2.0

, openssl.

, :

- ( )
-
- / CMS
- / CMS

- , JavaScript openssl.

USB- . .

```
var devices = Array();

try
{
    devices = plugin.enumerateDevices();
}
catch (error)
{
    console.log(error);
}
```

. , , . .

US- , PINPad. .

getRutokenModelName() https://github.com/AktivCo/blade-runner.github.io

> *getDeviceInfo* *TOKEN_INFO_DEVICE_TYPE* – .

getDeviceInfo :

-
-
-
- ,

PIN-

PIN- :

```
var options = {};

try
{
    plugin.changePin(deviceId, "12345678", "12345671", options);
}
catch (error)
{
    console.log(error);
}
```

PIN-, PIN-.

1. 3 :
   - (CERT_CATEGORY_USER)
     , . , , CMS/PKCS#7, TLS.
     , . , «» . , .
   - (CERT_CATEGORY_CA)
     , . ( ) , . , verify , . , .
   - (CERT_CATEGORY_OTHER)
     , .

2. , , .

:

```
 var certs = Array();

try
{
    certs = plugin.enumerateCertificates(deviceId, plugin.CERT_CATEGORY_USER);
}
catch (error)
{
    console.log(error);
}
```

3. PEM-:

```
var certpem;

try
{
    certpem = plugin.getCertificate(deviceId, certId);
}
catch (error)
{
    console.log(error);
}
```

:

```
-----BEGIN CERTIFICATE-----
MIIBmjCCAUegAwIBAgIBATAKBgYqhQMCAgMFADBUMQswCQYDVQQGEwJSVTEPMA0G
A1UEBxMGTW9zY293MSIwIAYDVQQKFBlPT08gIkdhcmFudC1QYXJrLVRlbGVjb20i
MRAwDgYDVQQDEwdUZXN0IENBMB4XDTE0MTIyMjE2NTEyNVoXDTE1MTIyMjE2NTEy
NVowEDEOMAwGA1UEAxMFZmZmZmYwYzAcBgYqhQMCAhMwEgYHKoUDAgIjAQYHKoUD
AgIeAQNDAARADKA/O1Zw50PzMpcNkWnW39mAJcTehAhkQ2Vg7bHkIwIdf7zPe2Px
HyAr6lH+stqdACK6sFYmkZ58cBjzL0WBwaNEMEIwJQYDVR0lBB4wHAYIKwYBBQUH
AwIGCCsGAQUFBwMEBgYpAQEBAQIwCwYDVR0PBAQDAgKkMAwGA1UdEwEB/wQCMAAw
CgYGKoUDAgIDBQADQQD5TY55KbwADGKJRK+bwCGZw24sdIyayIX5dn9hrKkNrZsW
detWY3KJFylSulykS/dfJ871IT+8dXPU5A7WqG4+
-----END CERTIFICATE-----
```

4. parseCertificate DN Subject, DN Issuer, , , , , ..

5. .

:

```
 var certpem = "-----BEGIN CERTIFICATE-----
MIIBmjCCAUegAwIBAgIBATAKBgYqhQMCAgMFADBUMQswCQYDVQQGEwJSVTEPMA0G
A1UEBxMGTW9zY293MSIwIAYDVQQKFBlPT08gIkdhcmFudC1QYXJrLVRlbGVjb20i
MRAwDgYDVQQDEwdUZXN0IENBMB4XDTE0MTIyMjE2NTEyNVoXDTE1MTIyMjE2NTEy
NVowEDEOMAwGA1UEAxMFZmZmZmYwYzAcBgYqhQMCAhMwEgYHKoUDAgIjAQYHKoUD
AgIeAQNDAARADKA/O1Zw50PzMpcNkWnW39mAJcTehAhkQ2Vg7bHkIwIdf7zPe2Px
HyAr6lH+stqdACK6sFYmkZ58cBjzL0WBwaNEMEIwJQYDVR0lBB4wHAYIKwYBBQUH
AwIGCCsGAQUFBwMEBgYpAQEBAQIwCwYDVR0PBAQDAgKkMAwGA1UdEwEB/wQCMAAw
CgYGKoUDAgIDBQADQQD5TY55KbwADGKJRK+bwCGZw24sdIyayIX5dn9hrKkNrZsW
detWY3KJFylSulykS/dfJ871IT+8dXPU5A7WqG4+
-----END CERTIFICATE-----";

try
{
    plugin.importCertificate(deviceId, certpem, plugin.CERT_CATEGORY_USER);
}
catch (error)
{
    console.log(error);
}
```

6. deleteCertificate .

1. , , PIN-. , , .

```
var keys = Array();

try
{
    plugin.login(deviceId, "12345678");
    keys = plugin.enumerateKeys(deviceId, null);
}
catch (error)
{
    console.log(error);
}
```

2. PIN-. . , .

- 34.10-2012 256 :
  - "A"
  - "B"
  - "C"
  - "XA"
  - "XB"
- 34.10-2012 512
  - "A"
  - "B"

34.10-2012:

```
var options = {};
var keyId;

try
{
    keyId = plugin.generateKeyPair(deviceId, undefined, marker, options);
}
catch (error)
{
    console.log(error);
}
```

3. deleteKeyPair .

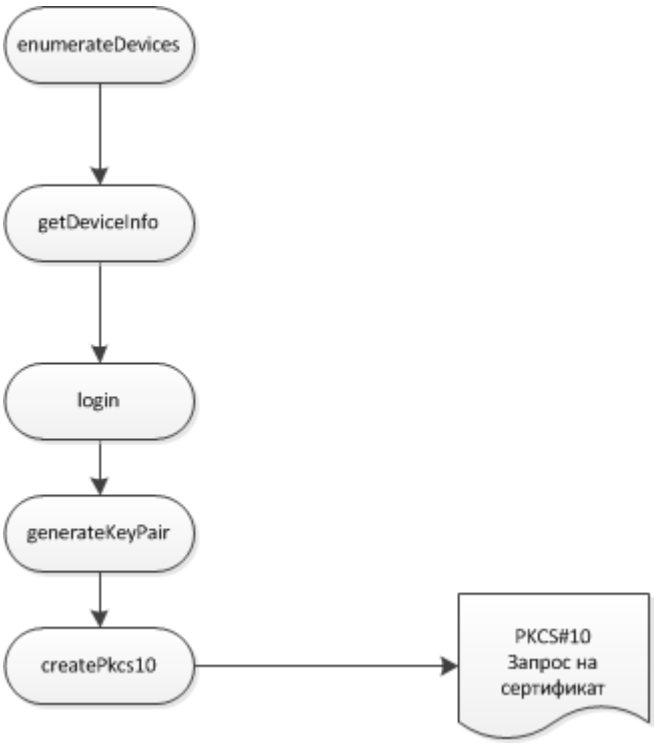
openssl

. 2012 OpenSSL 1.1.0 , OpenSSL

.

- 2.0
- 34.10-2012 2.0
- C PKCS#10
-
- , ( ). , , enumerateCertificates,
-
-
- 2.0

:



, .
openssl 1.0 .

1. :

```
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A -out ca.key
```

ca.key

2. :

```
openssl req -utf8 -x509 -key seckey.pem -out ca.crt
```

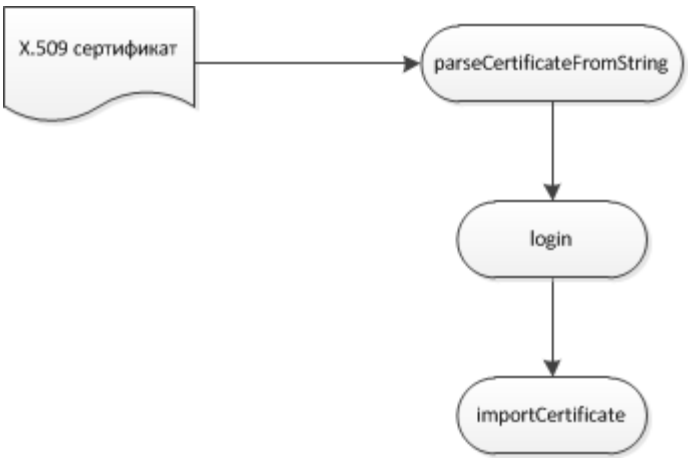
ca.crt .

user.csr ( ):

```
openssl ca -keyfile ca.key -cert ca.crt -in user.csr -out user.crt -outform PEM -batch
```

user.crt PEM . .

:

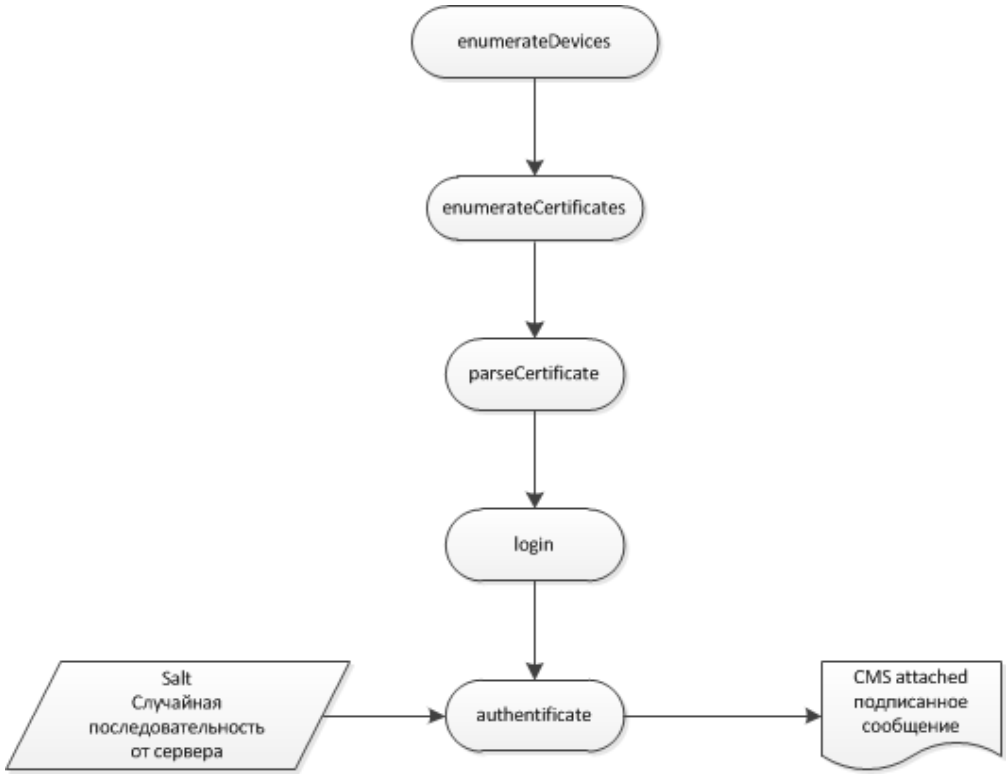


,

, rtPKCS11ECP 2.0.

- 2.0
- 2.0
-
-
- (salt)
- authenticate. salt authenticate 32 , CMS attached
-
- CMS attached
- CMS attached , "" salt
- , , CMS attached

:



base64-. openssl , PEM. :

```
-----BEGIN CMS-----
MIIDUQYJKoZIhvcNAQcCoIIDQjCCAz4CAQExDDAKBgYqhQMCAgkFADCBygYJKoZI
hvcNAQcBoIG8BIG5PCFQSU5QQURGSUxFIFVURjg+PFY+0JLRi9C/0L7Qu9C90LjR
gtGMINCw0YPRgtC10L3RgtC40YTQuNC60LDRhtC40Y4/PCE+c2VydmVyLXJhbmRv
bS1kYXRhZTI6ZGE6MmM6MDU6MGI6MzY6MjU6MzQ6YzM6NDk6Nzk6Mzk6YmI6MmY6
YzU6Mzc6ZGI6MzA6MTQ6NDQ6ODM6NjY6Njk6NmI6OWY6YTU6MDk6MzQ6YmY6YzQ6
NzY6YzmgggGeMIIBmjCCAUegAwIBAgIBATAKBgYqhQMCAgMFADBUMQswCQYDVQQG
EwJSVTEPMA0GA1UEBxMGTW9zY293MSIwIAYDVQQKFBlPT08gIkdhcmFudC1QYXJr
LVRlbGVjb20iMRAwDgYDVQQDEwdUZXN0IENBMB4XDTE0MTIyMjE2NTEyNVoXDTE1
MTIyMjE2NTEyNVowEDEOMAwGA1UEAxMFZmZmZmYwYzAcBgYqhQMCAhMwEgYHKoUD
AgIjAQYHKoUDAgIeAQNDAARADKA/O1Zw50PzMpcNkWnW39mAJcTehAhkQ2Vg7bHk
IwIdf7zPe2PxHyAr6lH+stqdACK6sFYmkZ58cBjzL0WBwaNEMEIwJQYDVR0lBB4w
HAYIKwYBBQUHAwIGCCsGAQUFBwMEBgYpAQEBAQIwCwYDVR0PBAQDAgKkMAwGA1Ud
EwEB/wQCMAAwCgYGKoUDAgIDBQADQQD5TY55KbwADGKJRK+bwCGZw24sdIyayIX5
dn9hrKkNrZsWdetWY3KJFylSulykS/dfJ871IT+8dXPU5A7WqG4+MYG7MIG4AgEB
MFkwVDELMAkGA1UEBhMCUlUxDzANBgNVBAcTBk1vc2NvdzEiMCAGA1UEChQZT09P
ICJHYXJhbnQtUGFyay1UZWxlY29tIjEQMA4GA1UEAxMHVGVzdCBDQQIBATAKBgYq
hQMCAgkFADAKBgYqhQMCAhMFAARAco5PumEfUYVcLMb1cnzETNOuWC8Goda8pdUL
W5ASK+tztCwM7wpXgAy+Y6/sLtClO9sh8dKnAaEY2Yavg3altQ==
-----END CMS-----
```

:

```
openssl cms -verify -in sign.cms -inform PEM -CAfile ca.crt -out data.file -certsout user.cr
```

sign.cms — , , ca.crt — , , data.file — , , user.crt — , . data.file 32 salt.

, :

:

```
openssl x509 -in cert.pem -noout -text
```

:

```
openssl x509 -in cert.pem -noout -serial
```

DN (subject):

```
openssl x509 -in cert.pem -noout -subject
```

DN (issuer):

```
openssl x509 -in cert.pem -noout -issuer
```

:

```
openssl x509 -in cert.pem -noout -email
```

:

```
openssl x509 -in cert.pem -noout -startdate
```

:

```
openssl x509 -in cert.pem -noout -enddate
```

, , :

- (salt)
- salt authenticate 32 , CMS attached
-
-
- CMS attached , “” salt
- , CMS

«, , ».

/ CMS

- (), ,
- (, PDF), base64
- , , sign

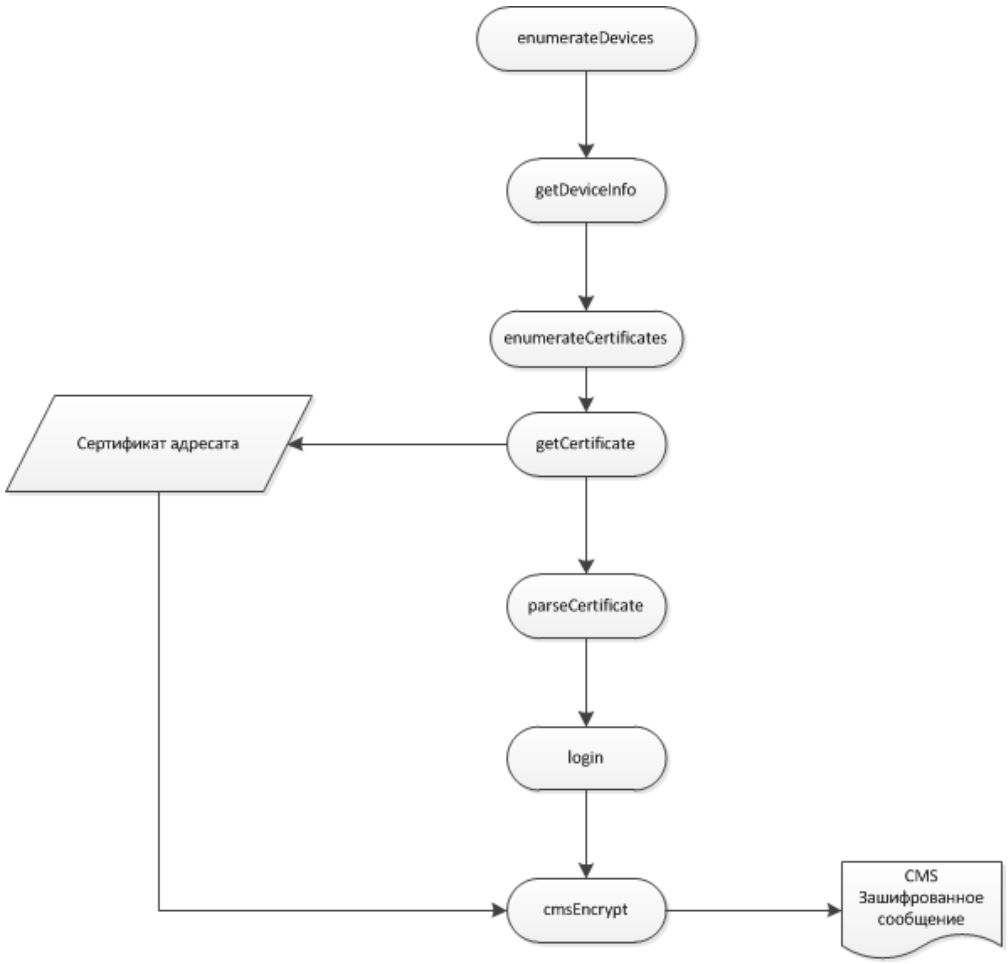
- base64 , isBase64 true, base64
- - 34.11-94 (, 60-70 /c), options useHardwareHash true. false, - 34.11-2012
- “” (detached) CMS, detached true, “” (attached)
- , / CMS- addUserCertificate
- addSignTime true , CMS-

.

/ / CMS

, / . CMS. , CMS, «». . 2.0. . importCertificate, category CERT_CATEGORY_OTHER. cmsEncrypt get Certificate. . , 28147-89, useHardwareEncryption true. 28147-89.

:



:

```
try
{
    var recipientCert = plugin.getCertificate(deviceId, certRecId);
}
catch (error)
{
    console.log(error);
}

var options = {};
options.useHardwareEncryption = true;
var cms;

try
{
    cms = plugin.cmsEncrypt(deviceId, certSenderId, recipientCert, data, options);
}
catch (error)
{
    console.log(error);
}
```

PEM- "-----BEGIN PKCS7-----" "-----END PKCS7-----":

```
openssl cms -decrypt -binary -in message.cms -inform PEM -recip respondent.cer -inkey recipient.key -out
drecipient.crt
```

recipient.crt — , , recipient.key — , .

, ,

, , cmsDecrypt. , , keyId , . . , , getKeyByCertificate.

:

```
openssl cms -encrypt -binary -gost28147-paramset_a-cfb -in data.file -out message.enc -outform PEM user.crt
```

:

```
var data;
var options = {};
try
{
    data = plugin.cmsDecrypt(deviceId, keyId, cms, options);
}
catch (error)
{
    console.log(error);
}
```

openssl:

WEB- , , ,
openssl