Algorithm Rollover what is the safest approach

Frederico A. C. Neves
<fneves@registro.br>

DNS-OARC 28 - San Juan - 20180309

Algorithm Rollover Safest Approach

Open source signer implementations that we are aware of, BIND "managed keys" and OpenDNSSEC, implements the “liberal” approach as described at 6781 4.1.4; 6781 describes and advice for the “conservative" approach;

The public log around Oct/2016, on support mailing lists, reports historically that the validator following the “conservative” approach have being "convinced" to update and better behave with the “liberal" approach; Digging further the starting version following the “liberal" approach is from Jan/2011, 7 years ago;

6840 in Feb/2013, 5 years ago, 5.11 clarifies the "confusing" 4035 language;

If at least one implementations followed the conservative approach there is a non zero probability of others following it as well… and it is a fact that is not possible to proof that there is no other implementations that followed the “conservative” approach.

With all of that taken in account, today, what would be the safest path, **conservative, liberal…** any other?

Discussion ?