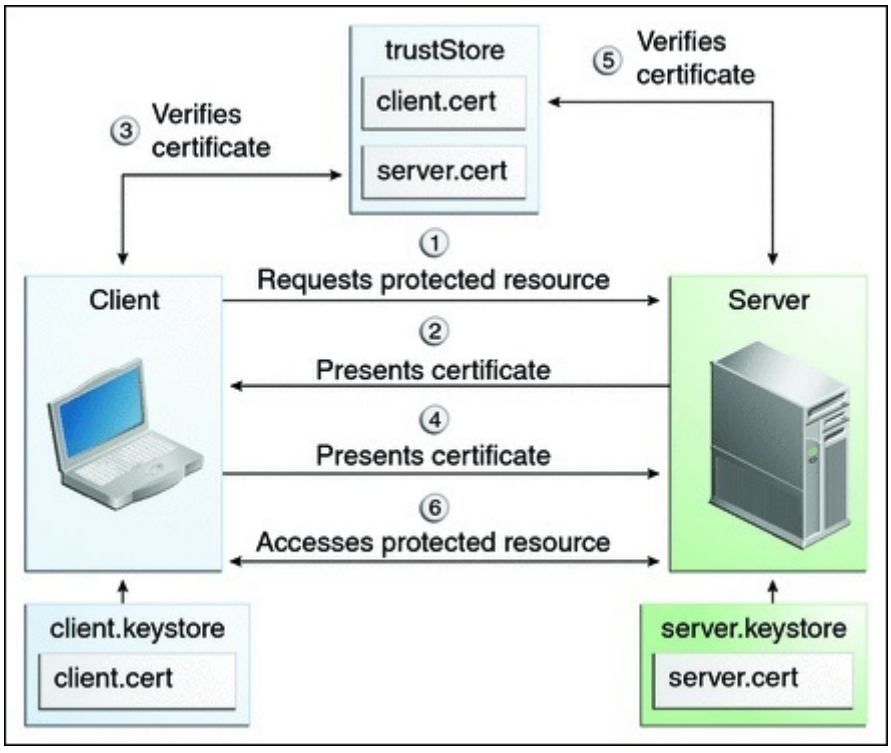
Activating Mutual SSL Authentication

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:

You will have to install the latest Java Development Kit (JDK), available from http://jav

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

In "C:\Program Files (x86)\TSplus\Clients\webserver" you will see the file 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
```

```
In 'C:\Program Files (x86)\TSplus\Clients' create a batch file, for example "createcertus
```

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

```
@rem keytool -genkey -v -alias jwts -keyalg RSA -validity 3650 -keystore cert.jks -storep
```

```
@keytool -genkey -v -alias AliasUser1 -keyalg RSA -storetype PKCS12 -keystore forBrowserU
```

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

```
@keytool -export -alias AliasUser1 -keystore forBrowserUser1.p12 -storetype PKCS12 -store
```

```
@keytool -alias AliasCertUser2 -import -v -file forCertUser1.cer -keystore cert.jks -stor
```

```
@del forCertUser1.cer
```

This will automatically import the cert key pair from the web browser into "cert.jks" aft

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 provided batch example should have generated a test file "BrowserUser1.p12".
```

When you will open the HTTPS address, you will get a security message and you will be una

With Chrome or IE, you can click on this 'BrowserUser1.p12' file to import the certificat

With FireFox, you have to go to Settings and to import this "BrowserUser1.p12" file under

As soon as you have properly imported it, you will be able to access the HTTPS address.

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.

If he wants to disable the access to one user he will just have to delete this user from

Doing so, the user will lose his authorization and will not be able to access the web ser

This mutual authentication only affects the HTTPS connections and HTTP connection will be

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