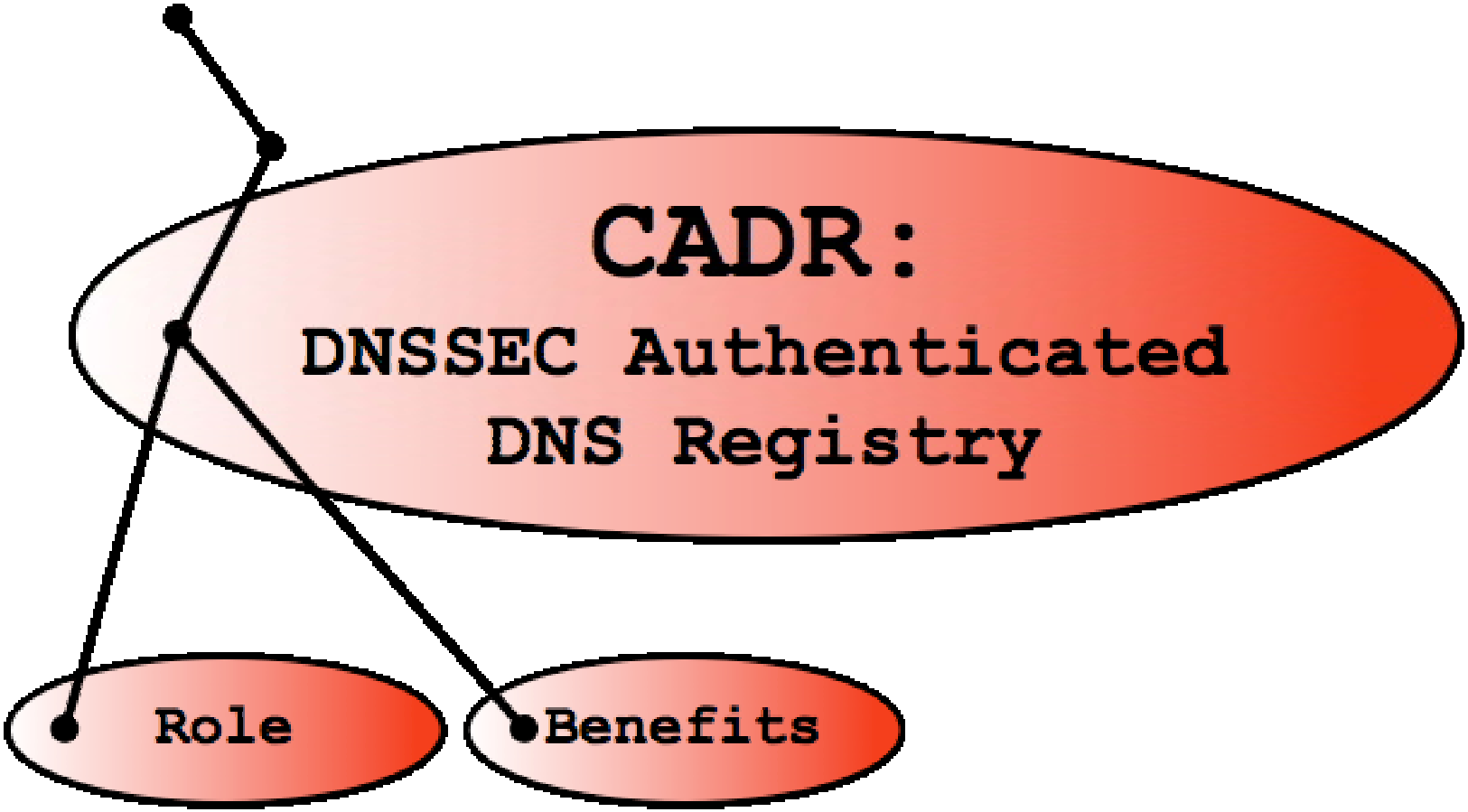


$Id: cadr-title.graffle,v 1.1 2005/09/04 09:56:52 johani Exp $

johani@axfr.net and **bmanning@ep.net**

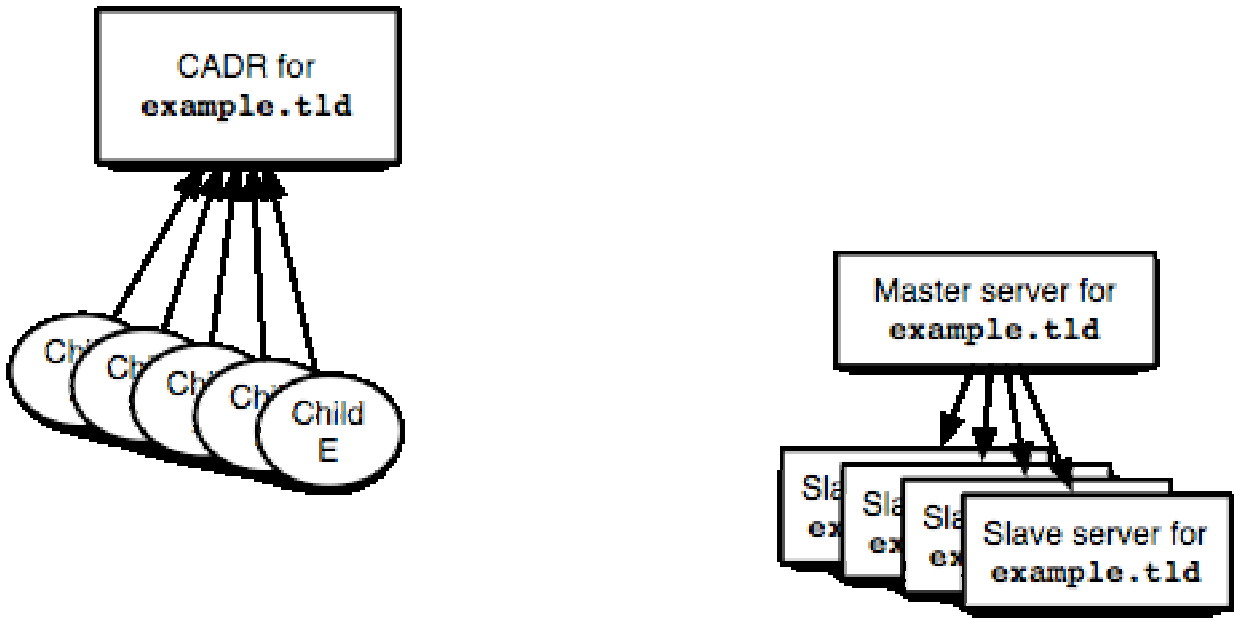
What is CADR?

- CADR is a registry for DNS data
  - i.e. CADR is a tool in the same ballpark as registries run by TLDs to manage delegation information
  - or, in some environments, run by registrars to manage delegation information for customers for further propagation to a registry (typically for a TLD)
- CADR is different from other registries by utilizing the in-band authentication of DNS data provided by DNSSEC
  - this enables a new level of simplicity in the management of the parent-child relation at a zone cut (aka a delegation point)
  - i.e. CADR is leveraging from DNSSEC to make the registry **simpler**

Why CADR?

- I believe that with DNSSEC the complexity of managing a zone, especially a zone with children, will be daunting enough that people will move away from the model of “flat text file” over to some sort of DNS management system
  - if there are delegations such systems are usually called “registries”
- I.e. I see a need for “registries” not only on the TLD level (where we already have them), but also further down
  - if we just get the software right then running a registry for “**`example.tld`**” should be **easier** than managing it via a plain text file and an editor

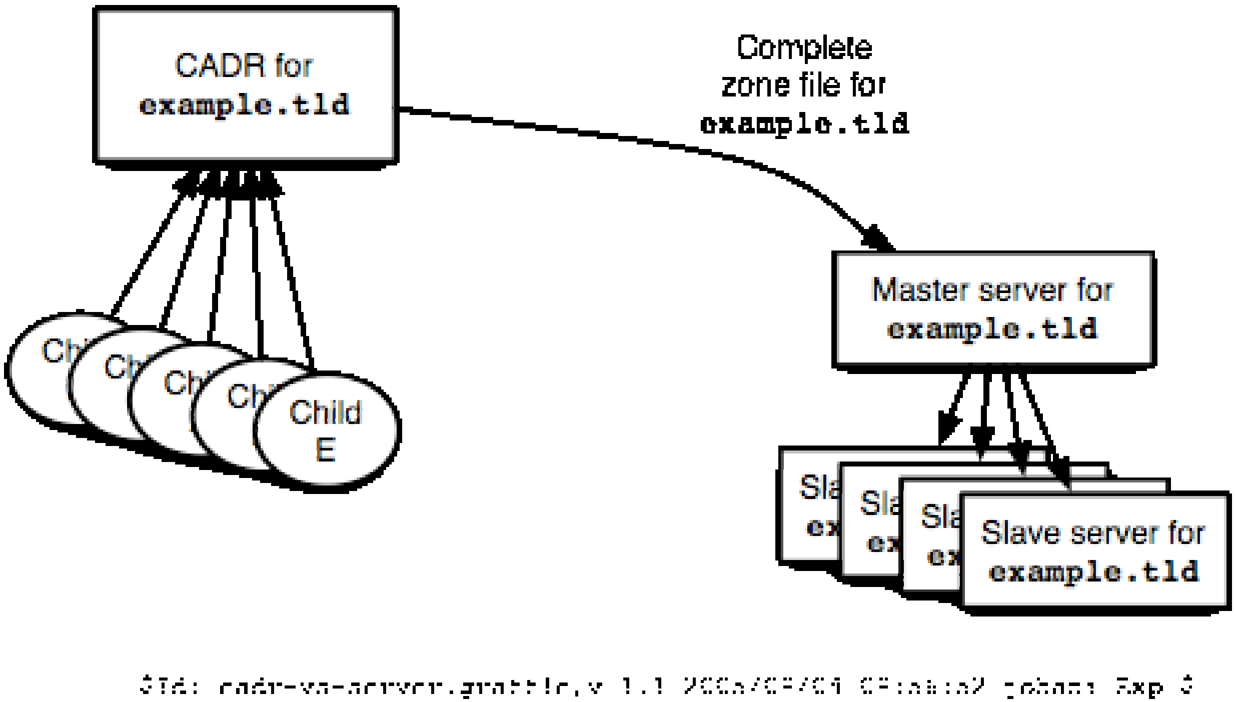
What is the role of CADR?



$Id: cadr-vs-server.graffle,v 1.1 2005/09/01 09:38:37 johani Exp $

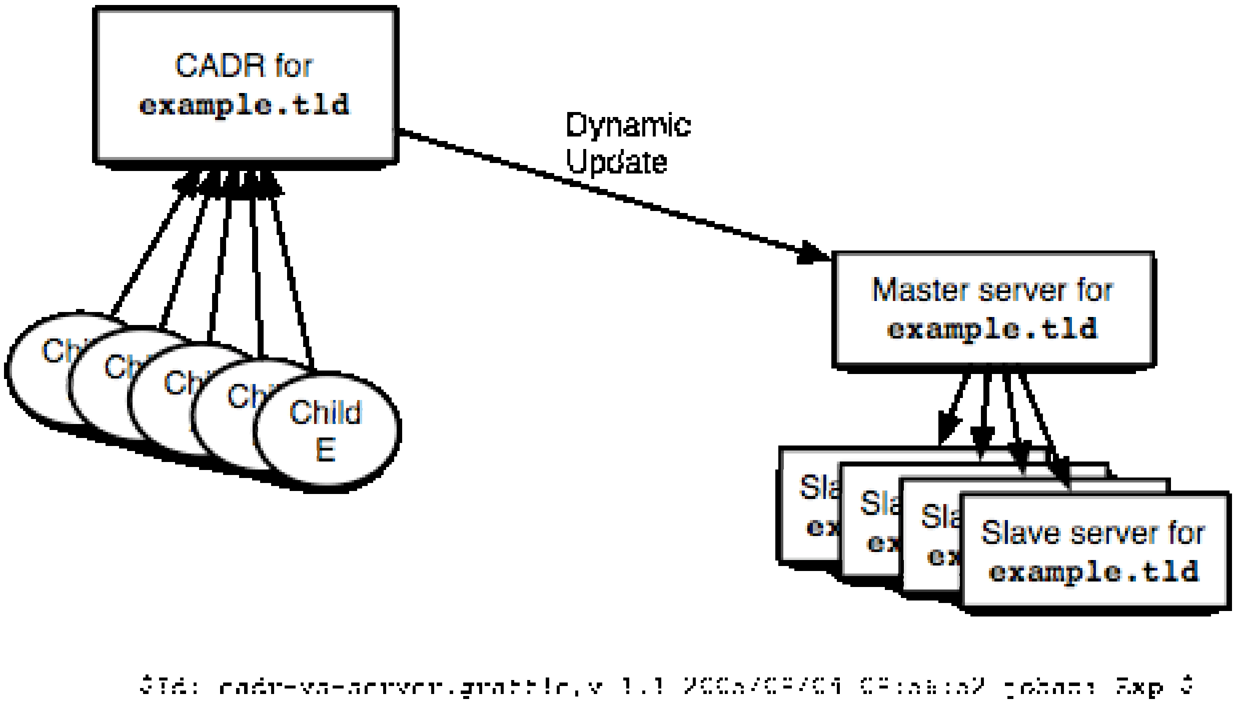
- Given that children can update their delegation information in the CADR registry, how should this update be communicated to the parent nameservers?

What is the role of CADR?



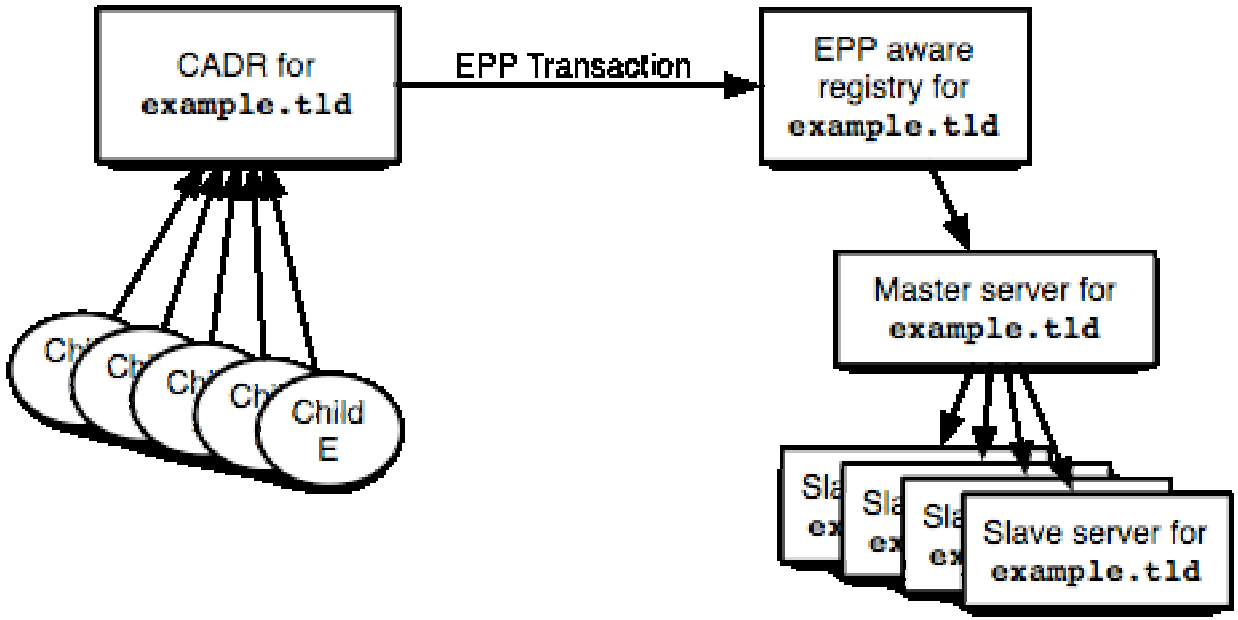
- One alternative (the most obvious one perhaps) is to just export the entire zone file.

What is the role of CADR?



- Another alternative is that the CADR registry sends a (secure) dynamic update to the nameserver infrastructure
  - there are pros and cons of this, but it **is one** of the possibilities

What is the role of CADR?



$Id: cadr-va-server.graffle,v 1.1 2005/09/01 09:38:37 johani Exp $

- The final alternative is to communicate the update from CADR to an EPP aware registry for the parent zone
  - most relevant for the registrant -- registrar -- registry model of many TLD zones

Benefits of the CADR model?

- "Traditional DNS" is very often misconfigured in various ways.
  - one of the most common sources of errors is the management of the delegation information for a child zone in the parent zone
  - typical stats indicate that around 15-25% of the delegations are more or less broken in this area
  - major causes of the problems are
    - entry of same information in multiple places (both child zone and parent zone)
    - authentication of child to parent for changes is complicated

“Synchronize parent!”

- The reason for entering the same information in both parent and child (instead of just copying when needed) is the absence of proof of the integrity of the data
  - i.e. the parent could easily look up the delegation information for the child in the public DNS, but it cannot **trust** the information to be correct
  - this assumption no longer holds true when we deploy DNSSEC
- With DNSSEC it is suddenly possible to prove (to the parent) that the information about the child in the public DNS is authentic and can be depended upon directly
  - this enables us to switch to the new model “synchronize parent” (i.e. in-band copying of delegation data from child to parent)

Assumptions of CADR

- We sort of assume that the child is signed with DNSSEC
  - well, not really
  - the requirement is that the “apex” of the child zone is signed
    - i.e. CADR needs a DNSSEC signature over the NS RRset in the child to be able to verify that it is authentic and hasn’t been tampered with
- The rest of the child zone **may** be left unsigned if child doesn’t want to do DNSSEC yet

Next Steps

- The goal is to contribute a complete CADR system to the community as open source
  - we're not quite there yet, more work is needed to polish this off as a piece of software useful to others
- There is significant functionality that is not yet implemented. Some examples (not a complete list):
  - "host records" (i.e. a way to manage out-of-zone glue in a CADR context)
  - EPP backend
  - Dynamic Update backend
  - Ability to manage several "parent zones" in one CADR
  - Child-side DNSSEC GUI tool that is able to communicate with the CADR parent

Thanks!

- Johan Ihrén --- **johani@axfr.net**
- Bill Manning **--- bmanning@ep.net**