Requirements

Основные технические требования для подсистемы подготовки данных и управления ключами системы WAY4

03.49.30

15.06.2020

СОДЕРЖАНИЕ

В документе используются следующие обозначения:

Предостережения в связи с возможностью совершения неправильных действий.

Предостережения в связи с возможностью совершения неправильных действий.

1. Архитектура подсистемы подготовки данных и управления ключами

Архитектура подсистемы подготовки данных и управления ключами представлена на Рис. 1.

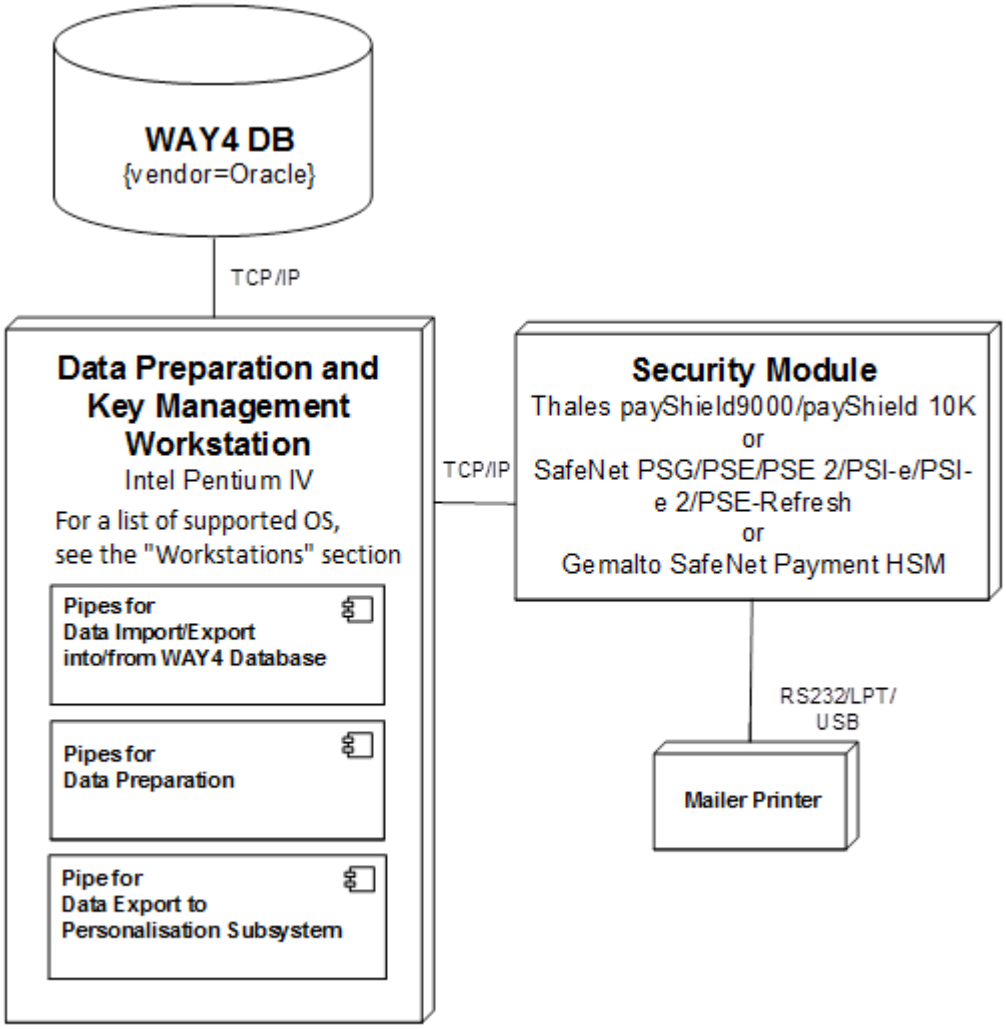

Рис. 1. Архитектура подсистемы подготовки данных и управления ключами

2. Требования к аппаратному обеспечению

Представленные требования являются обобщенными, они могут уточняться в ходе проведения анализа на этапе проекта внедрения системы WAY4 либо модернизации серверов. Указанные требования соответствуют стандартной конфигурации для ста тысяч карт.

2.1 Сервер базы данных

Архитектура системы

Платформа Unix, совместимая с Oracle Database

Процессор

2 или более

ОЗУ

2 GB или более

Дисковая подсистема

2 внутренних диска не менее 20 GB, аппаратно или программно-конфигурируемый RAID1.

Устройство резервного копирования

Любое, обеспечивающее регулярное копирование объемов соответственно размеру дисковой подсистемы

Поддержка ПО

Аппаратное обеспечение должно быть сертифицировано для Oracle Database и платформы Unix

Локальная сеть

не менее 100 Мбит Ethernet

Прочее оборудование

Привод DVD-ROM

Количество

1 комплект оборудования

2.2 Криптографическое оборудование

Для выполнения криптографических операций при подготовке данных для персонализации смарт-карт в системе должно быть установлено аппаратное криптографическое устройство.

В подсистеме подготовки данных и управления ключами поддерживаются два типа криптографических устройств:

- Thales payShield 9000 или payShield 10k;
- SafeNet PSG/PSE/PSE 2/PSI-e/PSI-e 2/PSE-Refresh.

2.2.1 Криптографическое оборудование производства Thales (payShield)

2.2.1.1 Архитектура системы

Thales payShield 9000 или payShield 10k с сетевым адаптером, обеспечивающим соединение по протоколу TCP/IP.

2.2.1.2 Служебное ПО (Software Environment)

Для производства EMV-карт на payShield 9000 может быть использована одна из двух конфигураций:

1.Для Smart Card Issuer Firmware версии 1119-09xx необходимо наличие следующих лицензий:

- HSM9-PAC301 Standard Base Package;
- HSM9-LIC002 RSA license;
- HSM9-LIC509 Russian CIF custom software for payShield 9000.

2. Начиная с версии 03.38.30 WAY4 Cards поддерживается Thales payShield 9000 с базовой прошивкой (HSM9-LIC001 Base Firmware версии 2.2a и выше) и набором лицензий:

- HSM9-LIC002 RSA License;
- HSM9-LIC011 Magnetic Stripe Contactless Card Data Preparation License;
- HSM9-LIC016 EMV based Card Data Preparation License;
- HSM9-LIC024 Magnetic Stripe Issuing;
- HSM9-LIC027 PIN and Key Printing License.

Для производства EMV-карт на Thales payShield 10k требуется Premium пакет лицензий и прошивка версии 1.0c.

2.2.1.3 Количество

2 (основной и резервный)

2.2.2 Криптографическое оборудование производства SafeNet (ProtectServer)

2.2.2.1 Архитектура системы

Модуль управления криптографическим устройством PSG /PSE (OWSeM) версии 4.17.075 и выше (для устройств с одним COM портом - PSI-e/PSE-Refresh, версии 4.17.079 и выше).

В качестве аппаратной платформы может быть использовано любое из нижеперечисленных устройств:

- SafeNet ProtectServer Gold (PSG)
- SafeNet ProtectServer External (PSE)
- SafeNet PSE-Refresh (с одним COM-портом) в режиме ручного ввода LMK без использования smart card
- SafeNet PSI-e (с одним COM портом) в режиме ручного ввода LMK без использования smart card
- SafeNet PSE 2 в режиме ручного ввода LMK без использования smart card
- SafeNet PSI-e 2 в режиме ручного ввода LMK без использования smart card

2.2.2.2 Служебное ПО (Software Environment)

Firmware – ПО уровня криптографического устройства.

Допустимо использовать Firmware следующих версий:

- v.2.04.xx
- v.3.00.xx

> ⚠ Запрещено использование Firmware версии v.2.06.xx/ v.2.07.xx из-за критической ошибки в работе с портом принтера.

Допустимо использовать Cryptoki (ProtectToolkit C (Runtime)) следующих версий:

- для внутренних (PCI) устройств: v.3.28 – v.4.00
- для внешних устройств – не используется DOM (Disk-On-Memory) Image – ПО уровня сервера, вмещающего криптографическое устройство.

Допустимо использовать DOM Image следующих версий:

- для внутренних (PCI) устройств – не используется
- для внешних устройств: v.2.00

Количество

2 (основной и резервный)

2.2.3 Криптографическое оборудование производства Gemalto (LUNA EFT 2)

2.2.3.1 Архитектура системы

Gemalto LUNA EFT 2 с сетевым адаптером, обеспечивающим соединение по протоколу TCP/IP.

2.2.3.2 Служебное ПО (Software Environment)

Для производства EMV-карт VISA PayWave и MasterCard PayPass на Gemalto LUNA EFT 2 требуется прошивка (firmware) версии 6.10.5 с установленным ПО SafeNet Luna EFT Payment HSM 2.2.0 .

2.2.3.3 Количество

2 (основной и резервный)

2.2.4 Дополнительное оборудование

Терминал, совместимый с RS-232-C (DTE). Скорость передачи данных от 300 бит/с (с возможностью увеличения до 115200 бит/с).

- Терминал не должен иметь возможности сохранять информацию для последующего вывода.
- Кабель для подключения терминала к криптографическому устройству, выполненный согласно спецификации производителя.

Количество терминалов: 1

Для SafeNet PSG/PSE: ASCII принтер для печати PIN-конвертов с последовательным интерфейсом RS-232-C (DCE) (не параллельным). Скорость передачи данных от 300 до 38400 бит/с.

Для Thales payShield 9000 и Thales payShield 10K может использоваться принтер для печати PIN конвертов с интерфейсом USB. Возможно использование принтеров с последовательным RS-232 (DCE/DTE) или с параллельным LPT интерфейсом через переходник USB-COM, USB-LPT.

Должен использоваться принтер ударного действия (например, матричный или посимвольно-печатающий) или специальный лазерный принтер для печати PIN-конвертов.

Принтер должен иметь возможность печати без использования красящей ленты для сохранения в секрете информации, содержащейся в PIN конверте. Протяжка бумаги с перфорированными краями должна осуществляться механизмом с зубчатым барабаном (не фрикционным) для выравнивания строк и столбцов текста.

Кабель для подключения терминала к криптографическому устройству, выполненный согласно спецификации производителя (для принтеров с последовательным интерфейсом – с учетом полной спецификации RS-232).

Для Gemalto LUNA EFT 2 может использоваться принтер для печати PIN-конвертов с интерфейсом USB / Serial, который соответствует техническим требованиям производителя криптографического устройства.

Количество принтеров: 1

> ⚠ Возможности конкретной модели оборудования необходимо уточнить у поставщика оборудования.

2.3 Рабочая станция оператора

Архитектура системы

Персональный компьютер с процессором Intel Pentium IV или более производительный

ОЗУ не менее 1 GB

Жесткий диск не менее 20 GB

Монитор с разрешением не ниже 1024x768

Клавиатура, мышь

Сетевой интерфейс (Ethernet)

Количество

2 (Количество рабочих станций определяется численностью персонала).

Для подсистемы подготовки данных и производства карт рекомендуется использовать выделенную рабочую станцию.

3. Требования к программному обеспечению

3.1 Сервер базы данных (Требования к программному обеспечению)

Операционная система семейства Unix (в зависимости от аппаратной платформы).

Oracle Database Standard Edition или Oracle Database Enterprise Edition.

Поддерживаемые версии Oracle Database:

- Oracle 12c 12.1.0.2 с обязательной установкой последнего PSU (Patch Set Update) и патча 21068213 (ORA-04043).
- Oracle 12c 12.2.0.1 с обязательной установкой последнего RU (Release Updates), патчей 27539876 и 24850493 (Doc ID 2463589.1).
- Oracle 18c с обязательной установкой последнего RU.
- Oracle 19c с обязательной установкой последнего RU.

ПО резервного копирования.

3.2 Рабочие станции

Поддерживаются следующие версии Microsoft Windows:

- Windows 7.
- Windows 8.
- Windows 8.1.
- Windows 10.
- Windows Server 2008 R2.
- Windows Server 2012 and Windows Server 2012 R2.
- Windows Server 2016.
- Windows Server 2019.

Для подсистемы подготовки данных и производства карт рекомендуется использовать выделенную рабочую станцию, на которой не запускаются другие процессы: как процессы системы WAY4, так и процессы, требующие большого количества операций ввода-вывода и/или вычислительных ресурсов (в том числе с использованием виртуальных машин).

Для рабочей станции рекомендуется увеличить объем памяти java-машины до 1024 MB. За инструкцией по настройке памяти необходимо обратиться в службу поддержки поставщика системы WAY4.

Кроме того, рекомендуется использовать стандартные каталоги системы WAY4 (<OWS_HOME>, <OWS_WORK> и <OWS_TEMP>), расположенные на локальной машине; при этом каталоги <OWS_WORK> и <OWS_TEMP> рекомендуется размещать на твердотельном накопителе (SSD). Не рекомендуется использовать сетевые диски.

Oracle JDK (номер требуемой версии и описание установки см. в документе "Oracle Java Commercial Updates для системы WAY4™").

Oracle Client для соответствующей версии ОС Windows, включая ODBC Driver.

Поддерживаемые версии Oracle Client: 12.1, 12.2, 18.3 и 19.3 (для Oracle Database 12c 12.2, Oracle Database 18c и Oracle Database 19c).

При использовании 64bit операционной системы:

- необходимо установить 32bit версию Oracle Client, иначе использование ODBC будет невозможно;
- источник ODBC на 64bit операционной системе настраивается запуском C:/Windows/SysWOW64/odbcad32.exe (32bit версия Инструмента Администратора ODBC), а не из "Панели управления".

В конфигурации Oracle ODBC Data Source на вкладке "Workarounds" необходимо установить флажок в поле "Bind TIMESTAMP as DATE". В противном случае некоторые SQL-запросы, выполняемые из DB Manager и включающие условия по дате, могут выполняться медленно.

4. Требования к персоналу

Ниже представлен перечень требований к персоналу для работы с системой WAY4. Требования компании OpenWay на период установки, тестирования и сертификации системы представлены в заключительном разделе настоящего документа.

4.1 Требования к персоналу клиента

Для нормального функционирования системы WAY4, установленной в банке или процессинговом центре, необходим соответствующий минимальный штат сотрудников клиента, обладающих определенными навыками и практическим опытом работы.

Решение о точном количестве и квалификации необходимого персонала клиент принимает в зависимости от профиля работы (объемы эмиссии и эквайринга). Однако для работы с системой WAY4 настоятельно рекомендуется располагать нижеперечисленным персоналом.

Следующие общие указания должны учитываться в процессе планирования комплектования штата сотрудников для работы с системой WAY4:

- Сотрудники, занятые работой с системой WAY4, должны обладать соответствующим уровнем образования и профессионального опыта в практической области.
- Весь персонал, занятый обслуживанием системы WAY4, должен пройти соответствующее обучение и сертификационное тестирование, прежде чем получить допуск к практической работе.
- Следует тщательно проанализировать моральный облик и психологический портрет каждого сотрудника с целью предотвращения возможного мошенничества.
- Желательно свободное владение разговорным английским языком всеми сотрудниками. Дополнительно требуется хорошее владение навыками письменной английской речи всем руководящим персоналом и сотрудниками, занимающимися взаиморасчетами и разрешением спорных ситуаций.
- Необходимо всестороннее обучение и сертификация сотрудников службы безопасности, бухгалтеров, а также инженеров по программному обеспечению, аппаратному обеспечению и телекоммуникациям.

4.1.1 Менеджер по карточным операциям

Количество

1

Подразделение

Отдел информационных технологий

Квалификация

Менеджмент + Маркетинг + Информационные технологии + Основы бухгалтерского учета

Английский язык

Свободное владение разговорной речью + хорошие навыки письменной речи

Специальное обучение

Управление карточной системой (OpenWay) + Курсы обучения, проводимы международными платежными системами

Сертификация

Рекомендуется сертификация в компании OpenWay

4.1.2 Инженер по выпуску карт и PIN-конвертов

Количество

2

Подразделение

Отдел информационных технологий

Квалификация

Информационные технологии + Основы карточного бизнеса

Английский язык

Хорошее владение разговорной речью

Специальное обучение

Производство карт и PIN-конвертов + Политика безопасности

Сертификация

Рекомендуется сертификация в компании OpenWay

4.1.3 Сотрудник службы безопасности

Количество

1-3

Подразделение

Отдел информационных технологий

Квалификация

Информационные технологии + Информационная безопасность + Управление персоналом

Английский язык

Хорошее владение разговорной речью

Специальное обучение

Карточные технологии + Политика безопасности VISA и MC + Работа с криптографическим оборудованием + Информация о мошенничестве в карточном бизнесе

Сертификация

Рекомендуется сертификация в компании OpenWay

4.1.4 Администратор базы данных

Количество

1

Подразделение

Отдел информационных технологий

Квалификация

Администратор баз данных, сертифицированный ORACLE

Английский язык

Нет специальных требований

Специальное обучение

Обучение среднего уровня в компании ORACLE обязательно

Сертификация

Желательна сертификация в компании ORACLE

4.2 Требования к персоналу на период установки системы

Следующие сотрудники банка, отвечающие за установку системы WAY4 должны быть доступны в течение всего периода установки и тестирования системы:

- Администратор базы данных ORACLE – весь период
- Сотрудники службы безопасности, располагающие всеми необходимыми механическими и электронными ключами и обученные работе с криптографическим оборудованием, имеющие в своем распоряжении документацию по криптографическому оборудовании – по требованию

5. Требования к условиям эксплуатации

Ниже приводится перечень требований к условиям эксплуатации системы WAY4.

5.1 Условия эксплуатации

При подготовке помещений для установки системы WAY4 необходимо учесть следующие указания:

- Размеры помещения должны обеспечивать свободу перемещения оборудования и персонала, а также свободный доступ ко всем элементам оборудования.
- Все помещения должны располагаться поблизости друг от друга для обеспечения удобства коммуникации и предотвращения нарушений безопасности.
- При установлении режима безопасности отдельных помещений должны строго соблюдаться руководящие указания международных платежных систем в области безопасности.
- Все помещения должны быть оборудованы устройствами кондиционирования воздуха с целью предотвращения перегрева оборудования и обеспечения комфортабельных условий работы.
- Необходимо использовать электронные замки для всех помещений. В помещениях, где размещаются оборудование для производства карт и серверы, должны быть установлены замки повышенного уровня безопасности.
- Все помещения должны быть обеспечены необходимой мебелью.

5.2 Требования к условиям эксплуатации на период установки системы

Все требования к условиям эксплуатации должны быть выполнены к моменту установки системы WAY4 с учетом необходимых условий для работы персонала компании OpenWay, участвующего в установке системы.

К моменту установки системы должна быть обеспечена необходимая настройка компьютерных сетей.