DNSSEC
DEPLOYMENT UNDER ".TR"

Dr. Attila Özgit
.tr ccTLD Manager

A BRIEF HISTORY OF ".TR"

- **Since 1991** (dates back to the first internet connection of the country – ***TR-NET***)
- Named as **"Nic.tr"**

.TR (AS OF 2014-Q4)

- > 350.000 domain names
  - 85% identity validated
    - proving documents (trade marks, CoC registrations, etc.)
    - national citizenship DB
    - Trust, strength add confidence for domain name owners
  - 20+ second level domain names
    - com.tr, gov.tr, info.tr, etc.
  - Second level domain names for special requirements
    - av.tr, dr.tr, pol.tr

.TR (AS OF 2014-Q4)

- Fully automated, paperless office
- Registry-Registrar Model since 2008
  - 10 active registrars
  - 3 inactive
  - 4 coming soon

IDN – INTERNATIONALIZED DOMAIN NAMES

- ğ, Ğ, ı, İ, ü, Ü, ş, Ş, ö, Ö, ç, Ç
- 10.000+ (3% of the total)

- Since 2006 ...

PRICING

Purchase / Extensions	1 Year	2 Years	3 Years	4 Years	5 Years
com.tr - net.tr	*$11*	$20	$29	$37	$45
biz.tr - info.tr - tv.tr - org.tr - web.tr - gen.tr - av.tr - dr.tr - bbs.tr	*$7*	$12	$18	$22	$27
namesurname.com.tr - namesurname.net.tr	*$5*	$10	$15	$19	$22
k12.tr - name.tr - tel.tr - bel.tr	*$2*	$4	$7	$9	$11
gov.tr - edu.tr - pol.tr - tsk.tr	*N/C*	*N/C*	*N/C*	*N/C*	*N/C*

EVOLUTION OF .TR

- One of the very first examples of MSHM (Multi-stake Holder Model)
- Internet Council – 1998 (30 seats)
- DNS Working Group – 2000 (11 seats)
- Legislation, Jurisdiction and Execution functions are separated from the very beginning
- Being held back since 2008 ☹

NOW … “DNSSEC”

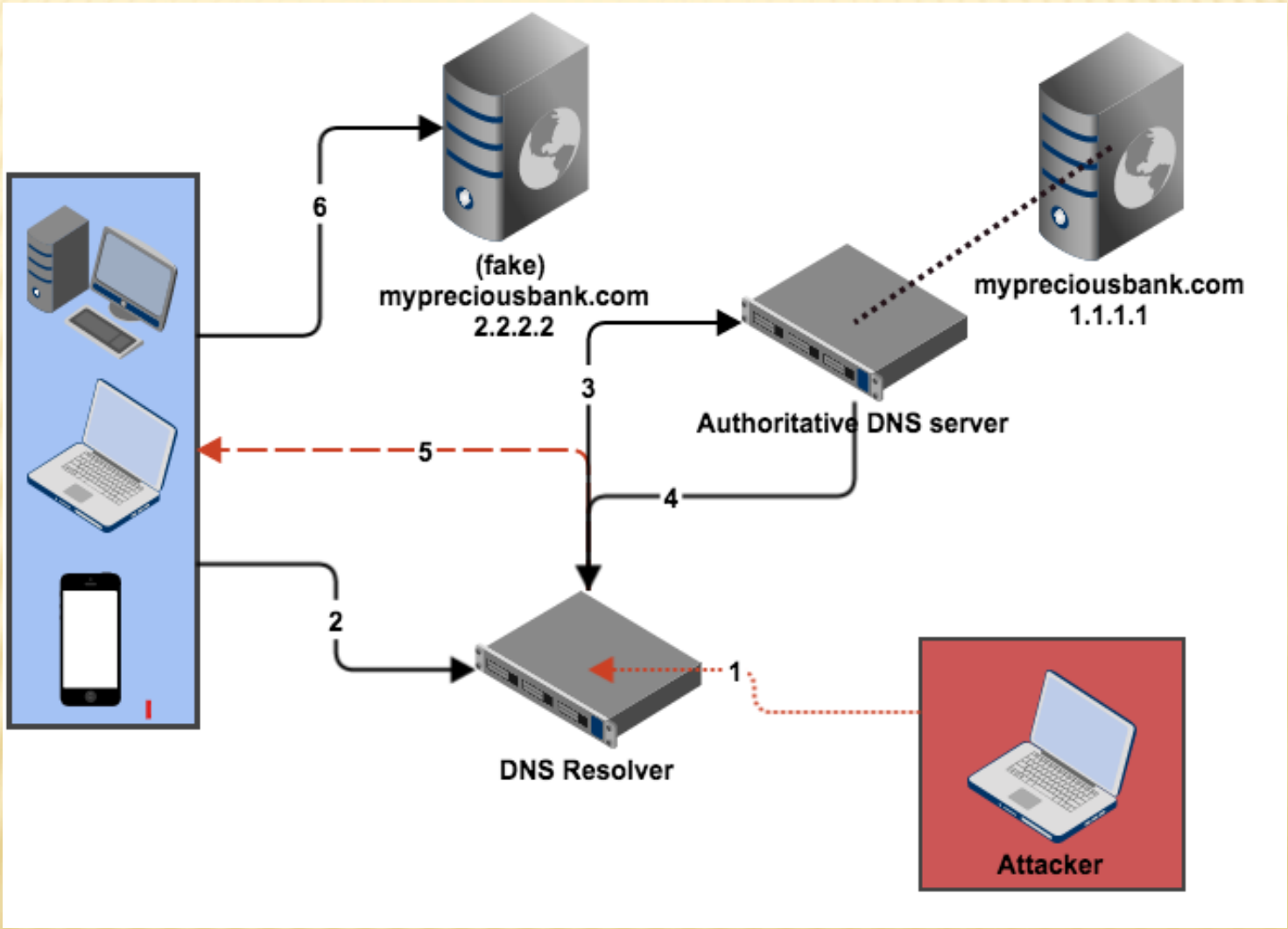
WHAT DNSSEC IS NOT?

- It is NOT
  - a protection against DDOS attacks
  - about privacy
  - a PKI
  - a protection against IP Spoofing
  - a provisioning of confidentiality of DNS responses
- It is basically a trust mechanism

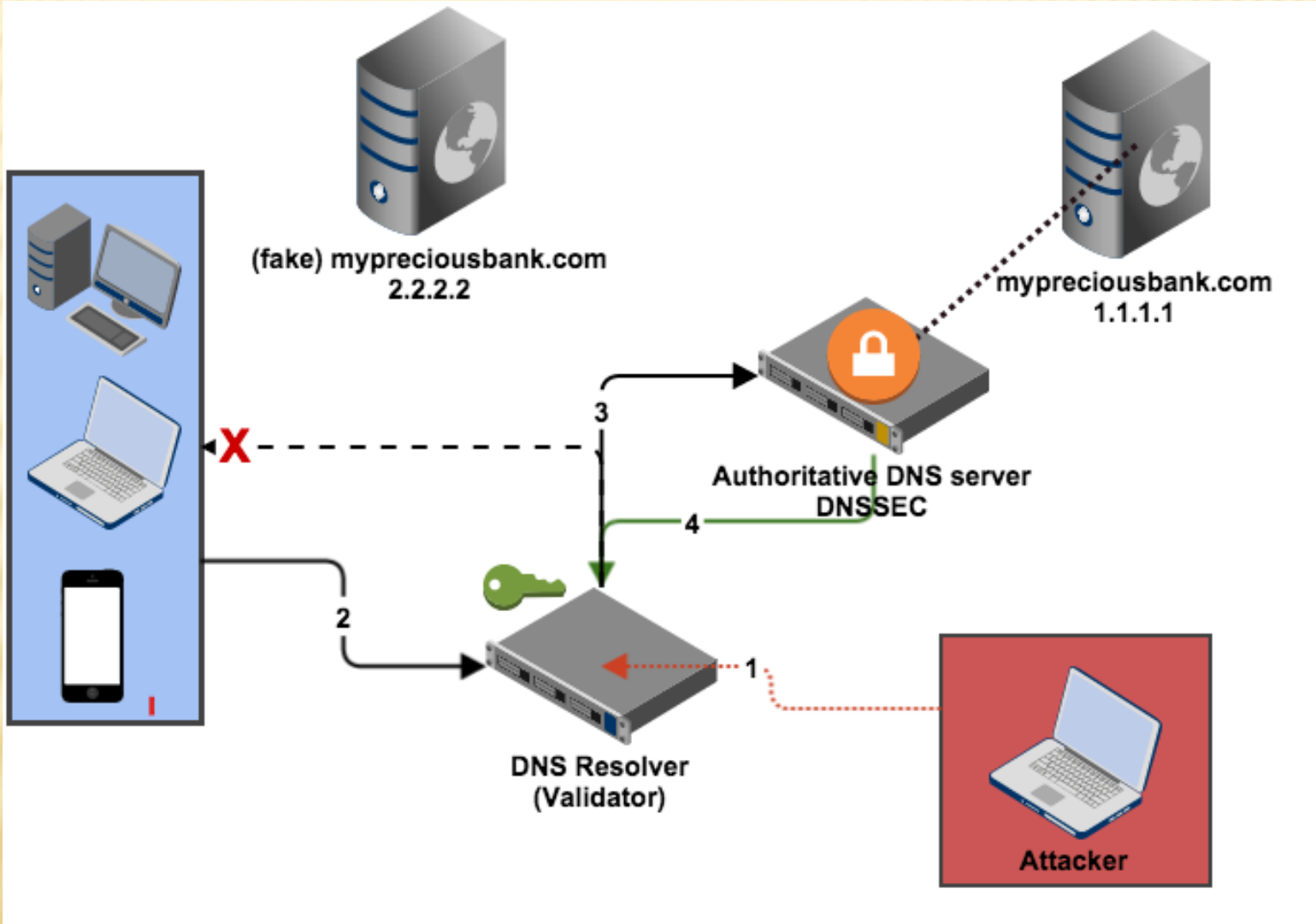
WHAT IS DNSSEC?

- DNSSEC
  - "Domain Name System Security Extensions"
- It adds digital signatures to a domain name's DNS records to determine the authenticity.
- It uses a digital signature to create a chain of authority (and a chain of trust).
  - Then, it uses the chain to verify the DNS record.
- It addresses an identified security risk and helps prevent some malicious activities
  - Cache poisoning, Man-in-the-middle etc.

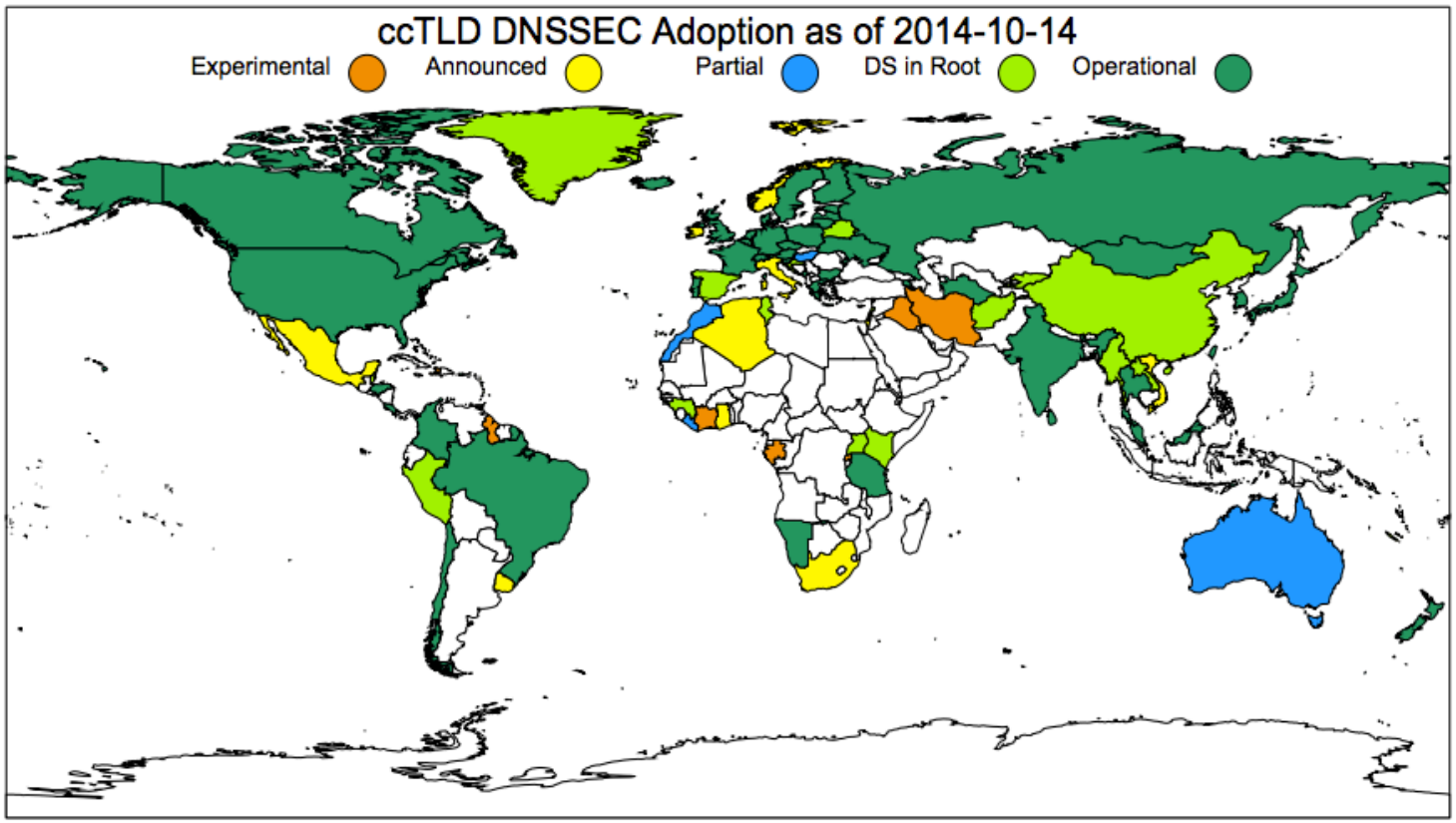
DNS WITHOUT DNSSEC



DNS WITH DNSSEC



CCTLD DEPLOYMENT STATUS

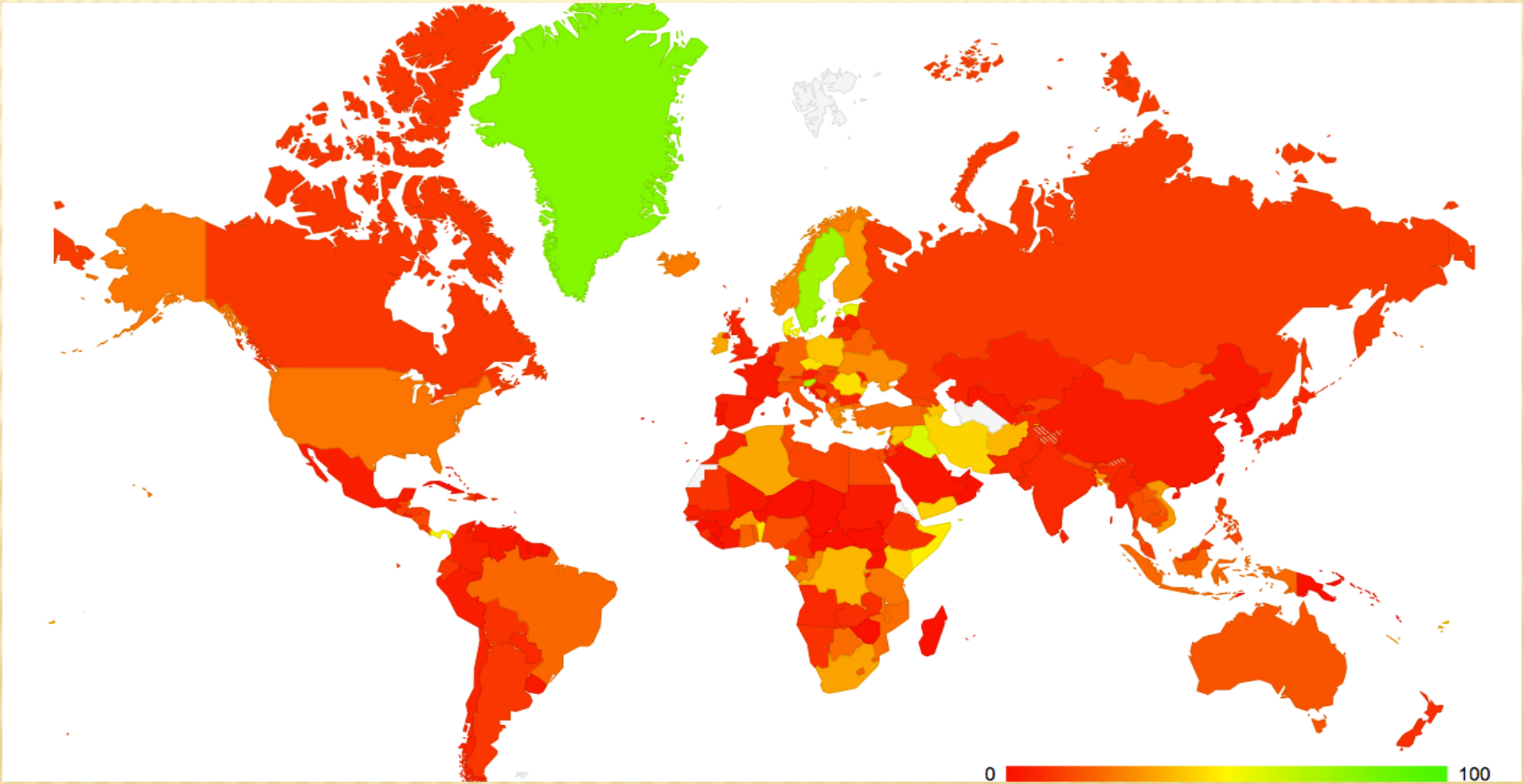


Experimental -- Internal experimentation announced or observed (11):	CI GA GY HK HT IQ IR MS MU RW TO
Announced -- Public commitment to deploy (11):	DZ GH IE IL IT MX NO SG UY VN ZA
Partial -- Zone is signed but not in operation (no DS in root) (5):	AU HU LR MA VC
DS in Root -- Zone is signed and its DS has been published (29):	AD AF AG AW BY BZ CC CN ES FO GI GL GN HR KE KG KI LA LB LC MM NC NU PE PW SJ TN TV UG
Operational -- Accepting signed delegations and DS in root (62):	AC AM AT BE BG BR CA CH CL CO CR CX CZ DE DK EE FI FR GR GS HN IN IO IS JP KR LI LK LT LU LV ME MN MY NA NF NL NZ PL PM PR PT RE RU SB SC SE SH SI SX TF TH TL TM TT TW TZ UA UK US WF YT

SIGNING AND VALIDATION

- Signing is not enough unless resolvers are dnssec aware
  - Validator
- DNSSEC-aware resolvers (validators) are less than %15
- Half of them are google public dns servers

DNSSEC VALIDATION



http://stats.labs.apnic.net/dnssec

IS DNSSEC DEPLOYMENT ENOUGH?

- Zones under TLDs (e.g. com.tr) being signed does not mean it's done
  - We need individual names being signed (e.g., google.com facebook.com microsoft.com and many many more are not signed yet)
  - We need more and more
    - DNSSEC-aware resolvers
    - Client-side validation

DNSSEC UNDER .TR

- .tr not signed yet
- DNSSEC hands on workshop with ICANN and NSRC in May 2014
  - 30 attendees
- Testbed almost ready (not announced)

.TR CCTLD ROADMAP

- Testbed
- .tr zone signing
- Adding DS record to IANA database (root servers)
- Signing some second level zones (com.tr, dnssec.tr)
- Signing names under nic.tr (ns1.nic.tr, www.nic.tr etc.)
- Accepting/registering DS records from domain owners (e.g., garanti.com.tr)

THEN?

- Big players should be involved
  - Finance
  - Telecom operators
  - Internet Service Providers
  - Registrars
  - Government (gov.tr)
- More and more DNSSEC-aware resolvers
- Increasing public interest
  - Users should demand for
    - DNSSEC-aware resolvers
    - DNSSEC-aware applications

DANE

- DNS-based Authentication of Named Entities (DANE)
- Trusting a large number of CAs might be a problem because any breached CA could issue a certificate for any domain name.
- DANE enables the administrator of a domain name to certify the keys used in that domain's TLS servers by storing them in the Domain Name System (DNS).
- DANE needs DNS records to be signed with DNSSEC.
- DANE allows a domain owner to specify which CA is allowed to issue certificates for a particular resource, which solves the problem of any CA being able to issue certificates for any domain.

THANK YOU ...