November 2018
Geoff Huston

Analyzing the KSK Roll

It's been more than two weeks since the roll of the Key Signing Key (KSK) of the root zone on October 11 2018, and it's time to look at the data to see what we can learn from the first roll of the root zone's KSK.

There are a number of reports that have been published, including one from the Root Canary work (http://bit.ly/2PttyHW). This report contains an informative time series plot looking at the Atlas Probes and their view of the KSK RRSIGs (Figure 1). It shows the 48-hour TTL in action, where old RRSIG value of the root zone DNSKEY RRset declines over the 48 hours following the roll, and the corresponding uptake of the new RRSIG value, signed by the incoming key. The SIDN labs report noted that "We did not detect any major issues with resolvers whatsoever."

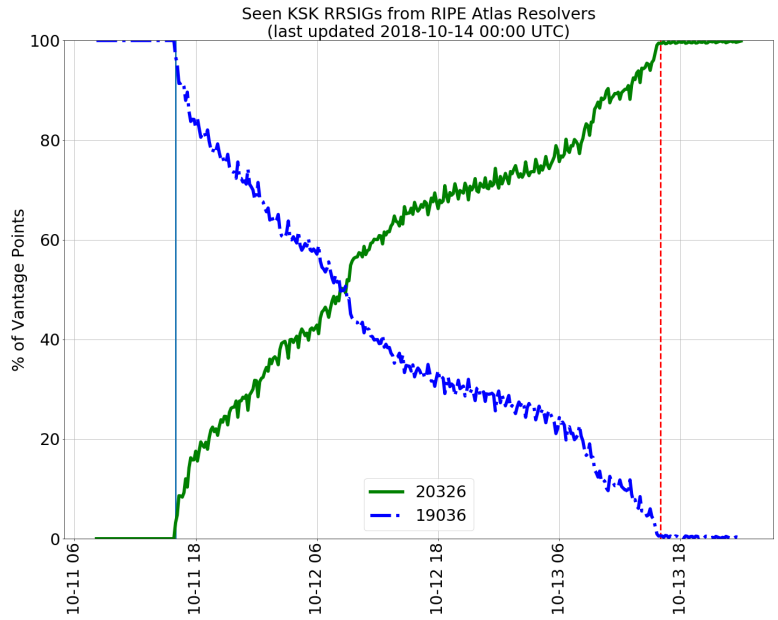


Figure 1 – KSK RRSIG values following the Root Zone KSK Roll (SIDN Labs, http://bit.ly/2PttyHW)

The KSK was originally scheduled to roll on October 11th, 2017. The procedure was halted because of the initial analysis of trust anchor data provided by the mechanism defined in RFC 8145. A plot of all of this RFC 8145 data spanning the period from 1 September 2017 until late October 2018 is shown in Figure 2. In September 2017 the small number of reporting resolvers indicated that some 6%-8% of visible resolvers were reporting that that they trusted the old KSK but not the new KSK. As the number of reporting resolvers increased over the ensuring 14 months the percentage of reporting resolvers that were indicating that they remained exclusively locked onto the old KSK rose to 20% of all reporting sources. This number only declined in May 2018. By the 9th October this number had declined to 5%, but oddly enough it rose by 2% on the 11th October at the time of the KSK roll. At the end of October this number is still at 4% of all sources still reporting that they do not trust the new KSK.

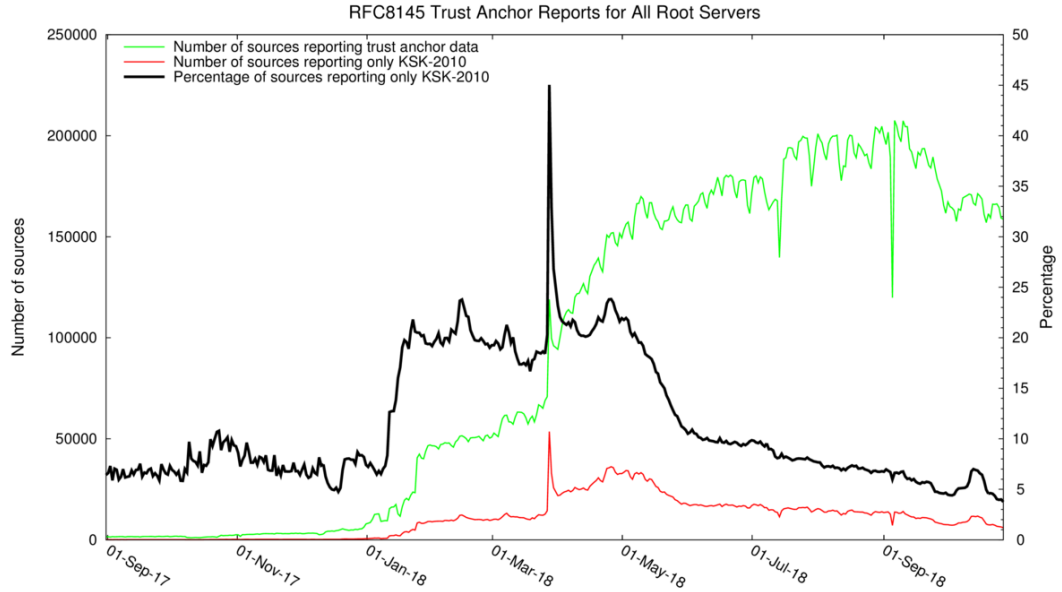


Figure 2 – RFC 8185 Trust Anchor Report data (ICANN, https://go.icann.org/2OV6iTN) (Retrieved 28th October)

So far, we have two data sets, based on Atlas probes and RFC 8145 reports and these two data sets point to very different outcomes for the KSK roll. The indirection of the relationship to reporting sources and measured impact to users points to some interpretation challenges with the RFC 8145 data when attempting to access user impact. The lack of third party reported outages tends to support the SIDN report of "no significant outage." As noted on the ICANN blog: "ICANN has heard of only two Internet Service Providers (*ISPs*) who experienced outages around the time of the rollover and who might have been negatively affected by the rollover, but we have not been able to investigate the root cause of their problems yet." But perhaps this claim deserves further investigation using additional data sources.

At APNIC Labs we were also performing a measurement of the DNS across the KSK roll. Here I'll look at our measurements and the results we have gathered. Obviously, we are interested in assessing whether our predictions matched what we observed during the roll.

APNIC Labs Measurement

The measurement technique we used was the use of end-user DNS queries embedded in online advertisement. We observed some 4M – 5M ad impressions per day (Table 1).

Date	Measurements
08/10/2018	5,091,293
09/10/2018	5,214,245
10/10/2018	5,322,040
11/10/2018	5,197,238
12/10/2018	5,163,504
13/10/2018	4,881,168
14/10/2018	4,726,317
15/10/2018	5,313,759
16/10/2018	5,256,944
17/10/2018	5,561,328
18/10/2018	5,981,700

Table 1 – Measurements per day

We used two measurement approaches. The first, a key sentinel measurement, was a detailed analysis of resolver behaviour using a recently defined resolver mechanism that is intended to reveal in the resolver's responses the trust status of a root zone key for the collective set of resolvers that each user is configured with, and the second was a count of the number of end users who are located behind DNSSEC-validating resolvers. The first

measurement is a predictive measurement to attempt to answer the question of what will happen, while the second can be used to estimate the extent of any impact of the KSK roll after the event to answer the question of what happened.

Measuring Resolver Trust State using Key Sentinel Queries

In this measurement exercise we use six individual DNS queries, all with a unique label component to circumvent DNS caching and to ensure that the DNS queries are answered by the experiment's authoritative DNS servers.

1) Unsigned DNS label
2) Validly signed DNS label
3) Invalidly-signed DNS label
4) Test KSK – not-KSK2010 (root-key-sentinel-not-ta-19036)
5) Test KSK – is-KSK2010 (root-key-sentinel-is-ta-19036)
6) Test KSK – is-KSK2017 (root-key-sentinel-is-ta-20326)

The APNIC Ad-based measurement system is a highly constrained environment. The script that is executed by the user cannot provide a direct way to measure what response the user received as a result of a DNS query. In this case we used the subsequent fetch of a small web object (a 1x1 pixel undisplayed image file) as an indication that the DNS resolution succeeded.

The first three queries are standard DNSSEC-validation capability queries, while the second group of three queries test the resolver trust status. This test uses a special; template for the left most label of a DNSSEC-signed DNS name to be resolved. If the resolver is unaware of the special processing for this left-most label, or if the resolver is not performing DNSSEC validation, or if the query type is neither A nor AAAA, then the query should be handled by the resolver like any other, without any special processing. Otherwise the resolver will process these queries as follows:

- For query 4, if a DNSSEC validating resolver is aware of the root-key-sentinel label processing specification then the resolver will return the validated response only if the key with the hash tag value of 19036 **is not** a locally trusted key for the root zone. This key tag value corresponds to KSK-2010, the old key. Otherwise the resolver will return SERVFAIL.

- For DNS query 5, if a DNSSEC validating resolver is aware of the root-key-sentinel label processing specification then the resolver will return the validated response only if the key with the hash tags value of 19036 **is** a locally trusted key for the root zone. Otherwise the resolver will return SERVFAIL.

- For DNS query 6, if a DNSSEC validating resolver is aware of the root-key-sentinel label processing specification then the resolver will return the validated response only if the key with the hash tags value of 20326 is a locally trusted key for the root zone. Otherwise the resolver will return SERVFAIL.

Details of this key sentinel are in the closing stages of publication as an RFC. The working documents can be found at: https://tools.ietf.org/html/draft-ietf-dnsop-kskroll-sentinel-17.

Categorising Observed Behaviours

Let's look at the anticipated results which looking at a number of user scenarios. We need to remember that many users use DNS configurations with more than one DNS resolver. A SERVFAIL response from a resolver, which occurs when a validating resolver fails to validate a signed DNS response, will cause the user to repeat the query to the next resolver in their local list, so the states below correspond to the state of the user's DNS resolution environment irrespective of the number of resolvers that each end-user system has included in its local configuration.

- **Not-Validating** - At least one of the user's resolvers does not perform DNSSEC validation

In this case we would expect the user to successfully resolve all 6 domain names.

- **Not-Recognised** - All of the user's resolvers perform DNSSEC validation, and at least one resolver does not recognise the key sentinel label

  In this case we would expect the user to successfully resolve URLs 1, 2, 4, 5 and 6. Only URL 3 should be unable to be resolved, as DNSSEC validating resolvers should not resolve this domain name.

- **Ready** - All of the user's resolvers perform DNSSEC validation, all recognise the key sentinel label, and at least one has loaded KSK-2017

  In this case we would expect the user to successfully resolve URLs 1, 2, 5 and 6. We would expect all validating resolvers to have KSK-2010 as a trusted key, so all resolvers should return SERVFAIL for URL 4, and as at least one resolver has loaded KSK-2017, then the user should be able to resolve URL 5.

- **Not-Ready** - All of the user's resolvers perform DNSSEC validation, all recognise the key sentinel label, and none have loaded KSK-2017

  In this case we would expect the user to successfully resolve URLs 1, 2, and 6.

We use web logs to show if the user has managed to resolve a DNS name, by inferring success when the corresponding web object is retrieved.

In almost all cases the script will be used in an environment of using HTTPS to retrieve the web object, and a successful retrieval requires that the web server presents a valid TLS certificate to the user script. As the key sentinel label is a fixed label in the left-most position in the DNS name and the unique name part is in the penultimate label, is not easy to manufacture a valid TLS certificate for the root key sentinel tests. Here we used the Server Name Indication field in the TLS handshake as an adequate confirmation that the user attempted to download the web object.

We can distinguish between Not-Validating and all other cases by ensuring that in all other cases the user's resolvers have been observed to query for the DNSKEY and DS RRsets that are consistent with DNSSEC validation for all five DNSSEC-signed DNS names.

Measurement Results

The results are shown in Table 2.

	Total	Not-Validating	Not-Recognised	Ready	Not-Ready
8/10/18	5,094,293	4,416,890	653,350	22,805	1,248
9/10/18	5,214,245	4,477,571	711,704	24,151	819
10/10/18	5,322,040	4,534,814	760,679	25,600	947
11/10/18	5,197,238	4,446,980	724,735	24,571	952
12/10/18	5,163,504	4,417,264	720,315	25,260	665
13/10/18	4,881,168	4,164,539	691,373	24,750	506
14/10/18	4,726,317	4,084,658	618,566	22,473	620
15/10/18	5,313,759	4,534,385	759,077	19,898	399
16/10/18	5,256,944	4,491,417	743,380	21,718	429
17/10/18	5,561,328	4,729,815	804,913	26,241	359
18/10/18	5,981,700	5,066,865	883,557	31,012	266

Table 2 – Key Sentinel Measurements per day

Let's split the results into three sections based on the KSK roll timing:

Before refers to the three-day period from the start of the 8th October to the end of the 10th October (all times are in UTC).

During refers to the five-day period from the start of the 11th October to the end of the 15th October. During this five-day period DNSSEC-validating resolvers were in the process of aging the root zone DNSKEY record from their local caches. Trust in the incoming root zone DNSKEY record relies on the resolver having trust in KSK-2017 once the cache entry expired and the resolver refreshed its cache by querying the root zone service system.

After refers to the three-day period from the start of the 16th October to the end of the 18th October.

The average measurements for each of these categories is shown in in Table 3.

	Not-Validating	Not-Recognised	Ready	Not-Ready
Before	85.917%	13.600%	0.464%	0.019%
During	85.625%	13.899%	0.463%	0.012%
After	85.048%	14.475%	0.470%	0.006%

Table 3 – Proportional Key Sentinel Measurements per day

What does the theory predict? After the KSK roll has completed no user should be reporting results that indicate they are in Not-Ready. Any user that sits behind a set of DNSSEC-validating resolvers that only trust KSK-2010 will have no DNS resolution service after the KSK roll and will be invisible to this particular measurement system. The residual levels of users reporting Not-Ready in the "After" section is part of the noise component of the experiment. This suggests that the level of uncertainty in measuring Cases C and D is ± 0.01%.

The next point to note is that there are relatively few resolvers that have implemented this key sentinel mechanism. Of the approximately 14% of users who sit behind DNSSEC-validating resolvers only a little over 3% of these users are using DNS resolvers that recognised the key sentinel mechanism at the time of the KSK roll. We are stretching the limits of experimental uncertainty here when the signal of the trusted key status is only visible to users at a rate of less than 5 per thousand across the entire Internet.

It is possible that a small number of resolvers may have stopped performing DNSSEC validation during the KSK roll. Comparing the Before and After numbers in Not-Validating then the number of users behind resolvers that do not all perform DNSSEC validation has risen by 0.9%. If this is indeed the case, then presumably this is due to a number of resolvers switching off DNSSEC validation during the KSK roll. The number of users behind resolvers who appeared to be ready for the KSK roll have increased very slightly, though it is hard to ascribe much significance to an improvement at a level of 0.006% when comparing the Before and After measurements in this form of experiment.

Of the users who are using resolvers that report their key status, the relative number of users who were reporting that they trusted KSK-2017 rose from 96% to 99%. A DNSSEC-validating resolver that only trusts KSK-2010 will be unable to answer any queries once its cached value of the old root zone DNSKEY record (signed by KSK-2010) has expired. This implies that the Not-Ready measurements in the After period are an artefact of experimental noise and does not provide any tangible evidence of recalcitrant resolvers. The After measurements point to the observation that at least 1.3% of those users who appear to sit behind key sentinel aware resolvers are receiving a noise signal in the key sentinel test.

The issue with these numbers is that they are limited to looking at users who sit behind DNS resolvers that were updated to include the key sentinel reporting mechanism. As this specification was only stabilised in mid-2018 we are looking at only a set of resolvers that are actively managed by sys admins who are happy to run with the most recent software updates. For many production environments this is not the case, and the software that is deployed in production environments is often deliberately positioned one or two releases behind the current release version in order to maximise stability of the production platform. The resolvers that may not be tracking the KSK roll are resolvers that are not managed so assiduously, and it is unlikely that these resolvers would be running the KSK sentinel mechanism.

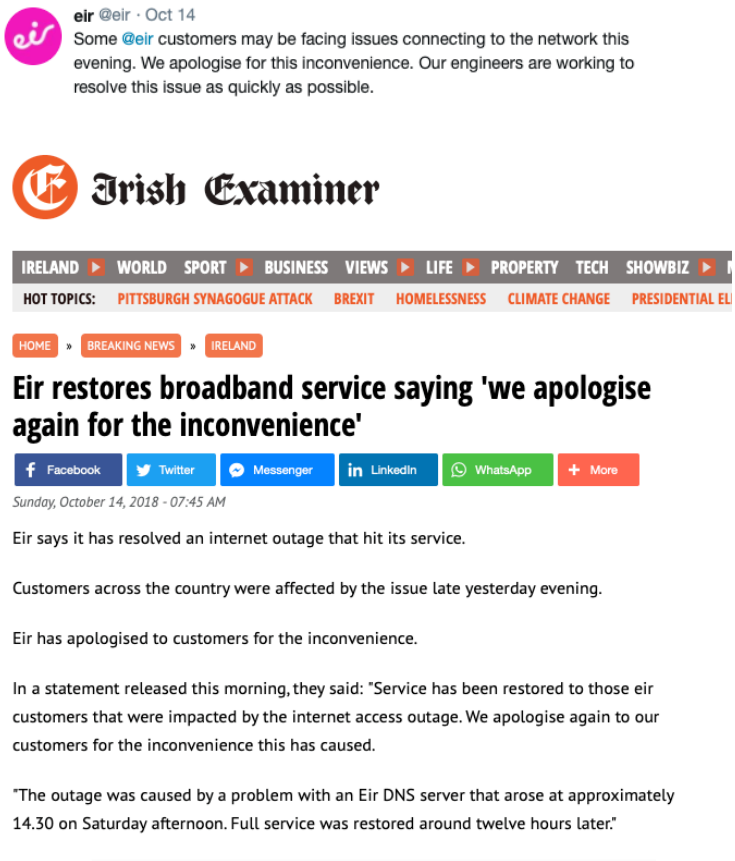
This is a predictive exercise and was useful to some extent in predicting an outcome of the KSK roll. However, due to its limited deployment, it is not very useful as a tool to assess the impact of the KSK roll. Let's look at the other measurement series, namely the measurement of DNSSEC validation capability, and see if this can shed any light on the KSK roll status.

Measuring DNSSEC Capability

Table 3 points to an interesting result that appears to be the opposite of expectations, namely that the number of users behind DNSSEC-validating resolvers appeared to increase by almost 1% when comparing the Before and After categories.

What's going on?

Perhaps we can start with one widely reported case of KSK-roll issues, which was reported from the Irish ISP EIR(http://bit.ly/2qdRAbY). While the exact nature of the outage was not reported at the time, the timing of the outage and the nature of the issue, namely a DNS problem, points to a KSK-related problem (Figure 3).



eir @eir · Oct 14
Some @eir customers may be facing issues connecting to the network this evening. We apologise for this inconvenience. Our engineers are working to resolve this issue as quickly as possible.

Irish Examiner

IRELAND WORLD SPORT BUSINESS VIEWS LIFE PROPERTY TECH SHOWBIZ
HOT TOPICS: PITTSBURGH SYNAGOGUE ATTACK BREXIT HOMELESSNESS CLIMATE CHANGE PRESIDENTIAL EL

HOME » BREAKING NEWS » IRELAND

Eir restores broadband service saying 'we apologise again for the inconvenience'

Facebook Twitter Messenger LinkedIn WhatsApp More

Sunday, October 14, 2018 - 07:45 AM

Eir says it has resolved an internet outage that hit its service.

Customers across the country were affected by the issue late yesterday evening.

Eir has apologised to customers for the inconvenience.

In a statement released this morning, they said: "Service has been restored to those eir customers that were impacted by the internet access outage. We apologise again to our customers for the inconvenience this has caused.

"The outage was caused by a problem with an Eir DNS server that arose at approximately 14.30 on Saturday afternoon. Full service was restored around twelve hours later."

Figure 3 – Reports of EIR DNS outage

The DNSSEC test data for the same period for EIR's AS, AS5466, is shown in Figure 4.

I should note that the scale in Figure 4 is different from the corresponding values in Table 4. Figure 4 shows the "raw" counts as seen by the analysis of ad presentations. The underlying Ad presentation network does not present these ads in a uniform manner across the entire Internet, and the ad placement program tends to over sample in some cases and under sample in others. We use the published figures of Internet users per country to perform a subsequent weighting of these ad presentation numbers in order to get closer to a weighted

number that is comparable across countries and across networks. This weighted value is used in Table 4.

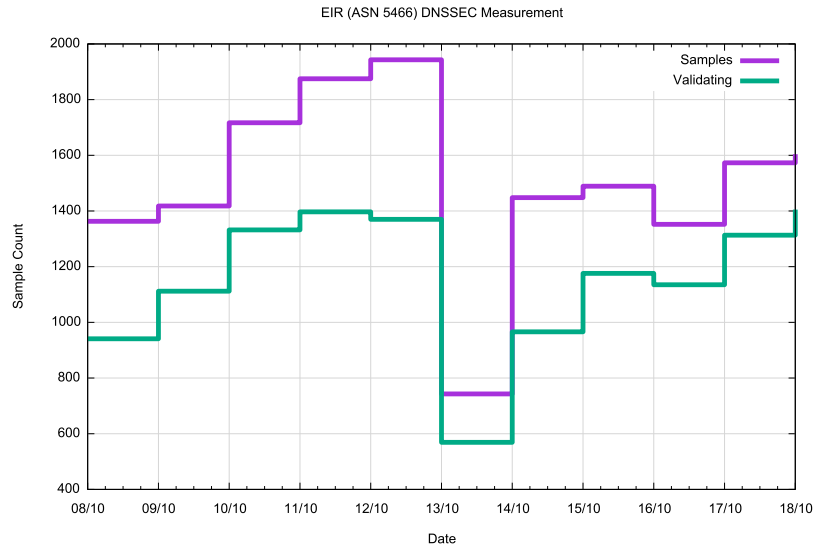


Figure 4 – EIR (ASN 5466) DNSSEC data

When a DNSSEC-validating resolver has the wrong trust anchor then it is unable to resolve any name, whether or not the name is DNSSEC-signed. This means that any users behind such a resolver effectively have no DNS service which implies that they have a very limited Internet service, including the ability to receive Ads. As shown in Figure 4, EIR received less than 50% of the normal ad volume on the 13th October. Were others affected as well? Figure 5 shows the total sample count for the period around the KSK roll.

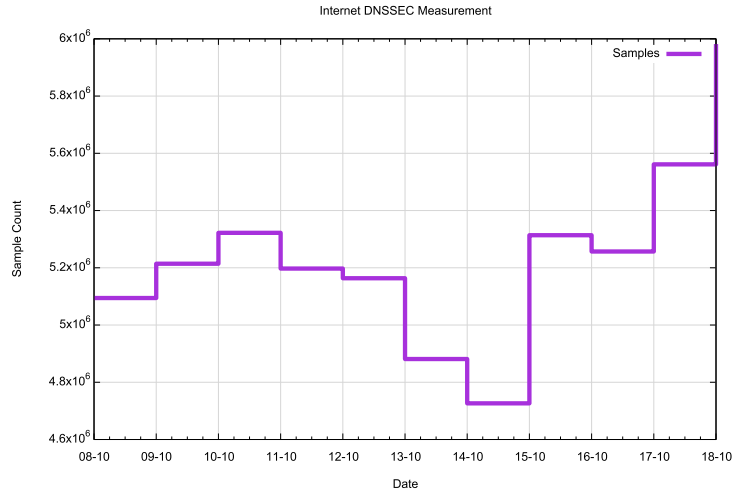


Figure 5 – Ad Sample Count data

There is a dip in the ad count in the period of the 13th October to the 14th October in this data, showing a 12% decline in ad presentations in this period. While it would be highly presumptive to attribute all of this 12% drop in ad presentations to the KSK roll, as the underlying ad presentation rate often varies by a similar amount from day to day, it may be the case that the KSK roll has had some impact here. How can we identify possible networks where this may have been the case?

If we take AS5466 as an example, then we can design a filter to look for impacted networks. In this case we will look for candidate networks which have an average weighted sample count of at least 400 samples per day in the three-day period 9 – 11 October, and where the count DNSSEC-validating users in that network is at least 30% of the sample count. In other words, in setting these values we are looking for networks that have a reasonable sample count so that the noise component can be contained, and a sufficiently high DNSSEC validation rate that implies that we are likely to be looking at networks where validation is provided by the ISP rather than by individual users redirecting their queries to some other DNS resolution service.

There are 233 such candidate networks (by unique AS number) that meet these criteria, out of a total of 42,732 that are seen within the overall ad placement framework over this period. These 197 networks cover some 9.8% of the total ad placement volume, so that filter covers a significant pool of the Internet's user population.

Networks that are classified as "impacted" by the KSK roll were seen as having a drop of DNSSEC-validating users on the 11th or 12th October. The criteria used here is a decline by a minimum of 33% of validating users when compared to the average of the three days immediately prior to the KSK roll. There are 35 networks that were seen to have experienced this drop, and these networks serve some 0.5% of the total seen user population. The total drop in seen users in the 12th and 13th October was some 46% from within this set of 35 networks, which corresponds to an impact level of some 0.24% of all users.

The list of these networks is shown in Table 4. It is noted that we have no direct way of confirming if the dip in visible users in these networks was due to DNS issues associated with the KSK roll or not, but it does provide a broader view of the possible scope of impact of the KSK roll.

Rank	AS	CC	Seen			Validating			AS Name
			Before	During	After	Before	During	After	
1	AS2018	ZA	1,858	1,122	1,473	694	220	288	TENET, South Africa
2	AS10396	PR	1,789	1,673	1,988	1,647	276	33	COQUI-NET - DATACOM CARIBE, Puerto Rico
3	AS45773	PK	1,553	388	1,393	606	178	540	HECPERN-AS-PK PERN, Pakistan
4	AS15169	IN	1,271	438	1,286	1,209	438	1,242	GOOGLE - Google LLC, India
5	AS22616	US	1,264	503	1,526	883	377	1,014	ZSCALER- SJC, US
6	AS53813	IN	1,213	689	1,862	1,063	582	1,419	ZSCALER, India
7	AS1916	BR	1,062	94	991	326	37	277	Rede Nacional de Ensino e Pesquisa, Brazil
8	AS9658	PH	931	281	842	440	136	404	ETPI-IDS-AS-AP Eastern Telecoms, Philippines
9	AS37406	SS	888	486	972	582	365	599	RCS, South Sudan
10	AS263327	BR	882	345	438	776	289	359	ONLINE SERVICOS DE TELECOMUNICACOES, Brazil
11	AS17557	PK	835	430	777	431	277	413	Pakistan Telecommunication, Pakistan
12	AS36914	KE	834	476	937	583	354	670	KENET , Kenya
13	AS327687	UG	802	473	834	390	189	332	RENU, Uganda
14	AS680	DE	773	966	1332	268	117	289	DFN Verein zur Foerderung, Germany
15	AS201767	UZ	761	538	729	461	200	371	UZMOBILE, Uzbekistan
16	AS37682	NG	695	401	728	593	274	568	TIZETI, Nigeria
17	AS7470	TH	674	214	507	219	94	182	True Internet, Thailand
18	AS51167	DE	670	378	479	214	78	156	CONTABO, Germany
19	AS15525	PT	600	260	593	287	125	284	MEO-EMPRESAS, Portugal
20	AS14061	GB	594	468	672	260	169	313	DigitalOcean, United Kingdom
21	AS37130	ZA	585	5	464	414	0	260	SITA, South Africa
22	AS30998	NG	583	264	484	192	54	143	NAL, Nigeria
23	AS135407	PK	569	227	457	419	207	344	TES-PL-AS-AP Trans World, Pakistan
24	AS16814	AR	565	235	456	258	120	208	NSS, Argentina
25	AS132335	IN	563	17	30	538	17	23	LeapSwitch Networks, India
26	AS5438	TN	559	532	579	526	171	27	ATI,Tunisia
27	AS5466	IE	547	240	401	419	184	329	EIRCOM, Ireland
28	AS18002	IN	538	467	614	277	176	242	WORLDPHONE-IN AS, India
29	AS37209	NG	532	109	438	269	45	194	HYPERIA, Nigeria
30	AS37100	ZA	454	161	401	168	95	131	SEACOM-AS, South Africa
31	AS5588	CZ	453	175	430	186	102	162	GTSCE GTS Central Europe, Czechia
32	AS1103	NL	446	38	363	189	7	132	SURFnet, The Netherlands
33	AS17563	PK	402	117	359	207	64	199	Nexlinx, Pakistan
34	AS327724	UG	401	120	538	208	103	266	NITA, Uganda
35	AS7590	PK	400	122	329	266	84	224	COMSATS, Pakistan

Table 4 – Proportional Key Sentinel Measurements per day

Of these 35 networks there are 3 networks that appear to have turned off DNSSEC validation during the KSK roll and had not turned validation back on by the 17th October. These are AS10396 Coqui-NET - Datacom Caribe in Puerto Rico, AS 5438, ATI in Tunisia and AS132335 Leapswitch in India.

Evaluating the KSK Roll

The KSK Rollover Design Team report (https://www.iana.org/reports/2016/root-ksk-rollover-design-20160307.pdf) recommended:

Recommendation 16: Rollback of any step in the key roll process should be initiated if the measurement program indicated that a minimum of 0.5% of the estimated Internet end-user population has been negatively impacted by the change 72 hours after each change has been deployed into the root zone.

From the data gathered by an extensive measurement program spanning the KSK roll period, it appears that some 35 networks experienced some form of failure that impacted networks. Of these networks 3 appear to have turned off DNSSEC validation to recover the service, with the other 26 appear to have taken measures to load the KSK-2017 trust anchor and restore service to their users.

The number of users impacted by the KSK roll, using the measurement approach described above, appears to be of the order of some 0.2% to 0.3% of the Internet's end-user population, which appears to be within the parameter specified by the KSK Roll Design Team.

Performing a KSK roll for the first time was always going to be a challenge. While it's always hoped that deployed software will faithfully comply to all the relevant standard specifications and DNSSEC-validating resolvers will be in a position to either follow the KSK roll signals as described in RFC5011 or are managed by system admins who are well prepared to make the local configuration changes in time for the KSK roll. The deferral of the original schedule in September 2017 was accompanied by an extensive campaign to spread the message about the KSK roll and alert DNS service operators of the forthcoming changes. The work, predominately carried out by the Office of the CTO within ICANN, needs special mention as without this considerable effort these numbers would probably have been much higher.

When should we roll the KSK again?

Before looking at this question let me stress that this process to roll the KSK is not over yet. The old KSK, KSK-2010 has been replaced, but not revoked. Any DNSSEC-validating resolver that has been configured to trust KSK-2010 will still be doing so today. To complete the process the key needs to be removed from all these resolvers' local trust anchor caches. Accordingly, KSK-2010 will re-appear in the root zone's DNSKEY resource record on the 11th January 2019, but will be used as a signing key for the record with the revocation bit set. This entry will remain in the root zone until 22nd March 2019. There is no "hold-down" period, so resolvers should remove this key from their local cache of trust anchors as soon as they see this revoked key state. The extended publication period is a precautionary measure, as most resolvers will perform this key removal in the 48-hour period starting on the 11th January.

The KSK roll is not straightforward and performing it infrequently will always have its elements of surprise and inadvertent errors. There is much to be said for performing this roll annually, if only to promote the use of automated DNS resolver tools that track the KSK state without the need for manual intervention. However, regularly rolling the KSK achieves little in and of itself. We now should look at further measures for the root zone KSK.

The first is the use of an elliptical curve crypto algorithm for the KSK to replace the RSA-based algorithm. This allows the use of smaller DNS responses which reduces the issues associated with larger packets and packet fragmentation.

The second is consideration of the provision of a backup key which could enable some form of KSK roll that does not require a lead time for 12 months or more to use in the root zone. The general model of some form of backup key envisages the introduction of a key into the root zone that is present for an extended period such that could be rolled in as the new KSK with a shorted lead time than is currently accommodated in the current key management processes. One view of the one year hiatus in the installation of KSK-2017 was that KSK-2017 was already in a trusted state by mid-August 2017, and was essentially playing the role of a backup key for the ensuring 14 months.

The third is a review of the DNS trust key state reporting tools. RFC 8145 is a potentially informative signal, but it has a number of majopr weaknesses in terms of its informative value. It needs to be fixed or killed off! The key sentinel effort also needs to be reviewed. The idea of a "special" label imposes a hefty load on every

resolver, and the measurement systems are very noise prone. Is there a way to device a sequence of DNS queries where the next query requires the client to have received the prior response? The CNAME concept is a possible candidate for such a measure, but more consideration is required at this stage.

The final measure in this list is consideration of the publication of a KSK chain. When a resolver is fired up with an old configuration its pre-configured KSK value will not match the current key. If the sequence of signed key changes were available, the resolver could find its configured KSK in the chain, then apply the forward rolls as described in the chain to bring itself into synchronisation with the current KSK value. This requires more rigorous analysis to ensure that it does not introduce any new vulnerabilities, but we need some mechanism to allow "old" systems to be brought into synchronisation with the current state without requiring a user to engage in a potentially complex key installation process.

There are probably more lessons to learn from this exercise, but perhaps that's for a later time.

The bottom line for the 2018 KSK roll is that thanks to extensive preparation the entire process was largely trouble-free.

The KSK has been rolled and the Internet has survived it largely unscathed!

Disclaimer

The above views do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.

Author

Geoff Huston B.Sc., M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region.

www.potaroo.net