Kurzeinführung in DNSSEC und der Stand unter .at

RTR Workshop E-Mail Sicherheit

Otmar Lendl
<lendl@cert.at>

Überblick

Vorstellung

- Mag. Otmar Lendl
  - Computerwissenschaften und Mathematik an der Universität Salzburg
  - Betreibe seit 1991 Server im Internet
  - 5 Jahre ISP-Erfahrung (EUnet, KPNQwest)
  - nic.at R&D (primär ENUM, zwei RFCs geschrieben)
  - Seit 2007: Teamleitung Österreichisches nationales CERT

Inhalt

- Warum DNSSEC?
- Wie funktioniert DNSSEC?
- Wie schaut es unter .at aus?

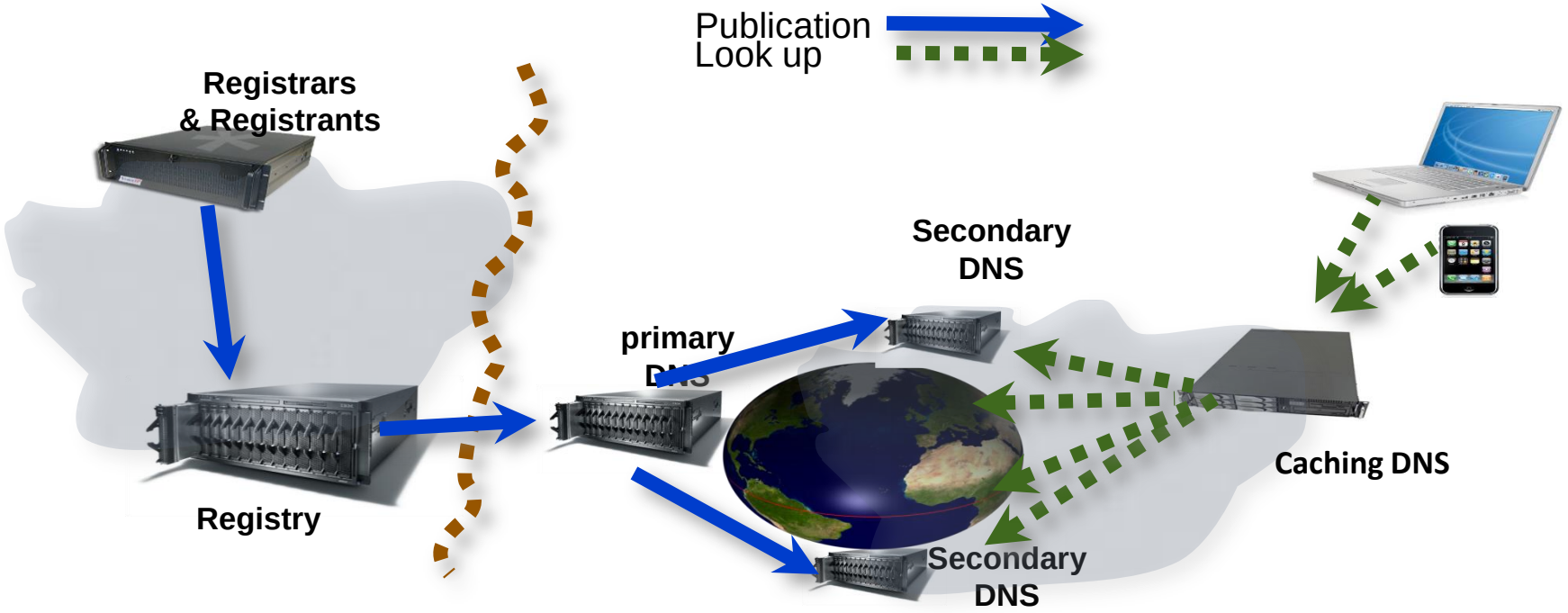
- (nur ganz kurz, mein üblicher DNSSEC Workshop dauert 4 Stunden)

Danke an Michael Braunöder, Olaf Kolkman, Phil Regnauld, … für die Erlaubnis, aus ihren Slides zu zitieren.

Wie wichtig ist das DNS?

- DoS (in beide Richtungen)
- Man-in-the-middle almost *everything*
  - Phishing
  - Email hijacking
- Password reset emails
- Software Updates
- SSL and PKI for the rescue?
  - How do users react to X.509 errors?
  - CA email-loop
  - CA whois lookup
- Für den Enduser ist „DNS kaputt“ nicht von „Internet ist kaputt“ unterscheidbar

Data flow

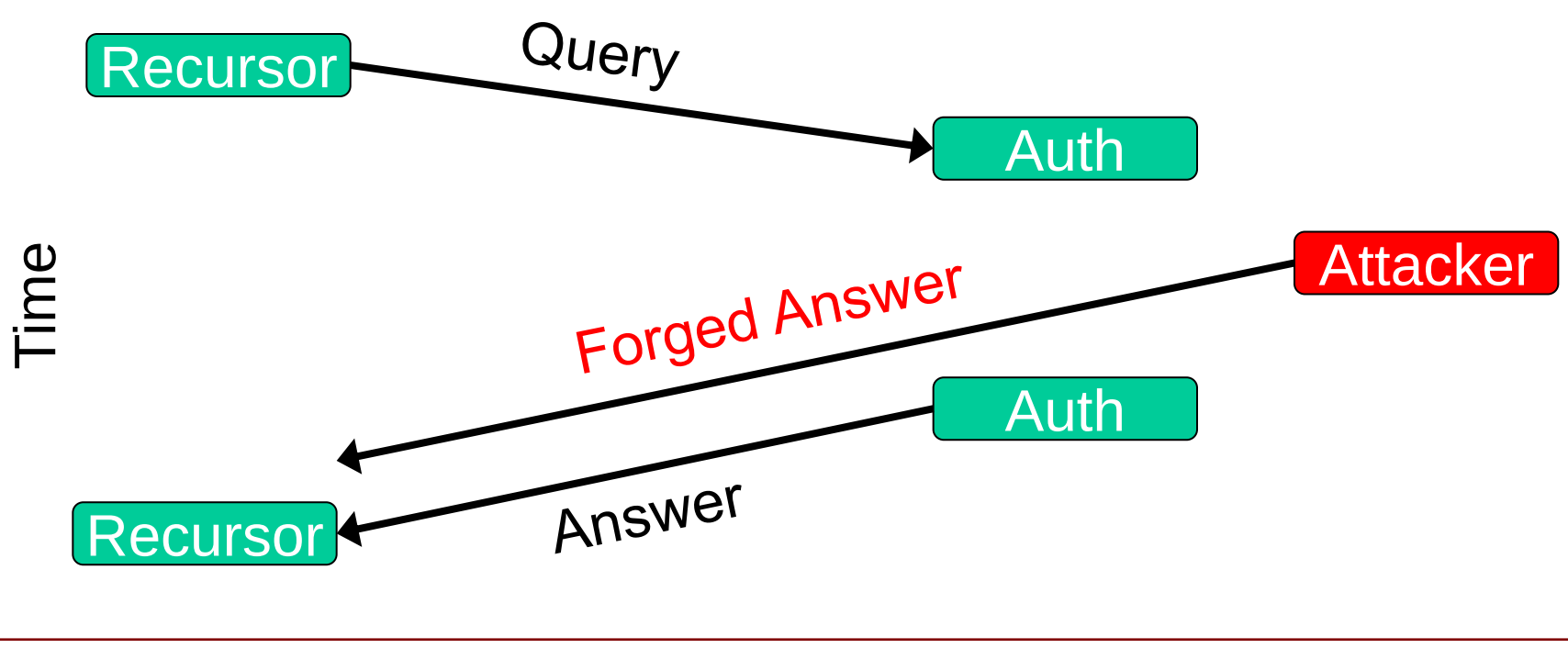

Publication
Look up
Registrars
& Registrants
Registry
primary
DNS
Secondary
DNS
Secondary
DNS
Caching DNS

Gefahrenanalyse

- Provisioning side
- Cache poisoning
  - Off-path attacks
  - On-path attacks
- Falsche Antwort durch den Recursor
  - Sitefinder
  - NXdomain monetizing

- Siehe auch RFC 3833

DNS Spoofing



Off-Path Cache-Poisoning

- Das ist nichts neues.
- Berechnungen zur Erfolgswahrscheinlichkeit in RFC 5452
- „Kaminsky“ Attack in 2008
  - Source Port Randomization als Mitigation

Welche Security?

- Confidentiality
  - Kann wer mitlesen?
- Integrity
  - Stimmt das, was ich bekommen habe?
- Availability
  - Bekomme ich überhaupt eine Antwort?

DNSSEC betrifft ausschließlich „Integrity“!

Grundidee

- Kompatible Erweiterung des DNS
- Public Key Kryptografie Signaturen innerhalb der DNS Antworten
- Schutz der Daten, nicht Schutz des Transports
- Delegationshierarchie des DNS wird auch zur Trust-Hierarchie

DNSSEC Specs

- Details zum Nachlesen:
  - RFC4033, “DNS Security Introduction and Requirements”
  - RFC4034, “Resource Records for the DNS Security Extensions”
  - RFC4035, “Protocol Modifications for the DNS Security Extensions”
  - RFC5011, “Automated Updates of DNS Security (DNSSEC) Trust Anchors“
  - RFC5155, “DNS Security (DNSSEC) Hashed Authenticated Denial of Existence”

New Resource Records

- Three Public key crypto related RRs
  - RRSIG — Signature over RRset made using private key
  - DNSKEY — Public key, needed for verifying a RRSIG
  - DS — Delegation Signer; ‘Pointer’ for building chains of authentication
- Two RR for internal consistency
  - NSEC — Indicates which name is the next one in the zone and which typecodes are available for the current name.
  - NSEC3 — NSEC++

DNSSEC Queries

- DO
  - DNSSEC OK (EDNS0 OPT header) to indicate client support for DNSSEC options
  - EDNS0 is required for DNSSEC
- CD
  - “Don’t check signatures for me, just give me the raw DNSSEC records”

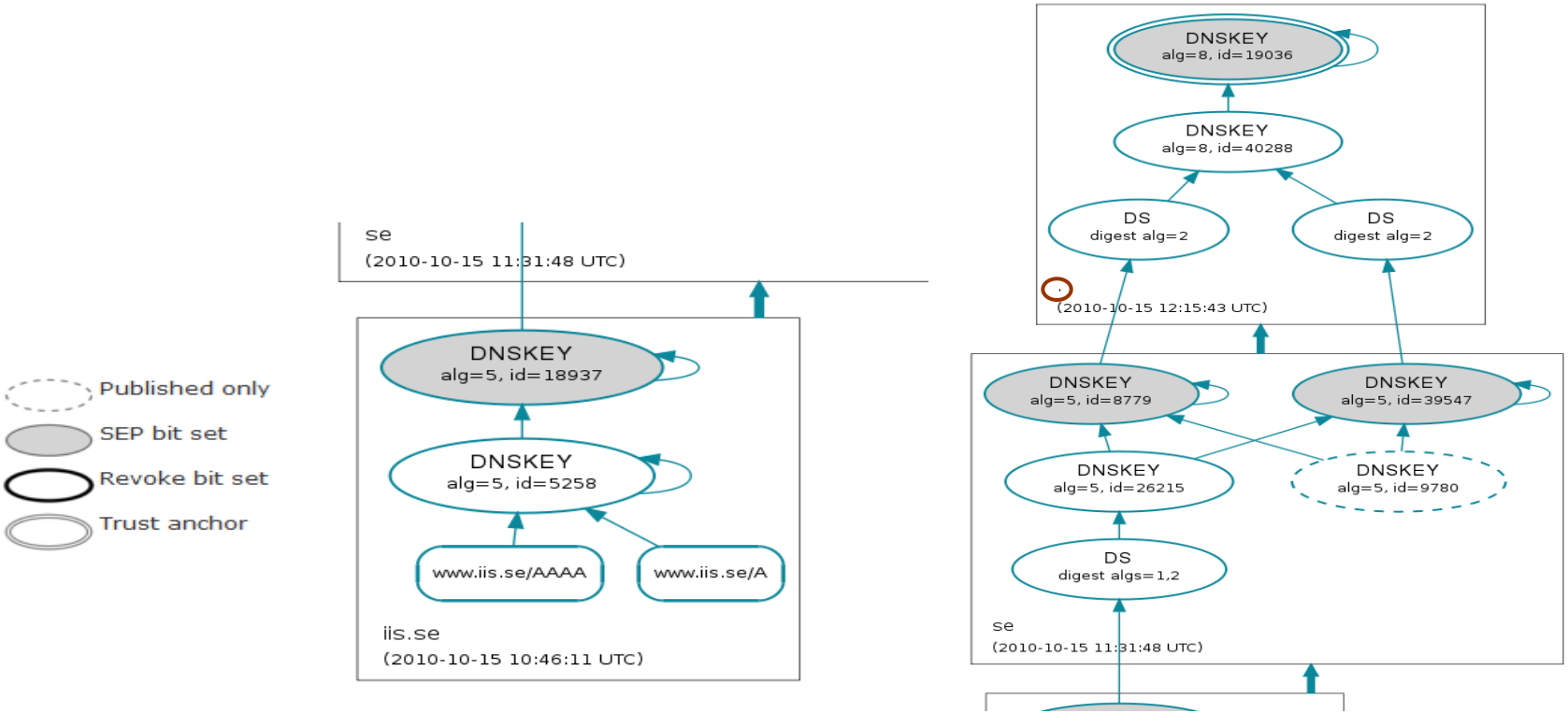
DNSSEC Answers

- SECURE Validated with key
  - AD – bit set in Packet
- INSECURE Validated but no key
- BOGUS Validation failed
- UNKNOWN ServFail etc

Key management

- To allow for key updates (“rollovers”), generate two keys:
  - Key Signing Key (KSK)
    - pointed to by parent zone (Secure Entry Point), in the form of DS (Delegation Signer)
    - used to sign the Zone Signing Key (ZSK)
  - Zone Signing Key (ZSK)
    - signed by the Key Signing Key
    - used to sign the zone data RRsets
- This decoupling allows for independent updating of the ZSK without having to update the KSK, and involve the parent.

http://dnsviz.net/



DNSSEC vs. X.509

- Komplett getrennte Systeme
  - Es basiert nur beides auf Public Key Crypto
- Konzept der „Certification Authority“ existiert bei DNSSEC nicht
  - Ein Einbruch bei z.B. der DENIC ist für die Sicherheit von .at irrelevant

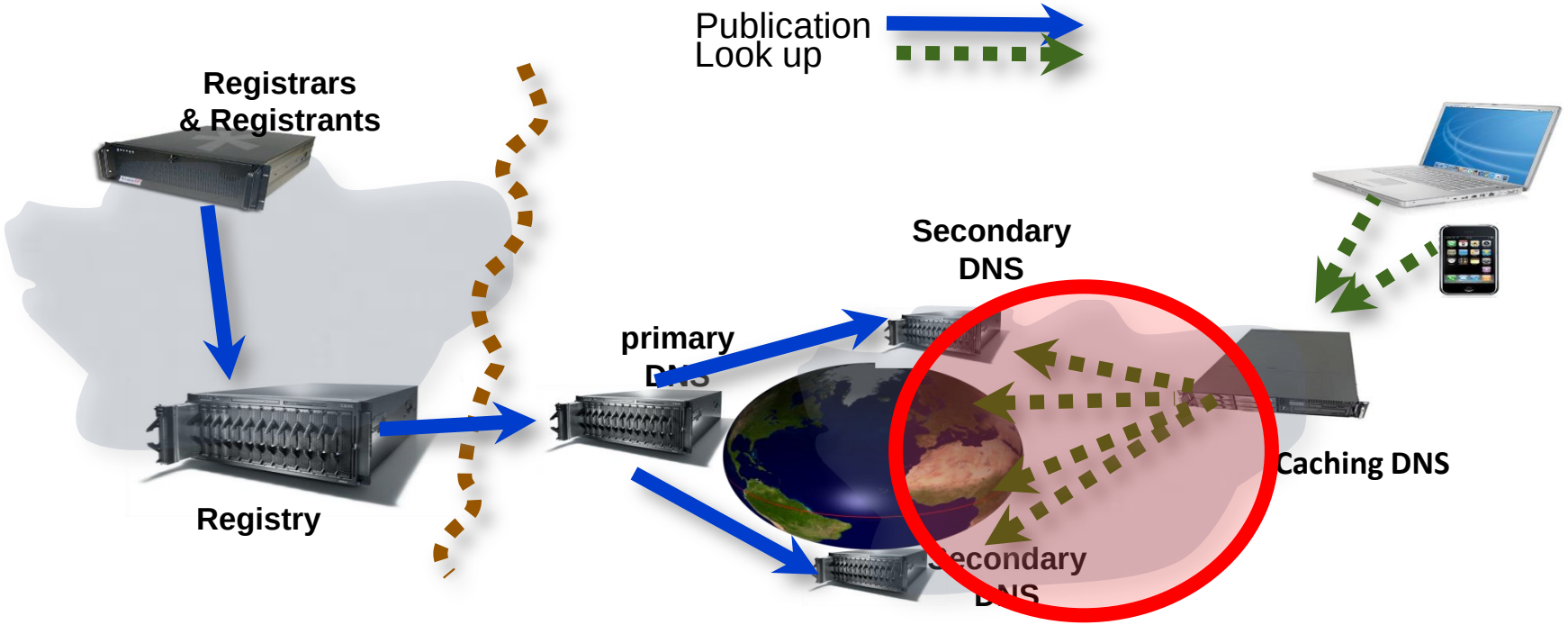
Deployment Server-side

- Key management
  - Generate keys
  - Add DNSKEY records
- Sign zone
  - Signing & serving need not be performed on same machine
  - Signing system can be offline
  - Signing can be out-sourced (e.g. rcodezero.at)
- Make sure authoritative nameservers handle DNSSEC
- Communicate your keys to parent zone

Deployment Client-side

- Stub-Resolver speaks DNSSEC
  - Inefficient
  - Slow rollout
  - Upsides in User-Interface
- Recursor does DNSSEC Validation
  - Need a way to secure last hop
  - Huge multiplier possibilities
- Secure Entry Points?

Was schützt DNSSEC?



Sicherheit vs. Verfügbarkeit

- Plain DNS ist robust
  - Sehr fehlertolerant
  - Oft komplett auf Autopilot
- DNSSEC ist spröde
  - Ein falsches Bit und die Zone ist offline.
  - Kompetentes Operating nötig.
  - DNSSEC nicht unüberlegt einführen!
  - Fehler werden passieren.

Deployment Timeline

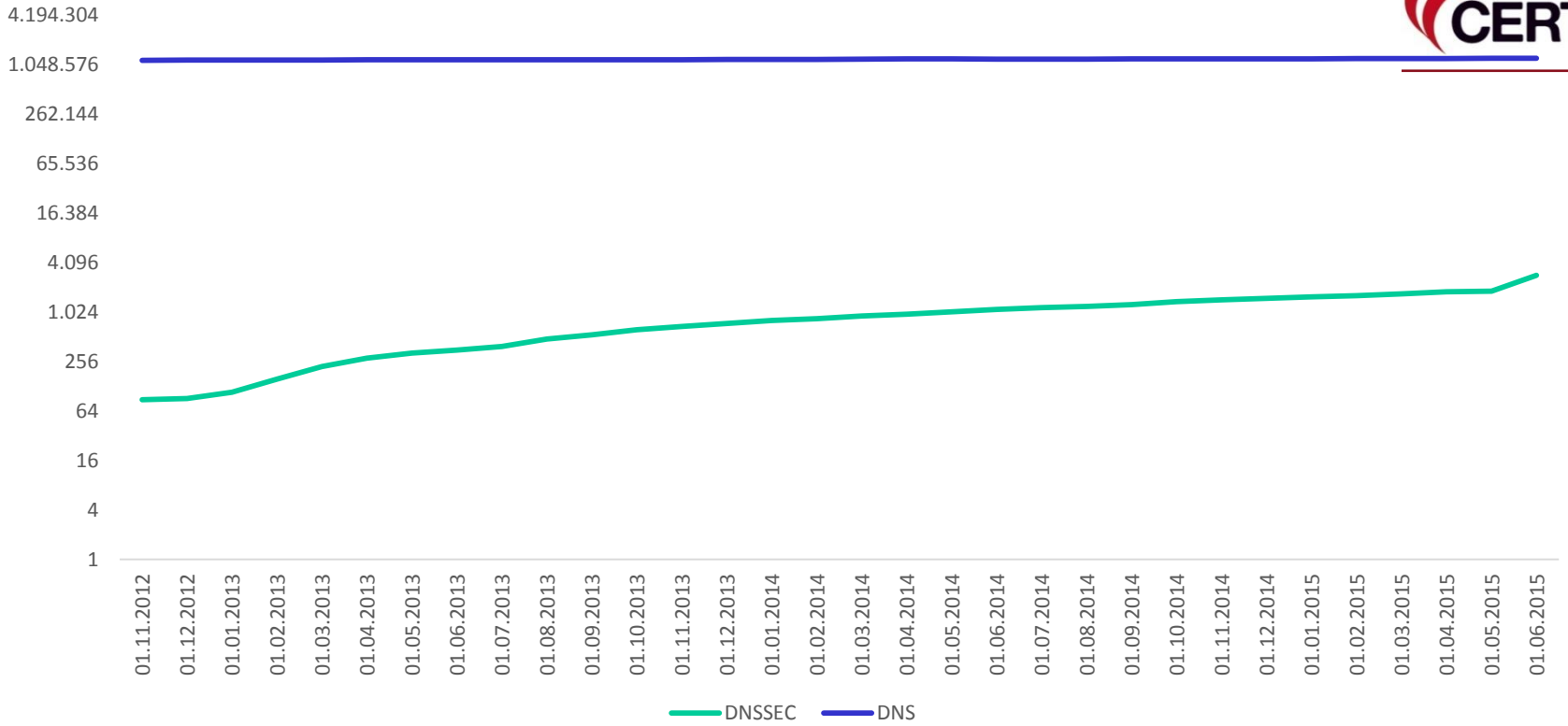
- Viele signierte Inseln, DLV, …
- Juli 2010: Root signiert
- Februar 2012: .at signiert
- Noch nicht signiert:
  - gv.at
  - ac.at
  - priv.at

Deployment-Statistiken?

- http://www.internetsociety.org/deploy360/dnssec/statistics/
- http://scoreboard.verisignlabs.com/
- http://www.huque.com/app/dnsstat/
- https://xs.powerdns.com/dnssec-nl-graph/
- https://www.dnssec-deployment.org/

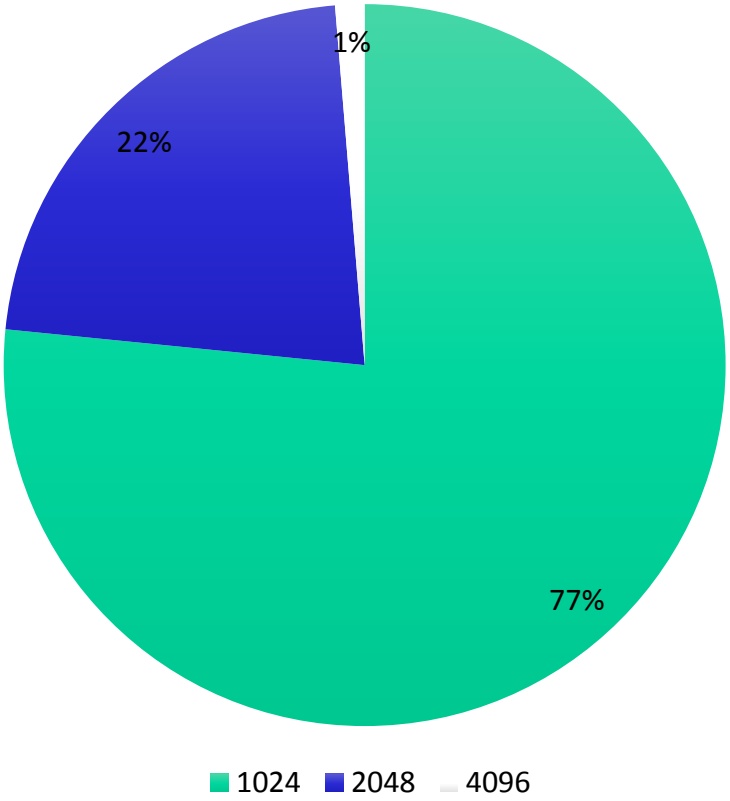
Aktueller Status .at:

Signierte Zonen:	2906 (~ 0.2%)
Gültig signierte Zonen:	2610 (89%)
Zonen mit fehlerhaften Signaturen:	300 (10%) (kann sich mit OK überschneiden, wenn mehrere Signaturen vorhanden sind)
Registrare, die DNSsec verwenden:	28

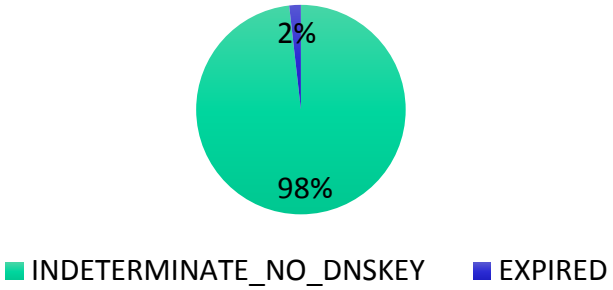


Die Graphen der nächsten vier Slides stammen von Daniel.kissler@gmail.com

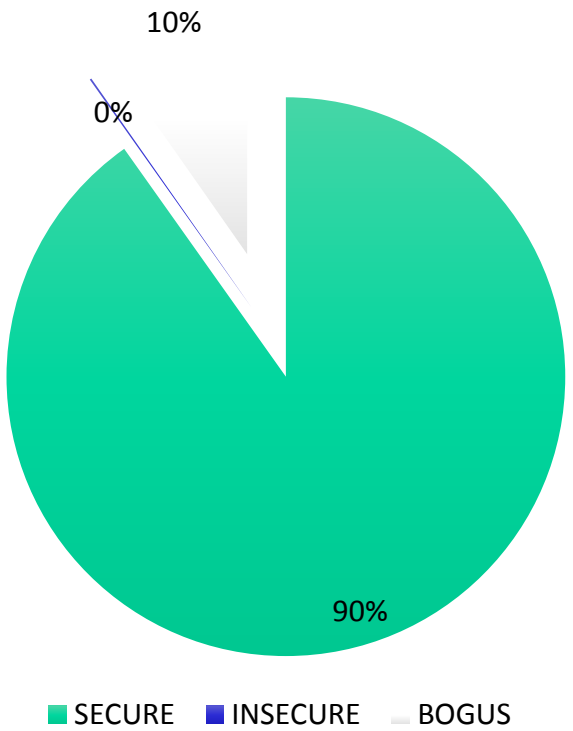
Keysize



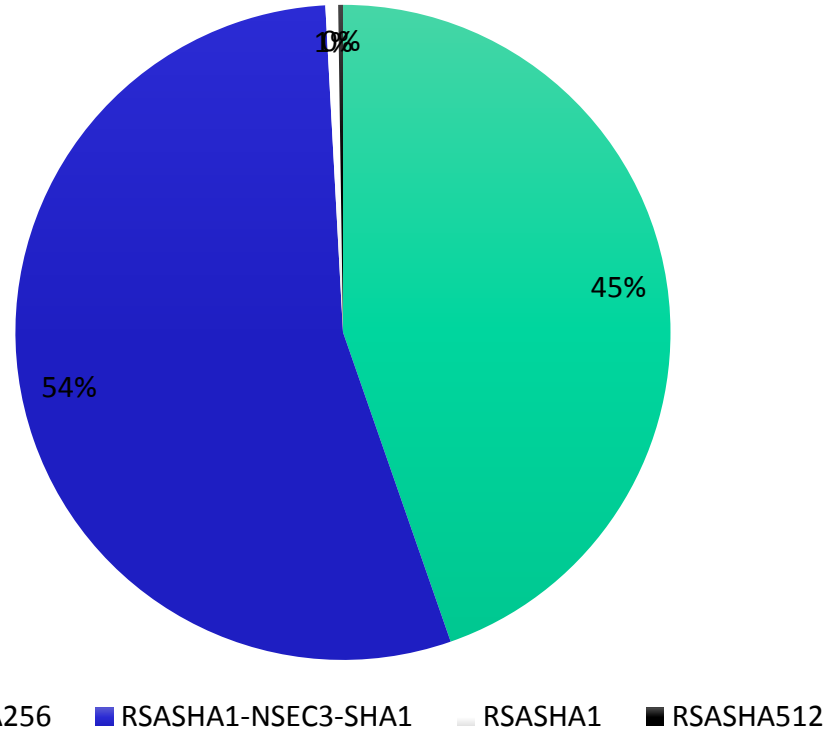
BOGUS


2%
98%
INDETERMINATE_NO_DNSKEY
EXPIRED

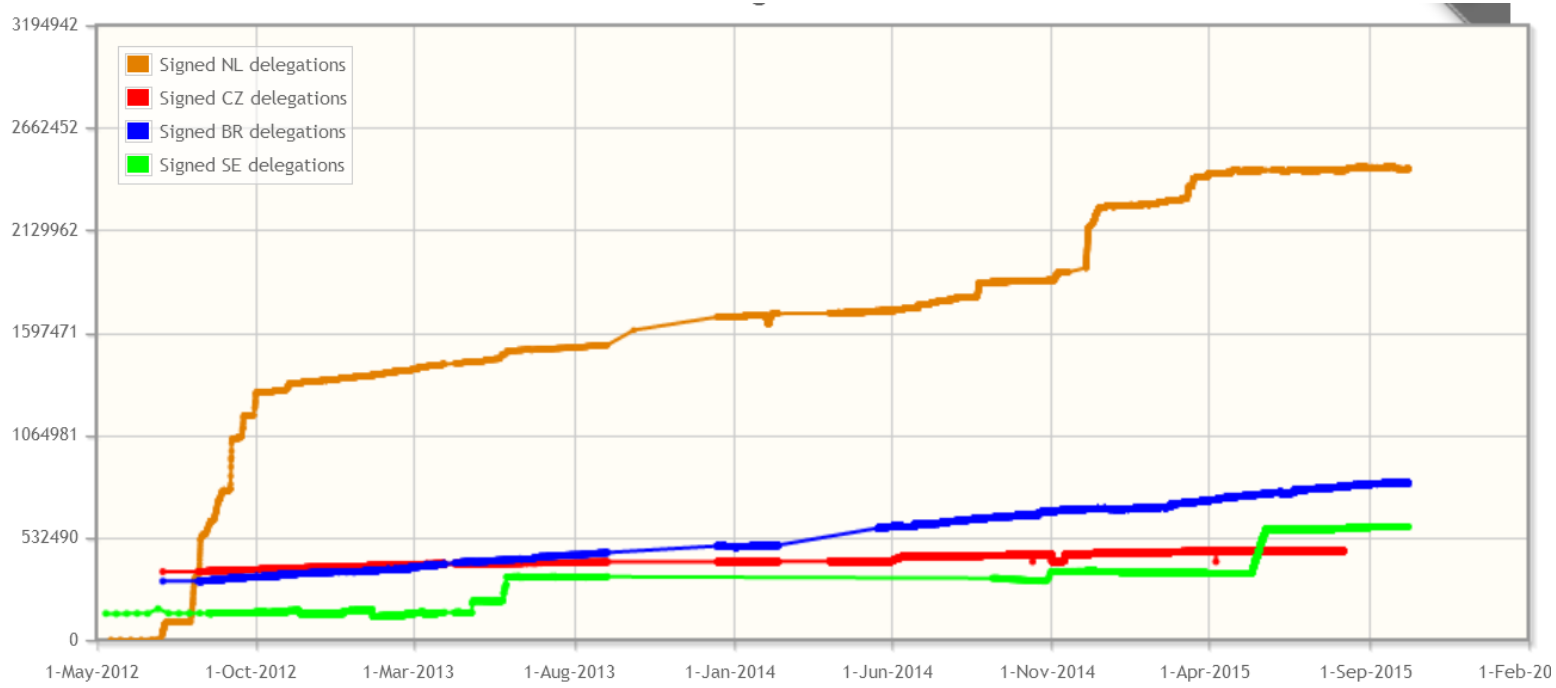
Count


10%
0%
90%
SECURE
INSECURE
BOGUS

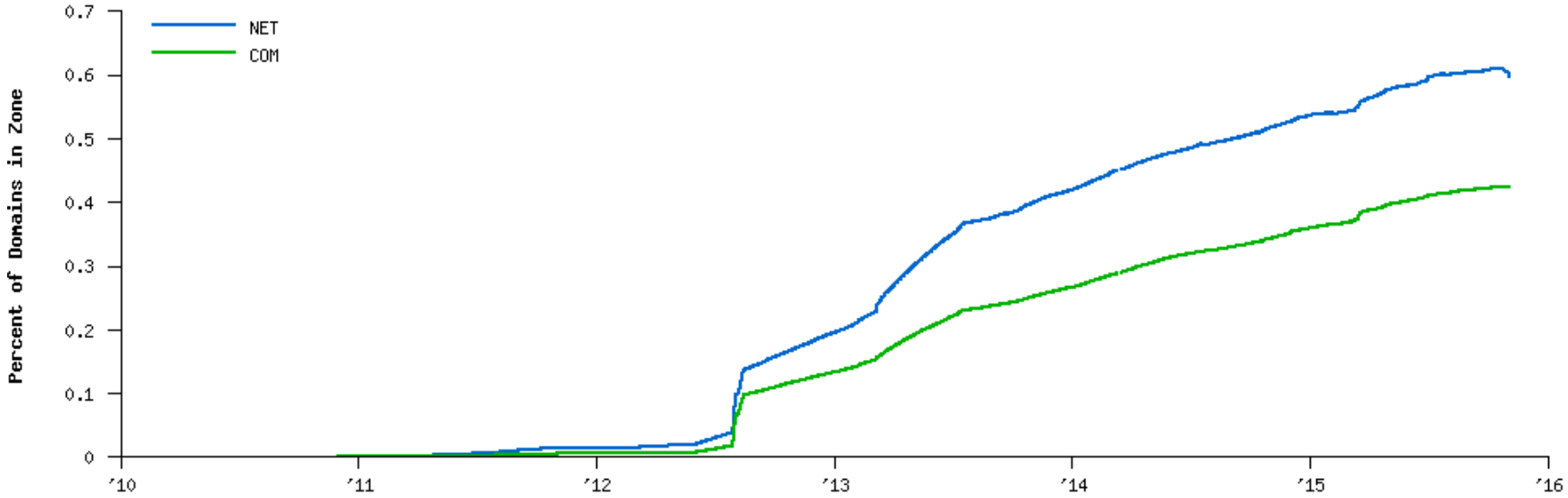
Algorithm



https://xs.powerdns.com/dnssec-nl-graph/



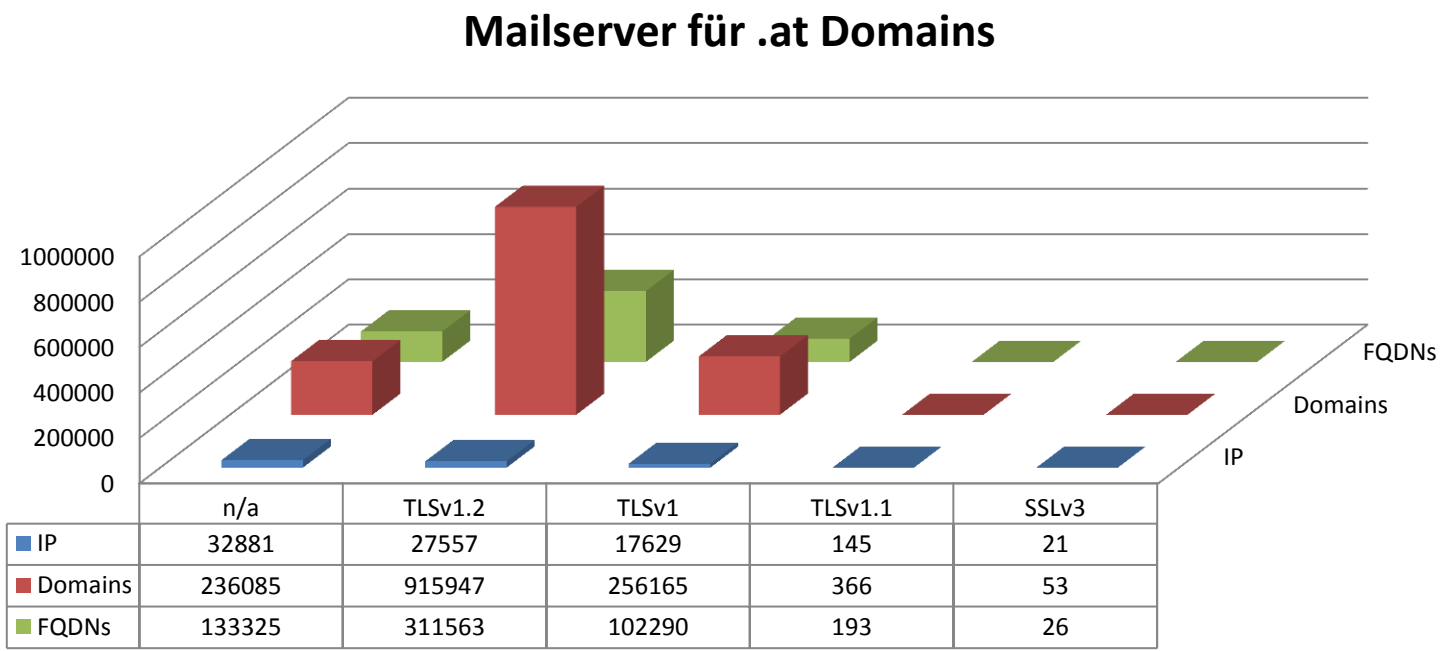
http://scoreboard.verisignlabs.com/percent-trace.png



TLS Studie

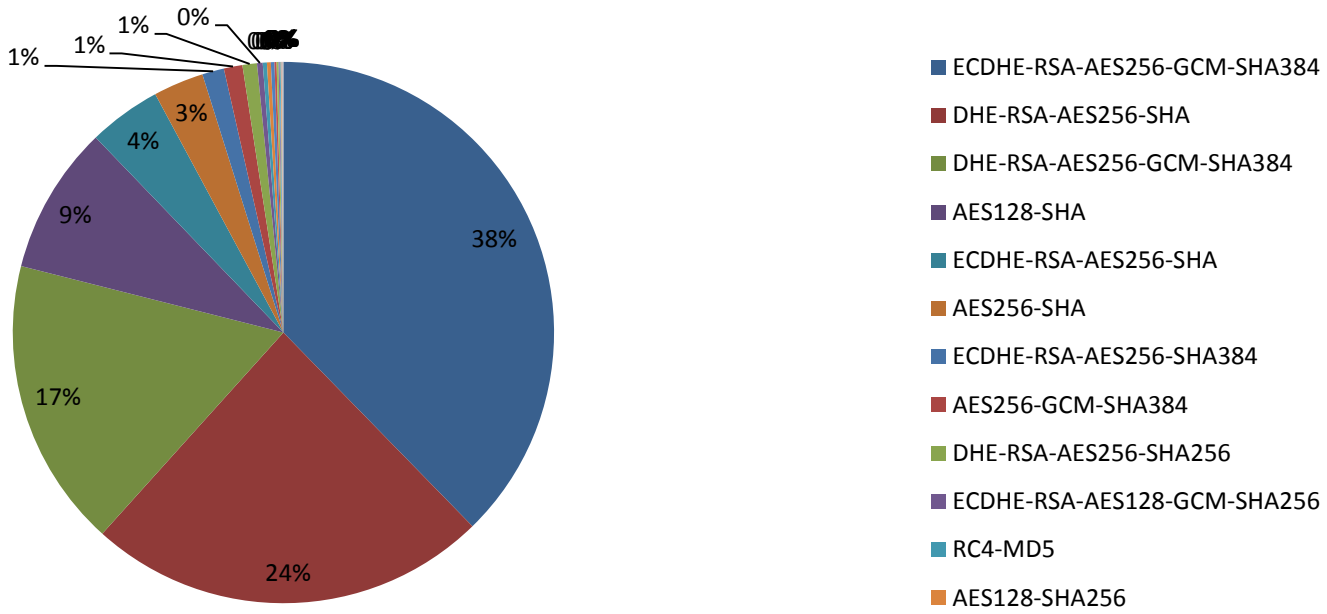
- 1.415.472 Domains unter .at
- 549.914 Hostname in MX records
- 78.233 IP Adressen

TLS Support

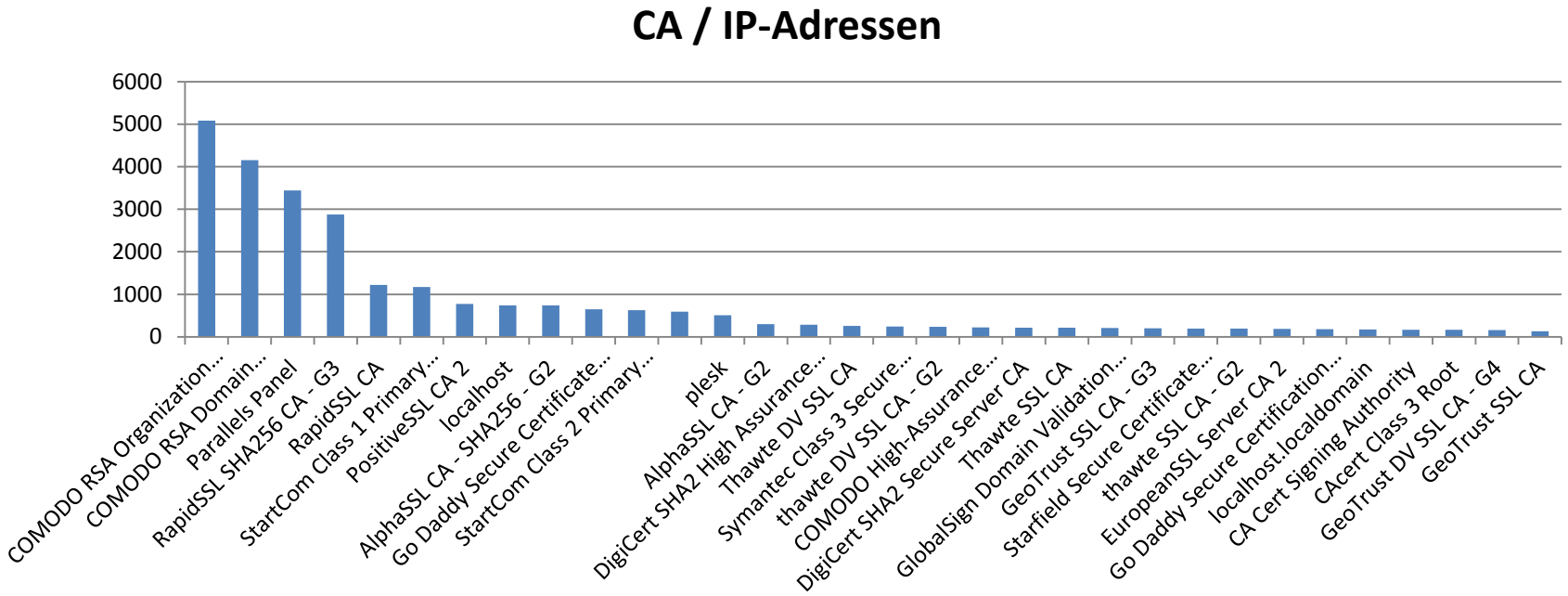


	n/a	TLSv1.2	TLSv1	TLSv1.1	SSLv3
IP	32881	27557	17629	145	21
Domains	236085	915947	256165	366	53
FQDNs	133325	311563	102290	193	26

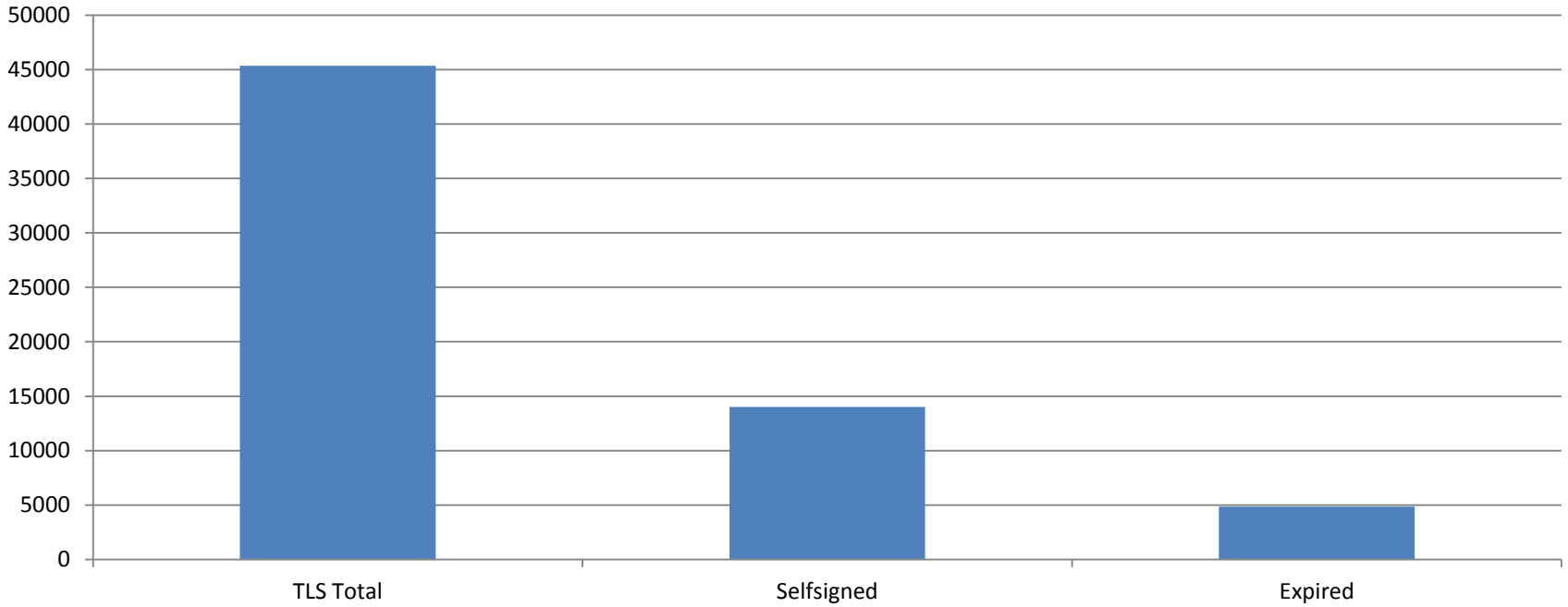
Ciphers


38%
24%
17%
9%
4%
3%
1%
1%
1%
0%
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-SHA
DHE-RSA-AES256-GCM-SHA384
AES128-SHA
ECDHE-RSA-AES256-SHA
AES256-SHA
ECDHE-RSA-AES256-SHA384
AES256-GCM-SHA384
DHE-RSA-AES256-SHA256
ECDHE-RSA-AES128-GCM-SHA256
RC4-MD5
AES128-SHA256

Welche CAs sehen wir?



Zertifikate



Fragen?

Otmar Lendl <lendl@cert.at>
+43 1 5056416 711