

# PSAM 2.3 Certificates management

## 2.3.1 Introduction

The certificates management is related to the server name and the services provided (please refer to [PSAM 2.2 Network Segregation](#) for details about the certificate assignation to a specific NIC/IP/name). In order to provide to the client a sure match of your identity you need to load and configure a secure certificate bonded to your server name (ie: name.server.tld).

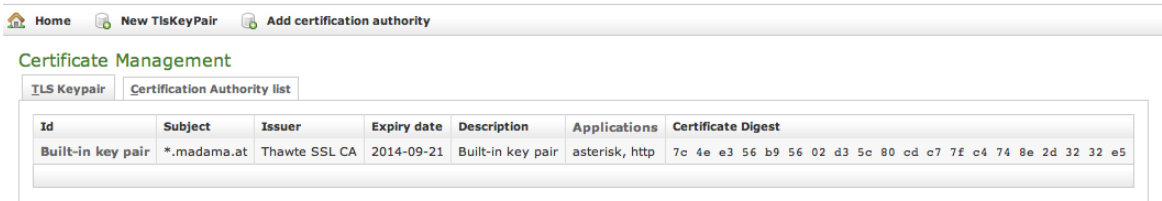


figure 1. Certificate configuration, default certificate installed

You can get the certificates configuration page using the **Certificate Management** link in the **main menu**. As shown above the default page is listing the installed TLS Keypair.

By default, on PrivateServer it's installed one "\*.madama.at" wildcard certificate as shown in [figure 1. Certificate configuration, default certificate installed](#)

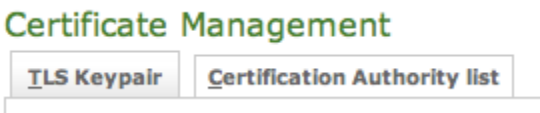


fig. 1. The tabs to access the two section related with the certificate management

From this page you can decide to view and delete your keypairs or the Certification Authority entries, using the tabs shown in the above [fig. 1. The tabs to access the two section related with the certificate management](#).

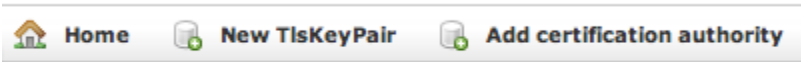


fig 1. link for adding new tis keypairs or new CAs

Instead if you need to create a new TLS key pair or add a new CA, then you have to use the buttons above the "TLS Keypair" list (the ones shown in [fig 1. link for adding new tis keypairs or new CAs](#)).

## 2.3.2 New TLS Key pair

If you need to upload a new certificate, click on the **New TlsKeyPair** link above the certificate table.

## Create TlsKeyPair

Description:	<input type="text"/>
Private Key:	<div></div>
Certificate:	<div></div>
Cert Chain:	<div></div>


 **Create**

figure 2. New certificate form


You are redirected on the **Create TlsKeyPair** page (it's shown in [figure 2. New certificate form](#)) where an upload form needs to be filled. Its fields are:

- Description: a generic name you choose to identify this certificate
- Private Key: your private key, provided by the signature authority
- Certificate: the certificate itself
- Cert Chain: a possible intermediate certificate used to link the certification authority to your certificate.

All the fields must be in **PEM (Privacy Enhanced Mail)** format and you just copy and paste each of them in the proper field. When your' done you just press the **Create** button on the bottom line and the certificates are ready to be assigned to an interface/IP.

### 2.3.3 Add Certification Authority

You might need to upload a new CA (Certification Authority) if you tried to install a tis key pair not signed by an installed CA.

 By default PrivateServer contains a default list of pre-loaded Certification Authorities.

## Certificate Management

TLS Keypair		Certification Authority list
subject	expiryDate	
GeoTrust Global CA	2022-05-21 06:00:00.0	Delete
GeoTrust Global CA 2	2019-03-04 06:00:00.0	Delete
GeoTrust Primary Certification Authority	2036-07-17 01:59:59.0	Delete
GeoTrust Primary Certification Authority - G2	2038-01-19 00:59:59.0	Delete
GeoTrust Primary Certification Authority - G3	2037-12-02 00:59:59.0	Delete
GeoTrust Universal CA	2029-03-04 06:00:00.0	Delete
GeoTrust Universal CA 2	2029-03-04 06:00:00.0	Delete
Thawte Premium Server CA	2021-01-01 00:59:59.0	Delete
thawte Primary Root CA	2036-07-17 01:59:59.0	Delete
thawte Primary Root CA - G2	2038-01-19 00:59:59.0	Delete
thawte Primary Root CA - G3	2037-12-02 00:59:59.0	Delete
Thawte Server CA	2021-01-01 00:59:59.0	Delete

fig 2. the default CA list

The new CA installation becomes mandatory because without a complete certificate chain the new TLS key pair would not be accepted by PrivateServer. If you need to upload a new certificate, click on the **Add certification authority** button above the certificate list table.

[Home](#) [Certificate Management](#)

### Add Certification Authority

Certificate:

[Create](#)

fig 3. New Certification Authority

You get the form shown in [fig 3. New Certification Authority](#) which is pretty straightforward. You just have to cut 'n' paste the CA's content in the **Certificate** box and click on the **Create** button at the bottom.

## Certificate Management

TLS Keypair		Certification Authority list
subject	expiryDate	
	2029-04-22 02:00:00.0	Delete
GeoTrust Global CA	2022-05-21 06:00:00.0	Delete
GeoTrust Global CA 2	2019-03-04 06:00:00.0	Delete
GeoTrust Primary Certification Authority	2036-07-17 01:59:59.0	Delete
GeoTrust Primary Certification Authority - G2	2038-01-19 00:59:59.0	Delete
GeoTrust Primary Certification Authority - G3	2037-12-02 00:59:59.0	Delete
GeoTrust Universal CA	2029-03-04 06:00:00.0	Delete
GeoTrust Universal CA 2	2029-03-04 06:00:00.0	Delete
Thawte Premium Server CA	2021-01-01 00:59:59.0	Delete
thawte Primary Root CA	2036-07-17 01:59:59.0	Delete
thawte Primary Root CA - G2	2038-01-19 00:59:59.0	Delete
thawte Primary Root CA - G3	2037-12-02 00:59:59.0	Delete
Thawte Server CA	2021-01-01 00:59:59.0	Delete

fig 4. CA list updated

As shown in [fig 4. CA list updated](#) the Certification Authority list shows a new entry. You can check the entry by subject (which is the entity that release the certificate) and the expiry Date (that shows how long the certificate is considered valid).

### 2.3.4 Delete TLS key pair

In a day-by-day secure VoIP service administration it's not unusual to delete a TLS key pair. The procedure starts right at the **Certificate Management** page (the one shown in [figure 1. Certificate configuration, default certificate installed](#)).

Certificate Management		Certification Authority list				
Id	Subject	Issuer	Expiry date	Description	Applications	Certificate Digest
testing entry to be deleted	*.madama.at	Thawte SSL CA	2014-09-21	testing entry to be deleted		7c 4e a3 56 b9 56 02 d3 5c 80 cd c7 7f c4 74 8e 2d 32 32 e5
Built-in key pair	*.madama.at	Thawte SSL CA	2014-09-21	Built-in key pair	http, asterisk	7c 4e a3 56 b9 56 02 d3 5c 80 cd c7 7f c4 74 8e 2d 32 32 e5

fig 5. the TLS key pair list with a testing entry to be deleted

In [fig 5. the TLS key pair list with a testing entry to be deleted](#) you can see we added an entry conveniently named **testing entry to be deleted** and that's what we're going to do.



Please make sure no services got association with the TLS entry you're going to remove, or else the deletion would fail.

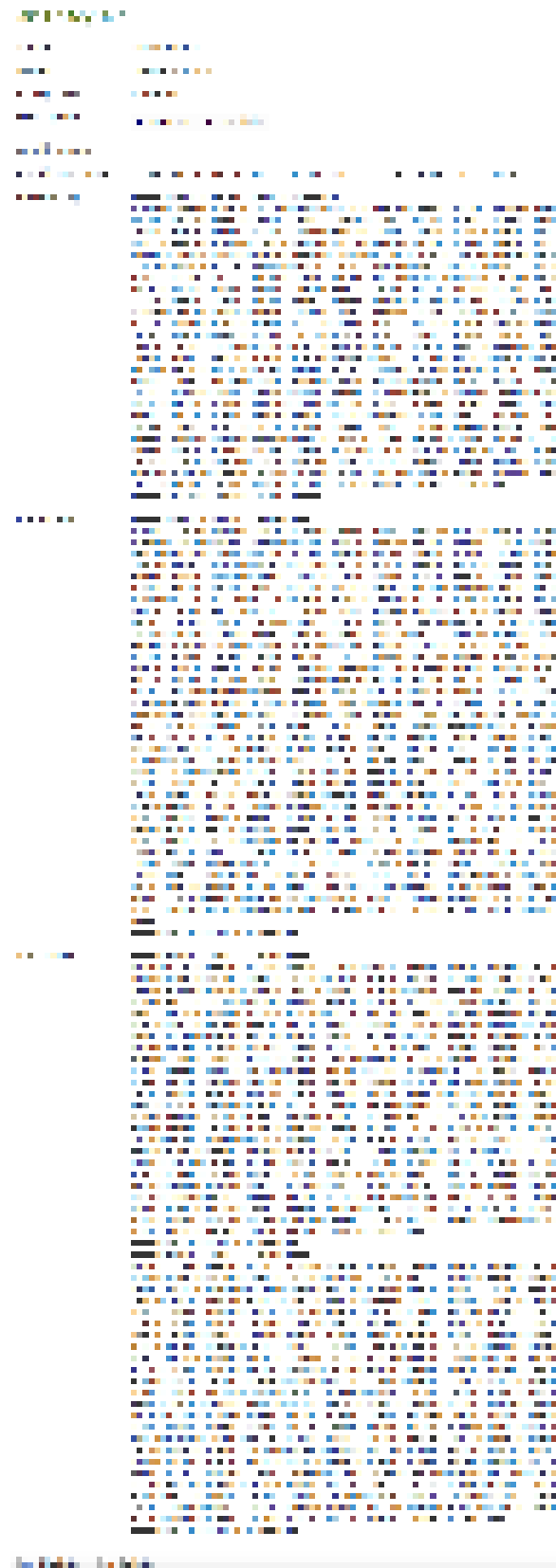


fig 6. TLS key pair details

First you click on the chosen entry and get a detail of the TLS key pair (as in [fig 6. TLS key pair details](#)). At the page's bottom there's a **Delete** button. Just press it.

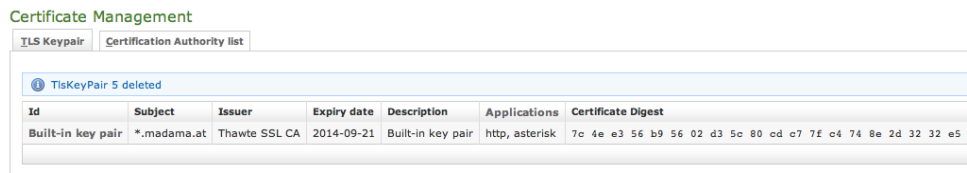


fig 7. the deletion is confirmed

Confirm the deletion in the following pop-up windows. After that you get the new TLS key pair list without the deleted entry and with a warning which explains the entry has been deleted (as in [fig 7. the deletion is confirmed](#)).

### 2.3.5 Delete Certification Authority

You cannot edit an entry in the CA list, but you still can delete a CA and create a new one for replacement. That said, the way for deleting a CA entry is quite simple. From the CA list shown in [fig 4. CA list updated](#) choose the CA you want to expunge and press the **Delete** link in the last right column.

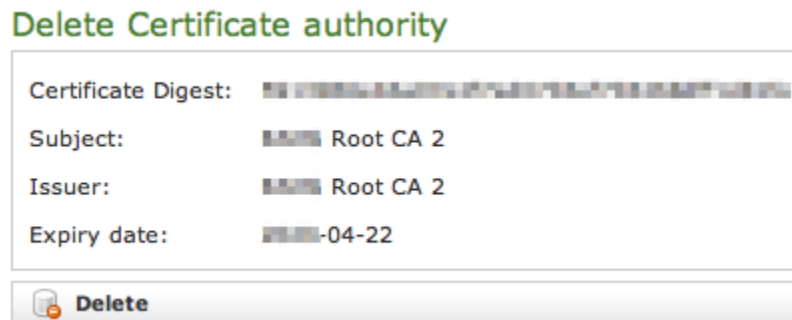


fig 8. CA's details

First you get a detail of the certificate you're going to delete. Just press the **Delete** button at the bottom and confirm your choice in the next pop up window.

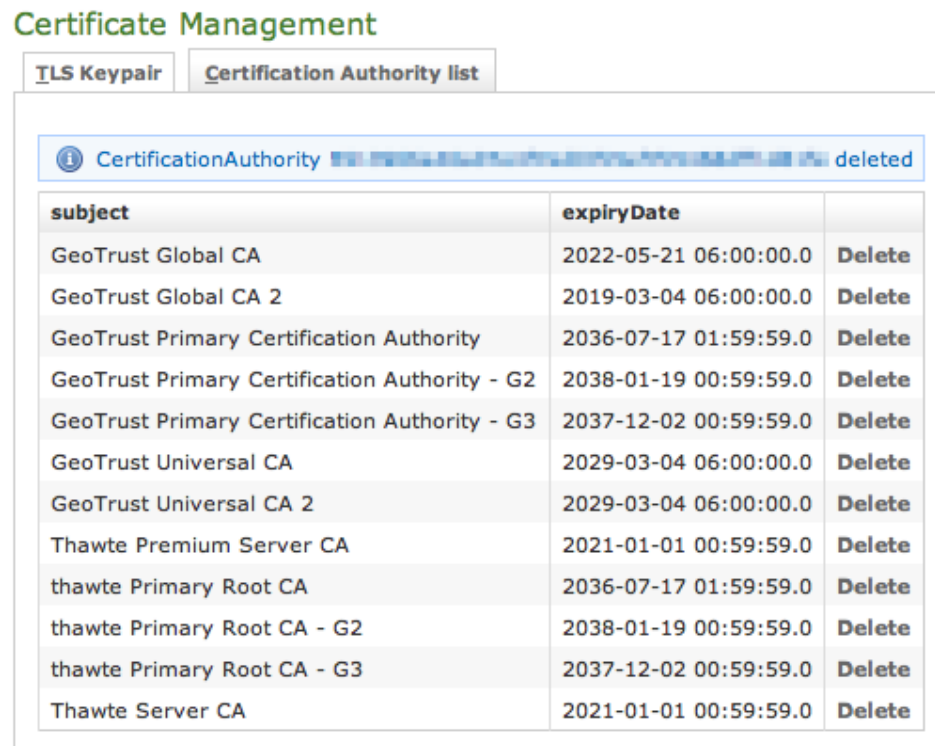


fig 9. The CA list updated and the warning

You receive a confirmation about the deletion in the new CA list page (shown above in [fig 9. The CA list updated and the warning](#)). Plus the list no more shows the deleted CA entry.

PSAM 2.2 Network Segregation

PSAM 2.4 Advanced configurations