genua Ein Unternehmen der Bundesdruckerei

- DKIM – Kryptografie auf wackligem Boden

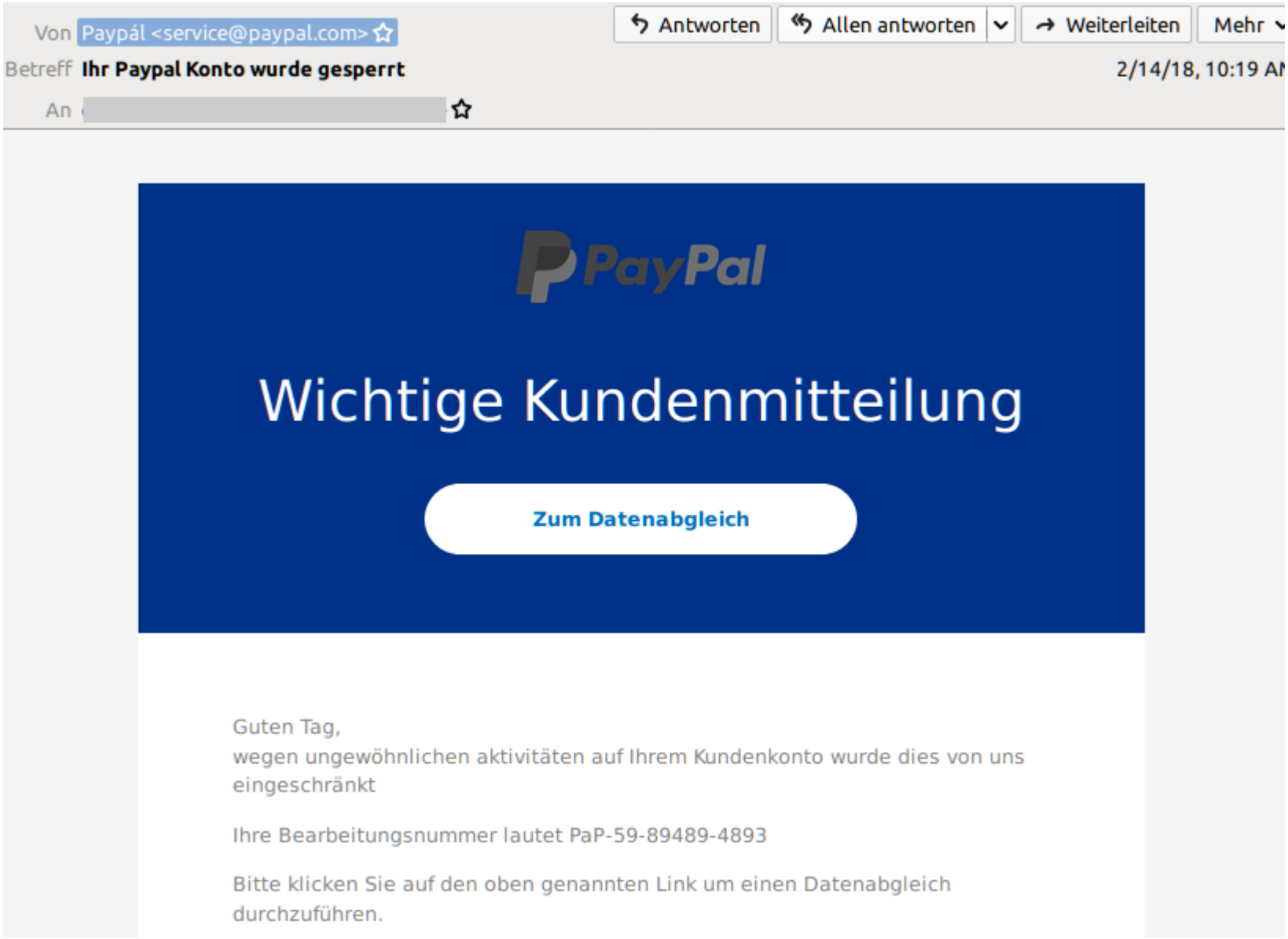
Steffen Ullrich, genua GmbH

16. Deutscher IT-Sicherheitskongress, 22.5.2019

- Mail ist ein wesentlicher Angriffsvektor
  - Phishing von Zugangsdaten
  - Malware (Ransomware, Banking-Trojaner...) attacht oder verlinkt
  - Spam als Ärgernis
- Absender der Mail oftmals gefälscht
  - zur Erhöhung der Glaubwürdigkeit
  - oder Umgehung von Filtern

Absenderspoofing

genua Ein Unternehmen der Bundesdruckerei



Inhalt des Vortrags

genua Ein Unternehmen der Bundesdruckerei

- Kurze Einführung in Mail
  - Format: Mail-Header, Mail-Body, MIME
  - Transport per SMTP
- Absenderspoofing in Mails
  - Warum und wie ist es möglich
  - Was kann man dagegen tun
- DKIM – Kryptografie auf wackligem Boden
  - Mail signifikant ändern, Signatur gleich
  - Mail unverändert transportieren, Signatur kaputt

genua Ein Unternehmen der Bundesdruckerei

- Mail – aus den Anfangszeiten des Internet
  RFC 822 1982, RFC 731 1977, ...
  - ASCII only, Zeilenlänge max 1000 Zeichen
  - Header (Subject, From, To...) und Body (Inhalt)
- MIME – Mail wie wir es heute kennen
  RFC 2045-2048 1996, RFC 2231 ...
  - Abbildung von Struktur und binären Inhalte auf ASCII und1000 Zeichen/Zeile
- SMTP – Transport der Mail
  RFC 821 1982, diverse Erweiterungen später ...
  - Hop-by-Hop von MUA über MTA zu finalem Server

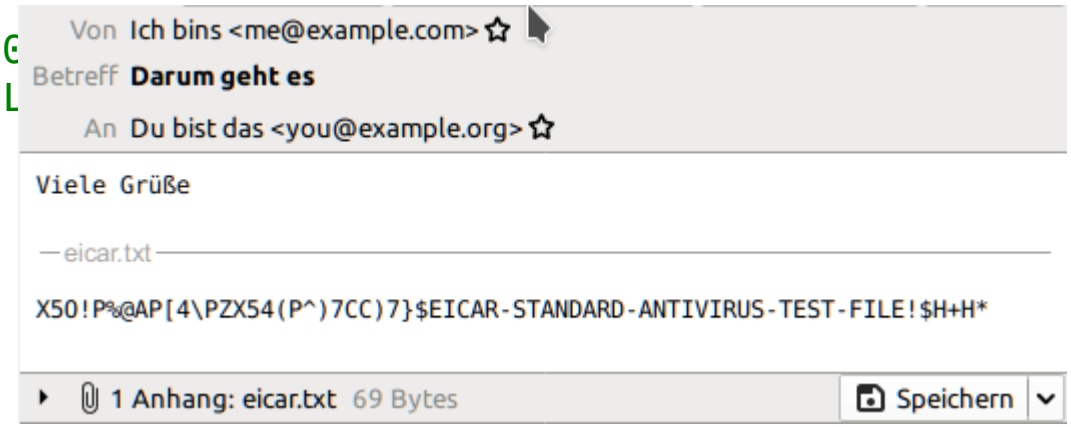
MIME in Kurzfassung

genua Ein Unternehmen der Bundesdruckerei

```
From: Ich bins <me@example.com>
To: Du bist das <you@example.org>
Subject: Darum geht es
Content-Type: multipart/mixed; boundary=xxx

--xxx
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: quoted-printable

Viele Gr=C3=BC=C3=9Fe
--xxx
Content-Type: application/octet-stream
Content-Disposition: attachment;
  filename="eicar.txt"
Content-Transfer-Encoding: base64

WDVPIVAlQEFQWzRcUFpYNTQoUF4pN0
UQU5EQVJELUFOVElWSVJVUy1URVNUL
--xxx--
```

Struktur als Text

Binär als ASCII



Absenderspoofing beim Mailtransport

genua Ein Unternehmen der Bundesdruckerei

```
 $  telnet mx.example.com 25

<-  250 mx.example.com ESMTP ready
->  HELO example.org
<-  250 ok
->  MAIL FROM: <A@domain-A.com>
<-  250 ok
    ...
->  DATA
<-  354 ok
->  Subject: test
->  From: <B@domain-B.com>
->  ...
```

Sender laut SMTP nicht im MUA gezeigt SMTP.MAILFROM

Sender lt. Mail-Header **im MUA angezeigt** RFC822.From

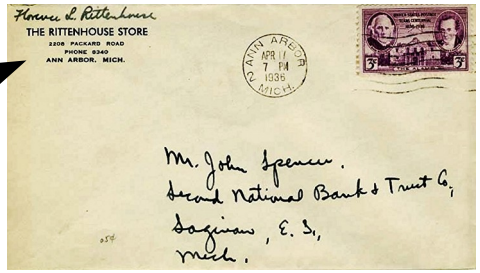
Weder Prüfung von Sender laut SMTP noch laut Mail-Header

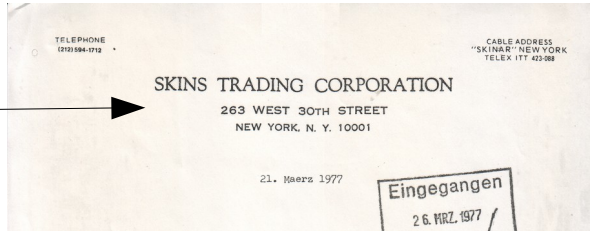
Absenderspoofing beim Snail-Mail

genua Ein Unternehmen der Bundesdruckerei

```
 $  telnet mx.example.com 25

<-  250 mx.example.com ESMTP ready
->  HELO example.org
<-  250 ok
->  MAIL FROM: <A@domain-A.com>
<-  250 ok
    ...
->  DATA
<-  354 ok
->  Subject: test
->  From: <B@domain-B.com>
->  ...
```

Umschlag: SMTP.MAILFROM





Kopfbogen: RFC822.From

genua Ein Unternehmen der Bundesdruckerei

- Absender signiert Mail: PGP bzw. S/MIME
  - **braucht Unterstützung in Sender und Empfänger**
  - S/MIME in vielen Mail-Clients eingebaut
    PGP oft über Erweiterungen möglich
  - Sender braucht eigenes Key-Pair
  - PKI, Web-of-Trust oder TOFU nötig für Verifikation der Signatur beim Empfänger
  - Komplexität der Nutzung wird als zu hoch angesehen, selbst kritische Sender wie Banken oder Mailprovider nutzen es daher nicht einmal zusätzlich

genua Ein Unternehmen der Bundesdruckerei

- SPF, DKIM und DMARC
  - **braucht Unterstützung nur bei MTA von Sender und Empfänger, nicht bei den Endnutzern**
  - SPF: Policy im DNS gibt an, von welchen IP-Adressen Mail im Namen der **Domain** verschickt werden darf – checkt nur SMTP.MAILFROM
  - DKIM: MTA garantiert über kryptografische Signatur, dass die Mail über ihn ging und danach nicht verändert wurde
  - DMARC: Abgleich der **Domain** aus SMTP.MAILFROM (SPF) bzw. **Domain** der DKIM-Signatur mit der **Domain** aus RFC822.From

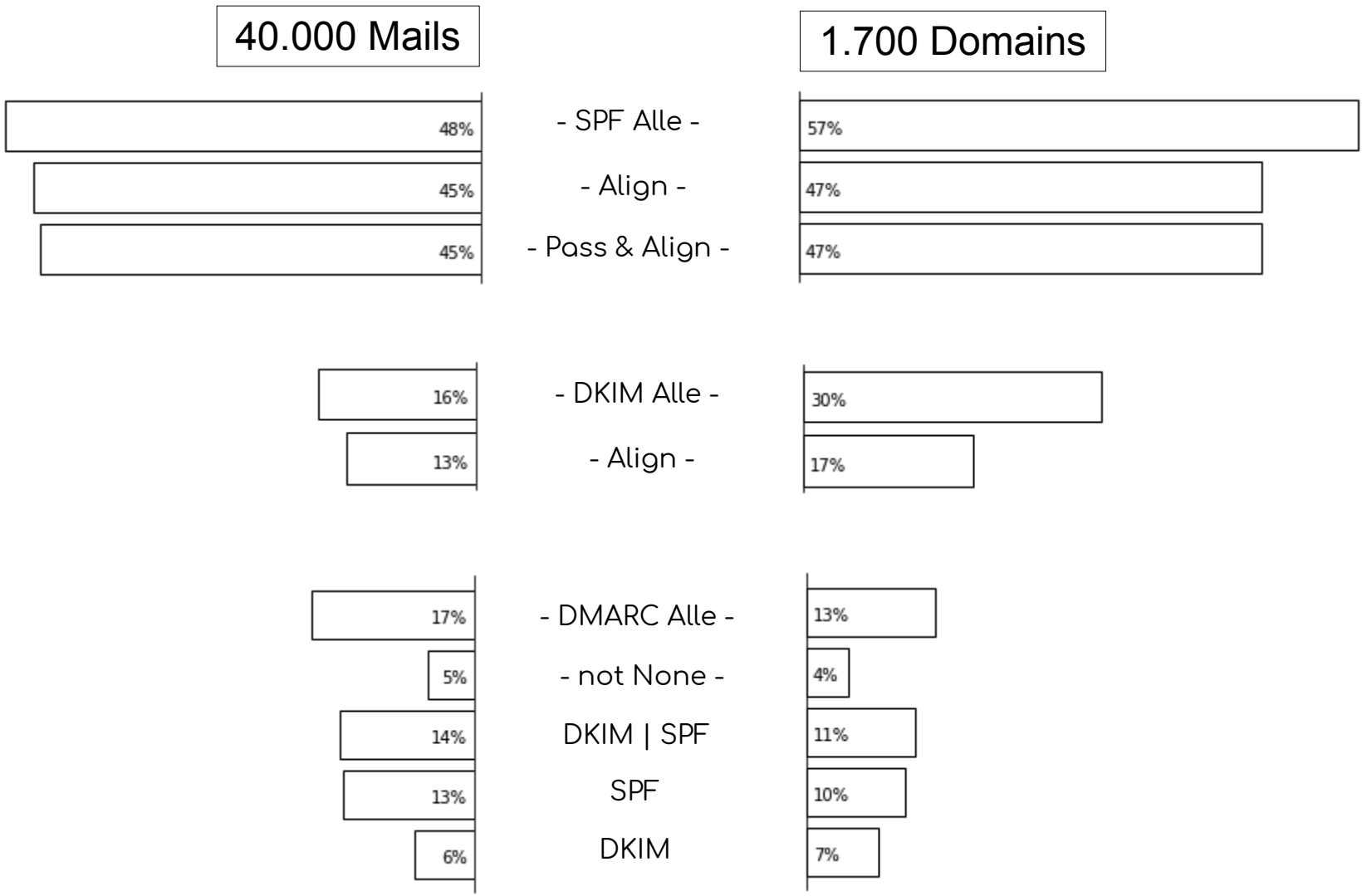
SPF, DKIM, DMARC – offensichtliche Probleme

genua Ein Unternehmen der Bundesdruckerei

- Nur DMARC macht den Abgleich mit der im MUA angezeigten Absenderadresse
- Verifiziert Sender-Domain, nicht Sender
  Hilft bei @paypal.com.
  Bei @gmail.com, @web.de ... hingegen muss man hoffen, dass MTA Spoofing innerhalb der Domain verhindert hat.
- SPF hat Probleme mit Weiterleitung
  Entweder bleibt SMTP.MAILFROM und Policy passt nicht.
  Oder Forwarder ändert SMTP.MAILFROM und DMARC-Abgleich mit RFC822.From schlägt fehl.
  DKIM hat diese Probleme nicht.

Statistiken aus Real-Life Mailverkehr

genua Ein Unternehmen der Bundesdruckerei



Grundideen von DKIM

genua Ein Unternehmen der Bundesdruckerei

- MTA fügt kryptografische Signature zu Mail hinzu. Signatur umfasst Mail-Header und Mail-Body.
- Empfänger kann Signatur prüfen: Public Key ist im DNS zu finden.
- Für Auslagern von Services an Dienstleister (wie Mailchimp) kann für diese ein extra Key erstellt und im DNS hinterlegt werden.

Grundideen von DKIM – das Kleingedruckte

genua Ein Unternehmen der Bundesdruckerei

- MTA fügt kryptografische Signature zu Mail hinzu.
  Signatur umfasst Mail-Header und Mail-Body.
  Signatur umfasst nur ausgewählte Felder vom Header.
  Signatur umfasst evtl. nicht den ganze Body.
  Signatur spezifisch für aktuelle Kodierung des Body.
- Empfänger kann Signatur prüfen:
  Public Key ist im DNS zu finden.
- Für Auslagern von Services an Dienstleister (wie Mailchimp) kann für diese ein extra Key erstellt und im DNS hinterlegt werden.
  Dienstleister kann damit beliebige Absender in Domain spoofen.

genua Ein Unternehmen der Bundesdruckerei

Andere Mail
Gleiche Signatur
Erfolgreiches Spoofing mit DKIM und DMARC

Erwartungen an DKIM

genua Ein Unternehmen der Bundesdruckerei

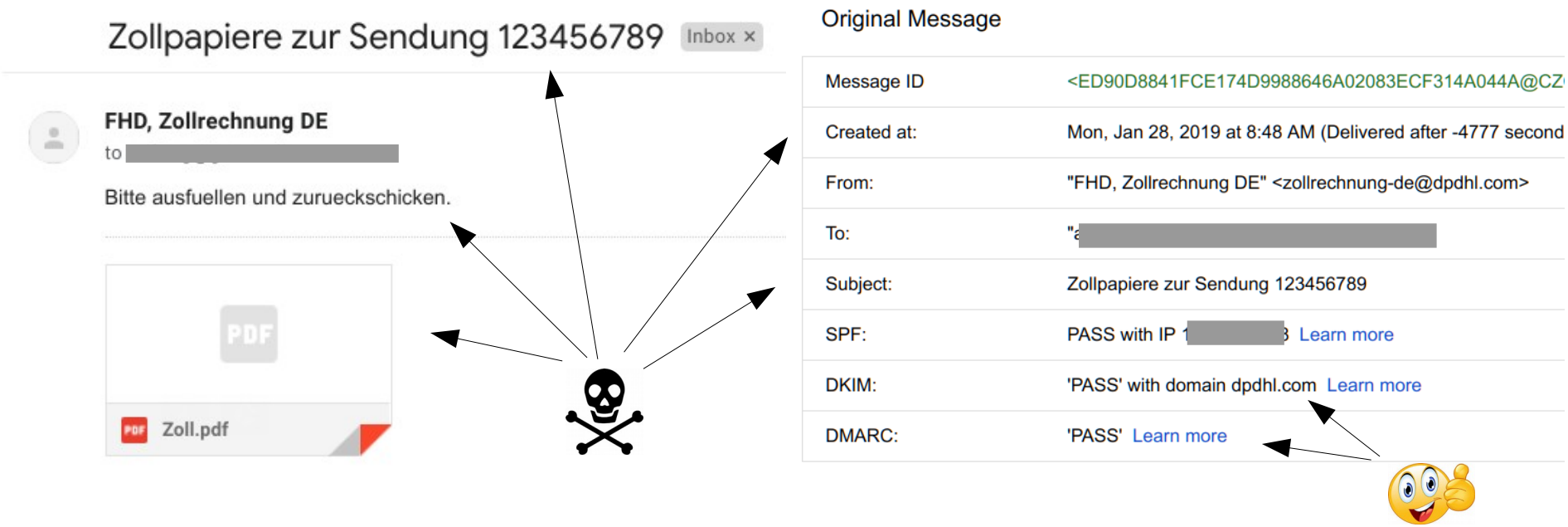
Request for Comments: 6376 ...
...
1. Introduction

DomainKeys Identified Mail (DKIM) permits a person, role, or organization to claim some responsibility for a message by associating a domain name [RFC1034] with the message [RFC5322], which they are authorized to use. This can be an author's organization, an operational relay, or one of their agents. Assertion of responsibility is validated through a cryptographic signature and by querying the Signer's domain directly to retrieve the appropriate public key. Message transit from author to recipient is through relays that typically make no substantive change to the message content and thus preserve the DKIM signature. A message can contain multiple signatures, from the same or different organizations involved with the message.

Kryptografie garantiert, dass Sender der behauptete ist

Da wollen wir hin als Angreifer …

genua Ein Unternehmen der Bundesdruckerei



1. Empfangene Mail mit DKIM-Signatur von DHL nehmen
2. Anpassen: Betreff, Inhalt, Attachment, Datum
   DKIM-Signatur gleich lassen
3. Mail verschicken: DKIM und DMARC Pass

Was umfasst eigentlich die DKIM-Signatur

genua Ein Unternehmen der Bundesdruckerei

- Typische Vorstellung:
  Mail-Header und -Body
- Realität:
  Ausgewählte Felder des Mail-Headers
  Eventuell nur Teile des Body
- In Real-Life sind Modifikation oder Hinzufügen kritischer Header-Felder oder Hinzufügen von Body-Inhalten oft ohne Auswirkungen auf die Signatur möglich

Aufbau einer DKIM-Signatur - 1

genua Ein Unternehmen der Bundesdruckerei

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=dhl.com; l=1850; s=20140901; t=1452769712;
  h=date:from:to:message-id:subject:mime-version;
  bh=yCbsFBJJ9k2VYBxKGgyNILalBP3Yzn1N8cMPQr92+zw=;
  b=bnuXrH/dSnyDR/kciZauK4...
```

- h welche Header-Felder von der Signatur umfasst sind
- bh Hash über den Body
- b kryptografische Signature über DKIM-Signature-Feld
  Umfasst damit auch bh, h, d, ...

- d Domain, für die die Signatur gilt - Abgleich in DMARC
- s Selektor für DNS:

```
$ dig txt 20140901._domainkey.dhl.com
... v=DKIM1; t=s; p=MIIBIjAN ...
```

Modifikation und Hinzufügen von Feldern

genua Ein Unternehmen der Bundesdruckerei

Felder, die von der Signatur nicht umfasst sind, können beliebig geändert werden.

```
DKIM-Signature: v=1; h=from:to:cc:content-type; ...
Subject: hier kann ich reinschreiben was ich will
From: <...>
To: <...>
```

Felder, wo die Signatur keine Neudefinition verhindert, können beliebig hinzugefügt werden.

```
Subject: hier kann ich reinschreiben was ich will
DKIM-Signature: v=1;
  h=from:to:cc:subject:content-type; ...
Subject: originales Subject
From: <...>
To: <...>
```

genua Ein Unternehmen der Bundesdruckerei

Aufnahme nicht existierender Felder in Signatur verhindert Hinzufügen dieser Felder.

```
Subject: hinzufuegen geht nicht
Content-type: hinzufuegen/geht-auch-nicht
DKIM-Signature: v=1;
  h=from:to:cc:subject:subject:content-type; ...
Subject: originales Subject
From: <...>
To: <...>
```

DKIM-Standard legt nicht fest, welche Felder zu schützen sind (außer `From`) und gibt auch keine sinnvollen Empfehlungen.

Hinzufügen kritischer Felder

genua Ein Unternehmen der Bundesdruckerei

MUA

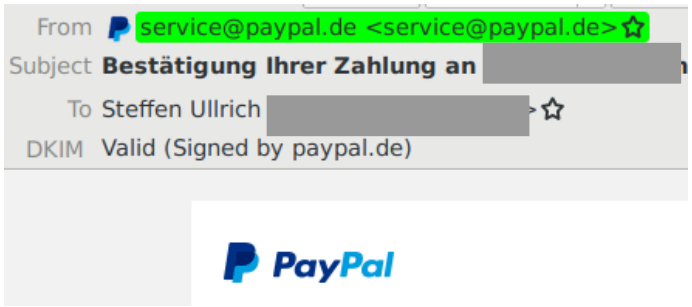
DKIM

```
Subject: Urgent Update at http://foo
Content-type: multipart/mixed; boundary=bar
DKIM-Signature: v=1; h=from:to:cc:subject:content-type; ...
From: <...>
To: <...>
Subject: originales Subject
Content-type: multipart/mixed; boundary=foo
Date: Wed, 20 Sep 2017 17:55:18 +0200

--foo
Content-type: text/plain

some text
--foo--
```

Davor

Thunderbird 60.2.1, DKIM Verifier 2.0.0

Danach



Aufbau einer DKIM-Signatur - 2

genua Ein Unternehmen der Bundesdruckerei

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=dhl.com; l=1850; s=20140901; t=1452769712;
  h=date:from:to:message-id:subject:mime-version;
  bh=yCbsFBJJ9k2VYBxKGgyNILalBP3Yzn1N8cMPQr92+zw=;
  b=bnuXrH/dSnyDR/kciZauK4...
```

- h welche Header-Felder von der Signatur umfasst sind
- bh Hash über den Body
- b kryptografische Signature über DKIM-Signature-Feld
  Umfasst damit auch bh, h, d, l ...

- l Teil des Body (Länge), der von der Signatur umfasst ist
  Genutzt, um beim Transport hinzugefügte Disclaimer etc zu erlauben (Virenscanner, Mailinglisten...)

Hinzufügen von Body

genua Ein Unternehmen der Bundesdruckerei

l=...

bh

außerhalb bh

```
Subject: Zollpapiere zur Sendung 123456789
Date: Mon, 28 Jan 2019 07:48:54 +0000
Content-Type: multipart/mixed; boundary="foo"
...
DKIM-Signature:   v=1; a=rsa-sha256; c=relaxed/relaxed;
   d=dpdhl.com; l=87336; s=20140901; t=1496389754;
   h=from:to:subject:date:message-id:mime-version;
   bh=3lnyE3...;
   b=fpw+kBAdLa4J...
...
From: "FHD, Zollrechnung DE" <zollrechnung-de@dpdhl.com>
To:   ...
Subject:    Zollpapiere zur Sendung 5689501322
...
Content-Type:     multipart/mixed;
   boundary="_005_ED90D8841FCE174D9988646A02083ECF314A044ACZCHOWS1342prgd_"
...
Der originale Inhalt der Mail
...
--_005_ED90D8841FCE174D9988646A02083ECF314A044ACZCHOWS1342prgd_--
--foo
Content-Type: text/plain

Bitte ausfuellen und zurueckschicken.
--foo
Content-Type: application/octet-stream; name="Zoll.pdf"

...
--foo--
```

Hinzufügen von Body

genua Ein Unternehmen der Bundesdruckerei

Preamble

MIME Part#1

MIME Part#2

bh

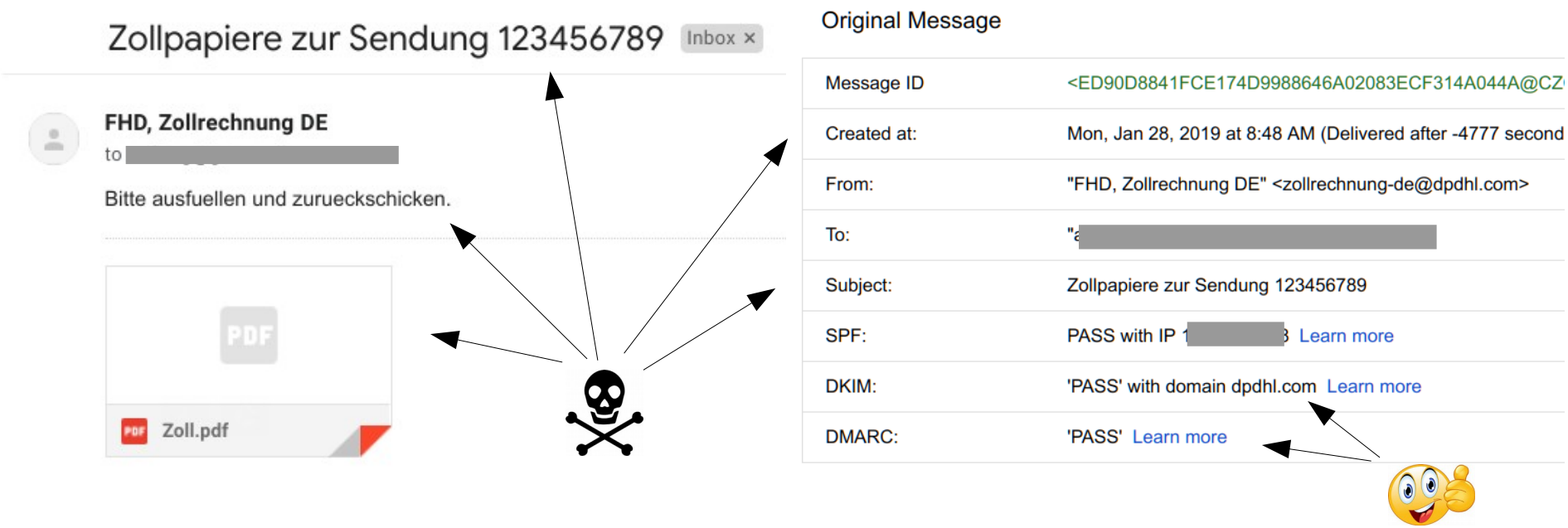
außerhalb bh

```
Subject: Zollpapiere zur Sendung 123456789
Date: Mon, 28 Jan 2019 07:48:54 +0000
Content-Type: multipart/mixed; boundary="foo"
...
DKIM-Signature:   v=1; a=rsa-sha256; c=relaxed/relaxed;
   d=dpdhl.com; l=87336; s=20140901; t=1496389754;
   h=from:to:subject:date:message-id:mime-version;
   bh=3lnyE3...;
   b=fpw+kBAdLa4J...
...
From: "FHD, Zollrechnung DE" <zollrechnung-de@dpdhl.com>
To:   ...
Subject:    Zollpapiere zur Sendung 5689501322
...
Content-Type:     multipart/mixed;
   boundary="_005_ED90D8841FCE174D9988646A02083ECF314A044ACZCHOWS1342prgd_"
...
Der originale Inhalt der Mail
...
--_005_ED90D8841FCE174D9988646A02083ECF314A044ACZCHOWS1342prgd_--
--foo
Content-Type: text/plain

Bitte ausfuellen und zurueckschicken.
--foo
Content-Type: application/octet-stream; name="Zoll.pdf"

...
--foo--
```

boundary=..

… Geschafft

genua Ein Unternehmen der Bundesdruckerei



1. Empfangene Mail mit DKIM-Signatur von DHL nehmen
2. Anpassen: Betreff, Inhalt, Attachment, Datum
   DKIM-Signatur gleich lassen
3. Mail verschicken: DKIM und DMARC Pass

genua Ein Unternehmen der Bundesdruckerei

- kein Schutz gegen Hinzufügen von

Content-Type	99%
Subject	99%
From	97%
Content-Transfer-Encoding	96%

- l-Attribut und kein Schutz von

Content-Type	14%

u.a. DHL, Cisco, HRS ... - 19% aller Absender-Domains

ca 10.000 mit DKIM signierte Mails aus ca 700 Domains, kein Spam

genua Ein Unternehmen der Bundesdruckerei

- Sender
  - Kritische Felder in Signatur einbeziehen und gegen Hinzufügen schützen
    From, Subject, Content-Type, Content-Transfer-Encoding
    evtl. Date, To, Cc
  - kein l-Attribut benutzen
    sowieso sinnlos bei Multi-Part-Messages, was fast alle sind
- Empfänger
  - Prüfen, ob alle kritischen Felder und kompletter Body von Signatur umfasst sind.
    Evtl. überflüssigen Body entfernen.
- Entwickler von Bibliotheken und Tools
  - sichere Defaults anbieten

genua Ein Unternehmen der Bundesdruckerei

Evtl. überflüssigen Body entfernen
→ macht evtl. Mail kaputt

immer l=10 für alle Mails

kritische Header ungeschützt

```
DKIM-Signature: v=1;
 a=rsa-sha256; c=relaxed/simple;
 d=grosser-deutscher-konzern;
 s=2015-01-21; t=1553781539;
 bh=tipqD6mO8uy...;
 l=10;
 h=From:From:Reply-To:Sender;
 b=xkIYig553TTIVx+PtZ2DinHp2ZW...
...
Definitiv mehr als 10 Byte Inhalt
```

genua Ein Unternehmen der Bundesdruckerei

Gleiche Mail
Ungültige Signatur
Kaputt durch Transport

Erwartungen an DKIM

genua Ein Unternehmen der Bundesdruckerei

```
Request for Comments: 6376                          ...
...
                DomainKeys Identified Mail (DKIM) Signatures
...
1.  Introduction
```

DomainKeys Identified Mail (DKIM) permits a person, role, or organization to claim some responsibility for a message by associating a domain name [RFC1034] with the message [RFC5322], which they are authorized to use. This can be an author's organization, an operational relay, or one of their agents. Assertion of responsibility is validated through a cryptographic signature and by querying the Signer's domain directly to retrieve the appropriate public key. Message transit from author to recipient is through relays that typically make no substantive change to the message content and thus preserve the DKIM signature. A message can contain multiple signatures, from the same or different organizations involved with the message.

Signatur ist robust gegen transportbedingte Änderungen

SMTP 8BITMIME

genua Ein Unternehmen der Bundesdruckerei

```
Request for Comments: 6152
   ...
            SMTP Service Extension for 8-bit MIME Transport
   ...
   If a server SMTP does not support the 8-bit MIME transport extension
   (either by not responding with code 250 to the EHLO command, or by
   not including the EHLO keyword value 8BITMIME in its response), then
   the client SMTP must not, under any circumstances, attempt to
   transfer a content that contains characters outside of the US-ASCII
   octet range (hex 00-7F).
   A client SMTP has two options in this case: first, it may implement a
   gateway transformation to convert the message into valid 7-bit MIME,
   or second, it may treat the barrier to 8-bit as a permanent error and
   handle it in the usual manner for delivery failures...
```

Wenn MTA kein 8BITMIME kann, wird transformiert zu 7bit.

Transformation wenn kein 8BITMIME

genua Ein Unternehmen der Bundesdruckerei

```
DKIM-Signature: v=1; bh=ABC...
From: me@example.com
To: you@example.com
Subject: test
Content-type: text/plain;
  charset=utf-8
Content-Transfer-Encoding: 8bit

Viele Grüße!
```

DKIM OK

DKIM kaputt

```
220 example.com
EHLO example.org
250-example.com
250-8BITMIME
250 HELP
```

```
DKIM-Signature: v=1; bh=ABC...
From: me@example.com
To: you@example.com
Subject: test
Content-type: text/plain;
  charset=utf-8
Content-Transfer-Encoding:
  quoted-printable

Viele Gr=C3=BC=C3=9Fe!
```

genua Ein Unternehmen der Bundesdruckerei

- 04/2019: ca 10% der öffentlichen MTA können kein 8BITMIME
  540 häufigste aus 1700 Absender-Domains in 40.000 Mails untersucht (umfasst 95% der Mails)
- MTA bei genua macht kein 8BITMIME:
  von 9000 Mails mit DKIM-Signature haben ca. 9% unpassenden Body-Hash
  Ursache nicht immer klar, aber in einigen Fällen klar auf 7bit Transformation zurückführbar

genua Ein Unternehmen der Bundesdruckerei

Request for Comments: 6376 ...

...

DomainKeys Identified Mail (DKIM) Signatures

...

5.3. Normalize the Message to Prevent Transport Conversions

Some messages, particularly those using 8-bit characters, are subject to modification during transit, notably conversion to 7-bit form. Such conversions will break DKIM signatures. In order to minimize the chances of such breakage, Signers SHOULD convert the message to a suitable MIME content-transfer encoding such as quoted-printable or base64 as described in [RFC2045] before signing. Such conversion is outside the scope of DKIM; the actual message SHOULD be converted to 7-bit MIME by an MUA or MSA prior to presentation to the DKIM algorithm.

MUST

DKIM ist per Design inkompatibel mit 8BITMIME.
Signer hat keine Kontrolle über Transformationen beim weiteren Transport und MUSS daher ein robustes 7-bit Format nutzen.

genua Ein Unternehmen der Bundesdruckerei

- DKIM setzt auf dem bereits kaputten MIME-Standard auf und der Fragilität von SMTP
- Probleme sind Autoren halbwegs bewusst, werden aber nur unzureichend adressiert
  - Keine (sicheren) Vorgaben welche Felder zwingend von Signatur umfasst sein müssen
  - Nutzloses aber gefährliches l-Attribut
  - SHOULD statt MUST für transport-resistente Kodierung vor Signierung
- Fundament wacklig → Kryptografie fragil