# Statement Of Needed Internet Capability: Trust Anchor Repositories

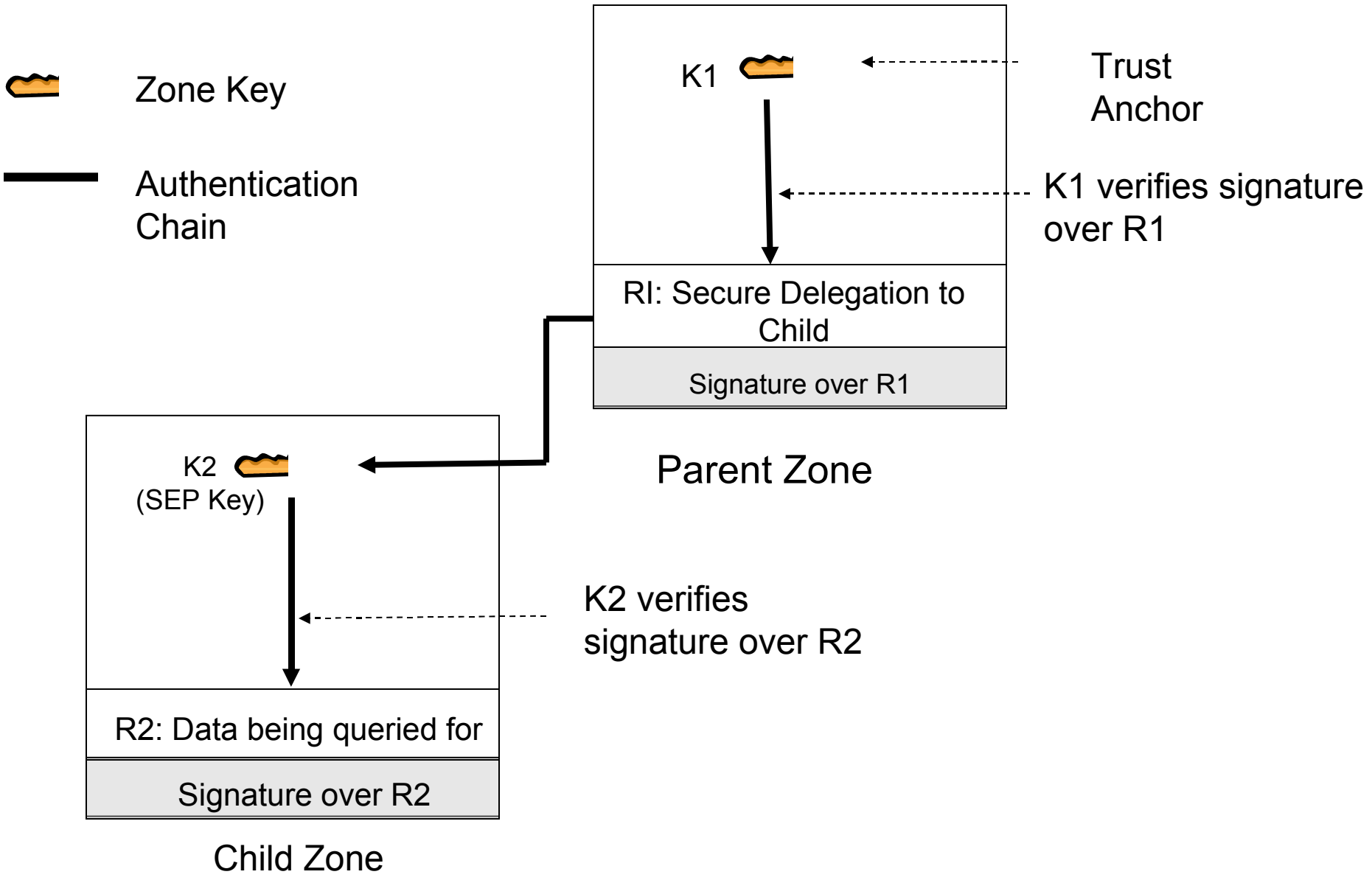
Prepared by:

SPARTA, Inc

Shinkuro, Inc

National Institute of Science and Techology

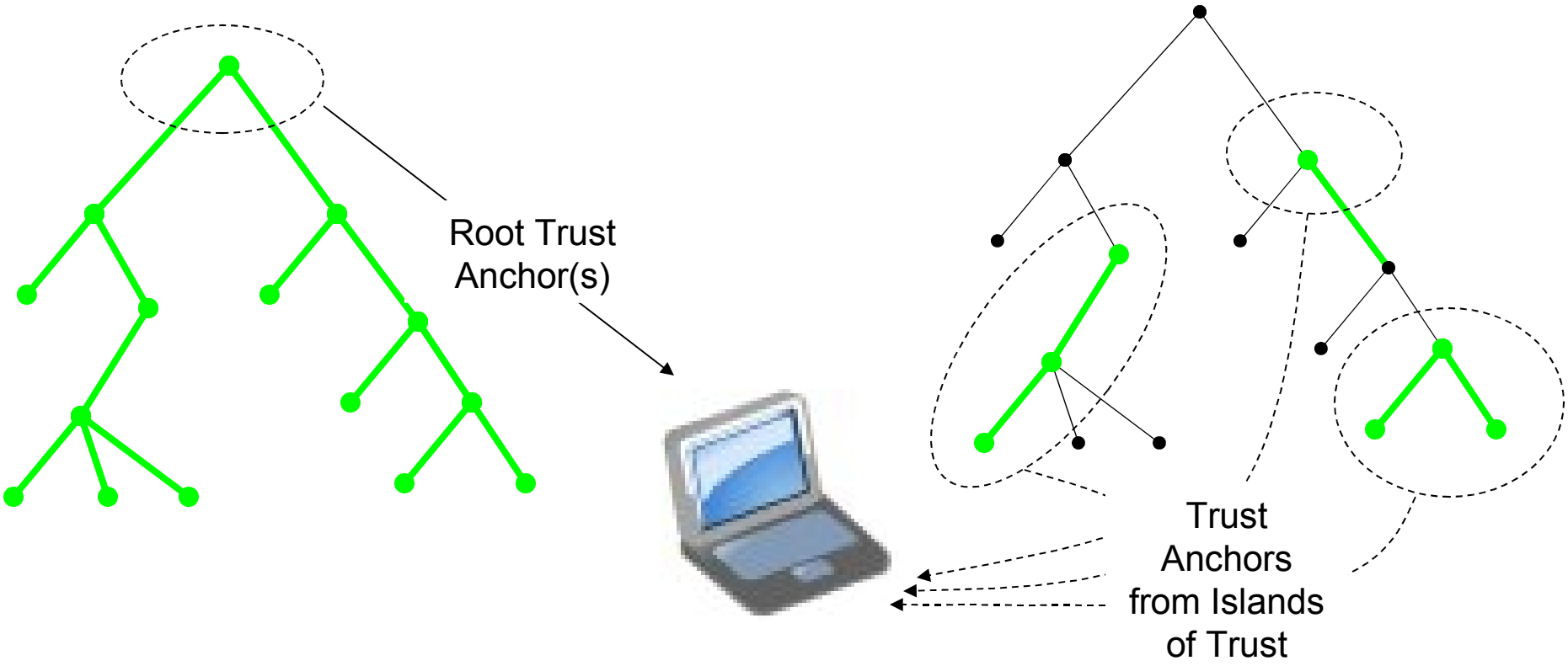
# DNSSEC Authentication Chain



# DNSSEC Trust Anchors

- Starting point for DNSSEC validation
- Choice of trust anchors is a local decision
  - Bad choice of trust anchors can completely undermine value of DNSSEC
- In the absence of a valid secure delegation from the parent zone to the child zone, a validator MUST have trust anchors for the child zone in order to be able to validate names from (and below) it.

# Number of Trust Anchors



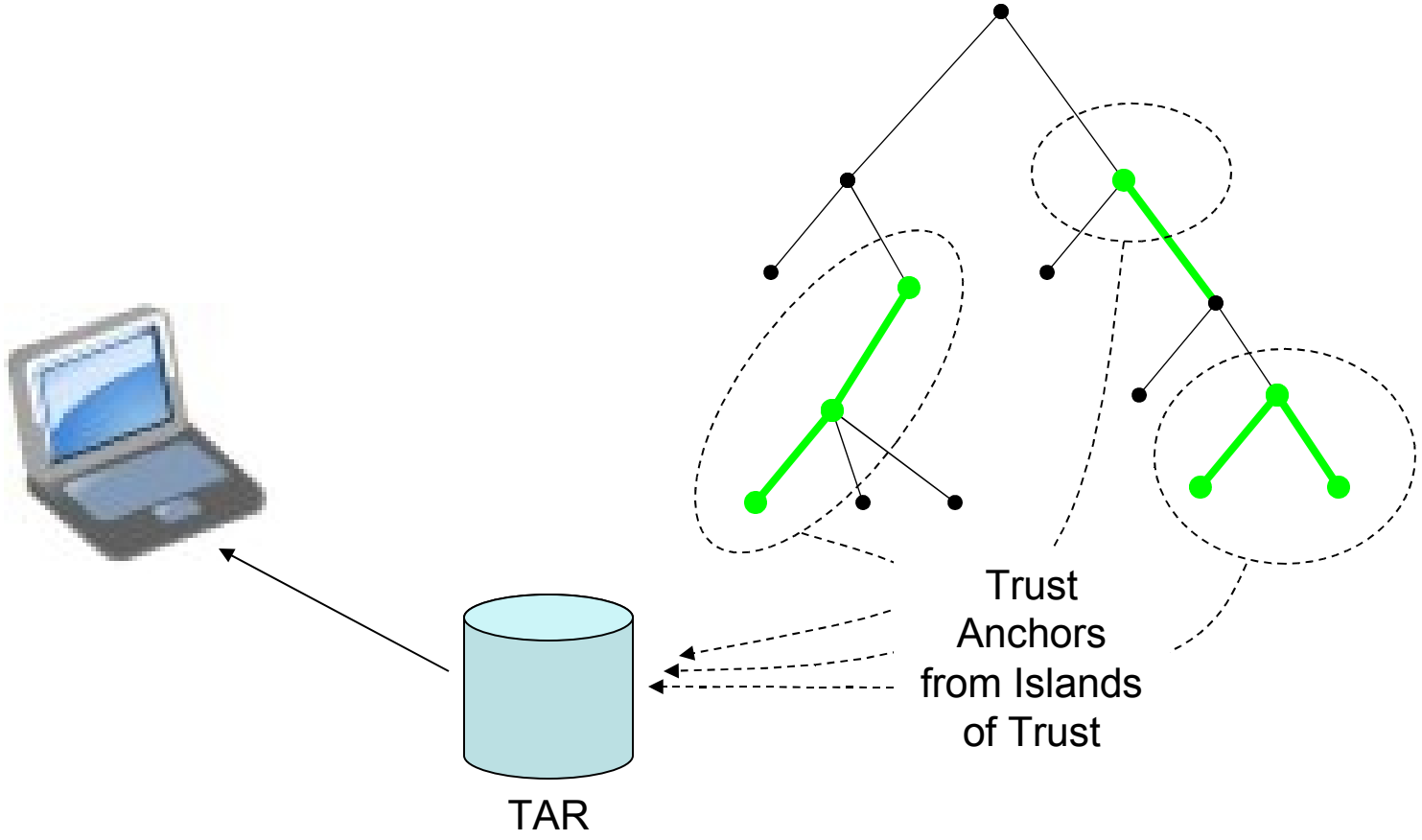

**Ideal**: Entire DNS Tree is signed

**Reality**: DNS Name Space is fragmented into a (potentially large) number of “islands of trust”

# Trust Anchor Repository

- A trusted DNS resource record store that contains SEP keys for one or more zones
- Provides the means for a DNSSEC validator to fetch Trust Anchor information for zones in some reliable manner without requiring the validator to maintain this information locally
- Makes the problem of managing a large number of Trust Anchors tractable
- Important to note that gaps in the signed name space can be anywhere, so the problem does not go away if the Root is signed
- In fact, the need for a TAR is more pronounced at lower levels in the DNS tree, where the potential number islands of trust can be much larger

# Trust Anchor Repository (cont.)



# Types of TARs

- Global TARs are TARs that are used as a deployment aid for the global Internet
  - Their existence is well-known
  - Operators are assumed to be clueful - have credibility within the Internet community (any arbitrary TAR set up on the Internet is not considered a Global TAR by this definition)
- Community of Interest TARs
  - Operated for a subset of zones
  - Will exist as long as the parterships within the community exist
- Enterprise TARs
  - Used within enterprises for  storing “internal” trust anchors or to mirror intra-organizational trust relationships
  - Mix between COI TARs and Global TARs
- Our focus is on Global TARs

# Arguments Against Global TARs

- It will reduce the need for parent zones to support DNSSEC
- Zones that currently publish SEP key information in the TAR will not see a need for switching over to using the parent
- TAR registration represents an additional burden for the zone owner
- A TAR, once established, will refuse to go away

# The Status Quo

- TARs have not (yet) been seen as a necessary evil for DNSSEC Deployment
  - No serious discussion of it during DNSSEC training sessions/workshops, for instance
- Many parent zones/registries are still waiting for the necessary market pressure in order to deploy DNSSEC
- In the absence of a compelling business case, DNSSEC continues to (mostly) progress slowly in a bottom-up fashion
- We're waiting for market pressure, but at the same time many zone operators are are not seeing the benefit with signing their zones if there is no way for an arbitrary validator to begin using their signed data

# Document Outline and Goals

- Assume that the availability of one or more Global TARs is a necessary evil for driving DNSEC Deployment in the Internet
- Outline the different architectural, operational and organizational models for a Global TAR and describe their properties
- Classify the different “flavors” of TARs currently in existence, under one of these models
- Lay the foundation for helping the community decide the architectural, operational and organizational approach that will favor DNSSEC deployment the most

# General Considerations

- Approach should encourage and cooperate with DNSSEC “aggregation points”
- Simplicity is important
- Should support DNSSEC Deployment on the main tree

# Architectural Alternatives - SEP Key Acquisition

- Option 1: Registration Scheme
  - Zone owner registers SEP Key information with TAR
  - E.g. ISC DLV Registry (https://secure.isc.org/index.pl?/ops/dlv/)
- Option 2: Lookup Scheme
  - Tar operator identifies new islands of trust and gathers SEP key information (may or may not ask the zone owner for permission before registering a SEP key)
  - Light-weight scheme, but can have some assurance mechanisms built in
  - E.g. SecSpider (http://secspider.cs.ucla.edu/) and the IKS Jena Survey (http://www.iks-jena.de/leistungen/dnssec.php)

# Architectural Alternatives - SEP Key Distribution

- Option 1: Use the DNS to store SEP keys
  - The TAR is identified by its domain name
  - Use DNSSEC to validate SEP key information obtained from the TAR (use the TAR's SEP key as a trust anchor)
  - E.g. DLV (RFC 5074)
- Option 2: Use some secure data distribution mechanism
  - Validating client will have to check the authenticity of data and will have to merge data with existing trust anchor information in the client
  - E.g. Use an SSL channel to distribute set of keys

# Architectural Alternatives - Multiple TARs

- Multiple instantiations of the same TAR
  - Managed by single organization, adds redundancy
- Multiple independent TARs containing the same information
  - Multiple TARs managed by independent organizations, but with high level of cooperation.
  - Need to make sure that data is always consistent across all TARs
- Multiple independent TARs
  - Multiple TARs managed by independent organizations.
  - Can evolve into a troubleshooting nightmare
- Distributed TAR
  - Decentralized operation; management of portions of the TAR is delegated to other entities

# Operational Alternatives - Registration Policy

- Option 1: Open Registration
  - Informal checks, low barrier to entry
  - Low assurance on the integrity of data in the TAR
- Option 2: Registration with Strict Checking
  - Stringent checks applied uniformly for all registrants
  - Higher barrier to entry for zone owners not accustomed to running these checks
- Option 3: “Same as Parent”
  - Match the rigor of checking to that currently being done by the zone for registering information with its parent
  - TAR will need to support various registration schemes

# Operational Alternatives - SEP Key Phase Out

- Option 1: Self Directed
  - TAR automatically removes (or suspends registration of) SEP keys for a domain when its parent zone appears to support DNSSEC.
  - False positives possible -- parent may not, actually, be ready
- Option 2: Parent Directed
  - Parent says when it is ready
  - Need to ensure that the current SEP keys from the TAR are properly migrated to the parent zone
- Option 3: Threshold Based
  - Stop registration if number if number of entries under a particular domain reaches a useful threshold
  - Allow market pressure to dictate future course of action

# Operational Alternatives - TAR Phase Out

- Option 1: Threshold Based
  - Number of entries in the TAR has dropped to some low threshold
- Option 2: Flag Event
  - A set of large/influential TLDs sign their zones

# Organizational Considerations

- Is the candidate organization internationally accepted and willing to provide transparency in its operations?
- Does the candidate organization have the necessary institutional knowledge?
- How will the candidate organization fund the effort?
- Will any of the technologies being used require any operating licenses?
- Who will provide the client side software?
- What is plan for gaining traction
  - Encouraging SEP key registration in TAR initially
  - Facilitating update of DNSSEC in the main tree thereafter
- Does the candidate organization have its own flag date for ceasing operation of the TAR?

# Closing Thoughts

- Is there value in having a Global TAR for the Internet?
- Are existing solutions sufficient for implementing the TAR or do we need something new?
- Is there a useful lifetime for this TAR?