Looking at DNSSEC Deployment in the Upper Zones

Edward Lewis
ed.lewis@neustar.biz
APRICOT 2013
February 26, 2013

Introduction

- DNSSEC has a number of operational parameters to set
- Using the root and TLD zones as examples, started to measure how they ran DNSSEC
  - Sizes
  - Durations
- At APRICOT 2012 this was first presented and then throughout the year more data gathered and stories learned
- At APRICOT 2013 an “annual wrap up” of what was measured, what it means, and recommendations
  - The work will continue, the talks won’t

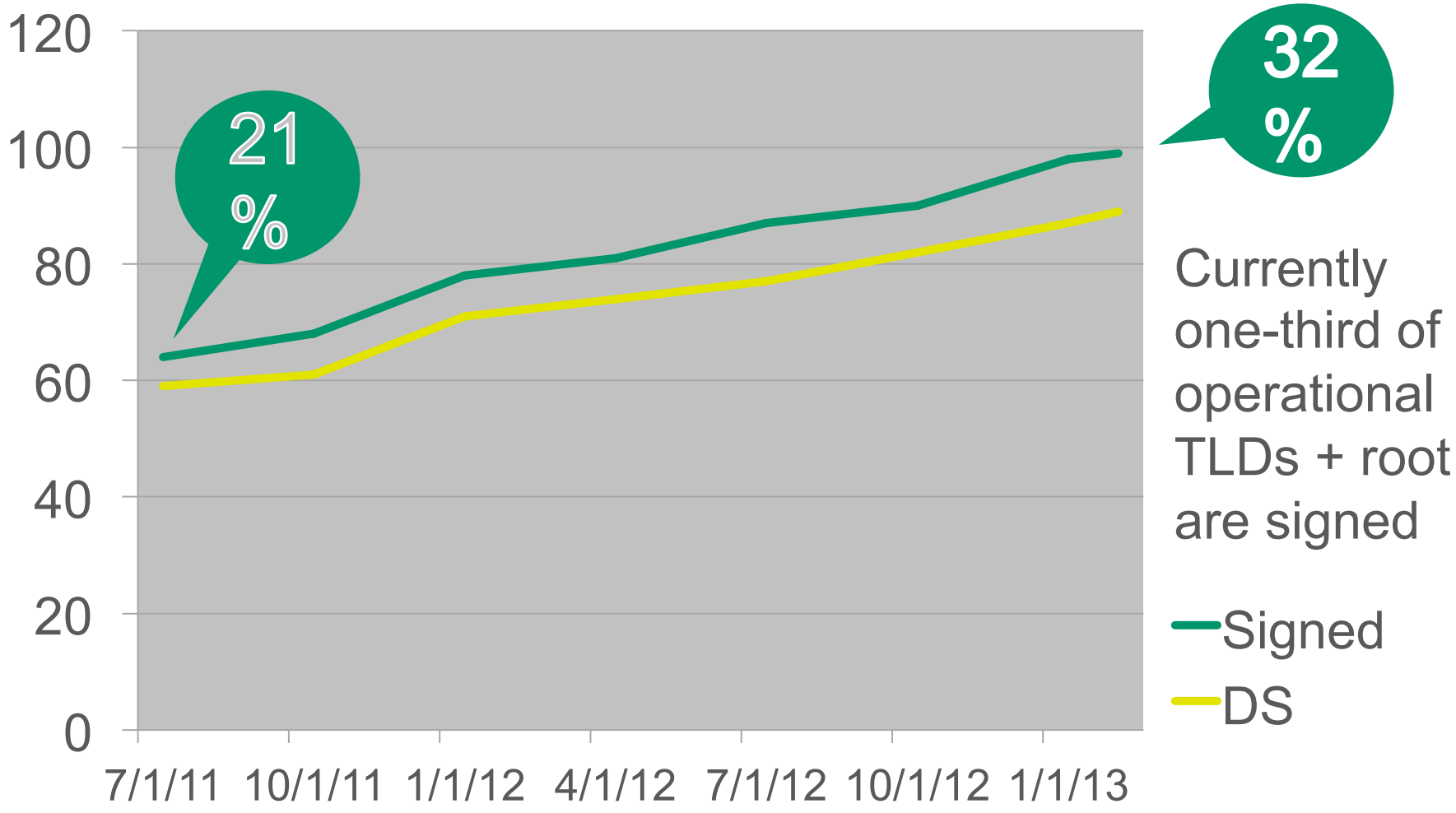
What is Measured

- Key Management
  - How keys are used, i.e., their cryptographic roles
  - Algorithms, sizes of keys and other cryptographic elements
  - Duration, frequency of operator actions
- Other operational choices
  - NSEC or NSEC3 choice
  - Delay in DS introduction; “Backup DS records”
  - Support for old code
- Some of the measurements will be presented here
  - If interested in other details, contact me later

What Has Been Learned

- The choices TLDs make
- The rationale behind choices (via anecdotes)
  - The significance of tool developer choices
- Differing views of protocol designers and operators (comparing RFCs to observations)
- Where more study and discussion needed
  - What operators want to know vs. what they have time to do
  - “Gaps” in documents, knowledge
  - Where tools/code differs from specification

First, Some Adoption Talk

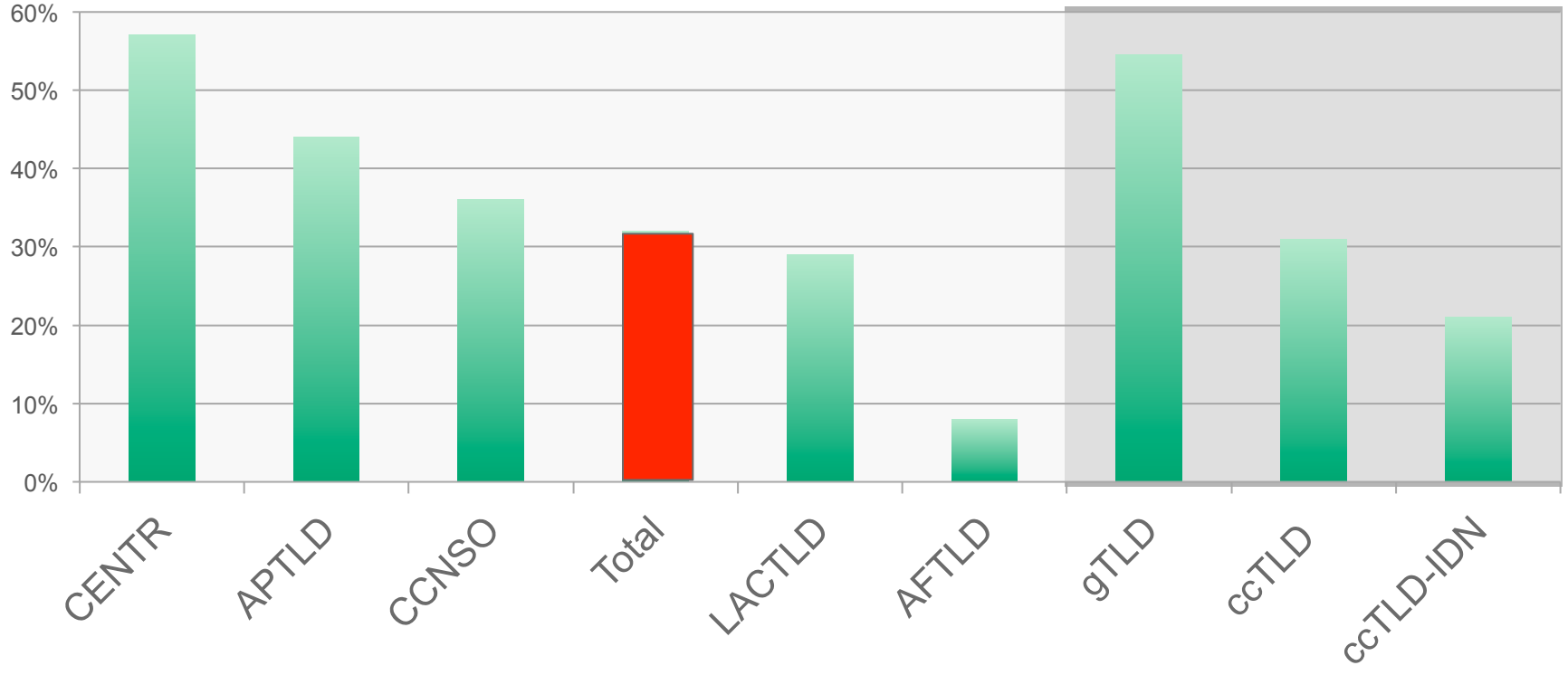


In Hard Numbers

- “Up and to the right”, reported quarterly
- The study has run for about 19 months
  - The number of zones increased from 299 to 306
  - This count excludes the 11 test zones in the root
  - Number of zones signed has risen from 64 to 99
  - Number of zones “completed” (DS record) is up from 59 to 89

Adoption by Category

» 32% of all TLDs (plus root) are signed. How does this compare to members of TLD organizations?



Key Management Study

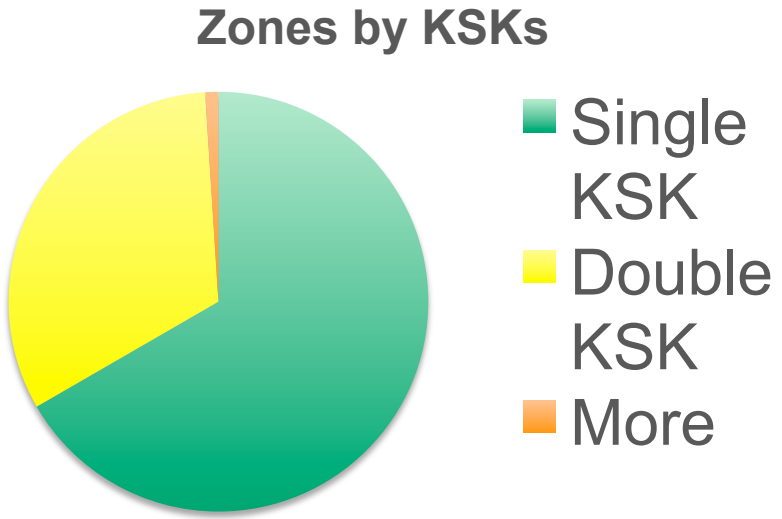
- Key Roles
  - Key Signing Keys and Zone Signing Keys
  - Presence of Emergency keys
- Cryptographic Choices
  - Algorithm and Bit Lengths
- Lifecycles
  - Durations of Key use

KSK, ZSK and Emergency

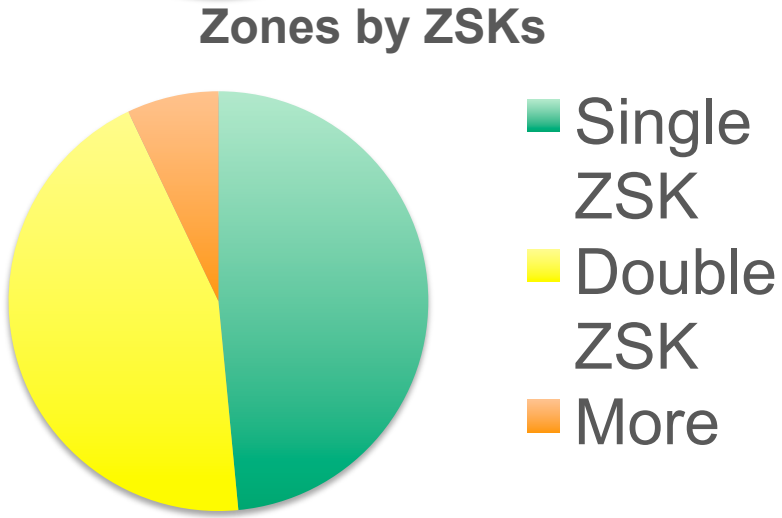
- Using “Key Signing Keys and Zone Signing Keys” is an operational choice, not a required part of the protocol
  - One TLD “joined the club” during the study
  - All TLDs make the choice to separate keys
- Publishing keys to be used in an emergency can quicken recovery but results in larger response sizes for DNSKEY
  - Not all TLDs publish emergency keys

Single/Emergency Keys

- For KSK, 67% choose to have a single KSK key



- For ZSK, the choice is split evenly



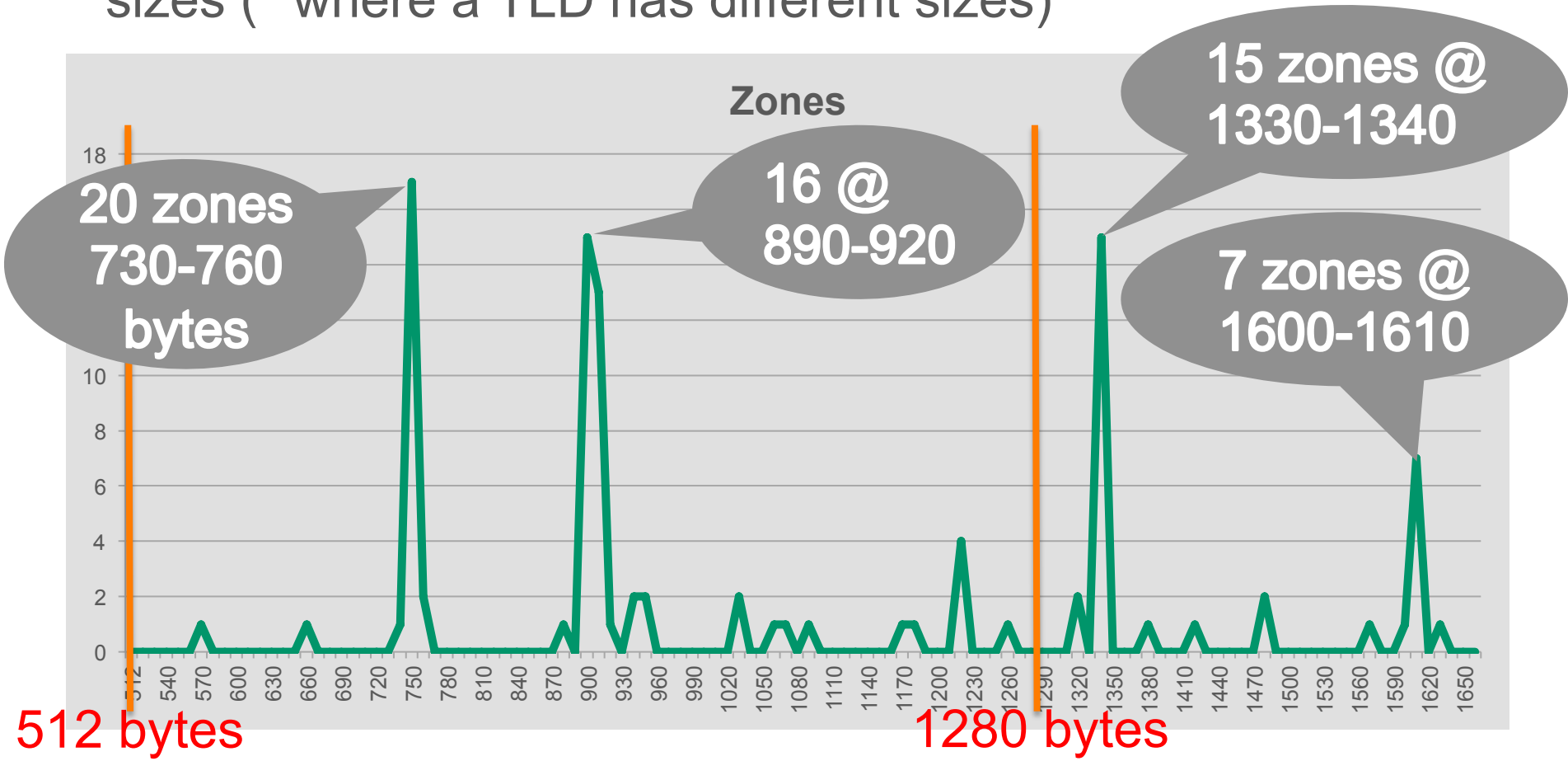
Why Not Emergency Keys?

- Extra keys take up extra space in responses
  - DNS works better with smaller responses

- Come to think of it, it's as good a time as any to look at the size of DNSKEY responses…

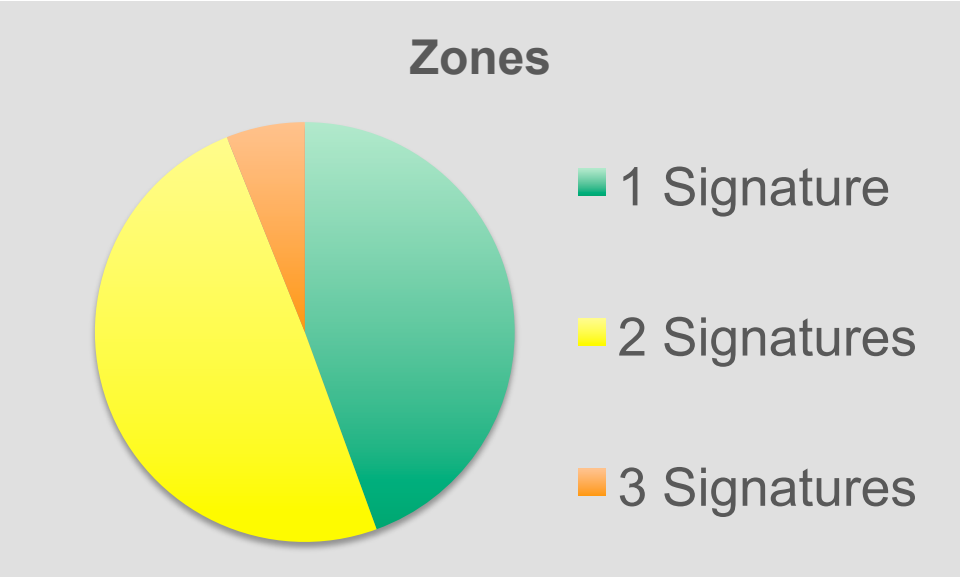
DNSKEY Response Sizes

» Looking *once* shows this distribution of smaller* response sizes (* where a TLD has different sizes)



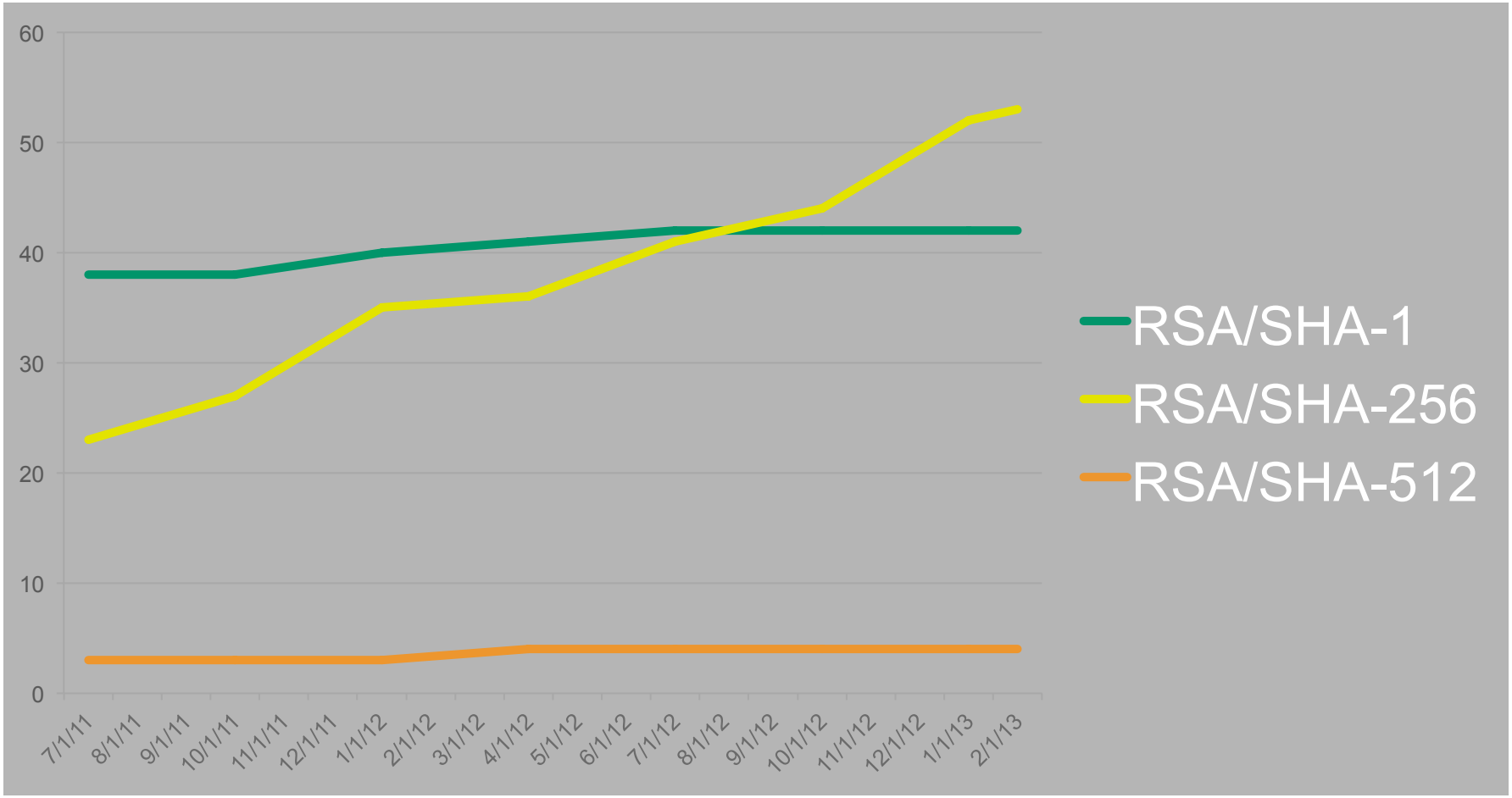
Signatures as a Size Factor

- Number of signatures on a DNSKEY set
  - This is an artifact of **tool choice** by the operators



- For the 3-sig zones, sizes were 1217 (x4), 1473, 1621 bytes

Cryptographic Algorithms



Choice of Cryptography

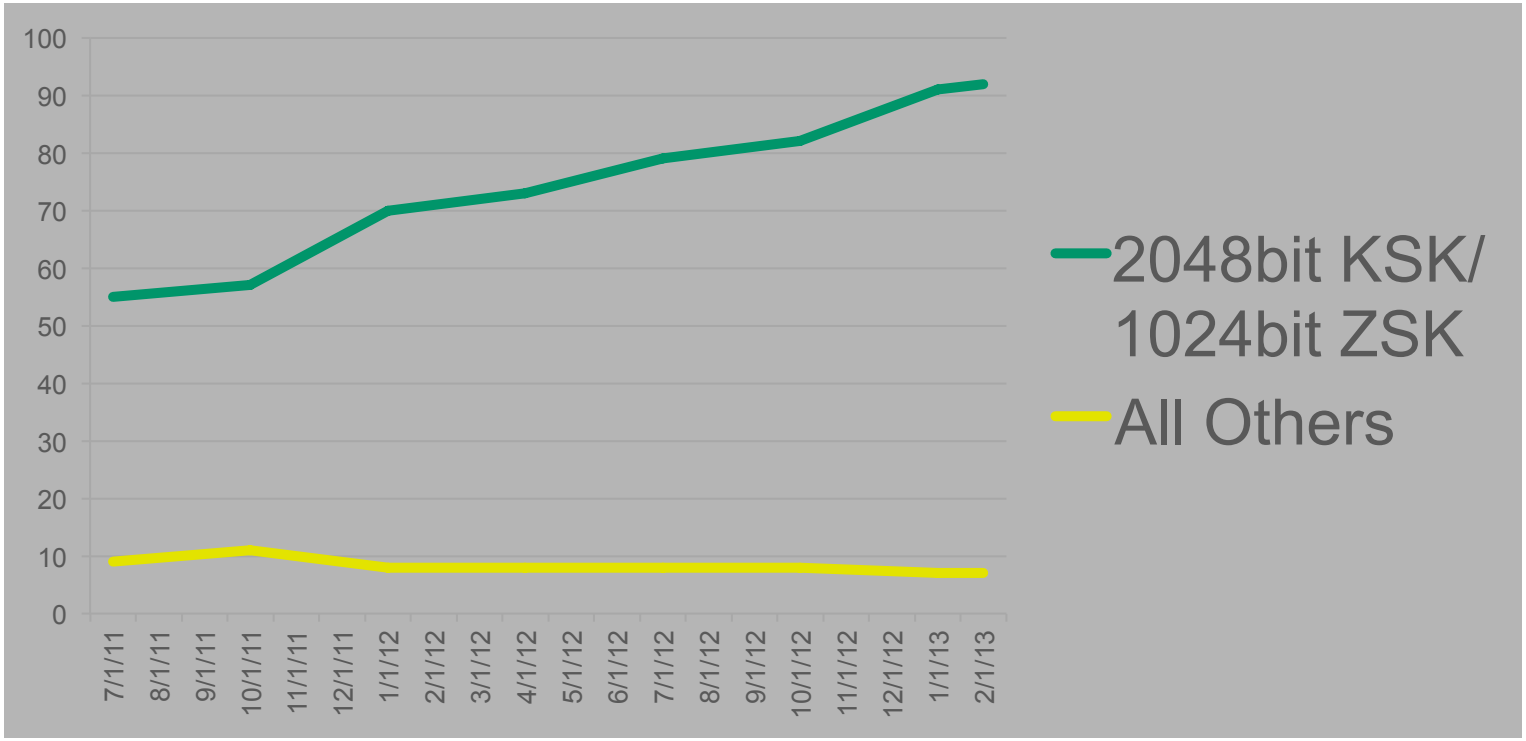
- Protocol is built to allow multiple algorithms/hashes in a zone
- But all operators uses just one algorithm/hash in a zone
- All upper zones use RSA for the algorithm but differ on the hash function
  - Over time a shift can be seen
  - SHA256 and SHA512 were documented (for DNSSEC) in 2009 after many zones started on SHA1 (documented in 2004)

Algorithm Changes

- Only four zones have changed algorithms, all from RSA-SHA1 to RSA-SHA256
- Of the zones starting DNSSEC during the study
  - 26 are signed with RSA-256
  - 8 are signed with RSA-SHA1

- About one quarter of the “new” (to DNSSEC) operators are starting out with the “old” stuff!

Key Lengths (in bits)



- The X-axis is “time” Y-axis is number of zones “complying”
- Yes, the green line is climbing and the yellow line is falling ***in absolute numbers***!

The Significance

- In RFC 4641, there is a suggestion to use 2048 bits for KSK and 1024 bits for ZSK.
  - RFC 4641 is not a requirements document, but customers see it as one
- Over time more DNSSEC zones adhere to these settings
- The growth is not only from new deployments but from old deployments “conforming” to the sizes

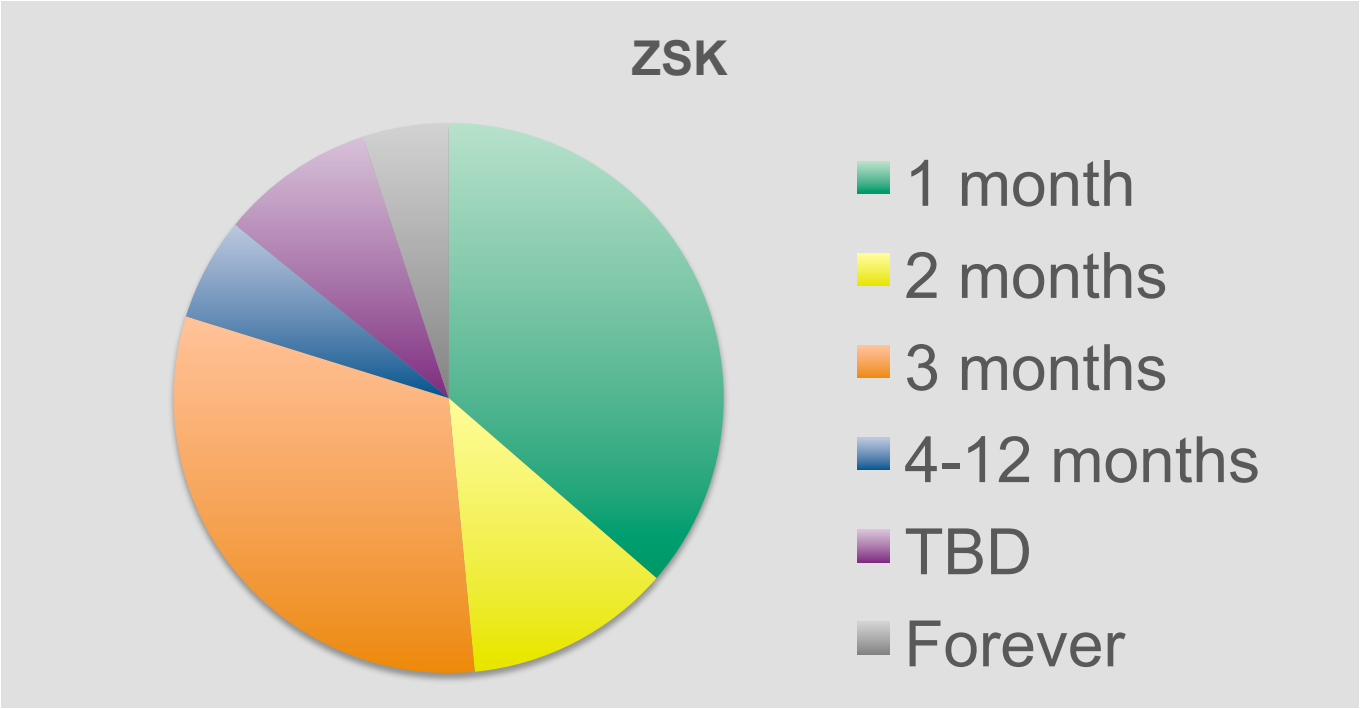
- These are the same operators that do not change the hashes!!!

One Operator's Story

- When I made this observation, one operator told me a story.
- His deployment had suggested a set of key sizes other than 2048/1024. A reason for this "other size" was a tradeoff in security versus response size.
- The review committee responded by selecting to "go with the 'normal' sizes of 2048/1024.
- Peer pressure rules!

Key Lifetimes

- RFC 4641 suggests that KSKs be used for a year and ZSKs for a month. "Suggests" in the same manner that the RFC suggested sizes. How do operators take this?



What about KSK Lifetimes?

- The study has tracked 193 KSKs
- Only 12 KSKs have been through a complete lifecycle in the 19 month study.
  - Only 7 appear to follow the 1 year recommendation, another appears to be a 6-month lifetime
  - The rest seem to be “tests” by the TLD (short duration)

- If operators intended to adhere to a 1 year recommendation, I’d have expected more
  - But all that can be said is “still not enough data”

Operator Adherence to Spec

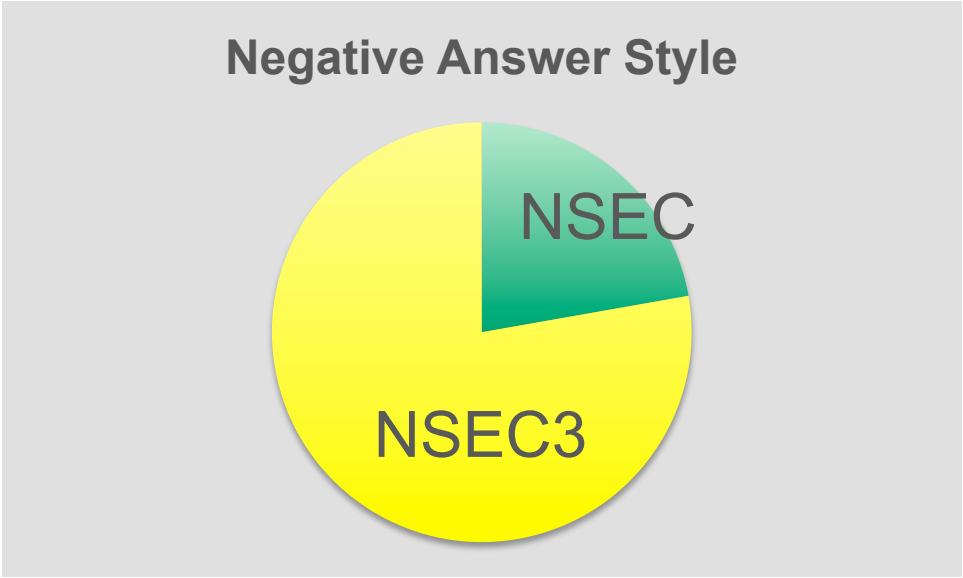
- Just to interject here, operators appear to
  - Make a decision at design time and stick with it (Algorithm)
  - Choose size numbers from specifications (Lengths)
  - Extend the time cycles from recommendations (Durations)
- When it comes to updates
  - Already operating zones tend to stick with the original
  - Some of the new deployments opt for the original
  - Are updates (meaning RFCs) as well-known?

Beyond Key Management

- Negative Answer Choices (NSEC/NSEC3, etc.)
- DS Record Choices

NSEC vs. NSEC3

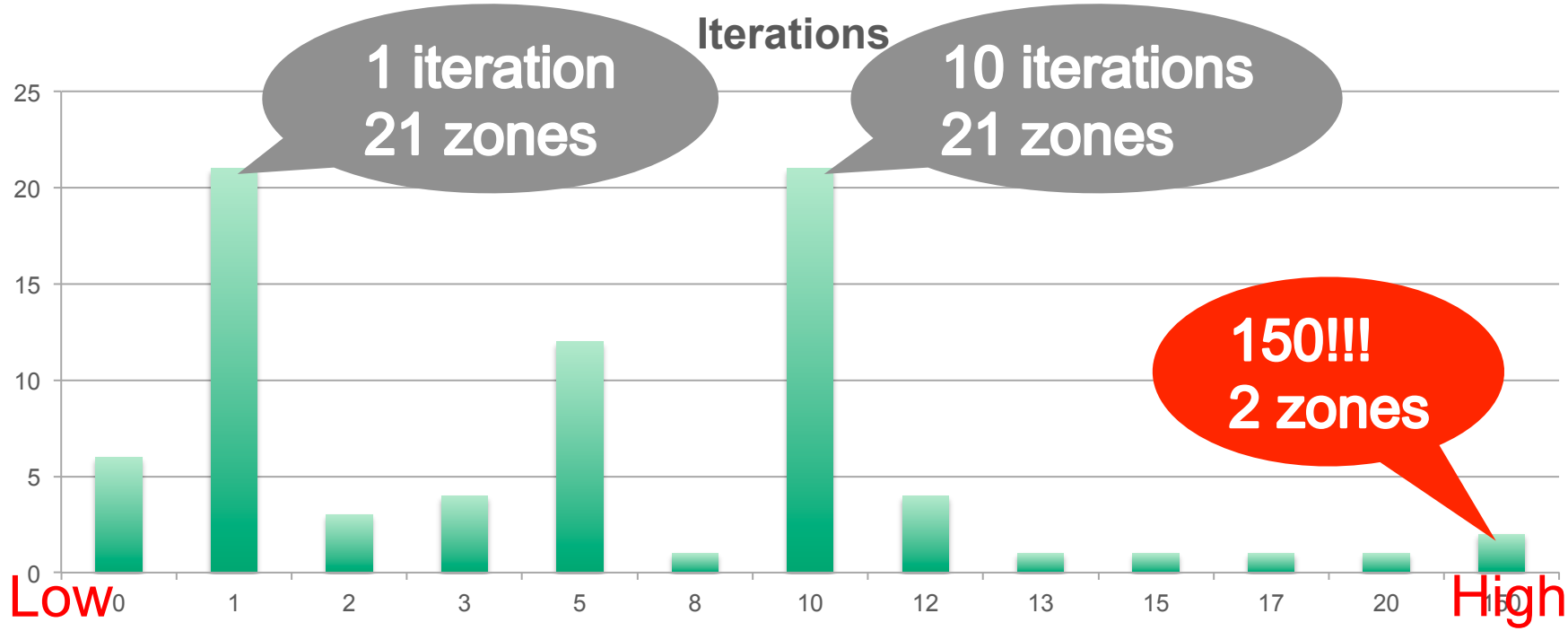
- First there's the choice between NSEC and NSEC3



- TLDs benefit more from NSEC3 than other zones
- Now, let's look at NSEC3 parameters

NSEC3 Iterations

- Iterations: the number of times the hash function is called
- RFC 5155 says this should be low and gives a hard upper limit of 150 (for a certain key size)

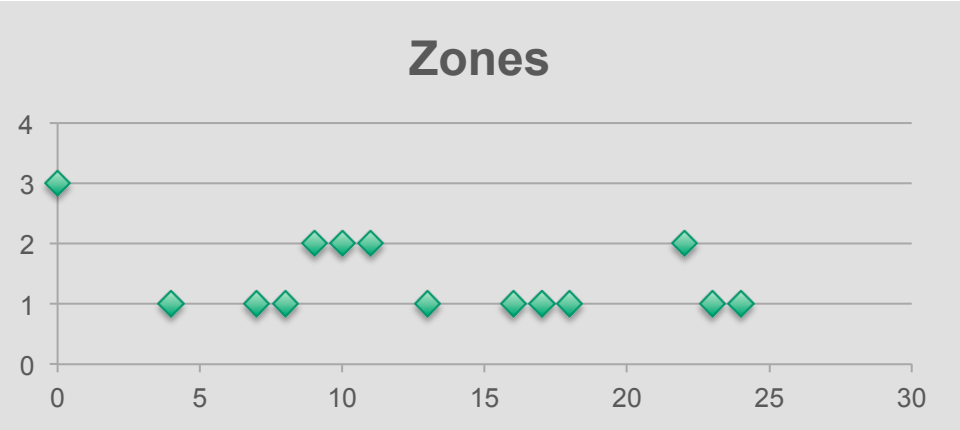


NSEC3 Salts

- RFC says “change every resigning” (but no one “re-signs”)
- Popular lengths: 0,4,8,16 (hex characters)
  - No guidance, but we like “round” numbers!
  - Interesting values: BA5EBA11, BADFE11A, 5CA1AB1E

DS Records

- How long does a zone wait to add DS records (“complete DNSSEC”)?
  - 29 were observed, 9 took more than a month. The chart shows the distribution of those adding within a month



- The “average” delay is getting longer as more zones sign
- And zones signing without adding DS is growing too

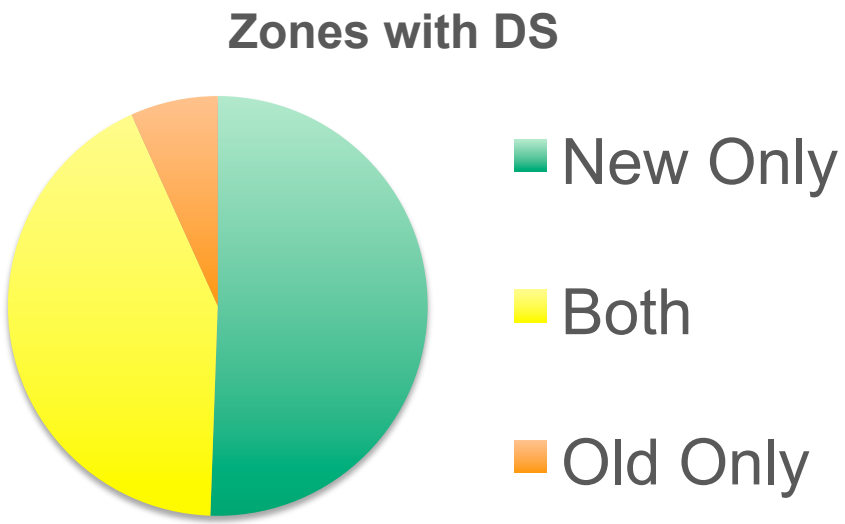
Question: Emergency DS?

- During discussions over the study one person asked whether any TLD pre-registered a DS record in case of an emergency.
  - I.e., has there been a DS record in the root that did not point to a DNSKEY in a TLD?

- The answer is: only one TLD has put a DS record into the root zone this way
  - It took a lot of time to find it!

Support for DS hashes

- RFC 4509 defines a new hash for DS records and recommends that old hashes be kept for backwards compatibility



- “New Only” and “Old Only” force clients to support old and new, this is not good for transition!

The Last Slide

- What has been learned?
  - Study how something is deployed…is interesting
  - Operators rely more on tools than on specifications
  - There are still gaps in knowledge about DNSSEC and the cryptography it uses

- It would be nice if there were documents describing “Best” or “Good” Current Practices as “buying guides” as a replacement for not having true specifications