Transaction SIGnature (TSIG) using CGA Algorithm in IPv6

draft-rafiee-intarea-cga-tsig

Authors: Hosnieh Rafiee

Martin v. Löwis

Christoph Meinel

IETF88

Intarea WG

Vancouver

November 4, 2013

Problem Statement

- Authentication during DNS query processes
  - No Security Mechanism
    - Solely based on the source IP address
  - Security Mechanisms
    - TSIG
      1. Compromised shared secret
      2. Generate shared secret and exchanging it among a group of hosts offline
      3. Generating a new IP address to maintain privacy (clients) needs to repeat step 2.
    - DNSSEC
      1. Client to recursive resolvers (not efficient to use DNSSEC because of configuration required on both sides)
      2. Sign the zone offline

Motivation

- **Reduce human intervention & secure DNS authentication during DNS query processes**
  - DNS update
    - Dynamic DNS update
    - Zone transfer
  - Authoritative to Recursive DNS servers
  - Recursive servers to stub DNS clients

- **Provide means for FQDN and ptr update for clients on DNS servers**
  - Dissimilar to DHCPv6, There is no option to update FQDN when NDP is used for an IP address generation

What is CGA-TSIG?

- Secure authentication
- Eliminate the human intervention or reduce the human intervention
- Use RFC 3972 (CGA) or SSAS (draft RFC) to provide the proof of IP address ownership
- Ensures the integrity of the messages (signing messages)

Old private key

Sign(IP address, timestamp)

new private key

Sign(update message)

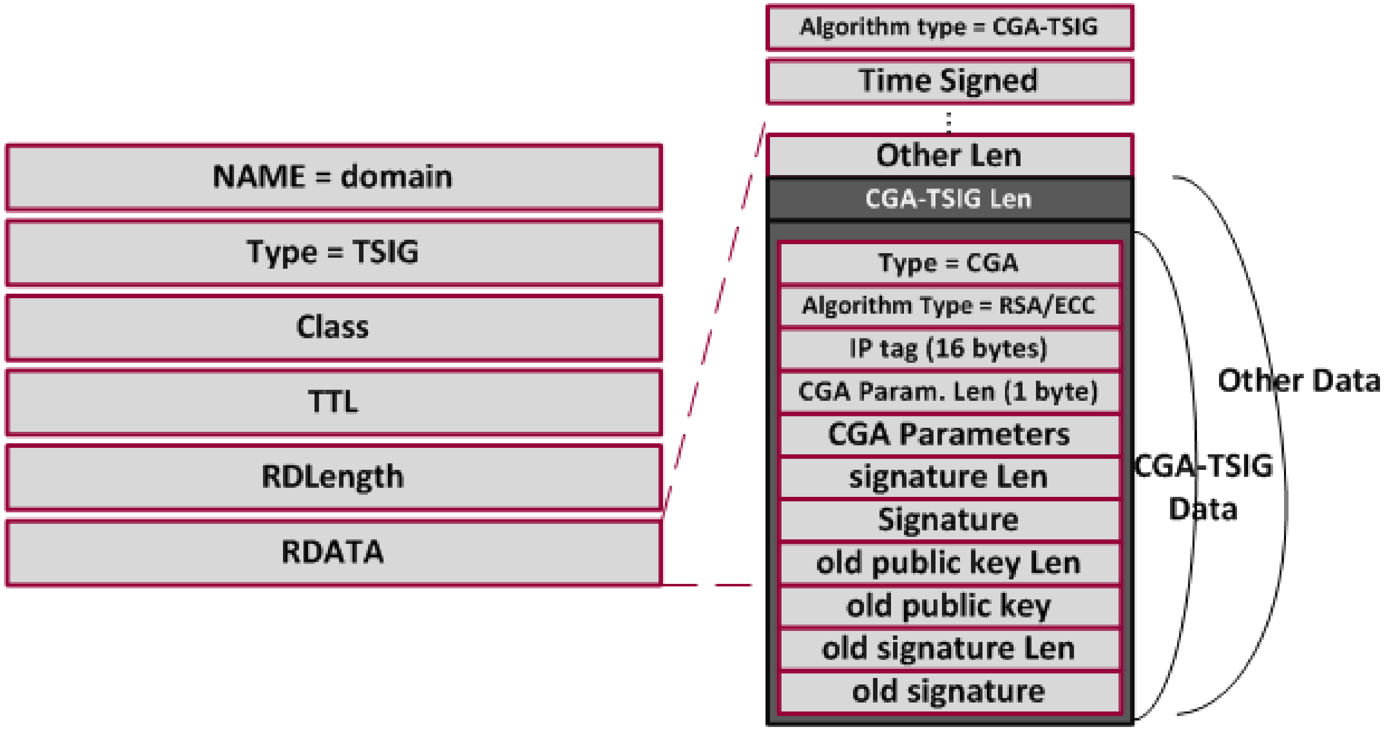
- Provide a means to authenticate the node after this node changes its IP address without increasing administrative operations

Threat Model

- IP spoofing
    - CGA/SSAS would provide the proof of IP address ownership
- DNS dynamic update message spoofing
    - Verify the signature
- Resolver Configuration attack
    - No need further configuration and avoid human errors
- Exposing shared secret
    - There is no shared secret in CGA-TSIG. If any node compromised only the compromised node changes its IP address
- Replay Attacks

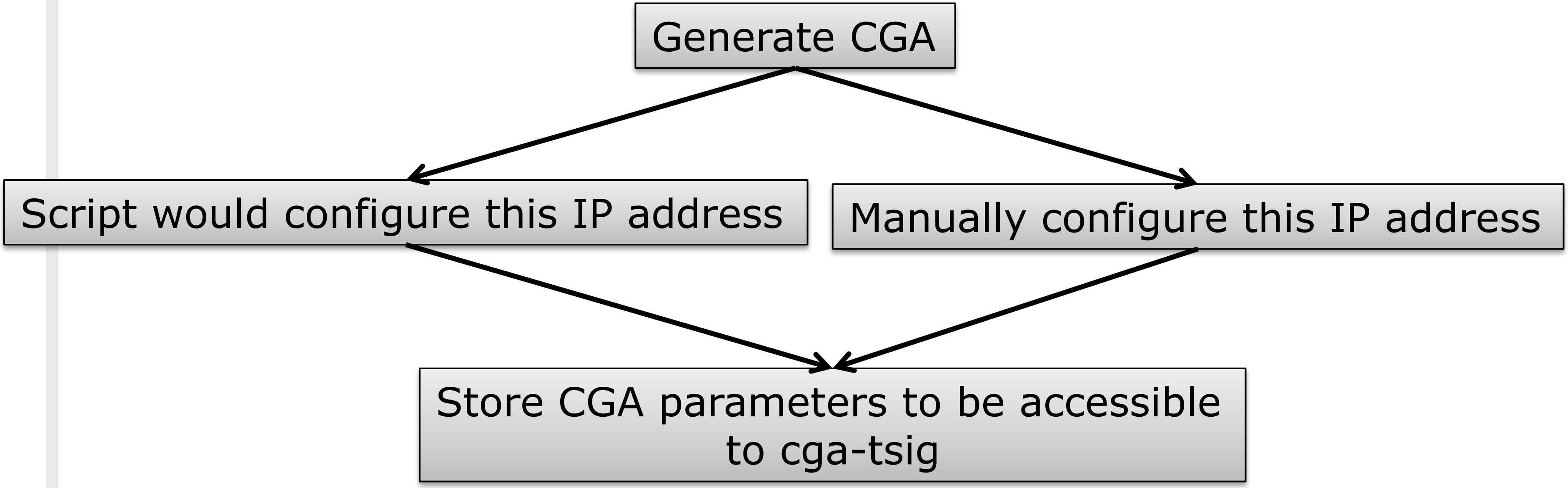
Is it a new Resource Records?

- No, it is a new algorithm in TSIG RDATA (other options section)



What if the node does not support CGA?

- The node can generate its keypair itself and sign the message (Not recommended in recursive resolver to client authentication)
- Use a small script for CGA generation


Generate CGA
Script would configure this IP address
Manually configure this IP address
Store CGA parameters to be accessible to cga-tsig

Modifications and Commented applied

- Explaining the secure authentication during different scenarios such as resolvers to clients, zone transfer, FQDN, etc.
- Clarifying the problem statement section
- Including terminology
- Remove typos

□ Does intarea want to adopt this draft as a WG draft?