

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

УТВЕРЖДЕН
ВАМБ.00115-06-ЛУ

**ПРИКЛАДНОЙ ПРОГРАММНЫЙ ИНТЕРФЕЙС
СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ВЕРСИЯ 6**

**ПРИКЛАДНОЙ ПРОГРАММНЫЙ ИНТЕРФЕЙС
СКАД «СИГНАТУРА» ВЕРСИЯ 6 ДЛЯ ПЛАТФОРМЫ JAVA**

Руководство по установке и настройке

ВАМБ.00115-06 91 01

2020

Аннотация

Данный документ содержит описание процесса установки и удаления прикладного программного интерфейса (ППИ) программного комплекса ВАМБ.00104-06 «Система криптографической авторизации электронных документов «Сигнатура» версия 6» (далее по тексту — СКАД «Сигнатура») для платформы Java (далее — ППИ Java СКАД «Сигнатура»).

Документ предназначен для специалистов, осуществляющих установку ППИ Java СКАД «Сигнатура».

Документ разработан специалистами ООО «Валидата».

Содержание

1 НАЗНАЧЕНИЕ, СОСТАВ И ТРЕБОВАНИЯ К ОПЕРАЦИОННОЙ СРЕДЕ И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ	4
1.1 Назначение	4
1.1.1 Характеристики	4
1.1.2 Использование библиотеки	5
1.2 Состав библиотеки	5
1.3 Требования к аппаратно-программной среде	5
2 УСТАНОВКА ППИ Java СКАД «СИГНАТУРА»	6
2.1 Контроль целостности и легальности эталонной копии ППИ Java СКАД «Сигнатура»	6
2.2 Инсталляция	6
2.3 Контроль целостности	10
3 УДАЛЕНИЕ ППИ JAVA СКАД «СИГНАТУРА»	11
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	11
ПЕРЕЧЕНЬ РИСУНКОВ	13

1 НАЗНАЧЕНИЕ, СОСТАВ И ТРЕБОВАНИЯ К ОПЕРАЦИОННОЙ СРЕДЕ И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

1.1 Назначение

ВАМБ.00115-06 «Библиотека прикладного программного интерфейса (ППИ) СКАД "Сигнатура" версия 6 для платформы Java» (далее - ППИ Java СКАД «Сигнатура») предназначен для встраивания СКАД «Сигнатура» версия 6 в прикладные системы. ППИ Java СКАД «Сигнатура» предоставляет программам, написанным на языке Java, доступ к набору констант, классов и функций библиотеки упрощенного прикладного программного интерфейса для работы с сертификатами (далее - библиотека упрощенного интерфейса) СКАД «Сигнатура».

ППИ Java СКАД «Сигнатура» функционирует под управлением Java Runtime Environment (далее – JRE) версии 1.6.0 или более поздней. ППИ Java СКАД «Сигнатура» функционирует под управлением операционных систем, перечень которых приведён в документе ВАМБ.00115-06 30 01 «Прикладной программный интерфейс средств криптографической защиты информации версия 6. Прикладной программный интерфейс СКАД «Сигнатура» версия 6 для платформы Java. Формуляр».

ППИ Java СКАД «Сигнатура» разработан в соответствии со спецификацией Oracle Java™ Native Interface 6.0 API Specification (в дальнейшем JNI), входящей в состав Oracle Java™ Platform, Standard Edition 6 (в дальнейшем Java™ SE). Состав и функциональность процедур, форматы обращений из прикладного программного обеспечения (ППО) к функциям библиотеки ППИ Java СКАД «Сигнатура» соответствуют составу и функциональности процедур, форматам обращений библиотеки упрощенного ППИ для работы с сертификатами СКАД «Сигнатура», соответственно, за исключением различий, обусловленных особенностями языка программирования Java.

1.1.1 Характеристики

В качестве алгоритма электронной подписи (ЭП) используется асимметричный вариант ЭП, а именно криптосистема с двумя ключевыми элементами - открытым (общедоступным) и закрытым - по ГОСТ Р 34.10-2012 (ГОСТ Р 34.10-2018). Для формирования хэш-функции сообщения используются алгоритмы по ГОСТ Р 34.11-2012 (ГОСТ Р 34.11-2018). Шифрование информации выполняется по ГОСТ 28147-89, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015.

Библиотека обеспечивает обращение к следующим функциям:

- зашифрование и расшифрование файла;
- зашифрование и расшифрование области памяти;
- создание ЭП файла;
- создание ЭП области памяти;
- проверка ЭП файла;
- проверка ЭП области памяти;

- удаление ЭП из файла;
- удаление ЭП из области памяти;
- выработка хэш-значения для файла;
- выработка хэш-значения для области памяти;
- преобразование отделенной и совмещенной ЭП;
- преобразование бинарных данных в/из формата Base64;
- создание ЭП хэш-функции данных;
- проверка ЭП хэш-функции данных;
- выработка случайного числа заданной длины.

1.1.2 Использование библиотеки

При использовании библиотеки необходимо соблюдать следующие условия:

- библиотека предназначена для использования в приложениях, написанных на языке программирования Java;
- при использовании библиотеки в приложениях, написанных на других языках программирования, должно выполняться требуемое преобразование форматов данных и параметров вызова функций.

1.2 Состав библиотеки

В состав ППИ Java СКАД «Сигнатура» входят следующие файлы:

- `spki1jni.dll` – модуль динамической библиотеки JNI интерфейса;
- `Pki1.LocalIface.Jar` – набор Java классов библиотеки интерфейса;
- `Pki1.Test.Jar` – набор Java классов тестовой утилиты;
- `Pki1.Test.Cmd` – командный файл для запуска тестовой утилиты.

1.3 Требования к аппаратно-программной среде

ППИ Java СКАД «Сигнатура» включает 32-битную библиотеку, функционирующую в среде 32-битных (x86) операционных систем (ОС) Microsoft Windows, и 64-битную библиотеку, функционирующую в среде 64-битных (x64) ОС Microsoft Windows. Перечень операционных систем приведён в документе ВАМБ.00115-06 30 01 «Прикладной программный интерфейс средств криптографической защиты информации версия 6. Прикладной программный интерфейс СКАД «Сигнатура» версия 6 для платформы Java. Формуляр».

Выбор варианта битности библиотеки производится в процессе установки.

2 УСТАНОВКА ППИ Java СКАД «СИГНАТУРА»

Перед установкой ППИ Java СКАД «Сигнатура» на ЭВМ необходимо предварительно установить ПО СКАД «Сигнатура», руководствуясь инструкциями по его установке.

2.1 Контроль целостности и легальности эталонной копии ППИ Java СКАД «Сигнатура»

Перед непосредственной установкой ППИ Java СКАД «Сигнатура» необходимо проверить целостность установочного комплекта. Это осуществляется с помощью программы контроля целостности.

Программа контроля целостности входит в состав программного комплекса ВАМБ.00107-06 «СКАД «Сигнатура» версия 6. Средство криптографической защиты информации СКАД «Сигнатура» версия 6». Программа предназначена для контроля целостности эталонных копий и контроля легальности использования этих продуктов, а также для контроля целостности установленного ПО.

Описание работы с программой контроля целостности приведено в документах ВАМБ.00107-06 92 01 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Программа контроля целостности. Руководство пользователя» и ВАМБ.00107-06 93 02 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Программа контроля целостности. Руководство администратора информационной безопасности».

2.2 Инсталляция

Инсталляция должна производиться пользователем, имеющим права администратора ОС.

Для установки ППИ Java СКАД «Сигнатура» следует использовать установочный комплект 00115-06 Setup.zip.

Установка ПО производится путем выбора необходимого пакета инсталляции (в зависимости от разрядности ОС) sjni_x86.msi или sjni_x64.msi и запуска процесса инсталляции двойным щелчком «мыши» по выбранному файлу, находящемуся на инсталляционном диске.

Дальнейшая установка производится в соответствии с сообщениями, выдаваемыми процедурой установки. После запуска процедуры установки появится окно мастера установки (Рисунок 1).

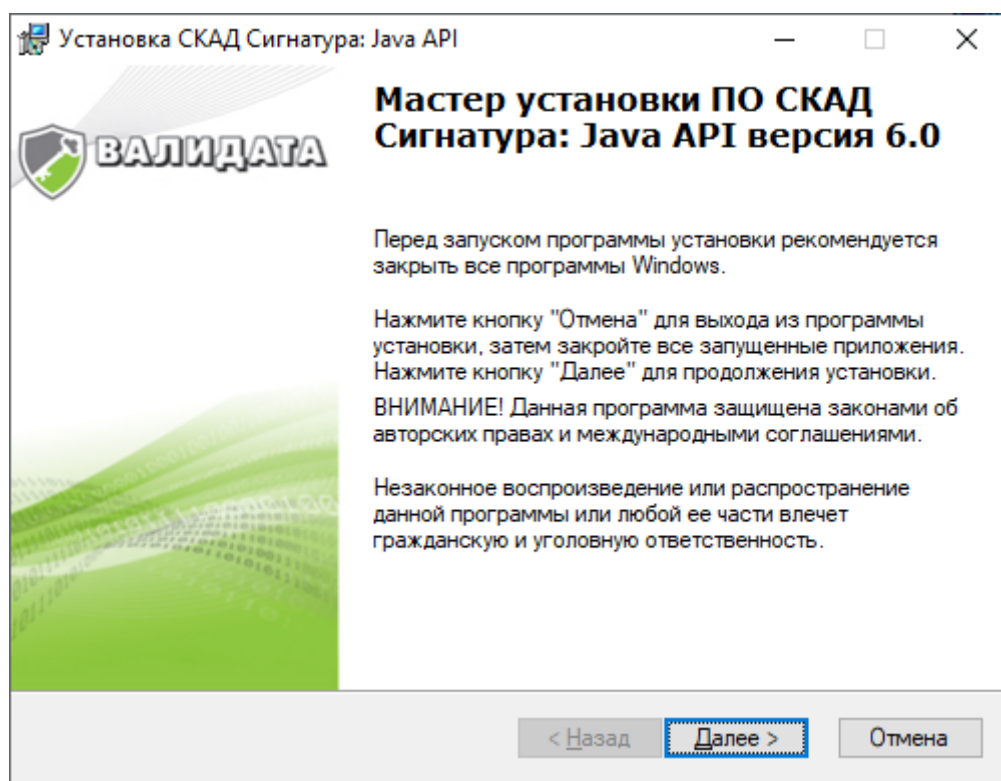


Рисунок 1 – Окно мастера установки

Нажмите кнопку «Далее». Появится окно «Сведения о пользователе» (Рисунок 2).

Рисунок 2 – Окно «Сведения о пользователе»

Введите информацию о пользователе и нажмите кнопку «Далее». Появится окно «Папка назначения» (Рисунок 3). Выберите каталог установки и нажмите кнопку «Далее».

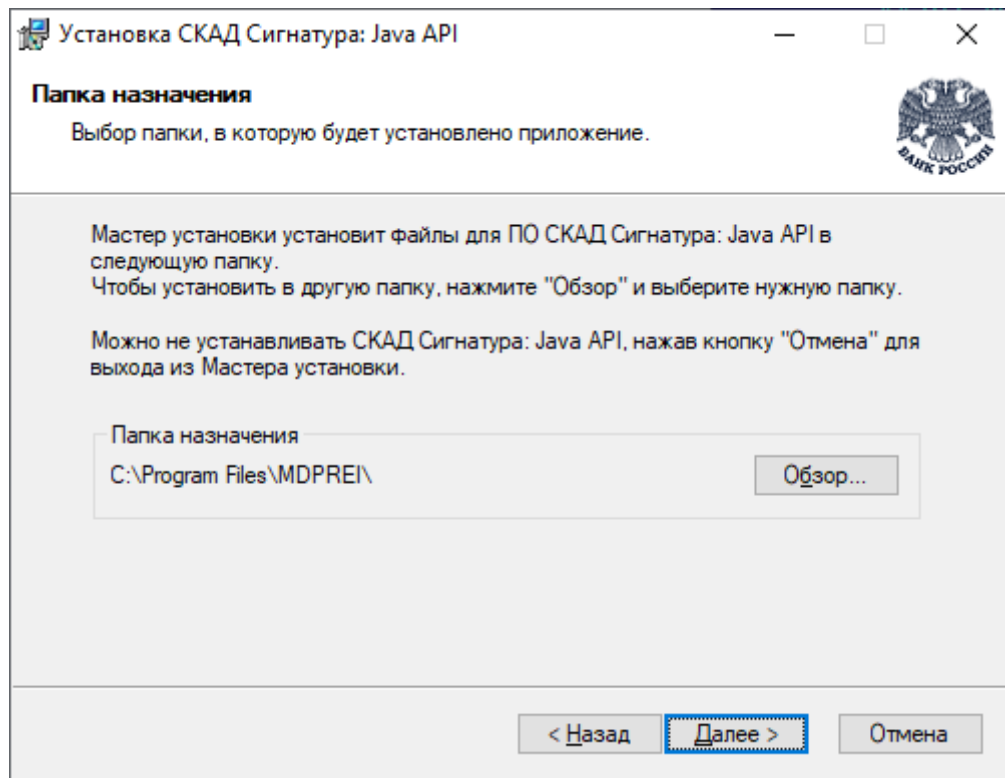


Рисунок 3 – Окно «Папка назначения»

Появится окно «Выбор типа установки» (Рисунок 4). Нажмите кнопку «Далее».

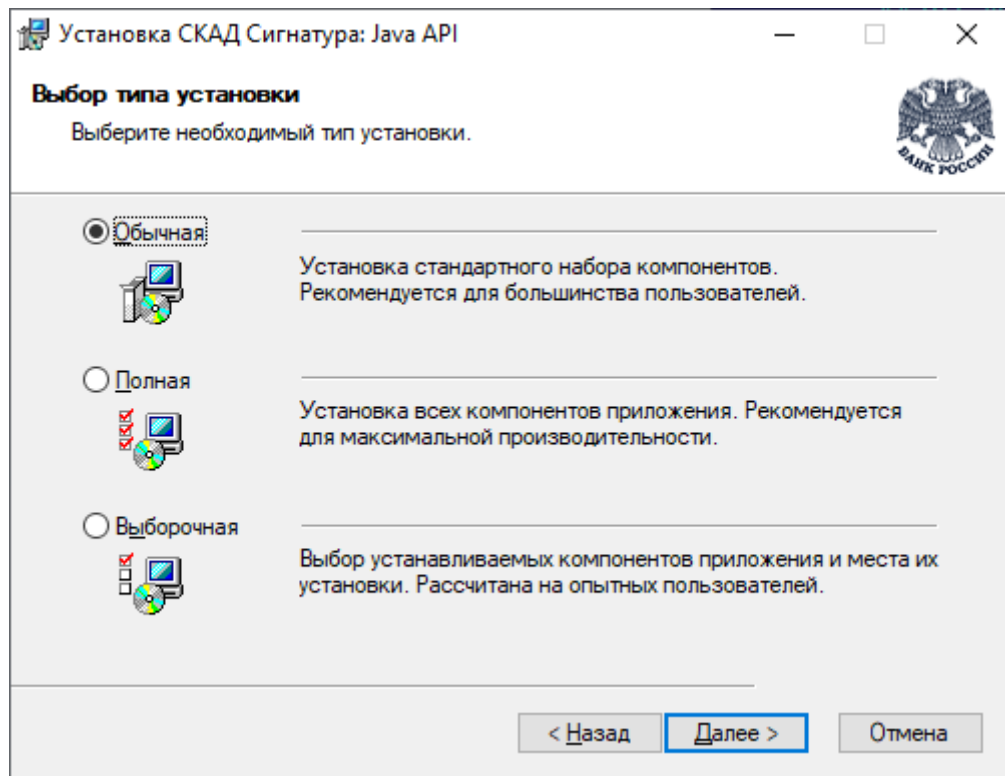


Рисунок 4 – Окно «Выбор типа установки»

Появится окно готовности к установке (Рисунок 5). Нажмите кнопку «Далее».

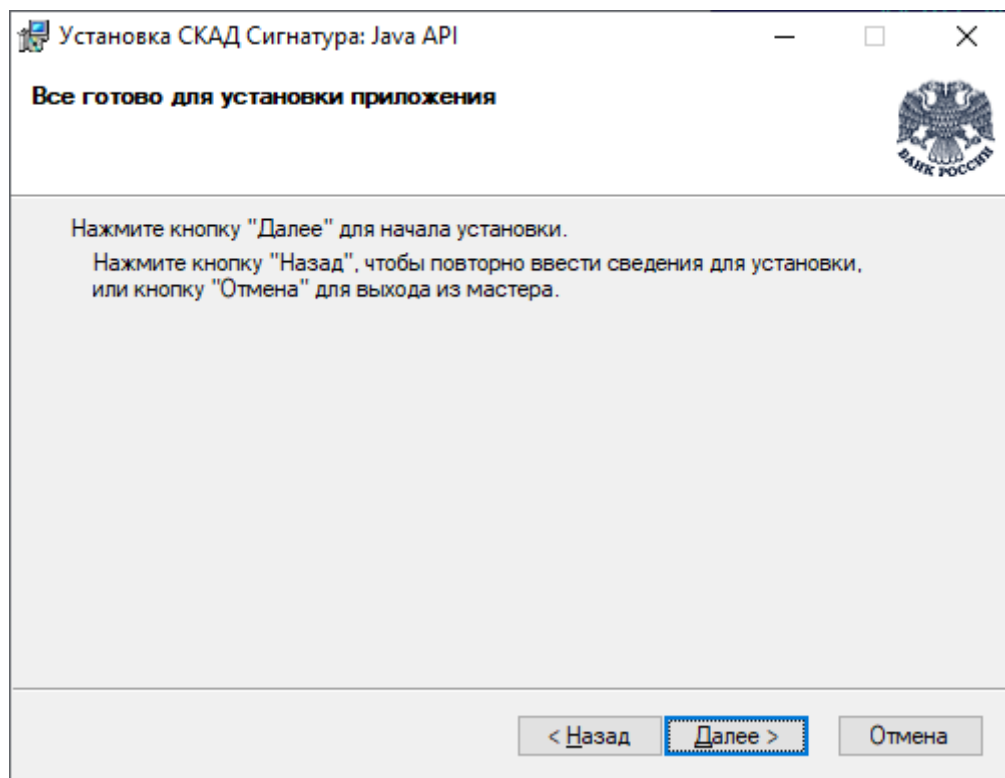


Рисунок 5 – Окно готовности к установке

По завершении установки будет показано окно завершения установки (Рису-

нок 6). Нажмите кнопку «Готово».

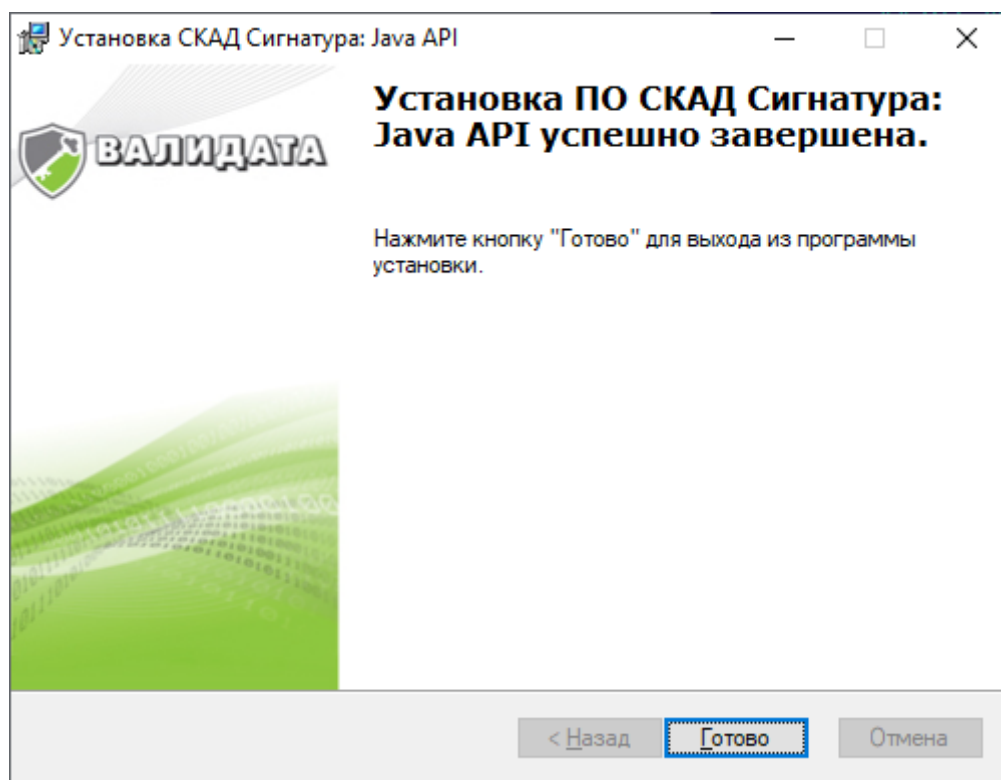


Рисунок 6 – Окно завершения установки

2.3 Контроль целостности

После успешной инсталляции ППИ Java СКАД «Сигнатура» необходимо обеспечить формирование файлов верификации и проведение требуемых мероприятий по контролю целостности (см. документ ВАМБ.00107-06 93 02 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Программа контроля целостности. Руководство администратора информационной безопасности»). Ниже приведён список файлов, входящих в ППИ Java СКАД «Сигнатура» и требующих обеспечения контроля целостности:

а) в системном каталоге ОС:

- spki1jni.dll;

б) в каталоге, в который установлен программный интерфейс ППИ Java СКАД «Сигнатура»:

- Pki1.LocalIface.Jar;
- Pki1.Test.Jar;
- Pki1.Test.Cmd.

3 УДАЛЕНИЕ ППИ JAVA СКАД «СИГНАТУРА»

Перед запуском процедуры удаления ППИ Java СКАД «Сигнатура» необходимо зарегистрироваться на компьютере с правами локального администратора.

Для удаления необходимо использовать пункт системного меню Windows «Пуск», «Настройка», «Панель управления», «Установка и удаление программ».

Далее подсветить строку с программным интерфейсом ППИ Java СКАД «Сигнатура»: либо СКАД Сигнатура: Java API – для 32-битной версии, либо СКАД Сигнатура: Java API (x64) – для 64-битной версии.

Нажать кнопку «Удалить» и следовать инструкциям мастера.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

КЗИ	Криптографическая защита информации
ОС	Операционная система (Operating System)
ППИ	Прикладной программный интерфейс
СКАД	Система криптографической авторизации электронных документов
ЭП	Электронная подпись (Digital Signature)

ПЕРЕЧЕНЬ РИСУНКОВ

1	Окно мастера установки	7
2	Окно «Сведения о пользователе»	7
3	Окно «Папка назначения»	8
4	Окно «Выбор типа установки»	9
5	Окно готовности к установке	9
6	Окно завершения установки	10

[illegible][illegible]