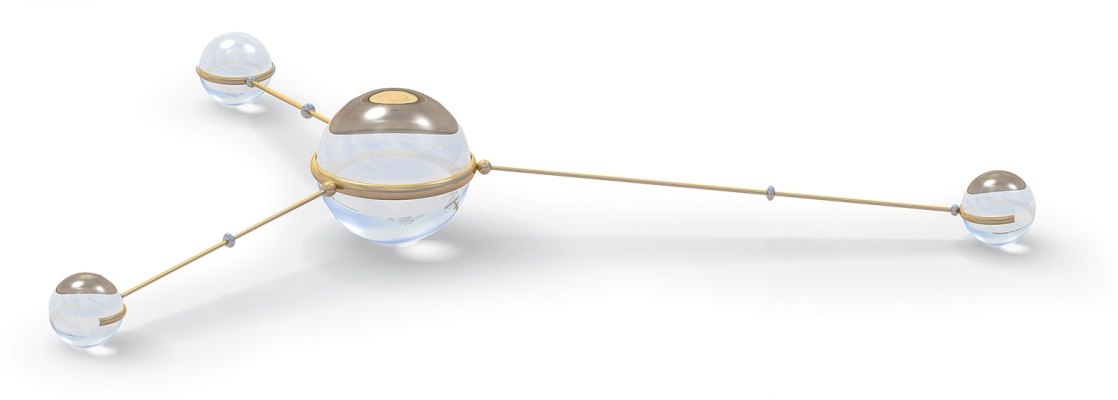
Банк`с софт системс

Система "ДБО BS-Client v.3"

Релиз 017.4.0, Централизованная схема

Документация клиента "Банк-Клиент". Комплект администратора

Криптозащита



Система "ДБО BS-Client v.3"
Релиз 017.4.0, Централизованная схема
Документация клиента "Банк-Клиент". Комплект администратора
Руководство по использованию
Криптозащита

Опубликовано 2007
Листов 131

© 2007 Банк'с софт системс

Содержание

Введение

Настоящий документ является частью документации по системе "ДБО BS-Client v.3" релиза 017.4.0, функционирующей в режиме Централизованной схемы .

На кого ориентирован документ

Документ предназначен для администратора клиентской части подсистемы "Банк-Клиент".

Назначение документа

Назначение документа состоит в предоставлении информации о криптографических механизмах, реализованных в системе "ДБО BS-Client v.3", и способах их настройки. Данный документ может быть полезен как на этапе начальной настройки системы, так и в процессе ее рабочей эксплуатации.

Организация документа

Документ разбит на несколько глав.

В главе 1, « Концепции криптозащиты » [стр. 8] освещаются основные понятия и концепции криптозащиты, приводится обзор систем криптографической защиты информации. Данная глава является вводной и рекомендована для прочтения для лучшего понимания изложенного далее материала.

В главе 2, «Криптозащита в системе "ДБО BS-Client v.3"» [стр. 24] приводится описание криптографических механизмов системы "ДБО BS-Client v.3", концепций криптозащиты в разрезе их применения в рамках системы. Описываются отвечающие за криптографическую защиту данных объекты системы, приводятся их характеристики и указываются операции, выполняемые над объектами и посредством объектов.

В главе 3, «Инструкции администратора» [стр. 59] собраны инструкции по настройке подсистемы криптозащиты системы "ДБО BS-Client v.3".

Дополнительная справочная информация приведена в приложениях:

- приложение А, «Механизм формирования и формат хранения подписи под документами» [стр. 89];
- приложение В, «Интерфейс задания параметров процедуры генерации ключей / запросов на сертификат» [стр. 97].

В конце документа приведены определения основных терминов и терминов, встречающихся в данном документе.

Рекомендации по использованию документа

Документ рекомендуется использовать и в качестве ознакомительного материала, и в качестве справочника при работе с системой "ДБО BS-Client v.3". Документ рекомендован как для последовательного, так и для выборочного изучения.

Внимание!

Для интенсивного изучения документации и быстрого поиска необходимой информации рекомендуется воспользоваться справочной системой системы "ДБО BS-Client v.3".

Документы, рекомендуемые для предварительного прочтения

Соглашения по оформлению

В данном документе для представления ссылок, терминов и наименований используются различные шрифты и средства оформления. Основные типы начертаний текста приведены далее.

Шрифт	Описание
Поле	Используется для выделения наименований полей, блоков, закладок экранных форм
Кнопка	Используется для выделения наименований кнопок
Меню	Используется для выделения наименований пунктов меню
Ctrl+X	Используется для выделения сочетаний клавиш
`cbank.exe`	Используется для выделения имен файлов и каталогов
Термин	Используется для выделения первого вхождения определяемого в документе термина в тексте документа
Термин	Используется для выделения прочих вхождений упоминаемых в документе терминов
Выделение	Используется для выделения отдельных значимых слов в тексте
Ссылка [стр. 6]	Используется для выделения перекрестных ссылок

Кавычками выделяются значения полей экранных форм.

Наименования пунктов меню отделяются друг от друга символом →.

Для выделения блоков текста используются специальные средства оформления, представленные ниже.

Примечание

Служит для выделения дополнительной или разъясняющей информации, в том числе ссылок на фрагменты документации, содержащие более подробные сведения. В основном следует непосредственно за элементом, к которому оно относится, но может предшествовать целой главе или разделу.

Внимание!

Служит для выделения важной информации, на которую следует обратить внимание.

Служит для выделения дополнительной информации, рекомендованной для углубленного изучения системы. В основном информация, помеченная подобным образом, представляет собой описание редкоиспользуемых возможностей системы. Данную информацию можно пропустить при ознакомительном чтении.

Глава 1. Концепции криптозащиты

Данный раздел является вводной частью, описывающей общие концепции и основные системы криптографической защиты информации. Рассматриваются такие понятия, как *абоненты*, *открытые*, *закрытые* и *сеансовые* ключи, *электронные сертификаты*, ключевые *пары*, *наборы* и *носители*, *ключевой кэш*, генерация, перегенерация и *компрометация* ключей, *инфраструктура открытых ключей*, *зашифрование*, *расшифрование*, *подпись* и *проверка подписи*, *системы криптографической защиты информации* и другие понятия. Знакомство с данными понятиями полезно, а местами и необходимо для понимания принципов криптозащиты с системе "ДБО BS-Client v.3". Приводится краткий обзор систем криптографической защиты информации. Если Вы знакомы с концепциями криптозащиты и системами криптографической защиты информации, Вы можете перейти непосредственно к гл. 2, «Криптозащита в системе "ДБО BS-Client v.3"» [стр. 24].

Примечание

В описании общих концепций криптографической защиты информации периодически встречаются комментарии относительно использования того или иного принципа или понятия в системе "ДБО BS-Client v.3".

Если при изучении изложенного материала у Вас возникнут трудности с пониманием некоторых принципов или понятий, Вы можете отложить данный материал и вернуться к нему в случае необходимости.

1.1. Абоненты

Крипрографические подсистемы систем "ДБО BS-Client v.3" банка и его клиентов образуют *криптографическую сеть*. В рамках этой сети осуществляется обмен зашифрованной информацией между субъектами, называемыми *абонентами криптографической сети* (далее – *абоненты*).

Следует отметить различие между понятием *клиент* и *абонент*. Во-первых, клиент банка – юридическое лицо – может иметь несколько абонентов. Например, абонентами могут быть главный бухгалтер и генеральный директор организации клиента. Во-вторых, на стороне банка также имеются абоненты – сотрудники банка.

Также имеется различие между понятиями *абонент* и *пользователь* в системе "ДБО BS-Client v.3". Обычно абоненту однозначно сопоставляется физический пользователь системы, однако в общем случае абонент может соответствовать группе пользователей или один пользователь может быть зарегистрирован как несколько абонентов. Также абонентами могут быть отдельные компоненты системы, выступающие посредниками в процессе передачи информации (например, компоненты BS-Defender).

В рамках системы "ДБО BS-Client v.3" посредством криптографической подсистемы возможен двусторонний обмен информацией между абонентами банка и абонентами клиентов. Обмен данными между двумя абонентами, относящимися к различным организациям-клиентам, посредством криптографической подсистемы не осуществляется.

В системе "ДБО BS-Client v.3" информация о каждом абоненте сохраняется в виде *криптографического профиля* (см. разд. 2.2, « Криптографические профили » [стр. 26]).

1.2. Симметричные и асимметричные криптографические алгоритмы

Для криптографической защиты информации используются как *симметричные криптографические алгоритмы*, так и и *асимметричные криптографические алгоритмы*. Симметричные алгоритмы используют для *зашифрования* и *расшифрования* один и тот же ключ. Асимметричные алгоритмы, называемые также *криптографическими алгоритмами с открытым ключом*, используют для зашифрования и расшифрования *ключевую пару*, состоящую из *открытого* и *секретного* ключей (см. разд. 1.3.1, «Ключевые пары» [стр. 9]).

Примечание

Подробнее об операциях зашифрования и расшифрования см. в разд. 1.4.1, «Зашифрование и расшифрование данных» [стр. 17].

Симметричные алгоритмы зачастую являются составной частью алгоритмов асимметричной криптографии. В чистом виде симметричные алгоритмы в системе "ДБО BS-Client v.3" практически не применяются. В силу сказанного, далее будут рассмотрены преимущественно алгоритмы асимметричной криптографии (см. разд. 1.4, «Базовые криптографические операции» [стр. 16]).

Криптографические алгоритмы реализуют в виде специального ПО – *систем криптографической защиты информации* (*СКЗИ*). Подробная информация о некоторых СКЗИ и об их использовании в системе "ДБО BS-Client v.3" изложена в разд. 1.5, «Системы криптографической защиты информации» [стр. 20].

1.3. Ключевая информация

1.3.1. Ключевые пары

Асимметричные криптографические алгоритмы используют так называемые *ключевые пары*, каждая из которых состоит из *секретного* и *открытого* ключей.

СКЗИ, основанные на асимметричных алгоритмах, используют секретный ключ для формирования электронной подписи и расшифрования данных. Секретный ключ является конфиденциальной информацией. Защита данного ключа от несанкционированного доступа лежит на владельце ключа. При выдаче набора ключей пользователю системы, последний должен быть поставлен в известность относительно правил хранения секретных ключей и недопустимости доступа третьих лиц к носителю секретного ключа. При использовании некоторых криптографических систем обеспечивается дополнительная функция защиты секретного ключа с помощью мастер-ключа или пароля. В первом случае все сказанное относительно правил хранения секретного ключа распространяется на мастер-ключ, сам секретный ключ в этом случае не требует специальной защиты и может быть расположен на накопителях общего пользования. В случае защиты секретного ключа паролем необходимо придерживаться тех же правил, что и при хранении ничем не защищенного ключа. Дело в том, что пароль не обеспечивает должный уровень криптостойкости защищенных им данных.

Второй частью ключевой пары является *открытый ключ*, используемый для зашифрования данных и проверки электронной подписи. Открытый ключ не является конфиденциальной информацией и может распространяться по открытым каналам связи, без дополнительной защиты.

1.3.2. Сертификаты

При использовании большинства современных СКЗИ открытый ключ распространяется в виде сертификата. Сертификат представляет собой открытый ключ, снабженный дополнительной информацией (о его владельце, сроке действия и т.д.) и заверенный *электронной цифровой подписью центра сертификации* (*ЦС*) – специального внешнего по отношению к системе "ДБО BS-Client v.3" органа, в функции которого входит выдача сертификатов (см. разд. «Инфраструктура открытых ключей (PKI)» [стр. 13]). Используя открытый ключ (сертификат) самого ЦС каждый пользователь может проверить достоверность сертификата, выпущенного ЦС.

Примечание

- В системе "ДБО BS-Client v.3" сертификатами считаются только сертификаты, соответствующие стандарту *X.509*. Подробнее о стандарте *X.509* изложено в разд. «Инфраструктура открытых ключей (PKI)» [стр. 13].
- Во избежание путаницы в дальнейшем для обозначения двух видов открытых ключей будут использованы термины *сертификат* и *неподписанный открытый ключ*. В качестве общего наименования будет использоваться термин *открытый ключ*.
- Конкретный вид открытого ключа определяется используемой системой криптографической защиты информации (см. разд. 1.5, «Системы криптографической защиты информации» [стр. 20]).

> Необходимо отметить, что в рамках системы "ДБО BS-Client v.3" использование сертификатов не является обязательным условием обеспечения соответствия открытого ключа владельцу. Поскольку в центре криптографической сети – системе банка – содержится информация о ключевых парах всех клиентов банка, то злоумышленник не может выдать себя за какого-либо абонента сети. Единственно возможный вариант нарушения безопасности – компрометация ключей клиента (см. разд. 1.3.6, «Компрометация ключевых наборов» [стр. 12]) – одинаково вероятен при использовании как сертификатов, так и неподписанных открытых ключей. Поэтому оба варианта распространения открытых ключей одинаково надежны в системе "ДБО BS-Client v.3". Однако если есть необходимость дополнительного использования открытых ключей для целей, не связанных с системой "ДБО BS-Client v.3", более надежным является использование сертификатов.

Сертификаты, в отличие от неподписанных открытых ключей, имеют ограниченный срок действия. После окончания срока действия сертификат считается недействительным. При необходимости ЦС осуществляет выпуск нового сертификата на основании данных старого сертификата .

Примечание

В системе "ДБО BS-Client v.3" для обычных открытых ключей посредством механизма *криптопрофилей* также могут устанавливаться ограниченные сроки действия (см. разд. «Срок действия ключевого набора» [стр. 32]).

Использование сертификатов имеет множество других особенностей, описанных в разд. 1.3.7, «Особенности использования сертификатов» [стр. 13].

1.3.3. UID ключевой пары

Секретный ключ и открытый ключ соответствуют друг другу. Соответствие определяется *UID* – уникальным идентификатором ключевой пары. UID однозначно определяет ключевую пару в рамках системы "ДБО BS-Client v.3": не может быть двух абонентов, которым соответствуют две различные ключевые пары с одинаковым UID. При использовании сертификатов уникальность UID обеспечивается ЦС, в остальных случаях уникальность должна обеспечиваться другими средствами. В любом случае при использовании полученных ключевых пар в системе "ДБО BS-Client v.3", системой обеспечивается контроль уникальности UID ключевых пар.

Примечание

В большинстве случаев UID записывается в самих ключах (в сертификатах при их использовании). Возможность извлечения UID из ключевой пары зависит от того, какая используется *СКЗИ* (см. разд. 1.5, «Системы криптографической защиты информации» [стр. 20]).

1.3.4. Ключевые наборы

При использовании асимметричной криптографии для того, чтобы абонент мог читать зашифрованные сообщения других абонентов, он должен иметь копии открытых ключей абонентов. Если открытый ключ абонента выполнен в виде сертификата, для того, чтобы гарантировать его правомерность, к нему должен прилагаться сертификат ЦС, выпустившего сертификат абонента. Эта и другая информация, необходимая для использования ключевой пары, составляет структуру, называемую *ключевым набором*.

При использовании сертификатов в ключевой набор входят:

- ключевая пара абонента;
- сертификат или цепочка сертификатов ЦС (см. разд. «Цепочки сертификатов ЦС» [стр. 15]);
- сертификаты абонентов, с которыми должен осуществляться обмен информацией.

Ключевой набор также может содержать дополнительную информацию, например, *списки отозванных сертификатов* (см. разд. «Списки отозванных сертификатов» [стр. 14]).

В случае, когда вместо сертификатов используются неподписанные открытые ключи, ключевой набор включает в себя только ключевую пару и дополнительную информацию при необходимости.

Примечание

В системе "ДБО BS-Client v.3" хранится вся необходимая информация для использования ключевых наборов. Состав данной информации подробно рассмотрен в разд. «Параметры использования ключевых наборов» [стр. 33].

Поскольку ключевой набор содержит ровно одну ключевую пару, UID ключевой пары / ключа является уникальным идентификатором и ключевого набора.

1.3.5. Ключевые носители

Ключевой набор размещается на материальном носителе, называемом *ключевым носителем*. Примеры ключевых носителей: дискеты, флэш-карты, смарт-карты, каталоги жестких дисков, реестр Windows и т.д. Носитель может состоять из комбинаций устройств, например, секретный ключ может храниться на флэш-карте, а все открытые ключи / сертификаты – на жестком диске.

> **Примечание**
>
> Структура данных на ключевом носителе определяется используемой *системой криптографической защиты информации* (см. разд. 1.5, «Системы криптографической защиты информации» [стр. 20]).

Поскольку ключевым носителем может являться медленное устройство, например, дискета, то в большинстве случаев с целью повышения быстродействия данные ключевого набора считываются в специальную область оперативной памяти – *ключевой кэш*, и последующие обращения к данным производятся уже в кэш. В процессе работы с ключевым набором происходит периодическое считывание данных с ключевого носителя и обновление кэша. Использование механизма *кэширования* позволяет сократить количество обращений к медленному ключевому носителю и увеличить быстродействие системы в десятки и тысячи раз, однако в некоторых случаях требует выполнения специальных действий по принудительному считыванию данных носителя в кэш (очистка кэша).

Примером ситуации, в которой может потребоваться очистка кэша, является посменное использование на одном рабочем месте нескольких ключевых носителей. Допустим, за рабочим местом работают в две смены два пользователя. Каждый пользователь имеет свой ключевой носитель, например, дискету, при этом в корне каждой дискеты располагается каталог открытых ключей абонентов `A:\Abonents`. При работе первого пользователя содержимое каталога подгружается в кэш. Когда смена первого пользователя заканчивается, второй пользователь вставляет в дисковод свою дискету, однако обращение к каталогу `Abonents` на дискете не происходит, поскольку его содержимое загружено в кэш. В этой ситуации могут возникнуть ошибки с операциями зашифрования и подписи (см. разд. 1.4, «Базовые криптографические операции» [стр. 16]). Во избежание ошибок необходимо произвести очистку кэша.

> **Примечание**
>
> В системе "ДБО BS-Client v.3" сведения о ключевых наборах и ключевых носителях, а также параметры работы ключевого кэша содержатся в *криптопрофилях* (см. разд. «Параметры использования ключевых наборов» [стр. 33]).

1.3.6. Компрометация ключевых наборов

При использовании ключей возможна ситуация *компрометации*, когда утеряно доверие к тому, что что секретный ключ обеспечивает безопасность информации, защищаемой с его использованием. Примером компрометации может служить утеря секретного ключа, утрата

владельцем ключа контроля за ограничением доступа к ключевому носителю, увольнение сотрудника, имеющего доступ к ключевому носителю и т.д.

При наличии ЦС функцию контроля скомпрометированных ключей берет на себя ЦС (см. разд. «Инфраструктура открытых ключей (PKI)» [стр. 13]). Абоненты уведомляют ЦС о ситуациях компрометации, в результате чего сертификаты абонентов отзываются и помещаются в *списки отозванных сертификатов* . Использование сертификатов из списка и соответствующих им секретных ключей при выполнении ряда криптографических операций становится невозможным. Подробное описание механизма отзыва сертификатов приведено в разд. «Списки отозванных сертификатов» [стр. 14].

Примечание

Система "ДБО BS-Client v.3" позволяет в ситуации компрометации независимо от наличия ЦС и механизма отозванных сертификатов напрямую запретить использование как сертификатов, так и неподписанных открытых ключей. Запрет использования ключей может быть произведен как на уровне *криптопрофиля* (когда скомпрометированы все ключи абонента, см. разд. 2.2, « Криптографические профили » [стр. 26]), так и на уровне *ключевых наборов* (когда скомпрометирован один ключевой набор, см. разд. 1.3.4, «Ключевые наборы» [стр. 11]).

1.3.7. Особенности использования сертификатов

Инфраструктура открытых ключей (PKI)

Криптография с открытыми ключами, распространяемыми в виде сертификатов, требует наличия определенной инфраструктуры, прикладного обеспечения и систем. Прикладное обеспечение и системы будет рассмотрено ниже (см. разд. 1.5, «Системы криптографической защиты информации» [стр. 20]), сейчас же будут рассмотрены основные концепции инфраструктуры открытых ключей.

Комитетом ISOC (Internet Society) разработана *инфраструктура открытых ключей* (*ИОК*, *Public key infrastructure - PKI*) – сервис для управления электронными сертификатами и ключами пользователей. Задачей PKI является определение политики выпуска цифровых сертификатов, выдача их и аннулирование, хранение информации, необходимой для последующей проверки правильности сертификатов. В число приложений, поддерживающих PKI, входят: защищенная электронная почта, протоколы платежей, электронные чеки, электронный обмен информацией, защита данных в сетях с протоколом IP, электронные формы и документы с электронной цифровой подписью (ЭЦП).

PKI включает в себя:

- *центр сертификации* (*ЦС*) или иерархию подчиненных друг другу ЦС, возглавляемых *корневым центром сертификации*;
- *центры регистрации* (*ЦР*);
- *сетевой справочник*;
- конечных пользователей инфраструктуры.

Центр сертификации (ЦС, или *Удостоверяющий центр -УЦ*) - основная управляющая компонента PKI, предназначенная для формирования электронных сертификатов подчиненных

Центров и конечных пользователей. Кроме сертификатов, ЦС формирует *списки отозванных сертификатов*. (см. разд. «Списки отозванных сертификатов» [стр. 14]).

К основным функциям ЦС относятся:

- формирование собственного секретного ключа и сертификата ЦС;
- формирование сертификатов подчиненных ЦС;
- формирование сертификатов открытых ключей конечных пользователей;
- формирование списка отозванных сертификатов;
- ведение базы всех изготовленных сертификатов и списков отозванных сертификатов.

Обычно центр сертификации представляет собой организацию, выдающую сертификаты и обладающую соответствующей лицензией. Однако в некоторых инфраструктурах центр сертификации может представлять собой всего лишь программное обеспечение, как, например, служба "Центр сертификации" ("Sertification authority") в ОС Windows 2003 Server.

Центр регистрации (ЦР) - опциональная компонента PKI, предназначенная для регистрации конечных пользователей. Основная задача ЦР - регистрация пользователей и обеспечение их взаимодействия с ЦС. Одному ЦС может соответствовать несколько ЦР. В задачи ЦР может также входить публикация сертификатов и списка отозванных сертификатов в сетевом справочнике.

Сетевой справочник – опциональная компонента PKI, содержащая сертификаты и списки отозванных сертификатов и служащая для целей распространения этих объектов среди пользователей с использованием протокола LDAP (HTTP, FTP).

Инфраструктура PKI базируется на ряде стандартов, наиболее важным из которых с точки зрения системы "ДБО BS-Client v.3" является стандарт *X.509*. Данный стандарт является фундаментальным стандартом PKI, определяющим формат сертификатов. Сертификаты, не соответствующие стандарту X.509, в системе "ДБО BS-Client v.3" сертификатами не считаются.

> **Внимание**!
>
> Необходимо отметить, что система "ДБО BS-Client v.3" не является PKI. В рамках системы нет ЦС, ЦР и других компонентов PKI. Инфраструктура открытых ключей является внешней по отношению к системе "ДБО BS-Client v.3" инфраструктурой.

Списки отозванных сертификатов

В ряде случаев ЦС может аннулировать сертификат до завершения срока его действия. Такая ситуация возникает в частности при *компрометации ключей* (см. разд. 1.3.6, «Компрометация ключевых наборов» [стр. 12]).

В ситуации компрометации:

1. Абонент уведомляет ЦС о том, что его ключевой набор скомпрометирован.

2. ЦС осуществляет отзыв сертификата абонента: помещает сертификат в *список отозванных сертификатов* (*Certificate revocation list, CRL*).

3. ЦС распространяет актуализированный список всем абонентам или всем узлам криптографической сети.

При выполнении криптографических операций, выполняемых посредством открытого ключа, таких как проверка подписи и зашифрование (см. разд. 1.4, «Базовые криптографические операции» [стр. 16]), производится ряд проверок действительности сертификата абонента, подписавшего / зашифровывающего документ. В том числе производится проверка наличия сертификата абонента в актуальном списке отозванных сертификатов соответствующего ЦС. В случае, если сертификат абонента числится в CRL, в выполнении криптографической операции будет отказано. Подробнее процесс проверки ключевых наборов описан в разд. «Верификация сертификатов» [стр. 16].

Примечание

Поскольку криптографические операции подписи и расшифрования (см. разд. 1.4, «Базовые криптографические операции» [стр. 16]) выполняются посредством секретного, а не открытого ключа, то в случае, если реализация СКЗИ этого не запрещает, возможно выполнение указанных операций, даже если сертификат абонента находится в списке отозванных сертификатов.

Списки отозванных сертификатов постоянно поддерживаются в актуальном состоянии и предоставляются абонентам. Актуальные копии списков могут храниться и на ключевых носителях абонентов (см. разд. 1.3.5, «Ключевые носители» [стр. 12]).

Цепочки сертификатов ЦС

Как было сказано в разд. 1.3, «Ключевая информация» [стр. 9], сертификат заверяется электронной цифровой подписью ЦС, выдавшего сертификат. Чтобы гарантировать правомерность цифровой подписи ЦС к сертификату прилагается сертификат самого ЦС, соответствующий секретному ключу, использованному для цифровой подписи (более подробно механизм цифровой подписи рассмотрен в разд. «Формирование и проверка электронной цифровой подписи в системе "ДБО BS-Client v.3"» [стр. 38]). В общем случае вместо сертификата ЦС может прилагаться цепочка сертификатов нескольких ЦС, каскадно заверяющих сертификат ключевой пары и сертификаты подчиненных ЦС вплоть до *корневого центра сертификации*. Корневой ЦС сам заверяет свой сертификат. Для примера рассмотрим следующую ситуацию:

- имеется корневой ЦС 1 с сертификатом С1 (заверенный самим ЦС 1);
- имеется подчиненный ЦС 2 с сертификатом С2, выданным ЦС 1;
- имеется подчиненный ЦС 3 с сертификатом С3, выданным ЦС 2;
- имеется сертификат абонента А1, выданный ЦС 3.

В рассмотренном примере цепочка сертификатов ЦС для А1 представляет собой цепочку С1-С2-С3. Наличие цепочки сертификатов вплоть до ЦС верхнего уровня, заверение которого считается гарантией подлинности всех выдаваемых сертификатов, благодаря механизму электронной цифровой подписи (см. разд. 1.4.2, «Электронная цифровая подпись данных и проверка подписи» [стр. 18]) гарантирует подлинность сертификата абонента.

Проверка цепочки сертификатов производится в процессе верификации сертификатов (см. **док. «Руководство по использованию. Криптозащита»**).

Цепочка сертификатов ЦС является частью ключевого набора, содержащего сертификат абонента (см. разд. 1.3.4, «Ключевые наборы» [стр. 11]).

Верификация сертификатов

Для определения, является ли сертификат действительным, проводится процедура его *верификации*. Система "ДБО BS-Client v.3" использует процедуру верификации, встроенную в ОС Windows. В ходе верификации осуществляется проверка выполнения различных условий, наиболее значимые из которых следующие:

- электронная цифровая подпись сертификата верна, содержимое сертификата соответствует его подписи (см. разд. 1.4.2, «Электронная цифровая подпись данных и проверка подписи» [стр. 18]);
- сертификат корневого ЦС из цепочки сертификатов ЦС (см. разд. «Цепочки сертификатов ЦС» [стр. 15]) соответствует сертификату, зарегистрированному в ОС Windows как допустимый корневой сертификат;
- сертификаты из цепочки сертификатов ЦС каскадно заверяют друг друга, сертификатом ЦС нижнего уровня заверен сертификат абонента;
- сертификат абонента не скомпрометирован и не содержится в CRL (см. разд. «Списки отозванных сертификатов» [стр. 14]);
- область применения сертификата допускает его использование в системе "ДБО BS-Client v.3".

Если хотя бы одно из указанных условий не будет выполнено, сертификат считается недействительным и не может быть использован при выполнении криптографических операций (см. разд. 1.4, «Базовые криптографические операции» [стр. 16]).

1.4. Базовые криптографические операции

После того, как рассмотрены базовые сущности, на которых основаны механизмы криптографической защиты информации, можно перейти непосредственно к принципам использования данных сущностей. Конечной целью использования ключей является выполнение криптографических операций для защиты данных. В основе всех криптографических операций лежит понятие криптографического преобразования.

Криптографическим преобразованием (*шифрованием*) называется взаимно-однозначное математическое преобразование, зависящее от ключа / ключевой пары (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации (представленной в некоторой цифровой кодировке) блок шифрованной информации, также представленной в цифровой кодировке. Термин объединяет в себе два процесса (базовых цикла): цикл *зашифрования* и цикл *расшифрования* информации.

На этих двух циклах основаны все *криптографические операции*, наиболее значимыми из которых являются:

- Зашифрование и расшифрование данных [стр. 17].
- Электронная цифровая подпись данных и проверка подписи [стр. 18].

В следующих подразделах будут рассмотрены криптографические операции на низком уровне – на уровне их реализации в *системах криптографической защиты информации* (*СКЗИ*) (см. разд. 1.5, «Системы криптографической защиты информации» [стр. 20]). Особенности выполнения криптографических операций на прикладном уровне в системе "ДБО BS-Client v.3" рассмотрены далее в разд. 2.3, «Криптографические операции в системе "ДБО BS-Client v.3"» [стр. 36].

1.4.1. Зашифрование и расшифрование данных

Зашифрование и расшифрование данных применяется с целью исключения несанкционированного доступа к данным при их хранении и передаче по каналам связи.

При использовании асимметричных алгоритмов *зашифрование* представляется собой преобразование защищаемой информации (открытого текста) в зашифрованное сообщение (шифрованный текст) с помощью открытых ключей получателей зашифрованного сообщения. *Расшифрование* представляется собой обратное действие – преобразование зашифрованного сообщения в открытый текст с помощью секретного ключа получателя шифрованных сообщений. Открытый ключ является свободно распространяемой частью ключевой пары абонента, и любой обладатель копии открытого ключа может зашифровать сообщение для абонента. В то же время расшифровать сообщение может только обладатель секретного ключа – абонент, для которого предназначено сообщение.

Примечание

- При использовании криптографических операций по работе с *электронной цифровой подписью* ситуация обратная: подпись выполняется секретным ключом абонента, подписывающего документ, проверка подписи – открытым ключом абонента (см. разд. 1.4.2, «Электронная цифровая подпись данных и проверка подписи» [стр. 18]).
- Конкретная реализация алгоритма определяется используемой системой криптографической защиты информации (см. разд. 1.5, «Системы криптографической защиты информации» [стр. 20]). При выполнении алгоритмов зашифрования некоторых СКЗИ дополнительно может требоваться секретный ключ отправителя зашифрованного сообщения.

Выполнение асимметричных алгоритмов зашифрования и расшифрования требует больших затрат процессорного времени, возрастающих с размером шифруемого сообщения. Поэтому обычно (зависит от СКЗИ) для увеличения быстродействия при зашифровании данных само сообщение зашифровывают с помощью симметричных алгоритмов *сеансовым* ключом, а уже сеансовый ключ зашифровывают открытым ключом с помощью асимметричных алгоритмов. Сеансовый ключ генерируется случайным образом при каждой операции зашифрования. Тело зашифрованного сообщения составляют зашифрованное сеансовым ключом исходное сообщение и зашифрованный открытым ключом сеансовый ключ. Поскольку длина сеансового ключа меньше длины исходного сообщения, то зашифрование сеансового ключа происходит быстрее зашифрования всего сообщения.

Многие СКЗИ предоставляют возможность *зашифрования на абонентов*: зашифрования сообщения таким образом, чтобы расшифровать зашифрованное сообщение мог не один абонент, а несколько заданных абонентов. Конкретный алгоритм зашифрования на абонентов

зависит от используемой СКЗИ. В большинстве случаев происходит многократное зашифрование сеансового ключа открытыми ключами всех абонентов-получателей. Зашифрованные копии сеансового ключа составляют заголовок конечного зашифрованного сообщения.

Примечание

- Использование сеансового ключа помимо уменьшения вычислительной сложности операции зашифрования позволяет также уменьшить объем конечного сообщения при зашифровании на абонентов, так как зашифрованные копии сеансового ключа имеют меньший размер, чем зашифрованные копии исходного сообщения.
- Зашифрование на абонентов активно используется в системе "ДБО BS-Client v.3" (например, см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]). В случае, если СКЗИ не поддерживает зашифрование на абонентов, данная функциональность реализуется на уровне системы "ДБО BS-Client v.3".

Ключи, используемые операциями зашифрования и расшифрования, называются *ключами шифрования*.

В системе "ДБО BS-Client v.3" зашифрование и расшифрование данных используется преимущественно для защиты информации, передаваемой по каналам связи (см. разд. «Шифрование данных в системе "ДБО BS-Client v.3"» [стр. 37]).

1.4.2. Электронная цифровая подпись данных и проверка подписи

В электронном документообороте аналогом собственноручной подписи является *электронная цифровая подпись* (*ЭЦП*) – реквизит электронного документа, предназначенный для защиты данного электронного документа от фальсификации и позволяющий идентифицировать владельца открытого ключа подписи, а также установить отсутствие искажения информации в документе.

С технической точки зрения электронная цифровая подпись представляет собой дайджест подписываемого сообщения, зашифрованный секретным ключом отправителя. *Дайджест* – последовательность символов заданной длины, получаемая из исходного подписываемого сообщения с помощью специальной *хэш-функции*. Дайджест применяется для увеличения быстродействия алгоритмов ЭЦП: зашифрование дайджеста небольшой длины (в зависимости от алгоритма – 128 бит, 160 бит, 256 бит) производится намного быстрее зашифрования всего сообщения.

Таким образом, исходными данными для процедуры *подписи документа* являются:

- подписываемый документ;
- секретный ключ абонента, подписывающего документ.

Алгоритм процедуры подписи можно описать следующим образом:

1. По исходному документу с помощью хэш-функции вычисляется дайджест документа.
2. Дайджест документа зашифровывается с помощью секретного ключа абонента, подписывающего документ.

3. Формируется подписанный документ из двух частей: исходного документа и приложенной к нему ЭЦП (зашифрованным дайджестом).

Обратной по отношению к процедуре подписи документа является процедура *проверки подписи документа*. Исходными данными для процедуры проверки подписи являются:

- подписанный документ;
- открытый ключ абонента, подписавшего документ.

Алгоритм процедуры проверки подписи можно описать следующим образом:

1. ЭЦП подписанного документа расшифровывается с помощью открытого ключа абонента, подписавшего документ.
2. По исходному сообщению в подписанном документе с помощью хэш-функции вычисляется дайджест документа.
3. Полученные величины сравниваются. Если величины равны, то подпись считается действительной, в противном случае подпись считается недействительной.

Примечание

Конкретная реализация алгоритмов определяется используемой системой криптографической защиты информации (см. разд. 1.5, «Системы криптографической защиты информации» [стр. 20]).

> Несмотря на то, что исходное сообщение в подписанном документе не шифруется, наличие ЭЦП гарантирует *аутентичность* подписанных данных: документ не был искажен и подпись соответствует абоненту. Соответствие подписи абоненту обеспечивается зашифрованием дайджеста секретным ключом абонента. Отсутствие искажений обеспечивается свойствами хэш-функции:
>
> - *Необратимость*. Свойство означает, что по возвращаемому хэш-функцией дайджесту невозможно восстановить исходное сообщение.
> - *Стойкость к коллизиям*. Свойство означает, что для заданного сообщения невозможно определить сообщения, обладающие теми же дайджестами, что и заданное сообщение.
> - *Свойство рассеивания* означает, что незначительные изменения исходного сообщения вызывают значительные изменения дайджеста.
>
> Указанные свойства хэш-функции гарантируют невозможность фальсификации документа: даже если злоумышленник изменит содержание исходного документа, он не сможет изменить ЭЦП таким образом, чтобы она соответствовала модифицированному документу. При изменении исходного документа ЭЦП, а соответственно и весь документ, будут просто считаться недействительными.

Ключи, используемые операциями подписи и проверки подписи называются *ключами подписи*.

ЭЦП применяется для заверения сертификатов абонентов и ЦС (см. разд. 1.3.1, «Ключевые пары» [стр. 9]) и заверения списков отозванных сертификатов (см. разд. «Списки отозванных сертификатов» [стр. 14]). В системе "ДБО BS-Client v.3" ЭЦП используется для заверения

документов и пакетов (см. разд. «Формирование и проверка электронной цифровой подписи в системе "ДБО BS-Client v.3"» [стр. 38]).

1.5. Системы криптографической защиты информации

Криптографические преобразования [стр. 16] и алгоритмы [стр. 9] объединяются в *системы криптографической защиты информации* (*СКЗИ*). Ниже приводится общая классификация СКЗИ [стр. 20] и обзор СКЗИ [стр. 21], поддерживаемых системой "ДБО BS-Client v.3".

1.5.1. Общая классификация СКЗИ

Классификацию СКЗИ можно проводить многими способами. Ниже приведены некоторые способы классификации СКЗИ:

- является СКЗИ сертификатной или несертификатной [стр. 20];
- выполнена ли СКЗИ в виде программной библиотеки [стр. 20];
- является ли СКЗИ криптопровайдером [стр. 21].

Сертификатные и несертификатные СКЗИ

На настоящее время наибольшее распространение получили *сертификатные* СКЗИ. В рамках системы "ДБО BS-Client v.3" сертификатными называются СКЗИ, выпускающие открытые ключи в виде сертификатов по стандарту *X.509* (см. разд. «Инфраструктура открытых ключей (PKI)» [стр. 13]). Примером сертификатной СКЗИ является система Crypto Pro.

Характерными особенностями сертификатных СКЗИ являются:

- Необходимость наличия ЦС для выпуска сертификатов (см. разд. «Инфраструктура открытых ключей (PKI)» [стр. 13]).
- Использование запросов на выдачу сертификатов, отсылаемых в ЦС для получения сертификатов по стандарту X.509.

Прочие СКЗИ считаются *несертификатными*. Часть несертификатных СКЗИ, например, Excellence, не снабжают открытые ключи дополнительной информацией и не заверяют их. Другая часть несертификатных СКЗИ выпускают открытые ключи в формате, не соответствующем стандарту X.509. К последним относятся, например, СКЗИ Crypto COM 2.2 и КриптоСИ.

Примечание

Термины *сертификатные СКЗИ* и *несертификатные СКЗИ* используются в рамках системы "ДБО BS-Client v.3" и не являются общеупотребительными.

СКЗИ в виде программных библиотек защиты информации

Алгоритмы, осуществляющие криптографические операции, могут быть реализованы в виде динамически компонуемых программных библиотек (*DLL*). Данные библиотеки называются

ПБЗИ – программные библиотеки защиты информации. Некоторые СКЗИ представляют собой только лишь ПБЗИ, для их использования достаточно поместить набор DLL в определенные каталоги системы. Другие СКЗИ требуют установки различного программного обеспечения посредством дистрибутивов, встраивают свои компоненты в ОС Windows. Более подробная информация приведена в разд. 1.5.2, « Обзор некоторых СКЗИ » [стр. 21].

Криптопровайдеры

Доступ к криптографическим алгоритмам СКЗИ на низком уровне осуществляется посредством предоставляемых СКЗИ интерфейсов. Стандартным в ОС Windows является интерфейс *MS Crypto API*. Модули, поддерживающие данный интерфейс, называются *криптопровайдерами* (*Cryptographic service provider*, *CSP*). К ним относятся, например, модули СКЗИ Crypto Pro CSP. Однако не все СКЗИ поддерживают интерфейс MS Crypto API и являются криптопровайдерами в строгом смысле: зачастую СКЗИ предоставляют собственный интерфейс взаимодействия. Система "ДБО BS-Client v.3" позволяет работать с СКЗИ, использующими как стандартный, так и нестандартные интерфейсы (см. разд. 2.1, « Механизмы взаимодействия с СКЗИ » [стр. 24]).

1.5.2. Обзор некоторых СКЗИ

В данном разделе приводится обзор СКЗИ, поддерживаемых системой "ДБО BS-Client v.3". Выбор СКЗИ для будущего использования осуществляется при заключении договора на поставку системы "ДБО BS-Client v.3".

Сравнение общих характеристик СКЗИ

Следующая сравнительная таблица (см. табл. 1.1, « Сравнение поддерживаемых СКЗИ » [стр. 21]) отображает несколько наиболее значимых параметров для поддерживаемых в системе "ДБО BS-Client v.3" СКЗИ. Пояснения к таблице даны ниже.

Таблица 1.1. Сравнение поддерживаемых СКЗИ

СКЗИ	Сертиф. ФАПСИ	ГОСТ 2001	X.509	CRL	Ключ. носители	Доп. ПО
Crypto Pro CSP 1.1	нет	нет	да	да	опред. CSP	Crypto Pro CSP
Crypto Pro CSP 2.0	да	да	да	да	опред. CSP	Crypto Pro CSP
Crypto Pro CSP 3.0	да	да	да	да	опред. CSP	Crypto Pro CSP
КриптоСИ	да	да	нет	нет	файл. носитель	нет
Верба 4	нет	нет	нет	нет	файл. носитель, TouchMemory	да
Верба 5	нет	нет	нет	нет	файл. носитель, TouchMemory	да
Message Pro 1.1	нет	нет	да	да	файл. носитель	NotaryPro

СКЗИ	Сертиф. ФАПСИ	ГОСТ 2001	X.509	CRL	Ключ. носители	Доп. ПО
Message Pro 1.3x	нет	нет	да	да	файл. носитель	NotaryPro, AdminPKI либо GenPair
Message Pro 2.x	да	да	да	да	файл. носитель	NotaryPro, AdminPKI (при необходимости)
Excellence 4.0	нет	нет	нет	нет	файл. носитель, есть возможность хранения мастер-ключа на TouchMemory	нет
Lan Crypto 2.35	нет	нет	нет	нет	файл. носитель, TouchMemory	нет
Crypto COM 2.2	нет	нет	нет	нет	файл. носитель	нет
OpenSSL	нет	нет	да	да	файл. носитель	нет

Рассмотрим значение сравнительных параметров:

- *Сертиф. ФАПСИ* – столбец показывает, была ли СКЗИ сертифицирована ФАПСИ на момент июня 2006 г.
- *ГОСТ 2001* – столбец показывает, поддерживает ли СКЗИ шифрование по сертифицированному ФАПСИ алгоритму ГОСТ Р34.10-2001. Прочие алгоритмы шифрования не являются сертифицированными ФАПСИ на момент июня 2006 г.
- *X.509* – столбец показывает, являются ли открытые ключи, выпускаемые СКЗИ, сертификатами по стандарту *X.509* (является ли СКЗИ сертификатной).
- *CRL* – столбец показывает, поддерживает ли СКЗИ списки отозванных сертификатов.
- *Ключ. носители* – перечень типов ключевых носителей поддерживаемых СКЗИ. В таблице перечислены только те ключевые носители, работоспособность которых в системе "ДБО BS-Client v.3" при использовании соответствующей СКЗИ гарантирована. Наиболее распространенным ключевым носителем является файловый носитель ("файл. носитель"). Для СКЗИ CryptoPro различных версий перечень поддерживаемых носителей определяется возможностями СКЗИ.
- *Доп. ПО* – перечень программного обеспечения, которое должно быть дополнительно установлено для обеспечения работоспособности СКЗИ. Установка данного ПО всегда производится до момента установки системы на стороне банка или клиента. Для СКЗИ, для которых в столбце *Доп. ПО* указано "нет", криптографические алгоритмы реализованы в виде программных библиотек (ПБЗИ), не требующих установки. Так, например, СКЗИ КриптоСИ поставляется в виде библиотеки `libcrypt.dll`. Состав дополнительного ПО для некоторых СКЗИ более подробно рассмотрен ниже.

Примечание

Все необходимое дополнительное ПО для СКЗИ, указанных в договоре на поставку системы "ДБО BS-Client v.3", поставляется вместе с дистрибутивом системы.

Глава 2. Криптозащита в системе "ДБО BS-Client v.3"

2.1. Механизмы взаимодействия с СКЗИ

В системе "ДБО BS-Client v.3" реализованы механизмы взаимодействия с большим количеством СКЗИ (см. разд. 1.5.2, « Обзор некоторых СКЗИ » [стр. 21]). Благодаря этому банк может выбрать СКЗИ, наиболее соответствующую его потребностям. Более того, в рамках криптографической сети одновременно могут использоваться несколько различных СКЗИ, то есть часть клиентов может использовать для защиты информации одну СКЗИ, часть клиентов – другую. Такая ситуация возможна, например, при постепенном переводе клиентов на новую СКЗИ.

Взаимодействие с СКЗИ осуществляется посредством *связок с СКЗИ*. Связка представляет собой всю совокупность механизмов, высокоуровневых и низкоуровневых интерфейсов, используемых системой "ДБО BS-Client v.3" для вызова функций конкретной СКЗИ. Схема взаимодействия – четырехуровневая (см. рис. 2.1 [стр. 24]).

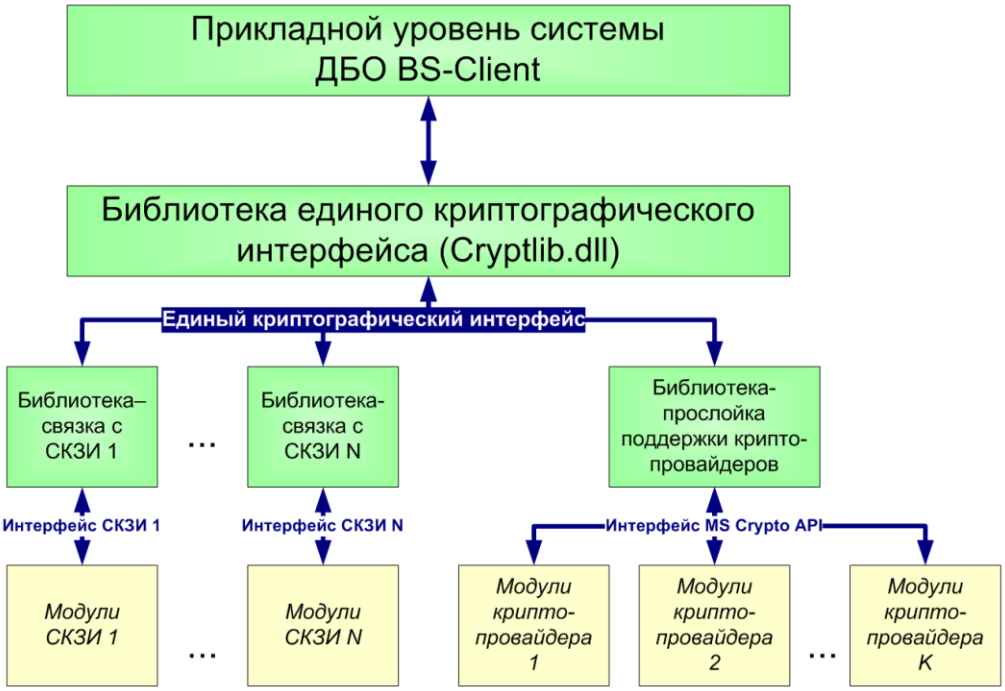


Рис. 2.1. Схема взаимодействия системы "ДБО BS-Client v.3" с внешними СКЗИ

На верхнем уровне находится прикладной уровень системы "ДБО BS-Client v.3": приложение cbank, *транспортная подсистема*, BS-Defender и другие компоненты. Прикладной уровень обращается к *библиотеке единого криптографического интерфейса* (`Cryptlib.dll`) для выполнения различных криптографических операций:

- зашифрования;
- расшифрования;
- подписи данных;
- проверки подписи;
- генерации ключевой пары (для несертификатных СКЗИ) или секретного ключа и запроса на сертификат (для сертификатных СКЗИ) и т.д.

В свою очередь, `Cryptlib.dll` обращается к специальным *криптобиблиотекам* (*библиотекам-прослойкам*), реализующим интерфейс взаимодействия с конкретными СКЗИ или классами СКЗИ. Криптобиблиотеки обращаются к модулям внешних СКЗИ, непосредственно выполняющим криптографические операции над блоками бинарных или текстовых данных (см. разд. 1.4, «Базовые криптографические операции» [стр. 16]).

Таким образом, каждая связка объединяет в себе библиотеку единого криптографического интерфейса, криптобиблиотеку для взаимодействия с конкретной СКЗИ и все используемые при взаимодействии интерфейсы.

То, какую криптобиблиотеку необходимо использовать, определяется по имени связки. Следующая таблица показывает соответствие между связками, криптобиблиотеками и СКЗИ:

Таблица 2.1. Связки с СКЗИ

Связка	Криптобиблиотека	Соответствующие СКЗИ	Примечания
Excellence/4.0	`cr_exc4.dll`	Excellence 4.0	
Lan Crypto/2.35	`cr_vesta.dll`	Lan Crypto 2.35	
Verba-OW/4	`cr_verb4.dll`	Верба 4, Верба 5	
Message-PRO 1.1	`cr_msp11.dll`	Message Pro 1.1	
M-Pro v1.34 (GOST PSE)	`cr_msp13.dll`	Message Pro 1.3x:	
M-Pro v2.x	`cr_msp2.dll`	Message Pro 2.x:	
Crypto COM/2.2	`cr_ccom2.dll`	Crypto COM 2.2	
CryptoPro CSP/1.1	`cr_msapi.dll`	Crypto Pro CSP 1.1, Crypto Pro CSP 2.0 (при использовании алгоритма Р34.10-94)	В настоящее время не используется, так как не поддерживает алгоритм ГОСТ Р34.10-2001. Вместо данной связки используется связка MS Crypto API 2.0
MS Crypto API 2.0	`cr_msapi.dll`	Crypto Pro CSP 1.1, Crypto Pro CSP 2.0, Crypto Pro CSP 3.0 и любые другие *криптопровайдеры*	
Open SSL	`cr_ossl.dll`	Open SSL	
Crypto-C	`cr_crypc.dll`	КриптоСИ	

Как видно из таблицы:

- некоторые связки (и соответственно криптобиблиотеки) используются для взаимодействия с несколькими СКЗИ;
- некоторые криптобиблиотеки (`cr_msapi.dll`) используются одновременно в нескольких связках.

Имена всех криптобиблиотек имеют префикс "cr_".

Имя используемой связки с СКЗИ и параметры ее работы задаются во всех *криптопрофилях* банка и его клиентов (см. разд. 2.2, « Криптографические профили » [стр. 26]).

2.2. Криптографические профили

Криптографический профиль (сокращенно *криптопрофиль*) – объект системы "ДБО BS-Client v.3", содержащий сведения об абоненте и используемых им ключах и определяющий права абонента на выполнение криптографических операций.

Криптопрофили используются для подписи документов, шифрования *транспортных пакетов "Банк-клиент"* и шифрования канала передачи данных подсистемы "Интернет-клиент" в случае, если используется средство защиты канала BS-Defender. Также криптопрофили используются при криптографической аутентификации пользователей подсистемы "Интернет-клиент". Подробное описание криптографических операций с использованием криптопрофилей приведено в разд. 1.4, «Базовые криптографические операции» [стр. 16].

Примечание

Все криптопрофили хранятся в БД системы "ДБО BS-Client v.3". Помимо этого, компонент BS-Defender локально хранит копию собственного криптопрофиля в своих настройках. Локальная копия криптопрофиля необходима для работы компонента, так как BS-Defender не обращается к БД. Криптопрофили других абонентов в работе BS-Defender не используются.

Криптопрофиль инкапсулирует в себе ключевую информацию. Всюду, где говорится о выполнении криптопрофилем каких-либо криптографических операций, подразумевается, что операции выполняются с использованием ключей, сопоставленных криптопрофилю, от имени соответствующего криптопрофилю абонента. При этом на прикладном уровне системы "ДБО BS-Client v.3" непосредственное обращение к ключевой информации не производится – все криптографические операции выполняются посредством криптопрофилей.

В рамках одного узла криптографической сети каждому абоненту соответствует один и только один криптопрофиль. Поэтому зачастую в контексте одного узла термины *абонент* и *криптопрофиль* используются как взаимозаменяемые. Однако в контексте всей криптографической сети между данными понятиями появляется существенное различие. Для обеспечения защищенного двустороннего обмена информацией между банком и клиентом для каждого абонента клиента и каждого абонента банка заводится криптопрофиль и на стороне клиента, и на стороне банка. То есть в пределах всей сети каждый абонент представлен двумя криптопрофилями. Таким образом, в каждом узле имеется вся необходимая ключевая информация и информация о правах на выполнение криптографических операций для каждого абонента, участвующего в информационном обмене.

Сведения, содержащиеся в криптопрофиле, включают в себя:

- название абонента (криптопрофиля);
- наименование связки с СКЗИ, используемой при работе с ключами (см. разд. 2.1, « Механизмы взаимодействия с СКЗИ » [стр. 24]);
- статус криптопрофиля (см. разд. 2.2.2, «Статус криптопрофиля» [стр. 29]);
- информацию о ключевых наборах или открытых ключах, сопоставленных криптопрофилю (см. разд. 2.2.3, « Ключевые наборы криптопрофиля » [стр. 29]);
- права на выполнение криптографических операций (подробное описание прав изложено в разд. 2.4, «Права на выполнение криптографических операций» [стр. 54]).

Кроме того, в системе содержится информация о принадлежности криптопрофиля АРМ, организациям и другим объектам системы [стр. 27]. Далее данные, относящиеся к криптопрофилю, будут рассмотрены более подробно.

2.2.1. Принадлежность криптопрофилей

В системе "ДБО BS-Client v.3" для криптопрофилей задается принадлежность или соответствие различным объектам системы:

- Принадлежность криптопрофиля АРМ и организациям [стр. 27].
- Принадлежность криптопрофиля пользователям [стр. 28].

Принадлежность / соответствие криптопрофилей ограничивает права на выполнение криптопрофилем криптографических операций (см. разд. 2.3, «Криптографические операции в системе "ДБО BS-Client v.3"» [стр. 36]).

Принадлежность криптопрофиля АРМ и организациям

Криптопрофиль абонента клиента может принадлежать одному или несколькми АРМ и одной или нескольким организациям клиента. В простейшем случае организации соответствует один АРМ, все криптопрофили принадлежат одному АРМ и одной организации. В более сложном случае, когда клиентом банка является холдинг, для взаимодействия с банком могут быть использованы как один АРМ – на все организации, так и несколько АРМ – на каждую организацию, входящую в холдинг. Часть лиц холдинга, например, генеральный директор холдинга или главный бухгалтер должны иметь возможность работать с документами всех дочерних организаций. Поэтому, если имеется один АРМ на несколько организаций, криптопрофили указанных лиц привязываются к одному АРМ и ко всем дочерним организациям. Если же имеется по одному АРМ на каждую организацию, криптопрофили указанных лиц привязываются ко всем АРМ и всем дочерним организациям.

Критопрофиль абонента банка принадлежит единственному АРМ банка.

Учитывая вышесказанное, система "ДБО BS-Client v.3" позволяет гибко настраивать принадлежность криптопрофилей к заданным АРМ, организациям и подразделениям банка.

Принадлежность криптопрофиля какому-либо АРМ влияет на различные процессы, например:

- С помощью криптопрофиля можно осуществлять электронную цифровую подпись (см. разд. «Подпись документов» [стр. 44]) только тех документов, которые принадлежат к тому же АРМ, что и криптопрофиль. При этом для каждого АРМ, которому принадлежит криптопрофиль, можно задать ограничения на выполнение операции подписи принадлежащих АРМ документов (см. разд. 2.4.1, «Права подписи документов» [стр. 55]).

- Принадлежность криптопрофиля какому-либо АРМ также играет роль, например, при определении списка абонентов-получателей в процессе зашифрования транспортных пакетов: любой абонент (криптопрофиль), принадлежащий конкретному АРМ, должен иметь возможность расшифровать транспортный пакет, адресованный данному АРМ, и проверить подпись пакета (см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]).

Принадлежность криптопрофиля определенной организации позволяет криптопрофилю с соответствии с его правами осуществлять криптографические операции над документами данной организации. В рассмотренном выше примере холдинга криптопрофили определенных лиц должны принадлежать всем организациям холдинга.

Принадлежность криптопрофиля пользователям

В общем случае соответствие между криптопрофилями и пользователями системы может не являться взаимно-однозначным: теоретически один криптопрофиль может использоваться несколькими пользователями и один пользователь может использовать несколько криптопрофилей. Этим криптопрофили похожи на профили пользователей (см. **разд. 2.4, «Настройка профиля пользователя»** документа *Руководство по использованию. Разграничение доступа*). Однако идеологически правильной и практически жизнеспособной является ситуация, когда:

- каждый криптопрофиль сопоставлен *ровно одному* пользователю;

- каждому пользователю сопоставлено *не более одного* криптопрофиля.

На это есть несколько причин, основные из которых следующие:

- Криптопрофиль используется в операциях электронной цифровой подписи, а так как ЭЦП является эквивалентом собственноручной подписи, то владельцем ключей подписи и, соответственно, криптопрофиля должно быть одно физическое лицо. То есть, один и тот же криптопрофиль не должен соответствовать нескольким пользователям.

- Транспортная подсистема подсистемы *"Банк-клиент"* и сервер обработки запросов RTS подсистемы "Интернет-клиент" могут работать некорректно в случае, когда пользователю, от имени которого работает транспортная подсистема / RTS, сопоставлено несколько криптопрофилей.

Некоторым пользователям криптопрофили могут быть не назначены вовсе. Например, оператору, только вводящему в систему платежные поручения, не нужно выполнять каких-либо криптографических операций, соответственно ему криптопрофиль не нужен.

Примечание

Выше была отмечена схожесть профилей пользователей и криптопрофилей. В то же время, имеется существенное различие между профилями пользователей и криптопрофилями: профили

пользователей регистрируются локально – только в рамках текущего АРМ, криптопрофили же регистрируются глобально – во всех АРМ, с которыми осуществляется обмен данными.

2.2.2. Статус криптопрофиля

Криптопрофиль может иметь два статуса: "разрешен" и "запрещен". Статус "разрешен" означает, что криптопрофиль может выполнять криптографические операции в соответствии с сопоставленными ему правами. Статус "запрещен" означает, что криптографический профиль не может выполнять никаких криптографическх операций. Присвоение криптопрофилю статуса "запрещен" может быть произведено при компроментации ключевого набора (см. разд. 1.3.6, «Компрометация ключевых наборов» [стр. 12]).

2.2.3. Ключевые наборы криптопрофиля

Криптопрофилю может соответствовать один или несколько ключевых наборов (см. разд. 1.3.4, «Ключевые наборы» [стр. 11]). При наличии нескольких наборов один из них является активным, полученным при очереденой перегенерации, остальные – неактивными. Подробнее данные статусы ключевых наборов будут рассмотрены ниже.

Условия хранения ключевых наборов, обеспечивающие защищенный обмен информацией

Как следует из материала, приведенного в разд. 1.3.4, «Ключевые наборы» [стр. 11], для обеспечения защищенного обмена информацией между абонентами A и B необходимо, чтобы в ключевом наборе каждого из абонентов присутствовал открытый ключ другого абонента. При этом наличие полного ключевого набора абонента A у абонента B или ключевого набора абонента B у абонента A не является необходимым, а наоборот, предоставляет возможность несанкцированного использования ключей. В разрезе системы "ДБО BS-Client v.3" это означает следующее:

- в ключевых наборах абонентов клиентов должны присутствовать открытые ключи абонентов банка и наоборот, в ключевых наборах абонентов банка должны присутствовать открытые ключи абонентов клиентов (подробнее см. в разд. 2.2.4, «Регистрация открытых ключей в ключевых наборах криптопрофилей» [стр. 35]);

- хранение ключевых наборов банка на стороне клиентов и ключевых наборов клиентов на стороне банка предоставляет возможность несанкционированного использования ключей.

Несмотря на утверждение в последнем пункте, допускается ситуация временного хранения ключевых наборов клиента на стороне банка. Такая ситуация может возникнуть в процессе регистрации нового клиента в системе, когда для удобства клиента подготовка ключевых наборов абонентов клиента может производиться на стороне банка. Однако даже при наличии описанного допущения, использование технологических ключей (см. разд. «Технологические ключевые наборы» [стр. 31]) и механизма перегенерации предотвращает любое несанкционированное использование ключей клиента на стороне банка.

Из сказанного следует, что ключевые наборы банка должны быть доступны только на стороне банка, а ключевые наборы клиента – на стороне клиента, а также, возможно, и на стороне банка для последующей передачи клиенту.

Информация о ключевых наборах

Криптопрофиль хранит информацию, необходимую для использования сопоставленных ему ключевых наборов. Информация о каждом наборе может включать в себя:

- статус ключевого набора [стр. 30];
- признак технологического ключевого набора [стр. 31];
- срок действия ключевого набора [стр. 32];
- параметры использования ключей [стр. 33];
- UID ключевой пары [стр. 34].

Данная информация изначально задается в процессе создания криптопрофиля на стороне банка. Часть этой информации может быть впоследствии изменена в процессе редактирования криптопрофиля или в процессе его установки (для криптопрофилей клиентов).

> **Примечание**
>
> Для использования некоторых криптопрофилей, например, криптопрофилей банка на стороне клиента, задание параметров использования ключей не требуется (см. разд. «Параметры использования ключевых наборов» [стр. 33]). Прочая информация о ключевых наборах (статус, UID и т.д.) задается для всех криптопрофилей.

Статус ключевого набора

Статус ключевого набора отражает статус ключевой пары, входящей в набор, и влияет на перечень допустимых к выполнению с помощью ключевой пары операций. Статус может принимать одно из следующих значений:

- "Активный" – ключевой набор является действующим и может быть использован при выполнении любых криптографических операций, разрешенных правами криптопрофиля. Только один ключевой набор криптопрофиля может быть активным.
- "Неактивный" – ключевой набор не является действительным. С помощью данного ключевого набора нельзя выполнять криптографические операции подписи документов и подписи и зашифрования пакетов. Статус ключевого набора автоматически меняется на "неактивный" после перегенерации ключевой пары (новый ключевой набор получает статус "активный"), а также при истечении срока действия сертификата ключевого набора, если открытый ключ выполнен в виде сертификата.

  > **Внимание**!
  >
  > Если ключевой набор, секретным ключом которого подписан документ или пакет, имеет статус "неактивный", это не является поводом для признания подписи неверной: это означает, что на момент подписи ключевой набор имел статус "активный" и был действительным, но в процессе передачи документа получателю статус набора был изменен.

- "Запрещен" – ключевой набор является скомпрометированным, его использование запрещено. Если в рамках АРМ, которому принадлежит криптопрофиль, статус криптопрофиля изменен на "запрещен", выполнение криптографических операций с помощью данного

криптопрофиля в данном АРМ будет невозможно. Так нельзя выполнять криптографические операции запрещенным на стороне банка криптопрофилем банка или запрещенным на стороне клиента криптопрофилем клиента. Однако возможна ситуация, когда, например, криптопрофиль на стороне банка имеет статус "запрещен", а на стороне клиента имеет статус "активный". В этом случае выполнение криптографических операций с помощью криптопрофиля на стороне клиента будет разрешено, но на стороне банка результаты выполнения криптографических операций не будут признаны действительными:

- подпись под документами и пакетами, произведенная с использованием данного ключевого набора, не будет признана действительной;
- пакеты, зашифрованные с помощью данного ключевого набора, не будут подлежать расшифрованию;
- криптографическая аутентификация пользователя по запрещенному открытому ключу не будет производиться.

- "Переходный" – новый ключевой набор банка при смене ключей. Данный ключевой набор не используется при выполнении криптографических операций до завершения процедуры смены ключей. После завершения процедуры активный ключевой набор меняет статус на "неактивный", а переходный – на "активный". Данный статус могут принимать только ключевые наборы банка.

> **Внимание**!
>
> Не следует путать статус ключевого набора со статусов криптопрофиля, которому он отнесен (см. разд. 2.2.2, «Статус криптопрофиля» [стр. 29]).

Технологические ключевые наборы

С целью обеспечения большей безопасности использования секретных ключей клиентов в системе "ДБО BS-Client v.3" для ключевых наборов клиентов введен признак *технологического ключевого набора*. При регистрации нового клиента в системе банка для удобства клиента ключевые пары абонентов клиента могут быть сформированы на стороне банка. Сформированные секретные и открытые ключи абонентов клиента помещаются в дистрибутив клиентской системы или передаются клиенту вместе с дистрибутивом. После установки системы на стороне клиента секретные ключи абонентов могут оставаться в системе банка, что уменьшает надежность их использования. С целью предотвращения возможного несанкционированного использования секретных ключей клиентов на стороне банка применяются два механизма:

- При использовании СКЗИ Excellence или Lan Crypto в момент установки системы клиента происходит автоматическая перегенерация клиентских ключей . Новые открытые ключи абонентов клиента передаются в банк для регистрации. С этого момента старые ключи абонентов считаются недействительными, что исключает возможность их использования.
- При использовании остальных СКЗИ перегенерация ключей в момент установки системы клиента не происходит, а используется механизм технологических ключевых наборов. Рассмотрим данный механизм более подробно.

При заведении нового клиента ключевой набор каждого криптопрофиля клиента помечается как "технологический". Ключи технологического ключевого набора, называемые *техноло-*

гическими ключами, подлежат обязательной перегенерации на клиенте после установки системы "ДБО BS-Client v.3". На выполнение операции подписи документов (см. разд. «Подпись документов» [стр. 44]) посредством технологического ключевого набора обычно накладывают определенные ограничения. По умолчанию (см. разд. «Количество подписей под документами» [стр. 41]) запрещена подпись технологическими ключами любых документов, кроме запросов клиентов на регистрацию сертификатов. Для обеспечения аутентичности прочих документов не рекомендуется отходить от данного ограничения. На выполнение операций над *транспортными пакетами* (см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]) посредством технологического ключевого набора дополнительных ограничений не накладывается.

После установки системы клиента в банк отправляется запрос на регистрацию сертификата. После перегенерации ключевого набора технологический ключевой набор изменяет статус на "неактивный", а новый ключевой набор помечается как "рабочий" со статусом "активный". С этого момента возможна штатная работа системы клиента с использованием нового ключевого набора, а использование технологических ключей при выполнении криптографических операций становится невозможным.

Таким образом, клиент не сможет отправлять в банк финансовые документы до тех пор, пока не будет сформирована новая ключевая пара. Описанная процедура гарантирует клиенту полную защиту его секретных ключей, так как они генерируются непосредственно на рабочем месте пользователя и могут быть известны только пользователю.

Ключевые наборы, не являющиеся технологическими, называются *рабочими*. Необходимо отметить, что технологическими могут быть только ключевые наборы клиентов, ключевые наборы банка (ГО и подразделений) всегда являются рабочими. В перегенерации ключей подразделений банка после установки системы "ДБО BS-Client v.3" в подразделениях нет необходимости. Также необходимо отметить, что термин "рабочий" не является синонимом статуса ключевого набора "активный" (см. разд. «Статус ключевого набора» [стр. 30]).

Срок действия ключевого набора

Если используется сертификатная СКЗИ, то в соответствии со сроком действия сертификата ключевого набора в криптопрофиле устанавливается срок действия всего ключевого набора. При использовании несертификатных СКЗИ есть возможность искусственно ограничить период использования ключей, установив срок действия ключевого набора. Система "ДБО BS-Client v.3" по умолчанию устанавливает срок действия ключевых наборов 1 год.

При использовании сертификатных СКЗИ существует возможность проверять срок действия сертификатов при старте системы "ДБО BS-Client v.3". Проверку срока действия выполняет автопроцедура "Проверка срока действия сертификатов" группы автопроцедур "Crypto" (см. **док. «Руководство по использованию. Операции и автопроцедуры»**). Если в процессе проверки выяснится, что у какого-либо из активных сертификатов, зарегистрированных в системе, истекает или уже истек срок действия, система выведет соответствующее сообщение. Проверка осуществляется для сертификатов всех зарегистрированных в системе пользователей.

Примечание

- Для того, чтобы проверка осуществлялась, необходимо, чтобы автопроцедура "Проверка срока действия сертификатов" была разрешена.

- Необходимость проверки и количество дней до истечения срока действия, за которое система начнет выводить предупреждающие сообщения, определяется настройками подсистемы криптозащиты (см. инстр. «Настройка общих параметров использования открытых ключей» [стр. 84]).
- При использовании несертификатных СКЗИ проверка срока действия ключевых пар не выполняется.

Параметры использования ключевых наборов

Для каждого ключевого набора в криптопрофиле содержится информация, необходимая для использования ключей набора. Состав данной информации зависит от конкретной СКЗИ, но можно выделить группы параметров, используемых большинством СКЗИ:

- *Параметры ключевого носителя*. Данная группа параметров задает прежде всего расположение ключевой пары и всех необходимых сертификатов (см. разд. 1.3.4, «Ключевые наборы» [стр. 11]):
  - расположение открытого ключа / сертификата абонента;
  - расположение секретного ключа;
  - путь к каталогу с открытыми ключами / сертификатами абонентов, с которыми осуществляется информационный обмен;
  - путь к каталогу с сертификатом или цепочкой сертификатов ЦС.

  Примечание

  Открытые ключи, как правило, хранятся в виде файлов в заданном каталоге, но в общем случае способ хранения ключевой информации определяется конкретной СКЗИ.

  Для некоторых СКЗИ на ключевых носителях располагается дополнительная информация, например, списки отозванных сертификатов (см. разд. «Списки отозванных сертификатов» [стр. 14]), мастер-ключ (см. разд. 1.3.1, «Ключевые пары» [стр. 9]). Расположение указанных объектов также задается параметрами данной группы.

  Внимание!

  При определенном способе создания криптопрофиля клиента параметры ключевого носителя принудительно изменяются в момент установки системы клиента. Пользователю, устанавливающему систему, будет предложено указать новое расположение файлов ключей.

- *Параметры работы СКЗИ*. Данные параметры задают алгоритмы, которые необходимо использовать при работе с ключами, длину ключей и т.д.
- *Параметры работы клиентского BS-Defender с ключевым набором*. Данная группа параметров используется только на стороне клиента компонентом BS-Defender подсистемы "Интернет-клиент". В группу входит всего один параметр (**Encrypt for UID**), который задает UID абонента или абонентов на стороне банка, для которых должно осуществляться зашифрование пакетов. Компонент BS-Defender, в отличие от транспортной подсистемы, не обращается к БД для определения списка абонентов, относящихся к АРМ

принимающей стороны, и требует явного задания UID абонентов-получателей (см. разд. «Шифрование данных в системе "ДБО BS-Client v.3"» [стр. 37]).

> **Примечание**
>
> Данный параметр в криптопрофилях банка не используется.

- *Параметры работы ключевого кэша*. К этой группе относятся параметры, задающие время хранения ключевой информации в *ключевом кэше* (см. разд. 1.3.4, «Ключевые наборы» [стр. 11]). Для большинства СКЗИ данная группа состоит из двух параметров:
  - время хранения секретного ключа в кэше с момента последнего его считывания с ключевого носителя (обычно параметр называется **Key request time out**);
  - время хранения секретного ключа в кэше с момента последнего его использования (обычно параметр называется **Last operation key time out**).
- *Параметры, используемые при генерации или перегенерации ключевого набора*. Названия данных параметров обычно имеют префикс "Key gen -". Конкретный набор параметров, относящихся к данной группе, существенно зависит от используемой СКЗИ.

UID **ключевой пары**

UID ключевой пары – параметр, задающий связь между криптопрофилем и соотнесенной ему ключевой парой. В отличие от параметров ключевых носителей (см. разд. «Параметры использования ключевых наборов» [стр. 33]), позволяющих по информации, содержащейся в криптопрофиле, определить расположение сопоставленных ему ключевых пар, описываемый параметр позволяет по *UID*, извлеченному из ключа, определить, какому криптопрофилю соотнесен данный ключ. Данная возможность необходима криптографическим операциям проверки подписи и зашифрования, рассмотренным далее в разд. 2.3, «Криптографические операции в системе "ДБО BS-Client v.3"» [стр. 36].

> **Примечание**
>
> Определение термина *UID* приведено в разд. 1.3.3, «UID ключевой пары» [стр. 11].

Параметры ключевых носителей и UID ключевой пары совместно задают соответствие между криптопрофилями и соотнесенными им ключами, как изображено на рис. 2.2 [стр. 35].

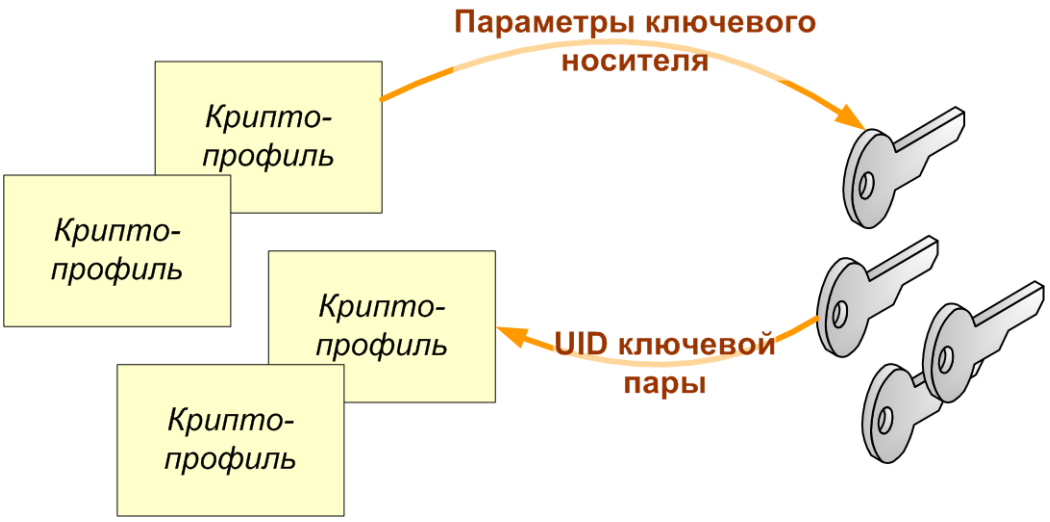


Рис. 2.2. Связь между криптопрофилями и ключами

Сохранение некорректного значения UID ключевой пары в информации о ключевом наборе приведет к нарушению связи между криптопрофилем и сопоставленной ему ключевой парой. В результате этого нельзя будет проверить права криптопрофиля на выполнение криптопрографических операций (см. разд. 2.4, «Права на выполнение криптографических операций» [стр. 54]) при проверке подписи, сделанной посредством криптопрофиля, или при расшифровании пакетов, зашифрованных с помощью криптопрофиля. Поэтому во избежание ошибок при использовании большинства СКЗИ в процессе создания криптопрофиля имеется возможность извлечь UID непосредственно из ключей, сопоставляемых криптопрофилю.

2.2.4. Регистрация открытых ключей в ключевых наборах криптопрофилей

В общем случае, для того, чтобы абонент мог обмениваться информацией с другими абонентами криптографической сети, он должен иметь доступ к копиям их открытых ключей. В системе "ДБО BS-Client v.3" абонент может обмениваться информацией (при наличии соответствующих прав) только с теми абонентами, открытые ключи которых содержатся в ключевых наборах криптопрофиля (см. разд. 2.2.3, « Ключевые наборы криптопрофиля » [стр. 29]). Соответственно, для того, чтобы абоненту А иметь возможность совершать информационный обмен с абонентом В, открытый ключ абонента В должен содержаться в ключевом наборе абонента А, а открытый ключ абонента А – в ключевом наборе абонента В (речь идет о действующих открытых ключах и ключевых наборах).

Процедура внесения открытых ключей абонентов в ключевые наборы называется *регистрацией открытых ключей* или *регистрацией абонентов*. Таким образом, между абонентами А и В возможен защищенный обмен информацией, если абоненты зарегистрированы друг на друга (открытый ключ абонента А зарегистрирован в ключевом наборе абонента В, а открытый ключ абонента В зарегистрирован в ключевом наборе абонента А).

В ряде случае регистрация производится системой автоматически:

- При создании нового криптопрофиля в системе банка открытый ключ его ключевого набора будет предложено автоматически зарегистрировать в ключевых наборах всех криптопрофилей банка, относящихся к той же СКЗИ, что и создаваемый криптопрофиль.

- При импорте криптопрофиля клиента в систему клиента открытые ключи сопоставленного криптопрофилю активного ключевого набора будут автоматически зарегистрированы во всех криптопрофилях клиента.

В остальных случаях регистрация открытых ключей должна производиться вручную. Ручная регистрация открытых ключей необходима только на стороне банка.

2.3. Криптографические операции в системе "ДБО BS-Client v.3"

В системе "ДБО BS-Client v.3" для защиты хранимых и передаваемых по каналам связи данных применяются следующие криптографические операции и группы операций:

- Криптографические операции над документами [стр. 40].
- Криптографические операции транспортной подсистемы [стр. 50].

Общее описание данных операций приведено в разд. 2.3.1, «Общее описание базовых криптографических операций в системе "ДБО BS-Client v.3"» [стр. 36], более подробное описание – в соответствующих разделах.

Ход выполнения криптографических операций отражается в соответствующем журнале, рассмотренном в разд. 2.3.4, «Журнал криптографических операций» [стр. 54].

2.3.1. Общее описание базовых криптографических операций в системе "ДБО BS-Client v.3"

В данном разделе приводится общее описание криптографических операций в системе "ДБО BS-Client v.3". Несмотря на то, что каждая криптографическая операция имеет свои особенности выполнения, можно выделить ряд характерных общих черт двух групп операций, рассматриваемых в следующих разделах:

- Шифрование данных в системе "ДБО BS-Client v.3" [стр. 37].
- Формирование и проверка электронной цифровой подписи в системе "ДБО BS-Client v. 3" [стр. 38].

Общей особенностью выполнения криптографических операций в системе "ДБО BS-Client v. 3" является необходимое условие использования криптопрофилей (см. разд. 2.2, « Криптографические профили » [стр. 26]), в то время как для выполнения базовых циклов шифрования на уровне конкретной СКЗИ требуется только ключевая пара абонента (см. разд. 1.4, «Базовые криптографические операции» [стр. 16]). Криптопрофили содержат информацию, необходимую для использования ключей: в зависимости от выполняемой криптографической операции - либо ключей самого абонента, либо ключей абонентов, с которыми осуществляется информационный обмен. Криптопрофили в числе прочего определяют права конкретного абонента на выполнение криптографических операций (см. разд. 2.4, «Права на выполнение криптографических операций» [стр. 54]).

Большинство криптографических операций можно рассматривать как трехуровневые:

- На *верхнем уровне* (*уровне прав*) выбираются криптографические профили участвующих в операции абонентов в соответствии с правами криптопрофилей.
- На *среднем уровне* (*уровне криптопрофилей*) по данным криптопрофилей определяются ключевые наборы абонентов, подходящие для выполнения криптографических операций, и параметры их использования.
- На *нижнем уровне* (*уровне СКЗИ*) средствами СКЗИ осуществляются криптографические операции с использованием ключей.

Верхний и средний уровень составляют прикладной уровень системы "ДБО BS-Client v.3", упоминаемый в разд. 2.1, « Механизмы взаимодействия с СКЗИ » [стр. 24]. В последующих разделах он будет рассмотрен более подробно. Нижний уровень реализуется посредством *библиотеки единого криптографического интерфейса* и механизмов используемых СКЗИ.

Шифрование данных в системе "ДБО BS-Client v.3"

> **Внимание**!
>
> Назначение и общие принципы шифрования данных изложены в разд. 1.4.1, «Зашифрование и расшифрование данных» [стр. 17]. Рекомендуется ознакомиться с указанным разделом перед изучением представленной ниже информации.

В системе "ДБО BS-Client v.3" используется:

- шифрование транспортных пакетов подсистемы *"Банк-клиент"* (см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]);
- шифрование пакетов подсистемы "Интернет-клиент" при использовании средства защиты канала BS-Defender.

Также с целью предотвращения несанкционированного использования пакетов обновлений систем для банков может осуществляться шифрование пакетов обновлений .

> **Примечание**
>
> Для обеспечения аутентичности пакетов дополнительно применяется электронная цифровая подпись пакетов (см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]).

В зависимости от используемой СКЗИ при зашифровании могут использоваться механизмы, обеспечивающие целостность шифруемых данных.

Для того, чтобы зашифрование данных было выполнено успешно, должны быть соблюдены следующие требования к криптопрофилю и ключевым наборам абонента, *осуществляющего зашифрование* (*абонента-отправителя*):

- криптопрофиль имеет статус "разрешен" (см. разд. 2.2.2, «Статус криптопрофиля» [стр. 29]);
- криптопрофиль обладает соответствующими правами на зашифрование (см. разд. 2.4.1, «Права подписи документов» [стр. 55]);

- в криптопрофиле содержится ключевой набор со статусом "активный" (см. разд. «Статус ключевого набора» [стр. 30]);

- в данном ключевом наборе зарегистрированы открытые ключи *абонентов-получателей*, которые должны иметь возможность расшифровать данные (см. разд. 2.2.4, «Регистрация открытых ключей в ключевых наборах криптопрофилей» [стр. 35]).

Расшифрование выполняется секретным ключом из активного (или переходного) ключевого набора криптопрофиля абонента-получателя.

Расшифрование данных будет выполнено успешно, если:

- соблюдены следующие требования к криптопрофилю и ключевым наборам абонента, *осуществившего зашифрование* (*абонента-отправителя*):

  - криптопрофиль обладает соответствующими правами на зашифрование (см. разд. 2.4.1, «Права подписи документов» [стр. 55]);

  - в криптопрофиле содержится ключевой набор со статусом "активный" или "переходный" (см. разд. «Статус ключевого набора» [стр. 30]);

- соблюдены следующие требования к криптопрофилю и ключевым наборам абонента, *осуществляющего расшифрование* (*абонента-получателя*):

  - криптопрофиль абонента имеет статус "разрешен" (см. разд. 2.2.2, «Статус криптопрофиля» [стр. 29]);

Формирование и проверка электронной цифровой подписи в системе "ДБО BS-Client v.3"

> **Внимание**!
>
> Назначение и общие принципы электронной цифровой подписи данных изложены в разд. 1.4.2, «Электронная цифровая подпись данных и проверка подписи» [стр. 18]. Рекомендуется ознакомиться с указанным разделом перед изучением представленной ниже информации.

В системе "ДБО BS-Client v.3" ЭЦП применяется:

- для подписи документов (см. разд. «Подпись документов» [стр. 44]);

- для подписи транспортных пакетов подсистемы "Банк-клиент" (см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]);

- для подписи пакетов подсистемы "Интернет-клиент" при использовании средства защиты канала BS-Defender.

При работе с ЭЦП пакетов применяются операции подписи и проверки подписи. При работе с ЭЦП документов также используется операция снятия подписи (см. разд. 2.3.2, «Криптографические операции над документами» [стр. 40]).

Общие принципы электронной цифровой подписи изложены в разд. 1.4.2, «Электронная цифровая подпись данных и проверка подписи» [стр. 18]. Напомним, что для подписи данных

используется секретный ключ абонента, подписывающего документ, а для проверки подписи – открытый ключ абонента (ключи подписи).

Как было сказано в разд. 2.2, « Криптографические профили » [стр. 26] в системе "ДБО BS-Client v.3" все криптографические операции совершаются с использованием данных, хранящихся в криптопрофилях. Поэтому, более точно, подпись осуществляется секретным ключом ключевого набора, поставленного в соответствие криптопрофилю абонента, подписывающего данные (документ или пакет). Проверка подписи осуществляется сертификатом абонента, подписавшего данные, из ключевого набора, поставленного в соответствие криптопрофилю абонента, проверяющего подпись. Таким образом для проверки подписи необходимо, чтобы в активном ключевом наборе криптопрофиля абонента, проверяющего подпись, был зарегистрирован абонент, подписавший данные.

Для выполнения подписи абонент должен обладать определенными правами (см. разд. 2.4, «Права на выполнение криптографических операций» [стр. 54]). Так для подписи документов абоненту необходимы соответствующие права на подпись документов, для подписи транспортных пакетов – право приема / отправки почты и т.д. При проверке подписи в числе прочего происходит проверка наличия у подписавшего абонента соответствующих прав подписи. Кроме того, при проверке подписи документа, подписанного технологическим ключом, дополнительно проверяется возможность подписи документа технологическими ключами.

Суммируя вышесказанное, для того, чтобы подпись данных была выполнена успешно, должны быть соблюдены следующие требования к криптопрофилю и ключевым наборам абонента, *осуществляющего подпись*:

- криптопрофиль имеет статус "разрешен" (см. разд. 2.2.2, «Статус криптопрофиля» [стр. 29]);
- криптопрофиль обладает соответствующими правами на подпись (см. разд. 2.4.1, «Права подписи документов» [стр. 55]);
- в криптопрофиле содержится ключевой набор со статусом "активный" (см. разд. «Статус ключевого набора» [стр. 30]);
- ключевой набор является либо рабочим, либо технологическим при определенных условиях (см. разд. «Технологические ключевые наборы» [стр. 31]).

При проверке ЭЦП будет считаться верной, если:

- соблюдены следующие требования к криптопрофилю и ключевым наборам абонента, *подписавшего данные*:
  - криптопрофиль зарегистрирован на проверяющей стороне и имеет статус "разрешен" (см. разд. 2.2.2, «Статус криптопрофиля» [стр. 29]);
  - криптопрофиль обладает соответствующими правами на подпись (см. разд. 2.4.1, «Права подписи документов» [стр. 55]);
  - ключевой набор, секретным ключом которого сформирована подпись, в данном криптопрофиле имеет статус "активный" или "неактивный" (см. разд. «Статус ключевого набора» [стр. 30]);

- данный ключевой набор является либо рабочим, либо технологическим при определенных условиях (см. разд. «Технологические ключевые наборы» [стр. 31]);

- соблюдены следующие требования к криптопрофилю и ключевым наборам абонента, *проверяющего подпись*:

  - в криптопрофиле зарегистрирован открытый ключ абонента, подписавший данные (см. разд. 2.2.4, «Регистрация открытых ключей в ключевых наборах криптопрофилей» [стр. 35]);

- содержимое блока подписанных данных не искажено, ЭЦП соответствует дайджесту (см. разд. 1.4.2, «Электронная цифровая подпись данных и проверка подписи» [стр. 18]).

В случае, если открытый ключ абонента, подписавшего данные, отсутствует в криптопрофиле абонента, проверяющего подпись (открытый ключ не зарегистрирован в криптопрофиле), проверка подписи не может быть произведена. При несоблюдении прочих указанных условий подпись считается неверной.

Примечание

Отметим, что подпись не будет считаться неверной если ключевой набор, секретным ключом которого подписаны данные, имеет статус "неактивный", так как на момент подписи ключевой набор являлся действительным. Также необходимо отметить, что для проверки подписи абоненту, проверяющему подпись, не обязательно обладать соответствующим правом подписи. Проверку подписи может выполнить любой пользователь системы, в криптопрофиле которого зарегистрирован абонент, подписавший данные.

2.3.2. Криптографические операции над документами

Над документами в системе "ДБО BS-Client v.3" определены три криптографические операции:

- подпись документов [стр. 44];

- проверка подписи [стр. 48];

- снятие подписи [стр. 49].

Выполнение перечисленных криптографических операций на прикладном уровне системы имеет некоторые особенности, рассмотренные в разд. «Особенности подписи документов в системе "ДБО BS-Client v.3"» [стр. 40].

Параметры, регулирующие ход операций над документами, подробно описаны в инстр. «Настройка общих параметров выполнения криптографических операций над документами» [стр. 82].

Особенности подписи документов в системе "ДБО BS-Client v.3"

Документы подписываются для обеспечения их *аутентичности*, другими словами – гарантии того, что документ действительно подписан лицом, отправившим документ. Подпись

документов клиента гарантирует банку, что документ получен именно от этого клиента, а подпись документов банка гарантирует клиенту, что документ получен из банка.

Подпись документов в системе "ДБО BS-Client v.3" имеет некоторые особенности по сравнению с общими принципами подписи, изложеннымы в разд. 1.4.2, «Электронная цифровая подпись данных и проверка подписи» [стр. 18] и разд. «Формирование и проверка электронной цифровой подписи в системе "ДБО BS-Client v.3"» [стр. 38]:

- документы могут подписываться несколькими подписями, а могут и не подписываться вообще (см. разд. «Количество подписей под документами» [стр. 41]);
- существует особая разновидность подписи – визирующая подпись (см. разд. «Визирующая подпись» [стр. 43]);
- подпись под *квитками на документ* не проставляется (см. разд. «Подпись документарных квитков» [стр. 43]);
- возможна подпись документов от имени другого пользователя системы "ДБО BS-Client v.3" (см. разд. «Подпись от имени другого пользователя» [стр. 43]);
- криптографические операции над документами реализованы в виде документарных операций, которые могут запускаться на выполнение как вручную, так и автоматически (см. разд. «Документарные операции формирования, проверки и снятия подписи» [стр. 44]);
- подпись осуществляется не всего документа, а только наиболее значимых его полей в соответствии со *схемой составления документа* (см. прил. А, «Механизм формирования и формат хранения подписи под документами» [стр. 89]).

Количество подписей под документами

Обычно под финансовыми документами *клиентов* требуется наличие двух подписей, например, главного бухгалтера и руководителя организации. В небольших организациях функции главного бухгалтера и руководителя может выполнять одно лицо. В этом случае достаточно одной подписи под документом. В системе "ДБО BS-Client v.3" для каждого типа документа клиента в зависимости от его принадлежности к АРМ и организации клиента задается количество подписей, которыми он должен быть подписан:

- требуется одна подпись – обычно для служебных документов (например, произвольные документы в банк);
- требуется две подписи – обычно для финансовых документов;
- подпись под документом не требуется.

> **Внимание**!
>
> Не рекомендуется настраивать систему таким образом, чтобы подпись под документами не требовалась вообще, так как в этом случае нельзя гарантировать *аутентичность* документов. Отсутствие подписи под документом усложнит процедуру разбора конфликтных ситуаций. Более предпочтительным является вариант автоматической подписи документов от имени текущего пользователя (см. разд. «Документарные операции формирования, проверки и снятия подписи» [стр. 44]).

Требуемое количество подписей можно задать различным для разных классов документов. Класс документа в данном контексте определяется:

- для документа клиента – принадлежностью документа документарным схемам (к одной конкретной или ко всем), АРМ (к одному конкретному или ко всем) и организациям клиента (к одной конкретной или ко всем);
- для документа банка – только принадлежностью документа документарным схемам (к одной конкретной или ко всем).

В простейшем случае в системе может быть определен единственный класс – все документы (документы, принадлежащие любой документарной схеме, любому АРМ - банка или клиента, любой организации).

Информация о классах документов содержится и на стороне банка, и на стороне клиентов в служебном справочнике *Количество подписей*. Помимо количества подписей для каждого класса в данном справочнике задается параметр, определяющий возможность подписи документов данного класса ключами *технологических наборов* (см. разд. «Технологические ключевые наборы» [стр. 31]).

Примечание

Значения справочника хранятся в таблице *CryptoNumOfSigns*..

Рассмотрим подробнее, каким образом определяется, каким количеством подписей должен быть подписан тот или иной документ. В процессе выполнения криптографических операций над документом по записям справочника определяется, какому классу документ соответствует больше всего (классы могут пересекаться). В порядке приоритетности проверяется соответствие документа документарной схеме, АРМ и организации клиента, определенных для каждого из классов. Например, если имеется класс документов – платежных поручений любых организаций и класс произвольных документов организации А, то платежное поручение организации А будет отнесено к первому классу, поскольку соответствие документарной схеме является более приоритетным, чем соответствие организации.

После того, как определен класс документа, определяется, каким количеством подписей должны подписываться документы данного класса, и могут ли данные документы быть подписаны ключами технологических наборов. Если документ не может быть отнесен ни к одному из имеющихся классов, требуемое количество подписей для данного документа устанавливается равным 1, при этом подпись данного документа *технологическим ключом* не разрешается.

Примечание

Из данного правила имеется исключение: независимо от значений в справочнике *Количество подписей*, запросы клиентов на регистрацию сертификатов всегда подписываются только одной подписью абонента, сертификат которого запрашивается, при этом допустимо использование технологических ключей.

Настройка записей справочника *Количество подписей*, относящихся к документам клиента, производится в процессе регистрации клиента в системе банка. На стороне клиента результаты настройки доступны только для просмотра, но не для изменения (см. инстр. «Просмотр справочника Количество подписей» [стр. 59]). При необходимости перенастроить количество подписей под документами обратитесь в банк.

В системе "ДБО BS-Client v.3" на уровне криптопрофилей реализовано разграничение прав пользователей на выполнение операций подписи документов. Для криптопрофиля можно указать возможность подписи документов только первой, только второй или единственной подписью. Более подробно права подписи изложены в разд. «Право подписи документов» [стр. 55].

Визирующая подпись

В системе "ДБО BS-Client v.3" реализован механизм визирования платежных поручений. Суть механизма состоит в том, что платежные поручения по определенному списку визируемых счетов не принимаются банком к обработке сразу же после их получения, а требуют предварительного визирования на стороне организации-депозитария клиента. Визирование платежного поручения осуществляется добавлением визирующей подписи к документу.

Визирующая подпись не является эквивалентом собственноручной подписи, так как для правомочности документа, получаемого банком от клиента, необходимо наличие только подписей клиента и банка и не требуется наличия подписи от организации-депозитария. Визирующая подпись выполняет исключительно служебную функцию.

Поставить визирующую подпись можно только при использовании подсистемы *"Интернет-клиент"*.

Подпись документарных квитков

Подпись под *квитками на документ* не проставляется. Однако в системе "ДБО BS-Client v.3" применяется подпись пакетов, посредством которых передаются документы, квитки и прочие данные (см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]). Таким образом, *аутентичность* документарных квитков обеспечивается не их ЭЦП, а ЭЦП содержащих квиток транспортных пакетов.

> **Примечание**
>
> Более подробная информация о квитках и транспортных пакетах приведена в **разд. 1.2, «Цикл приема / отправки документов»** документа *Руководство по использованию. Транспортная подсистема*.

Подпись от имени другого пользователя

При стандартной операции подписи документов (осуществляемой, например, с помощью команды **Подписать** контекстного меню) пользователем, подписывающим документ, является текущий пользователь. Все криптопрофили, сопоставленные текущему пользователю, могут быть использованы при подписи. Однако, в системе "ДБО BS-Client v.3" предусмотрена также возможность подписи документов от имени другого пользователя (команда контекстного меню **Подписать пользователем**). Фактически это означает возможность осуществить подпись посредством любого из криптопрофилей, сопоставленных другому пользователю системы.

Пользователь системы может осуществить подпись чужим криптопрофилем, только если знает пароль пользователя, обладающего данным криптопрофилем, и имеет в доверенном пользовании его ключевой набор.

Примечание

Подробные указания по операциям подписи и подписи пользователем приведены в **разд. 1.9.1, «Подпись документа»** документа *Руководство по использованию. Документы*.

Документарные операции формирования, проверки и снятия подписи

Криптографические операции над документами реализованы в виде *документарных операций* :

- операция подписи – SignNewDoc, имеется у всех документарных схем;
- операции проверки подписи – VerifySign или CheckNewDocAuto, в зависимости от документарной схемы (операция CheckNewDocAuto помимо проверки подписи осуществляется также проверку контролей, см. **док. «Руководство по использованию. Контроли»**);
- операция снятия подписи – ClearSign, имеется у всех документарных схем.

Вызов документарных операций может быть осуществлен как *вручную* – пользователями через графический интерфейс системы (см. **разд. 1.9.1, «Подпись документа»** документа *Руководство по использованию. Документы*), так и *автоматически*. Автоматически запускаются операции, настроенные как *автоматические*, а также операции, вызываемые *автопроцедурами*. Так, например, при стандартных настройках системы подпись рассылаемых клиентам сертификатов осуществляется автоматически, поскольку в соответствующей документарной схеме BankKeyExchange операция SignNewDoc отмечена как автоматическая.

Примечание

Подробная информация по настройке операций и автопроцедур приведена в **док. «Руководство по использованию. Операции и автопроцедуры»**

Автоматическая подпись документов обычно производится от имени пользователя, выполнившего запуск менеджера автопроцедур (точнее, абонента, соответствующего данному пользователю). Однако из данного правила есть исключения (см. разд. 2.3.2, «Криптографические операции над документами» [стр. 40]).

Внимание!

При настройке автоматической подписи документов необходимо убедиться, что пользователи, которым будут доступны операции автоматической подписи, обладают всеми необходимыми правами на подпись документов и могут подписывать документы необходимым количеством подписей (см. разд. 2.4, «Права на выполнение криптографических операций» [стр. 54]). В противном случае операция автоматической подписи будет завершена некорректно (см. далее [стр. 40]).

Подпись документов

Документы в системе "ДБО BS-Client v.3" подписываются с помощью *документарной операции* SignNewDoc, запускаемой на выполнение *вручную* или *автоматически* (см. разд. «Документарные операции формирования, проверки и снятия подписи» [стр. 44]). При подписи вручную возможны два варианта: подписывается один документ или подписываются сразу

несколько документов (*пакетная подпись документов*). При автоматической подписи документы всегда подписываются по одному. В процессе выполнения операции подписи определяется криптопрофиль, которым необходимо подписать документ. В случае подписи одного документа (вручную или автоматически) криптопрофиль для подписи определяется по следующему алгоритму:

1. Определяется пользователь, подписывающий документ. Им является:

   - при стандартной операции подписи документов вручную – текущий пользователь;
   - при подписи вручную от имени другого пользователя – пользователь, выбираемый из списка (см. разд. «Подпись от имени другого пользователя» [стр. 43]);
   - при подписи автопроцедурой или автоматической документарной операцией – пользователь, от имени которого запущен менеджер автопроцедур (см. разд. «Документарные операции формирования, проверки и снятия подписи» [стр. 44]).

   При использовании второго варианта подписи пользователю будет предложено выбрать из списка пользователя, от имени которого он хотел бы подписать документ, и соответствующий ему криптопрофиль, а затем ввести пароль данного пользователя.

   Внимание!

   Есть исключение из описанного выше правила, касающееся документов "Запрос на перегенерацию ключа" (схема GenerateKeyRequest) и "Запросы клиентов на новые сертификаты" (схема ClientKeyExchange). В момент подписи данных документов используется криптопрофиль абонента, сформировавшего запрос, независимо от того, какой пользователь инициировал операцию подписи.

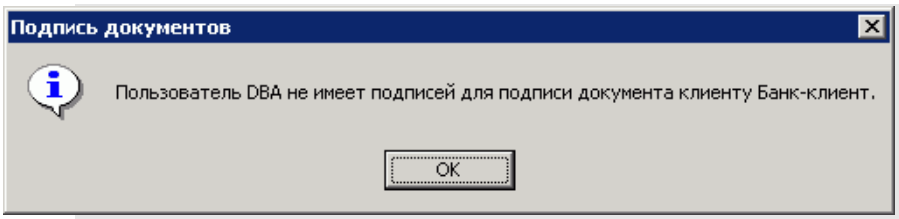
2. Определяется СКЗИ, используемая при подписи передаваемых между АРМ банка и АРМ клиента документов (информация о СКЗИ и на стороне банка, и на стороне клиента содержится в криптопрофилях клиента, на стороне банка клиент определяется по содержимому документов).

3. Среди криптопрофилей пользователя, подписывающего документ, системой отбираются криптопрофили, которыми возможно подписать документ. Ими должны быть:

   - незапрещенные криптопрофили;
   - обладающие соответствующими правами на подпись документов (см. разд. 2.4.1, «Права подписи документов» [стр. 55]).

   Примечание

   Если пользователю, подписывающему документ, не сопоставлено ни одного криптопрофиля, удовлетворяющего указанным условиям, система выведет сообщение об ошибке следующего вида:



4. Если в списке криптопрофилей, подготовленном на предыдущем шаге, содержится более одного криптопрофиля, производится выбор криптопрофиля, который должен быть использовать для подписи.

   - При подписи вручную криптопрофиль выбирается пользователем из предлагаемого системой списка (см. рис. 2.3 [стр. 46]). Отметим, что при выполнении рекомендаций, описанных в разд. «Принадлежность криптопрофиля пользователям» [стр. 28] , список будет содержать только один криптопрофиль, и окно выбора выводится не будет.

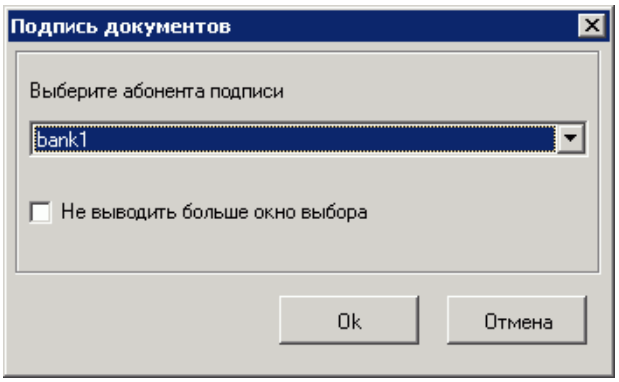


Рис. 2.3. Окно Подпись документов, выбор криптопрофиля из списка

Примечание

- Окно со списком криптопрофилей отображается системой только в случае, когда установлен соответствующий параметр в общих настройках криптозащиты (см. инстр. «Настройка общих параметров выполнения криптографических операций над документами» [стр. 82], поле **Выводить диалог выбора абонента подписи**). Пользователь может сбросить данный параметр и запретить последующий вывод окна непосредственно в самом окне, указав необходимость постоянного использования выбранного им криптопрофиля (см. окно *Подпись документов, выбор криптопрофиля из списка* , поле **Не выводить больше окно выбора**).

- При использовании открытых ключей в виде сертификатов, в зависимости от общих настроек криптозащиты в списке могут выводится либо имена криптопрофилей, либо имена владельцев сертификатов (см. инстр. «Настройка общих параметров выполнения криптографических операций над документами» [стр. 82], поле **Использовать название абонента из сертификата**).

   - При автоматической подписи в зависимости от количества подписей, которое необходимо поставить под документом (см. разд. «Количество подписей под документами» [стр. 41]), выбирается первый или первые два криптопрофиля из списка отобранных криптопрофилей. Таким образом, в автоматическом режиме можно под-

писать документ сразу всеми требуемыми подписями. Если документу не хватает двух подписей, а для подписи доступен только один криптопрофиль, документ будет подписан частично - только первой подписью.

В случае пакетной подписи документов вручную алгоритм определения криптопрофиля для подписи следующий:

1. Определяется пользователь, подписывающий документ, аналогично случаю подписи одного документа (подпись текущим или другим пользователем, см. п. 1 [стр. 45]).

2. Определяются криптопрофили пользователя, подходящие для подписи документов (аналогично п. 3 [стр. 45]). .

3. Если отобрано более одного криптопрофиля, пользователь выбирает криптопрофиль для подписи из списка всех криптопрофилей, определенных на предыдущем шаге (аналогично п. 4 [стр. 46]).

После того, как определен криптопрофиль, которым должен быть подписан документ, производится подпись документа подходящим секретным ключом сопоставленного криптопрофилю активного ключевого набора (см. разд. «Формирование и проверка электронной цифровой подписи в системе "ДБО BS-Client v.3"» [стр. 38]).

Примечание

- Подробное описание указанного действия приведено в прил. А, «Механизм формирования и формат хранения подписи под документами» [стр. 89].
- Возможность подписи документа *технологическими ключами* определяется настройками подсистемы криптозащиты (см. разд. «Технологические ключевые наборы» [стр. 31]).

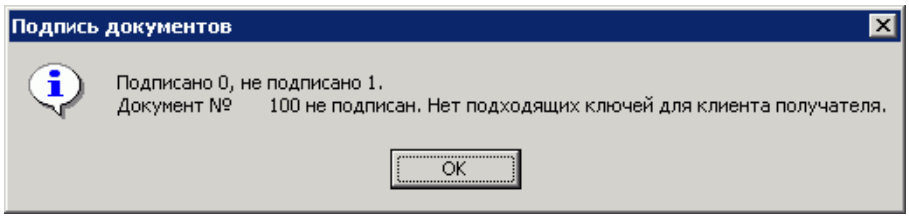
В случае удачного выполнения операции статус документа соответствующим образом изменяется на:

- "подписан" – если под документом проставлены все необходимые подписи;
- "подписан I (ждет II)" – если под документом поставлена только первая подпись (криптопрофиль имеет право только первой подписи), и дополнительно требуется поставить вторую подпись;
- "подписан II (ждет I)" – если под документом поставлена только вторая подпись (криптопрофиль имеет право только второй подписи), и дополнительно требуется поставить первую подпись.

Примечание

Возможность подписи документа различными подписями рассмотрена в разд. «Количество подписей под документами» [стр. 41].

В случае возникновения ошибки доступа к ключам в процессе выполнения операции подписи, система выведет соответствующее сообщение и отменит операцию:



Примечание

При возникновении ошибок в процессе *автоматической* подписи документов сообщения об ошибках не выводятся на экран, а отражаются только в журнале криптографических операций и прочих журналах системы (см. разд. 2.3.4, «Журнал криптографических операций» [стр. 54]).

Проверка подписи под документами

Проверка подписи осуществляется документарными операциями VerifySign или CheckNewDocAuto – в зависимости от документарной схемы. Как и в случае подписи [стр. 44], проверка подписи может быть осуществлена как вручную, так и автоматически (см. разд. «Документарные операции формирования, проверки и снятия подписи» [стр. 44]).

При проверке подписи выполняются следующие действия:

1. По ЭПЦ документа определяются криптопрофиль подписавшего документ абонента и UID использованного секретного ключа подписи.

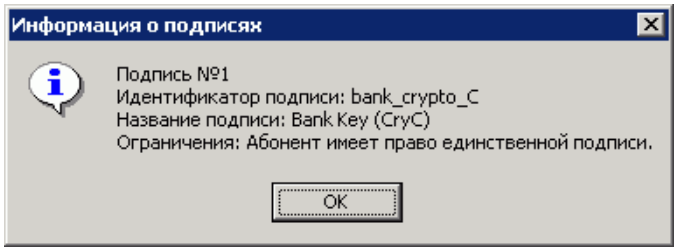
2. Проверяется соответствие ЭЦП содержимому документа (подписанным полям).

   Примечание

   Подробное описание данной проверки приведено в прил. А, «Механизм формирования и формат хранения подписи под документами» [стр. 89].

3. Производится проверка того, что криптопрофиль подписавшего документ абонента не запрещен и обладает соответствующими правами на подпись документов.

По результатам выполнения операции проверки подписи система выводит соответствующее информационное сообщение следующего вида:



Общие условия, при соблюдении которых ЭЦП признается верной, более подробно изложены в разд. «Формирование и проверка электронной цифровой подписи в системе "ДБО BS-Client v.3"» [стр. 38].

Как и операция подписи документов, операция проверки подписи может быть пакетной. При пакетной проверке подписи система последовательно выведет информацию об ЭЦП всех выделенных документов.

Снятие подписи под документами

Подпись под документом можно снять и сделать документ неподписанным. Данная операция снятия подписи необходима в следующих случаях:

- В подписанный документ необходимо внести изменения. Для этого необходимо снять старую подпись, внести изменения и подставить подпись заново.
- Документ подписан ключом, позднее скомпрометированным, причем документ еще не отправлен получателю. В подобной ситуации необходимо переподписать документ, так как документ со скомпрометированной подписью не будет принят принимающей стороной. Для переподписания документа необходимо сначала снять старую подпись, затем поставить новую.

Снять можно как первую, так и вторую подпись или обе сразу (о вариантах подписи см. разд. «Количество подписей под документами» [стр. 41]). Если снимается одна подпись, то имя абонента, подпись которого необходимо снять, выбирается из предлагаемого системой списка:

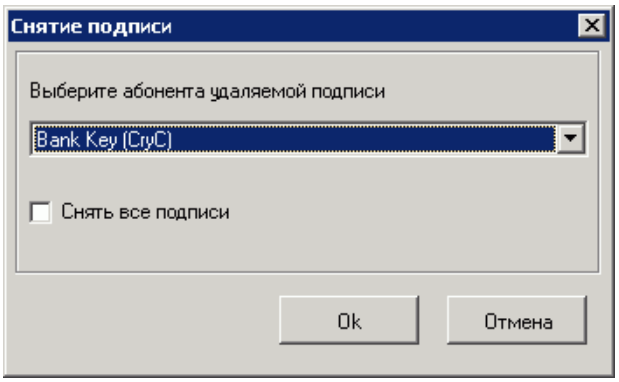


Рис. 2.4. Окно Снятие подписи

Примечание

При использовании открытых ключей в виде сертификатов, в зависимости от общих настроек криптозащиты в списке могут выводится либо имена криптопрофилей, либо имена владельцев сертификатов (см. инстр. «Настройка общих параметров выполнения криптографических операций над документами» [стр. 82], поле **Использовать название абонента из сертификата**).

Как и при подписи, пользователь системы может снять как свою подпись, так и подпись другого абонента, если он знает пароль пользователя, соответствующего этому абоненту (операция *снять подпись пользователем*). При выполнении операции снятия подписи пользователем система предложит выбрать из списка имя абонента (криптопрофиля) и имя соответствующего ему пользователя, а затем ввести пароль.

Примечание

На содержимое указанного списка криптопрофилей влияют общие параметры подсистемы криптозащиты (см. инстр. «Настройка общих параметров выполнения криптографических операций

над документами» [стр. 82]). Для уменьшения размера списка при стандартных настройках системы будут отображаться только разрешенные криптопрофили, имеющие активные ключевые наборы (см. разд. «Статус ключевого набора» [стр. 30] и разд. 2.2.2, «Статус криптопрофиля» [стр. 29]). Если документ подписан криптопрофилем, который впоследствии был запрещен, то для снятия подписи в общих настройках криптозащиты должна быть установлена опция **Показывать запрещенные криптопрофили при снятии подписи**. Если же документ был подписан ключом набора, ставшего впоследствии неактивным, то для снятия подписи должна быть установлена опция **Показывать неактивные сертификаты при снятии подписи**.

При снятии подписи система может проверять не только знание пароля пользователя, но также и наличие ключей, которыми осуществлялась подпись документа. В этом случае при недоступности соответствующего ключевого носителя снятие подписи будет невозможно. Необходимость проверки ключей при снятии подписи, определяется параметром **Проверять доступ к ключам при снятии подписи** (см. инстр. «Настройка общих параметров выполнения криптографических операций над документами» [стр. 82]).

Операция снятия подписи может быть пакетной: снимаются подписи указанного абонента (или все подписи) со всех выделенных документов.

Снятие подписи производится вызовом документарной операции ClearSign. Как и в случае подписи [стр. 44] и проверки подписи [стр. 48], вызов операции может быть произведен вручную или автоматически (см. разд. «Документарные операции формирования, проверки и снятия подписи» [стр. 44]).

2.3.3. Криптографические операции транспортной подсистемы

Внимание!

Общие принципы шифрования и подписи изложены в разд. 1.4, «Базовые криптографические операции» [стр. 16] и разд. 2.3.1, «Общее описание базовых криптографических операций в системе "ДБО BS-Client v.3"» [стр. 36]. Рекомендуется ознакомиться с указанными разделами перед изучением представленной ниже информации.

В рамках подсистемы *"Банк-клиент"* для обмена информацией между двумя АРМ (АРМ банка и АРМ клиента) используется *транспортная подсистема* (см. **док. «Руководство по использованию. Транспортная подсистема»**) . Единицей данных, передаваемых транспортной подсистемой, является *транспортный пакет*. С целью защиты передаваемых данных производится:

- шифрование транспортных пакетов;
- подпись транспортных пакетов.

Примечание

Существует возможность отключить функции шифрования и подписи пакетов (см. инстр. «Настройка параметров, используемых при работе с транспортными пакетами» [стр. 78]). Это может сильно ускорить процесс отправки пакетов, так как операции зашифрования и подписи достаточно трудоемкие. Однако использовать данную возможность не рекомендуется с целью обеспечения безопасности передаваемых данных.

При стандартных настройках подсистемы криптозащиты транспортные пакеты автоматически подписываются и зашифровываются в АРМ-отправителе при отправке пакетов и автоматически расшифровываются и проверяются в АРМ-получателе при получении пакетов. Параметры, определяющие ход криптографических операций над транспортными пакетами, подробно описаны в инстр. «Настройка параметров, используемых при работе с транспортными пакетами» [стр. 78].

Подпись и зашифрование транспортных пакетов

В процессе зашифрования и подписи пакетов на отправляющей стороне производятся следующие действия:

1. Определяется СКЗИ, используемая для защиты передаваемых между АРМ банка и АРМ клиента данных (информация о СКЗИ и на стороне банка, и на стороне клиента содержится в криптопрофилях клиента).

2. Среди криптопрофилей отправляющей стороны выбирается *криптопрофиль абонента-отправителя* – криптопрофиль:

   - соответствующий пользователю, от имени которого запущена транспортная подсистема;

   - обладающий правом на прием / отправку почты (см. разд. 2.4.2, «Право приема / отправки почты» [стр. 58]).

   > **Внимание**!
   >
   > Если пользователю, от имени которого запущена транспортная подсистема, не сопоставлено ни одного криптопрофиля, наделенного правом приема / отправки почты, то при отправке пакетов их подпись и зашифрование не могут быть произведены. При этом, если необходимость подписи и шифрования пакетов указана в настройках системы (см. инстр. «Настройка параметров, используемых при работе с транспортными пакетами» [стр. 78]), то, соответственно, не будет производиться и отправка пакетов.

3. Среди криптопрофилей принимающей стороны выбираются криптопрофили, соответствующие используемой СКЗИ и обладающие правом на прием / отправку почты (криптопрофили *абонентов-получателей*).

4. Определяется необходимость зашифрования и подписи транспортных пакетов. Зашифрование производится в случае соблюдения следующих условий:

   - список криптопрофилей абонентов-получателей, полученный на предыдущем шаге, не пуст;

   - включена опция шифрования транспортных пакетов (см. инстр. «Настройка параметров, используемых при работе с транспортными пакетами» [стр. 78], поле **Шифровать пакеты**).

   Подпись пакетов производится при соблюдении следующих условий:

   - список криптопрофилей абонентов-получателей не пуст;

- включена опция подписи и проверки подписи транспортных пакетов (см. инстр. «Настройка параметров, используемых при работе с транспортными пакетами» [стр. 78], поле **Подписывать пакеты**).

5. Определяется возможность отправки пакетов. Если включена опция подписи и проверки подписи пакетов, но при этом список криптопрофилей абонентов-получателей пуст, то пакеты будут отправлены (неподписанными и незашифрованными) только тогда, когда дополнительно включена опция **Отправка пакетов неподписанными, если клиенту-получателю не задана подпись** (см. инстр. «Настройка параметров, используемых при работе с транспортными пакетами» [стр. 78]). В остальных случаях на отправку пакетов не налагается дополнительных ограничений. Например, если включена опция шифрования пакетов, и при этом упоминаемый список криптопрофилей пуст, пакеты будут отправлены незашифрованными без необходимости установки каких-либо дополнительных опций.

   Примечание

   Таким образом, возможна ситуация, при которой пакеты будут отправлены, но при этом не будут подписаны и / или зашифрованы. Не следует допускать подобной ситуации, необходимо позаботиться о наличии всех необходимых криптопрофилей и о правильной настройке параметров криптозащиты.

6. Если определена необходимость подписи пакетов, пакеты подписываются секретным ключом *активного* ключевого набора из криптопрофиля абонента-отправителя. Затем, если определена необходимость зашифрования пакетов, пакеты зашифровываются на всех абонентов-получателей их открытыми ключами из того же ключевого набора криптопрофиля абонента-отправителя. Более подробное описание процессов зашифрования и подписи приведено в разд. 1.4, «Базовые криптографические операции» [стр. 16] и разд. 2.3.1, «Общее описание базовых криптографических операций в системе "ДБО BS-Client v.3"» [стр. 36].

   Примечание

   - Если в процессе подписи пакетов возникли ошибки подписи, то отправка пакетов будет произведена только в случае, если включена опция **Отправка пакетов при ошибках подписи** (см. инстр. «Настройка параметров, используемых при работе с транспортными пакетами» [стр. 78]).
   - Допустимы подпись и зашифрование пакетов как рабочими, так и технологическими ключами (см. разд. «Технологические ключевые наборы» [стр. 31]).

Для сокращения объема транспортных пакетов в системе предусмотрена возможность их сжатия с помощью встроенного архиватора, работающего по алгоритму ZIP. Сжатие производится после выполнения операций подписи и зашифрования, если включена соответствующая опция (см. инстр. «Настройка параметров, используемых при работе с транспортными пакетами» [стр. 78], поле **Сжатие данных**). Возможно также сжатие незашифрованных транспортных пакетов для случая, когда список криптопрофилей абонентов-получателей пуст (поле **Сжимать незашифрованные данные**).

Подготовленные к отправке (подписанные, зашифрованные и сжатые) транспортные пакеты отправляются транспортной подсистемой принимающей стороне.

Расшифрование и проверка транспортных пакетов

Получателем зашифрованного и подписанного транспортного пакета может быть любой абонент (криптопрофиль) АРМ-получателя, обладающий правом на прием / отправку почты. Конкретный криптопрофиль, который будет использован для расшифрования и проверки подписи пакетов, (конкретный абонент-получатель) определяется на принимающей стороне в момент приема пакетов. Им является криптопрофиль, соответствующий пользователю, от чьего имени запущена транспортная подсистема .

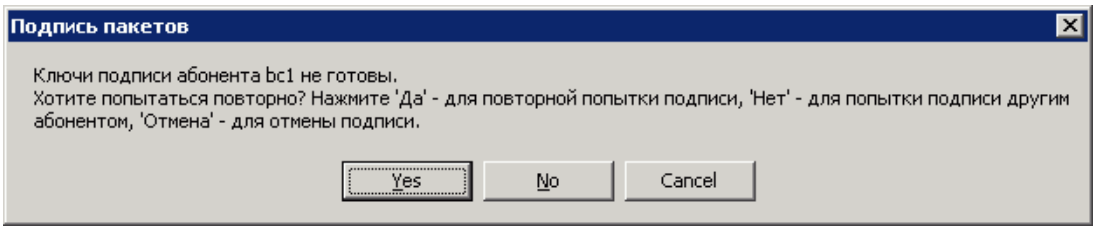
При получении пакетов на принимающей стороне при необходимости последовательно выполняются операции распаковки сжатых данных, расшифрования и проверки подписи (см. разд. 2.3.1, «Общее описание базовых криптографических операций в системе "ДБО BS-Client v.3"» [стр. 36]). Если пакет расшифровать не удалось пакет помечается как *ошибочный* и к дальнейшей обработке не допускается. Также пакет помечается как ошибочный, если подпись пакета неверна или ее не удалось проверить, и при этом отключена опция **Прием пакетов при ошибках проверки подписи** (см. инстр. «Настройка параметров, используемых при работе с транспортными пакетами» [стр. 78]).

Внимание!

Если в момент получения транспортных пакетов окажется, что крипропрофиль абонента-получателя запрещен или не обладает правом на прием / отправку почты, то полученные пакеты не смогут быть расшифрованы и проверены, будут помечены как ошибочные и не будут допущены к дальнейшей обработке. Поэтому и в АРМ-отправителе, и в АРМ-получателе все криптопрофили пользователя, от имени которого производится запуск транспортной подсистемы, должны обязательно обладать правом приема / отправки почты.

Ошибки, возникающие при выполнении криптографических операций транспортной подсистемы

Если при выполнении криптографических операций не удастся получить доступ к ключам шифрования или ключам подписи, то при используемых по умолчанию настройках системы будет выведен диалог следующего вида (приведен диалог для операции подписи):



С помощью данного диалога можно осуществить повторную попытку выполнения криптографической операции, выбрать другой криптопрофиль криптопрофиль для операции или отменить операцию. Необходимость вывода данного диалога системой определяется общими настройками криптозащиты (см. инстр. «Настройка параметров, используемых при работе с транспортными пакетами» [стр. 78]). Если в соответствии с настройками данный диалог не выводится, сообщения об ошибках отражаются только в журналах системы: журнале криптографических операций, журнале транспортной подсистемы и общем журнале системы (см. разд. 2.3.4, «Журнал криптографических операций» [стр. 54]).

2.3.4. Журнал криптографических операций

Ход выполнения криптографических операций отражается в соответствующем журнале. Файлы журнала (`*.log`) располагаются в каталоге `%BSSRoot%\Subsys\Logs\Crypto`, где `%BSSRoot%` – каталог, куда установлена система..

> **Примечание**
>
> Ошибки в ходе выполнения криптографических операций также могут отражаться (с меньшей степенью детализации) в общем журнале системы (`%BSSRoot%\error.log`), журнале транспортной подсистемы (`%BSSRoot%\SUBSYS\Logs\Transp\*.log`) и журнале документарных операций .

При формировании журналов возможны два уровня детализации сохраняемой в журналах информации. Степень детализации информации для различных групп операций задается общими настройками криптозащиты (см. инстр. «Настройка общих параметров криптозащиты» [стр. 77]):

- для криптографических операций над транспортными пакетами – параметром **Расширенный лог** (см. инстр. «Настройка параметров, используемых при работе с транспортными пакетами» [стр. 78]);
- для криптографических операций над документами – параметром **Детализация ошибок подписи / проверки подписи** (см. инстр. «Настройка механизма формирования и проверки подписи под документами» [стр. 86]).

> **Внимание**!
>
> При штатной работе системы не рекомендуется устанавливать высокую степень детализации сохраняемой в журналах информации, так как в этом случае существенно возрастает объем файлов журналов и замедляется работа системы.

2.4. Права на выполнение криптографических операций

Права криптопрофилей определяют криптографические операции, которые могут быть выполнены посредством криптопрофилей, и классы объектов, над которыми возможно выполнение данных операций.

> **Примечание**
>
> Подробная информация по криптопрофилям приведена в разд. 2.2, « Криптографические профили » [стр. 26], а по криптографическим операциям - в разд. 2.3, «Криптографические операции в системе "ДБО BS-Client v.3"» [стр. 36].

Каждый криптопрофиль (абонент) может обладать следующими правами:

- Права подписи документов [стр. 55].
- Право приема / отправки почты [стр. 58].

- Право защиты канала [стр. 58].

Каждое право наделяет абонента возможностью совершать определенные криптографические операции в рамках одного АРМ. Так право подписи позволяет подписывать документы АРМ, к которому принадлежит криптопрофиль, а право приема / отправки почты - выполнять криптографические операции над *транспортными пакетами*, пересылаемыми между АРМ криптопрофиля и АРМ, с которым осуществляется обмен данными. Возможна ситуация, когда криптопрофиль используется несколькими АРМ. В этом случае для каждого АРМ, к которому относится криптопрофиль, права криптопрофиля настраиваются отдельно.

Примечание

Возможность использования криптопрофиля несколькими АРМ может потребоваться, например, клиентам банка, являющимся холдингами (см. разд. «Принадлежность криптопрофиля АРМ и организациям» [стр. 27]).

Права криптопрофиля задаются в процессе его создания на стороне банка и в дальнейшем могут быть изменены в соответствии с указаниями банка (см. разд. «Выбор АРМ и задание прав криптопрофиля» [стр. 67]). Подробная информация об этапах жизненного цикла криптопрофилей приведена в разд. 3.3, «Работа с криптопрофилями» [стр. 64].

2.4.1. Права подписи документов

Каждый документ может быть подписан одной или несколькими подписями. Количество подписей под документом в зависимости от его типа и его принадлежности к АРМ и организациям определяется настройками системы (см. разд. «Количество подписей под документами» [стр. 41]).

Права на создание, редактирование и удаление документа для пользователя задаются в его профиле (см. **разд. 2.4, «Настройка профиля пользователя»** документа *Руководство по использованию. Разграничение доступа*). По аналогии права на подпись [стр. 44] документов задаются в криптопрофиле пользователя. Для выполнения операций проверки [стр. 48] и снятия [стр. 49] подписи задавать какие-либо дополнительные права криптопрофилей не нужно, криптопрофилю достаточно иметь активные ключевые наборы и не быть запрещенным (см. разд. «Формирование и проверка электронной цифровой подписи в системе "ДБО BS-Client v.3"» [стр. 38]).

Права на подпись документов определяют для криптопрофиля класс документов, которые могут быть подписаны криптопрофилем, и количество и вид допустимых подписей. В простейшем случае криптопрофиль наделяется возможностью формирования заданного вида подписей под всеми документами АРМ (см. разд. «Право подписи документов» [стр. 55]). Возможен более сложный случай, когда права криптопрофиля на подпись документов задаются отдельно для каждого требуемого класса документов АРМ (см. разд. «Расширенные права подписи документов» [стр. 56]). Дополнительно имеется возможность задать права криптопрофиля на осуществление визирующей подписи под документами (см. разд. «Право визирующей подписи документов» [стр. 58]).

Право подписи документов

Право подписи документов наделяет абонента (криптопрофиль) возможностью подписывать документы:

- первой подписью;
- второй подписью;
- единственной подписью.

Рассмотрим возможности подписи документов, требующих наличия двух подписей, для абонентов с различными правами:

- Абонент, наделенный правом первой подписи, может подписывать документ первой подписью, если первая подпись под документом еще не поставлена. При этом, данный абонент не может поставить вторую подпись под документом. Пример: главный бухгалтер организации клиента, осуществляет первую подпись, но не может подписать документ и за себя, и за руководителя организации.
- Абонент, наделенный правом второй подписи, может поставить вторую подпись под документом, если ее еще нет, и не может подписать документ первой подписью.
- Абонент, обладающий правом единственной подписи может подписать документы, требующие наличия двух подписей (сразу обоими подписями). Пример: руководитель организации может подписать документ, даже не имеющий подписи главного бухгалтера.

Порядок подписи документа (сначала первой подписью, затем второй или наоборот) системой "ДБО BS-Client v.3" не регламентируется, он может быть произвольным.

В случае, когда документ требует наличия только одной подписи, все указанные абоненты обладают возможностью подписи документа в равной степени .

> **Примечание**
>
> Принципы задания количества подписей под документами изложены в разд. «Количество подписей под документами» [стр. 41].

Система "ДБО BS-Client v.3" предоставляет две возможности задания прав криптопрофиля на подпись документов:

- задание единого права криптопрофиля на подпись всех документов АРМ;
- задание для каждого требуемого класса документов АРМ права криптопрофиля на подпись документов данного класса (*расширенные права подписи документов*).

Более подробно расширенные права подписи рассмотрены в следующем разделе [стр. 56].

Расширенные права подписи документов

Документы клиентов преимущественно являются финансовыми и содержат указания банку на выполнение тех или иных финансовых операций. Для обеспечения *аутентичности* таких документов они обязательно должы быть подписаны. При этом зачастую требуется разграничить возможность подписи документов для сотрудников организаций клиента в соответствии с их принадлежностью той или иной организации и занимаемой должности, в соответствии с типом и содержимым документов и т.д. С этой целью система "ДБО BS-Client v.3" позволяет задавать для абонентов (криптопрофилей) клиентов *расширенные права под-*

писи – права криптопрофилей на подпись документов по отдельности для каждого требуемого класса документов АРМ. Классы документов в данном контексте определяются:

- типом документов (*документарной схемой*);
- принадлежностью документов организациям;
- ограничениями на содержимое документов.

Для каждого заданного класса указывается вид подписи (первая, вторая, единственная), доступной криптопрофилю для документов данного класса. При этом, можно задавать не только классы документов, которые могут подписаны криптопрофилем, но и классы документов, которые не могут быть им подписаны.

> Принципы работы системы с классами документов аналогичны принципам, изложенным в разд. «Количество подписей под документами» [стр. 41]. Если классы пересекаются, то для определения принадлежности документа классу для каждого класса проверяется в порядке приоритетности принадлежность документа документарной схеме, принадлежность организации и соответствие содержимого ограничениям, заданным для класса. Если документ не принадлежит ни одному классу, то подпись документа данным криптопрофилем не допускается.

Пример задания расширенных прав подписи: холдинг из двух организаций, у которых два генеральных директора, один главный бухгалтер и одно АРМ. Допустим, генеральный директор первой организации должен иметь право второй подписи документов первой организации и не иметь прав подписи документов второй организации. В этом случае для него в соответствии с перечисленными правами и ограничениями настраивается криптопрофиль с расширенными правами подписи. Для бухгалтера настраивается криптопрофиль без расширенных прав подписи, но с правом первой подписи любых документов АРМ.

На содержимое документов, относимых к тому или иному классу, можно налагать ограничения двух видов:

- встроенные ограничения, проверяемые средствами системы "ДБО BS-Client v.3";
- ограничения, проверяемые внешними по отношению к системе "ДБО BS-Client v.3" модулями.

К первому виду ограничений относится ограничение на сумму платежных поручений. Благодаря наличию данного вида ограничений можно, например, запретить абоненту подписывать документы, сумма которых превышает некоторое значение.

Допустим, необходимо предоставить сотруднику возможность подписывать любые документы, кроме платежных поручений на сумму, превышающую 5000 рублей. Самый простой способ сделать это – назначить криптопрофилю сотрудника расширенные права на подпись для документов следующих классов:

- для любых документов – право подписи первой, второй или единственной подписью;
- для платежных поручений на сумму, превышающую 5000 рублей – нет права подписи.

Указанные классы пересекаются (второй класс является подмножеством первого), но в силу того, что при определении соответствия документа классу прежде всего в расчет принимается

тип документа (документарная схема), криптопрофиль с указанными расширенными правами будет удовлетворять заданным требованиям.

Право визирующей подписи документов

Если используется механизм визирования платежных поручений (см. разд. «Визирующая подпись» [стр. 43]), то необходимо задать абонентов, обладающих правом визирующей подписи документов. Пользователям с криптопрофилями, наделенными данным правом, доступны следующие возможности:

- просмотр платежных поручений, требующих визирования;
- визирование платежных поручений;
- отказ в визировании платежных поручений.

Прочим пользователям системы "ДБО BS-Client v.3" указанные действия недоступны.

Примечание

- Указанные действия реализованы только для пользователей подсистемы *"Интернет-клиент"* .
- В рамках одного АРМ все абоненты, получившие право визирующей подписи, имеют равные возможности просмотра, визирования и отказа в визировании.

2.4.2. Право приема / отправки почты

Право приема / отправки почты наделяет абонента (криптопрофиль) возможностью выполнять от своего имени криптографические операции *транспортной подсистемы "Банк-клиент"*: (см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]).

2.4.3. Право защиты канала

Право защиты канала наделяет абонента (криптопрофиль) возможностью выполнять от своего имени криптографические операции компонентов подсистемы "Интернет-клиент" ..

Глава 3. Инструкции администратора

3.1. Просмотр справочника Количество подписей

Документы, в зависимости от их типа (*документарной схемы*) и источника (банк / клиент), требуют подписания разным количеством подписей (см. разд. «Количество подписей под документами» [стр. 41]). Для просмотра установленного в системе количества подписей под документами выполните следующие действия:

1. Выполните команду меню **Настройки → Криптозащита → Количество подписей в документах**. Произойдет переход в окно **Количество подписей [1]**.

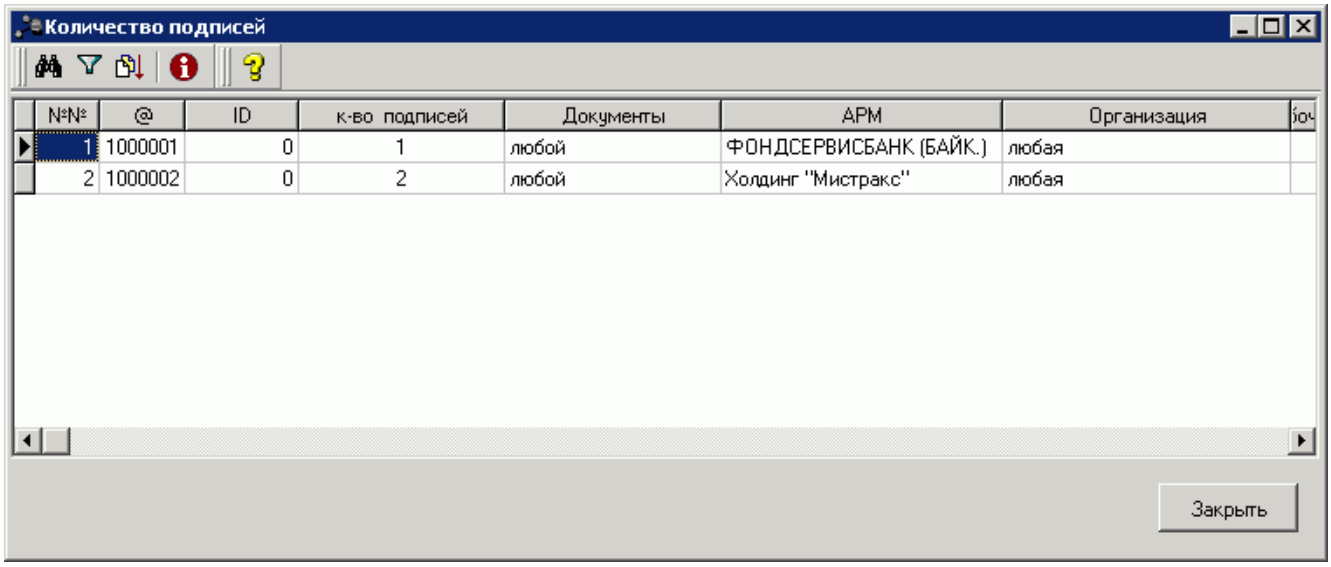


Рис. 3.1. Окно Количество подписей [1]

В скроллере будут представлены записи, отображающие установленное количество подписей в привязке к различным типам документов, организациям и АРМам.

2. При необходимости Вы можете отобразить каждую из записей в специальном окне просмотра. Для этого дважды щелкните левой кнопкой мыши на записи. Произойдет переход в окно ????.

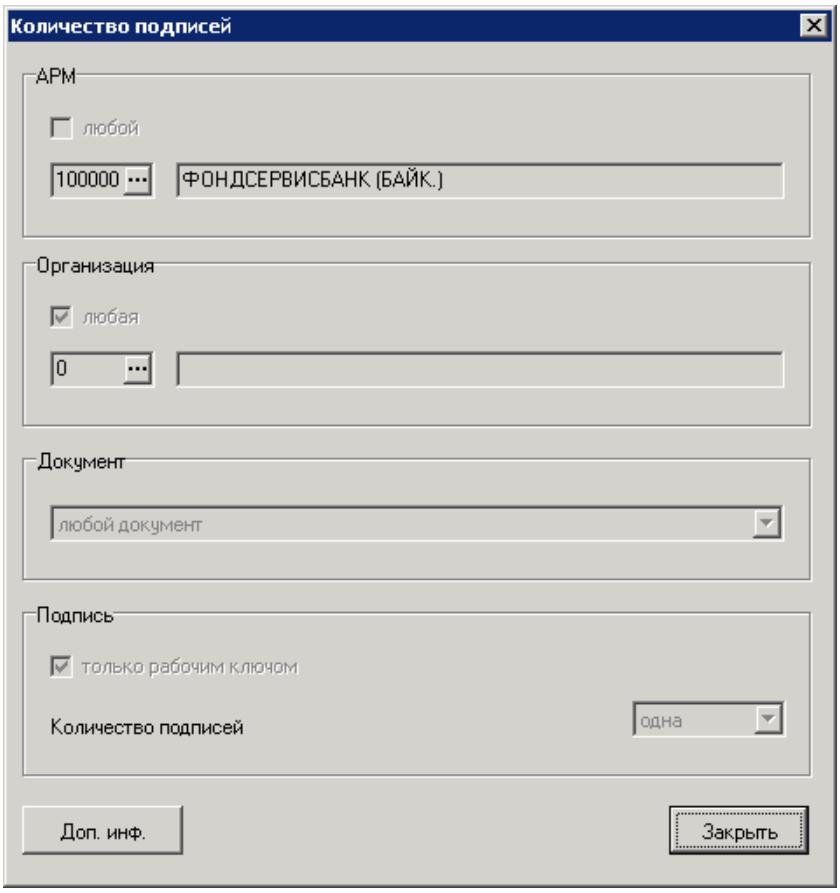


Рис. 3.2. Окно Количество подписей [2]

При необходимости изменить установленное количество подписей под документами обратитесь в банк.

3.2. Генерация ключей / запросов на сертификаты

3.2.1. Генерация ключей / запросов на сертификаты средствами системы "ДБО BS-Client v.3"

Данная инструкция описывает процесс генерации секретного и открытого ключей или секретного ключа и запроса на сертификат средствами системы "ДБО BS-Client v.3".

Для генерации ключей / запросов на сертификаты выполните следующие действия:

1. Выберите команду меню **Администрирование → Криптозащита → Ручная генерация сертификата**. Произойдет переход в окно **Генерация запроса на сертификат и секретного ключа [1]**.

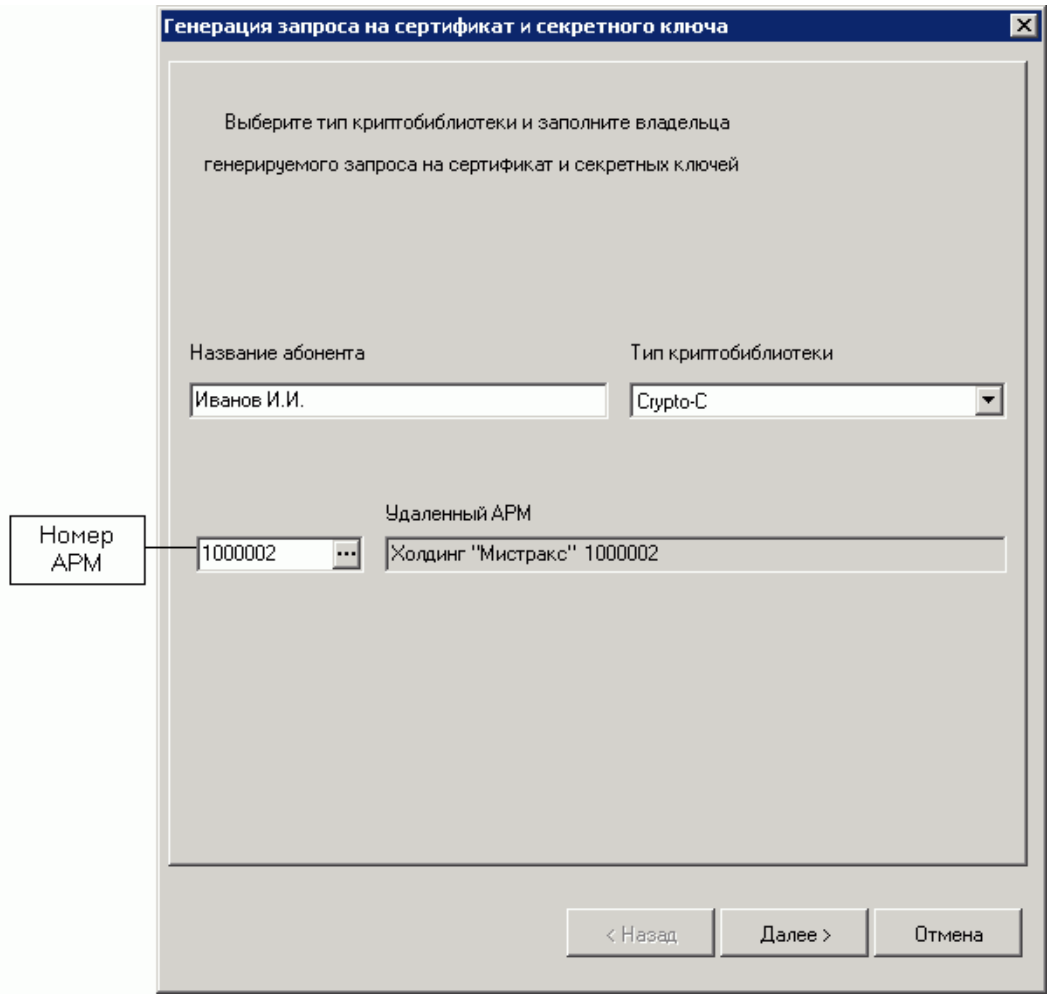


Рис. 3.3. Окно Генерация запроса на сертификат и секретного ключа [1]

2. Заполните поле **Название абонента**. В качестве названия абонента могут быть использованы:

   - фамилия и инициалы соответствующего пользователя в том случае, если каждый пользователь системы является отдельным абонентом;
   - обозначение группы пользователей, если генерируемые ключи должны использоваться группой пользователей;
   - любая другая последовательность символов.

   Рекомендуется использовать первый вариант (более подробные рекомендации приведены в разд. «Принадлежность криптопрофиля пользователям» [стр. 28]).

   Примечание

   Название абонента будет отражено в акте признания новых ключей (см. ниже). Если при генерации будет использована сертификатная СКЗИ, то название абонента будет помещено в запрос на сертификат, а после формирования сертификата в ЦС – в поле Common Name сертификата. Наличие данного поля в сертификате предписывается стандартом *X.509* (см. разд. «Инфраструктура открытых ключей (PKI)» [стр. 13]).

3. Выберите *СКЗИ*, с помощью которой должна осуществляться генерация, в поле **Тип криптобиблиотеки**.

4. В поле **Номер АРМ** выберите АРМ, к которому должны относится генерируемые ключи. Выбор АРМ осуществляется с помощью служебного справочника *Список АРМ* .

5. Нажмите на кнопку **Далее**. Произойдет переход в окно задания параметров генерации, вид которого определяется значением, введенным в поле **Тип криптобиблиотеки**. Внешний вид и состав полей окон для различных СКЗИ приведен в прил. В, «Интерфейс задания параметров процедуры генерации ключей / запросов на сертификат» [стр. 97].

6. Заполните поля окна параметрами генерации ключей / запроса на сертификат в соответствии с прил. В, «Интерфейс задания параметров процедуры генерации ключей / запросов на сертификат» [стр. 97] и нажмите кнопку **Далее**.

7. Произойдет переход в закладку **Окно Генерация запроса на сертификат и секретного ключа [2]**.

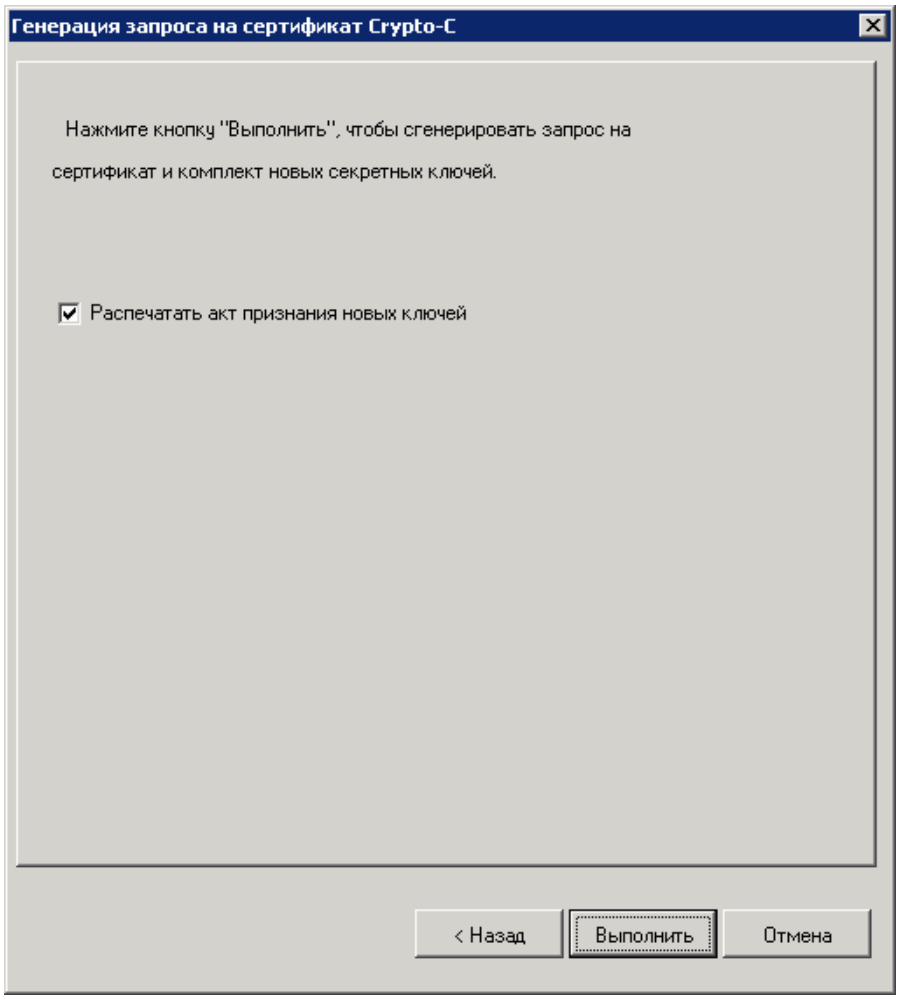


Рис. 3.4. Окно Генерация запроса на сертификат и секретного ключа [2]

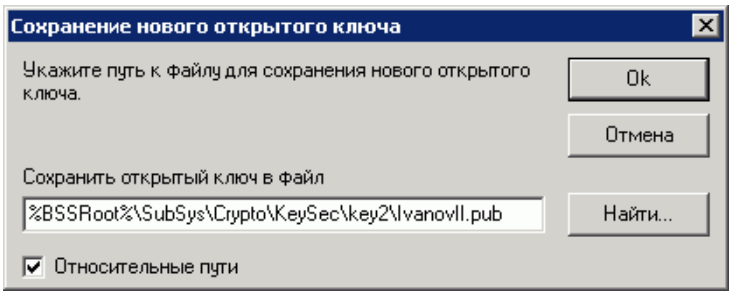
Примечание

Заголовок окна может меняться в зависимости от СКЗИ, используемой в процессе генерации секретного и открытого ключей / секретного ключа и запроса на сертификат.

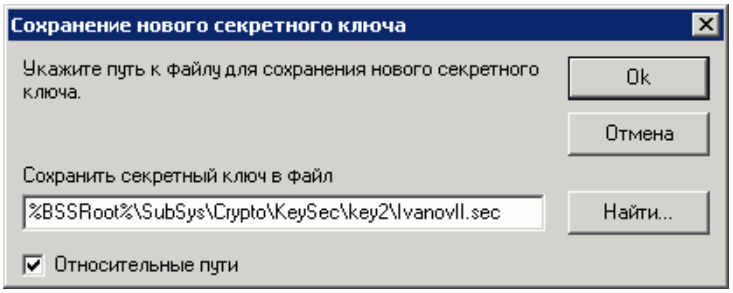
8. Снимите заполнение поля **Распечатать акт признания новых ключей** (в системах клиентов необходимость в печати акта признания новых ключей отсутствует).

9. Нажмите кнопку **Выполнить**. Будет запущена процедура генерации ключевой пары или секретного ключа и запроса на сертификат (в зависимости от указанной СКЗИ).

   В процессе генерации система выведет диалог сохранения нового открытого ключа / запроса на сертификат:



10. Введите имя файла генерируемого открытого ключа / запроса на сертификат и нажмите кнопку **Ok**. Система выведет диалог сохранения нового секретного ключа:



11. Введите имя файла генерируемого секретного ключа и нажмите кнопку **Ok**.

Примечание

По умолчанию система предлагает сохранить файлы в каталоге `%BSSRoot%\SubSys\Crypto\KeySec\key2\`, где `%BSSRoot%` – каталог, куда установлена система "ДБО BS-Client v.3". Основная часть имен файлов формируется по *UID* генерируемой ключевой пары, задаваемому при выполнении п. 6 [стр. 62]. Расширения имен файлов зависят от используемой СКЗИ.

12. В появившемся окне системы "ДБО BS-Client v.3" нажмите кнопку **Готово**.

После выполнения инструкции будут сгенерированы:

- секретный и открытый ключи – при использовании несертификатных СКЗИ;

- секретный ключ и запрос на сертификат – при использовании сертификатных СКЗИ.

В последнем случае полученный запрос на сертификат необходимо обработать в *ЦС*, соответствующем используемой СКЗИ, для формирования конечного сертификата.

3.3. Работа с криптопрофилями

3.3.1. Настройка криптопрофилей с помощью мастера настройки абонентов СКЗИ

Мастер настройки абонентов СКЗИ предоставляет удобный способ выполнения операций над криптопрофилями:

- Редактирование криптопрофиля (Мастер настройки абонентов СКЗИ) [стр. 64].
- Настройка принадлежности криптопрофилей пользователям (Мастер настройки абонентов СКЗИ) [стр. 73].

> **Примечание**
>
> Операции создания и экспорта криптопрофилей доступны только в системе банка.

Часть из перечисленных операций (импорт криптопрофилей) можно выполнить только с помощью мастера настройки абонентов СКЗИ. Кроме того, только с помощью данного мастера можно задать принадлежность криптопрофиля подразделению банка.

Вызов мастера настройки абонентов СКЗИ осуществляется выбором команды меню **Администрирование → Криптозащита → Мастер настройки абонентов СКЗИ** .

Редактирование криптопрофиля (Мастер настройки абонентов СКЗИ)

Для редактирования существующего криптопрофиля выполните следующие действия:

1. Вызовите мастер настройки абонентов СКЗИ выбором команды меню **Администрирование → Криптозащита → Мастер настройки абонентов СКЗИ** . Произойдет переход в окно **Мастер настройки криптозащиты**.

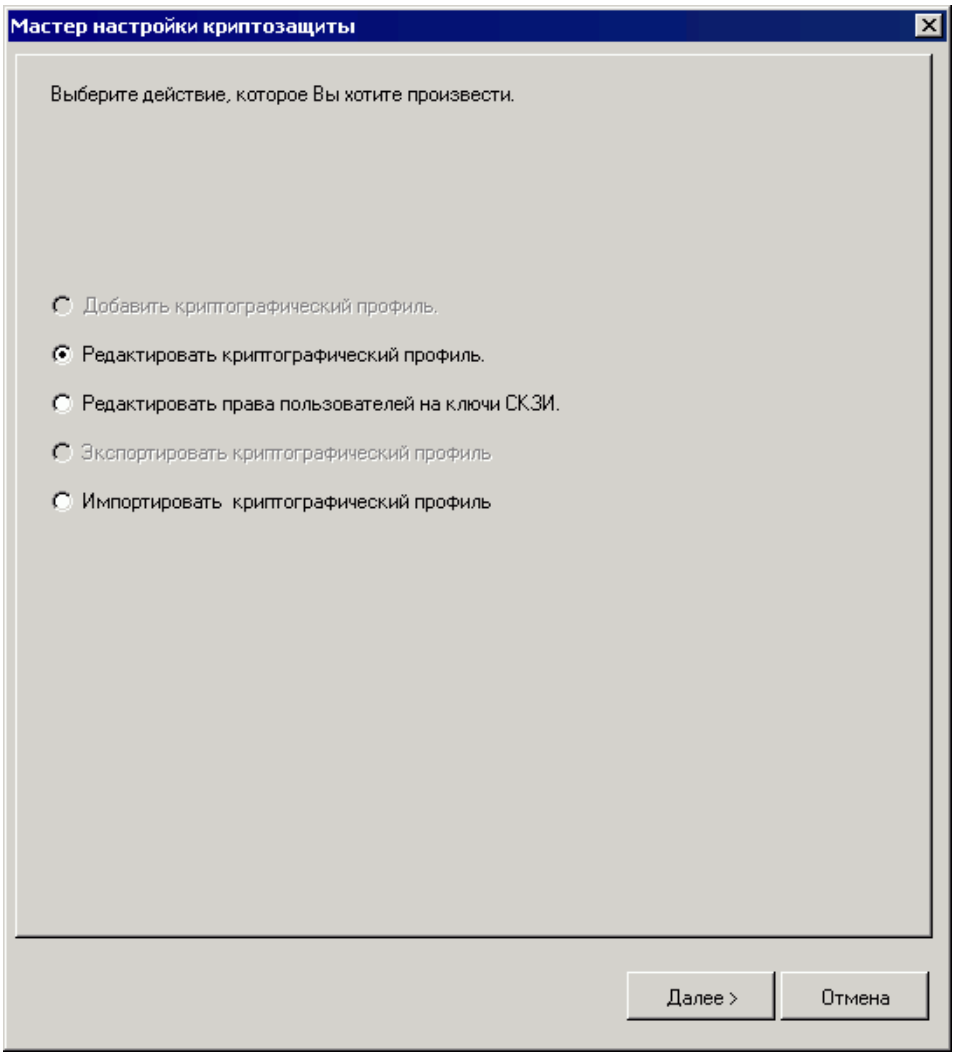


Рис. 3.5. Окно Мастер настройки криптозащиты, закладка Выбор операции

2. Выберите пункт **Редактировать криптографический профиль** и нажмите кнопку **Далее**. Произойдет переход к закладке **Редактирование базовых сведений**. Следуйте указаниям, приведенным в инстр. «Редактирование базовых сведений о криптопрофиле» [стр. 65].

Редактирование базовых сведений о криптопрофиле

> **Внимание**!
>
> Во избежание отказа в обслуживании редактирование базовых сведений о криптопрофилях рекомендуется производить только по согласованию с банком.

Редактирование базовых сведений о криптопрофилях клиента может потребоваться в основном в следующих случаях:

- ключи криптопрофиля были компрометированы (необходимо запрещение криптопрофиля и на стороне банка, и на стороне клиента);
- криптопрофиль клиента был прикреплен к подразделению банка, в котором производилось обслуживание организации клиента, однако в последующем обслуживание органи-

зации стало осуществляться в нескольких подразделениях банка (криптопрофиль не должен быть прикреплен ни к одному подразделению).

> **Внимание**!
>
> Во избежание отказа в обслуживании редактирование базовых сведений о криптопрофилях клиента должно производится согласованно на стороне банка и на стороне клиента.

Редактирование базовых сведений о криптопрофиле осуществляется в закладке **Редактирование базовых сведений** окна **Мастер настройки криптозащиты**.

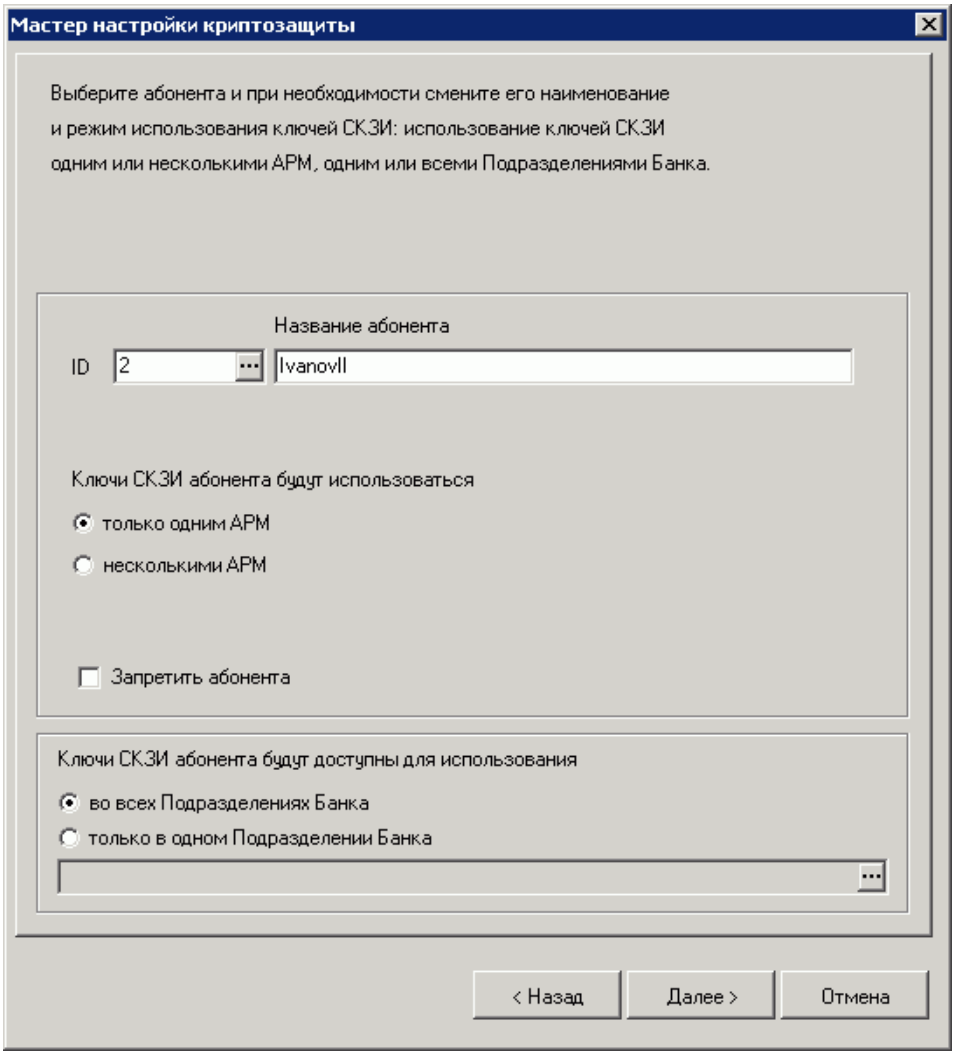


Рис. 3.6. Окно Мастер настройки криптозащиты с закладкой Редактирование базовых сведений

Для редактирования базовых сведений о криптопрофиле выполните следующие действия:

1. С помощью поля **ID** выберите криптопрофиль, данные которого необходимо отредактировать. Выбор криптопрофиля осуществляется посредством *справочника криптографических профилей*. После выбора криптопрофиля в поле будет отображен идентификатор криптопрофиля в системе.

2. При необходимости измените название криптопрофиля. Название криптопрофиля несет чисто информационную нагрузку и может отличаться от имени владельца ключей и

UID ключей, которые будут сопоставлены криптопрофилю. Изменение названия криптопрофиля не влияет на криптографические процессы.

3. Значение блока выбора **Ключи СКЗИ абонента будут использоваться** оставьте без изменений.

4. Если необходимо полностью запретить использование криптопрофиля для выполнения криптографических операций, заполните поле **Запретить абонента**. Запрещение криптопрофиля может потребоваться в случае компрометации ключей, сопоставленных криптопрофилю (см. разд. 1.3.6, «Компрометация ключевых наборов» [стр. 12]).

   Внимание!

   В случае компрометации недостаточно запрещения криптопрофиля на стороне клиента. Необходимо также обратиться в банк для запрещения криптопрофиля и на стороне банка.

5. Нажмите кнопку **Далее**.

После выполнения указанных действий произойдет переход к закладке **Права**. Выполните действия, описанные в инстр. «Выбор АРМ и задание прав криптопрофиля» [стр. 67].

Выбор АРМ и задание прав криптопрофиля

Выбор АРМ, которому или которым должен принадлежать криптопрофиль, и задание прав криптопрофиля на выполнение криптографических операций производится на стороне банка. На стороне клиента имеется возможность выполнения данных действий, однако без синхронного выполнения аналогичных действий на стороне банка внесение изменений на стороне клиента не имеет смысла. Поэтому в рамках данной инструкции все, что требуется выполнить на стороне клиента - оставить без изменения настройки прав криптопрофиля, установленные на банке. Выполните следующие действия:

1. Оставьте без изменения значения полей закладок, содержащих настройки прав криптопрофиля. Несколько раз нажмите кнопку **Далее** для перехода к закладке **Пользователи криптопрофиля**.

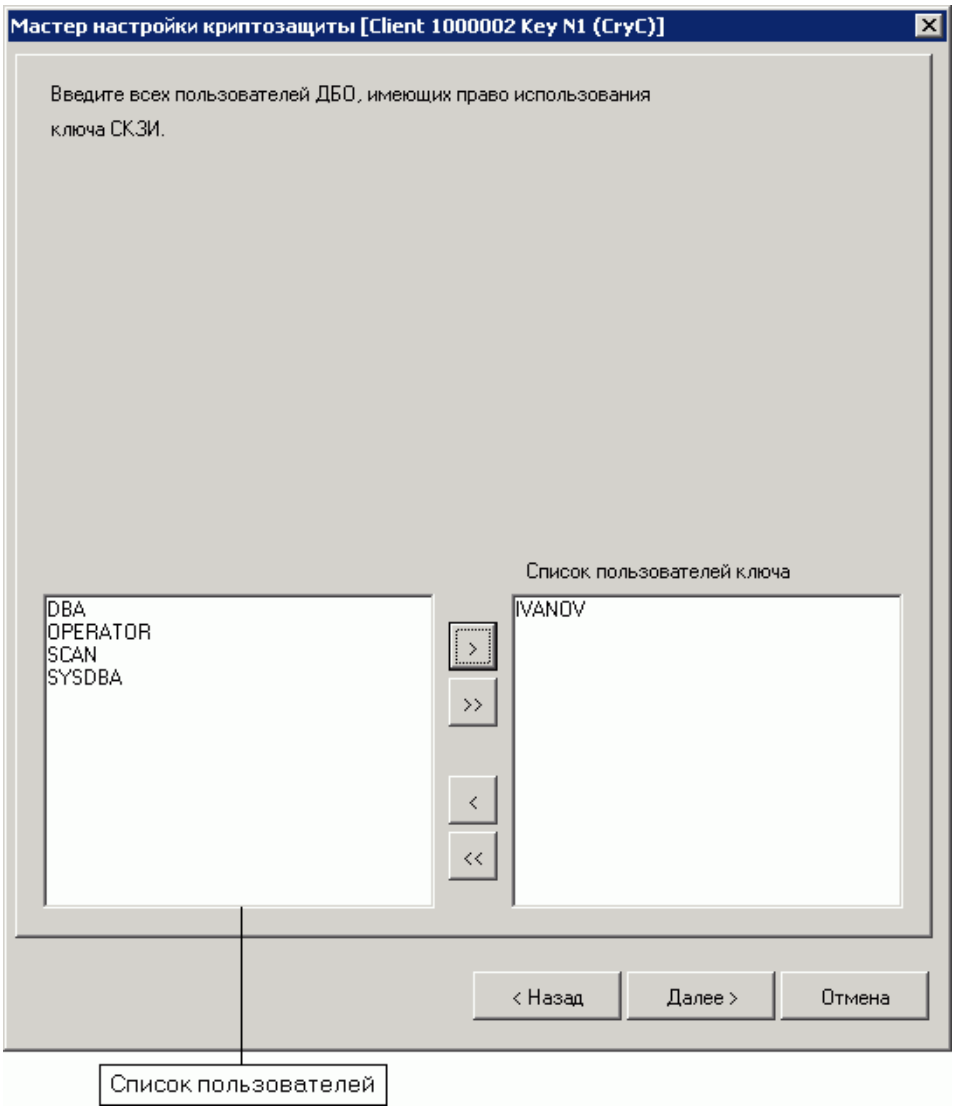


Рис. 3.7. Окно Мастер настройки криптозащиты с закладкой Пользователи криптопрофиля

2. Перейдите к выполнению инстр. «Задание принадлежности криптопрофиля пользователям» [стр. 69].

Примечание

Настройка прав криптопрофиля осуществляется в следующих закладках:

- **Права** - переход в данную закладку осуществляется после выполнения инстр. «Редактирование базовых сведений о криптопрофиле» [стр. 65], если в базовых сведениях о криптопрофиле была указана принадлежность криптопрофиля одному АРМ;
- **Выбор АРМ** - переход в данную закладку осуществляется после выполнения инстр. «Редактирование базовых сведений о криптопрофиле» [стр. 65], если в базовых сведениях о криптопрофиле была указана принадлежность криптопрофиля нескольким АРМ.

Изменять содержимое данных закладок допускается только при прямом указании из банка. Некорректное изменение содержимого закладок может привести к отказу в обслуживании Ваших документов!

Задание принадлежности криптопрофиля пользователям

Каждый криптопрофиль должен быть сопоставлен определенному пользователю системы (соответствие нескольким пользователям допустимо, но не рекомендуется, см. разд. «Принадлежность криптопрофиля пользователям» [стр. 28]). Перераспределение криптопрофилей по пользователям можно производить в любое время без согласования с банком.

Назначение криптопрофиля пользователям выполняется в закладке **Пользователи криптопрофиля** окна **Мастер настройки криптозащиты**. Переход в данную закладку осуществляется после выполнения инстр. «Выбор АРМ и задание прав криптопрофиля» [стр. 67] .

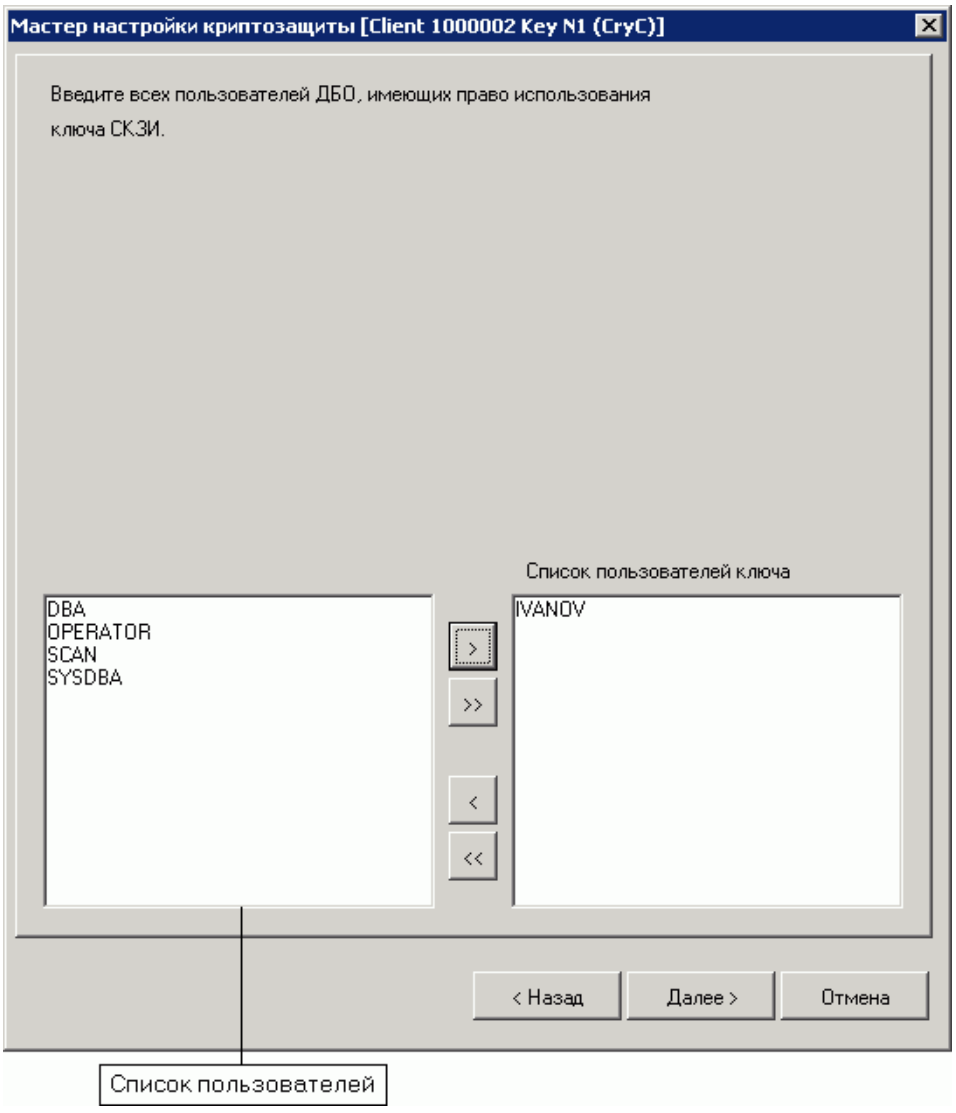


Рис. 3.8. Окно Мастер настройки криптозащиты с закладкой Пользователи криптопрофиля

В закладке изображены два списка:

- **Список пользователей** - список пользователей системы, которым недоступно использование криптопрофиля;

- **Список пользователей ключа** - список пользователей системы, которым доступно использование криптопрофиля.

Для назначения криптопрофиля пользователям отредактируйте содержимое указанных списков, а именно перенесите из первого списка во второй имена тех пользователей, которым должен быть сопоставлен криптопрофиль. Редактирование содержимого списков выполняется следующим образом:

- Для того чтобы перенести имена всех пользователей из одного списка в другой, нажмите кнопку  (криптопрофилем смогут воспользоваться все пользователи системы) или  (криптопрофилю не будет назначено ни одного пользователя).
- Для того, чтобы перенести имя конкретного пользователя из одного списка в другой, выделите имя данного пользователя в списке и нажмите кнопку  (криптопрофиль станет доступен пользователю) или кнопку  (криптопрофиль станет недоступен пользователю).

> **Внимание**!
>
> Рекомендуется каждому криптопрофилю назначить одного пользователя (подробная информация приведена в разд. «Принадлежность криптопрофиля пользователям» [стр. 28]).

После того, как содержимое списков будет настроено, нажмите кнопку **Далее**.

Произойдет переход к закладке **Ключевые наборы**. Выполните действия, описанные в инстр. «Редактирование информации о ключевых наборах криптопрофиля» [стр. 70].

Редактирование информации о ключевых наборах криптопрофиля

Редактирование информации о ключевых наборах выполняется в закладке **Ключевые наборы** окна **Мастер настройки криптозащиты**. Переход в данную закладку осуществляется в процессе редактирования криптопрофиля после выполнения инстр. «Задание принадлежности криптопрофиля пользователям» [стр. 69].

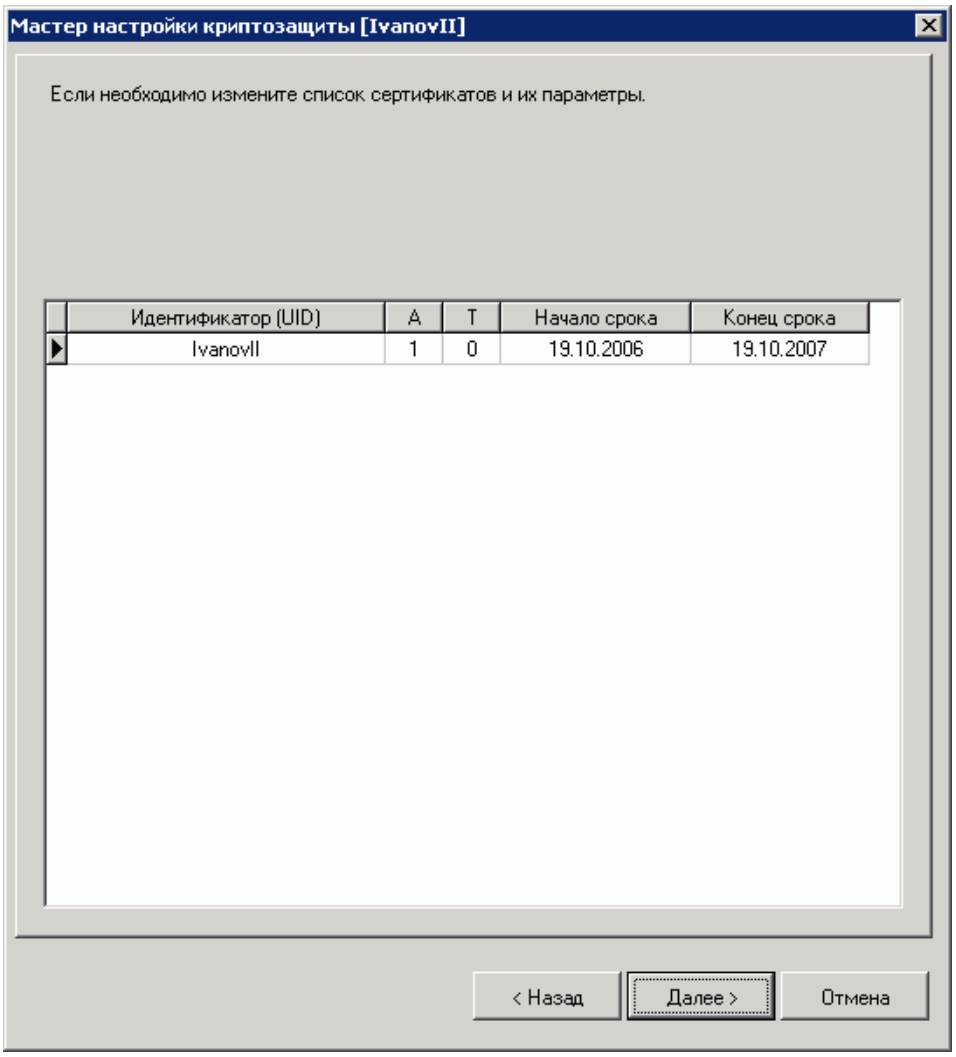


Рис. 3.9. Окно Мастер настройки криптозащиты с закладкой Ключевые наборы

Для редактирования информации о ключевых наборах, сопоставленных криптопрофилю, выполните следующие действия:

1. Настройте записи списка, представленного в закладке. Каждая запись списка содержит информацию об одном из сопоставленных криптопрофилю ключевых наборов.

   - Для создания новой записи (ввода информации об еще одном ключевом наборе) выделите какую-либо запись списка (поместите фокус в список) и нажмите клавишу **Insert**.

   - Для редактирования записи (редактирования информации о ранее сопоставленном ключевом наборе) выделите запись и выполните двойной щелчок левой кнопкой мыши.

   - Для удаления записи (удалении информации о ключевом наборе) выделите запись и нажмите клавишу **Delete**.

   В процессе создания или редактирования записи произойдет переход в окно **Сертификат абонента**.

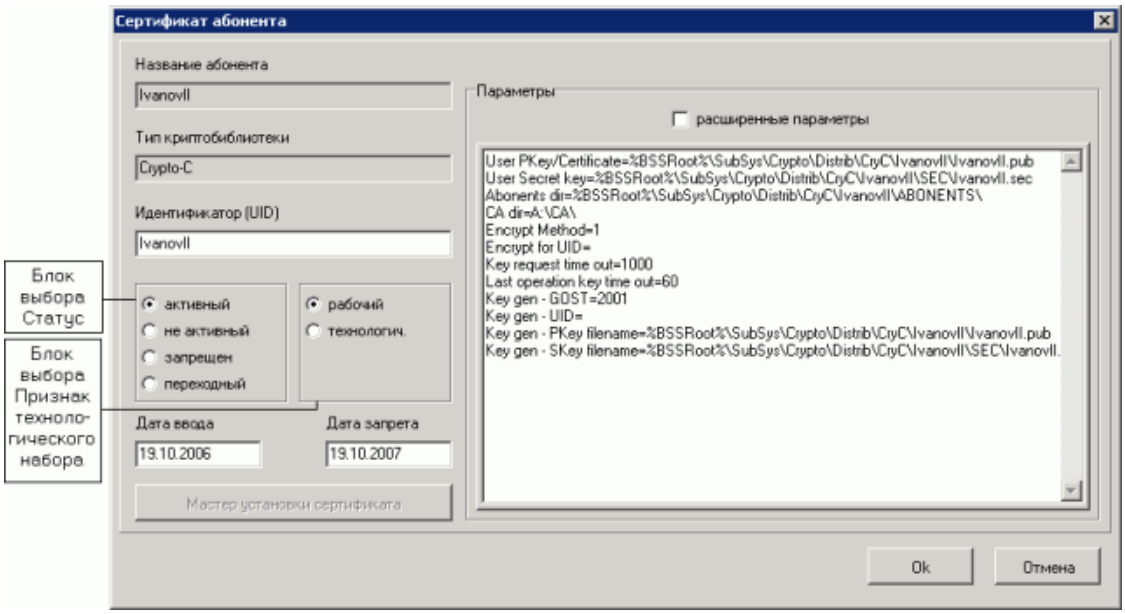


Рис. 3.10. Окно Сертификат абонента

a. В поле **Идентификатор (UID)** укажите UID ключевого набора.

b. В блоке выбора **Статус** укажите статус ключевого набора.

c. В блоке выбора **Признак технологического набора** укажите, должен ли ключевой набор быть технологическим или же он должен быть рабочим.

d. При необходимости ограничить срок действия ключевого набора введите период действия ключевого набора в полях **Дата ввода** и **Дата запрета**.

e. Заполните текстовое поле блока **Параметры** в соответствии с прил. C, «Параметры использования ключевых наборов для различных СКЗИ» [стр. 107].

f. Нажмите кнопку **Ok** для сохранения введенных параметров и возврата к закладке **Ключевые наборы** окна **Мастер настройки криптозащиты**.

Повторите описанные действия по вводу / редактированию информации для требуемого количества сопоставленных криптопрофилю ключевых наборов.

2. По окончании процесса ввода / редактирования информации о ключевых наборах, сопоставленных криптопрофилю, нажмите кнопку **Далее**.

После выполнения указанных действий произойдет переход к закладке **Завершение работы мастера**. Выполните действия, описанные в разд. «Завершение процесса редактирования криптопрофиля» [стр. 72].

Завершение процесса редактирования криптопрофиля

Система "ДБО BS-Client v.3" информирует пользователя о завершении процесса редактирования криптопрофиля переходом в закладку **Информация о ключевом наборе** окна **Мастер настройки криптозащиты**. Переход в данную закладку осуществляется после выполнения инстр. «Редактирование информации о ключевых наборах криптопрофиля» [стр. 70].

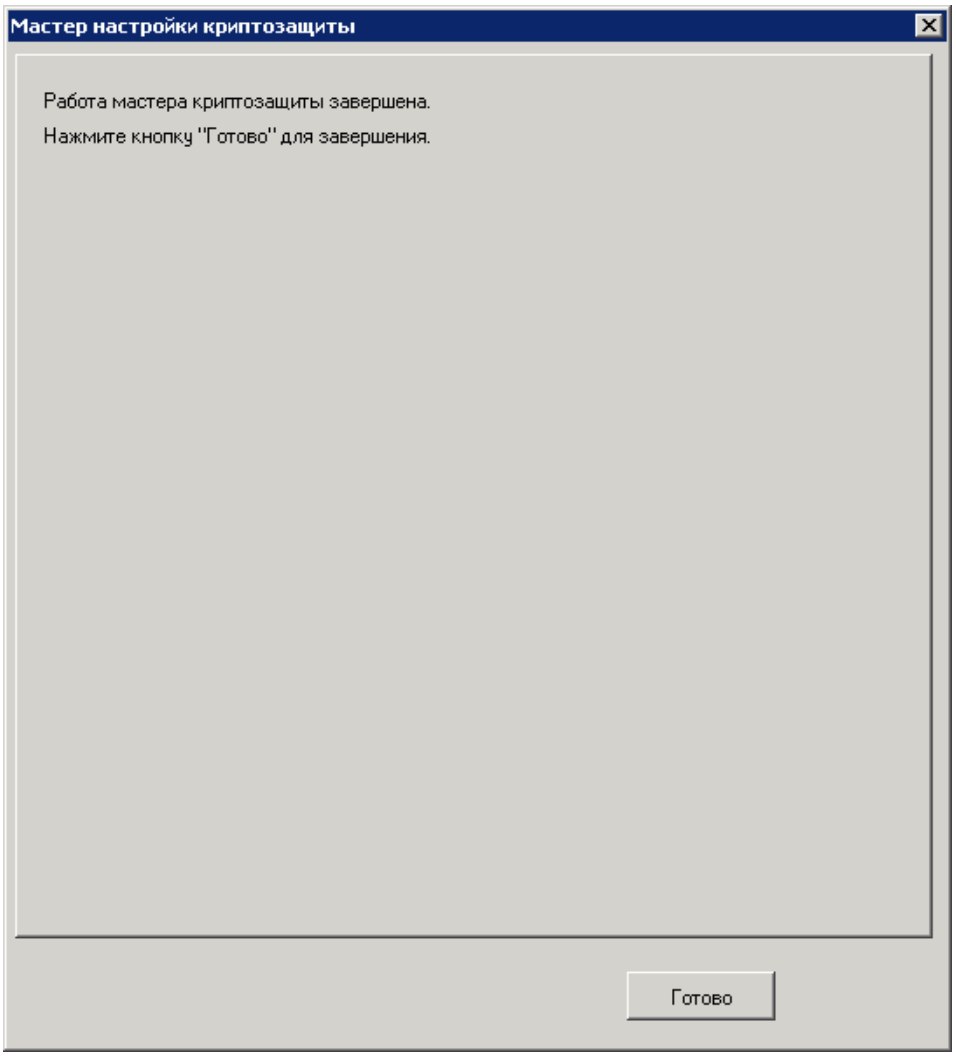


Рис. 3.11. Окно Мастер настройки криптозащиты с закладкой Завершение работы мастера

Нажмите кнопку **Готово** для завершения процесса редактирования криптопрофиля.

Настройка принадлежности криптопрофилей пользователям (Мастер настройки абонентов СКЗИ)

Для настройки принадлежности криптопрофилей пользователю выполните следующие действия:

1. Вызовите мастер настройки абонентов СКЗИ выбором команды меню **Администрирование → Криптозащита → Мастер настройки абонентов СКЗИ** . Произойдет переход в окно **Мастер настройки криптозащиты**.

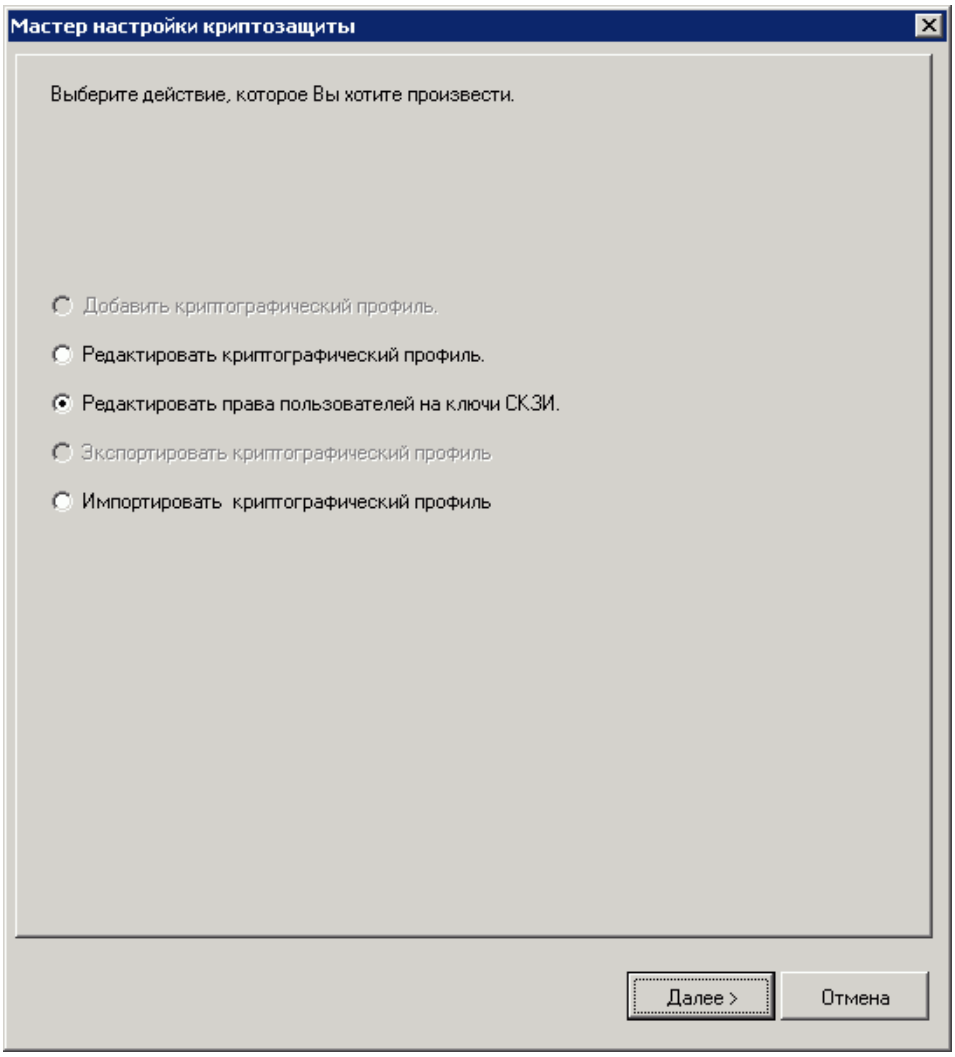


Рис. 3.12. Окно Мастер настройки криптозащиты, закладка Выбор операции

2. Выберите пункт **Редактировать права пользователей на ключи СКЗИ** и нажмите кнопку **Далее**. Произойдет переход к закладке **Принадлежность криптопрофилей пользователю**.

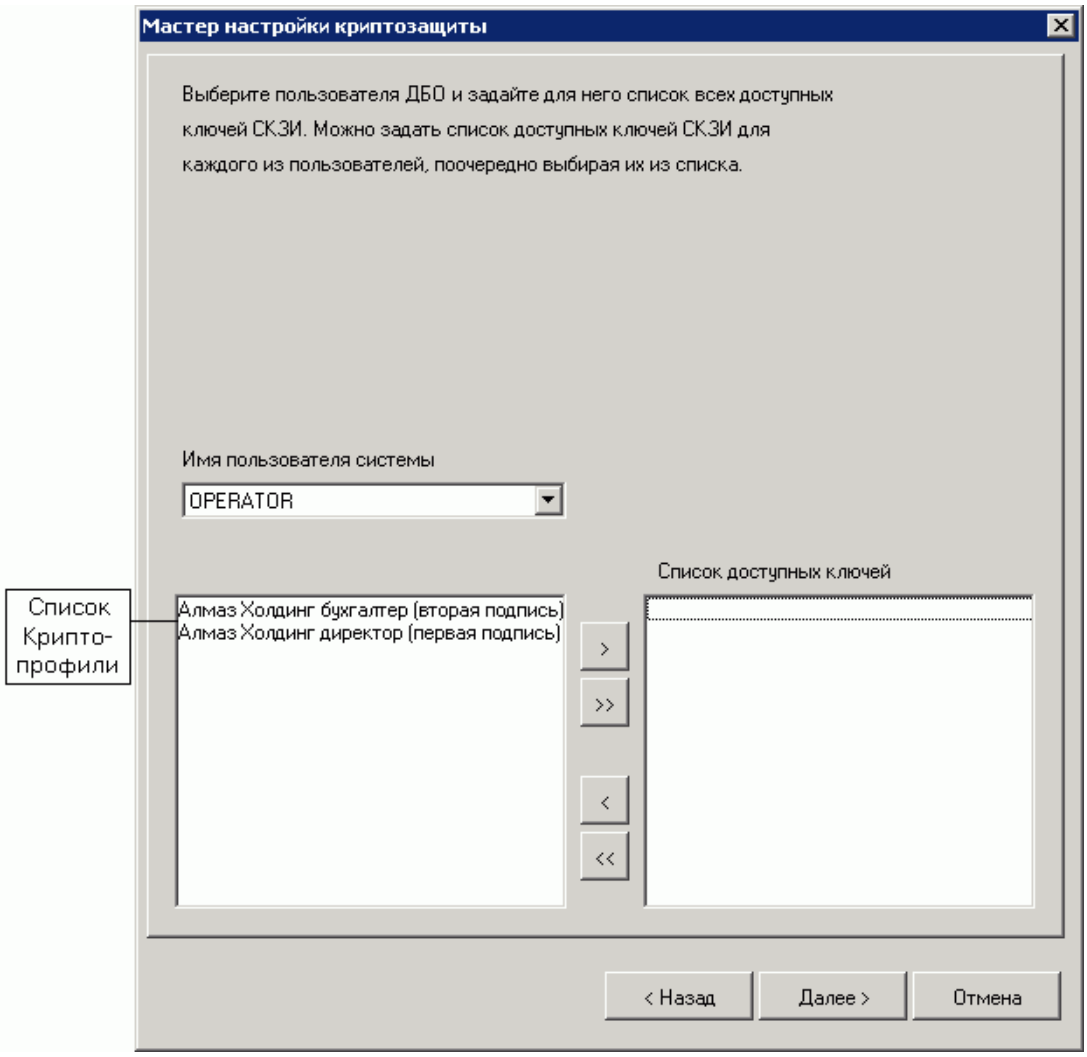


Рис. 3.13. Окно Мастер настройки криптозащиты, закладка Принадлежность криптопрофиля пользователю

3. Выберите пользователя, которому необходимо поставить в соответствие криптопрофили, в списочном поле **Имя пользователя системы**.

4. Укажите криптопрофили, которые необходимо сопоставить пользователю. Назначение криптопрофилей производится с помощью двух списков:

   - **Криптопрофили** - список криптопрофилей, не сопоставленных пользователю;
   - **Список доступных ключей** - список криптопрофилей, сопоставленных пользователю.

   Для назначения криптопрофилей пользователю отредактируйте содержимое указанных списков, а именно перенесите из первого списка во второй имена тех криптопрофилей, которые должны быть сопоставлены пользователю. Редактирование содержимого списков выполняется следующим образом:

- Для того чтобы перенести имена всех криптопрофилей из одного списка в другой, нажмите кнопку >> (пользователю будут сопоставлены все криптопрофили системы) или << (пользователю не будет сопоставлено ни одного криптопрофиля).
- Для того, чтобы перенести имя конкретного криптопрофиля из одного списка в другой, выделите имя данного криптопрофиля в списке и нажмите кнопку > (криптопрофиль станет доступен пользователю) или кнопку < (криптопрофиль станет недоступен пользователю).

5. После того, как содержимое списков будет настроено, нажмите кнопку **Далее**. Произойдет переход в закладку **Завершение работы мастера**.

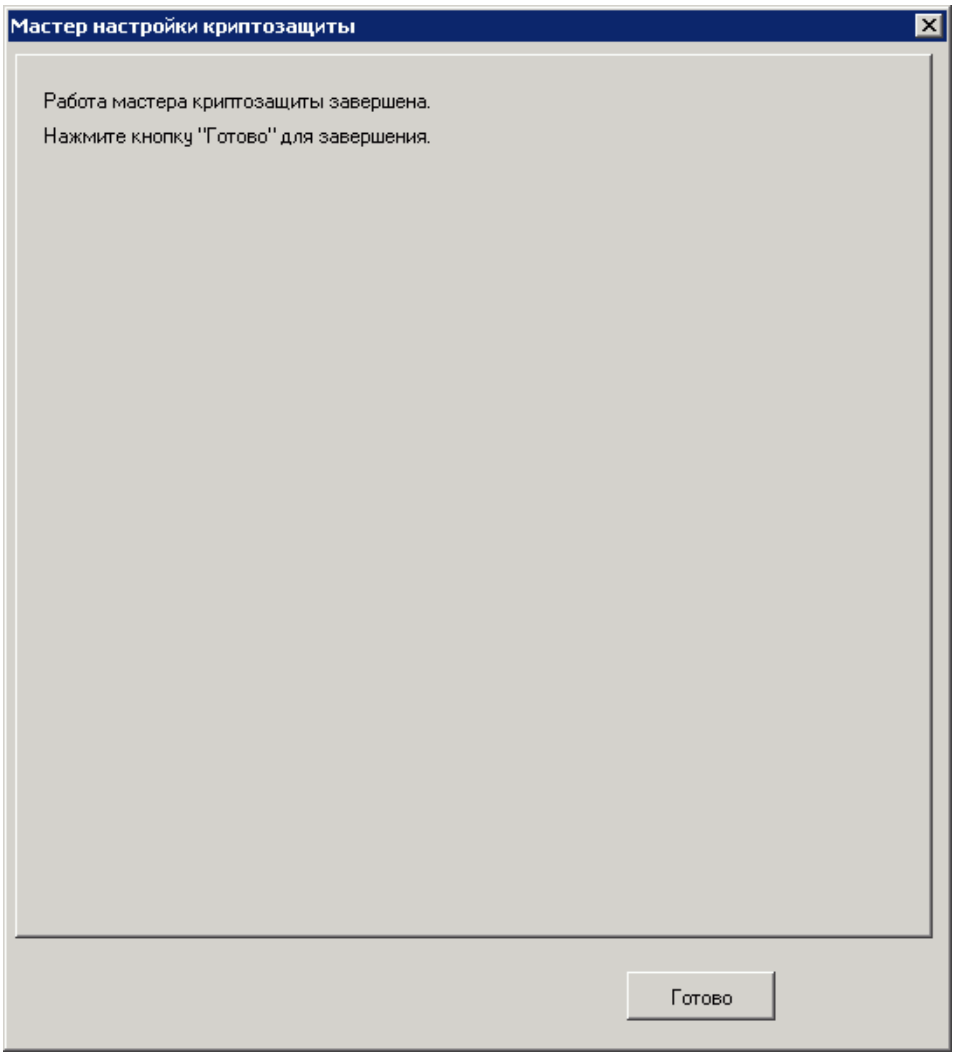


Рис. 3.14. Окно Мастер настройки криптозащиты, закладка Завершение работы мастера

6. Нажмите кнопку **Готово**.

После выполнения указанных действий пользователю станет доступно выполнение криптографических операций посредством назначенных криптопрофилей.

3.4. Настройка общих параметров криптозащиты

Общие параметры криптозащиты (за единичным исключением) определяют ход выполнения криптографических операций [стр. 36] в целом для всех абонентов системы. Настройка данных параметров может быть произведена как на этапе начальной настройки системы, так и в процессе ее штатной эксплуатации.

Настройка общих параметров криптозащиты осуществляется в окне **Дополнительные настройки криптозащиты**, вызываемом командой меню **Администрирование → Криптозащита → Доп. настройки криптозащиты**.

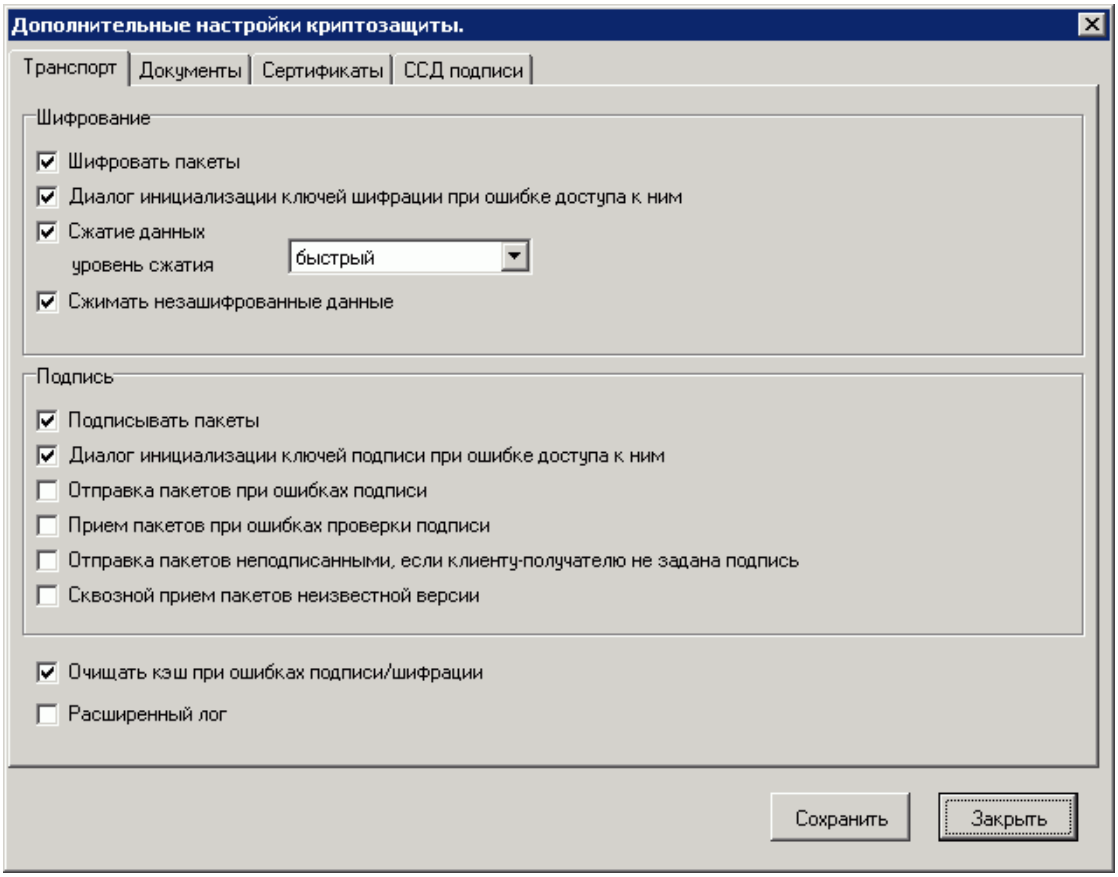


Рис. 3.15. Окно Дополнительные настройки криптозащиты

Окно состоит из четырех закладок, настройка каждой из которых описана отдельной инструкцией:

- **Транспорт** – см. инстр. «Настройка параметров, используемых при работе с транспортными пакетами» [стр. 78];
- **Документы** – см. инстр. «Настройка общих параметров выполнения криптографических операций над документами» [стр. 82];
- **Сертификаты** – см. инстр. «Настройка общих параметров использования открытых ключей» [стр. 84];

- **ССД подписи** – см. инстр. «Настройка механизма формирования и проверки подписи под документами» [стр. 86].

В процессе настройки общих параметров криптозащиты необходимо следить за согласованностью значений определенных параметров на стороне банка и на стороне клиента:

- параметры, используемые при работе с транспортными пакетами (закладка **Транспорт**):
  - **Шифровать пакеты**;
  - **Сжатие данных**;
  - **Сжимать незашифрованные данные**;
  - **Подписывать пакеты**;
- общие параметры выполнения криптографических операций над документами (закладка **Документы**):
  - **Подпись в текстовом режиме**;
- параметры формирования и проверки подписи под документами (закладка **ССД подписи**) – см. в соответствующей инструкции [стр. 86].

> **Внимание!**
>
> Несогласованность значений параметров может привести к отказу в обслуживании клиентов.

3.4.1. Настройка параметров, используемых при работе с транспортными пакетами

> **Внимание!**
>
> Перед выполнением данной инструкции рекомендуется обратиться к материалам разд. 2.3.1, «Общее описание базовых криптографических операций в системе "ДБО BS-Client v. 3"» [стр. 36] и разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50].

Для настройки параметров, используемых при работе с транспортными пакетами выполните следующие действия:

1. Выполните команду меню **Администрирование → Криптозащита → Доп. настройки криптозащиты**. Произойдет переход в окно **Дополнительные настройки криптозащиты**. Перейдите на закладку **Транспорт** (см. рис. 3.16 [стр. 79]).

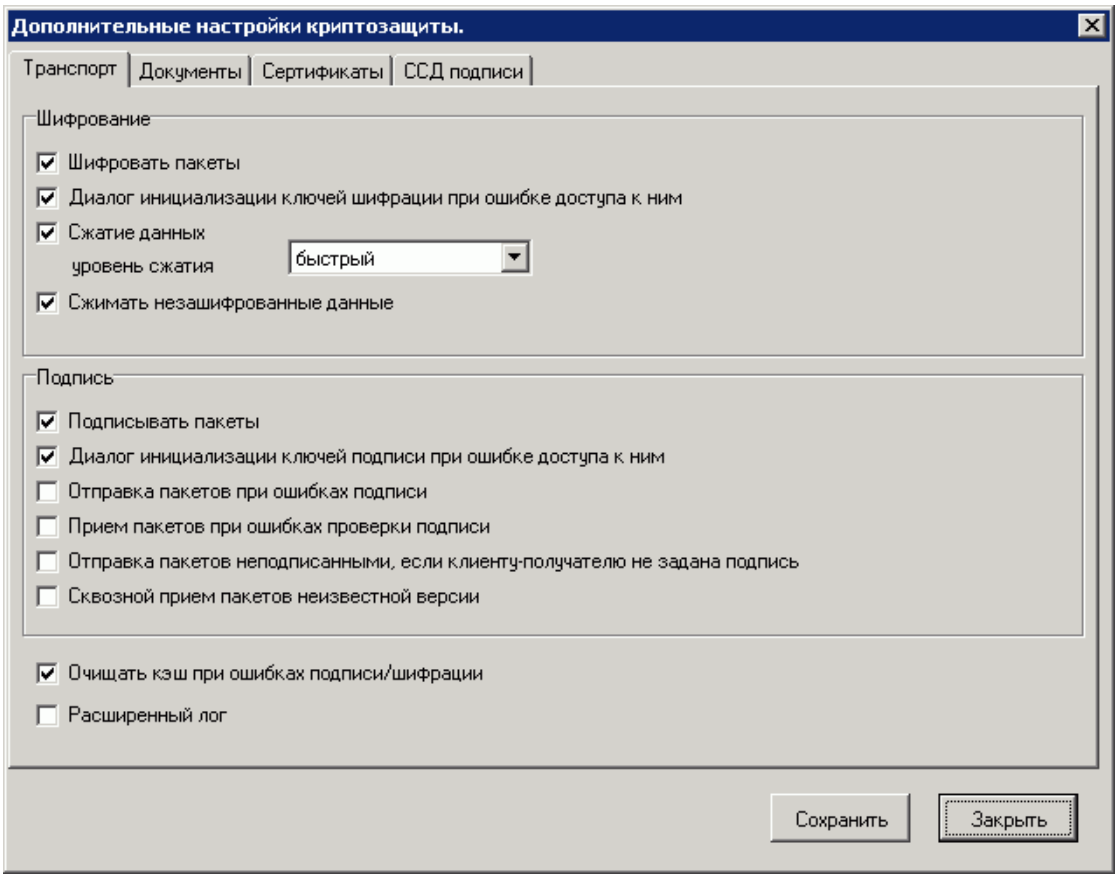


Рис. 3.16. Закладка Транспорт окна Дополнительные настройки криптозащиты

2. Для указания необходимости зашифрования пакетов при их отправке и расшифрования при получении заполните поле **Шифровать пакеты**. Если данное поле незаполнено, то зашифрование и расшифрование пакетов производится не будет. Если же поле заполнено, то зашифрование и расшифрование пакетов будет производится в зависимости от наличия криптопрофилей, обладающих правом приема / отправки почты в АРМ, с которым осуществляется обмен пакетами (см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]). Шифрование транспортных пакетов необходимо для исключения несанкционированного доступа, искажения и фальсификации пакетов при их хранении и передаче по каналам связи.

Внимание!

- Отключать опцию шифрования пакетов не рекомендуется (см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]).
- Значения данного параметра на стороне банка и на стороне клиентов должны совпадать.

Примечание

Значения описанных ниже полей блока **Шифрование** учитываются при выполнении криптографических операций, только если заполнено поле **Шифровать пакеты**. Если данное поле не заполнено, сразу перейдите к п. 5 [стр. 80].

3. При ошибках доступа к *ключам шифрования* при выполнении операций зашифрования и расшифрования транспортных пакетов предусмотрен вывод соответствующего диалога (см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]). Если вывод данного диалога необходим, заполните поле **Диалог инициализации ключей шифрации при ошибке доступа к ним**, в противном случае – снимите выделение поля.

4. Если необходимо сжатие транспортных пакетов, заполните поле **Сжатие данных** и выберите уровень сжатия в соответствующем списочном поле. Если требуется производить сжатие незашифрованных пакетов, заполните поле **Сжимать незашифрованные данные**.

> **Внимание**!
>
> Значения указанных параметров на стороне банка и на стороне клиентов должны совпадать.

> **Примечание**
>
> Пакеты могут передаваться незашифрованными в случае, когда снято заполнение поля **Шифровать пакеты** или когда на принимающей стороне отсутствуют криптопрофили, обладающие правом приема / отправки почты (см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]).

5. Для указания необходимости подписи пакетов при их отправке и проверки подписи при получении заполните поле **Подписывать пакеты**. Влияние данного параметра на операции подписи и проверки подписи аналогично влиянию параметра **Шифровать пакеты** на операции зашифрования и расшифрования (см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]). Электронная цифровая подпись транспортных пакетов необходима для обеспечения их *аутентичности*.

> **Внимание**!
>
> - Отключать опцию подписи пакетов не рекомендуется (см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]).
> - Значения данного параметра на стороне банка и на стороне клиентов должны совпадать.

> **Примечание**
>
> Значения описанных ниже полей блока **Подпись** учитываются при выполнении криптографических операций, только если заполнено поле **Подписывать пакеты**. Если данное поле не заполнено, сразу перейдите к п. 11 [стр. 81].

6. Как и в случае шифрования пакетов, при ошибках доступа к *ключам подписи* при выполнении операций подписи и проверки подписи транспортных пакетов предусмотрен вывод соответствующего диалога (см. разд. 2.3.3, « Криптографические операции транспортной подсистемы » [стр. 50]). Если вывод данного диалога необходим, заполните поле **Диалог инициализации ключей подписи при ошибке доступа к ним**, в противном случае – снимите выделение поля.

7. Если транспортные пакеты должны отправляться даже в том случае, когда их не удалось подписать, заполните поле **Отправка пакетов при ошибках подписи** .

8. Если транспортные пакеты должны приниматься даже в том случае, когда подпись под пакетами неверна, или когда ее не удается проверить, заполните поле **Прием пакетов при ошибках проверки подписи** .

9. Если необходимо отправлять пакеты неподписанными в случае, когда в АРМ-получателе отсутствуют криптопрофили, наделенные правом приема / отправки почты, заполните поле **Отправка пакетов неподписанными, если клиенту-получателю не задана подпись**.

> **Внимание**!
>
> Установка данных трех параметров может снизить защищенность канала передачи данных и не гарантирует аутентичности транспортных пакетов. В частности, это усложнит процедуру разбора конфликтных ситуаций.

10. В старших версиях системы "ДБО BS-Client v.3" подписанные транспортные пакеты снабжаются заголовком специального формата, содержащим дополнительную информацию об ЭЦП, в младших версиях системы – нет. Если необходимо пропускать проверку подписи при получении пакетов, не содержащих заголовок, заполните поле **Сквозной прием пакетов неизвестной версии**. В противном случае – снимите заполнение поля.

11. Если при возникновении ошибок выполнения криптографических операций необходимо очищать *ключевой кэш*, заполните поле **Очищать кэш при ошибках подписи / шифрации**. Если установлен данный параметр, при возникновении ошибки при работе с ключами будут произведены сброс ключевого кэша и повторная попытка выполнения криптографической операции. В ряде случаев очистка ключевого кэша устраняет причину ошибки, однако при большом количестве зарегистрированных в ключевом наборе абонентов данная операция может привести к значительному замедлению работы криптографической подсистемы (подробное описание работы с кэшем и возможных ошибок приведено в разд. 1.3.5, «Ключевые носители» [стр. 12]).

12. С помощью поля **Расширенный лог** Вы можете задать уровень детализации информации о ходе выполнения операций над транспортными пакетами, сохраняемой в журнале криптографических операций (см. разд. 2.3.4, «Журнал криптографических операций» [стр. 54]). Если требуется обычный уровень детализации, снимите заполнение поля, если требуется более детальный вывод – заполните поле.

> **Внимание**!
>
> При штатной работе системы не рекомендуется устанавливать высокую степень детализации сохраняемой в журналах информации, так как в этом случае существенно возрастает объем файлов журналов (в файле журнала будут сохраняться данные принимаемых / отправляемых пакетов) и замедляется работа системы.

13. Сохраните введенные значения параметров с помощью кнопки **Сохранить**. Нажмите кнопку **Закрыть** для закрытия окна **Дополнительные настройки криптозащиты**.

Для того, чтобы внесенные изменения вступили в силу, необходимо перезапустить транспортную подсистему. После перезапуска при работе с транспортными пакетами будут использованы новые значения параметров.

3.4.2. Настройка общих параметров выполнения криптографических операций над документами

Внимание!

Перед выполнением данной инструкции рекомендуется обратиться к материалам разд. 2.3.1, «Общее описание базовых криптографических операций в системе "ДБО BS-Client v. 3"» [стр. 36] и разд. 2.3.2, «Криптографические операции над документами» [стр. 40].

Для настройки общих параметров выполнения криптографических операций над документами выполните следующие действия:

1. Выполните команду меню **Администрирование → Криптозащита → Доп. настройки криптозащиты**. Произойдет переход в окно **Дополнительные настройки криптозащиты**. Перейдите на закладку **Документы** (см. рис. 3.17 [стр. 82]).

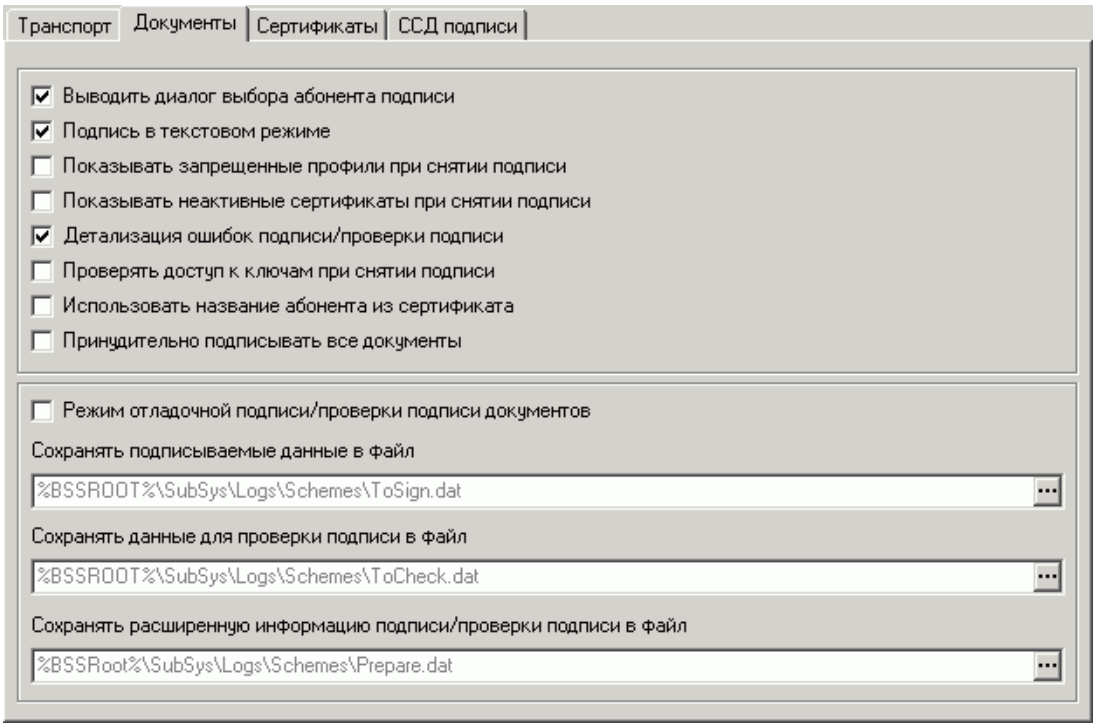


Рис. 3.17. Закладка Документы окна Дополнительные настройки криптозащиты

2. Если для Вас в системе заведено несколько криптопрофилей, обладающих правом подписи документов, возможна ситуация, когда тот или иной документ может быть подписан более чем одним криптопрофилем (см. разд. «Подпись документов» [стр. 44]). Если в подобной ситуации необходимо предоставлять возможность выбирать из списка криптопрофиль, которым будет осуществляться подпись, заполните поле **Выводить диалог выбора абонента подписи**. Заполнение данного поля позволит отображать диалог выбора криптопрофиля в случае, когда ранее Вами была указана необходимость постоян-

ного использования одного заданного Вами криптопрофиля (поле диалога **Не выводить больше окно выбора**, см. разд. «Подпись документов» [стр. 44]).

> **Примечание**
>
> - В отличие от прочих параметров криптозащиты, влияющих на весь АРМ в целом, данный параметр влияет только на работу текущего пользователя.
> - При выполнении рекомендаций, приведенных в разд. «Принадлежность криптопрофиля пользователям» [стр. 28] , при подписи одного документа пользователь не будет иметь более одного критопрофиля, пригодного для выполнения операции подписи. Соответственно окно выбора криптопрофиля не будет отображаться при любых значениях описываемого поля. Поэтому заполнение данного поля может потребоваться только для последующего выполнения операций*пакетной* подписи документов (см. разд. 2.3.2, «Криптографические операции над документами» [стр. 40]), а также в некоторых особых случаях.

3. Убедитесь, что поле **Подпись в текстовом режиме** заполнено. Заполнение данного поля активизирует текстовый режим подписи, позволяющий сделать процедуру разрабора конфликтных ситуаций более прозрачной. Подробнее о текстовом режиме подписи см. в разд. А.2.4, «Формирование блока подписываемых данных» [стр. 94].

> **Внимание**!
>
> Значения данного параметра на стороне банка и на стороне клиентов должны совпадать.

4. Если необходимо иметь возможность снятия подписи, сделанной криптопрофилем, который впоследствии был запрещен (см. разд. 2.2.2, «Статус криптопрофиля» [стр. 29]), заполните поле **Показывать запрещенные профили при снятии подписи**.

5. Если необходимо иметь возможность снятия подписи, сделанной ключом из ключевого набора, впоследствии ставшего *неактивным* (см. разд. «Статус ключевого набора» [стр. 30]), заполните поле **Показывать неактивные сертификаты при снятии подписи**.

6. Заполните поле **Проверять доступ к ключам при снятии подписи**, если при выполнении операции снятия подписи в дополнение к проверке пароля пользователя необходимо также проверять доступ к ключам, которыми были подписаны документы.

> **Примечание**
>
> Более подробно операция снятия подписи и влияние указанных трех параметров на ход ее выполнения рассмотрены в разд. «Снятие подписи под документами» [стр. 49].

7. С помощью поля **Детализация ошибок подписи / проверки подписи** Вы можете задать уровень детализации информации о ходе выполнения операций над документами, выдаваемой на экран пользователю. Если требуется обычный уровень детализации, снимите заполнение поля, если требуется более детальный вывод – заполните поле.

8. При печати подписанных платежных документов на печать выводится информация о подписавшем документ абоненте либо в виде имени криптопрофиля абонента, либо в виде имени владельца сертификата. Заполните поле **Использовать название абонента**

из сертификата, если необходимо выводить на печать имена владельцев сертификатов, или снимите заполнение поля, если требуется распечатывать имена криптопрофилей.

Примечание

- Имя владельца извлекается из поля Common Name сертификата. Наличие данного поля в сертификате предписывается стандартом *X.509* (см. разд. «Инфраструктура открытых ключей (PKI)» [стр. 13]). Имя криптопрофиля задается в процессе создания криптопрофиля.
- При использовании несертификатных СКЗИ значение данного поля системой не используется, при печати всегда используются имена криптопрофилей.

9. Значение поля **Принудительно подписывать все документы** оставьте без изменений.

Примечание

Данное поле системой "ДБО BS-Client v.3" на стороне клиента не используется.

10. Значение поля **Режим отладочной подписи / проверки подписи документов** и расположенных под ним текстовых полей того же блока оставьте без изменений.

Примечание

Изменять значение указанных полей при штатной работе системы не требуется. Указанные поля используются только в процессе разработки системы. Заполнение поля **Режим отладочной подписи / проверки подписи документов** должно быть снято.

11. Сохраните введенные значения параметров с помощью кнопки **Сохранить**. Нажмите кнопку **Закрыть** для закрытия окна **Дополнительные настройки криптозащиты**.

После выполнения инструкции при выполнении криптографических операций над документами будут использоваться новые значения параметров.

3.4.3. Настройка общих параметров использования открытых ключей

Для настройки общих параметров использования открытых ключей выполните следующие действия:

1. Выполните команду меню **Администрирование → Криптозащита → Доп. настройки криптозащиты**. Произойдет переход в окно **Дополнительные настройки криптозащиты**. Перейдите на закладку **Сертификаты** (см. рис. 3.18 [стр. 85]).

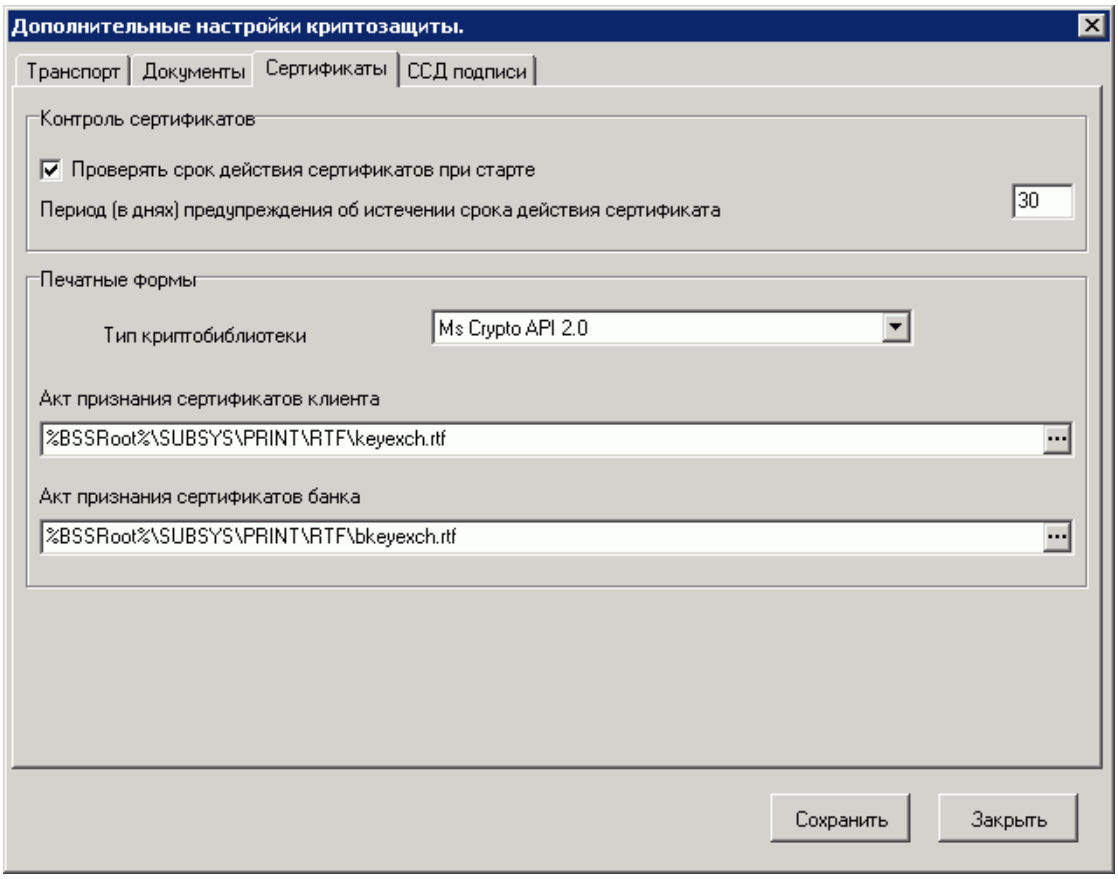


Рис. 3.18. Закладка Сертификаты окна Дополнительные настройки криптозащиты

2. Система "ДБО BS-Client v.3" предоставляет возможность при каждом старте системы осуществлять проверку истечения сроков действия сертификатов, зарегистрированных в системе (см. разд. «Срок действия ключевого набора» [стр. 32]). Если данная проверка необходима, заполните поле **Проверять срок действия сертификатов при старте** и в поле **Период (в днях) предупреждения об истечении срока действия сертификата** укажите количество дней до истечения срока, за которое система должна начать выводить предупреждения.

> **Примечание**
>
> Данная возможность существует только при использовании сертификатных СКЗИ.

3. Если Вы хотите использовать нестандартные печатные формы актов признания сертификатов, укажите для каждой используемой СКЗИ имена файлов печатных форм:

   a. Выберите соответствующую СКЗИ *криптобиблиотеку* в поле **Тип криптобиблиотеки** (о криптобиблиотеках см. разд. 2.1, « Механизмы взаимодействия с СКЗИ » [стр. 24]).

   b. В полях **Акт признания сертификатов клиента** и **Акт признания сертификатов банка** укажите пути и имена файлов соответствующих печатных форм.

4. Сохраните введенные значения параметров с помощью кнопки **Сохранить**. Нажмите кнопку **Закрыть** для закрытия окна **Дополнительные настройки криптозащиты**.

После выполнения инструкции новые параметры использования открытых ключей вступят в силу.

3.4.4. Настройка механизма формирования и проверки подписи под документами

Внимание!

Изменять параметры механизма формирования и проверки подписи под документами рекомендуется только в случае прямой необходимости, например, в процессе обновления системы. В остальных случаях вносить изменения не рекомендуется во избежание отказа в обслуживании.

Перед выполнением инструкции настоятельно рекомендуется обратиться к материалу прил. А, «Механизм формирования и формат хранения подписи под документами» [стр. 89] и запомнить прежние значения изменяемых параметров.

Для настройки механизма формирования проверки подписи под документами выполните следующие действия:

1. Выполните команду меню **Администрирование → Криптозащита → Доп. настройки криптозащиты**. Произойдет переход в окно **Дополнительные настройки криптозащиты**. Перейдите на закладку **ССД подписи** (см. рис. 3.19 [стр. 87]).

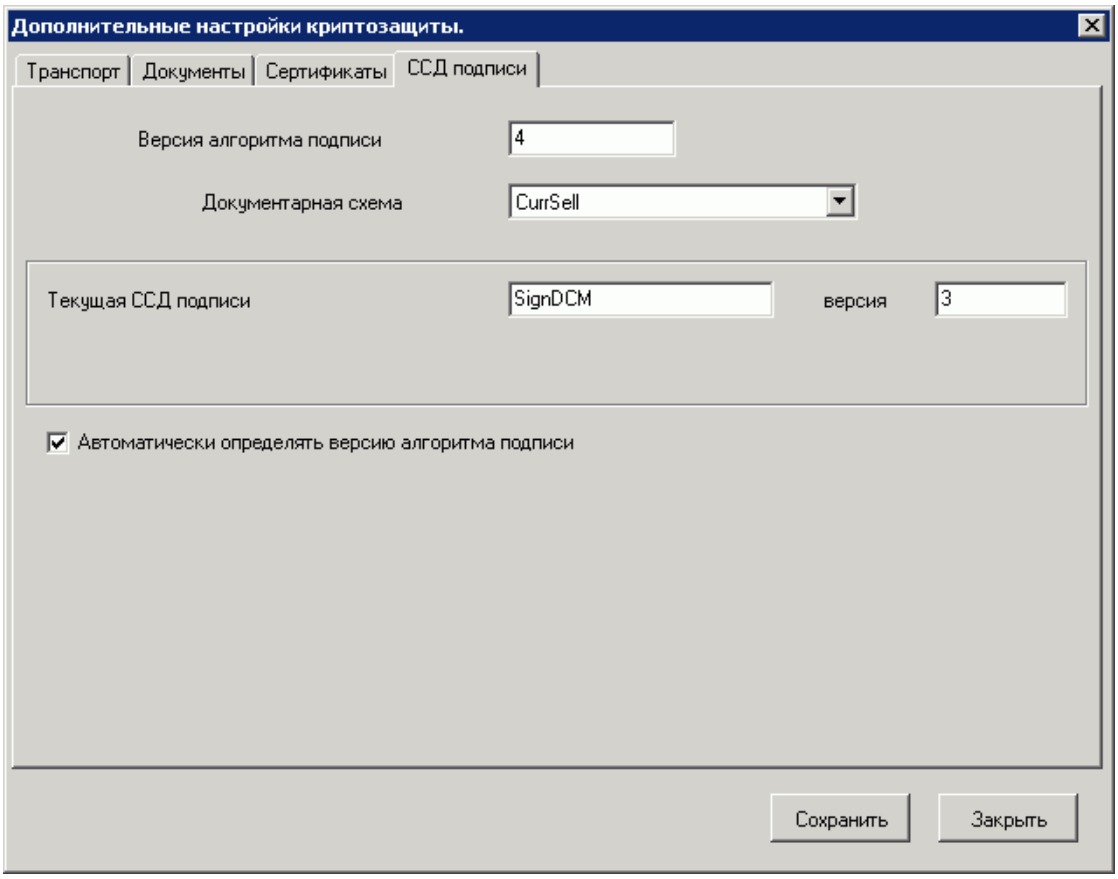


Рис. 3.19. Закладка ССД подписи окна Дополнительные настройки криптозащиты

Примечание

Внешний вид закладки **ССД подписи** (состав полей) изменяется в зависимости от значения поля **Версия алгоритма подписи**.

2. Задайте параметры выполнения алгоритмов формирования и проверки подписи версии 4:

   a. Введите в поле **Версия алгоритма подписи** значение "4".

   b. В поле **Документарная схема** выберите документарную схему, для которой Вы хотите задать параметры алгоритмов формирования и проверки подписи. Настройку алгоритмов можно последовательно произвести для всех имеющихся документарных схем.

   c. В полях **Текущая ССД подписи** и **Версия** введите соответственно имя и номер версии ССД, которую Вы хотите сделать текущей для указанных документарной схемы и алгоритмов.

   d. Повторите п. 2.b [стр. 87]-п. 2.c [стр. 87] для требуемого набора документарных схем.

Примечание

Если Вы хотите настроить систему таким образом, чтобы в процессе формирования и проверки подписи использовались алгоритмы более ранних версий, настраивать параметры

работы алгоритмов версии 4 не нужно. Однако рекомендуется использовать алгоритмы более поздних версий.

3. Убедитесь, что в поле **Версия алгоритма подписи** задан номер версии формата хранения и алгоритма подписи, которые необходимо использовать.

> **Примечание**
>
> Поле **Версия алгоритма подписи** имеет двойную нагрузку. Во-первых, с помощью данного поля можно задать параметры выполнения алгоритмов различных версий (см. п. 2 [стр. 87]). Во-вторых, поле задает текущую версию формата хранения и алгоритма подписи.

4. Значение поля **Автоматически определять версию алгоритма подписи** оставьте без изменений.

> **Примечание**
>
> Данное поле системой "ДБО BS-Client v.3" на стороне клиента не используется.

5. Сохраните введенные значения параметров с помощью кнопки **Сохранить**. Нажмите кнопку **Закрыть** для закрытия окна **Дополнительные настройки криптозащиты**.

После выполнения инструкции новые параметры формирования и проверки подписи под документами вступят в силу. Если из-за внесенных изменений возникнут проблемы с проверкой подписей под документами, верните значения параметров к исходному состоянию.

Приложение A. Механизм формирования и формат хранения подписи под документами

Приводимая в данном разделе информация полезна для углубленного понимания процессов подписи документов и проверки подписи под документами, особенно в случае взаимодействия системы банка поздних версий (17 и выше) с системами клиентов более ранних версий (до версии 17). Данная информация может потребоваться в процессе обновления системы и при создании новых документарных схем. Вы можете пропустить данный материал и вернуться к нему при необходимости.

В последующих разделах рассматриваются такие понятия, как *ССД подписи*, *формат хранения подписи документов*, версия алгоритмов формирования подписи и проверки подписи, разъясняется, какая часть данных документа подлежит подписи и в каком виде полученная ЭЦП хранится в системе. Рекомендуется перед изучением изложенного ниже материала обратиться к разд. 1.4.2, «Электронная цифровая подпись данных и проверка подписи» [стр. 18].

A.1. ССД подписи

Документы хранятся в системе "ДБО BS-Client v.3" в виде записей таблиц БД. В то же время все поддерживаемые *криптобиблиотеки* работают с блоками бинарных или текстовых данных (см. разд. 2.1, « Механизмы взаимодействия с СКЗИ » [стр. 24]). Поэтому для осуществления подписи документа необходимо решить проблему взаимнооднозначного сопоставления документу блока бинарных или текстовых данных.

При этом, на стороне банка и на стороне клиента состав полей (атрибутов) таблиц, содержащих документы, может быть различен: на банке может содержаться больше информации о документах, чем на клиенте. Для того, чтобы определить соответствие между документами на стороне банка и документами на стороне клиента применяются *схемы составления документа* (*ССД*), а именно *ССД подписи*. ССД подписи определяет для документов каждого заданного типа (для каждой *документарной схемы* - платежных поручений, поручений на перевод валют и т.д.) список полей, которые должны быть подписаны. На основе данных полей формируются блок данных для подписи и ЭЦП документа (см. рис. A.1 [стр. 90]). Поля документа, не входящие в ССД, не подписываются.

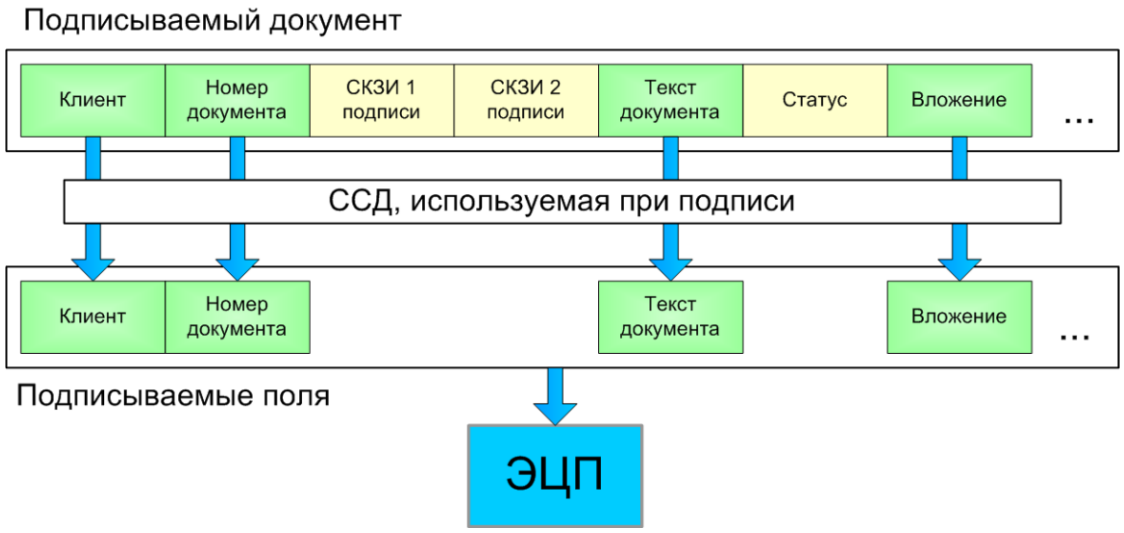


Рис. A.1. Формирование ЭЦП с использованием ССД подписи

Примечание

Кроме ССД подписи в системе "ДБО BS-Client v.3" применяются другие ССД, например, ССД отправки, используемые транспортной подсистемой в процессе формирования и обработки *транспортных пакетов* .

Поскольку в различных релизах системы "ДБО BS-Client v.3" состав полей документарных таблиц БД различается, в зависимости от версии системы применяются различные ССД. Кроме того, в различных версиях системы применяются различные алгоритмы формирования и проверки подписи под документами (см. разд. A.2, «Алгоритмы формирования и проверки подписи» [стр. 91]). При этом, система "ДБО BS-Client v.3" поддерживает обратную совместимость с используемыми ранее ССД и алгоритами. Благодаря этому система банка более поздней версии имеет возможность обмениваться документами с системами клиентов более ранних версий.

Примечание

Для обеспечения взаимодействия между системами различных версий необходимо следовать инструкциям по обновлению системы.

Каждая ССД идентифицируется именем и версией. Более ранние алгоритмы проверки подписи (до версии 4) используют в процессе своего выполнения информацию об использованной при подписи документа ССД (см. разд. A.2, «Алгоритмы формирования и проверки подписи» [стр. 91]). Поэтому для совместимости с данными алгоритмами информация о ССД подписи (а именно номер версии ССД) прилагается к подписанному документу. При этом ССД, имеющие одно и то же имя и номер версии, на банке и на клиенте могут различаться по составу полей. Таким образом, можно говорить о двух различных наборах полей с одинаковыми идентификаторами: ССД подписи и ССД проверки подписи. Более поздние алгоритмы проверки подписи не используют информацию об ССД подписи. Более подробно значение ССД при выполнении криптографических операций над документами рассмотрено далее [стр. 91].

Примечание

В более ранних версиях системы (до версии 17) для идентификации ССД использовался только номер версии ССД (без имени). Для совместимости с более поздними версиями системы считается, что подобные ССД имеют предопределенное имя (по умолчанию "SignDCM015"), хотя данное имя не прилагается к подписанным документам. Название ССД подписи ранних версий доступно для редактирования (см. разд. 3.4.4, «Настройка механизма формирования и проверки подписи под документами» [стр. 86]).

Для каждой версии алгоритма формирования и проверки подписи и для каждой документарной схемы (для каждого типа документа) одна из ССД является *текущей*. Текущая ССД используется при формировании и проверке подписи документов данного типа. Текущие ССД задаются в соответствии с инстр. «Настройка механизма формирования и проверки подписи под документами» [стр. 86].

Примечание

Изменение текущих ССД для входящих в поставку системы "ДБО BS-Client v.3" документарных схем может потребоваться в процессе обновления системы. Также задание текущей ССД может потребоваться в процессе создания новой документарной схемы. В прочих случаях изменять текущие ССД не рекомендуется.

A.2. Алгоритмы формирования и проверки подписи

В процессе подписи документа формируется ЭЦП документа - *дайджест* определяемых *ССД подписи* полей документа, зашифрованный секретным ключом подписи (см. разд. 1.4.2, «Электронная цифровая подпись данных и проверка подписи» [стр. 18]). Полученная ЭЦП прилагается к подписанному документу. Кроме того, в зависимости от применяемых алгоритмов формирования и проверки подписи, к документу может прилагаться дополнительная информация: версия алгоритма подписи, версия ССД подписи (см. разд. A.1, « ССД подписи » [стр. 89]), список наименований подписанных полей и проч. (см. далее). Указанная информация необходима для проверки подписи под документом.

В процессе формирования подписи документа ЭЦП документа (зашифрованный дайджест) и часть дополнительной информации, необходимой для проверки подписи, преобразуется в структуру специального формата, называемого *форматом хранения подписи документа*. Данная структура помещается в поле Signatures документа.

В разных версиях системы "ДБО BS-Client v.3" формат хранения подписи документа модифицировался. Соответственно изменялись и алгоритмы, формирующие и проверяющие подпись. Как было сказано выше [стр. 89], для обеспечения обратной совместимости с более ранними версиями системы, новые версии системы "ДБО BS-Client v.3" поддерживают все ранее используемые алгоритмы формирования и проверки подписи.

Внимание!

Не следует путать упоминаемые алгоритмы с алгоритмами прикладного уровня, описанными в разд. «Подпись документов» [стр. 44] и разд. «Проверка подписи под документами» [стр. 48]. Рассматриваемые здесь алгоритмы являются частью алгоритмов прикладного уровня.

Форматы хранения подписи и соответствующие им алгоритмы идентифицируются версией формата / алгоритмов. В более ранних релизах системы "ДБО BS-Client v.3" (до релиза 17) применялись формат и алгоритмы версий 1, 2 и 3, в более поздних (17 и выше) - формат и алгоритмы версии 4.

Примечание

Текущая версия формата подписи и алгоритмов подписи и проверки подписи задается в соответствии с инстр. «Настройка механизма формирования и проверки подписи под документами» [стр. 86]. В процессе обновления системы клиента допускается смена текущей версии формата / алгоритмов на более новую, если система банка поддерживает данную версию. В противном случае изменять текущую версию формата / алгоритмов не рекомендуется во избежание отказа в обслуживании.

A.2.1. Формирование подписи

Подпись документа при использовании алгоритмов различных версий происходит схожим образом:

1. Из настроек подсистемы криптозащиты определяется *текущая ССД подписи*, соответствующая текущей версии формата подписи и алгоритмов и документарной схеме подписываемого документа.

2. В соответствии с ССД подписи из документа отбираются поля, подлежащие подписи.

3. По данным полям в соответствии с текущим алгоритмом формируется блок данных для подписи, который затем подписывается (см. разд. A.2.4, «Формирование блока подписываемых данных» [стр. 94]).

4. Полученная ЭЦП, номер применяемой версии алгоритмов, а при использовании алгоритмов версии 4 - и список наименований подписанных полей, в соответствии с текущим форматом хранения подписи помещаются в поле Signatures документа. Номер версии ССД (для обеспечения обратной совместимости) помещается в поле SignDCM документа.

A.2.2. Проверка подписи

При проверке подписи по значению поля Signatures документа определяется версия алгоритма, использованного при подписи. Далее, в зависимости от версии алгоритма производится та или иная проверка подписи. Если подпись документа имеет формат версии 4:

1. В перечне ССД системы находится текущая ССД, используемая при подписи документов данного типа.

2. По значению поля Signatures документа определяется список наименований подписанных полей.

3. Аналогично процессу подписи, по полям, соответствующим списку наименований подписанных полей, в соответствии с текущим алгоритмом формируется блок данных для проверки (см. разд. A.2.4, «Формирование блока подписываемых данных» [стр. 94]).

4. Сравнивается дайджест сформированного блока с расшифрованным блоком подписанных данных (см. разд. 1.4.2, «Электронная цифровая подпись данных и проверка под-

писи» [стр. 18]). Если соответствия нет или оно неполное, то подпись считается недействительной.

5. Осуществляется проверка того, что все поля, соответствующие текущей ССД, имеются в списке наименований подписанных полей. При несоблюдении данной проверки подпись под документом считается недействительной. Ситуация, когда подписано больше полей, чем требует текущая ССД подписи, допускается.

Если подпись документа имеет формат версий 1, 2 или 3 (например, документ получен от клиента системы версии ниже 17):

1. По значению поля SignDCM документа определяется версия ССД, использованной при подписи документа. Если значение поля равно 0 или NULL или поле отсутствует в документе, используется предопределенный в системе номер версии текущей ССД (по умолчанию 10, см. разд. А.2.3, «Настройка алгоритмов» [стр. 93]).

2. В перечне ССД системы находится текущая ССД подписи, соответствующая версии алгоритма, использованного при подписи (по умолчанию - с предопределенным именем "SignDCM015", см. см. разд. А.2.3, «Настройка алгоритмов» [стр. 93]), с номером версии, определенном на предыдущем шаге.

3. Из документа отбираются поля, соответствующие полученной ССД подписи.

4. По данным полям, в соответствии с алгоритмом, использованным при подписи, формируется блок данных для проверки (см. разд. А.2.4, «Формирование блока подписываемых данных» [стр. 94]).

5. Сравнивается дайджест сформированного блока с расшифрованным блоком подписанных данных (см. разд. 1.4.2, «Электронная цифровая подпись данных и проверка подписи» [стр. 18]). Если соответствия нет или оно неполное, то подпись считается недействительной.

6. Осуществляется проверка того, что номер версии ССД подписи имеется в соответствующем документарной схеме документа *списке допустимых номеров ССД подписи*. Если номер версии ССД подписи отсутствует в данном списке, подпись считается недействительной.

А.2.3. Настройка алгоритмов

Предопределенные имена, предопределенные номера версий и списки допустимых номеров ССД подписи для каждой документарной схемы задаются в оответствии с инстр. «Настройка механизма формирования и проверки подписи под документами» [стр. 86]. Также возможно редактирование данных параметров с помощью модуля Построитель. Значения параметров сохраняются в ветке структуры базы данных **Структуры → Конфигурации → UserLib → Crypto → CBank → SignDCM**. В данной ветке располагаются подветки для каждой существующей документарной схемы, каждая подветка содержит набор параметров:

- Параметры алгоритмов версии 4 (используются в процессе подписи):
  - **Name** - имя текущей ССД;
  - **Version** - номер версии текущей ССД.

- Параметры алгоритмов версий 1, 2 и 3 (используются в процессе формирования и проверки подписи):
  - **Name015** - предопределенное имя текущей ССД ("SignDCM015");
  - **Active** - номер версии текущей ССД (обычно 10);
  - **Allowed** - список допустимых номеров ССД подписи.

> **Примечание**
>
> Задавать значения указанных параметров целесообразно только в процессе обновления системы и при создании новых документарных схем. В остальных случаях изменять значения параметров не рекомендуется во избежание отказа в обслуживании.

A.2.4. Формирование блока подписываемых данных

В процессе формирования [стр. 92] и проверки [стр. 92] подписи блоки подписываемых данных формируются из значений подписываемых полей документа. Существует два варианта формирования блоков данных:

- бинарный режим;
- текстовый режим.

При использовании бинарного режима блок данных для подписи формируется как конкатенация двоичных значений подписываемых полей. При использовании текстового режима применяется более сложная схема. Значение каждого поля преобразуется в строку с соответствии с табл. A.1, «Схема преобразования значений полей для подписи» [стр. 95]. Строка состоит обозначения типа поля, текстового представления значения поля и других данных. При вычислении текстового представления значения поля для некоторых типов происходит округление значения. Параметры округления задаются с помощью модуля Построитель в ветке структуры базы данных **Структуры → Конфигурации → SIGNATURES**:

- **Sign.DateTimePrecision** - признак округления значений типа DateTime до секунд. Параметр может принимать два значения: "1" - округление происходит, "0" - округления не происходит. По умолчанию значение "1".
- **Sign.FloatPrecision** - количество знаков после запятой, до которых происходит округление значений типа Double. По умолчанию значение "4".
- **Sign.MoneyPrecision** - количество знаков после запятой, до которых происходит округление значений типа Money. По умолчанию значение "4".
- **Sign.ProcessNULLString** - признак представления текстовых значений NULL в виде пустой строки. Параметр может принимать два значения: "TRUE" - значения NULL представляются в виде пустой строки, "FALSE" - значения NULL представляются в виде строки "NULL". По умолчанию значение "TRUE".

Преобразованные значения полей при использовании текстового режима далее объединяются в общую строку, разделяясь между собой символами #13#10:

<Блок данных записи>:=<Блок данных поля 1>#13#10<Блок данных поля 2>#13#10 ... <Блок данных поля N>#13#10

Таблица A.1. **Схема преобразования значений полей для подписи**

Тип поля	В случае NULL	В случае не NULL	Комментарий
String, LongString, LongBinary, SNR	NULL STRING (0):NULL	STRING(<Длина значения поля>):<Значение поля>	Длина значения поля указывается из-за того, что значение может содержать символы #13#10, которые являются разделителями, и возможен неоднозначный разбор. При установленном параметре **Sign.ProcessNULLString**перед вычислением блока данных поля будет происходить замена значения NULL на пустую строку
SmallInt, Integer, DocStatus, RPLStatus, SysDate, SysTime, AutoIncrement, Byte	NULL INTEGER:NULL	INTEGER:<Значение поля>	Значение поля в данном случае – это просто текстовое представление числового значения поля: IntToStr (Field.AsInteger)
Double	NULL DOUBLE:NULL	FLOAT:<Значение поля>	Значение в данном случае – это текстовое представление значения типа Double. Перевод осуществляется в представление с фиксированной точкой, с разделителем дробной части "." и с точностью, задаваемой параметром **Sign.FloatPrecision**
Date	NULL DATE:NULL	DATE:<Значение поля>	Значение в данном случае – это строковое представление даты в формате dd.mm.yyyy
DateTime	NULL DATETIME:NULL	DATETIME:<Дата>:<Время>	<Дата> - это дата из значения DateTime в формате dd.mm.yyyy. <Время> - это время из значения DateTime в формате hh:mm:ss.dddd. Время округляется в соответствии с параметром **Sign.DateTimePrecision**
Money	NULL MONEY:NULL	MONEY:<Значение поля>	Значение представляется также как и для типа Double, но вместо параметра **Sign.FloatPrecision** используется **Sign.MoneyPrecision**
BLOBTable	NULL BLOBTABLE (0):NULL	BLOBTABLE (<Длина значения поля>):<Значение поля>	См. примечания к типу String

Тип поля	В случае NULL	В случае не NULL	Комментарий
Boolean	NULL BLOBTABLE (0):NULL	BOOLEAN:TRUE BOOLEAN:FALSE	

Текстовый режим подписи предпочтительнее бинарного режима, так как текстовое представление подписываемых данных более прозрачно, что имеет значение в процессе разбора конфликтных ситуаций.

В процессе подписи [стр. 92] документов сформированные блоки данных подаются на вход процедурам подписи, реализованным на уровне СКЗИ. В процессе проверки подписи [стр. 92] сформированные блоки данных средствами СКЗИ сравниваются с расшифрованными ЭЦП. Общее описание действий, выполняемых на уровне СКЗИ, приведено в разд. 1.4.2, «Электронная цифровая подпись данных и проверка подписи» [стр. 18].

Приложение В. Интерфейс задания параметров процедуры генерации ключей / запросов на сертификат

Ниже приводится перечень и описание параметров процедуры генерации ключей / запросов на сертификат, задаваемых в процессе выполнения инстр. «Генерация ключей / запросов на сертификаты средствами системы "ДБО BS-Client v.3"» [стр. 60]:

B.1. **Параметры генерации при использовании криптопровайдеров** (MS Crypto API 2.0)

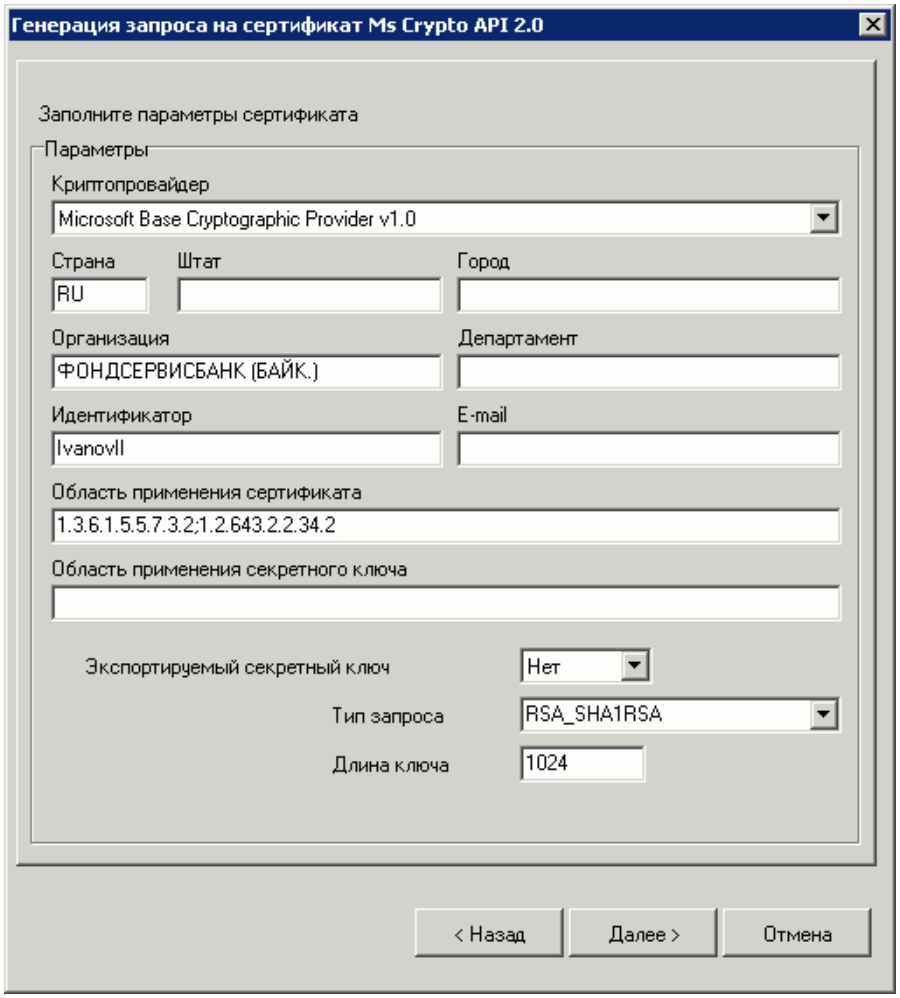


Рис. B.1. Окно Генерация запроса на сертификат Ms Crypto API 2.0

- **Крипропровайдер** - название криптопровайдера выбирается из списка.
- **Страна** - государство / область владельца ключей (2-х буквенный код). Поле является обязательным для заполнения.
- **Штат** - район владельца ключей. Поле является обязательным для заполнения.
- **Город** - город владельца ключей. Поле является обязательным для заполнения.
- **Организация** - название АРМ. Заполняется автоматически.
- **Департамент** - подразделение организации владельца ключей.
- **Идентификатор** - название профиля абонента. Заполняется автоматически.

- **E-mail** - электронный адрес абонента.
- **Область применения сертификата** - перечисление через ";".
- **Область применения секретного ключа** - перечисление через ";".
- **Экспортируемый секретный ключ** - значение поля выбирается из списка.
- **Тип запроса** - тип запроса на сертификат. Заполняется автоматически. Значение по умолчанию изменять не рекомендуется.

B.2. Параметры генерации при использовании СКЗИ Crypto Pro CSP/1.1

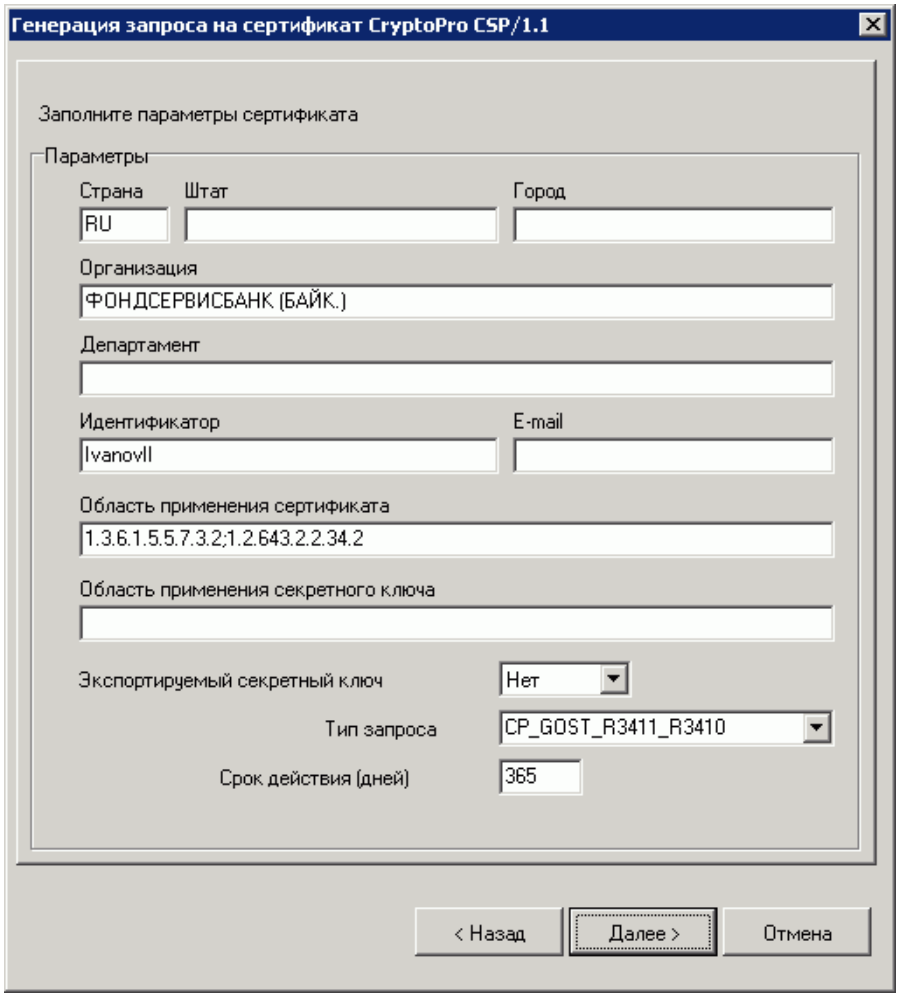


Рис. B.2. Окно Генерация запроса на сертификат CryptoPro CSP/1.1

- **Страна** - государство / область владельца ключей (2-х буквенный код). Поле является обязательным для заполнения.
- **Штат** - район владельца ключей. Поле является обязательным для заполнения.
- **Город** - город владельца ключей. поле является обязательным для заполнения.

- **Организация** - название АРМ. Заполняется автоматически.
- **Департамент** - подразделение организации владельца ключей.
- **Идентификатор** - название профиля абонента. Заполняется автоматически.
- **E-mail** - электронный адрес абонента.
- **Область применения сертификата** - перечисление через ";".
- **Область применения секретного ключа** - перечисление через ";".
- **Экспортируемый секретный ключ** - значение поля выбирается из списка.
- **Тип запроса** - тип запроса на сертификат. Заполняется автоматически. Значение по умолчанию изменять не рекомендуется.
- **Срок действия (дней)** - срок действия ключа в днях. По умолчанию 365.

B.3. Параметры генерации при использовании СКЗИ Crypto-C

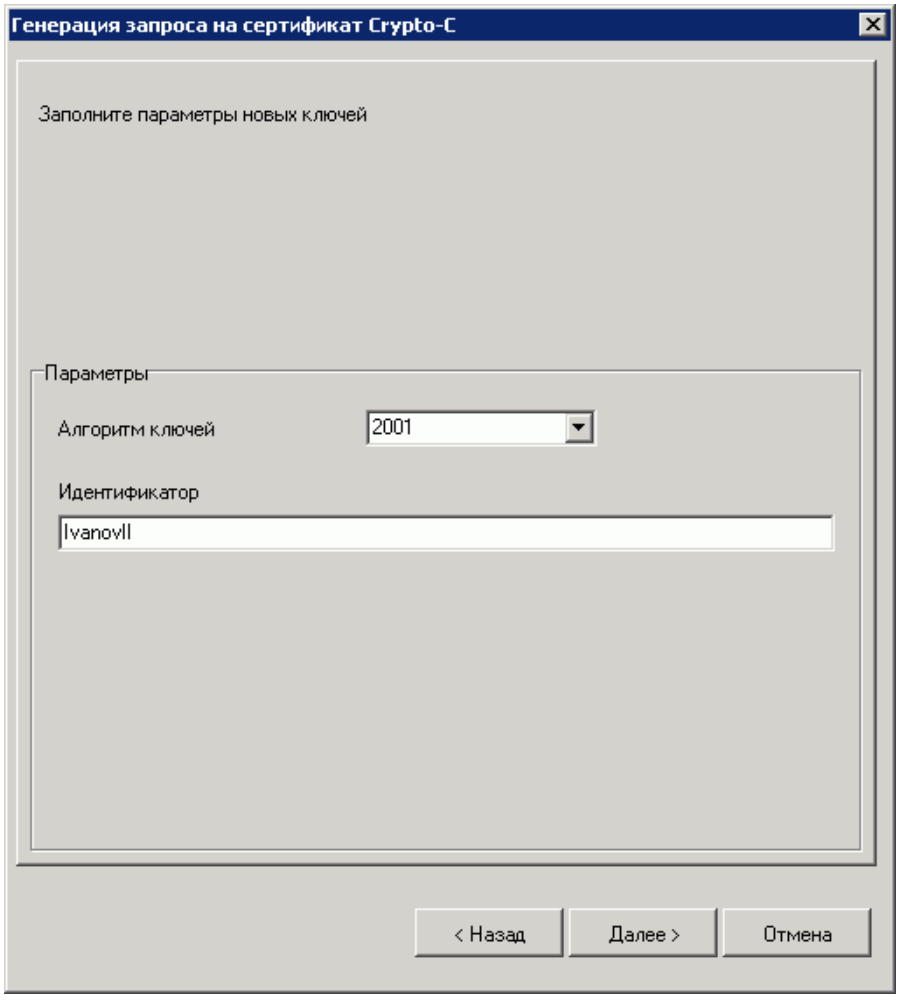


Рис. B.3. Окно Генерация запроса на сертификат Crypto-C

- **Алгоритм ключей** - допускаются значения:
  - "1994" - ГОСТ 34.10-1994;
  - "2001" - ГОСТ 34.10-2001.
- **Идентификатор** - название профиля абонента. Заполняется автоматически.

B.4. Параметры генерации при использовании СКЗИ M-PRO v2.x

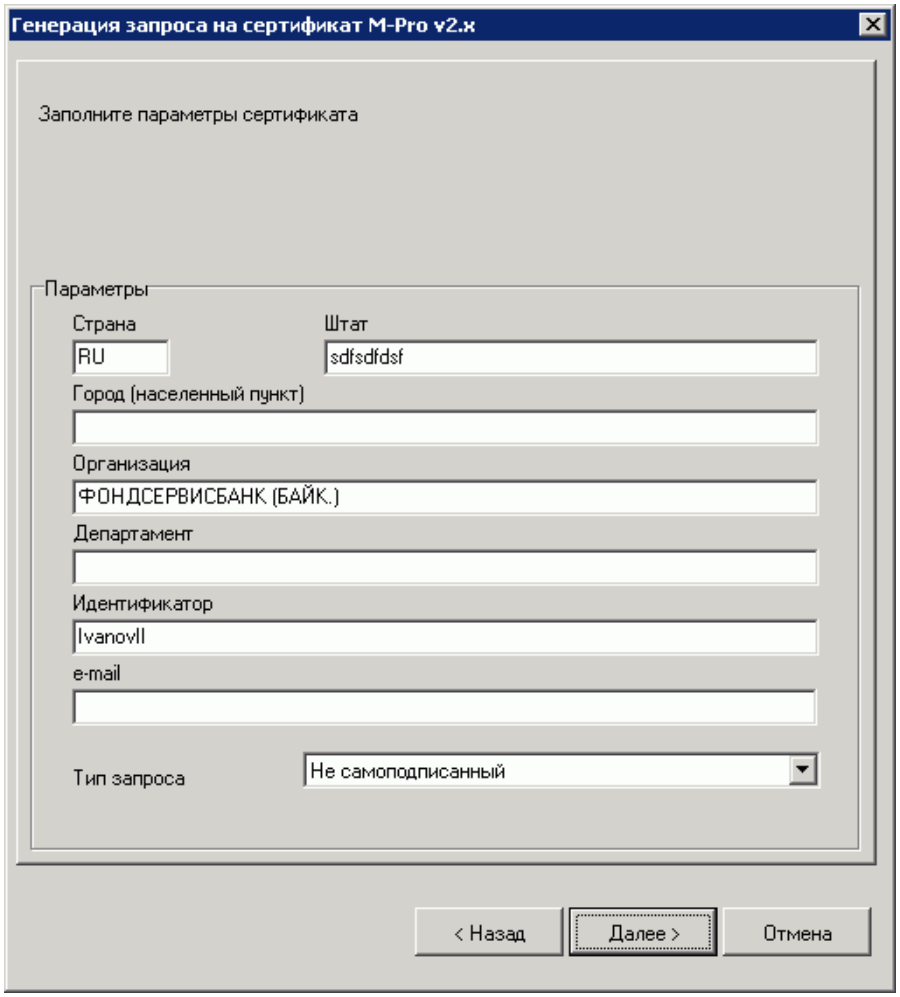


Рис. B.4. Окно Генерация запроса на сертификат M-Pro v2.x

- **Страна** - государство / область владельца ключей (2-х буквенный код). Поле является обязательным для заполнения.
- **Штат** - район владельца ключей. Поле является обязательным для заполнения.
- **Город** - город владельца ключей. поле является обязательным для заполнения.
- **Организация** - название АРМ. Заполняется автоматически.

- **Департамент** - подразделение организации владельца ключей.
- **Идентификатор** - название профиля абонента. Заполняется автоматически.
- **E-mail** - электронный адрес абонента.
- **Тип запроса** - тип запроса на сертификат. Заполняется автоматически. Значение по умолчанию изменять не рекомендуется.

B.5. **Параметры генерации при использовании СКЗИ** M-PRO v1.34 (GOST PSE)

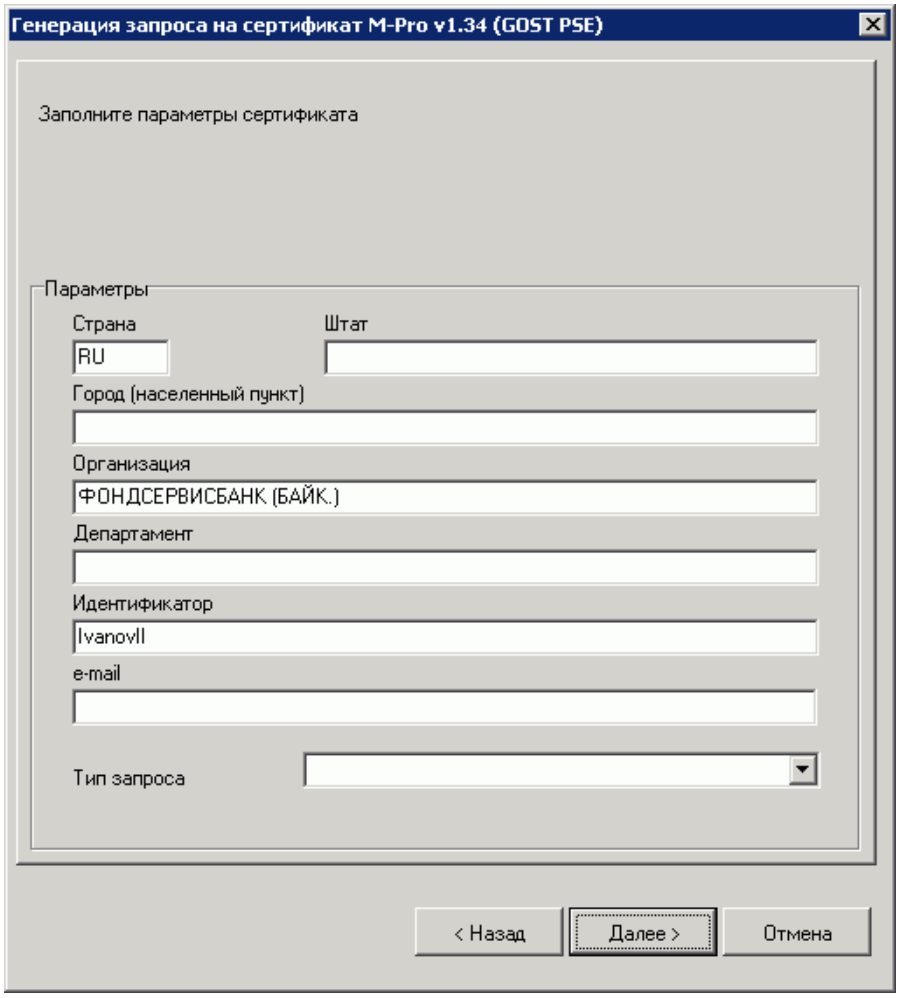


Рис. B.5. Окно Генерация запроса на сертификат M-Pro v1.34 (GOST PSE)

- **Страна** - государство / область владельца ключей (2-х буквенный код). Поле является обязательным для заполнения.
- **Штат** - район владельца ключей. Поле является обязательным для заполнения.
- **Город** - город владельца ключей. поле является обязательным для заполнения.

- **Организация** - название АРМ. Заполняется автоматически.
- **Департамент** - подразделение организации владельца ключей.
- **Идентификатор** - название профиля абонента. Заполняется автоматически.
- **E-mail** - электронный адрес абонента.
- **Тип запроса** - тип запроса на сертификат. Заполняется автоматически. Значение по умолчанию изменять не рекомендуется.

B.6. **Параметры генерации при использовании СКЗИ** Message-PRO 1.1

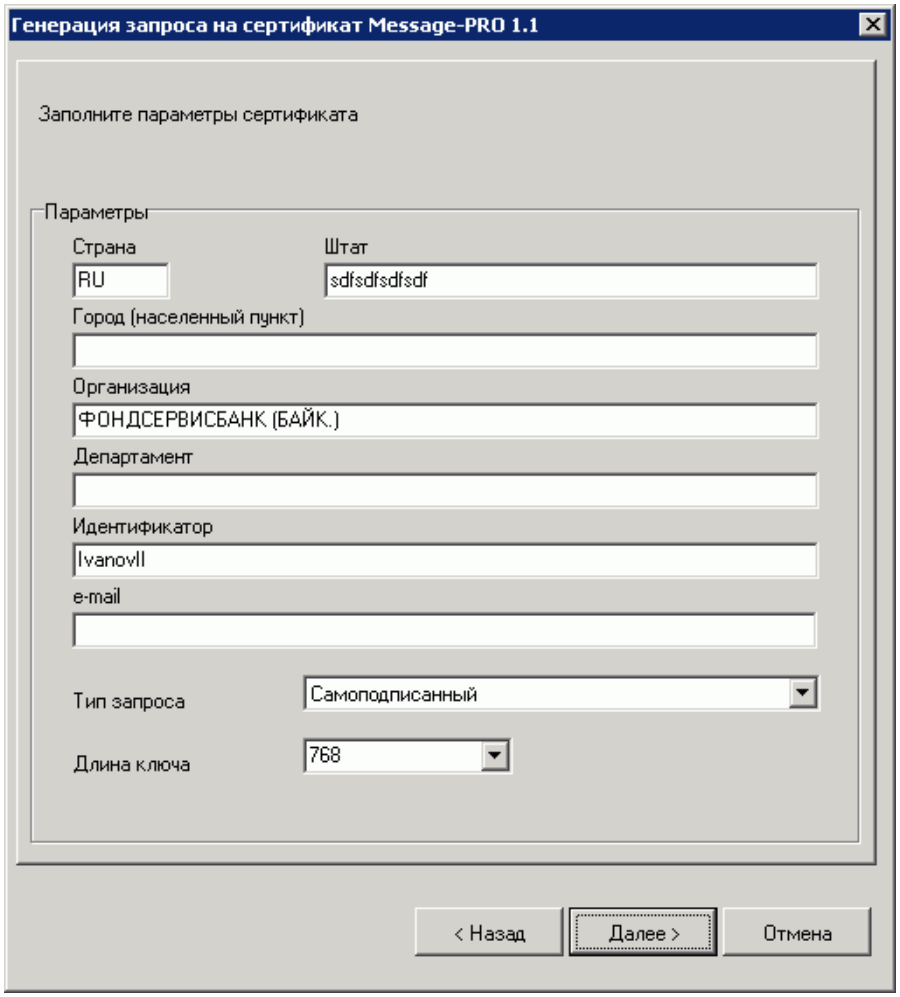


Рис. B.6. Окно Генерация запроса на сертификат Message-Pro 1.1

- **Страна** - государство / область владельца ключей (2-х буквенный код). Поле является обязательным для заполнения.
- **Штат** - район владельца ключей. Поле является обязательным для заполнения.
- **Город** - город владельца ключей. Поле является обязательным для заполнения.

- **Организация** - название АРМ. Заполняется автоматически.
- **Департамент** - подразделение организации владельца ключей.
- **Идентификатор** - название профиля абонента. Заполняется автоматически.
- **E-mail** - электронный адрес абонента.
- **Тип запроса** - тип запроса на сертификат. Заполняется автоматически. Значение по умолчанию изменять не рекомендуется.
- **Шифрация** - алгоритм шифрования. Заполняется автоматически. Значение по умолчанию изменять не рекомендуется.

B.7. **Параметры генерации при использовании СКЗИ** Crypto COM 2.2

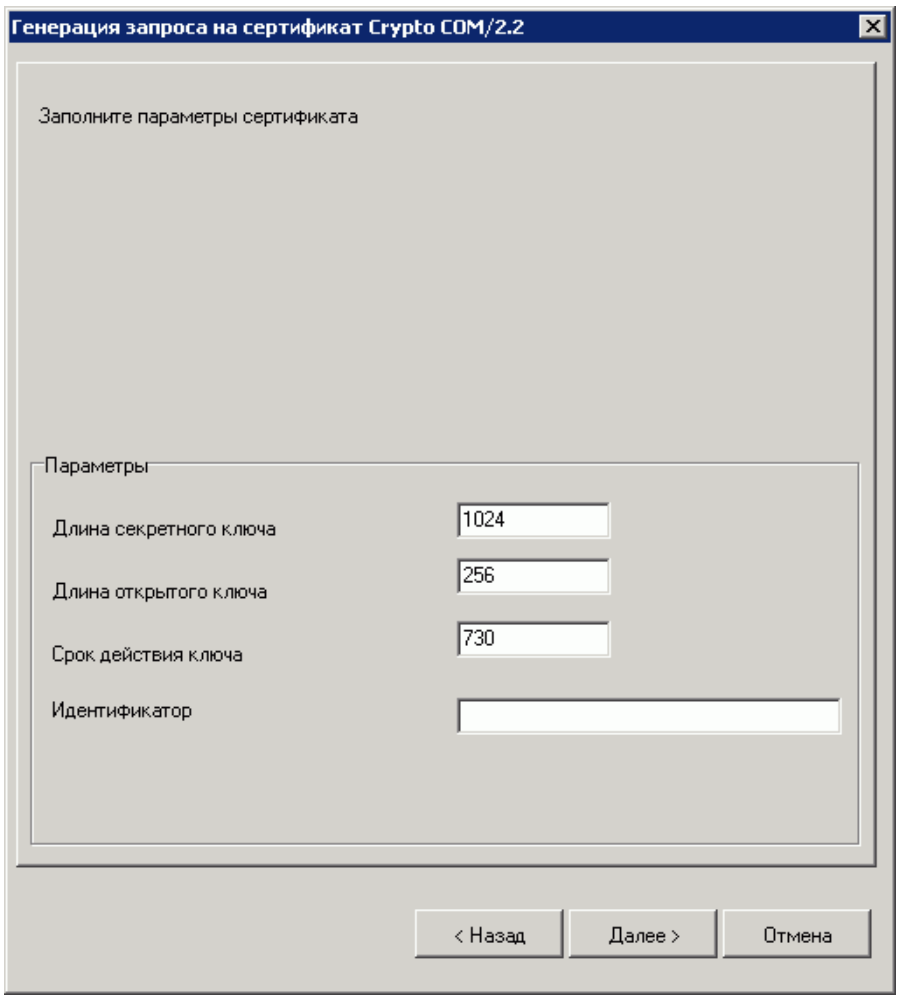


Рис. B.7. Окно Генерация запроса на сертификат Crypto COM/2.2

- **Длина секретного ключа** - длина секретного ключа (бит). По умолчанию 1024 для Gost.
- **Длина открытого ключа** - длина открытого ключа (бит). По умолчанию 256 для Gost.

- **Срок действия ключа** - период действия ключа (суток). По умолчанию 730.
- **Идентификатор** - идентификатор ключа банка. Необходимо узнать у сотрудника службы безопасности банка, который отвечает за генерацию ключа.

B.8. **Параметры генерации при использовании СКЗИ** Open SSL

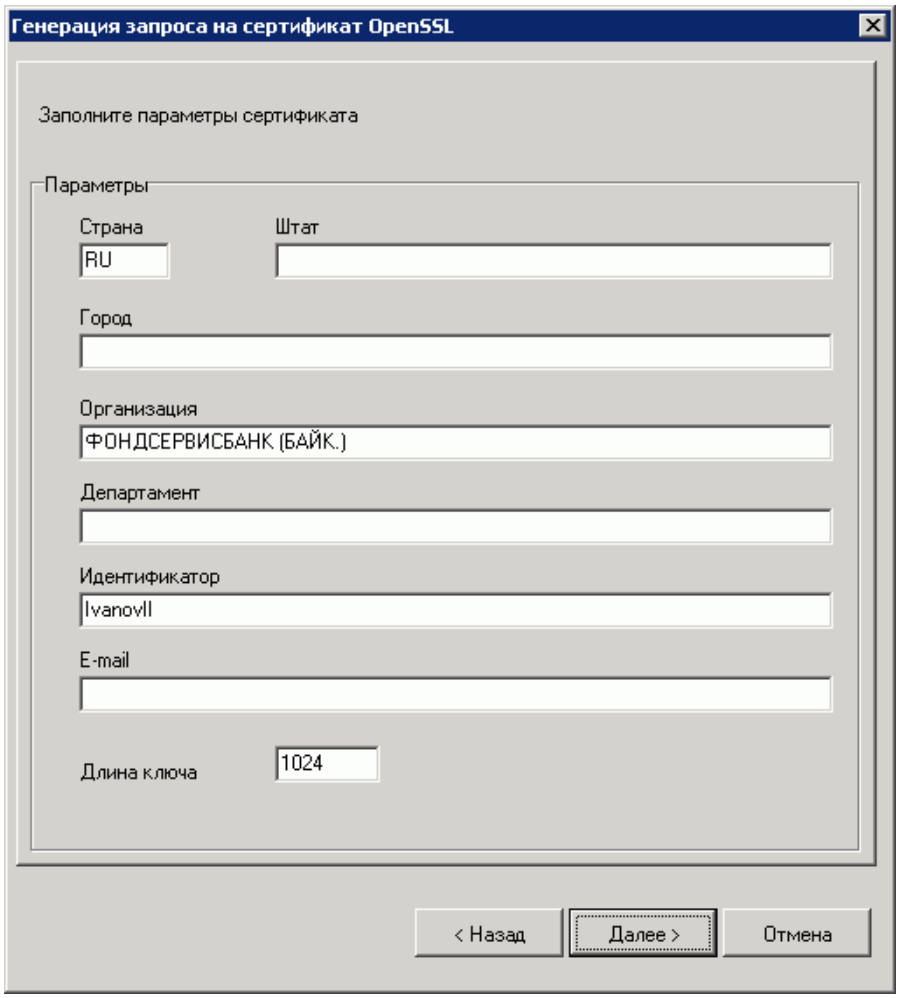


Рис. B.8. Окно Генерация запроса на сертификат OpenSSL

- **Страна** - государство / область владельца ключей (2-х буквенный код). Поле является обязательным для заполнения.
- **Штат** - район владельца ключей. Поле является обязательным для заполнения.
- **Город** - город владельца ключей. поле является обязательным для заполнения.
- **Организация** - название АРМ. Заполняется автоматически.
- **Департамент** - подразделение организации владельца ключей.
- **Идентификатор** - название профиля абонента. Заполняется автоматически.

- **E-mail** - электронный адрес абонента.
- **Длина ключа** - длина секретного ключа (бит). От 512 до 2048, кратно 8-ми (влияет на генерацию и перегенерацию ключей). По умолчанию 1024.

Приложение C. Параметры использования ключевых наборов для различных СКЗИ

C.1. Параметры использования ключевых наборов Excellence 4.0

Таблица C.1. Параметры использования ключевых наборов Excellence 4.0

Параметр	Значение	Значение по умолчанию
Mnemonic user name	Название пользователя, под которым будет осуществляться вход в систему криптозащиты Excellence	
Secret key directory	Путь к каталогу секретного ключа, с помощью которого подписывается/проверяется подпись	
Public key directory	Путь к каталогу открытых ключей, с помощью которого подписывается/проверяется подпись	
Signature algorithm	Алгоритм подписи: GOST – алгоритм ГОСТ Р34.10-94, RSA – алгоритм RSA	GOST
Encryption algorithm	Алгоритм шифрования: GOST - алгоритм ГОСТ 28147-89. Значение параметра оставить по умолчанию	GOST
Work directory	Рабочий каталог СКЗИ	
Language	Язык сообщений (RU-русский, EN-английский)	
Signature key length	Длина ключа подписи. Значение параметра оставить по умолчанию	512
Encrypt for UID	Не используется	
New abonent name	Идентификатор пользователя. Размер поля не должен превышать 255 символов	
Exchange key length	Длина в битах секретного ключа обмена (шифрования)	
Password request time out	Таймаут запроса пароля с ключевого устройства (Touch memory); задает сколько секунд хранить пароль в кэше с момента последнего запроса пароля; значение по умолчанию 60 при необходимости можно изменить; с помощью данного параметра производится настройка кэша. Возможно хранение нескольких паролей в кэше. Для каждого UID пользователя в кэше хранится свой пароль. Для структур с таблетки Touch Memory хранится одна запись в кэше, т.к. UID пользователя находится на самой таблетке и без считывания информации невозможно определить, чей ключ находится в кэше	60
Master key file	Имя файла с мастер-ключом для ключей, защищенных мастер-ключом	

Параметр	Значение	Значение по умолчанию
Last operation password time out	Период запроса пароля с момента выполнения последней операции (значение по умолчанию 5 при необходимости можно изменить); задает сколько секунд хранить пароль в кэше с момента последнего использования пароля	5
Template directory	Директория для хранения временных файлов, использующихся при удаленной генерации	
Device dll	Полный путь и имя файла библиотеки поддержки ключевого устройства	
Port number	Номер порта, к которому подсоединено ключевое устройство	
Device type	Тип ключевого устройства	
Use previous keys for decrypt	Используется для расшифровывания блоков памяти, зашифрованных отправителем на старых открытых ключах шифрования. Допустимые значения: • пустая строка, 0 (ноль) - использовать текущий секретный ключ для расшифровывания; • отрицательные числа (-1,-2,-3,.....) – использовать предыдущий, предшествовавший предыдущему и т.д. по мере убывания (естественно, надо задавать какое-нибудь одно число); • положительные числа - использовать ключ с заданным номером. Рекомендуется пользоваться отрицательными числами	
Touch Memory Window Time Out	Время в секундах ожидания таблетки; если в момент операции, требующей наличия таблетки Touch Memory в считывателе, ее там не оказалось, выдается окно типа "Вставьте таблетку в считыватель". Новый параметр определяет, сколько секунд это окно будет висеть на экране (ожидать, пока таблетку не вставят). Если пользователь так и не вставит таблетку, окно закрывается и выдается ошибка типа "отсутствует таблетка"	

C.2. **Параметры использования ключевых наборов** CryptoPro CSP 1.1

Таблица C.2. **Параметры использования ключевых наборов** CryptoPro CSP 1.1

Параметр	Значение	Значение по умолчанию
User UID (Common name)	Имя сертификата (соответствует имени ключевого контейнера); если параметр User UID (Common name) не задан	

Параметр	Значение	Значение по умолчанию
	(пустая строка), читается UID из сертификата, указанного в параметре User certificate file; в этом случае не происходит инициализация справочника сертификатов и проверка их подлинности. если же User UID (Common name) задан, все эти операции запускаются; кроме этого происходит сравнение User UID (Common name) и того, что находится в сертификате; в случае несовпадения значений выдается ошибка Регистр букв имеет значение!	
User certificate file	Полный путь и имя файла сертификата текущего пользователя	A:\Self.cer
CA certificates dir	Полный путь к каталогу, содержащему корневые сертификаты Сертификационных центров (CA)	A:\CA
Abonents cerificates dir	Путь к каталогу, содержащему сертификаты абонентов и сертификаты не корневых CA (т.е. несамоподписанные CA)	A:\BONNET
Hash Algorithm	Алгоритм хеширования (допускаются следующие значения: GOST_R3411, SHA1, MD2, MD5)	GOST_R3411
Encrypt Algorithm	Алгоритм шифрования (допускаются следующие значения: GOST_28147, RC2CBC, RC4, DESCBC)	GOST_28147
Encrypt for UID	При вызове функции EncodeData с пустой строкой вместо UID получателя, шифрование производится на UID, заданный этим параметром (используется только для работы Defender'ов)	
Key request time out	Задает время в секундах хранения кэша с момента последнего считывания ключа с дискеты	60
Last operation key time out	Время в секундах хранения ключа в кэше с момента последнего использования ключа	5
Key gen - Common name	UID (Common name) нового пользователя	New
Key gen - e-mail	e-mail владельца ключей	new@new.ru
Key gen - Company	Организация владельца ключей	New User Company
Key gen - Department	Подразделение организации владельца ключей	New User Department
Key gen - City	Город владельца ключей	New User City
Key gen - State	Район владельца ключей	New User State
Key gen - Country/ Region	Государство/область владельца ключей (2-х буквенный код)	RU
Key gen - Request filename	Полный путь и имя файла запроса на сертификат	A:\new.req
Key gen - Request Type	Тип запроса на сертификат (свой для каждого провайдера); возможные значения: RSA_MD5RSA, RSA_SHA1RSA, X957_SHA1DSA, либо маска алгоритма, например	для Crypto Pro: CP_GOST_R3411_R3410

Параметр	Значение	Значение по умолчанию
	1.2.643.2.2.4 соответствует CP_GOST_R3411_R3410; данный параметр зависит от типа ключей заданного провайдера	
Key gen - Expire period	Период действия сертификата (в сутках); данный параметр служит для формирования атрибута "срок действия будущего сертификата"; используется при генерации новых ключей и при перегенерации	365
User UID Location	Задает место хранения UID в сертификатах; распространяется на все сертификаты допустимые значения: CN,L,S,O,OU,E,SN соответствуют различным частям Subject сертификата; CN - Common Name (по умолчанию); O – Organization и т.д.; SN - UID = серийному номеру сертификата	CN
Container Name Location	Место хранения имени ключевого контейнера в сертификате допустимые значения: CN,L,S,O,OU,E - соответствуют различным частям Subject сертификата; CN - Common Name (по умолчанию) O - Organization и т.д. TITLE - имя контейнера хранится в поле TITLE extension сертификата.	

C.3. **Параметры использования ключевых наборов** Crypto COM 2.2

Таблица C.3. **Параметры использования ключевых наборов** Crypto COM 2.2

Параметр	Значение	Значение по умолчанию
Current dir	Путь до корневого каталога ключей (включительно), в котором находятся каталоги CRT и SEC (или SEC0)	A:\
Secret Path	Путь до подкаталога секретных ключей каталога SEC (или SEC0) (информация в каталоге секретна!)	A:\sec
Public Path	Путь до подкаталога открытых ключей CRT и сертификатов	A:\crt
User Id		H.0
Hash Algorithm	Алгоритм хеширования (возможные значения: 34.11, MD5, SQR)	34.11
Cipher Algorithm	Алгоритм шифрования (возможные значения: 28147, 28147-ECB, DES, DES-ECB)	28147
Random file	Имя файла (с полным путем) контекста генератора случайных чисел (информация в файле секретна!). Полный путь к файлу @rand. Обычно лежит либо в SEC, либо на одном уровне с каталогами CRT и SEC	A:\@rand

Параметр	Значение	Значение по умолчанию
	Внимание! Необходимо отметить, что Random File - информация, которую не стоит хранить на винчестере. Это начальный вектор инициализации датчика случайных чисел. Его стоит оберегать от доступа, наравне с секретными ключами. Кэширование этого файла обеспечивается стандартными методами, поэтому можно смело записывать его на дискету, вместе с секретными ключами.	
Encrypt for UID	Для банковских ЭЦП здесь ничего не пишется, для Клиентов здесь пишется UID той банковской подписи, которая будет использоваться банком для идентичных действий; используется для работы Defender'ов. При вызове функции EncodeData с пустой строкой вместо UID получателя, шифрование производится на UID, заданный эти параметром;	H.0
Key request time out	Время в секундах хранения КЭШа с момента последнего считывания ключа с дискеты	60
Last operation key time out	Время в секундах хранения ключа в КЭШе с момента последнего использования ключа	5
Verify validity of cert and key files	Используется для проверки подлинности и срока действия сертификатов и секретных ключей **Примечание** Чтобы включить проверку, необходимо установить значение нового параметра ="Yes" или "Да" в противном случае проверка подлинности и срока действия производиться не будет. Для того чтобы произвести проверку подлинности сертификатов, необходимо чтобы в каталоге, заданном параметром "Secret Path", находились сертификаты сертификационных центров (это файлы с расширением 'aut'). Сертификаты должны быть разложены по подкаталогам в соответствии с правилами хранения сертификатов CryptoCom по тому же принципу, что и сертификаты абонентов в каталоге сертификатов.	Yes
Use Intel Hardware Random driver	Параметр использования Intel Hardware Cryptographic Service Provider для подпитки генератора случайных чисел Crypto Com 2.2 **Примечание** Если значение этого параметра "Yes" или "Да", для подпитки используется аппаратный генератор случайных чисел, входящий в Intel Hardware Cryptographic Service Provider. Если параметр имеет значение "No", подпитка генератора осуществляется штатными средствами Crypto Com 2.2. Для использования аппаратного генератора случайных чисел необходимо: 1.Убедиться, что материнская плата компьютера имеет чипсет i810 или i815. 2.Проинсталлировать Intel Hardware Cryptographic Service Provider.	No

Параметр	Значение	Значение по умолчанию
	3.Проинсталлировать драйвер случайных чисел Intel Hardware Random driver. **Внимание**! Указанный драйвер может использоваться ТОЛЬКО на компьютерах с чип сетом i810 или i815. На других компьютерах параметр Use Intel Hardware Random driver должен быть установлен в "No"! Иначе нельзя гарантировать корректную работу драйвера случайных чисел Crypto Com 2.2. В случае ошибок при работе с драйвером Intel Hardware Random driver будет выдана ошибка с кодом 7 - Can not initialize Intel Hardware Random driver 81x либо ошибка Crypto API (большое отрицательное число).	
Key gen - Subject	UID новых ключей; используется при генерации ключей для библиотеки Crypto Com 2.2	
Key gen - Dir	Директория, в которую будут помещены ключи; используется при генерации ключей для библиотеки Crypto Com 2.2	A:\
Template dir	Директория для хранения временных файлов, использующихся при удаленной генерации	C:\
Key gen - Secret key length	Длина секретного ключа (бит); используется при генерации и перегенерации ключей;	1024 для Gost
Key gen - Public key length	Длина открытого ключа (бит); используется при генерации и перегенерации ключей;	256 для Gost
Key gen - Key expire period	Период действия ключа (суток); используется при генерации и перегенерации ключей	730
Current user certificate	Текущий сертификат владельца набора ключей; должен находиться в каталоге, заданном параметром Current dir	A:\self.crt

C.4. **Параметры использования ключевых наборов** Message-PRO 1.1

Таблица C.4. **Параметры использования ключевых наборов** Message-PRO 1.1

Параметр	Значение	Значение по умолчанию
Current certificate	Текущий сертификат владельца набора ключей; должен находиться в каталоге, заданном параметром Certificates directory	
Certificates directory	Полный путь к каталогу, в котором находятся все сертификаты; файлы сертификатов абонентов имеют имя = их UID (Common Name) и расширение .pem	

Параметр	Значение	Значение по умолчанию
Private disk/ directory	Директория подкаталога KEYS, в котором содержится текущий секретный ключ key.pem	
Cipher algorithm	Алгоритм шифрования	
Digest algorithm	Алгоритм для подписи	SHA1
Key length	Длина ключа должна быть не меньше 768	768
New private key	Полное имя файла, нового (перегенерированного ключа)	
Encrypt key on password	Параметр, указывающий на наличие или отсутствие пароля к ключу	
Certificate request	Путь к файлу запроса на сертификат ключа обмена	
Request signature key	Путь к файлу запроса на сертификат ключа подписи	
Country	Страна	
State or province	Область	
Locality	Город	
Organization	Организация владельца ключей	
Organization unit	Подразделение организации	
Common name	UID (Common name) нового пользователя; ограничение на длину - 40 символов	
E-mail address	e-mail владельца ключей	
Detail error file	Путь к лог-файлу	
Encrypt for UID	Если не задан UID получателя, шифрование производится на UID, заданный этим параметром (используется только для работы Defender'ов)	
Encode for UID	В параметре Encode for UID необходимо задавать UID (Common Name) получателя	
UID Type	Место хранения UID в сертификате пользователя; допустимые значения: CN - Common Name; SN - Серийный номер **Примечание** При использовании серийного номера сертификата в качестве UID файлы, находящиеся в каталоге сертификатов, автоматически переименовываются в соответствии с их серийными номерами, без пробелов, с сохранением регистра. Кроме этого, сертификат текущего пользователя необходимо хранить как в каталоге сертификатов с именем файла, соответствующим его UID, так и вне этого каталога с произвольным именем. Параметр Current Certificate этого пользователя должен быть настроен на файл вне каталога сертификатов.	
Request signature type	Тип запроса на сертификат	

C.5. Параметры использования ключевых наборов M-Pro v1.34 (GOST PSE)

Таблица C.5. Параметры использования ключевых наборов M-Pro v1.34 (GOST PSE)

Параметр	Значение	Значение по умолчанию
Current certificate	Текущий сертификат владельца набора ключей; должен находиться в каталоге, заданном параметром Certificates directory	
Certificates directory	Полный путь к каталогу, в котором находятся все сертификаты	
Private disk/ directory	Директория подкаталога KEYS, в котором содержится текущий секретный ключ key.pem	
Cipher algorithm	Алгоритм шифрования	RUS-GAMMAR
Digest algorithm	Алгоритм для подписи	R3410-R3411
Key length	Длина ключа	1024
New private key	Полное имя файла, нового (перегенерированного ключа)	
Encrypt key on password	Параметр, указывающий на наличие или отсутствие пароля к ключу	
Certificate request	Путь к файлу запроса на сертификат ключа обмена	
Request signature key	Путь к файлу запроса на сертификат ключа подписи	
Country	Страна	
State or province	Область	
Locality	Город	
Organization	Организация владельца ключей	
Organization unit	Подразделение организации	
Common name	UID (Common name) нового пользователя; ограничение на длину - 40 символов	
E-mail address	e-mail владельца ключей	
Detail error file	Путь к лог-файлу	
Encrypt for UID	Если не задан UID получателя, шифрование производится на UID, заданный этим параметром (используется только для работы Defender'ов)	
Encode for UID	В параметре Encode for UID необходимо задавать UID (Common Name) получателя	
UID Type	Место хранения UID в сертификате пользователя; допустимые значения: CN - Common Name; SN - Серийный номер	

Параметр	Значение	Значение по умолчанию
	Примечание При использовании серийного номера сертификата в качестве UID файлы, находящиеся в каталоге сертификатов, автоматически переименовываются в соответствии с их серийными номерами, без пробелов, с сохранением регистра. Кроме этого, сертификат текущего пользователя необходимо хранить как в каталоге сертификатов с именем файла, соответствующим его UID, так и вне этого каталога с произвольным именем. Параметр Current Certificate этого пользователя должен быть настроен на файл вне каталога сертификатов.	
Request signature type	Тип запроса на сертификат	
Private keys timeout	Используется при кэшировании секретного ключа	
New Keys Path	Путь к каталогу, в котором находится новый (перегенерированный) секретный ключ	

C.6. Параметры использования ключевых наборов M-Pro v2.x

Таблица C.6. Параметры использования ключевых наборов M-Pro v2.x

Параметр	Значение	Значение по умолчанию
Current certificate	Текущий сертификат владельца набора ключей; должен находиться в каталоге, заданном параметром Certificates directory	
Certificates directory	Полный путь к каталогу, в котором находятся все сертификаты	
Private disk/ directory	Директория подкаталога KEYS, в котором содержится текущий секретный ключ key.pem	
Cipher algorithm	Алгоритм шифрования	RUS-GAMMAR
Digest algorithm	Алгоритм для подписи	R3410-R3411
Key length	Длина ключа	1024
New private key	Полное имя файла, нового (перегенерированного ключа)	
Encrypt key on password	Параметр, указывающий на наличие или отсутствие пароля к ключу	
Certificate request	Путь к файлу запроса на сертификат ключа обмена	
Request signature key	Путь к файлу запроса на сертификат ключа подписи	
Country	Страна	
State or province	Область	

Параметр	Значение	Значение по умолчанию
Locality	Город	
Organization	Организация владельца ключей	
Organization unit	Подразделение организации	
Common name	UID (Common name) нового пользователя; ограничение на длину - 40 символов	
E-mail address	e-mail владельца ключей	
Detail error file	Путь к лог-файлу	
Encrypt for UID	Если не задан UID получателя, шифрование производится на UID, заданный этим параметром (используется только для работы Defender'ов)	
Encode for UID	В параметре Encode for UID необходимо задавать UID (Common Name) получателя	
UID Type	Место хранения UID в сертификате пользователя; допустимые значения: CN - Common Name; SN - Серийный номер **Примечание** При использовании серийного номера сертификата в качестве UID файлы, находящиеся в каталоге сертификатов, автоматически переименовываются в соответствии с их серийными номерами, без пробелов, с сохранением регистра. Кроме этого, сертификат текущего пользователя необходимо хранить как в каталоге сертификатов с именем файла, соответствующим его UID, так и вне этого каталога с произвольным именем. Параметр Current Certificate этого пользователя должен быть настроен на файл вне каталога сертификатов.	
Request signature type	Тип запроса на сертификат	
Private keys timeout	Используется при кэшировании секретного ключа	
New Keys Path	Путь к каталогу, в котором находится новый (перегенерированный) секретный ключ	
Title	Параметр зарезервирован	

C.7. Параметры использования ключевых наборов LanCrypto 2.35

Таблица C.7. Параметры использования ключевых наборов LanCrypto 2.35

Параметр	Значение	Значение по умолчанию
Sign private key	Путь к секретному ключу, с помощью которого подписывается/проверяется подпись	

Параметр	Значение	Значение по умолчанию
Sign vault	путь к файлу открытых ключей, с помощью которых подписывается/проверяется подпись	
Sign method	Значение параметра определяется автоматически, оставить по умолчанию	
Sign UID	Идентификатор открытого ключа, указанного в параметре Sign private key	
Encrypt private key	Путь к секретному ключу, с помощью которого производится шифрование/дешифрование	
Encrypt vault	Путь к файлу открытых ключей, с помощью которого производится шифрование/дешифрование	
Encrypt method	Значение параметра определяется автоматически, оставить по умолчанию	
Encrypt UID	Шифровать по умолчанию (для Defender'а); значение, определяемое автоматически, менять которое убедительно не рекомендуется	
New user name	Идентификатор пользователя	
New short user name	Имя владельца секретного ключа	
New key expire period	Время действия ключа в месяцах	
Touch memory port number	Номер порта, к которому подсоединено ключевое устройство (Touch memory); может не быть	
Password/TM Request Time Out	Таймаут запроса пароля с ключевого устройства (Touch memory); с помощью данного параметра производится настройка кэша. Возможно хранение нескольких паролей в кэше. Для каждого UID пользователя в кэше хранится свой пароль. Для структур с таблетки Touch Memory хранится одна запись в кэше, т.к. UID пользователя находится на самой таблетке и без считывания информации невозможно определить, чей ключ находится в кэше	
Encrypt for UID	Шифровать по умолчанию; если Encrypt for UID заполнен, шифрование производится на значение этого параметра; если параметр Encrypt for UID не заполнен, шифрование производится на UID, заданный параметром Encrypt UID (используется только для работы Defender'ов);	
Touch Memory Window Time Out	Время в секундах ожидания таблетки; если в момент операции, требующей наличия таблетки Touch Memory в считывателе, ее там не оказалось, выдается окно типа "Вставьте таблетку в считыватель". Новый параметр определяет, сколько секунд это окно будет висеть на экране (ожидать, пока таблетку не вставят). Если пользователь так и не вставит таблетку, окно закрывается и выдается ошибка типа "отсутствует таблетка";	

Параметр	Значение	Значение по умолчанию
Template directory	Директория для хранения временных файлов, использующихся при удаленной генерации	

C.8. Параметры использования ключевых наборов Verba-OW/4

Таблица C.8. Параметры использования ключевых наборов Verba-OW/4

Параметр	Значение	Значение по умолчанию
Path to secret	Путь к каталогу с ключами (в каталоге должны быть подкаталоги DB1,DB2,HD1,HD2 и файлы gk.db3 и uz.db3)	A:\
Path to public	Путь к открытым ключам подписи (к каталогу, содержащему каталоги Faxkey и Openkey)	A:\
Key serial number	Номер серии ключей (6 цифр, начиная с 5-ой в UID подписи). **Внимание!** Этот номер у банка и Клиента должен совпадать	
Encode UID	Собственный UID шифрования; то, что появляется в окне программы asrkeyw в колонке "шифрование" после загрузки ключей	
Sign UID	Собственный UID подписи; то, что появляется на стороне банка в окне программы asrkeyw в колонке "подпись" после загрузки ключей	
Encrypt for key number	Номер абонента, на которого производится шифрование; первые четыре символа UID шифрования получателя	
Key device	Ключевое устройство; может быть таблетка Touch memory	a:
Key request time out	Период хранения КЭШа с момента последнего считывания ключа с дискеты (в секундах)	
Last operation key time out	Время в секундах хранения ключа в КЭШе с момента последнего использования ключа	5
Use 0 slot for verify signature	Может принимать значения 'Yes' ('Да'), или что-то еще, что воспринимается, как 'No'. Если данный параметр установлен в 'Yes' ('Да'), считается, что проверка подписи может осуществляться только из 0-ого слота, в противном случае допускается проверка подписи из любого слота	No
Reset key in drv on start	Может принимать значения 'Yes' ('Да'), или что-то еще, что воспринимается, как 'No'. При значении ‘No’ ключи, находящиеся в драйвере asrwkey до выполнения первой после загрузки криптографической операции считаются загруженными туда в момент этой операции (т.е. при наличии в asrwkey ключей информация о них заносится в кэш). При других зна-	Yes

Параметр	Значение	Значение по умолчанию
	чениях параметра ключи, находящиеся в asrwkey, считаются просроченными и игнорируются	
Touch Memory Window Time Out	Время в секундах ожидания таблетки; используется только в случае таблетки Touch memory; если в момент операции, требующей наличия таблетки Touch Memory в считывателе, ее там не оказалось, выдается окно типа "Вставьте таблетку в считыватель". Новый параметр определяет, сколько секунд это окно будет висеть на экране (ожидать, пока таблетку не вставят). Если пользователь так и не вставит таблетку, окно закрывается и выдается ошибка типа "отсутствует таблетка"	5

C.9. Параметры использования ключевых наборов Open SSL

Таблица C.9. Параметры использования ключевых наборов Open SSL

Параметр	Значение	Значение по умолчанию
User Secret key	Имя файла секретного ключа	A:\self.key
User Certificate	Полный путь и имя файла сертификата текущего пользователя	A:\self.cer
Abonents dir	Путь к каталогу, содержащему сертификаты абонентов и сертификаты не корневых CA (т.е. несамоподписанные CA)	A:\ABONENTS
CA dir	Полный путь к каталогу, содержащему корневые сертификаты Сертификационных центров (CA)	A:\CA
CRL dir	Значение по умолчанию	A:\CRL
RND file	Имя файла инициализации датчика случайных чисел	A:\@rand
Hash Method	Алгоритм хеширования (допустимые значения: SHA, MD5)	SHA
Encrypt Method	Алгоритм шифрования (допускаются следующие значения: RC4, RC2_ECB, RC2_CBC, RC5_ECB, RC5_CBC);	RC4
Encrypt for UID	При вызове функции EncodeData с пустой строкой вместо UID получателя, шифрование производится на UID, заданный этим параметром (используется только для работы Defender'ов)	User1
Key request time out	Задает время в секундах хранения кэша с момента последнего считывания ключа с дискеты	60
Last operation key time out	Время в секундах хранения ключа в кэше с момента последнего использования ключа	5
Key gen - Key Length	Длина ключа; от 512 до 2048 кратно 8-ми (влияет на генерацию и перегенерацию ключей)	1024
Key gen - Common name	UID (Common name) нового пользователя	User1

Параметр	Значение	Значение по умолчанию
Key gen - e-mail	e-mail владельца ключей	User1@usermail.ru
Key gen – Company	Организация владельца ключей	BSS
Key gen – Department	Подразделение организации владельца ключей	Development
Key gen – City	Город владельца ключей	Moscow
Key gen – State	Район владельца ключей	RU
Key gen - Country/ Region	Государство/область владельца ключей (2-х буквенный код	Russia
Key gen - PKey filename	Имя файла, куда писать запрос на сертификат	A:\new.req
Key gen - SKey filename	Имя файла, куда писать секретный ключ	A:\new.sec

C.10. Параметры использования ключевых наборов Crypto-C

Таблица C.10. Параметры использования ключевых наборов Crypto-C

Параметр	Значение	Значение по умолчанию
User PKey/ Certificate	Файл открытого ключа пользователя-владельца ключей	A:\self.pub
User Secret key	Файл секретного ключа пользователя-владельца ключей	A:\self.sec
Abonents dir	Каталог сертификатов абонентов	A:\ABONENTS
CA dir	Зарезервировано для будущего использования	A:\CA
Encrypt Method	0 - гаммирование, 1-гаммирование с обратной связью	1
Encrypt for UID	По умолчанию шифруем на UID	User1
Key request time out	Задает время в секундах хранения кэша с момента последнего считывания ключа с дискеты	60
Last operation key time out	Время в секундах хранения ключа в кэше с момента последнего использования ключа	5
Key gen - GOST	Для какого алгоритма создавать ключи. Допускаются значения: "1994" - ГОСТ 34.10 - 1994 "2001" - ГОСТ 34.10 - 2001*; *параметр действует на функции генерации (перегенерации) ключей	1994
Key gen - UID	UID ключа при генерации	User2
Key gen - PKey filename	Файл нового открытого ключа при генерации	A:\new.pub
Key gen - SKey filename	Файл нового секретного ключа при генерации	A:\new.sec

Глоссарий

Перечень сокращений

CRL	*Certificate revocation list*.
CSP	*Cryptographic service provider*.
DLL	Dynamic Link Library, динамически компонуемая библиотека.
PKI	*Public key infrastructure*.
UID	Уникальный идентификатор *ключевой пары*.
АРМ	*Автоматизированное рабочее место*.
ГП	*Головное подразделение*.
ДБО	Дистанционное банковское обслуживание. См. также Централизованная система "ДБО BS-Client v.3".
ИОК	*Инфраструктура открытых ключей*.
ПБЗИ	*Программные библиотеки защиты информации*.
РМ	*Рабочее место*.
СКЗИ	*Система криптографической защиты информации*.
ССД	*Схема составления документа*.
УЦ	*Удостоверяющий центр*.
ЦР	*Центр регистрации*.
ЦС	*Центр сертификации*.
ЦС "ДБО BS-Client v.3"	*Централизованная система "ДБО BS-Client v.3"*.
ЭЦП	*Электронная цифровая подпись*.

Перечень терминов

Certificate revocation list	См. Список отозванных сертификатов.
Cryptographic service provider	Cryptographic service provider (*CSP*, *криптопровайдер*) - модуль, содержащий реализацию криптографических алгоритмов и поддерживающий интерфейс *MS Crypto API*.
MS Crypto API	Microsoft Cryptographic Application Programming Interface - интерфейс прикладного уровня, определяющий порядок взаимодействия приложе-

	ний с модулями, реализующими криптографические алгоритмы (*криптопровайдерами*), в ОС Windows.
Public key infrastructure	См. Инфраструктура открытых ключей.
X.509	Стандарт X.509 ITU-T - фундаментальный стандарт *ИОК*. Основное его назначение - определение формата *электронного сертификата* и *списков отозванных сертификатов*.
АРМ банка	См. Автоматизированное рабочее место.
АРМ клиента	См. Автоматизированное рабочее место.
АРМ удаленной площадки	См. Автоматизированное рабочее место.
Абонент криптографической сети	Субъект, обменивающийся информацией с другими субъектами в рамках *криптографической сети*. В системе "ДБО BS-Client v.3" информация об абоненте представлена *криптографическим профилем*.
Абонент транспортной сети	Узел *транспортной сети*, представляющий собой *транспортную подсистему* АРМ банка или АРМ клиента.
Автоматизированное рабочее место	Автоматизированное рабочее место (*АРМ*) - совокупность компонентов системы "ДБО BS-Client v.3". АРМ бывают трех видов: • *АРМ банка* - совокупность компонентов системы, установленных на всех рабочих станциях и серверах *головного подразделения* и всех *подразделений* банка, имеющих непосредственный доступ к БД банка; • *АРМ удаленной площадки* - совокупность компонентов системы, установленных в удаленной площадке подразделения банка, не имеющей непосредственного доступа к БД банка и осуществляющей взаимодействие с АРМ банка посредством подсистемы "Оператор Штрих-Кодов"; • *АРМ клиента* - совокупность компонентов системы, установленных на всех рабочих станциях клиента.
Автоматическая документарная операция	*Документарная операция*, выполняемая автоматически системой "ДБО BS-Client v.3", при переходе документа в определенный статус.
Автопроцедура	Объект системы, определяющий условия, параметры запуска и запуск заданной *операции*. В стандартную поставку системы "ДБО BS-Client v.3" входит комплект заранее созданных и настроенных автопроцедур, который можно настраивать и изменять в соответствии с потребностями.
Авторизация	Предоставление определенных полномочий *пользователю* на выполнение некоторых действий в системе. Посредством авторизации устанавливаются и реализуются права доступа к ресурсам. В системе "ДБО BS-Client v.3" необходимым и достаточным условием авторизации пользователя являются *идентификация* и *аутентификация* пользователя.

Асимметричные криптографические алгоритмы	Криптографические алгоритмы, основанные на использовании *ключевой пары* (для *зашифрования* используется *секретный ключ*, для *расшифрования* - *открытый*). Данные алгоритмы называются также *криптографическими алгоритмами с открытым ключом*. См. также Симметричные криптографические алгоритмы.
Аутентификация	Процедура проверки подлинности данных и субъектов информационного взаимодействия исключительно на основе внутренней структуры самих данных. В рамках системы "ДБО BS-Client v.3" применяется аутентификация пользователей посредством ввода *пароля*, а также *криптографическая аутентификация*. См. также Идентификация, Авторизация.
Аутентичность	Достоверность того, что данные были получены из правильного источника и не подвергались случайным или преднамеренным искажениям.
Библиотека единого криптографического интерфейса	Библиотека (Cryptlib.dll), предоставляющая интерфейс доступа к функциям *СКЗИ* на прикладном уровне системы "ДБО BS-Client v.3". См. также Криптобиблиотека.
Библиотека-прослойка	См. Криптобиблиотека.
Головное подразделение	Головное подразделение (*ГП*) - подразделение банка, в котором размещены сервера *системы "ДБО BS-Client v.3"*.
Дайджест	Последовательность символов заданной длины, получаемая из подписываемого сообщения с помощью *хэш-функции*.
Документ приложения	Данные, передаваемые/получаемые приложением посредством *транспортной подсистемы* для/от абонента транспортной сети. См. также Транспортный документ.
Документарная операция	*Операция*, работающая со списком записей только одной таблицы, соответствующей определенному типу документа. Отличается от табличной еще и тем, что для каждой документарной операции задан список входящих статусов. Соответственно операция будет обрабатывать только те документы, статусы которых удовлетворяют этому списку. См. также Простая операция, Табличная операция.
Документарная схема	Совокупность таблицы базы данных, содержащей записи о документах данного типа, *документарных операций*, *схем составления документов*, статусов документа, отражающих его состояние, почтовых статусов, правил преобразования и приема / отправки почты.
Документарный квиток	Уведомление об изменении статуса документа у получателя (сторона-обработчик документа), передаваемый средствами транспортной подсистемы отправителю (сторона-инициатор документа). В документарный квиток входят пересылаемы поля документа (*ССД*) и почтовый статус, по которому у отправителя принимается решение о смене статуса документа (при этом обновляются значения полей документа, пролученные в квитке). См. также Транспортный квиток.

Зашифрование	*Криптографическое преобразование* защищаемой информации (открытого текста) в зашифрованное сообщение (шифрованный текст). См. также Расшифрование, Криптографические операции.
Зашифрование на абонентов	*Зашифрование* данных в системе ДБО таким образом, чтобы их расшифрование могли произвести только фиксированные абоненты.
Идентификация	Распознавание *пользователя* компьютерной системы на основании ранее заданного описания. Идентификация имеет целью определение полномочий пользователя (права доступа к данным и выбора режима их использования). Идентификация в системе "ДБО BS-Client v.3" производится посредством ввода *системного имени пользователя*. См. также Аутентификация, Авторизация.
Инфраструктура открытых ключей	Инфраструктура открытых ключей (*ИОК*, *Public key infrastructure - PKI*) - сервис для управления *электронными сертификатами* и ключами пользователей. ИОК включает в себя: • *центр сертификации* (*ЦС*) или иерархию подчиненных друг другу ЦС, возглавляемых *корневым ЦС*; • *центр регистрации* (*ЦР*); • конечных пользователей; • *сетевой справочник*.
Клиент	Юридическое лицо, обслуживаемое системой.
Ключевая пара	Совокупность соответствующих друг другу *секретного* и *открытого* ключей. См. также Ключевой набор.
Ключевой кэш	Область памяти с быстрым доступом для временного хранения данных *ключевого набора*. См. также Кэширование.
Ключевой набор	Набор, состоящий из *ключевой пары абонента* и *сертификата* или цепочки *сертификатов ЦС*, завершивших *сертификат абонента*, и *сертификатов абонентов*, с которыми должен осуществляться обмен информацией. См. также Ключевой носитель.
Ключевой носитель	Материальный носитель, набор носителей или его часть, где располагается *ключевой набор*: дискета, флэш-карта, каталог жесткого диска и т.д.
Ключи подписи	*Секретный* и *открытый* ключи *абонента*, используемые в операциях *подписи* и *проверки подписи*.
Ключи шифрования	*Открытый* и *секретный* ключи *абонента*, используемые при *зашифровании* и *расшифровании*.

Компрометация ключа	Утрата доверия к тому, что используемый *секретный ключ* обеспечивает безопасность информации, защищаемой с его использованием.
Корневой центр сертификации	См. Инфраструктура открытых ключей.
Криптобиблиотека	Криптобиблиотека (*библиотека-прослойка*) - библиотека, осуществляющая взаимодействие между *библиотекой единого криптографического интерфейса* и модулями конкретной *СКЗИ*. См. также Библиотека единого криптографического интерфейса.
Криптографическая аутентификация	...
Криптографическая сеть	В рамках системы "ДБО BS-Client v.3": совокупность криптографических подсистем банка и его клиентов.
Криптографические алгоритмы с открытым ключом	См. Асимметричные криптографические алгоритмы.
Криптографические операции	Операции, основанные на *криптографическом преобразовании* данных: • *зашифрование данных*; • *расшифрование данных*; • *подпись данных*; • *проверка подписи*.
Криптографический профиль	Криптографический профиль (сокращенно *криптопрофиль*) - объект системы "ДБО BS-Client v.3", содержащий сведения об *абоненте криптографической сети* и используемых им *ключах* и определяющий права абонента на выполнение *криптографических операций*. Под выражением "операция выполняется криптопрофилем" подразумевается, что операция выполняется с использованием ключей сопоставленного криптопрофилю *ключевого набора* и от имени абонента - владельца криптопрофиля.
Криптографическое преобразование	Криптографическое преобразование (*шифрование*) - взаимно-однозначное математическое преобразование, зависящее от ключа / *ключевой пары* (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации (представленной в некоторой цифровой кодировке) блок шифрованной информации, также представленной в цифровой кодировке. Термин объединяет в себе два процесса (базовых цикла): *цикл зашифрования* и *цикл расшифрования* информации. На данных циклах основаны все *криптографические операции*, в том числе операции *формирования* и *проверки электронной подписи*. См. также Криптографические операции.
Криптопровайдер	См. Cryptographic service provider.
Криптопрофиль	См. Криптографический профиль.

Кэширование	Размещение наиболее важных данных в области памяти с быстрым доступом с целью увеличения производительности. В системе "ДБО BS-Client v.3" кэширование активно используется, например, при обращении к данным *ключевых наборов*. См. также Ключевой кэш.
Логин	См. Системное имя пользователя.
Несертификатные СКЗИ	*Системы криптографической защиты информации*, в рамках которых *открытые ключи* не снабжаются дополнительной информацией и не заверяются *электронной цифровой подписью* (не выпускаются в виде *сертификатов*) или выпускаются в виде *сертификатов*, не удовлетворяющих стандарту *X.509*. Несертификатными являются следующие СКЗИ: • КриптоСИ; • Верба 4; • Верба 5; • Excellence 4.0; • Lan Crypto 2.35; • Crypto COM 2.2. См. также Сертификатные СКЗИ.
Операция	Некоторое действие, выполняемое системой автоматически или по запросу пользователя. В системе ДБО существуют операции трех типов: *простые*, *табличные* и *документарные*. Все операции объединены в *схемы операций*.
Открытый ключ	Свободно распространяемая часть *ключевой пары*. Открытый ключ может быть выполнен в виде *сертификата*. См. также Секретный ключ.
Пакет документов	*Пакет*, содержащий в себе *документы приложения*, либо их части, преобразованные и зашифрованные определенным образом, или *документарные квитки*.
Пакет квитков	*Пакет*, состоящий только из *транспортных квитков*. На данные пакеты не генерируются транспортные квитки.
Пароль	Секретная последовательность буквенно-цифровых символов, соответствующая присвоенному *пользователю системному имени* и использующаяся для *аутентификации* пользователя при работе с системой.
Подпись данных	Процесс присвоения подписываемому сообщению *электронной цифровой подписи*. См. также Проверка подписи, Криптографические операции.

Подразделение банка	Обособленное подразделение кредитной организации, обладающее банковским идентификационным кодом. См. также Головное подразделение.
Пользователь	Пользователь системы. Каждый пользователь имеет *системное имя* и *пароль* для входа в систему. Пользователю всегда назначен ровно один *профиль* и одна или несколько *ролей*, а также, возможно, отдельные *привилегии*.
Права криптопрофилей	Объекты системы "ДБО BS-Client v.3", определяющие для каждого *криптопрофиля* перечень *криптографических операций*, которые могут быть выполнены данным криптопрофилем, и классы объектов, над которыми возможно выполнение данных операций.
Привилегия	Право или запрет на совершение некоторого действия в системе. Привилегии определяют тип и права доступа непосредственно к объектам базы данных. Набор привилегий в системе предопределен и редактированию не подлежит, возможна лишь настройка их параметров.
Проверка подписи	Процесс определения действительности *электронной цифровой подписи*: проверка отсутствия искажений в подписанном сообщении и соответствия *ЭЦП* абоненту, подписавшему сообщение. См. также Подпись данных, Криптографические операции.
Программные библиотеки защиты информации	Программные библиотеки защиты информации (*ПБЗИ*) - динамически компонуемые библиотеки (*DLL*), непосредственно реализующие алгоритмы *критопграфических преобразований*.
Простая операция	*Операция*, реализуемая как правило одной функцией, которая выполняет обработку некоторых параметров. См. также Табличная операция, Документарная операция.
Профиль	Набор правил работы *пользователя* с *паролем* (время истечения, временные ограничения и т. п.) и самой системой (имя главной формы для запуска, язык, необходимость запуска *автопроцедур* и *транспорта* при входе в систему и др.). Набор параметров предопределен, изменены могут быть только их значения. В системе можно завести несколько профилей.
Рабочие ключи	Ключи *рабочего ключевого набора*. См. также Технологические ключи.
Рабочий ключевой набор	*Ключевой набор* без дополнительных ограничений (помимо срока действия набора) на выполнение *криптографических операций*. Все ключевые наборы банка являются рабочими. Термин "рабочий" не является синонимом статуса ключевого набора "активный". См. также Технологический ключевой набор.
Расширенные права подписи	Права *криптопрофиля* на осуществление *подписи* документов, задаваемые для отдельных классов документов *АРМ*.

Расшифрование	Процесс, обратный *зашифрованию*, то есть *криптографическое преобразование* шифрованного сообщения в открытый текст. См. также Зашифрование, Криптографические операции.
Регистрация абонента	См. Регистрация открытого ключа.
Регистрация открытого ключа	Регистрация открытого ключа (*регистрация абонента*) – процесс внесения *открытого ключа* абонента в *ключевые наборы криптопрофиля*.
Роль	Набор *привилегий*. Задается списком привилегий (с заполненными параметрами) и списком ролей, включенных в данную роль. Все привилегии, содержащиеся во вложенных ролях, автоматически считаются принадлежащими данной роли. Привилегии могут быть указаны как предоставленные, так и запрещенные. Запрет привилегии всегда преобладает над ее разрешением. Роли могут редактироваться и являются настраиваемыми.
ССД подписи	*Схема составления документа*, определяющая список полей документа, которые должны быть подписаны. Поля документа, не входящие в ССД подписи, не подписываются.
Связка с СКЗИ	Совокупность механизмов, высокоуровневых и низкоуровневых интерфейсов, используемых системой "ДБО BS-Client v.3" для вызова функций конкретной *СКЗИ*.
Сеансовый ключ	Временный ключ шифрования.
Секретный ключ	Персональная (закрытая) часть *ключевой пары*. Секретный ключ является конфиденциальной информацией его владельца. См. также Открытый ключ.
Сертификат	*Открытый ключ*, снабженный информацией о его владельце и заверенный *цифровой подписью центра сертификации*. См. также Секретный ключ.
Сертификатные СКЗИ	*Системы криптографической защиты информации*, в рамках которых *открытый ключ* распространяется в виде *сертификата* по стандарту *X.509*. Сертификатными являются следующие СКЗИ: • Crypto Pro CSP 1.1; • Crypto Pro CSP 2.0; • Crypto Pro CSP 3.0; • Message Pro 1.1; • Message Pro 1.3x; • Message Pro 2.x; • OpenSSL.

	См. также Несертификатные СКЗИ.
Сетевой справочник	Опциональная компонента *ИОК*, содержащая *сертификаты* и *списки отозванных сертификатов* и служащая для целей распространения этих объектов среди пользователей с использованием протокола LDAP (HTTP, FTP). См. также Несертификатные СКЗИ.
Симметричные криптографические алгоритмы	Криптографические алгоритмы, использующие для *криптографических преобразований зашифрования* и *расшифрования* один и тот же ключ. См. также Асимметричные криптографические алгоритмы.
Система криптографической защиты информации	Система криптографической защиты информации (*СКЗИ*) - набор *криптографических преобразований* или алгоритмов, предназначенных для работы в единой технологической цепочке с целью решения определенной задачи защиты информации.
Системное имя пользователя	Системное имя пользователя (*логин*) - уникальная последовательность буквенно-цифровых символов, однозначно *идентифицирующая пользователя* в системе.
Список отозванных сертификатов	Список отозванных сертификатов (*Certificate revocation list, CRL*) - заверенная подписью *центра сертификации* структура, содержащая список *сертификатов*, непригодных к использованию с точки зрения *ЦС* и аннулированных раньше завершения срока их действия.
Схема операций	Набор *операций*, объединенных по области применения выполняемых действий. В схему могут быть объединены только операции одного типа. Каждая операция внутри схемы задается своим именем и не может содержать внутри себя другие операции. Создание, редактирование, удаление операций и схем операций выполняется с помощью модуля **Построитель** в случае наличия специальной лицензии.
Схема составления документа	Схема составления документа (*ССД*) - структура, определяющая для документов каждого заданного типа список значимых полей таблицы БД, содержащей документы данного типа. Различают два вида ССД: • *ССД подписи*, используемые в операциях *подписи документов* и *проверки подписи под документами*; • *ССД для отправки*, используемые при формировании и обработке *транспортных документов*.
Табличная операция	*Операция*, работающая со списком записей какой-либо таблицы. Одна и та же операция может при разных запусках работать с разными таблицами (так как имя таблицы, с которой ей предстоит работать, передается ей при запуске). См. также Простая операция, Документарная операция.
Технологические ключи	Ключи *технологического ключевого набора*.

	См. также Технологические ключи.
Технологический ключевой набор	Клиентский *ключевой набор* с ограниченными правами на выполнение операции *подписи* документов, действующий до момента перегенерации набора после установки системы клиента. См. также Рабочий ключевой набор.
Транспортная подсистема	Подсистема *АРМ* банка или *АРМ* клиента, осуществляющая обмен информацией между *абонентами транспортной сети* в рамках подсистемы *"Банк-клиент"*.
Транспортная сеть	Сеть, объединяющая *транспортные подсистемы* АРМ банка и АРМ клиентов.
Транспортный документ	*Документ приложения*, *документарный квиток* или *транспортный квиток*, преобразованный *транспортной подсистемой* для его дальнейшей обработки.
Транспортный квиток	Уведомление об изменении внутритранспортного статуса пакета. Существует только внутри *транспортной подсистемы* и в приложение не передается. См. также Документарный квиток.
Транспортный пакет	Единица данных, передаваемая *транспортной подсистемой*. Транспортные пакеты могут быть двух видов: *пакеты документов* или *пакеты квитков*.
Удостоверяющий центр	См. Центр сертификации.
Формат хранения подписи документа	Формат структуры, формируемой в процессе *подписи* документа и включающей в себя ЭЦП документа, версию алгоритма / формата подписи, список наименований подписываемых полей - информацию, необходимую при *проверке подписи* под документом. Данная структура помещается в поле Signatures документа. Формат хранения подписи документа идентифицируется номером версии формата.
Хэш-функция	Необратимое преобразование данных (односторонняя функция), отображающее сообщение произвольной длины в значение фиксированной длины - *дайджест*. Одно из применений хэш-функций - *криптографические операции формирования* и *проверки электронной подписи*.
Центр регистрации	Центр регистрации (*ЦР*) - опциональная компонента *ИОК*, предназначенная для регистрации конечных пользователей. Основная задача ЦР - регистрация пользователей и обеспечение их взаимодействия с *ЦС*. В задачи ЦР может также входить публикация *сертификатов* и *списка отозванных сертификатов* в *сетевом справочнике*. См. также Центр сертификации, Инфраструктура открытых ключей.
Центр сертификации	Центр сертификации (*ЦС*, или *Удостоверяющий центр*, *УЦ*) - основная управляющая компонента *ИОК*, предназначенная для формирования *электронных сертификатов* подчиненных Центров и конечных пользо-

вателей. Кроме сертификатов, ЦС формирует *список отозванных сертификатов*.

К основным функциям ЦС относятся:

- формирование собственного *секретного ключа* и сертификата ЦС;
- формирование сертификатов подчиненных ЦС;
- формирование сертификатов конечных пользователей;
- формирование списка отозванных сертификатов;
- ведение базы всех изготовленных сертификатов и списков отозванных сертификатов.

См. также Центр регистрации, Инфраструктура открытых ключей.

Шифрование — См. Криптографическое преобразование.

Электронная цифровая подпись — Электронная цифровая подпись (*ЭЦП*) - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием *секретного ключа* электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

С технической точки зрения ЭЦП представляет собой *дайджест* подписываемого документа, зашифрованный *секретным ключом* электронной цифровой подписи.

ЭЦП используется в качестве аналога собственноручной подписи.