INSTALLING AND CONFIGURING A WINDOWS SERVER 2003 STAND-ALONE CERTIFICATION AUTHORITY

A Microsoft Certificate Server can take on one of four roles:

- Enterprise Root CA
- Enterprise Subordinate CA
- Stand-alone Root CA
- Stand-alone Subordinate CA

A Microsoft Stand-alone CA has the following characteristics:

- The stand-alone CA does not require Active Directory. This makes the stand-alone CA the Certificate Authority of choice in environments where there is no Active Directory infrastructure
- The stand-alone CA knows nothing about the user or computer account requesting the certificate. You must manually and explicitly include all details required to obtain the type of certificate you require.
- The stand-alone CA isn't aware of the accounts in the Active Directory. If a user certificate is required, the user account must be in the local SAM of the stand-alone CA machine.
- The stand-alone CA does not immediately issue a certificate after the certificate request is made. By default, an administrator must approve the certificate request and then the client must retrieve the certificate after an administrator approves the request. The reason is the stand-alone CA does *not* check the validity of the user account.
- You cannot add or remove certificate templates to the stand-alone CA.
- The stand-alone CA can not issue user certificates that are stored on Smart Cards that allow the user to log on to a Windows Server 2003 domain
- The stand-alone CA's self-signed certificate is not automatically added to the requester's Trust Root Certification Authorities certificate store. You must add the CA certificate to the Root Store manually.
- The stand-alone CA can receive limited support from the Active Directory when it is installed by a domain administrator in an Active Directory domain. When the stand-alone CA is installed by a domain administrator, the CA certificate of the stand-alone CA will be added to the Trusted Root Certification Authorities certificate store for all domain users and computers.

We recommend that you install a stand-alone CA only when:

- You do not have an Active Directory domain, and/or
- You do not require automatic deployment of certificates to users and computers

Before you proceed to install the Certification Authority please make sure that IIS incl. the World Wide Web Service is installed already

Installing Microsoft Certificate Services

Perform the following steps to install and configure a stand-alone CA on a Windows Server 2003 computer:

.

1. At your server, log on as a administrator. Click **Start**, point to **Control Panel** and click **Add/Remove Programs**.
2. In the **Add or Remove Programs** click the **Add/Remove Windows Components** button.
3. In the **Windows Components** dialog box, click on the **Certificate Services** entry and click the **Details** button.
4. In the **Certificate Services** dialog box, put a checkmark in the **Certificate Services CA** checkbox. A **Microsoft Certificate Services** dialog box appears and informs you that you can not change the machine name or the domain membership of the machine while it acts as a certificate server. Read the information in the dialog box and click **Yes**.
5. Both the **Certificate Services CA** and **Certificate Services Web Enrollment Support** checkboxes are checked. Click **OK** in the **Certificate Services** dialog box.
6. Click **Next** in the **Windows Components** dialog box
7. Select the **Stand-alone root CA** option on the **CA Type** page. Click **Next**.
8. On the **CA Identifying Information** page, type in a **Common name for this CA**. The common name of the CA is typically the DNS host name or NetBIOS name (computer name) of the machine running Certificate Services. In this example, the name of the machine is **WIN2003DC**, so we will enter **WIN2003DC** in the **Common name for this CA** text box. The default **Validity Period** of the CA's self-signed certificate is 5 years. Accept this default value unless you have a reason to change it. Click **Next**.
9. On the **Certificate Database Settings** page, use the default locations for the **Certificate Database** and **Certificate Database Log**. You do not need to specify a shared folder to store configuration information because this information will be stored in the Active Directory. Click **Next**.
10. Click **Yes** on the **Microsoft Certificate Services** dialog box informing you that Internet Information Services must be stopped temporarily.
11. Click **Yes** on the **Microsoft Certificate Services** dialog box informing you that Active Server Pages must be enabled on IIS if you wish to use the Certificate Services Web enrollment site.
12. Click **Finish** on the **Completing the Windows Components Wizard** page.
13. Close the **Add or Remove Programs** window.

The standalone Certificate Server is now ready to accept certificate requests.

Approving Certificate Requests to a Standalone Certificate Authority

The stand-alone CA does not automatically issue a certificate when a certificate request is made. The reason is the standalone CA is not able to confirm the validity of the request. It does not check the information provided by the requestor against a directory, such as the enterprise CA does when validating credentials against the Active Directory.

You should keep this default behavior for your published standalone CA in order to prevent users on the Internet from obtaining certificates without your review. Perform the following steps to approve a certificate request:

1. Click **Start** and point to **Administrative Tools**. Click on the **Certification Authority** link.
2. In the **Certification Authority** console, expand the server name and then click on the **Pending Certificates** node. You see a list of pending certificate requests in the right pane of the console. You can see who requested the certificate by scrolling to the right and looking under the **Requester Name**. Right click on the certificate request in the right pane of the console, point to **All Tasks** and click **Issue**. The certificate request is removed from the **Pending Requests** node.
3. Click on the **Issued Certificates** node in the left pane of the **Certification Authority** console. The certificate request you approved appears in the right pane of the console. This indicates the certificate request was approved. It does not indicate the machine issuing the request has returned to the Web enrollment site to retrieve the certificate.

Rather than approving every certificate request it might be more convenient to auto approve certificates. To do so please right click on the CA Name in the Console and configure the CA to automatically approve requests!

To download and apply for a certificate please browse to http://localhost/certsrv

In case you need to use the private key later on several machines to view Aloaha PDF Crypter encrypted PDF Documents please make sure to enable option "Mark keys as exportable"