.TR CCTLD

DNSSEC DEPLOYMENT

ERDEM BAYRAK - ICT TURKIYE

erdem.bayrak@btk.gov.tr

OUTLINE

ABOUT TRABIS & .TR DNSSEC DEPLOYMENT

.TR ccTLD HISTORY

PRE-DEPLOYMENT STUDIES

ABOUT TRABIS

TECHNICAL SPECIFICATIONS

STATISTICS

DEPLOYMENT STRATEGY

.TR ccTLD DNS ARCHITECTURE

TEST BED & TESTING

SECURITY & BUSS. CONTINUITY

CURRENT STATUS & FUTURE WORKS

FURTHER PRECAUTIONS

Q&A

.TR CCTLD

.TR ccTLD MANAGEMENT

- Information and Telecommunication Authority of Turkiye (BTK)

TRABIS EXTENSION

- TR Network Information System
- http://www.trabis.tr

DUTIES of TRABIS

- Real Time Domain Name Operations
- Management of Central Database

RESPONSIBILITIES

- Service Continuity - %99.9 DNS
- Dispute Resolution
- Security of DNS & Domain Names

.TR CCTLD HISTORY

1991	17th April 2019	14th Sept. 2022
METU	Transfer of .tr ccTLD from University to BTK	

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

.TRABİS

.tr AĞ BİLGİ SİSTEMİ

- Written TRABIS Legislation
- MODEL: Registry - Registrar
  .tr Domain Name Registry
- Document-Free Domain Name REGISTRATION & TRANSFER (com.tr, net.tr, org.tr)
- Dispute Resolution Mechanism
- 20 Registrars - 2 Dispute Res. Providers
  TRABIS-KK: gov, edu, pol, tsk, k12

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

.TRABİS
.tr AĞ BİLGİ SİSTEMİ

NUMBER OF .TR ACTIVE DOMAIN NAMES

Before TRABIS (Nic.TR)

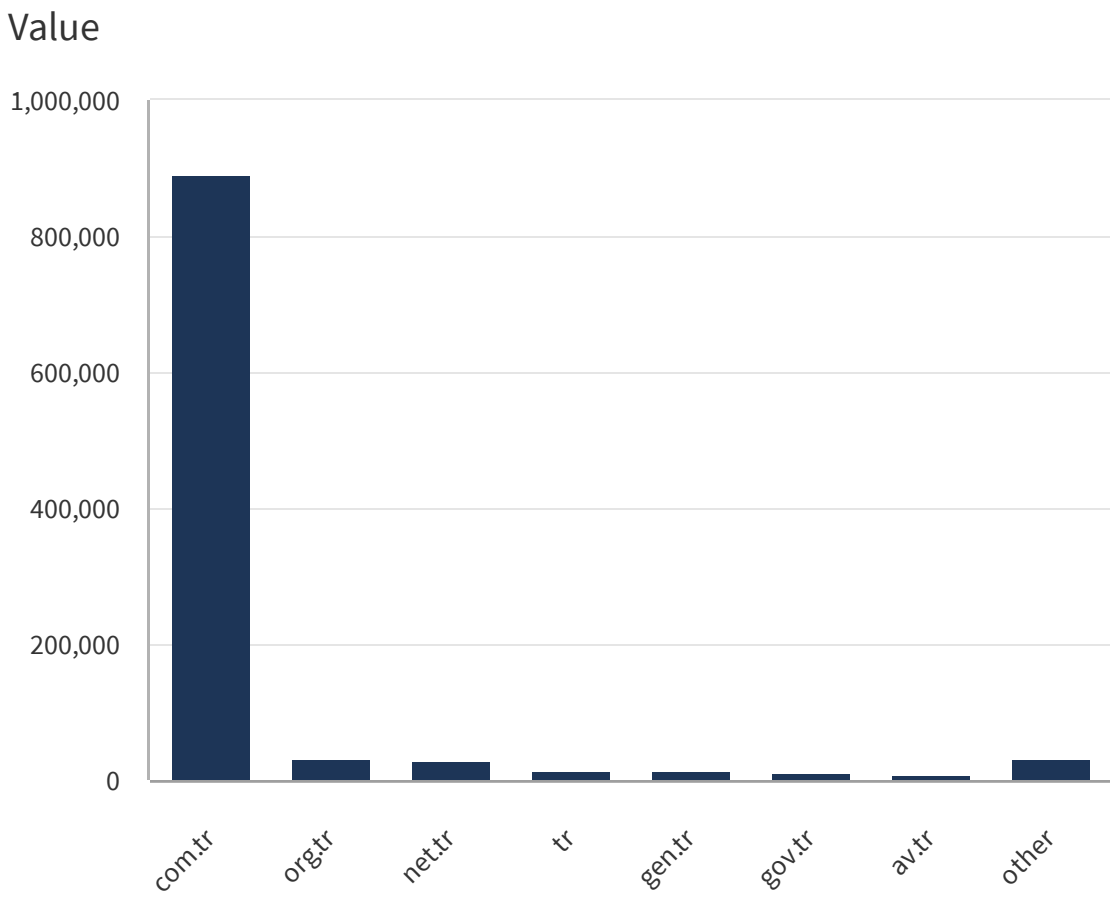
After TRABIS

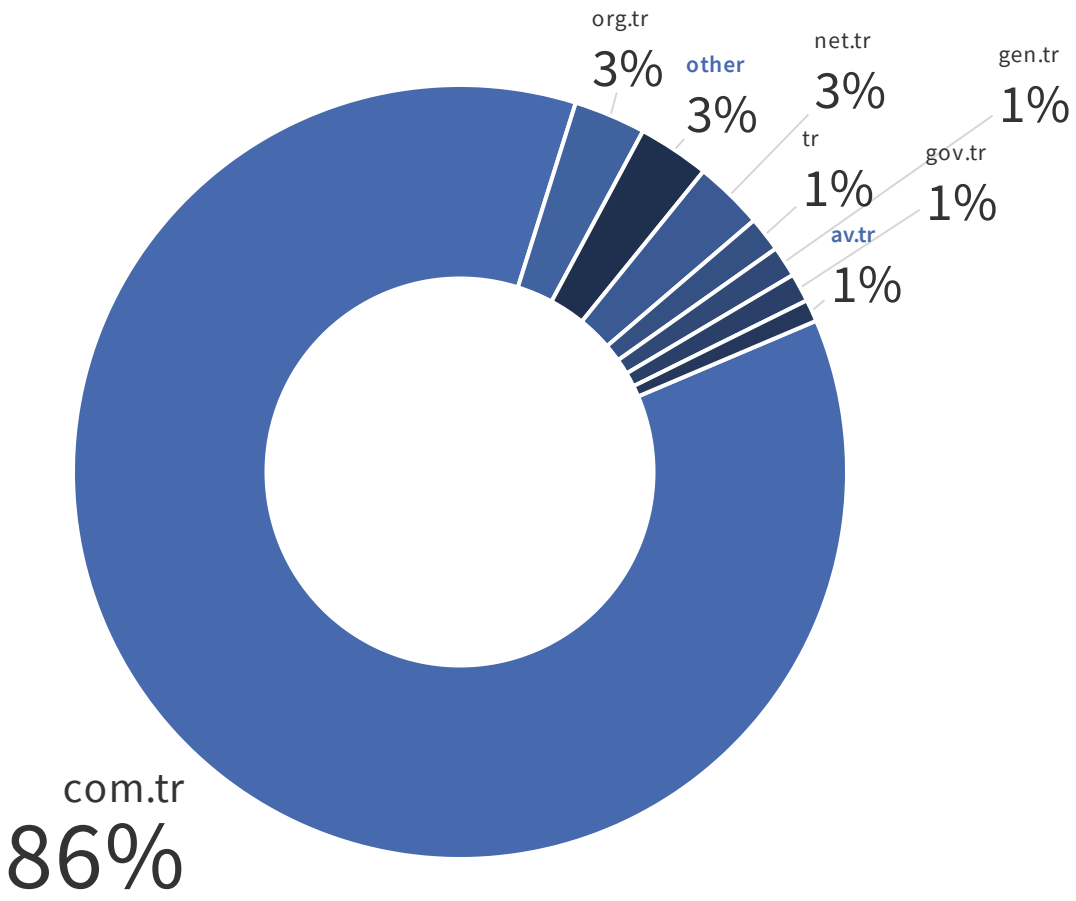
Total

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

.TRABİS .tr AĞ BİLGİ SİSTEMİ

ACTIVE DOMAIN NAMES / EXTENSIONS

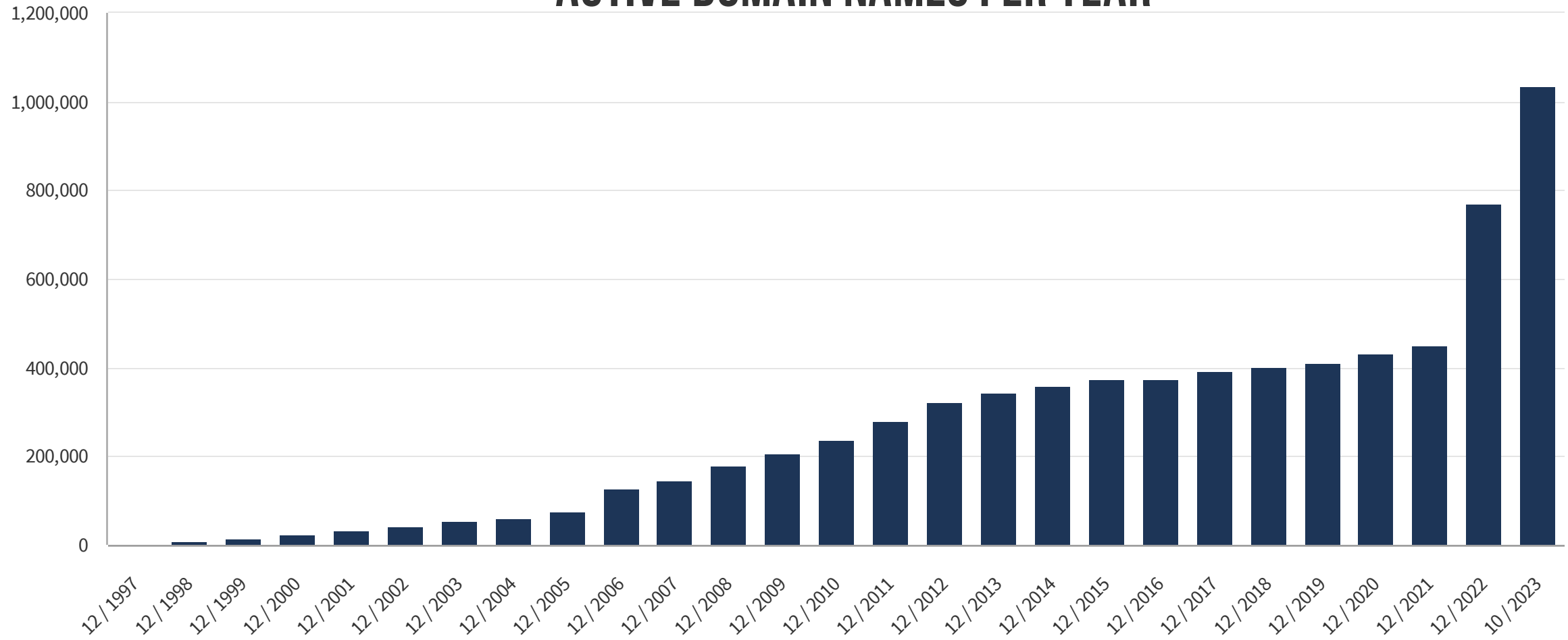




BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

.TRABİS .tr AĞ BİLGİ SİSTEMİ

ACTIVE DOMAIN NAMES PER YEAR



BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

.TR DNS INFRASTRUCTURE

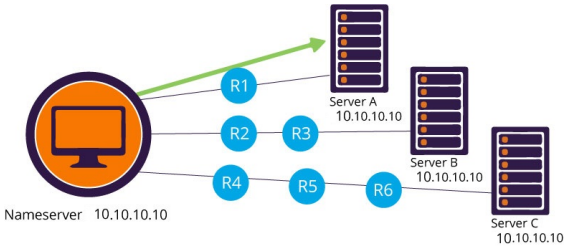
* A Hidden Master & Slave DNS Servers

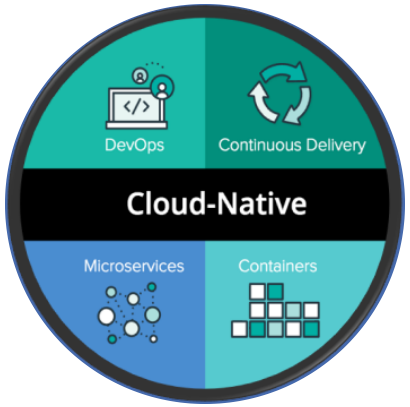
* Geographically distributed servers

* Monitoring DNS and zone (creation, transfer etc.)

* DDOS Protection mechanisms

SECURITY & BUSSINESS CONTINUITY





ANYCAST

Disaster Recovery

Centralized Management
& Scalability

TR-CERT - AZAD
Phishing Analysis

1123 Phishing Domain Detection

FURTHER PRECOUTIONS

RESTRICTED DOMAINS

- Similarity Words: finance, bank
- Exact Match: city names

NON-REGISTERED DOMAINS

Domain Names Contrary to;

- Legislation
- public order
- public moral

DOMAIN ABUSE COMPLAINTS

- Procedure defines mitigation against abusive domain names.
- TR-CERT capabilities / phishins site & malware analysis

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

.TR DNSSEC DEPLOYMENT

PRE-DEPLOYMENT STUDIES

1. Assessment of Current .TR DNS Infrastructure
2. ICANN Experience Sharing & Hands-on Training (hands on experince)
3. Test Environment / Test Plan / Test Scenarios
4. Deployment Strategy & Specifications (Keys, Algorithm etc.) & Configuration
5. Simulation (with real zone files - 20 2nd Level Zones)

TEST ENVIRONMENT & PHASES

Setup Test Env. / Inline Signing

- Software: OpenDNSSEC
- Key Generation & Storage: SoftHSM
- DNS / BIND

Key Generation

- Generate KSK & ZSK

Zone Signing

- Get unsigned zone into Signer server
- Sign the zone

Validate & Publish Zone

- Validate zone files before publishing on DNS

Scheduled / Emergency Rollovers

- Key/Signature Rollover Tests

Rollback Test

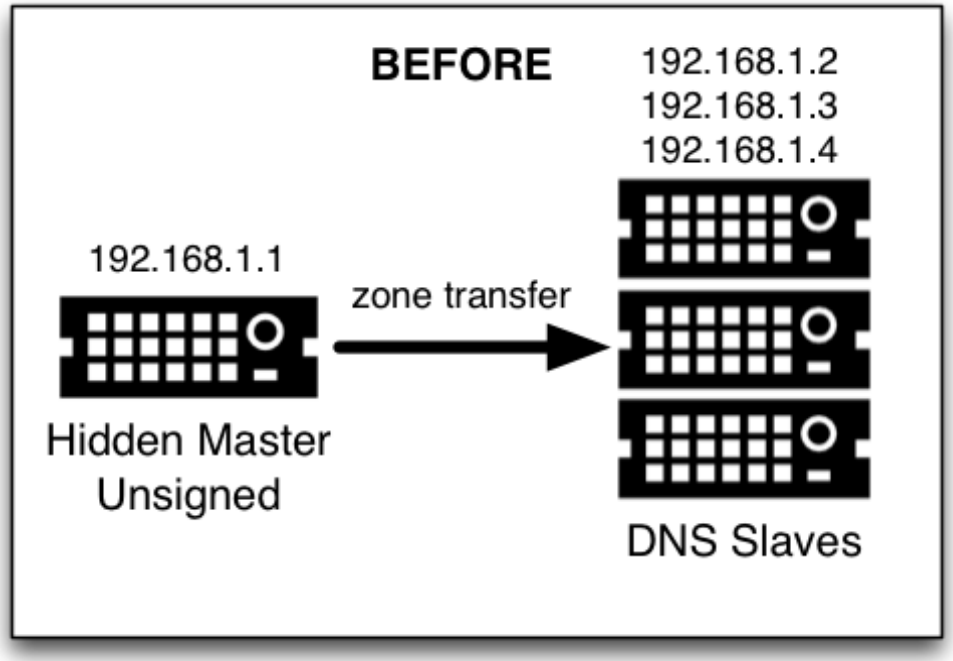
- serve unsigned zones (stripped of all DNSSEC information)
- Remove DS records from parent zone

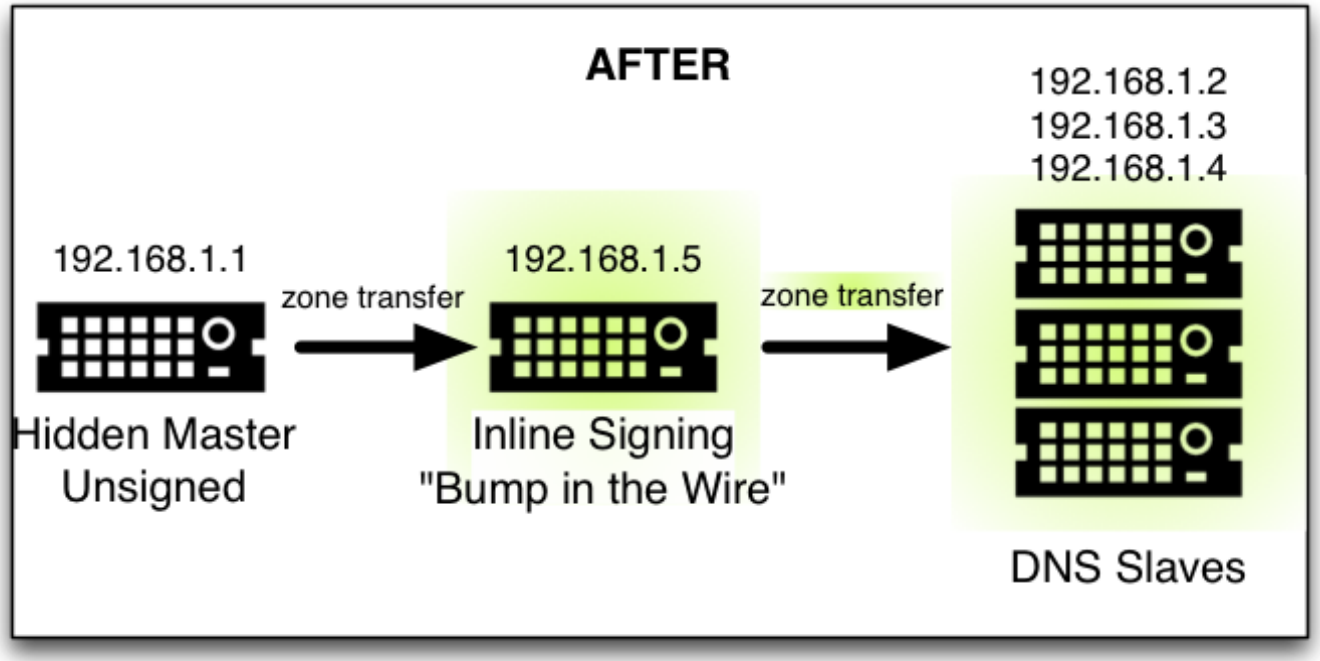
Simulation of The PROD Env.

- Transfer zone files into test bed
- Repeat all test steps
- Check results

SIGNING STRATEGY

INLINE SIGNING (BUMP IN THE WIRE)





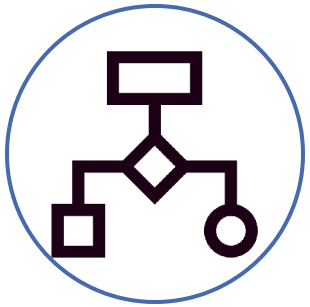
TECHNICAL SPECIFICATIONS

PUBLIC KEY CRYPTOGRAPHY

- **Public-Private Key Pairs** are used during the signing processes.
- Private keys stored in **SoftHSM**.

KEY TYPES

- **ZSK** is used for Zone Signing.
- **KSK** is used for Key Signing.



ALGORITHM

- **Elliptic Curve Digital Signature Algorithm / RFC 6605**
- **13 / ECDSAP256SHA256**
- **ECDSA Curve P-256 with SHA-256**

DENIAL OF EXISTANCE

- **NSEC3 feature** is used to enhance data privacy and protect against zone walking.

KEY ROLLOVERS & SIGNATURE LIFETIME

KSK ROLLOVER

- KSK lifte time is a year.
- New KSK is GENERATED & PUBLISHED 3 months before rollover
- After one month rollover takes place / old key is removed.

ZSK ROLLOVER

- ZSK is renewed in every 90 days.
- New ZSK is GENERATED & PUBLISHED 1 month before rollover
- After one month rollover takes place / old key is removed.

SIGNATURE LIFETIME & RE-SIGNING FREQUENCY

- ZSK signature has the validity of one month.
- KSK signature has the validity of two months.
- ZSK re-signing period is once a week.
- KSK re-signing period is once a month.

RR VERIFICATION & TTL VALUES

VERIFICATION

- Before publish
- Verify all RRs
- In terms of conformance with the protocol standards

RESOURCE RECORDs TTL

- KEYS: 43200
- DS: 21600
- NSEC3: 3600
- RRSIG: same as the TTL of the RRset it covers.

DPS

- DNSSEC Practice Statement
- www.trabis.tr

.TR DNSSEC DEPLOYMENT CURRENT SITUATION

1 Phase-1: Inline Signer Conf. / Authomated Signing

2 **Phase-2**: Staged 2nd-Level Zone Signing

Stage1: tel.tr, kep.tr, bbs.tr etc.

Stage2: com.tr, org.tr, net.tr etc.

3 **Phase-3**: Sign .tr Zone

4 **Phase-4**: Publish DS Record / Chain-of-Trust

5 **Phase-5**: Involvement of Registrars & the other parties

DELEGATION SIGNER (DS) VALIDATION

Syntax Check

DS format control

KeyTag Check

Should be greater than 1, less than 65535

Algorithm Check

RFC-8624 Algorithm Implementation Requirements and Usage Guidance for DNSSEC

5: RSA/SHA-1 [RSASHA1]

8: RSA/SHA-256 [RSASHA256]

10: RSA/SHA-512 [RSASHA512]

13: ECDSA Curve P-256 with SHA-256 [ECDSAP256SHA256]

14: ECDSA Curve P-384 with SHA-384 [ECDSAP384SHA384]

15: Ed25519 [ED25519]

16: Ed448 [ED448]

Digest Type

RFC 8624 - Algorithm Implementation Requirements and Usage Guidance for DNSSEC

1: SHA-1

2: SHA-256

3: GOST R 34.11-94 (DS validation is NOT obligatory)

4: SHA-384

Digest should meet following conditions

Type:1 => max. length of digest **40** characters

Type:2 => max. length of digest **64** characters

Type:4 => max. length of digest **96** characters

Validate RRSIG Record

Analyzing DNSSEC problems for www.kizilay.org.tr

not signed yet

.	✓ Found 2 DNSKEY records for . ✓ DS=20326/SHA-256 verifies DNSKEY=20326/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
tr	✓ Found 1 DS records for tr in the . zone ✓ DS=48972/SHA-256 has algorithm ECDSAP256SHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=46780 and DNSKEY=46780 verifies the DS RRset ✓ Found 2 DNSKEY records for tr ✓ DS=48972/SHA-256 verifies DNSKEY=48972/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=48972 and DNSKEY=48972/SEP verifies the DNSKEY RRset
org.tr	✓ Found 1 DS records for org.tr in the tr zone ✓ DS=57515/SHA-256 has algorithm ECDSAP256SHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=28835 and DNSKEY=28835 verifies the DS RRset ✓ Found 2 DNSKEY records for org.tr ✓ DS=57515/SHA-256 verifies DNSKEY=57515/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=57515 and DNSKEY=57515/SEP verifies the DNSKEY RRset
kizilay.org.tr	✗ No DS records found for kizilay.org.tr in the org.tr zone ✗ No DNSKEY records found ✓ ns2.kizilay.org.tr is authoritative for www.kizilay.org.tr ✓ www.kizilay.org.tr A RR has value 185.225.164.15 ✗ No RRSIGs found
kizilay.org.tr	✓ ns1.kizilay.org.tr is authoritative for www.kizilay.org.tr ✓ www.kizilay.org.tr A RR has value 185.225.164.15 ✗ No RRSIGs found

FURTHER STUDIES

Involvement of Registrars & Third Parties

ISPs, Governmental Institutes (e.g. e-devlet), Universities, Commercial and etc.

Experince Sharing

Meetings, trainings and events

Test Bed & Hands-on Training

SUMMARY

Assessment of current DNS infrastructure

Check updates & configurations

Training (teoritical & practical)

Defining Strategy & DNSSEC Specs

Testing all schenarios (rollover / rollback)

Monitoring