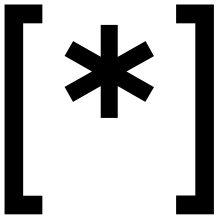


Patrick Ben Koetter | p@sys4.de | sys4 AG

Secure E-Mail Transport und E-Mail Authentication

Meine Rolle

- Autor beider Richtlinien im Auftrag des BSI
- Ich präsentiere für das BSI
- Ich repräsentiere nicht das BSI

Bundesamt
für Sicherheit in der
Informationstechnik

Inhalt

- TR-03108 für „Secure Email Transport“
  → Aktualisierungen
- TR-03182 für „Email Authentication“
  → Neufassung

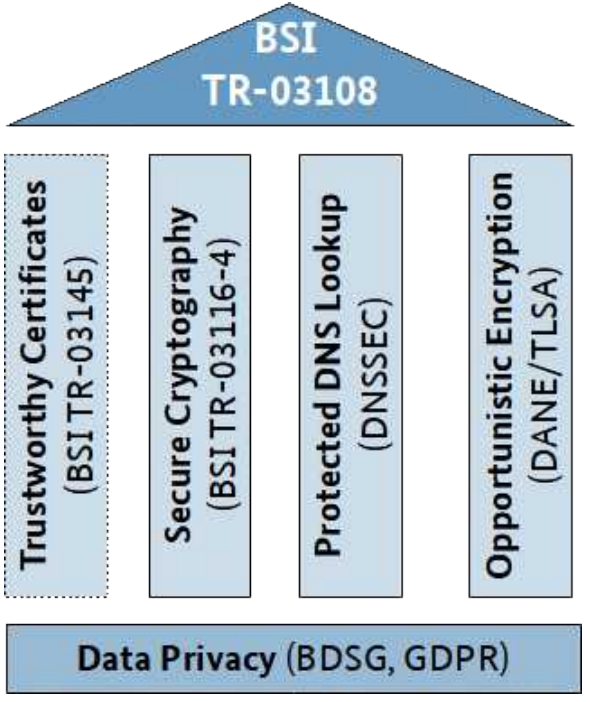
DNSSEC Resolution ist MUSS

DNSSEC Resolution: Argumentation

- DNS ist Policy-Dienst
- Missbrauchsvektor über Cache Poisoning
- Alle DNS-Abfragen müssen (RFC: MUST) DNSSEC-validierend durchgeführt werden
- Wenn eine DNS-Zone Antworten DNSSEC-signiert ausliefert kann durch DNSSEC-Validierung auf Empfängerseite Missbrauch erkannt und verhindert werden

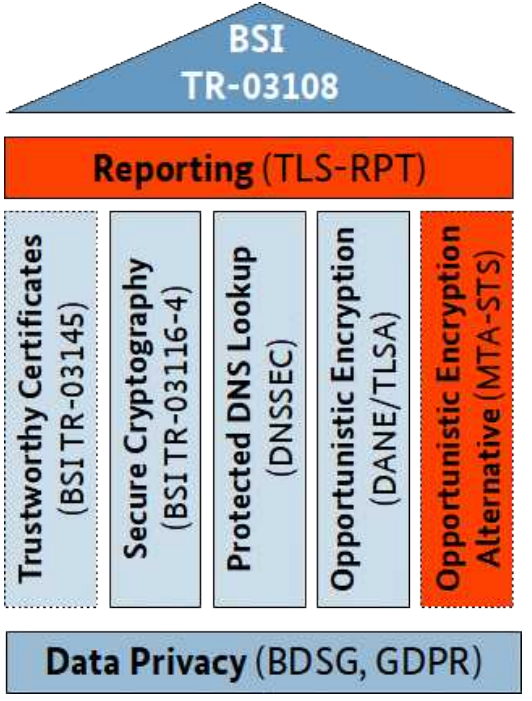
TR-03108

- Erstveröffentlichung 2016
- Sicherer E-Mail Transport
- Kernthemen
  - Opportunistic TLS
  - PFS
  - Sichere Zertifikate
  - DANE
- „Am Tisch“ mit der deutschen Internetindustrie entwickelt
- Blaupause für die EU-Mitgliedsstaaten



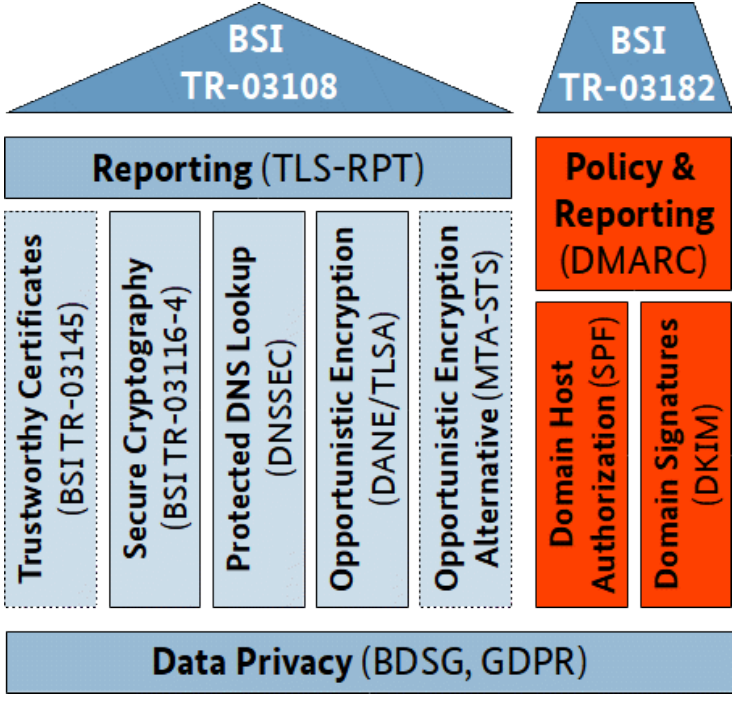
TR-03108: 2023

- Korrekturen / Konkretisierungen
- Neue Themen
  - DNSSEC Resolver (mandatory)
  - MTA-STS (optional)
  - TLS-RPT (mandatory)
- Best Practices / Kommentare



TR-03182

- Email Authentication
- Kernthemen
  - SPF
  - DKIM
  - DMARC
  - Reporting
- Best Practices / Kommentare
- Erstveröffentlichung 2023



TR-03182: Motivation

- Identitätsmissbrauch nach Malware größte Bedrohung durch E-Mail
- Großer wirtschaftlicher Schaden
- „no auth, no entry“ zwingt zur Einführung
- Belastbare, realitätsnahe Anforderungen
- Richtlinien, welche ein Sicherheitsniveau etablieren

CEO-FRAUD

Autozulieferer Leoni um 40 Millionen Euro betrogen

Mit dem sogenannten Chef-Trick erbeuten Kriminelle oft Millionenbeträge von Unternehmen. Mit fingierten E-Mails und Zahlungsanweisungen werden illegale Geldtransfers eingeleitet. Jetzt hat es einen großen deutschen Automobilzulieferer getroffen.

in Pocket speichern | merken

17. August 2016, 11:19 Uhr, Hauke Gierow

(Bild: Leoni AG)

Leoni stellt Kabelinfrastruktur her.

Der deutsche Automobilzulieferer Leoni ist um rund 40 Millionen Euro betrogen worden, wie das Unternehmen am Dienstag selbst bekanntgegeben hat. Die Angreifer nutzten dabei offenbar eine als Chef-Trick oder CEO-Fraud bekannt gewordene Masche, um sich Zugriff auf die Zahlungen zu sichern.

Quelle: Golem

TR-03182: Schutz geht vor Best Practices

- Bedeutung von SPF sinkt
  → DKIM in Richtlinie mandatory
- DKIM Algo ED25519 wichtig, aber wenig in Umlauf
  → ED25519 in Richtlinie mandatory
- DMARC-Reporting wichtig
  → meist nicht gesetzeskonform umsetzbar
- RUF-Reports könnten, temporär eingesetzt, gestattet sein, um „legitimes Interesse“ durchzusetzen
  → Rechtsgutachten bei eco in Arbeit
  → IETF will RUF abschaffen

Realität vs. BSI 1:0

Cisco ESA

„The email gateway supports keys from 512 bits up to 2048 bits. The 768 - 1024 bit key sizes are considered secure and used by most senders today. Keys based on larger key sizes can impact performance and are not supported above 2048 bits.“

BSI:Cisco – 0:1

BSI: RSA Schlüssellänge 2023

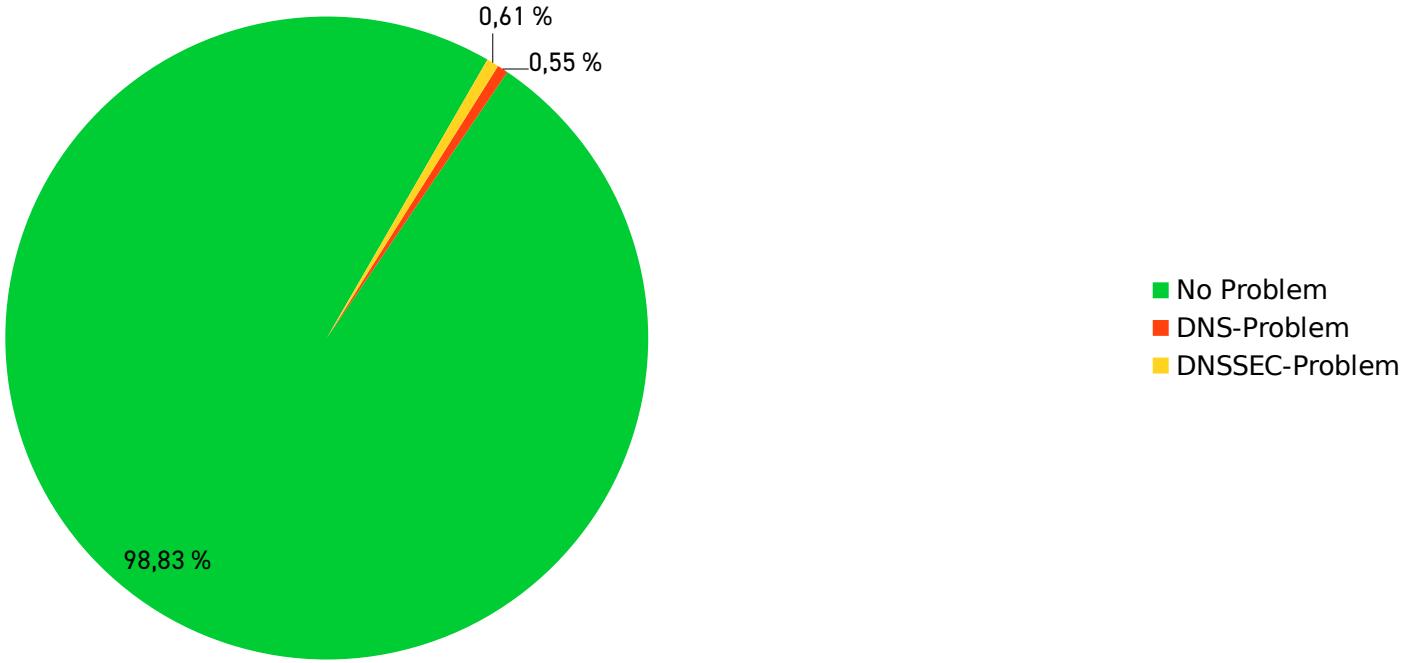
„Die Länge des Modulus n sollte mindestens 3000 Bits betragen…“

Quelle: BSI TR-02102-1

Cisco ESA

The email gateway supports keys from 512 bits up to 2048 bits. The 768 - 1024 bit key sizes are considered secure and used by most senders today. Keys based on larger **key sizes** can impact performance and **are not supported above 2048 bits.**

DNSSEC works!



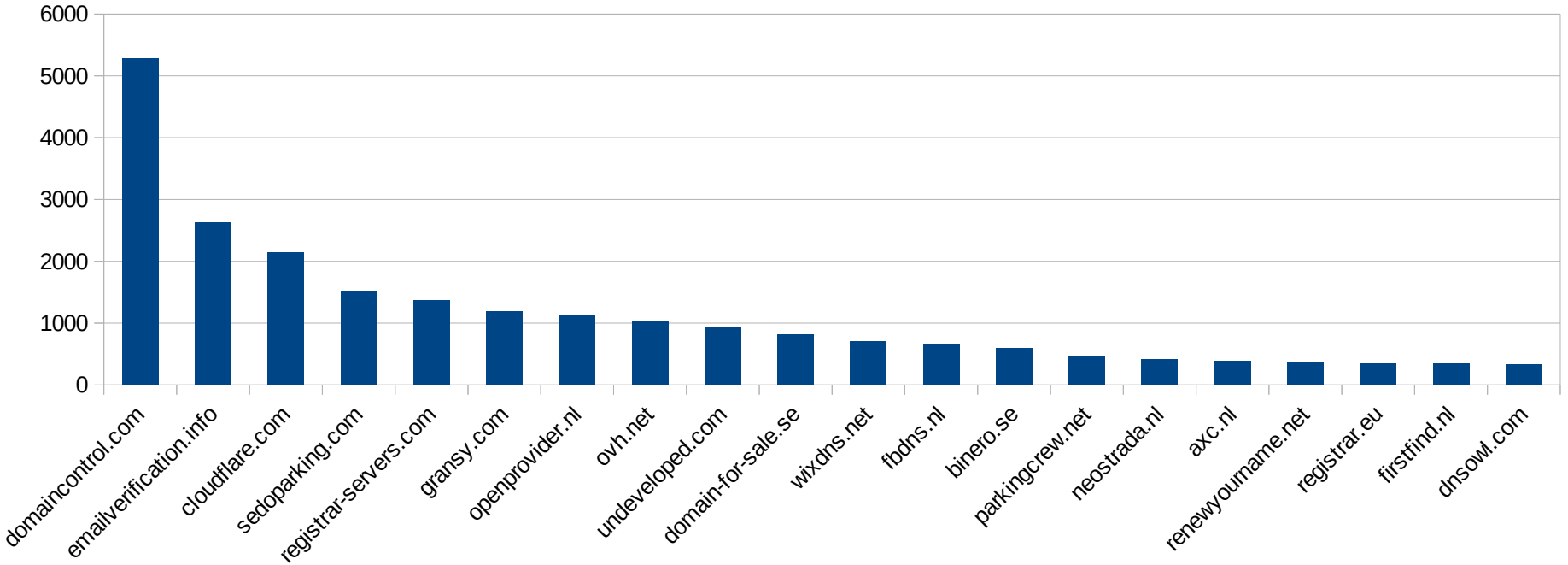
Viktor Dukhovni, 2020

Top 10 Tranco Ranking: Fake Shops

Domain	Rank
adidasnmds.com	23586
adidasoutletonline.com	26819
gb.com	58500
aru.ac.th	66661
gexperiments3.com	69196
nikefree-run.fr	74611
christian-louboutins.fr	76379
airjordanretro.fr	76665
ubu.ac.th	83489
saclongchamp-pascher.fr	90425

https://tranco-list.eu/

Owner sind Domain Reseller



Wissenswertes über SPF

- Policy der Senderdomain
- Publikation der Policy über DNS
- Policy legitimiert sendende Hosts und legt fest wie mit „allen anderen“ verfahren werden soll
- Use TXT TR. SPF RR ist deprecated

Positive SPF-Policy

```
sys4.de.     3600 IN TXT  "v=spf1
   ip4:194.126.158.132 \
   ip4:194.126.158.144 \
   ip4:188.68.34.52 \
   ip6:2001:1578:400:111::7 \
   ip6:2a03:4000:10:51d:b8ce:63ff:feca:a5a0 \
   -all"
```

- Relativ kurze TTL
- Einige werden direkt mit IP legitimiert
- Alle anderen Fail

Positive SPF-Policy mit include

```
list.sys4.de.     3600 IN TXT  "v=spf1 \
   include:_spf.list.sys4.de \
   -all"

_spf.list.sys4.de.  3600 IN TXT  "v=spf1 \
   ip4:188.68.34.52
   ip6:2a03:4000:10:51d:b8ce:63ff:feca:a5a0\
   -all"
```

- Senderdomain muss nicht aktualisieren
- Senderdomain kontrolliert all-Methode selbst

Negative SPF-Policy

```
example.com.   86400   IN TXT   "v=spf1 -all"
```

- Lange TTL
- Keiner wird legitimiert
- Alle anderen Fail

SPF-Policy: Best Practice

- Direkte Angabe von IP spart DNS round trips
- ~all ist gut wenn Mailinglisten im Spiel sind
- Kurze TTL gestattet schnelle Policy-Änderungen
- DNSSEC sichert Policy ab

SPF: Probleme

- Forwarder werden in Policy nicht berücksichtigt
- IP ist SPF trust anchor
- Shared-IP macht IP-basierte Reputation unbrauchbar
- Cloud-Nutzung
  - IP-basierte Policies schwierig
  - IP-Ranges konterkarieren „limited trusted range“

Der „UPS, Microsoft und Google“-Case

- UPS lagert (wie so viele) Mail Services an Microsoft aus
- UPS bindet include von Microsoft ein, damit MS-Plattform für SPF legitimiert wird

What could possibly go wrong?

```
dig +short TXT spf.protection.outlook.com
```

```
"v=spf1 \
  ip4:40.92.0.0/15 \
  ip4:40.107.0.0/16 \
  ip4:52.100.0.0/14 \
  ip4:104.47.0.0/17 \
  ip6:2a01:111:f400::/48 \
  ip6:2a01:111:f403::/49 \
  ip6:2a01:111:f403:8000::/50 \
  ip6:2a01:111:f403:c000::/51 \
  ip6:2a01:111:f403:f000::/52 \
  -all"
```

- `$JEMAND` sendet über einen MS-Tenant als ups.com an gmail.com
- gmail.com nimmt Mail an, weil legitimiert über SPF
- DMARC Policy ist erfüllt
- BIMI wird aktiviert
- Abuse Mail wird mit UPS-Logo in Inbox dargestellt

(siehe: Gmail spoofing vulnerability sparks Google ‘Priority 1’ probe)

SPF: Das Cloud-Problem

- Cloud hat große IP-Ranges
- Große IP-Ranges bieten große Angriffsfläche
- Große IP-Ranges gestatten zu wenig Kontrolle

→ SPF nicht mehr für Use Case „Email Authentication“ geeignet

→ [dmarc-ietf] DMARC2 & SPF Dependency Removal

Wissenswertes über DKIM

- Policy der Senderdomain
- Publikation der Policy über DNS
- Policy identifiziert legitim sendende Hosts mittels Signatur in der Nachricht
- Forward-Safe wenn `From:` und `Subject:` nicht verändert werden

101 DKIM-Signature

```
DKIM-Signature: v=1; a=ed25519-sha256; c=relaxed/simple; d=bsi.bund.de;
        s=211014-e768-ed25519; t=1689085905;
        bh=dmpvrsMo/bwTZ/cEsXfOVNGbtflNsCod5CP7uqyBpcQ=;
        h=From:To:CC:Subject:Date:References:In-Reply-To:Content-Type:
        MIME-Version:Autocrypt:Cc:Content-Transfer-Encoding:Content-Type:
        Date:From:In-Reply-To:Mime-Version:Openpgp:References:Reply-To:
        Resent-To:Sender:Subject:To;
        b=PVfuqzkQCrwpcs96p7VrWlQMkINTooqvlvybEZ+GLpSkCegXlDLGHPhRNpvu0lRVv
        3StdOaA8k1pssVy8Cj5Cg==
```

...

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=bsi.bund.de;
        s=211014-e768-rsa; t=1689085905;
        bh=dmpvrsMo/bwTZ/cEsXfOVNGbtflNsCod5CP7uqyBpcQ=;
        h=From:To:CC:Subject:Date:References:In-Reply-To:Content-Type:
        MIME-Version:Autocrypt:Cc:Content-Transfer-Encoding:Content-Type:
        Date:From:In-Reply-To:Mime-Version:Openpgp:References:Reply-To:
        Resent-To:Sender:Subject:To;
        b=dKcTXDW8jMIOUFgDqyZtQq9wZup+o43TfgaGLv2yZkgG5ihLpIqn3Az49X638lB0b
        bKZWD9hrVEUM1O+0D0kV5BQS1oePDA3cNTFyOP70NfrbiG+iZzpuuCE1252yp4HYma
        MU07x9FZt2rArtDvIemkFuFHg+qM10ApokXODc6fg0h2wDIkhU4rYq1vQKdrL8C9Ja
        uHBF57vv+sF9ddggDTQtxRIlD8rtt6vtzweZ77udjbjX9MMUQCefmblCSGVyxalQRz
        gDU6iVzMd45icqcrqkqd1lZL3rZ30S5js14yX3BJ5CxAEWvOYDfZzBSGu7za3/paSt
        NPUWX7N6jt/7A==
```

Algo-Migration

…

```
DKIM-Signature: v=1; a=ed25519-sha256; c=relaxed/simple;
d=bsi.bund.de;
```

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
d=bsi.bund.de;
```

…

- Doppelt signieren
- Verifier wählt aus

DKIM: Status Quo Algorithmen / Hashes

- SHA1 deprecated, aber immer noch ~1% in use
- RSA-SHA256 ist Standard
- ED25519-SHA256 sollte verwendet werden

DKIM: Theorie vs. Praxis

- RSA mit Bitlänge > 2048 gefordert
- Appliances failen bei Bitlänge > 2048

→ Nutzt max. Bitlänge 2048 **und** rotiert öfter

Wissens... DMARC

- Policy der Senderdomain
- Publikation der Policy über DNS
- Policy-Framework für Email Authentication
- Reporting-Mechanismus

DMARC-Policy: Example

```
_dmarc.bsi.bund.de.  600 IN  TXT "v=DMARC1; \
  p=reject;\
  rua=mailto:bsi.bund.de@dmarc.reports.bund.de;"
```

- Kurze TTL für schnelle Änderungen (→ business continuity)
- Nur `p=quarantine` oder `p=reject` etablieren Schutz
- `p=none` perfekt für Testphase während des Policy Stagings
- rua ist gut. ruf ist böse. ;-)

DMARC Reporting

- Reporting ist Schlüssel zur Einführung einer produktiv genutzten Domain
- Testphase mit `p=none`
- Schatten-IT identifizieren und compliant machen
- Stagen

Bonusrunde: Negative Policies

- taint-Mode für Senderdomains
  - Sunsetten / Parken von Domains
  - Subdomains aktiv vor abuse schützen
- Kombination von drei Mechanismen
  - „Null MX“-Eintrag
  - SPF „none und Fail“ policy
  - DMARC „p=reject“

Negative Policy: Example

```
www   IN    A     192.0.2.1
      IN    AAAA  2001:db8::2:1
      IN    TXT   "v=spf1 -all"
      IN    TXT   "v=DMARC1; p=reject; \
                     rua=mailto:rcpt@example.com;"
      IN    MX    0  .
```

Danke!

Patrick Koetter

sys4 AG
Schleißheimer Straße 26
80333 München

+49 176 30090466
p@sys4.de