DKIM Recommendations 2018 with consideration of the DKIM Crypto Update

1. Background

DKIM is a widely used method for the authentication of emails. But when DKIM is not used correctly, it is not effective and can offer a false sense of security. For this reason, here we have summarized the common Best Practices for DKIM.

2. Technical Measures

2.1 Length of the Key

With rapidly increasing processing power of computers, RSA keys with a 512-bit length, previously considered to be secure, can be cracked in a short period of time. Today, a minimum of 1024 bit RSA should be used. Organizations like the American National Institute of Standards and Technology (NIST) go further, and recommend a minimum of 2048 bits. Here, it should be noted that large keys (normally upwards of 4096 bits) can potentially cause problems in the DNS, as the answers then no longer fit into a UDP packet, but need to be answered using TCP.

2.2 Algorithms

The DKIM Standard only supports RSA as an algorithm, and more modern algorithms are not supported. Work is currently being done to resolve this disadvantage. The initiative "DKIM Crypto Update" is working to address this problem and update the DKIM Standard to the current cryptographic level. The current level can be found in RFC 8301.[1]

The most important changes relate to the aforementioned length of the key. In addition, the support of EdDSA is included as a cryptographic algorithm alongside RSA. EdDSA has several advantages. For the same security level, the keys are considerably shorter and thus avoid the already mentioned problems with the DNS. The signing and verification with EdDSA is also less resource intensive. However, it can be assumed that not every recipient is already at the point of being able to process a DKIM signature with EdDSA. Therefore, if using EdDSA, every email should be additionally - as fallback – signed with RSA a second time via another selector.

[1] https://datatracker.ietf.org/wg/dcrup/about/

A further innovation relates to the hash-algorithm used. Given that SHA-1 is no longer considered secure, SHA-256 should be the only one used.

2.3 Monitoring

To be able to monitor whether the emails are able to be correctly verified at the receiver end, the use of DMARC is recommended. Using a "none" policy will mean that the delivery of emails is not influenced by DMARC, but the reporting provides an overview of whether DKIM is working as expected.

3. Organizational Measures

3.1 Access to Private Keys

The security and confidentiality of the private key is essential. In the case of unauthorized access to the private key, it is possible for you to sign any emails for the associated domain yourself. As a result, the key should be secured using the standard methods (access limitations through the operating system, encryption of disks,..).

3.2 Key rotation

But even if all care is taken, it is possible for a private key to be compromised, e.g. through a former member of staff. Therefore, it is imperative for the keys to be rotated regularly, meaning that they are exchanged for a new pair of keys – at least once per year, or even better, each quarter or monthly. In particular when rotating at shorter intervals, it quickly becomes clear that key rotation should be automated, for example using an appropriate script and cronjobs. Details on the key rotation process are well described in the document "M3AAWG DKIM Key Rotation Best Common Practices".[2] If you send emails on behalf of others, for example as an email service provider, you will be faced with special challenges when it comes to the key rotation, because a new public key needs to be published in the DNS and changes generally need to be made by the domain owner, and therefore the customer. Solutions to this problem can be found in the document "DKIM setup the easy way".[3]

Author: Alexander Zeh, Certified Senders Alliance

[2] https://www.m3aawg.org/sites/default/files/document/M3AAWG_DKIM_Key_Rotation_BP-2013-12.pdf
[3] https://certified-senders.org/wp-content/uploads/2017/07/CSA_DKIM_the_easy_way.pdf