Proofpoint Hosted DKIM

Proofpoint Hosted DomainKeys Identified Mail (DKIM) is a DNS-based hosted authentication service available free of charge to customers of Email Fraud Defense. This service enables customers to manage DKIM selectors in DNS through a straightforward web-based DKIM management interface. Multiple DNS hosting methods are provided, as well as easy-to-use DKIM selector import capabilities, making DKIM selector management easy and in the full control of the email team.

Value

DKIM CHALLENGE OR LIMITATION	HOSTED DKIM SOLUTION
DNS provider limitations on key length	Support for up to 4,096-bit DKIM keys
DKIM selector query performance	Geolocation-based DNS query routing improves service resiliency
Complexity of DNS records prone to errors	Automatic verification of DKIM public key formatting
Cost of DNS changes discourages key rotation	Unlimited domains supported, along with unlimited DKIM selectors
DNS change control lead time	Near real-time updates

Specifications

FEATURE	DESCRIPTION
Customer portal	Easy-to-use interface for permitting and revoking sender rights
User security	Unique username and strong password
User rights	Configurable at both product and Proofpoint level (federated credential)
Multifactor authentication	Option to enforce MFA via customer's Identity Provider (IDP)
DKIM record mechanisms supported	TXT and CNAME
DNS security	Native DNS Security (DNSSEC) support
Protocol and port	UDP/TCP over port 53
Worldwide distributed hosting	Multiple Amazon Web Services (AWS) locations in the United States and European Union
Network access control	AWS Network Access Control
Application access control	AWS Identity and Access Management
DNS service redundancy	Local and regional redundancy
Load balancing	Amazon Network Load Balancer and Geoproximity DNS query routing
Monitoring	24/7 year-round proactive monitoring

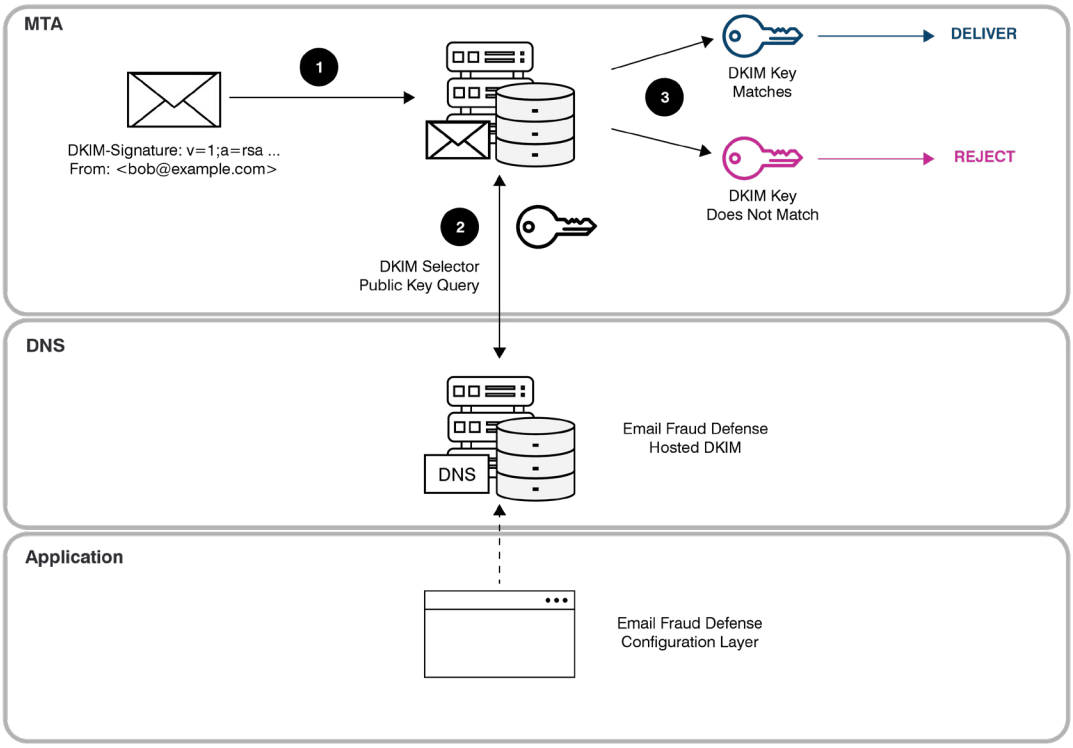

Figure 1: How Proofpoint Hosted DKIM works.

High Availability

Due to the redundancy and scalability of its architecture, Hosted DKIM operates at the highest levels of availability. In the unlikely event of a service disruption, automatic failover to alternate service location is seamless. Additionally, DNS caching and message inspection beyond DKIM would offset the risk to the deliverability of legitimate email.

For more information, contact your account manager.

LEARN MORE

For more information, visit **proofpoint.com**.