

RPKI ROA updates

Anurag Bhatia,
Hurricane Electric (AS6939)



Introduction

Working at Global backbone operator & datacenter provider - Hurricane Electric and based in Haryana, India. Spend lot of time in looking at BGP routing tables, traceroutes across the ocean, interesting patterns & tooling around those patterns.

Besides routing I got lot of interest in DNS, root DNS servers, network automation & virtualization.

Also a dad since Sept 2021! ;-)



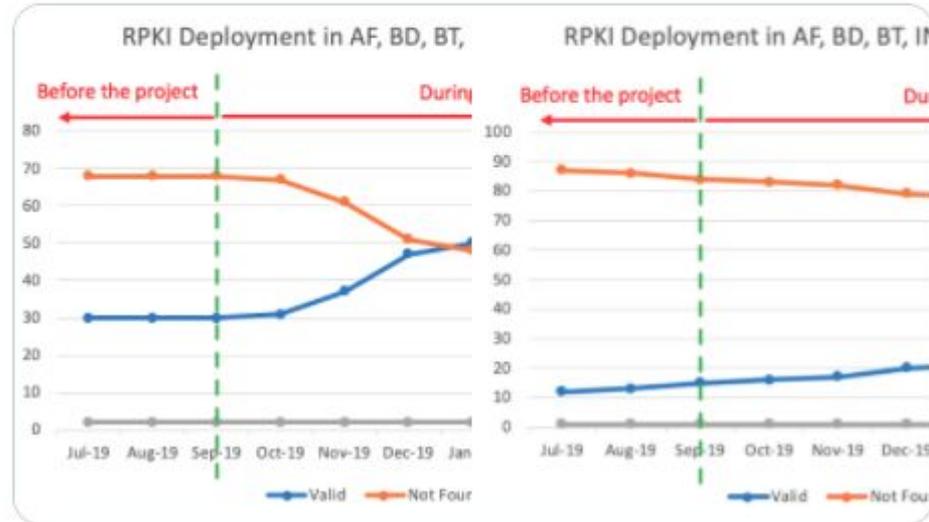
Starts with tweet from my friend Awal



Md Abdul Awal 🚲 @0xAwal · Jul 12, 2020

...

My routing security project with [@nsrcworld](#) & [@mozilla](#) started in Oct-19 to improve [#RPKI](#) deployment in South Asia+Myanmar. The two graphs show tremendous growth in RPKI and how [#INDIA](#) is lagging behind. [@anurag_bhatia](#) [@RoutingMANRS](#) [@routinator3000](#) [@Abuselp](#) [@routingtablepod](#)



Thoughts after looking at the tweet...

- Is Awal correct?
- How can I cross validate his claim?
- India has highest number of ASNs & IP prefixes in South Asia. Can that impact these results?
- If true and nothing done more of this will show up!



Thoughts after looking at the tweet...

- Is Awal correct? <- *Unfortunately he was correct*
- How can I cross validate his claim? <- *I actually did, more on this soon...*
- India has highest number of ASNs & IP prefixes in South Asia. Can that impact these results? <- *That can reflect in absolute numbers but not in relative percentage numbers*
- If true and nothing done more of this will show up! <- *No, and here I am to talk about it! :-)*



Validating the claim that India was lacking behind...



How to do RPKI validation of a country?

Find all prefixes originated by that country with origin ASNs and run them against a validator. Simple right?



Challenges with RPKI validation at country level

1. How do you map prefixes to a given country? What should be the starting point?
2. Running check sequentially against a RPKI validator is slow. When done for thousands of prefixes it's actually very slow.
3. How to store the output and track it over time?



~~Challenges~~ Solutions with RPKI validation at country level

1. How do you map prefixes to a given country? What should be the starting point? *<- Instead of prefixes, start with ASN from RIR delegation file. And do ASN -> Prefix mapping*
2. Running check sequentially against a RPKI validator is slow. When done for thousands of prefixes it's actually very slow. *<- Used rпки api binary from Louis Poinsignon (Cloudflare) - <https://github.com/lspgn/rпки-api>*
3. How to store the output and track it over time? *<- Store data in a MySQL database & analyse output using Grafana*



More details on RPKI validator lookup

- RIPE RIS is used for raw data to map ASNs to prefixes.
- Data is formatted in csv & queries in a GraphQL format to RPKI API.
- Can scan entire global routing table in 3-4mins! (*IN table takes a few seconds*)
- Lookup is triggered using Gitlab CI/CD pipeline. Gives cron like capability but with notification & more.
- Fair amount of code was re-used which I put internally @work to keep an eye on our own routing table as we were deploying RPKI validation across Hurricane Electric's AS6939 backbone.
- Everything is containerized with Docker



If it takes a few seconds on IN, why not scan
entire South Asia?



Presenting rpk.anuragbhatia.com !!!



Lookup container Dockerfile

```
Dockerfile 484 bytes
1 FROM ubuntu:20.04
2
3 # Install dependencies
4 RUN apt-get update
5
6
7 RUN apt-get install -y git \
8     curl \
9     jq \
10    mysql-client \
11    bc \
12    lynx \
13    whois \
14    grepcidr \
15    wget
16
17 COPY bgpscanner_1.0-1_20190320_amd64.deb /root
18 COPY libisocore1_1.0-1_20190320_amd64.deb /root
19 COPY rpki-api-v0.2.1-linux-x86_64 /root
20
21 RUN dpkg -i /root/*.deb
22
23
24 RUN git config --global user.email "me@anuragbhatia.com"
25 RUN git config --global user.name "Anurag Bhatia"
26
27
28 RUN rm -rf /root/.cache
29
```



Gitlab CI/CD pipeline

 .gitlab-ci.yml  47.04 KIB

```
1 stages:
2   - Docker build
3   - Raw Data
4   - BGP Table
5   - RPKI Lookup
6   - ASN to AS Name
7   - Raw table to MySQL
8   - Calculate Summary
9   - Inject Summary
10  - Specific AS Summary
11  - IN Invalid Summary
12
13 01_Build Docker Image:
14   # Use the official docker image.
15   image: docker:latest
16   stage: Docker build
17   services:
18     - docker:dind
19
20 variables:
21   DOCKER_HOST: tcp://docker:2375/
22   DOCKER_DRIVER: overlay2
23   DOCKER_TLS_CERTDIR: ""
24
25 before_script:
26   - docker login -u "$CI_REGISTRY_USER" -p "$CI_REGISTRY_PASSWORD" $CI_REGISTRY
27 script:
28   - docker build --pull -t "$CI_REGISTRY_IMAGE:main" ./Docker
29   - docker push "$CI_REGISTRY_IMAGE:main"
30 when: manual
```



Pipeline execution

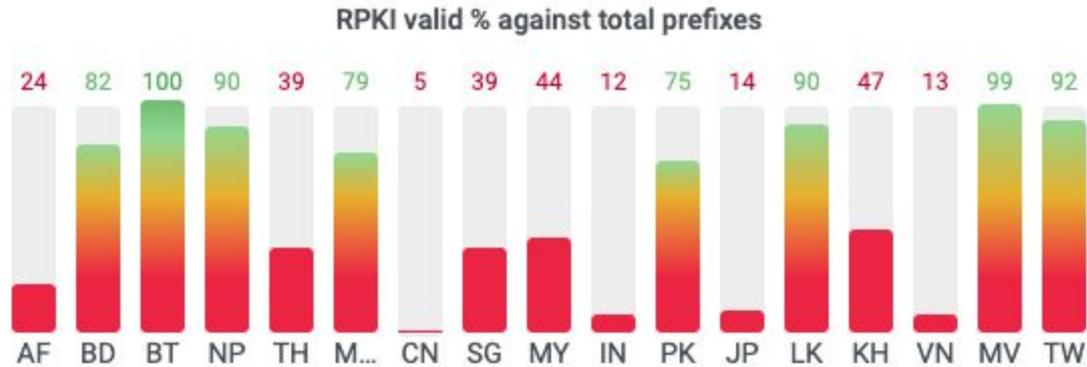
Status	Pipeline	Triggerer	Stages	
passed ⌚ 00:35:07 📅 14 hours ago	Updates #576605006 🐞 main -> 15af0240 📌 Scheduled latest		» ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	▶ ⌵ ⋮
passed ⌚ 00:45:33 📅 1 day ago	Updates #575547116 🐞 main -> 15af0240 📌 Scheduled latest		» ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	▶ ⌵ ⋮
failed ⌚ 00:43:45 📅 2 days ago	Updates #574535616 🐞 main -> 15af0240 📌 Scheduled latest		» ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✗ ✓ ✓ ✓	▶ ⌵ ↻ ⋮
passed ⌚ 00:45:11 📅 3 days ago	Updates #573527111 🐞 main -> 15af0240 📌 Scheduled latest		» ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	▶ ⌵ ⋮
passed ⌚ 00:44:01 📅 4 days ago	Updates #573154369 🐞 main -> 15af0240 📌 Scheduled latest		» ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	▶ ⌵ ⋮
passed ⌚ 00:42:06 📅 5 days ago	Updates #572820717 🐞 main -> 15af0240 📌 Scheduled latest		» ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	▶ ⌵ ⋮
passed ⌚ 00:41:55 📅 6 days ago	Updates #571884131 🐞 main -> 15af0240 📌 Scheduled latest		» ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	▶ ⌵ ⋮



Pipeline execution



Asian stats from July 2020

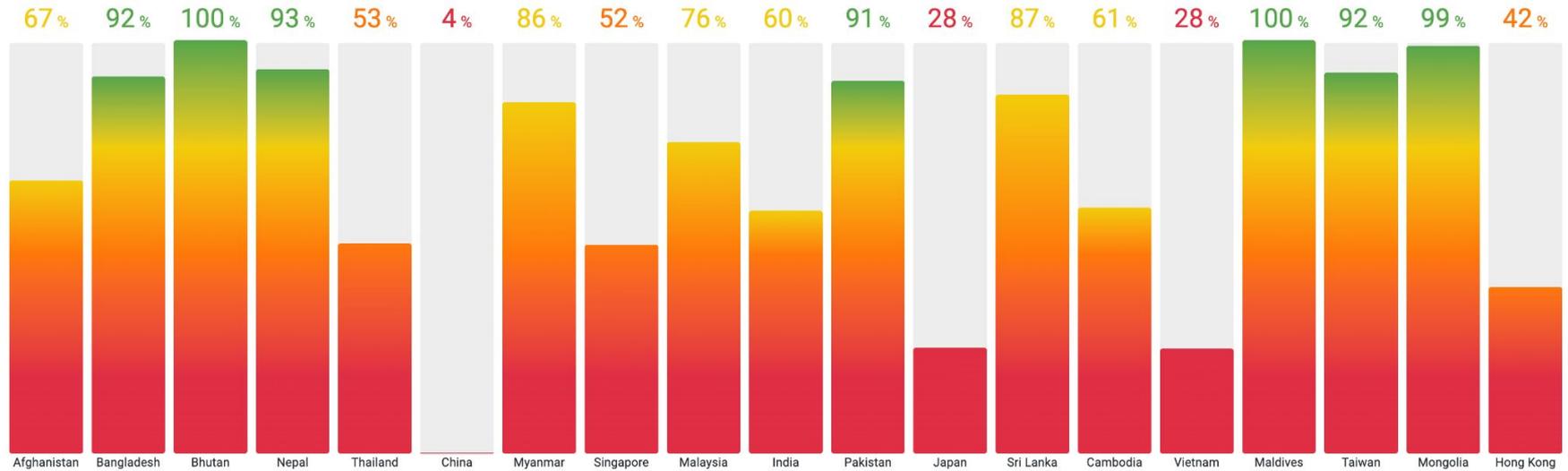


Warning: two years old data!

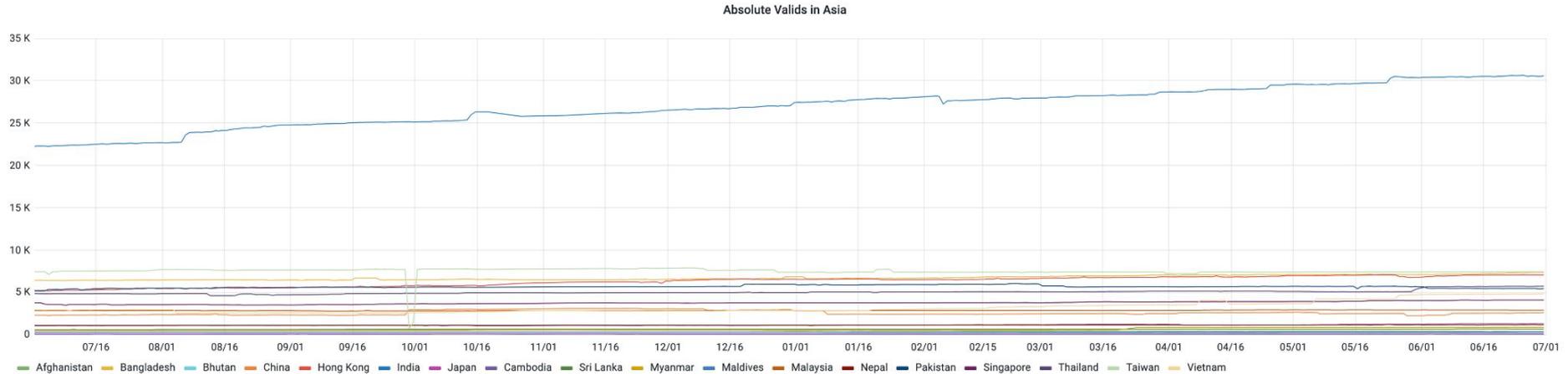


Asian stats now!

Summary Data - % of table signed by countries

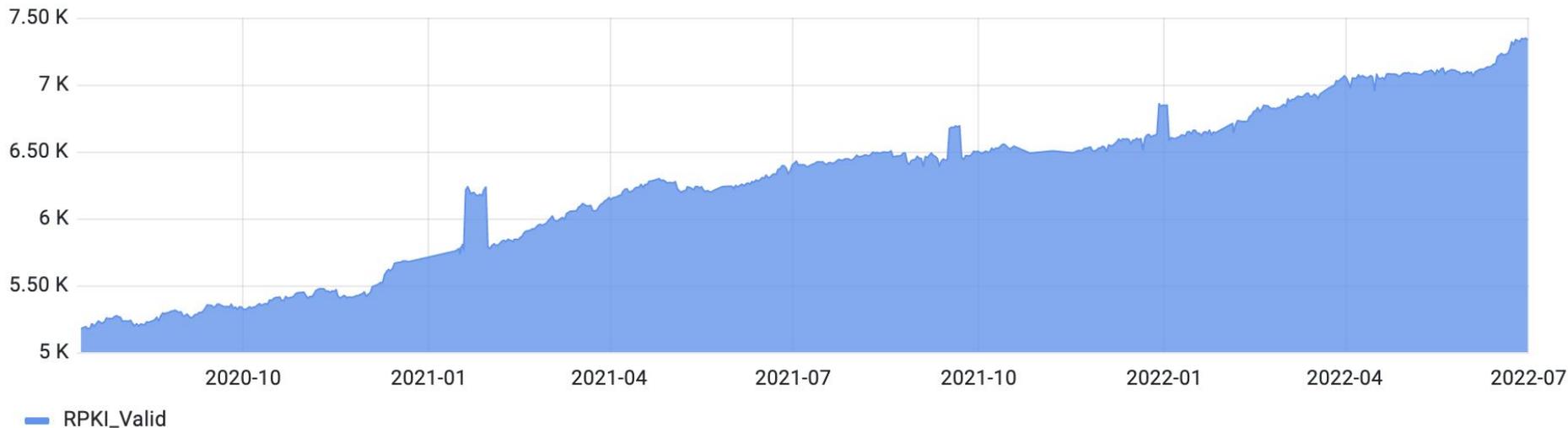


Growth of RPKI Valids in Asia

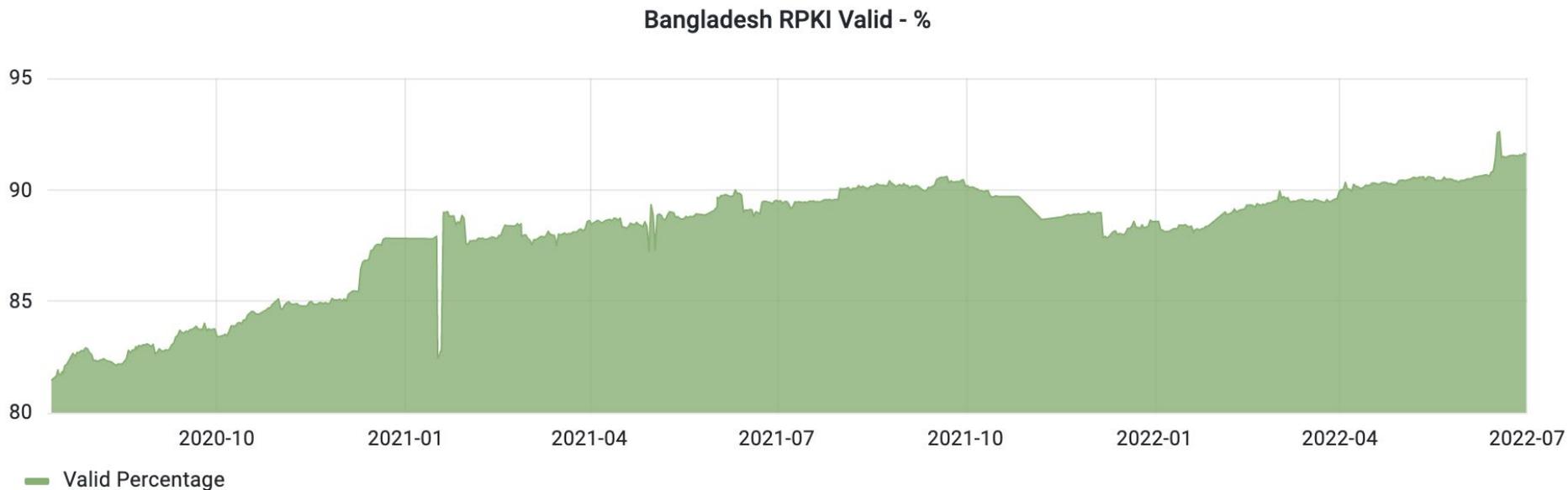


Bangladesh RPKI signed growth - absolute signed prefixes

Bangladesh RPKI Valid - Absolute

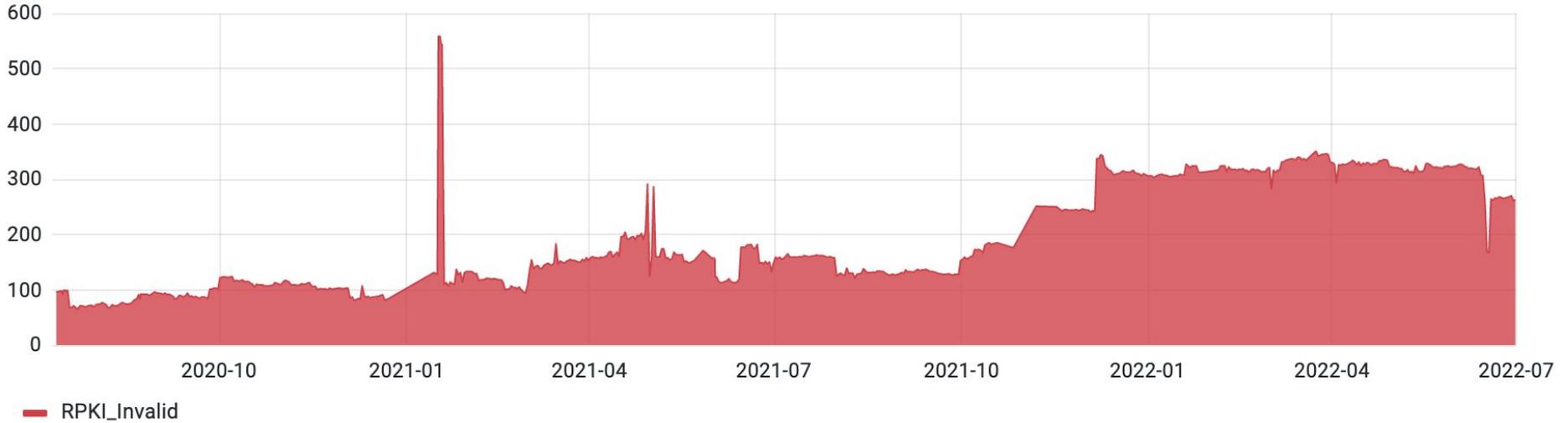


Bangladesh RPKI signed growth - % signed prefixes

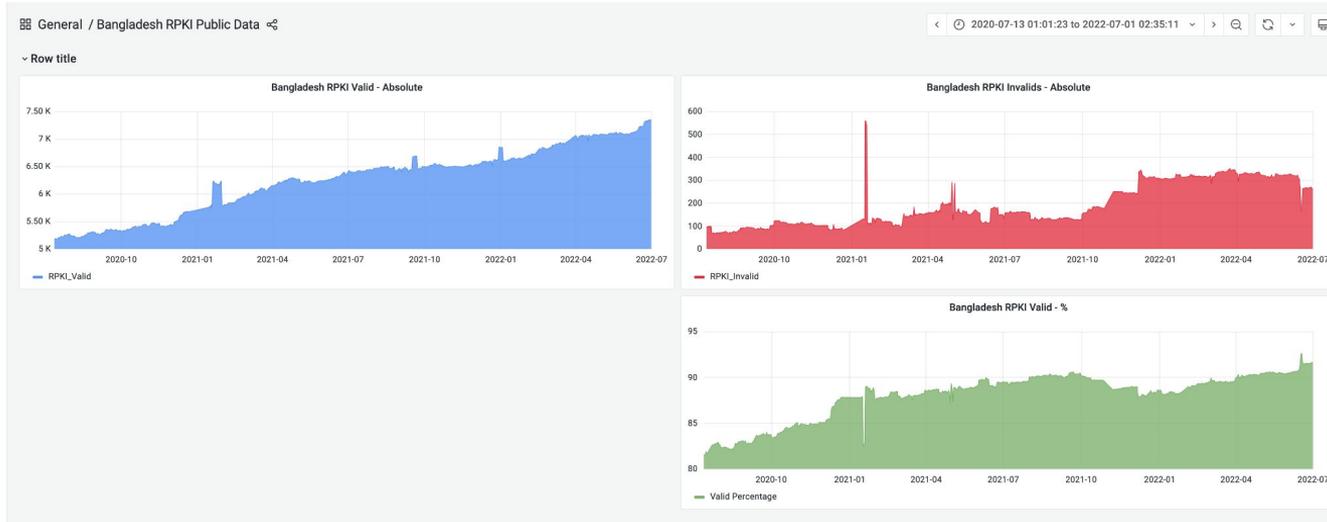


Indian RPKI invalids

Bangladesh RPKI Invalids - Absolute



Bangladesh RPKI ROA public data



Public data specific to Bangladesh - <https://bit.ly/3AcJ0zn>



Bangladesh RPKI Invalids...

BD RPKI ROA Stats : 30 June 2022

time	OriginAS	Prefix	RPKI_Status	OriginASName
2022-06-30 5:48:26	17494	103.110.215.0/24	Invalid	BTTB-AS-AP Telecom Operator & Internet Service Provider as well,
2022-06-30 5:48:26	138346	103.112.237.0/24	Invalid	SAJIDTRADINGLTD-AS-AP Sajid Trading Ltd., BD
2022-06-30 5:48:26	137554	103.113.14.0/23	Invalid	DREAMNET-AS-AP Dream.Net, BD
2022-06-30 5:48:26	134585	103.120.192.0/23	Invalid	SHEETALBROADBAND-AS-AP Sheetal Broadband, BD
2022-06-30 5:48:26	138575	103.133.140.0/24	Invalid	APPLE2-AS-AP APPLE NET, BD
2022-06-30 5:48:26	138638	103.135.91.0/24	Invalid	FENIEASYNET-AS-AP Feni Easy Net ISP, BD
2022-06-30 5:48:26	131464	103.138.155.0/24	Invalid	DJBL-AS-AP Digi Jadoo Broadband Ltd, BD
2022-06-30 5:48:26	138346	103.141.13.0/24	Invalid	SAJIDTRADINGLTD-AS-AP Sajid Trading Ltd., BD
2022-06-30 5:48:26	58715	103.155.118.0/24	Invalid	EARTHTELECOMMUNICATION-AS EARTH TELECOMMUNICATION Pvt LTD., BD
2022-06-30 5:48:26	132602	103.16.153.0/24	Invalid	BANGLADESH-AS-AP Bangladesh Submarine Cable Company Limited BSCC
2022-06-30 5:48:26	131464	103.160.158.0/24	Invalid	DJBL-AS-AP Digi Jadoo Broadband Ltd, BD
2022-06-30 5:48:26	133938	103.169.161.0/24	Invalid	XEON-BD Xeon, BD
2022-06-30 5:48:26	147295	103.174.135.0/24	Invalid	NEHNET-AS-AP N.B.H. NET, BD
2022-06-30 5:48:26	149514	103.189.242.0/24	Invalid	BAIPAIL1-AS-AP Baipail Network And Internet Service, BD
2022-06-30 5:48:26	135339	103.214.156.0/23	Invalid	FISSACOM-AS-AP Fuad Muhammad Shorfuiddin TA Fissa Communication,
2022-06-30 5:48:26	138024	103.79.219.0/24	Invalid	NETPLUSONLINE-AS-AP NETPLUS ONLINE, BD
2022-06-30 5:48:26	136134	103.81.70.0/23	Invalid	INDEPENDENT-AS-AP Independent Univeristy, Bangladesh, BD
2022-06-30 5:48:26	138197	103.89.244.0/24	Invalid	WINKNETWORK-AS-AP WINK NETWORK, BD
2022-06-30 5:48:26	23688	103.9.104.0/23	Invalid	LINK3-TECH-AS-BD-AP Link3 Technologies Ltd., BD
2022-06-30 5:48:26	23688	103.9.104.0/23	Invalid	LINK3-TECH-AS-BD-AP Link3 Technologies Ltd., BD
2022-06-30 5:48:26	23688	103.9.105.0/24	Invalid	LINK3-TECH-AS-BD-AP Link3 Technologies Ltd., BD
2022-06-30 5:48:26	17806	114.130.223.0/24	Invalid	MANGOTELESERVICE-AS-BD Tire-1 IP Transit Provider of Bangladesh,
2022-06-30 5:48:26	132608	114.130.95.0/24	Invalid	MTSL-ISP-AP Mango Teleservices Limited ISP, BD
2022-06-30 5:48:26	24323	116.206.45.0/24	Invalid	AAMRA-NETWORKS-AS-AP aamra networks limited, BD
2022-06-30 5:48:26	59316	116.206.60.0/24	Invalid	AOL-BD aamra Outsourcing Ltd., BD
2022-06-30 5:48:26	59316	116.206.61.0/24	Invalid	AOL-BD aamra Outsourcing Ltd., BD
2022-06-30 5:48:26	58656	118.179.22.0/23	Invalid	BDHUB-BD bdHUB Limited, BD
2022-06-30 5:48:26	23923	119.148.21.0/24	Invalid	AGNI-AS Agni Systems Limited, BD
2022-06-30 5:48:26	23923	119.148.22.0/24	Invalid	AGNI-AS Agni Systems Limited, BD
2022-06-30 5:48:26	133034	121.46.68.0/22	Invalid	VACL-AS-AP Virtual American Companies BD Limited, BD
2022-06-30 5:48:26	135339	144.48.112.0/23	Invalid	FISSACOM-AS-AP Fuad Muhammad Shorfuiddin TA Fissa Communication,
2022-06-30 5:48:26	58601	150.107.55.0/24	Invalid	AAMRA-ATL-BD Aamra technologies limited, BD
2022-06-30 5:48:26	18022	160.202.130.0/24	Invalid	SMART-AS-AP All Sumon ta SMART NET, BD
2022-06-30 5:48:26	141731	2001:df6:180:ffff::/64	Invalid	MAXHUBLTD-AS-AP Max Hub Limited, BD
2022-06-30 5:48:26	141731	2001:df6:180:ffff::/64	Invalid	MAXHUBLTD-AS-AP Max Hub Limited, BD
2022-06-30 5:48:26	134204	2400:4d40:1004::/48	Invalid	BUSINESSNETWORK-AS-AP Business Network, BD
2022-06-30 5:48:26	134204	2400:4d40:1005::/48	Invalid	BUSINESSNETWORK-AS-AP Business Network, BD



Full list here - <https://bit.ly/3uebAMS>



Anurag Bhatia - Hurricane Electric - RPKI ROA Updates - BDN0G 14 - Cox Bazar, Bangladesh

Some more details about Grafana

- Used it as frontend for this data. Essentially supports showing data in any form like graphs, table, time data etc.
- Supports different set of data sources including InfluxDB, MySQL, and lot more.
- Open source and free to use in self hosted format. Besides RPKI tool, also used it on RIPE Atlas data export.
- Supports authentication to give restricted access as well as making data available out in public without any authentication.



Questions/Feedback/Suggestions?

Anurag Bhatia
anurag@he.net
he.net

