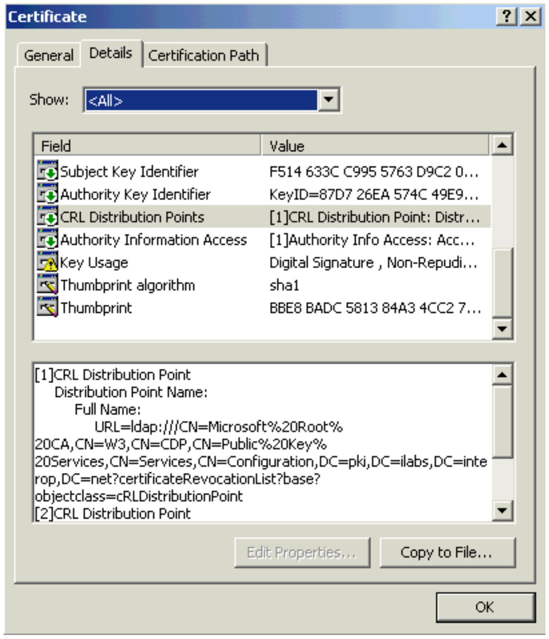
Title: (ilab_blk.eps)
Creator: Adobe Illustrator(R) 8.0
Preview: This EPS picture was not saved with a

What is a CRL?

(and how do I use one?)

A CRL is a Certificate Revocation List. When any certificate is issued, it has a validity period which is defined by the Certification Authority. Usually this is one or two years. Any time a certificate is presented as part of an authentication dialog, the current time should be checked against the validity period. If the certificate is past that period, or expired, then the authentication should fail.

However, sometimes certificates should not be honored even during their validity period. For example, if the private key associated with a certificate is lost or exposed, then any authentication using that certificate should be denied. Similarly, people will change jobs, names, and companies. When their certificates are replaced, the old certificates have to be marked somehow as “no longer accepted.” The purpose of the CRL is to list certificates which are valid, but are revoked.



Show: <All>

Field	Value
Subject Key Identifier	F514 633C C995 5763 D9C2 0...
Authority Key Identifier	KeyID=87D7 26EA 574C 49E9...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Key Usage	Digital Signature , Non-Repudi...
Thumbprint algorithm	sha1
Thumbprint	BBE8 BADC 5813 84A3 4CC2 7...

```
[1]CRL Distribution Point
   Distribution Point Name:
      Full Name:
         URL=ldap:///CN=Microsoft%20Root%
20CA,CN=W3,CN=CDP,CN=Public%20Key%
20Services,CN=Services,CN=Configuration,DC=pki,DC=ilabs,DC=inte
rop,DC=net?certificateRevocationList?base?
objectclass=cRLDistributionPoint
[2]CRL Distribution Point
```

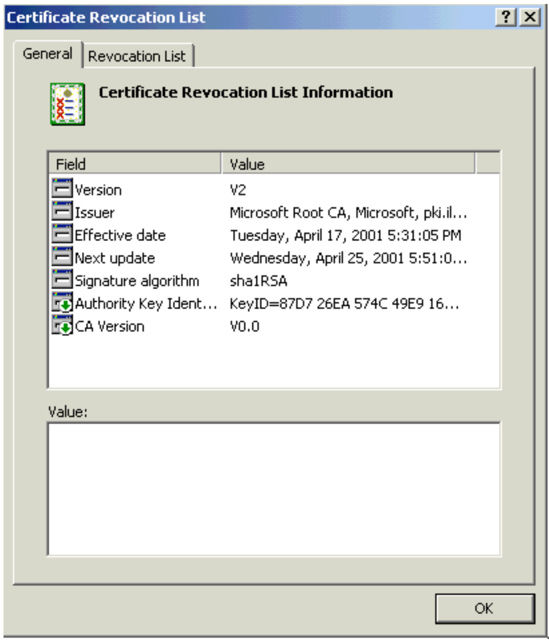
The starting point for the CRL is the CRL Distribution Point (the CDP), which is a field located in each certificate. The CDP is optional, but most well-run PKI installations include a CDP in each certificate. In the screen shot to the left, you can see the CDP we put in our iLabs demonstration certificates issued by the Microsoft Windows 2000 CA. In this case, the CRL has two distribution points, one available using an LDAP server and the other stored on an http server.

Of course, having a pointer to the CDP is not sufficient to activate the CRL. In addition, the client applications (such as your WWW browser, a mail client, or other tools) must look at the CDP, retrieve the CRL, and look up the certificate in the CRL to be sure that it has not been revoked.

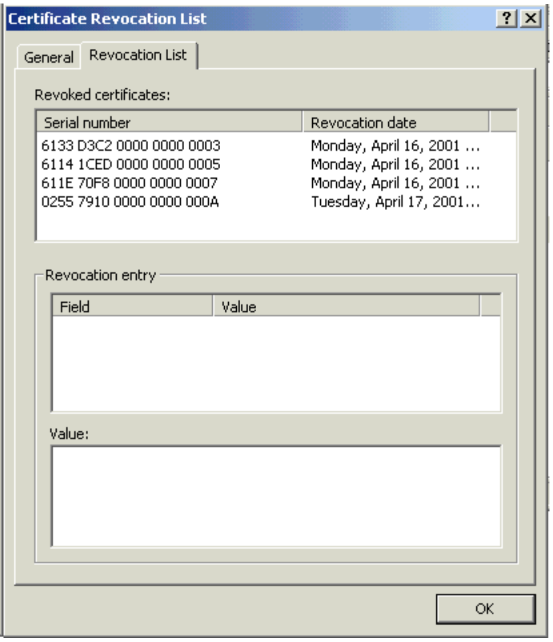
Very few common applications (such as web browsers and email clients) actually check the CRL. Even those that do will often encounter certificates which have no Certificate Distribution Point entry. For example, if you are using a WWW browser on the public internet, your browser does not, by default check the CDP. And it doesn’t matter if you change the setting: the largest and most important companies which sell certificates for WWW servers do not have a CDP, so even if you were interested in checking the CRL, you wouldn’t know where to get it.

One of the few common applications which does check the CRL is Microsoft’s Internet Explorer browser on the Windows platform. Although CRL checking is not the default, you can enable checking of the CRL by changing a setting in the Internet Explorer preferences.

A CRL, like a certificate, also has a validity date span. The date span ensures that the CRL is not used after a certain time (when it is likely to be out of date), but also allows the application checking the CRL to cache the CRL so that it doesn't have to keep downloading it over and over again. In the two screen shots below, you can see the CRL loaded on our Windows 2000 Certification Authority.


Certificate Revocation List
General
Revocation List
Certificate Revocation List Information
Value:
OK

Field	Value
Version	V2
Issuer	Microsoft Root CA, Microsoft, pki.il...
Effective date	Tuesday, April 17, 2001 5:31:05 PM
Next update	Wednesday, April 25, 2001 5:51:0...
Signature algorithm	sha1RSA
Authority Key Ident...	KeyID=87D7 26EA 574C 49E9 16...
CA Version	V0.0



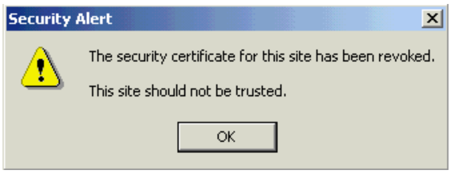
Revoked certificates:

Serial number	Revocation date
6133 D3C2 0000 0000 0003	Monday, April 16, 2001 ...
6114 1CED 0000 0000 0005	Monday, April 16, 2001 ...
611E 70F8 0000 0000 0007	Monday, April 16, 2001 ...
0255 7910 0000 0000 000A	Tuesday, April 17, 2001...

Notice that our CRL has four certificates on it. Those are stored with their Certification Authority-specific serial numbers and a revocation date; the long Distinguished Name field and all the other certificate fields can be omitted. This keeps the certificate distribution list fairly short. In addition, certificates which are no longer valid (i.e., they have expired) do not need to be held on the CRL.

If you care about revoked certificates, such as in a user-authentication environment, checking the CRL is particularly important. For example, in our iLabs demonstration testbed, the Check Point VPN gateway refused to authenticate end users unless it had access to a CRL so that it could tell whether a user was still authorized to connect or not.

In this demonstration, we have revoked the certificate of one of our web servers (the Microsoft IIS server running on w3.pki.ilabs.interop.net). If you try to connect to this server with a web browser which checks CRLs, you should be warned that you're doing something which is not secure. The web browser will also block you from seeing the page protected by the revoked certificate. You can try this from our w6, w7, and w8 client machines.



The security certificate for this site has been revoked.

This site should not be trusted.