УТВЕРЖДЕН

RU.ЛСАФ.00020-01 31 01 - ЛУ

СРЕДСТВО ЗАЩИТЫ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

«Fox-SSF 2012»

Описание применения

RU.ЛСАФ.00020-01 31 01

Листов 13

Аннотация

Настоящий документ описывает программное обеспечение «Fox-SSF 2012» в продуктах компании SAP AG.

Описываемое программное обеспечение представляет собой комплекс средств поддержки протокола SSF (Secure Store and Forward) в продуктах компании SAP AG и обеспечивает криптографическую защиту электронных документов за счет использования механизмов ЭП для подписи документов и хранения документов в зашифрованном виде.

Содержание

1 Назначение комплекса

1.1 Общие сведения

Для защиты информации, циркулирующей в системе SAP, могут использоваться как встроенные средства системы, так и продукты сторонних производителей. В частности, для обеспечения криптографической защиты электронных документов необходимо использовать сертифицированные российские средства. В качестве СКЗИ в системе SAP программное обеспечение «Fox-SSF 2012».

1.2 Назначение программного обеспечения «Fox-SSF 2012»

ПО «Fox-SSF 2012» обеспечивает возможность формирования и проверки ЭП документов и безопасное хранение документов в «цифровом конверте» в зашифрованном виде с использованием российских криптографических алгоритмов. Возможно подписывание документов несколькими пользователями. ПО реализует прикладной интерфейс компании SAP AG – SSF API. Для формирования и проверки электронной подписи используются алгоритмы ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012, для шифрования электронных документов – алгоритм ГОСТ 28147-89 (симметричное шифрование).

Технология работы комплекса основана на стандартах инфраструктуры открытых ключей (Public Key Infrastructure - PKI). Каждый пользователь информационной системы имеет свой цифровой сертификат стандарта X.509 v.3 и соответствующую ключевую информацию. Форматы данных, используемые подсистемой SSF в процессе формирования цифровых подписей и конвертов, соответствуют стандарту PKCS#7.

1.3 Состав поставляемого программного и аппаратного обеспечения

Комплекс состоит из двух компонент:

- «Fox-SSF Server», устанавливаемой на серверах приложений;
- «Fox-SSF Client», устанавливаемой на клиентских рабочих местах.

Электронные USB ключи (eToken, ruToken, Шипка) используются на клиентских рабочих местах для хранения ключевой информации.

Комплекс разработан на языке программирования C на базе криптографической библиотеки LISSI Crypto Core. Компонент «Fox-SSF Client» может также использовать функции криптопровайдеров, поддерживающих российскую криптографию. В качестве таких криптопровайдеров могут использоваться следующие продукты:

- ЛИРССЛ-CSP компании «ЛИССИ-Софт»;
- КриптоПро-CSP компании «КриптоПро».

Комплекс поставляется в виде дистрибутива на компакт-диске. Формат дистрибутива зависит от платформы. В состав дистрибутива входят:

- одна или несколько динамически загружаемых библиотек;

- комплект эксплуатационной документации.

Кроме того, в состав комплекса могут входить аппаратные средства хранения ключевой информации, в частности:

- электронный USB-ключ eToken[1];
- электронный USB-ключ ruToken[2];
- электронный USB-ключ Шипка[3].

Поскольку технология работы комплекса основана на стандартах инфраструктуры открытых ключей, то для нормального функционирования комплекса необходимо наличие удостоверяющего центра (УЦ), обеспечивающего выдачу сертификатов. В качестве УЦ может использоваться любой удостоверяющий центр, поддерживающий российскую криптографию, например, «ЛИССИ-УЦ», «КриптоПро УЦ». Для небольших организаций возможно использование компактного центра управления и выдачи сертификатов «Fox-XCA». УЦ в комплект поставки комплекса не входит.

1.4 Ограничения на область применения

Компонента «Fox-SSF Server» в настоящее время может функционировать на следующих платформах:

- MS Windows Server 2000/2003/2008/2012 (x86, x86_64) компании Microsoft;
- SPARC Solaris компании SUN;
- AIX компании IBM;
- HP-UX компании Hewlett-Packard;
- Linux (x86, x86_64).

Компонента «Fox-SSF Client» функционирует под управлением ОС:

- MS Windows 2000/XP/Vista/7/8/8.1/10 (x86, x86_64) компании Microsoft;
- Linux (x86, x86_64).

1.5 Характеристики комплекса «Fox-SSF»

Комплекс «Fox-SSF» обеспечивает надежную криптографическую защиту электронных документов следующими методами:

- подпись электронных документов пользователями с использованием сертификатов ЭП;
- проверка подписи электронных документов пользователями с использованием сертификатов ЭП;
- хранение зашифрованных электронных документов в цифровых конвертах, доступ к

[1] Поставляется по согласованию с заказчиком

[2] Поставляется по согласованию с заказчиком

[3] Поставляется по согласованию с заказчиком

которым определяется ответственным лицом.

Комплекс использует следующие криптографические алгоритмы:

- ГОСТ Р 34.10-2012 – для формирования и проверки электронной подписи;
- ГОСТ Р 34.11-2012 – для вычисления хэш-функции;
- ГОСТ 28147-89 – для симметричного шифрования.

Симметричное шифрование выполняется по ГОСТ 28147-89 с параметрами, указанными в таблице 1.

Таблица 1

Показатель	Значение
Режим шифрования	Гаммирование с обратной связью
Длина ключа шифрования	32 байта (256 бит)

Расчет дайджеста сообщения производится с помощью хэш-функции по ГОСТ Р 34.11-94. Длина дайджеста –32 байта.

Вычисление и проверка ЭП сообщения выполняется по ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 с параметрами, указанными в таблице 2.

Таблица 2

Показатель	Значение
Длина ключа ЭП ГОСТ Р 34.10-2012 (256 бит)	32 байта (256 бит)
Длина ключа проверки ЭП ГОСТ Р 34.10-2012 (256 бит)	64 байта (512 бит)
Длина ключа ЭП ГОСТ Р 34.10-2012 (512 бит)	64 байта (512 бит)
Длина ключа проверки ЭП ГОСТ Р 34.10-2012 (512 бит)	128 байт (1024 бит)

2 Условия применения

2.1 Требования к техническим средствам

Комплекс может функционировать на всех технических средствах, где работают продукты SAP, с учетом ограничений на условия применения. Клиентские ПК должны иметь один свободный USB-порт.

2.2 Требования к программному обеспечению

Компонента «Fox-SSF Server» может функционировать под управлением следующих ОС:

- MS Windows Server 2000/2003/2008/2012 (x86, x86_64) компании Microsoft;
- SPARC Solaris компании SUN;
- AIX компании IBM;
- HP-UX компании Hewlett-Packard;
- Linux (x86, x86_64).

Компонента «Fox-SSF Client» функционирует под управлением следующих ОС:

- MS Windows 2000/XP/Vista/7/8/8.1/10 (x86, x86_64) компании Microsoft;
- Linux (x86, x86_64).

2.3 Требования по взаимодействию с другими системами

Комплекс должен обеспечивать реализацию протокола SSF и взаимодействовать со всеми компонентами системы SAP, использующими данный протокол.

2.4 Требования к персоналу

2.4.1 Установка комплекса должна производиться администратором ОС.

2.4.2 Конфигурирование комплекса должно проводиться администратором системы SAP.

2.5 Требования к организации работ с применением комплекса

Для использования программного комплекса Fox-SSF в продуктах компании SAP необходимо выполнить следующие работы:

- осуществить генерацию и экспорт ключевой информации для всех пользователей системы;
- осуществить установку и настройку продукта «Fox-SSF» на серверах и рабочих станциях пользователей;
- разработать клиентское ПО для пользователей системы SAP с использованием языка программирования ABAP.

Подробное описание этих работ приведено в эксплуатационной документации на «Fox-SSF 2012» (см. «Руководство по установке Fox-SSF 2012» и «Руководство пользователя Fox-SSF 2012»)

3 Подготовка комплекса к работе

3.1 Состав и содержимое дистрибутивного носителя данных

Комплекс поставляется в виде дистрибутива на компакт-диске. Формат дистрибутива зависит от платформы. В состав дистрибутива входят:

- динамически загружаемая библиотека Fox-SSF;
- комплект эксплуатационной документации.

Кроме того, в состав комплекса могут входить аппаратные средства хранения ключевой информации, в частности:

- электронный USB ключ eToken;
- электронный USB ключ ruToken;
- электронный USB ключ Шипка.

3.2 Установка комплекса

Установка серверной компоненты «Fox-SSF Server» производится в соответствии с инструкцией по установке для конкретной платформы, находящейся на дистрибутивном носителе.

Настройка серверной компоненты производится путем редактирования соответствующих файлов конфигурации с учетом решаемых задач и принятой политикой безопасности. Дополнительно к настоящему документу при настройке серверной компоненты может использоваться документация компании SAP.

Установка клиентской компоненты «Fox-SSF Client» производится в соответствии с руководством по установке. Настойка клиентской компоненты заключается в установке переменных окружения или редактирования файла ssfrfc.ini.

Более подробно процесс установки и настройки Fox-SSF 2012 описан в документе «Руководство по установке Fox-SSF 2012».

Перед началом работы с использованием «Fox-SSF 2012» необходимо выработать и экспортировать необходимую ключевую информацию.

4 Описание задачи, решаемой комплексом

4.1 Задачи, решаемые комплексом

Комплекс решает задачу криптографической защиты информации, обрабатываемой в SAP системе. При обработке информации в SAP системе существуют следующие основные задачи криптографической защиты:

- защита информации от раскрытия и подмены за пределами информационной системы SAP, например, при передаче данных на дискете, по электронной почте и т.д;
- привязка информации к отдельным пользователям системы, обеспечение целостности и неотрекаемости для такой информации, например, электронная подпись документов в системе SAP.

4.2 Описание алгоритма решения задачи

Программное обеспечение «Fox-SSF 2012» обеспечивает защиту данных с использованием российских криптографических алгоритмов.

Защита информации от раскрытия обеспечивается путём шифрования информации по алгоритму ГОСТ 28147-89. Алгоритм применяется в режиме гаммирования с обратной связью, так как этот режим обеспечивает наибольшую криптостойкость.

Защита информации от изменения злоумышленником (защита целостности) и привязка её к пользователям системы реализуется с помощью алгоритма ЭП ГОСТ Р 34.10-2012.

Как средство хранения и распространения ключевой информации используются цифровые сертификаты X509 v3. Также используются другие методы и стандарты формирования Инфраструктуры Открытых Ключей (Public Key Infrastructure - PKI) – признанной во всём мире архитектуре для практического использования алгоритмов криптографии с открытым ключом.

4.3 Создание ключевой информации комплекса

Для создания ключевой информации, необходимой для функционирования ПО «Fox-SSF 2012» используется УЦ.

Пользователь должен иметь следующую ключевую информацию:

- ключ ЭП;
- сертификат ключа проверки ЭП в формате X.509 v.3;
- сертификат УЦ в формате X.509 v.3.

Для создания ключевой пары и получения сертификата пользователь обращается к УЦ, генерирует ключевую пару и запрос на сертификат. УЦ выдает сертификат пользователя.

Полученная ключевая информация экспортируется в хранилище (eToken, ruToken, Шипка).

5 Входные и выходные данные

5.1 Входные данные комплекса

Входными данными для работы комплекса являются:

- параметры конфигурации;
- ключевая информация;
- сертификаты ключа проверки ЭП пользователей;
- данные для шифрования и/или заверения ЭП;
- данные для расшифровывания и/или проверки ЭП.

5.2 Выходные данные комплекса

Выходными данными комплекса являются:

- зашифрованные данные с ЭП;
- расшифрованные и/или верифицированные (проверенные при помощи ЭП) данные;
- сообщения, записываемые в журнал работы комплекса и в системный журнал.

6 Аварийные ситуации

6.1 Отказ технических средств

При отказе технических средств могут быть утеряны параметры конфигурации и ключевая информация.

Для минимизации потерь при отказе технических средств необходимо выполнять резервное копирование файлов конфигурации и ключевой информации. Доступ к резервным копиям должен быть ограничен в соответствии с принятой политикой безопасности.

6.2 Компрометация ключевой информации

При компрометации ключевой информации необходимо выполнить следующие мероприятия:

- остановить работу комплекса;
- выяснить и устранить причины, приведшие к компрометации ключевой информации;
- сгенерировать новую ключевую информацию;
- осуществить экспорт ключевой информации и ее распределение;
- возобновить работу комплекса.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подпись	Дата
Изм	Измененных	Замененных	Новых	Аннулированных					