Certification Authority Renewal

learn.microsoft.com/en-us/windows/win32/seccrypto/certification-authority-renewal

alvinashcraft

January 7, 2021

- Article
- 01/08/2021

Certificate Services supports the renewal of a *certification authority* (CA). Renewal is the issuing of a new certificate for the CA to extend the CA's life beyond the end date of its original certificate. You can renew a CA as a task within the Certificate Authority MMC snap-in or by using the Certutil.exe tool (with the **-renewCert** command).

Each renewal results in a new CA certificate; however, the administrator can either generate a new public/private key pair or reuse the existing public/private key pair for the CA certificate. For consistency and integrity, CA certificates and *certificate revocation lists* (CRL) issued by the CA before its renewal will be available after the CA has been renewed. To make these available, Certificate Services maintains an index of CA certificates, CRLs, and keys.

The indexes and suffix names of CA certificates and CRLs during various CA renewal operations are as follows.

Operation	CA certificate index	CA certificate file name suffix	CRL and key index	CRL and key container name suffix
Original CA installation	0	""	0	""
Renewal with new key	1	"(1)"	1	"(1)"
Renewal reusing key	2	"(2)"	1	"(1)"
Renewal reusing key	3	"(3)"	1	"(1)"
Renewal with new key	4	"(4)"	4	"(4)"
Renewal reusing key	5	"(5)"	4	"(4)"
Renewal with new key	6	"(6)"	6	"(6)"
Renewal reusing key	7	"(7)"	6	"(6)"

When a CA is installed, the certificate index is zero and the certificate suffix is "" (an empty string). Each time the certificate is renewed (whether or not keys are reused), the certificate index is incremented by one, and the certificate file name suffix becomes a string of the form "(*n*)", where *n* represents the number of times the CA certificate has been renewed. After the first renewal, the certificate index is 1 and the certificate file name suffix is "(1)". After the second renewal, the certificate index is 2 and the certificate file name suffix is "(2)", and so on.

Although the CA certificate index and suffix are incremented by one each time the CA is renewed, the CRL and key indexes and the file name suffixes are set to the CA certificate index only if the renewal process includes a new public/private key pair. If it does not, the values of these indexes and suffixes remain the same as they were for the last index. During renewal, an administrator specifies whether a new key pair is generated or the existing key pair is used. (In the Certificate Authority MMC snap-in, an option in the user interface specifies a new or an existing key pair; in the Certutil.exe tool, the command **certutil -renewCert** renews the CA with a new key pair, while the command **certutil -renewCert ReuseKeys** renews the CA with the existing key pair.)

The CRL index is directly tied to the key index, which is set to the CA certificate index only when a new key pair is used for the renewal. After the first renewal (which used a new key pair), the index of the CRL and key is set to 1, and the CRL and key container name suffix is "(1)". After the second renewal, however, the index of the CRL and key remains 1, and the CRL and key container name suffix also remains "(1)"; this is because the second renewal used the existing key pair and only one CRL is issued for each CA key pair.

You can retrieve the indexed CA certificates and CRLs by calling the **GetCertificateProperty** method (in both the **ICertServerExit** and **ICertServerPolicy** interfaces). When you retrieve certain properties related to the CA certificate or CRL, you can append the CA certificate's zero-based index to the property names. For example, to retrieve the CRL index that corresponds to the CA's third certificate, pass the property "CRLIndex.2" to **ICertServerPolicy::GetCertificateProperty**; for the table, the retrieved "CRLIndex.2" property value would be 1. A property called "CertCount" can be used to determine the number of times the CA has been issued a CA certificate.

CA certificates and CRLs contain an extension that provides information about the certificate and key index. The extension is defined in Wincrypt.h as szOID_CERTSRV_CA_VERSION with a value of "1.3.6.1.4.1.311.21.1". The extension data is a **DWORD** value (encoded as X509_INTEGER in the extension); the low 16 bits are the certificate index, and the high 16 bits are the key index.

The initial installation of a CA produces a certificate index of zero and a key index of zero. Renewal of a CA certificate will cause the certificate index to be incremented. If the key is reused in the renewal, the key index will be the same as the previous key index. If the key is not reused, the key index will match the new certificate index.