opsel — библиотека для использования криптографических функций из пакета OpenSSL

Настройка

Для работы необходима библиотека OpenSSL (https://www.openssl.org). Компиляция проходила с версией 1.1.1. Разделяемая библиотека libcrypto-1_1.dll должна находиться в доступном месте. Если на сервере приложений нет полной установки OpenSSL, то libcrypto-1_1.dll можно подложить в каталог OBJ. Библиотека gost.dll (https://github.com/gost-engine/engine) это подключаемый модуль к OpenSSL, реализующий российские криптоалгоритмы. Каталог в котором она находится, должен быть задан переменной окружения OPENSSL_ENGINES. Это может быть, и каталог OBJ, и C:\Program Files (x86)\OpenSSL\lib\engines-1_1. Просьба учесть, что если переменная окружения была установлена через Свойсва системы/Переменные среды, то потребуется рестарт сервера приложений.

opselHash(function_name:String, string:String)

Функция возвращает хэш строки string. Алгоритм расчёта хэшфункции задаётся параметром function_name. Допустимые значения: blake2b512, blake2s256, md4, md5, mdc2, rmd160, sha1, sha224, sha256, sha3-224, sha3-256, sha3-384, sha3-512, sha384, sha512, sha512-224, sha512-256, shake128, shake256, sm3, md_gost94, md_gost12_256, md_gost12_512. Если в качестве первого параметра передан null, то используется md5.

opselHashFile(function_name:String, FilePath:String)

Функция возвращает хэш файла с именем FilePath. Алгоритм расчёта хэшфункции задаётся параметром function_name. Допустимые значения: blake2b512, blake2s256, md4, md5, mdc2, rmd160, sha1, sha224, sha256, sha3-224, sha3-256, sha3-384, sha3-512, sha384, sha512, sha512-224, sha512-256, shake128, shake256, sm3, md_gost94, md_gost12_256, md_gost12_512. Если в качестве первого параметра передан null, то используется md5.

opselX509cert(CertPath:String, ArrayKeys:TArray, ArrayValues:TArray)

Функция читает файл сертификата, по пути CertPath в формате PEM и извлекает из него поля. Поля сохраняются в двух массивах переданных вторым и третьим параметром. В массиве ArrayKeys сохранется имя поля, в массиве ArrayValues с таким же индексом сохраняется значение поля.

Пример сертификата:

```
-----BEGIN CERTIFICATE-----
MIIJkTCCCUCgAwIBAgIRALZn2XrEDCOl6BHpDy4kVwcwCAYGKoUDAgIDMIIBOzEb
MBkGCSqGSIb3DQEJARYMY2FAc2VydHVtLnJ1MRgwFgYFKoUDZAESDTExMTY2NzMw
…строки пропущены…
aWNhdGVzL3NlcnR1bS1xLTIwMTYuY3J0MAgGBiqFAwICAwNBALE1nSBcC/+101kt
5RH5VFln4k0NlNnSEv7N1kbHmGFMdyVgkvNU0BvAVd/VDXmkl2hX4kvd0OtKACgF
ZoeQkQQ=
-----END CERTIFICATE-----
```

Пример вывода макроса test-opsel-x509.mac:

```
 0 subject.INN: 222509089236
 1 subject.SNILS: 13056355029
 2 subject.emailAddress: assnetkova1@vostbank.ru
 3 subject.countryName: RU
 4 subject.stateOrProvinceName: Амурская область
 5 subject.localityName: г. Благовещенск
 6 subject.organizationName: ПАО КБ "ВОСТОЧНЫЙ"
 7 subject.givenName: Анна Сергеевна
 8 subject.surname: Снеткова
 9 subject.commonName: Снеткова Анна Сергеевна
```

```
10 issuer.emailAddress: uc_fk@roskazna.ru
11 issuer.stateOrProvinceName: г. Москва
12 issuer.INN: 007710568760
13 issuer.OGRN: 1047797019830
14 issuer.streetAddress: улица Ильинка, дом 7
15 issuer.localityName: Москва
16 issuer.countryName: RU
17 issuer.organizationName: Федеральное казначейство
18 issuer.commonName: Федеральное казначейство
19 not_before:  1.06.2018 (10:26:15.00)
20 not_after:  1.09.2019 (10:26:15.00)
```

Пример вывода макроса test-opsel-hash.mac:
(строки обрезаны по длине)

```
abc    blake2b512    ba80a53f981c4d0d6a2797b69f12f6e94c212f14685ac4b74b12bb6f
abc    blake2s256    508c5e8c327c14e2e1a72ba34eeb452f37458b209ed63a294d999b4c
abc    gost   -Error: Ошибка выполнения Хэш-функция gost не найдена
abc    md4    a448017aaf21d8525fc10ae87aa6729d
abc    md5    900150983cd24fb0d6963f7d28e17f72
abc    mdc2   3ff42120ee863f5d910cf2ee5064f82f
abc    rmd160 8eb208f7e05d987a9b044a8e98c6b087f15a0bfc
abc    sha1   a9993e364706816aba3e25717850c26c9cd0d89d
abc    sha224 23097d223405d8228642a477bda255b32aadbce4bda0b3f7e36c9da7
abc    sha256 ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015a
abc    sha3-224      e642824c3f8cf24ad09234ee7d3c766fc9a3a5168d0c94ad73b46fdf
abc    sha3-256      3a985da74fe225b2045c172d6bd390bd855f086e3e9d525b46bfe245
abc    sha3-384      ec01498288516fc926459f58e2c6ad8df9b473cb0fc08c2596da7cf0
abc    sha3-512      b751850b1a57168a5693cd924b6b096e08f621827444f70d884f5d02
abc    sha384 cb00753f45a35e8bb5a03d699ac65007272c32ab0eded1631a8b605a43ff5be
abc    sha512 ddaf35a193617abacc417349ae20413112e6fa4e89a97ea20a9eeee64b55d39
abc    sha512-224    4634270f707b6a54daae7530460842e20e37ed265ceee9a43e8924aa
abc    sha512-256    53048e2681941ef99b2e29b76b4c7dabe4c2d0c634fc6d46e0e2f131
abc    shake128      5881092dd818bf5cf8a3ddb793fbcba7
abc    shake256      483366601360a8771c6863080cc4114d8db44530f8f1e1ee4f94ea37
abc    sm3    66c7f0f462eeedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b8f4ba8e
abc    md_gost94     b285056dbf18d7392d7677369524dd14747459ed8143997e163b2986
abc    md_gost12_256 4e2919cf137ed41ec4fb6270c61826cc4fffb660341e0af3688cd062
abc    md_gost12_512 28156e28317da7c98f4fe2bed6b542d0dab85bb224445fcedaf75d46
```