ORACLE APEX KONCEPT AUTENTIFIKACIJA

Damir Vadas
http://damir-vadas.blogspot.com

TEB Informatika d.o.o.
www.teb-informatika.hr

HROUG
Rovinj 10/2010

Koncept

- Autentifikacija
- Model podataka
- Model server side koda
- Model Apex koda
- Prezentacija mogućnosti
- Q and A

NAJVAŽNIJE PRAVILO

Nikada svojim postupcima ne smijete dovesti u opasnost integritet podataka baze!

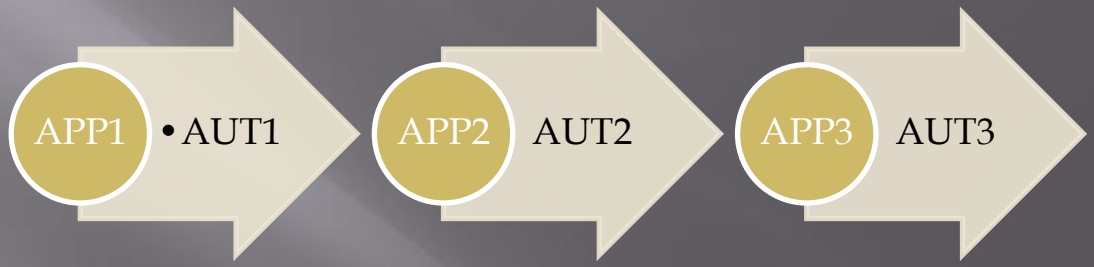
Autentifikacija

Jedna Apex aplikacija jedna autentifikacija

Preko Apex-a podržan „multi apps" ali samo na način kako je to zamislio Oracle bez jednostavne mogućnosti proširenja

Potreba za objedinjavanjem

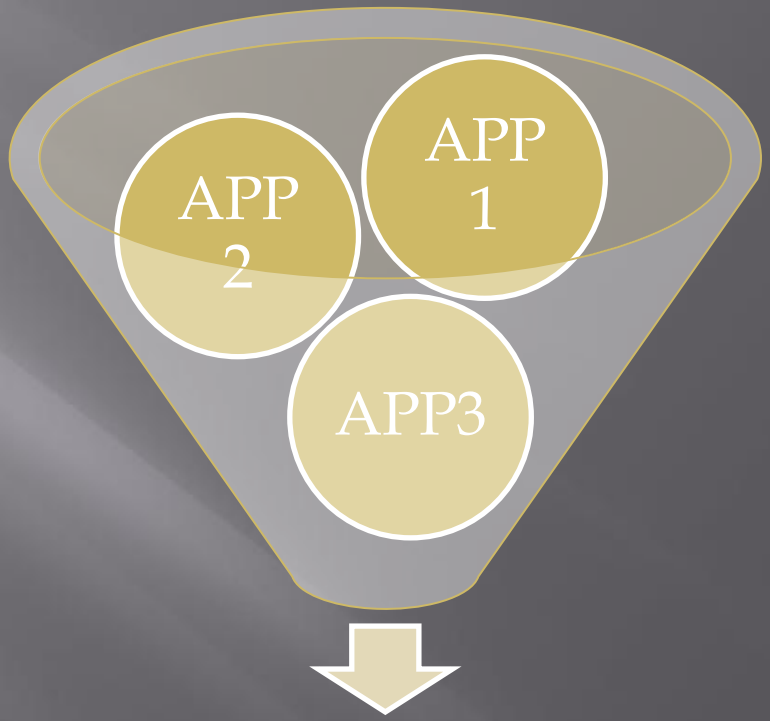
- Nemogućnost univerzalnosti sučelja
- Nemogućnost višestrukog login-a s istom lozinkom (1 pwd za više app)
- Problem održavanja i administracije općenito



Autentifikacija

Objedinjavanjem se postiže sve prije navedeno uz još neke napredne odlike

- Neovisnost od inačice Apex-a (ako promijene neke dijelove)
- Neovisnost od verzije baze
- Najviši stupanj sigurnosne politike



Jedna autentifikacija

U zasebnoj schemi-TOOLS

Model podatka

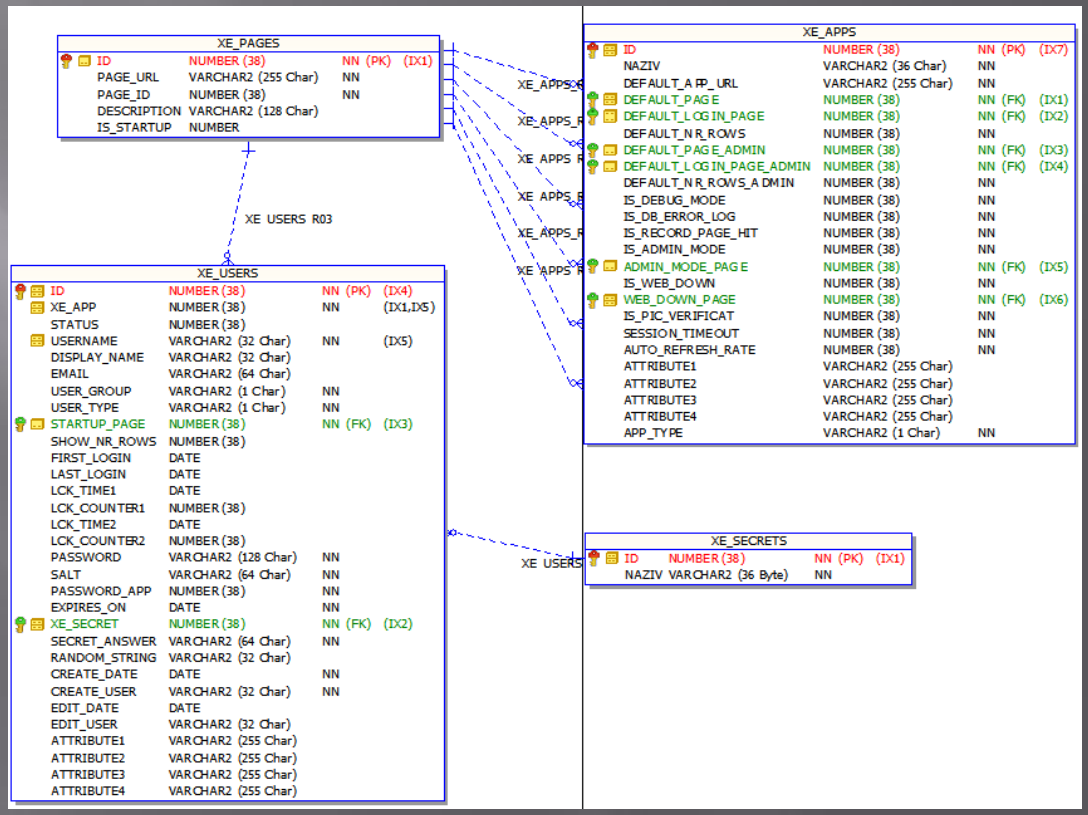
Model je jednostavan – samo 4 tablice

XE_USERS glavna tablica s podacima o korisnicima

XE_SECRETS-lookup tablica polja (xe_users.xe_secret)

XE_APPS-tablica s podacima o aplikacijama (xe_users.xe_app)

XE_PAGES-tablica s podacima o pojedinim stranicama



XE_SECRETS (01_xe_secrets.tbl)

```
ID      NUMBER(38) CONSTRAINT XE_SECRETS_ID_NN NOT NULL,
NAZIV   VARCHAR2(36 BYTE) CONSTRAINT XE_SECRETS_NAZIV_NN NOT NULL

COMMENT ON TABLE XE_SECRETS IS 'Tablica tajnih pitanja';
COMMENT ON COLUMN XE_SECRETS.ID IS 'Primarni kljuc tajnog pitanja';
COMMENT ON COLUMN XE_SECRETS.NAZIV IS 'Tajno pitanje';
```

XE_PAGES (02_xe_pages.tbl)

```
ID           NUMBER(38) CONSTRAINT XE_PAGES_ID_NN NOT NULL,
PAGE_URL     VARCHAR2(255 CHAR) CONSTRAINT XE_PAGES_PAGE_URL_NN NOT NULL,
PAGE_ID      NUMBER(38) CONSTRAINT XE_PAGES_PAGE_ID_NN NOT NULL,
DESCRIPTION  VARCHAR2(128 CHAR),
IS_STARTUP   NUMBER                              DEFAULT 0

COMMENT ON TABLE XE_PAGES IS 'Tablica u kojoj se upisuju stranice koje su znacajne za
aplikacije (login, web down, default page)';

COMMENT ON COLUMN XE_PAGES.ID IS 'Surogat key';
COMMENT ON COLUMN XE_PAGES.PAGE_URL IS 'WEB url stranice-klasican link';
COMMENT ON COLUMN XE_PAGES.PAGE_ID IS 'Ako je PAGE URL broj onda pokusa spremiti to
kao broj (za APEX stil rada and future compatibility...) 0 za neuspjeh';
COMMENT ON COLUMN XE_PAGES.DESCRIPTION IS 'Free from entry for that user';
COMMENT ON COLUMN XE_PAGES.IS_STARTUP IS 'Da li stranica može biti startup';
```

XE_APPS 03_xe_apps.tbl)

```
ID                      NUMBER(38) CONSTRAINT XE_APPS_ID_NN NOT NULL,
NAZIV                   VARCHAR2(36 CHAR) CONSTRAINT XE_APPS_NAZIV_NN NOT NULL,
APP_TYPE                VARCHAR2(1 CHAR)    DEFAULT 'J'                  NOT NULL,
DEFAULT_APP_URL         VARCHAR2(255 CHAR) CONSTRAINT XE_APPS_DEFAULT_APP_URL_NN NOT NULL,
DEFAULT_PAGE            NUMBER(38)     CONSTRAINT XE_APPS_DEF_PAGE_NN NOT NULL,
DEFAULT_LOGIN_PAGE      NUMBER(38)     CONSTRAINT XE_APPS_DEF_LOGIN_PAGE_NN NOT NULL,
DEFAULT_NR_ROWS         NUMBER(38)     DEFAULT 10 CONSTRAINT XE_APPS_DEF_NR_ROWS_NN NOT NULL,
DEFAULT_PAGE_ADMIN      NUMBER(38)     CONSTRAINT XE_APPS_DEF_PAGE_ADMIN_NN NOT NULL,
DEFAULT_LOGIN_PAGE_ADMIN NUMBER(38)    CONSTRAINT XE_APPS_DEF_LOGIN_PG_ADMIN_NN NOT NULL,
DEFAULT_NR_ROWS_ADMIN   NUMBER(38)     DEFAULT 30 CONSTRAINT XE_APPS_DEF_NR_ROWS_ADMIN_NN NOT NULL,
IS_DEBUG_MODE           NUMBER(38)     DEFAULT 0 CONSTRAINT XE_APPS_IS_DEBUG_MODE_NN NOT NULL,
IS_DB_ERROR_LOG         NUMBER(38)     DEFAULT 0 CONSTRAINT XE_APPS_IS_DB_ERROR_LOG_NN NOT NULL,
IS_RECORD_PAGE_HIT      NUMBER(38)     DEFAULT 0 CONSTRAINT XE_APPS_IS_RECORD_PAGE_HIT_NN NOT NULL,
IS_ADMIN_MODE           NUMBER(38)     DEFAULT 0 CONSTRAINT XE_APPS_IS_ADMIN_MODE_NN NOT NULL,
ADMIN_MODE_PAGE         NUMBER(38)     CONSTRAINT XE_APPS_ADMIN_MODE_PAGE_NN NOT NULL,
IS_WEB_DOWN             NUMBER(38)     DEFAULT 0 CONSTRAINT XE_APPS_IS_WEB_DOWN_NN NOT NULL,
WEB_DOWN_PAGE           NUMBER(38)     CONSTRAINT XE_APPS_WEB_DOWN_PAGE_NN NOT NULL,
IS_PIC_VERIFICAT        NUMBER(38)     DEFAULT 0 CONSTRAINT XE_APPS_IS_PIC_VERIFICAT_NN NOT NULL,
SESSION_TIMEOUT         NUMBER(38)     DEFAULT 300 CONSTRAINT XE_APPS_SESSION_TIMEOUT_NN NOT NULL,
AUTO_REFRESH_RATE       NUMBER(38)     DEFAULT 30 CONSTRAINT XE_APPS_AUTO_REFRESH_RATE_NN NOT NULL,
ATTRIBUTE1              VARCHAR2(255 CHAR),
ATTRIBUTE2              VARCHAR2(255 CHAR),
ATTRIBUTE3              VARCHAR2(255 CHAR),
ATTRIBUTE4              VARCHAR2(255 CHAR)
```

XE_USERS (04_xe_users.tbl)

```
ID              NUMBER(38) CONSTRAINT XE_USERS_ID_NN NOT NULL,
XE_APP          NUMBER(38) CONSTRAINT XE_APPLICATION_ID_NN NOT NULL,
STATUS          NUMBER(38)                    DEFAULT 1,
USERNAME        VARCHAR2(32 CHAR) CONSTRAINT XE_USERS_USERNAME_NN NOT NULL,
DISPLAY_NAME    VARCHAR2(32 CHAR),
EMAIL           VARCHAR2(64 CHAR),
USER_GROUP      VARCHAR2(1 CHAR)              DEFAULT 'U' CONSTRAINT XE_USERS_USER_GROUP_NN NOT NULL,
USER_TYPE       VARCHAR2(1 CHAR)              DEFAULT 'F' CONSTRAINT XE_USERS_USER_TYPE_NN NOT NULL,
STARTUP_PAGE    NUMBER(38) CONSTRAINT XE_USERS_STARTUP_PAGE_NN NOT NULL,
SHOW_NR_ROWS    NUMBER(38)                    DEFAULT 30,
FIRST_LOGIN     DATE,
LAST_LOGIN      DATE,
LCK_TIME1       DATE,
LCK_COUNTER1    NUMBER(38)                    DEFAULT 0,
LCK_TIME2       DATE,
LCK_COUNTER2    NUMBER(38)                    DEFAULT 0,
PASSWORD        VARCHAR2(128 CHAR) CONSTRAINT XE_USERS_PASSWORD_NN NOT NULL,
SALT            VARCHAR2(64 CHAR) CONSTRAINT XE_USERS_SALT_NN NOT NULL,
PASSWORD_APP    NUMBER(38) CONSTRAINT XE_USERS_ONE_PASSWORD_NN NOT NULL,
EXPIRES_ON      DATE      DEFAULT (ADD_MONTHS(SYSDATE,1200)) CONSTRAINT XE_USERS_EXPIRES_ON_NN NOT NULL,
XE_SECRET       NUMBER(38) CONSTRAINT XE_USERS_SECRETS_ID_NN NOT NULL,
SECRET_ANSWER   VARCHAR2(64 CHAR) CONSTRAINT XE_USERS_SECRET_ANSWER_NN NOT NULL,
RANDOM_STRING   VARCHAR2(32 CHAR),
CREATE_DATE     DATE CONSTRAINT XE_USERS_DATKRE_NN NOT NULL,
CREATE_USER     VARCHAR2(32 CHAR) CONSTRAINT XE_USERS_KORKRE_NN NOT NULL,
EDIT_DATE       DATE,
EDIT_USER       VARCHAR2(32 CHAR),
ATTRIBUTE1      VARCHAR2(255 CHAR),
ATTRIBUTE2      VARCHAR2(255 CHAR),
ATTRIBUTE3      VARCHAR2(255 CHAR),
ATTRIBUTE4      VARCHAR2(255 CHAR)
```

Model podatka

- PUBLIC sinonimi (ako ih se već definira) trebali bi biti drugog imena od pripadnog objekta (skrivanje)

```
SQL> desc tbl_pages
Name                                      Null?    Type
----------------------------------------- -------- ------------------
ID                                        NOT NULL NUMBER(38)
PAGE_URL                                  NOT NULL VARCHAR2(255 CHAR)
PAGE_ID                                   NOT NULL NUMBER(38)
DESCRIPTION                                        VARCHAR2(128 CHAR)
IS_STARTUP                                         NUMBER

SQL> desc xe_pages
Name                                      Null?    Type
----------------------------------------- -------- ------------------
ID                                        NOT NULL NUMBER(38)
PAGE_URL                                  NOT NULL VARCHAR2(255 CHAR)
PAGE_ID                                   NOT NULL NUMBER(38)
DESCRIPTION                                        VARCHAR2(128 CHAR)
IS_STARTUP                                         NUMBER
```

- Ali to ne preporučujem!
  Sve raditi kroz „code interface”

Model podatka

- Iz svake scheme (aplikacije) niti jedan podatak se ne bi trebao vidjeti:

```
SQL> select * from tools.xe_users;
select * from tools.xe_users
              *
ERROR at line 1:
ORA-00942: table or view does not exist
```

- ATTRIBUTEx (x=1..5) polja omogućuju proširenje modela bez redefiniranja objekta (princip iz eBS-a)

Model koda

- Kod je podijeljen u dva dijela
  - „CORE" dio
    - Dio koji je zajednički za mnogo šire radnje koje koriste mnogi drugi moduli
  - „XE_AUTH" dio
    - Dio koji je namijenjen samo autentifikaciji („XE" prefiks, eBS način imenovanja objekata)
- Ideja je sav bitan kod držati na jednom mjestu
- Kod je sučelje prema svim APEX/JAVA aplikacijama

Model koda

Ovaj kod koriste i neke druge (non Apex) aplikacije

Ako package nije definiran s „AUTHID CURRENT_USER" onda razmisliti o izradi proxy fcja/proc koje imaju izoliranu metodu a ne GRANT na cijeli package (security issue primjerice DEBUG_PKG i navedene procedure)

- TOOLS „CORE" dio
  - Packages:
    - BOOL
    - COMMON_PKG
    - TOOLS_PKG
    - DEBUG_PKG
  - Procedures:
    - AUTO_LOG_ERROR_JAVA
    - AUTO_LOG_ERROR_XE_AUTH
    - TGBIU_APEX
    - AUTO_LOG_ERROR_DEBUG

- TOOLS „XE_AUTH” dio
  - Packages:
    - XE_CRYPTO_PKG
    - XE_GLOBAL_PKG
    - XE_AUTH_PKG

Model koda

Problem „custom_auth“ (jednostruki HASH)-XE_AUTH stvar temeljena na privatnom i public key (kao kod PGP-a)

XE_CRYPTO wrapati i ne grantati nikome!

XE_GLOBAL sadrži globalne metode (primjerice mijenjanje jezika)

XE_AUTH glavni package

Sve funkcije vraćaju integer veći od nule (Java); u slučaju greške vraćaju negativne vrijednosti ORA greške

Model koda

- PUBLIC sinonimi trebali bi biti drugog imena od pripadnog objekta (skrivanje)

```
SQL> desc xe_global_pkg;
FUNCTION GET_XE_LANG RETURNS NUMBER(38)
PROCEDURE SET_XE_LANG
 Argument Name                  Type                    In/Out Default?
 ------------------------------ ----------------------- ------ --------
 AVALUE                         BINARY_INTEGER          IN

SQL> desc pkg_global;
FUNCTION GET_XE_LANG RETURNS NUMBER(38)
PROCEDURE SET_XE_LANG
 Argument Name                  Type                    In/Out Default?
 ------------------------------ ----------------------- ------ --------
 AVALUE                         BINARY_INTEGER          IN

SQL>
```

Model Apex koda

- Apex aplikacija komunicira isključivo preko poziva predefiniranih procedura/funkcija i package-a iz TOOLS scheme
- Sve bitne varijable učitavaju se samo jednom, nakon uspjele autentifikacije
- Varijable su zaštićene na dva načina:
  1. Definicija na server strani, nije moguće editiranje na klijentu (Application item -> Session State Protection->Restricted - May not be set from browser)
  2. Apex osiguranje (Application item -> Session State Protection->Checksum Required – Session Level)

Model Apex koda

- Nikada ne prikazujte vitalne podatke u browseru
  - USERNAME (za to koristite DISPLAYNAME)

```
IF #OWNER#.pkg_auth.IS_PUBLIC_USER THEN
  :APP_USER_DISPLAY := 'PUBLIC_USER';
ELSE
  :APP_USER_DISPLAY :=
#OWNER#.pkg_auth.get_user_display_name(:APP_USER);
END IF;
```

  - IP adrese sustava (klijent je OK)
  - Ostale podatke (bitne jedino adminima)

Prezentacija mogućnosti

- Preporuka koristiti #OWNER# u Apex-u (reusable kod za druge aplikacije u drugoj schemi!)
- Logout stranica neka ne bude login stranica (po mogućnosti ista ona koja je definirana „ Session Not Valid Page" opcijom)
- „Pre-Authentication Process" staviti
  :FSP_AFTER_LOGIN_URL := null
  ako se želi onemogućiti deep link
  (ne u ovom primjeru)
- Login stranica obvezno na „https" protokolu (Apache rule za korekciju http->https)

Prezentacija mogućnosti

- custom_auth (public-private key)
- Password management (change password)
  - User1 -> APP1 APP2 APP3 (3 ista passworda)
  - User2 -> APP1 i APP3 isti, APP2 posebni pasword
  - User3 -> APP1 APP2 APP3 (3 različita passworda)
- Locking counter management
  - 3 login failure X minuta timeout
  - Još 3 login failure X day timeout (send mail na usera?)
  - Admin može resetirati lock (ali najbolje kroz sučelje a ne direktno nad tablicama)

Prezentacija mogućnosti

- STARTUP_PAGE i SHOW_NR_ROWS
- External login (Forms, Java ili druga Appex) iz vanjske aplikacije (uporaba ATTRIBUTE1). Primjer poziva iz forme

```
declare
   var1 PLS_INTEGER;
   v_url VARCHAR2(1024);
BEGIN
   IF XE_AUTH_PKG.generate_autologin_data(1,v_url) = 1 THEN
     :block3.url := v_url ;
     var1:=DDE.App_Begin('C:\Program Files\Internet
Explorer\iexplore.exe '||v_url,DDE.APP_MODE_MAXIMIZED);
     DDE.App_Focus(var1);
  END IF;
END;
```

- David Copperfield is not dead!