



BAKALÁŘSKÁ PRÁCE

**Bezpečnost dat v
databázových systémech
Oracle®**

**Data security in Oracle® Database
Systems**

Tomáš Houžvička

Unicorn College © 2010

Unicorn College, V Kapslovně 2767/2, Praha 3, 130 00

Název práce v ČJ: Bezpečnost dat v databázových
systémech Oracle®

Název práce v AJ: Data security in Oracle® Database
Systems


Autor: Tomáš Houžvička

Akademický rok: 2010

Kontakt: E-mail:
tomas.houzvicka@seznam.cz
Tel.: (+420 602281682)

1 ZADÁNÍ

ZADÁNÍ ZÁVĚREČNÉ BAKALÁŘSKÉ PRÁCE (ZBP)

Název ZBP v češtině	Bezpečnost dat v databázových systémech Oracle
Název ZBP v angličtině	Data security in Oracle database
Studijní obor	 ICT Project Management
Akademický rok	2009/2010
Vedoucí závěrečné práce	Miroslav Žďárský
Termín odevzdání Zadání ZBP	16.10.2009
Termín odevzdání práce ZBP	07.05.2010

Cíl závěrečné bakalářské práce

Cílem práce je ukázat možnosti zabezpečení dat v databázích Oracle a analyzovat jejich účinnost a dopady na provoz a použití databáze.

Základní literatura

Bezpečnost v Oracle - Marlene Theriault, Aaron Newman

Mistrovství v Oracle - Kevin Loney, Marlene Theriault

Oracle® Database Security Guide - Patricia Huey

2 ABSTRAKT

Většina moderních informačních systémů je založena na třívrstvé architektuře, která se skládá z prezentační, aplikační a datové vrstvy. Datová vrstva, která spravuje data v informačních systémech, je nejčastěji realizována relačními databázemi. Databázové systémy obsahují velké množství dat, která mohou být zneužita v případě, že se dostanou do nepovolaných rukou, proto je potřeba klást důraz na jejich zabezpečení. Jedním z největších dodavatelů databázových systémů je společnost Oracle®¹, která si podle společnosti Gartner®² dlouhodobě udržuje dominantní postavení na trhu komerčně vyvíjených databázových systémů. Proto jsem se zaměřil na produkt Oracle® Database System verze 11g.

Cílem mojí práce bylo zjistit, jak je možné zabezpečit databázi Oracle® Database System 11g. Jaké k tomu nabízí prostředky a jestli je možné těmito prostředky pokrýt všechna běžná rizika. Zejména mne zajímalo, zda je možné data v databázi Oracle® Database System 11g zabezpečit proti útokům takzvaných „insiderů“³.

První část je věnována pojmu „insider“, jaká jsou doporučovaná opatření proti jejich útokům na informační systémy a jak mohou být tato opatření realizována pomocí prostředků Oracle® Database System 11g.

Druhá část se zabývá jednotlivými bezpečnostními možnostmi Oracle® Database System 11g.

První kapitola druhé části je věnována autentizaci uživatelů. Možnosti, které Oracle® Database System 11g nabízí, jsou bohaté. Od nejjednoduššího způsobu autentizace využitím uživatelského účtu v databázi a hesla až po možnost využít síťové autentizační protokoly, jako RADIUS, Kerberos, LDAP nebo SSL.

Druhá kapitola se zabývá možnostmi autorizace, to znamená řízením přístupu uživatelů k datům uloženým v databázi. V této oblasti nabízí databáze celou řadu prostředků pro řízení přístupu uživatelů k uloženým datům, jako jsou systémová nebo objektová práva a dále prostředky pro efektivní správu tohoto přístupu, jako jsou role.

1 Oracle® - Oracle je registrovaná ochranná značka společnosti Oracle Corporation a/nebo jejích poboček.

2 Gartner® - Gartner, Inc. Je světově uznávaná výzkumná a konzultační firma v oboru informačních technologií.

3 Insider – zaměstnanec nebo smluvní partner s autorizovaným přístupem do informačního systému.

Třetí kapitola popisuje možnosti zabezpečení síťové komunikace databáze se svým okolím. Databáze Oracle® verze 11g využívá velmi rozšířeného a široce podporovaného protokolu SSL a digitálních certifikátů.

Čtvrtá kapitola se zaměřuje na ochranu dat proti útokům privilegovaných uživatelů, to znamená databázových i jiných administrátorů. Databáze Oracle® nabízí dva účinné prostředky: Oracle® Database Vault, který rozděluje databázi do bezpečnostních zón a aplikuje rozdělení odpovědností a Oracle® Transparent Data Encryption, které chrání data při ukládání na paměťová média.

Pátá kapitola se zabývá možnostmi auditu přístupu uživatelů k datům uloženým v databázi a jak zabránit možné manipulaci se záznamy auditu ze strany administrátorů.

V závěru je konstatováno, že databáze Oracle® Database System 11g disponuje dostatečnými prostředky pro zabezpečení dat, pokud jsou tyto prostředky správně a důsledně používány a pokud jsou správně definována a aplikována pravidla rozdělení odpovědností.

Klíčová slova: bezpečnost, databáze, insider, Oracle®, Oracle® Database Vault, Transparent Data Encryption, audit

3 ABSTRACT IN ENGLISH

Most modern information systems are based on three layer architecture, which is comprised of presentation, application and data layers. The data layer, which manages data in information systems, is most frequently realized by relational databases. Database systems hold a lot of information, which could be abused in case they are accessed by an unauthorized person. That is why it has to be secured carefully.

One of the biggest suppliers of database systems is Oracle®⁴ Corporation, which by Gartner®⁵ has maintained a dominant position on the relational databases market. This was the reason why I decided to focus on Oracle® Database System 11g.

The point of my work was to find how to secure Oracle® Database System 11g. What instruments this database system offers and if they cover all common risks. Mainly I was interested in how it is possible to secure data in Oracle® Database System 11g against attacks from “insiders”.

In the first part of this document attention is paid to concept of “insider”⁶, what arrangements are recommended against attack from “insiders” and how can this recommendation be realized by instruments of Oracle® Database System 11g.

In the second part of this document attention is paid to security options of Oracle® Database System 11g.

The first chapter deals with user authentication. Possibilities of authentication in Oracle® Database System 11g are very rich. From basic authentication by inside database held user password to network authentication protocols like RADIUS, Kerberos, LDAP or SSL.

The second chapter is directed to the possibility of authorization, this means possibility of administering access of users to data in the database. In this area the database also offers a wide range of instruments such as system or object access rules and instruments “roles” for effective management of this access.

4 Oracle® - Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

5 Gartner® - Gartner, Inc. Is the world's leading information technology research and advisory company.

6 Insider - Current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system or data.

The third chapter describes the possibility of securing network communication of client with the database. Oracle® Database System 11g uses widely used and supported protocol SSL with combination of digital certificates.

The fourth chapter focuses on protection of data against attack by privileged users, this means database and other administrators. Oracle® Database System 11g offers two efficient tools - Oracle® Database vault, which divides the database into secure domains and implements separation of duty and Oracle® Transparent Data Encryption, which protects data when it is saved to storage.

The fifth chapter deals with the possibility of auditing of user access to data stored in the database and how it is possible to avoid manipulation of audit records from administrators side.

In the conclusion it is stated, that Oracle® Database System 11g offers a sufficient number of instruments for securing the database, if they are used correctly and consistently and if separation of duty is implemented.

Keywords: security, database, insider, Oracle®, Oracle® Database System, Oracle® Database Vault, Transparent Data Encryption, audit

4 PROHLÁŠENÍ

Prohlašuji, že svoji bakalářskou práci na téma Bezpečnost dat v databázových systémech Oracle® jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou v práci citovány a jsou též uvedeny v seznamu literatury a použitých zdrojů.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních, a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb.

V Praze dne 7.5.2010

.....

Tomáš Houžvička

5 PODĚKOVÁNÍ

Děkuji vedoucímu bakalářské práce Ing. Miroslavovi Žďárskému za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce.

6 OBSAH

1	Zadání.....	3
2	Abstrakt.....	4
3	Abstract in English.....	6
4	Prohlášení.....	8
5	Poděkování.....	9
6	Obsah.....	10
7	Úvod.....	11
8	Útoky NA Informační systémy.....	12
8.1	Kdo jsou „Insideři“.....	12
8.2	„Best practices“.....	13
9	Ochrana DAT Oracle® Database System 11g.....	15
9.1	Autentizace.....	15
9.1.1	Databázová autentizace a soubor hesel.....	15
9.1.2	Autentizace pomocí operačního systému.....	16
9.1.3	Síťová autentizace.....	16
9.2	Autorizace.....	18
9.2.1	Uživatelské účty.....	18
9.2.2	Profily.....	19
9.2.3	Schémata.....	19
9.2.4	Systémová oprávnění.....	19
9.2.5	Objektová oprávnění.....	20
9.2.6	Role.....	21
9.2.7	Virtuální Privátní Databáze.....	22
9.3	Zabezpečení síťové komunikace.....	22
9.3.1	SSL.....	22
9.3.2	Oracle® Wallet.....	24
9.3.3	Firewall.....	25
9.4	Ochrana dat proti útokům privilegovaných uživatelů.....	25
9.4.1	Oracle® Database Vault.....	26
9.4.2	TDE (Transparent Data Encryption).....	36
9.4.3	Fyzická bezpečnost.....	38
9.5	Audit.....	39
9.5.1	Audit příkazů.....	40
9.5.2	Audit oprávnění.....	40
9.5.3	Audit objektů schématu.....	40
9.5.4	Rozšířené možnosti auditu (Fine grained auditing).....	40
9.5.5	Oracle® Audit Vault.....	41
10	Závěr.....	42
11	Conclusion.....	44
12	Seznam použité literatury.....	45
13	Seznam použitých symbolů a zkratk.....	46
14	Seznam obrázků.....	47

7 ÚVOD

Všechny informační systémy jsou vystaveny útokům, které mají za cíl buď neoprávněné získání informací anebo narušení jejich dostupnosti. Počet těchto útoků stále roste. Podle [2010 CyberSecurity Watch Survey](#)^[1] více než jedna třetina z 526 respondentů zaznamenala v období mezi srpnem 2008 a červencem 2009 nárůst těchto útoků proti předchozímu roku. Ačkoli útoky zvenčí jsou častější, útoky zevnitř jsou pro vlastníka informačního systému nebezpečnější a větší-nou přinášejí i větší finanční ztráty. Útoky zevnitř jsou prováděny tzv. „insidery“. To jsou zaměstnanci nebo smluvní partneři, kteří mají výhodu znalosti prostředí i autorizovaného přístupu. Z uvedené studie nejen vyplývá, že velká část útoků je vedena zevnitř organizace, ale také, že v drtivé většině případů nejsou proti viníkům podnikány právní kroky. Je to proto, že organizace nemají žádnou nebo mají nedostatečnou evidenci nebezpečných aktivit uživatelů nebo nedokážou jednoznačně prokázat identitu uživatelů. Častým důvodem bývá strach ze ztráty dobrého jména organizace.

Po absolvování základního kursu, kde jsem se seznámil s relačními databázemi a absolvování navazujícího kursu zaměřeného na administraci a programování relačních databází společnosti Oracle® se mi zdálo seznámení se s možnostmi ochrany dat jako logický krok. Nejvíce mne zaujala otázka, jak zabezpečit data v databázi proti zneužití „insidery“ a zejména privilegovanými uživateli, jako jsou systémoví nebo databázoví administrátoři.

Cílem mojí práce je zjistit, jestli je možné data uložená v databázovém systému Oracle® Database systém 11g zabezpečit proti zneužití. Zaměřím se především na ochranu proti útokům tzv. „insiderů“ a zejména na privilegované uživatele, jako jsou systémoví nebo databázoví administrátoři. Budu se zabývat možnostmi autentizace, autorizace, zabezpečení síťové komunikace, ochraně dat proti neoprávněnému přístupu k datům privilegovanými uživateli a nakonec možnostmi auditu.

8 ÚTOKY NA INFORMAČNÍ SYSTÉMY

Jak jsem již bylo zmíněno v úvodu, tato práce se zaměřuje na zabezpečení dat v relačních databázích Oracle® Database System 11g. Zejména na zabezpečení dat proti útokům „insiderů“, to znamená současných i minulých zaměstnanců a smluvních partnerů organizace, která používá informační systém s relační databází. Zvláštní pozornost budu věnovat privilegovaným uživatelům.

Z výzkumu [2010 CYBERSECURITY WATCH SURVEY^{\[1\]}](#), kterou provedl CSO Magazine ve spolupráci s U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University a Deloitte vyplývá, kromě jiných, několik pro tuto práci zajímavých skutečností:

1. Počet bezpečnostních událostí neustále roste. To je pravděpodobně způsobeno jednak zvyšujícím se počtem informačních systémů, zvětšujícím se počtem jejich uživatelů a rostoucím trhem s nelegálně získanými informacemi.
2. Na celkovém počtu bezpečnostních událostí se významnou, v některých oblastech převažující měrou podílejí tzv. „insideři“. Tito uživatelé mají snadnější přístup k datům v informačních systémech, protože mají autorizovaný přístup a protože znají prostředí organizací a vědí, jak se k cenným informacím dostat.
3. V 72% zjištěných případů nenásledují právní kroky proti původcům bezpečnostních událostí. Organizace většinou nemají účinný systém evidence, pomocí něhož by mohly jednoznačně prokázat identitu uživatele a jeho činnosti v informačním systému. Dalším častým důvodem je obava ze zveřejnění a tím poškození dobrého jména a ztráty důvěry obchodních partnerů.

Z výše uvedeného vyplývá, že je potřeba věnovat zvláštní pozornost zabezpečení databázových systémů, protože v těch jsou často uchovávána citlivá data a je třeba se zaměřit nejen na útoky zvenčí, ale stejnou měrou na útoky zevnitř.

8.1 Kdo jsou „Insideři“

D.M.Cappeliho a A.P. Morea v prezentaci Best Practices For Mitigating Insider Threat uvedené na RSA Konferenci 2009^[2] definují „insidera“ jako „Současného nebo bývalého zaměstnance, smluvního nebo obchodního partnera, který má nebo měl autorizovaný přístup do sítě, systému

nebo dat organizace, a úmyslně překročil nebo nesprávně použil tento přístup, který negativně ovlivnil důvěrnost, celistvost nebo dostupnost informací organizace nebo informačních systémů.“

Podle téhož zdroje jsou nejčastějšími hrozbami „insiderů“ podvod, krádež intelektuálního vlastnictví a sabotáž IT technologií.

8.2 „Best practices“

D.M.Cappeli a A.P. More uvádějí v prezentaci Best Practices For Mitigating Insider Threat uvedené na RSA Konferenci 2009 tyto návody pro odvrácení hrozeb nejen „insiderů“:

1. Počítejte s riziky pocházejících od „insiderů“ a obchodních partnerů při provádění celofiremního hodnocení rizik. (Consider threats from insiders and business partners in enterprise-wide risk assessments.)
2. Jasně dokumentujte a důsledně uplatňujte plány a regulace. (Clearly document and consistently enforce policies and controls.)
3. Zaveďte pravidelné bezpečnostní školení pro všechny zaměstnance. (Institute periodic security awareness training for all employees.)
4. Sledujte a reagujte na podezřelé nebo nebezpečné chování od začátku náborového procesu zaměstnanců. (Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process.)
5. Počítejte s útoky insiderů ve vývojovém cyklu software. (Consider insider threats in the software development life cycle.)
6. Buďte zvláště opatrní v případě administrátorů a technických nebo privilegovaných uživatelů. (Use extra caution with system administrators and technical or privileged users.)
7. Zaveďte systém kontroly změn. (Implement system change controls.)
8. Zaznamenávejte, monitorujte a auditujte činnosti zaměstnanců. (Log, monitor, and audit employee online actions.)
9. Předcházejte a řešte problémy na pracovištích. (Anticipate and manage negative workplace issues.)
10. Sledujte a zabezpečte prostředí organizace. (Track and secure the physical environment.)
11. Zaveďte přísná pravidla pro vytváření hesel a správu účtů. (Implement strict password and account management policies and practices.)

12. Prosazujte rozdělení odpovědností a nejmenších možných práv. (Enforce separation of duties and least privilege.)
13. Používejte vícevrstvou obranu proti vzdáleným útokům. (Use layered defense against remote attacks.)
14. Po výpovědi pracovníka ihned zrušte všechny jeho přístupy. (Deactivate computer access following termination.)
15. Zavedte bezpečný systém zálohování a obnovy. (Implement secure backup and recovery processes.)
16. Zpracujte plán opatření proti útokům insiderů. (Develop an insider incident response plan.)

Řadu uvedených doporučení je možné aplikovat přímo nástroji, které nabízí Oracle® Database System 11g.

Pro aplikaci pravidla 6. - „Buďte zvlášť opatrní v případě administrátorů a technických, nebo privilegovaných uživatelů“ - je vhodné použít DB Vault.

Pro aplikaci pravidla 8. - „Zaznamenávejte, monitorujte a auditujte činnosti zaměstnanců“ - jsou určeny nástroje pro audit.

Pro aplikaci pravidla 11. - „Zavedte přísná pravidla pro vytváření hesel a správu účtů“ - lze použít profily uživatelských účtů.

Pro aplikaci pravidla 12. - „Prosazujte rozdělení odpovědností a nejmenších možných práv“ - je také součástí Oracle® Database Vault.

Pro aplikaci pravidla 15. - „Zavedte bezpečný systém zálohování a obnovy“ - použít Oracle® Recovery Manager.

9 OCHRANA DAT ORACLE® DATABASE SYSTEM 11G

V této části práce se budu zabývat možnostmi, které nabízí Oracle® Database systém 11g v oblasti zabezpečení. Jsou to možnosti, které je možné využít nejen proti útokům „insiderů“, ale v podstatě proti útokům prováděným odkudkoli a kýmkoli. Nebudou zde uváděny příklady použití a používané příkazy, protože k tomu je k dispozici celá řada publikací a není cílem této práce vytvářet manuál pro administrátory. Příklad použití uvedu pouze v části „Ochrana dat proti útokům privilegovaných uživatelů“, kde budu demonstrovat možnosti Oracle® Database Vault.

9.1 Autentizace

Řízení přístupu uživatelů k datům uloženým v databázích je prováděno na základě jejich identity, která je reprezentována uvnitř databázového systému uživatelským účtem. První krok, který je potřeba učinit, je ověřit totožnost uživatele a tím jeho oprávnění k přístupu k datům. Uživatelem, který se autentizuje nemusí být pouze konkrétní osoba, ale může to být i jiný systém nebo zařízení.

9.1.1 Databázová autentizace a soubor hesel

První možností autentizace uživatelů je databázová autentizace. Uživatelské účty a jejich hesla jsou uloženy přímo v databázi. Výhodou tohoto způsobu autentizace je, že není závislý na žádných dalších systémech. Databáze Oracle® poskytuje prostředky k zajištění používání silných hesel. (viz. Profily). Tento způsob je zpravidla používán u samostatných databází s malým počtem uživatelů.

Zvláštní kapitolu tvoří účty správce databáze. Tyto účty musí fungovat i v okamžiku, kdy databáze ještě není dostupná, tedy v okamžiku před jejím spuštěním nebo v okamžiku provádění offline zálohování. Pro tyto účely používá databáze Oracle® soubor hesel. Soubor hesel obsahuje seznam databázových uživatelů i s jejich hesly, kteří mohou provádět operace spuštění a zastavení databáze, zálohování databáze apod. Jedná se o účty uživatelů s oprávněními SYSDBA, SYSOPER a SYSASM. Protože se jedná o soubor s velmi citlivými informacemi z hlediska bezpečnosti, je nutné věnovat velkou pozornost správnému nastavení přístupových práv v operačním systému.

9.1.2 Autentizace pomocí operačního systému

V případě použití autentizace prostředky operačního systému, se v databázi neukládají uživatelská hesla. Databáze v tomto případě předpokládá, že když se uživatel dokázal autentizovat v operačním systému, je autentizován i v databázi. Správci využívající autentizaci operačního systému přihlašující se k databázi s oprávněním SYSDBA nebo SYSOPER, musí být členy skupiny operačního systému DBA nebo OPER. Pokud je databáze vypnutá nebo v módu MOUNT, používá se autentizace pomocí souboru hesel nebo operačního systému. Autentizace pomocí operačního systému má přednost před autentizací pomocí souboru hesel.

9.1.3 Síťová autentizace

Autentizace s použitím síťové služby je další možnost autentizace uživatelů v databázi Oracle Database System 11g. Na výběr je hned z několika možností. Nevýhodou je závislost na funkčnosti dalšího systému. Výhodou je naopak daleko větší škála autentizačních metod.

9.1.3.1 SSL (Secure Socket Layer)

SSL (Secure Socket Layer) je protokol, který byl původně vyvinut společností Netscape Communications Corporation. Umožňuje jednak zabezpečit přenos dat po síti ale také autentizovat obě strany komunikace. SSL může být kombinováno a autentizací pomocí certifikátů (viz. PKI).

9.1.3.2 DCE (Distributed Computing Environment)

DCE (Distributed Computing Environment) je multiplatformové prostředí, které poskytuje velké množství různých služeb, jako jsou časové služby, souborové služby, vzdálené volání procedur a autentizace. Také podporuje technologii SSO (Single sign-on). Pokud se uživatel autentizuje v prostředí DCE, může používat databáze Oracle®, které byly nakonfigurovány pro prostředí DCE bez nutnosti opakované autentizace.

9.1.3.3 Kerberos

Kerberos je síťový autentizační protokol, který umožňuje stranám komunikujícím na nezabezpečené síti bezpečně vzájemně ověřit jejich identitu. Je multiplatformní a také umožňuje SSO. Databáze Oracle® Database System 11g může být například nakonfigurována tak, že autentizuje uživatele vůči MS Active Directory. V Oracle® Database System 11g je podporován Kerberos v5.

9.1.3.4 PKI (Public Key Infrastructure)

PKI (Public Key Infrastructure) je systém správy a distribuce veřejných klíčů využívaných v asymetrické kryptografii. Systém asymetrického kryptování je využíván k autentizaci, zaručení integrity a privátnosti zpráv a nepopiratelnosti transakce pomocí elektronického podpisu.

Asymetrické kryptování využívá dvojice klíčů. Privátní klíč, který musí uživatel chránit, a veřejný klíč, který naopak dává k dispozici ostatním. Tento veřejný klíč je distribuován pomocí PKI. Pro dvojici klíčů platí, že pokud nějakou zprávu zašifrujeme veřejným klíčem příjemce, může být tato zpráva dešifrována pouze privátním klíčem příjemce a nikým jiným. Problém, jak zabezpečit důvěryhodnost veřejného klíče, řeší certifikáty a digitální podpis. Digitální podpis je podobný jako dříve popisovaný postup šifrování zprávy, ale používá k zašifrování privátní klíč certifikační autority a k dešifrování její veřejný klíč. Certifikát je veřejnou autoritou – CA (Certification Authority), které důvěřujeme, podepsaný veřejný klíč s informací o tom, kdo je vlastníkem tohoto veřejného klíče. CA tedy svým privátním klíčem podepíše kontrolní součet veřejného klíče třetí strany společně s informací, kdo je vlastníkem tohoto veřejného klíče a tím vytvoří certifikát. Pravost certifikátu může být ověřena použitím veřejného klíče CA.

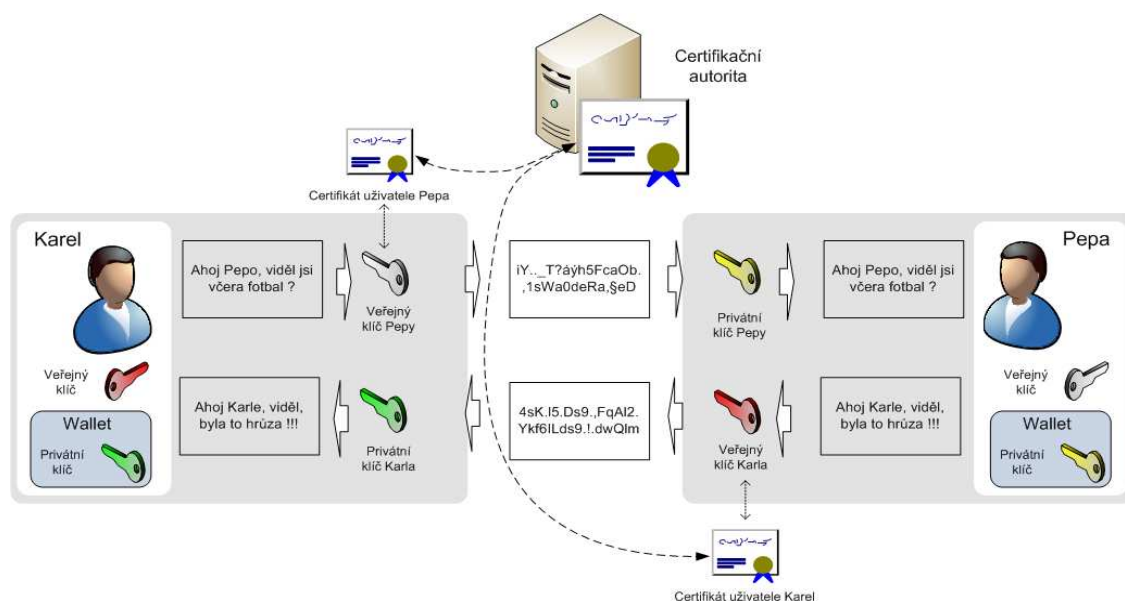
PKI používá následující komponenty:

Certifikační autoritu – vydává certifikáty potvrzující identitu vlastníka certifikátu.

Certifikáty – podepsaný veřejný klíč vlastníka certifikátu.

CRL (Certificate Revocation List) – seznam neplatných certifikátů

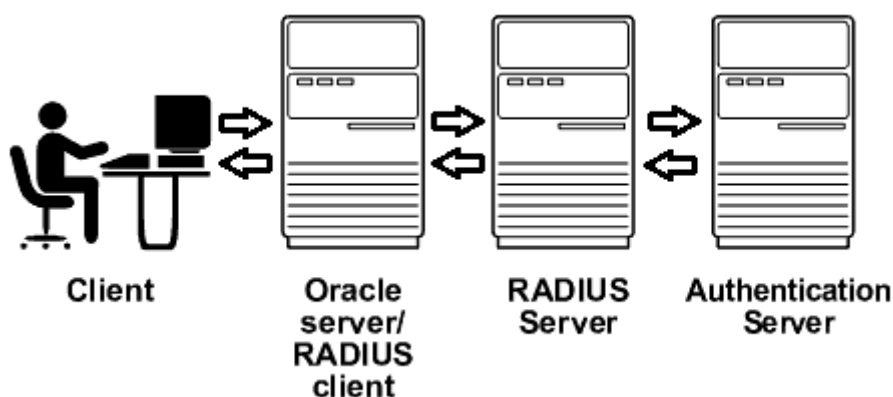
Wallet – kontejner k ukládání privátních klíčů, certifikátů apod. pro potřeby SSL.



Obr.1 PKI – šifrovaná komunikace

9.1.3.5 RADIUS

RADIUS (Remote Authentication Dial-In User Service) je klient/server protokol ,který se používá pro autentizaci, autorizaci a účtování služeb. Oracle® Database System server zde vystupuje v roli prostředníka mezi klientem a RADIUS serverem, který pro autentizaci může navíc využívat externí autentizační server. Pro autentizaci tak mohou být takto využity i Smart karty, Tokeny nebo biometrické způsoby autentizace. Změna autentizační metody je pro klienta, tomto případě Oracle® Database System server, transparentní.



Obr.2 RADIUS v prostředí Oracle® Databáze

(zdroj: Oracle® Database Advanced Security Administrator's Guide 11g Release 1)

9.2 Autorizace

V této části se bude popsáno, jaké možnosti nabízí databáze Oracle® Database System 11g v řízení přístupu uživatelů k datům a také, jaké prostředky nabízí k usnadnění administrace těchto oprávnění.

9.2.1 Uživatelské účty

Identita uživatele je v databázi představována jeho uživatelským účtem. Dříve, než je uživateli umožněn přístup k datům, musí být ověřena jeho identita. Způsoby, jak autentizovat uživatele, byly popsány v předchozí kapitole. Při vytváření uživatelského účtu mohou být kromě jména a způsobu autentizace nastaveny další parametry. Například jeho implicitní tabulkový prostor, dočasný tabulkový prostor, omezení objemu dat, který může uživatel ukládat v jednotlivých tabulkových prostorech apod. Následně jsou uživatelskému účtu přiřazena systémová nebo objektová

oprávnění která určují, se který daty mohou pracovat a jaké operace s nimi mohou provádět. Uživatelskému účtu je vždy přiřazen nějaký profil.

9.2.2 Profily

Protože každý databázový systém disponuje pouze omezenými systémovými prostředky, jako je například výkon procesorů nebo diskového subsystému, nabízí databáze Oracle® Database System 11g možnost omezit spotřebu těchto prostředků. Pojmenovaná sada těchto omezení se jmenuje profil. V profilu je možné nastavit nejružnější omezení týkající se uživatelského účtu. Například počtu současných připojení jednoho uživatele k databázi, maximální doby nečinnosti připojení k databázi, nebo velikosti alokované operační paměti.

Kromě omezování systémových prostředků nabízí profil možnost uplatnit pravidla pro vytváření uživatelských hesel. Profil může zajistit vynucení požadavků na složitost hesla, jako minimální délku, maximální nebo minimální dobu platnosti a dalších parametrů. Pokud není administrátor spokojen se standardně nabízenými parametry pro tvorbu hesel, je možné v profilu aktivovat parametr PASSWORD_VERIFY_FUNCTION. Tento parametr obsahuje jméno funkce, která provádí kontrolu dodržování zvolených pravidel pro vytváření hesel. Tuto funkci definuje administrátor a může do ní aplikovat své specifické požadavky. Každý profil může obsahovat jinou funkci kontroly hesel.

Při vytváření je uživatelskému účtu přiřazen výchozí profil DEFAULT, pokud není specifikován jiný, a tím jsou nastavena všechna pravidla tak, jak je uvedeno v profilu. Současně může v databázi existovat více profilů pro aplikaci rozdílných omezení různým skupinám uživatelů.

9.2.3 Schémata

Schéma je skupina databázových objektů vlastněných jedním uživatelem. Při vytváření uživatelského účtu je automaticky vytvořeno schéma se stejným jménem. Schéma je vlastněno tímto uživatelem a uživatel má všechna práva pro objekty ve schématu. Objekty patřící do schématu jsou logické struktury vytvořené uživatelem pro jeho data. Tyto struktury jsou například tabulky, pohledy nebo indexy.

9.2.4 Systémová oprávnění

Systémová oprávnění jsou oprávnění provádět akce nad jakýmkoli objektem databáze, nebo jsou to oprávnění týkající se například změny systémových parametrů, spouštění úloh, vytváření indexů, nastavení připojení k databázi nebo vytváření rolí (viz Role). Systémová oprávnění

jsou přidělována nebo odebírána konkrétnímu uživateli nebo roli. Také mohou být přidělena skupině PUBLIC, což je skupina zahrnující všechny uživatele databáze. Při přidělování systémového oprávnění je možné uživateli, kterému je toto oprávnění přidělováno, dát právo toto oprávnění přidělovat i jiným uživatelům. Systémová oprávnění jsou velmi silná, proto je důležité používat je opatrně. Opatrnost vyžaduje zejména přidělování práva ANY. Například přidělením práva SELECT ANY TABLE získá uživatel možnost číst data z libovolné existující nebo budoucí tabulky v libovolném schématu.

9.2.5 Objektová oprávnění

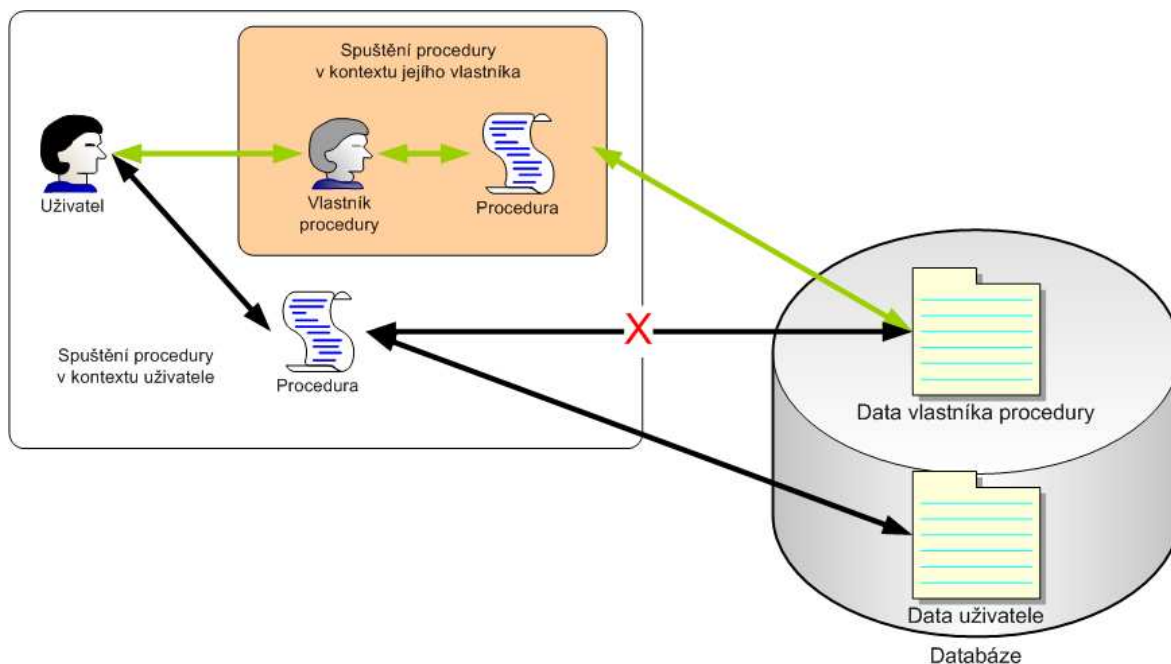
Objektová oprávnění jsou na rozdíl od systémových oprávnění práva provádět akce nad konkrétním objektem databáze. Jedná se o objekty, které nejsou ve vlastním schématu uživatele. Podobně jako u systémových oprávnění je možné objektová oprávnění přidělit konkrétnímu uživateli nebo skupině PUBLIC, pokud má být toto oprávnění přiděleno všem uživatelům v databázi. Také je možné přidělit objektové oprávnění s právem přidělovat toto oprávnění dalším uživatelům. Objektová oprávnění je možné přidělovat pro tabulky, pohledy nebo procedury.

Oprávnění pro tabulky databáze jsou dvojího druhu: operace definice dat (DDL – data definition language) a operace manipulace s daty (DML – data manipulation language). Operace definice dat jsou například vytváření nebo mazání tabulek a indexů, přidávání nebo mazání sloupců v tabulce. Jsou to tedy operace měnící strukturu dat. Operace manipulace s daty jsou například operace vyhledávání, vkládání, změny nebo mazání dat v tabulkách. Jedná se tedy o operace s řádky tabulek. Oprávnění je možné přidělovat jak pro operace definice dat, tak pro operace manipulace s daty. Uživateli tedy může být omezeno oprávnění práce s tabulkou pouze na některé sloupce.

Oprávnění pro pohledy je podobné oprávněním pro tabulky. Pohled je pojmenovaný SQL dotaz, který je uložen v databázi. Pro vytvoření pohledu je nutné mít oprávnění vytvořit pohled a také oprávnění alespoň číst ze všech tabulek, které jsou použity v pohledu. Pokud má být pohled aktualizovatelný, je potřeba mít navíc i práva vkládání, aktualizace a mazání pro všechny tabulky použité v pohledu.

Oprávnění pro procedury je možné aplikovat na procedury, funkce nebo balíčky těchto procedur a funkcí. Jediné oprávnění je oprávnění spustit proceduru nebo funkci. Procedury nebo funkce je možné spustit v kontextu vlastníka, to je uživatele který tento objekt definoval, nebo v kontextu uživatele, který tuto funkci nebo proceduru volá. V případě spuštění v kontextu vlastníka jsou použita všechna jeho oprávnění pro objekty se kterými funkce nebo procedura pracuje, které má její vlastník. Uživatel spouštějící tuto funkci nebo proceduru musí mít pouze právo ji spustit, ale vůbec

nemusí mít žádná práva pro objekty se kterými funkce nebo procedura pracuje. Díky této vlastnosti je možné velmi účinně řídit přístup uživatelů k datům. Pokud je funkce nebo procedura spuštěna v kontextu uživatele který ji volá je nutné, aby měl všechna potřebná oprávnění pro všechny objekty se kterými funkce nebo procedura pracuje.



Obr.3 Spouštění procedur

9.2.6 Role

Správa přístupových práv uživatelů k objektům databáze je usnadněna použitím rolí. Role je pojmenovaná skupina systémových a objektových oprávnění, kterou je možné přiřadit uživateli nebo dalším rolím. Jméno role musí být v rámci databáze unikátní a nesmí být stejné jako jméno uživatelského účtu. Pro správce databáze je snazší přidělovat práva uživatelským účtům prostřednictvím rolí, protože jen jednou nastaví systémová nebo objektová práva roli a tu potom přiřazuje jednotlivým účtům. V případě změny nemusí měnit nastavení pro všechny dotčené účty, ale stačí tuto změnu provést pouze v nastavení role. Stejně jako uživatelský účet může být použití role autorizováno heslem. Role přiřazené uživatelskému účtu mohou být v aktivním nebo neaktivním stavu. V aktivním stavu jsou účty přiřazena všechna oprávnění definovaná v roli, pokud ale role není v aktivním stavu, tato práva přiřazena nejsou. Pro aktivaci role je možné použít autorizační proceduru. Role je potom aktivována podle podmínek stanovených v této proceduře.

9.2.7 Virtuální Privátní Databáze

Kromě řízení přístupu uživatelů databáze k datům pomocí výše zmíněných možností nabízí databáze Oracle® Database System 11g vytvoření takzvané Virtuální Privátní Databáze (VPD). VPD umožňuje ještě jemněji určovat pravidla přístupu k datům v databázi a to nejen na úrovni sloupců tabulek, ale také na úrovni jednotlivých řádků. K této funkčnosti využívá dvou prostředků: aplikačního kontextu a zabezpečení na úrovni řádků. Důležitá vlastnost VPD je, že je zcela transparentní pro uživatele a funguje pro všechny operace manipulace s daty. VPD je metoda, jak například izolovat data několika organizací, oddělení nebo uživatelů v jedné databázi tak, že každý má pocit, že obsahuje pouze jeho data.

Aplikační kontext je sada atributů, které se používají při zajištění bezpečnostních zásad v průběhu relace uživatele. Atributy jsou nastaveny při připojení uživatele k databázi a mohou obsahovat nejrůznější hodnoty, jako název počítače klienta, jeho IP adresu, jméno uživatelského účtu v operačním systému, ze kterého se uživatel připojuje apod.

Zabezpečení na úrovni řádků umožňuje omezit přístup k záznamům v databázi na základě pravidel využívajících atributy aplikačního kontextu. Pravidla jsou implementována pomocí PL/SQL funkce vracející tzv. predikát. Predikát je řetězec, který je přidán k operaci manipulace s daty pomocí klauzule WHERE. Výsledkem je, že všechny operace manipulace s daty pracují pouze s podmnožinou dat danou predikátem.

9.3 Zabezpečení síťové komunikace

V dnešní době si lze jen těžko představit informační systém, který by nevyužíval síť pro komunikaci s uživateli nebo pro komunikaci mezi komponentami tohoto informačního systému. Velmi důležitou částí informačních systémů je databázový systém. Existuje mnoho způsobů, jak neoprávněně získat data přenášená po síti. Proto je potřeba přenosy dat po síti zabezpečit, ať se jedná o síť interní nebo veřejnou. V této části se bude popsáno, jak zabezpečit data přenášená po síti při komunikaci mezi klientem a databázovým serverem.

9.3.1 SSL

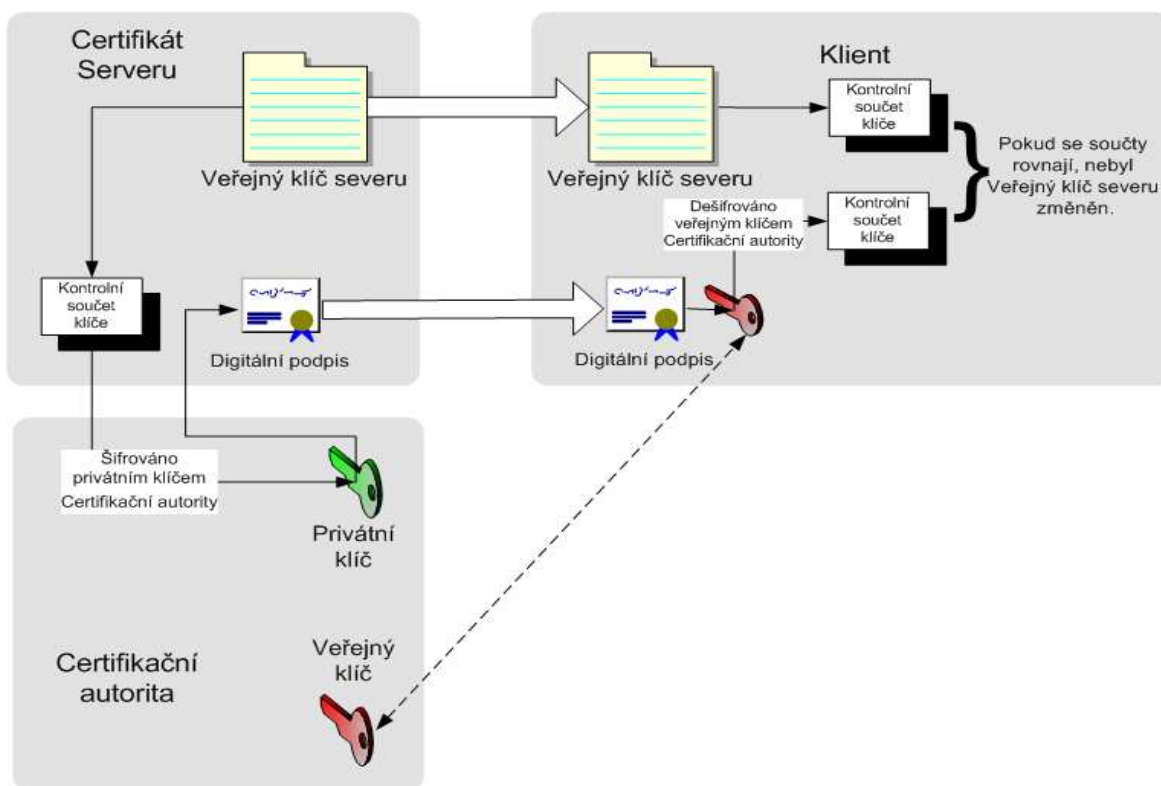
Jak již bylo zmíněno v kapitole o autentizaci, SSL (Secure Socket Layer) protokol byl původně vyvinut společností Netscape Communications Corporation. Později jeho vývoj převzala organizace IETF (Internet Engineering Task Force). SSL protokol byl rozšířen o další možnosti a

přejmenován na TLS (Transport Layer Security protocol). I když SSL a TLS poskytují stejné služby, jsou různě implementované, a proto protokoly SSL a TLS nejsou kompatibilní. Protokol TLS ale může pracovat v režimu kompatibilním s SSL. Služby, které protokoly nabízejí jsou: kontrola integrity, šifrování a ověřování identity. Výhodou SSL je, že jde o veřejný standard, který je široce rozšířen. V této části tedy bude popsán protokol SSL, ačkoli většina uvedených skutečností platí i pro TLS.

Podpora SSL a TLS je implementována Oracle® Advanced Security. Oracle® Advanced Security zajišťuje autentizaci použitím digitálních certifikátů, šifrování a kontrolu integrity. SSL zajišťuje ověřování identity pomocí digitálních certifikátů (viz PKI). Pokud má být při připojování klienta k databázi ověřována pouze identita serveru, stačí instalovat certifikát na straně serveru. Pokud má být ověřována identita serveru i klienta, musí být nainstalován certifikát nejen na serveru, ale i na všech klientech.

Komunikace mezi klientem a serverem je šifrována pomocí symetrických klíčů. Symetrické šifrování je použito proto, že má daleko menší nároky na výpočetní výkon komunikujících stran, než kdyby bylo použito asymetrické šifrování. Je ale nutné si tyto symetrické klíče bezpečně předat mezi komunikujícími stranami. Tento problém řeší asymetrické šifrování (viz PKI). Asymetrické šifrování zaručí bezpečné předání symetrických klíčů, ale nedokáže zaručit identitu komunikujících stran. Mohlo by se stát, že někdo si vygeneruje dvojici asymetrických klíčů a bude vydávat svůj veřejný klíč za klíč databázového serveru, aby získal autentizační údaje klienta. Takovému bezpečnostnímu útoku se říká man-in-the-middle⁷. Pro ověření identity komunikujících stran se používá certifikátů vydaných certifikační autoritou, které obě strany důvěřují. Certifikát vydaný certifikační autoritou obsahuje veřejný klíč klienta nebo serveru, informaci komu patří a jeho kontrolní součet zašifrovaný privátním klíčem této autority. Klient si pravost veřejného klíče ověří tak, že si spočítá kontrolní součet obsaženého veřejného klíče serveru, dešifruje kontrolní součet v certifikátu veřejným klíčem certifikační autority a porovná je. Pokud jsou kontrolní součty shodné, znamená to, že klíč v certifikátu nikdo nezměnil a patří skutečně tomu, kdo je uveden v certifikátu. Pokud komunikující strany důvěřují certifikační autoritě, důvěřují i veřejným klíčům, které tato certifikační autorita podepsala.

⁷ Man-in-the-middle – snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem.



Obr.4 Ověření veřejného klíče serveru pomocí certifikátu

Když je navazováno síťové spojení pomocí SSL, klient a server provádějí takzvaný SSL „handshake“, který má několik kroků. Nejdříve se klient a server dohodnou, které kryptovací algoritmy použijí. V dalším kroku server odešle svůj certifikát klientovi. Klient ověří, jestli byl certifikát ověřen certifikační autoritou, které důvěřuje. Pokud ano, je tím ověřena identita serveru a klient použije veřejný klíč serveru obsažený v certifikátu pro zašifrování náhodně vygenerovaného symetrického klíče a pošle ho serveru. Stejně, pokud je ověřována identita klienta, klient pošle svůj certifikát serveru a ten ověří, jestli byl podepsán důvěryhodnou certifikační autoritou. Pokud ano, také server použije veřejný klíč klienta obsažený v certifikátu pro zašifrování náhodně vygenerovaného symetrického klíče a pošle ho klientovi. Tyto klíče jsou pak používány pro symetrické šifrování komunikace mezi klientem a serverem, v každém směru jeden klíč. Aby byla zajištěna ještě větší bezpečnost takového symetrického šifrování, jsou tyto klíče pravidelně obměňovány stejným postupem.

9.3.2 Oracle® Wallet

Aby byl systém asymetrického šifrování bezpečný, musí být privátní část klíče bezpečně uložena. Stejně je nezbytné mít bezpečně uloženy vlastní certifikáty i certifikáty důvěryhodných certifikačních autorit. K tomuto účelu slouží Oracle® Wallet. Wallet je kontejner, zabezpečený hes-

lem, který obsahuje všechny tyto citlivé informace. Wallet je uložen v zašifrovaném souboru ewallet.der. Musí být před použitím otevřen pomocí hesla, které je nastaveno při vytváření tohoto kontejneru. Pro použití na serveru existuje ještě nezašifrovaná verze Walletu, který je vytvořen pokud povolíme automatické přihlašování a je uložena v souboru cwallet.sso. Protože je soubor nezašifrovaný, mohl by z něho každý jednoduše získat privátní klíč, proto musí být uložen v adresáři, kam má přístup pouze vlastník instance databáze a nikdo jiný.

Oracle® Wallet je používán nejen pro účely protokolu SSL, ale také pro TDE (Transparent data Encryption). TDE bude popsáno v další kapitole.

Pro bezpečné uložení privátního klíče je také možné použít Hardware Security Module. Hardware Security Module nejen uchovává privátní klíče jako Wallet, ale navíc provádí i vlastní kryptografické výpočty.

9.3.3 Firewall

Při zabezpečování síťové komunikace je používáno šifrování komunikace, jak bylo popsáno výše, ale také filtrování síťové komunikace mezi různými sítěmi. Toto filtrování je zajišťováno tzv. firewallem. Firewall je zařízení, kterým prochází síťový provoz a které na základě nastavených pravidel tento provoz propouští nebo nepropouští. V minulosti se firewally používaly nejčastěji k oddělení privátní sítě od veřejné sítě, jakou je například Internet. V současné době se zejména v sítích velkých organizací používají také interní firewally, které filtrují provoz na vnitřní síti. Toto opatření přináší větší bezpečnost databázových serverů proti útokům „insiderů“.

Kromě filtrování síťové komunikace pomocí firewallu, nabízí Oracle® Database System 11g možnost omezení připojení klientů k databázi na základě jejich IP adres. V konfiguraci listeneru⁸ databáze je možné specifikovat buď adresy, které se mohou připojit, nebo adresy kterým je připojení zakázáno. Toto nastavení se provádí přímo v konfiguračním souboru listeneru, kterým je sqlnet.ora.

9.4 Ochrana dat proti útokům privilegovaných uživatelů

Protože v databázových systémech jsou často ukládána data, která jsou považována za citlivá a mohou být zkopírována a zneužita, dostává se v posledních letech do popředí otázka, jak tato data zabezpečit. Mohou to být data nejrůznějšího charakteru, jako jsou informace o zdravotním stavu pacientů, čísla kreditních karet, informace o bankovních účtech nebo data získaná při

⁸ listener – proces databáze Oracle® Database System 11g který má za úkol přijímat od klientů požadavky na připojení.

vědeckém výzkumu. Na výrobce i provozovatele informačních systémů jsou proto kladeny požadavky na splnění bezpečnostních pravidel například ze strany oborových organizací, jako je PCI DSS (Payment Card Industry Data Security Standard) nebo nařízení Evropské unie a dalších.

Tato část se bude zabývat ochranou dat proti zneužití privilegovanými uživateli. Privilegovaným uživatelem je v Oracle® Database System například uživatel SYS. Takový super uživatel má všechna práva nad všemi objekty v databázi. Má tedy právo číst, měnit nebo mazat libovolná data v databázi. Pro administrátora je tedy velmi snadné získat data z jím spravovaných databázových systémů a ta následně modifikovat nebo poskytnout třetí straně.

9.4.1 Oracle® Database Vault

Oracle® nabízí k řešení tohoto problému Oracle® Database Vault, který umožňuje přesně nastavit přístup ke specifickým datovým oblastem v databázi všem uživatelům včetně administrátorů. Oracle® Database Vault nabízí prostředky k řešení nejpálčivějších bezpečnostních problémů dneška, jako je ochrana před útoky „insiderů“, naplnění požadavků bezpečnostních předpisů a rozdělení odpovědností.

V průběhu instalace Oracle® Database Vault jsou vytvořeny nové databázové role a databázové účty. Tyto role jsou součástí rozdělení odpovědností prováděným Oracle® Database Vault. Oracle® Database Vault provádí striktní oddělení správy účtů, správy bezpečnosti a správy zdrojů v databázi. Tím jsou všechna práva dosud společně přidělená privilegovaným uživatelům rozdělena mezi několik uživatelů, takže žádný z uživatelů nemá všechna práva. Současně jsou stávajícím privilegovaným rolím odebrána některá práva. Například rolím SYS a SYSTEM jsou odebrána práva vytvářet, měnit a mazat uživatelské účty a profily.

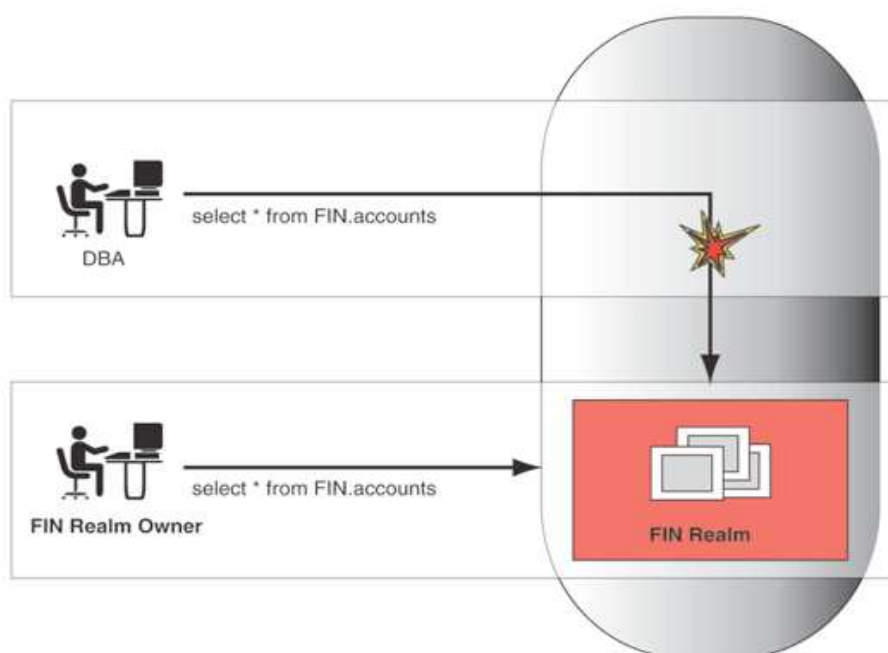
Oracle® Database Vault při instalaci vytváří několik nových účtů - DVOWNER a DVACCTMGR. DVOWNER má stejnojmennou roli, která mu umožňuje spravovat Oracle® Database Vault role konfiguraci. DVACCTMGR má také stejnojmennou roli, která mu umožňuje spravovat uživatelské účty. Kromě těchto rolí jsou ještě vytvořeny role: DVREALMOWNER, DVREALMRESOURCE, DVPUBLIC a DVSECANALYST. Například DVSECANALYST role je určena pro analytiku bezpečnosti a proto jsou její možnosti značně omezené jen na prohlížení některých objektů. Detailní popis zmiňovaných rolí je nad rámec tohoto dokumentu.

Oracle® Database Vault poskytuje možnosti generování reportů o různých aktivitách a monitorování změn pravidel, konfigurace databáze a jejich struktur nebo bezpečnostních událostí.

Oracle® Database Vault používá několik komponent řízení přístupu: oblasti, pravidla, příkazy, faktory, sady pravidel, bezpečnou aplikační roli.

9.4.1.1 Oblasti (Realms)

Oblasti jsou seskupení databázových schémat a rolí, které musejí být pro danou aplikaci zabezpečeny. Schéma je skupina databázových objektů, jako tabulky, pohledy a balíčky. Role je skupina oprávnění. Spojením schémat a rolí do skupiny můžeme řídit možnost použití systémových oprávnění a zabránit přístupu k datům administrátorům s těmito oprávněními. Takto mohou být například ochráněna všechna data patřící účetnímu oddělení proti neoprávněnému přístupu uživatelů se systémovými oprávněními.



Obr.5 Oblasti (Realm) Oracle® Database Vault

(zdroj: Oracle® Database Vault Administrator's Guide 11g Release 1)

9.4.1.2 Pravidla příkazů (Command rules)

Pravidla příkazů jsou pravidla která určují, jak může uživatel používat DDL nebo DML příkazy. Můžeme jimi ovlivňovat například SELECT, ALTER SYSTEM apod. Pravidla příkazů mají následující atributy:

- SQL příkaz, který chrání
- Vlastníka objektu, které pravidlo ovlivňuje
- Databázový objekt, které pravidlo ovlivňuje
- Stav pravidla – aktivní nebo neaktivní
- Asociovanou skupinu pravidel

Pravidla příkazů jsou rozdělena na pravidla s platností v celém systému (databázové instanci), s platností pro dané schéma, s platností pro daný objekt. Když uživatel spustí příkaz, na který se vztahuje pravidlo příkazů, Oracle® Database Vault provede asociovanou skupinu pravidel, a pokud všechna pravidla vrátí hodnotu TRUE, provede teprve vlastní příkaz.

9.4.1.3 Faktory (Factors)

Faktory jsou pojmenované proměnné nebo atributy, jako je IP adresa, databázová doména nebo metoda autentizace. Oracle® Database Vault poskytuje několik předdefinovaných faktorů a další mohou být vytvořeny uživatelem pomocí PL/SQL. Faktory jsou využívány v kombinaci s pravidly a skupinami pravidel.

9.4.1.4 Skupina pravidel (Rule sets)

Skupina pravidel je skupina jednoho nebo více pravidel, které mohou být spojeny s oblastí, faktorem, pravidlem příkazu nebo bezpečnou aplikační rolí. Skupina pravidel nabývá hodnoty TRUE nebo FALSE podle výsledků jednotlivých obsažených pravidel, která také nabývají hodnoty TRUE nebo FALSE. Jednotlivá pravidla jsou realizována pomocí PL/SQL. Jedno pravidlo může být obsaženo v jedné nebo více skupinách pravidel.

Skupiny pravidel mohou být použity pro zajištění následujících činností:

- další omezení autorizace oblasti, k definování podmínek za kterých je autorizace aktivní
- k definování kdy použít pravidla příkazů
- k povolení bezpečné aplikační role
- k definování kdy přiřadit hodnotu faktoru

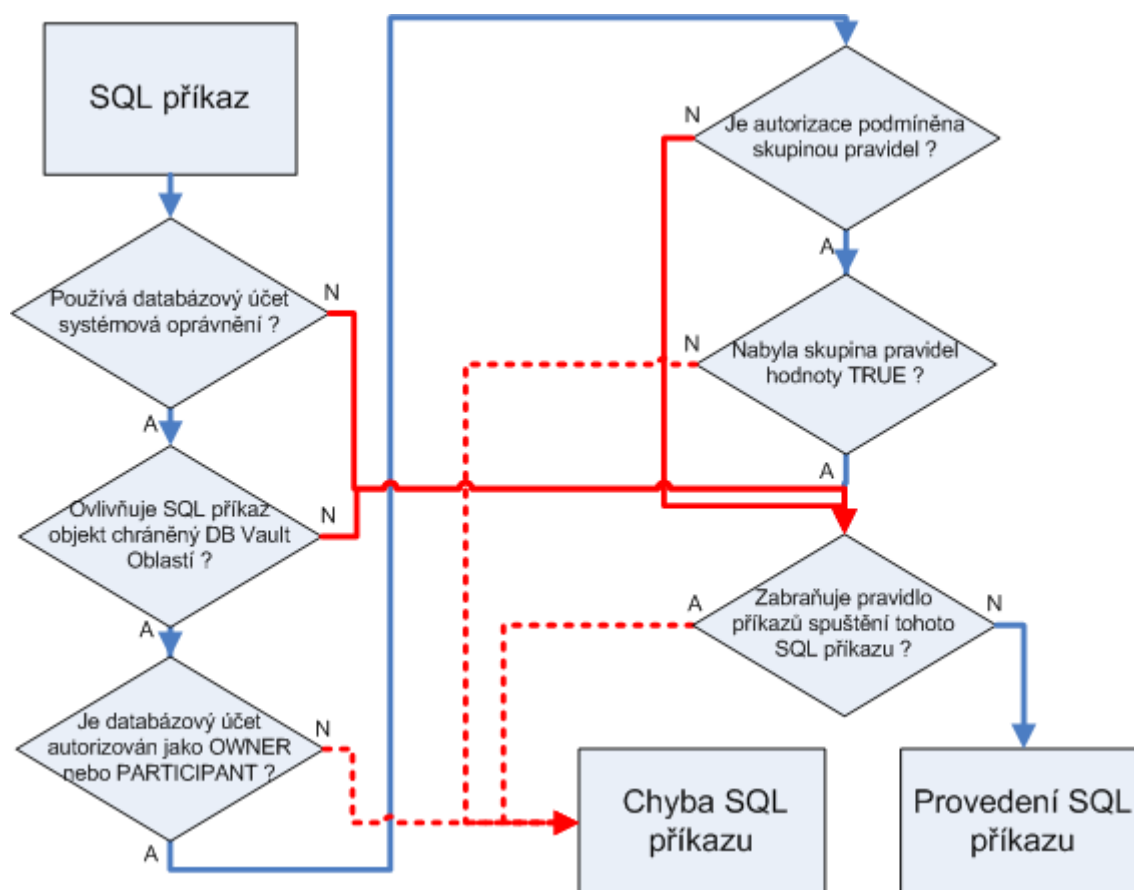
Oracle® Database Vault poskytuje několik předdefinovaných skupin pravidel. Další možností je vytvoření uživatelských skupin pravidel, které mohou obsahovat libovolná pravidla, která byla již vytvořena. Množství použitých skupin pravidel a množství pravidel v jednotlivých skupinách přímo úměrně zvyšuje zátěž systému. Pokud je počet pravidel opravdu veliký, může to mít výrazný dopad na výkon databáze.

9.4.1.5 Bezpečné aplikační role (Secure application roles)

Bezpečná aplikační role Oracle® Database Vault je speciální role, která umožňuje využívat Oracle® Database Vault skupiny pravidel. Standardní Oracle® Database System 11g bezpečné aplikační role využívají běžné PL/SQL procedury. Výhodou bezpečných aplikačních rolí Oracle® Database Vault je, že bezpečnostní pravidla jsou uložena na jednom společném místě. V případě

změny pravidel je změnu nutné udělat jen jednou ve skupině pravidel. Nezáleží na tom jak se uživatel připojuje k databázi, protože pravidla jsou svázána s rolí.

9.4.1.6 Jak pracuje Oblast Oracle® Database Vault ?



Obr.6 Diagram autorizace SQL příkazu v Oracle® Database Vault.

9.4.1.7 Příklad použití možností Oracle® Database Vault

Na tomto jednoduchém příkladu bude demonstrováno, jak Oracle® Database Vault zamezí přístupu uživatele SYS k tabulce ve schématu uživatele TH a jak povolit přístup uživateli TEST. Nejdříve budou vytvořeny uživatelské účty TH a TEST a uživateli TEST bude nastaven přístup do schématu uživatele TH. Potom budou ve schématu uživatele TH vytvořeny testovací tabulky a vygenerována náhodná data. V dalším kroku bude na databázi zprovozněn Oracle® Database Vault a otestován přístup uživatelů SYS, TH a TEST k datům v testovací tabulce TH.ADRESY. Dále bude provedena konfigurace Oracle® Database Vault tak, aby byl umožněn přístup k datům v testovací tabulce uživateli TEST.

1. Přihlášení do databáze jako uživatel SYS a vytvoření uživatelských účtů TH a TEST.

```
[oracle@thcentos1 dbhome_1]$ cd $ORACLE_HOME

[oracle@thcentos1 dbhome_1]$ bin/sqlplus sys/Passw0rd as sysdba
SQL*Plus: Release 11.2.0.1.0 Production on Thu Apr 29 17:09:12 2010

Copyright (c) 1982, 2009, Oracle. All rights reserved.

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options

SQL>
SQL> CREATE USER TH IDENTIFIED BY Passw0rd
      2  DEFAULT TABLESPACE USERS
      3  TEMPORARY TABLESPACE TEMP
      4  ;
User created.

SQL> GRANT RESOURCE TO TH;
Grant succeeded.

SQL> GRANT CONNECT TO TH;
Grant succeeded.

SQL> ALTER USER TH DEFAULT ROLE RESOURCE,CONNECT;
User altered.

SQL> GRANT UNLIMITED TABLESPACE TO TH;
Grant succeeded.

SQL> CREATE USER TEST IDENTIFIED BY Passw0rd
      2  DEFAULT TABLESPACE USERS
      3  TEMPORARY TABLESPACE TEMP
      4  ;
User created.

SQL> GRANT RESOURCE,CONNECT TO TEST;
Grant succeeded.

SQL> ALTER USER TEST DEFAULT ROLE RESOURCE,CONNECT;
User altered.

SQL> GRANT UNLIMITED TABLESPACE TO TEST;
Grant succeeded.
```

2. Nastavení práv SELECT uživateli TEST na tabulku TH.ADRESY

```
SQL> GRANT SELECT ON TH.ADRESY TO TEST;
Grant succeeded.

SQL>exit
```

Uživateli TEST byl úspěšně nastaven přístup k tabulce ADRESY ve schématu uživatele TH.

3. Vytvoření testovací tabulky a naplnění daty ve schématu TH

Je vytvořena testovací tabulka ADRESY ve schématu uživatele TH a naplněna testovacími daty. Testovací data jsou náhodně vygenerována pomocí PL/SQL skriptu.

4. Otestování příkazu SELECT uživatelem TH, TEST a SYS na testovací tabulce TH.ADRESY

```
[oracle@thcentos1 dbhome_1]$ bin/sqlplus th/Passw0rd
```

```
SQL*Plus: Release 11.2.0.1.0 Production on Thu Apr 29 17:27:06 2010  
Copyright (c) 1982, 2009, Oracle. All rights reserved.
```

```
Connected to:  
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production  
With the Partitioning, Oracle Label Security, OLAP, Data Mining,  
Oracle Database Vault and Real Application Testing options
```

```
SQL> SELECT * from TH.ADRESY WHERE ROWNUM <= 5;
```

ADRESA_ID	ULICE	MESTO	PSC	STAT_ID
584	Uzka 436	Liberec	81538	1
585	Masarykova 199	Brno	82655	1
586	Masarykova 137	Ostrava	64524	1
587	Masarykova 40	Praha	54050	1
588	Dvorakova 179	Plzen	93688	1

```
5 rows selected.
```

```
SQL>exit
```

```
[oracle@thcentos1 dbhome_1]$ bin/sqlplus test/Passw0rd
```

```
SQL*Plus: Release 11.2.0.1.0 Production on Thu Apr 29 19:25:19 2010  
Copyright (c) 1982, 2009, Oracle. All rights reserved.
```

```
Connected to:  
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production  
With the Partitioning, Oracle Label Security, OLAP, Data Mining,  
Oracle Database Vault and Real Application Testing options
```

```
SQL> SELECT * from TH.ADRESY WHERE ROWNUM <= 5;
```

ADRESA_ID	ULICE	MESTO	PSC	STAT_ID
590	Smetanova 235	Brno	80042	1
591	Dlouha 335	Liberec	76084	1
592	Bananova 849	Jablonec	68358	1
593	Masarykova 321	Praha	57488	1
594	Malinova 795	Ostrava	37682	1

```
5 rows selected.
```

```
SQL>exit
```

```
[oracle@thcentos1 dbhome_1]$ bin/sqlplus sys/Passw0rd as sysdba
```

```
SQL*Plus: Release 11.2.0.1.0 Production on Thu Apr 29 17:28:31 2010  
Copyright (c) 1982, 2009, Oracle. All rights reserved.
```

Connected to:

Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options

```
SQL> SELECT * from TH.ADRESY WHERE ROWNUM <= 5;
```

ADRESA_ID	ULICE	MESTO	PSC	STAT_ID
584	Uzka 436	Liberec	81538	1
585	Masarykova 199	Brno	82655	1
586	Masarykova 137	Ostrava	64524	1
587	Masarykova 40	Praha	54050	1
588	Dvorakova 179	Plzen	93688	1

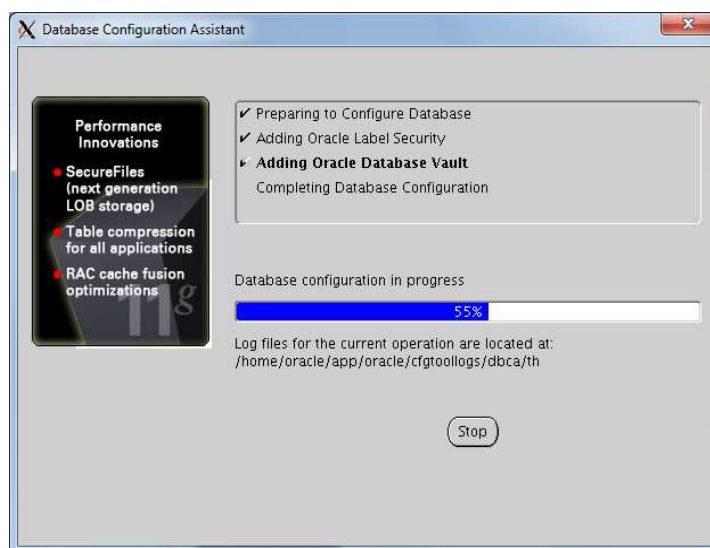
5 rows selected.

```
SQL>exit
```

Všichni tři uživatelé TH, TEST a SYS mají přístup k testovacím datům. Uživatel TH, protože jsou data jím vytvořena a jsou uložena v jeho schématu, uživatel TEST, protože mu byla práva pro SELECT nastavena v předchozím kroku a uživatel SYS, protože je to administrátorský účet který má standardně přístup všude.

5. Instalace DB Vault

V tomto kroku je provedena instalace Oracle® Database Vault na databázi ve které byly vytvořena testovací tabulka ADRESY. Není zde uveden celý postup, protože postup instalace není předmětem tohoto příkladu. Po ukončení instalace je vyžadován restart databáze.



Obr.7 Instalace Oracle® Database Vault.

6. Vytvoření Oblasti (Realm) DB Vault

Při instalaci Oracle® Database Vault jsou vytvořeny účty DVOWNER pro administrátora Oracle® Database Vault a DVACCTMGR pro administrátora uživatelských účtů. Administrátorovi SYS jsou některá jeho práva odebrána a rozdělena mezi výše jmenované účty. (Podrobnosti naleznete v *Oracle® Database Vault Administrator's Guide 11g*). Oracle® Database Vault nabízí pro administraci grafický webový nástroj Oracle® Database Vault Manager. Další kroky konfigurace budou prováděny v tomto nástroji. Prvním krokem je konfigurace vytvoření oblasti (Realm) Oracle® Database Vault. Tato oblast bude pojmenována TH Realm.

Database Instance: TH > Realm > Logged in as DVOWNER
Create Realm Cancel OK

Enable or disable the enforcements for objects protected by the realm and to control the auditing that occurs during this enforcement.

General

* Name: TH Realm

Description:

Status: ☒ Enabled ☐ Disabled

Audit Options

☐ Audit Disabled
☒ Audit On Failure
☐ Audit On Success or Failure

Cancel OK

Database | Help | Logout

Copyright (c) 2000, 2009, Oracle. All rights reserved.
[About Oracle Database Vault Administrator](#)

Obr.8 Vytvoření oblasti TH Realm.

7. Nastavení zabezpečení tabulky ADRESY v oblasti TH Realm

Nyní bude tabulka přidána do nadefinované oblasti TH Realm a tím bude omezen přístup všech uživatelů k této tabulce kromě jejího vlastníka uživatele TH.

Database Instance: TH > Realms > Edit Realm: TH Realm > Logged in as DVOWNER
Create Realm Secured Object Cancel OK

Define a database schema or database role that is protected by the realm.

Object Owner
TH

Object Type
TABLE

Object Name
ADRESY

Cancel OK

Database | Help | Logout

Copyright (c) 2000, 2009, Oracle. All rights reserved.
[About Oracle Database Vault Administrator](#)

Obr.9 Konfigurace oblasti TH Realm.

8. Otestování příkazu *SELECT* uživatelem *TH*, *TEST* a *SYS* na testovací tabulce *TH.ADRESY*

```
[oracle@thcentos1 dbhome_1]$ bin/sqlplus th/Passw0rd
```

```
SQL*Plus: Release 11.2.0.1.0 Production on Thu Apr 29 19:38:09 2010  
Copyright (c) 1982, 2009, Oracle. All rights reserved.
```

Connected to:

Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options

```
SQL> SELECT * from TH.ADRESY WHERE ROWNUM <= 5;
```

ADRESA_ID	ULICE	MESTO	PSC	STAT_ID
590	Smetanova 235	Brno	80042	1
591	Dlouha 335	Liberec	76084	1
592	Bananova 849	Jablonec	68358	1
593	Masarykova 321	Praha	57488	1
594	Malinova 795	Ostrava	37682	1

5 rows selected.

```
SQL> exit
```

Na právech přístupu uživatele *TH* k tabulce *TH.ADRESY* se nic nezměnilo.

```
[oracle@thcentos1 dbhome_1]$ bin/sqlplus test/Passw0rd
```

```
SQL*Plus: Release 11.2.0.1.0 Production on Thu Apr 29 17:36:35 2010  
Copyright (c) 1982, 2009, Oracle. All rights reserved.
```

Connected to:

Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options

```
SQL> SELECT * from TH.ADRESY WHERE ROWNUM <= 5;
```

```
SELECT * from TH.ADRESY WHERE ROWNUM <= 5  
*
```

ERROR at line 1:

ORA-00942: table or view does not exist

```
SQL>exit
```

```
[oracle@thcentos1 dbhome_1]$ bin/sqlplus sys/Passw0rd as sysdba
```

```
SQL*Plus: Release 11.2.0.1.0 Production on Thu Apr 29 18:57:30 2010  
Copyright (c) 1982, 2009, Oracle. All rights reserved.
```

Connected to:

Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options

```
SQL> SELECT * from TH.ADRESY WHERE ROWNUM <= 5;
```

```
SELECT * from TH.ADRESY WHERE ROWNUM <= 5  
*
```

ERROR at line 1:

ORA-01031: insufficient privileges

Uživatelé *TEST* a *SYS* už nemají práva *SELECT* na testovací tabulce *TH.ADRESY*

9. Přidání uživatele TEST do oblasti TH Realm.

Aby měl uživatel TEST opět právo provádět SELECT na tabulce TH.ADRESY, musí být toto právo nastaveno v oblasti TH Realm. Uživatel TEST je přidán do Realm Authorizations.

Database Instance: TH > Realm > Edit Realm: TH Realm

Logged in as DVOWNER

Enable or disable the enforcements for objects protected by the realm and to control the auditing that occurs during this enforcement.

General

* Name: TH Realm

Description:

Status: ☒ Enabled ☐ Disabled

Audit Options

☐ Audit Disabled
☒ Audit On Failure
☐ Audit On Success or Failure

Realm Secured Objects

Select	Owner	Object Type	Object Name
<input checked="" type="radio"/>	TH	TABLE	ADRESY

Realm Authorizations

Select	Grantee	Authorization Options	Authorization Rule Set Name
<input checked="" type="radio"/>	TEST	Participant	

Obr.10 Konfigurace oblasti Oracle® Database Vault.

10. Test SELECT uživatelem TEST a SYS

```
[oracle@thcentos1 dbhome_1]$ bin/sqlplus test/Passw0rd
```

```
SQL*Plus: Release 11.2.0.1.0 Production on Thu Apr 29 19:40:38 2010
Copyright (c) 1982, 2009, Oracle. All rights reserved.
```

Connected to:

Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options

```
SQL> SELECT * from TH.ADRESY WHERE ROWNUM <= 5;
```

ADRESA_ID	ULICE	MESTO	PSC	STAT_ID
590	Smetanova 235	Brno	80042	1
591	Dlouha 335	Liberec	76084	1
592	Bananova 849	Jablonec	68358	1

593 Masarykova 321	Praha	57488	1
594 Malinova 795	Ostrava	37682	1

5 rows selected.

SQL>

Uživatel TEST má opět právo SELECT na tabulce TH.ADRESY.

```
[oracle@thcentos1 dbhome_1]$ bin/sqlplus sys/Passw0rd as sysdba
SQL*Plus: Release 11.2.0.1.0 Production on Thu Apr 29 18:57:30 2010

Copyright (c) 1982, 2009, Oracle. All rights reserved.

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options

SQL> SELECT * from TH.ADRESY WHERE ROWNUM <= 10;
SELECT * from TH.ADRESY WHERE ROWNUM <= 10
*
```

ERROR at line 1:
ORA-01031: insufficient privileges

SQL>

Uživatel SYS nemá do tabulky TH.ADRESY přístup.

Na tomto jednoduchém příkladu bylo ukázáno, že Oracle® Database Vault je účinný nástroj pro zabezpečení data uložených v databázi i proti přístupu privilegovaných uživatelů.

9.4.2 TDE (Transparent Data Encryption)

Oracle® Database System pomocí autentizace a autorizace popsaných výše může řídit přístup k datům uloženým v databázi. Nemůže ale zajistit bezpečný přístup k datovým souborům databáze uloženým v operačním systému.

Databázové soubory bývají často uloženy na diskových polích, která používají pro zvýšení rychlosti nebo zajištění vysoké dostupnosti různé verze RAID (Redundant Array of Independent Disks). V případě poruchy pevného disku v diskovém poli není díky technologii RAID ohrožena dostupnost uložených dat. Pevné disky mohou být za provozu vyměněny za nové. U moderních polí, která jsou vybavena rozsáhlou diagnostikou, nemusí to, že je disk označen polem za vadný nutně znamenat, že jsou data na něm uložená zcela nečitelná. Diagnostika v polích provádí na pozadí normální činnosti testy disků a často preventivně odstaví disk dříve, než dojde ke skutečnému problému. Data na takovém disku zůstávají. Tím, že je pevný disk vyjmut z pole, ale také nejsou

smazána data, která jsou na něm uložena. Mohlo by se tedy stát, že někdo získá aktuální databázová data i z tohoto „vadného disku“.

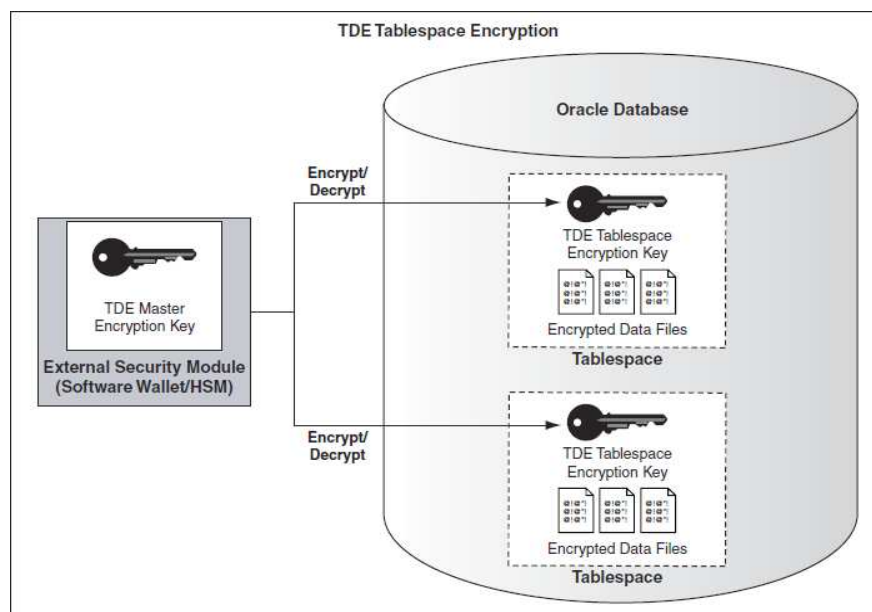
Další možností úniku dat je ztráta nebo krádež zálohovacích médií. Při záloze jsou data zkopírována z databáze na zálohovací médium. Zálohovací médium může být magnetická páska, pevný disk nebo jiné médium. Pokud by někdo nepovolaný takové médium získal, mohl by z něho získat také data uložená v databázi. Pokud by získal kompletní sadu zálohovacích médií, mohl by dokonce získat kompletní funkční kopii celé instance databáze.

I když nejmodernější disková pole i páskové jednotky nabízejí možnost transparentního šifrování dat při zápisu a jejich dešifrování při čtení, není toto řešení z bezpečnostního hlediska ideální, protože zamezí úniku dat pouze při ztrátě nebo krádeži médií, ale nezabezpečí databázová data před správci diskových polí nebo zálohovacích systémů.

Aby Oracle® nabídl řešení pokrývající tuto bezpečnostní mezeru, vyvinul Transparent Data Encryption (TDE). TDE provádí transparentní šifrování sloupců v tabulce. Protože se jedná o transparentní šifrování, oprávněný uživatel nebo aplikace vůbec nepozná, že pracuje se šifrovanými sloupci tabulky. Od verze Oracle® Database System 11g Release 1 je možné šifrovat i celý tabulkový prostor (tablespace⁹). Velkou výhodou tohoto řešení je, že nevyžaduje žádnou úpravu na straně aplikace. V obou případech je práce se šifrovacími klíči stejná. Liší se však některými omezeními. V případě šifrování tabulkových prostorů je omezení méně než při šifrování pouze některých sloupců. Šifrování tabulkových prostorů probíhá při operacích čtení a zápisu, naproti tomu šifrování jednotlivých sloupců tabulek probíhá na úrovni SQL.

Transparentní šifrování probíhá tak, že každá tabulka, která obsahuje nějaký šifrovaný sloupec, má svůj vlastní šifrovací klíč, kterým šifruje data ukládaná v šifrovaných sloupcích. V případě šifrování tabulkových prostorů je jeden klíč pro celý tabulkový prostor. Tyto klíče tabulek nebo tabulkových prostorů jsou zašifrovány hlavním klíčem a uloženy v databázi. Hlavní klíč se v databázi neuchovává, ale je uložen mimo v softwarové peněženke (Oracle Wallet) nebo v HSM (Hardware Security Modul). Pro transparentní šifrování je možné zvolit algoritmus 3DES nebo AES.

9 Tablespace – skupina datových souborů do kterých se ukládají data databáze.



Obr.11 Oracle® Transparent Data Encryption – šifrování tabulkových prostorů

(zdroj: Oracle® Database Advanced Security Administrator's Guide 11g Release 1)

9.4.3 Fyzická bezpečnost

Důležitou oblastí zabezpečení je kromě autentizace, autorizace nebo zabezpečení síťové komunikace i fyzické zabezpečení databázových serverů a jejich úložišť. Stejně jako v případě nastavení přístupových práv v databázi nebo v operačním systému, je potřeba klást důraz i na omezení fyzického přístupu k hardware jen na nezbytně nutnou míru. V případě krádeže hardware, na kterém běží informační systém s daty v databázi, organizace přichází nejen o cenná data, ale současně ani nemůže poskytovat služby svým zákazníkům. Proto je potřebné v rámci firemní bezpečnostní politiky stanovit pravidla přístupu k systémům a způsob kontroly a vymáhání jejich plnění.

9.5 Audit

Navazujícím krokem po nastavení přístupových práv je nastavení a používání prostředků Oracle® Database System pro audit. Audit je monitorování a zaznamenávání akcí, které uživatelé provádějí při práci s databází. Audit prováděné akci sice nemůže zabránit, ale poskytuje informaci o tom, že se uskutečnila. Auditování může být vztaženo například jen ke konkrétnímu uživateli, objektu databáze nebo akci, kterou uživatel provádí. Audit je využíván k vedení záznamů o akcích uživatelů, ke zjišťování a prokazování podezřelých aktivit uživatelů, pomocí záznamů auditu mohou být odhaleny nedostatky v nastavení přístupových práv a konečně audit je vyžadován organizacemi, jako je již výše zmiňovaná PCI (Payment Card Industry) nebo nařízeními Evropské unie týkajícími se bezpečnosti dat.

Záznamy auditu jsou v Oracle® Database System 11g ukládány buď do tabulek SYS.AUD\$ a SYS.FGA_LOG\$ nebo do souboru v operačním systému. Aby bylo možné v rámci ochrany proti útokům „insiderů“ zabránit databázovým administrátorům v manipulaci s těmito záznamy, doporučuje Oracle® využívat ukládání do souboru operačního systému tak, aby k nim databázový administrátor neměl přístup. Pokud je používán Oracle® Database Vault, je možné vytvořit nad jmenovanými tabulkami záznamů oblast (Realm) Oracle® Database Vault a tím zamezit v jejich neoprávněné modifikaci.

Provádění auditu zatěžuje databázový server a může mít výrazný dopad na výkon systému, proto je nezbytné dobré plánování a dodržování zásady nejmenšího možného počtu pravidel pro daný účel.

Oracle® Database System 11g nabízí různé typy auditů:

- Audit příkazů – záznam SQL příkazů zadaných jedním nebo více uživateli bez ohledu na schéma objektu s kterým pracuje.
- Audit oprávnění – záznam použití systémových příkazů buď všemi uživateli databáze nebo specifickou skupinou.
- Audit objektů schématu – záznam konkrétních příkazů nad určenými objekty schématu. Aplikuje se vždy na všechny uživatele databáze.
- Rozšířený audit – záznam o přístupu k tabulkám a oprávněním na základě obsahu dotčeného objektu.

9.5.1 *Audit příkazů*

Audit příkazů provádí záznam o SQL příkazech zadaných jedním nebo více uživateli bez ohledu na schéma objektu se kterým se pracuje. Je možné specifikovat, jestli se záznam má vytvářet při každém nebo jen prvním výskytu události. Dále je možné určit, jestli se mají zaznamenávat úspěšně provedené příkazy, neúspěšné příkazy, nebo obojí. Zaznamenávané příkazy je nutné buď přesně specifikovat, nebo je možné použít slovo ALL. Použitím slova ALL bude zaznamenávána většina příkazů, ale ne všechny. Bližší informace o tom, které příkazy obsahuje ALL a které ne, jsou uvedeny v dokumentaci Oracle® Database Vault Administrator's Guide. Pokud například nastavíme záznam příkazů pro operace s tabulkou, budou se zaznamenávat příkazy týkající se vytvoření, změny nebo smazání tabulky.

9.5.2 *Audit oprávnění*

Audit oprávnění provádí záznam o použití systémových příkazů buď všemi uživateli databáze nebo specifickou skupinou. Na rozdíl od auditu příkazů, musí být při auditu oprávnění přesně specifikován příkaz, který se bude zaznamenávat. Nestačí tedy říci, že se budou zaznamenávat příkazy týkající se například tabulky databáze, ale musí být přesně řečeno, že to bude právě příkaz vytvoření tabulky.

9.5.3 *Audit objektů schématu*

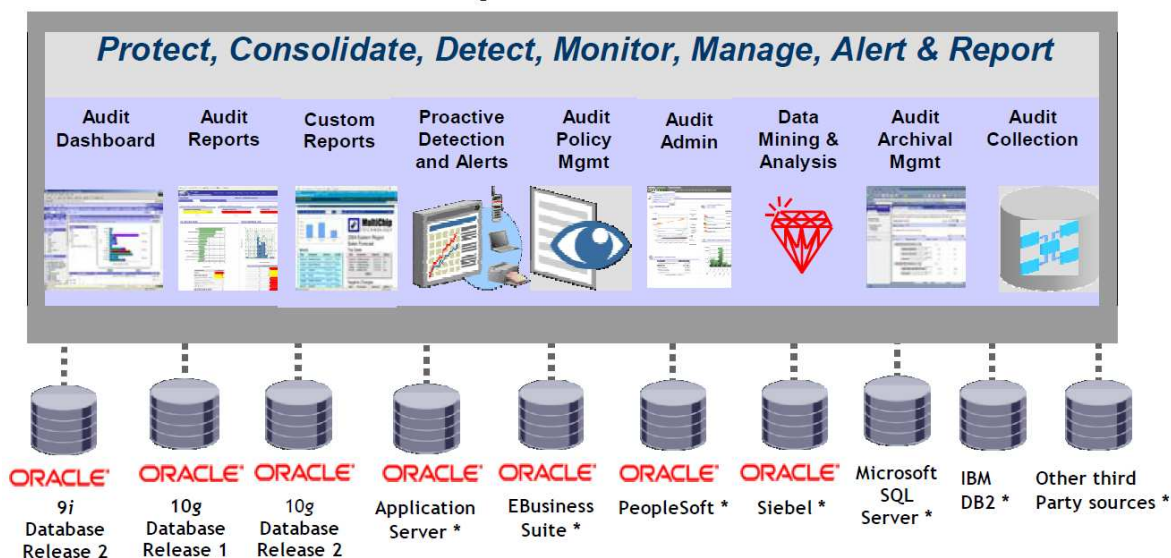
Audit objektů schématu vytváří záznamy o konkrétních příkazech nad určenými objekty schématu. Aplikuje se vždy na všechny uživatele databáze. Při nastavování tohoto typu auditu se specifikuje typ akce a objekt, kterého se týká. Například můžeme zaznamenávat všechny aktualizace vybrané tabulky.

9.5.4 *Rozšířené možnosti auditu (Fine grained auditing)*

Počínaje verzí Oracle® 9i byly možnosti auditu ještě více rozšířeny. Do té doby bylo možné ze záznamů auditu zjistit, kdo a k jakým tabulkám přistupoval, ale nebylo možné zjistit, ke kterým konkrétním sloupcům a řádkům tabulky. Rozšířené možnosti auditu (Fine grained auditing) tuto možnost přinášejí. Používají k tomu predikát WHERE, podobně jako u virtuálních privátních databází, s možností specifikovat konkrétní sloupce tabulky. Přínos tohoto rozšíření je ve snížení počtu záznamů auditu.

9.5.5 Oracle® Audit Vault

Protože sledování a vyhodnocování záznamů auditu je časově náročná činnost, která, aby byla účinná, musí být prováděna neustále, nabízí Oracle® produkt Oracle® Audit Vault. Tento produkt umožňuje řadu činností provádět automaticky, a to nejen u databází Oracle®, ale také pro databáze IBM DB2, Microsoft SQL a Sybase. Je založen na technologii Oracle® Warehouse pro konsolidaci dat a je schopen také využít možností Oracle® Real Application Clusteru pro zajištění vysoké dostupnosti. Nepřetržitě sbírá data z jednotlivých databázových serverů, analyzuje je, archivuje a vytváří z nich reporty. Díky analýze dat v reálném čase dokáže odhalit útoky „insiderů“ a ihned na ně upozornit. Také umožňuje vytvářet pravidla auditu a distribuovat je na jednotlivé databázové servery.



Obr.12 Oracle® Audit Vault

(zdroj: Oracle® Audit Vault 10g datasheet)

10 ZÁVĚR

Cílem této práce bylo zjistit, jestli databáze Oracle® Database System 11g nabízí dostatečné prostředky k zabezpečení uložených dat, a to nejen proti útokům zvenčí, ale také proti neoprávněnému přístupu ze strany privilegovaných uživatelů, to znamená databázových administrátorů, administrátorů operačních systémů, administrátorů datových úložišť nebo administrátorů zálohování.

V jednotlivých kapitolách byly probírány možnosti autentizace, autorizace, zabezpečení síťové komunikace a ochrany dat na datových úložištích a zálohách. Ve všech těchto oblastech nabízí databáze Oracle® Database System 11g dostatečné prostředky pro zabezpečení dat na úrovni odpovídající jejímu nasazení v aplikacích pracujících s citlivými daty. V oblasti autentizace poskytuje možnost využít nejmodernějších autentizačních prostředků včetně použití biometrických způsobů autentizace. V oblasti autorizace poskytuje prostředky pro efektivní řízení přístupu jednotlivých uživatelů a aplikací k datům uloženým v databázi a možnost velmi podrobně určit pravidla přístupu. Pro bezpečnost síťové komunikace používá osvědčený a široce podporovaný protokol SSL v kombinaci s možnostmi symetrického i asymetrického šifrování a využitím elektronických certifikátů. Jako ochranu dat na datových úložištích a zálohovacích systémech nabízí Transparent Data Encryption, která pro uživatele zcela transparentně a bez nutnosti úprav aplikací řeší tuto oblast zabezpečení.

V oblasti zabezpečení dat v databázi proti neoprávněnému přístupu administrátorů poskytuje databáze Oracle® Database System 11g prostřednictvím Oracle® Database Vault nadstandardní prostředky, které dokážou zabránit neoprávněnému přístupu k datům, ale neomezují přitom schopnost administrátorů spravovat databázi. Použití Oracle® Database Vault nevyžaduje zásah do stávajících aplikací, které využívají databázový systém, a proto nezvyšuje náklady spojené s jejich zabezpečením. Oracle® Database Vault aplikuje zásadu rozdělení pravomocí jako jednu ze základních podmínek pro dodržení doporučení a nařízení vyplývajících z bezpečnostních standardů a zákonných předpisů.

Informační systémy čelí neustálým pokusům z nejrůznějších stran o narušení jejich integrity, ať už se jedná o útoky zvenčí nebo zevnitř organizace. Protože způsoby útoků se stále mění a také samotná databáze prochází neustálým vývojem, je nezbytnou podmínkou bezpečnosti pravidelná aplikace bezpečnostních a aktualizčních softwarových balíčků, které rozšiřují možnosti systému, opravují chyby a reagují na zjištěná bezpečnostní rizika.

Pro zaručení bezpečnosti databázových systémů je kromě efektivního používání bezpečnostních možností samotných systémů také nezbytné stanovení firemní bezpečnostní politiky, která musí zahrnovat pravidla pro rozdělení pravomocí a postup provádění změn. Tato politika

musí být pravidelně aktualizována, aby dokázala reagovat na vývoj v oblasti informačních systémů i vývoj organizace samotné.

Závěrem lze říci, že i když tato práce není založena na dlouholetých praktických zkušenostech, ale především na teoretických poznatcích, lze databázi Oracle® Database System 11g považovat za bezpečnou i proti útokům privilegovaných uživatelů, ale pouze za podmínky využití všech výše zmíněných možností a doporučení.

11 CONCLUSION

The point of this work was to find, if Oracle® Database System 11g offers enough of instruments to secure data, not only against external attacks, but also against unauthorized access to data from privileged users, this means database administrators, administrators of operating systems, storage administrators and backup administrators.

In particular chapters the possibilities of authentication, authorization, securing of network communication and securing data on data storage and backups were discussed. In all these areas Oracle® Database System 11g offers sufficient instruments for data securing on corresponding level for work with sensitive data. For authentication it provides the possibility to use modern authentication methods including biometric. For authorization it provides instruments for effective administration of access of a particular user to data in the database and possibility to use granular rules. For security of network communication it uses well-established and widely supported SSL protocol with option of symmetric and asymmetric encryption in combination with certificates. For securing of data saved on data storage and backups it provides Transparent Data Encryption, which is absolutely transparent for users and requires no application modification.

In the area of data security Oracle® Database System 11g provides an outstanding tool Oracle® Database Vault, which secures data against unauthorized access by administrators without limiting their ability to administer the database system. Use of Oracle® Database Vault does not require modification of the application using the database and that is why it does not increase costs. Oracle® Database Vault implements separation of duty as a basic requirement for complying with security recommendation and law regulations.

Information systems are facing continuous attacks to their integrity from different sides. The attacks come from outside but also inside organizations. Because the manner of attacks changes fast and the database system is developed continuously, regular application of security and software patches is important condition, which extends functionality and fixes discovered bugs.

For ensuring security of a database systems is besides using of its security option also necessary setup of corporation security policy, which must contain rules for separation of duty and changes management. This policy must be regularly updated to respond to development of information systems and the corporation itself.

At the end it is possible to say that even this work is not based on long term experience but mainly on theoretical knowledge, the Oracle® Database System 11g is secure system also against attacks from insiders in case of compliance with previously mentioned rules.

12 SEZNAM POUŽITÉ LITERATURY

1. 2010 CyberSecurity Watch Survey – Conducted by CSO magazine in cooperation with the U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte.
2. CAPPELLI, Dawn M.; MORE, Andrew P. Best Practices For Mitigating Insider Threat : Lessons Learned From 250 Case. *RSA Conference 2009* [online]. 23.4.2009, RSA Conference 2009, [cit. 2010-04-06]. Dostupný z WWW: <<http://www.cert.org/archive/pdf/RSA-CERT-InsiderThreat.pdf>> .
3. HUEY, Patricia. *Oracle® Database Security Guide 11g Release 1 (11.1)* [online]. Oracle Corporation : Oracle Corporation, 2009 [cit. 2010-04-08]. Dostupné z WWW: <www.oracle.com> .
4. JELOKA, Sumit. *Oracle® Database Advanced Security Administrator* [online]. Oracle Corporation : Oracle Corporation, 2009 [cit. 2010-04-08]. Dostupné z WWW: <www.oracle.com>.
5. HUEY, Patricia. *Oracle® Database Vault Administrator's Guide 11g Release 1 (11.1)* [online]. Oracle Corporation : Oracle Corporation, March 2010 [cit. 2010-04-08]. Dostupné z WWW: <www.oracle.com>.
6. BRYLA, Bob; LONEY, Kevin. *Mistrovství v Oracle® database 11g*. Brno : Computer Press, a.s., 2009. 700 s. ISBN 978-80-251-2189-4, K1631.
7. ALAPATI, Sam R. *Expert Oracle Database 11g Administration*. Berkeley, CA, USA : Apress, 2009. 1344 s. ISBN 978-1-4302-1015-3.
8. THERIAULT, Marlene; NEWMAN, Aaron. *Bezpečnost v Oracle® : Metody-Nástroje-Rěšení problémů*. I. vydání. Brno, ČR : Computer Press a.s., 2004. 515 s. ISBN 80-7226-979-8.

13 SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Zkratka	Popisek
CA	Certification Authority - subjekt, který vydává digitální certifikáty.
CRL	Certificate Revocation List - seznam odvolaných certifikátů certifikační autority.
DCE	Distributed Computing Environment - multiplatformní prostředí, které poskytuje velké množství různých síťových služeb, jako jsou časové služby nebo vzdálené volání procedur apod.
DDL	Data Definition Language – skupina příkazů jazyka SQL používaná pro definici datových struktur.
DML	Data Manipulation Language – skupina příkazů jazyka SQL používaná pro manipulaci s daty.
PCI DSS	Payment Card Industry Data Security Standard - je bezpečnostní normou, jejímž cílem je zamezit únikům citlivých dat o držitelích platebních karet a karetním podvodům.
PKI	Public Key Infrastructure - systém správy a distribuce veřejných klíčů využívaných v asymetrické kryptografii.
PL/SQL	PL/SQL (Procedural Language/Structured Query Language) je procedurální nadstavba jazyka SQL od firmy Oracle®.
RAID	Redundant Array of Independent Disks – technologie diskových systémů ke zvýšení jejich výkonnosti a/nebo ochrany proti poruchám.
SQL	SQL Structured Query Language - strukturovaný dotazovací jazyk je standardizovaný dotazovací jazyk používaný pro práci s daty v relačních databázích.
SSL	Secure Socket Layer - protokol zabezpečující data na přechodu mezi aplikační a transportní vrstvou (protokolem TCP/IP).
SSO	Single sign-on – technologie vyžadující po uživateli jediné přihlášení při práci s více samostatnými systémy.
TDE	Transparent data Encryption - technologie firmy Oracle®, která provádí transparentní šifrování/dešifrování dat při práci s datovými úložišti.
TLS	Transport Layer Security protocol – rozšířený protokol SSL .
VPD	Virtuální Privátní Databáze – technologie firmy Oracle®, která zajišťuje řízení přístupu k datům na úrovni jednotlivých záznamů pomocí definovaných pravidel.

14 SEZNAM OBRÁZKŮ

1. Obr.1 PKI – šifrovaná komunikace
2. Obr.2 RADIUS v prostředí Oracle® Databáze
3. Obr.3 Spouštění procedur
4. Obr.4 Ověření veřejného klíče serveru pomocí certifikátu
5. Obr.5 Oblasti (Realm) Oracle® Database Vault
6. Obr.6 Diagram autorizace SQL příkazu v Oracle® Database Vault.
7. Obr.7 Instalace Oracle® Database Vault.
8. Obr.8 Vytvoření oblasti TH Realm.
9. Obr.9 Konfigurace oblasti TH Realm.
10. Obr.10 Konfigurace oblasti Oracle® Database Vault.
11. Obr.11 Oracle® Transparent Data Encryption – šifrování tabulkových prostorů
12. Obr.12 Oracle® Audit Vault