

afnic
Our Journey to
Elliptic stuff

Afnic, 10/2020

afnic

About Afnic in brief

- ✓ Non-profit association founded in 1998
- ✓ Operates 6 ccTLD (.fr/.re/.pm/.tf/.yt/.wf)
- ✓ Back-End registry for 12 gTLD (.paris/.ovh/.bzh/...) and a ccTLD (.sn)
- ✓ More than 3.5 millions domain names
- ✓ DNSSEC was introduced 10 years ago
- ✓ About 12% of domain names have a DS published

COVID-19 implications

- ✓ This presentation was initially planned for the « original » 33 OARC meeting (Paris, May 2020)
- ✓ Very difficult to get delivered during lock-down
- ✓ Not authorized to intervene in Datacenters
- ✓ Impossible to have face to face Key Ceremonies
- ✓ ... so RSA to ECDSA rollover had to be delayed

DNSSEC at Afnic (before Algo rollover)

- ✓ Keys are stored in AEP Keyper HSMs
- ✓ OpenDNSSEC is used to manage keys
- ✓ Bind is used to sign zones
- ✓ Home-made scripts are used to control/synchronize/update/distribute/... zone keys
- ✓ Zones are dynamically updates (every 10 minutes)
- ✓ NSEC3 with salt changed several times/month
- ✓ Keys and salt are not shared amongst TLDs
- ✓ Afnic zones (nic.fr, afnic.fr, ...) use their own keys/salt too
- ✓ KSK rollover every 2 years (we use standby keys, so 2 DS are presents in root but only one KSK is published), ZSK rollover every 2 months

How we started... 10 years ago

- ✓ First release technical choices
 - ✓ OpenDNSSEC 1.0.0
 - ✓ Bind 9.7 « DNSSEC for humans »
 - ✓ 2048 bits KSK 1024 bits ZSK (with Standby Keys)
 - ✓ DNSKEY RRset signed with both keys
 - ✓ SHA-2 only for DS
 - ✓ NSEC3 with opt-out
 - ✓ RFC5910 implementation few months after zone signature

afnic

What happened in 10 years

- ✓ 19 TLDs to sign instead of 6
 - ✓ 20 HSM to operate
 - ✓ Hundreds of KSK rollover, thousands of ZSK rollover
 - ✓ Around 100 key ceremonies (it takes time...)
- ✓ From Bind 9.7 to Bind 9.11
- ✓ Full 2K keys in 2017 (.fr in 2019)
- ✓ DNSKEY RRset KSK only signed now
- ✓ Introduce new AEP KeyperPlus (2019)
- ✓ ECDSA testing

ECDSA, why now ?

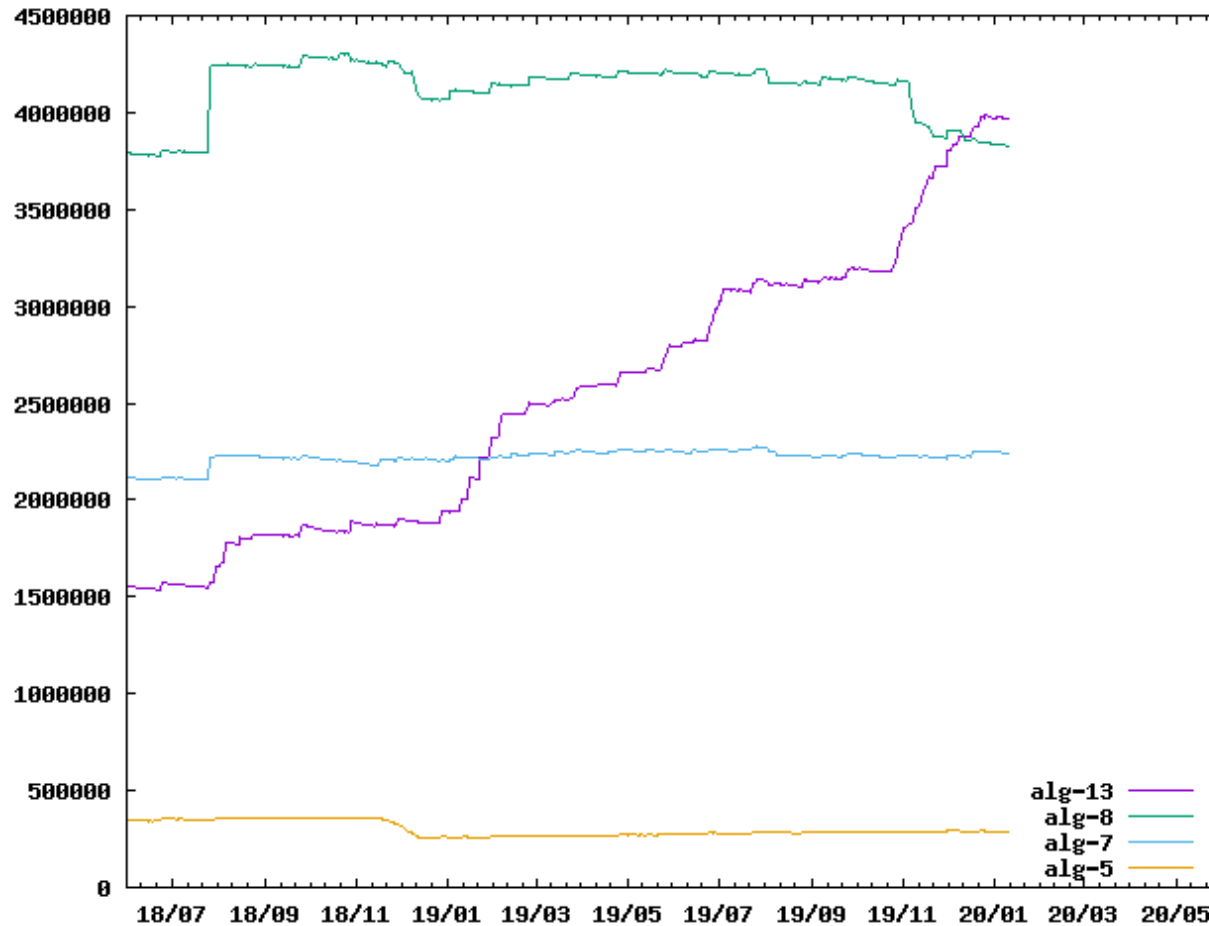
- ✓ 06/2019 => RFC8624 published
- ✓ 09/10/2020 => End of Life of ODS 1, we had to switch to ODS 2 (Algorithm Rollover supported).
- ✓ 31/12/2020 => End of support of AEP Keyper models we had. New ones have ECDSA.
- ✓ It's default choice for more and more registrars

AFNIC and RFC 8624 (.fr domains)

Number	Mnemonics	DNSSEC Signing	04/2020	10/2020	Comments
1	RSAMD5	MUST NOT	1	2	
3	DSA	MUST NOT	9	3	
5	RSA-SHA1	NOT RECOMMENDED	79	152	
6	DSA-NSEC-SHA1	MUST NOT	0	0	
7	RSASHA1-NSEC3-SHA1	NOT RECOMMENDED	338964	312663	81% => 70,5%
8	RSASHA256	MUST	47765	70265	11,4% => 15,8%
10	RSA-SHA512	NOT RECOMMENDED	85	138	
12	ECC-GOST	MUST NOT	5	12	
13	ECDSAP256SHA256	MUST	32290	59679	7,7% => 13,4%
14	ECDSAP384SHA384	MAY	56	74	
15	ED25519	RECOMMENDED	4	68	
16	ED448	MAY	0	0	

ECDSA adoption in the World

(provided by Viktor Dukhovni)



TLD in root and RFC 8624

Number	Mnemonics	DNSSEC Signing	04/2020	10/2020	Comments
1	RSAMD5	MUST NOT	0	0	
3	DSA	MUST NOT	0	0	
5	RSA-SHA1	NOT RECOMMENDED	30	30	
6	DSA-NSEC-SHA1	MUST NOT	0	0	
7	RSASHA1-NSEC3-SHA1	NOT RECOMMENDED	230	218	Migrations to RSASHA256
8	RSASHA256	MUST	1076	1042	AFNIC was Here !!!
10	RSA-SHA512	NOT RECOMMENDED	33	33	
12	ECC-GOST	MUST NOT	0	0	
13	ECDSAP256SHA256	MUST	14	35	AFNIC is here now !!!
14	ECDSAP384SHA384	MAY	0	0	
15	ED25519	RECOMMENDED	0	0	
16	ED448	MAY	0	0	
None			131	136	







ECDSA adoption in resolvers

- ✓ In the « past », many concerns but...
- ✓ <https://dnsthought.nlnetlabs.nl/> pages shows that algorithm 13 is as well supported as algorithm 8

ECDSA infrastructure







- ✓ Version upgrade of OpenDNSSEC
 - ✓ 1.4.14 => 2.1.x
- ✓ Replace all the HSMs
 - ✓ AEP Keyper => AEP KeyperPlus
- ✓ Change the way we use Bind, compile in a different way

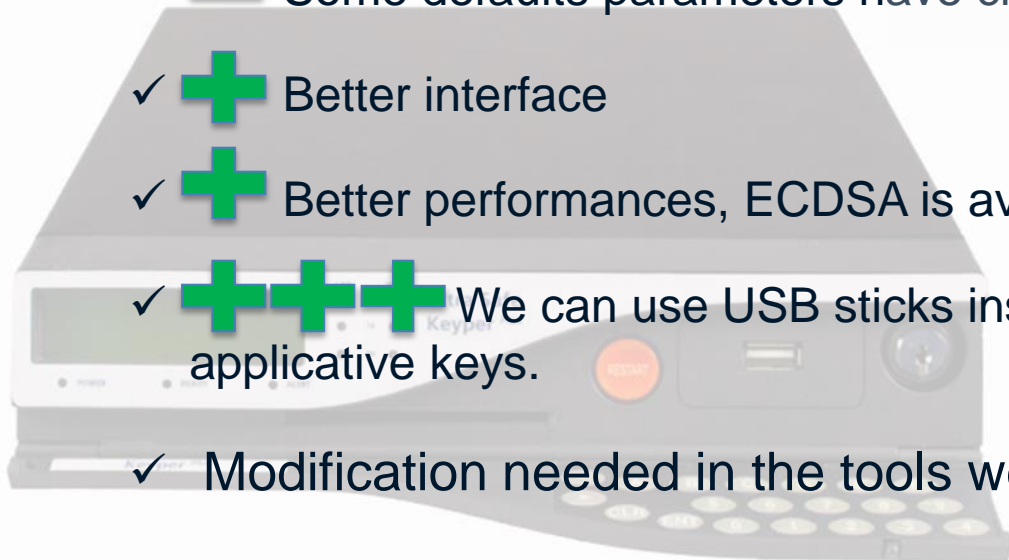
ECDSA Infrastructure details (1/3)

- ✓ Upgrade of OpenDNSSEC
 - ✓  « Standby Keys » concept (was experimental) is no longer supported
 - ✓  Database structure is really different
 - ✓  Keys life cycle is more complex
 - ✓  Commands output has changed
 - ✓  We had minor issues before version 2.1.6
 - ✓  « algorithm rollover » works fine
- ✓ We had to modify our code/scripts who process keys







Infrastructure ECDSA details (2/3)

✓ Replacement of HSM

- ✓  Not fully compatible if you have both Keyper and KeyperPlus
- ✓  Lower performances with last version of load-balancer (under investigations)
- ✓  Some defaults parameters have changed
- ✓  Better interface
- ✓  Better performances, ECDSA is available
- ✓  We can use USB sticks instead of smart cards to store applicative keys.
- ✓ Modification needed in the tools we developped



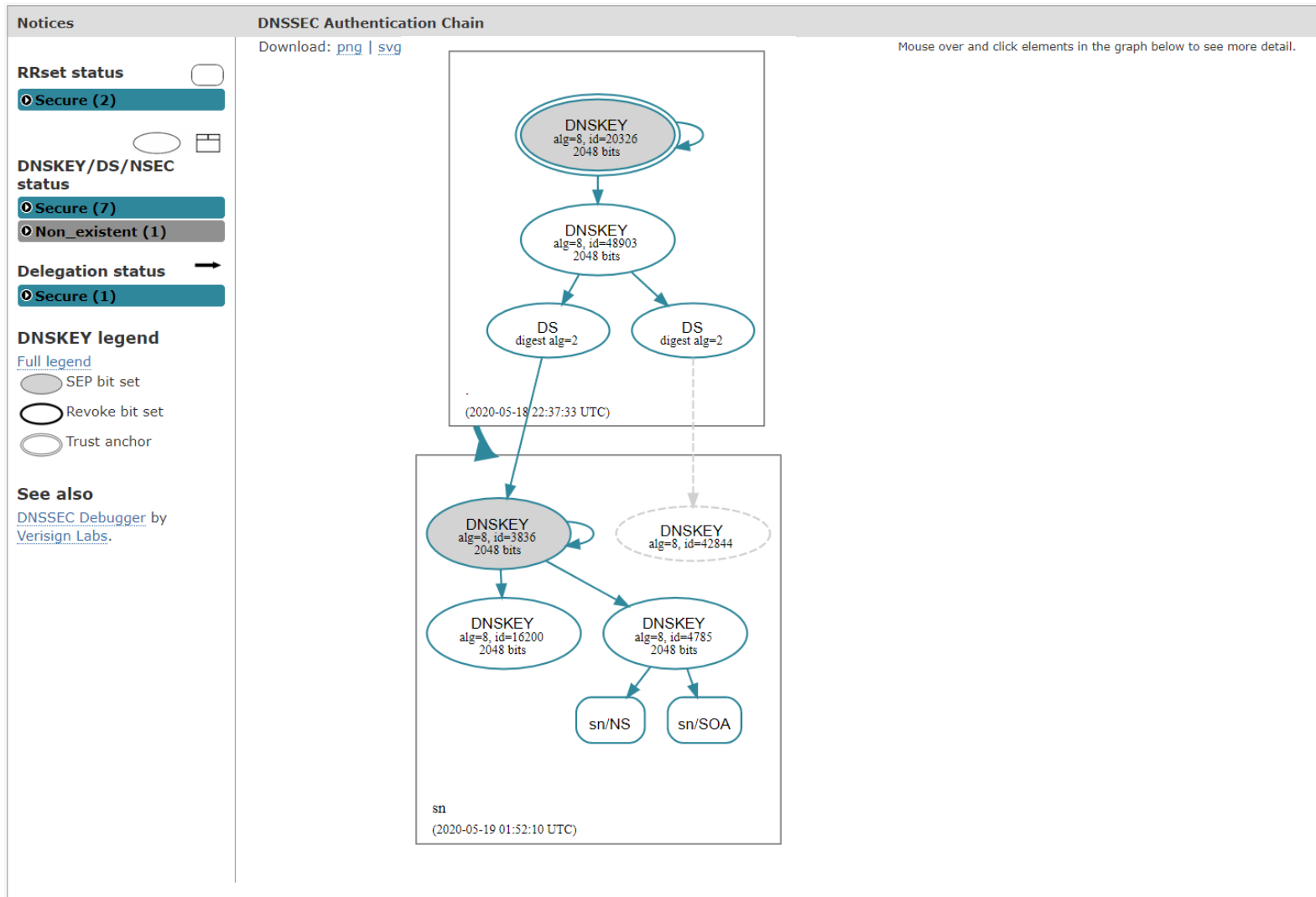
Infrastructure ECDSA details (3/3)

- ✓ Change the way we compile Bind (use of native mode)
 - ✓    Bad performances (Under investigation with ISC)
 - ✓  .key, .private files content have changed, transition might be tricky
 - ✓  dnssec-keyfromlabel parameters changed
 - ✓  Once migrated, it works as expected
- ✓ Modifications needed in compilation/deployment processes of Bind
- ✓ Modifications needed in the tools we developed
- ✓ We had to write some specific script to make the migration of keys in the new format (we have hundreds of keys)
- ✓ Workaround needed for .fr/.re

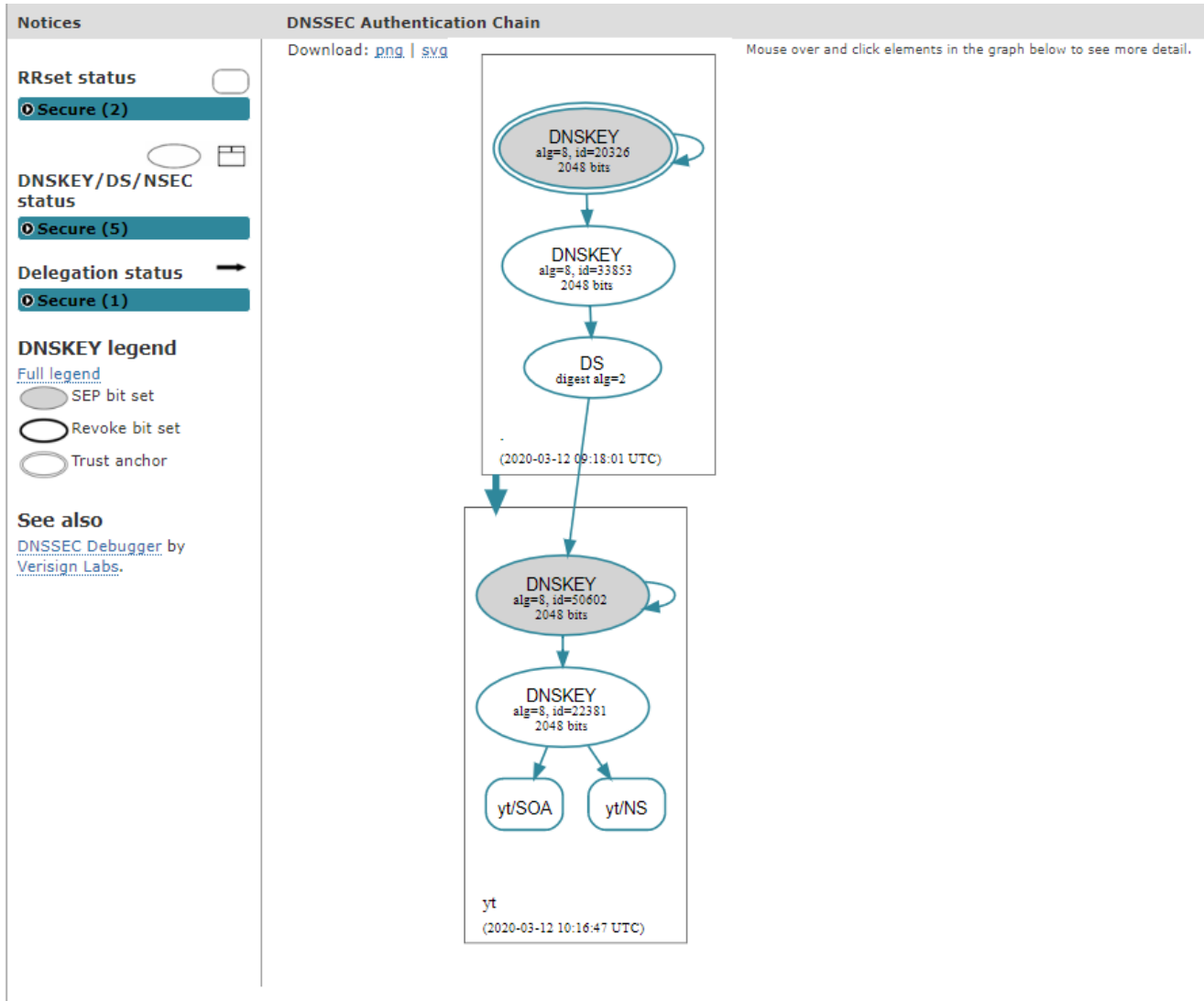
The algorithm rollover

- ✓ Once everything is ready we decided to start with our own domains (nic.fr, zonemaster.fr, ...)
- ✓ Then sandbox and pre-production infrastructures we operate
- ✓ Then small ccTLDs (.wf, .tf, .yt, ...) in production
- ✓ Then TLDs we operate as Back-End Registry

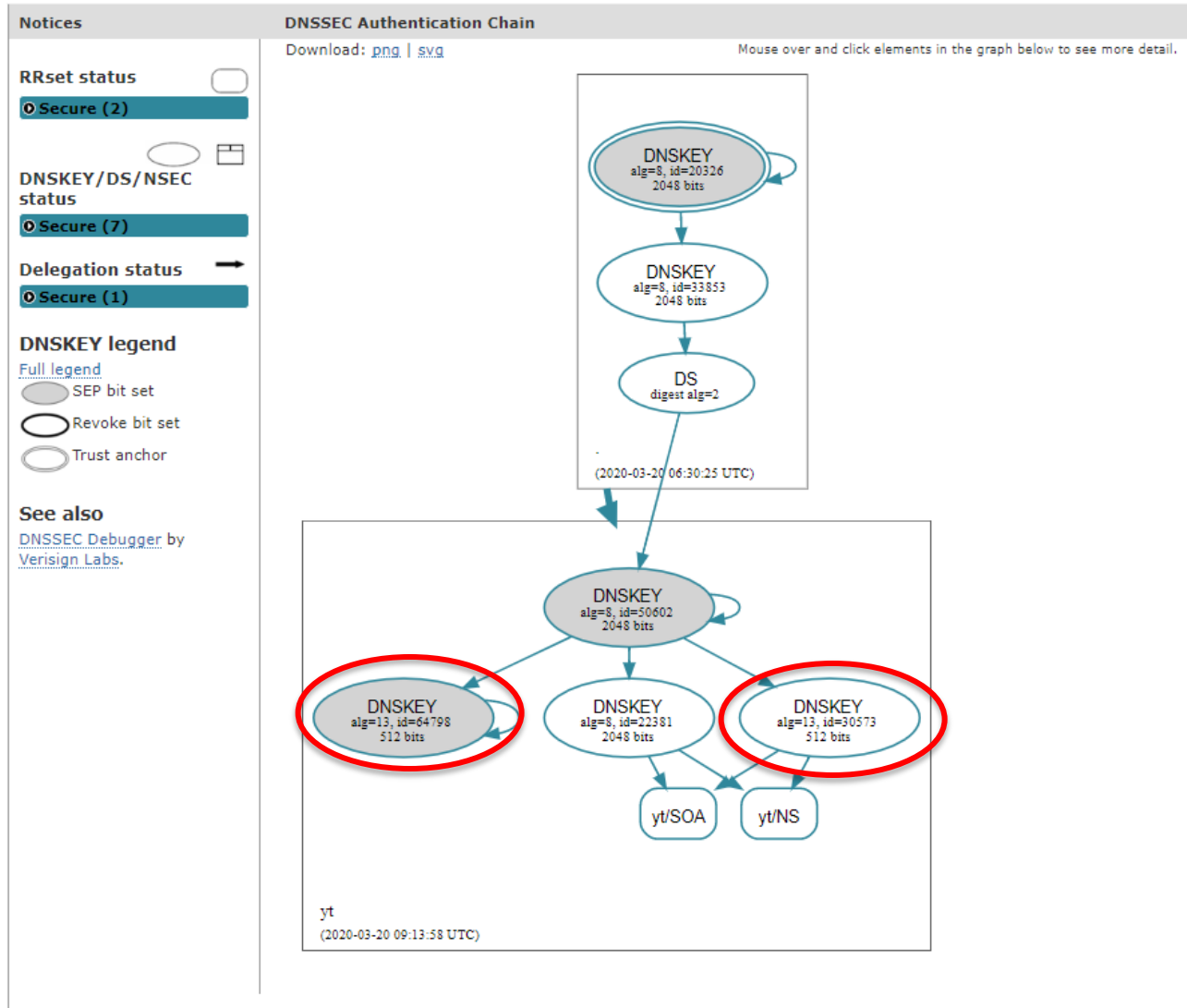
Algorithm Rollover details (1/6)



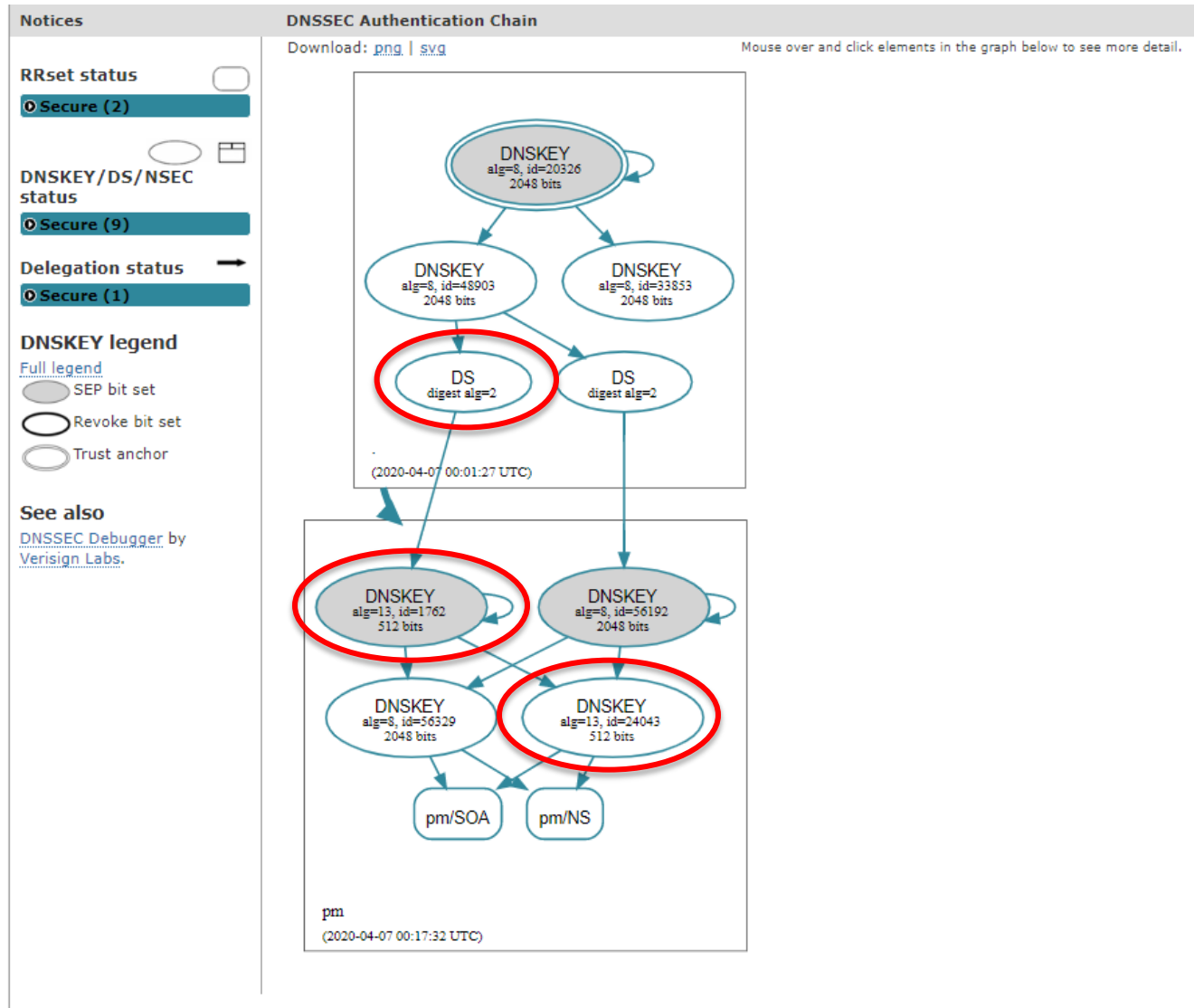
Algorithm Rollover details (2/6)



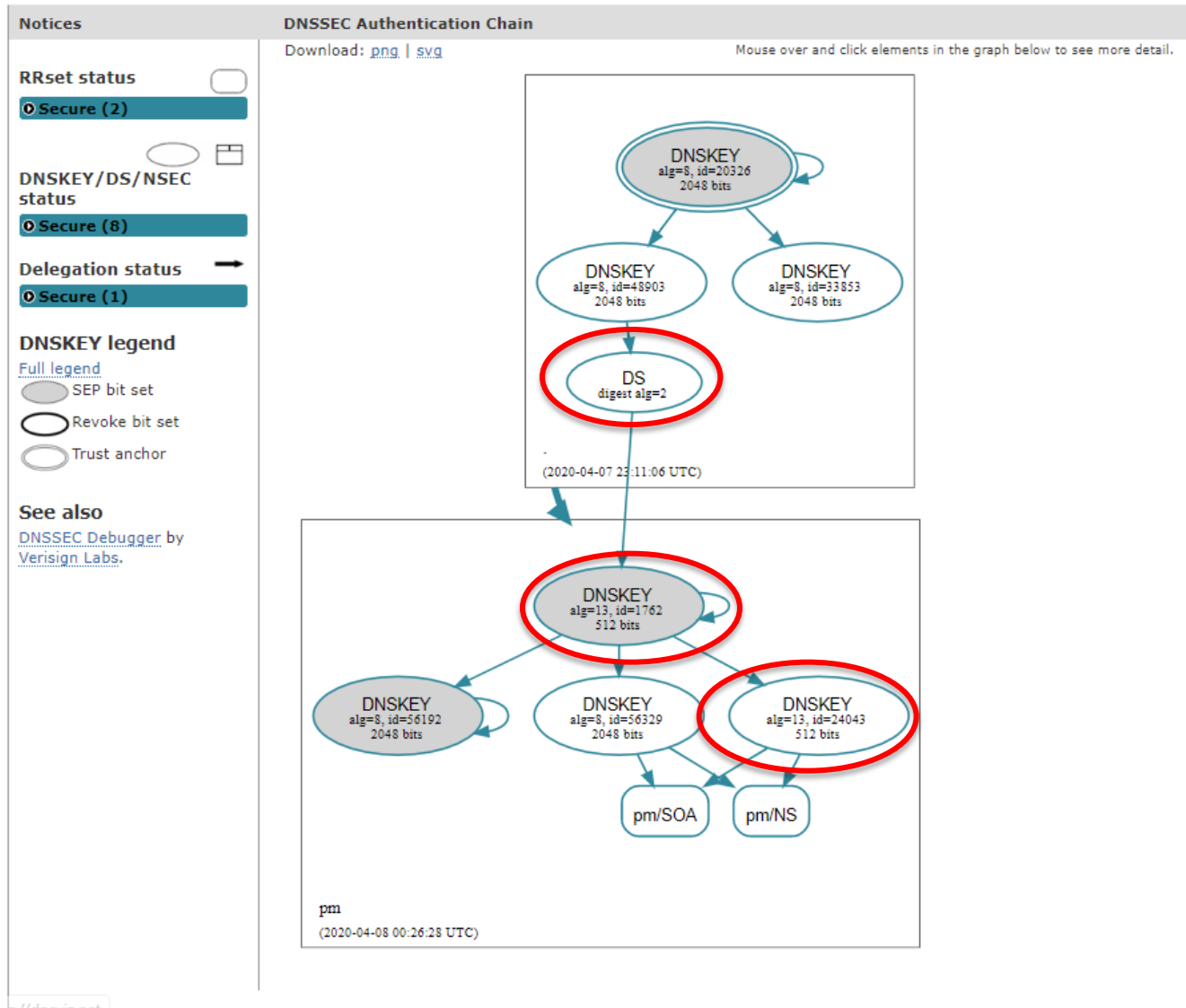
Algorithm Rollover details (3/6)



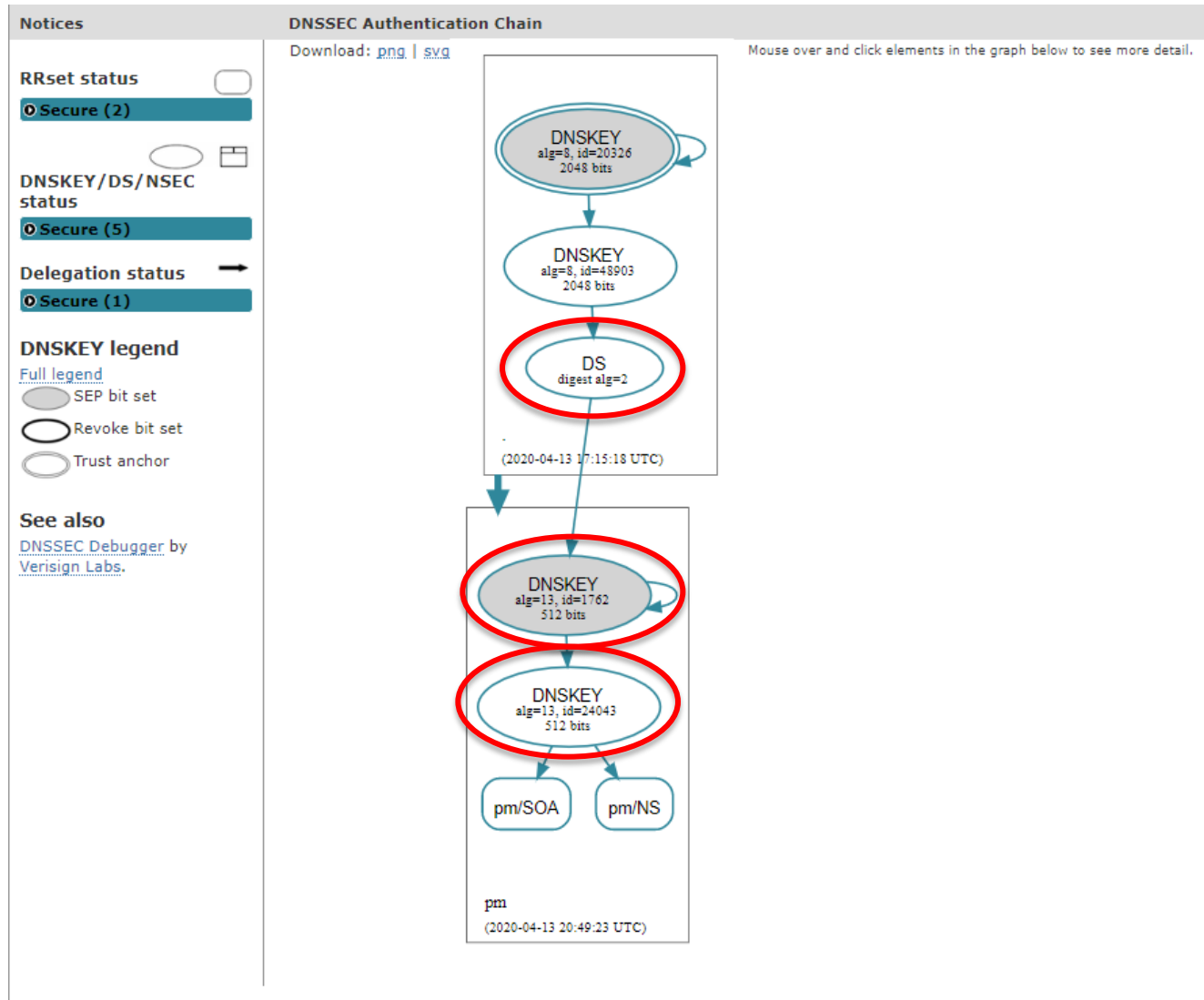
Algorithm Rollover details (4/6)



Algorithm Rollover details (5/6)



Algorithm Rollover details (6/6)



Size does matter (1/5)

- ✓ dig TLD dnskey +dnssec (with cookies)
 - ✓ RSA with Standbye Key : 1149 bytes
 - ✓ RSA without Standbye Key : 901 bytes
 - ✓ RSA+ECDSA signature : 1159 bytes
 - ✓ ECDSA signature : 317 bytes

Size does matter (2/5)

- ✓ Same query on all TLD in root
 - ✓ ECDSA signature: 289 bytes
 - ✓ Average : 1412 bytes
 - ✓ Median : 1337 bytes
 - ✓ Maximum : 3319 bytes ([.sl](#))

Size does matter (3/5)

✓ When we used only RSA (23/01/2020)

TLD	% NDD with DS	Unsigned zone	Signed with RSA	Evolution
.wf	15,9%	184Ko	400Ko	+121%
.tf	14%	300Ko	628Ko	+109%
.yt	15,8%	340Ko	764Ko	+125%
.pm	18,4%	576Ko	1400Ko	+143%
.re	15,6%	2,6Mo	5,7Mo	+119%
.fr	11,7%	320Mo	608Mo	+90%

Size does matter (4/5)

✓ During algorithm rollover

TLD	Signed with RSA	Signed with RSA+ECDSA	Évolution
.wf	400Ko	456Ko	+14%
.tf	628Ko	700Ko	+11,5%
.yt	764Ko	864Ko	+13%
.pm	1400Ko	1600Ko	+14%
.re	5,7Mo	6,5Mo	+12%
.fr	608Mo		

Size does matter (5/5)

✓ ECDSA only

TLD	Unsigned zone	Signed with ECDSA	Évolution
.wf	184Ko	292Ko	+59%
.tf	296Ko	456Ko	+54%
.yt	344Ko	548Ko	+59%
.pm	576Ko	972Ko	+68%
.re	2,6Mo	4,2Mo	+59%
.fr			

Conclusion

- ✓ The whole infrastructure has been updated and nothing broke
- ✓ 18 TLDs are now ECDSA signed
- ✓ TLD holders were happy with that change
 - ✓ .sn was the first african TLD to move to ECDSA

Next challenges

- ✓ Change Bind version from 9.11 to 9.16
- ✓ Do the algorithm rollover for the .fr when we will have better performances in signing process
 - ✓ Remove workarounds in our code

Thank you !



www.afnic.fr

Vincent.Levigneron@afnic.fr

