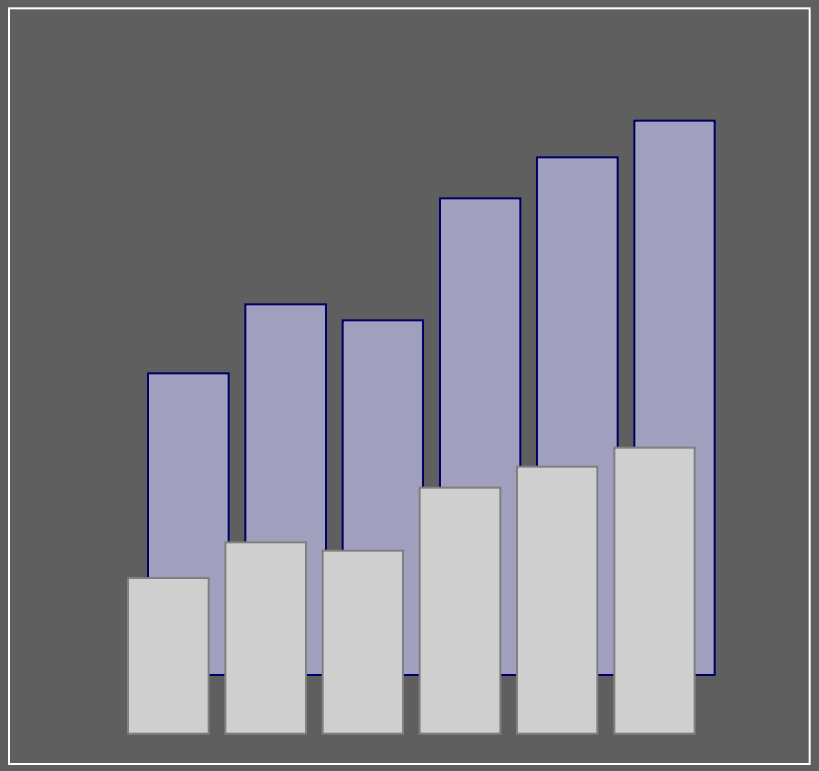
BUSINESS MAKING PROGRESS™

PROGRESS® 09

конференция пользователей

Transparent Data Encryption

OpenEdge 10.2B



Башкатов В.Г.
v.bashkatov@csbi.ru
www.openedge.ru

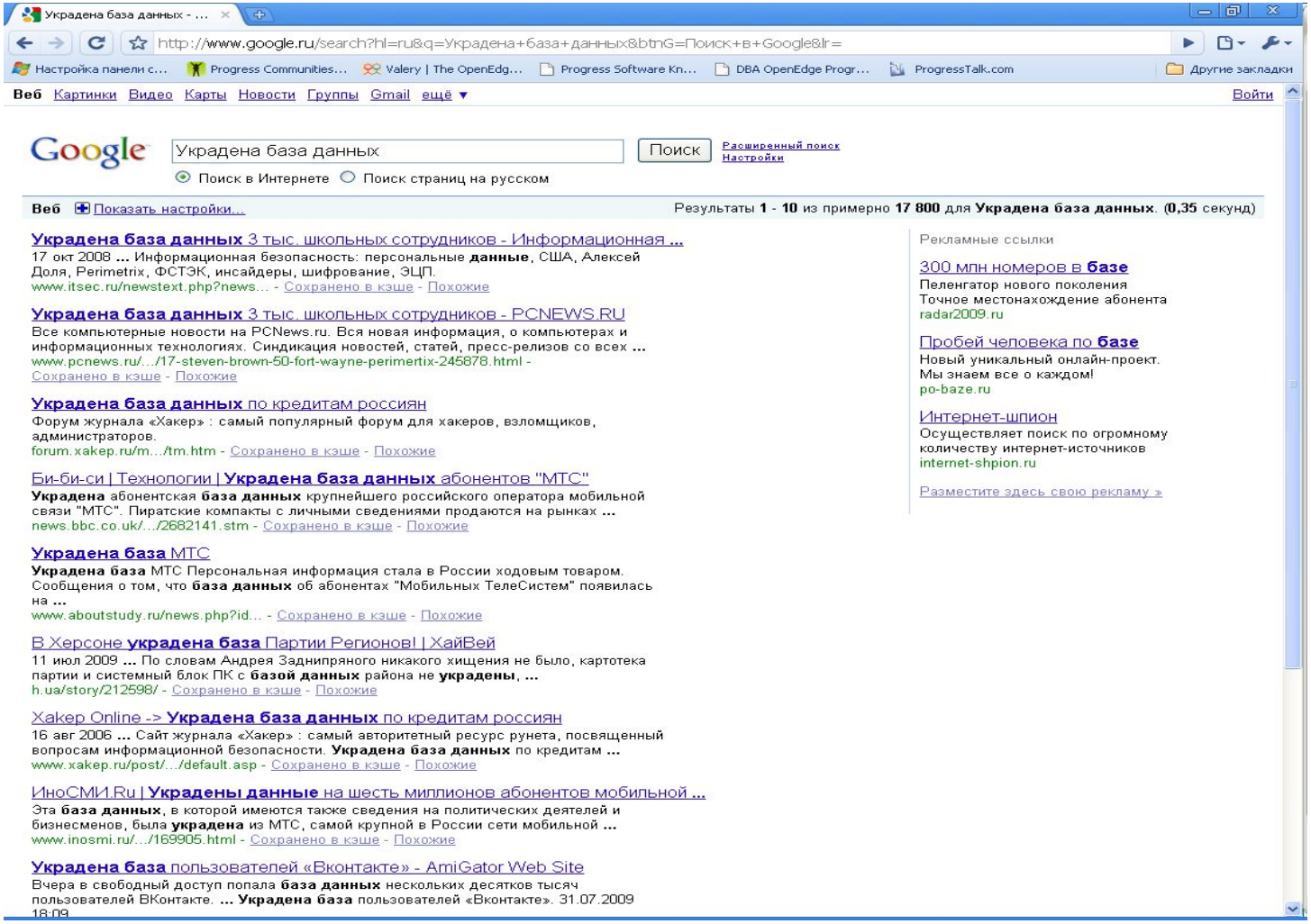
csbi bankier

Зачем необходимо шифрование базы данных?

- ✔ Защита бизнеса (примерно 65% компаний становятся банкротами вследствие утраты 20% служебной информации)
- ✔ Соблюдение законов

Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

Зачем необходимо шифрование базы данных?



Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

Что такое TDE?

1. **Прозрачность**
   - ❑ Без изменения приложения
   - ❑ Без перезагрузки данных
2. **Гибкость**
   - ❑ Шифрование конкретный объектов в области SAT-II
   - ❑ Шифрование конкретной области SAT-I
   - ❑ Шифрование блоков на диске
3. **Безопасность**
   - ❑ Поддержка хранилища ключей
   - ❑ Ограниченный доступ к физическим данным
   - ❑ Часть стратегии безопасности

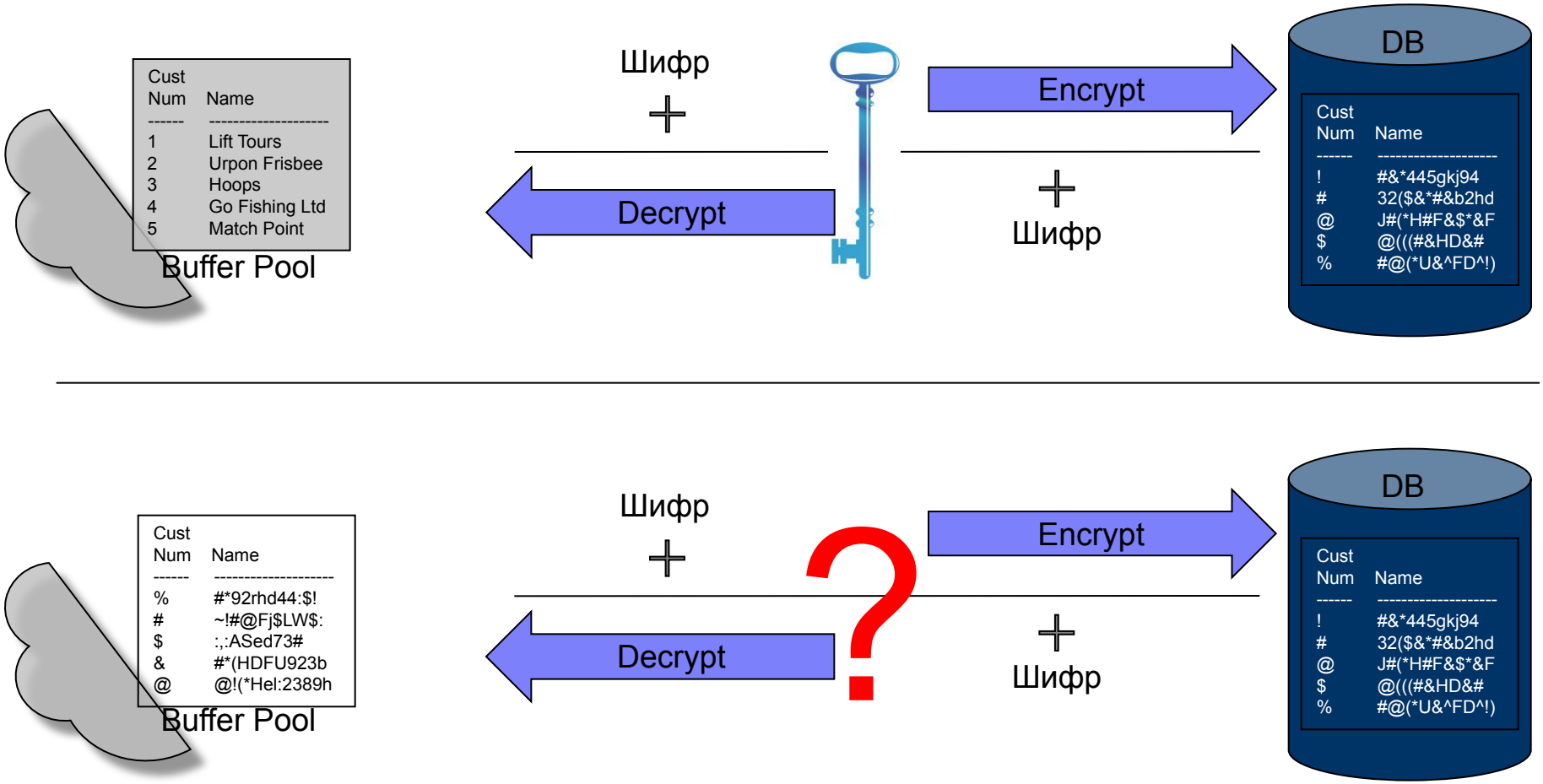
Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

OpenEdge TDE:

- Доступен начиная с 10.2B
- Отдельный продукт
- Лицензируется отдельно
- Необходима Enterprise лицензия

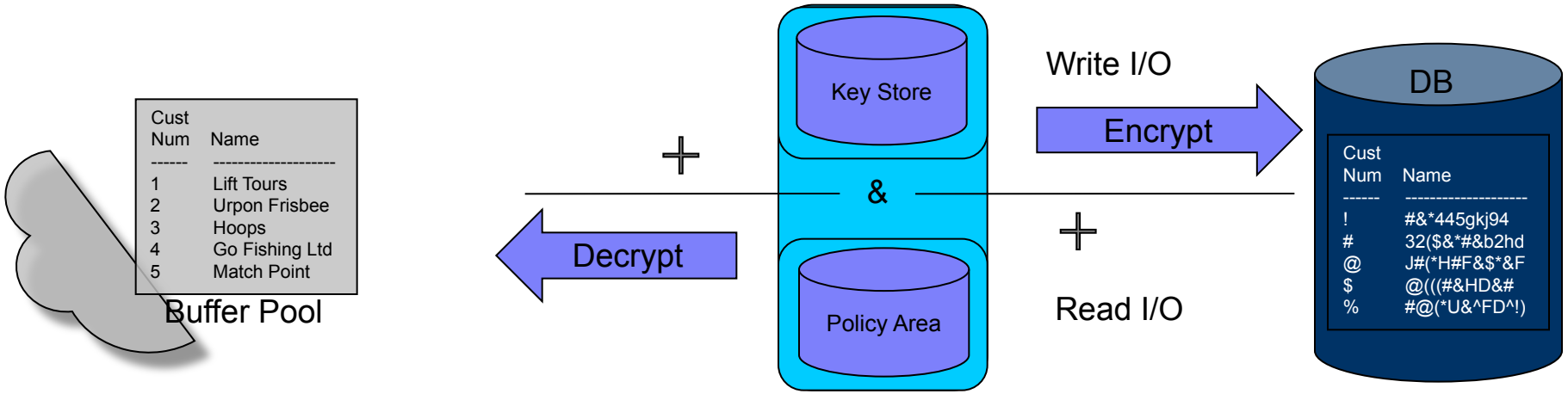
Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

Как работает TDE?



Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

Как работает TDE?



- Key Store
  - Database Master Key
  - Admin/User Passphrase
  - Manual/Automatic Authentication
- Encryption Policy Area
  - Encryption Policy – Что (объект) и Как (Шифр)

The Key Store

Уникальное название

- Имя файла: <dbname.ks>

Содержит Database Master Key (DMK)

- Обеспечивает уникальность зашифрованных данных

Обеспечивает безопасность DMK

- Хранилище отделено от базы данных
- Защита доступа к хранилищу на основе Passphrase
- Не входит в состав резервной копии (PROBKUP)

Your database backup is not complete until you have made an OS backup or copy of your keystore. (15525)

Почему?

Правила формирования Passphrase

- Количество символов: от 8 до 2048
- Набор символов: [a-zA-Z0-9]!@#$%^& *()_+-{}[]|\,./<>?;:<space>
- Минимальное количество целочисленных символов: 1
- Минимальное количество буквенных символов: 2
- Минимальное количество символов пунктуации: 1
- Максимальное количество повторяющихся символов: 0
- Использование верхнего и нижнего регистра: Да
- Чувствительность к регистру: Да

Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

Шифры DMK

ID	Шифр	Режим	Длина	Тип ключа
1	AES	CBC	128	BINARY
2	AES	CBC	192	BINARY
3	AES	CBC	256	BINARY
4	DES	CBC	56	BINARY
5	DES3	CBC	168	BINARY
6	DES	CBC	56	PBE
7	RC4	ECB	128	BINARY

Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

The Encryption Policy

Содержимое политики шифрования

- Объекты шифрования
  - ✔ Таблица, Индекс, LOB (SAT-II)
  - ✔ Область хранения (SAT-I)
  - ✔ AI/BI
- Шифр
  - ✔ Алгоритм
  - ✔ Длина ключа

Безопасность

- Отдельная область хранения (Encryption Policy Area)
- Защита от прямого доступа

Обслуживание

- EPOLICY MANAGE, Data Admin, OpenEdge SQL DDL
- Добавление, удаление, изменение ключа или шифра в online

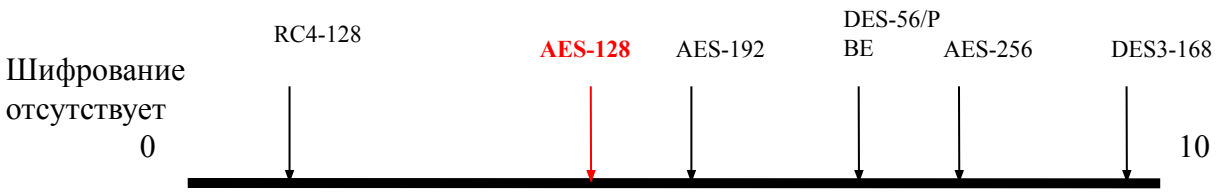
Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

Шифры политик шифрования

ID	Шифр	Режим	Длина	Тип ключа
0	NULL	NULL	-	-
1	AES	CBC	128	BINARY
2	AES	CBC	192	BINARY
3	AES	CBC	256	BINARY
4	DES	CBC	56	BINARY
5	DES3	CBC	168	BINARY
7	RC4	ECB	128	BINARY

Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

Выбор шифра



Шкала влияния на производительность

Шкала надежности алгоритма

- Политика безопасности
- Баланс между надежностью и производительностью

Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

Шаг №1: Включение шифрования.

1. Создайте новую область хранения SAT-II
   e **“Encryption Policy Area”**:12,**32**;**64** . f 1024
   e .

2. С помощью PROSTRC ADD/ADDONLINE добавьте область в базу

   prostrct add *mydb encrypt.st*

3. Обновите структурный файл базы данных

   prostrct list *mydb*

Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

Шаг №2: Включение шифрования.

proutil <*dbname*> **-C enableencryption**

[-Cipher <*cipher-num*>]

[-Autostart]

[-biencryption enable | disable]

[-aiencryption enable | disable]

- Будет усечен BI файл (offline)
- Будет создано хранилище ключей <dbname>.ks
- В область Encryption Policy Area будет загружена схема
- Будет запрошен Passphrase (User/Admin)
- Сгенерирован DMK
- Сгенерированы ключи для AI и BI, если не указано обратное
- Настроен Autostart
  - Manual/Automatic
- Появится возможность создания политик шифрования

- Шифрование данных не происходит!

Включение шифрования. Шаг №3.

Способы создания политик шифрования

- EPOLICY MANAGE
- Data Admin
- OpenEdge SQL DDL

Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

Шаг №3: Epolicy Manage

proutil <*dbname*> **-C epolicy manage** <*object-type*>
encrypt | cipher | rekey <*object-name*>
-Cipher < *num* >

$ proutil sports -C epolicy manage area encrypt "TestArea1"
Encryption policy setting for Area TestArea1 in Area 7 (15504)
Cipher specification setting to AES_CBC_128 completed. (15491)

$ proutil sports -C epolicy scan area "TestArea1"
OpenEdge Release 10.2B1B as of Thu Jul 30 19:00:21 EDT 2009
AREA TestArea1 / 7 CURRENT AES_CBC_128 V:0 **79 of 1784** blocks encrypted

---

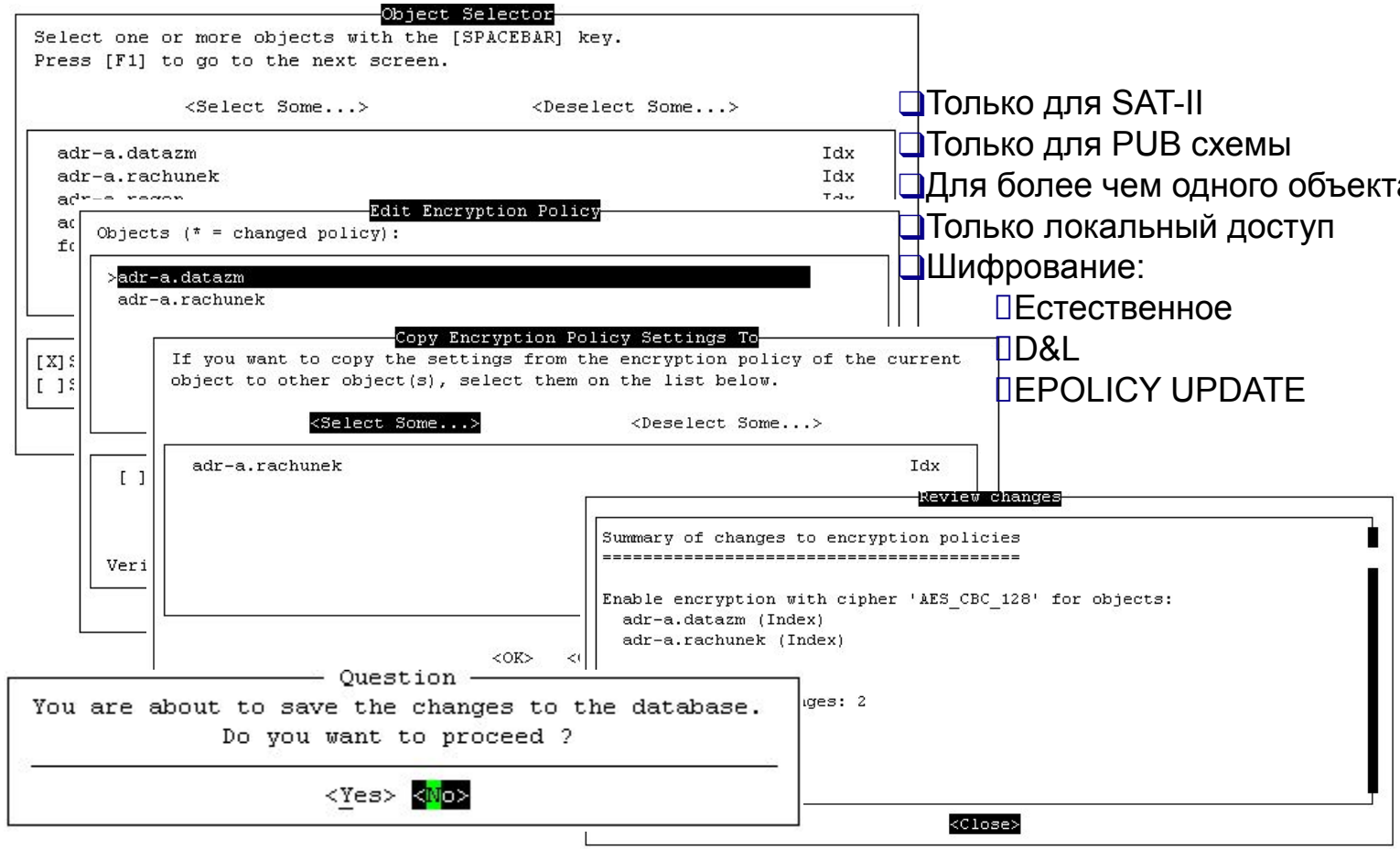
$ proutil sports -C epolicy manage area update "TestArea1"
OpenEdge Release 10.2B1B as of Thu Jul 30 19:00:21 EDT 2009
AREA TestArea1 / 7 CURRENT AES_CBC_128 V:0 1705 of 1784 blocks encrypted

---

- Шифрование области (object-type = Area) доступно только для SAT-I
- Объекты Table, Index, LOB должны размещаться в области SAT-II
- Данные могут быть зашифрованы тремя способами:
  - Естественный процесс шифрования
  - Dump & Load
  - PROUTIL EPOLICY MANAGE UPDATE

Шаг №3: Data Admin

Меню: Admin -> Security -> Encryption Policies -> Edit Encryption Policy



- Только для SAT-II
- Только для PUB схемы
- Для более чем одного объекта
- Только локальный доступ
- Шифрование:
  - Естественное
  - D&L
  - EPOLICY UPDATE

Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

Шаг №3: OpenEdge SQL DDL

```
CREATE TABLE PUB.enctab1
(encid int, encdes int, encdt varchar(25))
AREA "TestArea2"
ENCRYPT WITH 'AES_CBC_192';
COMMIT;
```

```
CREATE INDEX idx1
ON PUB.ENCTAB1
(encid ASC)
AREA "TestArea2"
ENCRYPT WITH 'AES_CBC_192';
COMMIT;
```

```
ALTER TABLE PUB.ENCTAB1
SET ENCRYPT WITH 'AES_CBC_128';
COMMIT;
```

```
ALTER TABLE PUB.ENCTAB1
SET ENCRYPT REKEY;
COMMIT;
```

```
ALTER TABLE PUB.ENCTAB1
SET DECRYPT;
COMMIT;
```

```
$ proutil sports -C epolicy manage table update ENCTAB1
```

SHOW ENCRYPT ON ALL [TABLE | INDEX | LOB];

OBJECT TYPE	OBJECT NAME	OBJECT TABLE	OBJECT OWNER	OBJECT ID	OBJECT POLICY STATE	OBJECT POLICY CIPHERSPEC	POLICY VERSION
TABLE	ENCTAB1	ENCTAB1	PUB	855	CURRENT	AES_CBC_192	0
INDEX	IDX1	ENCTAB1	PUB	2428	CURRENT	AES_CBC_192	0
AREA	TestArea1			7	CURRENT	AES_CBC_128	0

Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

Шаг №3: Data Definition File (.df)

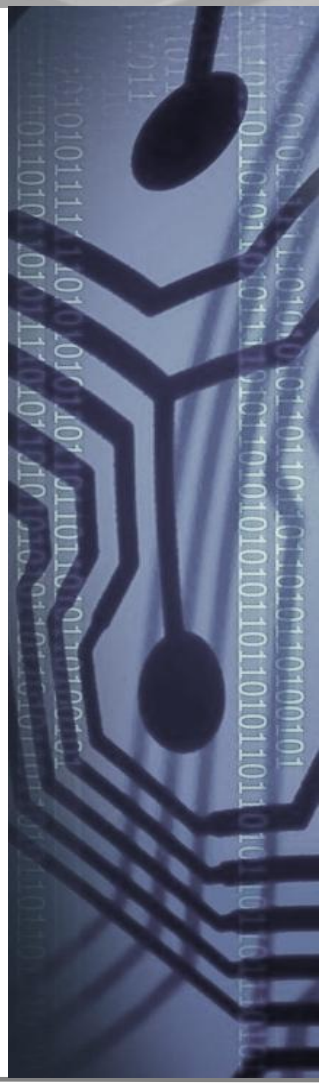
- **UPDATE TABLE**
  - **ENCRYPTION YES**
  - **CIPHER-NAME** ***<полное название шифра>***
- **DEFINITION TRAILER**
  - **encpolicy=yes**

```
ADD TABLE "ENCTAB1"
  AREA "TestArea2"
  DUMP-NAME "ENCTAB1"

ADD FIELD "ENCID" OF "ENCTAB1" AS integer
  FORMAT "->,>>>,>>9"
  INITIAL "?"
  POSITION 2
  MAX-WIDTH 4
  ORDER 10

ADD FIELD "ENCDT" OF "ENCTAB1" AS character
  FORMAT "x(8)"
  INITIAL "?"
  POSITION 4
  MAX-WIDTH 25
  LENGTH 0
  ORDER 30
  CASE-SENSITIVE

ADD INDEX "IDX1" ON "ENCTAB1"
  AREA "TestArea2"
  PRIMARY
  INDEX-FIELD "ENCID" ASCENDING

UPDATE TABLE "ENCTAB1"
  ENCRYPTION YES
  CIPHER-NAME AES_CBC_192


.
PSC
encpolicy=yes
cpstream=ibm866
.
0000000605
```

Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

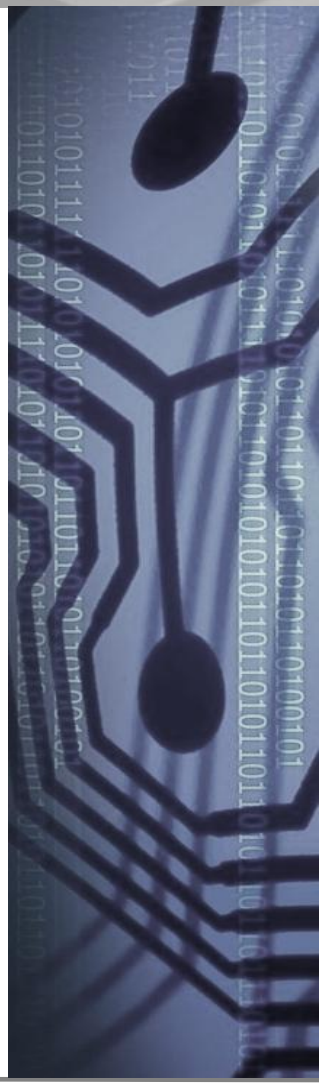
TDE и OpenEdge Replication

- TDE для Source и Target базы данных должен быть включен
- Шифрование BI для Target только после пересоздания Target
- Шифрование AI для Target включается автоматически Агентом репликации
- Номера областей Encryption Policy Area должны быть одинаковыми
- Хранилище ключей (*dbname.ks*), копируется с Source базы данных



Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

TDE и OpenEdge Replication



TDE для базы с OE Replication offline / online

1. Остановить Target базу данных
2. Добавить область Encryption Policy Area в Source и Target базы
3. Включить шифрование на Source базе
4. Настроить политики шифрования на Source базе
5. **Скопировать хранилище ключей (dbname.ks) с Source на Target**
6. Старт:
   - Source и Target базы данных.
   - Target

Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru

Выключение TDE

proutil <*dbname*> **-C epolicy manage** *object-type* **cipher** *object-name* **-Cipher 0**
proutil <*dbname*> **-C epolicy manage** *object-type* **update** *object-name*

proutil <*dbname*> **-C disableencryption**
[-Passphrase]
[
[-userid *userid*]
[-password *password*]
]

- Отключается шифрование BI (только в offline)
- Отключается шифрование AI
- Все данные расшифровываются
- Удаляются все политики шифрования
- Архивируется хранилище ключей, файл .ks переименовывается в .ksbk.

Производительность

1. **Показания Buffer Hit Rate**
   - Увеличьте Буферный пул (-B)
   - Используйте Альтернативный буферный пул для зашифрованных объектов (-B2)
2. **Нормализация данных**
   - Отделите конфиденциальную информацию от обычной
   - Используйте область с типом SAT-II
   - Тщательно выбирайте индексы для шифрования
3. **Тщательно выбирайте шифр (алгоритм + длина ключа)**
   - Баланс между безопасностью и производительностью

Санкт-Петербург, площадь Победы, 2 (812) 438.19.91, 371.00.22
Москва, проезд Ольминского, д.3а, стр.3 (495) 616.00.53, 616.00.54
http://www.csbi.ru info@csbi.ru
CSBI bankier

ВСПАСИБО ЗА ВНИМАНИЕ!

управляя информацией

OpenEdge 10.2B: Transparent Data Encryption

Башкатов Валерий Григорьевич
v.bashkatov@csbi.ru
www.openedge.ru