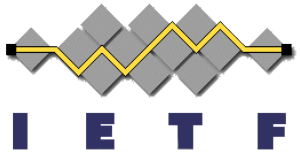
Non-CGA addresses in SEND

E. Levy-Abegnoli

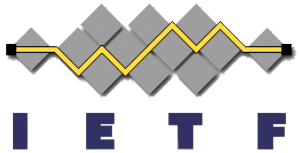


IETF 71, March 09/14th 2008
Philadelphia

What?

- Support for non-cga addresses in SEND
- Establish address ownership of addresses used in ND messages (NS, NA, RS, RA, REDIR) using certificates “instead of” or “on top of” Cryptographic verification
- Authorize addresses in ND
- Basically, fill the holes in RFC3971 to support non-CGA addresses
- Make CGA truly optional in RFC3971

Why?



- Some nodes (routers, …) want (secured) handcrafted addresses
- CGA may not be considered secure-enough in some environments
- CGA provide address ownership, not address authorization
- IPR on CGA may have slow down SEND adoption

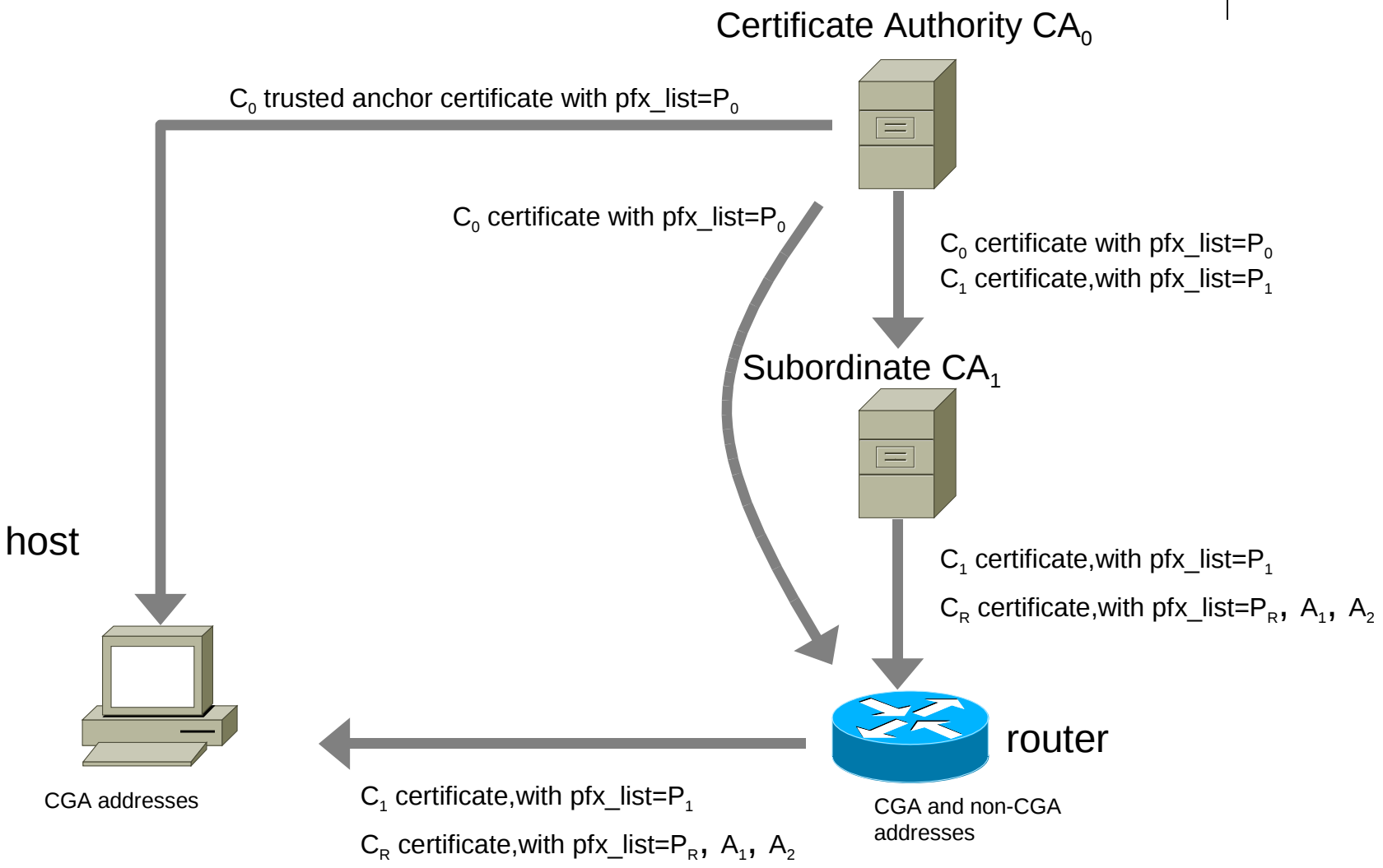
How

A node can be configured to use one the following authorization methods [RFC3971, 5.2.3] :

1. Trust anchor
2. CGA
3. Trust anchor and CGA
4. Trust anchor or CGA

- Trust anchor method is used in cases 1, 3 and case 4, if CGA option not present in the message.
- When trust anchor is used, node MAY retrieve a certificate previously cached matching the keyhash found in the RSA option
- If no certificate has been cached, node MUST obtain one thru a CPS/CPA flow

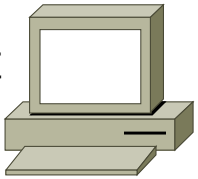
Deployment case-1



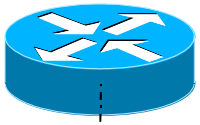
Example 1

Configuration: CGA *or* TA
Provisioning: TA certificate C_0
with pfx_list=P_0

Configuration: CGA
Provisioning: Router certificate C_R
with pfx_list=P_R , A_1, A_2



host



router

ND_msg [source=CGA, options=CGA,nonce,timestamp,RSA]

CGA verification

ND_msg [source=CGA, options=CGA,nonce,timestamp,RSA]

CGA verification

ND_msg [source = A_1, options=nonce,timestamp,RSA]

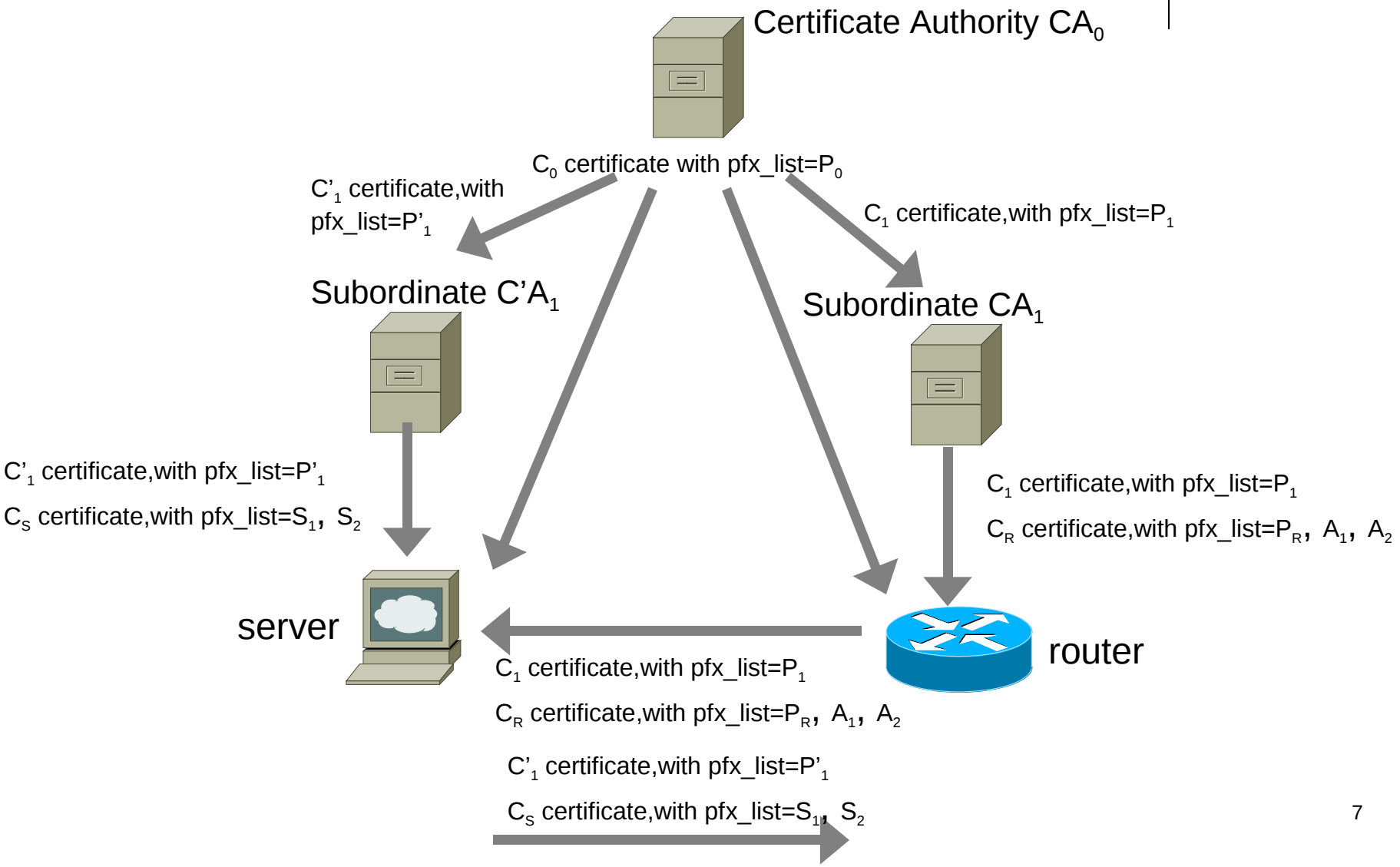
CPS [option = TA/C_0]

Cert. verification

CPA [option =cert/C_1]

CPA [option =cert/C_R]

Deployment case-2



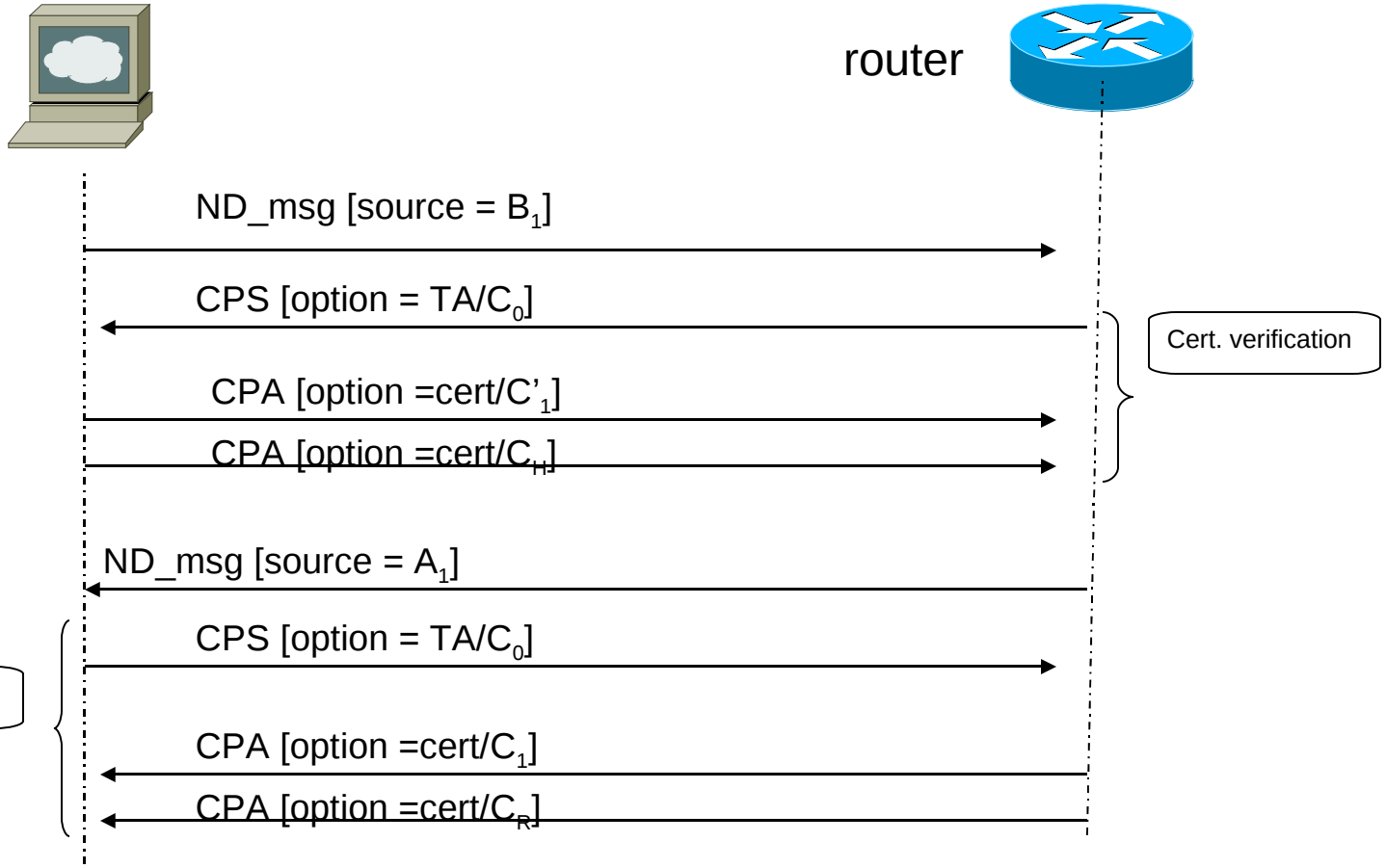
Example 2

Configuration: CGA or TA
Provisioning: TA certificate C_H
with pfx_list=B_1

Configuration: CGA or TA
Provisioning: Router certificate C_R
with pfx_list=P_R , A_1, A_2

server

router



Certificate profile

- /128 addresses grant address ownership and address authorization
- /n, n<128, prefix range and inherit grant router authorization
- Any combinations allowed in a single certificate, per "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779
- Or new Extended Key Usage Value?

TOC

OLD:

6. Authorization Delegation Discovery
  6.1. Authorization Model
  6.2. Deployment Model
  6.3. Certificate Format
    6.3.1. Router Authorization Certificate Profile
    6.3.2. Suitability of Standard Identity Certificates
  6.4. Certificate Transport
    6.4.1. Certification Path Solicitation Message Format
    6.4.2. Certification Path Advertisement Message Format
    6.4.3. Trust Anchor Option
    6.4.4. Certificate Option
    6.4.5. Processing Rules for Routers
    6.4.6. Processing Rules for Hosts
  6.5. Configuration
7. Addressing
  7.1. CGAs
  7.2. Redirect Addresses

NEW:

6. Authorization Delegation Discovery
  6.1. Authorization Model
  6.2. Deployment Model
  6.3. Certificate Format
    6.3.1. Router Authorization Certificate Profile
    6.3.2. Address Authorization Certificate Profile
    6.3.3. Suitability of Standard Identity Certificates
  6.4. Certificate Transport
    6.4.1. Certification Path Solicitation Message Format
    6.4.2. Certification Path Advertisement Message Format
    6.4.3. Trust Anchor Option
    6.4.4. Certificate Option
    6.4.5. Sending Certification Path Solicitation
    6.4.6. Receipt of Certification Path Solicitation
    6.4.7. Sending Certification Path Advertisement
    6.4.8. Receipt of Certification Path Advertisement
  6.5. Configuration
7. Addressing
  7.1. Address selection
  7.2. Redirect Addresses

CGA option become optional

Section 5.1.1., paragraph 1:
OLD:

> If the node has been configured to use SEND, the CGA option MUST be present in all Neighbor Solicitation and Advertisement messages and MUST be present in Router Solicitation messages unless they are sent with the unspecified source address. The CGA option MAY be present in other messages.

NEW:

> If the node has been configured to use SEND, the CGA option MUST be present in all Neighbor Solicitation, Neighbor Advertisement and Router Solicitation messages that contain a CGA address. The CGA option MAY be present in other messages that contain a CGA address.

Certificates authorize addresses

NEW:

6.3.2. Address Authorization Certificate Profile

Address Authorization Certificates are X.509v3 certificates. The same rules and examples described in Section 6.3.1 apply, except that these certificates are owned by nodes required to prove address ownership rather than prefix ownership or authority to be a router. This is used when the node want to prove address ownership and authorization via certificate.

From the certificate standpoint, this difference is purely rhetorical, as an Address Authorization Certificate could carry multiple addresses at once. From a receiver standpoint however, the difference is more visible. Upon receiving such certificate, the receiver expecting address ownership proof via a certificate MUST verify that the address(es) claimed in NS/NA/RA/RS and REDIR are contained in the certificate IP extension(s).

Specific behavior for /128 IP-extensions in the certificate

A certificate carrying only addresses (/128) in the IP extensions MUST NOT be used to authorize the sender of this certificate to be a router. A certificate carrying prefixes, prefix ranges and/or inherit from the parent but not addresses (/128) MUST NOT be used to authorize addresses.

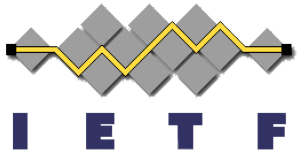
Note that in the case where a router would be required to prove address ownership with a certificate, the same certificate used for router authorization can be used for address authorization, provided it carries prefix list (allowed for the router to advertise), and address list (allowed for router to claim in NDP).

What's next?

- More changes (to RFC3971) to be added
  - unsolicited RA in response to one *or many RS.*
  - provisional certificate acceptance
  - Timestamp cache

What's next?

- Continue with diffs to RFC3971?
- Publish an rfc3971-bis proposal as an individual submission and gave the WG decides to make it a WG document?
- Start working on rfc3971-bis as a WG document?



THANK YOU!