

Trouble-shooting Digital Certificate Enrollment with Microsoft Windows Vista and Windows 7

This guide is to explore some of the issues that can be encountered using Windows Vista or Windows 7 when enrolling for a new digital certificate. If you do not already have a digital certificate, please visit PGP TrustCenter's website at <http://www.pgptrustcenter.com/digital-certificate-solutions> to obtain a "TC Personal ID" or "TC Business ID".

There are basically three known issues that are sometimes encountered enrolling for digital certificates when using Internet Explorer 7 or 8 with Windows Vista and Windows 7 operating systems:

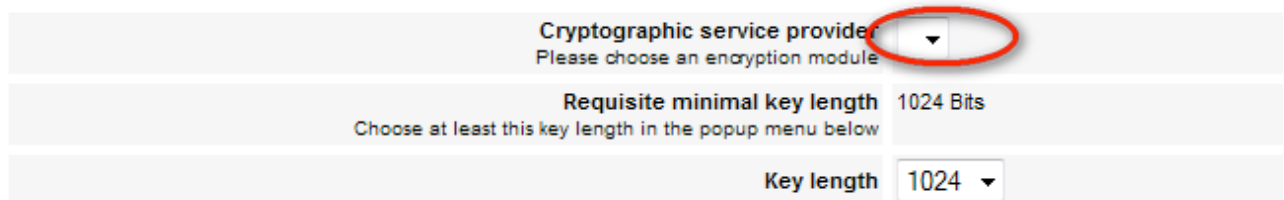
1. There is no Cryptographic Service Provider drop-down menu: Enable ActiveX controls.
2. Windows generates an error when installing the certificate: Add the TC website to your browser's trust sites list.
3. Windows fails the certificate installation due to an unknown Root certificate: Enable Root update in Windows. If installing the demo version of the "TC Business ID" certificate, manually install the TC Class 0 Root.

1. There is no Cryptographic Service Provider in the Drop-down Menu

If you are using Windows 7 and want to generate a certificate inside your browser but your Cryptographic Service Provider drop down menu is empty, you will to activate Active X.

▶ Cryptographic Service Provider

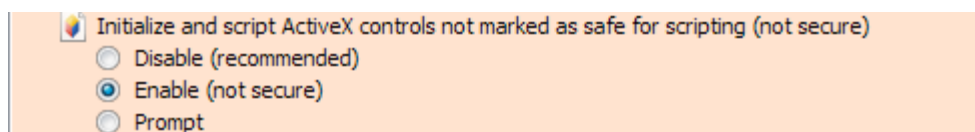
You can choose an encryption module, which will be used by Internet Explorer to generate the key pair. We recommend you select the Microsoft Enhanced Cryptographic Provider v1.0, which ensures a high security level (long key size).



Cryptographic service provider Please choose an encryption module	▼
Requisite minimal key length Choose at least this key length in the popup menu below	1024 Bits
Key length	1024 ▼

From Internet Explorer, click on **Tools | Internet Options | Tab Security Icon Internet** click on **Custom level...** and scroll down to ActiveX controls and plug-ins.

Here you can select the **Enable** option in the section "*Initialize and script ActiveX controls not marked as safe for scripting*".



Initialize and script ActiveX controls not marked as safe for scripting (not secure)

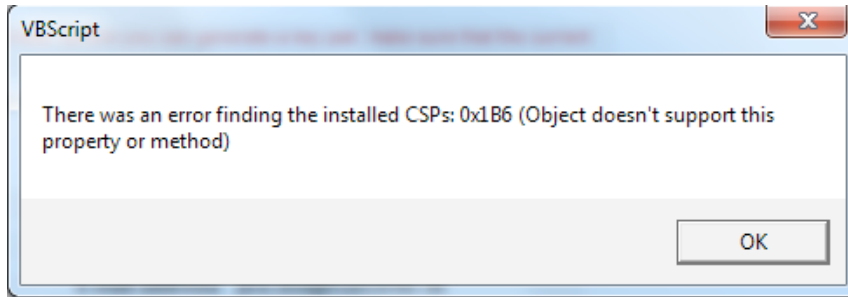
Disable (recommended)

Enable (not secure)

Prompt

You may also have to **enable** the “*active scripting*” option under the “*scripting*” section in the list that you have open above. (The default setting for IE8 on Windows 7 is “enable”.)

If you don't enable these options, you will most likely see the VBScript error message below.



2. Adding the TC TrustCenter Website to the Trusted Sites List

If using a Windows Vista or Windows 7 computer on a corporate network, you will most likely have to add the TC TrustCenter Website to your trusted sites to allow enrollment of certificates. You can do this manually or automatically by using a registry file which can be downloaded.

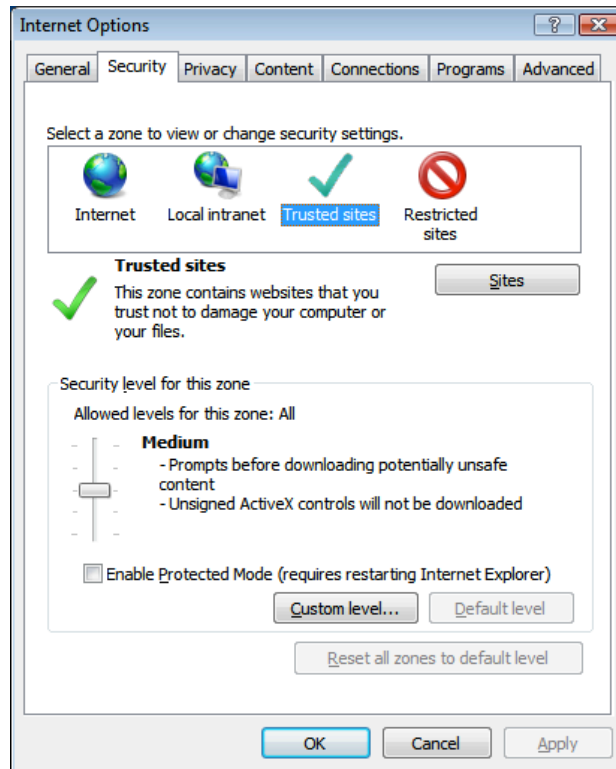
Automatically trusting the TC TrustCenter website:

Download the registry file and open it by double clicking it. The TC TrustCenter Website is now added to your trusted sites list. Download this file here:

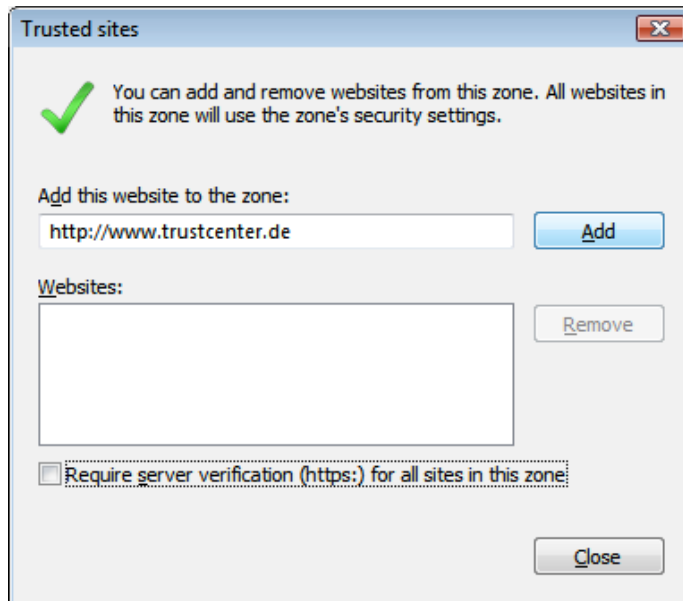
http://www.trustcenter.de/media/Trusted_sites_tc_TrustCenter.reg

Manually trusting the TC TrustCenter website:

Open Internet Explorer and select **Tools**, and then select the **Security** tab in the “Internet Options” dialog.



Select the **Trusted Sites** icon, and click on the **Sites** button. This will bring up a dialog which will allow you to add or remove sites from the zone. In this example, we have clicked on **Add** in order to add the TC TrustCenter website to the trusted list: <http://www.trustcenter.de>.



3. Why is the 2048 Bit TC TrustCenter Root Certificate not Pre-Installed in my Windows System?

In Windows XP, Windows 2003 and Windows Vista not all trusted root certificates are included in the installation media. The root certificates are obtained through an automatic Windows update.

In Windows Vista root certificates are automatically updated when a user visits a secure Web site (by using HTTPS), reads a secure email (S/MIME), or downloads an ActiveX control that is signed (code signing) and encounters a new root certificate. This process is seamless to the user, so no security dialog boxes or warnings are displayed.

For Windows XP and earlier, the Root certificates are delivered via the Microsoft Update Catalog. Visitors to the Catalog can search for “root update” or the KB article for the Root Certificate Program, “KB931125”, and download the latest Root Update package. Root Updates are cumulative, so it is only necessary to install the latest one to receive all root certificates in the Program.

Enabling Root Certificate Update in Windows Vista

If the root certificate does not appear to be installed, the root update may have been disabled in the Group Policy Settings. In Windows Vista, some of these policy settings can be found in Group Policy under the category named **Internet Communication Management**. This category can be seen through the Group Policy Object Editor (which can be opened through the Group Policy Management Console). **Internet Communication Management** is located in two places:

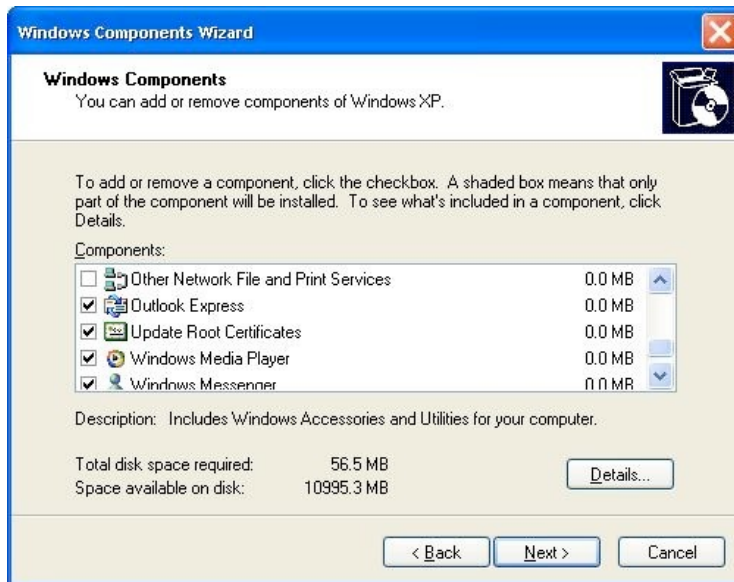
- Computer Configuration\Administrative Templates\System
- User Configuration\Administrative Templates\System\

1. Expand **Computer Configuration**, expand **Administrative Templates**, expand **System**, expand **Internet Communication Management**, and then click **Internet Communication settings**.
2. In the details pane, double-click **Turn off Automatic Root Certificates Update**, and then click **Disable**.

Enabling Root Certificate Update in Windows XP

The automatic Root Update can be used in Windows XP by adding it to the list of Windows Components. To access this list:

- Open the Control Panel
- Double Click Add-Remove Programs
- Click Add-Remove Windows Components
- Select **Update Root Certificates** and complete the Wizard



References:

- <http://technet.microsoft.com/en-us/library/cc749331.aspx>
- <http://technet.microsoft.com/en-us/library/cc749503.aspx>
- <http://technet.microsoft.com/en-us/library/bb457160.aspx>
- <http://support.microsoft.com/kb/931125>
- <http://technet.microsoft.com/en-ca/library/cc751157.aspx>
- <http://technet.microsoft.com/en-us/library/cc734054%28WS.10%29.aspx>

Using the Demo Certificate for TC Business ID

If you are testing the demo version of the TC Business ID certificate, you must manually install the Demo Root CA first. You can install this TC Class 0 Root by clicking on the following link:

https://www.trustcenter.de/en/infocenter/root_certificates.htm#2011

Once the demo Root is installed and trusted, you should then be able to install your demo certificate.