**Описание библиотеки php\_gost\_crypto.dll**

Библиотека php\_gost\_crypto.dll реализована в MS Visual Studio 2005 на языке VisualC и является расширением для языка php версии 5.21.

В библиотеке реализованы следующие функции:

**gostGetLastError()**  
 ***Возвращаемые значения:***

string - описание последней ошибки на англ.языке

**gostPathFileLog ( string $ sPathFileLog )**

***sPathFileLog*** *- путь к файлу журнала работы. Если значение пусто, то возвращается имеющееся значение.*

***Возвращаемые значения:***

В случае успеха - string *путь к файлу журнала работы.*

В случае неудачи - bool false. Узнать причину ошибки можно вызвав функцию gostGetLastError()

**gostSignBlock  ( string $sB64*Data*, string $ sID*Cert, bool bSignDetached = true* );**  
 **sB64*Data*** *- данные для подписи закодированные в Base64*  
 **sID*Cert*** *- ИД сертификата подписи (CN или Thumb)*  
 ***bSignDetached*** *- (false - подпись откреплена от подписываемых данных,  true – результатом работы функции будет единый контейнер, содержащий данные + подпись)*  
 ***Возвращаемые значения:***   
 В случае успеха - string содержащая результирующий контейнер в кодировке Base64  
 В случае неудачи - bool false. Причину ошибки можно узнать вызвав функцию gostGetLastError()  
  
**gostSignFile ( string $sPathFileSrc, string $sPathFileDst, string $ sID*Cert, bool bSignDetached = true* );**  
 **sPathFileSrc** *– путь к файлу содержащий данные для подписи.*

**sPathFileDst** *– путь к файлу, который будет содержать результат (либо только подпись, либо данные + подпись).*   
 **sID*Cert*** *- ИД сертификата подписи (CN или Thumb)*  
 ***bSignDetached*** *- (false - подпись откреплена от подписываемых данных,  true – результатом работы функции будет единый контейнер, содержащий данные + подпись)*  
 ***Возвращаемые значения:***   
 В случае успеха – bool true.

В случае неудачи - bool false. Причину ошибки можно узнать вызвав функцию gostGetLastError().  
  
**gostVerifyBlock  ( string $sB64*Data*, string $ s*B64Sign = ""*)**  
 **sB64*Data*** *- данные для проверки подписи закодированные в Base64. Если эти данные уже содержат в себе подпись, то следующий параметр* s*B64Sign должен быть равен пустой строке.*   
 **sB64Sign** *- значение подписи. Если параметр* sB64*Data содержит в себе подпись, то* sB64Sign *= "".*  
 ***Возвращаемые значения:***   
 В случае неудачи - bool false. Причину ошибки можно узнать вызвав функцию gostGetLastError().  
 В случае успеха - string содержащая значение ключевых параметров сертификата подписи в нижеследующем виде. Например:  
<?xml version="1.0" encoding="windows-1251"?>  
<Sign>  
<Subject>OID.1.2.643.3.131.1.1=7729633131, E=ee@garant.ru, C=RU, S=77 Москва, L=г. Москва, O=ООО Электронный экспресс, OU=0, CN=Максимов Сергей Вадимович, T=Специалист технической поддержки отдела №6</Subject>  
<DateTimeSign>09.11.2011 16:36:05</DateTimeSign>  
<Thumb>29d95ebe67a0bcbdc0f80e25f402e1be6114520b</Thumb>  
<OID>1.3.6.1.5.5.7.3.4 1.3.6.1.5.5.7.3.2 1.2.643.3.131.1000.0.2</OID>  
</Sign>  
<Sign>  
<Subject>OID.1.2.643.3.131.1.1=7729633131, E=ee@garant.ru, C=RU, S=77 Москва, L=г. Москва, O=ООО Электронный экспресс, OU=0, CN=Павлов Николай Юрьевич, T=Руководитель отдела №6</Subject>  
<DateTimeSign>17.11.2011 09:47:00</DateTimeSign>  
<Thumb>4639d5c0551562fdb4e6079c739ace77ed4a3fb6</Thumb>  
<OID>1.3.6.1.5.5.7.3.4 1.3.6.1.5.5.7.3.2 1.2.643.3.131.1000.0.2</OID>  
</Sign>  
<Sign>  
<Subject>OID.1.2.643.3.141.1.2=7718, OID.1.2.643.3.141.1.1=7718041395, T=доверенный представитель, CN=Довереннов Петр Сергеевич, OID.1.2.643.3.131.1.1=7729633131, OU=0, O=Тестовое ООО Электронный Экспресс, L=г. Москва, S=77 Москва, C=RU, E=dover@nomail.ru</Subject>  
<DateTimeSign>17.11.2011 09:39:27</DateTimeSign>  
<Thumb>e3fc21aa0bdec345b91dc50aa56434491f95fddd</Thumb>  
<OID>1.2.643.2.2.34.6 1.3.6.1.5.5.7.3.4 1.3.6.1.5.5.7.3.2 1.2.643.3.130.2.3.4.1 1.2.643.3.130.2.3.5.1 1.2.643.3.130.2.3.3.1 1.2.643.3.131.1067.0.3.3.1</OID>  
</Sign>

**gostVerifyFile  ( string $sPathFileSrc, string $ sPathFileSignDetached *= ""*)**  
 **sPathFileSrc** *– путь к файлу, содержащий данные для проверки подписи.*   
 **sPathFileSignDetached***– путь к файлу, содержащему открепленную подпись. Если это значение равно пустой строке, то это означает, что в параметре* **sPathFileSrc** *содержатся данные + подпись.*

***Возвращаемые значения:***   
 В случае неудачи - bool false. Причину ошибки можно узнать вызвав функцию gostGetLastError()  
 В случае успеха - string содержащая значение ключевых параметров сертификата подписи, в аналогичном формате, описанному в функции **gostVerifyBlock.**  
  
**gostEncryptBlock  ( string $sB64*DataSrc,*   string $ sID*CertPublic* )**  
 **sB64*DataSrc*** *- данные для шифрования закодированные в Base64.*   
 **sID*CertPublic*** *- ИД сертификатов получателей (CN или Thumb), через запятую. Закрытый ключ будет выбран на основании первого в списке сертификата.*  
 ***Возвращаемые значения:***   
 В случае успеха - string содержащая зашифрованные данные в кодировке Base64  
 В случае неудачи - bool false. Причину ошибки можно узнать вызвав функцию gostGetLastError()

**gostEncryptFile ( string $sPathFile*Src,* string $sPathFile*Dst,*  string $ sID*CertPublic* )**  
 **sPathFile*Src*** *– путь к файлу, содержащий данные для шифрования.*

**sPathFile*Dst*** *– путь к результирующему файлу, который будет содержать зашифрованные данные.*  
 **sID*CertPublic*** *- ИД сертификатов получателей (CN или Thumb), через запятую. Закрытый ключ будет выбран на основании первого в списке сертификата.*  
 ***Возвращаемые значения:***   
 В случае успеха – bool true.  
 В случае неудачи - bool false. Причину ошибки можно узнать вызвав функцию gostGetLastError()  
  
**gostEncryptBlockByCertContent ( string $ sB64DataSrc,  string $ sB64CertContentRec )**  
 **sB64DataSrc** - данные для шифрования закодированные в Base64.   
 **sB64CertContentRec** - список содержимого сертификатов получателей в кодировке Base64, через запятую.   
 При шифровании будет взят закрытый ключ первого сертификата из списка sB64CertContentRec.  
 ***Возвращаемые значения:***   
 В случае успеха - string содержащая зашифрованные данные в кодировке Base64  
 В случае неудачи - bool false. Причину ошибки можно узнать вызвав функцию gostGetLastError()

**gostEncryptFileByCertContent ( string $sPathFile*Src,* string $sPathFile*Dst*,  string $ sB64CertContentRec )**

**sPathFile*Src*** *– путь к файлу, содержащий данные для шифрования.*

**sPathFile*Dst*** *– путь к результирующему файлу, который будет содержать зашифрованные данные.*  
 **sB64CertContentRec** - список содержимого сертификатов получателей в кодировке Base64, через запятую.   
 При шифровании будет взят закрытый ключ первого сертификата из списка sB64CertContentRec.  
 ***Возвращаемые значения:***   
 В случае успеха - string содержащая зашифрованные данные в кодировке Base64  
 В случае неудачи - bool false. Причину ошибки можно узнать вызвав функцию gostGetLastError().  
  
**gostDecryptFile  ( string $sPathFile*Src,* string $sPathFile*Dst )***  
 **sPathFile*Src*** *– путь к файлу, содержащий зашифрованные данные.*

**sPathFile*Dst*** *– путь к результирующему файлу, который будет содержать расшифрованные данные.*  
 ***Возвращаемые значения:***   
 В случае успеха – bool true.  
 В случае неудачи - bool false. Причину ошибки можно узнать вызвав функцию gostGetLastError()  
  
**gostParseCertificate (string $ sB64CertContent, bool bRetXml = false)**  
 **sB64CertContent** - бинарное содержимое сертификата в кодировке Base64.

**bRetXml** – возвращаемое значение будет xml файл нижеследующего содержания или массив значений аналогичный тому, который возвращает функция openssl\_x509\_parse.  
 ***Возвращаемые значения:***   
 В случае неудачи - bool false. Причину ошибки можно узнать вызвав функцию gostGetLastError().  
 В случае успеха и **bRetXml = true** - string содержащая ключевые параметры сертификата в следующем xml формате:  
<?xml version="1.0" encoding="windows-1251"?>  
<Certificate>  
<Type>DER</Type> **- кодировка переданного сертификата (ASN or DER)**   
<Subject>OID.1.2.643.3.131.1.1=7729633131, E=ee@garant.ru, C=RU, S=77 Москва, L=г. Москва, O=ООО Электронный экспресс, OU=0, CN=Максимов Сергей Вадимович, T=Специалист технической поддержки отдела №6</Subject>  
<Issuer>E=ucinfo@gnivc.ru, C=RU, L=Москва, O=ФГУП ГНИВЦ ФНС России, OU=Удостоверяющий центр, CN=GNIVC FNS RUS</Issuer>  
<Thumb>29d95ebe67a0bcbdc0f80e25f402e1be6114520b</Thumb>  
<NotBeforeTimeXml>2010-12-29T16:01:00</NotBeforeTimeXml> **- дата-время в стандарте xml**  
<NotBeforeTimeLong>1293627660</NotBeforeTimeLong> **-  дата-время для удобства парсинга (число секунд с 01.01.1970)**  
<NotAfterTimeXml>2011-12-29T16:10:00</NotAfterTimeXml>  
<NotAfterTimeLong>1325164200</NotAfterTimeLong>  
<SerialNumber>1208e37a0000000056db</SerialNumber> **- серийный номер серта**  
<Version>V3</Version>  
<Encoding>1</Encoding> **- значение поля dwCertEncodingType. Возможные значения X509\_ASN\_ENCODING , X509\_NDR\_ENCODING и др.**  
<SignatureAlgorithm>1.2.643.2.2.3=0500</SignatureAlgorithm> **- ИД алгоритма подписи и его значение**   
<Extension> **- список всех EKU в виде <поле>=<значение HEX> разделитель пробел <поле>=<значение HEX> и т.д.**  
2.5.29.15=01000000940bb20204000000f0cdcdcdcdcdcdcd 2.5.29.37=02000000885fb202905fb202a85fb202312e332e362e312e352e352e372e332e3400cdcdcdcdcdcd312e332e362e312e352e352e372e332e3200cdcdcdcdcdcd 2.5.29.14=14000000189db2020e20818e8b98fa10169fc4d961b2cd156fd92cebcdcdcdcd 2.5.29.35=14000000100cb202000000000000000000000000000000001310b7924fbfe7a20fb8f59d891526cb10ebf45fcdcdcdcd 2.5.29.31=01000000785eb2020100000002000000985eb202000000000000000000000000000000000000000007000000b05eb202cdcdcdcd07000000005fb202cdcdcdcd68007400740070003a002f002f007700770077002e0067006e006900760063002e00720075002f00750063002f0047004e0049005600430046004e0053005200550053002e00630072006c000000cdcd68007400740070003a002f002f00630030003000300030002d006100700070003000300035002f0067006e006900760063002f0047004e0049005600430046004e0053005200550053002e00630072006c000000cdcdcdcd 1.3.6.1.5.5.7.1.1= 2.5.29.32=01000000000cb202100cb2020000000000000000cdcdcdcd312e322e3634332e332e3133312e313030302e302e3200cd  
</Extension>  
</Certificate>

В случае успеха и **bRetXml = false** будет возвращен массив содержащий ключевые параметры сертификата в формате, который получается в результате вызова openssl\_x509\_parse :

Array

(

[name] => OID.1.2.840.113549.1.9.2=Руководство 077-001-0101/001/077/PFR/RU/C=RU/L=г. Самара/S=Самарская область/OID.2.5.4.16=#30450C433434333033302C20D0B32E20D0A1D0B0D0BCD0B0D180D0B02C20D183D0BB2ED0A7D0B5D180D0BDD0BED180D0B5D187D0B5D0BDD181D0BAD0B0D18F2C20D0B42E203231/SERIALNUMBER=077-001-0230/E=077-001-0101@077.pfr.ru/O=ГУ — Управление ПФР в Железнодорожном районе г.Самары/OU=Руководство/T=Начальник Управления/CN=077-001(ЭДО) -начальник управления Костенюк А.Ю.

[subject] => Array

(

[OID.1.2.840.113549.1.9.2] => Руководство 077-001-0101/001/077/PFR/RU

[C] => RU

[L] => г. Самара

[S] => Самарская область

[OID.2.5.4.16] => #30450C433434333033302C20D0B32E20D0A1D0B0D0BCD0B0D180D0B02C20D183D0BB2ED0A7D0B5D180D0BDD0BED180D0B5D187D0B5D0BDD181D0BAD0B0D18F2C20D0B42E203231

[SERIALNUMBER] => 077-001-0230

[E] => 077-001-0101@077.pfr.ru

[O] => ГУ — Управление ПФР в Железнодорожном районе г.Самары

[OU] => Руководство

[T] => Начальник Управления

[CN] => 077-001(ЭДО) -начальник управления Костенюк А.Ю.

)

[issuer] => Array

(

[OID.1.2.840.113549.1.9.2] => 077UC/077/PFR/RU

[C] => RU

[L] => г. Самара

[S] => Самарская область

[OID.2.5.4.16] => #30390C373434333034312C20D0B32E20D0A1D0B0D0BCD0B0D180D0B02C20D183D0BB2E20D0A1D0B0D0B4D0BED0B2D0B0D18F2C20D0B42E20313735

[E] => 077UC@077.pfr.ru

[O] => ГУ - ОПФР по Самарской области

[OU] => Отдел по защите информации

[CN] => УЦ ОПФР по Самарской области

)

[extensions] => Array

(

[2.5.29.15] => 01000000249f3b0003000000f8cdcdcdcdcdcdcd

[2.5.29.37] => 02000000000c3b00080c3b00200c3b00312e332e362e312e352e352e372e332e3200cdcdcdcdcdcd312e332e362e312e352e352e372e332e3400cdcdcdcdcdcd

[2.5.29.19] => 000000000000000000000000

[2.5.29.31] => 01000000000c3b000100000001000000200c3b00000000000000000000000000000000000000000007000000300c3b00cdcdcdcdcdcdcdcd68007400740070003a002f002f00630061002e0070006600720066002e00720075002f006f0074005f00730061006d006100720061002f00630061005f00730061006d006100720061002e00630072006c000000cdcdcdcd

[2.5.29.14] => 14000000000c3b00dfa722fca16023c79420635d410acd6994d5adb2cdcdcdcd

[2.5.29.35] => 14000000100c3b00000000000000000000000000000000007faf340884e51af7e53c536ba77a4f3875baece3cdcdcdcd

)

[version] => 2

[serialNumber] => 01cbeaf80095fe10000012bf01920161

[validFrom\_time\_t] => 1301063030

[validTo\_time\_t] => 1332685430

)