Panasonic

SANNET DNSSEC Experience

SANYO Information Technology Solutions Co.,LTD
SANNNET Business Unit
Manabu Sonoda

2010

Jun:

Started DNSSEC validation at main full resolvers of our ISP.

Sep ~ Dec:

Development DNSSEC key and signing management system .(similar to OpenDNSSEC)

2011

Jan:

Started DNSSEC signing at authoritative DNS of DNS hosting service.

Before doing

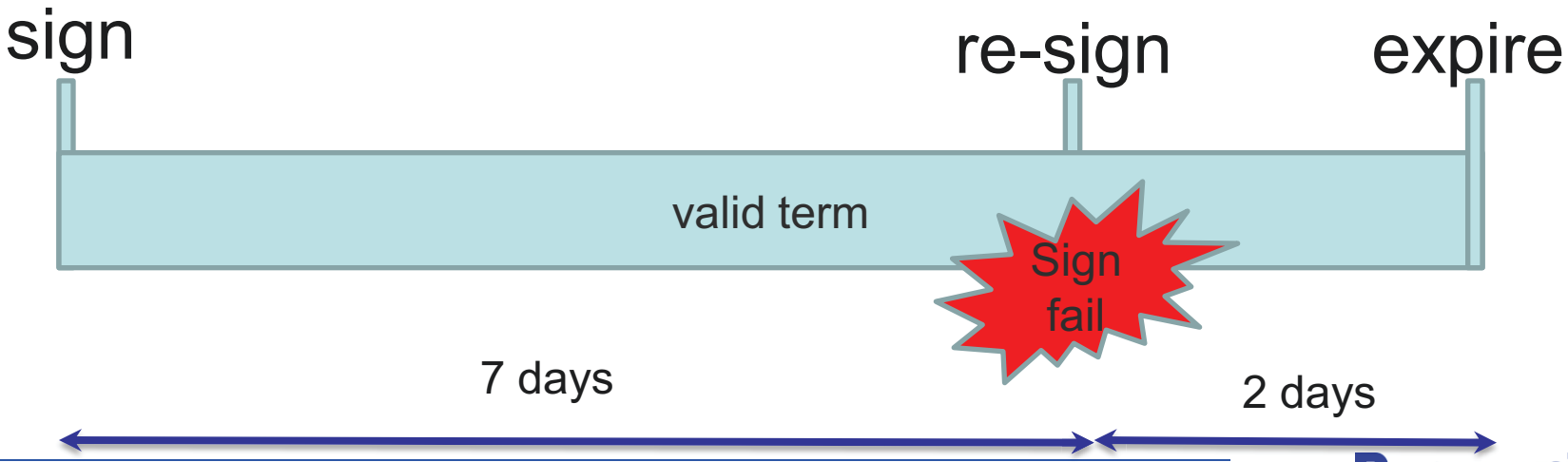
Protect our isp customers from phishing.

Now

Validity of DKIM and SPF.
hope DANE protocol.

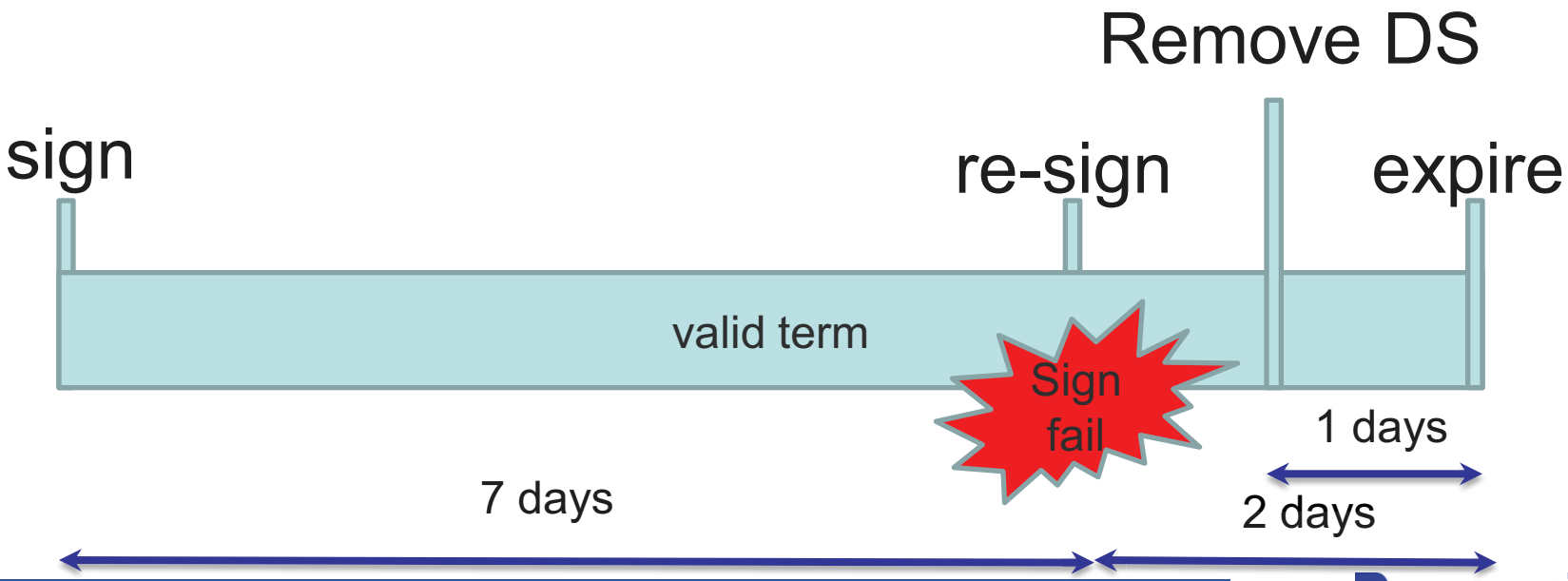
Dec 2012

- Detected that signatures did not updated by re-signing in some zones, But the reaseon was unclear.
- Domains will be bogus!!



- We decided to remove DS RR.
- DS TTL is 1day, So many hosting domains avoided bogus.

Signature Lifecycle design is important.



- We watch ROOT,COM,NET,ORG and JP zones.

- Our full resolver servers stop validation automatically when failure of it detected.

Dec 2012

Many Japanese ISP allocated reverse zones were bogus.

- Our full resolvers CPU utilization became three times higher than usual.
- 10% incoming query answers were servfail.
- Non recursive queries became eight times higher than usual.

Counter Plan when big impact zones were failure.

- Prepare a enough resources for availability.
- Considering Unbound which can use "domain-insecure"

No problem other than today 2 things.

We keep a stable operation validators and authoritative servers.

Panasonic


Panasonic