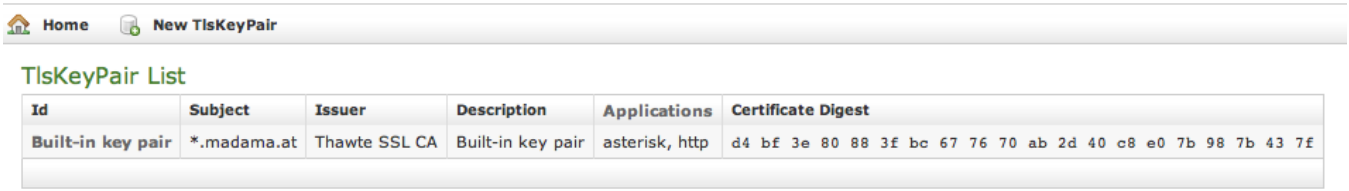
PSAM 2.3 Certificates configuration

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).



Id	Subject	Issuer	Description	Applications	Certificate Digest
Built-in key pair	*.madama.at	Thawte SSL CA	Built-in key pair	asterisk, http	d4 bf 3e 80 88 3f bc 67 76 70 ab 2d 40 c8 e0 7b 98 7b 43 7f

figure 1. Certificate configuration, default certificate installed

You can get the certificates configuration page using the **Certificates** entry in the **main menu**.

By default on the PrivateServer you can find a wildcard certificate for the madama.at domain name.

2.3.2 New certificates

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

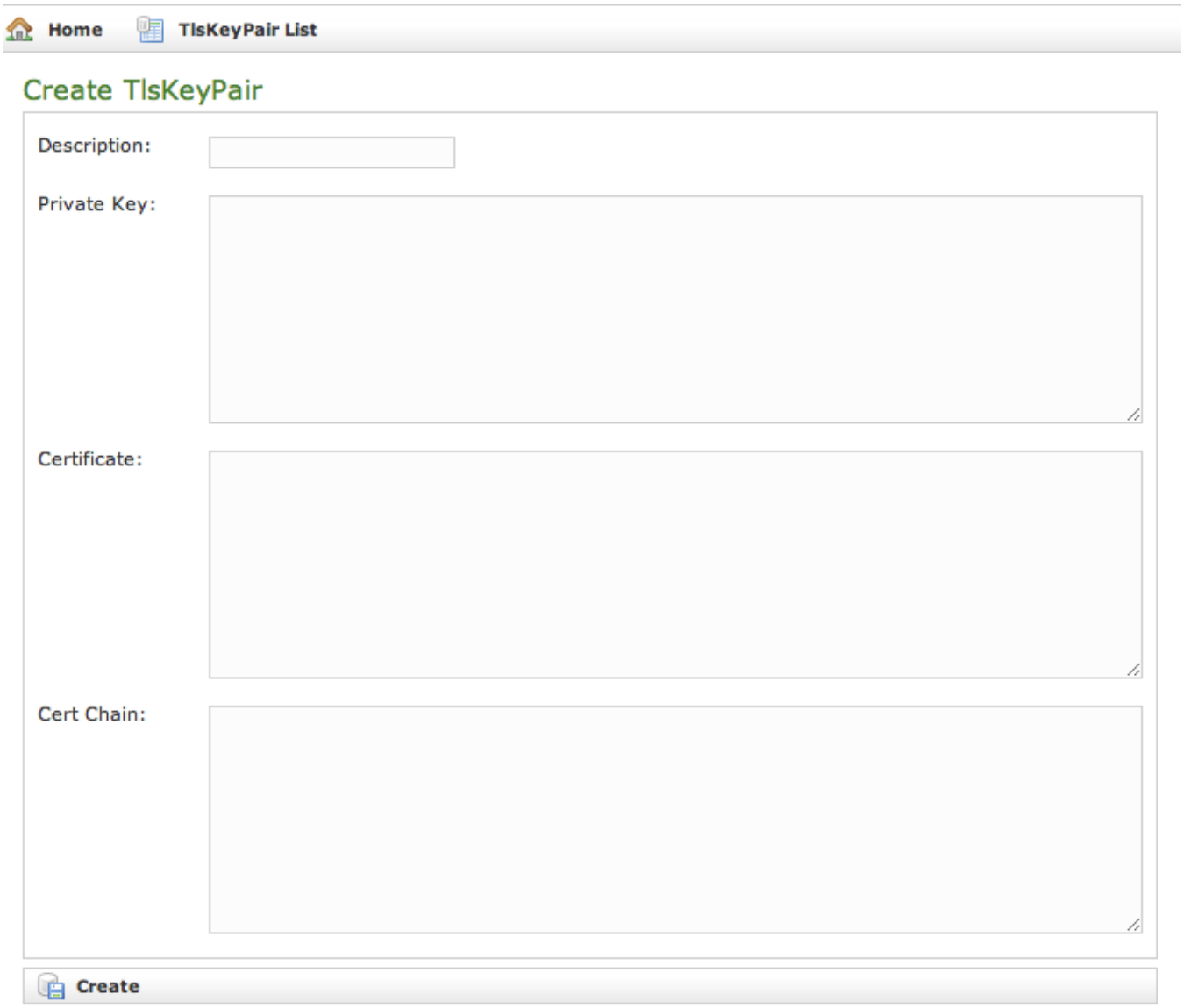


figure 2. New certificate form

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** 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.

PSAM 2.2 Network Segregation
PSAM 2.4 Asterisk advanced configurations