



## Avoiding email spoofing and tampering with DKIM

Besides SPF, there is another protocol that ensures sent emails have not been modified during their journey, and that the sender is really sending the email from the address listed in the email header. This is **DKIM**, DomainKeys Identified Mail.

DKIM uses cryptographic signing to ensure the content has not been modified during the journey, and the sender domain is really what it pretends to be.

### How DKIM works

When the mail administrator of the *example.com* domain wants to use DKIM to allow the recipients to check the content of the email has not been modified, he needs to take the following actions:

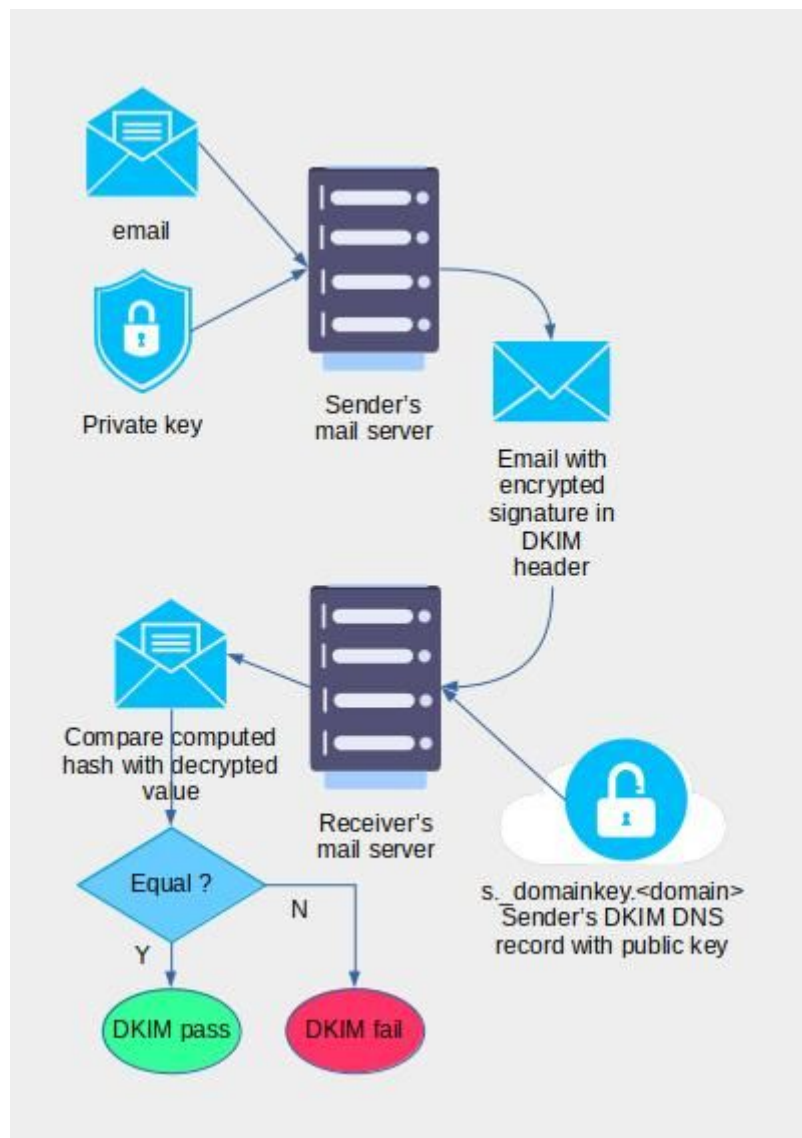
- Create a public/private cryptographic key pair;
- Publish a DNS TXT DKIM record containing his public key.

Then, he and other mail administrators of domains receiving emails from the *example.com* domain need to enable DKIM so the email handling software can sign and verify the emails.

**Note:** if a mail server is not configured to check DKIM, no defence against tampering will be put in place even if the sender has a DKIM record.

Let's assume *\*user1@example.com\** sends a mail to *\*user2@otherdomain.com\**. When DKIM processing is enabled, the following things happen:

- The sender server in the *example.com* domain (the signer) computes a hash of a list of headers, and a hash of the email body;
- It encrypts the hashes with its private key, creating a signature;
- It writes a *DKIM-Signature* header into the mail containing the list of headers protected by the signature, the signature itself, and a selector, which is the first part of the DNS TXT record containing its public key;
- The receiving server (the verifier) locates the selector in the DKIM header;
- It queries DNS to receive the DKIM record of the sending domain (in our case: *<selector>.\_domainkey.example.com*);
- It extracts the sender's public key from the DNS DKIM record;
- It decrypts the signature;
- It performs the same hash operations on the list of headers protected by the signature and on the email body;
- It now compares the 2 hash values;
- If they are identical, an *Authentication-Results:* header is added to the email with a dkim status 'pass'
- If not, the *Authentication-Results:* header is added to the email with a dkim status 'fail', and the mail is subject to the DKIM fail policy of the mail handler. Generally, it is marked as spam, junk, or is quarantined.



## The DKIM-Signature header

This is an example of a DKIM-Signature header created by the outlook.com (Microsoft) mail provider:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=outlook.com; s=selector1; h=From:Date:Subject:Message-
ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;
bh=J5xVXlIPB8b3aQVmIOVS4pAqIH4o0aHCb3LgLetuS1s=;
b=OSRH95fo/UTLgZrvDcO5B8HF306wPd5WZ76iZu9v0tRVgAXgPJEWjUJsqcmxtRnn
4ZnKhEpEfBx16XLMBbIebYfAK7NPdchpSv2yAfpqjmCkLotnvG/r1tpuz9qqW/
6vxdzxCGvoxw1DPpFA+Qh0Zs95P5k86h7w6EgXpsEh3jx5rU4eR0qIRoSOTUqdRHuL
XXb4zO96ftdNT7mneSkImRBhQbi6XSwLaJhW+Gm6Mkh/1/
KdbwF+pgKT2JmhPA+QDYhGENJpN601mjFLojOm9Aw1Y0AGmcOK6L80ESzULq3yvRWM
rmyHEATN0fOVrzFkwasyLujWd/+HedfgWtgaTg==
```

- **v=1**: means the format complies with DKIM version 1 (the current one).

- **a=rsa-sha256**: means that the algorithm used to compute the hashes is SHA-256. SHA-1 is also supported.
- **c=relaxed/relaxed**: means that the canonicalization used for the headers and the body is 'relaxed'. Canonicalization is the beautifying process applied to the texts before the hash is computed. *Simple* means no change (except deleting blank lines), *relaxed* means that the header names are converted to lowercase, extraneous spaces are deleted...
- **d=outlook.com**: this is the original sending domain from the From: header. It will be used to retrieve the DNS DKIM record.
- **s=selector1**: this is a name that must be prepended to `_domainkey.<domain>` to find the DNS DKIM record. A domain can have multiple DKIM records, they must be distinguishable uniquely by their selector.
- **h=From:Date...**: this is the list of headers that will be used to compute the header hashes, and therefore the headers that will be protected by the signature. For protection to be really effective, it should contain at least the *From:* and *To:* headers.
- **bh=J5...**: this is the hash of the canonicalized body part of the email.
- **b=OSRH...**: this is the signature, i.e. the result of the encryption by the private key of a value composed of the domain, the selector, and the hashing value obtained by hashing the headers and the hashed body. In short, the signature is obtained by the following actions:
  - body-hash = hash(canonicalized body)
  - data-hash = hash(headers in list, DKIM-Signature header name, body-hash)
  - signature = crypt(domain, selector, data-hash)The signature is converted to base64.

Other tags can be used, but these are the most common.

You can find the complete syntax of the DKIM headers and records in [RFC 6376](#).

## Setting up DKIM for a domain

A DKIM record is a DNS (Domain Name System) TXT record containing the public key and optionally the key type (the default is a RSA key).

The general syntax of an DKIM record is the following:

```
<selector>._domainkey.<domain> TXT "v=DKIM1; k=rsa; p=<public key in base64 representation>"
```

Usually, your email or domain provider provides an easy interface to create your DKIM records.

Otherwise the [Easydmarc](#) site offers an easy DKIM record generator and some explanation.

Note that DKIM does not require the setup of a complex public key infrastructure; a simple public/private key pair is needed. Of course, you must protect your private key like your crown jewels.

## Finding the DKIM record for a domain

As the DKIM record is a DNS TXT record, you can get it with the following commands:

```
dig -t txt <selector>._domainkey.<domain>
nslookup -ty=txt <selector>._domainkey.<domain>
```

Example: if you receive a mail with the following DKIM-Signature header:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=mail.datanews.be; s=sim; x=1712235864; i=@mail.datanews.be;
h=from:to:subject:date:reply-to:message-id:list-unsubscribe: list-
unsubscribe-post:feedback-id:list-id:mime-version: content-type;
bh=K2G3f0De2u9k7cjGRlQb/DT4b3UjMOTHgwV3JhL/n5g=;
b=MLyccGY84pMjl9fJ685sn2N/dTjKFIauN8CuFgxReCULTGtAgk7zmx87WAMNon
6htQ4d52+bPNMXedtP3mc1HkZdN17903DI/vFrqQV2m3xDDQj/EGef3aPaW8abxC
t1qSyXm07xrTpuhxx42LYIXvQay27QTbZ3BiQcWVi0Wk5HP3WZGmFVndy7ak4wgv
Hzsa/1x98z6hhEQEEEecSkPcj5+/TQ1izgVnpmoordUsGkx+P3gjbBPqk3615FD+
g81wW+SfuKTV7KmQAaGKwoUZHvm1MI5wh6zfmbE41/nynC15jAT8pzeWdwg1LTa1
7W9RcVED1V1CI02AntmSeNgA==
```

you have to lookup the following DNS TXT record: *sim.\_domainkey.mail.datanews.be*.

```
nslookup -ty=txt sim._domainkey.mail.datanews.be
Server: 9.9.9.9
Address: 9.9.9.9#53
Non-authoritative answer:
sim._domainkey.mail.datanews.be text = "k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAo9TT29ItqqnMwOHdMKv3
jsVoG7UZmVhm/VsXvxBFdCCjM/
t8160vNhbmtSNwNRbSMM8AzH0005qIFKLeF0Kqe+hVv15yJZ8AQTuU41JxqEM/
1FpMOTJ/
+IqWhzCdu33GWGdA3wYx8Nt19gLno7wY5I6PDBJvaiPiXn3uYNwwxaTu38UXYbqbny
P0jh0dmiGapk+ZQj5szK"
"SzNzZJ9R9ymtKsz2mKe0bjsqLiNhK1oDF0JUxsN4qwwED8k/e41nnmALepyWuSMNk
2vxW+uWdm2eA0RyljrC+I0DabF0qlfM+GJT01jgYrKr4YVsVw0ID0sujbh/
zWcW0yDszRAYrZBQIDAQAB"
```

You can also use the following free websites to find DKIM records:

- [MXToolbox](#)
- [EasyDmarc](#)

## Checking DKIM results in email headers

The DKIM protocol adds *Authenticated-Results*: headers in the emails it processes.

The general syntax is:

```
Authenticated-Results: <authenticating server> dkim=<result>  
<explanation of result with list of checked headers>
```

where <result> is pass or fail.

Let's check a real world mail header. This is an email sent from *pltrash2@outlook.com* to *pltrash2@gmail.com*. The DKIM-Signature is written by the *outlook.com* mail server (Microsoft), and is verified by the *gmail.com* server (Google).

```
Delivered-To: pltrash2@gmail.com  
Received: by 2002:a05:7412:220e:b0:106:1c01:d29c with SMTP id  
r14csp30940rda;  
Fri, 29 Mar 2024 11:16:11 -0700 (PDT)  
X-Google-Smtp-Source:  
AGHT+IHZ0MeAmsne8D6AaAPxBy7Y8L0KDX+Zfz95KJwiNu/N/Ws1kzA3nIeS8dp707  
ySuPIjX5yJ  
X-Received: by 2002:a05:6870:b28c:b0:22a:1e39:8bfa with SMTP id  
c12-20020a056870b28c00b0022a1e398bfamr3114970oao.25.1711736171497;  
Fri, 29 Mar 2024 11:16:11 -0700 (PDT)  
ARC-Seal: i=2; a=rsa-sha256; t=1711736171; cv=pass;  
d=google.com; s=arc-20160816;  
b=0WiDEJ21sPKPd9yXUqzW51MsBJu+Q8DXae45pt0tv/  
FnQD8DI4t4fIOXQ908RRDEJYK  
EkmNeq8BnqNvwTVNCzXrGsBcpT5c+0ALq7hMipt4QpVjQFj29hd4/  
b4kt5yuAdr00heY  
OBsvG7YNBRcAHvoF5+BtV41/Ch4A6ROLzVyh/  
JPIBuAPWuh4Q71RI2ymGFR1ex5ub0sh  
MG86oyJY33d9jPBj5M7Xjmo4TkrQbdZaw3ia3cJkjNsIoS0+gt5VAtrR3GStmHjZ7Y  
Un  
wRG70R9BAU6gio3ymLydZTa92qwaNfBot3KSgV2XsuUuUb1y31ZiPotFGrwCF3CqHw  
et  
e3oQ==  
ARC-Message-Signature: i=2; a=rsa-sha256; c=relaxed/relaxed;  
d=google.com; s=arc-20160816;  
h=mime-version:content-transfer-encoding:msip_labels:content-  
language  
:accept-language:message-id:date:thread-index:thread-topic:subject  
:to:from:dkim-signature;  
bh=J5xVXlIPB8b3aQVmIOVS4pAqIH4o0aHCb3LgLetuS1s=;  
fh=H8fS/F1Xi7k6c76u5mat11UzewD7stRXC+xTg8ayz9I=;
```



```
b=CTETjwm02n/YObWmGhbcsHv7Hqixz8dVbmIRgJMzdoIiUcDI/xK/
J6YoN07zaonWo1
5WcbThwZipLC/
bK83NqID0duQ6f24hwNqfh9M4xyMAxH7xLDfBRPxF7YBY3diKqnhn29
QSPX8kVDC4jay4bCCdiGHVvgHOU+wrJr+AynAoU8SwKxH/
zxNvcJpjxdxB58ZWPvXV7G
tMn87T79KGDVYZidhebuB2EqX49sUzsnk3HfyZyc9rILcJSJnzcvI4tiPzzpex9JWp
81
Juvwc9f0eITu0jEGTsKv0RwYPkKTm09/
vbk+gUFFbJneAlwJxkK1loqUxfH1atRKHKPp
r5dA==;
dara=google.com
ARC-Authentication-Results: i=2; mx.google.com;
dkim=pass header.i=@outlook.com header.s=selector1
header.b=OSRH95fo;
arc=pass (i=1);
spf=pass (google.com: domain of pltrash2@outlook.com designates
2a01:111:f403:2e0d::800 as permitted sender)
smtp.mailfrom=pltrash2@outlook.com;
dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=outlook.com
Return-Path: <pltrash2@outlook.com>
Received: from EUR03-DBA-obe.outbound.protection.outlook.com
(mail-dbaeur03olk20800.outbound.protection.outlook.com.
[2a01:111:f403:2e0d::800])
by mx.google.com with ESMTPS id ec27-
20020a05622a5b9b00b00432c7306e0csi1006434qtb.4.2024.03.29.11.16.11
for <pltrash2@gmail.com>
(version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256
bits=128/128);
Fri, 29 Mar 2024 11:16:11 -0700 (PDT)
Received-SPF: pass (google.com: domain of pltrash2@outlook.com
designates 2a01:111:f403:2e0d::800 as permitted sender) client-
ip=2a01:111:f403:2e0d::800;
Authentication-Results: mx.google.com;
dkim=pass header.i=@outlook.com header.s=selector1
header.b=OSRH95fo;
arc=pass (i=1);
spf=pass (google.com: domain of pltrash2@outlook.com designates
2a01:111:f403:2e0d::800 as permitted sender)
smtp.mailfrom=pltrash2@outlook.com;
dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=outlook.com
ARC-Seal: i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com;
cv=none;
```

b=RbRY3osi22pGFg1gRVysVuiL6or4+LRx1xnYftE1PVQeCAxFeucoGp9q7PKqM1BF  
tsrq2gGnAXMPpD8m/i3gBIrgbMuZdw5Cbo9YMIaAch2c0D6xyVr/  
gcphYLQgqdNRts4rQscDGgbhCFSe/  
7chHHJUiuhe9rGSaV7V010n6TdfS8FAYNLoi joR1+hJNQKxyYgizTI6q2e5qtIO7hb  
dUo3Qu25pYEiAPQockmViNBm/  
o68DtSD+CYdBE0Ed6FLiMMin8o+ixnj2UnVNFO+4WZF2godMTOMp5VbIAHKuTl2rhR  
5SBUSWk8H0sp6dQAYDR2YymV0wfCXq1e+AzAmqFA==  
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed;  
d=microsoft.com; s=arcselector9901; h=From:Date:Subject:Message-  
ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-MessageData-  
ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-Exchange-  
AntiSpam-MessageData-1;  
bh=J5xVXlIPB8b3aQVmIOVS4pAqIH4o0aHCb3LgLetuS1s=;  
b=GoCHS+cXfoc7vMbVtJx0hRue1MoRtNFTGC1ek6UvKwsPCoIL7uRUP+aUA0/LwqzG  
5Gzh6qzWzjJ9+zI1l8Swq3gF+FK289PUzDuWMsTC3TEnyb+ththbk66L17It1E6wQS  
/  
TKBALG2VHxRpv907E27v1q+8DxJ1vVXkYicZcjJqRXNaDapbbXuBGJaDWSB2TRjXwS  
+aikpc5mHqC+o7mEZ8RB06wldhd0uTin9o1goJSRr0i5d7fcLxPwfAg2rIXeoR+Th3  
P2gVKPx0mZlDj//+ztITVbFr5ZyBp0shks/2a2+JklApujzDx7hsweexQLd/Y8v/  
BjNmJXR476RFLNw==  
ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=none;  
dmarc=none; dkim=none; arc=none  
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
d=outlook.com; s=selector1; h=From:Date:Subject:Message-  
ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;  
bh=J5xVXlIPB8b3aQVmIOVS4pAqIH4o0aHCb3LgLetuS1s=;  
b=OSRH95fo/UTLgZrvDc05B8HF306wPd5WZ76iZu9v0tRVgAXgPJEWjUJsqcmxtRnn  
4ZnKhEpEfBx16XLMbbIebYfAK7NPdchpSv2yAfpqjmCkLotnvG/r1tpuz9qqW/  
6vxdzxCgvoxw1DPpFA+Qh0Zs95P5k86h7w6EgXpsEh3jx5rU4eR0qIRoSOTUqdRHuL  
XXb4z096ftdNT7mneSkImRBhQbi6XSwLaJhW+Gm6Mkh/1/  
KdbwF+pgKT2JmhPA+QDYhGENJpN601mjFLojOm9Aw1Y0AGmc0K6L80ESzULq3yvRWM  
rmyHEATN0fOVRzFkwasyLujWd/+HedfgWtgaTg==  
Received: from AS8P189MB1621.EURP189.PROD.OUTLOOK.COM  
(2603:10a6:20b:393::12) by GV1P189MB2107.EURP189.PROD.OUTLOOK.COM  
(2603:10a6:150:57::19) with Microsoft SMTP Server (version=TLS1\_2,  
cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.7409.39;  
Fri, 29 Mar 2024 18:16:09 +0000  
Received: from AS8P189MB1621.EURP189.PROD.OUTLOOK.COM  
([fe80::c7fb:d192:40d8:2f36]) by  
AS8P189MB1621.EURP189.PROD.OUTLOOK.COM  
([fe80::c7fb:d192:40d8:2f36%3]) with mapi id 15.20.7409.042; Fri,  
29 Mar 2024 18:16:09 +0000  
From: Philippe Leclerc <pltrash2@outlook.com>



To: pl\_trash <pltrash2@gmail.com>  
Subject: DKIM test email  
Thread-Topic: DKIM test email  
Thread-Index: AQHaggUsJ9Gmfe8zpEiMmMD/JwvuoQ==  
Date: Fri, 29 Mar 2024 18:16:09 +0000  
Message-ID:  
<AS8P189MB1621D4551CA36F99656602B78E3A2@AS8P189MB1621.EURP189.PROD  
.OUTLOOK.COM>  
Accept-Language: en-GB, en-US  
Content-Language: en-GB  
X-MS-Has-Attach:  
X-MS-TNEF-Correlator:  
msip\_labels:  
x-ms-exchange-messagesentrepresentingtype: 1  
x-tmn:  
[jzXPG0c9g+ZXCMDUkE1sJnz8V6w5/V0HjiSZ7Yk8wbBh49VldkKgt0Jy8bBY4Cbw]  
x-ms-publictraffictype: Email  
x-ms-traffictypediagnostic: AS8P189MB1621:EE\_|GV1P189MB2107:EE\_  
x-ms-office365-filtering-correlation-id: 13f067fd-5979-4993-8e46-  
08dc501c4f1d  
x-microsoft-antispam: BCL:0;  
x-microsoft-antispam-message-info:  
0MU0xJBN710avHpn9oTutzg/5eAygeMDZ0V1oZOHEphHEMiSgxNZTt0Mibe6iqn76N  
+qQRWDR+mBeMdAEQApPbPlI7I/vu/k3/w0ZWJ091Cn9N1/ZJQ5E46hx0c+B/  
vYE0HrILa0sPLSViH0s0M23MKh7TmznSdCBQuFeih8dvqbFPdpycGL2GZSBxA60WHC  
1kLUdySCZWydu1560jjxIRH6XVtzeNn6kcfHJrHiLvOU1L3UQM5j7nSQU1MKJHc2zh  
yv9VZ2kAqH6bJZiXk7avffyuZQy30v07mtLq0Xqd2fmLekMMuKp/  
KUoRht5Ibe9TqqaeQJDT0hkjtPbLnB1Svwz9DgZVIXss1zVENS7dhXiBBGaiF2190a  
x1YaMnw4S0iuDEfwZ51B9hc1Rkz1sX70rZGnRKi6Fztj1CodgAb0Qy/  
vtZLDs6NK0Epc0NAZLb3JRTGqJEs93TVnBFXYkyi iPtUKmQwoZfWm+a5dPRcigCpbF  
CkoWNLijVhA5U7gEGIk3CRVLGMyBOy0kKFvSI+X8xPue3bq1VEpsnzoIWPFIaIhutO  
KMHfqtUMisNj  
x-ms-exchange-antispam-messagedata-chunkcount: 1  
x-ms-exchange-antispam-messagedata-0:  
/U+Ey2sZ+my0qtdTC4Ye4oCsQHDecnA4asFpK+ujg4xc3UbaP03db6Uth9/jZJctDT  
h33z8FyNQFeHDhJRdQ2FMU/QN2pII8Pb1SYsUWRo4SA/  
cocAb7Sd5W0TyAZaUGzC2xHvnsQbwKTzWSS6NzQNY25QnZrNjQIW40N7FE/  
Wg4UexGy2ryYA4dwHUVSF5m/HfrHQ9qppcvo/  
3T7mp0FH6TqpNt+s+Cmfm4t1xnn1iMt7+wnMt4J6Se+RcMqjGmZNZoRYp1Ep4zc10P  
gbiJVKYpQi9G9AayT5b69avJko10A7XzPGRIjXUge60xbkIsHQET4PAAtnTCeXJX/  
eJXPbR8NDR+s3D7TB7ZgLABoEJQNuqXowQcyuPvfz68diM7c94T18YyCKDsUjIbbgJ  
zNrT9dSS40HVUEVaCnrX+2WyakHdd10jwbWSvWEvLpfKQ6MwuESq5sfXnuOr7e+Kk6  
Wxtmg15yKYzCfcAKYkoMgNkppEVNGxX/

```
7ko8Ik0hMH4Ik4j8onI71k5L+zdYs4eiDSFo0Y8yU2H7wiyZVdcYEe81qDQSi5UIxX
f13t6zP7tgArFUh2qrKjtn9UTGyJuuI2ot6aeN1wKJNStYWn0Defr+g2ACcCcv9Ed5
sqMz8kFp1UX92RDCT+v7b8TTjUap3cmVrtP/
XiGXCGFuiZwenm1xJ4t1GBv8dd6anEytoQByLHGj0v1Z973uJepuehkkNDtvJObqmK
DMEGcjFIotwrbzXmY39oYW6lQt+czeV+IV40+wNftGBODNyvs4a1n6mx9jnzCSKwFA
9eWHyy54R4FqCAxAnnpGoIUZ3tzErnpvprjGLWDYHfnE1D0U3rSiWIgpwtimIzIqT6
XHBzfrIL+OAjIgJ4+GycgaHPFGDZZOfQYT0/
buP+d83+MkupkDyapHoD8fT2eYRYq+J06IQgrJ6XTdLnsa+aCxR0tc7u1HmAv+onIX
K0lWOH88XrmD7CzK4647n8TGPwCULP358TfieTKW0GqZttrFbRHbslFRv4WPh0Ppot
D+YA/Ng433+y4fKCNg6oeuVPNJARhM/
v03xSX+ihZXUguIi+YgVXrQgN4HpHk3E+7/SfkHeZgxnhdE15t/xpaND1P7E/
1y4FOj40uEp0iJbDjYSynADD19D1Hw8JGitk7zLJIBuY4iIjLBt31z1NrCfDKfyFxn
5HSVRWJ8yZr7vSLbYuJA39W0vRPn7sWMKyRGI67I3vJFssJwJ7UowpBynSJ9/
r+b6rEAhlRrB1YiyR98by91VWnp0lLWANTvMm9xfeFE629EQ==
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
MIME-Version: 1.0
X-OriginatorOrg: outlook.com
X-MS-Exchange-CrossTenant-AuthAs: Internal
X-MS-Exchange-CrossTenant-AuthSource:
AS8P189MB1621.EURP189.PROD.OUTLOOK.COM
X-MS-Exchange-CrossTenant-RMS-PersistedConsumerOrg: 00000000-0000-
0000-0000-000000000000
X-MS-Exchange-CrossTenant-Network-Message-Id: 13f067fd-5979-4993-
8e46-08dc501c4f1d
X-MS-Exchange-CrossTenant-rms-persistedconsumerorg: 00000000-0000-
0000-0000-000000000000
X-MS-Exchange-CrossTenant-originalarrivaltime: 29 Mar 2024
18:16:09.5991 (UTC)
X-MS-Exchange-CrossTenant-fromentityheader: Hosted
X-MS-Exchange-CrossTenant-id: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaaa
X-MS-Exchange-Transport-CrossTenantHeadersStamped: GV1P189MB2107

DKIM test email.
```

The DKIM-Signature header is:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=outlook.com; s=selector1; h=From:Date:Subject:Message-
ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;
bh=J5xVXlIPB8b3aQVmIOVS4pAqIH4o0aHCb3LgLetuS1s=;
b=OSRH95fo/UTLgZrvDcO5B8HF306wPd5WZ76iZu9v0tRVgAXgPJEWjUJsqcmxtRnn
```

```
4ZnKhEpEfBx16XLMBbIebYfAK7NPdchpSv2yAfpqjmCkLotnvG/r1tpuz9qqW/  
6vxdzxCGvoxw1DPpFA+Qh0Zs95P5k86h7w6EgXpsEh3jx5rU4eR0qIRoSOTUqdRHuL  
XXb4z096ftdNT7mneSkImRBhQbi6XSwLaJhW+Gm6Mkh/1/  
KdbwF+pgKT2JmhPA+QDYhGENJpN601mjFLojOm9Aw1Y0AGmc0K6L80ESzULq3yvRWM  
rmyHEATN0fOVrzFkwasyLujWd/+HedfgWtgaTg==
```

The Authenticated-Results header is:

```
Authentication-Results: mx.google.com;  
flyordie.com text = "v=spf1 ip4:82.192.93.216 ip4:82.192.93.217  
ip4:82.192.93.218 ip4:208.167.241.84 -all"  
Authentication-Results: mx.google.com;  
dkim=pass header.i=@outlook.com header.s=selector1  
header.b=OSRH95fo;  
arc=pass (i=1);  
spf=pass (google.com: domain of pltrash2@outlook.com designates  
2a01:111:f403:2e0d::800 as permitted sender)  
smtp.mailfrom=pltrash2@outlook.com;  
dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=outlook.com
```

The verifier (or authenticating server) is *mx.google.com*, the Gmail mail server.

The result is pass, the domain and selector used for retrieving the DNS DKIM record are *outlook.com* and *selector1*.

Let's check the *selector1.\_domainkey.outlook.com* TXT record:

```
nslookup -ty=txt selector1._domainkey.outlook.com  
;; Truncated, retrying in TCP mode.  
Server: 9.9.9.9  
Address: 9.9.9.9#53  
Non-authoritative answer:  
selector1._domainkey.outlook.com canonical name =  
selector1._domainkey.outbound.protection.outlook.com.  
selector1._domainkey.outbound.protection.outlook.com text =  
"v=DKIM1;k=rsa;p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA vWykt  
rIL8DO/+UGvMbv7cPd/Xogpbs7pgVw8y9ld06AAMmg8+ijEN1/  
c7Fb1MfKM7uG3LMwAr0dVVKyM+mbkoX2k5L7lsROQr0Z9gGSpu7xrnZ0a58+/  
pIhd2Xk/  
DFPpa5+TKbWodbsSZPRN8z0RY5x59jdzSc1X1EyN9mEZdm0iKTsOP6A7vQxfSya9jg  
5"  
"N81dfNNvP7HnWejMMsKyIMrXptxOhIBuEYH67JDe98QgX14oHvGM2Uz53if/SW8MF  
09rYh9sp4ZsaWLIg6T343Jz1btrsGRGCDJ9JPpxRWZimtZ+Up/B1KzT6sCCrBihb/  
Bi3pZiEBB4Ui/vruL5RCQIDAQAB;n=2048,1452627113,1468351913"
```

In this case, the DNS DKIM record is a CNAME or an alias, pointing to the real record *selector1.\_domainkey.outbound.protection.outlook.com*.

In this one, we can find the public key used by google to decrypt the signature.

**Remember:** DKIM checks the entire email has not been modified, and ensures that it has been signed by a server belonging to the domain in the *From:* header.