Mail: DKIM - DomainKeys Identified Mail

What is DKIM?

DKIM (DomainKeys Identified Mail) is an email authentication mechanism that:

- adds a **a digital signature**,
- allows the recipient to check if the message has been modified,
- confirms that the email comes from an authorised domain.

DKIM does not restrict who can send messages - instead it **guarantees the integrity and authenticity** sender through a cryptographic signature.

How does DKIM work?

(1) When an email is sent, the sender's server:

- generates a digital signature (based on the message content and headers),
- adds it to the message in the header:

  ```
  DKIM-Signature
  ```

  .

2. the public key needed for verification is published in the DNS of the domain.

3. the recipient server:

- reads the signature from the message,
- retrieves the public key from the DNS,
- verifies that the signature matches the message content and the key.

If yes - the message is **authorised**. If not - considered as **potentially fraudulent**.

DKIM signature structure

Example of a DKIM header:

```
DKIM-Signature: v=1; a=rsa-sha256; d=ostrowski.net.pl; s=selector1;
c=relaxed/relaxed;
  h=from:to:subject:date;
  bh=fakehash==;
  b=fake_signature_data==
```

Element	Meaning
`v`	DKIM version (always `1`)
`a`	Cryptographic algorithm
`d`	Signing domain
`s`	Selector (DNS record name with public key)
`h`	List of headers covered by the signature
`b`	Proper signature
`bh`	Hash of message content

How to configure DKIM?

1. **Generate a key pair**:

- **private key** - remains on the mail server (signs messages),
- **public key** - published as a record **TXT** in DNS.

2. **Add the TXT record to DNS**:

- Name:

```
selector1._domainkey.ostrowski.net.pl
```

- Value:

```
v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQE...
```

3. **Configure the mail server**to sign messages using a private key and the selected selector.

Syntax of the DKIM record in DNS

```
v=DKIM1; k=rsa; p=KLUCZ_PUBLICZNY
```

Element	Meaning
`v`	DKIM version (DKIM1)
`k`	Key type (mostly `rsa`)
`p`	Public key in Base64 format.

What is a selector?

The selector is a unique name that identifies a given DKIM key. It allows you to:

- manage multiple keys for a single domain,
- rotate keys without interrupting DKIM operation.

The selector name is part of the DNS query:

```
[selector]._domainkey.[domena]
```

Example:

```
selector1._domainkey.ostrowski.net.pl
```

Example of a DKIM record

```
Nazwa: selector1._domainkey.ostrowski.net.pl
Typ: TXT
Wartość: v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApn...
```

DKIM testing

Once a record has been added, you can test its accuracy:

- https://mxtoolbox.com/dkim.aspx
- https://dkimcore.org/tools/keycheck.html
- https://www.mail-tester.com/

You can also send an e-mail to:

- `check-auth@verifier.port25.com`.
- `dkimcheck@auth.returnpath.net`

Recommendations for DKIM

- Use keys with a minimum length of **1024-bit** (2048-bit recommended).
- Regularly **rotate selectors/keys** - e.g. every 6-12 months.
- Don't delete the old record as soon as the selector changes - mail may be on the way.
- Ensure date/time synchronisation on the server (important for signature).

Is DKIM enough?

No. DKIM does not protect:

- against spoofing of the „From” address (because it does not check that the sender's server is legitimate),
- against spam - it only ensures that the message has not been modified.

To obtain **full email protection**, you need to combine:

- **SPF** - determines who can send email from the domain,
- **DKIM** - signs messages,
- **DMARC** - enforces SPF/DKIM compliance and reports violations.

Common problems with DKIM

- Missing or incorrect DNS record (bad selector, truncated key, no `v=DKIM1`).
- Server does not sign messages despite active DKIM.
- DNS record too long - may be badly parsed (break into several lines in DNS).
- Selector incompatibility with server configuration.

Summary

DKIM is an effective method of confirming that an email:

- came from an authorised source,
- has not been modified during transmission.

To work effectively:

- must be correctly configured on the mail server,
- The public key must be available in DNS,
- Should be used in conjunction with **SPF and DMARC**.

DKIM is not only protection, but also the foundation of mail credibility in the eyes of Gmail, Outlook and other providers.