Интеграция ГОСТ 2012 с Рутокен ЭЦП и OpenSSL 1.1.0 или новее

«Из коробки» OpenSSL не работает с токенами или смарт-картами, используя отечественную криптографию: используйте, встроенные в Рутокен ЭЦП, алгоритмы ГОСТ через OpenSSL 1.1.0 и новее, подключив модули интеграции.

Модули интеграции — специальные библиотеки rtengine для работы с российскими криптографичекими алгоритмами ГОСТ, реализованными в семействе Рутокен ЭЦП.

Работает на всех системах, где есть OpenSSL 1.1.0 и новее.

С Модулями интеграции для OpenSSL решаются через стандартный интерфейс OpenSSL задачи:

- электронная подпись по ГОСТ Р 34-10.2001 и ГОСТ Р 34-10.2012
- вычисление хеш-функции по ГОСТ Р 34-11.94 и ГОСТ Р 34-11.2012
- симметричное шифрование и вычисление имитовставки по ГОСТ 28147-89
- распределение ключей по схеме VKO 34.10-2001 и VKO 34.10-2012
- электронная подпись и шифрование PKCS#7, CMS, S/MIME
- формирование запросов на сертификаты PKCS#10
- работа с сертификатами X.509 и списками отзыва(CRL)
- клиентская часть протокола TLS-ГОСТ
- онлайн-проверка статуса сертификата (OCSP)
- работа с временными метками (TSP)

При этом:

- электронная подпись и согласование ключей (VKO) выполняются непосредственно на чипе токена
- симметричное шифрование и вычисление хеш-функции осуществляются программным образом
- rtengine работает с утилитой openssl tool и так и с OpenSSL API