DKIM praktikus volta

DomainKeys Identified Mail (DKIM) Signatures
RFC 6376 (Sep 2011) Internet Standard
https://tools.ietf.org/html/rfc6376
RFC 4870 (May 2007) Proposed Standard

A **levélfejléc és -törzs** szintjén működik, nem pedig a boríték szintjén.

- A szerző szervezetet vagy a létrehozó e-mail szolgáltató fennhatósága alatt történik az aláírás,
- a levélfejléc bizonyos elemei és törzs egy rész vagy egésze kerül aláírására, de
- a fejléc részét képező From mező mindig aláírásra kerül a DKIM által.

DKIM **antispam technika**ként szolgál,

- phishing elleni automatikus és manuális védelemben jól alkalmazható,
- spam (és így phishing) elleni automatikus védelemben a DMARC-kal kombinálva különösen jól alkalmazható.
- Az SPF és DKIM kiegészítheti egymást.

Mint minden védelmi technika, megvannak a maga problémái, árnyoldalai, gyengeségei, de mindennek ellenére nagyon hasznos technika.

Hitelesség + non-repudáció

Most egy másik praktikus oldalát emeljük ki a DKIM használatának, azt, hogy

- **hitelesíthetheti az email üzenet eredetét**,
  - sőt **akár magát a feladót** is (bár nem önmagában),
- **meghamisíthatatlanná teszi az aláírt fejléc elemeket és az aláírt levéltörzs szövegét**,
- **letagadhatlanná teszi az üzenetet és az aláírt tartalmát** (annak eredetiségét és megbabrálatlanságát garantálja).

A teljes hitelességhez a DNSSEC-kel történő együttes alkalmazás szükséges.

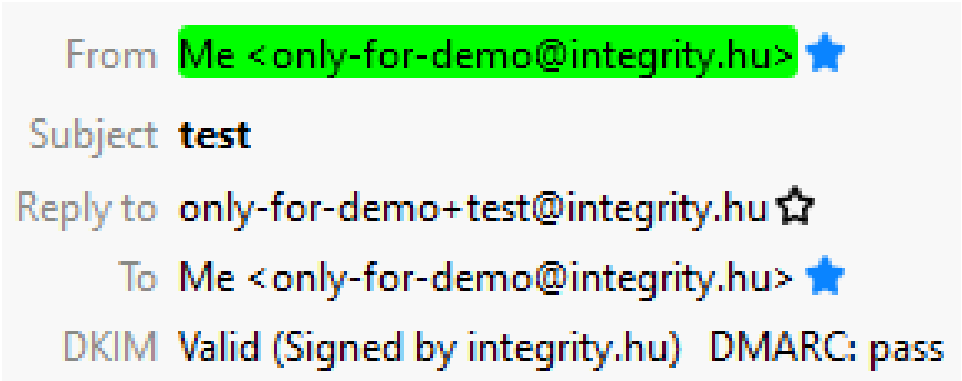
DKIM + DMARC

sőt inkább:

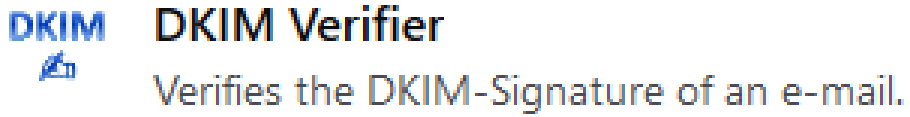
DNSSEC + SPF + DKIM + DMARC

(sőt: **+ARC** -- The Authenticated Received Chain (ARC) Protocol https://tools.ietf.org/html/rfc8617)

Feladó azonosítása



Thunderbird DKIM Verifier



```
Authentication-Results: INTMAIL-DMARC; dmarc=pass
header.from=integrity.hu
Authentication-Results: INTMAIL-DKIM;
     dkim=pass (2048-bit key; secure) header.d=integrity.hu
header.i=@integrity.hu header.b=1HtvYD1J;
     dkim-adsp=pass; dkim-atps=neutral
Received-SPF: Pass (sender SPF authorized) identity=mailfrom; client-
ip=212.52.165.188; helo=intmail-smtp.integrity.hu; envelope-from=only-
for-demo@integrity.hu; receiver=only-for-demo@integrity.hu

DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=integrity.hu;
s=mail;
     t=1605378420; bh=JQroEXDy5WlDsHGLPUA5ZYkZz54TY2GLsJsYI/fl6BE=;
     h=Reply-To:To:From:Subject:Date;
     b=1HtvYD1JIS45gpyn8lhL48UcBsgo1fyGOH8bMNnQr22/CWuQBC7fJO2BKrcZsi+1+
      YPpn+y6+Ne6neZsaZ/PSkf1WARtuTlv9x1YHdyLnFJfI0Z9KkySJglolulOXnVjXrR
      93GLgzZhgNTcEUFnxLdGsL/GSmlueg8x5ebvfqoCwE51tTA+b31z+7lVHRC5jQOnix
      8NskAsdbWQKGQCFpcH6D9QdFIqNmNBY5lU2Ji7kRtE9krOJXHojIdo8gBFMgWLO85a
      zW/5cHh98sTOUrgnfq2AdKB+7yZ4TCoovvjbJIWqUIBSonxmWc6I89U8cteLcWvxdc
      9cQAY8dMPb85A==
```

Reply-To: only-for-demo+test@integrity.hu
From: Demo User <only-for-demo@integrity.hu>
Subject: test
Date: Sat, 14 Nov 2020 19:26:59 +0100

Hogy hitelesíthetjük a feladót és az üzenetet?

Visszakérdezés: tipikusan válasz e-mailben megerősítés kérése.

Ha a levél vagy az abban küldött dokumentum

- hiteles elektronikus aláírással ellátott, a tanúsítvány elégséges információt tartalmaz az aláíróról,
- akkor az üzenetet vagy a küldött dokumentumot hitelesnek, a vélelmezett feladótól származónak fogadhatjuk el.

Elektronikus aláírást sem feltétlenül a szerző teszi a levélre vagy a dokumentumra, hiszen ezt valami program teszi valójában, mely akár egy automata aláíró alkalmazás is lehet.

AVDH vagy Docusign esetén sem a szerző fennhatósága alatt történik a szoftveres aláírás.

DKIM esetén az aláírás az ún. Mail Transfer Agent (MTA), illetve annak egy modulja végzi.

Jó kérdés: Miért és mikor bízhatunk a DKIM-ben?

Jogi értelemben a DKIM (noha elméletileg nem kizárt DKIM ilyen célra való alkalmazása) nem eredményez teljes bizonyítóerejű magánokiratot.

De ne becsüljük túl a teljes bizonyítóerejűség jogi fogalmát, és ne becsüljük le az authentikáció, hitelesség és non-repudáció értékét, amit különböző technológiák, mint a DKIM képesek nekünk nyújtani. Rendszerint nem bírósági perre készülünk, valamint ennél jellemzően fontosabb az, hogy azonosítani tudjuk a feladót és hitelesnek elfogadni az üzenetet.

A teljes bizonyító erejűnek vélt hagyományos papíralapú okiratok valós bizonyító képessége igen gyenge, főleg, ha nincs nagyon megbízható írásszakértőnk.

A DKIM praktikus és jó

DKIM jó eszköz, sok éve már, hogy a világ e-mail üzeteinek a többsége érvényes DKIM aláírással van ellátva, jelenleg kb. a világ e-mail üzeneteinek 90%-a érvényes (valid) DKIM aláírással van ellátva.

Figyeljünk! DKIM-mel spam és phishing leveleket is aláírnak!

A DKIM fogadó oldalon történő alkalmazása esetén figyelnünk kell bizonyos kérdésekre:

- természetesen arra figyelnünk kell, hogy ki is az aláíró;
- …

Alakítsuk ki az email FOGADÁS OLDALÁRA is SZERVEZETI SZABÁLYAINKAT is!

Miben ludasok azok a bankok és szolgáltatók akiknek nevükkel visszaélnek?

Mit csinálnak rosszul?

Védekezés phishing és zsaroló malware ellen

- Legfontosabb, hogy rendszerünkbe bejut, akkor **ne tudjon kért okozni!**

- Lehetőleg ne is jusson be a rendszerünkbe!

- Felhasználók nagyrészt kiszűrik a phishing és zsaroló malware-t, de …

Mai webinárunk tanulsága lehet: **ne adjunk ennyi teret a spammelőknek, phishingelőknek, zsarolóknak!** Lásd. pl. **DKIM-DMARC**, vagy **doménnév-regisztrációs** kérdések.

Köszönjük a figyelmet!

INTEGRITY Kft.

SZTAKI

MELASZ

RSOE