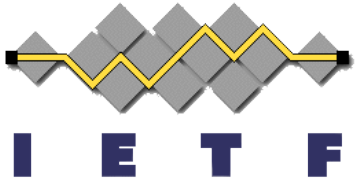


Secure DNS Authentication using CGA/SSAS Algorithm in IPv6 (CGA-TSIG)

draft-rafiee-intarea-cga-tsig

Presenter: Erik Nordmark

Arista Networks

Authors: Hosnieh Rafiee
Ciber AG, Germany

Martin v. Löwis, Christoph Meinel
Hasso Plattner Institute, Germany

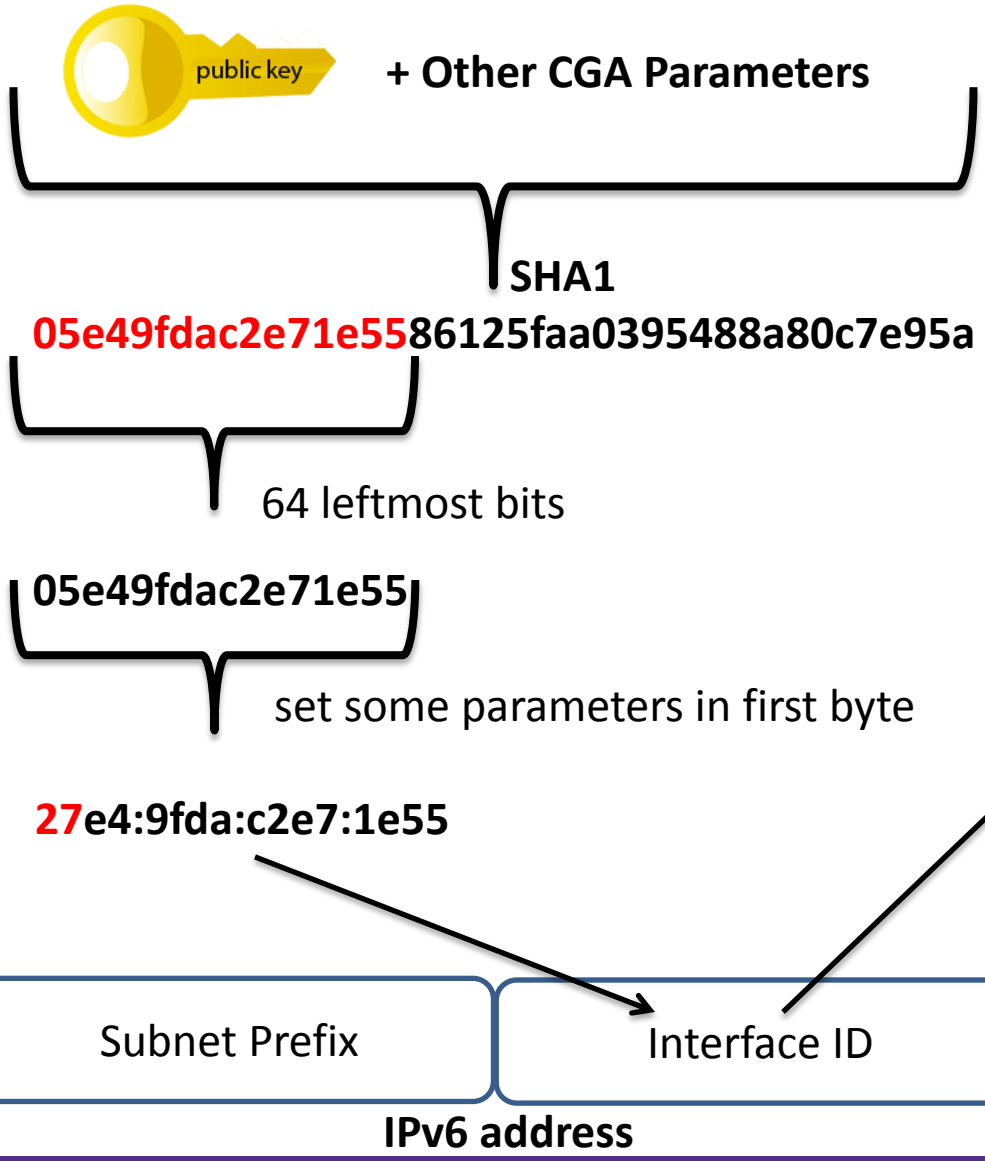
IETF89
Intarea WG
London
March 4, 2014

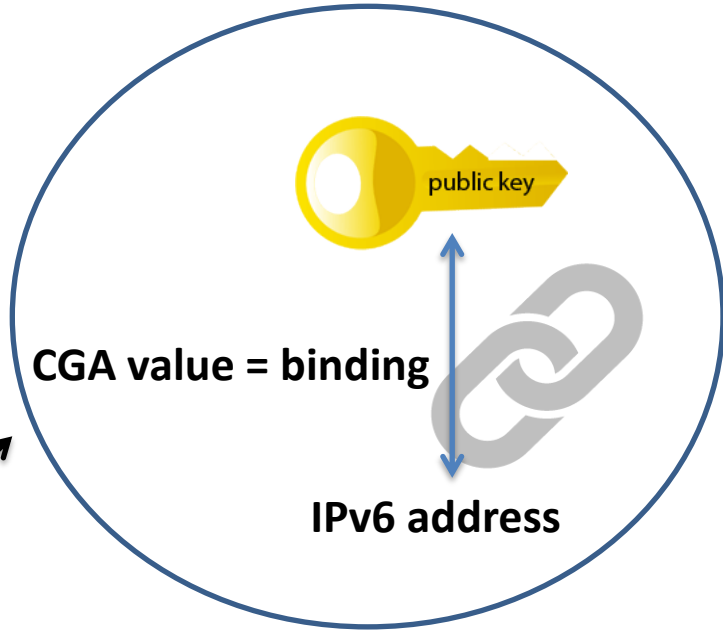
ciber®

CGA-TSIG/CGA-TSIGe Purposes

- Secure authentication
  - Eliminate/reduce human intervention
- Prevent IP spoofing and several other attacks
  - Use RFC 3972 (CGA) or SSAS (draft RFC) to provide the proof of IP address ownership
- Provide data integrity
  - Sign the messages using a private key and verify the signature using a public key that binds to the node's IP address
- Provide data confidentiality
  - Encrypt the packet using a secret key

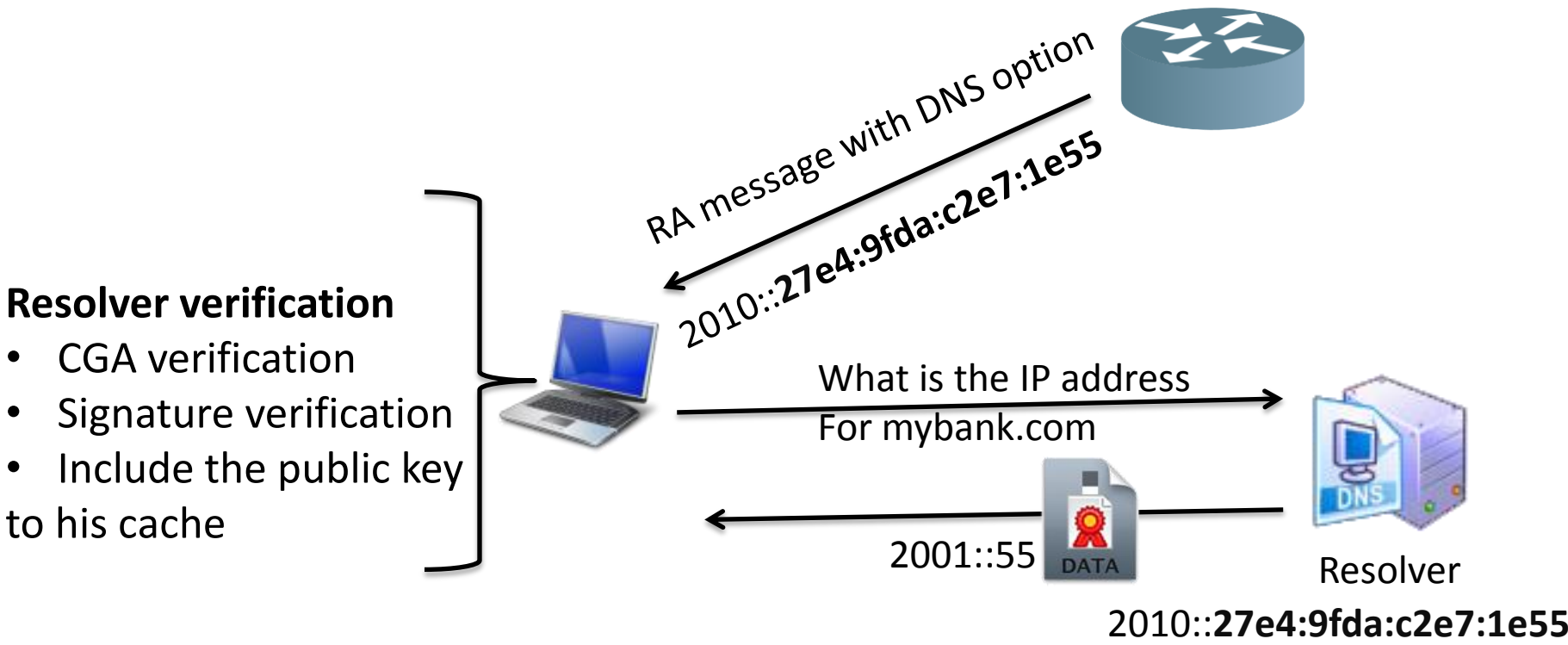
CGA In a Simple Example (RFC 3972)





CGA-TSIG in Resolving Scenario

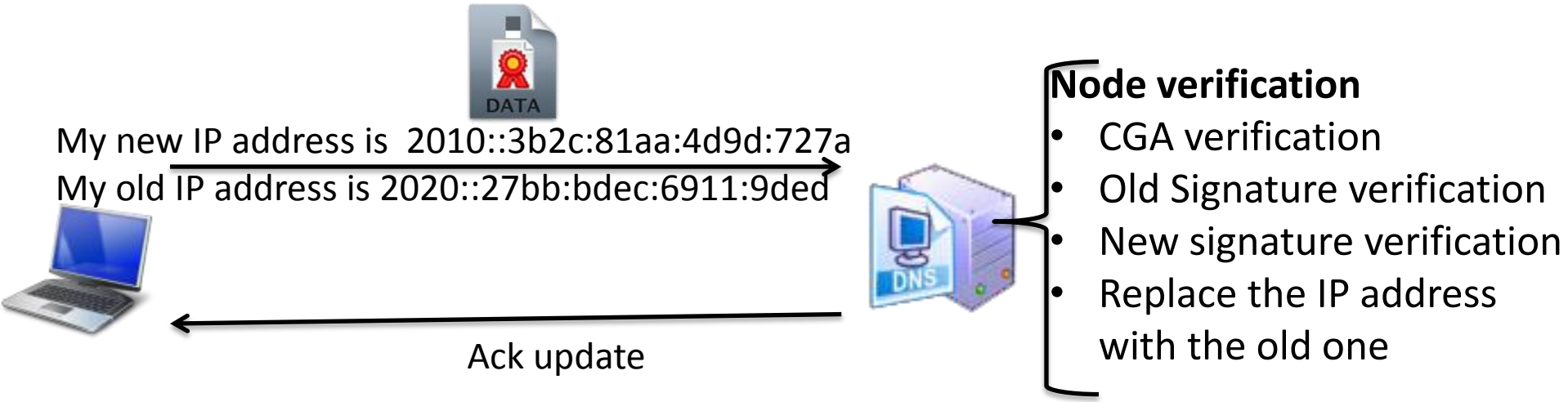
- Problem addressed:
  - Resolver secure authentication while it must answer to anonymous queries



CGA-TSIG in Dynamic Update Scenario

Secure PTR Update

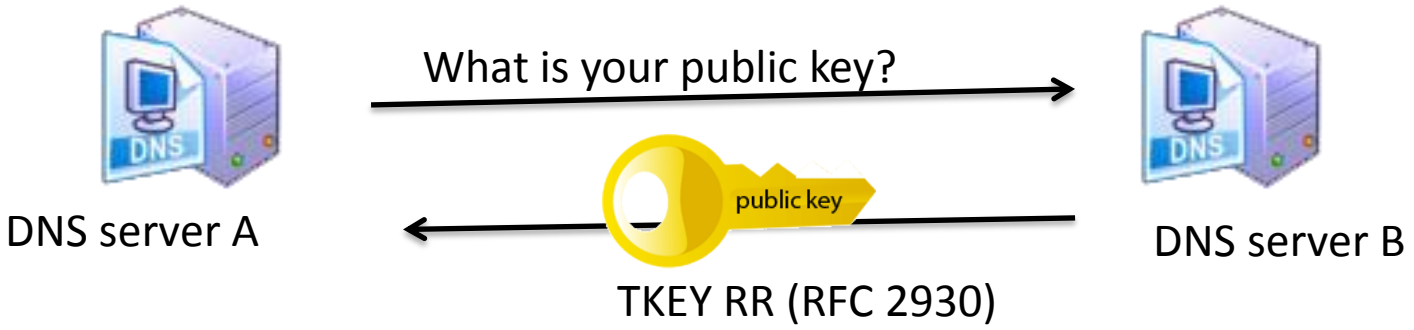
- Problem Addressed:
  - No option to update PTR or FQDN Resource Record in Neighbor Discovery Protocol (NDP)
    - Maintain privacy = change IP address = need to update PTR
  - No security option by using DHCPv6 option
  - Avoid IP spoofing and unauthorized update



CGA-TSIGe in Zone Transfer – I

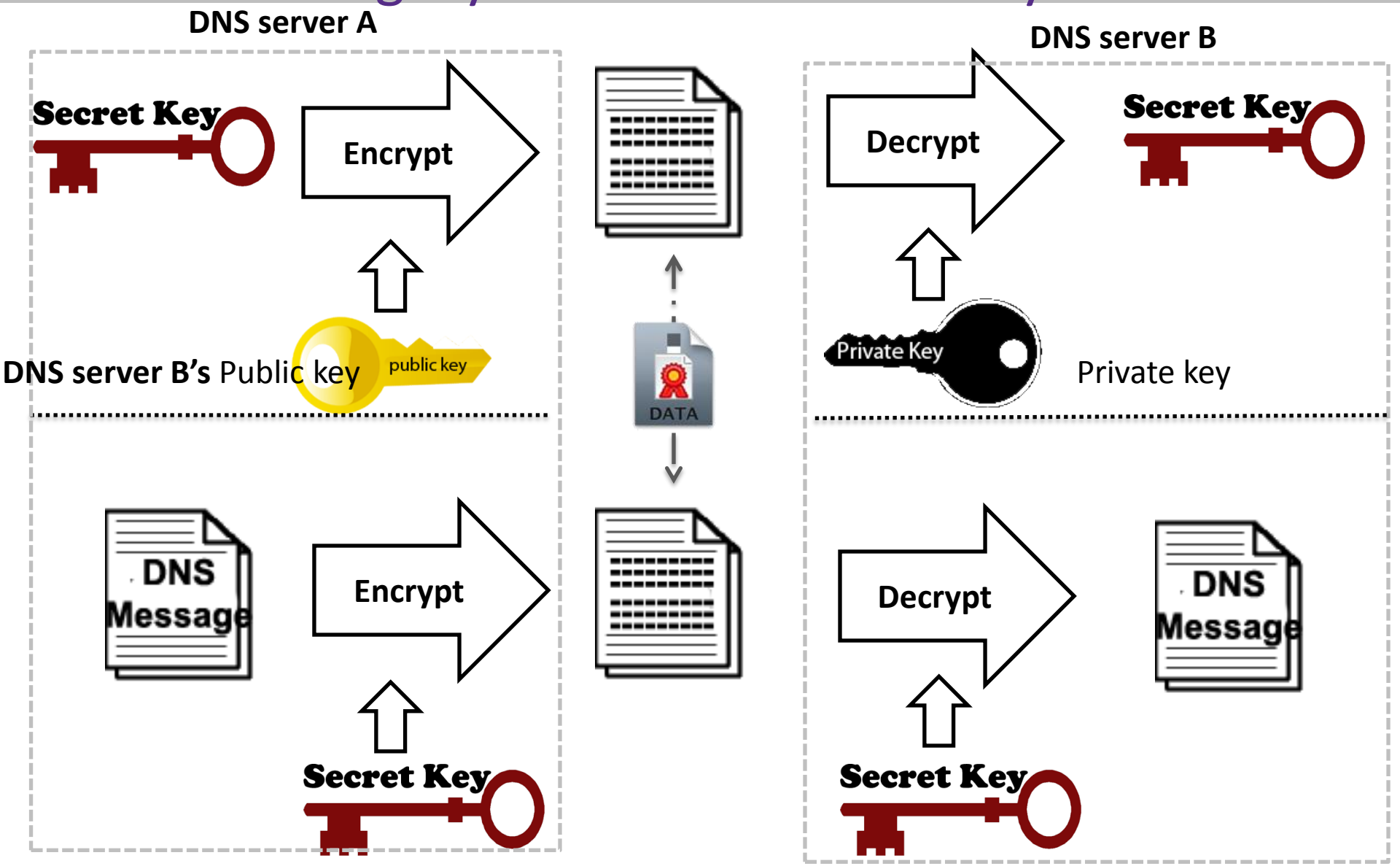
Data Integrity + Data Confidentiality Scenario

- Problem Addressed:
  - Manual distribution of TSIG shared secret among several nodes
    - Repeat this step in case of shared secret exposal to an attacker
  - TSIG provides NO data confidentiality (no privacy)



CGA-TSIGe in Zone Transfer – II

Data Integrity + Data Confidentiality Scenario



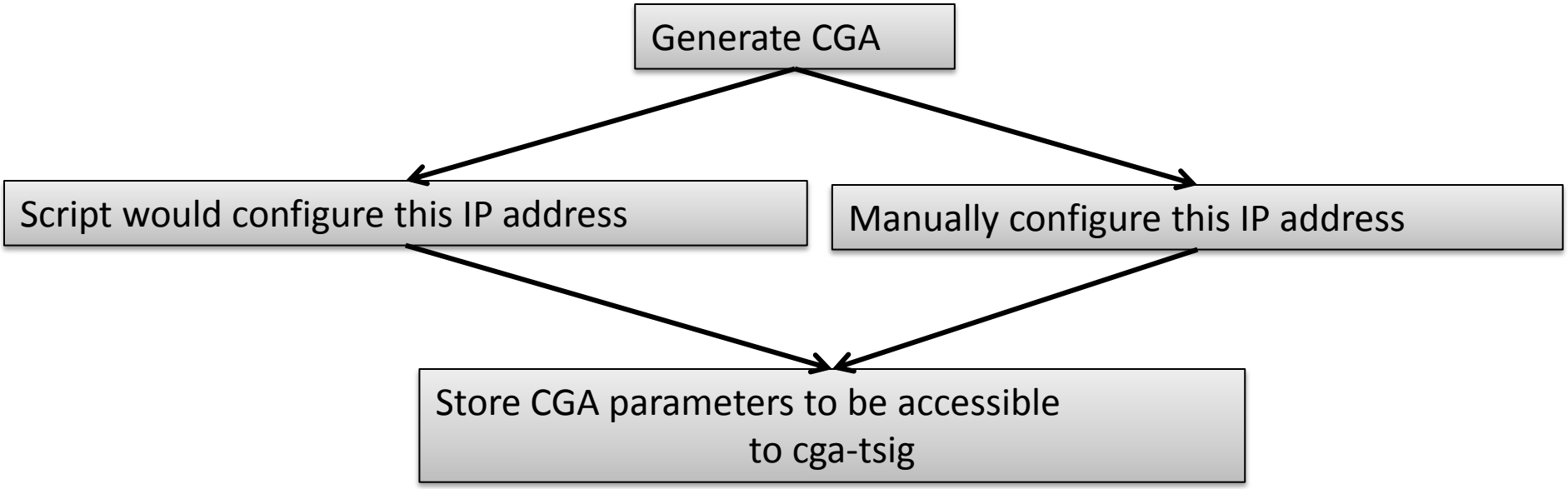
Modifications & Applied Comments

- Explanation of the necessary updates to TSIG RFC
- Modification based on the comments received from the implementer of this draft in OpenDNSSEC (support of NL net Labs)
- Explanation of the case where one needs to apply data confidentiality

Thank you for the supporters of this draft

Extra slides - I

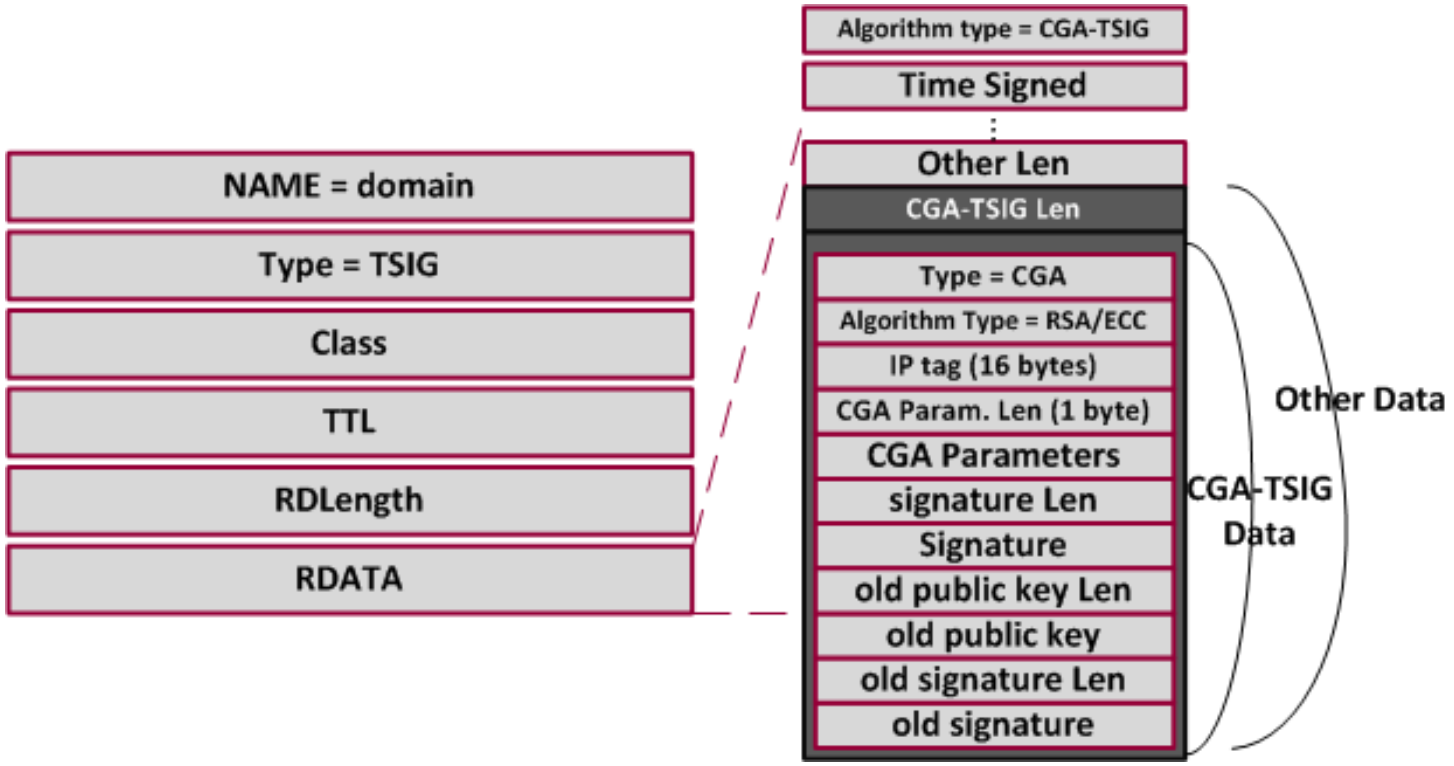
- What if the node does not support CGA?
  - The node can generate its keypair itself and sign the message (Not recommended in recursive resolver to client authentication)
  - Use a small script for CGA generation



Extra slides - II

- Is it a new Resource Records?

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



Extra slides - III

- What if the resolver changes its IP address?
  - The client first send the request to the previous IP address, if it receives no answer, then it sends a Router Solicitation message and receive resolver's IP from the option in RA message again.
- What if the node is in unsecure network (like a café and cannot trust the router?
  - It can set an IP address of a trusted resolver manually. Since the verification is based on the IP address, CGA/SSAS prevents any IP spoofing