Aloaha Time Stamp Server (TSS)[1]

Time stamping is very important in situations when the **date and time of your signed**[2] data play a significant role in the verification and authentication process of your document. Documents with a Time Stamp are secured against forgery or backdating. Therefore they are 100% credible for all companies, institutions, offices and even private individuals.

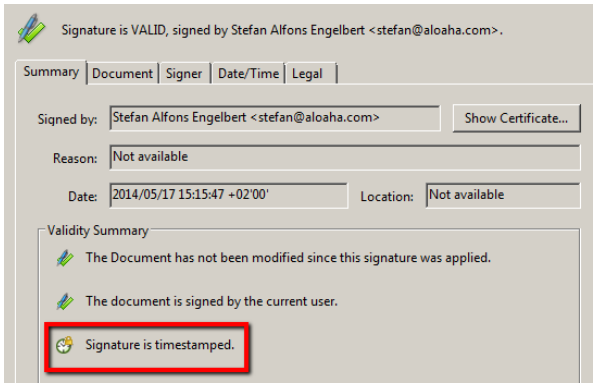
Why Time Stamp?

- Time stamps are an important measure of protecting your intellectual property rights. They protect documents and communication relating to patents
- They are important to protect documents and communication related to legal proceedings, contracts or even annual reports.
- Time Stamps are a great tool to prove that your e-tender documents have been created prior the closing date.

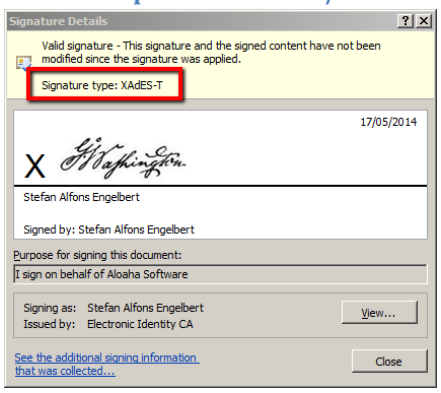
What can be time stamped?

Basically every electronic data or transaction can be time stamped. In this document we will focus on PDF and Office documents.

Time stamped PDF document



Time stamped Office 2010/2013 document



[1] http://blog.aloaha.com/category/aloaha-smartcard-software-en/time-stamping-authority/
evaluation version on http://www.aloaha.com/download/tsa.zip
request evaluation key from info@aloaha.com

[2] Time notarisation

Contents

Features and Benefits

- IIS **NOT required** but optional supported via ASP plug-in
- Integrated ASP.net compatible web server included
- Quick and easy to set up with no technical expertise required (no IIS configuration headaches)
- Recognized and compatible with most systems and applications such as Microsoft and Adobe
- Easy to use through friendly programs like Adobe Acrobat or Aloaha PDF Signator[3]
- **XAdES** compliant. (Make sure you have the Root Certificate of your Time Stamping Certificate trusted)
- **IETF RFC 3161**[4] compliant
- **Authenticode**[5] compliant
- Strong 256-bit hash algorithm supported
- **X.509** standards compliant
- Works with HSM (Hardware Security Module) devices
- Supports Software Certificates

Requirements

- Any Windows operating system
- IIS NOT required but optionally supported via .asp add-on
- Microsoft .NET Framework 2.0
- Time stamping certificate hosted in the Windows Certificate Store or on a HSM Module
- Required time stamping Certificate can be supplied free of charge to our customer

Licensing

- TSA hosted as “Software as a Service” (SaaS) first 100 Time Stamps / IP free of charge. For higher quantity contact info@aloaha.com
- License for stand-alone application (TSP) is a lifetime license. There are no additional costs like monthly / annual fees or fees per use. For prices please contact info@aloaha.com

[3] http://www.aloaha.com/wi-software-en/aloaha-signator.php

[4] http://tools.ietf.org/html/rfc3161

[5] http://msdn.microsoft.com/en-us/library/ie/ms537359(v=vs.85).aspx

Online Demo Server

Our demo server can be accessed via the URLs below:

IIS Plugin Version

This version of the Aloaha Time Stamping Server is running as an IIS Add-on.

Time Stamping URL: http://tsa.aloaha.com

Root Certificate[6]: http://tsa.aloaha.com/AloahaRoot_TSA.cer

Time Stamping Certificate: http://tsa.aloaha.com/TSA_Live.cer

Stand-Alone Version

This version of the Aloaha Time Stamping Server is the default configuration. It runs on the embedded Stand-Alone Web Server to eliminate possible IIS configuration headaches. I also detects "out of the box" if it has to issue **Authenticode** or **RFC3161** certificates.

Time Stamping URL: http://tsa.aloaha.com:8081/tsa.aspx

Root Certificate[7]: http://tsa.aloaha.com:8081/AloahaRoot_TSA.cer

Time Stamping Certificate: http://tsa.aloaha.com:8081/TSA_Live.cer

Please note that the time stamping request needs to be *posted* to the above Time Stamping URLs. Simply calling the URL will obviously NOT return any TSA Token!

To test PDF Signing and Time Stamping you can use http://tsa.aloaha.com:8081/PDFArchive.aspx and upload a PDF. The server will sign and timestamp it for you then. You can also use our Cloud Signer from: http://tsa.aloaha.com:8081/CloudSigner/CloudSigner.zip

Installation

Software

Please download the software from http://www.aloaha.com/download/tsa.zip und extract the package. The setup is called tsa.exe. You need to call it with administrative rights.

Ideally you call the setup with "Right mouse click" -> "Run as Administrator"

Once the software is installed you can already request your timestamps.
The URL is **http://<your server address>:8081/tsa.aspx**

[6] In case you are planning **XAdES** Signatures you need to make sure that the Root Certificate is registered as trusted root. Otherwise Office / Word might report the error: **"Signing cannot be completed due to problems applying the required timestamp. Check your network connection"**

[7] ibid.

Certificate

The Aloaha Time Stamping authority pre-installs a demo certificate[8] so that you are able to start right away.

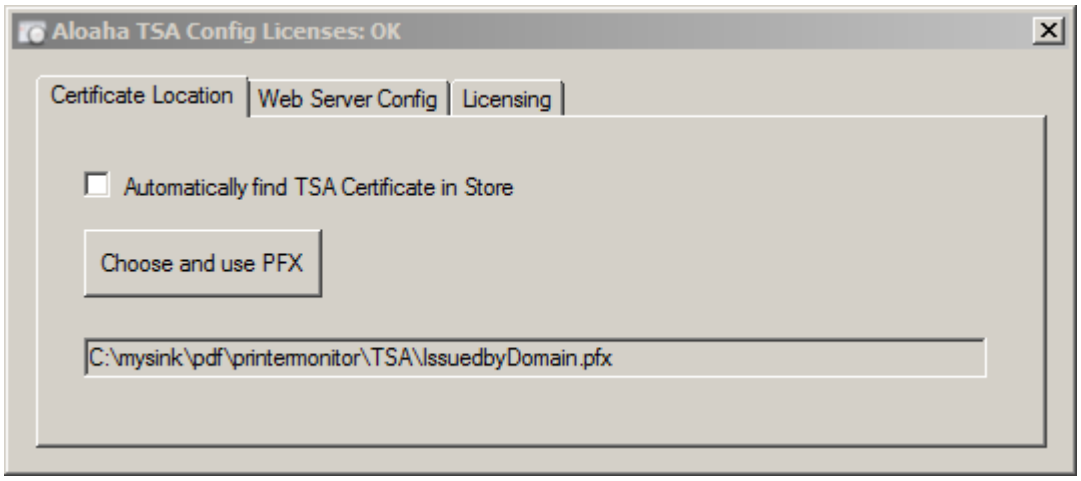
Once the customer decides to go productive it is very easy to re-place the certificate[9] with the real one or to use a HSM Module.

Replace certificate

To replace your certificate please call TSAConfig.exe. There you can choose either your PFX Certificate or you activate “Automatically find TSA Certificate in Store”

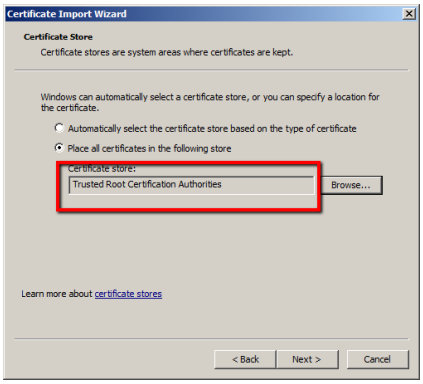
If you activate “Automatically find TSA Certificate in Store” Aloaha automatically finds the right certificate in the **current user store** of the user running the TSA Service. If no certificate is found there Aloaha will also look into the **machine store**.

This option should be used in case you are using a HSM Module!



Register Root Certificate in “Trusted Root Certification Authorities

1. Right click on the .CER File and choose “Install Certificate”
2. Choose the “Trusted Root Certification Authorites”



3. A Security Warning will pop up to warn you that you are going to trust a root authority. You need to confirm that warning with “Yes”.

[8] http://tsa.aloaha.com:8081/Demo_Timestamping_Certificate.zip

[9] Please note that Aloaha also sells Time Stamping Certificates which are compliant with Adobe and also with Office products.

How do I activate the Aloaha Demo Server in my Office Application to create XAdES Signatures?

1. Trust the root certificate of your time stamping certificate with importing it into “Trusted Root Certification Authorities” Store. If you are using a certificate issued by Aloaha please note that you find our root certificate at: http://tsa.aloaha.com:8081/AloahaRoot_TSA.cer
2. Configure your office to create XAdES-T Signatures using your TSA. That can be done via group policy as explained by Microsoft OR just modify the registry settings[10] below to reflect your TSA location and import it into your registry.

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Signatures]
"xadeslevel"=dword:00000002
"minxadeslevel"=dword:00000002
"tsalocation"="http://tsa.aloaha.com:8081/tsa.aspx"

[HKEY_CURRENT_USER\Software\Policies\Microsoft\office\15.0\common\signatures]
"enablecreationofweakxpsignatures"=dword:00000000
"suppressofficedefaultprovider"=dword:00000003
"suppressextsigningsvcs"=dword:00000001
"tsalocation"=http://tsa.aloaha.com:8081/tsa.aspx
"minxadeslevel"=dword:00000002
"xadeslevel"=dword:00000002
"requireocsp"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Signatures]
"xadeslevel"=dword:00000002
"minxadeslevel"=dword:00000002
"tsalocation"="http://tsa.aloaha.com:8081/tsa.aspx"

[HKEY_CURRENT_USER\Software\Policies\Microsoft\office\14.0\common\signatures]
"enablecreationofweakxpsignatures"=dword:00000000
"suppressofficedefaultprovider"=dword:00000003
"suppressextsigningsvcs"=dword:00000001
"tsalocation"=http://tsa.aloaha.com:8081/tsa.aspx
"minxadeslevel"=dword:00000002
"xadeslevel"=dword:00000002
"requireocsp"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Office\13.0\Common\Signatures]
"xadeslevel"=dword:00000002
"minxadeslevel"=dword:00000002
"tsalocation"="http://tsa.aloaha.com:8081/tsa.aspx"

[HKEY_CURRENT_USER\Software\Policies\Microsoft\office\13.0\common\signatures]
"enablecreationofweakxpsignatures"=dword:00000000
"suppressofficedefaultprovider"=dword:00000003
"suppressextsigningsvcs"=dword:00000001
"tsalocation"=http://tsa.aloaha.com:8081/tsa.aspx
"minxadeslevel"=dword:00000002
"xadeslevel"=dword:00000002
"requireocsp"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Signatures]
"xadeslevel"=dword:00000002
"minxadeslevel"=dword:00000002
"tsalocation"="http://tsa.aloaha.com:8081/tsa.aspx"

[HKEY_CURRENT_USER\Software\Policies\Microsoft\office\12.0\common\signatures]
"enablecreationofweakxpsignatures"=dword:00000000
"suppressofficedefaultprovider"=dword:00000003
"suppressextsigningsvcs"=dword:00000001
"tsalocation"=http://tsa.aloaha.com:8081/tsa.aspx
"minxadeslevel"=dword:00000002
"xadeslevel"=dword:00000002
"requireocsp"=dword:00000000
```

[10] http://tsa.aloaha.com:8081/enableXAdES.zip