

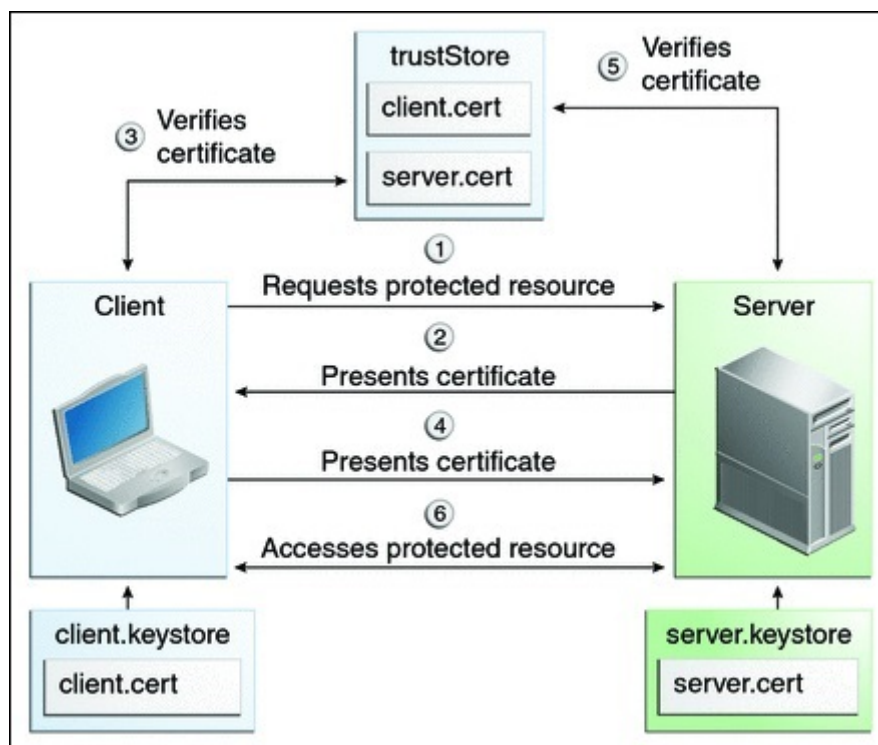
Activating Mutual SSL Authentication

What is Mutual Authentication?

Many people are expecting extra security and Mutual authentication is already supported in Terminal Service Plus. It is usually implemented by banks or government bodies.

To understand what that is, we can compare it to a standard SSL process where you will add extra check to verify if the user web browser is allowing SSL connection. You know what your server-side SSL certificate is. Imagine that the certificate is imported into the web browser to ensure that this specific web browser is trusted to create a connection. In the first step of communication, the web browser is acting as a client and in the second step, it is the reverse. At the end both side, client web browser and web server, have accepted the authority and the connection can start.

A more complete definition: Mutual SSL authentication or certificate-based mutual authentication refers to two parties authenticating each other through verifying the provided digital certificate so that both parties are assured of the others' identity. In technology terms, it refers to a client (web browser or client application) authenticating themselves to a server (website or server application) and that server also authenticating itself to the client through verifying the public key certificate/digital certificate issued by the trusted Certificate Authorities (CAs). Because authentication relies on digital certificates, certification authorities such as Verisign or Microsoft Certificate Server are an important part of the mutual authentication process.



Activating it on TSplus

TSplus built-in web server enables to setup mutual authentication.

To enable the mutual authentication follow this process:

1. Create and edit with Notepad the following file:
C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin

Add these 3 lines:

```
disable_http_only=true  
disable_print_polling=true  
force_mutual_auth_on_https=true
```

2. Remove cert.jks

Copy it in "C:\Program Files (x86)\TSplus\Clients\
Remove "C:\Program Files (x86)\TSplus\Clients\webserver\cert.jks"

3. Create the batch file

@rem uncomment next line, if you want to generate new self signed cert.jks

ST=FR, C=FR" -storepass mypassword -keypass mypassword

@del forCertUser1.cer

4. Restore the new created the modified "cert.jks"

Copy "C:\Program Files (x86)\TSplus\Clients\cert.jks" into
"C:\Program Files (x86)\TSplus\Clients\webserver" and restart the Web Servers.

5. Certificate import and Testing

The administrator can create a separate key pair file for each user.

For example:

```
forBrowserUser1.p12  
forBrowserUser2.p12  
forBrowserUser3.p12
```

And he can export theses certificates into cert.jks.


```
settings.bin>disable_http_only=true
```