CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

DKIM INTEGRATION & IMPLEMENTATION.

dnsbelgium

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

Content

DOCUMENT CONTROL AND REVIEW

Document Control	
Author	
Owner	
Date created	
Last revised by	
Last revision date	

.

VERSION CONTROL

Version	Date of approval	Approved by	Description of change

Introduction: the need for DKIM implementation

E-mail is one of the most widely used communication channels within organisations and plays a crucial role in business processes. However, the convenience and accessibility of e-mail also make it a popular target for cybercriminals. Phishing, spoofing and other forms of e-mail fraud pose a serious threat to the security and reliability of e-mail traffic.
To mitigate these risks and ensure the credibility of e-mail communications, it is imperative that organisations implement strong e-mail authentication mechanisms. One of the most effective methods for this is **DomainKeys Identified Mail (DKIM)**. DKIM provides a powerful way to ensure the integrity and authenticity of outgoing e-mails, aiming to protect both the sender and the recipient.

1 Why DKIM?

1.1 INCREASING TRUST IN EMAIL COMMUNICATION

DKIM helps establish that an e-mail actually comes from the claimed sender. This increases trust in emails sent from your domain, which is essential for communication with customers, partners and internal stakeholders.

1.2 PROTECTION AGAINST EMAIL SPOOFING

Spoofing is a technique where attackers use a fake e-mail address to establish trust and deceive victims. DKIM makes it more difficult for attackers to misuse legitimate domain names because the authenticity of emails can be cryptographically validated.

1.3 IMPROVING EMAIL DELIVERABILITY

Internet Service Providers (ISPs) and e-mail providers such as Gmail, Outlook and Yahoo! use DKIM to determine whether an e-mail should be considered legitimate. Emails without a DKIM signature may be flagged as suspicious and end up in the spam folder even if they are legitimate. DKIM therefore contributes to a higher delivery rate.

1.4 PART OF A BROADER EMAIL SECURITY STRATEGY

DKIM works seamlessly with other e-mail authentication mechanisms such as **SPF (Sender Policy Framework)** and **DMARC (Domain-based Message Authentication, Reporting, and Conformance)**. Together, these technologies form an integrated system to combat e-mail fraud and reduce the risk of data leakage.

1.5 COMPLIANCE AND LEGAL REQUIREMENTS

In sectors such as financial services, healthcare and government, there are increasingly stringent data protection and fraud prevention requirements. Implementing DKIM can help meet standards and regulations, such as the **AVG (General Data Protection Regulation)**.

1.6 PROTECTION OF CORPORATE REPUTATION

A compromised e-mail infrastructure can cause serious damage to an organisation's reputation. DKIM helps prevent your domain name from being used for malicious purposes, such as sending phishing emails.

2. Conclusion

Given the increasing frequency and complexity of e-mail-related threats, implementing DKIM is not a luxury but a necessity. DKIM offers a cost-effective solution to ensure email reliability, prevent email fraud and improve the overall security of your organisation. In this paper, we will elaborate on how DKIM works technically, the benefits of implementation and the steps required to successfully implement this technology within your organisation. By implementing it carefully and monitoring it regularly, you can significantly improve e-mail security. Combined with SPF and DMARC, DKIM creates a robust defence against email abuse

3. DKIM: Technical Explanation and Implementation

3.1. WHAT IS DKIM?

DKIM (DomainKeys Identified Mail) is an e-mail verification mechanism that ensures that an e-mail has not been modified in transit. It works by adding a digital signature to an e-mail, which can be validated by the receiving mail server.

- **Key features**:
    - Sender verification.
    - Ensuring the integrity of email content.
    - Prevention of e-mail manipulation in transit.

3.2. HOW DOES DKIM WORK?

3.2.1 KEY CONCEPTS

1. **Digital signature**:
    - The sending server generates a cryptographic signature with a private key.
    - This signature is included in the DKIM header of the e-mail.
2. **Public key in DNS**:
    - The public key associated with the private key is published in a DNS TXT record.
    - Receiving servers use this public key to validate the signature.
    - DNSSEC ensures that the DNS lookup is also cryptographically authenticated
3. **Selector**:
    - A unique identifier indicating which key was used for the signature. This makes it possible to manage multiple keys.

3.2.2 TECHNICAL OPERATION OF DKIM

1. **Signature generation**:
    - The sending mail server selects specific parts of the e-mail to sign, such as:
        - Headers: 'From', 'To', 'Subject'.
        - The body of the email.
    - A hashing algorithm (e.g. SHA-256) is used to create a hash of the selected parts.
    - This hash is encrypted with the private key, yielding the DKIM signature.

2. **Adding the DKIM header**:
    - The signature is added to the e-mail as a new header. A typical DKIM header looks as follows:

      ```
      DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=example.com; s=selector1;
      h=from:to:subject:date; bh=base64_body_hash;
      b=base64_signature
      ```

        - **v=1**: DKIM version.
        - **a=rsa-sha256**: Signature algorithm.
        - **d=example.com**: The domain of the sender.
        - **s=selector1**: Selector for the public key in DNS.
        - **h=from:to:subject:date**:Headers used when signing.
        - **bh=base64_body_hash**: Hash of the body of the e-mail.
        - **b=base64_signature**: The digital signature.

3. **Validation by the receiving server**:
    - The receiving server retrieves the domain's public key via DNS.
    - The server uses this public key to:
        - Recalculate the body hash.

    - Decoding the signature.
    - Compare the values to check if the e-mail is unchanged.

4. Benefits of DKIM

- **Integrity check**: DKIM guarantees that the content of an e-mail has not been altered in transit.
- **Better spam filtering**: Many e-mail providers give higher scores to verified e-mails, which improves delivery.
- **Protection of domain reputation**: Reduces the likelihood of domain misuse in phishing.

5. Steps to implement DKIM

5.1 OFFICE 365

https://learn.microsoft.com/en-us/defender-office-365/email-authentication-dkim-configure

5.2 GCP

https://support.google.com/a/answer/174124?hl=en

6. Best practices for DKIM

1. **Use strong cryptography**:
   - Use at least RSA 2048-bit keys to provide quantum computing-resistant security.
2. **Rotate keys regularly**:
   - Schedule annual rotation of DKIM keys to minimise risk.
3. **Manage selectors carefully**:
   - Use unique selectors for different environments (e.g. prod1, test1) to facilitate management.
4. **Combine with SPF and DMARC**:
   - DKIM alone does not fully protect against spoofing. Combine it with SPF and DMARC for comprehensive email security.
5. **Check for misconfigurations**:
   - Expired or improperly configured DKIM records can block emails. Test regularly with monitoring tools.(https://nl.internet.nl/)

7. Possible errors and solutions

Problem: "No DKIM signature found"

- **Cause**: The mail server is not correctly configured to sign e-mails.
- **Solution**: Check the configuration and make sure the correct private key is used.

Problem: "DKIM validation failed"

- **Cause**: The public key in DNS does not match the private key.
- **Solution**: Publish the correct public key in the DNS TXT record.

Disclaimer

THIS GUIDE WAS PREPARED BY THE CENTRE FOR CYBERSECURITY BELGIUM IN COLLABORATION WITH DNS BELGIUM. ALL TEXTS, LAYOUTS, DESIGNS AND ELEMENTS OF ANY KIND IN THIS GUIDE ARE PROTECTED BY COPYRIGHT. EXTRACTS FROM THIS GUIDE MAY ONLY BE PUBLISHED FOR NON-COMMERCIAL PURPOSES ON CONDITION THAT THE SOURCE IS ACKNOWLEDGED. THE CENTRE FOR CYBERSECURITY BELGIUM AND DNS BELGIUM DISCLAIM ALL LIABILITY FOR THE CONTENTS OF THIS GUIDE. The information provided : - Is of a general nature only and does not address the specific situation of an individual or legal entity. - Is not necessarily complete, accurate or up-to-date. - Does not constitute professional or legal advice. - Is not a substitute for expert advice. - Does not guarantee secure protection.