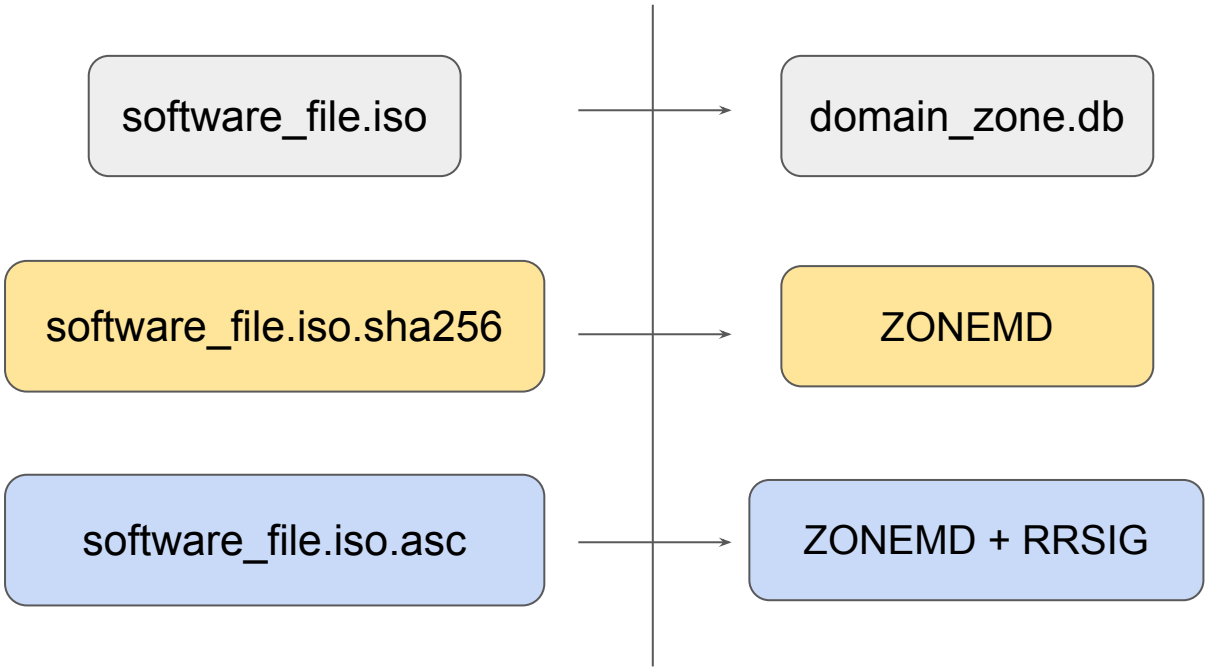
ZONEMD in .CL

Hugo Salgado
hsalgado@nic.cl

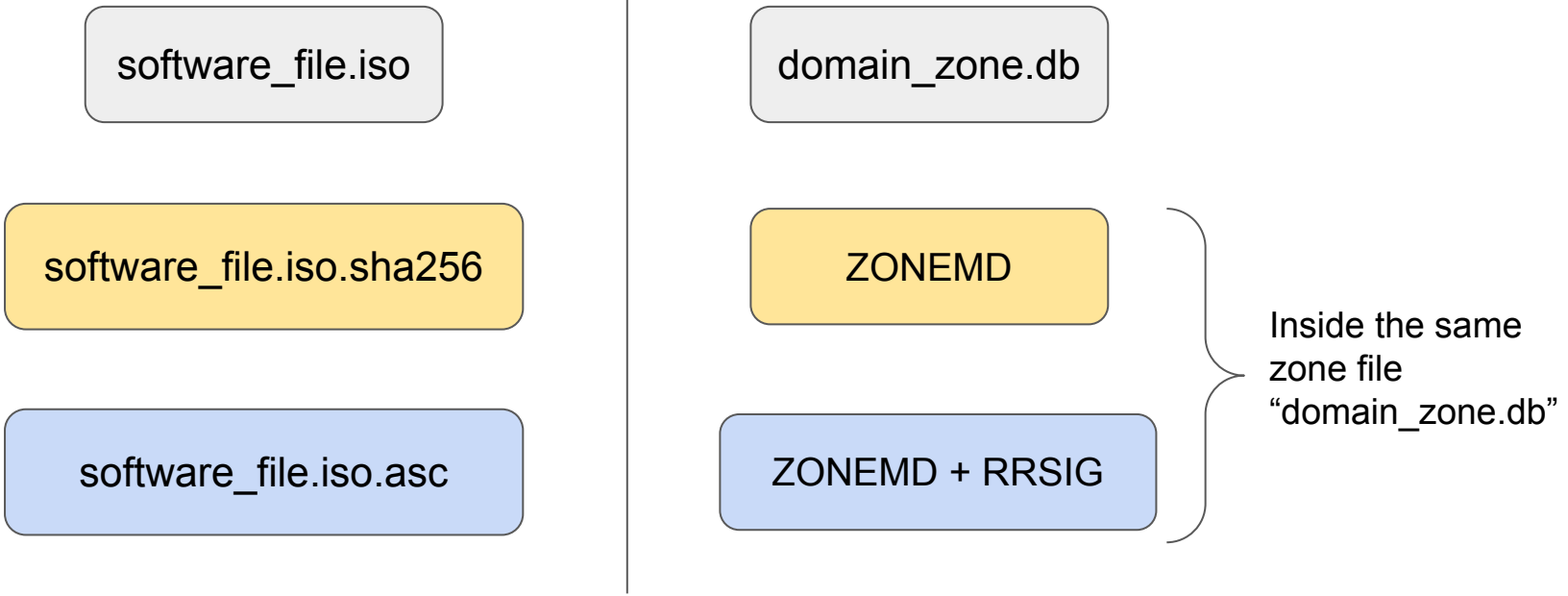
What is ZONEMD

- A new (feb. 2021) Resource Record: **Message Digest for Zones** (RFC8976).
- Provides a cryptographic message digest over DNS zone data “at rest” (file on disk).
- ZONEMD at its basics functions as a **checksum**, preventing against unintentional changes.
- When used in combination with DNSSEC, allows recipients to verify the zone contents for data integrity and origin authenticity.
- This provides assurance that received zone data matches published data, **regardless** of how the zone data has been transmitted and received.

Similar to software download checks



Similar to software download checks



```
; <<>> DiG 9.16.5 <<>> @a.nic.cl cl zonemd +norec +noauth +noadd
; (2 servers found)
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31757
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 7, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;cl.                            IN      ZONEMD

;; ANSWER SECTION:
cl.                     3600    IN      ZONEMD  2021102828 1 1 F1150AF26EA61CAE782856C4…

;; Query time: 11 msec
;; SERVER: 2001:1398:121:0:190:124:27:10#53(2001:1398:121:0:190:124:27:10)
;; WHEN: jue oct 28 14:32:37 -03 2021
;; MSG SIZE  rcvd: 423
```

Why to use ZONEMD in .CL?

- We already had an internal system to check file zone integrity
  - hash over zone dump, computed in each authoritative server
  - sent to a central checker
  - alerts for human operator

- Leverage other implementations
  - support inside DNS servers

- Better crypto

ZONEMD calculation

- **After** zone generation and signing
  - custom DNSSEC infrastructure
  - private keys unreachable
  - No RRSIG, no type in NSEC3 map
  - ZONEMD record not meant to be public consumed (nor validated)

- Signed with ldns-zone-digest
  - ~33 seconds over 1.3M records
  - generic format

ZONEMD calculation

- **After** zone generation and signing
  - custom DNSSEC infrastructure
  - private keys unreachable
  - ~~No RRSIG, no type in NSEC3 map~~ **Properly signed since Apr. 2022!**
  - ZONEMD record not meant to be public consumed (nor validated)

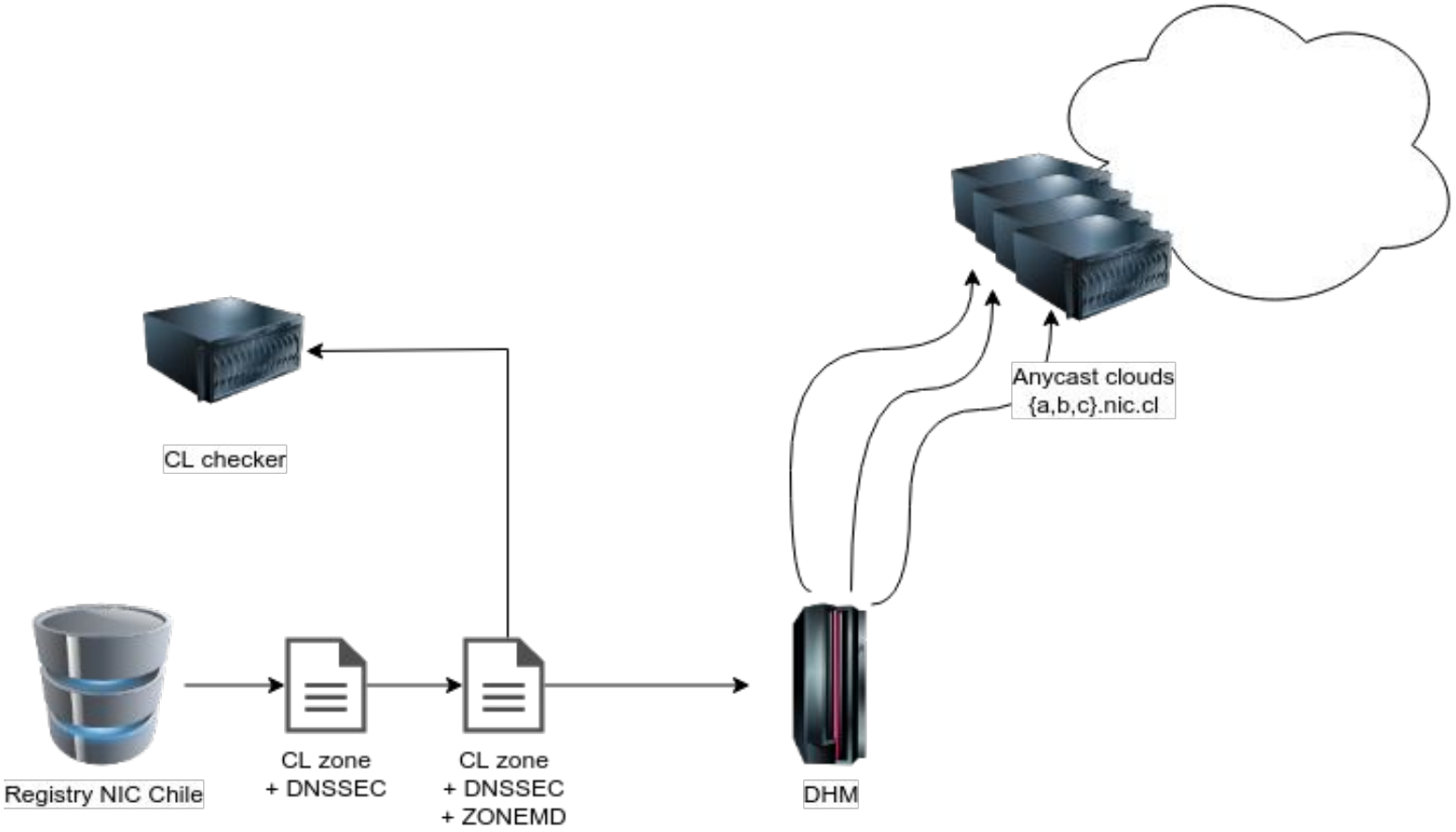
- Signed with ldns-zone-digest
  - ~33 seconds over 1.3M records
  - generic format

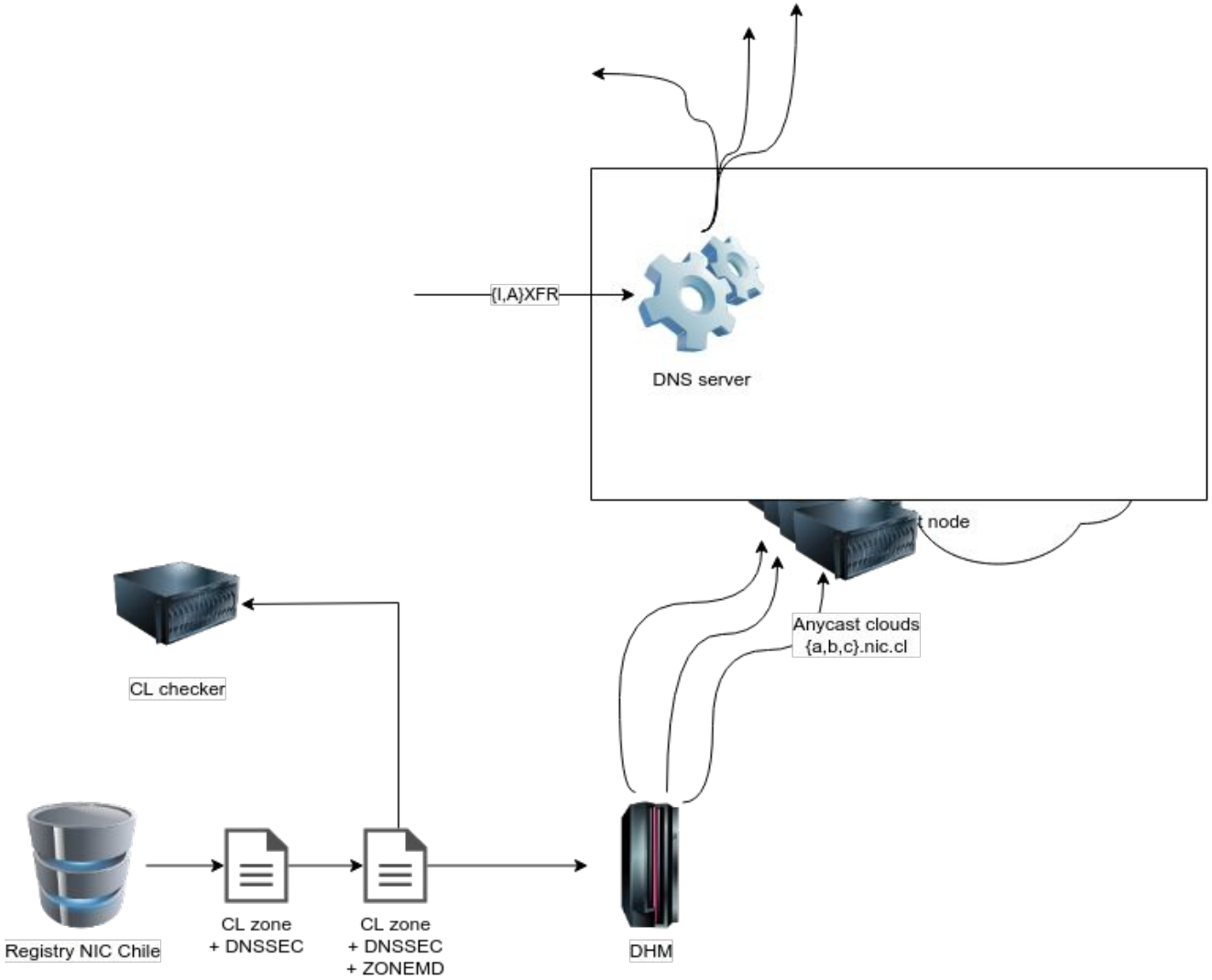
ZONEMD verification

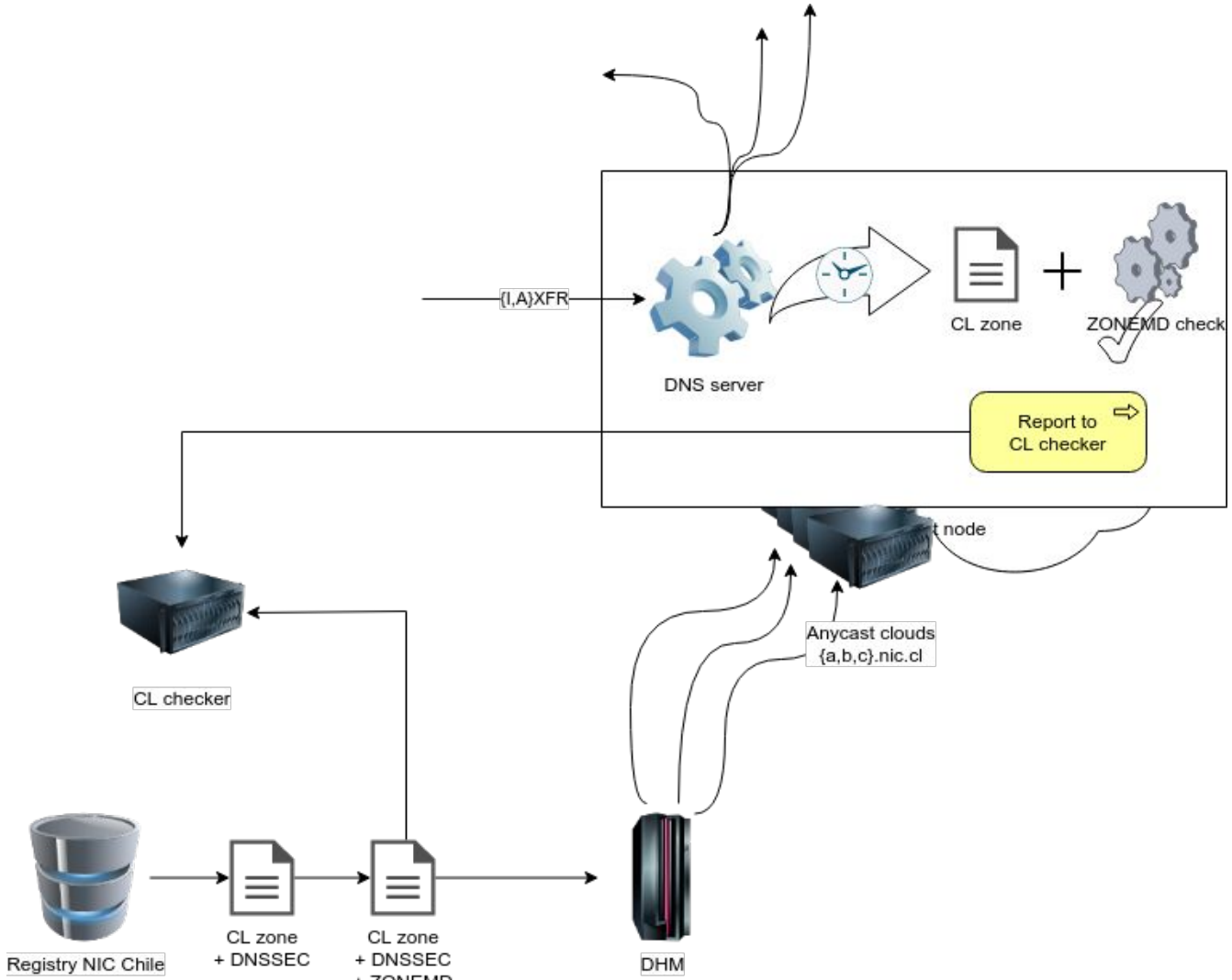
- Each anycast node (26) runs a job some minutes after loading a new zone
  - dump zone to disk
  - ZONEMD validation using dns-tools (~24 secs)
  - report to central repository
  - alerts in case of error

- Monitoring through a central checker

- Waiting for DNS server internal support.


CL checker
Anycast clouds
{a,b,c}.nic.cl
Registry NIC Chile
CL zone
+ DNSSEC
CL zone
+ DNSSEC
+ ZONEMD
DHM


{I,A}XFR
DNS server
node
Anycast clouds
{a,b,c}.nic.cl
CL checker
Registry NIC Chile
CL zone
+ DNSSEC
CL zone
+ DNSSEC
+ ZONEMD
DHM


{I,A}XFR
DNS server
CL zone
ZONEMD check
Report to
CL checker
t node
Anycast clouds
{a,b,c}.nic.cl
CL checker
Registry NIC Chile
CL zone
+ DNSSEC
CL zone
+ DNSSEC
DHM

Troubleshooting

- dns-tools is based on Go
  - fairly recent openssl libs
  - 1G RAM

- Generic format (TYPE63) vs ZONEMD

- DNS server support
  - Deactivating automatic checks (Knot)
    - zonemd-verify: off
    - zonemd-generate: none

Thanks

Hugo Salgado
hsalgado@nic.cl

NIC Chile - .CL