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

ISTI Technical Reports

REgistered eMail (REM) analisi semantica dell'elemento UntrustedPathToRecipient

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

ISTI-TR-2022/006

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

REgistered eMail (REM) analisi semantica dell'elemento UntrustedPathToRecipient

Martusciello L.; Gennai F.; Buzzi M.

ISTI-TR-2022/006

Abstract

Analisi di una particolare criticità presente nella specifica tecnica draft ETSI EN 119 532-4 V1.1.7 (2022 - 01), relativa alla fase di REM submission.

ETSI, Registered Email, REM, UntrustedPathToRecipient, Email, Internet, Posta certificata, Posta Elettronica Certificata, AGID, PEC, Etsi en 319 532-4

Citation

Martusciello L.; Gennai F.; Buzzi M. *REgistered eMail (REM) analisi semantica dell'elemento UntrustedPathToRecipient* ISTI Technical Reports 2022/006. DOI: 10.32079/ISTI-TR-2022/006

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

REgistered eMail (REM)
analisi semantica dell'elemento UntrustedPathToRecipient

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

Marzo 2022

Introduzione.

In questo rapporto tecnico viene analizzata una particolare criticità presente nella specifica tecnica draft ETSI EN 319 532-4 V1.1.7 (2022 – 01) [1], relativa alla fase di REM submission.

Per meglio comprendere l'analisi è necessaria una conoscenza della citata specifica ETSI.

Le specifiche tecniche REM (Registered Email) definiscono un sistema di comunicazioni certificate basate anche sul sistema email Internet [2], pertanto sarebbe opportuno trarre tutti i possibili vantaggi da questa scelta, nel rispetto delle caratteristiche funzionali dell'architettura di trasporto del sistema.

Un aspetto rilevante riguarda la semplicità delle soluzioni tecniche individuate e delle relative specifiche. Nel valutare una nuova idea progettuale siamo normalmente portati a individuare le soluzioni con una certa astrazione dalla realtà tecnologica. Il processo per giungere alla descrizione delle specifiche tecniche del progetto deve, quindi, tenere conto di molti aspetti: a partire dall'individuazione e dalla valutazione di soluzioni tecnologiche già presenti come standard, fino alla rivalutazione di ogni funzionalità presente nell'idea iniziale, con un confronto tra le implicazioni tecnologiche derivanti dalla loro implementazione e un ipotetico valore (importanza/utilità) assegnabile alla funzionalità all'interno dello schema progettuale. Questo può significare l'attivazione di un processo valutativo dinamico nel tempo, per individuare le funzionalità da rimuovere dall'iniziale idea progettuale, che, per quanto interessanti, possono avere un onere implementativo non giustificato dal loro valore all'interno del progetto.

Richiedere, per esempio, in fase di submission di una email, informazioni che il sistema email Internet incontrerà in una successiva fase del transito di una email, può introdurre problemi non facilmente controllabili.

Discussione.

Prendiamo in considerazione la clausola C.3.2.1 del draft ETSI EN 319 532-4 V1.1.7 (2022 – 01), che fornisce gli elementi per determinare, in fase di submission di una email, se il dominio remoto a cui l'email è indirizzata appartenga o meno al circuito REM, e vediamo come l'implementazione di questa richiesta possa essere dannosa al funzionamento della REM.

La prima cosa da osservare è che il sistema email Internet ha nella fase di relay tra sistemi diversi (mittente, destinatario) l'istante in cui verifica lo stato di un dominio a cui una email è indirizzata per poi, in base al risultato della verifica, procedere al suo inoltro.

Nella fase di submission REM, la richiesta di indicare nella *SubmissionAcceptance* se un dominio è REM o no, oltre a introdurre una maggiore complessità e un maggiore onere operativo, non potrà garantire una consistenza tra l'informazione determinata in questa fase e la corrispondente informazione determinata in quelle successive. Sono fasi distinte, separate da almeno un evento di *store&forward*, e generano, nel caso in cui siano consistenti, una duplicazione dell'informazione.

Una email REM può essere indirizzata ad uno o più domini. Per determinare se un dominio destinatario appartiene o meno al circuito REM, occorre effettuare una query al DNS per ognuno dei domini a cui l'email è indirizzata. La query può fallire anche con condizioni di errore temporaneo (timeout della query al name server), in questo caso il sistema non è in grado di determinare la tipologia (REM o non REM) per il dominio oggetto del timeout.

La mancata risoluzione della query, anche per un solo dominio tra quelli destinatari della email, può produrre un caso di inconsistenza tra quanto determinato in fase di submission e quanto potrà essere determinato nelle successive fasi a cui l'email sarà soggetta.

Per il dominio per cui la query al DNS è fallita con un errore temporaneo, non si può definire l'elemento *UntrustedPathToRecipient*. L'assenza dell'elemento *UntrustedPathToRecipient* può determinare le seguenti incongruenze:

1) Il mittente riterrebbe il dominio di tipo REM, mentre potrebbe essere riconosciuto come non REM dalla successiva fase di relay.
2) Nel caso, più raro ma che comunque non si può escludere, potrebbe avvenire che un dominio segnalato come non REM tramite l'elemento *UntrustedPathToRecipient* risulti, nella successiva fase di relay dominio di tipo REM.

Quindi, l'informazione "dominio appartenente o non appartenente al circuito REM", generata nella fase di submission potrebbe essere inattendibile.

Anche nel caso in cui si volesse tentare di risolvere questa criticità, con la ripetizione di un certo numero di tentativi di query, verrebbe comunque introdotto un ritardo nella generazione della *SubmissionAcceptance* con il rischio che risultato finale potrebbe comunque essere indeterminato. E' utile ricordare che la gestione dello spazio dei nomi di un dominio nel DNS può essere delegata a entità diverse dai provider REM, non sempre controllabili da un punto di vista di qualità e policy di gestione del name server, e che quello stesso dominio potrebbe non appartenere al circuito REM.

In merito alla dichiarazione della sua tipologia, un dominio può trovarsi in tre diversi stati nella fase di *submission*:

a) È REM: la query al DNS ha avuto successo e l'hostname risultante dal MX record è presente nella Trusted List.
b) Non è REM: la query al DNS ha avuto successo e l'hostname risultante dal MX record non è presente nella Trusted List.
c) Indeterminato: la query al DNS non ha avuto successo (timeout / errore temporaneo).

Per quanto definito nel draft ETSI EN 319 532-4 V1.1.7, non è presente la possibilità di indicare se un dominio è nello stato indeterminato, quindi l'unica opzione possibile sembrerebbe non inserire nell'XML della *SubmissionAcceptance* l'elemento *UntrustedPathToRecipient*, che però equivarrebbe a **dichiarare il dominio di tipo REM.**

La criticità del tentativo di dichiarare in fase di submission il tipo di dominio, può essere ulteriormente analizzata con il seguente esempio:

> Il provider mittente, nella fase di REM submission, riceve una email dal mittente. Deve effettuare delle query al DNS per determinare la tipologia dei domini a cui l'email è indirizzata. La query al DNS per uno o più di questi domini, fallisce (errore temporaneo), perciò il submission REM server non inserisce nella

SubmissionAcceptance l'elemento *UntrustedPathToRecipient*, azione che equivale a dichiarare REM il dominio di destinazione.
Nel caso che una successiva query al DNS del relay server abbia successo, questo potrebbe determinare che il dominio non è REM, perciò verrebbe generata una *RelayToNonERDS,* se la funzione di invio a destinatari non ERDS è abilitata, in evidente contrasto con quanto dichiarato nella *SubmissionAcceptance*.
Se anche la successiva query al DNS non ha successo (errore temporaneo), il sistema di trasporto email provvede alla gestione dell'errore temporaneo, inoltrando l'email ai destinatari per i quali la query al DNS ha avuto successso e attivando una serie di retry per gli altri.

Solo attraverso le ricevute di *relay* o di *contentconsignment* il mittente potrà avere una dichiarazione certa della tipologia dei diversi indirizzi di destinazione. Per contro il valore dell'nformazione, comunque incerta, che si ottiene nella fase di submission, non giustifica l'onere tecnico e operativo necesssario alla sua determinazione.

Nel caso di una email, indirizzata a più destinatari, consegnata alla fase di submission REM, il problema indotto dall'indeterminazione del tipo di dominio per almeno uno dei destinatari, potrebbe essere risolto introducendo la possibilità di segnalare nella *SubmissionAcceptance* la tipologia di dominio UNKNOWN.
Il provider S-REM, ha, opzionalmente, la possibilità di ritardare, per un periodo di tempo comunque non eccessivo, la generazione della *SubmissionAcceptance*, durante il quale potrebbe effettuare più retry nel tentativo di risolvere l'indeterminazione.
L'introduzione della tipologia di dominio UNKNOWN non introduce un rilevante vantaggio, poiché, in caso di dominio UNKNOWN, il mittente dovrebbe comunque attendere le successive fasi per avere la definitiva indicazione sulla tipologia del dominio (REM o non REM).

Per una visione completa dello scenario è utile, infine, considerare che il disalllineamento tra le informazioni relative a un dominio può comunque avvenire anche nella fase di relay tra diversi provider. Questi disallineamenti potrebbero verificarsi tra provider con diverse policy di gestione della Trusted List oppure essere causati da diversi tempi di aggiornamento delle cache nel DNS. Senza entrare nei dettagli di queste casistiche, si può osservare che tali criticità si concentrano nel punto di relay o, eventualmente, nelle fasi immediatamente successive, che sono transitorie (in genere si possono verificare in conseguenza a modifiche ai sistemi e al necessario tempo di sincronizzazione) e che per mitigare le stesse si possono adottare opportune precauzioni.

Sempre con riferimento alla clausola C.3.2.1 del draft ETSI EN 319 532-4 V1.1.7 (2022 – 01), l'elemento *UntrustedPathToRecipient* viene utilizzato anche per indicare al mittente se un indirizzo non è registrato presso il provider di destinazione. Si può notare come questa richiesta sia consistente, in quanto l'email si trova in una delle due fasi (relay o contentconsignment) che sono in grado di determinare la corretta valorizzazione dell'elemento *UntrustedPathToRecipient.*

Confronto con la Posta Elettronica Certificata.

Nella PEC [3] la tipologia del dominio di destinazione (PEC o non PEC) è rilevabile in modo efficiente da un dato locale al provider S-REM, acquisito tramite il file LDIF – IGPEC. Questo permette di anticipare alla fase di submission, con un buon livello di affidabilità, la dichiarazione della tipologia di un dominio di destinazione dell'email di trasporto (PEC o non PEC).

Conclusioni.

Considerazioni ed esempi riportati nel presente documento possono essere utili per la comprensione di uno specifico caso d'uso, a tale scopo è importante avere una approfondita conoscenza degli standard relativi al sistema email Internet.

Il sistema email Internet, è un sistema *store&forward*, per il quale è possibile individuare diverse fasi a cui una email è sottoposta durante il transito. Ogni fase è caratterizzata da proprie informazioni e caratteristiche di funzionamento: per ogni email, ognuna di queste fasi dispone di informazioni in ingresso e dovrà compiere azioni per determinare le condizioni di uscita della email.

Da ciò deriva come sia inopportuno e vincolante, per quanto desiderabile, cercare di acquisire nella fase di submission informazioni che tipicamente riguardano le fasi successive a cui una email sarà sottoposta.

Sarebbe desiderabile sapere, già nella fase di submission, se un dominio a cui l'email è destinata esiste, se la mailbox sul server di destinazione esiste (per esempio, aprendo una sessione SMTP per verificare la validità di un indirizzo di destinazione, posto che il server remoto segnali la sua inesistenza già a livello di sessione SMTP), etc. Ad alcune di queste richieste sarebbe tecnicamente possibile dare una risposta anche nella fase di submission, ma farlo costituirebbe, oltre che un inutile onere aggiuntivo, una violazione della semantica del sistema email Internet, con possibili conseguenze negative.

In particolare, la scelta del sistema email Internet per realizzare un sistema di comunicazione certificata come la REM, pone le basi su alcune delle caratteristiche proprie del sistema, che permettono di svincolare quanto prima il mittente (sia esso rappresentato da una persona o da un sistema automatico) da tutte le problematiche che l'email potrà incontrare nel percorso verso la sua destinazione.

La fase di submission, con la conseguente generazione della *SubmissionAcceptance* dovrebbe, perciò, basarsi sulla migliore soluzione per lo svincolo immediato del mittente da ogni ulteriore responsabilità. Responsabilità che, a questo punto, passano in carico al sistema email Internet (ai Provider). La fase di submssion ha, perciò,il compito di effettuare tutte le opportune e necessarie verifiche sulle informazioni in ingresso (esempio: formato della email, presenza virus, etc..), per arrivare alla accettazione o meno della email che si concretizza con la generazione della *SubmissionAcceptance* o della *SubmissionRejection*, ma non dovrebbe condizionare la generazione di tali ricevute al reperimento di informazioni che possono indurre ritardi e che appartengono alle successive fasi di trattamento della email con l'ulteriore rischio di disallineamento tra le informazioni reperite in fase di submission e le corrispondenti reperite nelle fasi successive.

Bibliografia.

1. ETSI EN 319 532-4 V1.1.7 (2022-01), https://www.etsi.org/deliver/etsi_en/319500_319599/31953204/01.01.07_20/en_31953204v010107a.pdf
2. https://datatracker.ietf.org/doc/html/rfc5598
3. https://www.agid.gov.it/sites/default/files/repository_files/leggi_decreti_direttive/pec_regole_tecniche_dm_2-nov-2005.pdf