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:

- HTTPS tunnel, authorization and encryption
- Channel forming

Further information:

- Cryptographic software

https tunnel with two sides authorization (using client's certificate). Depending on certificates type (RSA or GOST) the tunnel will be build on Microsoft CSP algorithms or Validata CPS ones.

Authorization using login and password.

https tunnel

Login/password authorization

Not signed and not encrypted data

Signed and encrypted data

Web-server

Client

Data which isn't required to be signed

Data which must be signed by clients signature and additionally packed into encrypted package (in addition to the https tunnel).
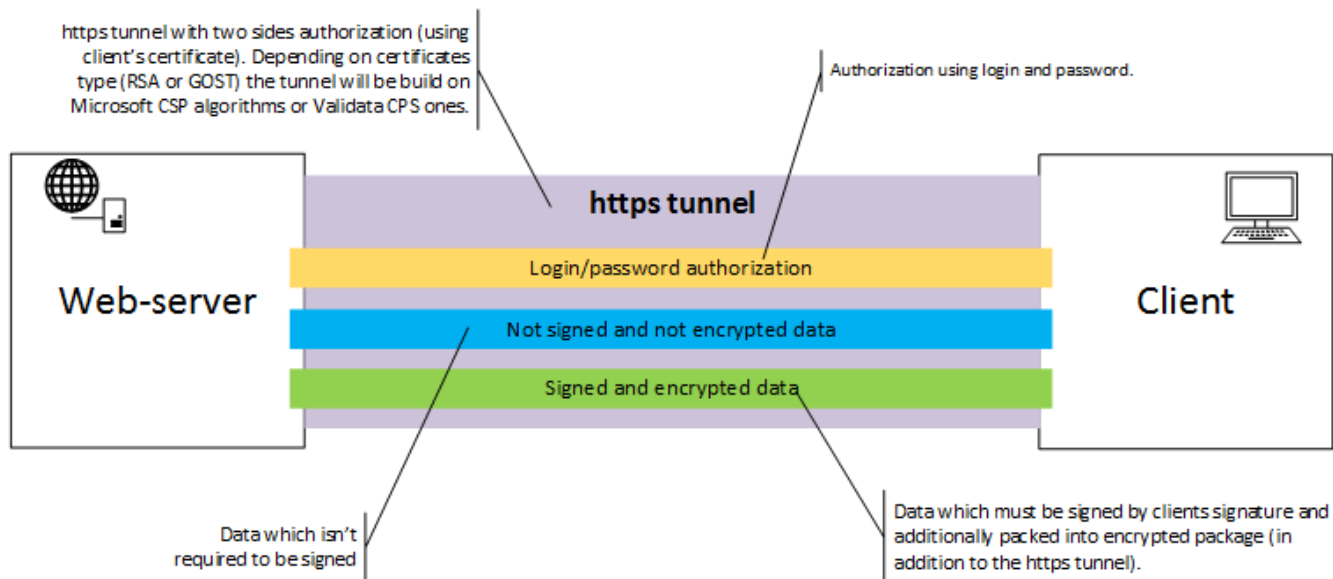
Fig. 1 – interaction between client and Web-server

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.

Client

https tunnel (RSA)

Signed and encrypted data

Microsoft CSP

Microsoft CSP

Sertificates storage

Java applet

https tunnel (GOST)
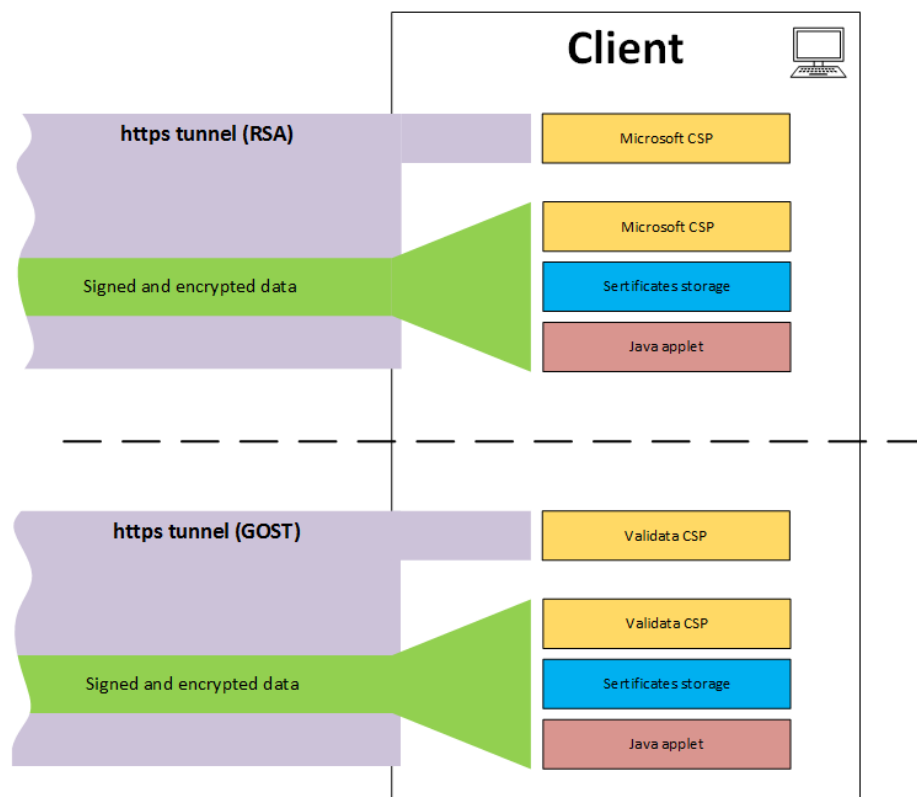
Signed and encrypted data

Validata CSP

Validata CSP

Sertificates storage

Java applet

Fig. 2 – forming a channel