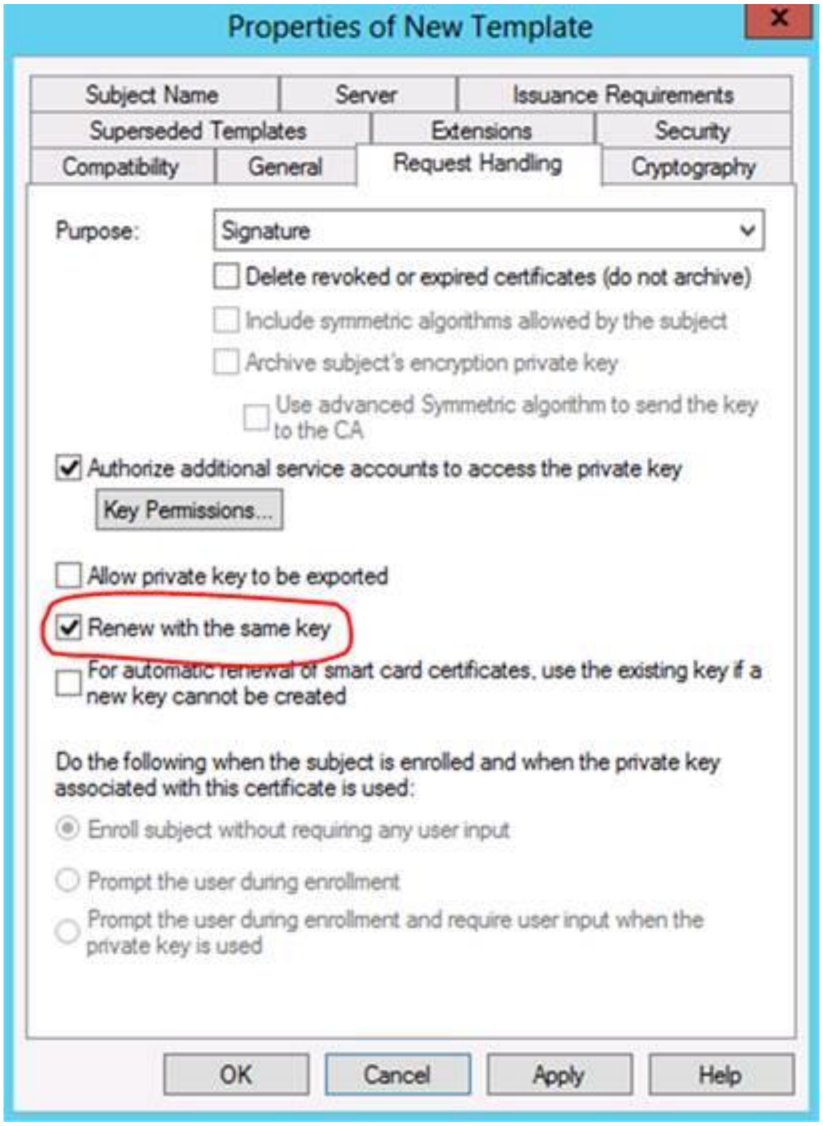
Key-based renewal and same-key renewal of certificates

Certificate renewal is always an issue in managing a PKI. You want the renewal process to be as easy as possible for both users and administrators, but you also want to maintain optimum security. Windows Server 2012 includes some new features pertaining to certificate renewal that will help with both aspects.

One of the new features in Windows Server 2012 Active Directory Certificate Services is support for key-based renewal. What this does is make it easier to obtain certificates when the computer is in an untrusted domain or even when it is not joined to a domain at all. In many organizations, not all computers are domain-joined. You might have some that are members of a workgroup. In the past, administrators were required to renew the certificates for those computers manually, making for additional administrative overhead. With Windows Server 2012 AD CS, as now certificate requests can be made online through the enrollment web services to automatically renew certificates for computers that belong to a different domain or forest, or are not domain members at all.

Another new feature that we get with this version of Windows Server is same-key certificate renewal. This is an important security enhancement, because administrators can now require that certificates be renewed with the same key with which they were originally issued. This means the key stays on the Trusted Platform Module (TPM) after renewal. The keys can't be exported, thus making them more secure. The TPM also provides for anti-hammering. This is designed to thwarted attempts at brute force attacks, because the anti-hammering logic will kick in if a Personal Identification Number (PIN) is entered incorrectly too many times in a row. When that happens, the TPM locks and will not accept subsequently PIN attempts until a specified amount of time has passed.

Same-key renewal is enforced through the certificate template. On the **Request Handling** tab of the certificate template's Properties dialog box, you simply check the box labeled **Renew with the same key**, as shown in Figure 1.



Purpose: Signature

□ Delete revoked or expired certificates (do not archive)

□ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

□ Use advanced Symmetric algorithm to send the key to the CA

☑ Authorize additional service accounts to access the private key

□ Allow private key to be exported

☑ Renew with the same key

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

Figure 1

With same-key renewal enforced, templates require that Windows 8 and Server 2012 clients use the same key to renew their certificates. Trying to use a different key will result in a failed renewal. Unfortunately, this doesn't work with clients running previous versions of Windows.