Демо-приложение для работы с ЭЦП формата XAdES-BES с использованием алгоритмов ГОСТ на .NET

Общее описание

Исходный код размещен по адресу: https://github.com/Good-Samaritan/signature-demo-net

Утилита представляет собой пример приложения, использующего ЭЦП XAdES-BES для подписания xml файлов и soap запросов с применением алгоритмов ГОСТ.

Также, утилита осуществляет отправку подписанных soap запросов в ГИС ЖКХ и разбор ответов в csv файл.

За основу был взят проект Microsoft France, доступный по адресу https://www.microsoft.com/france/openness/open-source/interoperabilite_xades.aspx. Проект распространяется по лицензии CeCILL-B. В исходный проект была внесена серия изменений для реализации требуемого функционала. Доработанный проект находится в каталоге *«Xades\Xades-master»*.

Проект имеет следующую структур:

- Library – доработанная библиотека из исходного проекта. Содержит вспомогательный функционал для работы с подписанным xml документом.
- Xades – библиотека-обертка, реализующая XaDES-BES подпись по алгоритмам ГОСТ. Более подробно описана в разделе «Внутренне устройство библиотеки Xades».
- XadesDemo – демо-приложение использующее библиотеку-обертку.
- Tests – юнит и интеграционные тесты для библиотеки-обертки.
- CommandLine – доработанная библиотека для обработки параметров командной строки.

Системные требования

Для запуска приложения необходимы следующие компоненты:

- .NET Framework 4.5
- КриптоПро CSP 3.9 или выше. Используется в качестве криптопровайдера.
- КриптоПро .NET 1.0.5913 или выше. Необходим для работы с алгоритмом хеширования GOST3411 (http://www.w3.org/2001/04/xmldsig-more#gostr3411).
- Соединение с API ГИС ЖКХ по TLS. Для организации шифрованного соединения можно использовать МагПро Криптопакет, поставляемый вместе с документацией к API ГИС ЖКХ.

Примечание: компоненты необходимо устанавливать в соответствии с порядком, используемым в списке.

Сборка приложения из исходных кодов

Для сборки проекта из исходных кодов необходимо использовать Microsoft Visual Studio 2015.

Использование утилиты

Утилита содержит следующие команды:

- sign – подписание xml файла. Подписывается элемент с заданным Id или корневой элемент.
- verify – проверка подписи в xml файле. Проверяется подпись элемента с заданным Id или корневого элемента.
- send – обращение к асинхронному методу сервиса ГИС ЖКХ. Формирует soap пакет на основе шаблона и csv файла с параметрами запроса, выполняет подписание, отправку запроса и разложение ответа.
- get-state – получение состояния обработки асинхронного запроса к методу сервиса ГИС ЖКХ. Функционирует аналогично методу send, но выполняет отправку запроса к методу getState.
- list-certs – команда для отображения информации о сертификатах, установленных в локальном хранилище пользователя.

Более подробную информацию о командах можно получить, вызвав их с ключом --help.

Конфигурационные параметры

Настройки демо-приложения хранятся в файле *«xades-demo.exe.config»*.

Для выполнения команды подписи и отправки запроса необходимо, что бы в конфигурационном файле были настроены следующие параметры:

- отпечаток сертификата. Список сертификатов, установленных в локальное хранилище и их отпечатки можно посмотреть с помощью команды *list-certs*.
- пароль от контейнера. Если пароль от сертификата недопустимо хранить в конфигурационном файле приложения, его можно задать с помощью ключа *-p (--password)* при запуске.

Для команд отправки запроса и получения статуса обработки запроса также необходимо заполнить информацию о методе и сервисе ГИС ЖКХ.

Более подробно параметры конфигурационного файла описаны ниже.

Секция	Параметр	Назначение
SigningConfig	CertificateThumbprint	Отпечаток сертификата, используемого для подписи
	CertificatePassword	Пароль от контейнера, в который установлен сертификат
GisServicesConfig	OrgPpaGuid	Идентификатор поставщика данных
	BaseUrl	Url адрес шифрованного тунеля до API ГИС ЖКХ
GisServicesConfig. Services		Описание сервисов ГИС ЖКХ
GisServicesConfig. Services.Service	ServiceName	Имя сервиса
	Path	Относительный путь сервиса
	AddSignature	Использовать ли ЭЦП при отправке запросов
	AddOrgPpaGuid	Добавлять ли идентификатор поставщика в soap заголовок
GisServicesConfig. Services.Service.Methods		Описание методов сервиса ГИС ЖКХ

GisServicesConfig. Services.Service.Methods.Method	MethodName	Имя метода
	Action	Soap действие
	Template	Шаблон запроса к методу
	RequiredBody	Требуются ли csv файл с данными для формирования запроса. По умолчанию имеет значение true. Игнорируется для метода getState.

Описание команды send

Файл с входными данными представляет собой csv файл, в первой строке которого расположены пути до узлов документа (xpath выражения), а во второй строке – соответствующие значения. Для генерации случайного guid в качестве значения поля можно использовать специальное значение «{Util:RandomGuid}» (без кавычек).

При отправке запроса считывается шаблон запроса, указанный в конфигурационном файле, к шаблону применяются данные из файла, происходит замена версии форматов ГИС ЖКХ. Полученные данные помещаются в тело soap пакета.

Soap пакет также формируется на основе шаблонов. Формат заголовка, используемого в soap пакете, зависит от необходимости передачи подписи.

Полученный soap пакет подписывается и отправляется в ГИС ЖКХ.

Результатом вызова метода сервиса является soap пакет. В случае, если ответный пакет содержит ЭЦП – выполняется проверка подписи. Если ЭЦП отсутствует или присутствует и успешно проверена, содержимое тела пакета раскладывается на составляющие и сохраняется в файл. Формат выходного файла совпадает с форматов выходного файла операции getState (см. далее).

Описание команды get-state

Кроме имени сервиса, команде get-state необходимо передать уникальный идентификатор запроса в ГИС ЖКХ.

Команда сформирует и отправит soap пакет по аналогии с командой send (кроме подписи запроса).

Выходной файл представляет собой csv таблицу, в которой в первой строке находятся пути до элементов (xpath выражения), а во второй значения этих элементов. При этом в выходной файл попадают только конечные листья дерева xml. Для разложения выбирается первый узел в дереве, содержащий более одного дочернего узла. ЭЦП не включается в выходной файл.

Basic авторизация

Для успешной отправки запросов (команды get-state и send) в ГИС ЖКХ необходимо дополнительно использовать basic-авторизацию. Логин и пароль задаются с помощью ключа **-a** в формате логин:пароль, например **-a test:test123.**

Примеры использования утилиты

Ниже описаны примеры команд для утилиты

Пример	Команда	Примечание
Получение перечня НСИ	`xades-demo.exe send -s NsiCommonAsync -m exportNsiList -o "exportNsiList response.csv" -a test:test123`	Результат будет сохранен в файл *«exportNsiList response.csv»*. Гуид запроса находится в первой колонке

		второй строки.
Получение ответа на запрос перечня НСИ	`xades-demo.exe get-state -s NsiCommonAsync -g 1377f6ce-e78e-11e6-88b0-005056b6513d -o "exportNsiList get-state response.csv" -a test:test123`	Необходимо заменить гуид запроса.
Импорт плана проверок	`xades-demo.exe send -s Inspection -m importInspectionPlan -c "importInspectionPlan request.csv" -o "importInspectionPlan response.csv" -a test:test123`	Пример файла *«importInspectionPlan request.csv»* есть в каталоге examples.
Получение ответа на запрос импорта плана проверок	`xades-demo.exe get-state -s Inspection -g f29ababe-e7a7-11e6-88b0-005056b6513d -o "importInspectionPlan get-state response.csv" -a test:test123`	Необходимо заменить гуид запроса.

Дополнительные примеры расположены в каталоге «*examples*» см. файл «*команды.txt*».

Внутренне устройство библиотеки Xades

Библиотека представляет собой обертку над доработанной библиотекой из проекта Microsoft France.

Функционал по подписанию документов и проверке подписи скрыт за фасадным классом GostXadesBesService. Реализация проверок и алгоритма подписи частично содержится в классе XadesBesSignedXml. В таблице ниже представлено описание основных классов сборки.

Класс	Назначение
GostXadesBesService	Фасад для работы с ЭЦП
XadesBesSignedXml	Обертка над XadeSignedXml из проекта Library, реализующая алгоритмы подписания и проверки подписи
CertificateMatcher	Поиск сертификата, использованного для подписания документа
GostCryptoProvider	Получению алгоритмов хеширования и форматеров подписи специфичных для ГОСТ.
IssuerComparer	Проверка соответствия строки Issuer сертификатов

При проверке корректности ЭЦП выполняются следующие проверки:

- корректность ЭЦП XMLDSIG;
- отсутствие свойств, не используемых в XAdES-BES.
- корректность информации о сертификате;
- доверительность корневого сертификата (сертификат должен быть установлен в качестве «Доверенного корневого центра сертификации»);
- действительность сертификата на дату проверки.