Packet Clearing House

DNSSEC Multi signer for PG

2025-10

DNS OARC, Stockholm, Sweden

Tamás Csillag
DNS Services Engineer

Who am I?

Started in operations on an R&E network at a university

Then at one of the big-five global banks

DNS and operations engineering at NIC.HU, the Hungarian ccTLD

DNS services engineer at PCH since 2022

DNSSEC is my main job which is never-ending learning

A Short History of PCH

Originated as an outcome of the 1992 “National Information Infrastructure” transition of Internet governance from the US government to the global private sector.

Responsible for providing operational security and stability for critical Internet infrastructure globally, much like a “fire department” for the Internet.

PCH works primarily in four areas: the core of the DNS, IXPs, regulatory & policy, and cybersecurity coordination.

Packet Clearing House

A Short History of PCH

Operating production anycast since 1994, precursor organizations since 1989

Advocating for the anycasting of the root nameservers since 1996

Began providing ccTLD nameservice in 1997

Started anycasting root nameservers in 2000

Began providing services over IPv6 in 2001

Anycasted the second DNSSEC-signed ccTLD in 2006

Started providing FIPS 140-2 L4 DNSSEC key management in 2011

Deployed first DNSSEC-validating, GDPR-compliant, recursive resolver in 2016

Packet Clearing House

PCH's Other DNS Services

We currently provide infrastructure for 2 root server administrators:

- D-root (University of Maryland)
- E-root (NASA)
- Infrastructure or assistance for most root server letters over the last thirty years

Global anycast for hundreds of TLDs, by far the largest provider of auth DNS services

- Broadest server footprint, racks of self-owned servers in 287 IXPs in 125 countries
- Only DNS service network large enough to not depend on transit: more than 8,000 peers

Registry services provider

Established and continue to host the Quad9 recursive resolver

- 99.21% effective malware/phishing/stalkerware blocking by independent lab test
- First global recursive resolver to apply DNSSEC validation
- Only global recursive resolver to be GDPR-compliant
- Exempted from law enforcement and intelligence data-collection requirements
- Globally bound by Swiss criminal privacy law

Packet Clearing House

Server clusters deployed at IXPs
327 locations

Motivations for multi signer

Before this development TLD operators we work with had two options:

1. Do DNSS signing on their own
2. Ask PCH to do DNSSEC signing for them

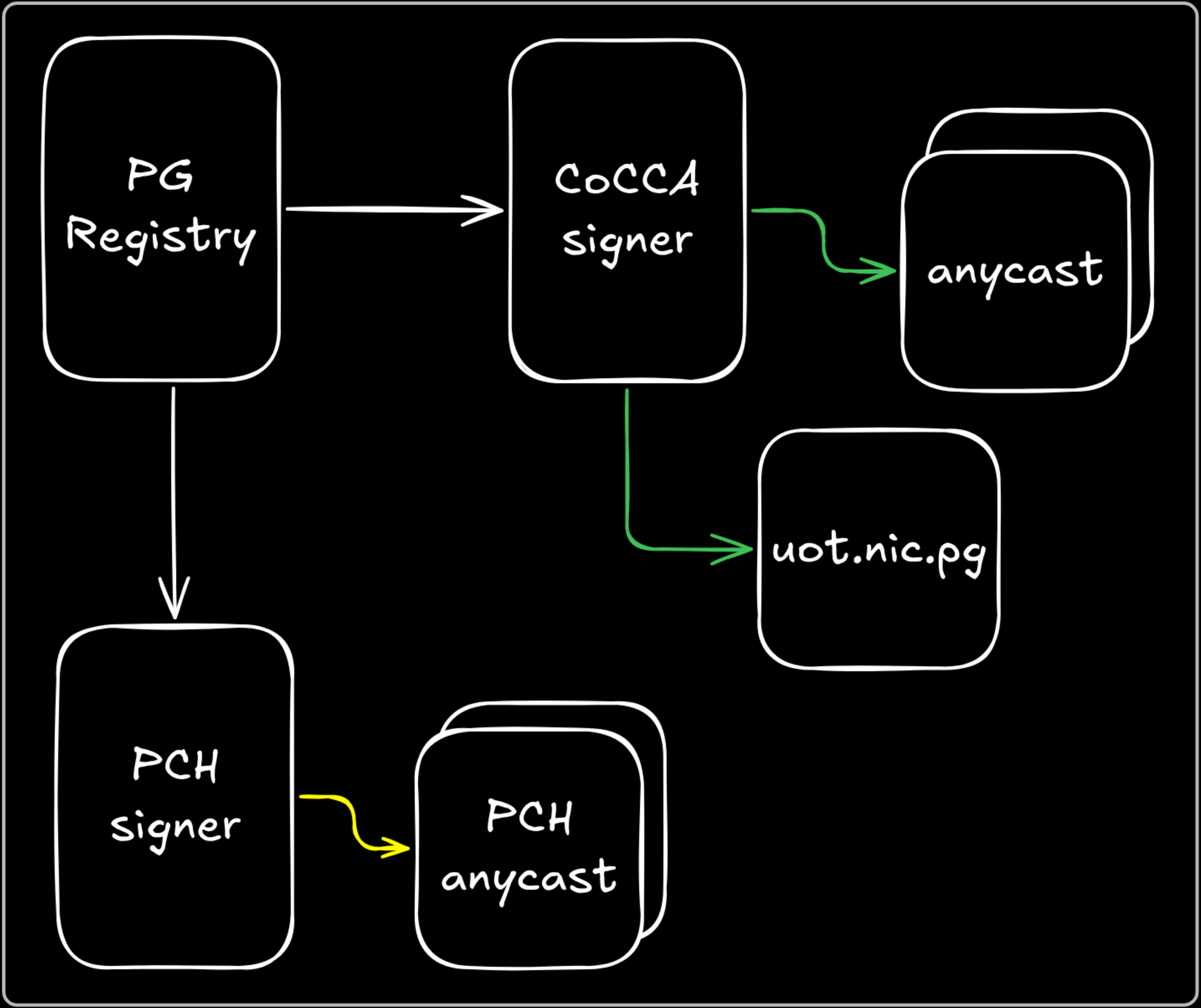
This used to be an either/or, but now there is a third option:

3. Sign themselves and have PCH to sign the zone independently.

This redundancy could help to protect against operational errors.

Packet Clearing House

Multi signer for PG



RFC 8901

For the purposes of this talk DNSKEY records are in focus.

Signer keys need to be published in the DNSKEY rrset to be accepted by validating resolvers.

Multi signer with: common KSK, unique ZSK per provider.

The method explained here is different to the usual route which involves syncing between parties and many moving parts. Involving DDNS at times.

Packet Clearing House

DNSSEC

Each column represents a point-in-time.

2 or 3 keys are in use at a time.

You always have the KSK and the current ZSK.

The previous/next ZSK during rollovers only.

T1	T2	T3
KSK	KSK	KSK
ZSK1	ZSK1	
	ZSK2	ZSK2

Multi signer with common KSK, unique ZSK per provider

In the case of 2 signers, it is a bit more complicated.

Provider1: ZSKa*

Provider2: ZSKb*

The DNSKEY rrset now have at least 3 keys and if properly aligned only 4 at most.

T1	T2	T3	T4	T5
KSK	KSK	KSK	KSK	KSK
ZSKa1	ZSKa1			
	ZSKa2	ZSKa2	ZSKa2	ZSKa2
ZSKb1	ZSKb1	ZSKb1	ZSKb1	
			ZSKb2	ZSKb2

Setup with knot dns

DNSKEY rrset is signed by the KSK, everything else is signed by a ZSK.

offline-ksk feature allows operations without the KSK available for signing.

The KSK is used to sign the DNSKEY rrset in advance for months or years. This can be done during a key ceremony (KC) or someone running a few commands at a terminal.

The root zone and some TLDs use pregenerated DNSKEY rrset + RRSIGs. (One of the PCH signers use this strategy.)

Packet Clearing House

Setup with knot dns (2)

In manual mode:
knot has a schedule for KSK/ZSK use in KASP.

In offline-ksk mode (which needs manual mode on) also in KASP:
it has timing for which DNSKEY rrset + RRSIG to use at a given time.

The original goal it to keep the KSK secure (e.g.: air gapped).

<u>This manipulates the signer's DNSKEY rrset in the process</u>.

This is exactly what we need to get the right keys published.

Let me show you how...

Packet Clearing House

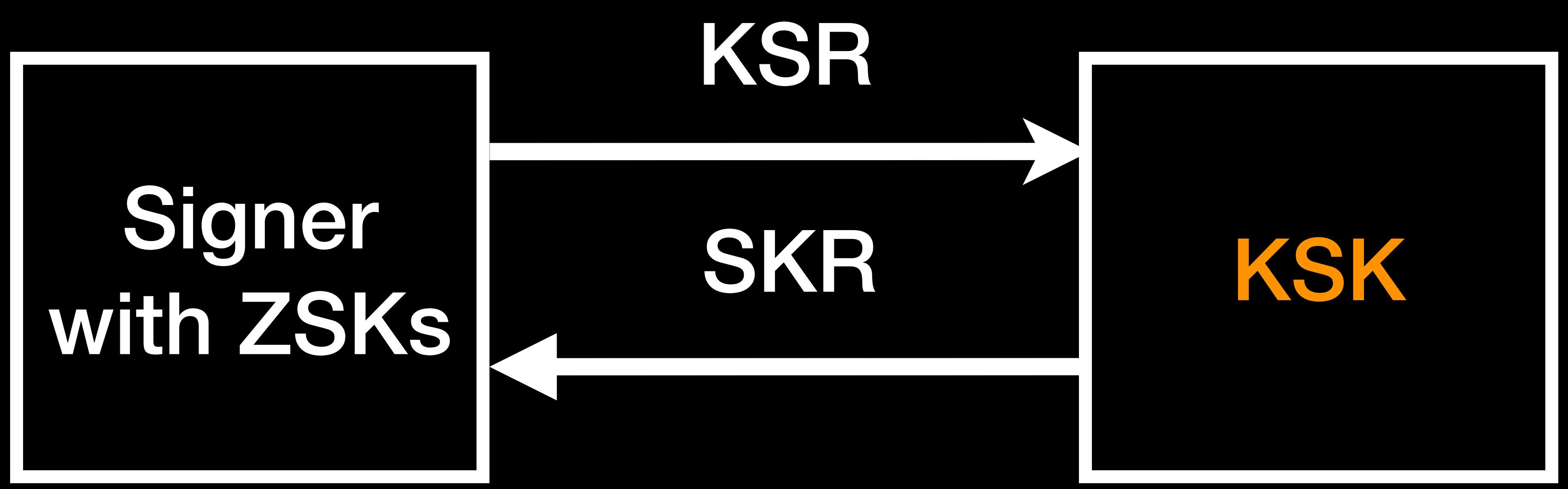
Setup with knot dns (2)

keymgr $z pregenerate
to generate ZSKs
using your timing from config

keymgr $z generate-ksr
generate key-signing-request

keymgr $z sign-ksr
the KSK signs the request

keymgr $z import-skr
import signed key request



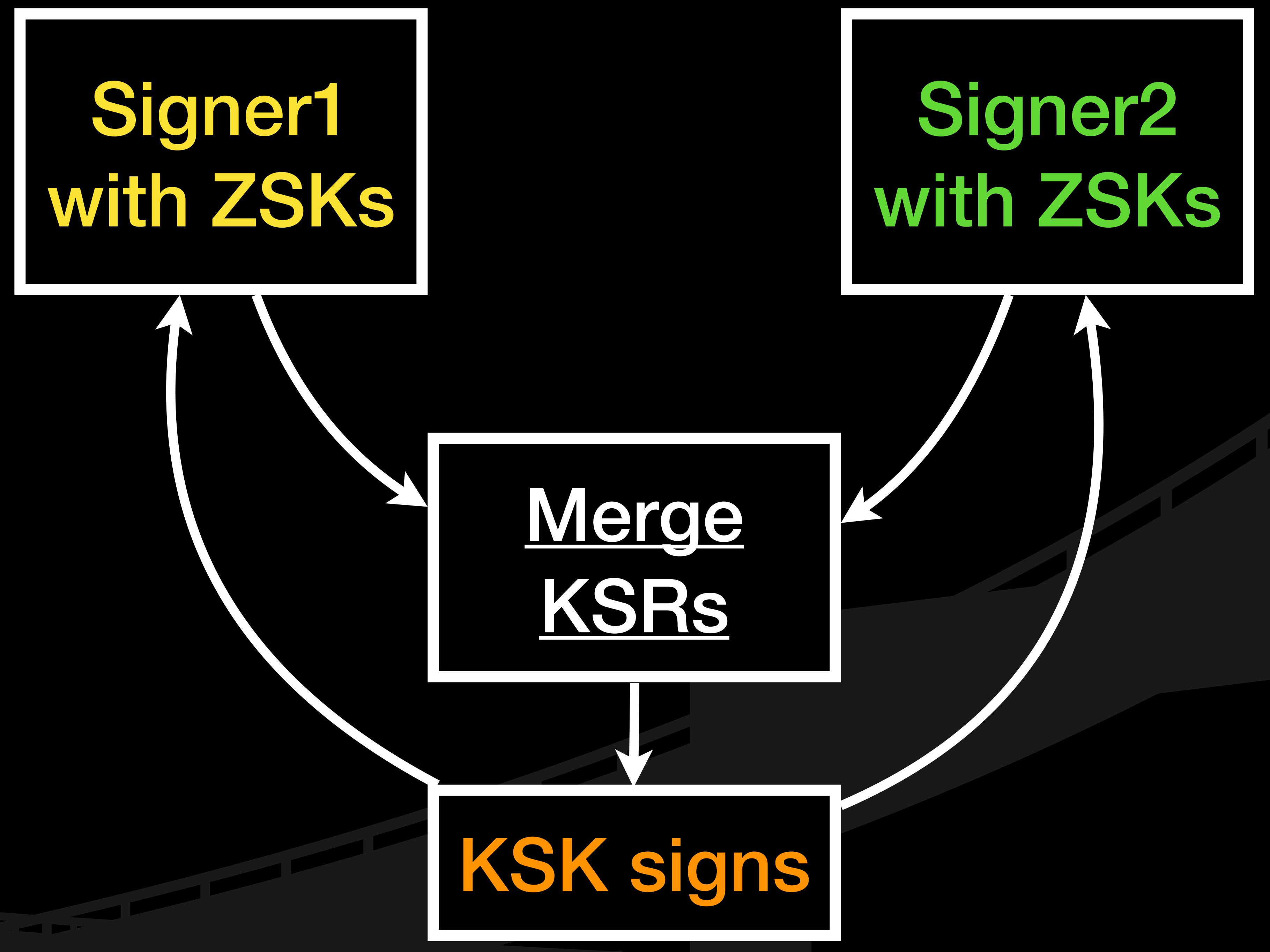
Perl script to merge KSRs

Tooling holds your hand to generate/sign/import these requests.

The only missing piece is to merge requests from the 2 providers.

For that purpose I wrote a Perl script. Which does the job.

(A nicer solution can be made in the future... :)



DNSViz

Responses for pg/DNSKEY

Name	TTL	Type	Data	Status	Returned by: gransy1.nic.pg. (185.28.194.194)	gransy1.nic.pg. (2a00:fea0:dead::beef)	gransy2.nic.pg. (185.38.108.108)	uot.nic.pg. (202.1.32.125)	dns.pch.pg. (2001:500:14:6152:ad::1)	dns.pch.pg. (204.61.216.152)
pg	3600	DNSKEY	256 3 15 Z+u4mLh1MxvTxrl/Vi5dAO0DL6dSdPDc Tu+6+agHL7s= ; **key tag = 37441** 256 3 15 ySa1vDEoL6UrP8EWus/reRRT5HoWhu9N 9vFDKcXU5Ts= ; **key tag = 23085** 257 3 15 sPk7K2UNpifGmrj0dNUO6rM6MiLYuswA mfkdHXLIqwA= ; **key tag = 23985**	OK	Y	Y	Y	Y	Y	Y
	3600	RRSIG	DNSKEY 15 1 3600 20250625134205 20250604121205 23985 pg. kv7KnZjrETWMd9MBH7Y0whHpWtBGUf9K fBEvRuvavXxgo1mcElXehVlN4pC+nMzY kq9DBPEDGV5VfMFhgPOKAg==	VALID	Y	Y	Y	Y	Y	Y
RR count (Answer/Authority/Additional)				OK	4/0/1	4/0/1	4/0/1	4/0/1	4/0/1	4/0/1
Response size (bytes)				OK	273	273	273	301	314	314
Response time (ms)				OK	49	206	50	215	50	48

Packet Clearing House

DNSViz

Responses for pg/SOA

Name	TTL	Type	Data	Status	Returned by: gransy1.nic.pg. (185.28.194.194)	gransy1.nic.pg. (2a00:fea0:dead::beef)	gransy2.nic.pg. (185.38.108.108)	uot.nic.pg. (202.1.32.125)	dns.pch.pg. (2001:500:14:6152:ad::1)	dns.pch.pg. (204.61.216.152)
pg	3600	SOA	ns1.unitech.ac.pg. dns.unitech.ac.pg. 2025060731 21600 3600 604800 3600	OK	Y	Y	Y	Y	Y	Y
	3600	RRSIG	SOA 15 1 3600 20250628160041 20250607143041 37441 pg. NbgzZWKebMxSmYITRHNdgz2TAt+9d7iK 4P6CI+E6oQ6td2Dk4LTmmAiu2Q/p0c+R mzIQ51vn++tLVPiKJvggBQ==	VALID					Y	Y
	3600	RRSIG	SOA 15 1 3600 20250628160039 20250607143039 23085 pg. Ess8vZx+94z5pyPhBDiV4pQBKte/bLIq 0sUJAvU3KcSNOMnMWq6hKHGmV+gyf8Ig EYj0OggVb5C/pZV0VZW6CA==	VALID	Y	Y	Y	Y		
RR count (Answer/Authority/Additional)				OK	2/5/1	2/5/1	2/5/1	2/0/1	2/5/1	2/5/1
Response size (bytes)				OK	370	370	370	212	417	417
Response time (ms)				OK	60	206	60	204	60	57

Packet Clearing House

Other nameservers?

Is this a knot only feature?

No, bind 9.20 gained offline-ksk functionality so the two providers can mix knot or bind9.

https://bind9.readthedocs.io/en/stable/dnssec-guide.html#offline-ksk

Packet Clearing House

Acknowledgements

Thanks to PG for trusting us with this task.

CoCCA is hosting one of the signers.

PCH is hosting the other one.

Thanks to the software developers for working hard to make DNSSEC easier and safer to use.

Thanks, and Questions?

https://pch.net

Tamás Csillag
DNS Services Engineer
Packet Clearing House
tom@pch.net