

ЧФ «Энигма-Софт»

61072, Украина, г. Харьков, ул. 23 Августа 38, к. 23.
<http://enigmasoft.com.ua>, office@enigmasoft.com.ua
+380-577-177-977, (+380-577- 590-723,+380-577-590-724)

Комплекс «Стиль»

«Стиль» - Клиент банк

**Сканер пакетов
финансовых документов**

Техническое описание

Харьков

Оглавление

1. Основные возможности Сканера.....	3
2. Эксплуатационные возможности Сканера.....	3
3. Вход в программу Сканера.....	3
4. Обработка файлов Сканером.....	3
5. Особенности обработки зашифрованных файлов	4
6. Протоколы работы Сканера.....	4

1. Основные возможности Сканера

В практической работе по дистанционному обслуживанию клиентов банка с помощью комплекса «Стиль» Клиент-банк периодически возникает необходимость детального анализа информации о файле финансовых документов от клиента, самих финансовых документов файла и их подписантах. Программный модуль «Сканер пакетов финансовых документов» (далее по тексту **Сканер**) предназначен для расшифрования, контроля, просмотра ^F- файлов формата DOCPOST, сформированных клиентом комплекса «Стиль» Клиент-Банк. Результатом работы Сканера являются протоколы с детальным документированием выполненных действий. Сканер работает с файлами формата DOCPOST и системами защиты:

- Шифр-РКІ (ЗАО «Сайфер», Киев)
- ЭЦП х.509 (ИИТ, Харьков)

2. Эксплуатационные возможности Сканера

Сканер используется на стороне Банка как самостоятельная программная система. С ПК, на котором эксплуатируется Сканер, должен быть установлен информационный доступ к файловым хранилищам сертификатов нужных систем защиты. Сканер обрабатывает следующие виды файлов:

- ^FAAAAAA.DCC – Подписан Шифр-РКІ
- ^FAAAAAA.DCC – Подписан и зашифрован Шифр-РКІ
- ^FAAAAAA.DCC – Подписан библиотекой ЭЦП х.509
- ^FAAAAAA.DCC – Подписан и зашифрован библиотекой ЭЦП х.509

3. Вход в программу Сканера

Сканер работает в диалоговом режиме. При запуске Сканера на экран выводится окно загрузки личного ключа Технолога банка. Загрузка личного ключа Технолога требуется для:

- Обеспечения доступа к Сканеру только уполномоченных лиц.
- Документирования в протоколе работы Сканера данных о пользователе.
- Расшифрования файлов клиента, зашифрованных в адрес данного пользователя.

В окне загрузки ключа задается следующая информация:

- Тип системы защиты (Шифр-РКІ /ЭЦП х.509);
- Путь к сертификатам — путь к каталогу с сертификатами (файловому хранилищу);
- Пароль личного ключа Технолога банка.
- Устройство считывания личного ключа Технолога банка.

4. Обработка файлов Сканером

После успешной загрузки личного ключа Технолога банка на экран выводится окно сеансового протокола. В начальный момент в протоколе присутствует только информация из сертификата ключа Технолога. Дальнейшая работа со сканером ведется в данном окне и заключается в

обработке групп файлов или одиночных файлов. Информация о каждом обработанном файле отражается в окне сеансового протокола. Для поиска каких-либо элементов текста в сеансовом протоколе, в окне предусмотрена подстрока поиска.

5. Особенности обработки зашифрованных файлов

Если для обработки, не зашифрованных файлов финансовых документов, допустимо использование любого ключа Технолога банка. То успешное расшифрование зашифрованных файлов возможно лишь при условии загрузки ключа Технолога(ов), в адрес которых обрабатываемый файл был зашифрован. Для любой системы защиты комплекса «Стиль» Клиент-Банк это все действующие ключи технологов банка, действующие на момент зашифрования файла финансовых документов.

Так как ключи Технологов банка имеют срок действия, то расшифрование файла возможно только при наличии **действующего** ключа технолога банка. Если срок действия нужного Нам ключа истек, то файл можно расшифровать сканером только :

- Создав вспомогательное файловое хранилище сертификатов (не штатное)
- Установив дату на ПК пользователя в пределах периода действия ключа.

Если все ключи технологов за какой-либо период утрачены, расшифрование файлов за соответствующий период становится невозможным.

Приемлемым решениями могут быть:

1. Долговременное хранение расшифрованных файлов
2. Наличие ключей Технолога банка с неограниченным сроком действия (ключ архивариуса). Но в случае физической утери такого ключа — файлы расшифровать будет невозможно.

Все обработанные сканером файлы сохраняются в **расшифрованном** виде в подкаталоге \Tmp рабочей директории сканера и могут быть использованы для повторной обработки сканером, но уже без расшифрования. Имена **расшифрованных файлов** имеют вид

^FXXXXXX.DCC_YYYYMMDD.SSSS, где

^FXXXXXX.DCC – Имя обрабатываемого файла,

YYYYMMDD – Дата создания обрабатываемого файла.

SSSS - Имя системы защиты (PKI, x509)

Примечание: Дата и время создания файлов финансовых документов, полученных от клиентов по системе файлового обмена ESFS соответствуют дате и времени приема файла банком.

При повторной обработке файлов **расшифрованных** сканером, они сохраняются в подкаталоге \Tmp без изменения.

6. Протоколы работы Сканера

В процессе работы, помимо сеансового протокола, доступного для просмотра только в окне программы, **Сканер пакетов финансовых документов** формирует еще 2 вида текстовых протоколов (кодировка Windows 1251):

- Протокол обработки файла;

- Суточный протокол работы.

Эти протоколы записываются в виде отдельных файлов и доступны для просмотра и обработки сторонними программами. Файлы обоих видов формируются в подкаталоге \Log рабочей директории сканера.

Имя протокола обработки файла имеет вид ^FXXXXXX.DCC_YYYYMMDD.Log, где ^FXXXXXX.DCC – Имя обрабатываемого файла, YYYYMMDD – Дата создания обрабатываемого файла.

Примечание: Дата и время создания файлов финансовых документов, полученных от клиентов по системе файлового обмена ESFS соответствуют дате и времени приема файла банком. При многократной обработке одного и того же файла протокол обработки файла перезаписывается.

1. Пример протокола обработки файла (ШИФР-РКИ):

Обработка выполнена : 09/12/2013 10:41:28
 Идентификатор владельца ключа: XXXXXXXXXXXXXXXXXXXX
 Идентификатор ключа: YYYYYYYYYYYYYYYYYY
 Полное имя владельца ключа: Иванов Иван Иванович
 Наименование организации: ПАО «КредиАдриколь»
 Должность: Технолог системы «Клиент-Банк»
 Электронный адрес владельца: 000000@indexbank.ua
 Внешний идентификатор ключа: 000000
 Время генерации ключа: 25/06/2013 07:41:18
 Время регистрации ключа на ЦСК: 26/06/2013 08:48:18
 Время начала действия ключа: 25/06/2013 21:00:00
 Время окончания действия ключа: 23/06/2014 21:00:00

Обработка файла D:\Temp\Spr\F\^FUKR108.501
 MD5 = 48 00 F2 6D 30 4A 32 B4 FD 0D 13 D9 7B DB 79 F5
 Номер DOCPOST – UKR108, номер сеанса 01

Расшифрование файла D:\Temp\Spr\F\^FUKR108.501
 Фай не зашифрован системой защиты Шифр-РКИ

Проверка подписи файла .\Tmp\^FUKR108.501
 Идентификатор владельца ключа: 34EEFE60677D57E7
 Идентификатор ключа: 936558CB2757687C
 Полное имя владельца ключа: Большуткин Александр Дмитриевич
 Наименование организации: ПФ "Энигма-Софт"
 Должность: Директор
 Электронный адрес владельца: UKR108@indexbank.ua
 Время выработки подписи: 06/12/2013 16:29:55

Документы файла

Порядковый номер документа в файле – 1

Платежное поручение

DOCPOST: UKR108
 Дата: 77775
 Номер: 160
 Дебет: 26003000009103 300614 23320003 Приватна фірма "Енігма-Софт"
 Кредит: 37195201002030 851011 38773125 ДП І у Дзержинському районі м.Харкова

Сумма: 980 1125.48
Назначение: *;23320003;101 ;единий соц.податок 36,77% за 1 пол.листопада 2013р., до
бюджету перераховується повністю по сроку 22.11.13р., перерах на
карт.рах.22.11.13р.; ; ;

Первая подпись

Идентификатор владельца ключа: 34EEFE60677D57E7
Идентификатор ключа: 936558CB2757687C
Полное имя владельца ключа: Большуткин Александр Дмитриевич
Наименование организации: ПФ "Энигма-Софт"
Должность: Директор
Электронный адрес владельца: UKR108@indexbank.ua
Время выработки подписи: 06/12/2013 16:28:59

Вторая подпись

Идентификатор владельца ключа: 88A9A6722D5EFA89
Идентификатор ключа: 15BB9782789761EC
Полное имя владельца ключа: Большуткина Наталья Владимировна
Наименование организации: ПФ "Энигма-Софт"
Должность: Головной бухгалтер
Электронный адрес владельца: UKR108@indexbank.ua
Время выработки подписи: 06/12/2013 16:29:11

Порядковый номер документа в файле - 2

Платежное поручение

DOCPOST: UKR108
Дата: 77775
Номер: 161
Дебет: 26003000009103 300614 23320003 Приватна фірма "Енігма-Софт"
Кредит: 29249000000178 300614 14361575 ПАТ"Кредіатріколь-Банк"
Сумма: 980 2508.08
Назначение: Зарплата за 1 половину листопада 2013р.

Первая подпись

Идентификатор владельца ключа: 34EEFE60677D57E7
Идентификатор ключа: 936558CB2757687C
Полное имя владельца ключа: Большуткин Александр Дмитриевич
Наименование организации: ПФ "Энигма-Софт"
Должность: Директор
Электронный адрес владельца: UKR108@indexbank.ua
Время выработки подписи: 06/12/2013 16:28:59

Вторая подпись

Идентификатор владельца ключа: 88A9A6722D5EFA89
Идентификатор ключа: 15BB9782789761EC
Полное имя владельца ключа: Большуткина Наталья Владимировна
Наименование организации: ПФ "Энигма-Софт"
Должность: Головной бухгалтер
Электронный адрес владельца: UKR108@indexbank.ua
Время выработки подписи: 06/12/2013 16:29:11

Порядковый номер документа в файле - 3

Платежное поручение

DOCPOST: UKR108
Дата: 77775
Номер: 162
Дебет: 26003000009103 300614 23320003 Приватна фірма "Енігма-Софт"
Кредит: 61107000006993 300614 14361575 ПАТ"Кредіатріколь-Банк"
Сумма: 980 25.08
Назначение: Перераховується 1% за комісію за послуги банку.

Первая подпись

Идентификатор владельца ключа: 34EEFE60677D57E7
 Идентификатор ключа: 936558CB2757687C
 Полное имя владельца ключа: Большуткин Александр Дмитриевич
 Наименование организации: ПФ "Энигма-Софт"
 Должность: Директор
 Электронный адрес владельца: UKR108@indexbank.ua
 Время выработки подписи: 06/12/2013 16:29:00

Вторая подпись

Идентификатор владельца ключа: 88A9A6722D5EFA89
 Идентификатор ключа: 15BV9782789761EC
 Полное имя владельца ключа: Большуткина Наталя Володимирівна
 Наименование организации: ПФ "Энигма-Софт"
 Должность: Головний бухгалтер
 Электронный адрес владельца: UKR108@indexbank.ua
 Время выработки подписи: 06/12/2013 16:29:12

2. Пример протокола обработки файла (ЭЦП x.509):

Обработка выполнена: 16/12/2013 17:21:44
 ЦСК, выдавшее сертификат: Enigma_csk
 Регистрационный номер сертификата: 4A208CDB612EC8F5040000000100000013000000
 Наименование организации: ЧФ "Энигма-Софт"
 Идентификационный код: 23320003
 Административная единица: Харківська область
 Населенный пункт: Харків
 Адрес:
 Владелец сертификата: Иванов Иван Иванович
 Подразделение: Дирекция
 Должность: Генеральный директор
 Телефон:
 Адрес электронной почты:
 Длина открытого ключа (бит): 264
 Открытый ключ:
 82976F0526CC64675AB0BF408632419373C323FF003754158972CC2D3FF6ACC300
 Идентификатор открытого ключа: 4C B0 37 36 37 03 EC 30 B1 52 4F 97 F8 6E 13
 EB B4 43 8F E1 3A 8A 34 98 11 AE 47 77 B2 EA A9 1B
 Время ввода сертификата в действие: 21/05/2013 00:00
 Время окончания действия сертификата: 21/05/2014 00:00
 Время начала действия ключа: 21/05/2013 00:00
 Время окончания действия ключа: 21/05/2014 00:00

Обработка файла D:\ENIGMA.WIN\WORK\Out\^FUKR108.101
 MD5 = AC 86 9D 9F 8E 37 66 A1 CF 15 7E DE FD A0 90 CA
 Номер DOCPOST - UKR108, номер сеанса 01

Расшифрование файла D:\ENIGMA.WIN\WORK\Out\^FUKR108.101
 Файл расшифрован успешно
 MD5 = 9F 02 3B 13 BC E7 76 7D CC 6A 20 01 99 35 88 49

Проверка подписи файла .\Tmp\^FUKR108.101_20131209.x509
 ЦСК, выдавшее сертификат: Enigma_csk
 Регистрационный номер сертификата: 4A208CDB612EC8F5040000000100000013000000
 Наименование организации: ЧФ "Энигма-Софт"
 Идентификационный код: 23320003
 Административная единица: Харківська область
 Населенный пункт: Харків

Адрес:

Владелец сертификата: Иванов Иван Иванович
 Подразделение: Дирекция
 Должность: Генеральный директор
 Телефон:

Адрес электронной почты:

Длина открытого ключа (бит): 264

Открытый ключ:

82976F0526CC64675AB0BF408632419373C323FF003754158972CC2D3FF6ACC300

Идентификатор открытого ключа: 4C B0 37 36 37 03 EC 30 B1 52 4F 97 F8 6E 13

ЕВ В4 43 8F E1 3A 8A 34 98 11 AE 47 77 B2 EA A9 1B

Время ввода сертификата в действие: 21/05/2013 00:00

Время окончания действия сертификата: 21/05/2014 00:00

Время начала действия ключа: 21/05/2013 00:00

Время окончания действия ключа: 21/05/2014 00:00

Время выработки подписи : 09/12/2013 14:24

Документы файла

Порядковый номер документа в файле - 1

Платежное поручение

DOCPOST: UKR108

Дата: 77778

Номер: 792

Дебет: 26002000033001 350619 23320003 ЧФ "Энигма-Софт"

Кредит: 61108000000294 351469 09351468 ХОД АК АПБ "УКРАИНА"

Сумма: 980 0.50

Назначение: Оплата за розрахункове обслуговування юр. ос_б

Первая подпись

ЦСК, выдавшее сертификат: Enigma_csk
 Регистрационный номер сертификата: 4A208CDB612EC8F504000000100000013000000
 Наименование организации: ЧФ "Энигма-Софт"
 Идентификационный код: 23320003
 Административная единица: Харківська область
 Населенный пункт: Харків

Адрес:

Владелец сертификата: Иванов Иван Иванович
 Подразделение: Дирекция
 Должность: Генеральный директор
 Телефон:

Адрес электронной почты:

Длина открытого ключа (бит): 264

Открытый ключ:

82976F0526CC64675AB0BF408632419373C323FF003754158972CC2D3FF6ACC300

Идентификатор открытого ключа: 4C B0 37 36 37 03 EC 30 B1 52 4F 97 F8 6E 13

ЕВ В4 43 8F E1 3A 8A 34 98 11 AE 47 77 B2 EA A9 1B

Время ввода сертификата в действие: 21/05/2013 00:00

Время окончания действия сертификата: 21/05/2014 00:00

Время начала действия ключа: 21/05/2013 00:00

Время окончания действия ключа: 21/05/2014 00:00

Время выработки подписи : 09/12/2013 14:22

Вторая подпись

ЦСК, выдавшее сертификат: Enigma_csk
 Регистрационный номер сертификата: 4A208CDB612EC8F504000000100000012000000
 Наименование организации: ЧФ "Энигма-Софт"
 Идентификационный код: 23320003
 Административная единица: Харківська область
 Населенный пункт: Харків

Адрес:

Владелец сертификата: Сидоров Сидор Сидорович
 Подразделение: Бухгалтерия
 Должность: Главный бухгалтер
 Телефон:

Адрес электронной почты:

Длина открытого ключа (бит): 264

Открытый ключ:

E75F56DE6A9ABEEA11B260FDA8308951412C2BA248DD7CFB69492BBD27F68DFA00

Идентификатор открытого ключа: 0A E1 1E 22 95 B4 74 EF 10 88 23 C5 D3 08 27

F0 1F 13 11 71 E2 8D 73 19 5C 16 EB BF 6F CE E1 B9

Время ввода сертификата в действие: 21/05/2013 00:00

Время окончания действия сертификата: 21/05/2014 00:00

Время начала действия ключа: 21/05/2013 00:00

Время окончания действия ключа: 21/05/2014 00:00

Время выработки подписи : 09/12/2013 14:24

Порядковый номер документа в файле - 2

Платежное поручение

DOCPOST: UKR108

Дата: 77778

Номер: 793

Дебет: 26002000033001 350619 23320003 ЧФ "Энигма-Софт"

Кредит: 26000011964 351652 22678323 ЧФ "СТЕЙТ"

Сумма: 980 0.27

Назначение: Оплата за розрахункове обслуговування

Первая подпись

ЦСК, выдавшее сертификат: Enigma_csk
 Регистрационный номер сертификата: 4A208CDB612EC8F5040000000100000013000000
 Наименование организации: ЧФ "Энигма-Софт"
 Идентификационный код: 23320003
 Административная единица: Харківська область
 Населенный пункт: Харків

Адрес:

Владелец сертификата: Иванов Иван Иванович

Подразделение: Дирекция

Должность: Генеральный директор

Телефон:

Адрес электронной почты:

Длина открытого ключа (бит): 264

Открытый ключ:

82976F0526CC64675AB0BF408632419373C323FF003754158972CC2D3FF6ACC300

Идентификатор открытого ключа: 4C B0 37 36 37 03 EC 30 B1 52 4F 97 F8 6E 13

EB B4 43 8F E1 3A 8A 34 98 11 AE 47 77 B2 EA A9 1B

Время ввода сертификата в действие: 21/05/2013 00:00

Время окончания действия сертификата: 21/05/2014 00:00

Время начала действия ключа: 21/05/2013 00:00

Время окончания действия ключа: 21/05/2014 00:00

Время выработки подписи : 09/12/2013 14:23

Вторая подпись

ЦСК, выдавшее сертификат: Enigma_csk
 Регистрационный номер сертификата: 4A208CDB612EC8F5040000000100000012000000
 Наименование организации: ЧФ "Энигма-Софт"
 Идентификационный код: 23320003
 Административная единица: Харківська область
 Населенный пункт: Харків

Адрес:

Владелец сертификата: Сидоров Сидор Сидорович

Подразделение : Бухгалтерия
Должность : Главный бухгалтер
Телефон :
Адрес электронной почты :
Длина открытого ключа (бит) : 264
Открытый ключ :
E75F56DE6A9ABEEA11B260FDA8308951412C2BA248DD7CFB69492BED27F68DFA00
Идентификатор открытого ключа : 0A E1 1E 22 95 B4 74 EF 10 88 23 C5 D3 08 27
F0 1F 13 11 71 E2 8D 73 19 5C 16 EB BF 6F CE E1 B9
Время ввода сертификата в действие : 21/05/2013 00:00
Время окончания действия сертификата : 21/05/2014 00:00
Время начала действия ключа : 21/05/2013 00:00
Время окончания действия ключа : 21/05/2014 00:00
Время выработки подписи : 09/12/2013 14:24

Имена файлов суточных протоколов работы имеют вид **YYYYMMDD.Log**, где **YYYYMMDD** - системная дата ПК.

В протоколе регистрируются время входа пользователей в программу и данные сертификатов ключей, загруженных ими. Далее в протокол последовательно выводится информация по всем обработанным пользователями файлам. (Аналогично протоколам обработки файлов).

**Специалисты ЧФ «Энигма-Софт» желают Вам
ПРИЯТНОЙ РАБОТЫ**