Аладдин РД
www.aladdin-rd.ru

Защита информации в базах данных

Обеспечение выполнения требований стандарта PCI DSS 2.0 в части хранения PAN, критичных аутентификационных данных и информации о держателях карт.

Справочная информация

для специалистов
по информационной
безопасности и ИТ

Оглавление

Аннотация

Настоящий документ описывает возможности программно-аппаратных решений "Крипто БД" и "SafeData" в плане применения в информационных системах, обрабатывающих данные пластиковых карт и их владельцев. Рассматриваются технические и технологические методы применения указанных решений для прямого выполнения требований п.3 PCI DSS 2.0, а также некоторых других положений стандарта.

Термины, определения и сокращения

№	Термин/определение	Описание
1	"Крипто БД", "SafeData"	Наименование продуктов
2	Прикладное ПО	ПО, использующее информацию из колонок таблиц, защищенную с помощью "Крипто БД"/"SafeData"
3	БД / БД Oracle	База данных, база данных Oracle.
4	СКЗИ	Средство криптографической защиты информации

Назначение "Крипто БД"/"SafeData"

Средства криптографической защиты "Крипто БД"/"SafeData" предназначены для обеспечения конфиденциальности информации с помощью криптографического преобразования. "Крипто БД" позволяет также контролировать целостность информации с помощью выработки и проверки имитовставки.

Основные характеристики

- Реализация криптографических алгоритмов;
- Реализация механизма управления ключами шифрования данных;
- Дискретная и мандатная модели разделения доступа;
- Контроль целостности собственного ПО и служебной информации;
- Аудит и мониторинг доступа к зашифрованным данным;
- Консоль управления шифрованием, ключами, пользователями, аудитом и т.д.

Реализованные алгоритмы

Крипто БД	SafeData
Симметричные алгоритмы шифрования (шифрование данных)	
ГОСТ 28147-89 с размером ключа 256 бит, в режимах: • простой замены (ECB); • гаммирования (OFM); • гаммирования с обратной связью (CFB); • сцепления блоков (CBC); • простой замены с диверсификацией ключа шифрования (ECB-UKM); • гаммирования с диверсификацией ключа шифрования (OFB-UKM); • гаммирования с обратной связью с дивер-	• DES с размером ключа 56 бит; • TripleDES с размером ключа 168 бит; • AES с размером ключа 128,192 и 256 бит.

Крипто БД	SafeData
сификацией ключа шифрования (CFB-UKM); • сцепления блоков с диверсификацией ключа шифрования (CBC-UKM) • простой замены с выработкой имитовставки (ECB-MAC); • гаммирования с выработкой имитовставки (Counter mode-MAC); • гаммирования с обратной связью и выработкой имитовставки (CFB-MAC); • сцепления блоков с выработкой имитовставки (CBC-MAC); • простой замены с диверсификацией ключа шифрования и выработкой имитовставки (ECB-MAC-UKM); • гаммирования с диверсификацией ключа шифрования и выработкой имитовставки (OFB-MAC-UKM); • гаммирования с обратной связью, с диверсификацией ключа шифрования и выработкой имитовставки (CFB-MAC-UKM); • сцепления блоков с диверсификацией ключа шифрования и выработкой имитовставки (CBC-MAC-UKM).	
Асимметричные алгоритмы шифрования (защита ключей шифрования данных)	
ГОСТ Р 34.10-2001: • открытый ключ — 512 бит.	RSA: открытый ключ — 1024, 2048 или 4096 бит.

Область применения “Крипто БД”

- Информационные системы с приложениями “Клиент-сервер”
- Многозвенные приложения информационных систем
- Терминальный доступ
- Автоматические процессы
- Облачные системы (IaaS, SaaS)

Общие ограничения применения

- Версии сервера Oracle Database:
  - 9i, 10g, 11g (SE/SE1/EE);
- ОС клиента:
  - MS Win XP/Vista/7 32/64 бит;
- Деградация производительности (время отклика) 5-35%;
- Не поддерживается шифрование индекс-организованных таблиц;
- Не поддерживаются объектные типы данных, типы данных LONG, LONG RAW, BFILE;
- Индексирование только по строгому совпадению; [1)]

- Не работоспособно в кластерных конфигурациях Oracle (Real Application Cluster) [2)].

Ограничения применения «Крипто БД»

- Криптографическая защита по классам КС1, КС2;
- Не применимо для защиты гостайны;
- ОС сервера БД Oracle:
  - MS Win 2003/2008, RHE Linux, SLES Linux, IBM AIX, HP-UX, Oracle Solaris (Intel/SPARC), IBM z SLES Linux;
- ОС клиента:
  - MS Win XP/Vista/7 32/64 бит.

Сертификация

СКЗИ "Крипто БД" имеет сертификат соответствия ФСБ по классам защиты КС1, КС2 № СФ/124-1569, действительный до 06.11.2013 г.

[1)] Для использования индексов, в том числе для полнотекстового поиска и поиска по частичному совпадению, возможно применение специальных техник.
[2)] Ограничение будет устранено в следующих версиях продукта.

”Крипто БД”, “SafeData” и PCI DSS 2.0

Прямое выполнение требований PCI DSS относительно обязательного шифрования PAN традиционно представляет собой наиболее серьёзную проблему для операторов процессинговых систем. Особенно остро такая проблема стоит перед операторами, использующими уже готовые системы, зачастую хранящие огромные объёмы данных. “Крипто БД” и “SafeData” разработаны для реализации следующих возможностей:

- защита информации от несанкционированного доступа со стороны неуполномоченных пользователей, в том числе привилегированных (администраторы БД, ОС и т.п.);
- надёжная защита ключей шифрования на протяжении их жизненного цикла;
- прозрачное встраивание в готовые информационные системы;
- аудит и мониторинг доступа к защищённым данным;
- централизованное управление функциями безопасности (ключи шифрования, аудит, пользователи и т.п.);
- контроль целостности собственного ПО и служебной информации.

Подобные функциональные возможности позволяют выполнить ряд требований стандарта без какой-либо значительной переделки готовой информационной системы.

<table>
<tr><th colspan="2">Пункт PCI DSS</th><th>Содержание</th><th>Соответствующая возможность «Крипто БД», «SafeData»</th></tr>
<tr><td colspan="4">Создание и поддержка безопасной сетевой инфраструктуры</td></tr>
<tr><td>2</td><td></td><td>Не использовать установленные производителем системные пароли и иные параметры безопасности.

Злоумышленники (внешние и внутренние) при атаке на систему часто пытаются использовать установленные производителем пароли и иные параметры по умолчанию. Эти пароли хорошо известны в определенных сообществах, и их легко получить из открытых источников информации.</td><td rowspan="2">Компонент клиента “Крипто БД”, “SafeData” дополнительно обеспечивает возможность аутентификации пользователя в БД по протоколу SSL, поддерживаемому Oracle. Такая возможность обеспечивает:
• отказ от использования паролей;
• строгую двухфакторную аутентификацию;
• защиту канала передачи данных одним из стойких криптоалгоритмов, предлагаемых Oracle.
Для хранения ключей и сертификатов для SSL аутентификации используется аппаратный носитель - смарт-карта или USB-токен. Допускается использование одних и тех же аппаратного носителя и ключей/сертификатов для аутентификации и доступа к зашифрованным данным. Компонент клиента расширяет штатную функциональность ПО Oracle Client, его работа полностью прозрачна для административных и прикладных систем.</td></tr>
<tr><td></td><td>2.3</td><td>При использовании неконсольного административного доступа к системе, следует всегда шифровать канал с использованием стойких криптографических алгоритмов. Следует использовать такие технологии, как SSH, VPN или SSL/TLS для веб-ориентированных систем администрирования и иных способов неконсольного административного доступа.</td></tr>
<tr><td colspan="4">Обеспечить безопасное хранение данных о держателях карт</td></tr>
<tr><td>3</td><td></td><td>Методы защиты данных, такие как шифрование, обрезка, маскирование и хеширование являются критичными компонентами защиты данных о держателях карт.

Если взломщик обойдет остальные средства управления безопасностью сети и получит доступ к зашифрованным данным, не зная ключа шифрования, то эти данные останутся для него нечитаемыми и практически бесполезными. Иные способы защиты хранимых данных должны
рассматриваться как средства уменьшения</td><td>“Крипто БД”/”SafeData” реализуют защиту данных с помощью шифрования. Промышленные стойкие алгоритмы шифрования совместно с безопасной системой сохранения в тайне ключей шифрования обеспечивают надёжную защиту данных, позволяющую выполнить требования данного пункта стандарта. Методы защиты данных, управление шифрованием и ключами шифрования, реализованные в “Крипто БД”/”SafeData” также соответствуют рекомендациям VISA [11].</td></tr>
</table>

Пункт PCI DSS	Содержание	Соответствующая возможность «Крипто БД», «SafeData»
	риска.	
3.2	Запрещается хранить критичные аутентификационные данные после авторизации (даже в зашифрованном виде). К критичным аутентификационным данным относятся данные, перечисленные в требованиях: 3.2.1. Запрещается хранить полное содержимое дорожки (содержимое магнитной полосы, находящейся на обратной стороне карты, его аналог на чипе либо в ином месте). Эти данные также называются "полная дорожка", "дорожка", "дорожка 1", "дорожка 2" и "данные магнитной полосы". Примечание: Для ведения бизнеса может быть необходимо хранение следующих элементов данных магнитной полосы: • имя держателя карты • номер платежной карты (PAN) • дата истечения срока действия карты • сервисный код. Для минимизации рисков разрешается хранить только указанные элементы данных. 3.2.2. Запрещается хранение кода CVC или значения, используемого для подтверждения транзакций, выполняемых без непосредственного считывания информации с кредитной карты (трех - или четырехзначного числа, изображенного на лицевой или обратной стороне карты). 3.2.3. Запрещается хранение персонального идентификационного номера (PIN), а также зашифрованного PIN-блока. Примечание: Эмитенты и компании, обеспечивающие эмиссионные сервисы, могут иметь обоснованную необходимость хранения критичных аутентификационных данных. Такая необходимость должна иметь обоснование с точки зрения бизнеса, а хранимые данные должны быть надежно защищены.	См. выше.
3.3	Следует маскировать PAN при его отображении (максимально возможное количество знаков PAN для отображения – первые 6 и последние 4). Примечание: • Данное требование не относится к сотрудникам и иным сторонам, для работы которых необходимо видеть весь PAN; • Данное требование не заменяет собой иные более строгие требования к отображению данных о держателях карт (например, на чеках POS-терминалов). ☐	Для просмотра полного PAN сотрудниками или иными сторонами они должны иметь необходимые права – закрытый ключ и сертификат для доступа к соответствующим ключам шифрования. Данная информация хранится на USB-ключе или смарт-карте и доступна только при вводе правильного PIN-кода. Для маскирования PAN соответствующими приложениями должны быть применены специальные процедуры с использованием API "Крипто БД"/"SafeData".
3.4	PAN должен быть представлен в нечитаемом виде во всех местах хранения (включая данные на съемных носителях, резервных	"SafeData" позволяет зашифровывать требуемые данные с помощью различных криптографических алгоритмов.

Пункт PCI DSS	Содержание	Соответствующая возможность «Крипто БД», «SafeData»
	копиях и журналах протоколирования событий). Для этого следует использовать любой из следующих методов: • стойкая однонаправленная хэш-функция (должен быть хеширован весь PAN); • укорачивание (хеширование не может использоваться для замещения укороченного сегмента PAN); • использование механизмов One-Time-Pad ("одноразовых блокнотов", хранение которых должно быть безопасным) и использование и хранение ссылок на данные вместо самих данных (index tokens); • стойкие криптографические алгоритмы совместно с процессами и процедурами управления ключами. Примечание: При наличии доступа одновременно к маскированному и хешированному номерам карты для злоумышленника не составит большого труда восстановить данные исходного PAN. Если маскированное и хешированное значение одного и того же PAN содержатся внутри среды какой-либо структуры, необходимо ввести дополнительные средства контроля для недопущения корреляции между маскированным и хешированным значениями. В подобных условиях исходный PAN становится легко восстановимым.	В стандартном исполнении могут использоваться симметричные алгоритмы: • 3DES с длиной ключа 168 бит; • AES с ключами длиной 128, 192, 256 бит; Защита ключей шифрования при хранении и передаче осуществляется с помощью асимметричного алгоритма RSA с открытым ключом длиной до 4096 бит. "Крипто БД" использует симметричный алгоритм ГОСТ28147-89 с длиной ключа 256 бит. Для защиты ключей шифрования используется метод передачи защищённых сообщений, согласно RFC 4490. В специальном исполнении возможна реализация иных (например, соответствующих национальным стандартам) симметричных алгоритмов для шифрования и асимметричных для защиты ключей шифрования. Примечание: Ключ шифрования данных привязан к закрытому ключу и сертификату конкретного пользователя, которые хранятся на смарт-карте или USB-токене. Таким образом, косвенно выполняется требование п.3.4.1 (Ключи шифрования не должны быть привязаны к учетным записям пользователей).
3.5	Следует обеспечить защиту всех ключей шифрования данных о держателях карт от их компрометации или неправильного использования: Примечание: Данное требование также применимо к ключам шифрования ключей, используемых для защиты ключей шифрования данных. Такие ключи шифрования ключей должны быть, как минимум, не менее стойкими, чем ключи шифрования данных.	Для защиты ключей шифрования данных используются стойкие асимметричные алгоритмы, которые рекомендованы [11] также как и используемые длины ключей. Ключи защиты ключей шифрования данных хранятся на аппаратных носителях и не могут быть из них извлечены.
3.5.1	Доступ к ключам шифрования должен быть разрешен наименьшему возможному количеству ответственным за их хранение и использование сотрудников.	Поскольку доступ к ключам шифрования обеспечивается с помощью аппаратных (физических) носителей, имеющих аппаратно "прошитый" идентификатор, то их легко персонифицировать, хранить и учитывать. Возможно применение централизованных систем управления такими носителями.
3.5.2	Ключи должны храниться только в строго определенных защищенных хранилищах и строго определенном виде.	
3.6	Должны быть полностью документированы и внедрены все процессы и процедуры управления ключами шифрования данных о держателях карт, в том числе: 3.6.1 Генерация стойких ключей; 3.6.2 Безопасное распространение ключей; 3.6.3 Безопасное хранение ключей; 3.6.4 Смена ключей шифрования, криптопериод которых истек (например, когда истек установленный срок, и/или когда данным ключом было зашифровано неко-	"Крипто БД"/"SafeData" полностью реализует управление жизненным циклом ключей шифрования, включая: • генерацию; • распространение; • смену; • изъятие у пользователя/временное приостановление; • резервное копирование и восстановление. Для создания резервный копий ключей шифрования, защищённых паролем, может применяться

Пункт PCI DSS	Содержание	Соответствующая возможность «Крипто БД», «SafeData»
	торое количество криптотекста), основана на передовых практических методах индустрии безопасности и руководствах (например, специальное издание 800-57 NIST) и должна производиться согласно предписаниям соответствующего производителя или владельца ключа; 3.6.5 Изъятие или смена ключей (например, архивация, уничтожение или/и аннулирование) при нарушении его целостности (например, увольнение сотрудника, обладающего информацией об открытом коде ключа), а также ключей, относительно которых существуют подозрения в их компрометации. Примечание: Если существует необходимость сохранения изъятых или замененных ключей, они должны быть надежно заархивированы (например, посредством ключа шифрования ключей). Помещенные в архив криптографические ключи должны использоваться только в целях дешифрования/верификации; 3.6.6. Если процедуры управления криптографическими ключами в открытом виде осуществляются вручную, данные процедуры должны управляться с использованием раздельного знания и двойного контроля (например, таким образом, чтобы для расшифрования данных требовался составной ключ, компоненты которого хранятся у 2-3 сотрудников); Примечание: Примеры процедур управления ключами включают (но не ограничиваются): • генерацию ключа; • передачу ключа; • загрузку ключа в устройство; • хранение и уничтожение ключа; 3.6.7 Защита от неавторизованной смены ключа; 3.6.8 Определение обязанностей и ответственности сотрудников по хранению и использованию ключей с официальным подтверждением их согласия с ознакомлением и принятием таких обязанностей и ответственности. Примечание: Существует множество различных источников, из которых можно почерпнуть информацию о стандартах в управлении ключами (например, стандарт национального института стандартов и технологий США (NIST), с которым можно ознакомиться на сайте http://csrc.nist.gov).	пороговая схема 3/2 (Из трёх лиц, обладающих частями ключа, любые двое могут восстановить его). Документация “Крипто БД”/”SafeData” регламентирует обязанности администратора безопасности по управлению шифрованием и ключами шифрования, а также действия пользователей и администратора в случае компрометации ключей и нештатных ситуаций. Даются рекомендации для пользователей и администраторов безопасности и баз данных по работе с “Крипто БД”/”SafeData”, учёту ключей и носителей и примеры документов.

Пункт PCI DSS	Содержание	Соответствующая возможность «Крипто БД», «SafeData»
Внедрение строгих мер контроля доступа		
7	Ограничить доступ к данным платежных карт в соответствии со служебной необходимостью. Для гарантии того, что доступ к критичным данным есть только у авторизованного персонала, системы и приложения должны ограничивать доступ к данным в соответствии с принципом служебной необходимости. Принцип служебной необходимости – права доступа предоставляются только к тем данным, которые необходимы для выполнения должностных или договорных обязанностей.	В "Крипто БД"/"SafeData" реализованы две модели разграничения доступа: • дискреционная - есть или нет ключ шифрования той или иной колонки у пользователя; • мандатная - соответствует ли метка доступа ключа (чтение/запись) пользователя метке зашифрованных этим ключом данных. Дискреционная модель позволяет запретить доступ к зашифрованной информации для любого пользователя, даже обладающего административными привилегиями. Мандатная модель позволяет ограничить права на доступ к информации авторизованных пользователей, имеющих ключи шифрования, в соответствие со служебными обязанностями. Указанное управление доступом позволяет полностью выполнить требования п.7.
7.1	Доступом к вычислительным ресурсам и информации о держателях карт должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями. Ограничения доступа должны включать в себя: 7.1.1. Доступ пользователям предоставлен только к тем данным, которые необходимы им для выполнения своих должностных обязанностей; 7.1.2. Назначение привилегий пользователям должно быть основано на их должностных обязанностях; 7.1.3. Подписание уполномоченными лицами заявки о предоставлении прав доступа; 7.1.4. Внедрение автоматизированной системы контроля доступа;	
7.2	Для многопользовательских систем следует установить механизм разграничения доступа, основанный на факторе знания и применяющий принцип "запрещено все, что явно не разрешено". Механизм контроля доступа должен включать следующее: 7.2.1. Покрытие всех системных компонентов; 7.2.2. Назначение привилегий пользователям должно быть основано на их должностных обязанностях; 7.2.3. По умолчанию должен быть запрещен любой доступ. Примечание: Некоторые механизмы контроля доступа применяют правило "разрешить все" по умолчанию до тех пор, пока явно не прописано правило запрещения доступа.	
8	Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре. Назначение уникального идентификатора каждому человеку, имеющему доступ к	Лица, допущенные к работе с открытыми данными PAN, идентифицируются аппаратным номером персональной смарт-карты или USB-токена. Аппаратный идентификатор не может быть изменён, его можно использовать при аудите действий и его легко учитывать поэкземплярно в различной

Пункт PCI DSS	Содержание	Соответствующая возможность «Крипто БД», «SafeData»
	компьютерной сети, позволяет гарантировать, что действия, производимые с критичными данными и системами, производятся известными и авторизованными пользователями и могут быть отслежены.	документации.
8.1	Каждому пользователю должно быть назначено уникальное имя учетной записи до предоставления ему доступа к компонентам системы и данным о держателях карт.	
8.2	Помимо идентификатора, должен применяться хотя бы один из следующих методов для аутентификации всех пользователей: • То, что вы знаете (пароль и парольная фраза); • То, что у вас есть (ключи или смарт-карты); • То, что вы есть (биометрические параметры). ☐	Используется смарт-карта или USB-токен, защищённые PIN-кодом.
8.3	Все пароли должны храниться и передаваться только в зашифрованном виде с использованием стойких криптографических алгоритмов. ☐	Для работы с защищённой информацией “Крипто БД”/”SafeData” пароли не используются. PIN-код USB-токена или смарт-карты, который используются для доступа к ключам шифрования, нигде не хранится и не передается.
8.5	Должен быть установлен контроль над выполнением процедур идентификации и аутентификации пользователей и управления паролями учетных записей сотрудников и администраторов на всех системных компонентах, включающий в себя...	Выполнение п. 8.5.1-8.5.13 может быть обеспечено любой системой централизованного управления смарт-картами.
Регулярный мониторинг и тестирование сети		
10	Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт. Наличие механизмов ведения записей о событиях, а также возможности проследить действия пользователей необходимо для системы, так как они позволяют провести расследование и анализ инцидентов. Определение причин инцидентов затруднено при отсутствии журналов записей о событиях в системе.	Доступ к данным, защищённым с помощью “Крипто БД”/”SafeData” осуществляется с помощью встроенного агента аудита и коллекторов аудита.
10.1	Должен быть разработан процесс мониторинга доступа к компонентам системы (особенно доступа с административными полномочиями), а также привязки событий к определенным сотрудникам.	Механизм разделения доступа в “Крипто БД”/”SafeData” предусматривает наличие у пользователей административных полномочий и даже в случае их наличия блокирует несанкционированные попытки изменения целостности компонентов системы.
10.2	Для каждого системного компонента должен быть включен механизм протоколирования следующих событий: 10.2.1 Любой доступ пользователя к данным о держателях карт; 10.2.2 Любые действия, совершенные с использованием административных полномочий; 10.2.3 Любой доступ к записям о событиях в системе; 10.2.4 Неуспешные попытки логического доступа; 10.2.5 Использование механизмов иденти-	Механизм встроенного аудита позволяет регистрировать указанные события. Данные аудита защищены от администраторов БД. Примечание: в качестве системного компонента в данном случае подразумевается сервер БД.

Пункт PCI DSS	Содержание	Соответствующая возможность «Крипто БД», «SafeData»
	фикации и аутентификации; 10.2.6 Инициализация журналов протоколирования событий; 10.2.7 Создание и удаление объектов системного уровня.	
10.3	Для каждого события каждого системного компонента должны быть записаны как минимум следующие параметры: 10.3.1 Идентификатор пользователя; 10.3.2 Тип события; 10.3.3 Дата и время; 10.3.4 Успешным или неуспешным было событие; 10.3.5 Источник события; 10.3.6 Идентификатор или название данных, системного компонента или ресурса, на которые повлияло событие.	Механизм встроенного аудита позволяет регистрировать для каждого события указанные параметры. В качестве идентификатора пользователя используется отличительное имя сертификата, использованного для получения ключа шифрования. В качестве типа события различаются: • административные (шифрование, управление ключами, управление аудитом); • служебные (аутентификация пользователя); • доступ к данным (вставка, чтение, обновление, удаление). В качестве источника события регистрируется IP-адрес, доменное имя, имя пользователя БД (схема БД), отличительное имя из сертификата пользователя, аппаратный идентификатор смарт-карты. Идентификатором ресурса выступает физический адрес строки таблицы, к которой был доступ.
10.5	Журналы протоколирования событий должны быть защищены от изменений.	Доступ к журналам имеет только администратор безопасности.
11.5	Следует использовать средства контроля целостности файлов для оповещения персонала о несанкционированных изменениях критичных системных файлов, конфигурационных файлов и файлов данных; сопоставительный анализ критичных файлов должен проводиться не реже одного раза в неделю. Примечание: Обычно контролируется целостность файлов, которые изменяются нечасто, но изменение которых может служить признаком компрометации или попытки компрометации системы. Средства контроля целостности обычно содержат предустановленный перечень файлов, подлежащих контролю, в зависимости от используемой операционной системы. Другие критичные файлы, такие как файлы для клиентских приложений, должны быть определены самой компанией (т.е. торгово-сервисным предприятием или поставщиком услуг).	Механизм контроля целостности “Крипто БД”/”SafeData” позволяет проверять целостность процедур шифрования, процедур аудита, настроек, объектов, создаваемых в процессе шифрования (дополнительные представления, триггеры), а также произвольных объектов БД.

Сравнение со штатными механизмами защиты Oracle

Сравнение функциональных возможностей "Крипто БД"/"SafeData" с возможностями средств защиты Oracle в части защиты данных, разделения доступа и аудита проводилось на основании документа [10].

Для реализации выполнения требований по пунктам PCI-DSS, перечисленным в предыдущем разделе, СУБД Oracle предполагает использование следующих опций СУБД и программных продуктов:

Функциональность	Реализация	Примечание
Шифрование канала	Oracle Advanced Security	Опция Oracle DB Server Enterprise Edition
Шифрование данных	Oracle Advanced Security Transparent Data Encryption (TDE)	Опция Oracle DB Server Enterprise Edition. Позволяет зашифровывать данные на уровне колонок таблиц и на уровне табличного пространства (группа файлов данных). Более подробно о TDE см. [12].
Хранение ключей шифрования данных	Oracle Advanced Security	Мастер-ключ шифрования данных хранится в БД, защищен с помощью ключа, который в свою очередь сохраняется в файле, защищённом паролем (wallet) или в HSM. На БД может быть один мастер-ключ, его распространение рекомендуется производить с помощью Oracle Data Guard (см. [10]).
Разграничение доступа	Oracle Database Vault (ODV), Oracle Label Security (OLS)	ODV реализует разделение доступа на основе реалмов (позиционируется как защита от администратора БД). OLS - мандатную модель ограничения доступа (метки безопасности). Обе опции Oracle DB Server Enterprise Edition
Аудит	Oracle Audit Vault	ПО третьих изготовителей.
Защита резервных копий данных	Oracle Secure Backup	Данная функциональность не требуется при использовании "Крипто БД"/"SafeData".

Как мы видим функциональность, реализуемую "Крипто БД"/"SafeData" можно реализовать, применяя несколько опций, предлагаемых Oracle. К плюсам подобного подхода можно отнести следующее:

- применение встроенных средств прозрачно для прикладных приложений и служебного ПО Oracle;
- все механизмы защиты (за исключением Oracle Audit Vault) интегрированы в ядро сервера БД, что позволяет избежать накладных расходов по производительности, свойственных наложенным средствам;
- имеется обширная база знаний по данному направлению;
- при использовании HSM определённых производителей возможно использование аппаратного ускорения шифрования.

Очевидные минусы:

- требуется Oracle DB Server Enterprise Edition + опции;
- накладные расходы на управление безопасностью со стороны администраторов;
- неавтоматизируемое управление ключами шифрования данных;
- значительная нагрузка на процессор при шифровании табличных пространств;
- значительная стоимость лицензий и техподдержки.

Сравнение стоимости

Стоимость реализации защиты для выполнения требований PCI-DSS приводится для справки, учитывается только стоимость оборудования (ключи), лицензий на ПО и техподдержки.

В качестве примера используется система, обрабатывающая данные карт и их держателей на 100 пользователей. Сервер БД - Oracle DB Server EE 11g, 2 Intel Xeon X 4. Объем таблицы с PAN > 100M записей.

Для «Крипто БД»/«SafeData» (на основании розничного прайс-листа Ключи, Лицензии):

Позиция	Количество	Цена ($)	Стоимость ($)
Ключ Java 72K USB	100	30	3000
Лицензия клиента SafeData	100	42	4200
Лицензия сервера SafeData	1	50000	50000
Техподдержка (22% от стоимости серверных лицензий, первый год включен в стоимость)	1	11000	0
		Итого	57200

Для продуктов Oracle (на основании розничного прайс-листа и сайта OraShop) [1]:

Позиция	Количество	Цена ($)	Стоимость ($)
Oracle Advanced Security option (ASO)	4 [2]	11500	46000
Техподдержка ASO	4 [2]	2530	10120
Oracle Database Vault (ODV)	4 [2]	11500	46000
Техподдержка ODV	4 [2]	2530	10120
		Итого	122240

[1] Без учета лицензий Oracle Label Security ($11500 * 4 = $46000, + ТП $10120) и Audit Vault ($57500 (один процессор) + ТП $12650 (один процессор)).
[2] Количество процессоров = число процессоров * число ядер * 0.5 = 4. См. Расчет числа процессоров.

Дополнительные и справочные материалы

1. PCI DSS (PCI Data Security Standard) v.2.0.
2. PA-DSS (Payment Application Data Security Standard).
3. RFC 4357. Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms.
4. RFC 4490. Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS).
5. RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
6. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1.
7. RFC 5830. GOST 28147-89: Encryption, Decryption, and Message Authentication Code (MAC) Algorithms.
8. RFC 5831. GOST R 34.11-94: Hash Function Algorithm.
9. RFC 5832. GOST R 34.10-2001: Digital Signature Algorithm.
10. Решения Oracle для PCI DSS (eng).
11. Лучшие практики VISA. Шифрование полей данных (eng).
12. Додохов А.Л., Сабанов А.Г. Исследование применения СУБД Oracle для защиты персональных данных. Журнал «Доклады ТУСУР», №2(24), 2011г., стр.267-270.