TLS-

TLS :

-
-
-

TLS . WEB- TLS-.

, , WEB-.

TLS , - . **GOST2001-GOST89-GOST89**, VKO GOST 34.10-2001.

TLS. TLS- , : Internet Explorer Microsoft Crypto API schannel; Mozilla Firefox NSS; Google Chrome NSS, OpenSSL.

sTunnel. sTunnel – “” , TLS WEB-, .

STunnel OpenSSL, c **GOST2001-GOST89-GOST89,** . VKO GOST 34.10-2001 , “” , , .

sTunnel engine PKCS11_GOST.

sTunnel 5-16

! openssl 1.0.1f.

Stunnel (5-16).

```
diff --git a/src/client.c b/src/client.c
index 53292a6..8ba2673 100644
--- a/src/client.c
+++ b/src/client.c
@@ -358,7 +358,7 @@ NOEXPORT void remote_start(CLI *c) {
 NOEXPORT void ssl_start(CLI *c) {
     int i, err;
     SSL_SESSION *old_session;
-    int unsafe_openssl;
+    int unsafe_openssl = 1;
     X509 *peer_cert;

     c->ssl=SSL_new(c->opt->ctx);
@@ -395,8 +395,6 @@ NOEXPORT void ssl_start(CLI *c) {
         SSL_set_accept_state(c->ssl);
     }

-    unsafe_openssl=SSLeay()<0x0090810fL ||
-        (SSLeay()>=0x10000000L && SSLeay()<0x1000002fL);
     while(1) {
         /* critical section for OpenSSL version < 0.9.8p or 1.x.x < 1.0.0b *
          * this critical section is a crude workaround for CVE-2010-3864   *
diff --git a/src/ssl.c b/src/ssl.c
index 82a15e1..e651a30 100644
--- a/src/ssl.c
+++ b/src/ssl.c
@@ -82,6 +82,8 @@ NOEXPORT void cb_free(void *parent, void *ptr, CRYPTO_EX_DATA *ad,
 }

 int ssl_configure(GLOBAL_OPTIONS *global) { /* configure global SSL settings */
+    OpenSSL_add_all_algorithms();
+    SSLeay_add_ssl_algorithms();
 #ifdef USE_FIPS
     if(FIPS_mode()!=global->option.fips) {
         RAND_set_rand_method(NULL); /* reset RAND methods */
```

sTunnel.conf:

sTunnel Windows.

```
;
verify=2

;    TLS-
client=yes

;
CAFile=ca2001_A-root.crt

;   TLS
sslVersion=TLSv1

;
taskbar=yes

;
DEBUG=7

;  engine PKCS11_GOST
engine=pkcs11_gost

;   PKCS#11
engineCtrl=MODULE_PATH:rtpkcs11ecp.dll

; -  engine
engineDefault=ALL


[remote system]

;     engine PKCS11_GOST
engineNum = 1

;
cert=client.crt

; ID
key = 03:bf:4a:c2:a9:7a:bc:de:9b:e0:bb:6e:45:7c:0c:82:07:85:c6:fd

;
accept = 127.0.0.1:1443

;
connect = 192.168.0.78:2443

;     TLS
ciphers = GOST2001-GOST89-GOST89

; for IE
TIMEOUTclose = 0
```

sTunnel Windows

sTunnel . stunnel :

- stunnel.exe
- stunnel.conf

openssl:

- libeay32.dll
- ssleay32.dll
- gost.dll

engine :

- pkcs11_gost.dll

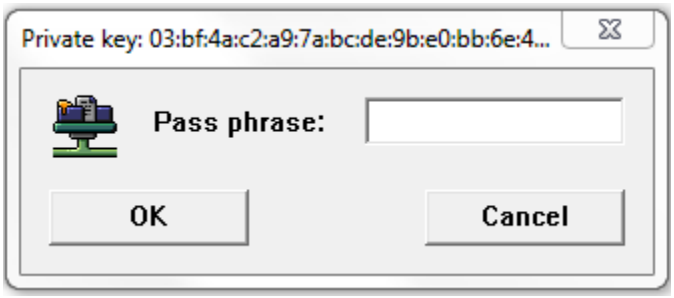
PKCS#11 :

- rtpkcs11ecp.dll

, .

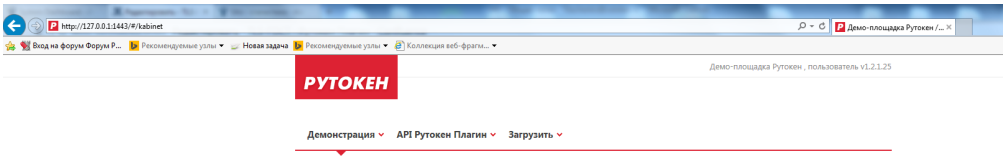
sTunnel OPENSSL_ENGINES = [, pkcs11_gost.dll gost.dll].

, sTunnel PIN- :



PIN- :

http://127.0.0.1:1443 :



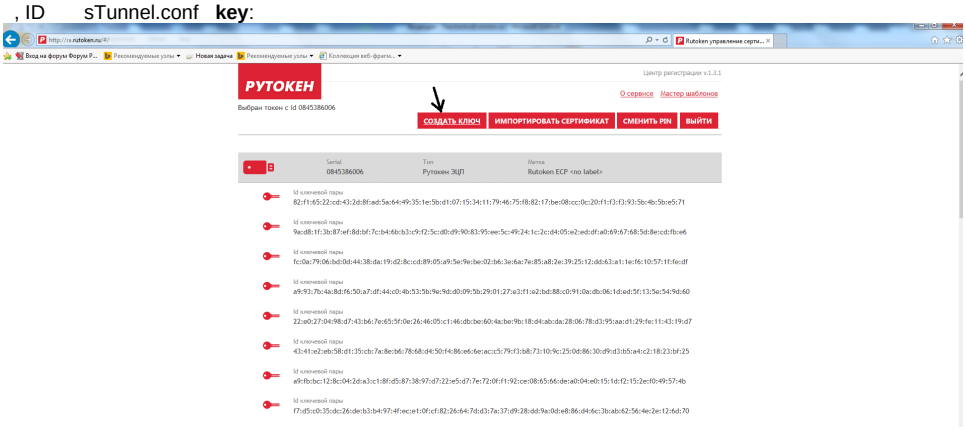
TLS-

, sTunnel , ca.crt, **CAFile** stunnel.conf. .

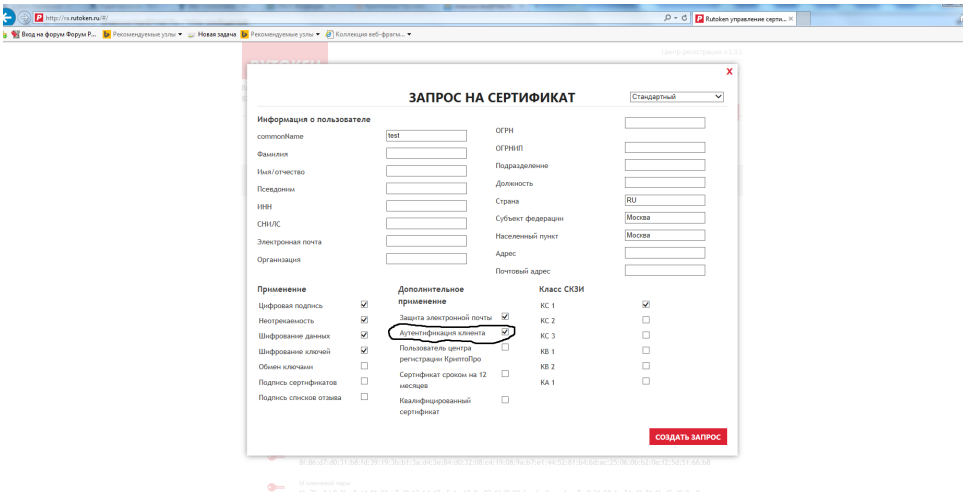
```
-----BEGIN CERTIFICATE-----
MIICTDCCAfugAwIBAgIQK24zUf1usq1IIAIDy1uhQTAIBgYqhQMCAgMwfzEjMCEG
CSqGSIb3DQEJARYUc3VwcG9ydEBjcnlwdG9wcm8ucnUxCzAJBgNVBAYTAlJVMQ8w
DQYDVQQHEwZNb3Njb3cxFzAVBgNVBAoTDkNSWVBUTy1QUk8gTExDMSEwHwYDVQQD
ExhDUllQVE8tUFJPIFRlc3QgQ2VudGVyIDIwHhcNMTQwODA1MTM0NDI0WhcNMTkw
ODA1MTM1NDAzWjB/MSMwIQYJKoZIhvcNAQkBFhRzdXBwb3J0QGNyeXB0b3Byby5y
dTELMAkGA1UEBhMCUlUxDzANBgNVBAcTBk1vc2NvdzEXMBUGA1UEChMOQ1JZUFRP
LVBSTyBMTEMxITAfBgNVBAMTGENSWVBUTy1QUk8gVGVzdCBDZW50ZXIgMjBjMBwG
BiqFAwICEzASBgcqhQMCAiMBBgcqhQMCAh4BA0MABEDgUgrcR9wpvdcgXwxIfO/U
jR52JdC9UgWOrc3Ky2YMpunm+lAm5JIgbnCASrzW/Q43EMfmhQGy7dZijrm3zcee
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUFTF8
sI0a3mbXFZxJUpcXJLkBeoMwEAYJKwYBBAGCNxUBBAMCAQAwCAYGKoUDAgIDA0EA
2MocS+lhIGVHLNXI6jiI3s3scchFv7+c5d7/VVp3JJnt4Lki0avn90/m0G97j1oq
407pZA2QUDLB8eO0SRJX1Q==
-----END CERTIFICATE-----
```

:

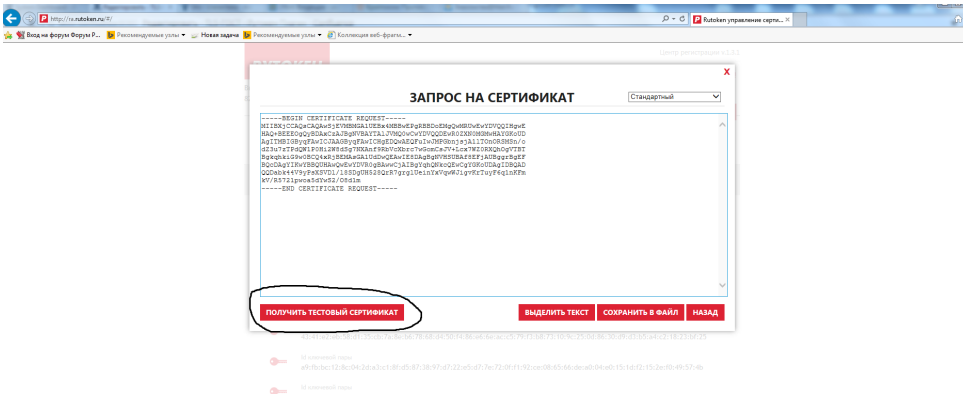
1. , http://ra.rutoken.ru
2. ,
3. , ID sTunnel.conf **key**:



4. :



5. :



6. client.crt, **cert** stunnel.conf