Time Stamp Server
Installation Manual

Introduction

Time stamping is an important mechanism for the long-term preservation of digital signatures, time sealing of data objects to prove when they were received, protecting copyright and intellectual property and for the provision of notarization services.

Our Time Stamp Server works as an IIS application for most Windows web servers. It means that it is not required to operate an extra TSA machine.

Links

Download Time Stamp Server for IIS: http://www.signfiles.com/apps/TSAServer.zip
Time Stamp Server Live Demo: https://ca.signfiles.com/tsa/
Time Stamp Server main page: http://www.signfiles.com/timestamping/

Time Stamp PDF and Microsoft Office Documents
Use the TSA Server for Microsoft Authenticode

Warning and Disclaimer

Every effort has been made to make this manual as complete and accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this manual.

Trademarks

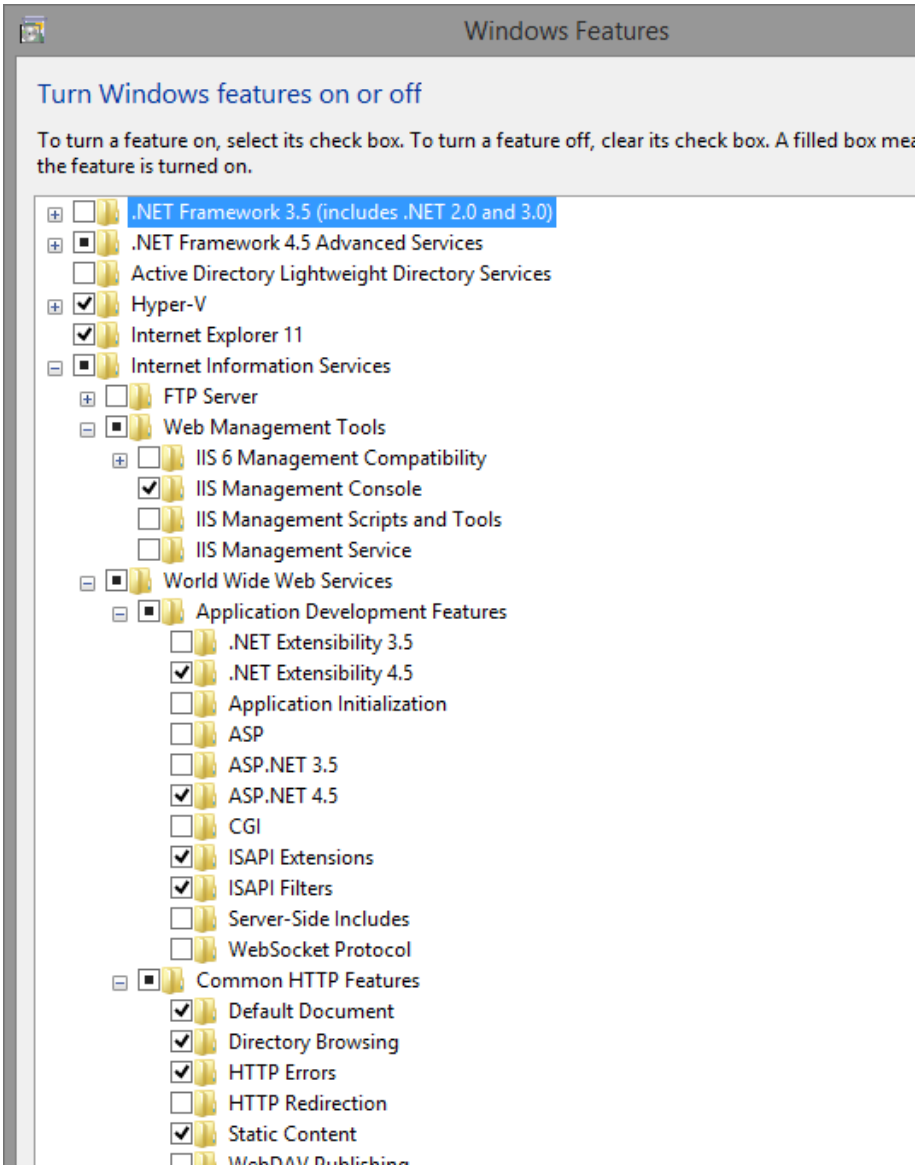
.NET, Visual Studio .NET are trademarks of Microsoft Inc.
Adobe, Adobe Reader are trademarks of Adobe Systems Inc.
All other trademarks are the property of their respective owners.

Prerequisites

Time Stamp Server requires the following:

- Windows operating system with IIS (Windows 7 or later)
- Microsoft .NET Framework 4.0
- ASP.NET enabled on your IIS

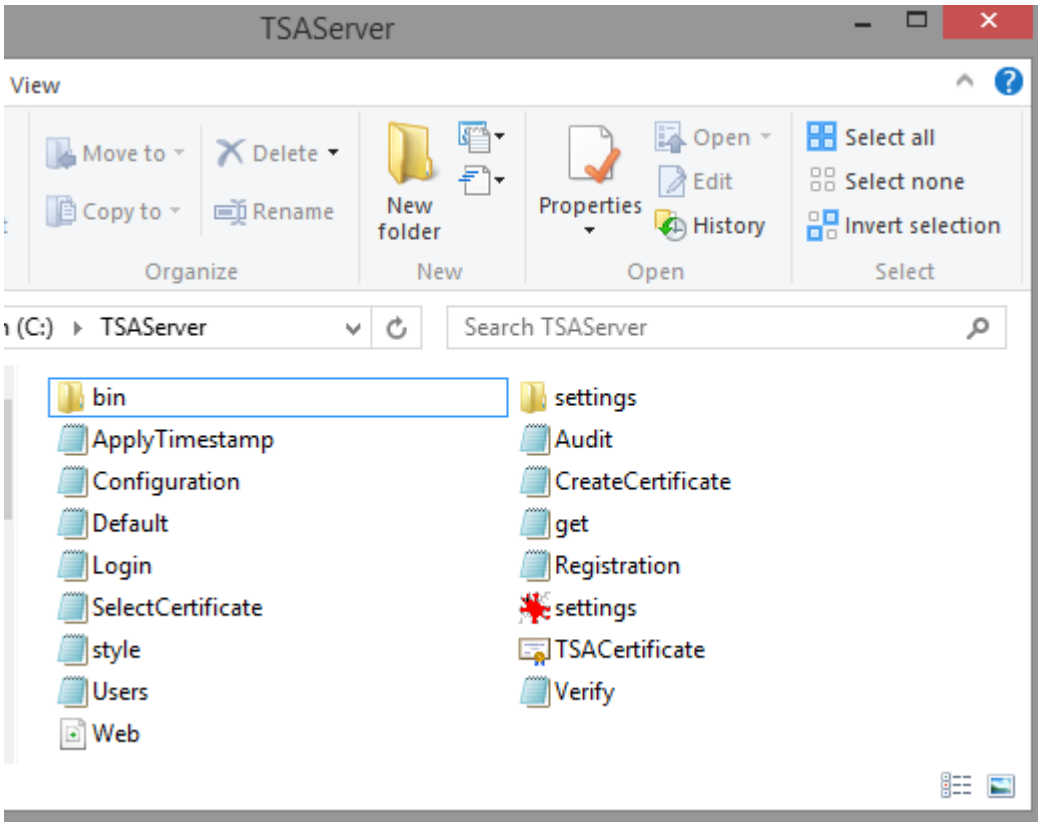
To enable ASP.NET in your IIS web server, go to *Control Panel – Programs and Features – Turn Windows features on or off* and on *Internet Information Services*, select ASP.NET as on the image below.



Enable ASP.NET and Custom Features

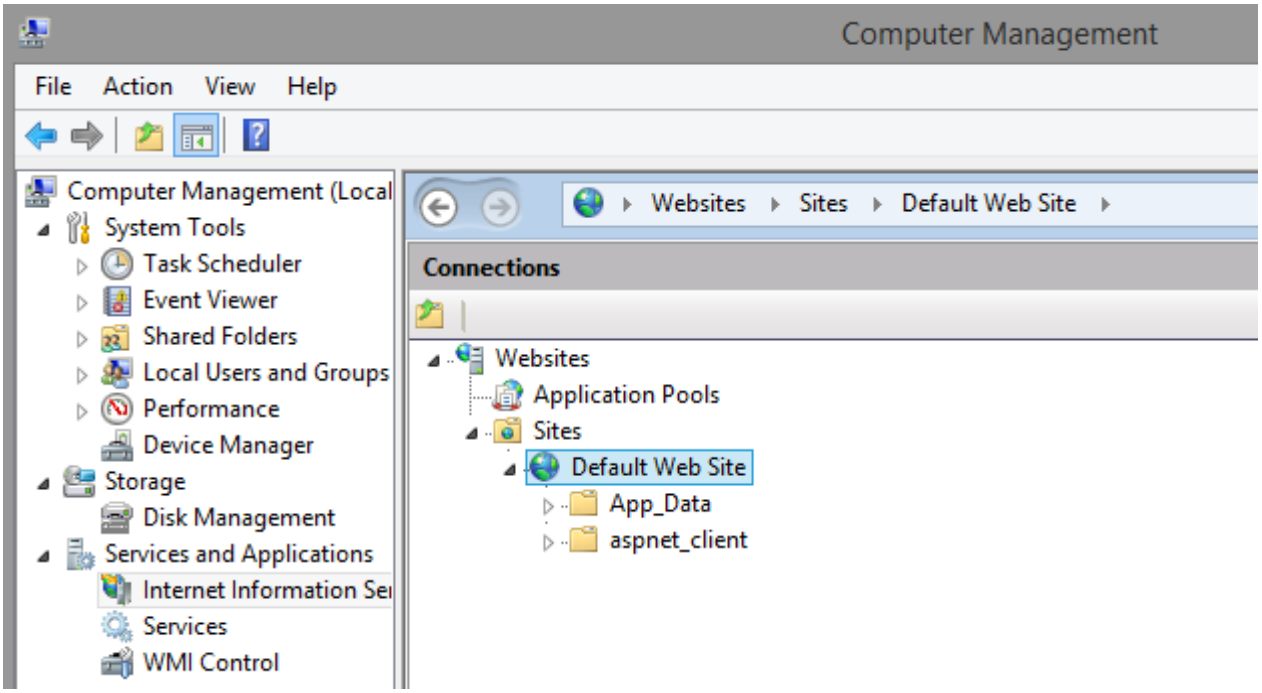
Installation

Download **Time Stamp Server** from this link: http://www.signfiles.com/apps/TSAServer.zip and unzip the content of the TSAServer folder on your IIS webserver (e.g. *C:\TSAServer*).



Time Stamp Server Folder Content

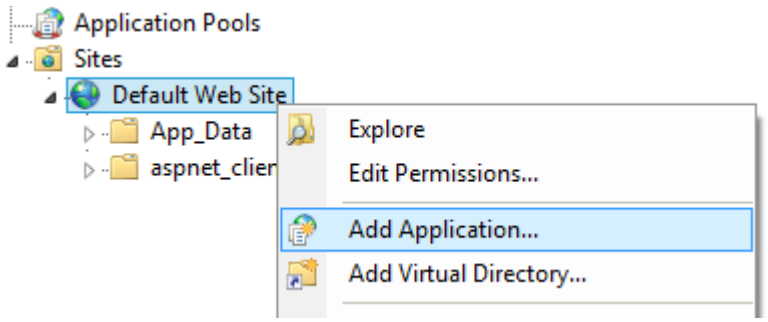
Time Stamp Server must be added as an application on IIS web server.
Go to *Computer* icon – Right click *Manage* – Computer Management – Services and Applications – Internet Information Services (IIS) Manager.

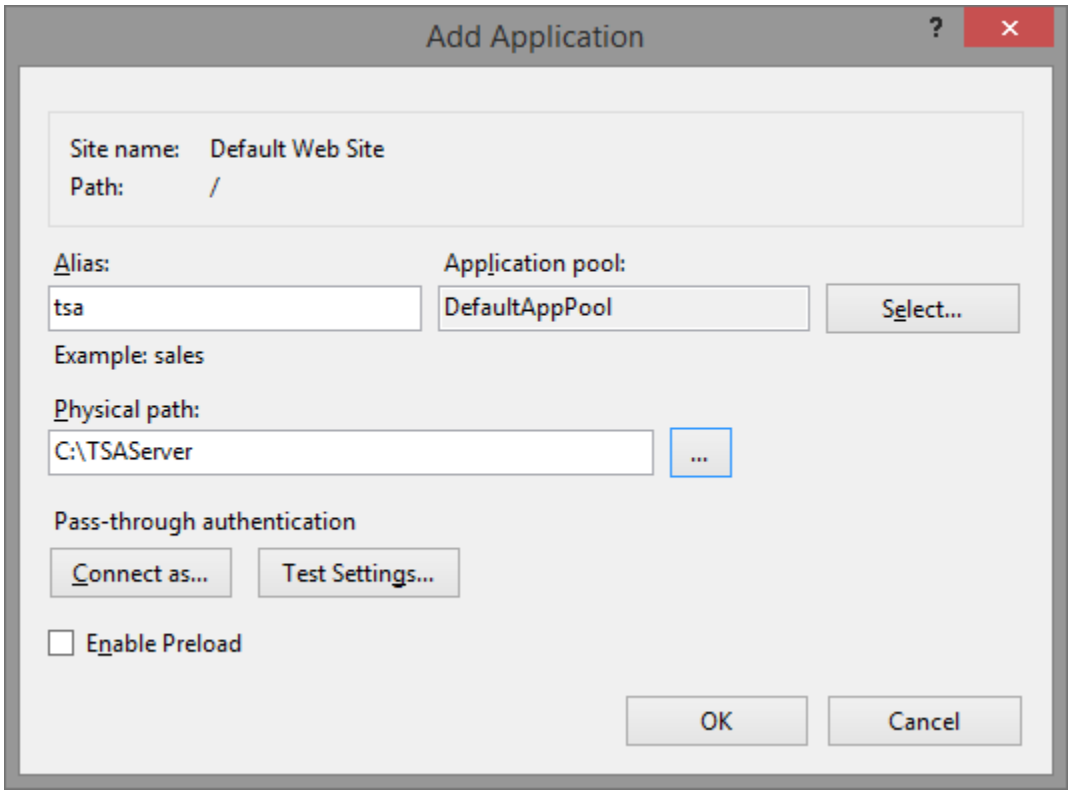


IIS Websites

On your website, **Time Stamp Server** must be added as a new Application.

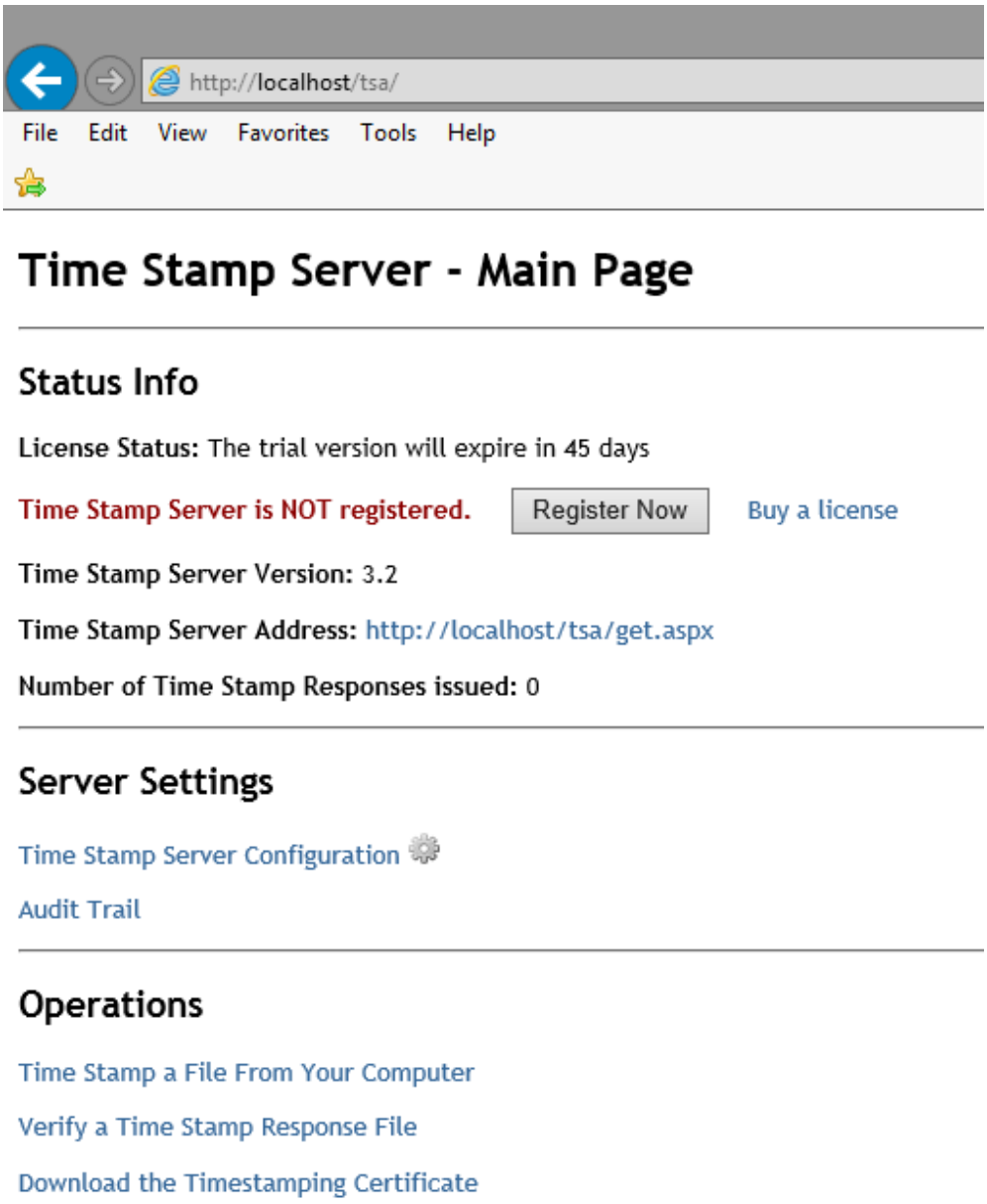
Right click on your IIS website (*Default Web Site*) – *Add Application...* and set the application alias and the physical path as below.





Attention: Time Stamp Server requires Read, Write and Execute permissions to be enabled for the physical path. IIS user must have this rights for the specified physical path.

At this moment, **Time Stamp Server** is be installed. To check the installation, go to: http://localhost/tsa/.



TSA Server Main Page

Time Stamp Server Certificate

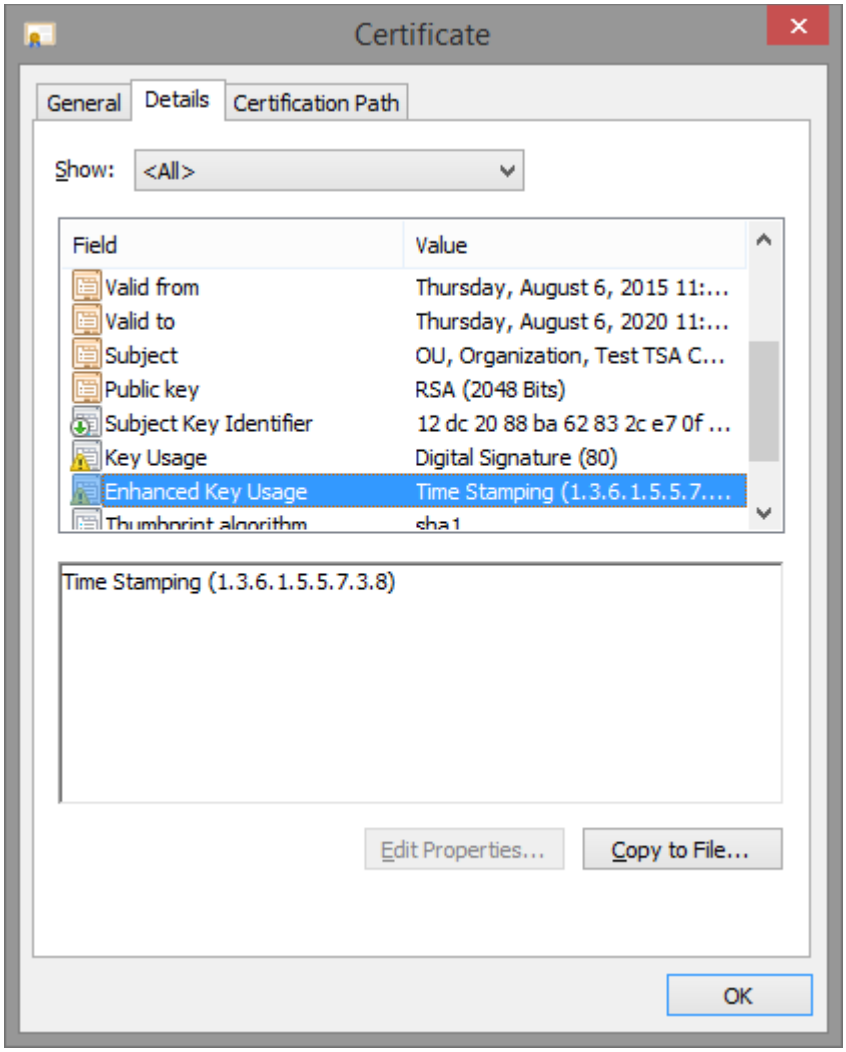
Create a Timestamping Certificate

Time Stamp Server needs a special digital certificate (Timestamping certificate) to be used in order to digitally sign the Time Stamp Requests came from external applications.

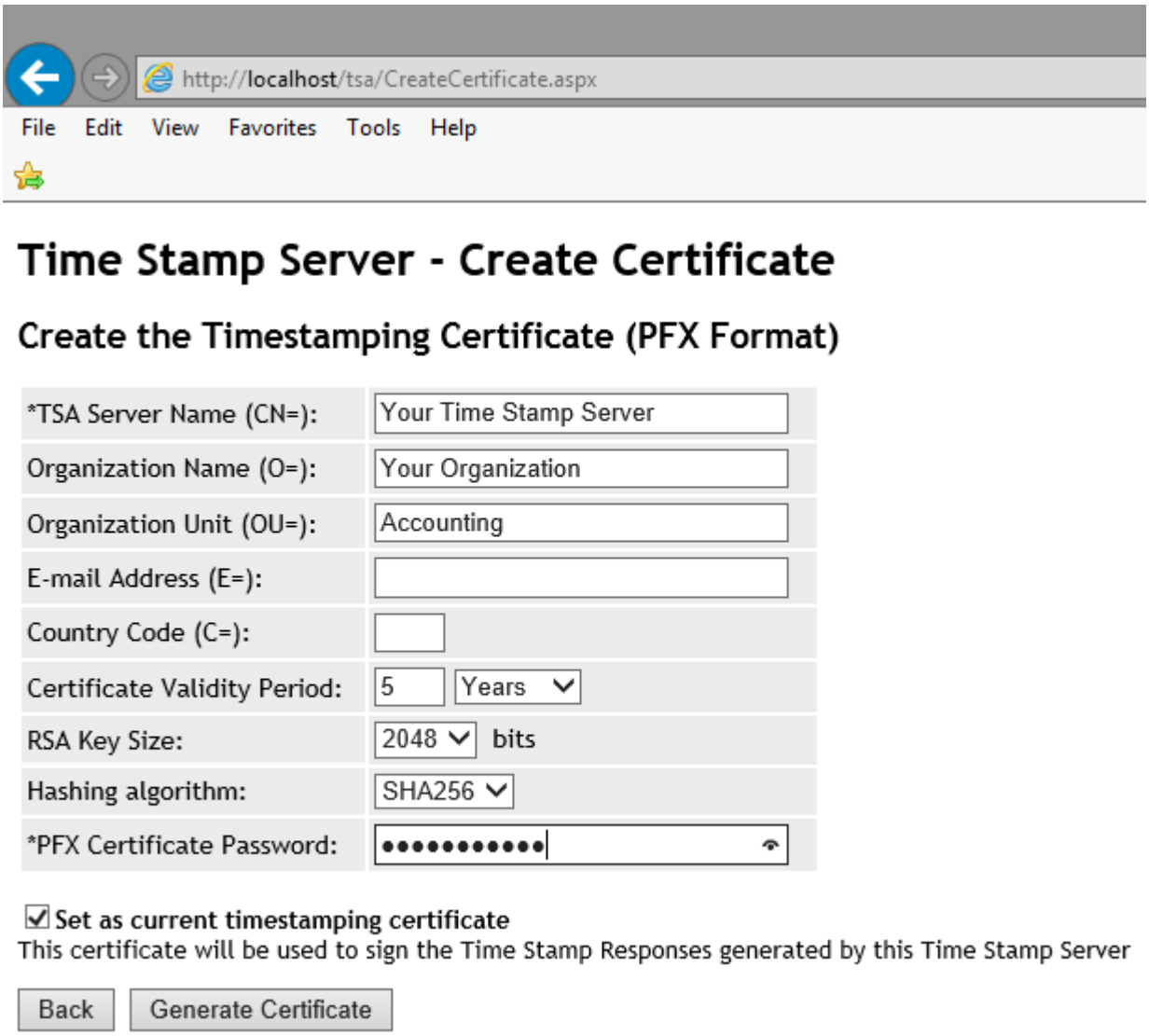
Note that the SSL certificates (for HTTPS connections), Code Signing or regular digital signatures certificates cannot be used as time stamp certificates.

The Timestamping certificate is a special type of certificate and must be created as below:

- Use RSA 2048 (or RSA1024 for large quantity of timestamps in a short time)
- Key Usage extension marked as critical: Digital Signature
- Extended Key Usage - add ONLY Time Stamping extension (OID: 1.3.6.1.5.5.7.3.8) as critical.
- Expiration date: at least 5 years.



If you do not have a such of certificate, it could be created by Time Stamp Server by following this link: http://localhost/tsa/CreateCertificate.aspx



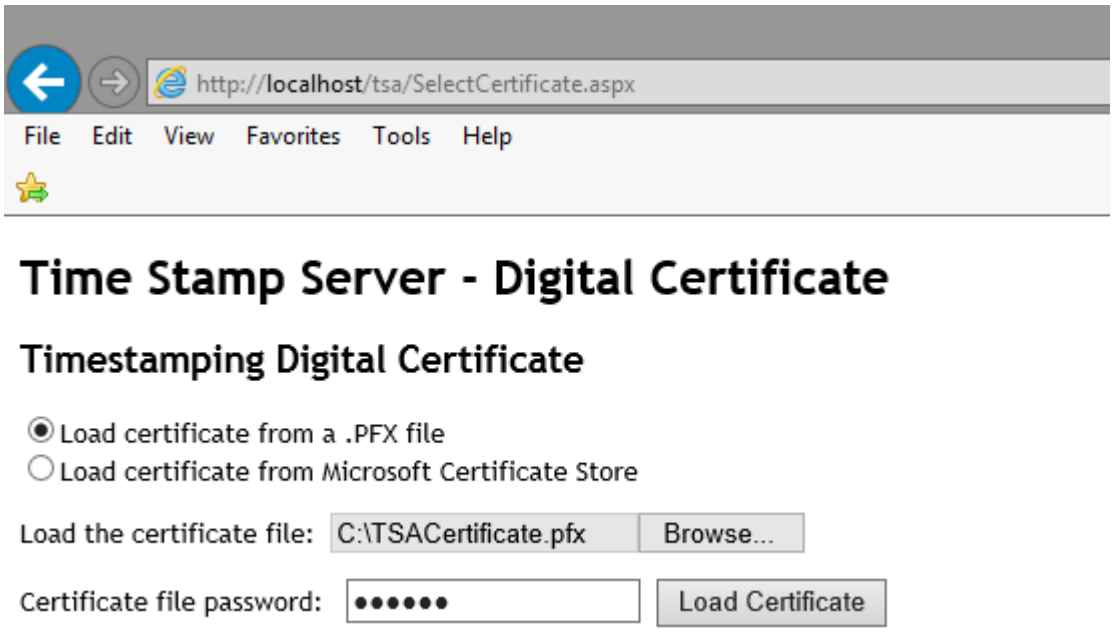
If *Set as current Timestamping certificate* checkbox is checked, this certificate will be used to digitally sign the Time Stamping Responses generated by the Time Stamp Server.

Select the Timestamping Certificate From a PFX File

Time Stamp Server can use for time stamp operation a PFX certificate already generated by an external application (like X.509 Certificate Generator).

Also, you can import a Timestamping certificate issued by Microsoft Certification Authority installed on your Windows Server.

To select a PFX certificate from your computer, follow this link:
http://localhost/tsa/SelectCertificate.aspx



To use this certificate, be sure that the PFX password is correct. After *Load Certificate* button is pressed, the PFX certificate is verified if it can be used for time stamp operation.

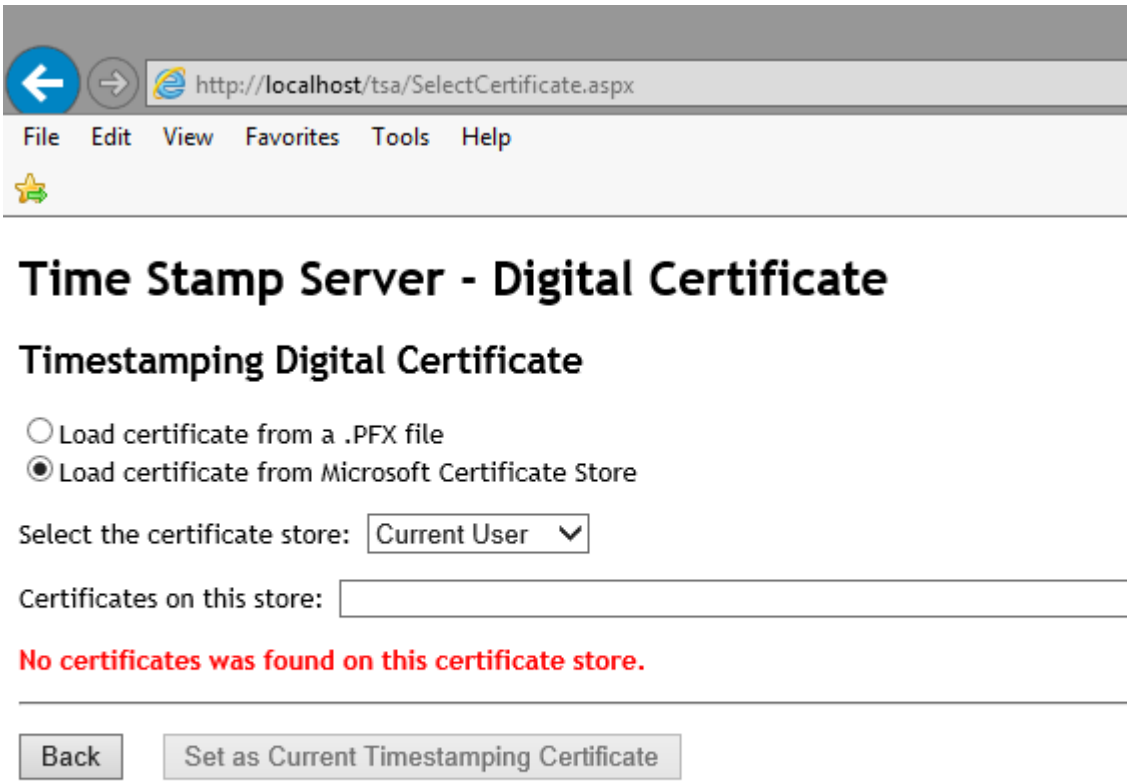
If *Set as current Timestamping certificate* button is pressed, the certificate will be saved and the PFX password will be encrypted on the server.

Note that the Timestamping PFX certificate must have some special extensions (see section above: *Create a Timestamping Certificate*).

Select the Timestamping Certificate from Microsoft Certificate Store

In some cases, the Timestamping certificate is not available as PFX file but it is installed on Microsoft Certificate Store (e.g certificates stored on Hardware Security Modules – HSM).

By default, the Microsoft Certificate Store certificates are not available for ASP.NET applications.

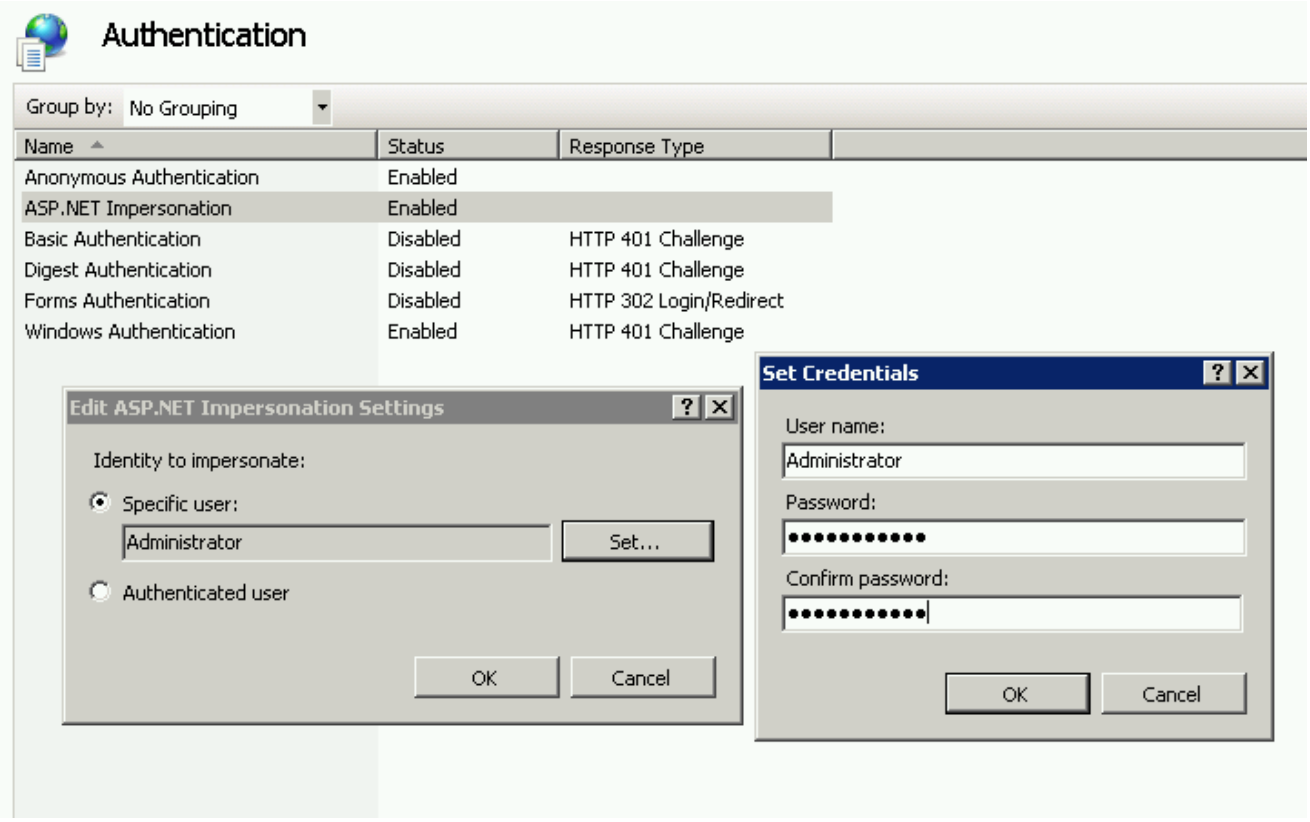


The User Certificates installed on Microsoft Store cannot be accessed

To enable access to Microsoft Certificate Store of Time Stamp Server application, follow the steps below.

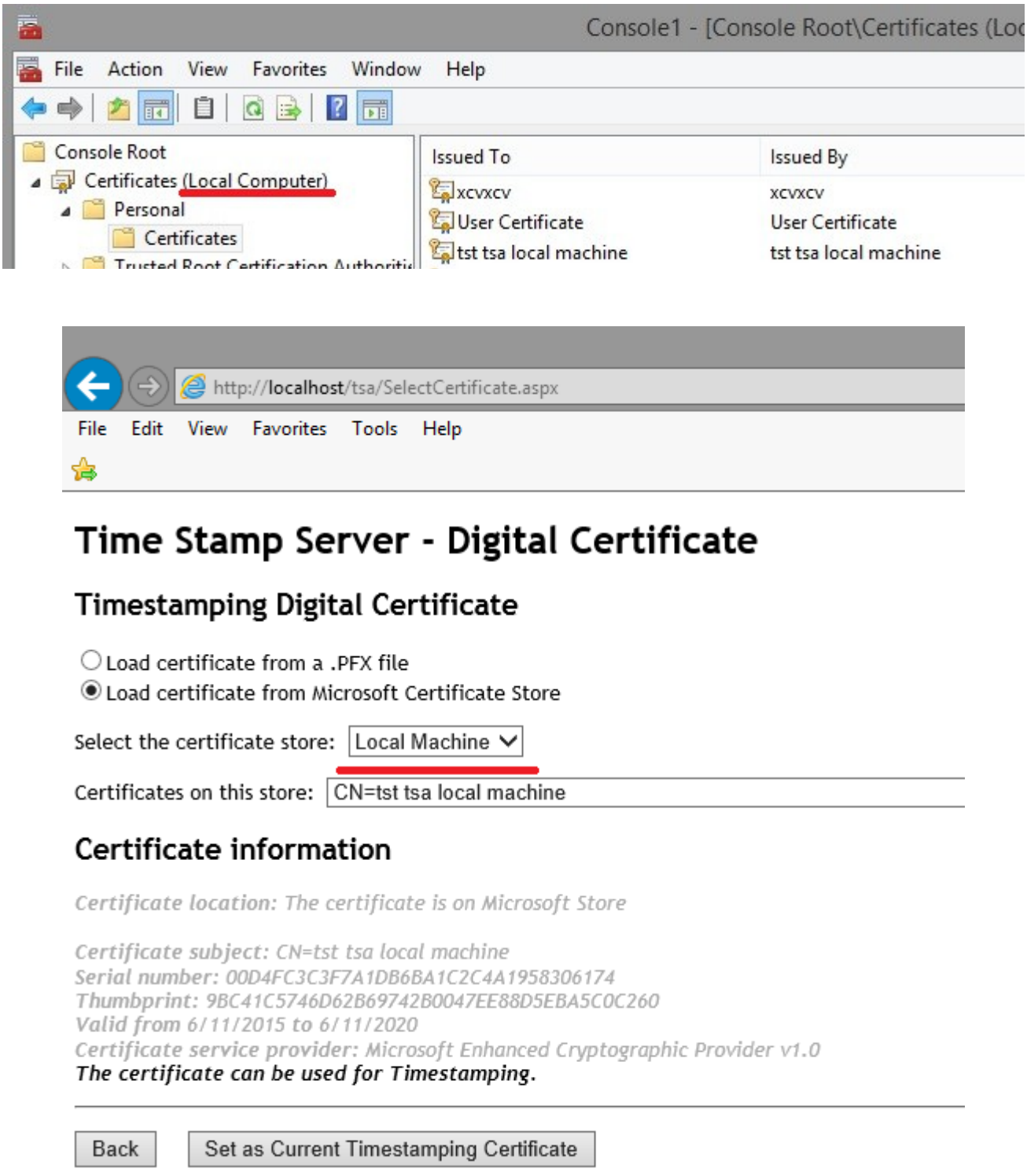
On *Authentication* section of the **Time Stamp Server** application (IIS), be sure that *ASP.NET Impersonation* is enabled and the provided user is the same as the Timestamping digital certificate user (e.g. the Administrator account ar an account with high privileges).

Attention: Be sure that the certificate was issued and is available for the selected user. If the certificate was issued in other Windows account, it cannot be used.



Enable Certificates Located on Microsoft Certificate Store

As an alternative, in case that the certificate is installed on Current User will not work or it is not visible, the certificate can be installed on Local Machine store instead of Current User (mmc – Add/Remove Snap-in-Certificates-Computer Account).

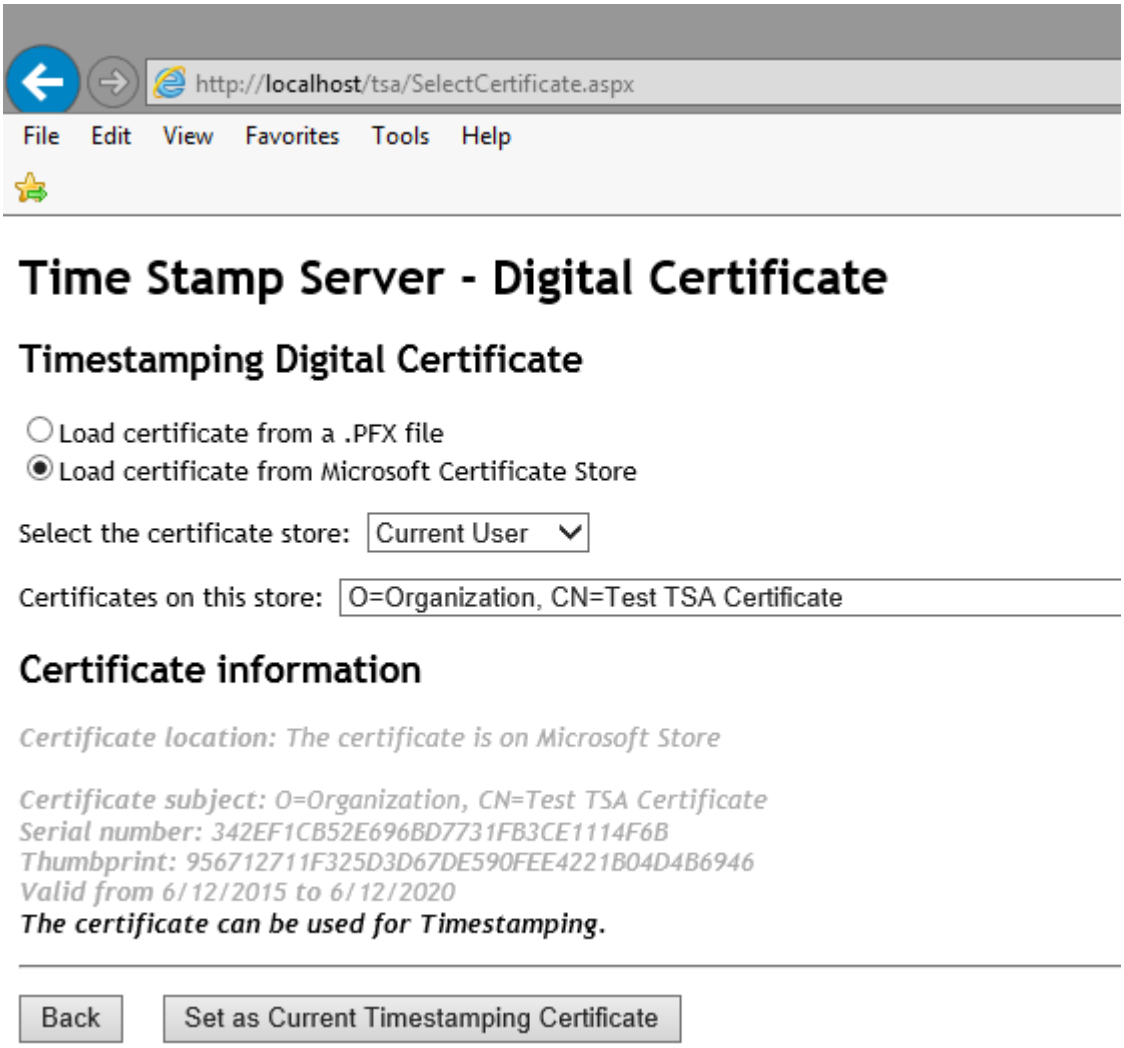


A certificate installed on Local Machine Certificate Store

After the certificate is selected, if *Set as current Timestamping certificate* button is pressed, the certificate is verified if it can be used for time stamp operation.

After that, the certificate Thumbprint will be saved encrypted on the configuration file in order to be used as Timestamping certificate.

Note that the Timestamping certificate must have some special extensions (see section above: *Create a Timestamping Certificate*).



Microsoft Store Timestamping Certificate Selection

Certificates Installed on Hardware Devices

If the certificate is stored on a HSM (Hardware Security Module like Luna), be sure that the partition is activated and the certificate can be used for digital signature without any user intervention (disable PED PIN, Administrator PIN, any other PIN mechanisms).

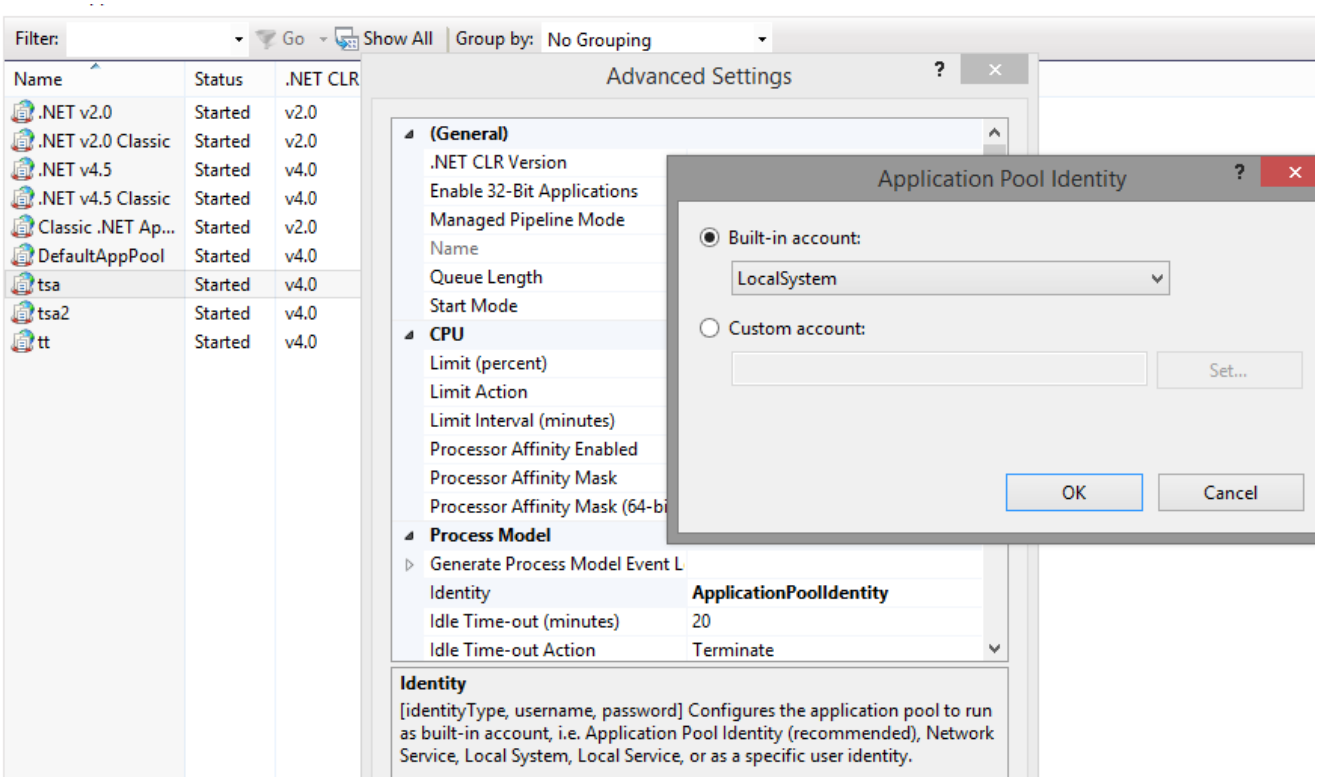
Time Stamp Server can use only the certificates available on Microsoft Certificate Store. If the HSM device has only PKCS#11 interface the HSM certificate cannot be used until the certificate is not installed on Microsoft Certificate Store.

To issue a CSR (Certificate Signing Request) on a hardware device, follow this steps: How to Generate a Certificate on a Hardware Device

In most of the cases, the certificates stored on smart cards/USB tokens cannot be used in ASP.NET websites because of the middleware limitations and because the certificate is protected by a PIN dialog that cannot be bypassed.

Because of this limitations, we cannot guarantee that the timestamping certificates stored on smart cards/USB tokens can be used by the Time Stamp Server.

In some cases you might need to change the IIS Application Pool in order to use an account with high privileges.



Time Stamp Server Options

General Settings

Time Stamp Server has some additional settings available by following this link: http://localhost/tsa/Configuration.aspx

Time Stamp Server Policy ID - Every Time Stamp Server must issue timestamps using a Policy ID. You can set this field on the configuration by entering a valid Object identifier.

Time Stamp Request must include the current TSA Policy ID - If the requests sent by the client not contains the TSA Policy ID, they can be rejected. The Time Stamp response will contain the following error status message: *"Invalid TSA Request. The TSA Policy ID is not accepted by the TSA Server."*.

Set Ordering to True - If the ordering field is present and set to true, every time-stamp token can always be ordered regardless of the accuracy.

Time stamp request must include a Nonce extension - NONCE is used to detect replays attacks. The TSA may reject the requests that not contain a NONCE. The Time Stamp response will contain the following error status message: *"Invalid TSA Request. NONCE field must be set."*.

Include whole chain on the Time Stamp Response - The TSA certificate is usually issued a a Root CA. The time stamping response can contains the entire certificate path.

If the Time Stamp Server will be used for time stamp an important number of documents and the size of each document should be small, disable this option.

Set Accuracy - By adding the accuracy value, an upper limit of the time at which the Time Stamp Response has been created by the Time Stamp Server can be obtained. The accuracy of the TSA server can be also set on the interface.

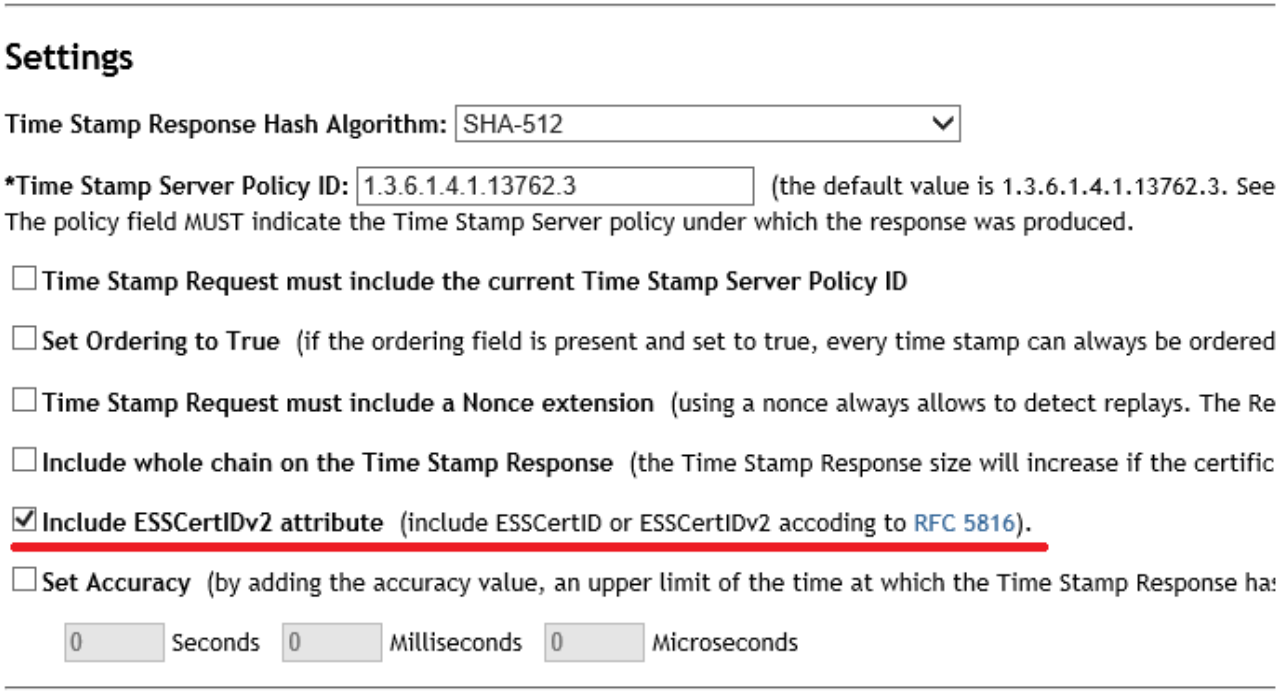
Log all the Time Stamp Responses
By checking *Log all the Time Stamp Responses issued by the Time Stamp Server* checkbox, all Time Stamp Responses will be saved on a CSV file. If you are planning to issue more that 100.000 timestamps or the server speed is an important factor, use this option carefully.

Include ESSCertIDv2 Attribute According to RFC 5816

In some cases, ESSCertIDv2 must be added as signed attribute on the Time Stamp response.

ESSCertID provides a means based on the SHA-1 hash algorithm for identifying the certificate used to verify the signature on a time stamp.
The use of ESSCertIDv2 aims to enable implementers to comply with policies that require phasing out all uses of the SHA-1 algorithm.

In order to enable ESSCertIDv2 attribute, check the checkbox *Include ESSCertIDv2 attribute* on the Configuration page.

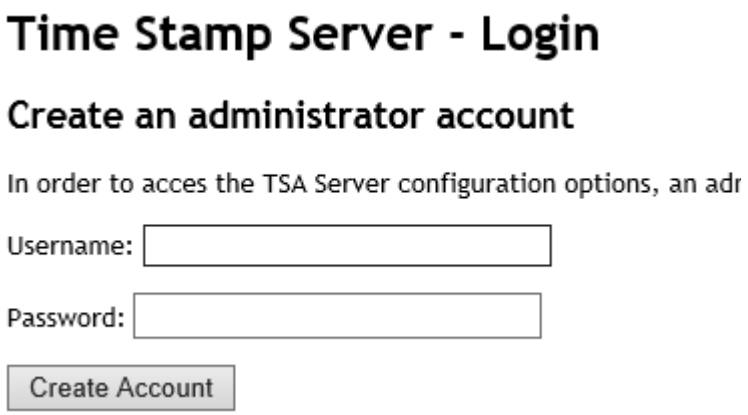


Create an Administrator Account

On the default installation of the Time Stamp Server, the Administrator account is disabled so the Time Stamp Server settings can be viewed and changed by anybody.

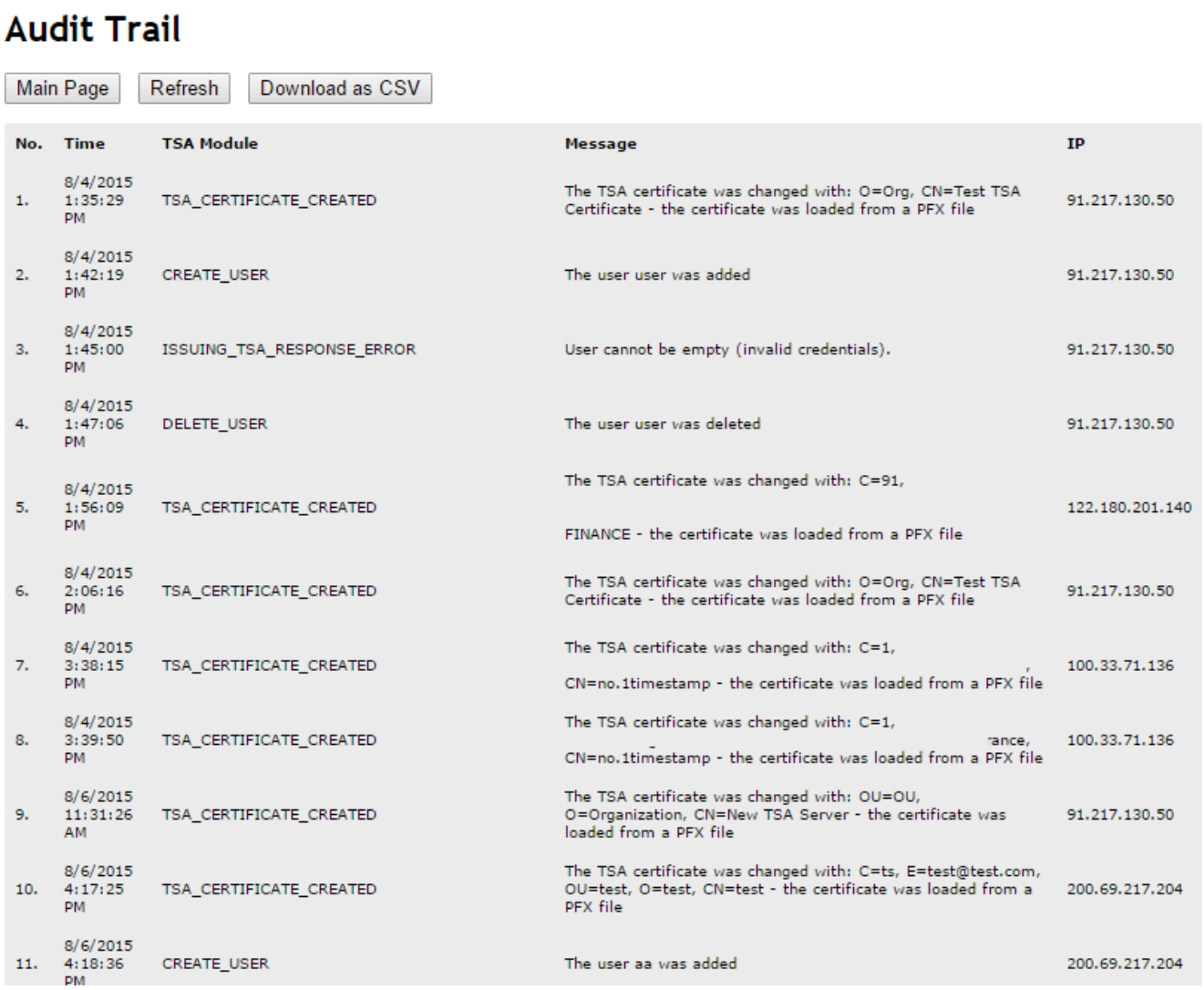
To enable the Administrator Account, manually create a file named *authentication.sys* on the */settings* directory and the Administrator Account will be enabled.

Attention: In order to create and use the Administrator account, the Time Stamp Server must NOT be accessed from localhost (e.g. http://localhost/tsa/) but using the Internet name (e.g. https://ca.signfiles.com/tsa/).



Time Stamp Server Audit Trail

All Time Stamp Server operations and errors are logged on the Audit Trail Page.
Also, the raw file log is available on the *\settings\log.sys* file.



Audit Trail

Main Page | Refresh | Download as CSV

No.	Time	TSA Module	Message	IP
1.	8/4/2015 1:35:29 PM	TSA_CERTIFICATE_CREATED	The TSA certificate was changed with: O=Org, CN=Test TSA Certificate - the certificate was loaded from a PFX file	91.217.130.50
2.	8/4/2015 1:42:19 PM	CREATE_USER	The user user was added	91.217.130.50
3.	8/4/2015 1:45:00 PM	ISSUING_TSA_RESPONSE_ERROR	User cannot be empty (invalid credentials).	91.217.130.50
4.	8/4/2015 1:47:06 PM	DELETE_USER	The user user was deleted	91.217.130.50
5.	8/4/2015 1:56:09 PM	TSA_CERTIFICATE_CREATED	The TSA certificate was changed with: C=91, FINANCE - the certificate was loaded from a PFX file	122.180.201.140
6.	8/4/2015 2:06:16 PM	TSA_CERTIFICATE_CREATED	The TSA certificate was changed with: O=Org, CN=Test TSA Certificate - the certificate was loaded from a PFX file	91.217.130.50
7.	8/4/2015 3:38:15 PM	TSA_CERTIFICATE_CREATED	The TSA certificate was changed with: C=1, CN=no.1timestamp - the certificate was loaded from a PFX file	100.33.71.136
8.	8/4/2015 3:39:50 PM	TSA_CERTIFICATE_CREATED	The TSA certificate was changed with: C=1, CN=no.1timestamp - the certificate was loaded from a PFX file	100.33.71.136
9.	8/6/2015 11:31:26 AM	TSA_CERTIFICATE_CREATED	The TSA certificate was changed with: OU=OU, O=Organization, CN=New TSA Server - the certificate was loaded from a PFX file	91.217.130.50
10.	8/6/2015 4:17:25 PM	TSA_CERTIFICATE_CREATED	The TSA certificate was changed with: C=ts, E=test@test.com, OU=test, O=test, CN=test - the certificate was loaded from a PFX file	200.69.217.204
11.	8/6/2015 4:18:36 PM	CREATE_USER	The user aa was added	200.69.217.204

Time Stamp Server Client Authentication

The **Time Stamp Server** could issue Time Stamp Responses only if the user is authenticated.

To allow only authenticated users to access the Time Stamp Server, check *Only authenticated users can obtain a Time Stamp Response from this server* checkbox on configuration page and add users on the list by pressing *Manage Users* button.

If the program has an option to enter the username and password, fill the fields with the proper values.

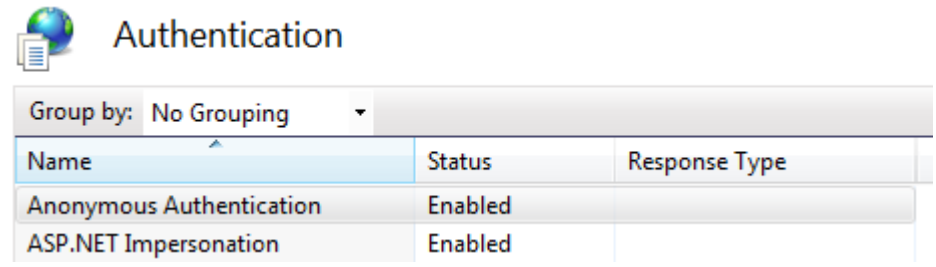
Attention: If this option is not available or the program not accept basic authentication (like Adobe Reader), the Time Stamp Server can be accessed like this: http://localhost/tsa/get.aspx?u=username&p=passwd

If an invalid user will acces the Time Stamp Server, the following error codes will be returned:
0 - “Operation OK” (everything was OK, the response is correct)
2 - “User cannot be empty (invalid credentials)” - Invalid credentials to login to the TSA server.
2 - “User not exist (invalid credentials)” - Invalid credentials to login to the TSA server.
2- "User is not active."
2- "Incorrect password (invalid credentials)." - Invalid credentials to login to the TSA server.
2- "Not enough time stamp requests."

For authentication, Time Stamp clients like .NET Digital Signature Library SDK or PDF Signer send the username and the password as for HTTP Basic Authentication.

For this reason, the basic authentication must be disabled on IIS like below because the verification of the username and password will not be done by the IIS but by the TSA Server internal engine.

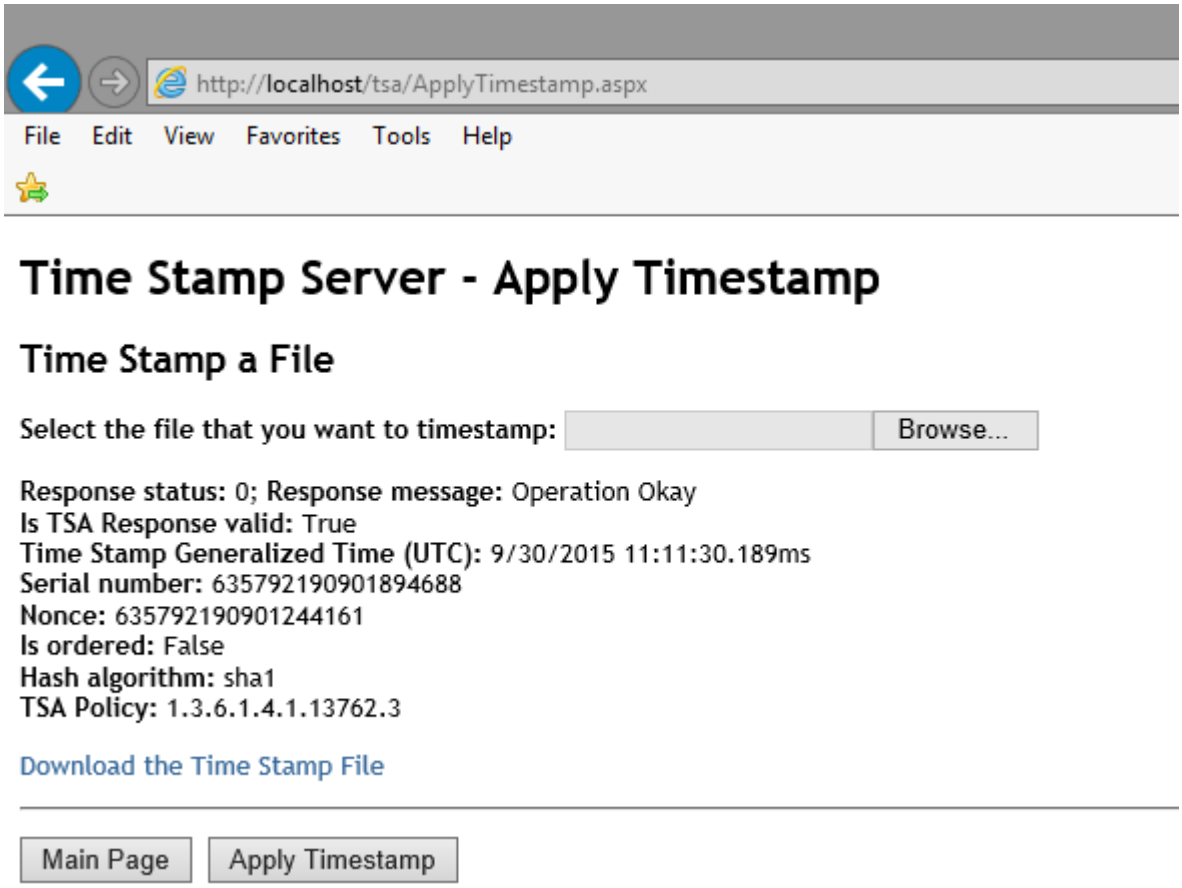
Authentication on webserver



Authentication on IIS

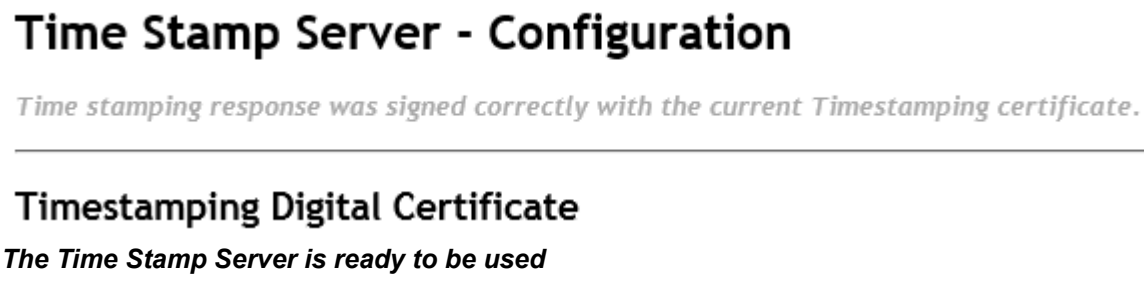
Timestamp a File Directly From the Time Stamp Server

In order to manually time stamp a file, go to http://localhost/tsa/ApplyTimestamp.aspx and select the file that must be timestamped.

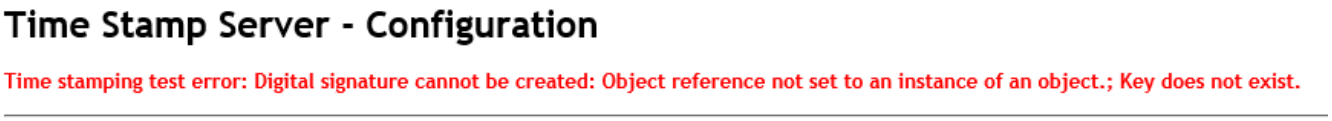


Verify the Time Stamp Server

After all customizations are made, you can test the Time Stamp Server configuration by pressing *Run a Test* button available on the Configuration page.



If the certificate is not correctly installed, you will get an error like below. On this case you must reinstall/reissue the certificate or to check the user rights (see the section *Select the Timestamping Certificate from Microsoft Certificate Store*).



The private key of the certificate is not accessible and it cannot be used.

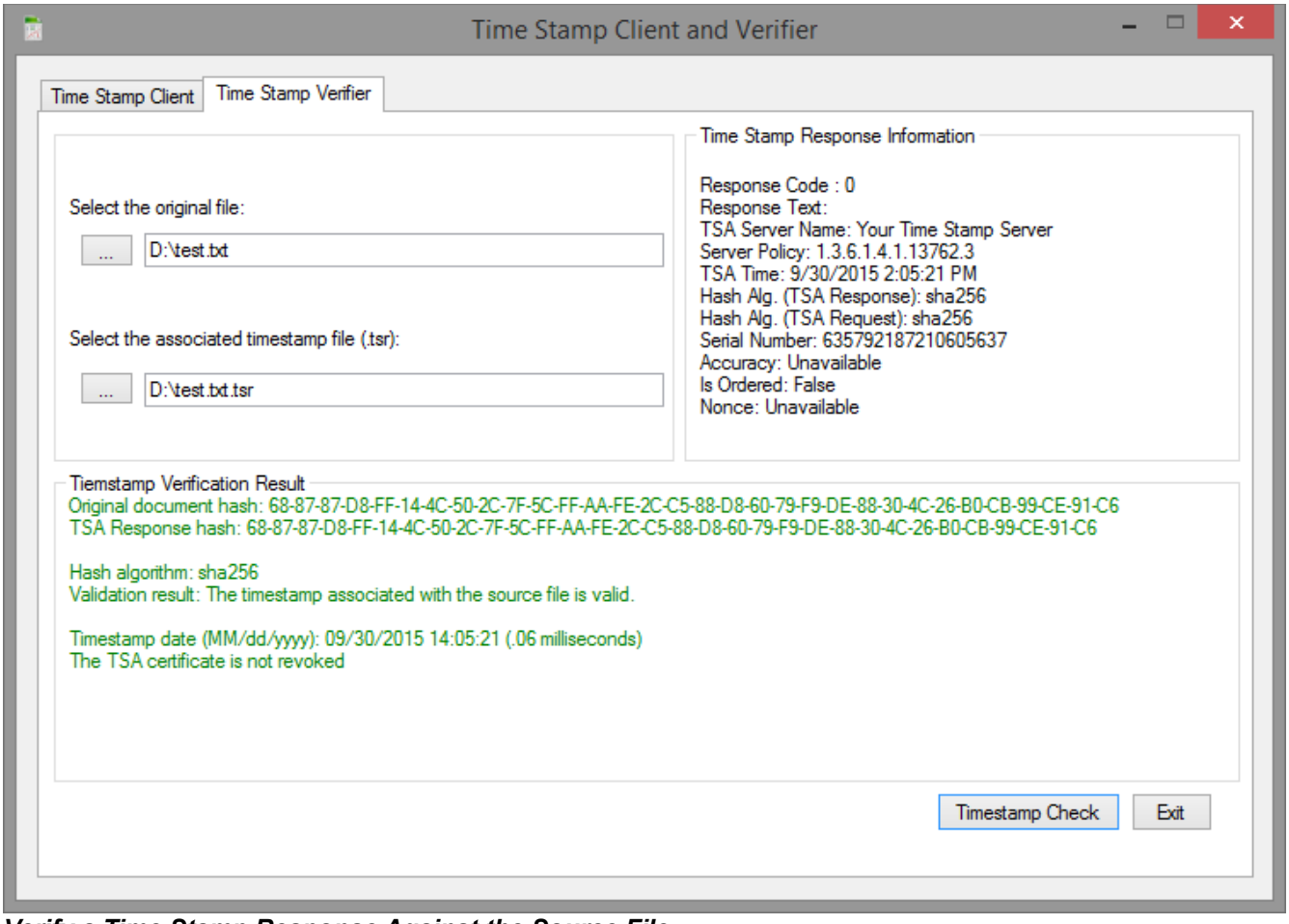
The private key of the certificate is not accessible and it cannot be used.

Time Stamp Client Application

After all necessary customizations are made, the Time Stamp Server is now available at this link: http://localhost/tsa/get.aspx

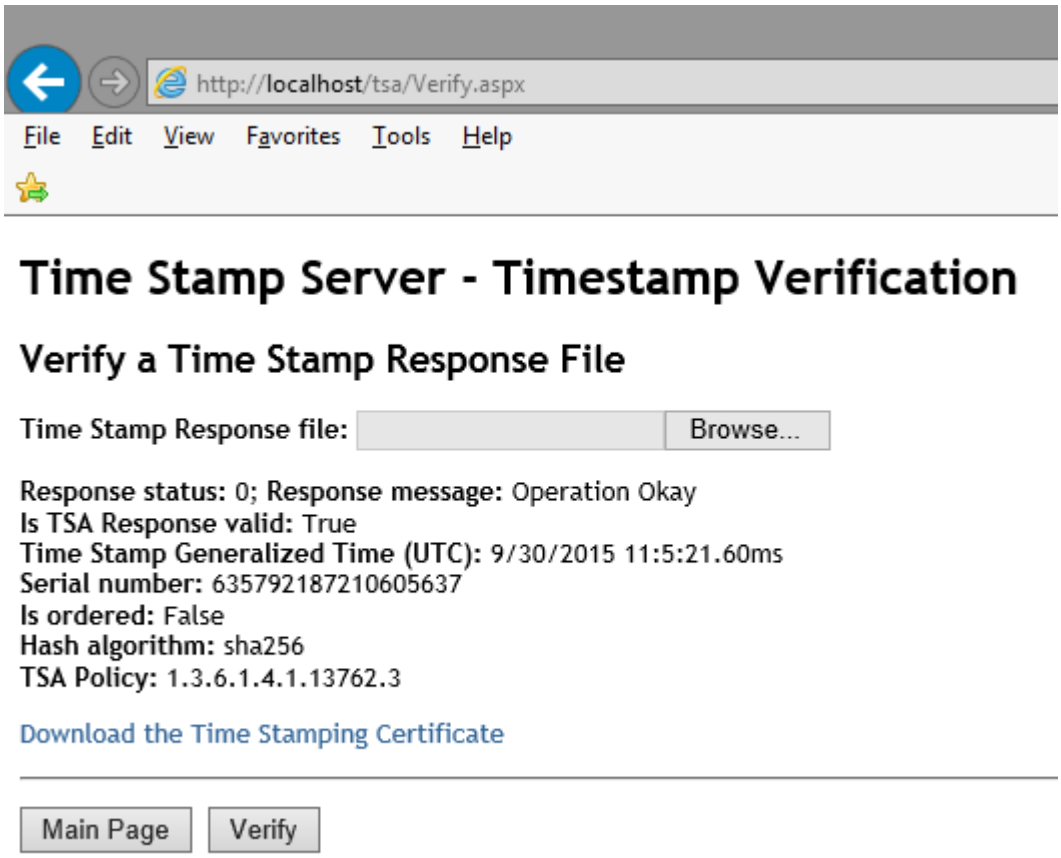
A simple Time Stamp Client is avaliable on the *TSAServer.zip* archive (*\Utils\Time Stamp Client*).

Using this client you can simply test the connection, speed and the Time Stamp Server settings.



Verify a Time Stamp Response Against the Source File

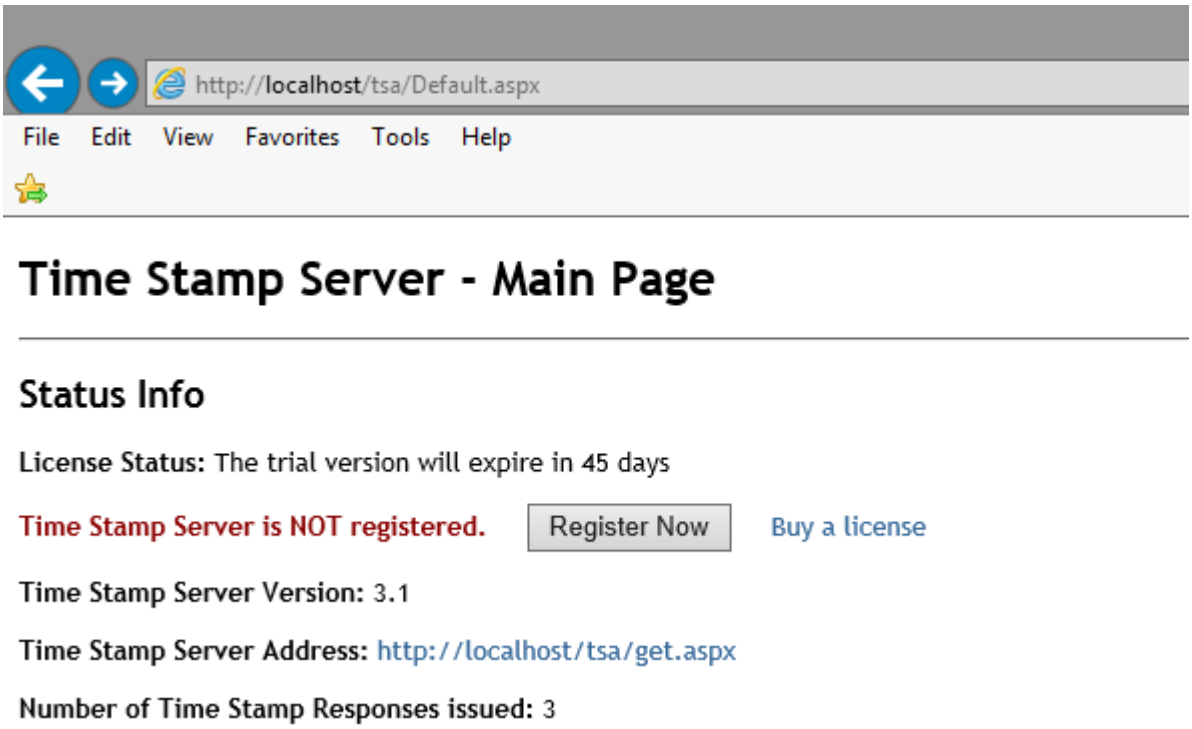
To verify a Time Stamp Response, go to http://localhost/tsa/Verify.aspx and select a response file generated by the TimeStampClient application.



Verifiy a Time Stamp Response File

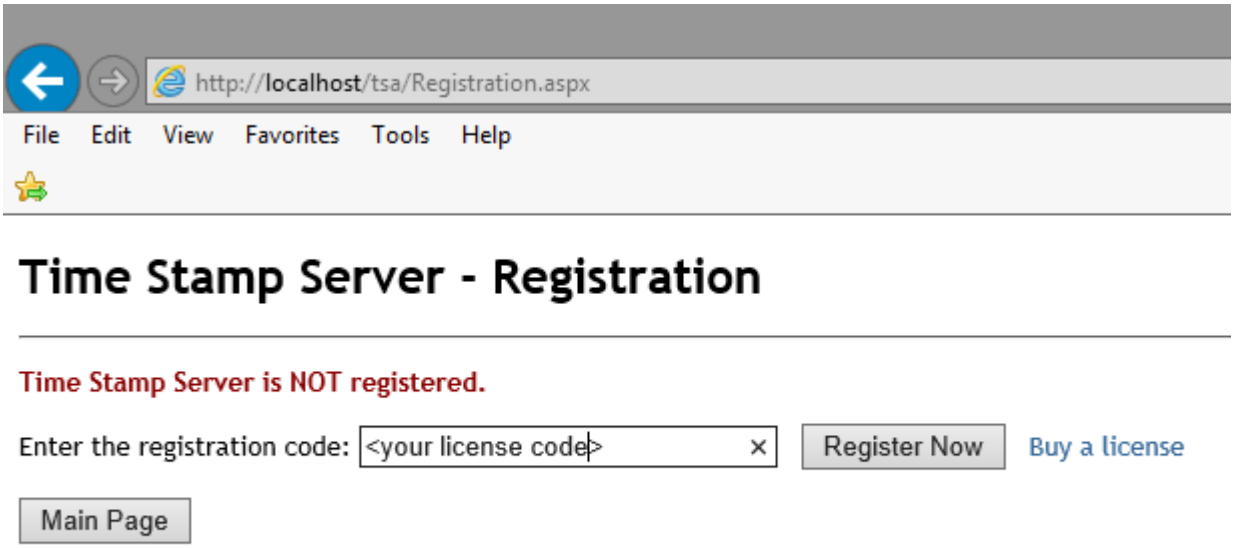
Time Stamp Server Registration

On the demo version, the Time Stamping Server can be used 45 days.

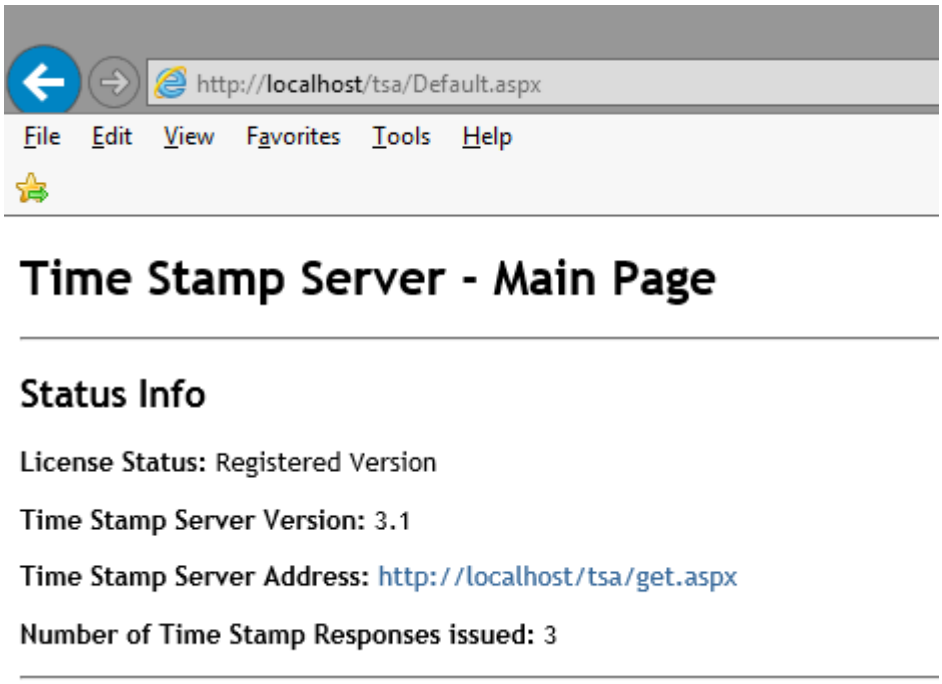


To register the Time Stamp Server you must buy a Registration Code. More information can be found on the product main page.

When you get your Registration Code, it must be entered on the Registration page:



After you have entered the Registration Code and the button *Register Now* is pressed, the unregistered version of the Time Stamp Server will be replaced by the registered version.



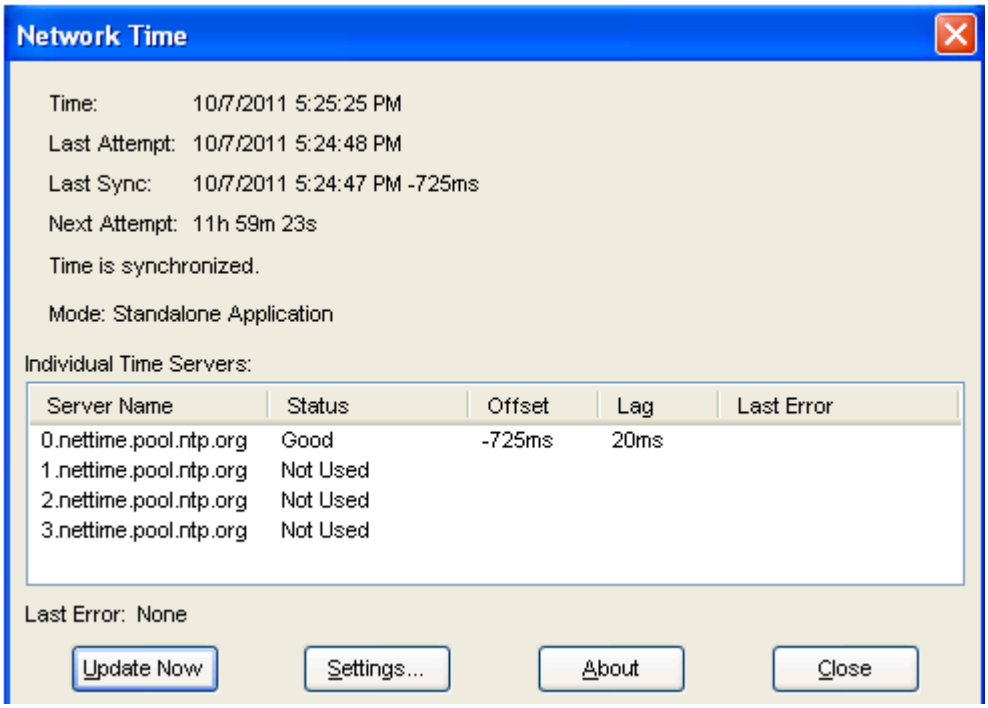
Time Stamp Server Time Source

Time Stamp Server uses as time source the IIS server machine time so be sure that the local time is synchronized with a time server.

You may use the Domain Controller clock if the server is a member of Active Directory or you may use an application that will do this for you.

A time synchronizer application is available free of charge at this link: http://timesynctool.com/

The product might needs a (S)NTP connection so UDP/123 port must be opened.



Timestamp Validation in Adobe

Usually, the Timestamping certificates are issued by a Root CA (Certification Authority).

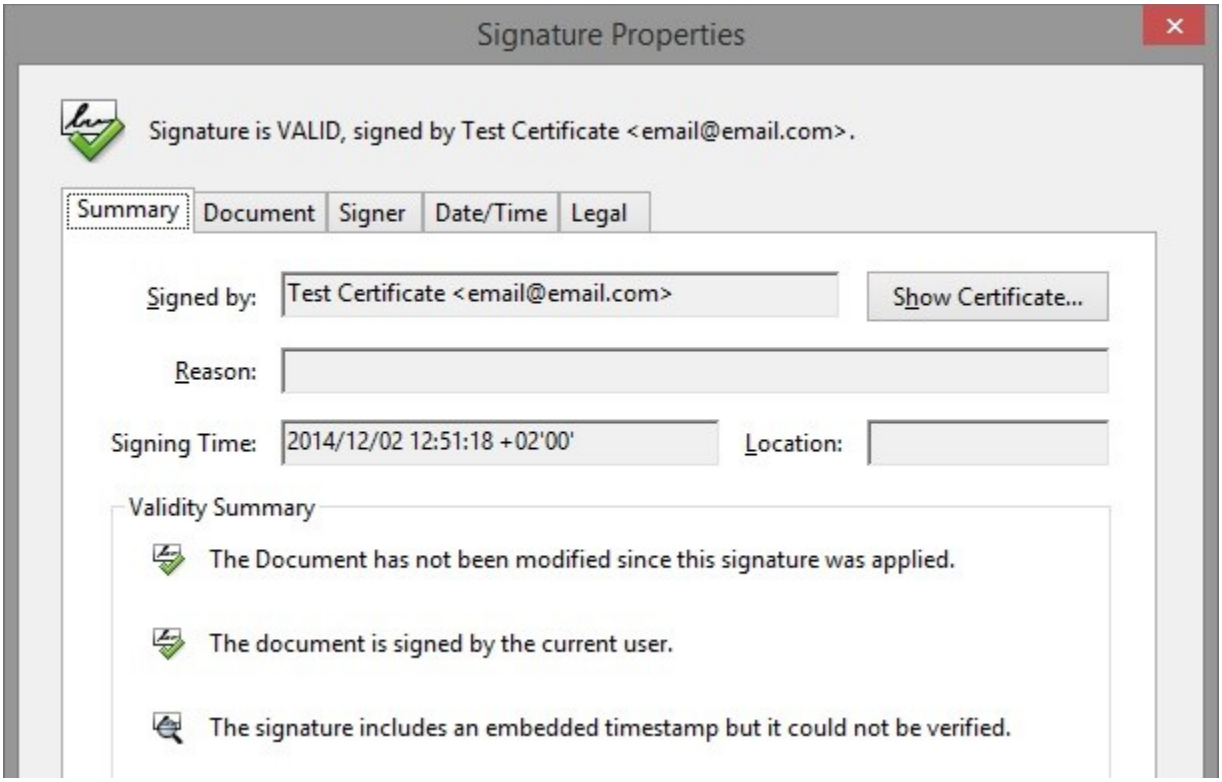
If the Root CA that issued the Timestamping certificate is not included in Adobe Trusted Identities, the timestamp is considered "unverified" (but NOT invalid) when the document is opened in Adobe Reader.

This behavior has nothing to do with the Time Stamp Server but with the Adobe certificate validation procedure.

The user can validate the signature if the Root CA is already installed on Microsoft Certificate Store.

As an alternative, the recipient must manually add the Root Certificate of the signing certificate on Adobe Trusted Identities.

An Adobe Timestamp is a subsequent signature added to the PDF signature so to validate an Adobe Timestamp, follow the instructions available here: [Validating Digital Signatures in Adobe]



The Time Stamp Response is considered "unverified"