Mail: DKIM – DomainKeys Identified Mail

Co to jest DKIM?

DKIM (DomainKeys Identified Mail) to mechanizm uwierzytelniania poczty e-mail, który:

- dodaje do wiadomości **cyfrowy podpis**,
- pozwala odbiorcy sprawdzić, czy wiadomość została zmodyfikowana,
- potwierdza, że e-mail pochodzi z uprawnionej domeny.

DKIM nie ogranicza, kto może wysyłać wiadomości — zamiast tego **gwarantuje integralność i autentyczność** nadawcy poprzez podpis kryptograficzny.

Jak działa DKIM?

1. W momencie wysyłania e-maila, serwer nadawcy:

- generuje cyfrowy podpis (na podstawie treści wiadomości i nagłówków),
- dodaje go do wiadomości w nagłówku:

  `DKIM-Signature`

  .

2. Klucz publiczny potrzebny do weryfikacji jest publikowany w DNS domeny.

3. Serwer odbiorcy:

- odczytuje podpis z wiadomości,
- pobiera klucz publiczny z DNS,
- sprawdza, czy podpis jest zgodny z treścią wiadomości i kluczem.

Jeśli tak – wiadomość jest **autoryzowana**. Jeśli nie – uznawana za **potencjalnie sfałszowaną**.

Struktura podpisu DKIM

Przykład nagłówka DKIM:

```
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	Znaczenie
`v`	Wersja DKIM (zawsze `1`)
`a`	Algorytm kryptograficzny
`d`	Domena podpisująca
`s`	Selektor (nazwa rekordu DNS z kluczem publicznym)
`h`	Lista nagłówków objętych podpisem
`b`	Właściwy podpis
`bh`	Hash treści wiadomości

Jak skonfigurować DKIM?

1. **Wygeneruj parę kluczy**:

- **klucz prywatny** – pozostaje na serwerze pocztowym (podpisuje wiadomości),
- **klucz publiczny** – publikowany jako rekord **TXT** w DNS.

2. **Dodaj rekord TXT do DNS**:

- Nazwa:

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

- Wartość:

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

3. **Skonfiguruj serwer pocztowy**, aby podpisywał wiadomości za pomocą klucza prywatnego i wybranego selektora.

Składnia rekordu DKIM w DNS

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

Element	Znaczenie
`v`	Wersja DKIM (DKIM1)
`k`	Typ klucza (najczęściej `rsa`)
`p`	Klucz publiczny w formacie Base64

Co to jest selektor (selector)?

Selektor to unikalna nazwa identyfikująca dany klucz DKIM. Pozwala:

- zarządzać wieloma kluczami dla jednej domeny,
- rotować klucze bez przerywania działania DKIM.

Nazwa selektora jest częścią zapytania DNS:

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

Przykład:

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

Przykład rekordu DKIM

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

Testowanie DKIM

Po dodaniu rekordu możesz przetestować jego poprawność:

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

Można także wysłać e-mail na:

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

Zalecenia dla DKIM

- Używaj kluczy o długości minimum **1024-bit** (zalecane 2048-bit).
- Regularnie **rotuj selektory/klucze** – np. co 6–12 miesięcy.
- Nie usuwaj starego rekordu od razu po zmianie selektora – poczta może być w drodze.
- Zadbaj o synchronizację daty/godziny na serwerze (ważne dla podpisu).

Czy DKIM wystarczy?

Nie. DKIM nie chroni:

- przed spoofingiem adresu „From” (bo nie sprawdza, czy serwer nadawcy jest uprawniony),
- przed spamem — tylko zapewnia, że wiadomość nie została zmodyfikowana.

Aby uzyskać **pełną ochronę e-maila**, należy połączyć:

- **SPF** – określa, kto może wysyłać maile z domeny,
- **DKIM** – podpisuje wiadomości,
- **DMARC** – egzekwuje zgodność SPF/DKIM i raportuje naruszenia.

Częste problemy z DKIM

- Brak lub błędny rekord DNS (zły selektor, skrócony klucz, brak `v=DKIM1`)
- Serwer nie podpisuje wiadomości mimo aktywnego DKIM
- Zbyt długi rekord DNS – może być źle rozparsowany (rozbij na kilka linii w DNS)
- Niezgodność selektora z konfiguracją serwera

Podsumowanie

DKIM to skuteczna metoda potwierdzania, że wiadomość e-mail:

- pochodzi z autoryzowanego źródła,
- nie została zmodyfikowana w trakcie przesyłu.

Aby działał skutecznie:

- Musi być poprawnie skonfigurowany na serwerze pocztowym,
- Klucz publiczny musi być dostępny w DNS,
- Powinien być stosowany razem z **SPF i DMARC**.

DKIM to nie tylko ochrona, ale także fundament wiarygodności poczty w oczach Gmaila, Outlooka i innych dostawców.