5.2.6. Freshest CRL (a.k.a. Delta CRL Distribution Point)

The freshest CRL extension identifies how delta CRL information for this complete CRL is obtained. Conforming CRL issuers MUST mark this extension as non-critical. This extension MUST NOT appear in delta CRLs.

The same syntax is used for this extension as the cRLDistributionPoints certificate extension, and is described in Section 4.2.1.13. However, only the distribution point field is meaningful in this context. The reasons and cRLIssuer fields MUST be omitted from this CRL extension.

Each distribution point name provides the location at which a delta CRL for this complete CRL can be found. The scope of these delta CRLs MUST be the same as the scope of this complete CRL. The contents of this CRL extension are only used to locate delta CRLs; the contents are not used to validate the CRL or the referenced delta CRLs. The encoding conventions defined for distribution points in Section 4.2.1.13 apply to this extension.

```
id-ce-freshestCRL OBJECT IDENTIFIER ::=  { id-ce 46 }

FreshestCRL ::= CRLDistributionPoints
```

5.2.7. Authority Information Access

This section defines the use of the Authority Information Access extension in a CRL. The syntax and semantics defined in Section 4.2.2.1 for the certificate extension are also used for the CRL extension.

This CRL extension MUST be marked as non-critical.

When present in a CRL, this extension MUST include at least one AccessDescription specifying id-ad-caIssuers as the accessMethod. The id-ad-caIssuers OID is used when the information available lists certificates that can be used to verify the signature on the CRL (i.e., certificates that have a subject name that matches the issuer name on the CRL and that have a subject public key that corresponds to the private key used to sign the CRL). Access method types other than id-ad-caIssuers MUST NOT be included. At least one instance of AccessDescription SHOULD specify an accessLocation that is an HTTP [RFC2616] or LDAP [RFC4516] URI.

Where the information is available via HTTP or FTP, accessLocation MUST be a uniformResourceIdentifier and the URI MUST point to either a single DER encoded certificate as specified in [RFC2585] or a collection of certificates in a BER or DER encoded "certs-only" CMS message as specified in [RFC2797].

Conforming applications that support HTTP or FTP for accessing certificates MUST be able to accept individual DER encoded certificates and SHOULD be able to accept "certs-only" CMS messages.

HTTP server implementations accessed via the URI SHOULD specify the media type application/pkix-cert [RFC2585] in the content-type header field of the response for a single DER encoded certificate and SHOULD specify the media type application/pkcs7-mime [RFC2797] in the content-type header field of the response for "certs-only" CMS messages. For FTP, the name of a file that contains a single DER encoded certificate SHOULD have a suffix of ".cer" [RFC2585] and the name of a file that contains a "certs-only" CMS message SHOULD have a suffix of ".p7c" [RFC2797]. Consuming clients may use the media type or file extension as a hint to the content, but should not depend solely on the presence of the correct media type or file extension in the server response.

When the accessLocation is a directoryName, the information is to be obtained by the application from whatever directory server is locally configured. When one CA public key is used to validate signatures on certificates and CRLs, the desired CA certificate is stored in the crossCertificatePair and/or cACertificate attributes as specified in [RFC4523]. When different public keys are used to validate signatures on certificates and CRLs, the desired certificate is stored in the userCertificate attribute as specified in [RFC4523]. Thus, implementations that support the directoryName form of accessLocation MUST be prepared to find the needed certificate in any of these three attributes. The protocol that an application uses to access the directory (e.g., DAP or LDAP) is a local matter.

Where the information is available via LDAP, the accessLocation SHOULD be a uniformResourceIdentifier. The LDAP URI [RFC4516] MUST include a <dn> field containing the distinguished name of the entry holding the certificates, MUST include an <attributes> field that lists appropriate attribute descriptions for the attributes that hold the DER encoded certificates or cross-certificate pairs [RFC4523], and SHOULD include a <host> (e.g., <ldap://ldap.example.com/cn=CA,dc=example,dc=com?cACertificate;binary,crossCertificatePair;binary>). Omitting the <host> (e.g., <ldap:///cn=exampleCA,dc=example,dc=com?cACertificate;binary>) has the effect of relying on whatever a priori knowledge the client might have to contact an appropriate server.