



83

POLICY
FORUM



Secondary resilience with DNSSEC



Ulrich Wisser

ICANN 83
June 2025

SOA Expire



SOA Expire



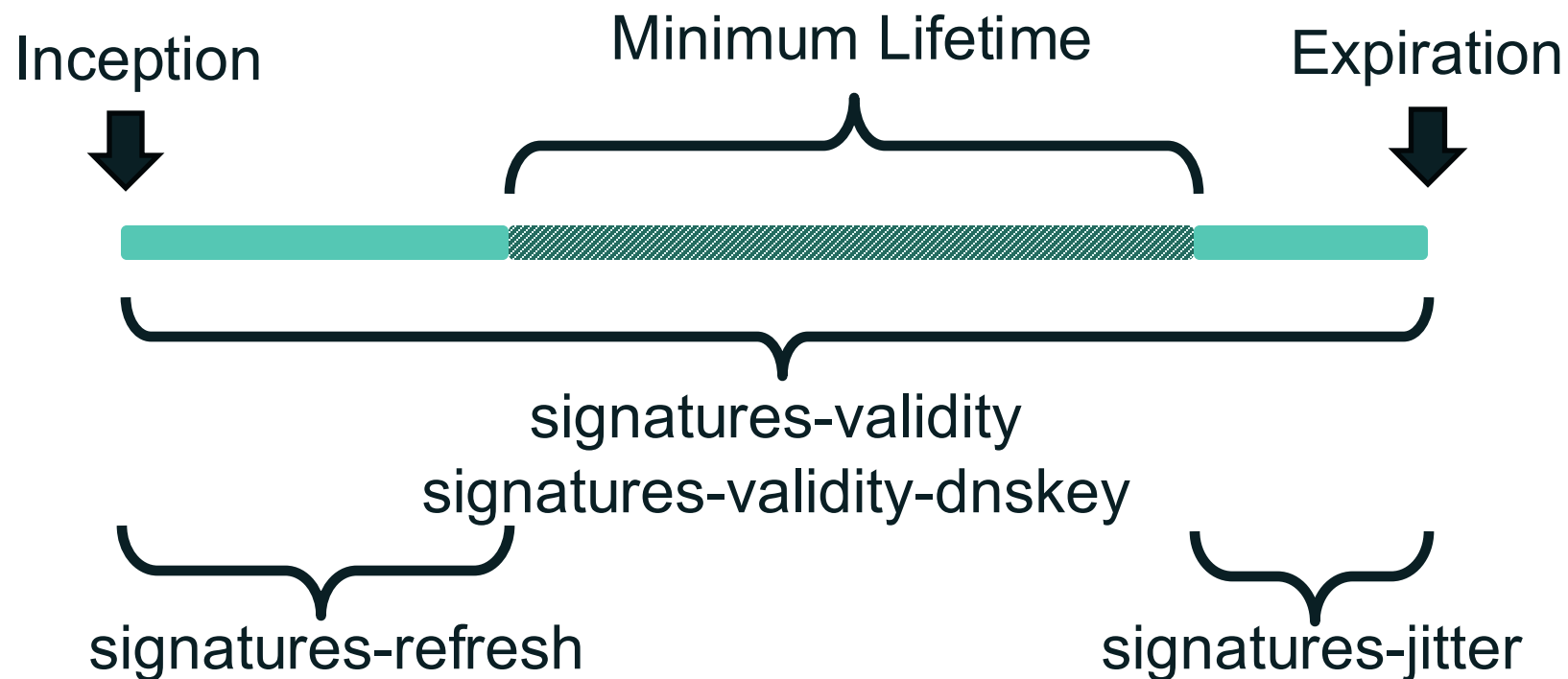
SOA Expire

TLD SOA expire values 2024-11-01			
# TLD	Seconds		
1	7200	0d	2h 0m 0s
2	86400	1d	0h 0m 0s
50	259200	3d	0h 0m 0s
1	432000	5d	0h 0m 0s
2	518400	6d	0h 0m 0s
428	604800	7d	0h 0m 0s
1	720000	8d	8h 0m 0s
2	864000	10d	0h 0m 0s
511	1209600	14d	0h 0m 0s
5	1296000	15d	0h 0m 0s
4	1728000	20d	0h 0m 0s
34	1814400	21d	0h 0m 0s

TLD SOA expire values 2024-11-01			
# TLD	Seconds		
1	2419000	27d	23h 56m 40s
121	2419200	28d	0h 0m 0s
19	2491200	28d	20h 0m 0s
35	2592000	30d	0h 0m 0s
3	2764800	32d	0h 0m 0s
1	3024000	35d	0h 0m 0s
6	3456000	40d	0h 0m 0s
10	3600000	41d	16h 0m 0s
5	5184000	60d	0h 0m 0s
109	6048000	70d	0h 0m 0s
1	604800000	7000d	0h 0m 0s

RRSIG lifetime

Timing Considerations



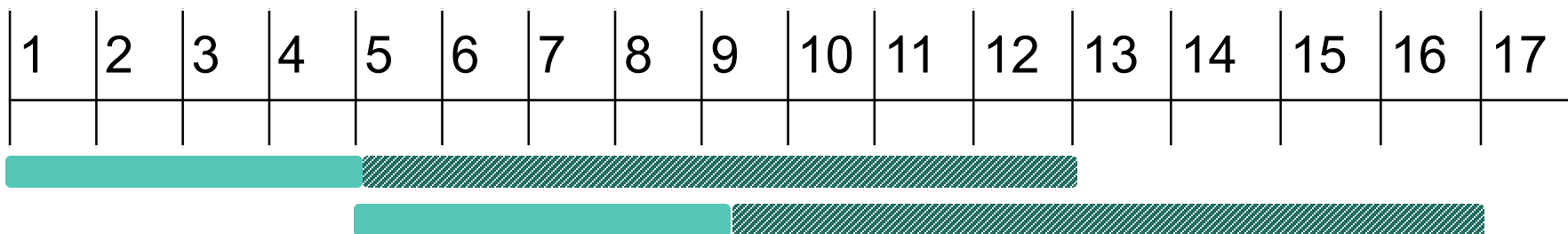
Timing Considerations

refresh

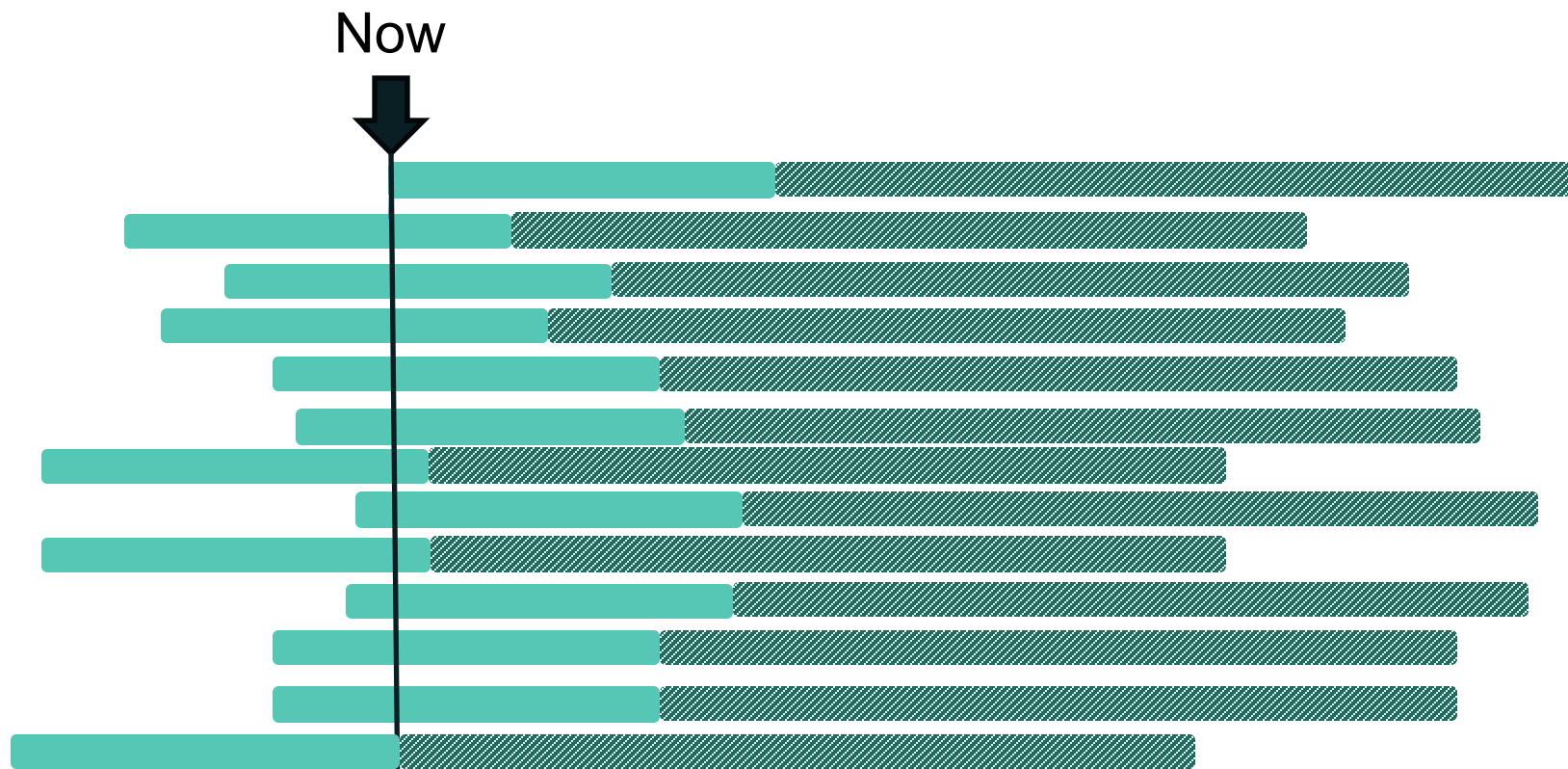


RRSIG Lifetime 12 days
RRSIG Refresh 4 days

Days



Timing Considerations



Problem

At a minimum
RRSIG lifetime
needs to be longer than
SOA Expire

RFC 6781 Section 4.3.4 suggests:

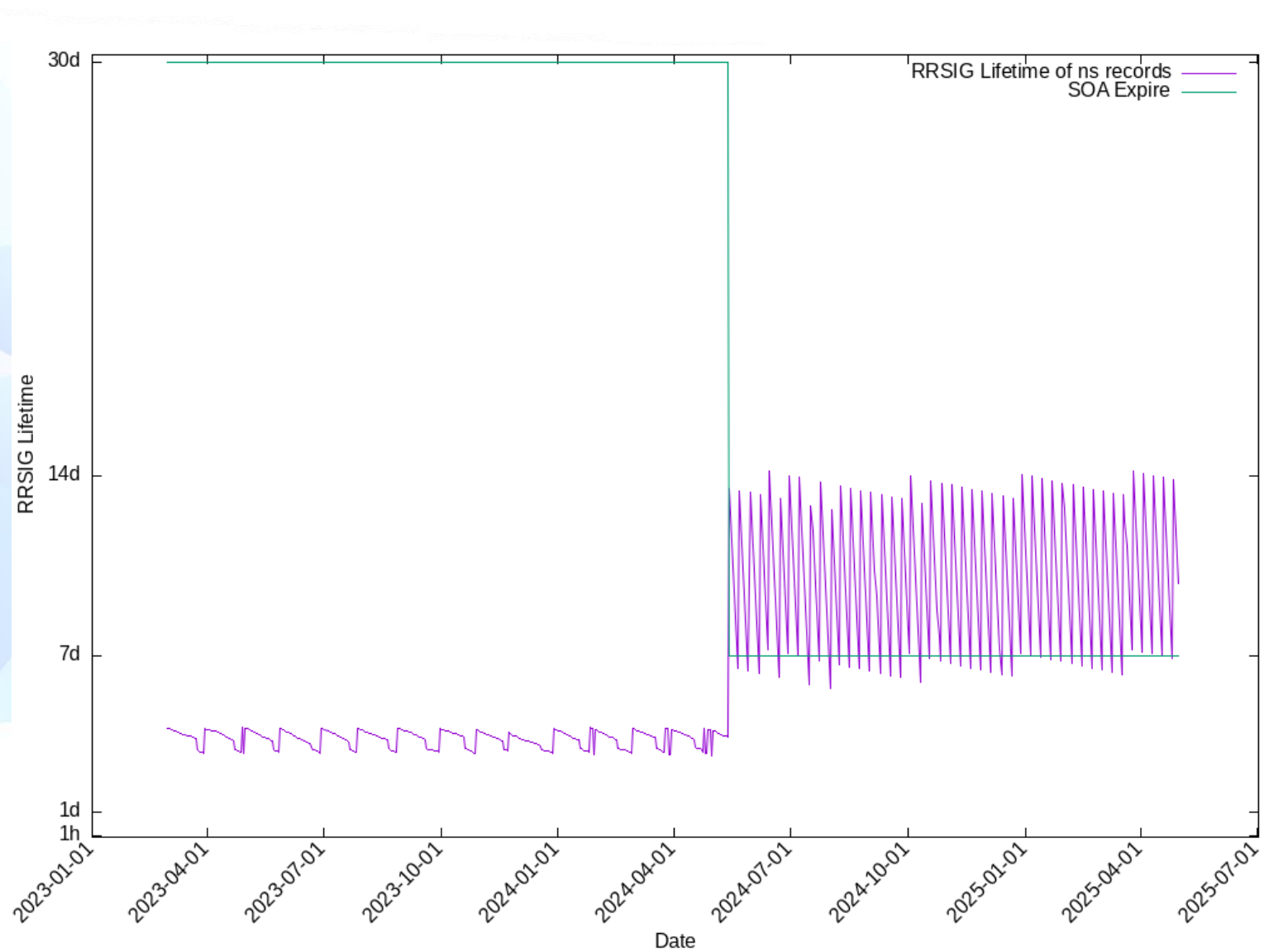
<https://www.rfc-editor.org/rfc/rfc6781#section-4.3.4>

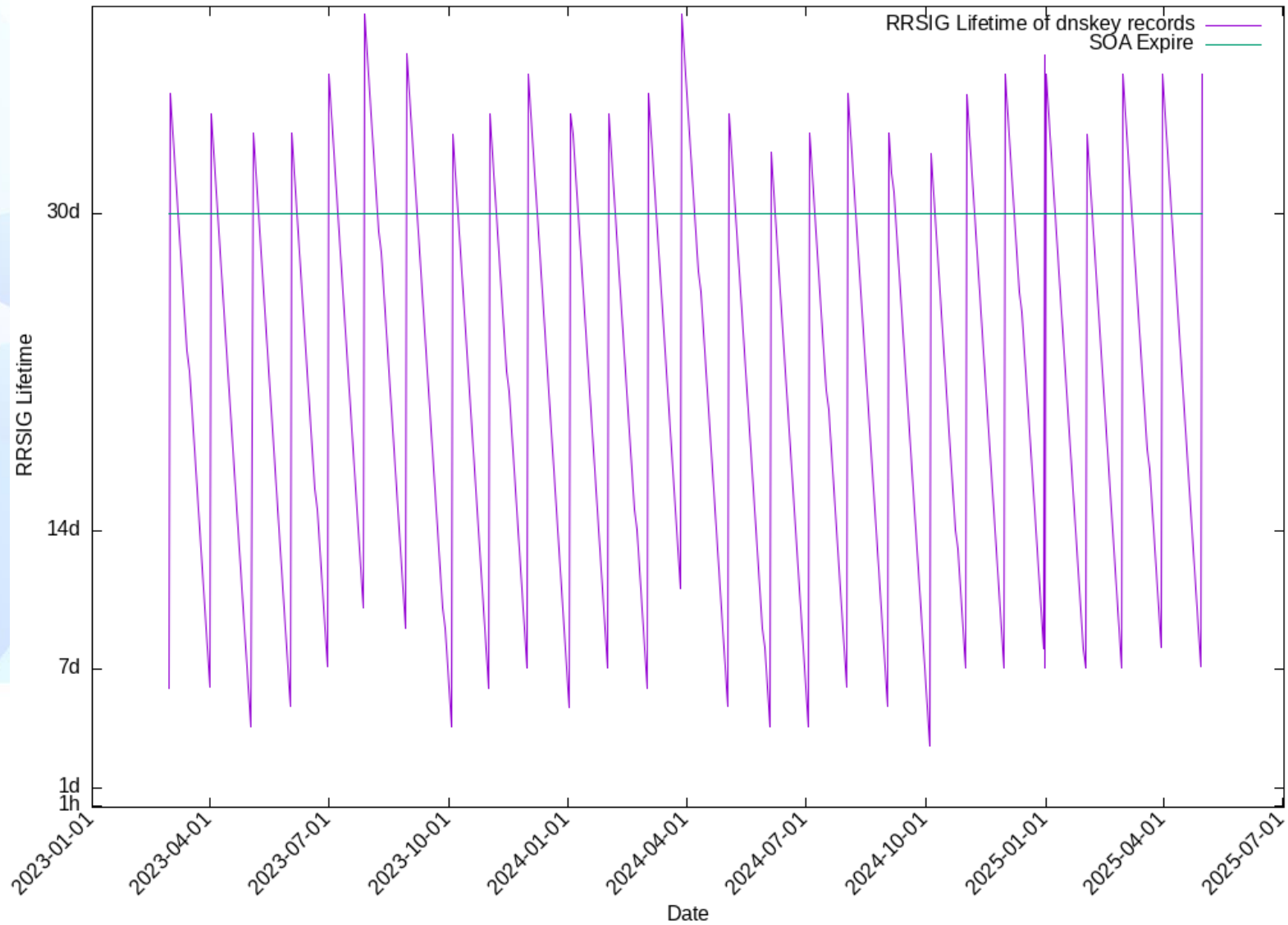
We suggest that the SOA expiration timer be approximately one third or a quarter of the signature validity period. It will allow problems with transfers from the master server to be noticed before signatures time out.

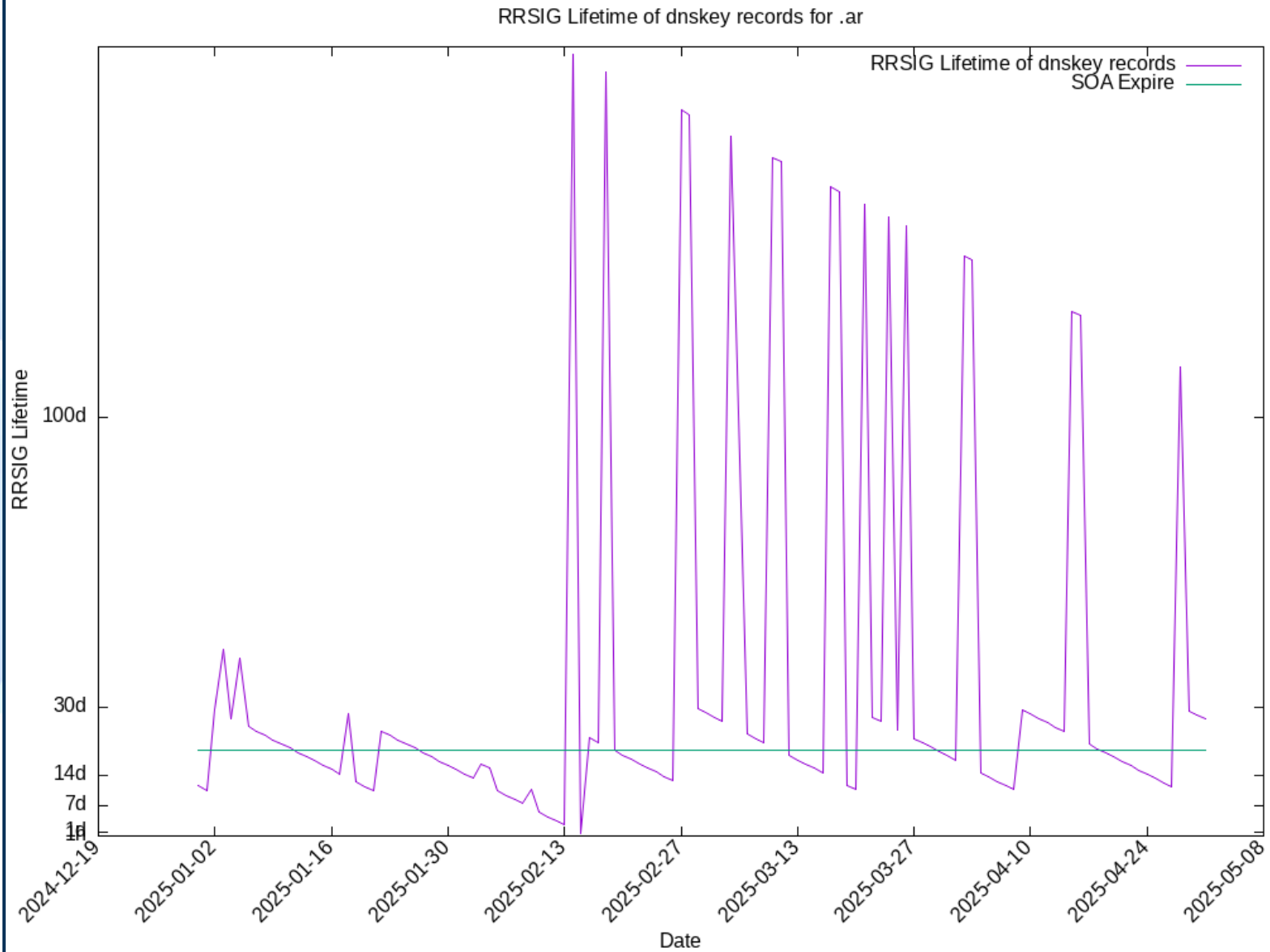
Problem Size

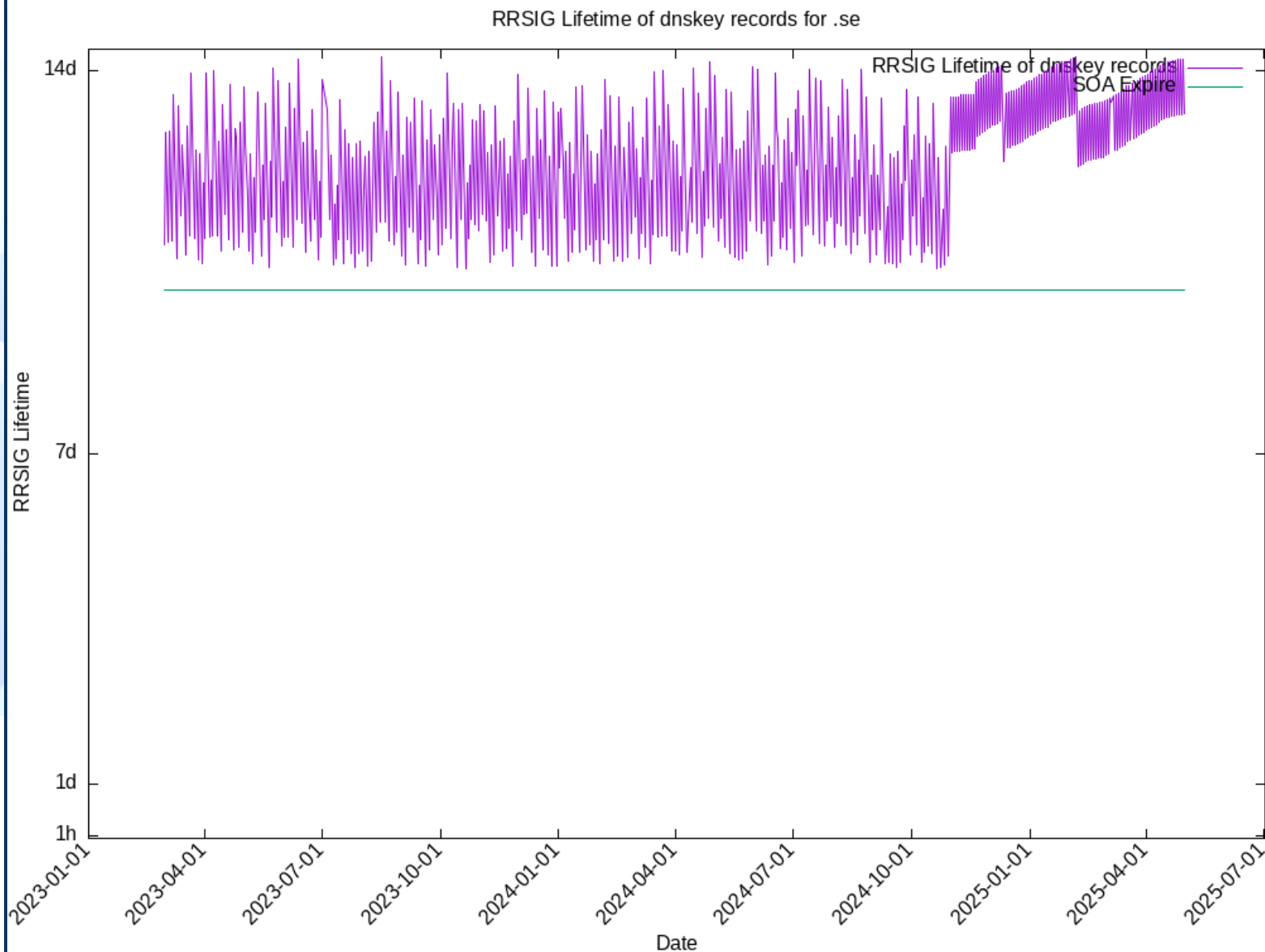


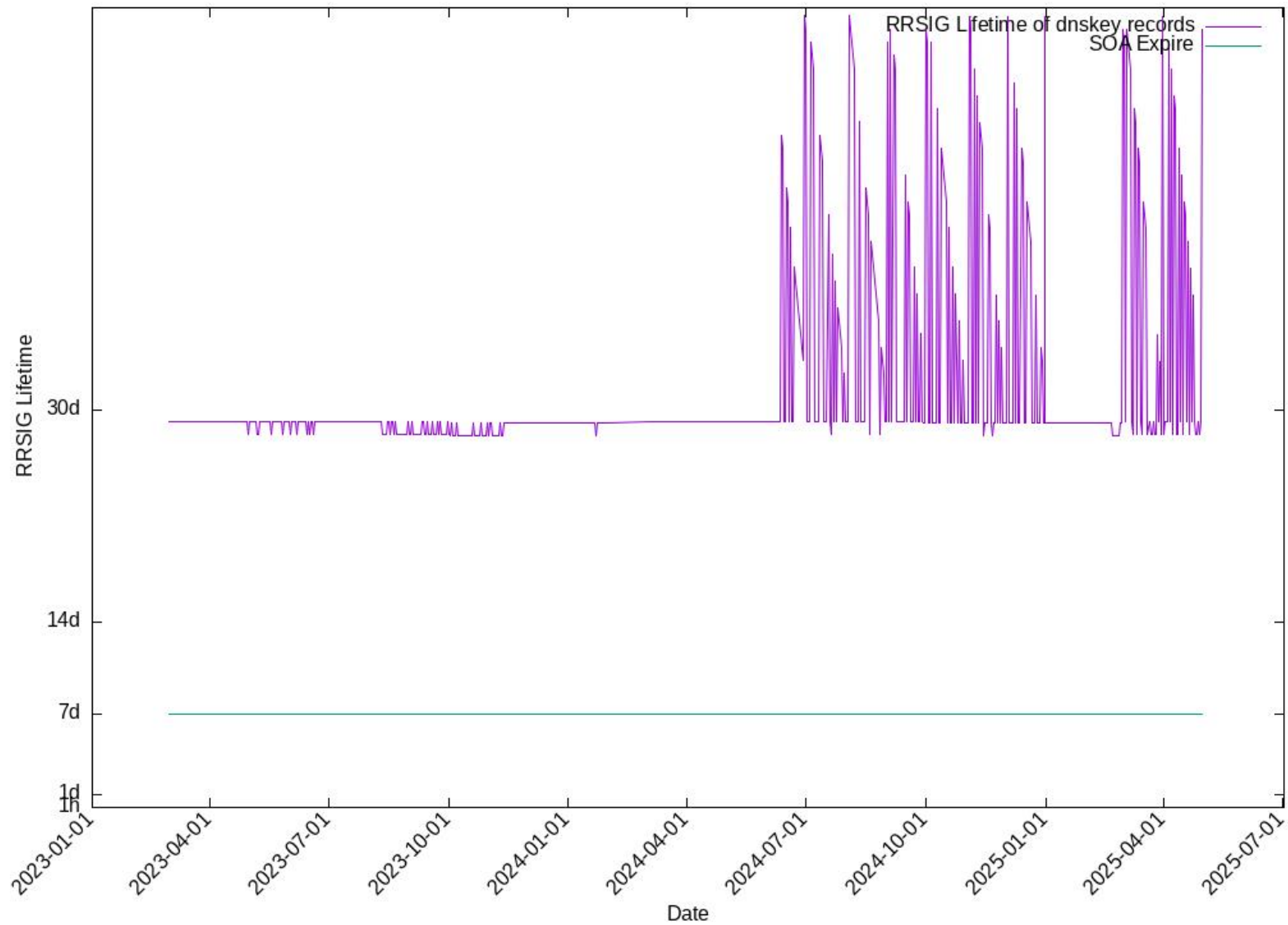
Real World Examples











CONCLUSION

Conclusion

- Use Reasonable SOA Timers
- The SOA Refresh, Retry, and Expire fields should reflect your operational reality — not just inherited defaults.
- The Expire value should cover even the most extreme disaster scenarios.
- Make sure RRSIG Expiration is greater than SOA Expire at all times
- DNSSEC has many timing configurations, make sure to understand all their implications
- Monitor Signature Expiry proactively
- Implement checks to alert operators if RRSIGs will expire before expected SOA timeouts.
- **Update RFC 6781 or start following it!**