

Name : Shreya Singh Id : 2022pct0019



ASSIGNMENT : 3 DNSSEC

DNSSEC validation for a given domain name using Verisign labs.
Domain : raspberrypi.org

Domain Name:

Analyzing DNSSEC problems for raspberrypi.org

.	<ul style="list-style-type: none">Found 2 DNSKEY records for .DS=20326/SHA-256 verifies DNSKEY=20326/SEPFound 1 RRSIGs over DNSKEY RRsetRRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
org	<ul style="list-style-type: none">Found 1 DS records for org in the . zoneDS=26974/SHA-256 has algorithm RSASHA256Found 1 RRSIGs over DS RRsetRRSIG=46780 and DNSKEY=46780 verifies the DS RRsetFound 3 DNSKEY records for orgDS=26974/SHA-256 verifies DNSKEY=26974/SEPFound 1 RRSIGs over DNSKEY RRsetRRSIG=26974 and DNSKEY=26974/SEP verifies the DNSKEY RRset
raspberrypi.org	<ul style="list-style-type: none">Found 1 DS records for raspberrypi.org in the org zoneDS=2371/SHA-256 has algorithm ECDsap256SHA256Found 1 RRSIGs over DS RRsetRRSIG=61110 and DNSKEY=61110 verifies the DS RRsetFound 2 DNSKEY records for raspberrypi.orgDS=2371/SHA-256 verifies DNSKEY=2371/SEPFound 1 RRSIGs over DNSKEY RRsetRRSIG=2371 and DNSKEY=2371/SEP verifies the DNSKEY RRsettony.ns.cloudflare.com is authoritative for raspberrypi.orgraspberrypi.org A RR has value 172.67.36.98Found 1 RRSIGs over A RRsetRRSIG=34505 and DNSKEY=34505 verifies the A RRset
raspberrypi.org	<ul style="list-style-type: none">april.ns.cloudflare.com is authoritative for raspberrypi.orgraspberrypi.org A RR has value 104.22.0.43Found 1 RRSIGs over A RRsetRRSIG=34505 and DNSKEY=34505 verifies the A RRset

Move your mouse over any  or  symbols for remediation hints.

Want a second opinion? Test your domain now at [domain-test](#)

Step 1: Root server : - [.]

dig +dnssec DNSKEY . @8.8.8.8

- ✓ 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

It is giving DNSKEY of root . here there are two DNSKEY first one is ZSK and second one is KSK .

```
Activities Terminal Oct 30 01:48 shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx: ~
;; MSG SIZE rcvd: 28
shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:~$ dig +dnssec DNSKEY . @8.8.8.8
<<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> +dnssec DNSKEY . @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 47728
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;;      .                IN      DNSKEY
;; ANSWER SECTION:
;;      79986 IN      DNSKEY 256 3 8 AwEAAadzS9RV5uUtkUCN7vvyvpb0kDZgmtXwN5Sj/d08+X7ND2sgWBabK nFhftr0s5x9DUhKR3gp
MPIxac84Nou8Wzkiu2A/5TZP1f6KpCL8epgem dLZVd1ATHEjp80KHlQmDjSE0/ffrGgi8ij02vDF3AMsRUmH7qntL1E5uf PHGKRM+agGghcAVfJhJN1dw7Ki3Fo22RD83VZ
Bxu9yJ3vL/T4hngelZ K84vg162tLJJwIRK55/3U4p/bZarjtmFOHDfh0DEj1ywrRpkpPnge03g nINoa2tz+Kff67kbQb0NhHJYzPRpVlaMEWZI9pgGH9ZyuFdNrNRx68X
S i07sya7/i+c=
;;      79986 IN      DNSKEY 257 3 8 AwEAAaz/tAm8yTn4Mfeh5eyI96MSVexTBavkMgJzkKTOiW1vkIbzxef3 +/4RgW0q7HrxRixHfL
ExOLAjr5emLVN7SWXgnLh4+B5xQLNVz80g8kv ArMtNR0xVQuCaSnIDdD5LkyWbRd2n9WGe2R8PzgCmr3EgVLRjyBxwzF 0jLHwVNBef53rCj/EWgviWqb9tarpVUDK/b58
Da+sqqls3eNbu7pr+e oZG+SrDK6nWeL3c6H5ApXz7LjVc1uTidsIXxu0LYA4/lLBmSVIZuWdFd RUfhHdY6+cn8HFRm+2hMBANXGxws9555KrUB5qqlhylGa8subX2Nn6Uw
N R1AkUTV74bU=
;;      79986 IN      RRSIG  DNSKEY 8 0 172800 20231111000000 20231021000000 20326 . ed6zMto/T8IDh3jRa7exH7fCaD9Q
VVVGJ8SXuc0JKGrD4YYqwyxYZzpw 6JkgBkP05YwEMPbQEc+KLW93mdEFL7pyWxzQhWX8hY+npFGxdfcZtmpn QoJbNTa1n15iHrrBN6wDn+4/s5FgdLWghMPJdG1tBNkcBj
8ZeZta/2YH K9kL9S4fI+SkZ25vcfdJmFhFC4u87Wpk36gFQPB0UTbr6FN/S90cWLDp g1mCS5v4zjgt13501otGrVY1fnzKpzH4WmZj829BRGdyk5PScqD9FnX3 kHcoq/p
Hlu0TtGPP9bh9Uj/Lgd5ZHCQqtJGxJaNdZHsmg9FrrB6m5gd8 nTXK0g==
;; Query time: 192 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Oct 30 01:48:37 IST 2023
;; MSG SIZE rcvd: 864
shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:~$
```

Step 2: Top level domain server :-(com)

dig +dnssec DNSKEY com @8.8.8.8

- ✓ Found 1 DS records for org in the . zone
- ✓ DS=26974/SHA-256 has algorithm RSASHA256
- ✓ Found 1 RRSIGs over DS RRset
- ✓ RRSIG=46780 and DNSKEY=46780 verifies the DS RRset

- ✔ Found 3 DNSKEY records for org
- ✔ DS=26974/SHA-256 verifies DNSKEY=26974/SEP
- ✔ Found 1 RRSIGs over DNSKEY RRset
- ✔ RRSIG=26974 and DNSKEY=26974/SEP verifies the DNSKEY RRset

It is requesting the DNSKEY records for the “com” top level domain from google public DNS .

```

shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx: ~
;; WHEN: Mon Oct 30 01:48:37 IST 2023
;; MSG SIZE rcvd: 864

shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:~$ dig +dnssec DNSKEY com @8.8.8.8

;<<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> +dnssec DNSKEY com @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 117411
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;com.                                IN      DNSKEY

;; ANSWER SECTION:
com.      2299      IN      DNSKEY  256 3 8 AwEAAcBxnScZaHfDT9aepsoUJgaaVLBPtxmQ7W/yj3Vmn6JNaCJ/Z3c Trpmw1f3xLH127F1Zoe
3bR018wOfsI26I9k4GTMIo3fTODyQud7c52n5 4gH0aeluncejrokqg79cGr7AUNCTZvRAW74eshI33py92WiscAm/r5s gygyWNYrsb8f8DLoMHaxngn9Rh5KkehMFLMC
oBUvsVfvFRl3h8=
com.      2299      IN      DNSKEY  257 3 8 AQPDzldNmMVZF4NcNj0uEnKDg7tnv/F3MyQR0lpBmVcNcsIszxNFxsB fKNW9JVCYqplk8366LE
7VbICNRzfzP2h9008HRL+H+E08zauK8k7evWEm u/6od+2boggPotLEfGnyvNPasI7FOiroDsnw/taggzHRX1Z7S0101PWPn IwSUyW0Z79VmcQ1GLkc6NLYvG3HwYmynQv6oF
wGV/RELSw7Z5drbTQ0H XvZbqMUI7BaHskmvgn1G7oKZ1YLF709LoVNC0+7ASbqmZN7Z9EGU/Qh 2K/BgUe8Hs0XVcdPKrtyYnoQHD2ynKPCmMLTElh2/2HDHJRPJ2aywIp
K Mnv40Po/
com.      2299      IN      RRSIG  DNSKEY 8 1 86400 20231111172421 20231027171921 30909 com. aXVTnutTc0sKnoFcVSENMWIFSI
F3ZDDvPb+TgWBBFEmujL2ccq+jgg5 9gP4Y0ukvmVfM8q3r8+YKlu+LgSm8Wj9GUMxMqai+zhRRWLLr3h3I+ZB ZOfngM4E9L0XGZ5Skz///lq7oW/YewkoY7juorjfmhaO
ZM/9u84cmnt5 J25D8LLuudG0E08cp7DEr/LQxcFzHYWuA1RjnhYQ13Bers0A6vLUfNu 7j0cpilesDsokctBjKKLXLEh3htysg190DNQWAKhXPP2dEC2cFadVIBj Ys90s
FNZQ4Ds1HqCRk/n9XrdZqrvBsePokthu+estXocjsUuPDRlhb5 5+xx5Q==

;; Query time: 168 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Oct 30 01:49:42 IST 2023
;; MSG SIZE rcvd: 777

shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:~$

```

Step 3: dig +dnssec com. DS @8.8.8.8

Requesting DS(Delegation signer) record for the “com” TLD server from google public DNS server .

```

shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:~$ dig +dnssec com. DS @8.8.8.8

;<<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> +dnssec com. DS @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38233
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;com.                                IN      DS

;; ANSWER SECTION:
com.      81581     IN      DS      30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CF C41
com.      81581     IN      RRSIG  DS 8 1 86400 20231111050000 20231029040000 46780 . wD83DQE+Gbwle3R1xax
S3Hjiy6aUwIPOLBT3Lwc+7X LcCjiJtSWLU6J+r0yILBFVzBX/zjiPxFUTXNEkhvJz8kxwZFG8nkcP1B Uw+JX/TG+NxarQyo6ljbzZXwGTvU2tZKDuIG1
RTzoc F3lyT0+0NR17bLIQbslnZKq+PnX9vQXm6jdQqwmJojuub8pERah513HS REaGAe7n0y2g9wb6K8HtVoUrT771AbQlu/pRMR3UnNbJ12fqCbWOW0f
30VnAmy/61W5l1/XPUSeYp8BTczFoubgwQ8RXjh72MVo cH/ODg==

;; Query time: 156 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Oct 30 01:50:43 IST 2023
;; MSG SIZE rcvd: 367

```

Step 4: Authoritative Nameserver: raspberrypi.com

dig +dnssec DNSKEY raspberrypi.com @8.8.8.8

- ✓ Found 1 DS records for raspberrypi.org in the org zone
- ✓ DS=2371/SHA-256 has algorithm ECDSAP256SHA256
- ✓ Found 1 RRSIGs over DS RRset
- ✓ RRSIG=61110 and DNSKEY=61110 verifies the DS RRset
- ✓ Found 2 DNSKEY records for raspberrypi.org
- ✓ DS=2371/SHA-256 verifies DNSKEY=2371/SEP
- ✓ Found 1 RRSIGs over DNSKEY RRset
- ✓ RRSIG=2371 and DNSKEY=2371/SEP verifies the DNSKEY RRset
- ✓ april.ns.cloudflare.com is authoritative for raspberrypi.org
- ✓ raspberrypi.org A RR has value 104.22.0.43
- ✓ Found 1 RRSIGs over A RRset
- ✓ RRSIG=34505 and DNSKEY=34505 verifies the A RRset

DNSKEY record for the raspberrypi.org domain from google public DNS server .

```
shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:~$ dig +dnssec DNSKEY raspberrypi.org @8.8.8.8

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> +dnssec DNSKEY raspberrypi.org @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 26677
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
; raspberrypi.org.                IN      DNSKEY

;; ANSWER SECTION:
raspberrypi.org.      3600    IN      DNSKEY  257 3 13 mdsswUyr3DPW132m0i8V9xESWE8jTo0dxCjjnopKl+GqJxpVXckHAeF+ KkxLbxILfDLUT0rAK9
iUzy1L53eKQ==
raspberrypi.org.      3600    IN      DNSKEY  256 3 13 oJMRESz5E4gYzS/q6XDrVU1qMPYIjCWzJa0au8XNEZeqCYKD5ar0IRd8 KqXXFJkqmVfRvMGPmM
1x8fGAa2XhSA==
raspberrypi.org.      3600    IN      RRSIG   DNSKEY 13 2 3600 20231205040123 20231005040123 2371 raspberrypi.org. rCU7MmQP8hSmcj
AqoDqypnxFBVr/rct9t969Z1JmK8pz7Cm4Xgu4mrF 4JkpiBSrAfdRjY7ti/o+FDsaH1pbxQ==

;; Query time: 152 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Oct 30 01:52:12 IST 2023
;; MSG SIZE rcvd: 315
```

Step 5: dig +dnssec DNSKEY raspberrypi.org DS @8.8.8.8

Performing queries for the DNSKEY records and another for the DS record for raspberrypi.org domain from Google public DNS server.

```
;; MSG SIZE rcvd: 515
shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:~$ dig +dnssec DNSKEY raspberrypi.org DS @8.8.8.8
;; Warning, extra type option

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> +dnssec DNSKEY raspberrypi.org DS @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59332
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;raspberrypi.org.                IN      DS

;; ANSWER SECTION:
raspberrypi.org.                3600    IN      DS      2371 13 2 6984AB832CEC75FC12324E60859BB6100AF26D797F0D06468C802EA8 D71E522A
raspberrypi.org.                3600    IN      RRSIG   DS 8 2 3600 20231115152550 20231025142550 61110 org. GSe7TAExMsvQcaIXMtAETP9DuUIpMkW
t7ZzpP8X6+E6rDlIXlDDsIMG w0L3fBtpRc2C5TrPGEqYPPLB1BatB+Nf5gcGMP+pICmkXZWLKwzBCDD Nyv/Z0o7YrK17Cvo9gDHDwA1YvxyU3kgL9Aomr56HlWG+hXPk
RDsA9nX SqQ=

;; Query time: 332 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Oct 30 01:53:09 IST 2023
;; MSG SIZE rcvd: 255
```

Step 6: dig +dnssec raspberrypi.org @8.8.8.8

It will retrieve RRSIG and DNSKEY records for raspberrypi.org.

```
Use 'dig +help' (or 'dig -h' for more) for complete list of options
shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:~$ dig +dnssec raspberrypi.org @8.8.8.8

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> +dnssec raspberrypi.org @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63711
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;raspberrypi.org.                IN      A

;; ANSWER SECTION:
raspberrypi.org.                300     IN      A       172.67.36.98
raspberrypi.org.                300     IN      A       104.22.1.43
raspberrypi.org.                300     IN      A       104.22.0.43
raspberrypi.org.                300     IN      RRSIG   A 13 2 300 20231030212912 20231028192912 34505 raspberrypi.org. Km3Ib1+aZXF28d11Ukuz
rwhNAZ8JHBBGWJFs668w0Qn/x/08L2T97Xz2 Z2bDu5hKNV3cxq1x1J900RXDI0dICA==

;; Query time: 60 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Oct 30 01:59:12 IST 2023
;; MSG SIZE rcvd: 203
```