Agenzia per la Cybersicurezza Nazionale

Linee Guida

Configurazione del servizio di posta elettronica per l'autenticazione.

Aprile 2026

Controllo di versione

VERSIONE	DATA PUBBLICAZIONE	NOTE
1.0	Aprile 2026	Prima pubblicazione.

INDICE

1. Introduzione

1.1. Premessa

La posta elettronica rappresenta oggi uno dei servizi maggiormente critici nel contesto digitale in quanto è tra i principali canali utilizzati da organizzazioni e utenti per le comunicazioni e lo scambio di informazioni[1].

Il funzionamento del servizio di posta elettronica e in particolare la trasmissione dei messaggi, si basa sul protocollo **SMTP** che, tuttavia, non incorpora nativamente adeguati meccanismi di autenticazione del mittente e di protezione della riservatezza e dell'integrità dei messaggi. Queste vulnerabilità espongono al rischio di attacchi come lo **spoofing**, il **phishing**, la **manomissione** e l'**intercettazione** del messaggio durante il transito.

Per mitigare le debolezze del protocollo *SMTP* e ridurre pertanto il rischio dovuto agli attacchi sopra richiamati, sono stati sviluppati, nel corso del tempo, meccanismi di autenticazione del mittente e di protezione dell'integrità del messaggio quali **SPF** (*Sender Policy Framework*), **DKIM** (*DomainKeys Identified Mail*) e **DMARC** (*Domain-based Message Authentication, Reporting and Conformance*).

Le presenti linee guida illustrano questi meccanismi con l'obiettivo di rafforzare l'affidabilità del servizio di posta elettronica e incrementarne il livello complessivo di sicurezza, con particolare riferimento alle minacce descritte nel capitolo 4.

> Non sono oggetto delle presenti linee guida le contromisure e i protocolli necessari a proteggere la riservatezza dei messaggi di posta elettronica (quali ad esempio S/MIME e OpenPGP che riguardano la cifratura del messaggio).

1.2. Normative di riferimento

NORMATIVA	DESCRIZIONE
Perimetro di Sicurezza Nazionale Cibernetica (PSNC)	Decreto-legge 21 settembre 2019, n. 105. Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica.
Regolamento Cloud per la Pubblica Amministrazione	Decreto Direttoriale ACN n. 21007/24 del 27 giugno 2024.
Decreto legislativo 4 settembre 2024, n. 138.	Decreto legislativo 4 settembre 2024, n. 138. Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

[1] Dati Eurostat 2026, https://ec.europa.eu/eurostat/databrowser/view/tin00094/default/table?lang=en&category=t_isoc.t_isoc_i.t_isoc_iiu.

1.3. Documenti di riferimento

TITOLO E INDIRIZZO DI PUBBLICAZIONE
NIST Technical Note 1945. https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1945.pdf
NIST SP 800-177 R1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf
ACN. Framework di Autenticazione per la Posta Elettronica. https://www.acn.gov.it/portale/w/framework-di-autenticazione-per-la-posta-elettronica
RFC 5321 – Simple Mail Transfer Protocol https://datatracker.ietf.org/doc/html/rfc5321
RFC 5322 – Internet Message Format https://datatracker.ietf.org/doc/html/rfc5322
RFC 7208 – Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1 https://datatracker.ietf.org/doc/html/rfc7208
RFC 6376 – DomainKeys Identified Mail (DKIM) Signatures https://datatracker.ietf.org/doc/html/rfc6376
RFC 7489 – Domain-based Message Authentication, Reporting, and Conformance (DMARC) https://datatracker.ietf.org/doc/html/rfc7489

2. Contesto normativo

A tutela degli assetti digitali del Paese, ivi inclusi i servizi di posta elettronica e le infrastrutture che li ospitano, insiste un ampio corpus di misure di sicurezza discendenti dalla normativa vigente, oggetto di costante aggiornamento.

Il livello più elevato di protezione per i servizi più critici del Paese, connessi alla tutela della sicurezza nazionale, è assicurato dal Perimetro di sicurezza nazionale cibernetica, istituito con decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133. Questo prevede misure di sicurezza con livelli di tutela particolarmente elevati, declinate nell'allegato B del decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, che si applicano alle reti, ai sistemi informativi e ai servizi informatici dei soggetti pubblici e privati da cui dipende l'esercizio di una funzione essenziale dello Stato o la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato dalla cui compromissione possa derivare un pregiudizio per la sicurezza nazionale.

Inoltre, i servizi di posta elettronica, come tutti i servizi digitali della pubblica amministrazione, sono soggetti alle previsioni del cd. Regolamento Cloud, adottato ai sensi dell'articolo 33-septies del decreto-legge 18 ottobre 2012, n. 179 e aggiornato dall'Agenzia per la cybersicurezza nazionale (ACN) con Decreto Direttoriale n. 21007 del 27 giugno 2024. Ai sensi del citato Regolamento, tutte le pubbliche amministrazioni sono chiamate a classificare i propri dati e servizi digitali quali ordinari, critici o strategici, secondo il modello predisposto da ACN. Tale attività è finalizzata ad assicurare che i dati e i servizi digitali della pubblica amministrazione siano trattati ed erogati attraverso infrastrutture digitali e servizi cloud che rispettano requisiti, ivi inclusi quelli di sicurezza, adeguati ai rischi connessi al relativo livello di classificazione, così come declinati dal Regolamento.

Il decreto legislativo del 4 settembre 2024, n. 138 (cd. decreto NIS) di recepimento della direttiva (UE) 2022/2555 ha altresì stabilito – tramite gli allegati 1 e 2 alla determinazione ACN 379907/2025 – le misure di sicurezza di base che i soggetti essenziali e importanti adottano ai fini degli obblighi di cui agli articoli 23 e 24 del decreto NIS, definendo una cornice di sicurezza al fine di rafforzare la protezione dei sistemi informativi e di rete ivi inclusi i servizi di posta elettronica.

3. Architettura del servizio di posta elettronica

Come osservato in premessa, il funzionamento del servizio di posta elettronica si basa sul protocollo *SMTP* che regola la trasmissione dei messaggi email dal *mittente* al *destinatario*.

Il protocollo SMTP è stato originariamente definito nel 1982[2] come protocollo *store-and-forward*, in cui il mittente genera un messaggio attraverso il proprio *client* di posta, in gergo *Mail User Agent* (MUA), che lo invia al *server* di posta del mittente. Questo, tramite una componente denominata *Mail Transfer Agent* (MTA) inoltra il messaggio, eventualmente anche attraverso uno o più MTA intermedi, consegnandolo all'MTA del server di posta del destinatario. L'utente destinatario accede al messaggio attraverso il proprio *client* di posta (MUA) [1].

L'MTA è quindi un componente del servizio di posta elettronica che si occupa della trasmissione dei messaggi email dal mittente al destinatario. I componenti MTA sono presenti sui server di posta del mittente e del destinatario e inoltre possono essere configurati degli MTA intermedi, ad esempio per gestire le liste di distribuzione.

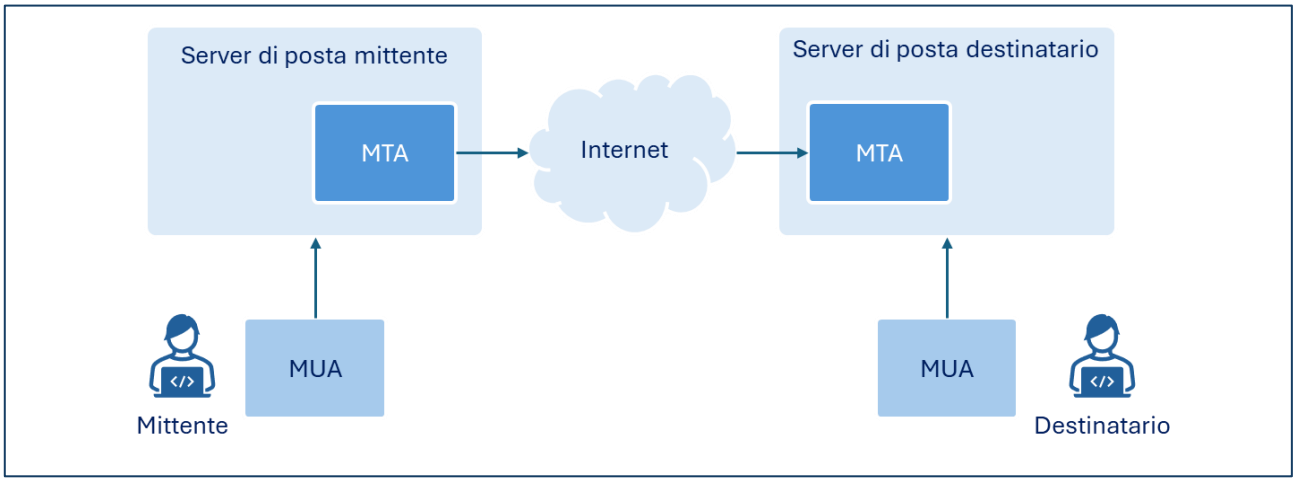

Figura 1. Architettura di alto livello del servizio di posta elettronica. Nella figura sono rappresentati solo i componenti di interesse per le presenti linee guida.

Sebbene il termine MTA individui una componente specifica dei server di posta elettronica[3], poiché ai fini del presente documento si fa riferimento a questi ultimi principalmente nella loro funzione di MTA, laddove non sussista ambiguità, per semplicità di esposizione si userà sovente il termine server di posta elettronica in luogo del più specifico MTA.

Nella presente linea guida ci si concentra sulla configurazione dei protocolli SPF, DKIM e DMARC per consentire ai server di posta di verificare l'**autenticità** e l'**integrità** dei messaggi di posta elettronica.

---

[2] RFC 821 successivamente aggiornata dal RFC 5321 del 2008.

[3] In generale, infatti, i server di posta elettronica includono ulteriori moduli che assolvono a compiti diversi da quelli dell'MTA, come, ad esempio, quelli per l'archiviazione locale dei messaggi e per l'accesso dei client alle proprie caselle di posta elettronica.

4. Minacce

Il protocollo SMTP introdotto nel precedente capitolo era stato inizialmente progettato per funzionare in una rete accademica di dimensioni relativamente ridotte e non teneva in considerazione aspetti relativi alla sicurezza dei messaggi trasmessi o all'autenticazione del mittente [1].

La diffusione sempre maggiore della posta elettronica e le debolezze intrinseche del protocollo SMTP hanno favorito, nel tempo, l'emergere di attacchi le cui principali tipologie sono sinteticamente illustrate nei successivi paragrafi.

4.1. Spoofing del mittente

Lo *spoofing* è una tecnica di attacco informatico utilizzata per falsificare l'indirizzo del mittente di un messaggio e far così apparire quest'ultimo come proveniente da un indirizzo affidabile (come, ad esempio, quello di un collega, di un conoscente, o del proprio istituto bancario), inducendo il destinatario a compiere azioni potenzialmente pericolose, come, ad esempio, aprire un allegato dell'email o cliccare su collegamenti contenuti nel messaggio.

Questo tipo di attacco è relativamente semplice da realizzare, in quanto il protocollo SMTP non include meccanismi di autenticazione del mittente e, pertanto, attraverso il *client di posta elettronica* è possibile configurare *qualunque* indirizzo mittente quando si origina il messaggio.

Indirizzo email mittente: envelop-from e message-from

Il formato dei messaggi di posta elettronica prevede due campi distinti per indicare l'indirizzo email del mittente. Questi campi sono denominati **envelope-from** e **message-from**: il primo (anche indicato come *return-path* in quanto specifica l'indirizzo email a cui devono essere inviati gli eventuali messaggi di errore generati quando un'email non raggiunge il destinatario) è l'indirizzo utilizzato per instradare correttamente il messaggio, il secondo è l'indirizzo visualizzato dal destinatario nell'intestazione del messaggio ricevuto.

Facendo un'analogia con l'invio di una lettera all'interno di una busta per mezzo della posta tradizionale, l'*envelop-from* rappresenta l'indirizzo del mittente riportato sulla busta della lettera, mentre il *message-from* corrisponde all'intestazione presente nella lettera che indica chi ha scritto al destinatario della lettera.

È importante osservare che i due indirizzi potrebbero non coincidere. Questa distinzione permette di gestire situazioni come, ad esempio, l'inoltro di messaggi da parte di servizi di terze parti, la distribuzione tramite *mailing list* o le risposte tramite email automatiche.

È infatti possibile indicare qualsiasi mittente sia a livello di *message-from* (indirizzo email del mittente visualizzato dal destinatario nell'intestazione del messaggio ricevuto) che di *envelope-from* (indirizzo email del mittente usato per la trasmissione del messaggio).

Per contrastare tali minacce è quindi essenziale prevedere meccanismi che permettano di autenticare in modo affidabile il mittente e di verificare che chi ha inviato il messaggio sia effettivamente autorizzato a farlo.

4.2. Phishing

Il *phishing* è una tecnica di attacco informatico finalizzata all'acquisizione fraudolenta di informazioni (come, ad esempio, credenziali di accesso, numeri di carte di credito o altri dati sensibili), generalmente mediante l'invio di messaggi ingannevoli che simulano l'origine da mittenti affidabili[4].

Lo *spoofing*, esaminato nel paragrafo precedente, è tra le principali tecniche adottate da un attaccante per contraffare l'identità del mittente e far apparire il messaggio come proveniente da un utente o da un dominio legittimo.

In alternativa, può essere utilizzato un indirizzo/dominio mittente simile a uno riconoscibile dal destinatario, alterando, ad esempio, il cosiddetto *display name*[5] al fine di rafforzare l'apparente autenticità del messaggio.

Per inviare messaggi di phishing, possono essere inoltre utilizzati account legittimi precedentemente compromessi dall'attaccante.

Un messaggio di *phishing* ha tipicamente un contenuto costruito per generare urgenza, allarme o interesse economico nei confronti del destinatario, creando situazioni che lo inducano a reagire impulsivamente ed effettuare specifiche azioni come aprire allegati malevoli o cliccare su collegamenti che rimandano a siti web apparentemente legittimi, ma che in realtà sono stati creati dall'attaccante con l'obiettivo di sottrare informazioni e/o installare malware.

Solitamente, gli attacchi di *phishing* sono condotti trasmettendo uno stesso messaggio email ad un gran numero di vittime, senza adattarne il testo al profilo specifico delle vittime.

Una variante del *phishing* è il cosiddetto **spear phishing**, in cui l'attaccante conosce e prende di mira specificamente il profilo della vittima.

A differenza di un'email di phishing generica, un messaggio di *spear phishing* utilizza informazioni contestuali più precise per convincere l'utente che sta interagendo con un mittente affidabile [2] .

4.3. Manomissione del messaggio

Il contenuto di un messaggio di posta elettronica, come qualsiasi altra comunicazione che viaggia sulla rete Internet e che non fa uso di tecniche di crittografia *end-to-end* (E2EE) può essere intercettato e modificato durante il transito tra mittente e destinatario (un tipo di minaccia comunemente denominata *man-in-the-middle*).

Di conseguenza, oltre alla perdita di riservatezza, il messaggio ricevuto potrebbe non corrispondere a quello originariamente composto dal mittente.

---

[4] Tra i mittenti simulati rientrano sovente figure con ruolo di autorità come dirigenti o amministratori della rete informatica.

[5] Il *display name* è il campo testuale associato all'indirizzo email del mittente mostrato al destinatario dal client di posta elettronica nell'intestazione del messaggio. È distinto dall'indirizzo email e serve per identificare in modo leggibile e riconoscibile il mittente.

Un attaccante potrebbe, ad esempio, manipolare il contenuto del messaggio per farlo apparire proveniente da un mittente affidabile, modificare il testo o eventuali collegamenti e/o allegati presenti nel messaggio o inserire codice malevolo.

Il destinatario, confidando nell'apparente autenticità del messaggio, può così essere indotto a compiere azioni potenzialmente dannose, come comunicare credenziali di accesso, autorizzare pagamenti o aprire file malevoli.

Per contrastare tali minacce è quindi fondamentale adottare meccanismi che garantiscano l'integrità e l'autenticità del messaggio, assicurando che il contenuto ricevuto non sia stato modificato e che il mittente sia realmente chi dichiara di essere.

5. Azioni di contrasto

Nel capitolo 2 sono state richiamate le normative che prevedono misure di sicurezza anche a tutela dei servizi di posta elettronica. Con il presente documento si intende anzitutto fornire una guida all'implementazione delle misure di sicurezza, previste da tali normative e riportate in Appendice A, che rilevano anche ai fini della *configurazione dei servizi di posta elettronica*, al fine di mitigare i rischi connessi alle minacce discusse nel capitolo 4. Si osserva nondimeno che le indicazioni contenute nelle presenti linee guida sono raccomandate anche a quei soggetti che non soggiacciono alle predette normative.

Le misure di sicurezza in parola non fanno esplicitamente riferimento alla configurazione del servizio di posta elettronica ma – a seconda della normativa considerata – alla configurazione di *sistemi IT e di controllo industriale* (PSNC e Regolamento Cloud) o di *sistemi informativi e di rete* (NIS2). I servizi di posta elettronica, oggetto delle presenti linee guida, rientrano in entrambe le tipologie di sistemi.

In particolare, sono di seguito illustrati i protocolli **SPF**, **DKIM**, **DMARC** che prevedono meccanismi di sicurezza progettati con l'obiettivo di rafforzare la sicurezza complessiva del servizio di posta elettronica e in particolare dell'autenticazione del mittente e del controllo dell'integrità del messaggio.

5.1. SPF

SPF – Sender Policy Framework è un protocollo di autenticazione, formalizzato dall'*RFC 7208*, che permette al proprietario di un dominio di specificare quali indirizzi IP sono autorizzati a inviare messaggi di posta elettronica per suo conto e di stabilire le politiche che il destinatario deve applicare se l'indirizzo IP associato al *dominio*[6] dell'indirizzo email del mittente non è tra quelli esplicitamente autorizzati.

Gli indirizzi IP autorizzati sono elencati in un record TXT del DNS relativo al dominio mittente denominato *record SPF* e illustrato nella successiva sezione del presente paragrafo.

In questo modo, il server di posta elettronica[7] del destinatario quando riceve un messaggio da un determinato dominio può interrogare il relativo *record SPF* e autenticarne la provenienza verificando che l'indirizzo IP dal quale è stato ricevuto il messaggio rientra tra quelli autorizzati a inviare messaggi per conto del dominio.

È importante osservare che il dominio che viene verificato a livello di SPF è quello relativo all'*envelope-from*, di conseguenza l'adozione del solo protocollo SPF non è sufficiente a contrastare lo spoofing in quanto questo tipo di attacco potrebbe essere effettuato a livello di *message-from*[8].

---

[6] Un indirizzo email ha una struttura del tipo *local-part@domain-part* dove **local-part** identifica lo specifico utente all'interno del sistema di posta elettronica o del server associato alla **domain-part**, che corrisponde, invece, al nome di dominio del sistema o del servizio che ospita l'account dell'utente identificato dalla *local-part* [2].

[7] Ove non si crei ambiguità, per scorrevolezza del testo, si userà "server di posta elettronica" in luogo di MTA, che è la componente del server di posta elettronica che si occupa del trasferimento dei messaggi da mittente a destinatario.

[8] Per la distinzione tra envelop-from e message-from, si faccia riferimento al riquadro di approfondimento *Indirizzo email mittente: envelop-from e message-from* al paragrafo 3.1.

Nel caso in cui un'organizzazione esternalizzi, in tutto o in parte, il proprio servizio di posta elettronica a una terza parte, come, ad esempio, un fornitore cloud, deve assicurarsi che i messaggi inviati da tali fornitori superino i controlli SPF. A tal fine, l'organizzazione dovrebbe includere nel proprio record SPF gli indirizzi IP dai quali i fornitori inviano email per conto del dominio dell'organizzazione.

Nel caso di inoltro automatico delle email, poiché i messaggi vengono tipicamente reindirizzati da un server intermedio, l'indirizzo IP che effettua la consegna finale non coincide più con quello originariamente autorizzato dal dominio mittente. In questi casi, per non far fallire la verifica SPF è necessario autorizzare anche gli eventuali server intermedi di inoltro, oppure ricorrere a meccanismi quali SRS (*Sender Rewriting Scheme*) o ARC (*Authenticated Received Chain*) che possono risultare più efficaci, specie in presenza di numerosi server intermedi di inoltro.

Va evidenziato che affinché SPF sia effettivamente efficace, è necessario che sia correttamente configurato non solo dal mittente, ma anche dal destinatario. In particolare:

- il **mittente** deve pubblicare il record SPF nel relativo server DNS dichiarando gli indirizzi che sono autorizzati a inviare email per suo conto;
- il **destinatario** deve configurare il proprio server di posta affinché esegua la verifica SPF sui messaggi ricevuti e applicare coerentemente le politiche risultanti.

5.1.1. Record SPF

Un Record SPF è un record DNS di tipo TXT il cui nome corrisponde al dominio mittente e il cui contenuto è costituito[9] dalla sezione che indica la versione[10] e da una serie di *direttive* che indicano il comportamento del server di posta del destinatario quando vi è una corrispondenza tra l'indirizzo IP del dominio mittente e una direttiva.

Le direttive sono formate da un *meccanismo* preceduto da un *qualificatore*. I principali meccanismi utilizzati nei record SPF sono [2]:

- **ip4**, elenca gli indirizzi IPv4 autorizzati;
- **ip6**, elenca gli indirizzi IPv6 autorizzati;
- **a**, autorizza gli indirizzi IP presenti nel record A del dominio;
- **mx**, autorizza gli indirizzi IP relativi ai record MX del dominio;
- **include**, autorizza gli IP presenti nel record SPF di un altro dominio;
- **all**, rappresenta tutti gli indirizzi IP che non sono stati autorizzati esplicitamente attraverso gli altri meccanismi.

In particolare, il meccanismo *all* permette di stabilire le politiche per i messaggi che provengono da indirizzi IP che non sono stati dichiarati dai precedenti meccanismi.

[9] Possono inoltre essere presenti anche i cosiddetti *modificatori* che specificano informazioni aggiuntive, eccezioni alle regole e variazioni rispetto ai valori predefiniti.

[10] Al momento è presente una sola versione del protocollo (v=spf1).

Inoltre, SPF prevede i seguenti qualificatori da associare ai meccanismi:

- **+**, (*pass*) indica che gli indirizzi IP che corrispondono al meccanismo associato sono autorizzati. È il qualificatore predefinito se non ne viene specificato un altro;
- **-**, (*fail*) indica che gli indirizzi IP che corrispondono al meccanismo associato non sono autorizzati;
- **~**, (*softfail*) indica che gli indirizzi IP che corrispondono al meccanismo associato *probabilmente* non sono autorizzati. Si tratta di una dichiarazione più incerta della precedente. In questi casi il messaggio dovrebbe essere accettato ma contrassegnato per un'analisi più approfondita, si usa ad esempio nei casi di debugging o quando si prevede che la verifica SPF potrebbe non andare a buon fine;
- **?**, (*neutral*) indica che per gli indirizzi IP che corrispondono al meccanismo associato non viene data alcuna indicazione. Il comportamento predefinito è quello di accettare il messaggio.

È bene evidenziare che nella pratica, il record SPF è composto in modo da specificare gli indirizzi IP autorizzati, facendo poi ricorso alla direttiva "-all" per specificare che tutti gli altri indirizzi non sono autorizzati (al riguardo si faccia riferimento agli esempi sotto riportati). Questa rappresenta la configurazione raccomandata in quanto permette di indicare esplicitamente gli indirizzi IP autorizzati ed escludere tutti gli altri.

In ogni caso si raccomanda di non usare mai la direttiva "+all" (o l'equivalente "all") in quanto corrisponderebbe all'autorizzazione di tutti gli indirizzi IP.

Esempi di record SPF

Autorizzare uno specifico indirizzo IP

```
v=spf1 ip4:203.0.113.0 -all
```

Il record SPF sopra riportato utilizza la versione 1 di SPF e autorizza attraverso il meccanismo "ip4" l'indirizzo IP 203.0.113.0 (infatti, non essendo specificato alcun qualificatore per il meccanismo ip4, viene implicitamente utilizzato quello predefinito "+"). La direttiva "-all" formata dal meccanismo "all" e dal qualificatore "-" (*fail*) specifica che tutti gli altri indirizzi non sono autorizzati.

Autorizzare uno specifico spazio di indirizzamento IP

```
v=spf1 ip4:203.0.113.0/24 -all
```

Il record SPF sopra riportato è analogo al precedente, ma autorizza tutti gli indirizzi IP dello spazio di indirizzamento 203.0.113.0/24.

Autorizzare più indirizzi IP

```
v=spf1 ip4:203.0.113.22 ip4:203.0.113.44 -all
```

Il record SPF sopra riportato autorizza esclusivamente gli indirizzi IPv4 203.0.113.22 e 203.0.113.44.

Autorizzare gli indirizzi dei record MX e di un dominio specifico

```
v=spf1 mx include:spf.emailprovider.it -all
```

Il record SPF sopra riportato autorizza esclusivamente gli indirizzi IP dei record MX dello stesso dominio del record SPF e quelli autorizzati del dominio *spf.emailprovider.it* (ad esempio, il dominio di un fornitore del servizio di posta elettronica).

5.1.2. Processo di autenticazione

Se correttamente configurato per eseguire la verifica SPF, il server di posta del destinatario alla ricezione di un nuovo messaggio email recupera il record SPF del dominio mittente interrogando il server DNS che contiene i record di tale dominio così come risulta dall'indirizzo riportato nel campo envelope-from. Ad esempio, se l'indirizzo riportato nel campo envelope-from è alice@example.com, il server di posta del destinatario recupera il record SPF del dominio example.com.

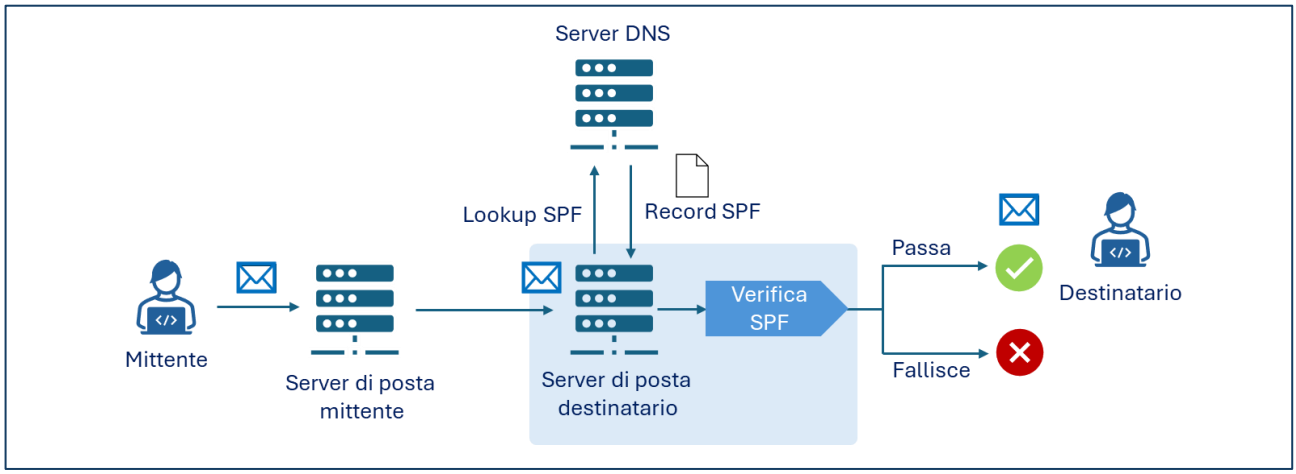

Figura 2. Meccanismo di funzionamento della verifica SPF.

Il server di posta del destinatario effettua quindi la verifica SPF, analizzando il record SPF per determinare se l'indirizzo IP dal quale ha ricevuto il messaggio è autorizzato a inviare email per il dominio example.com. Nel caso in cui il messaggio email passi la verifica SPF viene consegnato al destinatario.

Ad esempio, se il record SPF del dominio example.com fosse "v=spf1 ip4:203.0.113.22 -all" la verifica passerebbe solo se l'indirizzo IP del server mittente fosse 203.0.113.22, mentre fallirebbe per qualsiasi altro indirizzo.

5.2. DKIM

DKIM – DomainKeys Identified Mail è un protocollo di autenticazione, formalizzato dall'*RFC 6373*, che permette al proprietario di un dominio di garantire l'autenticità dei messaggi di posta elettronica inviati apponendogli una firma digitale (*firma DKIM*) generata dal server di posta tramite algoritmi di crittografia pubblica e inserita nelle intestazioni del messaggio da trasmettere.

Per permettere al destinatario di verificare che il messaggio non sia stato modificato durante la trasmissione, la chiave pubblica associata alla firma DKIM è conservata in un record TXT del DNS pubblico del dominio mittente, denominato *record DKIM*, che viene interrogato dal server di posta destinatario alla ricezione del messaggio.

La firma e il record DKIM sono illustrati nelle successive sezioni del presente paragrafo.

Come per SPF, anche DKIM deve essere correttamente configurato dal mittente e dal destinatario e in particolare:

- il mittente deve configurare il proprio server di posta per generare le firme DKIM e pubblicare il record DKIM nel relativo server DNS;
- il destinatario deve configurare il proprio server di posta affinché esegua la verifica DKIM sui messaggi ricevuti.

5.2.1. Firma DKIM

La firma DKIM è generata a partire da elementi designati del corpo e delle intestazioni del messaggio ed è costituita da una serie di coppie chiave-valore che specificano elementi tra i quali:

- **v**: versione del protocollo[11];
- **a**: algoritmo di cifratura usato[12];
- **d**: dominio firmatario che dichiara l'autenticità del messaggio[13];
- **s**: selettore che indica quale chiave pubblica DKIM cercare nel record DNS[14];
- **h**: elenco degli header dell'email inclusi nella firma[15];
- **bh**: hash del corpo del messaggio codificato in formato base64[16];
- **b**: firma digitale vera e propria generata con la chiave privata e codificata in formato base64[17];
- **x**: data di validità della firma;
- **c**: tipologia di canonicalizzazione.

La canonicalizzazione è il processo di normalizzazione degli elementi del messaggio prima di essere firmati digitalmente al fine di ridurre l'impatto di piccole modifiche che possono avvenire durante il transito, come spazi ripetuti o interruzioni di riga. Esistono due tipologie di canonicalizzazione: semplice, che richiede una corrispondenza esatta tra il messaggio originale e quello ricevuto, e relaxed, che applica normalizzazioni come la rimozione di spazi, la conversione di lettere maiuscole in minuscole nelle intestazioni e la riduzione di righe vuote consecutive nel corpo del messaggio.

---

[11] Al momento è presente una sola versione del protocollo (v=1).

[12] L'algoritmo di *default* è rsa-sha256.

[13] Il dominio firmatario è quello che garantisce l'autenticità del messaggio tramite la firma digitale e al quale i destinatari fanno riferimento per recuperare la chiave pubblica DKIM dal DNS e verificare la firma. Non deve necessariamente coincidere con il dominio del campo *message-from* e/o del campo *envelope-from* ma le politiche DMARC potrebbero richiederne l'allineamento ad essi (si faccia riferimento a riguardo al paragrafo DMARC).

[14] Il *selettore* permette di identificare univocamente la coppia di chiavi crittografiche usata per creare la firma. Per un determinato dominio possono essere infatti generate più coppie di chiavi al fine di consentire che MTA di un medesimo dominio possano usare chiavi differenti o per permettere un'efficace rotazione periodica delle chiavi.

[15] In particolare, sono firmati specifici *header* del messaggio (come ad esempio i campi *From*, *To*, *Oggetto*, *Data*) che non sono modificati durante la trasmissione del messaggio.

[16] L'hash del messaggio viene generalmente calcolato sull'intero corpo del messaggio. Per gestire eventuali scenari in cui il messaggio è modificato durante il transito aggiungendo ad esempio elementi come *footer* o *disclaimer* (si pensi al riguardo a servizi di mailing list o di inoltro automatico) è possibile considerare, ai fini della firma, solo una parte del messaggio. Tuttavia, tale pratica introduce dei rischi in quanto non garantisce la piena integrità del messaggio ricevuto.

[17] La firma digitale viene ottenuta a partire dagli header elencati *h* e dall'hash del corpo del messaggio in *bh*.

5.2.2. Record DKIM

Il *record DKIM* è conservato in un record DNS di tipo TXT il cui nome ha la struttura **<selettore>._domainkey.<dominio_firmatario>**, dove *_domainkey* è un'etichetta usata per indicare che il record DNS è appunto un record DKIM. Il contenuto del record DKIM è costituito da una serie di coppie chiave-valore che specificano elementi tra i quali:

- **v**: versione del protocollo;
- **k**: tipo di chiave, che per impostazione predefinita è RSA;
- **p**: chiave pubblica codificata in formato base64.

Esempio di record DKIM

Nome: s1._domainkey.example.com

Valore: `v=DKIM1; k=rsa; p=Y2hpYXZlcHViYmxpY2FkaWVzZW1waW8h...`

Il record DKIM in esempio è associato al selettore s1 del dominio example.com, utilizza la versione 1 e contiene la chiave pubblica RSA codificata in formato base64 (Y2hpYXZlcHViYmxpY2FkaWVzZW1waW8h...).

5.2.3. Processo di autenticazione

Se il protocollo DKIM è configurato correttamente sia presso il server di posta del mittente che quello del destinatario, il funzionamento del processo di autenticazione e verifica DKIM prevede che il server di posta mittente crei la firma DKIM del messaggio come descritto nel paragrafo 5.2.1, che viene aggiunta al messaggio stesso. In particolare, la firma DKIM contiene nel campo "d" il domino firmatario[18] e nel campo "b" la firma digitale del messaggio generata con la chiave privata del dominio firmatario.

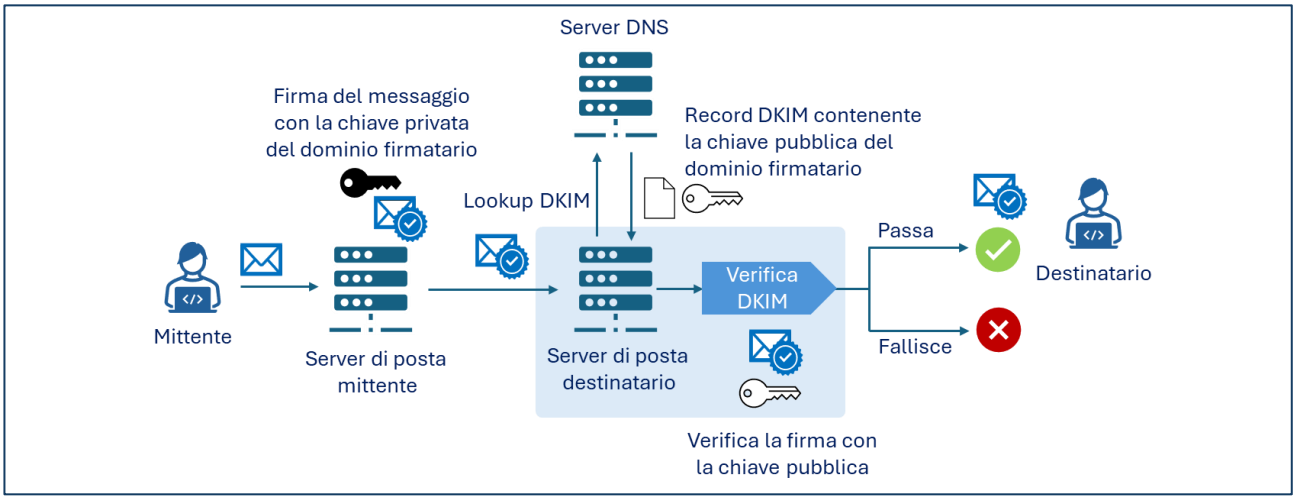

Figura 3. Meccanismo di funzionamento della verifica DKIM.

[18] Come già osservato nel paragrafo 5.2.1, in generale il dominio firmatario può non coincidere con il dominio del campo *message-from* e/o del campo *envelope-from*, ma le politiche DMARC potrebbero richiederne l'allineamento (come sarà descritto nel paragrafo DMARC).

Alla ricezione di un messaggio il server di posta destinatario recupera il record DKIM del dominio firmatario (campo "d" della firma DKIM) dal server DNS che contiene i record di tale dominio. Quindi usa la chiave pubblica contenuta nel record DKIM per verificare la firma digitale (campo "b") contenuta nella firma DKIM. Se la verifica ha successo il messaggio viene consegnato al destinatario.

5.2.4. Aspetti crittografici

Sul piano crittografico, DKIM ha storicamente utilizzato l'algoritmo **RSA**, in particolare nella variante **rsa-sha256**, considerata lo standard dal 2007. La nuova alternativa, introdotta dalla **RFC 8463**, è **Ed25519-SHA256**, una forma moderna di firma digitale basata su curve ellittiche che garantisce maggiore efficienza e chiavi molto più compatte.

Sul piano tecnico RSA, con lunghezza delle chiavi di 2048 bit, rimane lo standard universale, ma le chiavi sono lunghe e le firme relativamente grandi, mentre Ed25519 offre chiavi nove volte più corte e firme quattro volte più piccole, con prestazioni di firma fino a trenta volte superiori rispetto a RSA 2048. Nonostante questi vantaggi, il supporto reale è limitato: nel 2026 Ed25519 è verificato solo da pochi provider, mentre alcuni dei principali operatori non ne supportano né la firma né la verifica in modo affidabile, rendendolo inadatto come unica soluzione in produzione.

Per questo motivo, pur essendo tecnicamente superiore, al momento della scrittura di questo documento, l'uso di **Ed25519 non è consigliato se non in combinazione con RSA**, tramite *doppia firma*, in ottica di sperimentazione e come misura di compatibilità futura. Fino a quando i maggiori provider non ne implementeranno pienamente la verifica, RSA resta imprescindibile per garantire la massima garanzia di consegna dei messaggi.

Sul fronte della sicurezza a lungo termine, è importante ricordare che **né RSA né Ed25519 sono resistenti agli attacchi dei futuri computer quantistici** [3], e la transizione verso algoritmi post-quantum richiederà nuovi standard DKIM che al momento non esistono, rendendo essenziale monitorare gli sviluppi della crittografia di nuova generazione e le future raccomandazioni di ACN in tale ambito.

Relativamente agli aspetti di gestione delle chiavi crittografiche, la chiave privata DKIM deve essere protetta con rigorose misure di sicurezza, mantenendola su sistemi isolati e accessibili solo a servizi autorizzati, adottando permessi restrittivi, rotazione periodica e monitoraggio costante per prevenire accessi non autorizzati o compromissioni.

5.3. DMARC

DMARC – Domain-based Message Authentication, Reporting and Conformance è un protocollo di autenticazione, formalizzato dall'*RFC 7489*, che integra[19] i meccanismi di SPF e DKIM permettendo al proprietario di un dominio di specificare, ai destinatari dei messaggi trasmessi da quel dominio, le **politiche** per la gestione di quei messaggi che falliscono le verifiche SPF e DKIM.

[19] Ai fini del funzionamento di DMARC, deve essere implementato almeno uno tra SPF e DKIM. In questa guida, come riportato nel capitolo 5, è raccomandata l'implementazione congiunta di tutti e tre i protocolli.

In particolare, DMARC introduce un meccanismo di autenticazione – denominato *allineamento* – che verifica la corrispondenza tra i domini autenticati da SPF e DKIM e il dominio relativo al campo *message-from* del messaggio ricevuto. Si noti che il controllo dell'allineamento tra il campo message-from e il dominio SPF/DKIM fallisce in ogni caso se fallisce la corrispondente verifica SPF/DKIM (si veda la Figura 4).

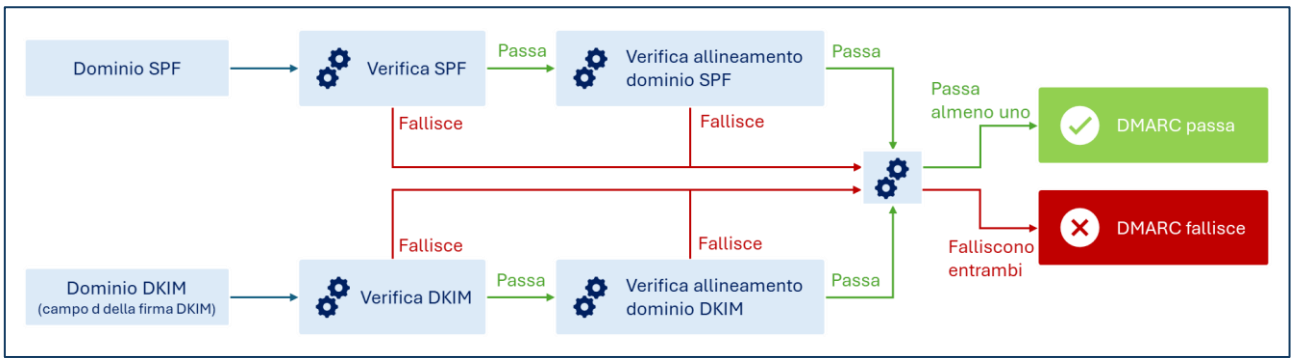

Figura 4. Meccanismo di verifica DMARC.

L'allineamento può essere verificato secondo la modalità *strict*, in cui è richiesta un'esatta corrispondenza tra i domini autenticati da SPF/DKIM e quello relativo al campo message-from, o *relaxed*, in cui è sufficiente che i domini primari coincidano, anche se i sottodomini possono essere diversi.

Ad esempio, nella modalità relaxed per i domini sub1.example.com e sub2.example.com verrebbe riscontrato un allineamento ai fini della verifica DMARC (poiché il dominio primario, example.com, è il medesimo). In modalità strict, invece, il controllo di allineamento DMARC fallirebbe per la mancanza di una corrispondenza esatta tra i domini.

Attraverso la verifica dell'allineamento, anche se un attaccante riuscisse a superare i controlli SPF e/o DKIM usando un *message-from* differente dall'*envelope-from* autenticato da SPF e/o dal dominio firmatario autenticato, DMARC rileverebbe comunque la discrepanza, garantendo una verifica coerente e affidabile dell'identità del mittente [2].

Le politiche per la gestione dei messaggi che non superano[20] la verifica DMARC sono specificate in un record TXT del relativo server DNS del dominio mittente denominato *record DMARC* e illustrato nella successiva sezione del presente paragrafo.

DMARC consente inoltre di indicare ai destinatari di inviare *report*, ai proprietari del dominio mittente, relativi ai messaggi che dichiarano di provenire da quel dominio. In questo modo, il titolare del dominio può verificare se il proprio dominio sia utilizzato in modo non autorizzato e in quale misura, analizzando, ad esempio, quanti messaggi siano effettivamente riconducibili a lui sul totale dei messaggi che ne rivendicano la provenienza.

Come per SPF e DKIM, anche DMARC deve essere correttamente configurato dal mittente e dal destinatario e in particolare:

- il mittente deve pubblicare il record DKIM nel proprio DNS specificando le politiche con le quali gestire i messaggi che falliscono la verifica DMARC;

[20] Ai fini del superamento della verifica DMARC è necessario che almeno uno dei due allineamenti (SPF o DKIM) sia valido.

- il destinatario deve configurare il proprio server di posta affinché esegua la verifica DMARC sui messaggi ricevuti.

5.3.1. Record DMARC

Il nome del *record DMARC* ha la struttura **_dmarc.<dominio_mittente>**, dove *_dmarc* è un'etichetta usata per indicare che il Record DNS è un record DMARC e <*dominio_mittente*> è il dominio al quale fa riferimento la politica.

Il record DMARC è costituito da una serie di coppie chiave-valore che specificano elementi tra i quali:

- **v**: versione del protocollo DMARC[21] ;
- **p**: politica da applicare ai messaggi che falliscono la verifica DMARC, può assumere uno tra i valori *none*, *quarantine*, *reject*;
- **aspf**: modalità di allineamento da applicare al controllo SPF (può essere *relaxed*, valore di default, o *strict*);
- **adkim**: modalità di allineamento da applicare al controllo DKIM (può essere *relaxed*, valore di default, o *strict*);
- **rua**: indirizzi email ai quali inviare i report aggregati con le informazioni statistiche e riassuntive sui messaggi ricevuti dal dominio mittente;
- **ruf**: indirizzi email ai quali inviare i report di dettaglio sui singoli messaggi ricevuti dal dominio mittente che hanno fallito la verifica DMARC.

Esempio di record DMARC

Nome: _dmarc.example.com

Valore: `v=DMARC1; p=reject; rua=mailto:dmarc-reports@example.com; ruf=mailto:dmarc-fail@example.com; adkim=s; aspf=s`

Il record DMARC in esempio è associato al dominio example.com, utilizza la versione 1 e specifica la politica "reject" per i messaggi che non passano la verifica DMARC, richiedendo la modalità "strict" per la verifica dell'allineamento dei domini SPF e DKIM e di trasmettere i report complessivi all'indirizzo email dmarc-reports@example.com e quelli di fallimento all'indirizzo dmarc-fail@example.com.

5.3.2. Politiche DMARC

Come descritto nel paragrafo precedente, il record DMARC indica la politica che il server di posta destinatario dovrebbe applicare per i messaggi che non passano la verifica DMARC. Le possibili politiche sono le seguenti:

- **none**: il dominio mittente non dà indicazioni in merito alla consegna dei messaggi che non passano la verifica DMARC;

[21] Al momento è presente una sola versione del protocollo (v=DMARC1).

- **quarantine:** il dominio mittente indica che i messaggi che non passano la verifica DMARC dovrebbero essere considerati sospetti (ad esempio, sottoposti a ulteriore scrutinio, trattati come spam o etichettati come sospetti);
- **reject**: il dominio mittente indica che i messaggi che non passano la verifica DMARC dovrebbero essere rifiutati.

5.3.3. Processo di verifica e applicazione delle politiche

Se il protocollo DMARC è configurato correttamente sia presso il server di posta del mittente che quello del destinatario, alla ricezione di un messaggio il server di posta destinatario recupera i record SPF e record DKIM per effettuare le relative verifiche, nonché quella DMARC (dettagliata nell'incipit del paragrafo 5.2.4). Nel caso in cui il messaggio non passi la verifica DMARC, viene applicata la politica indicata nel record DMARC (*none*, *quarantine* o *reject*).

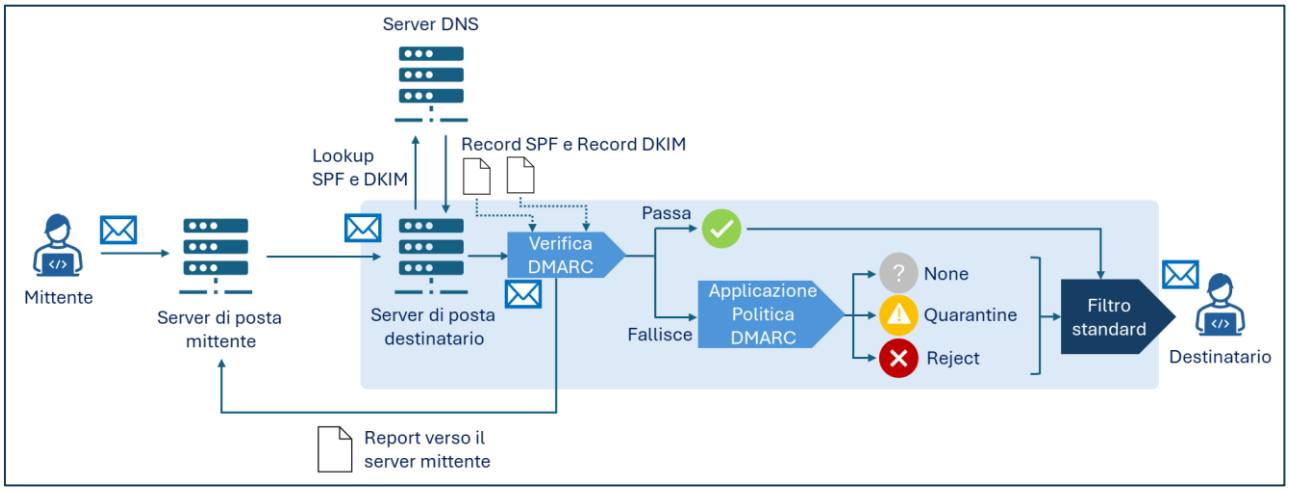

Figura 5. Processo di verifica e applicazione delle politiche DMARC.

Si noti che ciascun server di posta può adottare euristiche e politiche locali per determinare la consegna o meno di un messaggio, tenendo conto anche dell'esito delle verifiche SPF, DKIM e DMARC. Pertanto, generalmente, è presente un ulteriore processo decisionale ("*Filtro standard*" in Figura 5) a valle delle predette verifiche, che può includere anche ulteriori controlli (come, ad esempio, filtri anti-spam e anti-malware).

Inoltre, il server di posta destinatario può trasmettere:

- agli indirizzi indicati nel campo "rua" del record DMARC, report aggregati con le informazioni statistiche e riassuntive sui messaggi ricevuti dal dominio mittente;
- agli indirizzi indicati nel campo "ruf" del record DMARC, report di dettaglio sui singoli messaggi ricevuti dal dominio mittente che hanno fallito la verifica DMARC.

6. Conclusioni

Come discusso nel precedente capitolo, al fine di contrastare al meglio le minacce legate all'impersonificazione del dominio mittente è necessario che tutti e tre i protocolli esaminati siano implementati congiuntamente e, in particolare, che [3]:

- il dominio mittente pubblichi correttamente i record SPF, DKIM e DMARC nel DNS;
- il server di posta del mittente sia configurato per firmare i messaggi con DKIM;
- il server di posta del destinatario sia configurato per eseguire le verifiche SPF e DKIM e applicare le politiche DMARC.

Con riferimento all'implementazione dei protocolli, sono inoltre formulate le seguenti raccomandazioni [2]:

- configurare SPF specificando quali indirizzi IP sono autorizzati a inviare email per conto del dominio; per i domini che non sono utilizzati per la trasmissione di posta elettronica, ad esempio quelli destinati esclusivamente ai siti web, dovrebbe comunque essere creato un record SPF per indicare esplicitamente che non esistono mittenti email validi per quel dominio;
- usare protocolli e algoritmi di cifratura allo stato dell'arte e considerati sicuri per le chiavi DKIM, alla data di scrittura di questo documento si raccomanda RSA a 2048 bit;
- proteggere adeguatamente la chiave privata DKIM conservata sul server di posta, adottando permessi di accesso restrittivi, e assicurarsi che solo il software del server di posta abbia i privilegi in lettura della chiave;
- configurare ogni server di posta con una coppia di chiavi e un selettore univoci, in modo da ridurre l'impatto di un'eventuale compromissione di una chiave privata;
- proteggere la chiave privata sia da divulgazioni accidentali che da tentativi di accesso o modifica da parte di un attaccante;
- prevedere che il software relativo a eventuali *mailing list* verifichi le firme DKIM sui messaggi in arrivo e apponga nuove firme DKIM su quelli in uscita;
- utilizzare coppie di chiavi DKIM univoche per ogni terza parte che invia email per conto dell'organizzazione;
- ruotare periodicamente le coppie di chiavi DKIM (almeno ogni sei mesi) per mitigare l'impatto di un'eventuale compromissione;
- revocare immediatamente le chiavi in caso di sospetta compromissione;
- monitorare i report DMARC per identificare eventuali errori di configurazione o tentativi di abuso.

Per ulteriori approfondimenti si può far riferimento alle risorse elencate in Documenti di riferimento.

Si osserva che, per proteggere adeguatamente la sicurezza della posta elettronica, oltre ai protocolli di autenticazione qui esaminati, esistono ulteriori protocolli – non oggetto delle presenti linee guida – come, ad esempio, il *TLS – Transport Layer Security* che garantisce la cifratura del canale di trasmissione e *S/MIME* e *OpenPGP* che riguardano la cifratura end-to-end e l'autenticazione del messaggio.

Si rileva altresì che – pur non essendo un protocollo di sicurezza della posta elettronica in senso stretto – ai fini della sicurezza dei servizi di posta elettronica è raccomandato implementare DNSSEC (*Domain Name System*

Security Extensions), un'estensione del protocollo DNS che aggiunge firme crittografiche ai record DNS al fine di garantire l'integrità e l'autenticità delle query DNS. Grazie a DNSSEC, ad esempio, le informazioni relative ai record SPF, DKIM e DMARC sono protette durante la trasmissione, riducendo il rischio che siano alterate e aumentando pertanto la sicurezza del servizio di posta elettronica.

Appendice A: misure di sicurezza

Perimetro di Sicurezza Nazionale Cibernetica

PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità).

1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
   a) le politiche di sicurezza adottate per lo sviluppo di configurazioni di sistemi IT e di controllo industriale e il dispiegamento delle sole configurazioni adottate;
   b) l'elenco delle configurazioni dei sistemi IT e di controllo industriale impiegate e il riferimento alle relative pratiche di riferimento;
   c) i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

Regolamento Cloud – Infrastrutture Digitali e dei Servizi per la Pubblica Amministrazione

PR.IP-01: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità).

1. Sono definite politiche e procedure con riferimento alla sicurezza delle applicazioni per fornire un adeguato supporto alla pianificazione, realizzazione e manutenzione delle funzionalità di sicurezza delle applicazioni, le quali dovranno essere riviste e aggiornate almeno su base annuale.
2. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
   a) le politiche di sicurezza adottate per lo sviluppo di configurazioni di sistemi IT e di controllo industriale e il dispiegamento delle sole configurazioni adottate;
   b) l'elenco delle configurazioni dei sistemi IT e di controllo industriale impiegate e il riferimento alle relative pratiche di riferimento;
   c) i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
3. Sono definiti e documentati requisiti di base per la sicurezza delle diverse applicazioni.
4. Sono definite ed implementate metriche, di natura tecnica, utili a monitorare il livello di aderenza ai requisiti di sicurezza definiti e gli obblighi di conformità.
5. Esiste un processo di mitigazione delle vulnerabilità applicative e ripristino per la sicurezza delle applicazioni, automatizzando la riparazione quando possibile.
6. È presente un processo per la convalida della compatibilità del dispositivo con sistemi operativi e applicazioni.
7. È presente un sistema di gestione delle variazioni in termini di sistema operativo, patching e/o applicazioni.

Regolamento Cloud – Servizi Cloud per la Pubblica Amministrazione

PR.IP-01: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità).

1. Sono definite politiche e procedure con riferimento alla sicurezza delle applicazioni per fornire un adeguato supporto alla pianificazione, realizzazione e manutenzione delle funzionalità di sicurezza delle applicazioni, le quali dovranno essere riviste e aggiornate almeno su base annuale [IaaS, SaaS].
2. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
   a) le politiche di sicurezza adottate per lo sviluppo di configurazioni di sistemi IT e di controllo industriale e il dispiegamento delle sole configurazioni adottate;
   b) l'elenco delle configurazioni dei sistemi IT e di controllo industriale impiegate e il riferimento alle relative pratiche di riferimento;
   c) i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza [SaaS].
3. Sono definiti e documentati requisiti di base per la sicurezza delle diverse applicazioni.
4. Sono definite ed implementate metriche, di natura tecnica, utili a monitorare il livello di aderenza ai requisiti di sicurezza definiti e gli obblighi di conformità.
5. Esiste un processo di mitigazione delle vulnerabilità applicative e ripristino per la sicurezza delle applicazioni, automatizzando la riparazione quando possibile.
6. È presente un processo per la convalida della compatibilità del dispositivo con sistemi operativi e applicazioni [PaaS, SaaS].
7. È presente un sistema di gestione delle variazioni in termini di sistema operativo, patching e/o applicazioni [PaaS, SaaS].

NIS 2

PR.PS-01: Sono stabilite e applicate pratiche di gestione della configurazione.

1. Per almeno i sistemi informativi e di rete rilevanti, sono definite, e documentate in un elenco aggiornato, le loro configurazioni di riferimento sicure (*hardened*).
2. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.

Bibliografia

[1] NIST, «Technical Note 1945». https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1945.pdf.

[2] NIST, «NIST Special Publication 800-177 Revision 1» https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf.

[3] Agenzia per la Cybersicurezza Nazionale, «Crittografia post-quantum e quantistica - Preparazione alla minaccia quantistisca». https://www.acn.gov.it/portale/documents/20119/85999/ACN_Crittografia_Quantum_Safe.pdf.

[4] Agenzia per la cybersicurezza nazionale, «Framework di autenticazione per la posta elettronica». https://www.acn.gov.it/portale/w/framework-di-autenticazione-per-la-posta-elettronica.