E-Mail Security

SPF, DKIM, DMARC

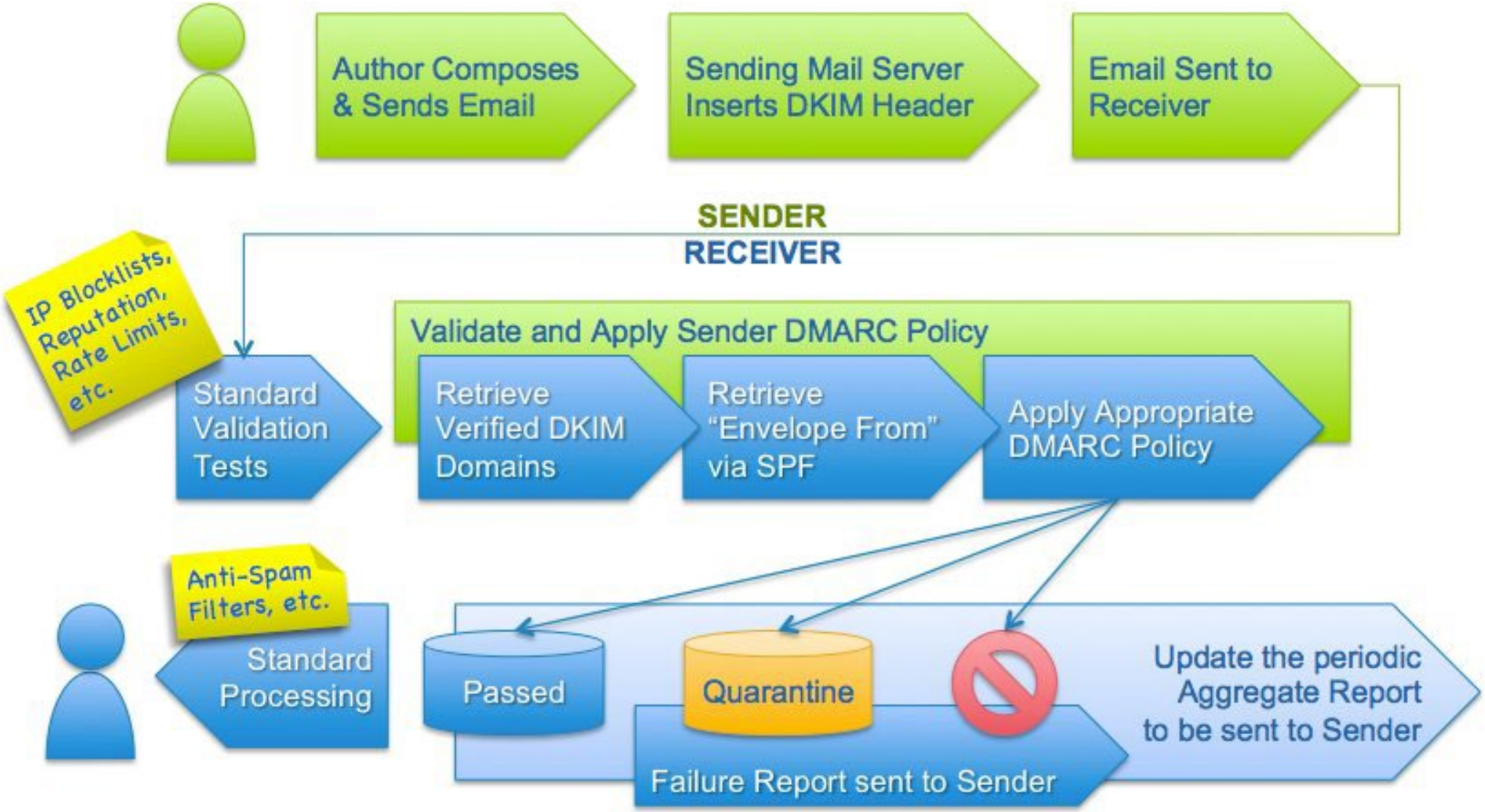
Mail Security Features

SPF (Sender Policy Framework)
DKIM (DomainKeys Identified Mail)
DMARC (Domain-based Message Authentication, Reporting, and Conformance)

DKIM, SPF, and DMARC are all standards that enable different aspects of email authentication. They address complementary issues.

- **SPF** allows senders to define which IP addresses are allowed to send mail for a particular domain.
- **DKIM** provides an encryption key and digital signature that verifies that an email message was not faked or altered.
- **DMARC** unifies the SPF and DKIM authentication mechanisms into a common framework and allows domain owners to declare how they would like email from that domain to be handled if it fails an authorization test.

SPF, DKIM, DMARC



Source: https://dmarc.org/overview/

SPF

https://tools.sparkpost.com/spf/builder

SPF for Compass Security und Hacking-Lab

ibuetler — -bash — 122×21

```
Ivans-MacBook-Pro:~ ibuetler$ dig -t txt compass-security.com +noall +answer

; <<>> DiG 9.10.6 <<>> -t txt compass-security.com +noall +answer
;; global options: +cmd
compass-security.com.   70      IN      TXT     "v=spf1 mx ip4:193.135.215.47/32 ip4:193.135.215.55/32 -all"
compass-security.com.   70      IN      TXT     "MS=ms81325037"
Ivans-MacBook-Pro:~ ibuetler$
```

ibuetler — -bash — 156×21

```
Ivans-MacBook-Pro:~ ibuetler$ dig -t txt hacking-lab.com +noall +answer

; <<>> DiG 9.10.6 <<>> -t txt hacking-lab.com +noall +answer
;; global options: +cmd
hacking-lab.com.        300     IN      TXT     "google-site-verification=BecZnpotgns1Kt1KHKQsmmIH4rNR3fpc_HQRfNYvam8"
hacking-lab.com.        300     IN      TXT     "v=spf1 mx ip4:80.74.154.112/32 ip4:80.74.154.113/32 ip4:80.74.154.114/32 include:spf.smtp2go.com -all"
Ivans-MacBook-Pro:~ ibuetler$
```

SPF Query using dig +short

dig +short hacking-lab.com txt

root@global:/var/www/largefiles/livecd/daily

```
[root@global daily]# dig +short hacking-lab.com txt
"google-site-verification=BecZnpotgns1Kt1KHKQsmmIH4rNR3fpc_HQRfNYvam8"
"v=spf1 mx ip4:80.74.154.112/32 ip4:80.74.154.113/32 ip4:80.74.154.114/32 ip4:159.89.215.106/32 ip4:134.209.251.22/32 include:spf.smtp2go.com -all"
[root@global daily]#
```

SPF (DNS Entry)

https://mxtoolbox.com/SuperTool.aspx?action=spf%3acompass-security.com&run=toolpage

Certificate Transpar...

MX TOOLBOX

MX Lookup | Blacklists | Diagnostics | Domain Health | Analyze Headers | Free Monitoring | DMARC | Investigator | DNS Lookup | More

SuperTool Beta7

compass-security.com | SPF Record Lookup

spf:compass-security.com Find Problems | Solve Email Delivery Problems

```
v=spf1 mx ip4:193.135.215.47/32 ip4:193.135.215.55/32 -all
```

Prefix	Type	Value	PrefixDesc	Description
v	version	spf1		The SPF record version
+	mx		Pass	Match if IP is one of the MX hosts for given domain name
+	ip4	193.135.215.47/32	Pass	Match if IP is in the given range
+	ip4	193.135.215.55/32	Pass	Match if IP is in the given range
-	all		Fail	Always matches. It goes at the end of your record.

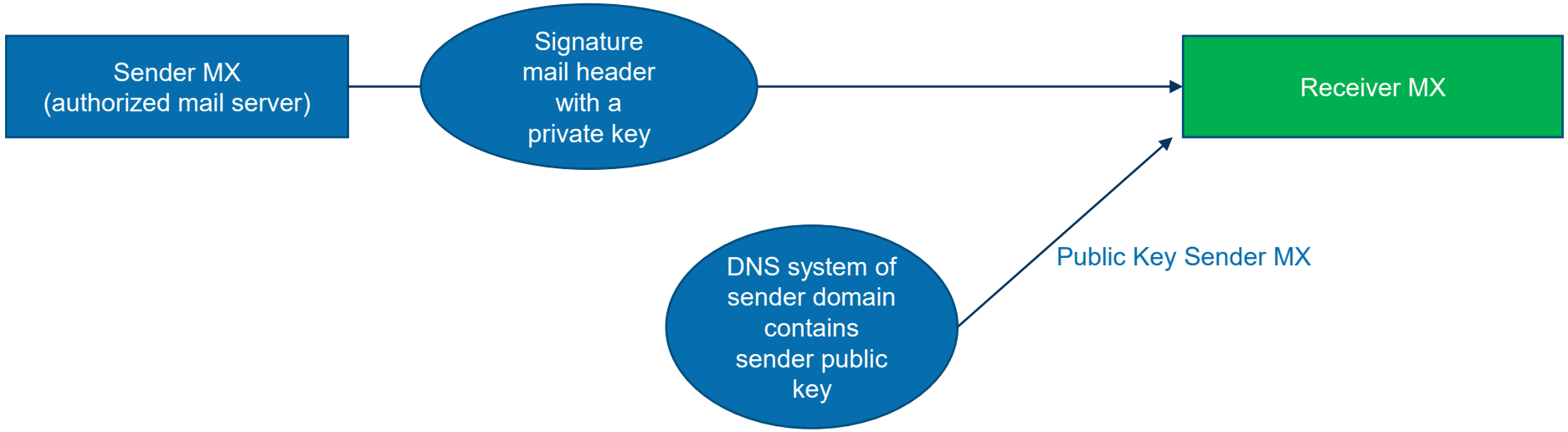
	Test	Result
✓	DNS Record Published	DNS Record found
✓	SPF Record Published	SPF Record found
✓	SPF Record Deprecated	No deprecated records found
✓	SPF Multiple Records	Less than two records found
✓	SPF Contains characters after ALL	No items after 'ALL'.
✓	SPF Syntax Check	The record is valid
✓	SPF Included Lookups	Number of included lookups is OK
✓	SPF Type PTR Check	No type PTR found
✓	SPF Void Lookups	Number of void lookups is OK
✓	SPF Exceeds Maximum Character Limit	String lengths are OK.

DKIM

DKIM

DomainKeys Identified Mail, or DKIM, is a technical standard that helps protect email senders and recipients from spam, spoofing, and phishing. It is a form of email authentication that allows an organization to claim responsibility for a message in a way that can be validated by the recipient.

Specifically, it uses an approach called “public key cryptography” to verify that an email message was sent from an authorized mail server, in order to detect forgery and to prevent delivery of harmful email like spam. It supplements SMTP, the basic protocol used to send email, because it does not itself include any authentication mechanisms.



DKIM how it works

It works by adding a digital signature to the headers of an email message. That signature can be validated against a public cryptographic key in the organization's Domain Name System (DNS) records. In general terms, the process works like this:

A domain owner publishes a cryptographic public key as a specially-formatted TXT record in the domain's overall DNS records.

When a mail message is sent by an outbound mail server, the server generates and attaches a unique DKIM signature header to the message. This header includes two cryptographic hashes, one of specified headers, and one of the message body (or part of it). The header contains information about how the signature was generated.

When an inbound mail server receives an incoming email, it looks up the sender's public DKIM key in DNS. The inbound server uses this key to decrypt the signature and compare it against a freshly computed version. If the two values match, the message can be proved to authentic and unaltered in transit.

DKIM with «hacking-lab.com» domain

outlook-headers.txt - Editor

Datei Bearbeiten Format Ansicht Hilfe

```
Received: from Wapiti.compass-security.com (10.4.10.10) by
 Wapiti.compass-security.com (10.4.10.10) with Microsoft SMTP Server (TLS) id
 15.0.1473.3 via Mailbox Transport; Mon, 17 Feb 2020 09:31:37 +0100
Received: from Wapiti.compass-security.com (10.4.10.10) by
 Wapiti.compass-security.com (10.4.10.10) with Microsoft SMTP Server (TLS) id
 15.0.1473.3; Mon, 17 Feb 2020 09:31:37 +0100
Received: from mx2.compass-security.com (62.2.85.154) by
 Wapiti.compass-security.com (10.4.10.10) with Microsoft SMTP Server (TLS) id
 15.0.1473.3 via Frontend Transport; Mon, 17 Feb 2020 09:31:37 +0100
Received: from hacking-lab.com (postfix.infra.hacking-lab.com [134.209.251.22])
        by mx2.compass-security.com (Postfix) with ESMTP id C748657CE
        for <ivan.buetler@compass-security.com>; Mon, 17 Feb 2020 09:36:21 +0100 (CET)
DKIM-Filter: OpenDKIM Filter v2.11.0 mx2.compass-security.com C748657CE
Authentication-Results: mx2.compass-security.com;
        dkim=pass (1024-bit key) header.d=hacking-lab.com header.i=@hacking-lab.com header.b="iWCpxriV"
Received: from infra.hacking-lab.com (unknown [134.209.251.22])
        by hacking-lab.com (Postfix) with ESMTPSA id B2FDE2E618
        for <ivan.buetler@compass-security.com>; Mon, 17 Feb 2020 08:31:34 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=hacking-lab.com;
        s=mail; t=1581928294;
        bh=fQVBcH3ZdUmUS/sVXND23wnaDaPO+2HC/QwnvGZVHNk=;
        h=From:To:Subject:From;
        b=iWCpxriV5CdMyZARtDWlYQG7LZQBQPvO/8uico+jZpVK/nb567hWYfu//NFEhbnUk
         ATGWkZ5gUdWVsIYd5zRco/s+eiDsHBlOvQwZH+/eXcNk3L7+3rLpiY6aWIKJKTWkqX
         J0L7Fw1JaIUZjHErEPEVp+YNOzsDlxVWGtkc+S5M=
From: ivan.buetler@hacking-lab.com
To: ivan.buetler@compass-security.com
Subject: Test Message from smtptest at 2020-02-17 08:31:34
```

mail._domainkey.hacking-lab.com

DKIM

DNS query public key of a sender MX

root@ncjonmx02:/etc/postfix

```
[root@ncjonmx02 postfix]# dig +short mail._domainkey.hacking-lab.com txt
"v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCovtl8Pg23mrQcmx385mJNqbjy+SSv8feDrm/rX0nDTLuuO9clk+FFTupS0wuWRDU
gQ4WTsNUG5AP98VvIkyoZQftwlhFGYMs47O6j+yRzN4/9wz+W8bMAhS2g9pU7AGI4BkSas75n2MHRnZHhMUCyN432kSRdQ9hbZtlWTtb7nQIDAQAB"
[root@ncjonmx02 postfix]#
```

SMTP Server Log (DKIM validation)

```
Feb 17 09:35:13 ncjonmx02 opendkim[1203]: CBFB3B3: postfix.infra.hacking-lab.com [134.209.251.22] not internal
Feb 17 09:35:13 ncjonmx02 opendkim[1203]: CBFB3B3: not authenticated
Feb 17 09:35:13 ncjonmx02 opendkim[1203]: CBFB3B3: DKIM verification successful
```

DKIM with «GMAIL» domain

outlook-headers.txt - Editor

Datei Bearbeiten Format Ansicht Hilfe

```
Received: from Wapiti.compass-security.com (10.4.10.10) by
 Wapiti.compass-security.com (10.4.10.10) with Microsoft SMTP Server (TLS) id
 15.0.1473.3 via Mailbox Transport; Mon, 17 Feb 2020 09:01:06 +0100
Received: from Wapiti.compass-security.com (10.4.10.10) by
 Wapiti.compass-security.com (10.4.10.10) with Microsoft SMTP Server (TLS) id
 15.0.1473.3; Mon, 17 Feb 2020 09:01:06 +0100
Received: from mx1.compass-security.com (193.135.215.41) by
 Wapiti.compass-security.com (10.4.10.10) with Microsoft SMTP Server (TLS) id
 15.0.1473.3 via Frontend Transport; Mon, 17 Feb 2020 09:01:06 +0100
Received: from mail-wr1-f43.google.com (mail-wr1-f43.google.com [209.85.221.43])
        (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
        (No client certificate requested)
        by mx1.compass-security.com (Postfix) with ESMTPS id 20CF0AB
        for <ivan.buetler@compass-security.com>; Mon, 17 Feb 2020 09:01:05 +0100 (CET)
DKIM-Filter: OpenDKIM Filter v2.11.0 mx1.compass-security.com 20CF0AB
Authentication-Results: mx1.compass-security.com;
        dkim=pass (2048-bit key) header.d=gmail.com header.i=@gmail.com header.b="muU2eob/"
Received: by mail-wr1-f43.google.com with SMTP id w15so18418027wru.4
        for <ivan.buetler@compass-security.com>; Mon, 17 Feb 2020 00:01:05 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20161025;
        h=mime-version:from:date:message-id:subject:to;
        bh=rqeuHAUKkRSJAzGay2P6Es3P1IkGwr/CntjZpv0iiHY=;
        b=muU2eob/sn+bCAzH3E5PQAKweV8H3i2+elchuCL7149aj5NbN0vXO1996o38
         cS7ViX0ZGJaM+VExbMzMAyT41ojggdw3XOpIB5XjIT/5rfIH420yHOjvtEsENpu68/m
         +CPcEjGinkKNOHQVHhUniR2Qx6sgTFMZpBcwj6oO1nxPpZGzbqD61EGCRCq80uLvPhoO
         cTHO4rhXm0FuSNoE5dZRvrc58MfoMcJ+29r/vBlOJu/3RpabCFKbrIpSx4NN3cDeZJCq
         cCzLbg+NK0M2+Rq0E6a9ZD8OWW9UdHkZt/LzO1PxqZY/tZDt+uUkCJygN6eSiVnD1s7e
         6Ekg==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20161025;
        h=x-gm-message-state:mime-version:from:date:message-id:subject:to;
        bh=rqeuHAUKkRSJAzGay2P6Es3P1IkGwr/CntjZpv0iiHY=;
        b=alYOAZUcPhI3xbOt8sKMgEQ1upqgS32EyBVfRGg3bb5PH+0PafzvHKnhFcuFrb10e2
         WDTVIG/Avl4aEZu5C120mQp1tyMp5S8Dk81Rq3Aiu4vifnbCTFAAIU6OjswwV3uHx0lw
         TOd1IABC95PahDc8fe0niid6TZB38t6CPQzDvtbfE1JTUR6wUAaSkoHX7KnQdv6zkdPP
         hNKO8Q10NYF3vgb3whOo39ojCoE+KSt9oQiU+48oOwTYwMg+s1sdOTtV4QyDpiYuyuEP
         jaXRk7A4CPSaubDCybC1wHNRea0MOL0EvGv0zuO4yaaECeTZWJRKX5VPnIiY4BpRLIx/
         5PTg==
X-Gm-Message-State: APjAAAWYuhHvzzK0H8QwfI/RalSYnurHINsgMfoLlosw48d2znwmOnlZ
        BuSXvZ9M/mritKsDz+ojQTxgnnjVP12NL5/7MK0CkgDg
X-Google-Smtp-Source: APXvYqzMSWfeTS1FGkvSaJ3o4qFpFrs8GLLoiX9hh5v7QQnBxtfyOhLYQV5CtuaEtcpp3QjeDfMwRw1/SYwRpsUNRLg=
X-Received: by 2002:a5d:4cc9:: with SMTP id c9mr20328626wrt.70.1581926464523;
 Mon, 17 Feb 2020 00:01:04 -0800 (PST)
```

20161025._domainkey.google.com

DKIM «Google»

DNS query public key of a sender MX

root@ncjonmx02:/etc/postfix

```
[root@ncjonmx02 postfix]# dig +short 20161025._domainkey.google.com TXT
"k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwXNZFlj8sJPDleRjf9SPBNem0ik58kFlilClnUgKAttl9v7FX9hXJXPmLNhVtSKVZ8yr
uaeOZLeIxtgtkls8lzzIE5Mj0AiGn2wlFt4kYfqlDfYe95YLQHjynu4i7vjlTj" "ksf62btcCbL+3XhbK+oD5PlqYhXHWuzoKoEp5L4lCihgkONvU/oy7NNeE
6quqfF/y0YSLwF2WVA2Kd8L6R0Ar2dYT/3wZCFknI7xhvPqh9HNcIWBELGPwtXcsHbXlwvBlCgNQAUcdJrf2YWzAwqmZ564/lipLlIMklnafPJk75ktumVNz6O
RuIn3jbZWp9rRpnaeI9cu/8KfSKH2EY9QIDAQAB"
[root@ncjonmx02 postfix]#
```

SMTP Server Log (DKIM validation)

```
Feb 17 09:01:06 ncjonmx01 opendkim[1170]: 20CF0AB: mail-wr1-f43.google.com [209.85.221.43] not internal
Feb 17 09:01:06 ncjonmx01 opendkim[1170]: 20CF0AB: not authenticated
Feb 17 09:01:06 ncjonmx01 opendkim[1170]: 20CF0AB: DKIM verification successful
```

DMARC

DMARC policies are published in the DNS as text (TXT) resource records (RR) and announce what an email receiver should do with non-aligned mail it receives.

DMARC using «dig»

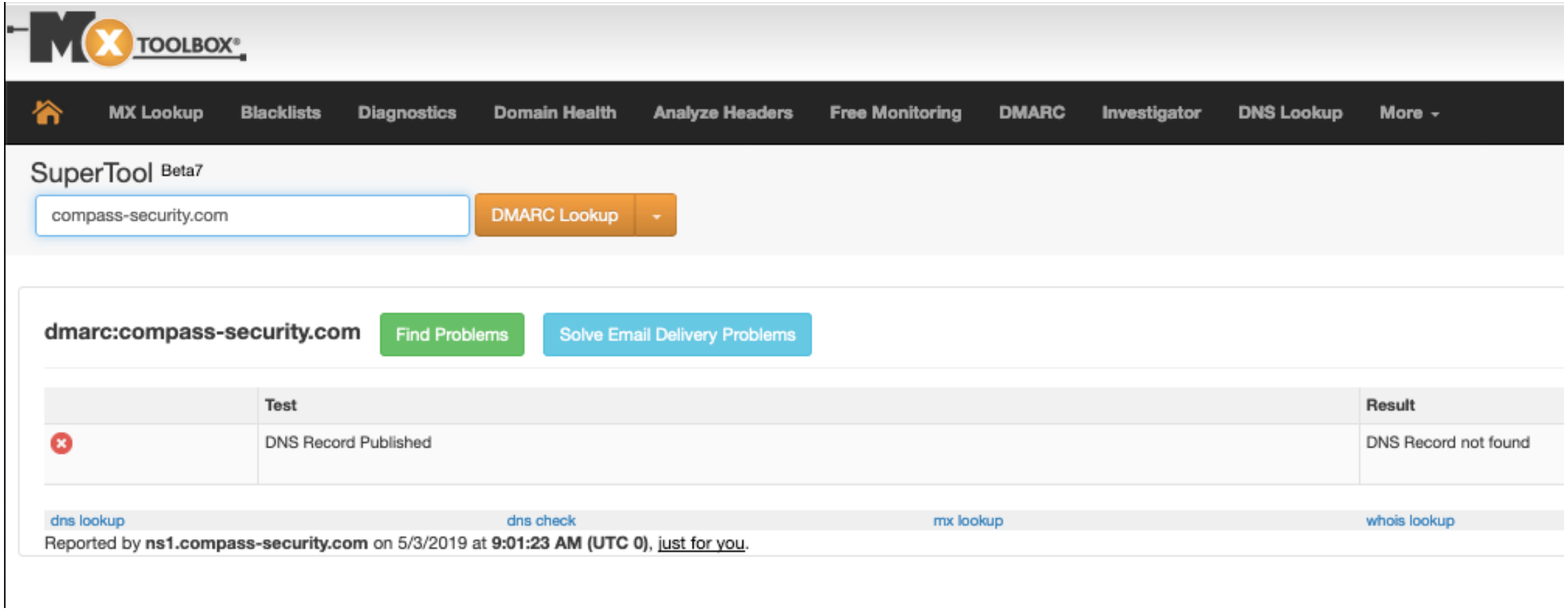
DMARC unifies the SPF and DKIM authentication mechanisms into a common framework and allows domain owners to declare how they would like email from that domain to be handled if it fails an authorization test.

```
ibuetler — -bash — 158×45
Ivans-MacBook-Pro:~ ibuetler$ dig -t txt _dmarc.hacking-lab.com +short
"v=DMARC1; p=none; rua=mailto:dmarc-reports-6b6568733237313030 0a@hacking-lab.com; ri=86400"
Ivans-MacBook-Pro:~ ibuetler$
```

Tag Name	Purpose	Sample
v	Protocol version	v=DMARC1
pct	Percentage of messages subjected to filtering	pct=20
ruf	Reporting URI for forensic reports	ruf=mailto:authfail@example.com
rua	Reporting URI of aggregate reports	rua=mailto:aggrep@example.com
p	Policy for organizational domain	p=quarantine
sp	Policy for subdomains of the OD	sp=reject
adkim	Alignment mode for DKIM	adkim=s
aspf	Alignment mode for SPF	aspf=r

DMARC not enabled for «compass-security.com»

https://mxtoolbox.com



DMARC is enabled for «hacking-lab.com»

https://mxtoolbox.com

MX TOOLBOX®

Upgrade | Delivery Center | Supertool | Monitoring

MX Lookup | Blacklists | Diagnostics | Domain Health | Analyze Headers | Free Monitoring | DMARC | Investigator | DNS Lookup | More

SuperTool Beta7

hacking-lab.com | DMARC Lookup

dmarc:hacking-lab.com | Find Problems | Solve Email Delivery Problems | dmarc

```
v=DMARC1; p=none; rua=mailto:dmarc-reports-6b65687332373130300a@hacking-lab.com; ri=86400
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	none	Policy	Policy to apply to email that fails the DMARC test. TagValue can be 'none', 'quarantine', or 'reject'.
rua	mailto:dmarc-reports-6b65687332373130300a@hacking-lab.com	Receivers	List of URIs for receivers to send XML feedback to. URIs are required to be added in the format of 'mailto:address@example.com'.
ri	86400	Reporting Interval	The reporting interval for how often you'd like to receive aggregate XML reports. You'll likely receive reports once a day regardless of this setting.

	Test	Result	
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
✓	DNS Record Published	DNS Record found	
✓	DMARC Record Published	DMARC Record found	
✓	DMARC Syntax Check	The record is valid	
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.	
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.	

DMARC Policy Generator (Online)

mxtoolbox.com/DMARCRecordGenerator.aspx?domain=hacking-lab.com

Apps | Slack | hacking-lab-... | Wiki | Tasks

Domain or Host Name

hacking-lab.com | Check DMARC Record | Solve Email Delivery Problems

HOW TO CREATE A DMARC RECORD

Answer the questions below and we'll generate a record for you in the correct format. For more details about each question or option list, click on the "Help" link beside it for more detailed information.

1. How do you want mail that fails DMARC to be treated by the recipient?

We recommend that you start with a policy of "none" - which is "Reporting Mode".

Quarantine ▾ Help

2. What email address(s) should aggregate DMARC reports be sent to?

*If adding multiple email addresses, please use a comma to separate each one.

dmarc-reports-6b65687332373130300a@hacking-lab.com Help

3. What email address(s) would you like to receive forensic DMARC failure reports?

*If adding multiple email addresses, please use a comma to separate each one.

dmarc-forensic-reports-6b65687332373130300a@hacking-lab.com Help

Would you like to have MxToolbox automatically process your DMARC reports for analysis and delivery insights?

No ▾ Help

What percentage of email do you want to apply this to?

Help

Show Advanced

Suggested Record:

The below record is updated as you modify the above fields. Once you have made all the changes above please click the "Finalize Record" button so we can validate the record for any syntax issues.

Once you have clicked the "Finalize Record" button, visit your DNS hosting provider and create a new record with the values presented below.

Type: TXT
Host/Name: _DMARC.hacking-lab.com
Value: v=DMARC1; p=quarantine; rua=mailto:dmarc-reports-6b65687332373130300a@hacking-lab.com; ruf=mailto:dmarc-forensic-reports-6b65687332373130300a@hacking-lab.com; ri=86400

* Note: For many DNS hosting providers, you'll just type "_DMARC" as the host/name and the tool add/append your domain name automatically.

Current Record:

v=DMARC1; p=none; rua=mailto:dmarc-reports-6b65687332373130300a@hacking-lab.com; ri=86400

Finalize Record

https://dmarcian.com/dmarc-record-wizard/

dmarcian

Why DMARC Solutions Pricing Tools

DMARC Record Wizard

DMARC Record Generator

The DMARC Record Wizard allows you to create your DMARC Record ready for pu
abusing your domain.

Not sure what a DMARC record is? Read more about it here.

Our Wizard guides you step by step through the creation by offering a detailled 7

- Step 1: Enter the domain
- Step 2: Choose your Policy
- Step 3: Provide your Aggregate reports address
- Step 4: (Optional) Provide your Failure Reporting address
- Step 5: Choose Identifier Alignment
- Step 6: (Optional) Choose Subdomain Policy
- Step 7: (Optional) Choose DMARC Policy percentage