**Principal Authentication  
in “Yandex.Money” payment service**

Version from 13.04.2012

The SSL connections authentication between Principal and “Yandex.Money” Payment Service (hereinafter “PS”) are made by using the server and client SSL certificates issued by PS certification authority (“Yamoney Issuing CA”). To get started to use PS services the Principal should request the SSL Client Certificate.

## Certificates exchange procedure

The certificates conforms the standard “Internet X.509 Public Key Infrastructure”, publicly available at: <http://www.ietf.org/rfc/rfc2459.txt>

The certificate format is: X.509 Version 3.

Principal have to generate a key pair with following parameters:

* Algorithm: RSA;
* Key length: 2048 bits;
* Hash-function: SHA-1.

Principal is allowed to use any cryptographic software and hardware that conforms to standard: RFC 2459 (X.509 version 3 certificate format). Examples, shown below, have created with OpenSSL software version 0.98.

**Step 1: Generating a private key**

Principal creates the private key on its own side. Principal must secure the private key to be confidential, because it’s Principal secret information. Private Key must be encrypted and password (or other way)-protected.

|  |
| --- |
| *openssl genrsa –des3 –out private.key 2048*  *Enter pass phrase for private.key:*  *Verifying - Enter pass phrase for private.key:* |

**Step 2: Creating a certificate request**

Principal, using the private key generated before, creates the “Certificate Request” with the following parameters:

|  |  |
| --- | --- |
| **Request Field** | **Description** |
| CN (Common Name) | /business/userName, where userName is the Principal login, assigned by PS. |
| C (State) | Russia |
| L (Locality) | field must be empty |
| O (Organization Name) | Full name of legal entity |
| OU (Organizational Unit Name) | field must be empty |
| E (email) | An E-mail address of the person, responsible for the service from Principal side. |

A certificate request creation example:

|  |
| --- |
| *openssl req –new –key private.key –out request.csr*  *Country Name (2 letter code) [AU]:****RU***  *State or Province Name (full name):* ***Russia***  *Locality Name (eg, city): []:*  *Organization Name (eg, company) [Internet Widgits Pty Ltd]:* ***Snake Oil LLC***  *Organizational Unit Name (eg, section) []:*  *Common Name (eg, YOUR name) []:****/business/snakeoil***  *Email Address []:****snakeoil*@yandex.ru** |

**Step 3: Requesting the certificate**

Principal has to send to the PS:

* File with certificate request, generated before.

**Step 4: Installing certificate**

PS sends to Principal the file with issued certificate. Certificate validity period is 1 year.

Principal downloads the PS certification chain from address: <http://crls.yamoney.ru/ym.p7b> then installs it into the trusted certification authorities list.

Note: It is convenient to keep the pair of private key and certificate in a single encrypted file in PKCS#12 format. For example, the command for PKCS#12 keystore file creation:

|  |
| --- |
| *openssl pkcs12 –export –in username.crt –inkey private.key –out username.p12* |

## Principal obligations

Principal is obliged to:

* Verify the PS server’s authenticity by server SSL certificate validation thorough PS certification chain. If server authenticity check fails, Principal should terminate the connection.
* Use its own private key and certificate for connection.
* Keep the private key secure.
* Check the certificate validity period by one’s own.

Additional recommendations for the Principals:

* Check the PS server certificates, using PS Certificate Revocation List (CRL), available at <http://crls.yamoney.ru/issuingca.crl>
* Request different certificates for different subsystems of Principal server’s system.

If the Principal’s private key has compromised, the Principal must immediately notify PS about certificate compromise.

The certificate replacement due to expiration or private key compromise should be made by the same procedure as requesting a new certificate.