# Several algorithms in DS or DNSKEY RRsets, and consequences

The problem was noticed on cepn.asso.fr (the configuration changed since). Some resolvers or DNS checkers complained about its setup, while other accepted it. What was right?

## Setup

The zone had the following DNSKEY RRset:

```
cepn.asso.fr.           7808 IN DNSKEY 257 3 5 (
                                AwEAAaBtXBNAyFHVvRBB4K9z79+1YRXkUDyycyCzPRpm
                                Xi9lhBOEg5vM3XlaS6OuNOdnFHItpZFNIDBDrPsN1OCf
                                1ULKWpD3KDl1mE7zRK2WOHXeu4WOoFpUcC/1hO6W26DT
                                CkisntU9L8JfPi9osmI+CuzWZhdmyZt+hPvMpjmDthyh
                                MZpb//kNv7+TUeczCo4MExHxjHHIVHOvRmhfyo/J1KBe
                                6eS3G5lDbJEEFUdxuLyGQLaG2f6wlQxoHGnzvM+V/Mj8
                                yGHae//7Z5rMCdaiLJy03u5+l2WVVy954dsrFC6mkB5s
                                M4n8nvbo1d5ap7cI76dJi9XOIUJQohZk5b5eef0=
                                ) ; KSK; alg = RSASHA1; key id = 36778
cepn.asso.fr.           7808 IN DNSKEY 256 3 5 (
                                AwEAAc6AqnBoi+hfxMqtbOeokyqWT46Os5N6ZYoFm8Gb
                                t9OEF3hTpuwDClEsulKSckhr4zFTDj3SvHc9krzeQEl5
                                UNCqmmZeMo/wsxKHTzIVU75fPrs1zOuM9m9zRNV4q9eG
                                YO+I2h4D7E/WlPE7n57EOlmPOxK9g46xE8p9eX3bWVVK
                                FSm60VvginZfTzN3Zgt+peecrboEZnSzWvDVcHY2dq+o
                                w0UEekI1+nfwcIgEOn0Wh8B5Gx3pG5XkV3QvHVN514FH
                                eJLdsk0iFPHv1Xc0rLYWssFVS9s7Z8u0tEju6LshGaPQ
                                +zrQr54RMD9IecwbMCERcrjV2Dm5CZq+Jf53pGc=
                                ) ; ZSK; alg = RSASHA1; key id = 54030
cepn.asso.fr.           7808 IN RRSIG DNSKEY 5 3 10800 (
                                20250115124200 20150216080551 36778 cepn.asso.fr.
                                fc1YnbjbglVC8alL9NN9LUo54kUODgk6gblFt+CjDJ4+
                                0i9HqEdbbW/49wksEMkFySPf24yRaswbf9W/OHeJtXid
                                6CEcVdZiHfPuTzxBelQVfPiIQreJ9yvxBF1z/pmTBf0X
                                o8TEMUjaV4f2c5eqELKdZ986RRk6J35tDd0w3cbeHGV1
                                mnAagjT+SOLlmF8mx6MZkgsgFylBIt0MfEaX1ZS4PfAh
                                TCIXi6shM0KcwZ7rI24nVGcu6wDfxdiwUZ5lJ6KWFBsM
                                pC0beLiKRYlqnQidkech+dlSHQGj0DXAINi6ZrS+iRhv
                                mCLlId4oezMaxx8P3dLo71cAqPGNBwM62A== )
cepn.asso.fr.           7808 IN RRSIG DNSKEY 5 3 10800 (
                                20250115124200 20150216080551 54030 cepn.asso.fr.
                                v1b7K0jZ4WH1yMCvJHOkxWp7EUHtsFPpKjwplu8EhqDs
```

```
                                WAwBOORSFMN6YOPDMfSydXeSwn3+L75OKk1Ne6VNaE5E
                                jeYi7BEChEOwZH1L6/qyIHgwOYCDfQN4HuGOO5RFRKgi
                                p1tO6h3iKnVHFzduSxSby5Oq3iZgbyaSPeAhDa/LZPXv
                                oNb1cVmVrPKTIhZqSxKNCOt4XQ3iUffgrLvq1ErFeuut
                                QQeD3uzwWXCUkZA5rK7fp9eKKlSOJpP3na2r8cEyOWlC
                                jZ2HNPA6pIUnq+w7eDOoGpOaukJ1C85TeE1a8cr3Luf8
                                LnSXm7cIxSWOdw9GZEjaavWFfpYdguFxQQ== )
```

There are two keys, both with the same algorithm, RSASHA1. The DS RRset in the parent zone was (signature ommitted):

```
cepn.asso.fr.           171998 IN DS 36778 5 2 (
                               D21FC827CF4621DF88D06A8F6EA5F4B4DE72A362AB2E
                               03D440C315A9D8FE1407 )
cepn.asso.fr.           171998 IN DS 13585 8 2 (
                               AB057D7A9BBDB721EBD33FC64F3C6CC53D9020D12F18
                               BCEFC696494C9F9D6111 )
```

This time, there are two algorithms, 5 (RSASHA1) for the key 36778 and 8 (RSASHA256) for the 13585 (the list of algorithms is registered at IANA). Note that only 36778 is in the zone (a dangling DS, which is legal, and irrelevant here). Note also that both DS use the same digest type, 2 (SHA256).

## Results

Unbound reliably servfails on this setup. DNSviz indicates errors in the zone and says "cepn.asso.fr./DNSKEY (alg 5, id 54030): The DS RRset for the zone included algorithm 8 (RSASHA256), but no RRSIG with algorithm 8 covering the RRset was returned in the response. (195.68.96.3, 217.70.177.40)"

BIND reliably validates the zone:

```
; <<>> DiG 9.9.5-8-Debian <<>> @relay1.nic.fr DNSKEY cepn.asso.fr
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30861
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;cepn.asso.fr.          IN DNSKEY
```

```
;; ANSWER SECTION:
cepn.asso.fr.           7808 IN DNSKEY 257 3 5 (
                                AwEAAaBtXBNAyFHVvRBB4K9z79+1YRXkUDyycyCzPRpm
...
```

And so does Google Public DNS. The zone tester Zonemaster does not indicate a problem (it just emits a warning for a signature validity period which is too long).

## Standards

RFC 4035, section 2.2, said "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). This is to avoid downgrade attacks, as explained in RFC 5702, section 8.2.

RFC 6840, section 5.11, clarified that and says "A signed zone MUST include a DNSKEY for each algorithm present in the zone's DS RRset and expected trust anchors for the zone. The zone MUST also be signed with each algorithm (though not each key) present in the DNSKEY RRset." The zone violated the first requirment (there was an algorithm 8 in the DS RRset but not in the DNSKEY RRset) but not the second (there was only algorithm 5 in the DNSKEY RRset).

But the RFC 6840 adds "This requirement applies to servers, not validators. Validators SHOULD accept any single valid path. They SHOULD NOT insist that all algorithms signaled in the DS RRset work, and they MUST NOT insist that all algorithms signaled in the DNSKEY RRset work. A validator MAY have a configuration option to perform a signature completeness test to support troubleshooting."

## Analysis

The important point is that the zone was *wrong* but it does not mean the resolver should refuse to validate it (the second paragraph in RFC 6840 mentioned above).

So, Unbound was probably too strict here. There was a valid path from fr to cepn.asso.fr and it should have validate, by using it, since Unbound knows both algorithms (RSASHA1 and RSASHA256).

For programs which are not validators but zone testers, we expect them to be picky and to report errors, even if they are not fatal. For instance, an hypothetical validator which understands only RSASHA256 and not RSASHA1 (not possible with today's DNSSEC rules, where RSASHA1 is mandatory, see RFC 4034, section A.1) would have break with such a setup. So, Zonemaster missed an opportunity to report the problem.

## Thanks

Mark Andrews, Mukund Sivaraman, Yuri Schaeffer, and Casey Deccio, for explanations.