Subject: Implementation Guide for DKIM (DomainKeys Identified Mail)

DKIM Implementation Guide
Overview:
DomainKeys Identified Mail (DKIM) is an email authentication method designed to detect forged sender addresses in emails. This guide provides detailed instructions for implementing DKIM for your domain.
---
1. Prerequisites:
 - Access to your domain's DNS settings
 - Mail server configuration access
2. Generate DKIM Keys:
 - Use a DKIM key generation tool. Here's an example command using OpenSSL:
 ```
 openssl genrsa -out private.key 1024
 openssl rsa -in private.key -pubout -out public.key
 ```
 - Save the generated private key securely on your mail server.
3. Create DKIM DNS Record:
 - Format: `selector._domainkey.yourdomain.com`
 - Example Record:
 ```
 DKIM Record: v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3...
 ```
 - Add this record to your DNS settings.
4. Configure Mail Server:
 - For Postfix:
 ```
 opendkim-genkey -s selector -d yourdomain.com
 ```
 - Edit your Postfix configuration file (`/etc/postfix/main.cf`):
 ```
 milter_protocol = 2
 smtpd_milters = inet:localhost:8891
 non_smtpd_milters = inet:localhost:8891
 ```
 - Restart Postfix to apply changes.
5. Test Your DKIM Setup:
 - Use online DKIM validators or send a test email and check the headers.
 - Look for:
 ```
 DKIM-Signature: ...
 ```
 - Check that the signature aligns with the expected selector and domain.
6. Monitoring and Troubleshooting:
 - Monitor email delivery reports and server logs.
 - Common issues include:
 - Incorrect DNS record
 - Key length issues
 - Mismatched selectors

Conclusion:

Implementing DKIM enhances your email security and helps prevent spoofing. Ensure to regularly update your private key and monitor your DKIM signatures.

Contact Information:

For further assistance, contact the IT support team at support@yourdomain.com.

Document Version: 1.0

Last Updated: October 2023
