.it    IN    MX 10    email.remproviderx.it.
```

2X) email.remproviderx.it è il nome con cui il server SMTP del provider di destinazione è registrato in Internet.
Se il nome email.remproviderx.it è presente nella *Trusted List* (gestita in modo centralizzato e resa disponibile ad ogni provider REM da una autorità di controllo e certificazione), il dominio è REM, altrimenti non è REM.

(i prossimi due passi (3X e 4X) vengono descritti ancora nella modalità standard Internet, le specifiche REM che influenzano questi due punti vengono introdotte nelle successive descrizioni)

3X) il Provider apre la sessione SMTP verso il server email.remproviderx.it.

4X) se il server email.remproviderx.it annuncia, nella risposta inviata al mittente, l'estensione STARTTLS significa che il è in grado di accettare una sessione SMTP criptata.

Abbiamo già visto come i passi 3X e 4X siano quelli soggetti ad attacchi MOTM.
È su questi due passi che la REM interviene introducendo la Common Service Interface (CSI), per evitare l'apertura di una sessione SMTP tra Provider REM se questa non è SMTP-TLS (eliminando, quindi, l'opportunistic TLS) e per identificare il server di destinazione come uno dei server appartenenti ad un Provider REM.
La certificazione che un dominio di posta Internet sia REM (dom1.it nell'esempio) è invece completamente assente. Si richiama ancora l'attenzione sul fatto che il record MX, con cui un dominio Internet è identificato come REM attraverso l'associazione al server SMTP di un Provider REM, si trova in Zone DNS spesso gestite da organizzazioni esterne al sistema REM, con proprie policy e propri livelli di sicurezza.

Descrizione del funzionamento della REM

In questo paragrafo viene data una descrizione della REM in relazione alle criticità sopra esposte. In particolare non viene fornita una descrizione completa della Trusted List e della CSI, ma vengono individuati e descritti gli elementi rilevanti per lo scopo di questo documento, utilizzando una pseudo-terminologia. Si rimanda alla documentazione ufficiale per una presentazione più completa e formale delle definizioni.

Nel sistema REM sono presenti due componenti per le applicazioni di funzioni crittografiche, tra loro indipendenti:
1) la prima è rappresentata dal certificato e dalla relativa chiave privata con la quale un Provider REM applica le seguenti firme:
- firma del file XML (*evidence*) che viene inserito nella struttura MIME multipart/mixed di una email REM;
- firma della struttura MIME multipart/mixed (generazione di una email in formato S/MIME)
- firma del documento *CapabilityAndSecurityInformartion.xml* (descritto più avanti)
Chiameremo di seguito questo certificato: Certificato di Firma.
2) la seconda è rappresentata dal certificato e dalla relativa chiave privata che ogni Provider deve configurare nel proprio server SMTP per l'attivazione delle sessioni SMTP-TLS tra provider mittente e provider destinatario.
Chiameremo di seguito questo certificato: Certificato TLS.

La Trusted List

È un documento XML, digitalmente firmato da un'autorità di controllo e certificazione, che contiene dettagli tecnico/amministrativi per ogni service provider REM.
In particolare, a noi interessano gli elementi relativi alle funzioni di certificazione e alla creazione di relazioni di *trusting*.
Un Provider è riconosciuto (certificato) come provider REM attraverso la relativa definizione presente nella Trusted List.

Tra i dati di certificazione di un Provider presenti nella Trusted List, per il nostro scopo ci interessano i due elementi chiamati Service Supply Point (SSP):
1) il primo contiene il nome Internet con il quale il server SMTP del Provider è registrato nel DNS ed ha la sintassi:

smtp://hostname:25 (esempio: smtp://mailserv.example.it:25)

2) il secondo contiene un link a una pagina web che ogni Provider è tenuto a presentare, contenente un file XML (digitalmente firmato dal Provider). Il documento XML scaricabile da questo sito web, gestito ovviamente dal Provider, viene referenziato con il nome Capability And Security Information [1].

Vediamo adesso le azioni e le condizioni di sicurezza con cui può operare un Provider REM (Provider REM mittente) che deve inviare una email indirizzata a mario.rossi@dom1.it.

Il Provider REM estrae il dominio dom1.it dall'indirizzo mario.rossi@dom1.it e lo utilizza nei seguenti passi per ottenere le informazioni che gli occorrono per completare l'invio della email verso la sua destinazione.

Qui si rappresenta la fase di Relay, cioè il momento in cui il Provider REM mittente effettua le azioni necessarie per trasmettere l'email verso il Provider di destinazione.

1Z) interroga il DNS per ottenere il record MX

Il name server, amministrato dall'organizzazione (o dall'individuo) titolare della Zona DNS dom1.it darà la seguente risposta (esempio):

dom1.it IN MX 10 email.remproviderx.it.

Nessun controllo è presente nella REM per avere la certezza che la risposta a questa query sia corretta, cioè non sia vittima di uno tra i possibili attacchi, tra cui MOTM.

Supponiamo che la risposta sia quella corretta.

2Z) email.remproviderx.it è il nome con cui il server SMTP del provider di destinazione è registrato in Internet.

Se il nome è presente nella Trusted List (gestita in modo centralizzato e resa disponibile ad ogni provider REM da una autorità di controllo e certificazione), il dominio è REM, altrimenti non è REM.

Supponiamo che email.remproviderx.it sia presente nella Trusted List, come SSP del Provider REM X. Ecco che, a questo punto, il Provider REM mittente sa che sta inviando ad un altro Provider REM (Provider REM X).

Nota: l'interrogazione al DNS, di cui al precedente punto 1Z, potrebbe essere fatta in una fase antecedente a quella di Relay, per effettuare eventuali verifiche qualora la risposta ci indichi un Provider REM. La necessità di interrogare il DNS in fase di composizione della email (*submission*) è un aspetto molto critico, da trattare con opportune considerazioni e conseguenti soluzioni ottimali. Questa necessità risulta

dalla clausola C.3.2.1 b) ii, NOTE2 del documento REM ETSI[7] e introduce criticità già segnalate nella nota "Note relative alla REM 28/01/2022 (ver. 1.1, paragrafo 2)" fase di submission, relativa a REM Policy IT paragrafo 2.4.2.6)[8]. L'argomento non viene ulteriormente approfondito in questo documento.

3Z) apre la sessione SMTP verso il server email.remproviderx.it
Sapendo che email.remproviderx.it è un Provider REM (presenza del SSP smtp://email.remproviderx.it:25) nella Trusted List, può prelevare dalla stessa Trusted List (sezione del Provider identificato dal precedente SSP) l'altro SSP della forma (esempio) https://capa.remproviderx.it/capsec.
Dal link https://capa.remproviderx.it/capsec ottiene il file CapabilityAndSecurityInformartion.xml, ne verifica la firma tramite il certificato X509 (Certificato di Firma) dal quale estrae il certificato X509, Certificato TLS, che il server SMTP email.remproviderx.it presenta nelle sessioni SMTP-TLS

4Z) se il server email.remproviderx.it annuncia, nella risposta che invia al server mittente, l'estensione STARTTLS significa che è in grado di accettare una sessione SMTP-TLS.
Sapendo che il server email.remproviderx.it è un Provider REM, il Provider mittente REM (client SMTP):
- non aprirà la sessione SMTP in assenza della keyword STARTTLS nella risposta del server, così l'eventuale attacco MOTM già descritto (rimozione della stringa STARTTLS dalla risposta del server) non potrà avere successo.
- ottenuta, altrimenti, la keyword STARTTLS, il Provider mittente REM (client SMTP), aprirà la sessione SMTP-TLS e verificherà (prima di procedere con gli ulteriori passi della sessione stessa) che il certificato ottenuto dal server SMTP email.remproviderx.it corrisponda a quello che lo stesso Provider remoto presenta nella sua CapabilityAndSecurityInformartion.xml.
Cosa potrebbe fare un attacco MOTM in questo caso?

- interferire sulle risposte che il DNS dà alle query del provider mittente reindirizzando il nome email.remproviderx.it verso un server SMTP sotto il suo controllo (non più quello del Provider X)

[7] vedi ETSI EN 319 532-4 v.1.1.7 Clausola C.3.2.1 b) ii, NOTE2
[8] Gruppo di Lavoro AGID-ISTI - protocollo 0001734/2021 [accordo di collaborazione fra CNR-ISTI e AGID ex art. 15 legge n. 241/1990 e ss.mm.ii. per la messa a disposizione di una piattaforma di test per la verifica dei servizi REM, conformi al regolamento eIDAS n. 910/2014, erogati dai Gestori PEC a supporto della migrazione dalla PEC alla REM]

- ottenere un certificato da una CA (tra le tante precaricate nei sistemi operativi, ma non tanto affidabile) dove inserisce nel Subject il nome del Provider, da utilizzare come certificato TLS.
- potrebbe, allo stesso modo, far corrispondere il link https://capa.providex.it/capasec a una pagina sotto il suo controllo, dove ha caricato una CapabilityAndSecurityInformartion.xml (ovviamente falsa), che presenta il Certificato TLS ottenuto dalla CA
- quello che NON POTRA' FARE è firmare il CapabilityAndSecurityInformartion.xml [1] con la firma corrispondente al certificato del Provider (hackerato) presente nella Trusted List. Questo permetterà al Provider REM mittente di rilevare l'errore nella verifica della firma della CapabilityAndSecurityInformartion.xml, quindi di evitare il completamento della sessione SMTP-TLS.

L'attacco non ha avuto successo.
La catena di Trusting Certificato-TLS/CapabilityAndSecurityInformation/Certificato-di-Firma/Trusted List è stata interrotta.

Vi sono altri attacchi possibili, bloccati dalla catena di trusting che è implicitamente descritta nell'esempio sopra.

Purtroppo, nella REM (REM ETSI, REM Policy IT [9]) manca l'altrettanto fondamentale elemento di trusting tra un dominio di posta Internet e un provider REM. Fondamentale non solo per certificar" la relazione di trusting tra un dominio di posta Internet e il suo corretto Provider REM, ma anche perchè a tale funzione è delegata l'identificazione di un dominio REM o NON-REM.

Vediamo un esempio.
Il Provider mittente REM deve inviare una email a mario.rossi@dom1.it
Preleva, quindi, il dominio dom1.it per la determinazione del server SMTP a cui inoltrare l'email.

1W) interroga il DNS per ottenere il record MX
Il name server, amministrato dall'organizzazione (o dall'individuo) titolare della Zona DNS dom1.it darà la seguente risposta (esempio).

```
dom1.it  IN  MX 10  email.remproviderx.it.
```

Il record MX indirizza verso il server SMTP del Provider REM X, pertanto dom1.it è un dominio REM.
Come già detto, queste query/answer al DNS avvengono in chiaro.
Un possibile attacco potrebbe modificare la risposta cambiando il nome del server del Provider REM X email.remproviderx.it, con un altro nome Internet (esempio: mx.domproviderhk.it), che corrisponde a un server SMTP evidentemente sotto il controllo dell'attaccante.

2W) mx.domproviderhk.it è il nome con cui il server SMTP di destinazione è registrato in Internet e sarà presumibilmente un server gestito dall'attaccante.
Il nome mx.domproviderhk.it, evidentemente (in questo esempio), non è registrato nei SSP di tipo smtp://hostname:25 presenti nella Trusted List, pertanto il Provider REM mittente identificherà il dominio dom1.it (che doveva essere REM), come dominio non REM e potrà inviare l'email (il Dispatch) verso tale server, come External al sistema REM.

3W) il provider REM mittente apre la sessione SMTP verso il server mx.domproviderhk.it secondo le modalità standard di gestione delle email Internet.
L'attacco è concluso con successo.

Un altro tipo di attacco potrebbe prevedere la modifica del server di destinazione (REM) con un altro server di destinazione sempre REM. Qui, ovviamente, occorrerebbe la complicità del Provider REM ricevente, ma il Provider REM mittente non dispone di alcuno strumento per rilevare anche questo tipo di attacco.

Va detto che alcune delle anomalie derivanti dagli attacchi qui descritti, potrebbero essere determinate anche da configurazioni errate, che potrebbero non essere rilevate in modo opportuno.

Ricordando il caso delle azioni, denunciate nel 2013 dal tecnico della CIA Edward Snowden, con le quali gli USA spiavano Ambasciate e Diplomatici di tutto il mondo, incluso gli Europei, risulta evidente come queste lacune siano inaccettabili per un sistema come la REM, dove si può presumere che le comunicazioni che dovrebbe gestire possano anche essere di particolare rilievo amministrativo, legale, politico.

La buona volontà, attenzione, competenza degli amministratori degli oggetti che sono in gioco (name server, etc..) non è sufficiente a contrastare in modo efficace questa grave lacuna di sicurezza.
I name server delle organizzazioni che delegano un proprio dominio all'uso REM, le infrastrutture di rete ed informatiche intorno ad essi, le policy di amministrazione, non sono controllabili.

Discussione

In un qualsiasi sistema di Certified Electronic Email, categoria alla quale la REM appartiene, si possono identificare due principali componenti nel nucleo del suo schema di funzionamento che sono:
a) i provider, che si presentano su Internet con i propri server SMTP (di seguito Provider REM, che costituiscono il Gruppo Provider REM in grado di comunicare tra loro secondo specifiche comuni).
b) i domini email (di seguito Domini REM, ognuno appartenente ad un Provider REM) che definiscono lo spazio dei nomi delle mailbox certificate.

Si può presupporre che il numero dei Provider REM presenti in un Gruppo Provider REM sia di qualche ordine di grandezza inferiore al numero totale dei Domini REM.

A questo punto si evidenzia la necessità di individuare le opportune soluzioni tecnologiche per l'identificazione e la certificazione di un Provider e della sua appartenenza ad un Gruppo e per l'identificazione e certificazione di un Domino REM e della sua appartenenza ad un Provider REM.
Le due funzioni di identificazione/certificazione, che per brevità chiameremo "Certificazione di un Provider" e "Certificazione di un Dominio", sono indipendenti l'una dall'altra, ma possono anche confluire in un’unica soluzione tecnologica.

Confronto con la PEC

Nella Posta Elettronica Certificata (PEC) [10] la soluzione tecnologica scelta, rappresentata dal file LDIF - IGPEC, permette l’identificazione di un Provider e dei Domini PEC che gli appartengono.
Al contrario della REM, nella PEC non è presente un meccanismo che permetta a un Provider di avere le necessarie garanzie per identificare il Provider remoto all’apertura

di una sessione SMTP-TLS: in pratica, fa uso della semplice soluzione opportunistic TLS, quindi non è protetta da un attacco MITM che diriga la sessione SMTP-TLS verso un Provider sotto il controllo dell'hacker.
La soluzione PEC, tecnologicamente semplice, assolve invece alla funzione di certificazione di un Dominio (associazione sicura di un dominio al Provider che lo gestisce) ma, come spesso avviene nelle soluzioni semplici, può presentare maggiori problemi nella sua gestione e scalabilità.
In particolare, la criticità relativa alla sua scalabilità è principalmente dovuta alla Certificazione dei Domini, non tanto alla identificazione dei Provider che difficilmente raggiungeranno un numero così elevato paragonabile a quello dei domini.

Nella REM, troviamo la completa Certificazione di un Provider ma manca totalmente la "Certificazione di un Dominio".
Un dominio email Internet si presenta al sistema REM nello stesso identico modo con cui si presenta al sistema PEC, cioè tramite un MX record inserito in un name server al di fuori dell'applicabilità di una policy di controllo centralizzata. Ricordo che il name server è gestito da unità organizzative esterne (organizzazioni, individui con sistemi personali, etc.).
Il sistema PEC ha, quindi, correttamente adottato una soluzione che, evitando ogni interferenza con la gestione di componenti non controllabili quali i name server di altre unità organizzative, certifica un dominio come PEC a costo di una gestione centralizzata di alcune informazioni, con conseguenti problemi di scalabilità.
Per una gestione distribuita si può certamente fare ricorso ad altre soluzioni, che fanno uso del DNS (DANE) o del web (MTA-STS), ma queste due soluzioni prevedono un coinvolgimento delle citate unità organizzative esterne e attività di manutenzione (rinnovo certificati, etc.).
In conclusione, nel caso specifico descritto nelle precedenti righe, la migliore scalabilità di un sistema si ottiene al costo di distribuire configurazioni e relative attività di manutenzione tra molteplici unità organizzative. Rinunciare alla distribuzione, per evitare di caricare su unità organizzative esterne aspetti operativi che potrebbero non essere gestiti correttamente, è possibile centralizzando, ma a costo della minore scalabilità del sistema (caso PEC).
Si possono certamente individuare dei compromessi, che riducano o eliminino gli aspetti gestionali esterni rinunciando a parte della scalabilità.
Le citate soluzioni distribuite (DANE, MTA-STS) sono tali da garantire la necessaria sicurezza/certificazione anche a fronte di operazioni/configurazioni errate da parte

delle singole unità operative esterne. In questi casi la singola unità potrà essere soggetta ad un disservizio, senza però compromettere sicurezza/certificazione/funzionalità al di fuori del suo spazio dei nomi DNS.

Considerazioni finali

I documenti presentati come standard (ETSI REM, REM Policy IT) contengono, oltre alla grave lacuna di cui sopra, altre rilevanti criticità (come, ad esempio, la richiesta di identificare il tipo di dominio, REM o non REM, in fase di submission), definizioni di modalità operative che non sono applicabili (come la gestione dell'invio verso provider NON-REM), forzature/violazioni degli standard di riferimento (come il rifiuto totale di una email indirizzata a più destinatari, nel caso che anche un solo indirizzo di destinazione sia sconosciuto).
In conclusione, riteniamo che sarebbe opportuna una accurata revisione dei documenti di riferimento per risolvere le debolezze evidenziate e rendere la REM un sistema robusto ed affidabile.

Bibliografia

[1] «Draft ETSI EN 319 532-4 V1.1.7 (2022-01)». Available: https://www.etsi.org/deliver/etsi_en/319500_319599/31953204/01.01.07_20/en_31953204v010107a.pdf.

[2] «RFC 5321 - Simple Mail Transfer Protocol». Available: https://datatracker.ietf.org/doc/html/rfc5321.

[3] «RFC 3207 - SMTP Service Extension for Secure SMTP over Transport Layer Security». Available: https://www.rfc-editor.org/rfc/rfc3207.txt.

[4] «RFC 7435 - Opportunistic Security: Some Protection Most of the Time». Available: https://datatracker.ietf.org/doc/html/rfc7435.html.

[5] «RFC 7671 - The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance». Available: https://datatracker.ietf.org/doc/html/rfc7671.

[6] «RFC 7672 - SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)». Available: https://datatracker.ietf.org/doc/html/rfc7672.

[7] «RFC 8461 - SMTP MTA Strict Transport Security (MTA-STS)». Available: https://www.rfc-editor.org/rfc/rfc8461.txt.

[8] «RFC 4033 - DNS Security Introduction and Requirements». Available: https://datatracker.ietf.org/doc/html/rfc4033.

[9] «REM SERVICES – Criteri di adozione degli standard ETSI – Policy IT - Versione 1.1». Available: https://www.agid.gov.it/sites/default/files/repository_files/rem_services_-_criteri_di_adozione_degli_standard_etsi_-_policy_it_1.1_29_luglio_2021_0.pdf.

[10] «Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata». Available: https://www.agid.gov.it/sites/default/files/repository_files/leggi_decreti_direttive/pec_regole_tecniche_dm_2-nov-2005.pdf.