



Alg 18 in 1.1.1.1

Bas Westerbaan, Cloudflare  
DNSOP, Oct 2<sup>nd</sup>

# Deadlines aren't that far away

US Federal Government: PQ authentication by Dec 31, 2031 for high-value assets and high-impact systems.

EU roadmap (not binding): by Dec 31, 2030: fully PQ for high-risk use cases and critical infrastructure.

Similar national guidance from UK, Australia, France, ...

Following quantum advances earlier in the year, Google, Cloudflare, and Microsoft target to be fully PQ by 2029.

We need a PQ DNSSEC story

# I don't care much what the story is

DNSSEC isn't a high value system.

DNS doesn't believe in quantum computers.

ML-DSA-44 in DNSSEC will work just fine.

We need better post-quantum signature schemes.

We need to rework DNSSEC drastically.

I do care about having more clarity soon.

That allows everyone that depends on DNSSEC to plan accordingly.

# Which one is easiest to check?

DNSSEC isn't a high value system.

DNS doesn't believe in quantum computers.

ML-DSA-44 in DNSSEC will work just fine.

We need better post-quantum signature schemes.

We need to rework DNSSEC drastically.

# Which one is easiest to check?

DNSSEC isn't a high value system.

DNS doesn't believe in quantum computers.

ML-DSA-44 in DNSSEC will work just fine.

We need better post-quantum signature schemes.

We need to rework DNSSEC drastically.

```
bas@MXCXF2JM70 ~ $ dig +dnssec @1.1.1.1 valid.mldsaa44.dnstest.dev
;; Truncated, retrying in TCP mode.

; <>> DiG 9.10.6 <<>> +dnssec @1.1.1.1 valid.mldsaa44.dnstest.dev
(1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 54218
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;valid.mldsaa44.dnstest.dev.      IN      A

;; ANSWER SECTION:
valid.mldsaa44.dnstest.dev. 0      IN      A      188.114.96.0
valid.mldsaa44.dnstest.dev. 0      IN      A      188.114.97.0
valid.mldsaa44.dnstest.dev. 0      IN      RRSIG  A 18 4 0 20261002205839 20261001195839 23176 valid.mldsaa44.dnstest.dev. 3CYyvuugmaN8jQtu1LNb00G0/ucsyPoNk9S9oigHs44irCAVSByaZprIL
/ LoyiVQ9v5/u88a9waCNObHgEQV6U+10fN0376D3Uy3WNIESBmtTdDuHp /yLncqsg5+XjioQzDW519H+31u2rF70PPCVzwsZko2ZQcIxsu9guI2t Vh26ZJlkiWhS0UQMBUMf6G3S5oKvBTo4kZxhJyH/c0RLxZQp7hwYsvIC BD
B71avRVM2azoKQ3eS+79rqPCVw3jBb+186EEKMsJYNewGsHKC+zmSX 5szjnd4y9ZukLZTCjPSF3tBYCL+d4P6QyHrhjqNbAan7KoErwEmaoI mQdTJFNDRaHb0/48cDzJp4jqaWM1s0N+UFTLkmfcPC4H2Fgi2yzZXhhx jfp4VM
K/UW5fzVE0ISc2vsfL8azfa0+uQzPfFmgom78MEc61hozrDbnb sPJclEqbH/TLd00FZ0AK+gov4o4mk9mzc9KAN25vhiJrTmVMjvmc9N5b 4bb1lpwqP0nfmpde5UAWGoxpVHJknnfegsUbuRpcTHxgCvIEHaMFwu7K 0WZTTXZ/Pu
vlQcX+fmR0s8a0BV9MtsFX/gbYD650SHFubqAgKZnVif0 /9t1NJc4TL3WUPuW1915Ew0rqsAgx6Z9DCEtha/09GBXdJhNE69YJ84z1 eRdVJiSUEZP02GTnHnLaXPUhICLzeFJvK925QD4WhtU5/5/WBGSZcWI o/+CYDW1PXpppd
TpkCvphW0k62cl0nBx80jk+x+RHeySVNEFBT1jYE8F h2LWQM2hi1+YepTYPe+HTsTp0QXQJ/Ji0fanEKlmaKha+rIHvZPaUwzr nBvP1QncUvFp0ScJ0kEUKI1AzTU9WX+8HWWVZqdrSEkggAahC3959y2c7 n/AsB0jQU/7k7YyH23
dVutZjRq28XsRLY4sUDW68fYeMJWfirA7GVf+2 Kjsueo7Aeg+kyqy10ChwoMidBH373KA8I72//EGinWwQ0TpAueaTQfq bIngOYsSN6QNDRO5uTX6kz1XQospczH/VEI6xCmAUTVL+QKdbrsDJo/K j3mfAPm8C6M9VyFF+pb8Vx
3gg6FTGwuHHeytoMKRWyqiD+pAQAEtBmhy xkSnmMwnpQmU7863hvsRojl1QnyZ83IZt9UaUSbC26YV0LQvapfqhawn rfbhqmXWws3qXBS0YJgxoiv/nsUW2klZXB8mCHN8ox90JSdz4q9HwS6 4gz18Sp5EsBhQ6n0li2o/yD47X
Ekmaq+VLDFtU6GQzHfPUqTvNZMQRk8+ sPYvo4FhcnpjYw2efJk2XjYc91aryKip5ERmKPYuoy61bJvn1s3xTaLS Js7RwDiTy2RmISW6gmf5m3rkyYZs8T3ClVn56FFYoWvCXRG60mY1z8Q CRCS68vi10NFMQNX0BU9E8EijY2j6+
gWB0M0TRv0S9y6j6AA1iEX/qyW d9z9qbnwSmsMfao9UvgGpVLuzBnsfP2j2G96bb3/L55maHK5szjuFnt IjP/EqIJSKHToPLUXzGbnVrxPxZ+1Saqe9VpIgrMI+0y/3FVYUq/Nk iMud9q/S7RdvAN47M41KRv+b1bjWLF7Q31
0MApV2ICezxtKQ7FNA+6A DdLhBxaG6A0SE3DImZ0+BUWk54H6L9I1lcqPIEonGu80KqR4VortAs86Ww bxBbVWPURD0jBTwXWqe/Qsnt+0DZtLFyxL4nvl6a0B/id8dz3ZjebJHY NdktwZ9aBoAdCUvBXbzQ6zr3fgickhZLh705y
3JVdwsJihX1p4kM/3i 9e3aLgxaXgYdXsMd9uLdMNVsZsoQnfSFtZr5pL74NPPqv540YwLVIL bCEwZ7kmxXImEXnn6fft2DrLrNIMLSNj1gvxdYZ5bgvLMBkQnD72S7q 9fp6XIgZAIIn7ZcA7+jGN4niF00bK6FK/jC0/AP0s+b
mvj722xSNq0M 1yX428bHqkhwG0Xh5o4uhzTLl/gsXMx031oM4NMav0QJviriJrmCp6kL 9p1eF3gVtb0rWSEMDQzeZnovnc1T0FA9RC5WP4LFMPHYHouuQLZLSgcMX QIpgM0C3Z4ZwSrTe1IAsn0clKhTb1hru0liLYqHn65Dmhv
UycNiZe0ZS 6QoQtbe1283TJQ/N8Bb1LZ5NnoCnyavdyYCe8dIK42JrDZEWtZQ8kqu 7F53S0YJIUazVWqt/9pvixj1Bd3QdcHy9K3ZXKUI/LY1+cYUvA5AxU4 3SbgazDmZ14ftZdC39wFssn1lN9pPi79+VrVvmucDTIKciuib5
e+mcAB ajJn0Ktm7Bv+xBc8BAqtWkY6jKBXuaxxb5U8waUsyCJEGi3QcRIOPS6a 4Cvp79VWT0eIzYqzLX2H+VLJFUBIGJiaZ+ww3SL6CHF+xxBLcdC80Yk tZEs0oivlv+pi6JAt95/DIFoidK6m/L2JLPpYJPbwrM9jt9YkCAQX6
Fi 0rVn3F+cnfX/9Rg5UEG6aslsyb4Dp6uUGS2WldTB8RTAhtYPL97GE75TN BCvk6i4xYLN31AabQXHA3A08D2AYLZyg4uxYav3vgNWG/He+S4qni5 UipMwYdMefHwP8M6cjpexD34TRL09VvQDHFV2EyyqY9aSEVCBAc1etHg x
swzLT80fo7b0v1nmIEG101w4RT5EBrfvyGSC6P1mZ0+BUWk54H6L9I1lcqPIEonGu80KqR4VortAs86Ww bxBbVWPURD0jBTwXWqe/Qsnt+0DZtLFyxL4nvl6a0B/id8dz3ZjebJHY NdktwZ9aBoAdCUvBXbzQ6zr3fgickhZLh705y
JLs1ETEs4744jQxGK0RqactSVRSxvW8Vi/68P+1VcP0bZHa9nH+ UPaIUJ9CqPagFb4nkKFeixf/WgricdW6RLqfcvNaKc8BWP1r+irknVfx wmtcgh/gxhSvTiJLRsNESQ4+Q44hf1JzH196M5LZgLY+euIIFwVYJB s3xr4PMjD
/z1tKeeU0wdPzy4GcPHH5tTX+5hd/ndzb2tKhwsyxnuUlu6NR /u0P7legcg64Xb0YeMdHIZgQ8nS1m/9bqJmExyoCv+yzfLQMK0sJ6LA d6KpiR9Ju5Ho0Sg+P3bskfaKRICahvoeQekNFhk5QEVGSVC6jpaSwtTW 3Q8ab42TpcDD6
erv8/gRIZEyEqYqnMgROXF1d4WMK5yhpdd3j7P8AAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAABEEJzY=

;; Query time: 16 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Thu Oct 01 22:58:39 CEST 2026
;; MSG SIZE rcvd: 2563
```

# Testing ML-DSA-44 at scale

IANA assigned alg 18 to ML-DSA-44.

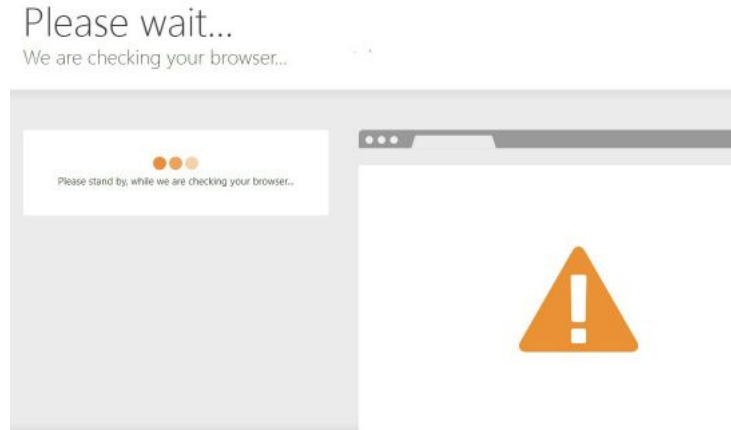
1.1.1.1 support alg 18 by default with downgrade protection\*.

Added support to authoritative (for now opt-in.)

Test zones, eg. [valid.mldsa44.dnstest.dev](https://valid.mldsa44.dnstest.dev)

Starting today (?) we're running probes  
From challenges pages (those )  
to gather data on breakage and  
performance.

Vicky will present results at OARC 47.



If data looks good, we'll roll out alg 18 signing

That won't be the end of the story: we will still have 2,420 bytes of motivation to do better.

DNSSEC isn't a high value system.

DNS doesn't believe in quantum computers.

ML-DSA-44 in DNSSEC will work just fine.

We need better post-quantum signature schemes.

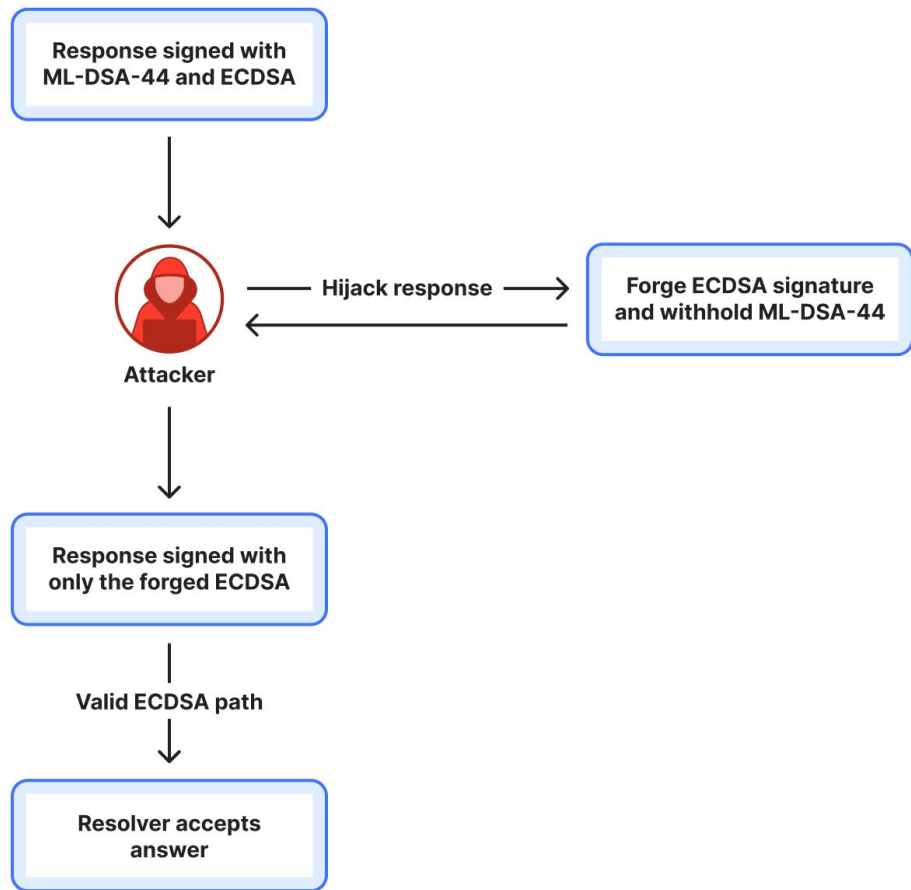
We need to rework DNSSEC drastically.

# Better PQ signatures

There are promising signature schemes in the NIST on-ramp (eg. MAYO), but need more time to gain confidence, and will not be broadly available before 2031. Recent attacks on HAWK and SQISign underscore this.

I would be surprised to see a final FN-DSA (Falcon) standard in 2029, given its specification complexity and planned changes.

\* Downgrades with dual-signed zone



## \* Preventing downgrades

Downgrade is easy to prevent by having the validator insist on a PQ signature if the parent zone advertises it in authenticated DS record.

This does go against RFC 6840's "validators SHOULD accept any single valid oath".

# Thank you!

[blog.cloudflare.com/post-quantum-dnssec-1111](https://blog.cloudflare.com/post-quantum-dnssec-1111)  
[dnstest.dev/post-quantum](https://dnstest.dev/post-quantum)  
[draft-westerbaan-dnssec-mlds](#)