GMO INTERNET

An example case of deploy DNSSEC by GMO Internet

2020/06/22
DNSSEC and Security Workshop Program
in ICANN68 Virtual Meeting

Yuya Nagai & Yoshikazu Kojima

Agenda

1. Introduction
2. Begin the DNSSEC
3. Decided of Policy
4. Current State

1. Introduction

Who are we?

Speaker: Yuya Nagai
(Sorry, I can't speak English...)

I am in charge of services for DNS in GMO Internet.
I found the djbdns in 2003, after that I have been studying the DNSSEC since 2009.
by the way, my favorite program language is Perl.

Interpreter: Yoshikazu Kojima

I am in charge of technical on our shared hosting service in GMO Internet. My specialty is web and mail.
Before I have build DNS server for our service myself. It was BIND with text file based DLZ. 170 qps fast.

What is GMO Internet?

The Domain Name Registrar.
We called “onamae.com”. (“onamae” = “a name”)

- Main services.
  - The domain name registration.
  - DNS provide for registrant.
  - Sale web hosting service (with the domain name).
  - (we provide other more services, but scope out)

What is GMO Internet?

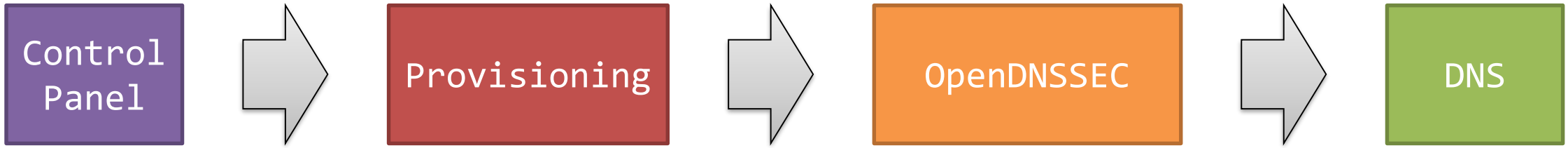
- The DNS provide service started at since 1999.
  - Free additional service for domain name registration.
  - The customers able to use functions to the follows:
    The management DNS, zone XFR-in, and control panel for there.

- The DNSSEC service started at Aug 27th 2014.
  - Advanced optional service. (fee)
  - The customers able to use function to zone XFR-out, more zone edit features, zone file import/export, zone file template, URL redirector, mail transfer, and managed DNSSEC.
  - Easy to use DNSSEC for customers by simply apply from the control panel.

2. Begin the DNSSEC

The architecture of DNSSEC service

- Front-end DNS servers.
  - ✓ BIND 9 and NSD.
    - Must be implement diversity in preparation for software bugs.
- DNSSEC software.
  - ✓ OpenDNSSEC (ods)
  - ✓ SoftHSM
- A little provisioning script.



Development point

- Choose software for the DNSSEC.
  - ✓ Major DNS products support DNSSEC.
    - BIND 9, NSD, PowerDNS, KnotDNS.

- Setup the OpenDNSSEC is simple.
  - ✓ Setup with HSM is difficult, however SoftHSM is easy.
  - ✓ To two point for run:
    - Should be monitering the process.
    - All databases should be backup after KSK and ZSK generated. (for ods, softhsm)

Difficult point

- Explanation for project members.
  - ✓ No other members understood the DNSSEC.
    - Project members are developers for registrar system, developers for web application, and me (DNS servers).
  - ✓ Begin explain about DNS, then the DNSSEC.
    - RFC 1033, 1034, 1035.
    - RFC 6781 reading in turns by members.
      (RFC 6781: DNSSEC Operational Practices, Version 2)
  - ✓ Share information to manager of the customer support.
    - FAQ, meeting, and more.
- Transfer Policy
  - ✓ Next slide.

3. Decide Transfer Policy

Transfer policy

- Why decide transfer policy?
  - ✓ Clarify how we will provide what kind of DNSSEC services to our customers.
    - Allow transfer with enabled DNSSEC?
    - Or deny? (must disable DNSSEC to transfer?)
  - ✓ We have to be prepared for problems occur.

- Reports for domain name transfer with DNSSEC.
  - ✓ In Japan, JPRS and the DNSSEC Japan community have published reports on domain name transfer with DNSSEC between registrars.
    - https://jprs.jp/dnssec/doc/DNSSEC-testbed-report-odv1.0.pdf
    - https://dnssec.jp/wp-content/uploads/2012/07/20110509-techwg-registrar-transfer-experiment.pdf
  - ✓ We used this report as a reference when making our policy decisions.

Transfer policy

- Our DNSSEC service recommends transfer domain name without DNSSEC.
  - ✓ The relationship between registrar and DNS provider (or registrars) is sometimes not strong.
    - Registrar recognize their domain name is transferred to another registrar after transfer process finished.
  - ✓ May increase inquiries to customer support.
    - Some customers may forget that DNSSEC is still enabled.
- How hard to transfer domain name with DNSSEC enabled?
  - Verify, explain, exchange keys, re-sign, delete...
  - Do it everything manually, is nightmare.

4. Current State

Known Issues

- We have no big trouble now.
  - ✓ There were a few cases that customer complaints us.

- Case 1
  - ✓ Transfer-In was performed with DNSSEC enabled.
    Then they cannot resolve their domain name.
    - Validator doesn’t trust response from our authoritative DNS, because our DNS servers doesn't have DNSSEC keys and signature.
    - We manually removed data the delegation signer information.
    - Customer could be resolved their domain name with the DNSSEC disabled.

Known Issues

- Case 2
  - ✓ Transfer-Out was performed with DNSSEC enabled.
    Then they cannot resolve their domain name.
    - Even if we receive an inquiry from a customer,
      we cannot do anything because the domain is already transferred out.
    - We let the customer to ask current registrar to
      remove data the delegation signer information.

- In both cases, customers forgot to disable DNSSEC.
  - ✓ Fortunately we don’t have major problems other than these cases.

Future Issues

- We do not yet have feature to add data the delegation signer information to the registry for our customers.

- When we will do it?
  - ✓ Our DNS service have around 200 domain names enabled DNSSEC.
    - Less than 0.01% of 2 million domains...
  - ✓ I personally want provide the DNSSEC and other features, but without customer’s request, business director doesn’t think it is important for us.
  - ✓ I hope I will offer better the DNS services.

Thank you!