Collabra Professional Email

DKIM - DomainKeys Identified Mail

Versione 1.0
21 agosto 2015

Dkim - Domainkeys Identified Mail

Cos'è DKIM

DomainKeys Identified Mail (DKIM) è un sistema di validazione della posta elettronica progettato per riconosce ed intercettare lo **spoofing** fornendo un meccanismo che permette al mail exchanger ricevente di verificare che un messaggio da un determinato dominio è autorizzato dall'amministratore del dominio stesso e che il messaggio (allegati inclusi) non sia stato modificato durante il trasporto.

La **firma digitale** inclusa nel messaggio può essere infatti convalidata dal destinatario tramite la chiave pubblica del firmatario pubblicata sul **DNS** del dominio mittente.
Si tratta quindi di un sistema di **anti-spoofing** che lavora a livello di dominio di posta: il suo scopo è di permettere il riconoscimento di messaggi il cui domino mittente è stato falsificato in quanto questo falso mittente non avendo accesso alla chiave privata del dominio non è in grado di generare una firma valida e convalidabile tramite la chiave pubblica presente sul DNS.

Come tutti i sistemi che usano una tecnologia di cifratura asimmetrica necessita di due componenti:

1. La **chiave privata**: che deve essere detenuta esclusivamente dai sistemi abilitati alla firma di un documento. Nel nostro caso dai sistemi di posta elettronica abilitati alla spedizione dei messaggi per un dominio.
2. La **chiave pubblica**: che deve essere necessariamente resa pubblica. Questo relativamente a DKIM viene fatto tramite la sua pubblicazione sul DNS del domino.

Zimbra e DKIM

Zimbra implementa la tecnologia DKIM dalla versione 8.0.

Configurazione DKIM

Per attivare il servizio DKIM per un dominio, l'amministratore del dominio deve contattare il Suporto Tecnico Collabra (tramite i recapiti in suo possesso o tramite il modulo di contatto https://collabra.email/contatto/) specificando:

- il nome del dominio per cui si vuole procedere con l'attivazione del servizio
- la data in cui si vuole procedere in modo da poter procedere celermente alla modifica DNS necessaria per il corretto funzionamento

Alla data concordata lo staff Collabra provvederà a creare le chiavi sui sistemi di posta e risponderà all'amministratore indicando il record da inserire nel DNS.
Tale record avrà il seguente formato:

```
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX._domainkey IN TXT "v=DKIM1;=rsa;
p=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
```

con caratteri alfanumerici al mal posto delle X.

L'amministratore, una volta ricevuta la risposta, dovrà inserire questo record nella zona DNS relativa al dominio per cui si sta attivando il servizio DKIM e comunicare l'avvenuto inserimento allo staff Collabra che procederà alle verifiche e confermerà il corretto funzionamento delle impostazioni.

La firma delle mail

Una volta configurato DKIM tutti i messaggi spediti da un account appartenente al dominio conterranno alcuni header di firma simili a quello riportato qui di seguito:

```
DKIM-Filter: OpenDKIM Filter v2.9.2 mx.collabra.it 4404713F86D
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=example.com;
      s=0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB; t=1436790980;
      bh=xb/JoQSE9tb5AEr4gTxFcn5E7gFSGc9z/jKDG6uwhNtg=;
      h=Date:From:Reply-To:Message-ID:To:Subject:MIME-Version:
       Content-Type;
      b=d1OWY8oBOY6JNLTl39TrOhKeeIK4do4/DfiWeDQCgptgLAEL8TVXBiqEAnzaxeYM5
       gEQ+pJDjSv8KCmdFUKnhycwaSklsbNIkXCGRL2LuBb0M8W+LWEEtJ7/uQFZlanwfSR
       ByhFZFtdJM2y9YAJVKRFOqAfUT7JCkcXpMh/tJLs=
```