УДК 004.089

А.Л. Додохов, А.Г. Сабанов

Исследование применения СУБД Oracle для защиты персональных данных

Рассмотрена задача возможности применения СУБД Oracle для хранения и обработки персональных данных. Показано, что встроенные средства шифрования не удовлетворяют требованиям российских регуляторов. Сделан вывод о необходимости разработки наложенных средств шифрования в соответствии с ГОСТ 28147–89 для применения в государственных органах и учреждениях.

Ключевые слова: СУБД Oracle, шифрование, персональные данные.

Актуальность. В связи с выходом Федерального закона от 25 июля 2011 г. №261-ФЗ «О внесении изменений в Федеральный закон №152-ФЗ «О персональных данных» в настоящее время остро стоит задача защиты персональных данных граждан, хранящихся в базах данных государственных органов. Поскольку самое широкое распространение для хранения данных в государственных органах имеет СУБД Oracle, необходимо исследовать данную СУБД на предмет соответствия требованиям законодательства и современного состояния нормативной документации. Для этого подробно рассмотрим встроенные алгоритмы шифрования Oracle TDE.

Опция «прозрачного» шифрования данных Oracle Transparency Data Encryption (TDE)

Термины и определения

Табличное пространство (tablespace) – логическая единица хранения структур и данных в Oracle. Представляет собой группы файлов, идентифицируемых одним именем.

HSM (Hardware Security Module) **–** аппаратный модуль, снабженный криптопроцессором. Реализует функции безопасного хранения ключей, криптографические операции, их аппаратное ускорение.

Wallet (бумажник) – файл, защищённый паролем (формат PKCS#12) для хранения ключей шифрования, паролей, а также личных ключей и сертификатов. Как правило, хранится в файловой системе сервера БД или АРМ'а клиента, но личный ключ может быть сохранён и в HSM.

Варианты использования TDE

TDE входит в состав опции Oracle Advanced Security с версии 10g. Позволяет «прозрачно» для приложений шифровать данные на уровне колонок таблиц или табличных пространств (с версии 11g).

TDE на уровне колонок

Работа TDE на уровне колонок выглядит следующим образом:

- приложение обращается к зашифрованной колонке;
- сервер БД определяет по словарю данных, что колонка зашифрована;
- сервер БД извлекает из словаря данных зашифрованный ключ шифрования данной колонки;
- сервер БД расшифровывает ключ шифрования колонки с помощью мастер-ключа;
- сервер БД расшифровывает или зашифровывает данные ключом колонки в зависимости от типа доступа (чтение/запись).

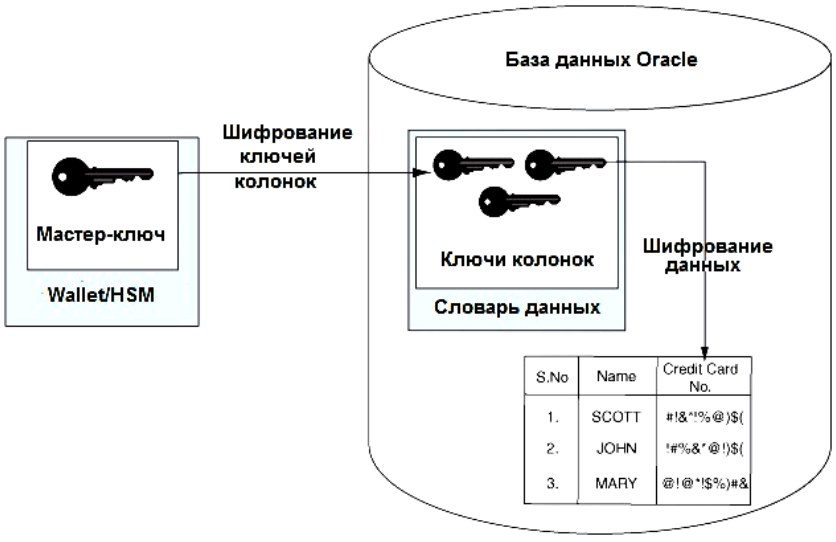

Рис. 1. Шифрование с помощью TDE на уровне колонок

Условия для прозрачного шифрования на уровне колонки:

- должен быть создан wallet;
- в wallet должен быть создан мастер-ключ;
- wallet с мастер-ключом должен быть «открыт», т.е. сделан доступным для сервера БД;
- колонки таблиц должны быть зашифрованы.

TDE на уровне табличных пространств

Работа TDE на уровне табличных пространств выглядит следующим образом:

- приложение обращается к колонке таблицы, размещённой на зашифрованном табличном пространстве;
- сервер БД извлекает из словаря данных зашифрованный ключ шифрования данного табличного пространства;
- сервер БД расшифровывает ключ шифрования табличного пространства с помощью мастер-ключа;
- сервер БД читает зашифрованные блоки данных из файла, расшифровывает данные ключом табличного пространства и помещает в свой кэш для последующей обработки и отправки клиенту. В случае записи операция зашифрования происходит непосредственно при записи блоков данных в файл.

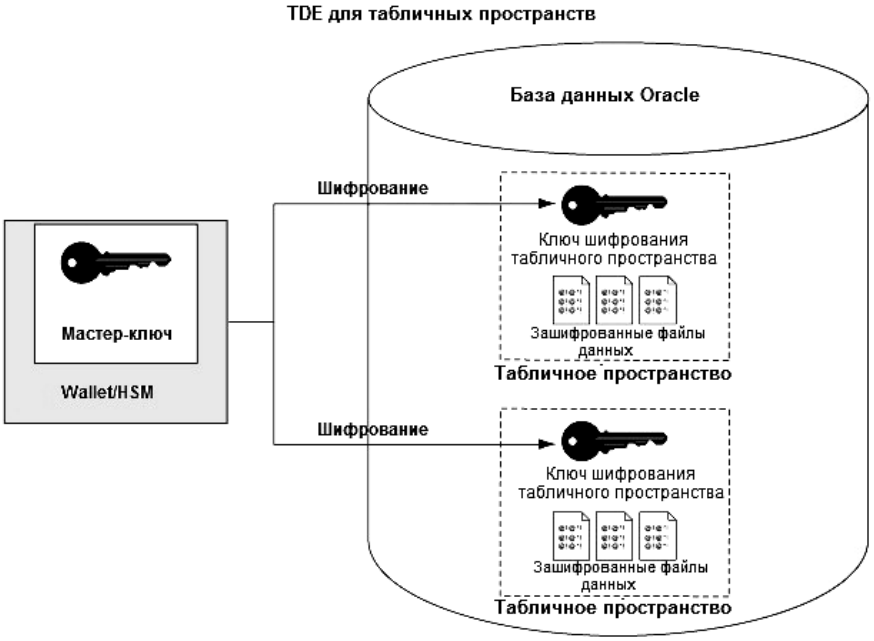

Рис. 2. Шифрование с помощью TDE на уровне табличных пространств

Условия для прозрачного шифрования на уровне колонки:

- должен быть создан wallet;
- в wallet должен быть создан мастер-ключ;
- wallet с мастер-ключом должен быть «открыт», т.е. сделан доступным для сервера БД;
- табличное пространства должны быть зашифрованы.

SQL-операторы для управления TDE

Задача	Команда SQL
Добавление колонки в существующую таблицу	ALTER TABLE <имя таблицы> ADD (<имя колонки> <тип данных колонки> ENCRYPT);
Создание таблицы с зашифрованной колонкой	CREATE TABLE <имя таблицы> (<имя колонки> <тип данных колонки> ENCRYPT)
Зашифрование существующей колонки	ALTER TABLE <имя таблицы> MODIFY (<имя колонки> ENCRYPT)
Установка/переустановка мастер-ключа	ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY «password»
Установка/переустановка мастер-ключа с использованием пары ключей (личный и открытый)	ALTER SYSTEM SET ENCRYPTION KEY «certificate_ID» IDENTIFIED BY «password»
Wallet: открытие для доступа к мастер-ключу	ALTER SYSTEM SET ENCRYPTION WALLET OPEN IDENTIFIED BY «password»

Характеристики

Поддерживаемые алгоритмы шифрования

Алгоритм	Размер ключа, бит	Имя для TDE
Triple DES (Data Encryption Standard)	168	3DES168
AES (Advanced Encryption Standard)	128	AES128
AES	192 (используется по умолчанию)	AES192
AES	256	AES256

Ограничения TDE для защиты колонок

Возможные типы данных колонки:

- BINARY_DOUBLE;
- BINARY_FLOAT;
- CHAR;
- DATE;
- INTERVAL DAY TO SECOND;
- INTERVAL YEAR TO MONTH;
- LOBs (Internal LOBs and SECUREFILE LOBs Only);
- NCHAR;
- NUMBER;
- NVARCHAR2;
- RAW;
- TIMESTAMP (includes TIMESTAMP WITH TIME ZONE and TIMESTAMP WITH LOCAL TIME ZONE);
- VARCHAR2.

Ограничения по длине данных

Тип данных	Максимальная длина незашифрованных данных (байт)
CHAR	1932
VARCHAR2	3932
NVARCHAR2	1966
NCHAR	966

Прочие ограничения:

- не поддерживается шифрование колонок, входящих в индекс, отличный от B-tree;
- не поддерживается Range scan по индексу;
- не поддерживается шифрование внешних больших объектов (BFILE);
- Synchronous Change Data Capture;
- не поддерживается шифрование таблиц на перемещаемых табличных пространствах;
- не работают утилиты экспорта/импорта (exp/imp).

Ограничения TDE для защиты табличных пространств

- Не поддерживается шифрование внешних больших объектов (BFILE).
- Не работают утилиты экспорта/импорта (exp/imp).

Общие замечания по применению TDE для защиты АС. TDE является средством защиты данных, но не разделения доступа. То есть когда wallet открыт, то любой получивший доступ к БД будет иметь доступ к зашифрованным данным. Иными словами, шифрование с помощью TDE защищает от таких угроз, как кража файлов данных, носителя и т.п., и только при условии, что вместе с носителем не был украден wallet с опцией Autologin.

Заключение. Встроенные в СУБД Oracle алгоритмы криптографии, применяемой для защиты данных, ключей шифрования, контроля целостности не соответствуют требованиям законодательства РФ. Встраивание внешних криптоалгоритмов разработчиками Oracle не предусмотрено. Для применения СУБД Oracle для защиты персональных данных необходима разработка наложенных средств шифрования в соответствии с требованиями регуляторов. Наиболее предпочтительными будут разработки средств шифрования, использующие алгоритмы ГОСТ 28147–89.

Додохов Александр Леонидович
Руководитель направления защиты баз данных ЗАО «Аладдин Р.Д.», г. Москва
Тел.: 8-903-585-94-34
Эл. почта: a.dodokhov@aladdin-rd.ru

Сабанов Алексей Геннадьевич
Канд. техн. наук, заместитель генерального директора ЗАО «Аладдин Р.Д.»
Эл. почта: a.sabanov@aladdin-rd.ru

Dodokhov A.L., Sabanov A.G.
Investigation of data privacy protection on Oracle data base use

In this article there is an investigation of opportunity of use Oracle embedded encrypting algorithms to data privacy protection. It is showed that Oracle embedded encrypting algorithms aren't sufficient to satisfy the requirements of Federal Defense Service. There is suggested a necessary to build an addition encrypting facilities GOST 28147–89 to use in government services and enterprises are designed.
Keywords: Oracle data base, encryption, data privacy.