

ООО «ВАЛИДАТА»

УТВЕРЖДЕН  
ВАМБ.00143-06-ЛУ

**«СИГНАТУРА-СЕРТИФИКАТ L» ВЕРСИЯ 6  
ПРИКЛАДНОЙ ПРОГРАММНЫЙ ИНТЕРФЕЙС**

Руководство по установке и настройке

ВАМБ.00143-06 91 01

2023

## **Аннотация**

Данный документ содержит описание процесса установки и удаления библиотеки прикладного программного интерфейса работы с сервисами Центра Регистрации (далее – ЦР) и Центра Сертификации (далее – ЦС) Удостоверяющего Центра (далее – УЦ) для операционных систем (ОС) семейства Linux программного комплекса (ПК) ВАМБ.00128-06 «Сигнатура-сертификат L» версия 6».

Документ предназначен для специалистов, осуществляющих установку и настройку ПК «Сигнатура-сертификат L» версия 6. Прикладной программный интерфейс» (далее по тексту — ППИ ПК «Сигнатура-сертификат L»).

Документ разработан специалистами ООО «Валидата».

## Содержание

<b>1</b>	<b>НАЗНАЧЕНИЕ, СОСТАВ И ТРЕБОВАНИЯ К ОПЕРАЦИОННОЙ СРЕДЕ И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ</b>	<b>4</b>
1.1	Назначение библиотеки . . . . .	4
1.2	Характеристики библиотеки . . . . .	4
1.3	Использование библиотеки . . . . .	5
1.3.1	Основные понятия и определения . . . . .	5
1.3.2	Условия использования библиотеки для языков C/C++ . . . . .	5
1.3.3	Условия использования библиотеки для языка Java . . . . .	6
1.3.4	Описание состава библиотеки для языков C/C++ . . . . .	6
1.3.5	Описание состава библиотеки для языка Java . . . . .	7
<b>2</b>	<b>УСТАНОВКА ППИ ПК «Сигнатура-сертификат L»</b>	<b>8</b>
2.1	Контроль целостности и легальности эталонной копии ППИ ПК «Сигнатура-сертификат L» . . . . .	8
2.2	Инсталляция библиотеки для языков C/C++ . . . . .	8
2.3	Инсталляция библиотеки для языка Java . . . . .	8
<b>3</b>	<b>УДАЛЕНИЕ ППИ ПК «Сигнатура-сертификат L»</b>	<b>10</b>
3.1	Удаление библиотеки для языков C/C++ . . . . .	10
3.2	Удаление библиотеки для языка Java . . . . .	10

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

## **1.1 Назначение библиотеки**

Библиотека прикладного программного интерфейса работы с сервисами ЦР и ЦС для операционных систем (ОС) семейства Linux (далее по тексту - библиотека) предназначена для совместной работы с программным комплексом ВАМБ.00128-06 "Сигнатура-сертификат L" версия 6, предоставляет программный интерфейс работы с запросами на выпуск и отзыв сертификатов.

Библиотека ППИ ПК «Сигнатура-сертификат L» обеспечивает удаленный доступ к функциям ЦР и ЦС обработки запросов на выпуск и отзыв сертификатов прикладному программному обеспечению, написанному на языках C/C++ и Java.

Удаленный доступ к функциям осуществляется посредством использования протокола DCE-RPC поверх протокола TCP/IP.

Библиотека ППИ ПК «Сигнатура-сертификат L» обеспечивает доступ к следующим функциям ЦР:

- проверка соединения с ЦР;
- обработка запроса на выпуск сертификата с выработкой запроса для ЦС;
- обработка запроса на выпуск сертификата с модифицирующим шаблоном с выработкой запроса для ЦС;
- обработка выпущенного ЦС сертификата;
- обработка запроса на отзыв сертификата с выработкой запроса для ЦС;
- получение объектов из указанного справочника ЦР по критерию поиска;
- проверка соединения ЦР с ЦС;
- вызов ЦС для выпуска сертификата по запросу на выпуск;
- вызов ЦС для выпуска сертификата по запросу на выпуск с модифицирующим шаблоном;
- вызов ЦС для обработки запроса на отзыв сертификата;

Библиотека ППИ ПК «Сигнатура-сертификат L» обеспечивает доступ к следующим функциям ЦС:

- проверка соединения с ЦС;
- выпуск сертификата по запросу на выпуск;
- выпуск сертификата по запросу на выпуск с модифицирующим шаблоном;
- обработка запроса на отзыв сертификата;

## **1.2 Характеристики библиотеки**

Библиотека предназначена для встраивания ППИ ПК «Сигнатура-сертификат L» в прикладные системы. Требования к аппаратно-программной среде, в которой функционирует библиотека, приведены в документе

ВАМБ.00143-06 30 01 ««Сигнатура-сертификат L» версия 6. Прикладной программный интерфейс. Формуляр».

Запрос на выпуск сертификата передаётся в формате PKCS#10. Модифицирующий шаблон передаётся в формате XML. Запрос на отзыв сертификата для ЦС может быть сформирован в ЦР на основании запроса на отзыв в формате XML.

Форматы сертификатов ключей проверки ЭП и/или открытых ключей шифрования, списков аннулированных сертификатов (САС) и PKCS#10 запросов на получение сертификатов, формируемых и поддерживаемых библиотекой, соответствуют Рекомендациям по стандартизации Р 1323565.1.023-2022 «Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS#10 инфраструктуры открытых ключей X.509», которые в свою очередь соответствуют одноименной спецификации Технического комитета № 26.

## 1.3 Использование библиотеки

### 1.3.1 Основные понятия и определения

Все операции, выполняемые посредством вызовов функций библиотеки, оперируют объектами **системы управления сертификатами (СУС)** - сертификатами, САС, запросами PKCS#10, запросами на аннулирование. Также для некоторых операций используются шаблоны и/или модифицирующие шаблоны в формате XML.

### 1.3.2 Условия использования библиотеки для языков C/C++

При использовании библиотеки для языков C/C++ необходимо соблюдать следующие условия:

- если не указано обратное, все строковые данные, получаемые и возвращаемые библиотекой, должны быть в кодировке Windows Code Page 1251 (Windows-1251, CP1251);

- библиотека предназначена для использования в приложениях либо написанных на языках программирования C/C++, либо совместимых с ними по форматам данных и параметрам вызовов функций. При использовании библиотеки в приложениях, написанных на других языках программирования, должно выполняться требуемое преобразование форматов данных и параметров вызовов функций.

Приложение должно вызывать функции библиотеки последовательно:

- начало работы приложения;
- инициализация сессии библиотеки с локальным или удалённым сервисом ЦР/ЦС одной из функций **RACLI\_OpenSessionLocal()**, **CACLI\_OpenSessionLocal()**, **RACLI\_OpenSessionRemote()**, **CACLI\_OpenSessionRemote()**;
- использование сессии - вызов функций библиотеки для проверки соединения, обработки запросов на выпуск или отзыв сертификатов или получения списка объектов;

- освобождение сессии библиотеки функцией **RACLI\_CloseSession()** или **CACLI\_CloseSession()**;
- окончание работы приложения.

*Примечание - В процессе своей работы приложению разрешается инициализировать и деинициализировать несколько различных сессий библиотеки, в том числе в целях их одновременного (параллельного) использования.*

### 1.3.3 Условия использования библиотеки для языка Java

При использовании библиотеки для языка Java необходимо соблюдать следующие условия:

- при совместном использовании данной библиотеки и ВАМБ.00127-06 12 08 библиотеки прикладного программного интерфейса криптографического сервера для платформ "Java" и "IBM WebSphere Application Server", входящей в состав ПК ВАМБ.00127-06 СКЗИ «Янтарь L» версия 6, необходимо использовать компоненты Java DCE-RPC, входящие в состав данной библиотеки;
- библиотека предназначена для использования в приложениях либо написанных на языке программирования Java, либо совместимых с ним по форматам данных и параметрам вызовов функций. При использовании библиотеки в приложениях, написанных на других языках программирования, должно выполняться требуемое преобразование форматов данных и параметров вызовов функций.

*Примечание - При необходимости использования библиотеки из нескольких потоков приложения необходимо обеспечить эксклюзивное использование каждого контекста конкретным потоком, т.е. не допускается одновременное использование данного контекста несколькими потоками приложения.*

### 1.3.4 Описание состава библиотеки для языков C/C++

В состав библиотеки для языков C/C++ входят следующие файлы:

- **ra\_cli\_extiop.a** - модуль статической библиотеки функций работы с ЦР, используемый для линковки;
- **ca\_cli\_extiop.a** - модуль статической библиотеки функций работы с ЦС, используемый для линковки;
- **ra\_cli\_extiop.h** - файл заголовков с определениями констант, структур и прототипов функций библиотеки работы с ЦР;
- **ca\_cli\_extiop.h** - файл заголовков с определениями констант, структур и прототипов функций библиотеки работы с ЦС;
- **cara\_cli\_extiop.h** - вспомогательный файл заголовков с определениями констант, структур и прототипов функций библиотеки. Используется в 2 предыдущих файлах заголовков;
- **caracom.h, nbase.h, idlbase.h, ndrtypes.h** - вспомогательные файлы заголовков с определениями констант, структур библиотек DCE RPC;
- **ra\_test.cpp, ca\_test.cpp, makefile.tests** - файлы с исходными текстами тестовых утилит командной строки.

– **sra\_test, sca\_test** - исполняемые файлы тестовых утилит командной строки, собранных из вышеуказанных исходных текстов.

Файлы из вышестоящего списка, имеющие расширения **.a** и **.h**, подлежат контролю целостности по методике, приведённой в документе ВАМБ.00126-06 93 02 ««Сигнатура-клиент» версия 6. Программа контроля целостности. Руководство администратора информационной безопасности».

### 1.3.5 Описание состава библиотеки для языка Java

В состав библиотеки для языка Java входят следующие файлы:

– **CARASVCLib.jar** - архив, содержащий собственно библиотеку ППИ ПК «Сигнатура-сертификат L»;

– **CARASVCTest/CARASvcTest.class** - тестовая утилита, предназначенная для вызова функций библиотеки ППИ ПК «Сигнатура-сертификат L»;

– **jarapac/jarapac.jar** - архив, содержащий транспортно-независимую часть библиотеки Java DCE-RPC;

– **jarapac/ncacn\_ip\_tcp.jar** - архив, содержащий транспортно-зависимую часть библиотеки Java DCE-RPC;

– **jarapac/lib/jcifs-1.1.2.jar** - архив, содержащий библиотеку Java реализации протоколов CIFS/SMB;

– **run.bat** - командная процедура, позволяющая запускать тестовые утилиты в ОС Windows;

– **run.sh** - командная процедура, позволяющая запускать тестовые утилиты в ОС Linux.

Файлы из вышестоящего списка, имеющие расширение **.jar**, подлежат контролю целостности по методике, приведённой в документе ВАМБ.00126-06 93 02 ««Сигнатура-клиент» версия 6. Программа контроля целостности. Руководство администратора информационной безопасности».

## 2 УСТАНОВКА ППИ ПК «Сигнатура-сертификат L»

Перед установкой ППИ ПК «Сигнатура-сертификат L» на ЭВМ необходимо предварительно установить следующее программное обеспечение, руководствуясь инструкциями по его установке:

- ВАМБ.00126-06 12 02 ПК «Справочник сертификатов» из состава ПК «Сигнатура-клиент L» версия 6;
- ВАМБ.00126-06 12 03 «Комплект разработчика прикладного программного обеспечения» из состава ПК «Сигнатура-клиент L» версия 6.

### 2.1 Контроль целостности и легальности эталонной копии ППИ ПК «Сигнатура-сертификат L»

Перед непосредственной установкой ППИ ПК «Сигнатура-сертификат L» необходимо проверить целостность установочного комплекта. Это осуществляется с помощью программы контроля целостности.

Программа контроля целостности входит в состав программного комплекса ВАМБ.00126-06 «Сигнатура-клиент L» 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.00126-06 92 03 ««Сигнатура-клиент» версия 6. Программа контроля целостности. Руководство пользователя» и ВАМБ.00126-06 93 02 ««Сигнатура-клиент» версия 6. Программа контроля целостности. Руководство администратора информационной безопасности».

### 2.2 Установка библиотеки для языков C/C++

Установка библиотеки для языков C/C++ должна производиться пользователем, имеющим права локального администратора (пользователем **root**), в присутствии и под контролем администратора информационной безопасности.

Установка пакета библиотеки для языков C/C++ в ОС с типом установочных пакетов RPM должна выполняться командой вида **rpm -i scarasdk-6.0.<NNN>.0-0.<AAA>.rpm**, где **<NNN>** обозначает трехзначный номер сборки пакета, а **<AAA>** - код архитектуры (**x86\_64** для x64).

Установка пакета библиотеки для языков C/C++ в ОС с типом установочных пакетов DEB должна выполняться командой вида **dpkg -i scarasdk-6.0.<NNN>.0-0.<AAA>.deb**, где **<NNN>** обозначает трехзначный номер сборки пакета, а **<AAA>** - код архитектуры (**amd64** для x64, **e2k-8c** для e2k).

### 2.3 Установка библиотеки для языка Java

Установка библиотеки для языка Java выполняется посредством распаковки файла установочного комплекта **CaraInstall.jar** утилитой **Jar**.



Для установки необходимо выполнить следующие действия:

- зарегистрироваться в системе с правами системного администратора;
- смонтировать носитель установочного комплекта на соответствующее устройство;
- создать каталог (далее называемый каталогом установки), в который будет произведена установка;
- скопировать, пользуясь стандартными средствами ОС, файл установочного комплекта **CaraInstall.jar** в каталог установки;
- распаковать файл дистрибутива с помощью команды **jar -xvf CaraInstall.jar**, выполненной в каталоге установки;
- после распаковки необходимо убедиться, что в каталоге установки были созданы следующие файлы:
  - CARASVCLib.jar;
  - CARASVCTest/CARASvcTest.class;
  - jarapac/jarapac.jar;
  - jarapac/ncacn\_ip\_tcp.jar;
  - jarapac/lib/jcifs-1.1.2.jar;
  - run.bat;
  - run.sh.

## 3 УДАЛЕНИЕ ППИ ПК «Сигнатура-сертификат L»

### 3.1 Удаление библиотеки для языков C/C++

Удаление библиотеки для языков C/C++ должно производиться пользователем, имеющим права локального администратора (пользователем **root**).

Удаление пакета библиотеки для языков C/C++ в ОС с типом установочных пакетов RPM должно выполняться в командой вида **rpm -e scarasdk**.

Удаление пакета библиотеки для языков C/C++ в ОС с типом установочных пакетов DEB должно выполняться в командой вида **dpkg -r scarasdk**.

### 3.2 Удаление библиотеки для языка Java

Удаление библиотеки для языка Java выполняется стандартными средствами ОС.

Для удаления необходимо выполнить следующие действия:

- зарегистрироваться в системе с правами системного администратора;
- перейти в каталог установки;
- удалить следующие файлы:
  - CARASVCLib.jar;
  - CARASVCTest/CARASvcTest.class;
  - jarapac/jarapac.jar;
  - jarapac/ncacn\_ip\_tcp.jar;
  - jarapac/lib/jcifs-1.1.2.jar;
  - run.bat;
  - run.sh.

[illegible][illegible]