# .TW DNSSEC update automation

TWNIC

Nai-Wen Hsu

# Current State of .TW DNSSEC Automation

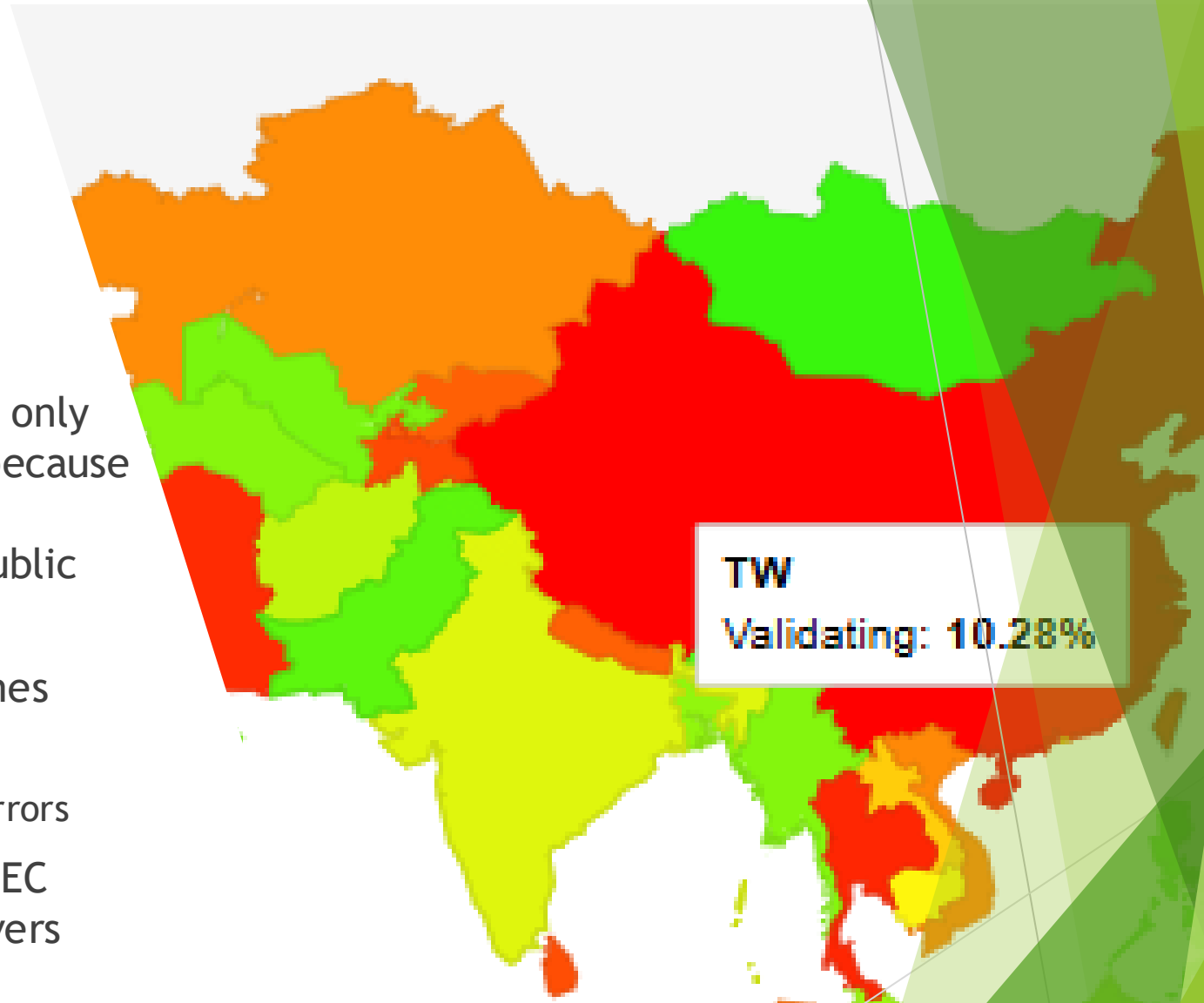
- DNSSEC operations are mostly automated between TWNIC (.TW registry) and registrars
  - registrar➔EPP➔registry database➔zone file generator➔.TW DNS servers
- However, DS record provisioning remains largely manual when the registrant uses a third-party DNS service
  - DNS service provider➔registrant➔registrar

# Why Automation Matters

- Manual updates are error-prone, increasing the risk of vulnerabilities and jeopardizing the integrity of the DNS
- To make matters worse, registrants know nothing about DNSSEC and don't know how to operate it in the registrar's interface or when to do key rollover

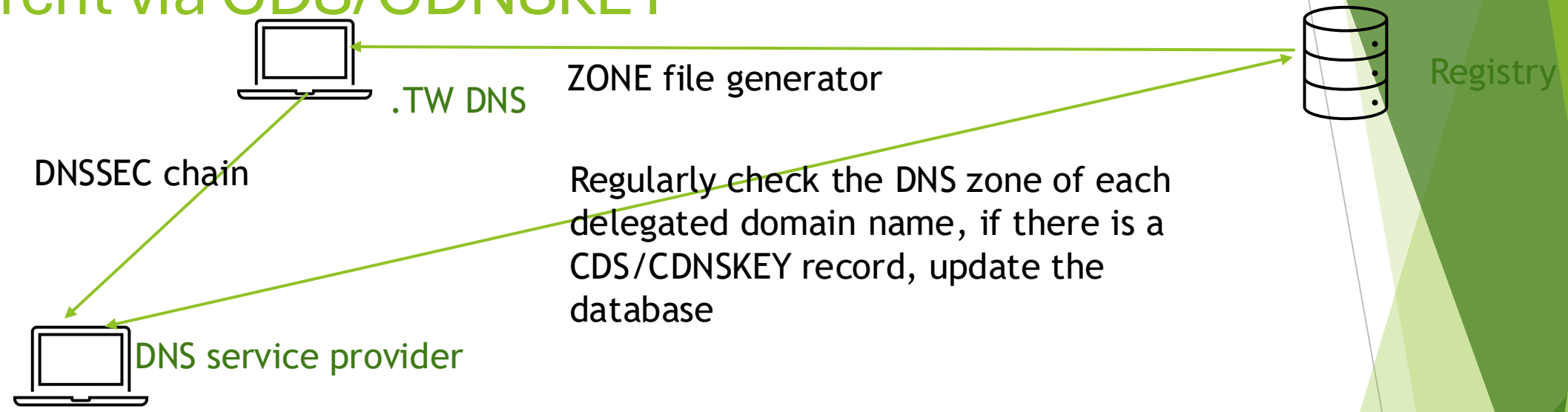
# DNSSEC deployment issues in Taiwan

- APNIC DNSSEC survey show Taiwan only 10% DNS queries enable DNSSEC, because some small ISPs don't have own recursive DNS servers, They use public DNS resolver like google DNS
- Less than 0.5% of .TW domain names enable DNSSEC
  - Over 10% are DNSSEC validation errors
- No ISP in Taiwan has enabled DNSSEC validation in its recursive DNS servers




Source: https://stats.labs.apnic.net/dnssec/XD

# RFC8078 Managing DS Records from the Parent via CDS/CDNSKEY




RFC8078 bypass registrant involve DNSSEC update, eliminate DNSSEC error

# Some issues in implementing RFC8078

- Checking all .TW delegated domains for CDS records takes more than 24 hours
- For some large DNS service providers, TWNIC's DNS query is equivalent to a network attack
- Do we accept DNSSEC being enabled or disabled via CDS record
  - RFC9615 defines a complex process for enabling DNSSEC for a domain via CDS record

# TWNIC’s approach

- Only supports CDS, not CDNSKEY (same as EPP, only supports DS but not DNSKEY)
- Check once a day all DNSSEC-enabled domain CDS record exist or not, if exist
  - If the DS is the same as the one in the existing repository, then stop
  - Check whether the NS records are consistent with the database. If they are different, stop
  - Check whether the SOA of all DNS are consistent. If not, stop
  - Check if the CDS of all DNS are consistent. If not, stop
  - Whether the zone has been signed and validate by the new DNSKEY, if yes, update database
  - If CDS is "0 0 0 0", delete the DS record from the database and disable DNSSEC for the domain

# TWNIC’s approach (continued)

- Currently .TW has dynamic update enabled. If the nameserver is updated via EPP command, TW zone file for the domain name will be updated immediately, and
  - Follow the steps on the previous page to check if there is a CDS record exist
  - If an emergency key rollover is needed, just update the nameservers (keep the old and new nameservers the same)
  - If DNSSEC is not enabled, you can enable DNSSEC in this way
    - The mechanism of RFC8078 3.1-3.5 is not adopted
    - RFC9615 Session 4 Bootstrapping a DNSSEC Delegation is not supported

# Conclusion

- Automation of DNSSEC updates remains complex, especially when involving third-party DNS service provider
- RFC8078 Managing DS Records from the Parent via CDS/CDNSKEY is a good approach to implement DNSSEC update for third-party DNS service provider
- Currently, many third-party DNS service providers support RFC8078. If these service providers enable RFC8078 for .TW hosted domains, .TW DNSSEC will grow from less than 0.5% to more than 20%

# Any Questions?