

# FRAMEWORK DI AUTENTICAZIONE PER LA POSTA ELETTRONICA

In un contesto in cui la posta elettronica è uno dei principali canali di comunicazione, proteggere il proprio dominio e-mail è essenziale. Comunemente gli attaccanti cercano di impersonare domini affidabili per inviare e-mail fraudolente, con l'obiettivo di ingannare utenti, partner o dipendenti. Le tecniche principali con cui gli attaccanti operano sono: **Phishing**: consiste nell'invio di e-mail fraudolente che imitano comunicazioni legittime — spesso da parte di banche, fornitori, colleghi o dirigenti — con l'obiettivo di ingannare il destinatario e indurlo a compiere un'azione dannosa. Queste e-mail possono contenere link a siti web falsi che raccolgono credenziali, allegati infetti che installano malware, o richieste urgenti di trasferimenti di denaro. Il tutto facendo leva su fiducia, urgenza e apparenza di legittimità. **Spoofing**: è una tecnica utilizzata per **falsificare l'identità del mittente di un'e-mail**, facendo sembrare che il messaggio provenga da un indirizzo affidabile — spesso appartenente a un'azienda, un fornitore o un dirigente interno. In pratica, un attaccante può inviare un'e-mail che, a prima vista, sembra provenire da `ceo@nomeazienda.com`, ma in realtà è stata inviata da un server esterno e malevolo. Pertanto, al fine di ridurre i rischi connessi con questo tipo di minaccia, oltre ad una costante formazione del personale, è fondamentale implementare il framework di autenticazione basato su 3 protocolli standard: **SPF, DKIM e DMARC**.

**DMARC** (*Domain-based Message Authentication, Reporting & Conformance*) è un protocollo che consente ai proprietari di un dominio di specificare come i server destinatari devono trattare i messaggi che falliscono i controlli SPF e DKIM. Se configurato correttamente, DMARC riduce drasticamente la possibilità che e-mail fraudolente vengano recapitate con successo. DMARC si basa sull'integrazione di due tecnologie fondamentali:

- **SPF** (Sender Policy Framework)

Verifica, tramite l'interrogazione di un record DNS, che il server di invio della email sia autorizzato a farlo per conto del dominio.

- **DKIM** (DomainKeys Identified Mail)

Firma digitalmente i messaggi tramite crittografia asimmetrica. Il destinatario può verificarne l'autenticità tramite la chiave pubblica reperibile in uno specifico record DNS del dominio mittente.

L'integrazione di SPF e DKIM protegge il dominio da usi non autorizzati. Se i controlli falliscono, il server ricevente può applicare le policy definite dal dominio mittente (none, quarantine, reject) e inviare report diagnostici.

Per implementare correttamente questo framework, è necessario pubblicare i seguenti record DNS:

# SPF

- **Tipo di record:** TXT
- **Nome/Host:** es. @ oppure <nomedominio.it>
- **Valore:** v=spf1 ipv4:<xxx.xxx.xxx.xxx> include:\_spf.provider.com -all

Sostituire xxx.xxx.xxx.xxx con l'IP del tuo server e provider.com con il tuo provider email (es. Google, Microsoft, etc.) se necessario. Questo record individua, come server autorizzati all'invio di posta elettronica per lo specifico dominio, solo l'IP specificato e i server del provider indicato. Il flag -all indica che le email provenienti da tutti gli altri server devono essere rifiutati.



Figura 1 - Processo di autorizzazione previsto nel protocollo SPF

# DKIM

- Genera una coppia di chiavi crittografiche (pubblica/privata) tramite il tuo server di posta o provider.
- **Tipo** di record: TXT
- **Nome/Host:** <>.\_domainkey.<nomedominio.it> (sostituisci <selettore> con un nome univoco)
- **Valore:** v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A... (sostituisci p= con la chiave pubblica completa generata)

Il server di posta deve essere configurato per firmare i messaggi in uscita con la chiave privata corrispondente.



Figura 2 - Funzionamento del protocollo DKIM

# DMARC

- **Tipo di record:** TXT
- **Nome/Host:** \_dmarc.<nomedominio.it>
- **Valore:** v=DMARC1; p=reject; rua=mailto:dmarc-report@<nomedominio.it>; ruf=mailto:dmarc-fail@<nomedominio.it>; sp=reject; adkim=s; aspf=s

**Parametri chiave:**

- p=reject: rifiuta i messaggi non conformi.
- rua / ruf: indirizzi per ricevere report aggregati e forensi.
- sp=reject: applica la stessa policy anche ai sottodomini.

Usare aspf=s e adkim=s è **consigliato** quando si vuole **massima sicurezza** ed evitare che sottodomini o servizi esterni possano inviare e-mail a nome del dominio principale senza autorizzazione esplicita. Questa configurazione richiede che tutti i tuoi servizi email siano **perfettamente configurati** e il controllo su tutti i domini e sottodomini coinvolti.

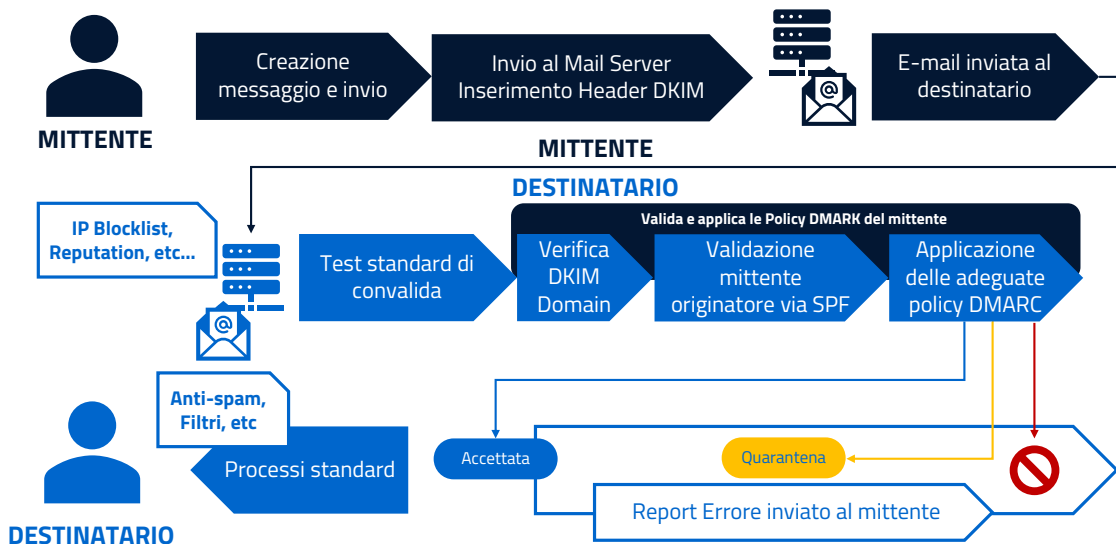


Figura 3 - Esempio di funzionamento del protocollo DMARC



## COMPLESSITÀ DI IMPLEMENTAZIONE

Protocollo	Complessità	Note operative
SPF	Bassa	Richiede solo la pubblicazione di un record TXT nel DNS.
DKIM	Media	Richiede la generazione di una copia di chiavi e la configurazione del server di posta.
DMARC	Bassa	Richiede conoscenza dei flussi email e monitoraggio dei report per una corretta policy.

## CONSIDERAZIONI FINALI

Per garantire l'efficacia del framework di autenticazione:

- Il dominio mittente deve pubblicare correttamente i record SPF, DKIM e DMARC nel DNS.
- Il server di posta mittente deve essere configurato per firmare i messaggi con DKIM.
- Il server destinatario deve essere configurato per eseguire le verifiche SPF e DKIM e applicare le policy DMARC.

È fortemente consigliato monitorare i report **DMARC** per identificare eventuali errori di configurazione o tentativi di abuso.