**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, bool bReturnAsXML = false*)**  
 **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 *должно быть пустым.*

***bReturnAsXML*** *– возвращаемое значение должно быть XML. Иначе будет возвращен массив с информацией о подписях (см.ниже).*

***Возвращаемые значения:***   
 В случае неудачи - bool false. Причину ошибки можно узнать вызвав функцию gostGetLastError().  
 1) В случае успеха и ***bReturnAsXML = true*** - 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>*

2) В случае успеха и ***bReturnAsXML = false*** массив. Например:

*Array*

*(*

*[0] => Array*

*(*

*[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*

*[Thumb] => 29d95ebe67a0bcbdc0f80e25f402e1be6114520b*

*[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*

*[DateTimeSign] => 17.12.2011 15:08:14*

*)*

*[1] => Array*

*(*

*[Subject] => OID.1.2.643.3.131.1.1=7729633131, E=sos@garant.ru, C=RU, S=77 Москва, L=г. Москва, O=ООО Электронный экспресс, OU=0, CN=Доверенов Петр Сергеевич, T=Администратор*

*[Thumb] => 25f402e1be6114520b29d95ebe67a0bcbdc0f80e*

*[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*

*[DateTimeSign] => 13.12.2011 10:08:14*

*)*

*)*

**gostVerifyFile  ( string $sPathFileSrc, string $ sPathFileSignDetached*, bool bReturnAsXML = false*)**  
 **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.*

***bReturnAsXML*** *– возвращаемое значение должно быть XML. Иначе будет возвращен массив с информацией о подписях (см.выше).*

***Возвращаемые значения:***   
 В случае неудачи - bool false. Причину ошибки можно узнать вызвав функцию gostGetLastError()  
 1) В случае успеха и ***bReturnAsXML = true*** - string содержащая значение ключевых параметров сертификата подписи в нижеследующем виде, в аналогичном формате, описанному в функции **gostVerifyBlock.**  
2) В случае успеха и ***bReturnAsXML = false*** массив, 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 $ sPathCertFile\_Or\_B64CertContent, bool bReturnAsXml = false)**  
 **sPathCertFile\_Or\_B64CertContent** – путь к файлу сертификата или содержимое сертификата в кодировке Base64 в одном из следующих форматов:

1. Любое бинарное содержимое файла сертификата преобразованное в Base64.
2. -----BEGIN CERTIFICATE-----

MIIEfzCCBCygAwIBAgIKEgjjegAAAABW2zAKBgYqhQMCAgMFADCBwDEeMBwGCSqG.

…..

-----END CERTIFICATE-----

1. Содержимое файла сертификата ASN1 преобразованное в Base64 MIIEfzCCBCygAwIBAgIKEgjjegAAAABW2zAKBgYqhQMCAgMFADCBwDEeMBwGCSqG…..

**bReturnAsXml** – 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().  
 1) В случае успеха и **bReturnAsXml = 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 «новая строка» <поле>=<значение HEX> и т.д.*** *2.5.29.15=Использование ключа: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)*

*2.5.29.37=Улучшенный ключ: Защищенная электронная почта (1.3.6.1.5.5.7.3.4)*

*2.5.29.14=Идентификатор ключа субъекта: 4a e9 fd b6 79 83 fe 48 30 26 53 5f e2 c7 60 7f 6f ad c3 a9*

*2.5.29.35=Идентификатор ключа центра сертификатов: Идентификатор ключа=13 10 b7 92 4f bf e7 a2 0f b8 f5 9d 89 15 26 cb 10 eb f4 5f*

*2.5.29.31=Точки распространения списков отзыва (CRL): [1]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://www.gnivc.ru/uc/GNIVCFNSRUS.crl, URL=http://c0000-app005/gnivc/GNIVCFNSRUS.crl*

*1.3.6.1.5.5.7.1.1=Доступ к информации о центрах сертификации: [1]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://www.gnivc.ru/uc/GNIVCFNSRUS.crt, [2]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://c0000-app005/gnivc/GNIVCFNSRUS.crt*

*2.5.29.32=Политики сертификата: [1]Политика сертификата:Идентификатор политики=1.2.643.3.131.1000.0.11</Extension>*

*</Certificate>  
</Extension>  
</Certificate>*

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

*Array*

*(*

*[name] => OID.1.2.643.3.131.1.1=7729633131/E=bydancev@garant.ru/C=RU/S=77 г. Москва/L=Москва/O=ООО Электронный экспресс/OU=0/CN=Быданцев Максим Валерьевич/T=Руководитель УЦ ГАРАНТ*

*[subject] => Array*

*(*

*[OID.1.2.643.3.131.1.1] => 7729633131*

*[E] => bydancev@garant.ru*

*[C] => RU*

*[S] => 77 г. Москва*

*[L] => Москва*

*[O] => ООО Электронный экспресс*

*[OU] => 0*

*[CN] => Быданцев Максим Валерьевич*

*[T] => Руководитель УЦ ГАРАНТ*

*)*

*[issuer] => Array*

*(*

*[E] => ucinfo@gnivc.ru*

*[C] => RU*

*[L] => Москва*

*[O] => ФГУП ГНИВЦ ФНС России*

*[OU] => Удостоверяющий центр*

*[CN] => GNIVC FNS RUS*

*)*

*[extensions] => Array*

*(*

*[2.5.29.15] => Использование ключа: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)*

*[2.5.29.37] => Улучшенный ключ: Защищенная электронная почта (1.3.6.1.5.5.7.3.4)*

*[2.5.29.14] => Идентификатор ключа субъекта: 4a e9 fd b6 79 83 fe 48 30 26 53 5f e2 c7 60 7f 6f ad c3 a9*

*[2.5.29.35] => Идентификатор ключа центра сертификатов: Идентификатор ключа=13 10 b7 92 4f bf e7 a2 0f b8 f5 9d 89 15 26 cb 10 eb f4 5f*

*[2.5.29.31] => Точки распространения списков отзыва (CRL): [1]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://www.gnivc.ru/uc/GNIVCFNSRUS.crl, URL=http://c0000-app005/gnivc/GNIVCFNSRUS.crl*

*[1.3.6.1.5.5.7.1.1] => Доступ к информации о центрах сертификации: [1]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://www.gnivc.ru/uc/GNIVCFNSRUS.crt, [2]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://c0000-app005/gnivc/GNIVCFNSRUS.crt*

*[2.5.29.32] => Политики сертификата: [1]Политика сертификата:Идентификатор политики=1.2.643.3.131.1000.0.11*

*)*

*[version] => 2*

*[serialNumber] => 34b3c901000000005d7b*

*[validFrom\_time\_t] => 1308738120*

*[validTo\_time\_t] => 1340361060*

*[thumb] => bd1c668dfb319adb8fe82824298d6817e0af3ac1*

*)*