Certificate Option for DHCP

C. Popoviciu, **R. Droms**,
E. Levy-Abegnoli,

IETF 70, December 3rd 2007
Vancouver

Concept Overview

Premise

- DHCP-PD provides a prefix to a CPE to use for provisioning its interfaces
- The DHCP-PD server maintains state on how long the CPE is allowed to use that prefix
- If devices behind the CPE use SEND (RFC 3971), they will require the CPE to certify it is allowed to advertise the prefix via RAs

Proposal

- Have the DHCP-PD server do one of the following:
  - Provide the CPE with certificates to advertise the prefix assigned to it
  - Helper the process of obtaining a certificate for the assigned prefixes

Certificate and SEND Background

Elements

- In the context of SEND, a certificate proves that a router can act as a gateway and advertise certain prefixes (in RAs)
- The Certificate relates to: Identifier (Distinguish Name), Public Key, Extensions (such as prefix)
- The Certificate has a lifetime
- It is offered by a certificate server. There is also a server which maintains the list of revoked certificates (CRL). The address of this server can be included in the certificate

Process

- The acquisition process does not require special security considerations, the information exchanged is public
- Methods currently in use for this: manual, File System, SCEP, PKCS12, HTTP, Self-Signed
- Obtaining the certificate:
  - Client generates a pair of RSA keys and builds a certificate request which includes its ID, the public key and the extensions
  - The Server receives the request, builds the certificate and sends it to the client

Proposed Option

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          OPTION_CO            |         option-length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|C|P|P|       |                                               |
+-+-+-+-+-+-+-+-+                                               .
.                        CO-option data                         .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

C=Capabilities bits

-00=Any capability

-01=Pointer to Certificate Server

-10=Certificate

-11=Both pointer and certificate

P=Payload Type bits

-00=Certificate chain anchor

-01=Public Key

-10=Pointer to certificate server

-11=Certificate

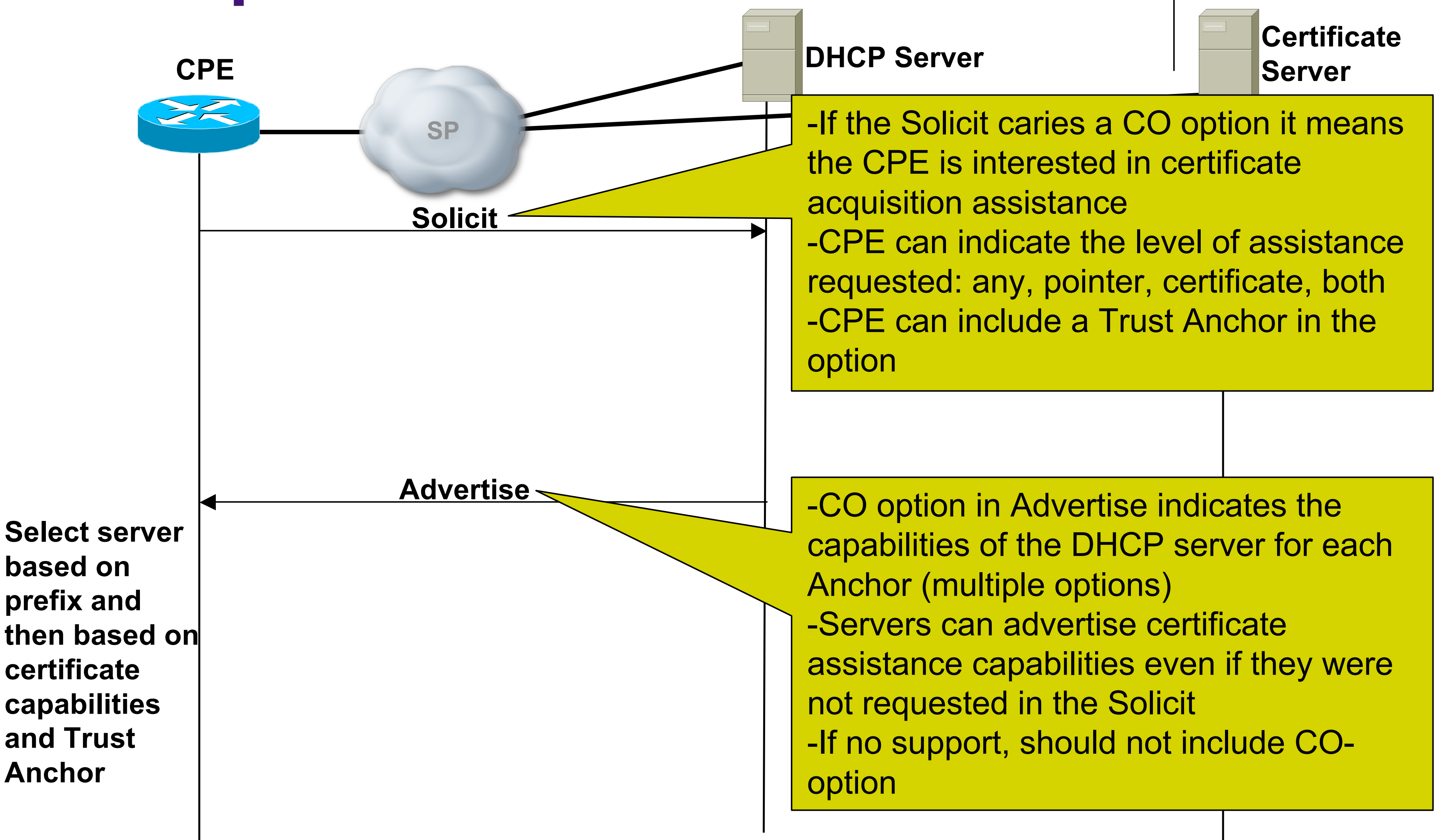
Option and protocol considerations

- The option is defined for the IA_PD
- Multiple CO-options can be present
- Alternative 1: The certificate is for all prefixes managed under the given IA_PD
- Alternative 2: One certificate for each prefix

draft-popoviciu-dhc-certificate-opt-00.txt

THANK YOU!

DHCP Server Discovery – description

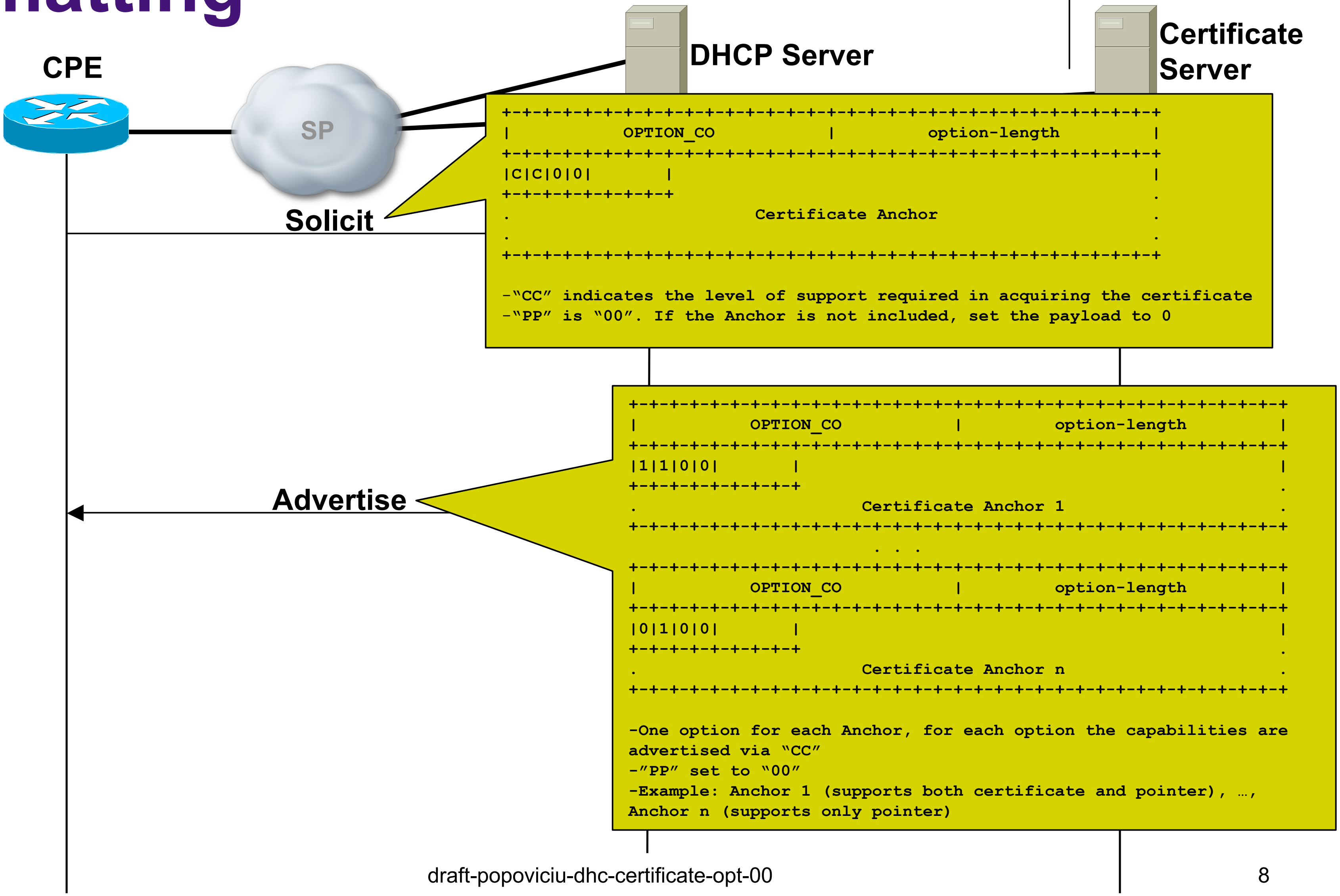


-If the Solicit caries a CO option it means the CPE is interested in certificate acquisition assistance
-CPE can indicate the level of assistance requested: any, pointer, certificate, both
-CPE can include a Trust Anchor in the option

-CO option in Advertise indicates the capabilities of the DHCP server for each Anchor (multiple options)
-Servers can advertise certificate assistance capabilities even if they were not requested in the Solicit
-If no support, should not include CO-option

Select server based on prefix and then based on certificate capabilities and Trust Anchor

DHCP Server Discovery – option formatting



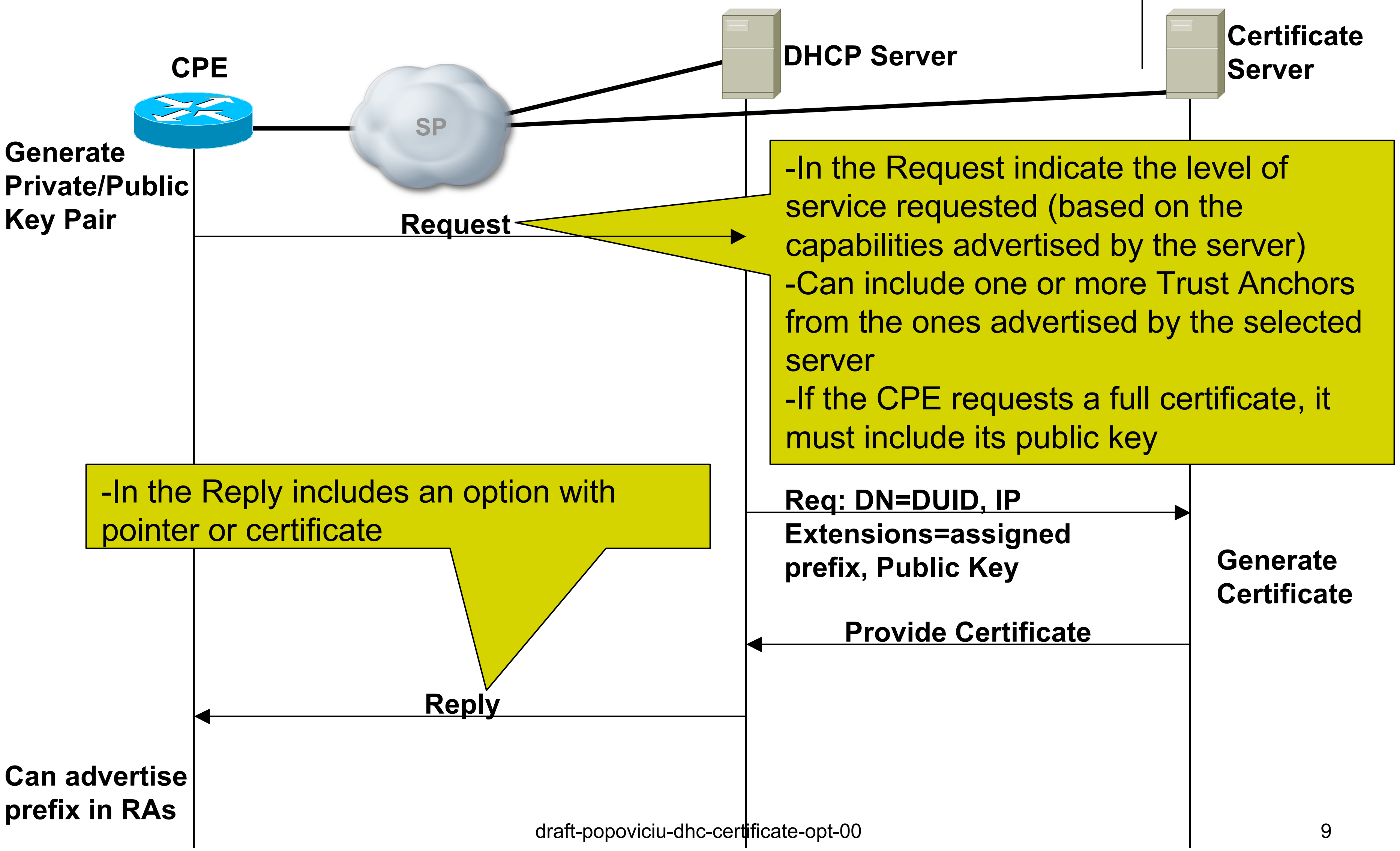
```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          OPTION_CO            |         option-length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|C|0|0|       |                                               |
+-+-+-+-+-+-+-+-+                                               .
.                       Certificate Anchor                      .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

-"CC" indicates the level of support required in acquiring the certificate
-"PP" is "00". If the Anchor is not included, set the payload to 0

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          OPTION_CO            |         option-length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1|1|0|0|       |                                               |
+-+-+-+-+-+-+-+-+                                               .
.                      Certificate Anchor 1                     .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                             . . .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          OPTION_CO            |         option-length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|1|0|0|       |                                               |
+-+-+-+-+-+-+-+-+                                               .
.                      Certificate Anchor n                     .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

-One option for each Anchor, for each option the capabilities are advertised via "CC"
-"PP" set to "00"
-Example: Anchor 1 (supports both certificate and pointer), …, Anchor n (supports only pointer)

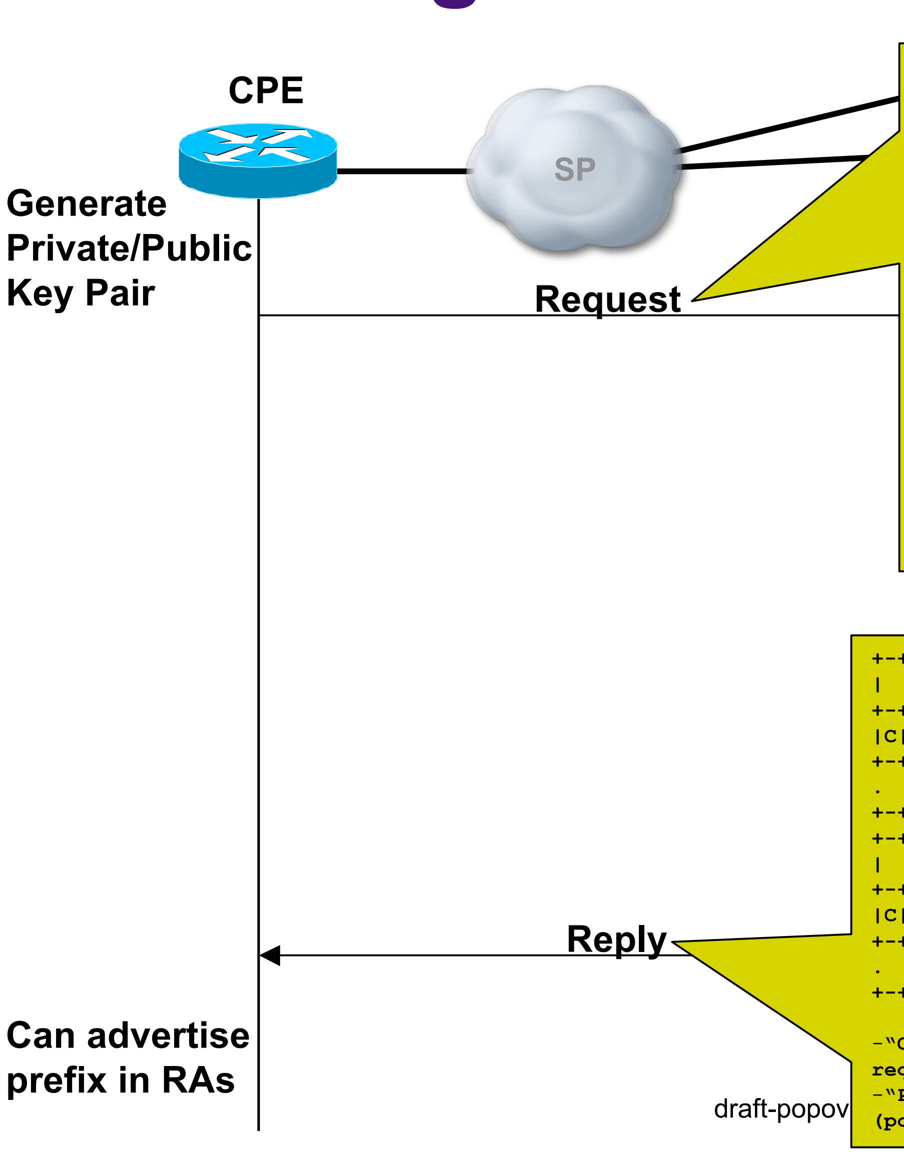
Prefix Delegation – description


CPE
SP
DHCP Server
Certificate Server
Generate Private/Public Key Pair
Request
Req: DN=DUID, IP Extensions=assigned prefix, Public Key
Generate Certificate
Provide Certificate
Reply
Can advertise prefix in RAs

-In the Request indicate the level of service requested (based on the capabilities advertised by the server)
-Can include one or more Trust Anchors from the ones advertised by the selected server
-If the CPE requests a full certificate, it must include its public key

-In the Reply includes an option with pointer or certificate

Prefix Delegation – option formatting



CPE

SP

Generate Private/Public Key Pair

Request

Reply

Can advertise prefix in RAs

Certificate

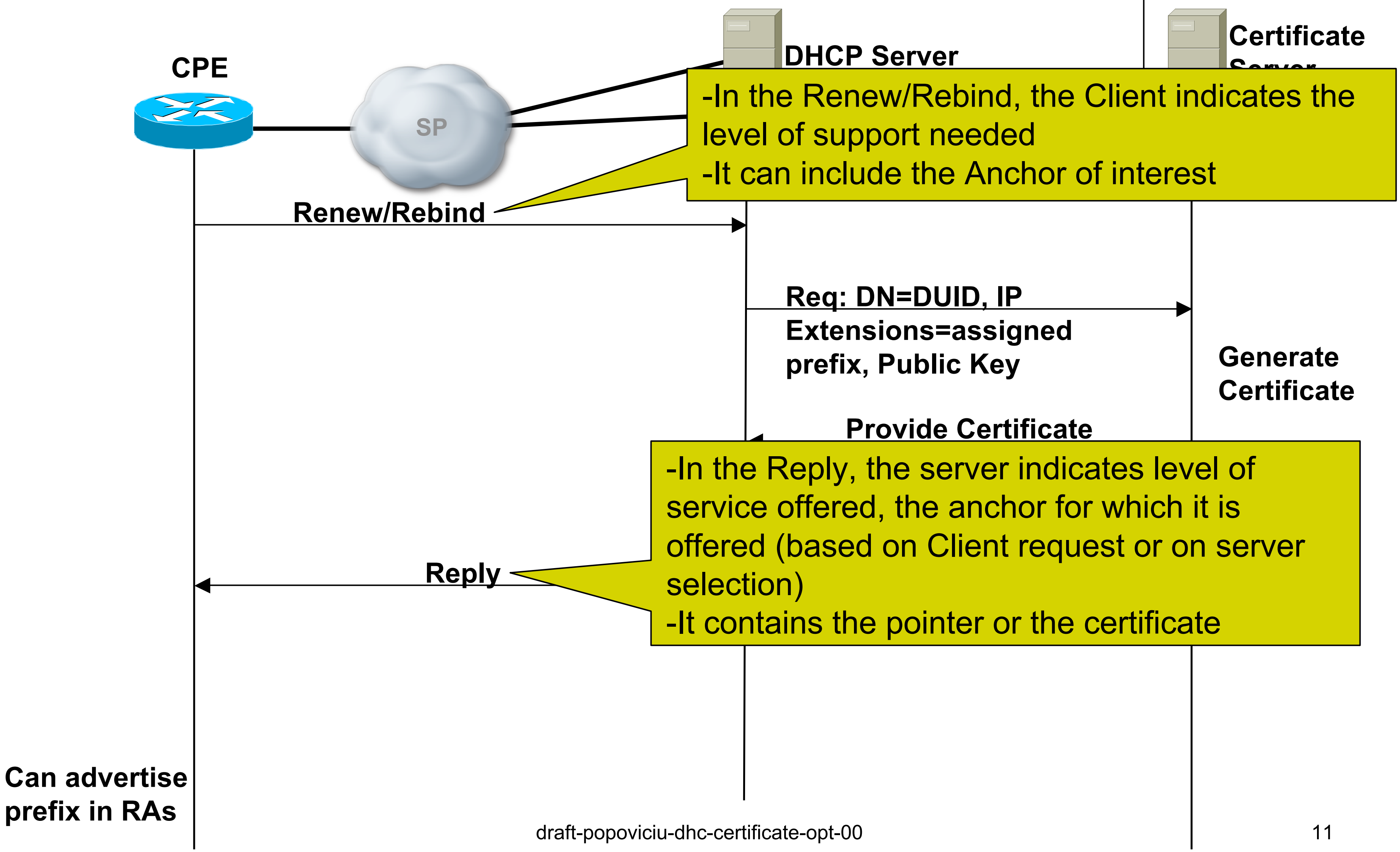
```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           OPTION_CO           |          option-length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|C|0|1|       |                                               |
+-+-+-+-+-+-+-+-+                                               .
.                        Public Key                             .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           OPTION_CO           |          option-length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|C|0|0|       |                                               |
+-+-+-+-+-+-+-+-+                                               .
.                        Anchor of Interest                            .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

-First CO-option carries the Public Key and the precise level of service requested. If not Anchor is specified then the service is provided in relation to one or more anchors selected by the server
-Can include an Anchor advertised by the server, the “CC” bits must be synced with the ones in the option carrying the public key

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           OPTION_CO           |          option-length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|C|0|0|       |                                               |
+-+-+-+-+-+-+-+-+                                               .
.                    Selected Anchor                            .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           OPTION_CO           |          option-length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|C|P|P|       |                                               |
+-+-+-+-+-+-+-+-+                                               .
.              IP address or Name of Certificate Server         .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

-“CC” indicates the level of support offered by the server for the Anchor requested by the Client
-“PP” indicates the info offered in relation to that Anchor (pointer/certificate=10/11)

Renew/Rebind – description



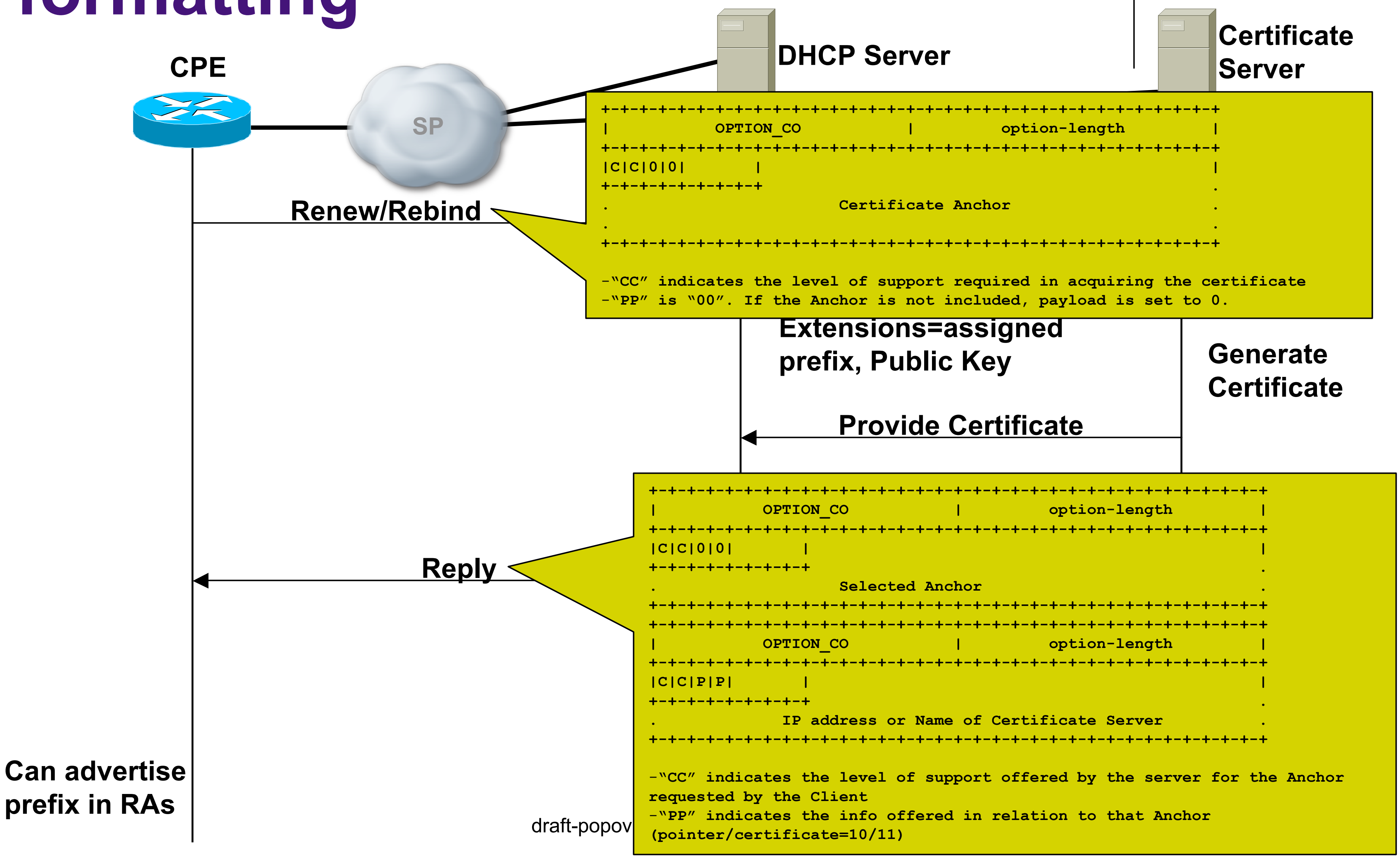
-In the Renew/Rebind, the Client indicates the level of support needed

-It can include the Anchor of interest

-In the Reply, the server indicates level of service offered, the anchor for which it is offered (based on Client request or on server selection)

-It contains the pointer or the certificate

Renew/Rebind – option formatting



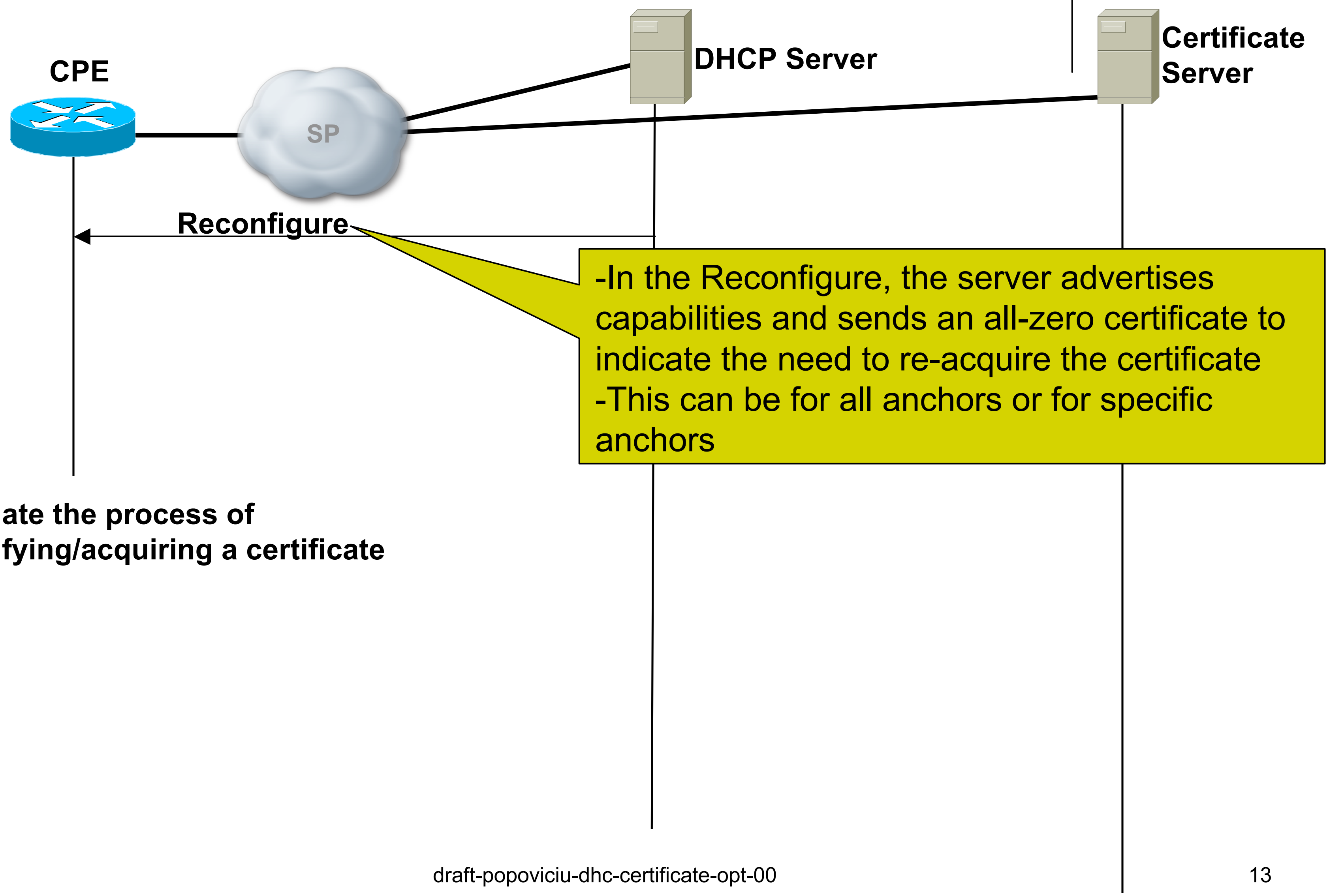
```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           OPTION_CO           |          option-length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|C|0|0|       |                                               |
+-+-+-+-+-+-+-+-+                                               .
.                        Certificate Anchor                     .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

-“CC” indicates the level of support required in acquiring the certificate
-“PP” is “00”. If the Anchor is not included, payload is set to 0.

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           OPTION_CO           |          option-length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|C|0|0|       |                                               |
+-+-+-+-+-+-+-+-+                                               .
.                   Selected Anchor                             .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           OPTION_CO           |          option-length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|C|P|P|       |                                               |
+-+-+-+-+-+-+-+-+                                               .
.             IP address or Name of Certificate Server          .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

-“CC” indicates the level of support offered by the server for the Anchor requested by the Client
-“PP” indicates the info offered in relation to that Anchor (pointer/certificate=10/11)

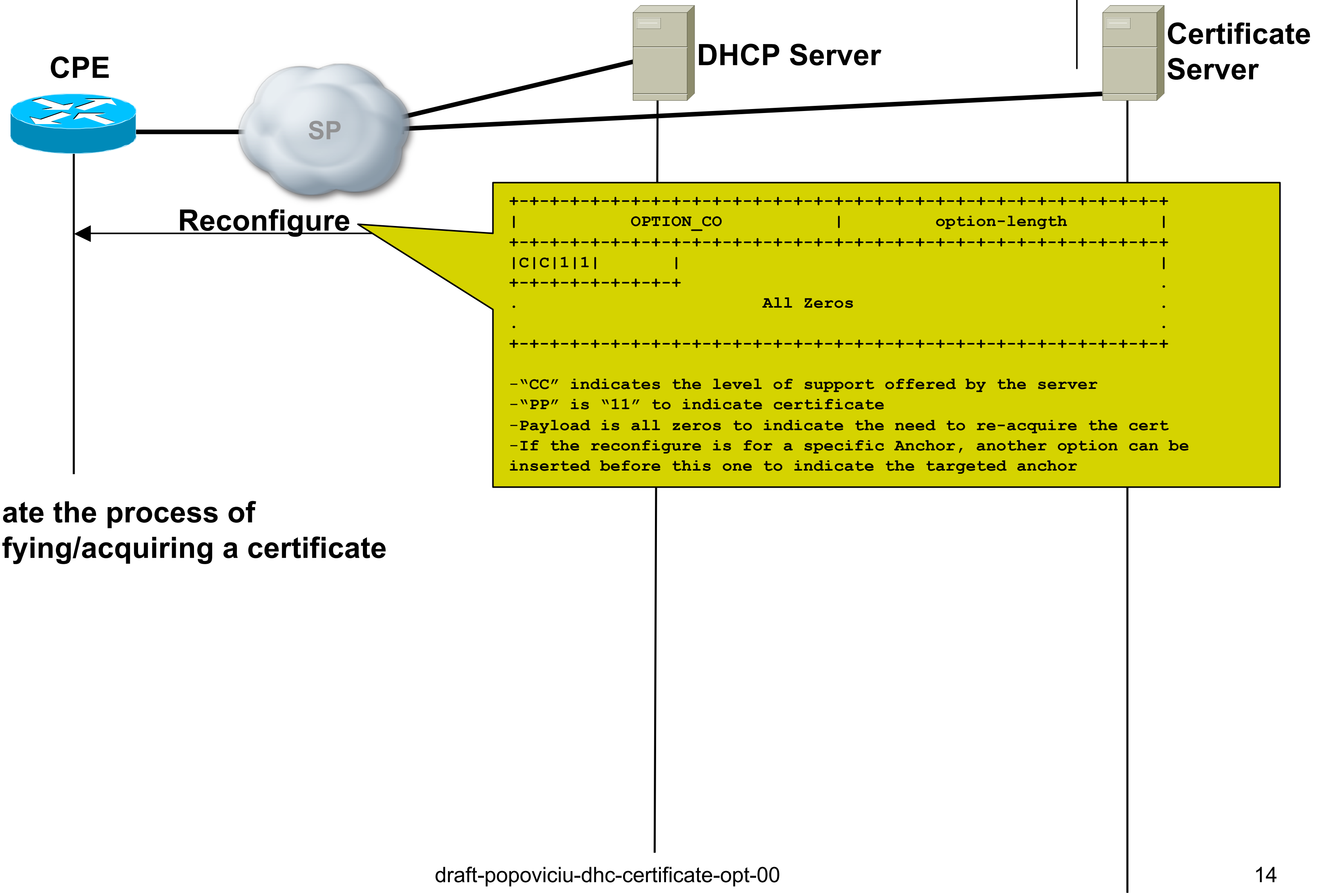
Reconfigure – description



-In the Reconfigure, the server advertises capabilities and sends an all-zero certificate to indicate the need to re-acquire the certificate
-This can be for all anchors or for specific anchors

Initiate the process of verifying/acquiring a certificate

Reconfigure – option formatting



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           OPTION_CO           |         option-length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|C|1|1|       |                                               |
+-+-+-+-+-+-+-+-+                                               .
.                        All Zeros                              .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

-“CC” indicates the level of support offered by the server
-“PP” is “11” to indicate certificate
-Payload is all zeros to indicate the need to re-acquire the cert
-If the reconfigure is for a specific Anchor, another option can be inserted before this one to indicate the targeted anchor

Initiate the process of verifying/acquiring a certificate