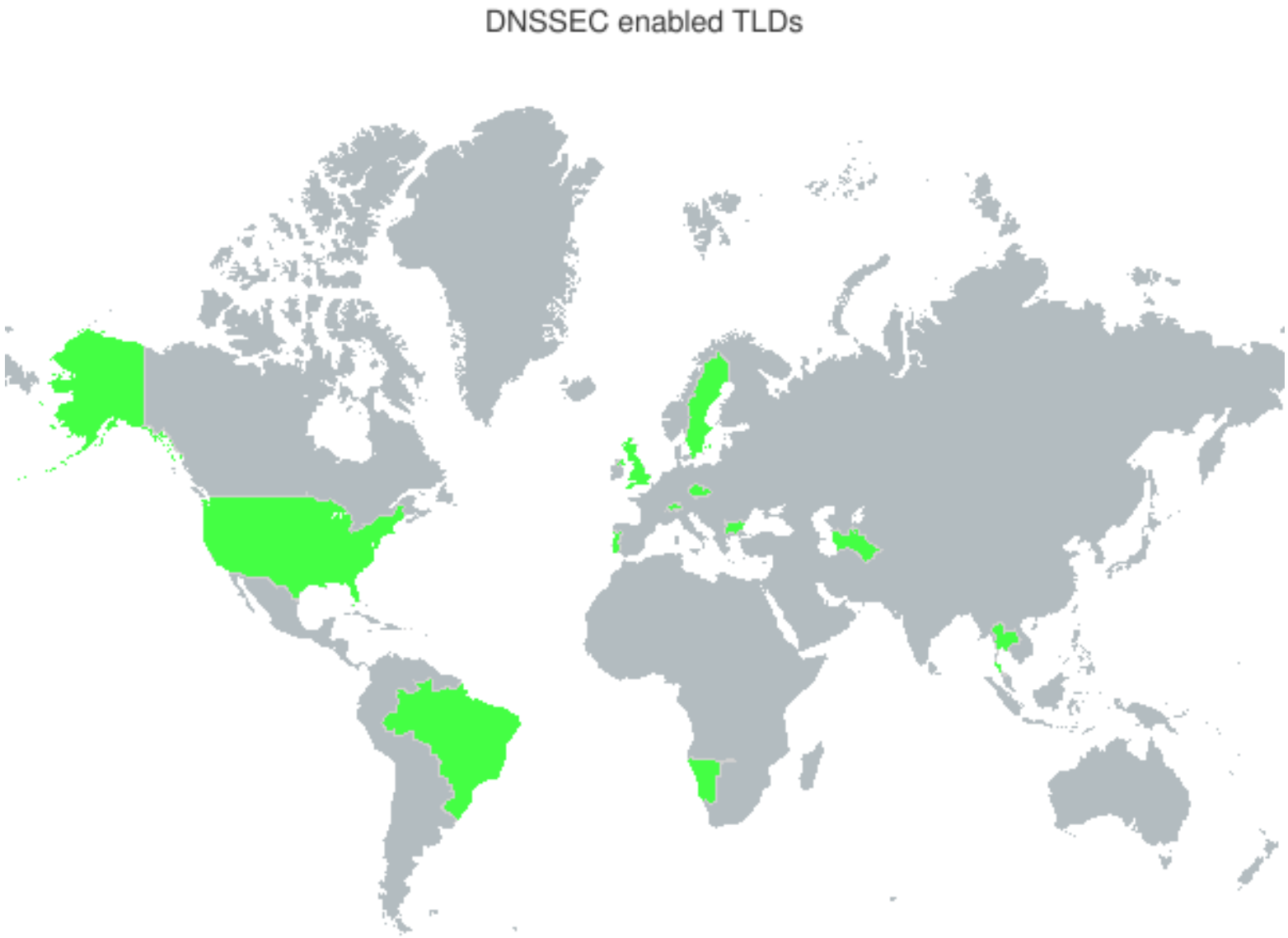
Bundesamt
für Sicherheit in der
Informationstechnik

DNSSEC im globalen Kontext
Aktueller Stand

Thorsten Dietrich

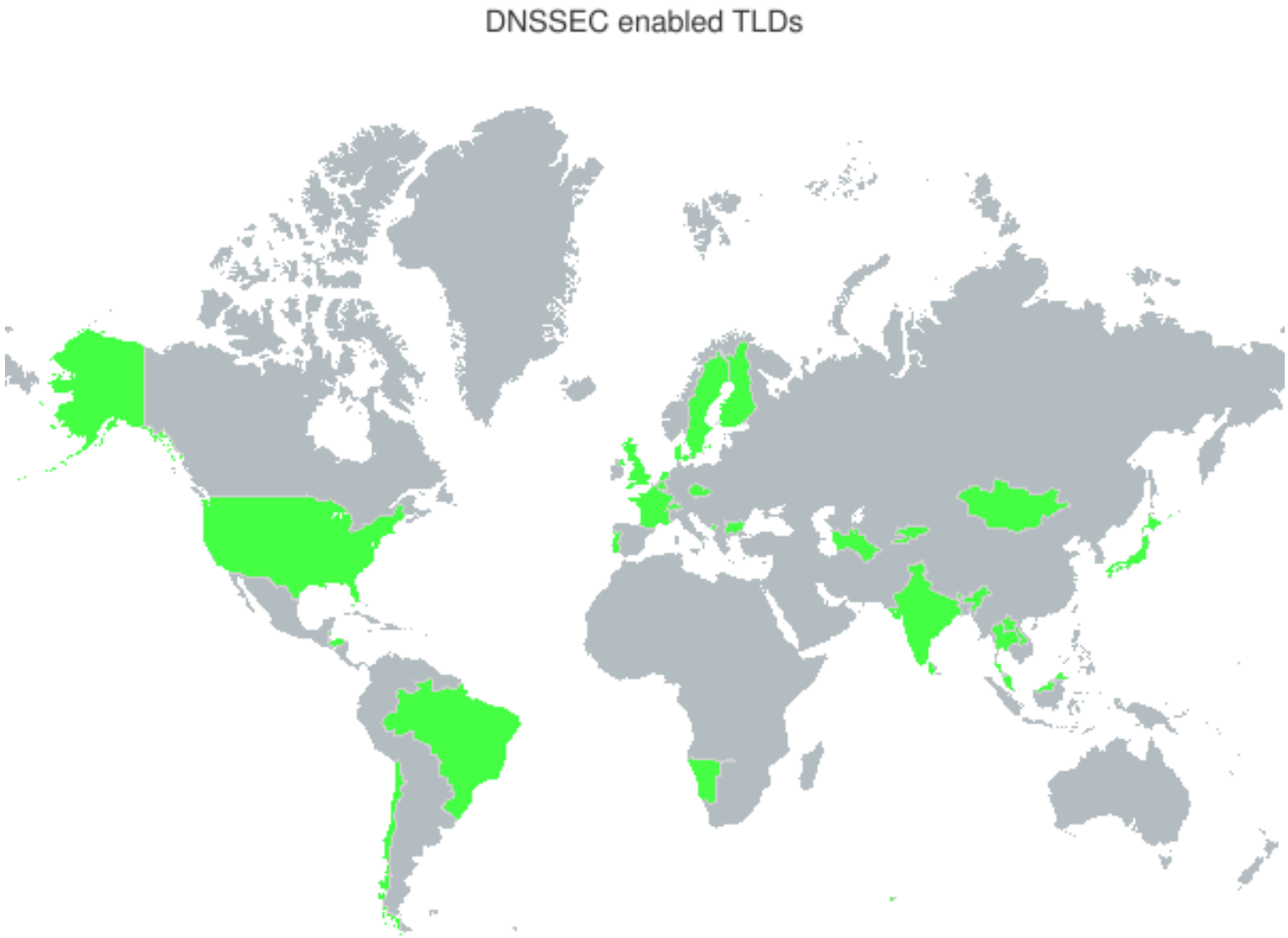
4. DNSSEC Testbed-Meeting, 24. November 2010

Globale Sicht:
DNSSEC signierte Domains Stand 06/10



29 signierte TLDs im Juni 2010

Globale Sicht:
DNSSEC signierte Domains Stand 11/10



64 signierte TLDs im November 2010

. (Root-Zone)

Root-Zone
DNSSEC signiert seit 15. Juli 2010

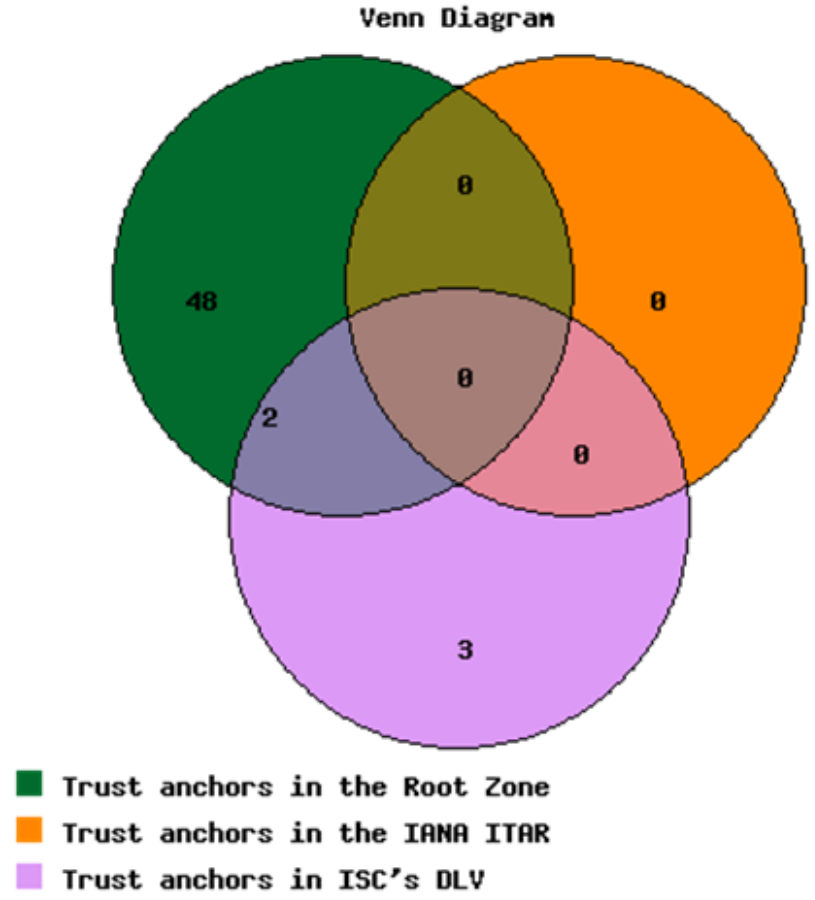
Historie:

- Juni 2010
  - Unvalidierbare signierte Root-Zone wird ausgeliefert (Deliberately-Unvalidatable Root Zone (DURZ))
  - 1. Schlüssel-Zeremonie in Culpeper, Virginia
  - Erzeugung des initialen KSK
  - Erste DS records wurden der Root-Zone hinzugefügt
- Juli 2010
  - 2. Schlüssel-Zeremonie in Los Angeles, California
  - Die validierbare signierte Root-Zone wurde an die Root-Server ausgeliefert
  - Der Trust Anchor wurde durch ICANN veröffentlicht: https://www.iana.org/dnssec/
- November 2010
  - 3. Schlüssel-Zeremonie in Culpeper, Virginia

Root-Zone
DNSSEC signiert seit 15. Juli 2010

- Künftige Termine:
  - 4. Zeremonie in El Segundo, California (7.-8. Februar 2011)
  - 5. Zeremonie in Culpeper, Virginia (5.-6. Mai 2011)
- Prozedurbeschreibung für TLD-Betreiber zur Veröffentlichung von DS Records in der Root-Zone: http://www.iana.org/procedures/root-dnssec-records.html

- z.Zt. 50 Trust Anchors in der Root-Zone
- 3 weitere in ISC DLV



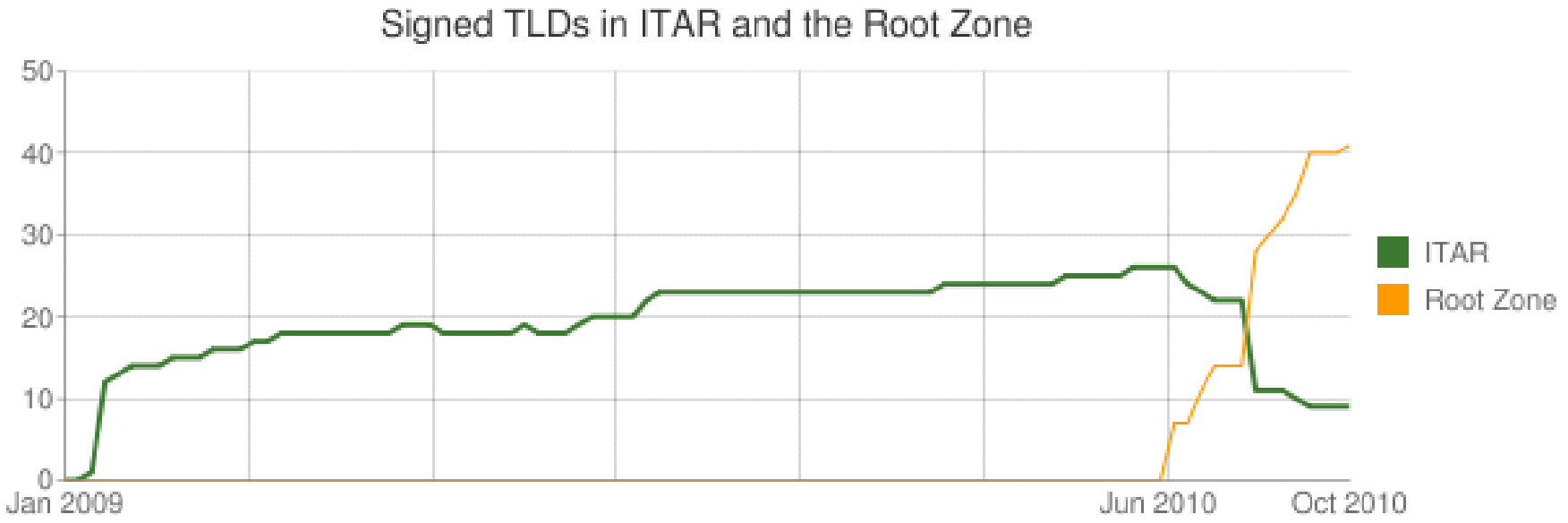
Quelle:
http://stats.research.icann.org/dns/tld_report/

IANA ITAR

Interim Trust Anchor Repository

End of Life Notice

This service is being discontinued. Listing requests are no longer being accepted, and the existing listings will be removed toward the end of November 2010. **Users relying on this service should discontinue its use, and migrate to using the signed DNS root zone.**



Quelle: „Update on ITAR", Elise Gerich, Vice President, IANA, RIPE-61

Bundesamt
für Sicherheit in der
Informationstechnik

DNSSEC Deployment
Signierte Top-Level-Domains (1)

TLD	Land	DS in Root	DNSSEC Algorithmus
be.	Belgien	X	RSA/SHA-256
bg.	Bulgarien	X	RSA/SHA-1
ch.	Schweiz	X	RSASHA1-NSEC3
cz.	Tschechische R.	X	RSA/SHA-512
dk.	Dänemark	X	RSA/SHA-256
eu.	Europäische Union	X	RSASHA1-NSEC3
fi.	Finnland	X	RSA/SHA-256
fr.	Frankreich	X	RSA/SHA-256
gi.	Gibraltar	X	RSASHA1-NSEC3
li.	Liechtenstein	X	RSASHA1-NSEC3
nl.	Niederlande	X	RSA/SHA-256
pt.	Portugal	X	RSASHA1-NSEC3
se.	Schweden	X	RSA/SHA-1
uk.	Großbritannien	X	RSA/SHA-256

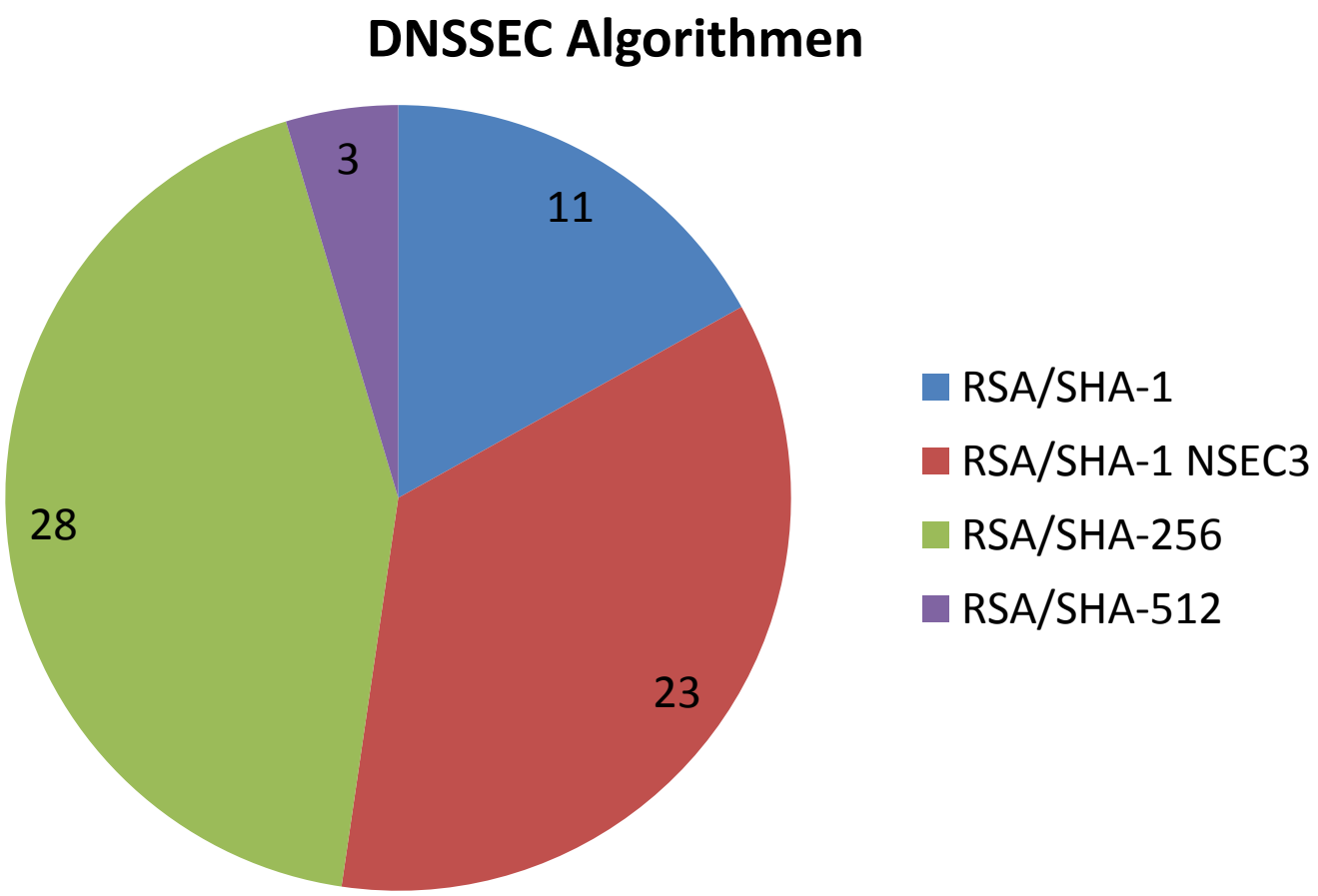
TLD	Land	DS in Root	DNSSEC Algorithmus
ag.	Antigua & Barbuda		RSASHA1-NSEC3
br.	Brasilien	X	RSA/SHA-1
bz.	Belize	X	RSASHA1-NSEC3
cl.	Chile		RSASHA1-NSEC3
hn.	Honduras	X	RSASHA1-NSEC3
in.	Indien		RSASHA1-NSEC3
jp.	Japan		RSA/SHA-256
kg.	Kirgisistan	DLV	RSA/SHA-1
la.	Laos	DLV	RSASHA1-NSEC3
lc.	Saint Lucia	X	RSASHA1-NSEC3
lk.	Sri Lanka	X	RSA/SHA-1
me.	Montenegro		RSASHA1-NSEC3
mn.	Mongolei	X	RSASHA1-NSEC3
my.	Malaysia		RSA/SHA-256
na.	Namibia	X	RSA/SHA-1

DNSSEC Deployment
Signierte Top-Level-Domains (2)

TLD	Land	DS in Root	DNSSEC Algorithmus
nu.	Niue	X	RSASHA1-NSEC3
pm.	Saint Pierre & Miquelon	X	RSA/SHA-256
pr.	Puerto Rico	X	RSA/SHA-1
re.	Reunion	X	RSA/SHA-256
sc.	Seychellen	X	RSASHA1-NSEC3
tf.	Franz. Südgebiete	X	RSA/SHA-256
th.	Thailand	X	RSA/SHA-1
tm.	Turkmenistan	X	RSASHA1-NSEC3
us.	United States	X	RSA/SHA-1
vc.	Saint Vincent & Grenadines		RSASHA1-NSEC3
wf.	Wallis & Futuna		RSA/SHA-256
ලංකා.	Sri Lanka (.lanka)		RSA/SHA-1
இலங்கை.	Sri Lanka (.Ilangai)		RSA/SHA-1
yt.	Mayotte	X	RSA/SHA-256

TLD	DS in Root	DNSSEC Algorithmus
arpa.	DLV	RSA/SHA-256
asia.	X	RSASHA1-NSEC3
biz.	X	RSA/SHA-256
cat.	X	RSA/SHA-512
edu.	X	RSASHA1-NSEC3
gov.	X	RSASHA1-NSEC3
info.	X	RSASHA1-NSEC3
museum.	X	RSA/SHA-512
net.	_	RSA/SHA-256
org.	X	RSASHA1-NSEC3
11 IDN Testdomains	X	RSA/SHA-256

Verteilung der DNSSEC Algorithmen



.arpa

.ARPA

- .arpa signiert seit März 2010
- Aktivitäten zur Hinterlegung des DS-Eintrags in der Root-Zone laufen
- Als Zwischenlösung wurde der .arpa Schlüssel in der ISC DLV hinterlegt
- Second Level Domains unterhalb .arpa sind seit April signiert. Ausnahme: IN-ADDR.ARPA

.IN-ADDR.ARPA & .IP6.ARPA

- ICANN und RIRs haben eine Systematik entwickelt, die den RIRs die Aktualisierung der RRSets in IP6.ARPA und IN-ADDR.ARPA ermöglicht
- Implementierung läuft
- Betrieb von IN-ADDR.ARPA wird von ARIN und den Root-Servern zur ICANN und eigenen Servern verlagert (2011)
- Im Anschluß ist Signierung geplant
- IP6.ARPA wird bereits durch Server der RIRs betrieben und ist seit April 2010 signiert

Aktivitäten einzelner Registries

AFNIC

DNSSEC Deployment AFNIC

The signing of AFNIC zones in 2010

.pm (Saint-Pierre and Miquelon) have been signed on April 15th, 2010, *.tf* (French Southern Territories) on September 3rd and *.yt* (Mayotte) on September 9th, 2010.

***.fr* and *.re* (Reunion Island) have been signed on September 14th, 2010.**

The DS records are published in the root within a month.

DS provisionning will be available for *.fr* delegations within the second quarter of 2011

With the signature of AFNIC zones, a major milestone has been achieved on the road to securing French DNS. Security of the French DNS will be progressively and ultimately achieved through a combination of: Signatures of subsequent delegations (*.fr*, *.re*, ...); Publication of the corresponding cryptographic fingerprints; Activation of secured resolutions by ISPs.

Zone	Date of first signature	Date of DS publication (Root)
.fr	14 September 2010	1st October 2010
.pm	15 April 2010	27 August 2010
.re	14 September 2010	25 September 2010
.tf	3 September 2010	11 September 2010
.yt	9 September 2010	17 September 2010
.wf	8 November 2010	

Quelle: http://www.afnic.fr/afnic/r_d/dnssec_en

Aktivitäten einzelner Registries

Afilias

DNSSEC Deployment Afilias

ag.	Antigua and Barbuda
asia.	gTLD
bz.	Belize
gi.	Gibraltar
hn.	Honduras
in.	India
info.	gTLD
lc.	Saint Lucia
me.	Montenegro
mn.	Mongolia
org.	gTLD
sc.	Seychelles
vc.	Saint Vincent and the Grenadines

Afilias secures .INFO domain with DNSSEC

SHARE Contact a PR rep Subscribe to our news

Sep 9, 2010

Deployment of Domain Name System Security Extensions improves global security for .INFO

DUBLIN, IRELAND - 9 September 2010 - Afilias, a global provider of Internet infrastructure services, today announced that it has enabled Domain Name System Security Extensions (DNSSEC) for the .INFO top-level domain (TLD). .INFO was officially signed on September 1, 2010 and its Delegation Signer (DS) records were entered into the DNS Root by the Internet Assigned Numbers Authority (IANA) on September 4th, allowing the .INFO zone to be validated using DNSSEC. The signing of the .INFO domain enhances global security for the seventh largest TLD in the world, home to more than 6.5 million registrations.

Quelle:
http://www.afilias.info/news/2010/09/09/afilias-secures-info-domain-dnssec

Afilias Secures .GI, .MN, and .SC Domains with DNSSEC

SHARE Contact a PR rep Subscribe to our news

Nov 18, 2010

Brings added security to three more countries around the world

DUBLIN, IRELAND - 18 November 2010 - Afilias, a global provider of Internet infrastructure services, today announced that it has enabled Domain Name System Security Extensions (DNSSEC) for .GI, the country code Top Level Domain (ccTLD) for Gibraltar, .MN for Mongolia, and .SC for the Seychelles.

Quelle:
http://www.info/news/2010/11/18/afilias-secures-gi-mn-and-sc-domains-dnssec

.ASIA DNSSEC Signing Event November 2010

SHARE

On November 11, 2010 Afilias secured the .ASIA TLD with DNSSEC. You can find media, presentations, and comments from the event here.

Quelle:
http://www.info/ASIA+DNSSEC+event

Aktivitäten einzelner Registries

LKNIC

DNSSEC Deployment LKNIC

lk.	Sri Lanka
xn--fzc2c9e2c. ලංකා.	Sri Lanka (.lanka)
xn--xkc2al3hye2a. இலங்கை.	Sri Lanka (.Ilangai)

Welcome to DNSSEC @ LKNIC

LK Domain Registry is proudly announcing that all its domains are now secured with **DNSSEC** . It has enabled DNSSEC in all the three TLDs namely .lk, .lanka and .ilangai since July 2010.

Quelle: http://www.dnssec.lk/

DNSSEC Deployment ICANN
IDN Testdomains

xn--0zwm56d. 测试.	Chinesisch
xn--11b5bs3a9aj6g. परीक्षा.	Hindi
xn--80akhbyknj4f. испытание.	Russisch
xn--9t4b11yi5a. 테스트.	Koreanisch
xn--deba0ad. .טעסט	Jiddisch
xn--g6w251d. 測試.	Chinesisch in trad. Schrift
xn--hgbk6aj7f53bba. آزمایشی.	Persisch
xn--hlcj6aya9esc7a. பரிட்சை.	Tamil
xn--jxalpdlp. δοκιμή.	Griechisch
xn--kgbechtv. .إختبار	Arabisch
xn--zckzah. テスト.	Japanisch

ICANN Blog

Internet Corporation for Assigned Names and Numbers

DNSSEC on IDN .test zones

by RICHARD LAMB *on* FEBRUARY 29, 2008

Yesterday ICANN began DNSSEC signing the IDN .test zones. Over the next few days, we will be testing and carefully monitoring the system. It is not expected that DNSSEC or the testing will have any effect on normal DNS operations. Any user experiences or problems or feedback should be reported to <richard.lamb@icann.org>. This deployment is intended to demonstrate certain capabilities and also provide both ICANN and those interested in DNSSEC an opportunity to gain further experience with this new technology.

Quelle: http://blog.icann.org/2008/02/dnssec-on-idn-test-zones/

.net & .com

.net DNSSEC Deployment
Major milestones

- "The **.net DNSSEC deployment** consists of the following major milestones:
  - **September 25, 2010:** The .net registry system was upgraded to allow ICANN-accredited registrars to submit DS records for domains under .net. These DS records will not be published in the .net zone until the .net zone is actually signed.
  - Each registrar will implement support for DNSSEC on its own schedule, and some registrars might be accepting DS records for .net domains now.
  - **October 29, 2010:** A deliberately unvalidatable .net zone will be published.
    Following the successful use of this technique with the root DNSSEC deployment, VeriSign will publish a signed .net zone with the key material deliberately obscured so that it cannot be used for validation.
    Any DS records for .net domains that have been submitted by registrars will be published in the deliberately unvalidatable zone.
  - **December 9, 2010:** The .net key material will be unobscured and the .net zone will be usable for DNSSEC validation. DS records for .net will appear in the root zone shortly thereafter."

Quelle: Matt Larson, Verisign

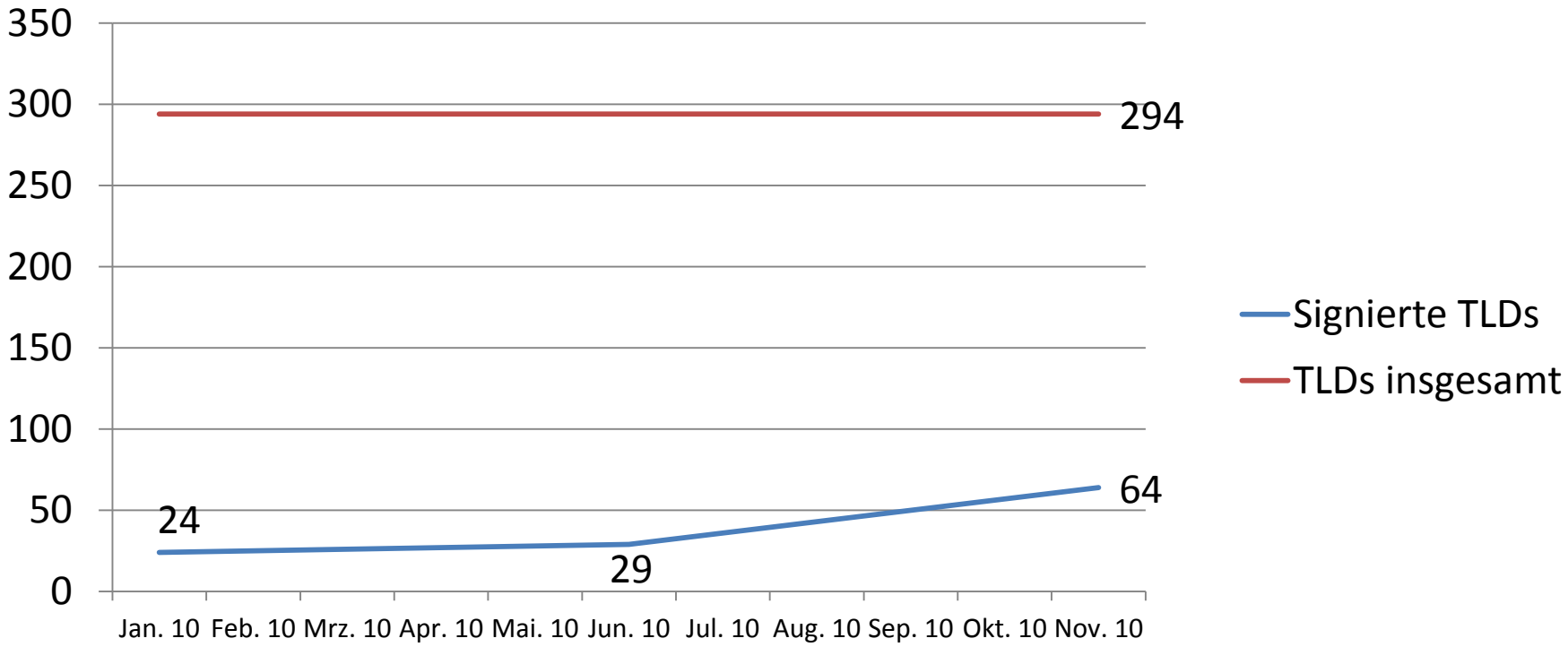
.com DNSSEC Deployment
Major milestones

- "The **.com DNSSEC deployment** consists of the following major milestones:
  - **February, 2011:** The .com registry system will be upgraded to allow ICANN-accredited registrars to submit DS records for domains under .com. These DS records will not be published in the .com zone until the .com zone is actually signed.
  - **March, 2011:** A deliberately unvalidatable .com zone will be published.
    Any DS records for .com that have been submitted by registrars will be published in the deliberately unvalidatable zone.
  - **March, 2011:** The .com key material will be unobscured and the .com zone will be usable for DNSSEC validation. DS records for .com will appear in the root zone shortly thereafter."

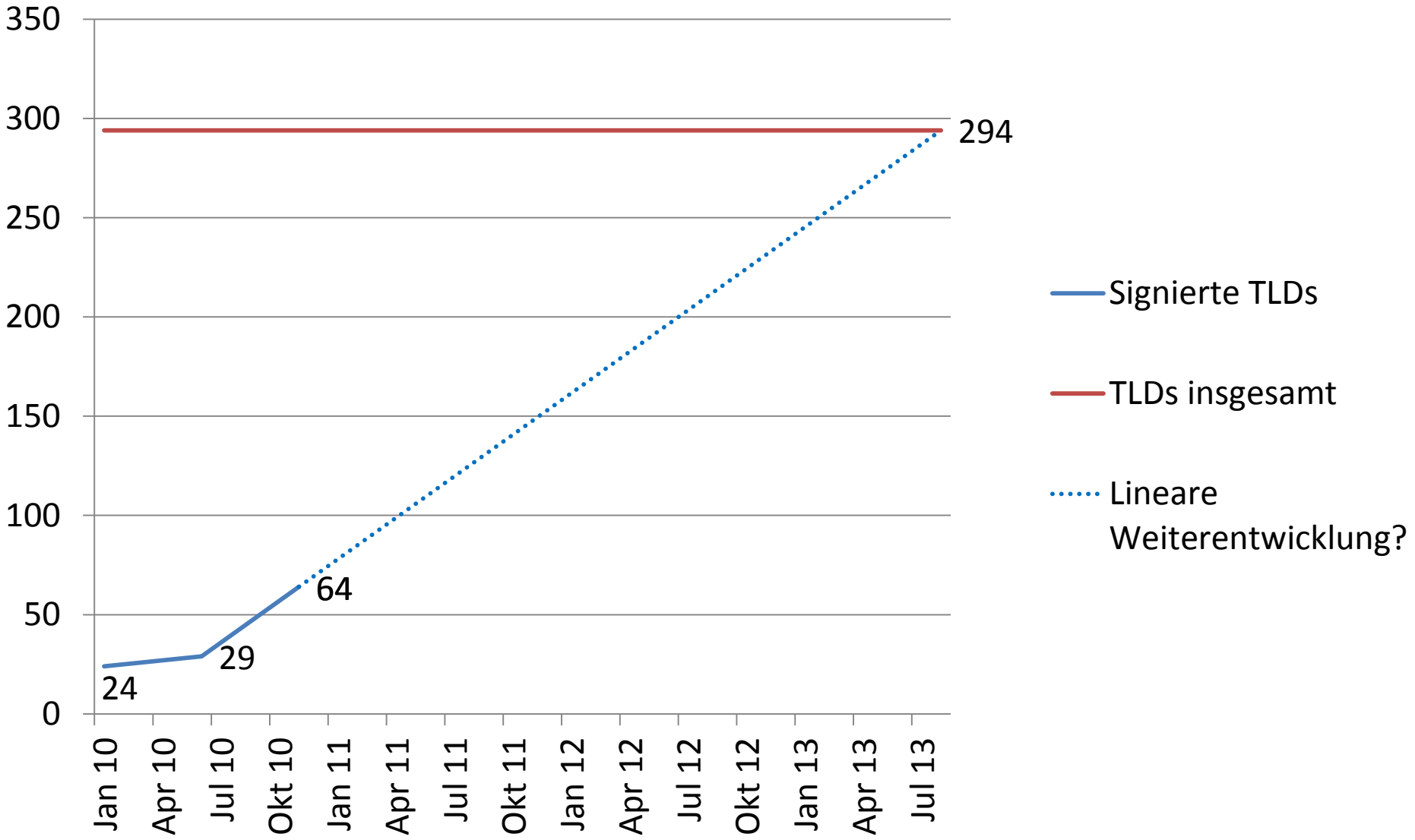
Quelle: Matt Larson, Verisign

Signierte TLDs

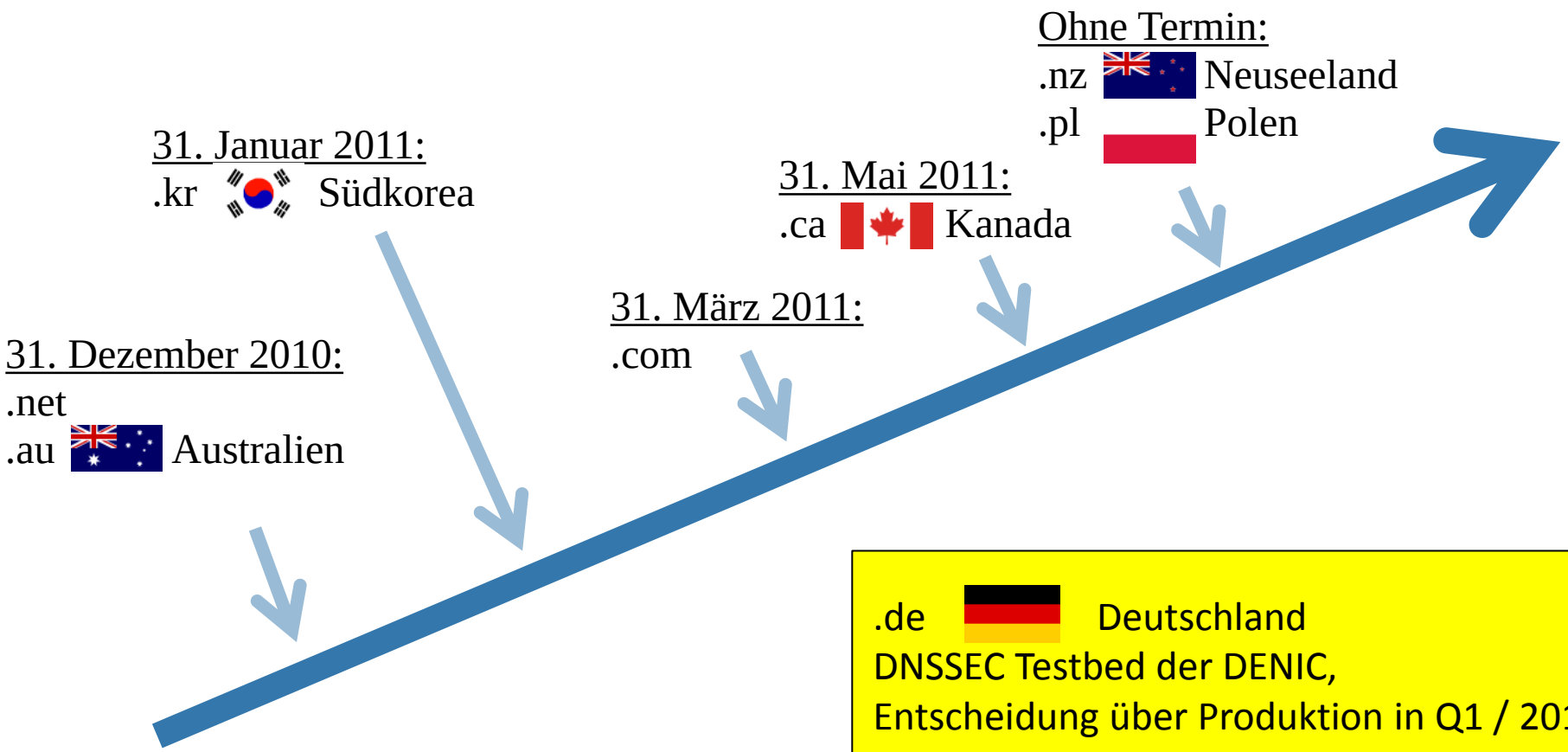
- Stand 01/2010: 24 signierte TLDs
- Stand 06/2010: 29 signierte TLDs
- Stand 11/2010: 64 signierte Top-Level-Domains (davon 50 mit Trust Anchor in der Root-Zone)



Signierte TLDs (2)



DNSSEC Deployment
Signierte Top-Level-Domains (Ausblick)



.de Deutschland
DNSSEC Testbed der DENIC,
Entscheidung über Produktion in Q1 / 2011

Sonstiges

DNSSEC validation issue .uk

http://blog.nominet.org.uk/tech/wp-content/uploads/2010/09/dnssec-incident-report.pdf:

- On **Saturday, 11 September 2010**, following a hardware failure on the Main Signing system the evening before, **we switched over to our Disaster Recovery (DR) Signing System**. During this switch over an error occurred leading to a **non-synchronised zone signing key being issued**. **This led to validation failures** on a small number of resolvers which were DNSSEC enabled.
- Once we had identified the problem we issued a technical announcement on Saturday evening at 11pm **to alert resolver operators to 'flush' their DNS caches**. The majority of validating resolver owners either pre-empted or followed this advice.
- **By Monday, all DNSSEC caches had pulled the new key** across so that no additional action needed to be taken.
- We […] are still working to establish the exact cause of two issues:
  - 1. The root cause of the hardware failure that caused us to switch over to our DR signing system.
  - 2. How the DR signer managed to insert a non synchronized ZSK key into the zone-file.
- We have taken a number of additional steps to prevent an event such as this from re-occurring:
  - 1. We have lowered the TTL of the DNSKEY from 2 days to 1 hour.
  - 2. We have added additional monitoring to make sure the systems are synchronized prior to switch over.
  - 3. We have simplified the processes for re-starting or switching over to the DR signing system
  - 4. We have revised our switch over procedures to include additional checks, specifically around manual validation of the zone-file prior to deployment in a failover situation.

KSK key algorithm rollover .cz (NSEC -> NSEC3)

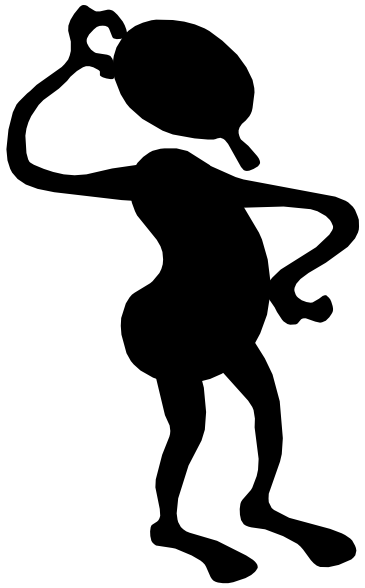
- .cz Entscheidung, von NSEC auf NSEC3 zu wechseln
- Motivatoren:
  - Zonewalking
  - Signierung der Root-Zone
- Vorbereitungen
  - Wechsel von NSEC auf NSEC3 erfordert KSK-Wechsel
  - Wechsel auf aktuellste BIND / NSD -Version
  - Marketing
- Aussage: Pre-Publish Methode kann aufgrund von Algorithmen-Wechsel nicht verwendet werden, da durch zusätzliche Veröffentlichung eines DNSKEY mit einem anderen Algorithmus die Zone als „bogus“ eingestuft wird.
  (Praxis: Unterschiedliche Auslegung durch BIND und Unbound)
- Manueller Prozess, KSK Rollover im Double-Signature Verfahren wird von aktuellen Tools nicht unterstützt.

Hintergrund
KSK Algorithmenwechsel

- RFC 4035 – section 2.2:
  There MUST be an RRSIG for each RRset using at least one DNSKEY of **each algorithm** in the zone apex DNSKEY RRset. The apex DNSKEY RRset itself MUST be signed **by each algorithm** appearing in the DS RRset located at the delegating parent (if any).

- (1) You need to sign each RRset with new DNSKEY
- (2) You need to put signatures into zonefile before DNSKEY
- (3) You need to send DS upstream after previous steps

Vielen Dank für Ihre Aufmerksamkeit!



Fragen?

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Thorsten Dietrich
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-5947
Fax: +49 (0)22899-10-9582-5947

Thorsten.Dietrich@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de