



PA-DSS Implementation Guide

Руководство по обеспечению безопасности в системе WAY4™ согласно стандарту PA-DSS

2.24

09.12.2020

СОДЕРЖАНИЕ

| | | |
|----------|--|-----------|
| 1 | Конфиденциальные данные карт (Sensitive Authentication Data) | 8 |
| 1.1 | Определение конфиденциальных данных карт | 8 |
| 1.2 | Особенности предыдущих версий системы WAY4 | 9 |
| 1.2.1 | LifeStyle Banking | 10 |
| 1.2.2 | Web Banking/Mobile Web Banking | 11 |
| 1.3 | Обработка конфиденциальных данных | 11 |
| 2 | Хранение данных карт (Cardholder Data) и криптографических ключей | 12 |
| 2.1 | Требования к управлению ключами | 12 |
| 2.2 | Срок хранения данных карт (Data Retention) | 14 |
| 2.3 | Требования к хранению данных | 16 |
| 2.3.1 | Зашифрованные табличных пространств | 17 |
| 2.3.2 | Настройка сценариев при использовании TDE | 17 |
| 2.3.3 | Housekeeping и TDE | 18 |
| 2.3.4 | Шифрование дисковых разделов | 18 |
| 2.4 | Требования к хранилищу данных | 19 |
| 2.5 | Требования к серверу базы данных | 19 |
| 2.6 | Требования к рабочим станциям пользователей | 20 |
| 2.7 | Строго определенные механизмы доступа к PAN | 20 |
| 2.8 | Поддержка требований стандарта PCI DSS продуктами и компонентами WAY4 | 20 |
| 3 | Регистрация пользователей и установка паролей | 24 |
| 3.1 | Учетные записи администраторов, создаваемые по умолчанию | 24 |
| 3.1.1 | NetServer | 24 |
| 3.1.2 | Transaction Switch | 24 |
| 3.2 | Принципы безопасной аутентификации | 25 |
| 3.2.1 | NetServer | 26 |
| 3.2.2 | WAY4 Web | 26 |
| 3.2.3 | Messenger banking | 27 |
| 3.2.4 | Transaction Switch | 27 |
| 3.2.5 | Web Banking/Mobile Web Banking | 27 |
| 3.2.6 | Шифрование конфигурационных параметров | 28 |

| | | |
|----------|---|-----------|
| 3.3 | Шифрование пароля к СУБД Oracle | 28 |
| 3.3.1 | Как определить алгоритм шифрования паролей | 28 |
| 3.4 | Хранение ключей в Java Keystore | 29 |
| 3.5 | Требования для доступа к данным | 30 |
| 3.6 | Требования к серверу базы данных [Регистрация пользователей и установка паролей] | 30 |
| 3.7 | Требования к рабочим станциям пользователей [Регистрация пользователей и установка паролей] | 30 |
| 4 | Ведение аудитного журнала | 31 |
| 4.1 | NetSever | 32 |
| 4.2 | Transaction Switch | 32 |
| 4.3 | WAY4 Web | 32 |
| 4.4 | Поддержка централизованного протоколирования | 33 |
| 4.4.1 | Копирование файлов аудитных журналов с локального компьютера на удаленный 3 | 3 |
| 4.4.2 | Использование распределенной файловой системы | 35 |
| 4.5 | Требования к серверу базы данных [Ведение аудитного журнала] | 35 |
| 4.6 | Требования к файловому серверу | 35 |
| 4.7 | Протоколирование приложений | 35 |
| 5 | Разработка безопасных платежных приложений | 39 |
| 5.1 | Требования к приложениям | 39 |
| 5.1.1 | Application Server | 39 |
| 5.1.2 | WAY4 Web | 39 |
| 5.1.3 | Messenger banking | 40 |
| 5.1.4 | Web Banking/Mobile Web Banking | 40 |
| 5.2 | Методика версионирования WAY4 | 40 |
| 5.2.1 | Допустимые подстановочные знаки (Wildcards) | 41 |
| 6 | Использование беспроводных технологий передачи данных | 42 |
| 7 | Обеспечение безопасности обновлений | 43 |
| 7.1 | Требования | 43 |
| 7.2 | Процедура | 44 |
| 7.3 | Обзор процесса установки | 44 |

| | | |
|-----------|---|-----------|
| 8 | Обеспечение безопасности платежного приложения | 46 |
| 8.1 | Перечень используемого стороннего программного обеспечения, аппаратной архитектуры, используемых системных служб и протоколов | 46 |
| 8.2 | Требования к серверу базы данных [Обеспечение безопасности платежного приложения] | 52 |
| 8.3 | Требования к файловому серверу [Обеспечение безопасности платежного приложения] | 52 |
| 8.4 | Требования к рабочим станциям пользователей [Обеспечение безопасности платежного приложения] | 53 |
| 8.5 | Требования для доступа к данным [Обеспечение безопасности платежного приложения] | 53 |
| 8.5.1 | NetServer и Transaction Switch | 53 |
| 8.6 | Требования к конфигурации системы | 53 |
| 9 | Безопасность сетевой инфраструктуры | 54 |
| 9.1 | Требования к базе данных сервера | 54 |
| 9.2 | Требования к файловому серверу [Безопасность сетевой инфраструктуры] | 54 |
| 9.3 | Требования к рабочей станции пользователя | 54 |
| 9.4 | Требования к хранилищу данных [Безопасность сетевой инфраструктуры] | 54 |
| 10 | Удаленный доступ | 55 |
| 10.1 | Мультифакторная аутентификация | 55 |
| 10.1.1 | Не консольный административный доступ с использованием USB-токен | 56 |
| 10.1.2 | NetServer | 58 |
| 10.1.3 | Health Monitoring | 58 |
| 10.1.4 | WAY4 Web (WS Runtime and Application Server) | 60 |
| 10.2 | Удаленный доступ к файловому серверу | 60 |
| 10.3 | Требования к удаленным рабочим станциям пользователей | 60 |
| 11 | Защита данных карт при передаче по открытым каналам связи | 62 |
| 11.1 | Использование шифрования и защищенных протоколов передачи данных | 62 |
| 11.2 | Маскирование PAN | 66 |
| 12 | Защита неконсольного административного доступа | 67 |
| 12.1 | NetServer и Transaction Switch | 67 |
| 13 | Тестирование | 68 |
| 13.1 | Требования к данным, используемым при тестировании системы | 68 |

| | | |
|-----------|--|-----------|
| 14 | Настройка криптографического оборудования (HSM) | 69 |
| 15 | История изменения документа | 70 |

Введение

В данном документе приведены требования и описаны настройки, которые необходимо выполнить в модулях системы WAY4™ для того, чтобы обеспечить выполнение требований стандарта Payment Card Industry Data Security Standard (PCI DSS).

Данный документ не является полным руководством по установке и настройке системы WAY4, однако выполнение данных требований необходимо для обеспечения совместимости с требованиями безопасности по стандарту PCI DSS v. 3.2.1.

Выполнение требования к обеспечению безопасности минимизирует потенциальные риски, связанные с компрометацией Sensitive Authentication Data / Cardholder Data, таких как содержимое треков карт, кодов проверки подлинности карт (CAV2, CID, CVC2, CVV2), данных PIN-кодов и PIN-блоков и, соответственно, помогают устранить возможность мошенничества с использованием данных, относящихся к платежным картам.

Соблюдение требований Visa 3-D Secure и MasterCard SecureCode требования к компонентам WAY4, реализующим функциональность 3-D Secure отделена от проверки PA-DSS и является предметом отдельного тестирования с помощью Visa и MasterCard соответственно.

Данный документ предназначен для системных администраторов (сотрудников банков и процессинговых центров), в задачи которых входит создание и поддержка сетевой инфраструктуры для работы приложений системы WAY4, администрирование приложений системы WAY4, а также выполнение всевозможных служебных функций, связанных с обеспечением безопасности.

Данный документ основывается на следующих источниках:

- "Payment Card Industry (PCI) Data Security Standard" Version 3.2.1 May 2018";
- "Payment Card Industry (PCI) Data Security Standard. Glossary, Abbreviations and Acronyms";
- "Payment Card Industry (PCI) Payment Application Data Security Standard" Version 3.2 October 2016".

С данными документами можно ознакомиться на сайте <http://www.pcisecuritystandards.org>

Рекомендуется пользоваться следующими источниками из комплекта документации OpenWay:

- "Housekeeping в системе WAY4™";
- "Аудит работы с базой данных в системе WAY4™";
- "Выгрузка аудитного журнала системы WAY4";
- "Безопасный административный доступ к БД Oracle в соответствии со стандартом PCI DSS";
- "Администрирование пользователей в системе WAY4™";
- "Управление криптографическими ключами в системе WAY4™";
- "Установка и Конфигурирование NetServer Java Secure Console";
- "Администрирование WAY4™ Application Server";
- "Redefinition Tool".

Рекомендуется пользоваться следующим источником из комплекта документации компании Oracle:

- "Sustainable Compliance for the Payment Card Industry Data Security Standard".

В документации используются следующие обозначения:

- названия полей экранных форм выделяются *курсивом*;
- комбинации клавиш приводятся в угловых скобках, например, <Ctrl>+<F3>;
- названия кнопок экранных форм и вкладок приводятся в квадратных скобках, например, [Approve];
- последовательность выбора пункта в меню пользователя или контекстном меню отображается с помощью стрелок следующим образом: "Issuing → Contracts Input & Update";
- последовательность выбора пункта в системном меню отображается с помощью стрелок следующим образом: Database => Change password;
- различные переменные значения, например, имена каталогов и файлов, а также пути к файлам, варьируемые для каждой локальной машины, приводятся в угловых скобках, например, <OWS_HOME>.

Предостережения и информационные сообщения размечаются следующим образом:



Предостережения в связи с возможностью совершения неправильных действий.



Сообщения, содержащие информацию о важных особенностях, дополнительных возможностях или оптимальном использовании некоторых функций системы.

Данное руководство предназначено для системы WAY4 версии 03.51.1.3.x.

Документ подлежит регулярному (ежегодному) обновлению, а также подлежит обновлению в случаях изменений в системе WAY4, затрагивающих аспекты совместимости со стандартом PA-DSS, либо в случае изменений стандартов PCI DSS или PA-DSS.



В случае возникновения разночтений между русской и английской версиями документа следует руководствоваться английской версией документа.

1 Конфиденциальные данные карт (Sensitive Authentication Data)

Данная глава посвящена удовлетворению требований п.п. 1.1.4 – 1.1.5 стандарта PA-DSS, приведенных ниже.

| PA-DSS Requirement | PA-DSS Topic |
|--------------------|---|
| 1.1.4 | Delete sensitive authentication data stored by previous payment application versions. |
| 1.1.5 | Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application. |

1.1 Определение конфиденциальных данных карт

Стандарт PA-DSS относит к конфиденциальным следующие данные карт:

1. Полные данные любой дорожки магнитной полосы карты, расположенной на задней стороне карты, либо образ любой дорожки магнитной полосы, расположенный в памяти микропроцессора карты.
2. Трех- или четырех-символьный код проверки подлинности карты, расположенный на лицевой части карты, либо на полосе для подписи (CVV2, CVC2, CID, CAV2 data)
3. PIN-код и зашифрованный PIN-блок.



Поля PVV и Encrypted PIN являются полями, без которых нормальное функционирование системы невозможно. Поля содержат PVV, IBM 3624 OFFSET, HSM PIN OFFSET (рассчитан по алгоритму Thales) и не подпадают под запрет на хранение у эмитента или компании, предоставляющей эмиссионные сервисы. Хранение этих величин в базе не запрещено PCI DSS.

1.2 Особенности предыдущих версий системы WAY4

В предыдущих версиях системы WAY4 Sensitive Authentication Data / Cardholder Data могли храниться в таблицах APPL_CARD_INFO, CARD_INFO и MAILBOX базы данных, из-за отсутствия в этих версиях поддержки требований PCI DSS, а также в результате миграции карт, для которых величины проверки карт должны проверяться при недоступном значении ключа CVK. Удаление данных из таблиц APPL_CARD_INFO, CARD_INFO и MAILBOX абсолютно необходимо для приведения системы в соответствие с требованиями PCI DSS.

Перечень полей, данные которых подлежат удалению:

- APPL_CARD_INFO.CVC
- APPL_CARD_INFO.CVC2
- APPL_CARD_INFO.ICVV
- APPL_CARD_INFO.OFFSET_DATA
- APPL_CARD_INFO.PIN
- APPL_CARD_INFO.PVV
- CARD_INFO.CVC
- CARD_INFO.CVC2
- CARD_INFO.ICVV
- MAILBOX.BUF1
- MAILBOX.BUF10
- MAILBOX.BUF11
- MAILBOX.BUF12
- MAILBOX.BUF13
- MAILBOX.BUF14
- MAILBOX.BUF15
- MAILBOX.BUF16
- MAILBOX.BUF17
- MAILBOX.BUF18
- MAILBOX.BUF19
- MAILBOX.BUF2
- MAILBOX.BUF20
- MAILBOX.BUF21
- MAILBOX.BUF22
- MAILBOX.BUF23
- MAILBOX.BUF24
- MAILBOX.BUF3
- MAILBOX.BUF4
- MAILBOX.BUF5
- MAILBOX.BUF6
- MAILBOX.BUF7
- MAILBOX.BUF8

- MAILBOX.BUF9

Перед удалением полей таблицы CARD_INFO: CARD_INFO.CVC, CARD_INFO.CVC2, CARD_INFO.ICVV необходимо произвести дополнительный анализ используемых конкретном экземпляре системы методов проверки карт. В форме "Full → Configuration Setup → Card Production Setup → Bank Production Parameters → Validation" следует убедиться, что не используются методы проверки криптографических величин "HSM both" и "HSM both YYYYMM". Если данные методы используются, необходимо изменить настройку следующим образом:

- вместо "HSM both" установить значение "HSM both, no DB CVV2";
- вместо "HSM both YYYYMM" установить значение "HSM both YYYYMM, no DB CVV".

Для проверки величин должны быть доступны ключи CVK.

В случае невозможности удаления полей CARD_INFO.CVC, CARD_INFO.CVC2, CARD_INFO.ICVV из-за того, что значения используются для проверки значений CVV. CVC и аналогичных, в случае, когда надлежащее свойство валидации ключа отсутствует (как правило, это бывает в случае если карта была перенесена из другой системы), необходимо перевыпустить карты в WAY4. Если перевыпуск данных карт невозможен, то необходимо руководствоваться замечанием 2 к требованию 1.1 PA-DSS, а именно тем, что хранение данных величин допускается для эмитента или компании, предоставляющей эмиссионный сервис при условии безопасного хранения этих данных.

Поля CARD_INFO.PVV, CARD_INFO.OFFSET_DATA, CARD_INFO.ENCRYPTED_PIN содержат PVV, IBM 3624 OFFSET, HSM PIN OFFSET и, соответственно не подпадают под запрет на хранение у эмитента или компании, предоставляющей эмиссионные сервисы.

Удаление данных из таблиц БД производится при помощи запуска соответствующих скриптов, предоставляемых по запросу. Запуск удаления данных может производиться только после полного завершения текущего цикла обработки заявлений и при остановленном режиме онлайн. После удаления средствами СУБД необходимо произвести действия, предотвращающие восстановление удаленных данных.

1.2.1 LifeStyle Banking

Предыдущие версии Lifestyle Banking могут содержать чистый текст PAN в журналах сообщений, поэтому все файлы журналов из предыдущих версий должны быть надежно удалены. Файлы журналов сообщений хранятся в папках (некоторые из них могут не существовать в конкретных версиях):

```
<Linux user home directory >/logs
```

Для поддержки требований PA-DSS, в конфигурации Lifestyle Banking создан идентификатор ([play.id](#)) со значением "padss" ([play.id](#) является атрибутом Play Framework и позволяет создать специфические настройки для разных вариантов запуска Lifestyle Banking).

При помощи этого идентификатора в конфигурационном файле "application.conf" задаются параметры приложения, используемые, в том числе, для работы в режиме промышленной

системы. Например, ip-адрес интеграционного шлюза (в стандартной конфигурации - WAY4 Gate), соответствующего требованиям PA-DSS.

Для обеспечения работы в режиме промышленной системы также должна быть установлена соответствующая настройка:

```
%padss.application.mode=prod
```

1.2.2 Web Banking/Mobile Web Banking

Предыдущие версии Web Banking/Mobile Web Banking могут содержать чистый текст PAN в журналах сообщений, поэтому все файлы журналов из предыдущих версий должны быть надежно удалены.

Файлы журналов сообщений хранятся в папках (некоторые из них могут не существовать в конкретных версиях):

```
<Customer Profile webapp>/WEB-INF/runtime/log  
<Web Banking webapp>/WEB-INF/runtime/log  
<Mobile Web Banking webapp>/WEB-INF/runtime/log  
<Frontend Web Banking webapp>/WEB-INF/runtime/log  
<Backend Web Banking webapp>/WEB-INF/runtime/log
```

Вывод отладочной информации должен быть выключен (в файле ows-application.properties параметр debug_enabled должен иметь значение false).

1.3 Обработка конфиденциальных данных

Если конфиденциальные данные должны появляться в журналах, в отладочных файлах, в базе данных или где-либо еще вследствие необходимости решения проблем или отладки, должны соблюдаться следующие требования к их обработке:

1. Конфиденциальные данные должны собираться исключительно в случаях возникновения проблем, решение которых без сбора этих данных невозможно.
2. Конфиденциальные данные должны собираться исключительно в специально отведенных для этого хранилищах, имеющих ограничения по доступу к ним.
3. Конфиденциальные данные могут собираться только в строго ограниченных количествах, позволяющих решать проблемы, описанные в п. 1.
4. Конфиденциальные данные должны быть зашифрованы при хранении, то есть для их хранения необходимо использовать безопасное хранилище, не связанное с регистрационной записью и паролем пользователя операционной системы (см. документ Управление ключами в системе WAY4™™).
5. Конфиденциальные данные должны быть безопасно и полностью удалены сразу после их использования. Для удаления данных рекомендуется использовать утилиту BCWipe последней версии.

2 Хранение данных карт (Cardholder Data) и криптографических ключей

Данная глава посвящена удовлетворению требований п.п. 2.1. – 2.6 стандарта PA-DSS, приведенных ниже.

| PA-DSS Requirement | PA-DSS Topic |
|--------------------|---|
| 2.1 | Securely delete cardholder data after customer-defined retention period. |
| 2.2 | Mask PAN when displayed so only personnel with a business need can see more than the first six/last four digits of the PAN. |
| 2.3 | Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs). |
| 2.4 | Protect keys used to secure cardholder data against disclosure and misuse. |
| 2.5 | Implement key management processes and procedures for cryptographic keys used for encryption of cardholder data. |
| 2.5.1 - 2.5.7 | Implement secure key management functions. |
| 2.6 | Provide a mechanism to render irretrievable cryptographic key material or cryptograms stored by the payment application. |

2.1 Требования к управлению ключами

Требования по работе с ключами шифрования, относящиеся к шифрованию данных держателей карт:

- Ограничение доступа к ключам и ключевым компонентам до минимально необходимого для хранения данных (в соответствии с требованием PA DSS 2.4).
- Надежное хранение ключей и ключевые компоненты в как можно меньшем числе мест и форм (в соответствии с требованием PA DSS 2.4).
- Внедрение процессов и процедур управления ключами для криптографических ключей, используемых для шифрования данных держателей карт (в соответствии с требованием PA DSS 2.5).

- Формирование криптографических ключей с использованием сильных алгоритмов шифрования (в соответствии с требованиями PA DSS 2.5.1). Ознакомьтесь с рекомендациями стандарта FIPS 140-2 для сильных алгоритмов шифрования и правильных длин криптографических ключей.
- Безопасное распространение криптографических ключей (требование PA 2.5 DSS). Распространение криптографических ключей не должно требоваться при нормальной обработке.
- Безопасное хранение криптографических ключей (требование PA DSS 2.5.3). Рекомендуемая опция для хранения главного ключа находится внутри HSM. Рабочие клавиши, зашифрованные главным ключом, могут храниться вне HSM. Также допустимо хранение основного ключа внутри Oracle Key Vault (подробнее см. документацию Oracle Database).
- Безопасная смена криптографических ключей (в соответствии с требованием PA DSS 2.5.4). Пожалуйста, ознакомьтесь с текстом ниже, чтобы узнать подробности о требовании.
- Безопасное удаление в связи с окончанием срока действия криптографических ключей (в соответствии с требованием PA DSS 2.5.5). Пожалуйста, ознакомьтесь с текстом ниже, чтобы узнать подробности о требовании.
- Управление криптографическим ключом с двумя контрольными функциями (в соответствии с требованием PA DSS 2.5.6). Пароль доступа для главного ключа либо для токена PKCS #11 HSM, либо для Oracle Key Vault должен быть защищен паролем с использованием двух компонентов-паролей, известных, по меньшей мере, двум различным хранителям ключей, соответственно.
- Предотвращение несанкционированной замены криптографических ключей (в соответствии с требованием PA DSS 2.5.7). Каждая процедура управления ключами должна выполняться с использованием отдельного знания пароля хранения основного ключа и под двойным контролем и должна быть зарегистрирована в журнале управления ключами. Подробнее см. "Управление ключами в WAY4™".
- Используйте механизм для формирования безвозвратного криптографического ключевого материала или криптограмм, хранящихся в платежном приложении (в соответствии с требованием PA DSS 2.6). Стандартная операция Resetting или Rotating TDE (RE-KEY) поддерживается для ключей, хранящихся в хранилище HSM (из базы данных Oracle 11gR1) или в Oracle Key Vault. Этот процесс деактивирует предыдущий ключ шифрования TDE, создает новый ключ шифрования TDE, а затем активирует его. Старый ключ может быть сохранен, чтобы расшифровать ранее зашифрованные данные. Это относится к ключевым ключам TDE и таблице (столбцам) - они могут быть изменены независимо. Ключи табличного пространства нельзя переустановить, но можно переместить их в новое зашифрованное табличное пространство (подробнее см. документацию Oracle Database). Обратите внимание, что ротация колонок и ключей табличных пространств может быть сопряжено со значительным накладным расходам.

Для проведения процедур управления ключами необходимо пользоваться документом "Управление ключами в системе WAY4™".

Для получения информации о способах удовлетворения указанных требований следует обратиться к документу "Управление криптографическими ключами в системе WAY4™".

Следование основным принципам и процедурам, описанным в указанном документе, является необходимым условием для обеспечения совместимости системы WAY4 со стандартами PCI DSS.

Любой сотрудник, выступающий в роли держателя ключа, должен полностью понимать и принимать свою ответственность, что должно быть документально подтверждено: каждый держатель ключа должен заполнять и подписывать специальную форму каждый раз для каждого ключа шифрования, информация о котором становится ему известна. Пример формы держателя ключа приводится в документе "Управление криптографическими ключами в системе WAY4™".

Каждый сформированный ключ шифрования должен быть криптоустойчив. Необходимая длина ключа в соответствии с требованиями стандартов индустрии безопасности и передовых практических методов, например, для симметричного алгоритма 3DES составляет минимум 168 непредсказуемых битов, для алгоритма AES составляет минимум 128 непредсказуемых битов, для асимметричного алгоритма RSA – по меньшей мере 2048 непредсказуемых бита.

Все ключи шифрования должны храниться и распространяться только безопасным способом. За дополнительной информацией следует обращаться к документу "Управление криптографическими ключами в системе WAY4™".

Ключи шифрования должны периодически заменяться после окончания заданного срока действия. Срок действия зависит, в частности, от следующих факторов:

- Эффективная длина ключа;
- Сколько раз использовался ключ;
- Тип алгоритма шифрования;
- Максимальный заданный период времени.

Подробная информация, касающаяся периода действия ключей шифрования для различных случаев, может быть получена из действующих стандартов индустрии безопасности и передовых практических методов, например, NIST Special Publication 800-57.

Ключ шифрования должен быть немедленно аннулирован и заменен при выполнении любого из следующих условий:

- Целостность ключа нарушена;
- Ключ скомпрометирован или предположительно скомпрометирован;
- Срок действия ключа истек.

За дополнительной информацией об аннулировании и замене ключей следует обратиться к документу "Управление криптографическими ключами в системе WAY4™".

Следование рекомендациям по управлению ключами является необходимым условием для обеспечения совместимости системы со стандартами PCI DSS.

2.2 Срок хранения данных карт (Data Retention)

Срок хранения неиспользуемых данных карт не может превышать соответствующий срок, устанавливаемый пользователем системы WAY4. Данные, срок хранения которых истек, должны удаляться из системы. Выполнение данного требования абсолютно необходимо для обеспечения совместимости со стандартами PCI DSS.

В системе WAY4 данные, подлежащие обязательному удалению с точки зрения стандарта PCI DSS по истечении срока хранения, находятся в следующих таблицах:

- ACC_LVL
- ACNT_CONTRACT
- APPL_ACNT
- APPL_AUTH_SCH
- APPL_AUTH_VAL
- APPL_BATCH
- APPL_CARD_INFO
- APPL_CONTRACT
- APPL_INFO
- APPL_LOG
- APPL_PAYM_REC
- APPL_PAYM_REC_PARTY
- APPL_PM_KEYS
- APPL_STANDING_ORDER
- BP_PROCESS
- CARD_INFO
- CARD_STOP_LIST_EXT
- COMS_LOG
- DOC
- DOC_MAILBOX
- INVOICE_PARTY
- LOG_FIELDS
- MAILBOX
- M_TRANSACTION
- ORIGINAL_DOC
- PM_KEYS
- REMOTE_FILE_REQ
- SAFE_DOC
- STANDING_ORDER
- TD_AUTH_VAL
- TD_CONS_DOC
- TD_DOC
- TELEX_AUTH
- TPPS_CARD
- USAGE_HISTORY
- UT_ADDENDUM_DOC
- VOICE_AUTH



В соответствии с требованиями стандарта PCI DSS поля CARD_INFO.PVV и CARD_INFO.PIN можно хранить в базе данных эмитента.

Любые исторические данные, сохраняемые в БД, в том числе вышеуказанные, автоматически удаляются из системы с помощью процедур Housekeeping.

Настройка и запуск процедур автоматического удаления данных, с истекшим сроком хранения описан в документе "Housekeeping в системе WAY4™".

Запуск процедур Housekeeping должен осуществляться не реже одного раза в квартал.

Хранение архивных данных Housekeeping должно осуществляться в зашифрованном виде в безопасном хранилище (см. документ "Управление ключами в системе WAY4™").

Система WAY4 обрабатывает клиринговые и диспутные файлы, а также файлы расчетов. Эти файлы, содержащие данные держателей карт, должны быть удалены сразу после обработки. Удаление файлов должно выполняться безопасным образом, т.е. после удаления данные не должны быть пригодны к восстановлению даже если они хранились на RAM-диске или безопасном хранилище, поскольку данные держателей карт не должны сохраняться, если они не используются. Удаление клиринговых, диспутных файлов, а также файлов расчетов абсолютно необходимо для обеспечения совместимости системы со стандартами PCI DSS. Точное размещение файлов определяется настройками соответствующих пунктов меню.



HCE Data Retention. В Host Card Emulation, данные, которые в соответствии с PCI DSS должны быть удалены, когда его срок хранения истечет, автоматически удаляются с помощью процедуры Housekeeping. Чтобы указать период хранения, используйте параметр "endOfLifeGraceDay" из конфигурационного файла "hce.json".

2.3 Требования к хранению данных

Поскольку информация о держателе карты хранится в БД, необходимо обеспечить шифрование критически важных с точки зрения безопасности данных (Sensitive Authentication Data / Cardholder Data). Для этого следует использовать технологию Oracle Advanced Security Transparent Data Encryption (TDE), а также следовать другим требованиям, приведенным в разделе "Protect Cardholder Data" документа "Oracle Database Security and the Payment Card Industry Data Security Standard". Выполнение данных требований абсолютно необходимо для обеспечения совместимости системы со стандартами PCI DSS.

Следует иметь в виду, что использование TDE предъявляет дополнительные аппаратные требования к серверу БД.

При настройке TDE необходимо определить следующие положения:

- где будет находиться хранилище мастер-ключа: на внешнем диске, на внутреннем диске или на специальном устройстве безопасности;
- как ограничить права доступа к хранилищу и предотвратить кражу ключа;
- как организовать безопасное резервное копирование хранилища; необходимо учесть, что недопустимо держать хранилище ключа или его копию вместе с резервным хранилищем базы данных.

Технологию TDE используется для шифрования табличных пространств.

При отсутствии опции Oracle Partitioning (например, в Oracle Database Standard Edition) для хранения файлов данных необходимо использовать зашифрованные дисковые разделы, см. раздел "[Шифрование дисковых разделов](#)".

2.3.1 Зашифрованные табличных пространств

Для использования зашифрованных табличных пространств необходимо указать разметку табличных пространств с суффиксом _E (encrypted, например, OWLARGE_E_D) так, чтобы они указывали на заранее созданные администратором табличные пространства Oracle, которые зашифрованы. Для создания разметки нужно скопировать существующий разметку для всех табличных пространств, кроме OWTEMP, добавив суффикс _E к каждой строке:

```
# early present lines
OWLARGE_D=LARGE_D
OWLARGE_I=LARGE_I
# mapping added for Tablespace Encryption
OWLARGE_D=LARGE_D
OWLARGE_I=LARGE_I
OWLARGE_E_D=LARGE_ENC_D
OWLARGE_E_I=LARGE_ENC_I
```

Если параметры DB.INI были указаны перед установкой системы, то данные уже будут зашифрованы. В противном случае для шифрования необходимо воспользоваться инструментом Online Table Migration Tool, описанным в документе "Redefinition Tool".

2.3.2 Настройка сценариев при использовании TDE

Следующая схема работы рекомендуется при использовании TDE (Transparent Data Encryption):

- Для шифрования, рекомендуется использовать отдельный "Encryption Wallet" без функции "автоматического входа в систему". Это повышает безопасность, так как, чтобы открыть "Wallet", дополнительный пароль должен быть введен каждый раз при запуске базы данных.
- Для хранения (скрытия) имен пользователей и паролей, может использоваться другой "Wallet" с функцией "auto-login" (т.к. скрипты выполняются только под пользователем Oracle).

"Wallet" должны быть созданы следующим образом:

- Сделайте все необходимые настройки для шифрования. Это включает в себя создание "Wallet" для шифрования (Encryption "Wallet" создается автоматически во время выполнения выражения SQL "alter system set encryption key identified by <wallet_password>"). Рекомендуется проверить параметры шифрования на тестовой системе (желательно с повторным запуском базы данных).
- Создать "Wallet" для хранения паролей сценариев. "Auto-login Wallet" создается вручную с помощью программы mkstore. "Auto-login Wallet" создается после того, как все настройки шифрования были выполнены (и проверены).

Описанная процедура позволяет избежать ситуаций, когда Oracle добавляет шифрование "Auto-login Wallet", предназначенный для хранения паролей сценариев.

Убедитесь в том, что привилегии для каталогов и для файлов, созданных в этих каталогах в процессе создания "Wallet" были предоставлены соответствующим пользователям операционной системы (Oracle в Linux, SYSTEM в Windows). В ряде случаев, привилегии для cwallet.sso и ewallet.p12 файлов для "Wallet" с "Auto-login Wallet" должны быть созданы вручную для SYSTEM.

2.3.3 Housekeeping и TDE

Если для таблиц WAY4 используется шифрование на уровне таблиц, то HSK должен быть настроен для шифрования архивных табличных пространств.

Если используется автоматическое создание табличных пространств, HSK параметры должны быть установлены в Housekeeping → Configuration → Tablespace Group → Tablespace Parameters:

- для Oracle 12c:

```
DATAFILE '...' SIZE ...  
ENCRYPTION USING 'ENCRYPTION_ALGORITHM'  
DEFAULT STORAGE(ENCRYPT)
```

- для Oracle 18c, Oracle 19c:

```
DATAFILE '...' SIZE ... ENCRYPTION USING 'ENCRYPTION_ALGORITHM' ENCRYPT
```

где, ENCRYPTION_ALGORITHM – AES128. Другие алгоритмы также поддерживаются (AES256, AES192, 3DES168).

Если HSK использует созданные вручную табличные пространства, администратору базы данных необходимо создать эти табличные пространства вручную:

- для Oracle 12c:

```
ENCRYPTION USING 'ENCRYPTION_ALGORITHM'  
DEFAULT STORAGE(ENCRYPT)
```

- для Oracle 18c, Oracle 19c:

```
ENCRYPTION USING 'ENCRYPTION_ALGORITHM' ENCRYPT
```

Параметры указать в Housekeeping → Configuration → Tablespace Group → Tablespace Parameters → Tablespace Mask.

2.3.4 Шифрование дисковых разделов

Шифрование дисковых разделов выполняется специальными утилитами. Ниже приведен пример шифрования дисковых разделов, используемых для хранения файлов данных табличных пространств WAY4, при помощи утилиты cryptsetup в ОС Linux:

- Создание зашифрованного раздела:

```
cryptsetup -v luksFormat /dev/sdc1
```

- Открытие зашифрованного раздела и назначение псевдонима:

```
cryptsetup luksOpen /dev/sdc1 sdc1e
```

- Конфигурация Oracle ASM:
- Group Name – DATAE.
- Disk – /dev/mapper/sdc1e.
- Redundancy = External.
- Файлы данных табличных пространств WAY4 создаются в группе Oracle ASM – DATAE.

2.4 Требования к хранилищу данных

Необходимо регулярно выполнять архивирование файлов обмена, их хранение должно осуществляться в зашифрованном виде.

Необходимо регулярно выполнять архивирование формируемых в системе отчетов, их хранение должно осуществляться в зашифрованном виде.

Данные, полученные в процессе обнаружения причин неисправностей в работе системы, должны гарантировано удаляться непосредственно после выполнения требуемых процедур.

Подкачка в системах, работающих под управлением Java-компонентов обработки CHD должны быть отключена или для подкачки должен использоваться зашифрованный диск.



Требования к хранилищу данных HCE. Host Card Emulation не имеет DB Server, но содержит персистентные данные на зашифрованном диске каждого узла (см. раздел "Preparing Protected Disk Space" документа "WAY4™ Host Card Emulation Installation and Setup").

2.5 Требования к серверу базы данных

В случае необходимости выполнить трассировку запросов к СУБД Oracle надлежит выполнять ее без сохранения значений Bind-переменных. Использование трассировки с сохранением значений Bind-переменных может осуществляться только на тестовой системе. Выполнение данного требования абсолютно необходимо для обеспечения совместимости системы со стандартами PCI DSS.

Требования выполняются согласно документу "Oracle Database Security and the Payment Card Industry Data Security Standard".

2.6 Требования к рабочим станциям пользователей

Трассировка на рабочих станциях должна быть выключена.

2.7 Строго определенные механизмы доступа к PAN



В соответствии с требованием PA-DSS, PAN по умолчанию отсекается на всех экранах.




Однако доступ к PAN может предоставляться персоналу с соответствующей бизнес-компетенцией. Чтобы обеспечить постоянное и четкое протоколирование доступа к данным держателей карт, такой доступ предоставляется с помощью кнопки [Get Card Number] (и однотипной). Ниже приведен список всех экранных форм, с данным типом кнопки:


- экранные формы "Case lists" и "Case details" (кнопки [Show Contract Number] или [Show Card Number]) на следующих рабочих местах: "Dispute Management Workbench", "Issuing (Acquiring) Risk Monitoring", "Claim Management Workbench", "Risk Management Workbench", "Stop List", "Issuing (Acquiring) Risk Monitoring", "Issuing Risk Management Expert Tools", "Issuing (Acquiring) Application Management", "Supervisor Application Management", "Customer Service Workbench" и "Merchant Service Workbench");
- экранные формы со сведениями о документах и их свойствах (кнопки [Show Card Number] или [Get Card Number], или [Show Source Contract Number], или [Show Target Contract Number]) на следующих рабочих местах: "Documents", "Document Administration", "Document Management Workbench", "Customer Service Workbench", "Merchant Service Workbench", "Issuing (Acquiring) Risk Monitoring", "Issuing Risk Management Expert Tools", "Dispute Management Workbench" и "Reversal Management Workbench";
- экранные формы "Contract lists" и "Card contract details" (кнопка [Get Card Number]) на следующих рабочих местах: "Customer Service Workbench" и "Collection Management Workbench".

2.8 Поддержка требований стандарта PCI DSS продуктами и компонентами WAY4

В приведенной ниже таблице содержится информация по поддержке требований по хранению и протоколированию критической с точки зрения безопасности информации продуктами и компонентами WAY4.

| Наименование продукта или компонента | Выполнение требований |
|---|---|
| Datamart | PAN хранится усеченным с 7 от начала и до 4-го с конца знака в базе данных Datamart, поэтому получить полный текст Sensitive Authentication Data / Cardholder Data из Datamart невозможно. |
| WAY4U SMS Banking | <p>Sensitive Authentication Data / Cardholder Data отсекаются в журналах.</p> <p>Усечение данных включено по умолчанию с помощью параметра <code>log_filtering_enabled=yes</code> файла "WEB-INF/config/work/ows-application.properties".</p> <div>  <p>Отключение указанного параметра приводит к потере совместимости с требованиями стандарта PCI DSS.</p> </div> |
| WAY4 manager | <p>PAN всегда усекается во всех формах "только для чтения" и формах редактирования, используемых в режиме "View". Если какая-то форма позволяет редактировать PAN, PAN отсекается в момент установки фокуса на поле. Меню, доступное для определенного сотрудника, должно быть настроено в соответствии с бизнес-потребностями офицера.</p> <p>При записи в журнал усекаются все последовательности цифр длиной более 6 знаков.</p> |
| Remote access | При записи в журнал усекаются все последовательности цифр длиной более 6 знаков. |
| eCommerce issuing, eCommerce acquiring, Bill payments | Данные всегда усекаются в журналах. Сохранение полных данных в журналах невозможно. |
| Clearing Files | <p>Требуется использовать для хранения файлов RAM-диск или шифрование в безопасном хранилище (см раздел "Управление ключами в безопасном хранилище" документа "Управление ключами в системе WAY4™"). Загруженные в систему или отправленные получателю файлы должны немедленно удаляться с диска.</p> <div>  <p>Выполнение данных требований абсолютно необходимо для обеспечения совместимости системы со стандартами PCI DSS.</p> </div> |

| Наименование продукта или компонента | Выполнение требований |
|--------------------------------------|--|
| Application Server | Sensitive Authentication Data / Cardholder Data не хранятся и не записываются в журнал. |
| Payment Server | Sensitive Authentication Data / Cardholder Data не хранятся и не записываются в журнал. |
| Reporting | <p>Sensitive Authentication Data / Cardholder Data усекаются в журналах. По умолчанию режим формирования отчета с трассировкой отключен.</p> <div>  Включение указанного режима приводит к потере совместимости с требованиями стандарта PCI DSS. </div> |
| File Exchange Engine (pipes) | <p>Sensitive Authentication Data / Cardholder Data отсекаются в журналах. При хранении требуется дисковое шифрование. Java-пайпы сохраняют информацию в стандартном журнале WAY4 Manager, поэтому невозможно существование журнала с немаскированными данными для Java-пайпов.</p> <p>С-пайпы: для отключения усечения данных может использоваться параметр пайпа "NOMASK_TRACE_START".</p> <div>  Включение указанного режима приводит к потере совместимости с требованиями стандарта PCI DSS. </div> <p>Для усечения PAN в пайпе "RBS. Analytic Transfers Export.dll" параметр MASK_CARD_NUMBER должен иметь значение "Y".</p> |
| WAY4 Web | <p>Усечение сохраняемых данных (Sensitive Authentication Data / Cardholder Data) включено по умолчанию. В целях отладки возможность усечения номеров карт в логах может быть временно отключена на 15 минут в запущенном экземпляре сервера консольной командой "<WS_Runtime_Path>/WEBINF/commands/Logging/Filter/suspendMaskingMode".</p> <div>  Включение указанного режима приводит к потере совместимости с требованиями стандарта PCI DSS. </div> |

| Наименование продукта или компонента | Выполнение требований |
|--------------------------------------|--|
| Transaction Switch | <p>Усечение сохраняемых данных (Sensitive Authentication Data / Cardholder Data) включено по умолчанию.</p> <p>В целях отладки уровень логирования может быть увеличен командой AllowUnsafeLogLevel. При этом соответствующий уровень логирования устанавливается на 10-минутный интервал.</p> <div>  <p>Пользоваться командой AllowUnsafeLogLevel рекомендуется только в целях тестирования. Использование команды AllowUnsafeLogLevel в промышленном режиме не соответствует требованиям PA-DSS.</p> </div> |
| NetServer | Sensitive Authentication Data / Cardholder Data усекаются в журналах. |
| Access server | Sensitive Authentication Data / Cardholder Data усекаются в журналах. |
| NetServer Console | Sensitive Authentication Data / Cardholder Data усекаются в журналах. |
| Web Banking/Mobile Web Banking | Sensitive Authentication Data / Cardholder Data усекаются в журналах. |
| Lifestyle Banking | Sensitive Authentication Data / Cardholder Data усекаются в журналах. |
| Host Card Emulation (HCE) | Sensitive Authentication Data / Cardholder Data усекаются в журналах. |
| Authentication Server and Data Gate | Входящие подключения к AuthServer используют TLS 1.2 подключения AuthServer к Data Gate используют интерфейс Secure ISO. Эти опции включены по умолчанию после установки. Если параметр изменяется, совместимость PCI DSS будет потеряна. |

3 Регистрация пользователей и установка паролей

Данная глава посвящена удовлетворению требований п.п. 3.1 - 3.2 стандарта PA-DSS, приведенных ниже.

| PA-DSS Requirement | PA-DSS Topic |
|--------------------|--|
| 3.1 | Use unique user IDs and secure authentication for administrative access and access to cardholder data. |
| 3.2 | Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications. |

3.1 Учетные записи администраторов, создаваемые по умолчанию

Доступ к платежному приложению не может осуществляться при помощи административных учетных записей, создаваемых по умолчанию при установке, например, не должны использоваться административные учетные записи (такие как "sys") для доступа к данным.

Всем учетным записям администраторов, созданные по умолчанию, должны быть назначены безопасные политики аутентификации (даже если учетные записи не используются), и после этого все неиспользуемые учетные записи администраторов должны быть деактивированы.

Везде, где это возможно, учетным записям пользователей должны назначаться безопасные политики аутентификации. Это касается как платежного приложения, так и окружения, в котором оно работает (ОС, серверы и т. д.).

3.1.1 NetServer

Настройка учетных записей администратора и пользователя является обязательным этапом установки платежного приложения. Эта процедура описана в документе "Установка и Конфигурирование NetServer Java Secure Console".

3.1.2 Transaction Switch

WAY4-приложение Transaction Switch устанавливается на платформу WAY4 Application Server и управляется web-консолью. О настройке работы с пользователями web-консоли см. раздел "Управление WAY4-приложениями" документа "Администрирование WAY4™ Application Server".

3.2 Принципы безопасной аутентификации

Данный раздел посвящен удовлетворению требований стандарта PA-DSS 3.1.1. – 3.1.11.

Для соответствия указанным требованиям аутентификация пользователей для доступа к платежному приложению, включая доступ ко всем рабочим станциям, серверам и базам данных, должна соответствовать следующим рекомендациям:

1. Запрещено использовать разделяемые идентификаторы доступа (учетные записи и пароли), в том числе в административных целях. Каждому пользователю должно быть выдано уникальное значение в качестве пароля, используемого при первичной регистрации в системе (first-time password). Необходимо также использовать заданную по умолчанию функциональность системы, принудительно требующую смены пароля при его использовании в первый раз.
2. Пароли пользователей удовлетворяют следующим требованиям:
 - A. пароли пользователя должны изменяться минимум раз в 90 дней (password life time);
 - B. длина пароля не менее 7-ми символов;
 - C. обязательное использование в пароле букв и цифр;
 - D. повторная регистрация того же самого пароля возможна только через 4 замены (password reuse max);
 - E. установлено ограничение (не более 6-ти раз) для числа попыток ввода неправильного пароля; при превышении должна блокироваться возможность доступа в систему для данной учетной записи как минимум в течение 30-ти минут или до тех пор, пока администратор не разблокирует возможность доступа (password lock time).
3. Автоматическая блокировка клиентских приложений должна выполняться не позже, чем через 15 минут простоя.

Необходимо использовать функциональность блокирования неиспользуемых учетных записей (см. раздел "Блокирование неиспользуемых учетных записей" документа "Администрирование пользователей в системе WAY4™"). Блокирование неиспользуемых учетных записей необходимо для обеспечения совместимости со стандартом PCI DSS.

СУБД Oracle позволяет выполнять проверку предъявляемых к паролям требований с помощью функций стандартного SQL-скрипта. Указанный скрипт должен использоваться для обеспечения совместимости настройки паролей со стандартом PA-DSS. Описание правил использования функций см. в документации Oracle "Oracle® Database Security Guide" в разделах "Authentication Methods" и "Password Complexity Verification".

Необходимо настроить выполнение автоматической проверки качества паролей при их формировании с помощью функции "PASSWORD_VERIFY_FUNCTION" СУБД Oracle.

"PASSWORD_VERIFY_FUNCTION" позволяет задать PL/SQL функцию проверки сложности пароля сложность в качестве аргумента CREATE PROFILE.

Пример изменения профиля по умолчанию:

```
ALTER PROFILE "DEFAULT" LIMIT
  PASSWORD_LIFE_TIME 90  <-- Renewal of password every 90 days
  PASSWORD_GRACE_TIME 10  <-- Give the user 10 days' grace period
  PASSWORD_REUSE_MAX 5  <-- Ensure at least 5 different passwords before reusing a
password
  FAILED_LOGIN_ATTEMPTS 6  <-- Allow 6 attempts to login
  PASSWORD_LOCK_TIME .0208 <-- After 5 unsuccessful login attempts, lock account for
30 min, then allow new attempts
  PASSWORD_VERIFY_FUNCTION ora12c_verify_function; <-- enforce password complexity as
desired
```

Где "PASSWORD_VERIFY_FUNCTION" - "ora12c_verify_function" (<ORACLE_HOME> /rdbms/admin/utlpwmg.sql). Для Oracle 12c существуют четыре функции: "ora12c_verify_function" и "ora12c_strong_verify_function" и две вспомогательные функции "complexity_check" и "string_distance".

Следует предъявлять повышенные требования к качеству (сложности) паролей для учетных записей пользователей, обладающих правами администратора СУБД.

Поскольку учетная запись пользователя-владельца схемы БД системы WAY4 используется только при установке системы и установке обновлений, требуется, чтобы в остальное время данная учетная запись была заблокирована.

Модификация установок безопасности, относящихся к уникальным пользовательским учетным записям, а также ослабление политики аутентификации по сравнению с рекомендуемыми ведет к нарушению требований стандарта PCI DSS.

3.2.1 NetServer

Java Secure Console поддерживает две различные роли пользователей: "Active" и "Passive". Роль "Active" дает пользователю возможность управлять платежным приложением. Роль "Passive" только обеспечивает возможность осуществлять мониторинг статуса приложения. По истечении заданного времени ожидания (значение по умолчанию 10 минут), происходит переключение режима работы консоли с ролью пользователя "Active" на режим работы с ролью "Passive".

Пароль учетной записи администратора должен соответствовать следующим требованиям:

- Длина пароля не менее 7-ми символов.
- Пароль содержит буквы и цифры.
- Пароль не должен совпадать с последними четырьмя использовавшимися паролями.
- Число попыток ввода пароля не превышает 6-ти.

3.2.2 WAY4 Web

Для пользователей WAY4 Web существует возможность задать требования к паролю с помощью параметров типа аутентификации. Для этого необходимо выполнить следующие действия в WAY4 Web:

- в окне "Authentication Configuration" на вкладке "Schemes" выбрать схему с кодом "W4W_PWA";
- нажать на кнопку [Edit], в открывшемся окне нажать на кнопку [NEXT STEP];
- в открывшемся окне нажать на кнопку [Create] и добавить соответствующий параметр:
- в поле *Name* задать произвольное наименование параметра;
- в поле *Code* задать один из поддерживаемых параметров (см. ниже);
- в поле *Default Value* задать значение параметра;
- в поле *Global* задать значение "Yes";
- в поле *Type* задать тип параметра;
- в поле *Mandatory* задать значение "Yes".

Поддерживаемые параметры для задания сложности пароля:

- WS_PWD_MIN_LENGTH – минимальная длина пароля (число);
- WS_PWD_MAX_LENGTH – максимальная длина пароля (число);
- WS_PWD_CONTAINS_UPPER – пароль должен содержать букву в верхнем регистре (значение – Y|N);
- WS_PWD_CONTAINS_LOWER – пароль должен содержать букву в нижнем регистре (значение – Y|N);
- WS_PWD_CONTAINS_DIGIT – пароль должен содержать цифру (значение – Y|N);
- WS_PWD_CONTAINS_SYMB – пароль должен содержать символ (не букву, цифру или пробел). Значение – Y|N.
- WS_PWD_NO_RESERVED – пароль не должен содержать специальные символы (пробел /!*"()&+=\$,?#/[]). Значение – Y|N.

3.2.3 Messenger banking

Продолжительность пользовательского сеанса задается параметром `session_expiry_sec` (файл `ows-application.properties`) и не должна превышать 300 секунд.

3.2.4 Transaction Switch

О настройке работы с пользователями web-консоли, с помощью которой выполняется управление приложением Transaction Switch, см. раздел "Управление WAY4-приложениями" документа "Администрирование WAY4™ Application Server".

3.2.5 Web Banking/Mobile Web Banking

Следующие файлы содержащие параметры доступа к БД WAY4 должны быть зашифрованы с помощью утилиты `nscipher` (см. раздел "[Шифрование конфигурационных параметров](#)"):

```
<Customer Profile webapp>/WEB-INF/config/work/ows-application.properties
<Web Banking webapp>/WEB-INF/config/work/w4c.properties
<Mobile Web Banking webapp>/WEB-INF/config/work/w4c.properties
<Messenger Banking webapp>/WEB-INF/config/work/ows-application.properties
```

3.2.6 Шифрование конфигурационных параметров

Некоторые параметры в файлах конфигурации должны быть зашифрованы, о чем сообщается, в комментариях к параметру. Например,

```
password="encrypted:specify password encrypted by nscipher.exe"
```

Параметр "password" с заданным зашифрованным значением, может выглядеть следующим образом:

```
password="encrypted:5CD2466B4D8D25ED0B05DBBFFFC8A81B4D5A640A7D356"
```

Значение после "encrypted:" является зашифрованным значением.

Для получения зашифрованного значения следует воспользоваться утилитой ns_cipher. Утилита входит в состав дистрибутива WAY4 Application Server:

```
<APP_SERVER>/appserver/bin/tools/nscipher.exe
```

Утилита запускается из командной строки. Формат команды:

```
nscipher.exe ows_application > <путь к файлу (полный, или относительный), в который  
будет записан зашифрованный пароль>
```

Например,

```
nscipher.exe ows_application > c:/pass.txt  
nscipher.exe ows_application > ./out/pass.txt
```

После запуска утилита запросит пароль, создаст его зашифрованное значение и сохранит его в виде строки в файл "pass.txt" (значение, указанное в командной строке). Путь указанный, в командной строке должен существовать, если путь не существует – утилитой будет возвращена ошибка: "The system cannot find the path specified".

3.3 Шифрование пароля к СУБД Oracle

Для шифрования пароля к СУБД недопустимо использовать небезопасные алгоритмы.

Пример сильных криптографических алгоритмов: PBKDF2, Bcrypt, Blowfish, SHA256+.

3.3.1 Как определить алгоритм шифрования паролей

В рамках данной процедуры, алгоритм шифрования MD5 (или SHA256, SHA512) используется по умолчанию в BSD-Linux в случае, когда пользователь изменяет свой пароль. Алгоритм подходит

для тех случаев, когда в сети присутствуют разнородные версии операционных систем UNIX: Solaris, BSD и Linux.

Получить права супер-пользователя или эквивалентные.

Задайте идентификатор алгоритма шифрования в качестве значения переменной CRYPT_DEFAULT (/etc/security/policy.conf).

Для документирования изменений используйте комментарии в конфигурационном файле.

```
# vi /etc/security/policy.conf
...
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6
#1 = crypt_bsdmd5
#2a = crypt_bsdbf
#md5 = crypt_md5
#5 = crypt_sha256
#6 = crypt_sha512
#__unix__ = crypt_unix
#
# Use the version of MD5 that works with Linux and BSD systems.
# Passwords previously encrypted with __unix__ will be encrypted with MD5
# when users change their passwords.
#
#CRYPT_DEFAULT=__unix__
CRYPT_DEFAULT=1
```

В данном примере конфигурация гарантирует, что слабый алгоритм модуля "crypt_unix" никогда не используется для шифрования пароля. Пользователи, при смене своих паролей, зашифрованных с помощью модуля "crypt_unix", получают пароль, зашифрованный с помощью модуля "crypt_bsdmd5".

В следующем примере, идентификатор алгоритма шифрования Blowfish - "2a", указан в качестве значения переменной CRYPT_DEFAULT. Фрагмент файла policy.conf:

```
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6
#CRYPT_ALGORITHMS_DEPRECATED=__unix__
CRYPT_DEFAULT=2a
```

Данная конфигурация актуальна для системы BSD, которые используют алгоритм шифрования Blowfish.

3.4 Хранение ключей в Java Keystore

Хранение ключей в Java Keystore безопасно при условиях:

- private-ключи хранятся в Java Keystore, защищенные паролем;
- защита паролем соответствует стандарту PBE (Password-Based Encryption), для этого Java Keystore должен создаваться и наполняться определенным образом.
- пароль сильный.

3.5 Требования для доступа к данным

Настоятельно рекомендуется использовать встроенную в клиентские приложения, поставляемые в комплекте с системой WAY4, функцию шифрования паролей пользователей (см. раздел "Ограничение доступа к данным при использовании шифрования пароля пользователя" документа "Администрирование пользователей в системе WAY4™").

Категорически запрещается использовать приложения сторонних производителей для доступа к данным, содержащимся в БД.

Oracle Database обеспечивает network encryption и strong authentication.

3.6 Требования к серверу базы данных [Регистрация пользователей и установка паролей]

Неиспользуемые учетные записи пользователей СУБД, в том числе служебные, должны быть заблокированы или удалены. Для используемых служебных учетных записей пользователей, в том числе созданных по умолчанию и при установке программного обеспечения, должны быть изменены пароли доступа.

Должны быть также выполнены рекомендации, изложенные в документе "Sustainable Compliance for the Payment Card Industry Data Security Standard".

3.7 Требования к рабочим станциям пользователей [Регистрация пользователей и установка паролей]

Автоматическая блокировка клиентских приложений должна выполняться не позже, чем через 15 минут простоя.

4 Ведение аудитного журнала

Данная глава посвящена удовлетворению требований п.п. 4.1 – 4.4. стандарта PA-DSS, приведенных ниже.

| PA-DSS Requirement | PA-DSS Topic |
|--------------------|-----------------------------------|
| 4.1 | Implement automated audit trails. |
| 4.4 | Facilitate centralized logging. |

В системе WAY4, начиная с версии 03.34.30 автоматически ведется аудитный журнал в соответствии с требованиями PA-DSS. Журнал ведется в таблице SY_AUDIT_LOG. Ведение аудитного журнала является обязательным условием соответствия установленного экземпляра системы WAY4 стандарту PCI DSS. По умолчанию запись в аудитный журнал включена. Для просмотра аудитного журнала используется пункт меню "Full → DB Administrator Utilities → Users & Grants → Audit Log".

В данном журнале сохраняется следующая информация:

- Идентификатор пользователя, дополнительно (если применимо) с указанием сетевого адреса (IP).
- Тип события.
- Дата и время события.
- Индикатор успешности действия.
- Подтверждение, что событие произошло.
- Идентификатор или имя данных, или объекта системы, на которые было произведено воздействие.

При помощи аудитного журнала можно восстановить следующие события:

1. Действия пользователей по доступу к данным карт, т. е.: открытие форм, где есть данные карт, вызов процессов, которые имеют доступ к данным карт.
2. Все действия администраторов, предусмотренные приложением, а также сохраняемые в аудитный журнал Oracle (подробнее см. "[Требования к серверу базы данных](#)").
3. Доступ к аудитному журналу из приложения.
4. Неудачные попытки доступа к данным карт.
5. Все попытки (удачные и неудачные) входа в приложение.
6. Все попытки инициализации аудитного журнала через приложение.
7. Создание и удаление объектов системы (пользователи, формы, процессы, меню, и т. д.) через приложение.
8. Действия пользователя по запуск/остановке приложения и его компонентов.
9. Запрос на доступ к аудитному журналу приложения.

10. Административные действия с аудитным журналом.

Режим использования аудитного журнала должен быть всегда включен, невыполнение этого требования приводит к несоответствию стандарту PCI DSS.

4.1 NetSever

Аудитный журнал NetServer ведется в соответствии с требованиями PA-DSS. Журнал ведется в файле "action.log". Ведение аудитного журнала является обязательным условием соответствия данного экземпляра NetServer стандарту PCI DSS.

Режим использования аудитного журнала должен быть всегда включен; не должно существовать вариантов конфигурации, допускающих выключение указанного режима.

Файлы аудитного журнала не могут быть удалены или изменены с помощью Java Secure Console.

4.2 Transaction Switch

За справками следует обращаться к разделу "Просмотр и анализ log-файлов" главы "Управление WAY4-приложениями" документа "Администрирование WAY4™ Application Server".

4.3 WAY4 Web

В аудитном журнале сохраняется следующая информация:

- Идентификатор пользователя, дополнительно (если применимо) с указанием сетевого адреса (IP).
- Имя выполненного сервиса.
- Дата и время события.
- Индикатор успешности действия.
- Подтверждение, что событие произошло.
- Для сервисов получения доступа к дереву контрактов в Customer Service Workbench, Merchant Service Workbench, Merchant Portal: идентификатор объекта системы (контракта или клиента), к дереву которого был получен доступ.
- Идентификатор сессии, по которой можно восстановить все действия внутри нее.

При помощи аудитного журнала можно восстановить следующие события:

1. Действия пользователей по выполнению сервиса.
2. Попытка просмотра номера карты для отдельного сервиса.
3. Все попытки (удачные и неудачные) входа в приложение, в том числе несуществующим пользователем.

Для включения записи в аудитный журнал информации о попытках входа несуществующим пользователем необходимо в конфигурации Authserver (файл authserv.ini) раскомментировать следующие параметры:


```
[AuthServer]
...
TDDocParams="CLIENT_IP:IP"
TDDocDummyClient=1
...
```

4.4 Поддержка централизованного протоколирования

Для поддержки сторонних систем централизованного протоколирования, а также для автоматического резервирования аудитного журнала в системе WAY4 существует специальный процесс, который при запуске копирует данные аудитного журнала в текстовый файл. Формат файла соответствует RFC 5424 "The Syslog Protocol", поля в файле разделены символами табуляции, что позволяет экспортировать данные аудитного журнала в практически любую стороннюю систему централизованного протоколирования.

Для ограничения доступа к указанным файлам рекомендуется копировать данные аудитного журнала на носитель, например, на файловый сервер, доступ к которому имеют ограниченный список сотрудников, в частности, в этот список не должны входить администраторы СУБД и пользователи WAY4 с административными правами.

Для запуска процесса копирования данных аудитного лога используется пункт меню "Full → DB Administrator Utilities → Users & Grants → Dump Log (более подробная информация приведена в документе "Выгрузка аудитного журнала системы WAY4"). Копирование должно выполняться регулярно, периодичность определяется политиками безопасности клиента. Для автоматизации этого процесса рекомендуется использовать Планировщик.

Для NetServer и Transaction Switch, Lifestyle Banking, Web Banking/Mobile Web Banking требуется создание специального процесса, обеспечивающего централизованное протоколирование и резервное копирование аудитного журнала.

Существуют два варианта централизованного протоколирования:

- [Копирование файлов аудитных журналов с локального компьютера на удаленный.](#)
- [Использование распределенной файловой системы.](#)

В первом варианте система работает при недоступном Log Server. Во втором случае необходимо уточнение возможности записи в файлы аудитных журналов в случае недоступности Log Server.

Файлы аудитных журналов, созданные всеми WAY4 приложениями имеют текстовый формат (поля в файле с разделителями табуляции), что позволяет экспортировать данные аудита в, практически, любую систему централизованной регистрации.

4.4.1 Копирование файлов аудитных журналов с локального компьютера на удаленный

1. Существует компьютер с RHEL для хранения файлов аудитных журналов в Internal Network, далее Log Server.

2. Сконфигурирован SSH доступ по ключу (данный механизм должен быть применен в связи с необходимостью безопасной передачи данных).
3. Log Server устанавливает SSH соединение с Frontend Server (задача CRON с периодичностью – час) и выполняет RSYNC для каталога с файлами аудитных журналов (см. "<http://troy.jdmz.net/rsync/index.html>"). Пример скрипта:

```
# Linux get logs script
#-----
RHOST=server1
RUSER=way4
RPATH=/home/way4/appserver
APPLS="frontend content way4u"
LPATH=/opt/all_logs
#-----
RSYNC=/usr/bin/rsync
SSH=/usr/bin/ssh
#KEY=/home/way4/.ssh/id_rsa
OPTS="-azru -e"
#-----
if [ ! -d $LPATH ]; then
    mkdir -p $LPATH
fi
date
for APPL in $APPLS ; do
    if [ ! -d $LPATH/$APPL ]; then
        mkdir -p $LPATH/$APPL
    fi
    $RSYNC $OPTS $SSH $RUSER@$RHOST:$RPATH/applications/$APPL/logs $LPATH/$APPL
    if [ ! -d $LPATH/$APPL ]; then
        mkdir -p $LPATH/$APPL/runtime
    fi
    $RSYNC $OPTS $SSH $RUSER@$RHOST:$RPATH/applications/$APPL/webapps/$APPL/
runtime/logs $LPATH/$APPL/runtime
done
#$RSYNC $OPTS "$SSH -i $KEY" $RUSER@$RHOST:/logs $LPATH
```

4. Файлы аудитных журналов на Log Server анализируются и очищаются (задача CRON). Файлы аудитных журналов на Frontend Server очищаются автоматически приложением. Пример очистки всех файлов в каталоге "/opt/all_logs" старше 30 дней:

```
# Deletes files in /opt/all_logs older than 30 days
find /opt/all_logs/ -mtime +30|xargs rm -f
```

5. Перезапись файлов журналов в случае превышения из размеров установленного значения не рассматривается, т.к. предыдущий пункт означает, что изменение файлов проблематично или невозможно.
6. Защиту файлов журнала от изменения любого приложения, отличного от WAY4U ("appserver/jdk/current/bin/java"), под определенного пользователя для RHEL, предлагается осуществлять с помощью SELinux (http://www.linuxtopia.org/online_books/rhel6/rhel_6_selinux/, http://www.linuxtopia.org/online_books/rhel6/

[rhel_6_confined_services/rhel_6_services_sect-Managing_Confined_Services-rsync-Booleans.html](#)). В настоящее время, эта инструкция не готова.

4.4.2 Использование распределенной файловой системы

1. Выполнены требования инструкции "<http://www.cyberciti.biz/tips/rhel-centos-mounting-remote-filesystem-using-sshfs.html>". Данный механизм используется в связи с необходимостью обеспечения безопасной передачи данных.
2. Каталоги Frontend Server на удаленном сервере сортированы.
3. Защита и удаление файлов выполнена в соответствии с рекомендациями пп. 3 и 4 раздела "[Копирование файлов аудитных журналов с локального компьютера на удаленный](#)".

4.5 Требования к серверу базы данных [Ведение аудитного журнала]

Аудит ведется средствами операционной системы. Журналы аудита хранятся не менее трех месяцев. Старые журналы выгружаются и хранятся вместе с другими архивными данными.

Средствами СУБД Oracle ведется необходимый аудит, как описано в документе "Аудит работы с базой данных в системе WAY4™". Рекомендуется выполнять аудит доступа к файлам-журналам аудита СУБД Oracle средствами операционной системы.

Следует иметь в виду, что отключение или отказ от использования аудита средствами СУБД Oracle и средствами операционной системы приводит к несоответствию требованиям, предъявляемым к системе стандартом PCI DSS.

4.6 Требования к файловому серверу

Аудит ведется средствами операционной системы. Журналы аудита хранятся не менее трех месяцев. Старые журналы выгружаются и хранятся вместе с другими архивными данными.

4.7 Протоколирование приложений

Компоненты системы WAY4 ведут собственные журналы. Для целей унификации формат журнала для всех компонентов может рассматриваться как простой воспринимаемый человеком текстовый формат, каждая запись журнала отделяется от предыдущей последовательностью CR/LF.

Размещение журналов приведено в следующей таблице:

| Наименование продукта или компонента | Размещение файлов журнала |
|---|---|
| Datamart | Отдельный журнал не используется. |
| WAY4U SMS Banking | Файлы журнала сохраняются в каталоге <webapp>/WEB-INF/runtime/log/. |
| WAY4 manager | Файлы журнала сохраняются в каталоге USER_HOME/.OWS/PROFILE_NAME/log. |
| Remote access | Файлы журнала сохраняются в каталоге USER_HOME/.OWS/PROFILE_NAME/log. |
| eCommerce issuing, eCommerce acquiring, Bill payments | Файлы журнала сохраняются в каталоге "log" приложения. |
| Clearing Files | Отдельный журнал не используется, используется журнал File Exchange Engine. |
| Application Server | Отдельный журнал не используется. |
| Payment Server | Отдельный журнал не используется. |
| Reporting | Отдельный журнал не используется, используется трассировка Oracle Reports. |
| File Exchange Engine (pipes) | <p>Java-пайпы сохраняют информацию в стандартном журнале WAY4 Manager.</p> <p>С-пайпы: путь к файлу журнала задается с помощью параметра пайпа "TRACE".</p> |

| Наименование продукта или компонента | Размещение файлов журнала |
|--------------------------------------|--|
| WAY4 Web | <p>Файлы журнала сервера WS Runtime сохраняются в каталоге "<WS_Runtime_Path> /WEB-INF/logs/". настройки сервера WS Runtime сохраняются в каталоге "<WS_Runtime_Path> /WEB-INF/conf/".</p> <p>"Log-файлы IIS (Internet Information Services) располагаются в каталоге "<local disk>/inetpub/logs/logFiles".</p> <p>Log-файлы ошибок, возникающих во время работы веб-сайта (WAY4 Web Site), располагаются в каталоге "<path to site>/App_Data/ErrLog", где <path to site> - каталог с именем "installation_name", расположенный в каталоге "install_dir" (описание параметров см. в разделе "Секция [Common]" документации WAY4 Web). При отсутствии ошибок каталог "ErrLog" создаваться не будет.</p> |
| Transaction Switch | Файлы журнала сохраняются в каталоге <webapp>/WEB-INF/logs/. |
| NetServer | Файлы журнала сохраняются в каталоге, в котором установлено приложение, с ограничением доступа средствами операционной системы. |
| Access server | Файлы журнала сохраняются в каталоге, в котором установлено приложение, с ограничением доступа средствами операционной системы. |
| Java Secure Console | Файлы журнала сохраняются в каталоге, в котором установлено приложение Java Secure Console, в подкаталоге "logs". |
| Lifestyle Banking | Файлы журнала сохраняются в каталоге <Linux user home directory>/logs |
| Web Banking/Mobile Web Banking | <p>Файлы журнала сохраняются в каталогах:</p> <p><Customer Profile webapp>/WEB-INF/runtime/log</p> <p><Web Banking webapp>/WEB-INF/runtime/log</p> <p><Mobile Web Banking webapp>/WEB-INF/runtime/log</p> <p><Messenger Banking webapp>/WEB-INF/runtime/log</p> |

| Наименование продукта или компонента | Размещение файлов журнала |
|--------------------------------------|---|
| Host Card Emulation | Журнал сохраняется в каталоге: "%GRID_HOME%/owwork/logs/{date,yyyy-MM-dd~HH.mm}-gigaspace-{service}-{host}-{pid}.log" |
| IFP (Intelligent Fraud Prevention) | Файлы журнала TS-IFP адаптера сохраняются в каталоге "<appserver>/applications/<ts_ifp>/webapps/<ts_ifp>/WEB-INF/logs". Файлы журнала IFP engine сохраняются в каталоге "<appserver>/applications/<ifp>/logs". |
| Merchant QR Wallet | Файлы журнала QR Frontend Application сохраняются в каталоге "<QR_Frontend_Path>/logs/qr-frontend". |
| Mobile Authentication Cloud | Журнал сохраняется в Elasticsearch и доступен для просмотра по адресу <logView-cloud-app-url> в mCloud Log View Application. |



Переменная окружения %GRID_HOME% будет установлена после первого запуска GS Bootstrap.

5 Разработка безопасных платежных приложений

Данная глава посвящена удовлетворению требований п. 5.1, п.п. 5.2.5, п.п. 5.2.9, п.п. 5.2.10 и п.п. 5.4.4 стандарта PA-DSS, приведенных ниже.

| PA-DSS Requirement | PA-DSS Topic |
|--------------------|--|
| 5.1 | Develop secure payment applications. |
| 5.2.5 | Prevention of information leakage about applications configuration, their internal workings through improper error-handling methods. |
| 5.2.9 | Cross-site request forgery (CSRF). |
| 5.2.10 | Session management. |
| 5.4.4 | Implement and communicate application versioning methodology. |

5.1 Требования к приложениям

Данный раздел посвящен удовлетворению требований п. 5.1 стандарта PA-DSS.

5.1.1 Application Server

Техническая информация Apache Web Server (Status page) не должна предоставляться пользователю (файл httpd-info.conf):

```
#<Location /server-status>
#   ...
#</Location>
```

5.1.2 WAY4 Web

Техническая информация (Developer info) не должна предоставляться пользователю (файл web.config):

```
<add key="EnableDeveloperInfo" value="false" />
```

На промышленной системе для WS Runtime, в системных журналах, должна быть скрыта отладочная информация. Следует убедиться, что настроечный параметр `sql_debug` (Enable/Disable including SQL-query of service into response) установлен в значение "no":

```
<options
  sql_debug="no"
...
```

Параметр `sql_debug` определен в файле:

```
%WAY4ApplicationServer%/appserver/applications/wsruntime_xxx/webapps/wsruntime_xxx/  
WEB-INF/conf/global-options.xml
```

Заголовок с версией Microsoft ISS (Server Header) не должен предоставляться пользователю. Требуется создать параметр реестра `DisableServerHeader` типа `DWORD` со значением 1.

```
HKLM\SYSTEM\CurrentControlSet\Services\HTTP\Parameters
```

5.1.3 Messenger banking

Данный раздел посвящен удовлетворению требований п.п. 5.2.5 стандарта PA-DSS.

В конфигурации Messenger banking не должно быть открытых IP-адресов,

Публичные ссылки должны использовать доменные имена, а не IP-адреса:

```
public_url=https://demo.openwaygroup.com/chatbot  
send2friend_url=https://demo.openwaygroup.com/messenger-bot/send2friend
```

5.1.4 Web Banking/Mobile Web Banking

Данный раздел посвящен удовлетворению требований п.п. 5.2.9 – 5.2.10 стандарта PA-DSS.

Для защиты от атак вида Cross-site request forgery (CSRF) параметр `csrf_protection` в файле `ows-application.properties` должен иметь значение `true`.

Возможность параллельной работы пользователя в нескольких http-сессиях должна быть отключена (в файле `ows-application.properties` параметр `allow_multiple_user_sessions` должен иметь значение `false`).

5.2 Методика версионирования WAY4

Данный раздел посвящен удовлетворению требований п.п. 5.4.4 стандарта PA-DSS.

Номер версии WAY4 имеет следующий формат:

GG.MM.p.m.bbbb

Где:

- GG – две цифры обозначают номер поколения системы, они изменяются (номер увеличивается на 1) в случае глобальных архитектурных изменений.
- MM – две цифры обозначают номер мажорного функционального релиза, номер увеличивается на 1 в случае существенных функциональных изменений системы. Мажорный функциональный релиз может включать изменения, оказывающих влияние на безопасность по классификации PA-DSS.
- p – одна цифра обозначает PA-DSS релиз, число увеличивается на 1, если присутствуют изменения, оказывающие влияние на безопасность по классификации PA-DSS. Счетчик обнуляется после каждого мажорного функционального релиза.
- m – одна цифра обозначает номер минорного функционального релиза, номер увеличивается на 1 в случае несущественных функциональных изменений системы (обнуляется после каждого мажорного функционального релиза). Минорный релиз не может содержать изменений, оказывающих влияние на безопасность по классификации PA-DSS.
- bbbb – пять цифр означают номер сборки, номер увеличивается на 1 при выпуске каждой системной сборки с bugfix или patches (обнуляется после каждого минорного функционального релиза). Не может содержать существенных изменений по классификации PA-DSS.



Данный формат используется с версии 03.44. До версии 03.43 (включительно) использовался следующий формат:

GG.MM.mb.bb

Where:

- G – Generation Number
- M – Major Functionality Number
- m – Minor Functionality Number
- b – Build Number

5.2.1 Допустимые подстановочные знаки (Wildcards)

Подстановочный знак может быть использован только для компонента bbbb (GG.MM.p.m.x).

Пример: 03.50.1.3.0006.

Такая версия шаблона используется для обозначения группы небольших функциональных релизов без каких-либо изменений, которые могут повлиять на безопасность или выполнение требований PA-DSS. Только изменения, не влияющие на безопасность или выполнение требований PA-DSS.

6 Использование беспроводных технологий передачи данных

WAY4 не предназначен для использования с беспроводными сетями и все сетевые коммуникации между компонентами WAY4 должны быть сделаны только через проводные сети. Использование беспроводных сетей для связи компонентов WAY4 запрещено и все сетевые интерфейсы беспроводной на всех системных и сетевых компонентах обработки внутренних WAY4 связи должны быть отключены.

Если есть какие-либо беспроводные сети внутри организации, они должны быть либо с воздушным зазором от сетей обработки внутренних коммуникаций WAY4 или брандмауэр быть на месте между любыми беспроводными сетями и сетями обработки внутренней WAY4 связи и разрешение только явного разрешения трафика между беспроводной средой и сетями обработки внутренних коммуникаций WAY4. Для всех беспроводных сетей внутри организации (даже если они не обрабатывают внутренние WAY4связи) должно быть выполнено:

- все беспроводные ключи шифрования по умолчанию, пароли и строки SNMP должны быть изменены после установки.
- ключи шифрования беспроводного соединения, пароли и SNMP строки должны быть изменены в тот момент, когда кто-то со знанием ключей / паролей покидает компанию или меняет позицию.
- для обеспечения надежного шифрования для аутентификации и передачи должны использоваться передовые практические методы (например, IEEE 802.11.i - Wi-Fi Protected Access II / WPA2).

7 Обеспечение безопасности обновлений

Данная глава посвящена удовлетворению требований п.7.2.3 стандарта PA-DSS, приведенных ниже.

| PA-DSS Requirement | PA-DSS Topic |
|--------------------|--|
| 7.2.3 | Provide instructions for customers about secure installation of patches and updates. |

Для распространения обновлений безопасности WAY4 применяется регулярный процесс выставления Hotfix.

7.1 Требования

1. Для шифрования и подписи передаваемых данных между Клиентом и Службой поддержки (Customer Support) должны быть установлены PGP ключи.
2. Лица, которые могут быть вовлечены в процесс получения Hotfix и процесс установки на стороне Клиента, должны быть зарегистрированы в OpenWay Delivery JIRA в качестве официальных пользователей. Клиент должен поддерживать последнюю актуальную информацию о своих пользователях, указанных в регистрационной форме, и обязан своевременно информировать Службу поддержки об изменениях в информации о пользователях. Следует различать обычных зарегистрированных пользователей и официальных пользователей. Зарегистрированные пользователи – это все пользователи, которые имеют доступ к OpenWay Delivery JIRA. Официальные пользователи – это подгруппа зарегистрированных пользователей, которые участвуют в процессах получения и установки Hotfix.
3. Система WAY4, а также все обновления и исправления к ней распространяются при помощи индивидуальных FTP-соединений со стороны клиентов и защищены при помощи протокола шифрования PGP.
4. Соединение с FTP сервером предоставляется по запросу и деактивируется сразу же после использования.
5. Компоненты WAY4 не обновляются и не исправляются при помощи предоставления доступа к ним.
6. В системе WAY4 клиентское приложение удаленного доступа и изменения к нему распространяются в защищенном виде. Защита осуществляется при помощи электронной подписи, которая автоматически проверяется при установке.

7. В NetServer клиентское приложение удаленного доступа и изменения к нему распространяются в защищенном виде. Защита осуществляется при помощи электронной подписи, которая автоматически проверяется при установке.

7.2 Процедура

1. Служба поддержки готовит Hotfix, индивидуально для каждого клиента шифрует и подписывает Hotfix с помощью предварительных установленных ключей PGP и помещает исправление на FTP в специальные каталоги конкретного Клиента.
2. Служба поддержки информирует официальных пользователей о наличии Hotfix, используя электронную почту или телефон.
3. Официальный пользователь со стороны Клиента загружает Hotfix с FTP и расшифровывает его, проверяет подпись. Если возникают какие-либо проблемы с расшифровкой или проверкой подписи, официальный пользователь должен немедленно сообщить в Службу поддержки о происшествии и должен прекратить обработку Hotfix (установка Hotfix не должна быть произведена). Инцидент должен быть исследован Клиентом и Службой поддержки.
4. Если Hotfix имеет правильную подпись и может быть успешно расшифрован, он должен быть установлен в соответствии с инструкцией от Hotfix.

7.3 Обзор процесса установки



В различных решениях, система WAY4 может быть представлена в виде определенного набора компонентов. Набор компонентов может изменяться от решения к решению, в зависимости от требуемой функциональности.

При работе с этим документом, рекомендуется использовать следующие ресурсы из серии OpenWay документации:

- "Сервер приложений Администрирование WAY4™" (WAY4_Application_Server_Administering.pdf).
- "WAY4 Upgrade" (WAY4_Upgrade.pdf).

WAY4 представляет собой многокомпонентную систему. Процесс установки WAY4 состоит из следующих шагов:

- Планирование установки. Процедура установки должна быть документально оформлена с учетом специфики определенного экземпляра системы. Файлы журнала установки не должны быть потеряны при выполнении процедуры. План установки должен быть согласован с документацией системы WAY4 (руководства по установке, требования, примечания к выпуску).
- Завершение предустановочных задач. Рабочее окружение на стороне Клиента, организационное обеспечение перед началом установки WAY4, должно соответствовать

требованиям, персонала OpenWay. Все сети должны также быть полностью настроены к этому времени.

- Установка и настройка из БД Oracle (база данных, Oracle Partitioning, Advanced Security Option, программное обеспечение резервного копирования).
- Настройка рабочих станций.
- Установка и настройка компонентов на базе платформы Oracle (Cards, DataMart).
- Поиск и устранение неисправностей после установки каждого компонента.
- Установка компонентов, основанных на платформе Cards и платформе DataMart.
- Поиск и устранение неисправностей после установки каждого компонента.
- Установка Application Server.
- Поиск и устранение неисправностей после установки.
- Установка компонентов на основе платформы Application Server.
- Поиск и устранение неисправностей после установки каждого компонента.

8 Обеспечение безопасности платежного приложения

Данная глава посвящена удовлетворению требований п. 8.2 стандарта PA-DSS, приведенных ниже.

| PA-DSS Requirement | PA-DSS Topic |
|--------------------|--|
| 8.2 | Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties. |

8.1 Перечень используемого стороннего программного обеспечения, аппаратной архитектуры, используемых системных служб и протоколов

| Наименование продукта или компонента | Стороннее ПО | Аппаратная архитектура | Системные службы | Системные протоколы |
|--------------------------------------|-------------------------|---|------------------|---|
| WAY4 Cards | Oracle 12с/18с или выше | Для сервера БД: платформа Unix. Для файлового сервера: Intel PC. Рабочая станция: Intel PC. | Не используются | TCP/IP сервера БД, порт для Oracle Listener задается в конфигурации Oracle CIFS (Windows), SAMBA (Linux) для файлового сервера |
| WS Runtime | Не требуется | См. Application Server | Не используются | HTTP или HTTPS (1 порт для приема WS Runtime внешних запросов), SQL - NET (1 порт для связи с БД) |
| Payment Server | JRE 1.8 | См. Application Server | Не используются | TCP/IP, порт должен быть задан в конфигурации |

| Наименование продукта или компонента | Стороннее ПО | Аппаратная архитектура | Системные службы | Системные протоколы |
|--------------------------------------|---|-----------------------------------|------------------|---|
| Billing Gateway | Не требуется | x86 PC server, Sun Solaris server | Не используются | TCP/IP, порт зависит от Billing Provider и должен быть задан в конфигурации |
| WAY4 Web | Не требуется | См. Application Server | Не используются | HTTP, HTTPS (порт 443) |
| WAY4 Manager Client | JRE 1.8, Oracle DB Client (версия должна быть та же, что и версия БД) | Intel PC | Не используются | TCP/IP (связь с БД Oracle, host и порт задаются администратором в файле db.ini file) |
| Reports | Oracle Fusion Middleware с Oracle Reports Services 12c | Платформа Unix | Не используются | HTTP/HTTPS |
| Remote Access Server | Oracle DB Client (версия должна быть та же, что и версия БД) | Enterprise-level Intel PC Server | Не используются | TCP/IP/ HTTP/ Oracle OCI Порты: 1) Входной порт TCP, выбранный при создании приложения (например, 8080) 2) Выходной порт БД, выбранный в Oracle Connection Manager или порт DB Listener (например, 1521) |

| Наименование продукта или компонента | Стороннее ПО | Аппаратная архитектура | Системные службы | Системные протоколы |
|--------------------------------------|---|--|------------------|---|
| Datamart | Oracle 12c/18c или выше | Для сервера БД: платформа Unix. Для файлового сервера: Intel PC. Рабочая станция: Intel PC. | Не используются | TCP/IP, порт для Oracle Listener, заданный в конфигурации Oracle |
| File Exchange Engine (Pipes) | JRE 1.8 | Intel PC | Не используются | TCP/IP, порт, заданный в файле DB.ini, должен соответствовать настройкам Oracle Server |
| 3-D Secure | JRE 1.8, Apache Web Server 2.4.x | См. Application Server | Не используются | TCP/IP, TLS 1.2+ Порты: IP HTTPS(443) + MasterCard/VISA DS (заданные на этапе внедрения) |
| POS Management Server | Не требуется | Intel PC, UltraSparc III, IBM Power 5 or higher | Не используются | TCP/IP, порт зависит от сети POS и должен быть настроен |
| Application Server | Apache Web Server 2.4.x, Apache Tomcat 8.5.x, JDK 1.8 | Enterprise-level Intel PC Server, SPARC Enterprise T-Series Servers, IBM Power System S8XX / Power 7XX / Power 5XX Servers | Не используются | TCP/IP Порты Web Server: Входной HTTP (8080 по умолчанию) Входной HTTPS (8443 по умолчанию) данные порты могут быть изменены клиентом в конфигурации Web Server |

| Наименование продукта или компонента | Стороннее ПО | Аппаратная архитектура | Системные службы | Системные протоколы |
|--------------------------------------|--------------|---|---|---|
| WAY4U SMS Banking | JRE 1.8 | См. Application Server | Virtual COM port, если используется GSM modem | TCP/IP, порт задается в конфигурации, HTTP (если используется канал HTTP), SMPP (если используется канал SMPP) |
| NetServer | JRE 1.8 | Oracle SPARC, IBM Power Systems, Intel PC | Network Service | TCP/IP |
| Access Server | JRE 1.8 | См. Application Server | Network Service | TCP/IP |
| NetServer Console | JRE 1.8 | Intel PC | Network Service | TCP/IP |
| Transaction Switch | JRE 1.8 | См. Application Server | Network Service | TCP/IP |
| Web Banking Mobile Web Banking | JRE 1.8 | См. Application Server | Не используются | HTTPS, порт задается в конфигурации |
| Customer Profile | JRE 1.8 | См. Application Server | Не используются | TCP/IP, порт задается в конфигурации |
| Messenger Banking | Не требуется | См. Application Server | Не используются | HTTPS, порт задается в конфигурации |
| Lifestyle Banking | JRE 1.8 | См. Application Server | Не используются | HTTPS, порт задается в конфигурации; TCP/IP, порт задается в конфигурации; JDBC, порт задается в конфигурации; HTTP, порт задается в конфигурации. |

| Наименование продукта или компонента | Стороннее ПО | Аппаратная архитектура | Системные службы | Системные протоколы |
|--------------------------------------|---|--|------------------|--|
| Host Card Emulation | JRE 1.8 | См. Application Server. HSM: Safenet Protect Server External 2 / Protect Server Card 2 HSM, Thales PayShield 9000 HSM | Network Service | TCP/IP |
| Kiosk management | JRE 1.8 | Enterprise-level Intel PC Server, SPARC Enterprise T-Series Servers, IBM Power 710 Express | Не используются | TCP/IP, порт задается в конфигурации |
| IFP (Intelligent Fraud Prevention) | FoundationDB 6.2.11 | См. Application Server | Не используются | HTTP/HTTPS, порт задается в конфигурации |
| Merchant QR Wallet | JRE 1.8, Apache Ignite 2.8 | См. Application Server | Не используются | HTTP/HTTPS, порт задается в конфигурации |
| Mobile Authentication Cloud | JRE 1.8, Apache Mesos 1.9, Marathon 1.8, Elasticsearch 7,7, Zookeeper 3.6 | Enterprise-level Intel PC Server, SPARC Enterprise T-Series Servers, IBM Power 710 Express | Не используются | HTTP/HTTPS, порт задается в конфигурации |

Ни один из компонентов не использует фоновые приложения (daemons).



Компонент mod_security, который поставляется вместе с компонентами на базе Application Server, является обязательным для использования, так как он поставляется вместе с набором правил безопасности и является неотъемлемой частью приложения в плане безопасности (инструкцию по настройке компонента mod_security см. в документе "Администрирование WAY4™ Application Server").

Обратите внимание, что для работы с GigaSpaces XAP требуется получение лицензионного файла у представителей компании OpenWay. Файл необходимо скопировать в папку "gigaspace"

экземпляра приложения GS Bootstrap. Далее необходимо перезапустить приложение GS Bootstrap и развернуть WAY4Grid.



Для Application Server должно быть запрещено автоматическое создание JVM Heap Dump. Данное поведение установлено как поведение по умолчанию. Необходимо убедиться, что параметр `jvm_heap_dump` имеет значение `False` или `no` (описание параметра см. в документе "Administering WAY4™ Application Server"):

```
jvm_heap_dump = False
```



Необходимо своевременно устанавливать Oracle Java Commercial Updates, закрывающие уязвимости на промышленных и тестовых серверах, а также на рабочих станциях со следующими компонентами WAY4: Appserver, DB/WAY4 Manager, Testing Framework, Cards/WWEB Installers, CMT и прочих компонентах системы WAY4, использующих Java.

8.2 Требования к серверу базы данных [Обеспечение безопасности платежного приложения]

Все неиспользуемые, а также потенциально опасные сервисы операционной системы и приложения на сервере должны быть остановлены или заблокированы.

Минимальные требования к операционной системе для установки требуемой версии СУБД Oracle описаны в следующих ресурсах:

- https://docs.oracle.com/database/121/nav/portal_11.htm
- <https://docs.oracle.com/en/database/oracle/oracle-database/12.2/install-and-upgrade.html>
- <https://docs.oracle.com/en/database/oracle/oracle-database/18/install-and-upgrade.html>
- <https://docs.oracle.com/en/database/oracle/oracle-database/19/install-and-upgrade.html>

Все неиспользованные protocols/services/software на RHEL (например, IPv6, rpc.statd, rpcbind, cups, postfix, wpa_supplicant, abrt, certmonger, pulseaudio, и т.д.), AIX, Solaris и Windows, должны быть отключены.

На сервере базы данных должна быть отключена memory swapping.

8.3 Требования к файловому серверу [Обеспечение безопасности платежного приложения]

Должны быть остановлены или заблокированы все неиспользуемые, а также потенциально опасные сервисы операционной системы (в частности Restore Points OC Windows) и приложения на сервере.

8.4 Требования к рабочим станциям пользователей [Обеспечение безопасности платежного приложения]

Должны быть остановлены или заблокированы все неиспользуемые, а также потенциально опасные сервисы операционной системы (в частности Restore Points OC Windows), и сторонние приложения.

8.5 Требования для доступа к данным [Обеспечение безопасности платежного приложения]

Для доступа пользователей к данным, содержащимся в БД, должны использоваться только поставляемые в комплекте с системой WAY4 приложения, при работе с которыми в системных журналах гарантированно ведется аудит действий пользователей.

Категорически запрещается использовать приложения сторонних производителей для доступа к данным, содержащимся в БД.

8.5.1 NetServer и Transaction Switch

NetServer и Transaction Switch являются приложениями, не требующими контроля пользователя и использующими ограниченный набор строго предопределенных запросов к БД. Взаимодействие платежного приложения с БД осуществляется с использованием стандартной технологии шифрования СУБД. Необходимо, чтобы режим шифрования был включен при установке платежного приложения. За справками следует обращаться к документу "Oracle Database Security and the Payment Card Industry Data Security Standard".

8.6 Требования к конфигурации системы

Для соответствия требованиям безопасности необходимо выполнение следующих условий в конфигурации системы:

1. Доступ к формам, содержащим информацию о карточных и счетовых контрактах и держателях карт, ограничен и выдается только в случае служебной необходимости.
2. Настраиваемые пользователем элементы конфигурации (нестандартные таблицы, настраиваемые процедуры, разработанные пользователем формы и пайпы) должны хранить данные банковских карт только в предусмотренных для этого местах – таблицах БД и специальным образом организованных файловых областях (см. раздел "Права доступа к стандартным каталогам системы WAY4" документа "Администрирование пользователей в системе WAY4™").

9 Безопасность сетевой инфраструктуры

Данная глава посвящен удовлетворению требований п. 9.1 стандарта PA-DSS, приведенных ниже.

| PA-DSS Requirement | PA-DSS Topic |
|--------------------|---|
| 9.1 | Store cardholder data only on servers not connected to the Internet |

Любая система, содержащая компоненты платежных приложений, должна быть размещена во внутренней сети банка, изолированной от демилитаризованной зоны (DMZ).

9.1 Требования к базе данных сервера

Сервер базы данных должен находиться в отдельном сегменте внутренней сети банка, доступ к которому защищен с помощью отдельного межсетевого экрана (firewall).

9.2 Требования к файловому серверу [Безопасность сетевой инфраструктуры]

Файловый сервер находится в отдельном сегменте внутренней сети банка, доступ к которому защищен с помощью отдельного межсетевого экрана.

9.3 Требования к рабочей станции пользователя

Доступ во внешнюю сеть с рабочих станций должен осуществляться только через межсетевые экраны.

9.4 Требования к хранилищу данных [Безопасность сетевой инфраструктуры]

Запрещено хранить информацию о держателях карт на компьютерах, имеющих доступ в Интернет.

10 Удаленный доступ

Данная глава посвящен удовлетворению требований п.п. 10.1, 10.2.1, 10.2.3 стандарта PA-DSS, приведенных ниже.

| PA-DSS Requirement | PA-DSS Topic |
|--------------------|---|
| 10.1 | Implement multi-factor authentication for all remote access to payment application that originates from outside the customer environment. |
| 10.2.1 | Securely deliver remote payment application updates. |
| 10.2.3 | Securely implement remote-access software. |

10.1 Мультифакторная аутентификация

Мультифакторная аутентификация обычно используется вместо простой проверки подлинности пользователя, где простая проверка представляет собой процесс, в рамках которого инициатор запроса предоставляет другой стороне подтверждение того, что он именно тот, за кого себя выдает. Мультифакторная аутентификация призвана уменьшить вероятность предоставления инициатором запроса недостоверного подтверждения своей личности. Большое количество факторов обеспечивает более высокую вероятность того, что предъявитель подтверждения личности действительно является таковой в другой области (например, в компьютерной системе в сравнении с реальной жизнью). На самом деле следует учитывать большее количество переменных при установлении соответствующих гарантий подтверждения подлинности, чем просто количество использованных "факторов".

Мультифакторная аутентификация требует использования двух из трех нормативно утвержденных факторов. Это следующие факторы:

- Что-либо, что пользователь знает (например, пароль, PIN);
- Что либо, чем пользователь обладает (например, USB-брелок, смарт-карта);
- Что-либо, что характеризует собственно пользователя (например, биометрические характеристики, такие как отпечатки пальцев).

При любом удаленном доступе к системе должен использоваться механизм мультифакторной аутентификации.

10.1.1 Не консольный административный доступ с использованием USB-токен

USB-токен должен быть установлен и настроен в соответствии с рекомендациями изготовителя. Должен быть установлен и настроен PuTTY с поддержкой PKCS#11.

Для настройки PuTTY для USB-токена необходимо использовать "PKCS11" вкладку (эти параметры также используются SSH-агентом):

- "Attempt PKCS#11 smartcard auth (SSH-2)" - этот параметр используется для включения проверки подлинности смарт-карты в целом.
- "PKCS#11 library for authentication" - указать нужную библиотеку (DLL) для доступа к смарт-карте (PKCS # 11 файлов библиотек, Token метки и метки сертификата, соответствующего PKCS#11 межплатформенные, например, C:/Windows/System32/eToken.dll).
- "Token label" - укажите название вашей смарт-карты. Это то же самое имя, которое вы обычно видите при получении запроса на ввод пароля при доступе к смарт-карте для криптографических операций, например, при подписании электронной почты.
- "Certificate label" - ярлык на свидетельство соответствующего частного и публичного ключа, который вы хотите использовать для проверки подлинности.
- "SSH KeyString" – сохранить свой открытый ключ в <Home>/SSH файл /authorized_keys на сервере.

Подключение к Oracle под PMO, OWS_A, OWS_N, SYS, SYSTEM разрешено только с сервера и прокси-хоста. Триггер "ON DATABASE LOGIN" создается для управления соединением. Триггер анализирует IP-адрес клиента, от которого пришел запрос.

Пример:


```
create or replace trigger DBA_LOGON
after logon on DATABASE
declare
    v_session V$SESSION%rowtype;
    procedure KILL_SESSION_JOB (p_sid integer, p_serial integer) as
    pragma autonomous_transaction;
        v_job integer;
    begin
        dbms_scheduler.CREATE_JOB(
            job_name => 'JOB_KILL_SESSION_'||p_sid
            , job_type => 'PLSQL_BLOCK'
            , job_action => 'begin execute immediate ''alter system disconnect session ''''
            ||p_sid||'', ''||p_serial||'''' immediate''; end;'
            , start_date => sysdate
            , enabled => true
        );
        commit;
    end;
begin
    if sys_context('userenv', 'sessionid') != 0 then
        select s.*
        into v_session
        from V$SESSION s
        where 1=1
            and s.sid = (select sid from V$MYSTAT where rownum = 1);
        if user in ('OWS', 'OWS_A', 'OWS_N', 'SYS', 'SYSTEM') then
            if sys_context('userenv', 'ip_address') is not null and
                sys_context('userenv', 'ip_address') not in ('<oracle-host>', '<proxy-
host>')
            then
                KILL_SESSION_JOB(v_session.sid, v_session.serial#);
                raise_application_error(-20000, 'Connections by administrator is allowed
only from specific hosts.');
```

Для подключения к станции клиента под PMO, OWS_A, OWS_N, SYS, SYSTEM, на станции необходимо открыть SSH-соединение с прокси-хоста (настроить переадресацию портов клиента к Oracle Listener).

Пример (*nix):

```
ssh -N -L <local-port>:<oracle-host>:<oracle-port> <oracle-user>@<proxy-host>
```

Пример (Windows):

```
plink.exe -N -L <local-port>:<oracle-host>:<oracle-port> <oracle-user>@<proxy-host>
```

Так же на клиентской станции в tnsnames.ora указывается имя tns, использующее локальный порт. Example:

```
LOCAL=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=127.0.0.1)(PORT=<local-port>))  
(CONNECT_DATA=(SID=<oracle-sid>)))
```

10.1.2 NetServer

Приложение NetServer использует двухфакторную аутентификацию на основе сертификатов пользователя и платежного приложения в качестве первого фактора и пароля пользователя в качестве второго фактора.

В дополнение к двухфакторной аутентификации, используемой в NetServer, необходимо, чтобы механизм двухфакторной аутентификации использовался также при удаленном доступе к операционной системе сервера на котором установлено платежное приложение. Рекомендуемые технологии: SSH v.2 с использованием RSA-шифрования, TLS 1.2+ и VPN с сертификатами доступа. В каналах связи для удаленного доступа должно выполняться шифрование данных с использованием следующих технологий шифрования: SSH v.2, TLS 1.2+ и VPN.

10.1.3 Health Monitoring

Для соответствия требованиям безопасности необходимо выполнить следующие действия:

- Выполнить конфигурирование системных приложений "monitoring_ui" и "monitoring" с использованием защищенного соединения по протоколу TLS 1.2+:
 - Выполнить настройку параметров приложений ""monitoring_ui" и "monitoring" (см. раздел "Конфигурирование системного приложения "monitoring_ui"" документа "Администрирование WAY4 Health Monitoring Gen2"):
 - remoteServiceAPI="ssl".
 - rmi_ssl_protocols=TLSv1.2.
 - rmi_ssl_cipher_suites, например, значение TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384.

Примеры значений параметров в файле "config.properties" приложения "monitoring":

```
remoteServiceAPI=ssl
keyStore=conf/monitoring-app.jks
keyStorePassword=plain:eyA1xRbh
trustStore=conf/monitoring-app-trust.jks
trustStorePassword=plain:eyA1xRbh
rmi_api_port = 1099
rmi_service_port = 1098
rmi_ssl_protocols=TLSv1.2
rmi_ssl_cipher_suites=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
```

Примеры значений параметров в файле "config.properties" приложения "monitoring-ui":

```
keyStore=conf/monitoring-ui.jks
keyStorePassword=plain:eyA1xRbh
trustStore=conf/monitoring-ui-trust.jks
trustStorePassword=plain:eyA1xRbh
```

- Создать сертификаты для приложений ""monitoring-ui" и "monitoring" при помощи консольной утилиты "monitoring" (для платформы MS Windows – "monitoring.bat"), расположенной в каталогах "<AppServer_HOME>/applications/monitoring-ui/app/bin" и "<AppServer_HOME>/applications/monitoring/app/bin":

```
monitoring certificate -g
```

- Выполнить обмен сертификатами:
 - Для ОС Linux:

```
monitoring certificate -e way4@appsrv_host
```

где, way4@appsrv_host – <user@host>.

- Для ОС Windows (при помощи утилиты "keytool", расположенной в каталоге "<AppServer_HOME>/jdk/current/bin"):

```
keytool -import -v -trustcacerts -alias monitoring-app -file monitoring-app.cer
-keystore monitoring-ui-trust.jks -keypass eyA1xRbh -storepass eyA1xRbh
keytool -import -v -trustcacerts -alias monitoring-ui -file monitoring-ui.cer
-keystore monitoring-app-trust.jks -keypass eyA1xRbh -storepass eyA1xRbh
```

- Выполнить настройку безопасного доступа к приложению "monitoring-ui", а также добавление пользователей, которые будут работать с данным приложением, см. раздел "Включение двухфакторной аутентификации" документа "Администрирование WAY4™ Application Server". При добавлении пользователя необходимо использовать значение "hm_administrator" для параметра "role_name".

10.1.4 WAY4 Web (WS Runtime and Application Server)

Для приложений Application Server, для удовлетворения требований PA-DSS, должна быть включена авторизация приложений (и WS API) с помощью клиентских TLS-сертификатов, см. раздел "Авторизация приложений с использованием клиентских сертификатов" документа "Администрирование WAY4™ Application Server".

Для шифрования соединения от клиентского браузера до web-сервера IIS необходимо выполнить настройку WAY4 Web IIS сайта (конфигурационный файл web.config file) – атрибуту requireSSL должно быть определено значение "true":

```
...  
<configuration>  
...  
<system.web>  
...  
  <authentication mode="Forms">  
    <forms requireSSL="true">  
  </authentication>  
...
```

Между WAY4 Web IIS сайтом и WS Runtime необходимо настроить шифрование к приложениям Application Server и убедиться, что путь, указанный в параметре WsEngineURL файла web.config начинается с "https://":

```
...  
<configuration>  
...  
  <configSections>  
...  
  <appSettings>  
    <add key="WsEngineURL" value="https://padss-ws:8443/wsruntime_XX_X/ws/" />  
...  

```

10.2 Удаленный доступ к файловому серверу

Для удаленного доступа к файловому серверу должны использоваться только защищенные протоколы удаленного доступа, не имеющие на момент использования обнаруженных уязвимостей.

10.3 Требования к удаленным рабочим станциям пользователей

Сетевое взаимодействие между удаленными рабочими местами и внутренней сетью банка должно выполняться только по проводным каналам связи и при использовании защищенного

соединения (VPN или TLS 1.2), не имеющего на момент использования обнаруженных уязвимостей.

Рекомендуется при организации доступа с удаленных рабочих мест использовать фиксированные MAC- и IP-адреса.

11 Защита данных карт при передаче по открытым каналам связи

Данная глава посвящен удовлетворению требований п.п. 11.1, 11.2 стандарта PA-DSS, приведенных ниже.

| PA-DSS Requirement | PA-DSS Topic |
|--------------------|--|
| 11.1 | Secure transmissions of cardholder data over public networks |
| 11.2 | Encrypt cardholder data sent over end-user messaging technologies. |

В стандарте PA-DSS приведены следующие примеры открытых каналов связи:

1. Интернет
2. Беспроводные сети
3. GSM
4. GPRS

11.1 Использование шифрования и защищенных протоколов передачи данных

Система WAY4 обеспечивает отправку PAN в режиме онлайн и с помощью специальной технологии передачи сообщений клиентам. Настройки по умолчанию системы WAY4 и стандартные шаблоны сообщений/отчетов предполагают использование усеченных данных о держателях карт. Если в шаблонах сообщений клиенту или отчетов, настроенных пользователем, используется полный PAN, для каждого отсылаемого сообщения должно использоваться шифрование:

- 3DES с использованием ключа не менее чем тройной длины (168 непредсказуемых бита);
- AES (128 бита);
- RSA с не менее чем 1024-битным ключом.



При использовании протокола TLS 1.2 должно быть исключено:

- использование слабых групп шифров на основе 3DES, подобных:
TLS_RSA_WITH_3DES_EDE_CBC_SHA, DES-CBC3-SHA.
- шифрование по небезопасным алгоритмам базирующимся на: RC2, RC4, DES, MD4, MD5, EXP, EXP1024, AH, ADH, aNULL, eNULL, SEED nor IDEA.

Данная настройка может быть выполнена при помощи утилиты IIS Crypto (см. <https://www.nartac.com/Products/IISCrypto>). Порядок использования утилиты:

- на вкладке "Schannel" нажать кнопку [Best Practices], отключить TLS 1.0, 1.1, оставить только TLS 1.2, нажать кнопку [Apply];
- на вкладке "Cipher suites" нажать кнопку [Best Practices], отключить SHA1, оставить только SHA256 и SHA384, нажать кнопку [Apply];
- выполнить перезагрузку (приведенный порядок действий соответствует версии утилиты 2.0).



Использование шифрования при формировании отчетов и клиентских сообщений, которые содержат полный PAN, является абсолютно необходимым для удовлетворения требованиям стандарта PCI DSS.

Любая передача данных, содержащих информацию о счетовых и карточных контрактах, клиентах и другую критически важную с точки зрения безопасности информацию (в том числе данные (Sensitive Authentication Data / Cardholder Data), полученные в процессе обнаружения причин неисправностей в работе системы), может осуществляться только в зашифрованном виде. Шифрование данных должно обеспечиваться внешними техническими средствами.

Передача PIN-блока на любом из поддерживаемых интерфейсов должна осуществляться в зашифрованном виде с использованием ключа DES не менее чем тройной длины (168 непредсказуемых бита).

Данные требования следует учитывать, в том числе, при разработке интерфейсов к системе WAY4, удовлетворяющих специфическим потребностям пользователя. В частности, при необходимости передавать информацию о контракте держателю карты с помощью писем (Letters), необходимо обратиться в OpenWay для обеспечения безопасного (в зашифрованном виде) хранения шаблонов писем в БД и передачи данных безопасным способом.

В приведенной ниже таблице содержится информация по поддержке требований к передаче критической с точки зрения безопасности информации (Sensitive Authentication Data / Cardholder Data) продуктами и компонентами WAY4.

| Наименование продукта или компонента | Выполнение требований |
|---|--|
| Remote access | <p>При передаче Sensitive Authentication Data / Cardholder Data необходимо использовать VPN.</p> <div>  <p>Неиспользование VPN приводит к потере совместимости с требованиями стандарта PCI DSS.</p> </div> |
| eCommerce issuing, eCommerce acquiring, Bill payments | <p>3-D Secure передает Sensitive Authentication Data / Cardholder Data по защищенным каналам (TLS 1.2).</p> |
| ATM | <p>При передаче Sensitive Authentication Data / Cardholder Data необходимо использовать VPN.</p> <div>  <p>Неиспользование VPN приводит к потере совместимости с требованиями стандарта PCI DSS.</p> </div> |

| Наименование продукта или компонента | Выполнение требований |
|--|---|
| POS | 3DES с использованием ключа не менее чем двойной длины (не менее 168 непредсказуемых бита). |
| H2H | <p>При передаче Sensitive Authentication Data / Cardholder Data необходимо использовать VPN.</p> <div>  <p>Неиспользование VPN приводит к потере совместимости с требованиями стандарта PCI DSS.</p> </div> |
| Transaction Switch based eCommerce | 3DES с использованием ключа не менее чем двойной длины (не менее 168 непредсказуемых бита) |
| Lifestyle Banking | Все Sensitive Authentication Data / Cardholder Data должны передаваться по сетям общего пользования по протоколу HTTPS. Протокол HTTPS должен быть настроен на использование протокола TLS 1.2. |
| Web Banking/Mobile Web Banking, Customer Profile и Messenger Banking | <p>Все Sensitive Authentication Data / Cardholder Data должны передаваться по сетям общего пользования по протоколу HTTPS. Протокол HTTPS должен быть настроен на использование протокола TLS 1.2.</p> <p>Чтобы включить соединение по TLS 1.2 необходимо, в файл "ows-application.properties", добавить следующие параметры:</p> <pre>use_tcp_tls=true javax.net.ssl.trustStore=/home/way4/certs/owroot.jks javax.net.ssl.trustStorePassword=changeit</pre> <div>  <p>При указании пути к файлу "owroot.jks" должен использоваться знак "/", а не "\".</p> </div> |
| HCE | AES, 128 bits |
| Authserver | В конфигурации Authserver нельзя использовать SHA1 и другие скомпрометированные алгоритмы. |

11.2 Маскирование PAN

При передаче PAN по открытым каналам связи без шифрования он обязательно должен усекаться в соответствии с требованиями PCI DSS

Данное требование должно обязательно учитываться, в том числе, при разработке интерфейсов к системе WAY4, удовлетворяющих специфическим потребностям пользователя.

WAY4 SMS Banking усекает PAN в посылаемых SMS сообщениях.

12 Защита неконсольного административного доступа

Данная глава посвящен удовлетворению требований п. 12.1 стандарта PA-DSS, приведенных ниже.

| PA-DSS Requirement | PA-DSS Topic |
|--------------------|---|
| 12.1 | Encrypt non-console administrative access. |
| 12.2 | Use multi-factor authentication for all personnel with non-console administrative access. |

Для шифрования неконсольного административного доступа к системе должны использоваться защищенные протоколы, не имеющих на момент использования обнаруженных уязвимостей.

В настоящий момент таковыми являются следующие протоколы:

- SSH
- VPN
- TLS 1.2

Использование защищенных протоколов для неконсольного административного доступа является абсолютно необходимым для удовлетворения требованиям стандарта PCI DSS.

Инструкции по настройке неконсольного административного доступа см. в документе "Безопасный административный доступ к БД Oracle в соответствии со стандартом PCI DSS".

12.1 NetServer и Transaction Switch

Необходимо, чтобы доступ к операционной системе сервера, на котором установлено платежное приложение, осуществлялся с использованием многофакторной аутентификации.

Рекомендуемые технологии: SSH с использованием RSA-шифрования, TLS 1.2 и VPN с сертификатами доступа. В каналах связи для удаленного доступа должно выполняться шифрование данных с использованием следующих технологий шифрования: SSH, TLS 1.2 и VPN.

13 Тестирование

13.1 Требования к данным, используемым при тестировании системы

Не допускается использовать реальные данные в тестовых целях.

Если тестовая система формируется из производственной, то данные о счетовых и карточных контрактах, клиентах, значения ключей и Sensitive Authentication Data / Cardholder Data должна быть предварительно искажена.

14 Настройка криптографического оборудования (HSM)

Для криптографического устройства (HSM) производства Thales рекомендуется выполнить следующие настройки:

- Отключить хостовую команду (Host Command) "P0". Отключение производится через консоль управления криптографическим устройством, инструкция по отключению содержится в соответствующей документации на криптографическое устройство.
Отключать команду "P0" необходимо только для тех криптографических устройств, которые не используются в модуле электрической персонализации.
- Использовать для персонализации смарт-карт отдельное криптографическое устройство.
- При выполнении консольной команды "CS" (Configure Security) рекомендуется указывать следующие ответы на вопросы:
 - Echo [oN/ofF]: **F**
 - Select clear PINs? [Y/N]: **N**
 - Enable Single-DES? [Y/N]: **N**
 - Prevent Single-DES keys masquerading as double or triple-length key? [Y/N]: **Y**
 - Single/double length ZMKs [S/D]: **D**
 - Restrict Key Check Values to 6 hex chars [Y/N]: **Y**
 - Enable multiple authorised activities [Y/N]: **Y**
 - Enable PIN Block Format 34 as output format for PIN Translations to ZPK [Y/N]: **N**
В случае использования опции "PIN Change" необходимо в качестве ответа указать значение **"Y"**.
- Key export and import in trusted format only? [Y/N]: **N**

15 История изменения документа

R/N:2.7 - 17.08.2017

Added requirements:

- prohibit automatic creation of Heap Dump.
- encryption of the connection from the client browser to the IIS web server
- hide wsruntime debugging information
- mandatory setup of application authorization using client certificates.

Application version: 03.42.3.x, 03.43.3.x, 03.44.1.3.x, 03.45.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2

R/N:2.8 - 30.10.2017

3DES (112 bits), AES (128 bits), RSA (2048 bits)

Application version: 03.42.3.x, 03.43.3.x, 03.44.1.3.x, 03.45.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2

R/N:2.9 - 06.03.2017

Corrected key management requirements. Updated WAY4 Web logs file location.

Application version: 03.44.1.3.x, 03.44.2.3.x, 03.45.1.3.x, 03.46.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2

R/N:2.10 - 28.04.2018

Clear PAN access mechanisms. Encryption of the Oracle DBMS password. Key storage in Java Keystore.

Application version: 03.44.1.3.x, 03.44.2.3.x, 03.45.1.3.x, 03.46.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2

R/N:2.11 - 16.10.2018

Data storage requirements. Support of centralized logging.

Application version: 03.44.1.3.x, 03.44.2.3.x, 03.45.1.3.x, 03.46.1.3.x, 03.47.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2

R/N:2.12 - 30.10.2018

Data storage requirements. Support of centralized logging.

Application version: 03.44.1.3.x, 03.44.2.3.x, 03.45.1.3.x, 03.46.1.3.x, 03.47.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2

R/N:2.13 - 17.12.2018

Изменен раздел "[Использование шифрования и защищенных протоколов передачи данных](#)" (добавлена информация о запрете использования SHA1 в конфигурации Authserver).

Изменен раздел "[Перечень используемого стороннего программного обеспечения, аппаратной архитектуры, используемых системных служб и протоколов](#)" (добавлена информация о своевременности установки Oracle Java Commercial Updates).

Изменен раздел "[2018-12-20_12-30-58_Срок хранения данных карт \(Data Retention\)](#)" (добавлено замечание о хранении полей PVV и ENCRYPTED_PIN).

Application version: 03.45.1.3.x, 03.46.1.3.x, 03.47.1.3.x, 03.48.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2

R/N:2.14 - 11.01.2019

Все ссылки на "SSL" заменены на "TLS 1.2+".

Все упоминания "конфиденциальные данные" (sensitive data) заменены на "Sensitive Authentication Data / Cardholder Data".

Все упоминания "маскированного PAN" заменены на "усеченный PAN".

Application version: 03.45.1.3.x, 03.46.1.3.x, 03.47.1.3.x, 03.48.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2

R/N:2.15 - 24.04.2019

Изменен раздел "[Протоколирование приложений](#)". Удалено описание возможности анализа Log-файлов ошибок посредством Web-браузера.

Изменен раздел "[Использование шифрования и защищенных протоколов передачи данных](#)":

- Добавлена информация о слабых шифрах.
- Добавлена информация о настройке TLS в приложениях Web Banking/Mobile Web Banking, Customer Profile и Messenger Banking.

Application version: 03.45.1.3.x, 03.46.1.3.x, 03.47.1.3.x, 03.48.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2

R/N:2.16 - 08.08.2019

Изменены разделы: "[Использование шифрования и защищенных протоколов передачи данных](#)", "[Требования к управлению ключами](#)" (112 заменены на 168 непредсказуемых бит).

Изменена версия PCI DSS с 3.2 на 3.2.1.

Application version: 03.45.1.3.x, 03.46.1.3.x, 03.47.1.3.x, 03.48.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2.1

R/N:2.17 - 11.11.2019

Изменен раздел: "[Требования к хранению Sensitive Authentication Data / Cardholder Data](#)".

Добавлена информация о параметрах создания зашифрованных табличных пространств в Housekeeping для Oracle 18c.

Application version: 03.45.1.3.x, 03.46.1.3.x, 03.47.1.3.x, 03.48.1.3.x, 03.49.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2.1

R/N:2.18 - 31.12.2019

Изменен раздел: "[Требования к приложениям](#)". Добавлена информация о настройках продукта Application Server и компонента WAY4 Web IIS.

Изменен раздел: "[Обеспечение безопасности обновлений](#)". Добавлено описание различий между обычными зарегистрированными пользователями и официальными пользователями.

Application version: 03.45.1.3.x, 03.46.1.3.x, 03.47.1.3.x, 03.48.1.3.x, 03.49.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2.1

R/N:2.19 - 04.03.2020

Изменен раздел: "[Поддержка требований стандарта PCI DSS продуктами и компонентами WAY4](#)".

Дополнена информация о настройках File Exchange Engine (pipes).

Изменен раздел: "[Требования к приложениям](#)". Дополнена информация о настройках продуктов WAY4 Web и Messenger banking.

Application version: 03.46.1.3.x, 03.47.1.3.x, 03.48.1.3.x, 03.49.1.3.x, 03.50.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2.1

R/N:2.20 - 06.05.2020

Изменен раздел: "[Ведение аудитного журнала](#)". Дополнена информация о настройках продукта WAY4 Web.

Application version: 03.46.1.3.x, 03.47.1.3.x, 03.48.1.3.x, 03.49.1.3.x, 03.50.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2.1

R/N:2.21 - 14.05.2020

Изменен раздел: "[Протоколирование приложений](#)". Добавлена информация о продуктах IFP, Merchant QR Wallet и Mobile Authentication Cloud.

Изменен раздел: "[Перечень используемого стороннего программного обеспечения, аппаратной архитектуры, используемых системных служб и протоколов](#)". Добавлена информация о продуктах IFP, Merchant QR Wallet и Mobile Authentication Cloud.

Изменен раздел: "[Шифрование пароля к СУБД Oracle](#)". Добавлена информация об алгоритмах шифрования SHA256/SHA512.

Все упоминания "Oracle 10g/11g" заменены на "Oracle 12c/18c".

Все упоминания "RHEL 7.2/6.8" заменены на "RHEL 7.8/6.10".

Application version: 03.46.1.3.x, 03.47.1.3.x, 03.48.1.3.x, 03.49.1.3.x, 03.50.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2.1

R/N:2.22 - 13.07.2020

Изменен раздел: "[Поддержка требований стандарта PCI DSS продуктами и компонентами WAY4](#)".

Дополнена информация о настройках компонента Transaction Switch.

Application version: 03.46.1.3.x, 03.47.1.3.x, 03.48.1.3.x, 03.49.1.3.x, 03.50.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2.1

R/N:2.23 - 16.10.2020

Изменен раздел: "[Ведение аудитного журнала](#)". Дополнена информация о продукте WAY4 Web.

Application version: 03.47.1.3.x, 03.48.1.3.x, 03.49.1.3.x, 03.50.1.3.x, 03.51.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2.1

R/N:2.24 - 09.12.2020

Изменен раздел: "[Требования к хранению Sensitive Authentication Data / Cardholder Data](#)".

Добавлено упоминание Oracle 19c в команды создания архивных табличных пространств.

Изменен раздел: "[Требования к серверу базы данных](#)". Добавлены ссылки на ресурсы с требованиями к операционной системе по поддерживаемым версиям СУБД Oracle.

Application version: 03.47.1.3.x, 03.48.1.3.x, 03.49.1.3.x, 03.50.1.3.x, 03.51.1.3.x

PA-DSS Version – 3.2

PCI DSS Version – 3.2.1