M³AAWG Best Practices for Implementing DKIM To Avoid Key Length Vulnerability

October 2012, December 2013
Revised: July 2017
URL to Reference this Document: www.m3aawg.org/Implement-DKIM-BP

The Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) strongly encourages organizations to review their DKIM email authentication implementation due to potential vulnerabilities associated with the use of short DKIM keys at well-known organizations.

The recommended best practices are:

1.) **Key Length**: Use a minimum of a 1024-bit key length to increase key complexity. This is because shorter keys, such as 512-bit, have a higher vulnerability and can be cracked within 72 hours using inexpensive cloud services.
2.) **Rotation**: Keys should be rotated at least twice per year to reduce the period of time the key could be maliciously used to compromise the integrity of email.[1]
3.) **Expiration**: Signatures should have an expiration period greater than your current key rotation period. Old keys should be revoked in DNS as appropriate. (Delete the contents from the "p=" field.)
4.) **Test Mode**: The "t=y" declaration is for testing only. Experience has shown that several mail providers ignore the presence of the DKIM signature when they find "t=y". This mode is to be used for a very short period and only during the initial DKIM ramp-up.
5.) **Monitoring**: To be able to monitor how receivers are accepting email signed with DKIM, it is recommended to implement DMARC with a "p=none" policy (also referred to as "monitoring mode"). Use DNS to monitor how frequently keys are queried. DMARC, Domain-based Message Authentication, Reporting and Conformance, standardizes how email receivers perform email authentication using the well-known SPF and DKIM mechanisms[2].
6.) Domain Keys is a deprecated protocol; use DKIM instead.
7.) **Hashing Standards**: Deprecate the use of SHA1 for hashing and move to SHA256 as per RFC 6376, Section 3.3.
8.) **Third Party Mailers**: Organizations should be engaged with anyone that sends mail on their behalf to ensure that their third-party vendor (i.e., their email service provider) complies with these best practices.

[1] **NOTE**: An earlier version of this best practices document recommended that DKIM keys be rotated quarterly. Subsequent research resulting in a more detailed M³AAWG best common practices document on the topic of key rotation updated this recommendation to rotate keys at least twice a year. For more information on best practices for DKIM key rotation, see: https://www.m3aawg.org/sites/default/files/document/M3AAWG_DKIM_Key_Rotation_BP-2013-12.pdf

[2] See www.dmarc.org for more information on this protocol.

Additional resources:
M³AAWG DKIM Implementation Training Videos: http://www.maawg.org/activities/training/dkim-video-list

News reports on key vulnerability:
http://www.wired.com/threatlevel/2012/10/dkim-vulnerability-widespread/
http://www.wired.com/threatlevel/2012/10/dkim-third-party-emailers/
http://www.computerworld.com/s/article/9232944/Google_s_email_security_flaw_is_embarrassing_but_no_catastrophe
http://www.forbes.com/sites/eliseackerman/2012/10/29/google-says-google-apps-domains-were-protected-from-massive-spoofing-vulnerability/

US-CERT vulnerability report:
http://www.kb.cert.org/vuls/id/268267

Demonstration of cracked keys:
https://www.wired.com/2012/10/dkim-vulnerability-widespread/
https://blog.returnpath.com/does-googles-hack-reveal-dkim-vulnerability-not-really-v2/

Referenced protocols:
www.dkim.org, www.openspf.org, www.dmarc.org

As with all documents that we publish, please check the M³AAWG website (www.m3aawg.org) for updates to this paper.

M3AAWG064 – Revised 2017-07, 2013-12, 2012-10