Motivation

- DNSSEC is highly recognized and getting popular, but penetration is still low.
- DNSSEC operational practices are not accumulated enough yet (rare to publish experiences?)
- Misoperation of DNSSEC will cause serious impact such as name resolution failure.
- Especially, impact of KSK rollover failure is huge and its recovery requires cooperation of child/parent zone and full resolver operators.
- Having best practices for DNSSEC operation will be useful.
Problem definition

• DNSSEC validators will cause failure when DS in parent zone and DNSKEY in child zone are inconsistent
  – This will happen if child zone operator registers wrong DS or parent zone operator stores wrong DS by misoperation
• However DS and/or DNSKEY are corrected, influence will remain until DS and/or DNSKEY cache in validator be expired
• For prompt recovery from failure, TTL control of these RRs and/or cache management are very important
Cases of countermeasure

- There are some countermeasures for the recovery

<table>
<thead>
<tr>
<th>Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>case1</td>
<td>Ask ISPs to flush cache</td>
</tr>
<tr>
<td>case2</td>
<td>Use short TTL for DS and NS</td>
</tr>
<tr>
<td>case3</td>
<td>Use short TTL for DS only</td>
</tr>
<tr>
<td>case4</td>
<td>Use short TTL for DS and NS when modified</td>
</tr>
<tr>
<td>case5</td>
<td>Do nothing</td>
</tr>
</tbody>
</table>

- Each countermeasure have pros and cons
- Need to investigate these and select one for the best practice
Case 1

• Countermeasure
  – Correct or remove DS in parent zone
  – Ask major ISP to flush corresponding cache

• Pros
  – No need to consider TTL of RRs

• Cons
  – Impossible to ask all major ISPs
Case 2

• **Countermeasure**
  – Use short TTL for DS and NS

• **Pros**
  – Impact of failure is shortened

• **Cons**
  – Queries to parent/child zone will increase
Case 3

- **Countermeasure**
  - Use short TTL for DS only
- **Pros**
  - Impact of failure is shortened
- **Cons**
  - Queries to parent/child zone will increase
  - Will not effective for implementations that query DS only when NS is expired
Case 4

- **Countermeasure**
  - Use short TTL for DS and/or NS only when they are registered/modified
  - Use long TTL after a certain duration passed

- **Pros**
  - Impact of failure is shortened
  - Increase of queries will be suppressed

- **Cons**
  - Operation of parent zone will be complicated
Case 5

• Countermeasure
  – Do nothing
• Pros
  – No changes to current systems/procedures
• Cons
  – Impact will remain until TTLs of NS and DS are passed
Feedback, please

• *(I believe)* this topic is useful especially large zone operators like TLDs and DNS providers

• Please give your comments, thoughts, and countermeasures that you are taking

• For better life with DNSSEC 😊