

ПС «Купол-СКЗИ для Linux»
Описание программы
ВЕР.00118-01 13 01

Листов 13

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дудл.	Подпись и дата

АННОТАЦИЯ

Настоящий документ является описанием программного средства «Купол-СКЗИ для Linux» ВЕР.00118-01 (далее – ПС «Купол-СКЗИ для Linux»).

В документе приведены сведения, описывающие функциональное назначение, логическую структуру, алгоритм работы, условия выполнения, способы вызова и загрузки, входные и выходные данные ПС «Купол-СКЗИ для Linux».

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ	4
2. ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ.....	5
3. ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ.....	6
4. ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА.....	9
5. ВЫЗОВ И ЗАГРУЗКА.....	10
6. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ	11
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	12

1. ОБЩИЕ СВЕДЕНИЯ

Наименование программного средства: ПС «Купол-СКЗИ для Linux».

Обозначение программного средства: ВЕР.00118-01.

1.1 ПС «Купол-СКЗИ для Linux» предназначен для построения защищённых распределённых хранилищ данных.

1.2 ПС «Купол-СКЗИ для Linux» функционирует в среде операционной системы Astra Linux 1.6 Special Edition (Смоленск).

1.3 Ядро ПС «Купол-СКЗИ для Linux» написано на языке программирования С.

2. ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

2.1 ПС «Купол-СКЗИ для Linux» предназначено для использования в автоматизированных информационно-управляющих системах, обрабатывающих информацию, не содержащей сведения, составляющие государственную тайну. Изделие предназначено, в том числе, для хранения конфиденциальной информации, передаваемой по сетям УКВ радиосвязи, построенных на основе комплексов технических средств «Поле-СКЗИ» и «Гранит-ДМР».

2.2 ПС «Купол-СКЗИ для Linux» обеспечивает решение следующих функциональных задач:

- хранение данных реестра с выполнением функций резервного копирования;
- приём данных и их запись в реестр;
- формирование и передача данных в соответствии с полученными заявками;
- формирование блока для записи;
- индексирование данных, хранящихся в распределённом реестре;
- передача заявок на поиск в распределённых реестр;
- передача результатов поиска на фронт-сервер в соответствии с поступившими заявками;
- взаимодействие пользователей с инфраструктурой распределённого реестра;
- вывод пользователю результатов поиска в распределённом реестре;
- аудит консенсуса базы данных;

Реализация функционального предназначения ПС «Купол-СКЗИ для Linux» осуществляется путём сбора, обработки и предоставления в удобном для просмотра пользователя виде необходимой информации.

2.3 Дополнительных функциональных ограничений на применение ПС «Купол-СКЗИ для Linux» не предъявляется.

3. ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ

3.1 Структура программного средства

Структура программного средства представлена на рис. 1.

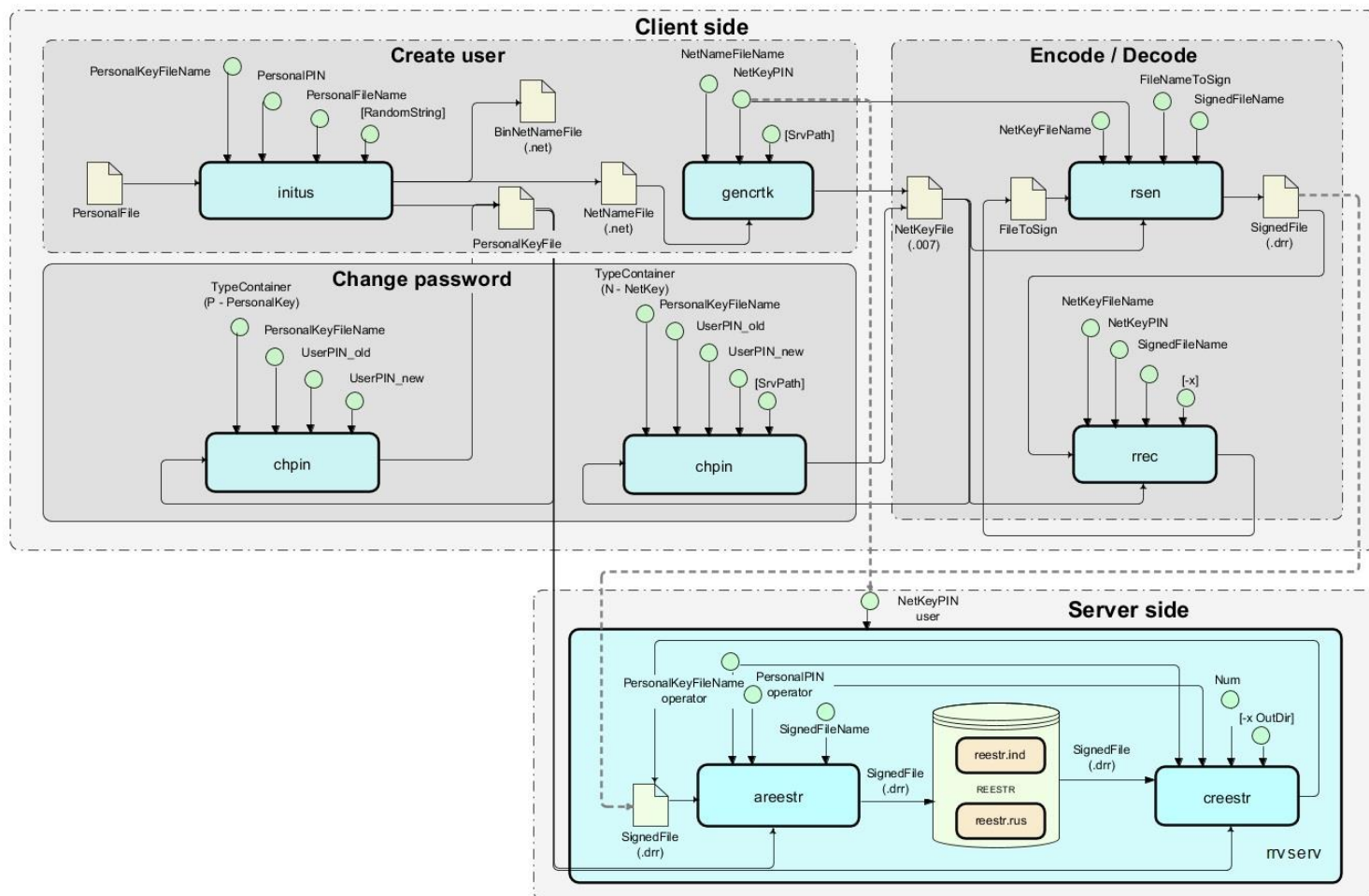


Рис. 1

ПС «Купол-СКЗИ для Linux» включает в свой состав следующие компоненты (модули):

1) Модуль формирования сетевого имени (`initus`) генерирует сетевое имя пользователя на основе пароля и файла с пользовательскими данными, а также файл, закрытый на пароле персональным идентификатором пользователя (фактически защищенный контейнер для хранения и передачи персонального идентификатора/ключа пользователя).

2) Модуль генерации контейнеров для связи с оператором РР (`gencrtk`) формирует сетевой контейнер пользователя на основе сетевого имени пользователя и пароля для закрытия транспортного ключа. Этот пароль далее будет использоваться для защиты контейнера с транспортным ключом. Оператор РР должен иметь ключи всех пользователей, поэтому пользователи могут выработать транспортные ключи самостоятельно и направить их оператору РР, а пароль сообщить оператору отдельно (по смс, письмом или голосом). Либо пользователи высылают оператору РР бинарный файл своего сетевого имени, и оператор РР формирует транспортные ключи пользователей и также отдельно (по другим каналам) сообщает им их пароли. С точки зрения безопасности это равноценная схема, поскольку пользователи не знают пароля друг друга, а оператор РР является доверенной стороной (доверенным компонентом системы).

3) Модуль изменения пароля (`chpin`) позволяет менять пароль как для индивидуального, так и сетевого контейнеров.

4) Модуль формирования файла для передачи оператору РР (`rseu`) используется пользователем для подписания файла и его подготовки к дальнейшей отправке в РР.

5) Модуль проверки и экстракции файла (`grsc`) применяется для получения исходного файла на основе пароля и сетевого контейнера пользователя.

6) Модуль записи в РР (`areestr`) добавляет новые записи в реестр.

7) Модуль извлечения информации из РР по номеру звена (`creestr`) позволяет получать данные о транзакции (порядковый номер, добавленный файл, сетевое имя пользователя, время добавления и т.д.)

8) Модуль сервера РР (`grwseu`) обрабатывает запросы пользователей, а также вызывает сервер записи в РР.

3.2 Сценарий работы системы

1) Первоначально производится регистрация пользователей платформы, включая оператора, создаются их ключевые контейнеры при помощи модулей `initus`

(генерация контейнера с персональным ключом и сетевого имени) и `gencrtk` (генерация контейнера с сетевым ключом пользователя).

2) Пользователь подписывает файлы при помощи модуля `rse`. На данном этапе подготовлена информация для записи в распределённый реестр.

3) Подписанный файл передается на криптомаршрутизатор, находящийся на стороне пользователя, и принимается другим криптомаршрутизатором, находящимся на стороне оператора. Это действие производится при помощи другого (коммуникационного) программного обеспечения, не входящего в состав данного программного средства. Таким образом, с криптомаршрутизатором ПО непосредственно не взаимодействует.

4) Получив файл, оператор производит запуск модуля сервера `rwserver`, во входную область приема данных сервера (директория `in`) помещаются файлы, подписанные КА при помощи модуля `rse`. Модуль `rwserver` постоянно следит за обновлением этой области.

5) В случае полной валидации файла, он добавляется в реестр и формируется соответствующая квитанция (в директории `in_k`). В случае ошибки, файл попадает область данных ошибочного формата (директория `in_err`).

6) Оператор может извлечь данные из реестра по запросу пользователя при помощи модуля `creestr`.

7) После получения извлеченного из реестра файла пользователь может проверить его неизменность, запустив модуль `grec`. После извлечения файла из реестра пользователь экстрагирует его и получает исходный файл.

4. ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

ПС «Купол-СКЗИ для Linux» функционирует на ЭВМ с характеристиками не ниже следующих:

- процессор Intel Core 2 Duo 1,8 ГГц;
- оперативная память 2048 Мбайт;
- жесткий диск 100 Гбайт;
- сетевая плата Fast Ethernet 100 Мбит/с.

Для полноценного функционирования КП «Купол-СКЗИ» необходимо наличие следующих программных средств, установленных на ЭВМ:

- операционной системы Astra Linux 1.6 Special Edition (Смоленск).

Шифрование обеспечивается внешним СКЗИ (используется криптомаршрутизатор М-479Р2К производства компании «Фактор-ТС» под управлением Dionis NX).

5.ВЫЗОВ И ЗАГРУЗКА

Для начала работы с ПС «Купол-СКЗИ для Linux» необходимо выполнить следующие операции:

- установку модулей ПС «Купол-СКЗИ для Linux»;
- последовательный запуск исполняемых файлов модулей ПС «Купол-СКЗИ для Linux» в соответствии с документом ВЕР.00118-01 34 01 Руководство оператора.

После выполнения данных операций пользователю необходимо ввести свои данные и предоставить файл с цифровой информацией (описывающей пользователя реестра - ФИО, паспортные данные и т.д.), на основе которого будет сформировано сетевое имя. Далее пользователь генерирует ключ, которым он сможет подписывать файлы и отправлять их в реестр.

6. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными ПС «Купол-СКЗИ для Linux» является информация, полученная от пользователя:

- файл с цифровой информацией, описывающей пользователя реестра (может содержать ФИО, паспортные данные и т.д.);
- пароль (пин-код) для закрытия персонального идентификатора пользователя;
- пароль (пин-код) для закрытия транспортного ключа;
- файл для подписания.

Выходными данными ПС «Купол-СКЗИ для Linux» являются файлы, вся текстовая, графическая информация на дисплее (экране), включающая:

- данные о сетевом имени пользователя;
- файл с персональным контейнером пользователя;
- файл с сетевым контейнером пользователя;
- подписанный файл с данными, позволяющими провести идентификацию пользователя и контроль неизменности полученной информации;
- квитанция о транзакции;
- сигналы о попытках совершения неразрешенных операций.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

КП	– комплекс программ
РР	– распределенный реестр
ОС	– операционная система
КА	– код аутентификации
ПО	– программное обеспечение

