Architecture

HTTPS tunnel, authorization and encryption

The picture below shows a general scheme of interconnection between a client and the web-server. When a client connects to the server a https tunnel is set up on the basis of the server and client certificates, i.e. with bilateral authorisation. This is a first level of client authorization in the system. Then a user enters a login and a password in the authorisation form to get an access directly to the web-application.

On this page:

Further information:

- Cryptographic software

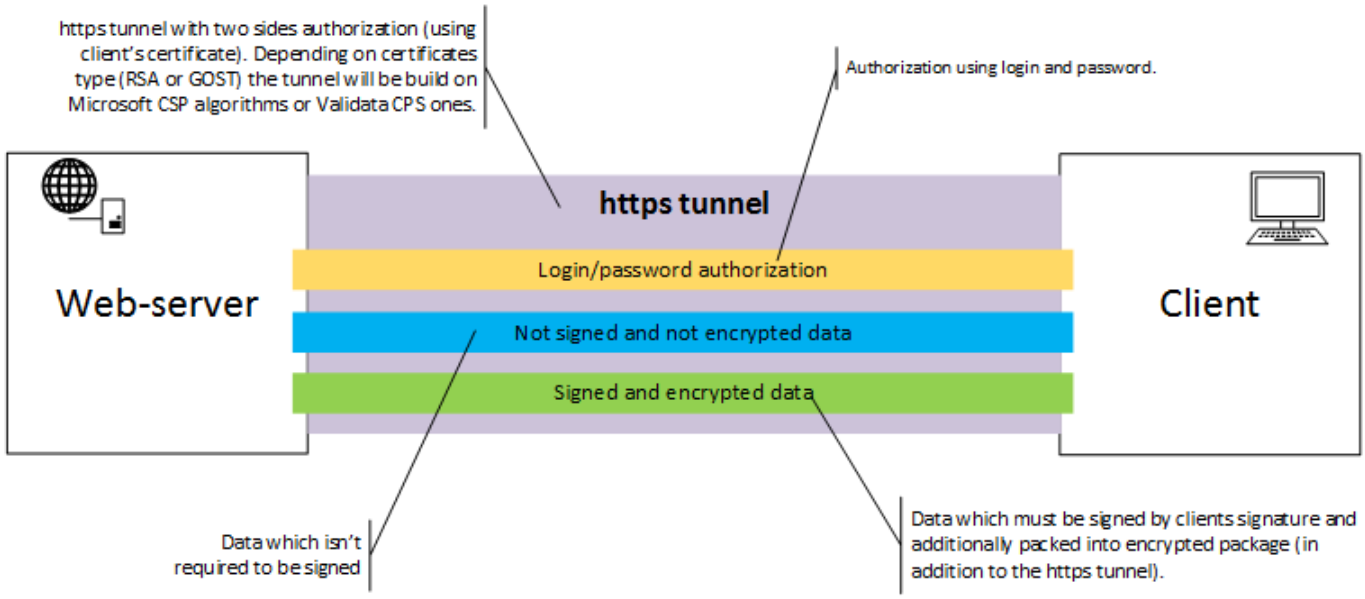

Fig. 1 – interaction between client and Web-server

Channel forming

Depending on the type of the certificate (RSA or GOST), https tunnel is set up using the cryptographic service provider Microsoft CSP or Validata CSP, respectively (Fig 2). Also, depending on the certificate type the client space puts a digital signature and encrypts documents with a CSP.

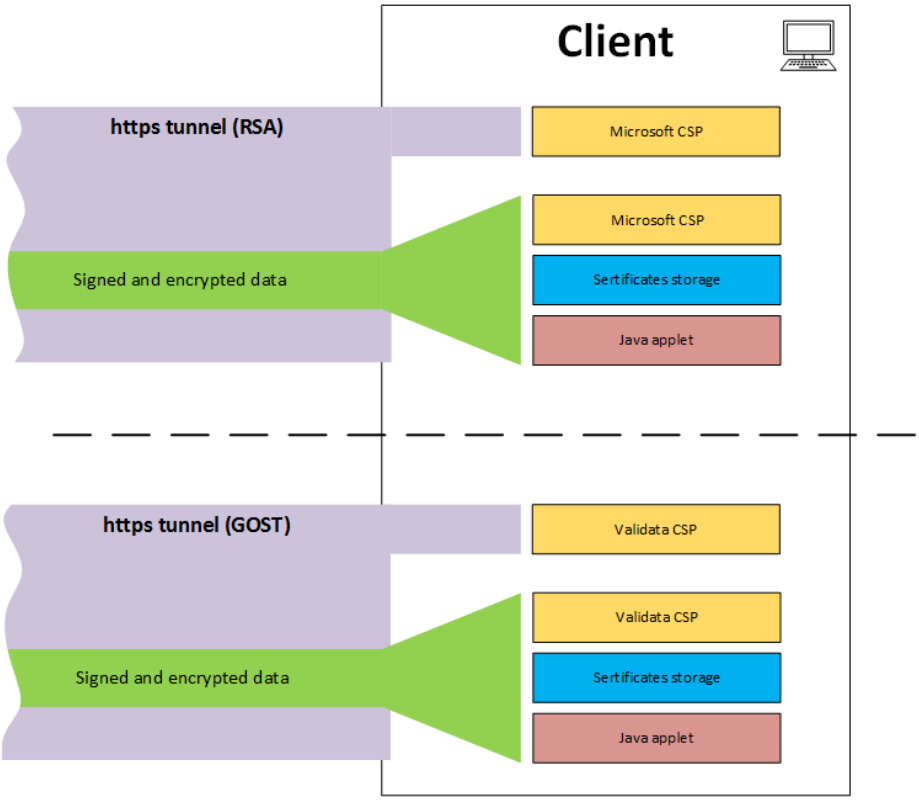

Fig. 2 – forming a channel