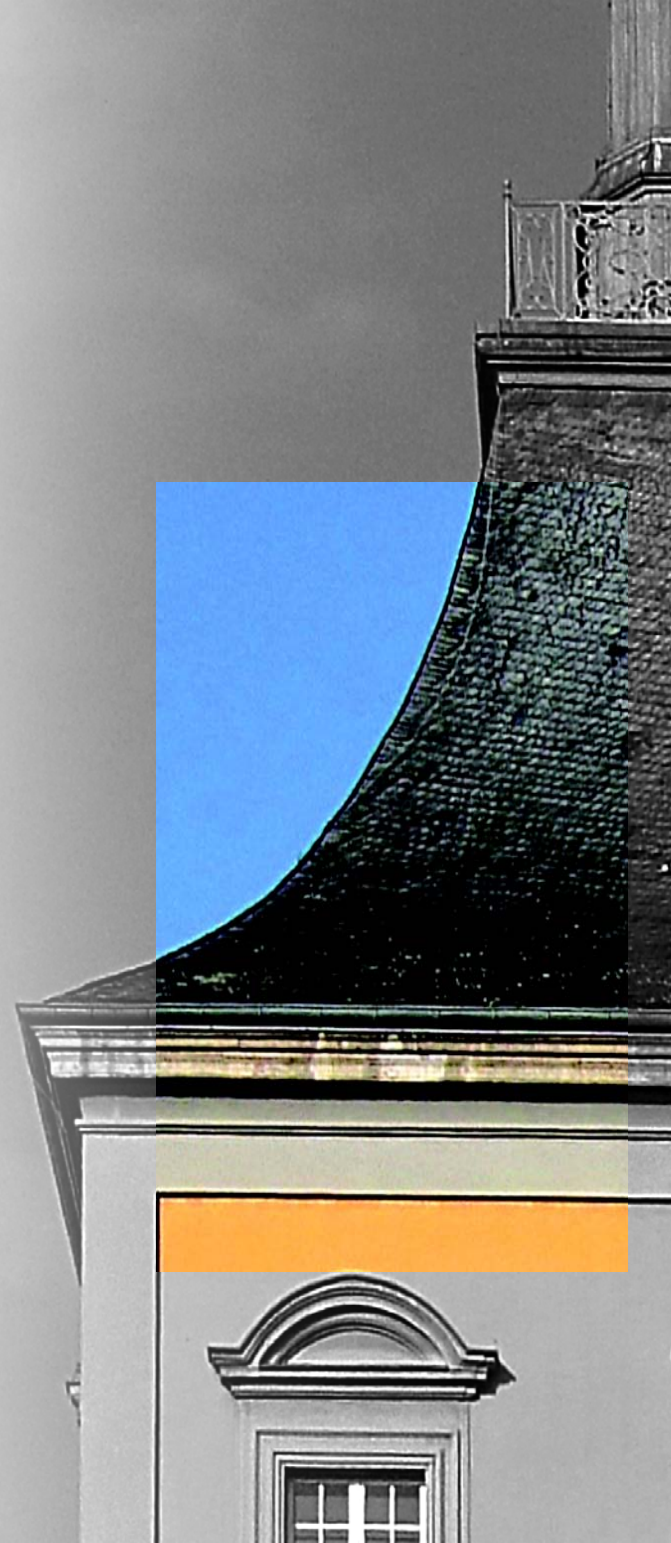
UNIVERSITÄT BONN

VORLESUNG

NETZWERKSICHERHEIT

SOMMERSEMESTER 2022

MO. 14-16 UHR



UNIVERSITÄT BONN

KAPITEL 9

DMARC

UNIVERSITÄT BONN

HISTORIE

Erste Idee 2010

- 17 Unternehmen (Empfänger & Sender)
  - u.a. Hotmail, AOL, GMail, Facebook, LinkedIn, Paypal
- Ziel: Die Entwicklung eines Standards, um
  - Absendern zu ermöglichen, leicht Richtlinien für nicht authentifizierte E-Mails zu veröffentlichen, und
  - Empfängern zu ermöglichen, den Absendern Authentifizierungsberichte zu erstellen, damit diese ihre eigene Infrastruktur überwachen und verbessern können.

Konzept basiert auf den im praktischen Umgang gemachten Erfahrungen mit

- SPF (Sender Policy Framework)
- DKIM (DomainKeys Identified Mail)

UNIVERSITÄT BONN

HISTORIE

Domain-based Message Authentication, Reporting, and Conformance (DMARC)

- RFC 7489
- veröffentlicht im März 2015

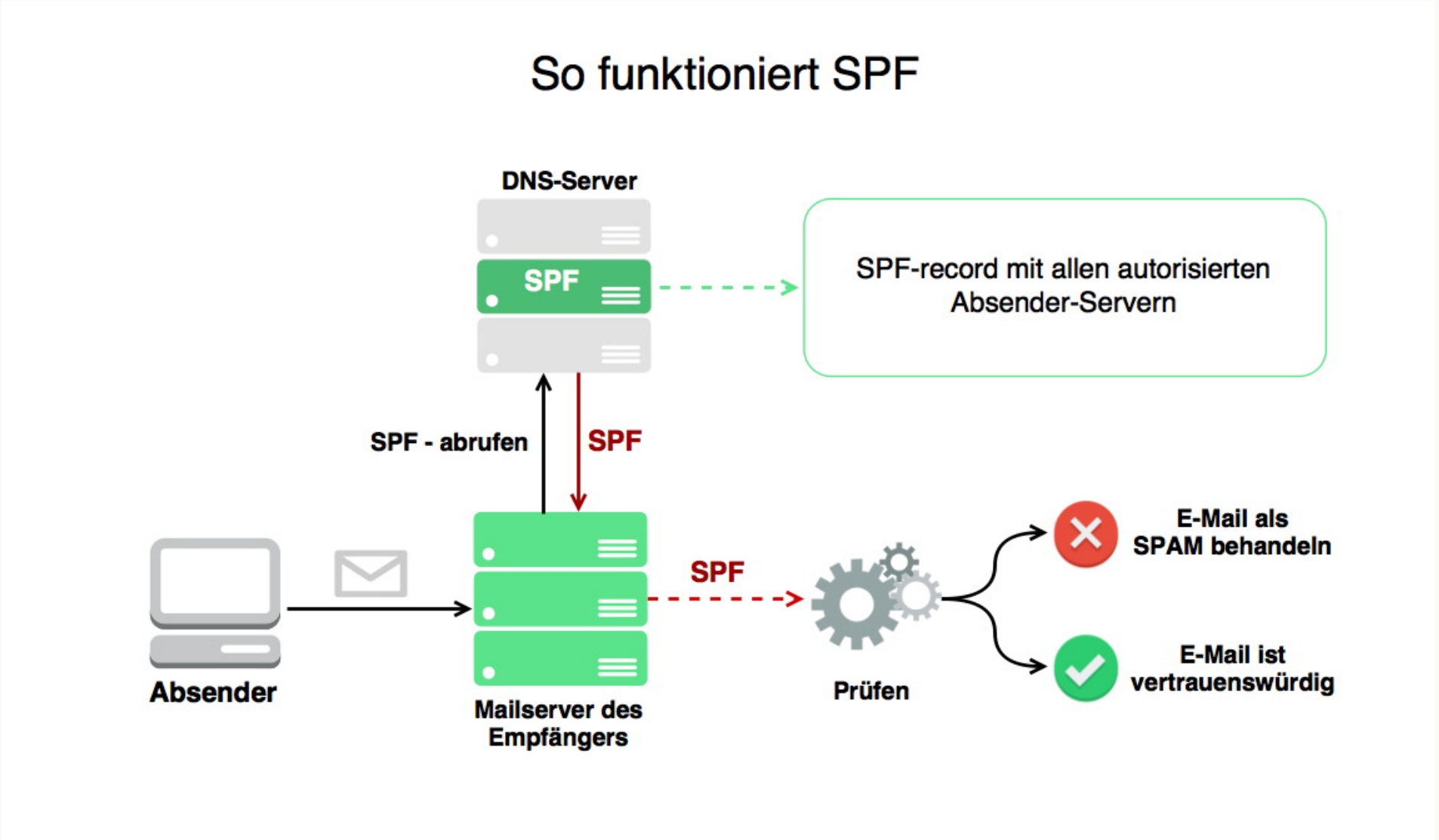
- aktualisiert durch RFC 8616 (Email Authentication for Internationalized Mail)
- veröffentlich im Juni 2019 (IDNA / Punycode RFC von 2003 / 2010)

- referenziert RFC 5322 (Internet Message Format) – From-Header
- veröffentlicht im Oktober 2008 (historisch vom RFC 561 von September 1973)

SENDER POLICY FRAMEWORK

- Idee: Hinterlegen von Sender-Informationen im DNS
- Erstmals diskutiert 2000 – 2002
- Kombination aus Reverse MX (RMX) und Designated Senders Protocol (DSP)
  - Ähnliche Ansätze zum authentifizieren von E-Mail-Sendern, insb. durch hinterlegte Informationen im DNS
  - Seit 2003 / 2004 in „größerer“ Runde diskutiert
  - 2006 als RFC 4408 (experimentell) veröffentlicht
  - 2014 in RFC 7208 als „Standard“ veröffentlich

SENDER POLICY FRAMEWORK



SENDER POLICY FRAMEWORK

SPF-Einträge

- uni-bonn.de. 29059 IN TXT
  "v=spf1 ip4:131.220.15.112 […] ip4:131.220.116.75 ?all"

- Elemente (Tags):
  - v=spf1 (Version / Prefix)
  - all
  - a
  - mx
  - ip4
  - ip6
  - Include
  - ptr (deprecated)
  - exists
  - redirect

- Qualifier:
  - + (pass)
    Implizit
  - - (Fail)
    Unautorisierte Absender ablehnen
  - ~ (SoftFail)
    Unautorisierte Absender markieren
  - ? (Neutral)
    Absender nicht bekannt / neutral

SENDER POLICY FRAMEWORK

SPF-Abfragen

- automatisch durch empfangene Mailserver – Reaktion im Eintrag definiert
- manuelle Prüfung, z.B. mit dig

```
[matze@bonn2] ~ $ dig TXT cs.uni-bonn.de

; <<>> DiG 9.16.27 <<>> TXT cs.uni-bonn.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37602
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cs.uni-bonn.de.                        IN      TXT

;; ANSWER SECTION:
cs.uni-bonn.de.         860     IN      TXT     "v=spf1 -ip4:131.220.8.144/28 +ip4:131.220.8.0/27 +ip4:131.220.9.0/27 +ip4:131.220.10.0/27 +ip4:131.220.63.192/28 ~all"
cs.uni-bonn.de.         860     IN      TXT     "v=spf2/pra -ip4:131.220.8.144/28 +ip4:131.220.8.0/27 +ip4:131.220.9.0/27 +ip4:131.220.10.0/27 +ip4:131.220.63.192/28 ~all"
cs.uni-bonn.de.         860     IN      TXT     "Institute of Computer Science, University of Bonn"

;; Query time: 0 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Mon Jul 11 01:29:19 CEST 2022
;; MSG SIZE  rcvd: 369
```

- V=spf2/pra (prüft gegen SPF und Sender ID - deprecated)

SENDER POLICY FRAMEWORK

Einschränkungen

- Maximale Länge eines SPF-Eintrags: 255 Zeichen (DNS-Limit)
- Maximale „Tiefe“ bei DNS-Lookups: 10 DNS-Lookups pro Prüfung
- Basiert auf der MAIL FROM (Return Path) Angabe (SMTP)
  - ➢ Sichtbarer Absender ist noch immer fälschbar
- „Weiterleitungen“ funktionieren nicht mehr (Aliases)
  - matthias.wuebbeling@cs.uni-bonn.de matthias.wuebbeling@uni-bonn.de
  - Mailserver cs.uni-bonn.de nicht als Absender für fremde Domains hinterlegt

SENDER POLICY FRAMEWORK

Mailserver-Einstellungen

- Beim Absender sind neben dem DNS-Eintrag keine Änderungen nötig!

- Beim Sender muss die Prüfung aktiviert werden (am Beispiel Postfix)
  - Installation des SPF-Policy-Dienstes
  - Konfiguration des Dienstes (in der master.cf)
    - policy unix - n n - - spawn user=nobody argv=/usr/bin/perl /usr/lib64/postfix/policyd-spf-perl
  - Aktivieren der Prüfung (in der main.cf)
  - smtpd_recipient_restrictions = […] reject_unauth_destination, […], check_policy_service unix:private/policy

UNIVERSITÄT BONN

SENDER POLICY FRAMEWORK

```
alpha ~ # cat /var/log/mail.log | grep -i spf | grep -B1 'reject'
Jul 10 14:52:36 alpha postfix/policy-spf[23123]: Policy action=550 Please see http://www.openspf.net/Why?s=mfrom;id=ambassador-
europa%40web.de;ip=178.239.250.140;r=alpha
Jul 10 14:52:36 alpha postfix/smtpd[22694]: NOQUEUE: reject: RCPT from unknown[178.239.250.140]: 550 5.7.1 <[redacted]
e>: Recipient address rejected: Please see http://www.openspf.net/Why?s=mfrom;id=ambassador-europa%40web.de;ip=178.239.250.140;
r=alpha; from=<ambassador-europa@web.de> to=[redacted] proto=ESMTP helo=<137-193-2-129.novotelecom.ru>
--
Jul 10 22:32:21 alpha postfix/policy-spf[22362]: Policy action=550 Please see http://www.openspf.net/Why?s=helo;id=tigo.com.hn;
ip=190.181.209.154;r=alpha
Jul 10 22:32:21 alpha postfix/smtpd[22210]: NOQUEUE: reject: RCPT from unknown[190.181.209.154]: 550 5.7.1 [redacted]
.com>: Recipient address rejected: Please see http://www.openspf.net/Why?s=helo;id=tigo.com.hn;ip=190.181.209.154;r=alpha; from
=<hzytoff@tigo.com.hn> to=[redacted] proto=ESMTP helo=<tigo.com.hn>
```

UNIVERSITÄT BONN

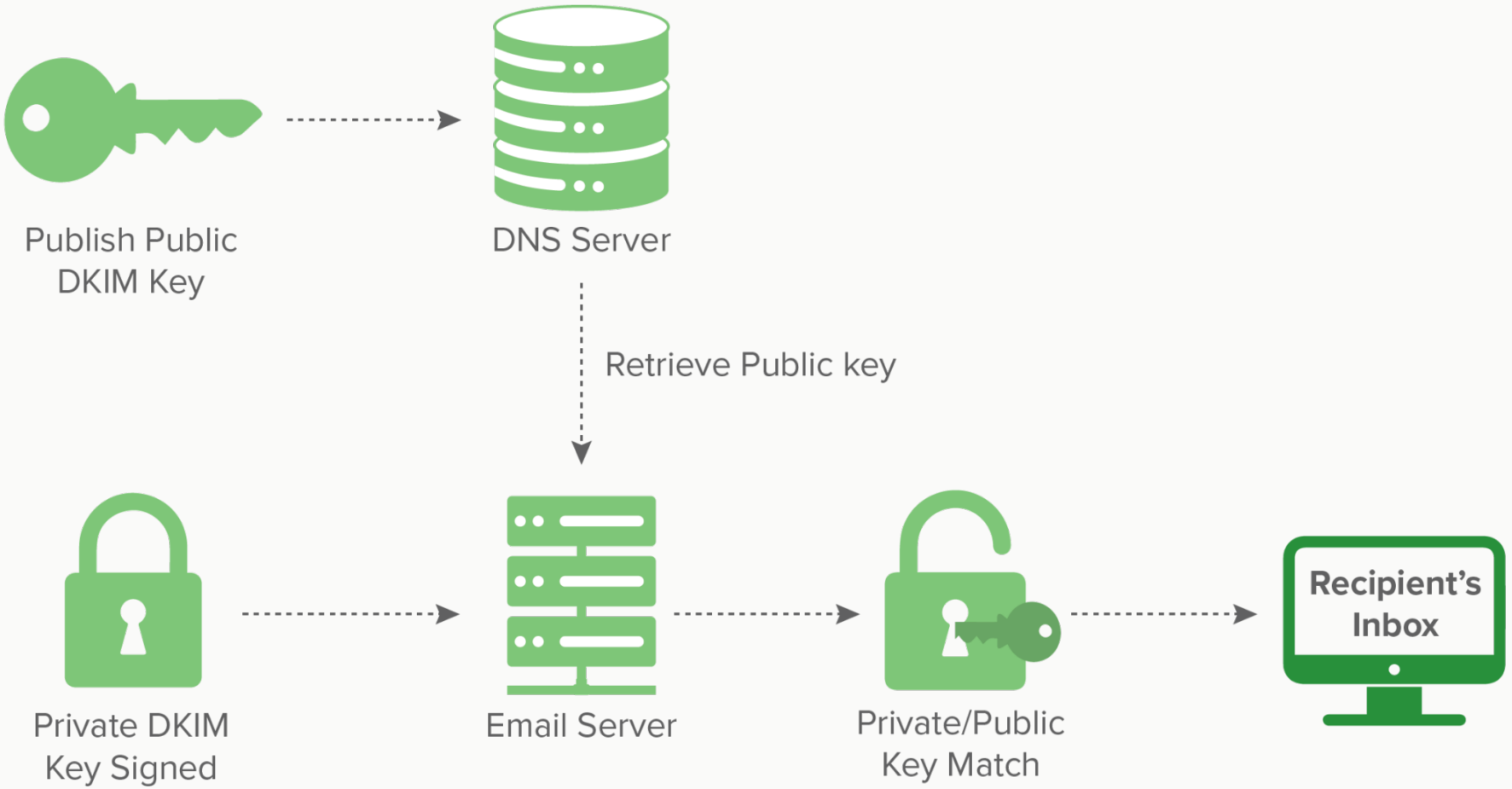
DOMAINKEYS IDENTIFIED MAIL

Idee: Signatur basierend auf Public Key Kryptographie

- DomainKeys (DK – RFC 4870) im Februar 2007 von Yahoo veröffentlicht
- Mit Identified Internet Mail kombiniert zu DKIM (RFC 4871 von Mai 2007)
  - erlaubt die Authentifikation des Absenders
  - Verhindert wie SPF nicht SPAM – aber die Fälschung des Absenders
- Der Absender
  - generiert ein asymmetrisches Schlüsselpaar,
  - hinterlegt den öffentlichen Schlüssel im DNS,
  - signiert Teile des E-Mail-Headers, den Body und die gesamte E-Mail.
- Der Empfänger
  - fragt den entsprechenden Schlüssel aus dem DNS
  - überprüft die vorliegende E-Mail

UNIVERSITÄT BONN

DOMAINKEYS IDENTIFIED MAIL



UNIVERSITÄT BONN

DOMAINKEYS IDENTIFIED MAIL

```
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
    s=pll2ago2xczc7sowe34fon3srmgil4mm; d=springer.com; t=1657286564;
    i=@newsletter.springer.com;
    h=Date:From:To:Reply-To:Subject:Content-Type:MIME-VERSION:Message-ID;
    bh=+PCY9y16c00Gb92SXrJxdOQeK/PPHV1EtM/EMYKg9EU=;
    b=Yp08SXr64FuEPN4MvVwroajNW66GV+T3/qZFJYQOuI3SBLp8P+51JYLRi9fHIS2n
    wQTN2KMgR/kKxq1kR5a1IsB48YB1+LHYmtjZoumtn7R71mi4ocr29NIBFB4n5JNV5IF
    gqn3irr+Zl0wZnRffgxZr57/t5RRHnyhSuSet/8M=
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
    s=ihchhvubuqgjsxyuhssfvqohv7z3u4hn; d=amazonses.com; t=1657286564;
    h=Date:From:To:Reply-To:Subject:Content-Type:MIME-VERSION:Message-ID:Feedback-ID;
    bh=+PCY9y16c00Gb92SXrJxdOQeK/PPHV1EtM/EMYKg9EU=;
    b=ANLTMhXDGk/UAv3SYZs+RXqMt0b4LH53bGICFWfvYRys5Ix++JMz5mMLfVgEc+oh
    0MwSgpiBceSbcTu0o5N0msCwypoisFRG+Ao1ndTLX+tana+mlG5MQO5IPEYd30/fQRO
    1PjdmevrJi3dQJ2JQPtDlQ0k4ek2Gd3HYTfNfjlQ=
```

UNIVERSITÄT BONN

DOMAINKEYS IDENTIFIED MAIL

Tags in Signaturen

- **v** (required), version
- **a** (required), signing algorithm
- **d** (required), Signing Domain Identifier (SDID)
- **s** (required), selector
- **c** (optional), canonicalization algorithm(s) for header and body
- **q** (optional), default query method
- **i** (optional), Agent or User Identifier (AUID)
- t (recommended), signature timestamp
- x (recommended), expire time
- **l** (optional), body length
- **h** (required), header fields - list of those that have been signed
- **z** (optional), header fields - copy of selected header fields and values
- **bh** (required), body hash
- **b** (required), signature of headers and body

UNIVERSITÄT BONN

DOMAINKEYS IDENTIFIED MAIL

Vorbereitungen

- Erstellen des Schlüsselpaars
  - opendkim-genkey -b 2048 -d uni-bonn.de -D ./opendkim -s default
    - -b Anzahl Bits
    - -d domain
    - -D Verzeichnis
    - -s Selector
  - erstellt zwei Dateien, <Selector>.private und <Selector>.txt

```
[matze@alpha] ~/opendkim/uni-bonn.de $ cat default.private
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDsVOx5ktGANpdGSiFmFAwMqUP+aYZBpu3QYzeGW4YhKkogHuV9
81Br3nsKHxhkGMRgZT/3EbnQs92EJbkrtIhjn6bgW1gLOsbX66k8yiLRVAg86SOt
uLENtxF6xo7Nmg2WhOP99BNRzuKKVe1JHGBFJQUHaZaroWllXN+5gcar8QIDAQAB
AoGASiMAXEqP6VY2kdgDLhAvz3DxYUcc1E9W3j2hVOYyhwjLA9RtTNscaRn7Iquq
bQvP3iUksY4f6bXiUOe8dFdHSM6hivDKNM2RvXnqzVwy6dMO86wsq+CpOlQIqfRt
4tiaXaNQnFkb1+wC4rAQKNTrxf+SMKDOnUk3NR7Zm9ZKP1kCQQD425LMPmOkLNaD
GfhfBQeh/+lZdQDZCG5Mub6q1Z68J1dOHfFMhrsa4FLkOTEgeYQtskOuFyHlz1r/
gox4YzqLAkEA8x/C+4w2D/H1HAws8f/NQdmewsIs5PmAl47f+6XEHgTbCOjWNx/9
Sg1XKVfu+galVF3YSjBvrySbyP6zv/eO8wJAV3MhlPBi/hFbmFpp8OobMoxxfeQl
1h6mVAP5wqKqOOdN+BoFj3TRD1LBDj4iy1yoXD6Glgi++rjxK1S+9Bc6nQJAYr7R
uM1X394MCZpAXwHgYhB7VOr8xPs5aVUUT+ch4ndiZxn6d2U8wOjuL9KRM2ejmsKK
6IcHtYEO7PHWG+/2VQJBANmv3Vv9If9UkqBdqkJiMpFDxHw+CYi1Pk9/tMUJhSvK
EdgXy+KDl7sfofYpfynLqiOMS9MMIsuGG3JZxWOasIs=
-----END RSA PRIVATE KEY-----
```

```
[matze@alpha] ~/opendkim/uni-bonn.de $ cat default.txt
default._domainkey      IN      TXT     ( "v=DKIM1; k=rsa; "
          "p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDsVOx5ktGANpdGSiFmFAwMqUP+aYZBpu3QYzeGW4YhKkogHuV981Br3nsKHxhkGMRgZT/3EbnQs9
2EJbkrtIhjn6bgW1gLOsbX66k8yiLRVAg86SOtuLENtxF6xo7Nmg2WhOP99BNRzuKKVe1JHGBFJQUHaZaroWllXN+5gcar8QIDAQAB" )  ; ----- DKIM key def
ault for uni-bonn.de
```

DOMAINKEYS IDENTIFIED MAIL

Vorbereitungen

- Erstellen des Schlüsselpaars
  - opendkim-genkey -b 2048 -d uni-bonn.de -D ./opendkim -s default
    - -b Anzahl Bits
    - -d domain
    - -D Verzeichnis
    - -s Selector
  - erstellt zwei Dateien, <Selector>.private und <Selector>.txt
- Hinterlegen des Public Keys im DNS unter
  - <Selector>._domainkey.uni-bonn.de
- Konfigurieren von OpenDKIM und des Mailservers

DOMAINKEYS IDENTIFIED MAIL

Konfiguration

- OpenDKIM
  - KeyTable (z.B. für mehrere Domains mit %-Platzhalter)

    <Selector>._domainkey.% %:<Selector>:/etc/opendkim/keys/%/<Selector>.private

    default._domainkey.uni-bonn.de uni-bonn.de:default:/etc/opendkim/keys/%/default.private
  - SigningTable

    * **<Selector>._domainkey.%**

    matthias.wuebbeling@uni-bonn.de **default._domainkey.uni-bonn.de**
- Postfix

```
# OpenDKIM
milter_default_action = accept
milter_protocol = 2
smtpd_milters = inet:localhost:8891
non_smtpd_milters = inet:localhost:8891
```

DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING AND CONFORMANCE (DMARC)

DMARC bringt nun alles zusammen

- Vor allem: Policy für SPF und DKIM Ereignisse
  - Aber auch: Hinweis auf den Schutz von Absender und Inhalten durch den Sender!
  - Eher nicht: SPAM-Schutz
  - Aber: Phishing-Schutz
- DMARC basiert, wie auch SPF und DKIM auf DNS
  - TXT-Eintrag unter der Subdomain _dmarc

```
[matze@alpha] ~ $ dig TXT _dmarc.uni-bonn.de
;; ANSWER SECTION:
_dmarc.uni-bonn.de.     21600   IN      TXT     "v=DMARC1; p=none; sp=none; adkim=s; aspf=s; rua=mailto:dmarc@uni-bonn.de;"
```

  - “Wie soll sich ein E-Mail-Empfänger verhalten?”

DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING AND CONFORMANCE (DMARC)

DMARC-Eintrag

- V (required)
  Version
- pct (optional)
  %-Anteil geprüfter Mails
- fo (optional)
  Fehlerberichtsoption
- ruf (optional)
  Empfänger forensischer Berichte
- rua (optional)
  Empfänger aggregierter Bericht
- rf (optional)
  Format des Berichts
- ri (optional)
  Berichtsintervall
- p (required)
  <"none", "quarantine", "reject" >
  Handlung für Mails der Hauptdomain
- sp (optional)
  <"none", "quarantine", "reject" >
  Handlung für Mail der Subdomain
- Adkim (optional)
  Abgleichmodus für DKIM
- Aspf (optional)
  Abgleichmodus für SPF

DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING AND CONFORMANCE (DMARC)

DMARC – Schöne heile Welt?

- Ja! Sender können entscheiden, wer mit welchem Absender E-Mails senden darf und können diese E-Mails als Absender signieren.
- Nein! Empfänger müssen beim Empfang der E-Mails prüfen! Hat ein Admin diese Prüfung nicht aktiviert, gibt es keinen Schutz.
- Ja! Alle “großen” Mailprovider implementieren DMARC sehr zuverlässig.
- Nein! Viele andere (z.B. Unternehmen, Universitäten, Organisationen, Behörden) verwenden DMARC nicht oder nicht richtig
- Nein! Mailinglisten funktionieren mit DMARC nicht mehr wie gewohnt
  - Hier musste gängige Mailinglisten-Software angepasst werden.
- Nein! SPF / DMARC / DKIM verhindern kein SPAM!

UNIVERSITÄT BONN

ENDE

Vielen Dank für die Aufmerksamkeit!

Fragen?

Keine nächste Vorlesung:

- Heute ist die letzte!

Nächste Übung:

- Dienstag, 12. Juli 2022 – 16 Uhr
- Abgabe des Übungszettels 12 bis morgen – 16 Uhr

- 1. Klausur: Freitag, 15. Juli 2022 – Zeitslot 15:00 bis 18:00 Uhr
  - Beginn: 15 Uhr! Friedrich-Hirzebruch-Allee 5 – Hörsaal 2