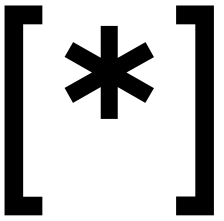


Patrick Ben Koetter | p@sys4.de | sys4 AG

Secure Email Transport and E-Mail Authentication

My role

- Author of both Technical Guidelines on behalf of BSI
- I present on behalf of BSI
- I do not represent BSI

Bundesamt
für Sicherheit in der
Informationstechnik

TOC

- TR-03108 for „Secure Email Transport“
  → Updates
- TR-03182 for „Email Authentication“
  → New Formulation

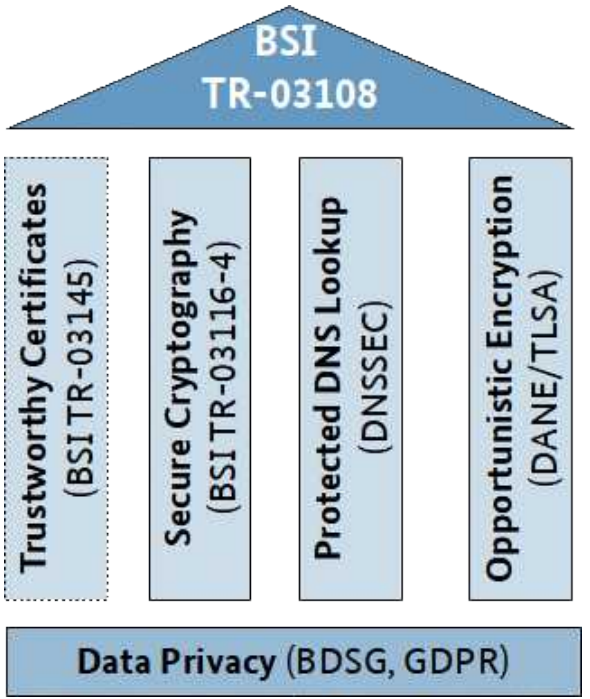
DNSSEC Resolution is a MUST

DNSSEC Resolution: Argumentation

- DNS has become a policy service
- Attack vector via DNS Cache Poisoning
- All DNS-Queries must (RFC: MUST) use DNSSEC validation
- A DNSSEC signed DNS zone will allow to detect and prevent DNS based abuse

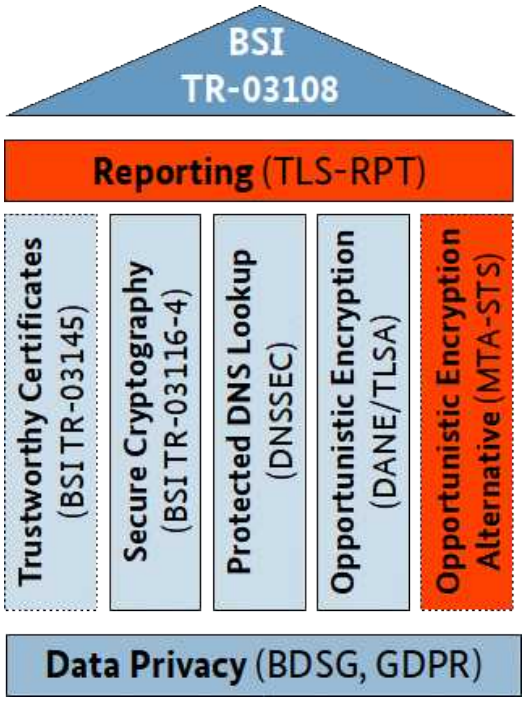
TR-03108

- First release in 2016
- Secure Email Transport
- Core topics
  - Opportunistic TLS
  - PFS
  - Secure Certificates
  - DANE
- Developed in close cooperation with German Internet industry
- Blueprint for Secure Email in many EU member states



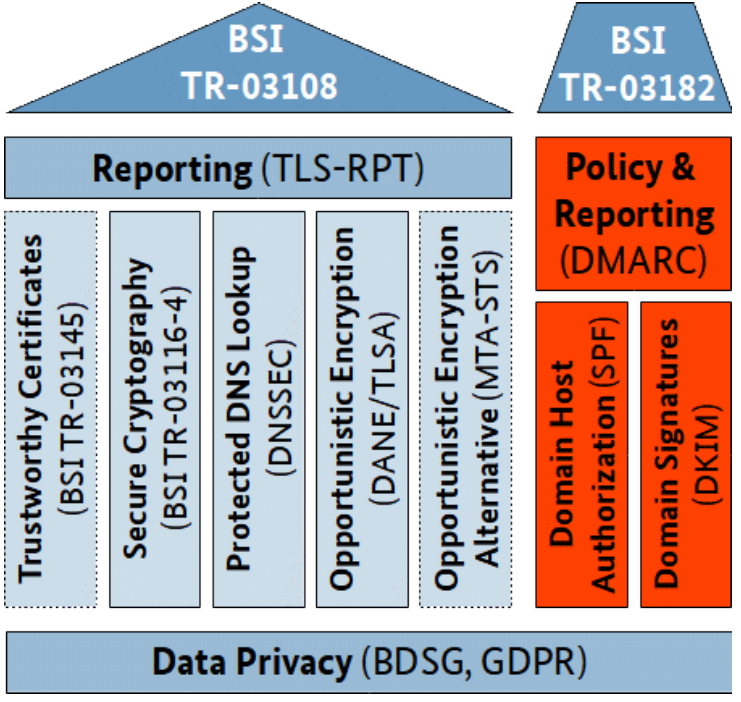
TR-03108: 2023

- Corrections / Concretizations
- New topics
  - DNSSEC Resolver (mandatory)
  - MTA-STS (optional)
  - TLS-RPT (mandatory)
- Best Practices / Commented



TR-03182

- Email Authentication
- Core topics
  - SPF
  - DKIM
  - DMARC
  - Reporting
- Best Practices / Commented
- First release 08 / 2023 (planned)



TR-03182: Motivation

- Identity abuse in Email biggest threat after Malware
- Major economic loss
- „no auth, no entry“ forces introduction
- Realistic, practical requirements
- Policies that establish a security level

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: Protection over Best Practices

- Importance of SPF on the decline
  → DKIM becomes mandatory
- DKIM Algo ED25519 important, but hardly used
  → ED25519 becomes mandatory
- DMARC-Reporting important
  → hard to implement conforming to (German) law
- RUF-Reports could be permitted temporarily to enforce „legitimate interest“
  → legal opinion on its way at eco e.V.
  → IETF likely to deprecate RUF

Reality 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 Keylength 2023

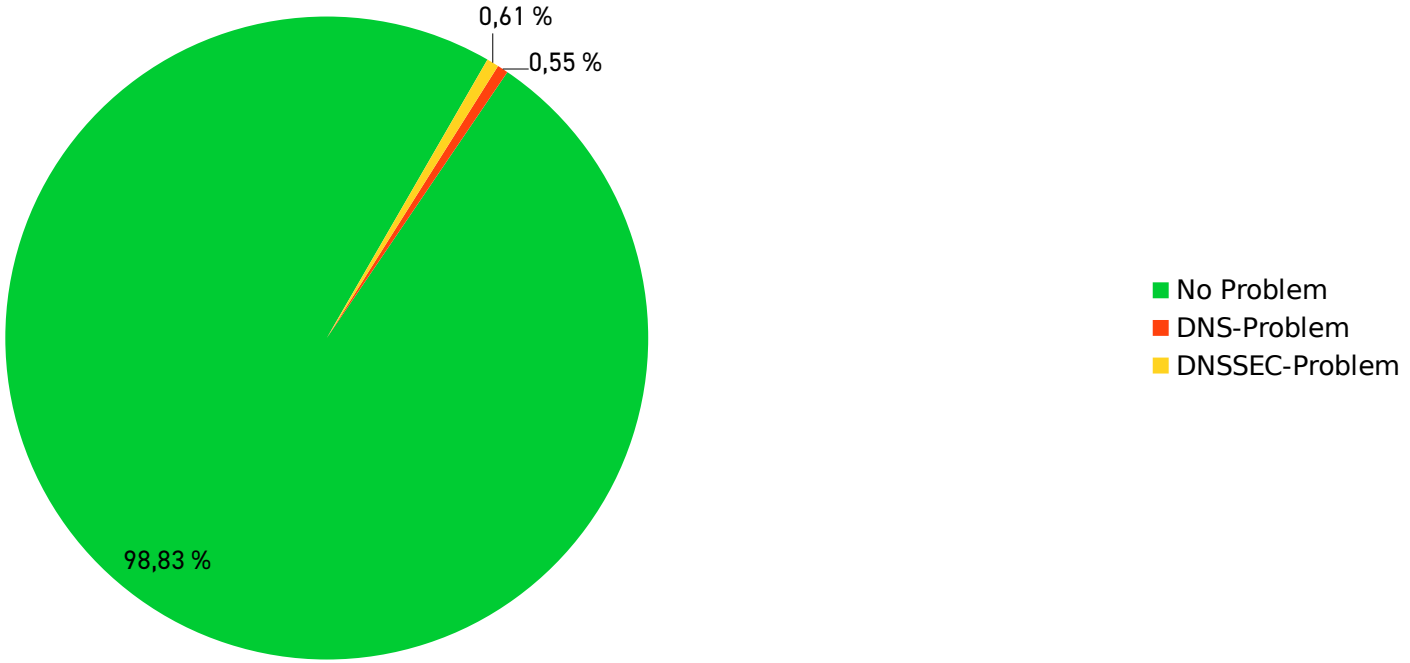
„Die Länge des Modulus n sollte mindestens 3000 Bits betragen…“

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!



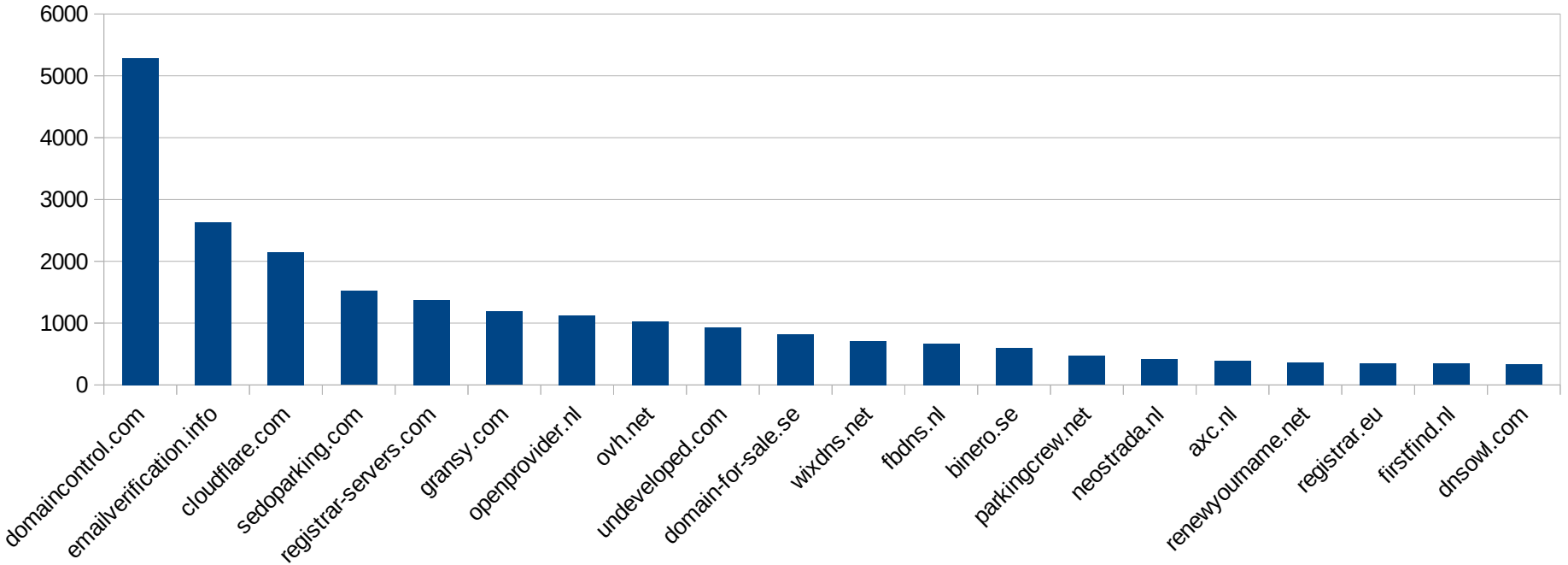
Viktor Dukhovni, 2020

Top 10 Tranco Ranking

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



Thank you!

Patrick Koetter

sys4 AG
Schleißheimer Straße 26
80333 München

+49 176 30090466
p@sys4.de