Wie sicher ist die Datenbank vorm Administrator?

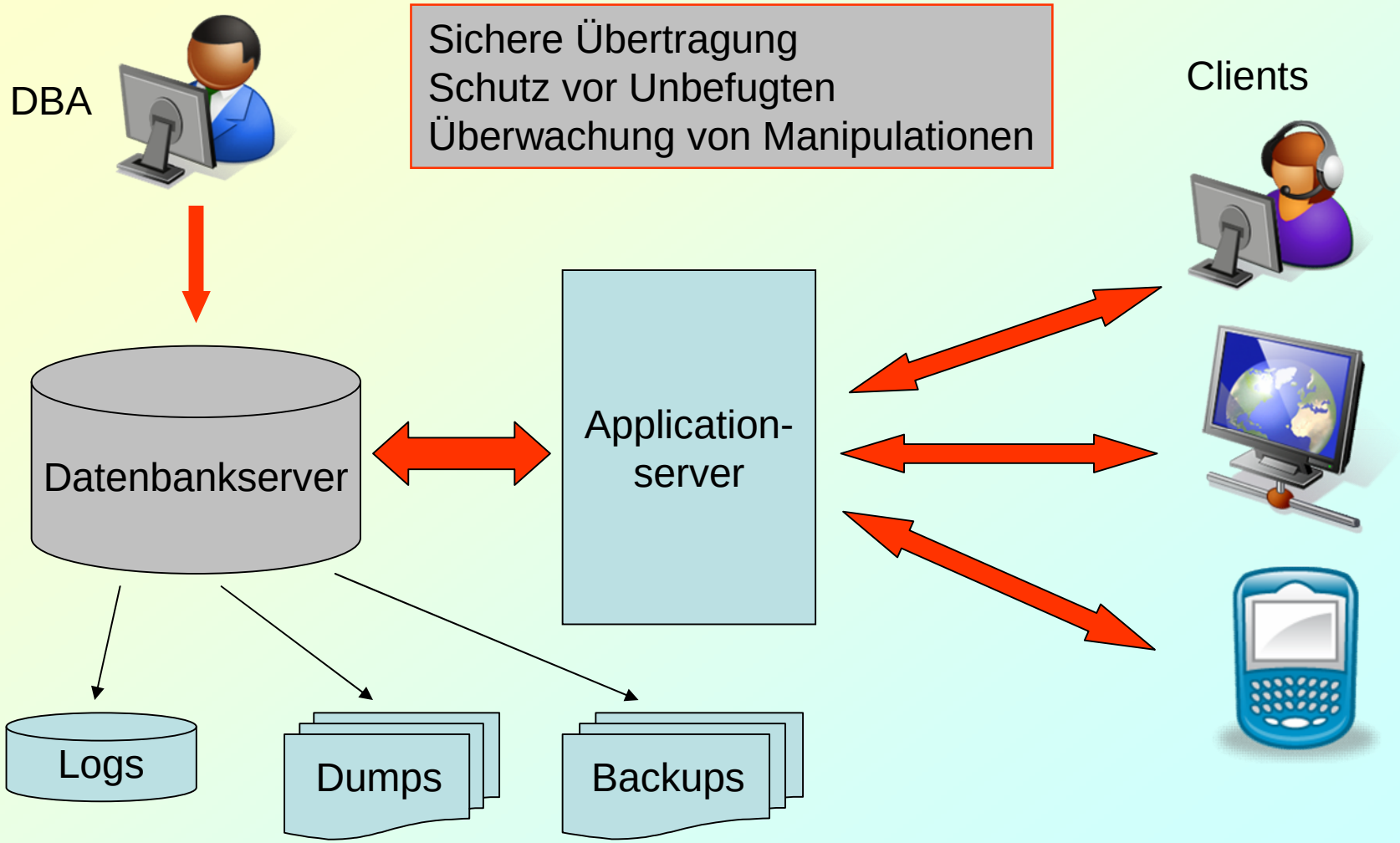
Nürnberg, 19.11.2009

Dr. Frank Haney

Inhalt

- Sicherheit wovor?
- Oracle-Sicherheits-Features im Überblick
- Transparent Data Encryption
- Auditing
- Oracle Database Vault – Übersicht
- Rechtliche Regelungen und Database Vault
- Database Vault – Komponenten
  - Sicherheitsbereiche
  - Trennung der Verantwortlichkeiten
  - Multifaktorielle Zugriffskontrolle
  - Kommandobasierte Sicherheitsregeln
  - Berichte über sicherheitsrelevante Zugriffe
- Die Administrationsoberfläche DVA
- Beispiele

Sicherheit der Daten –Herausforderungen



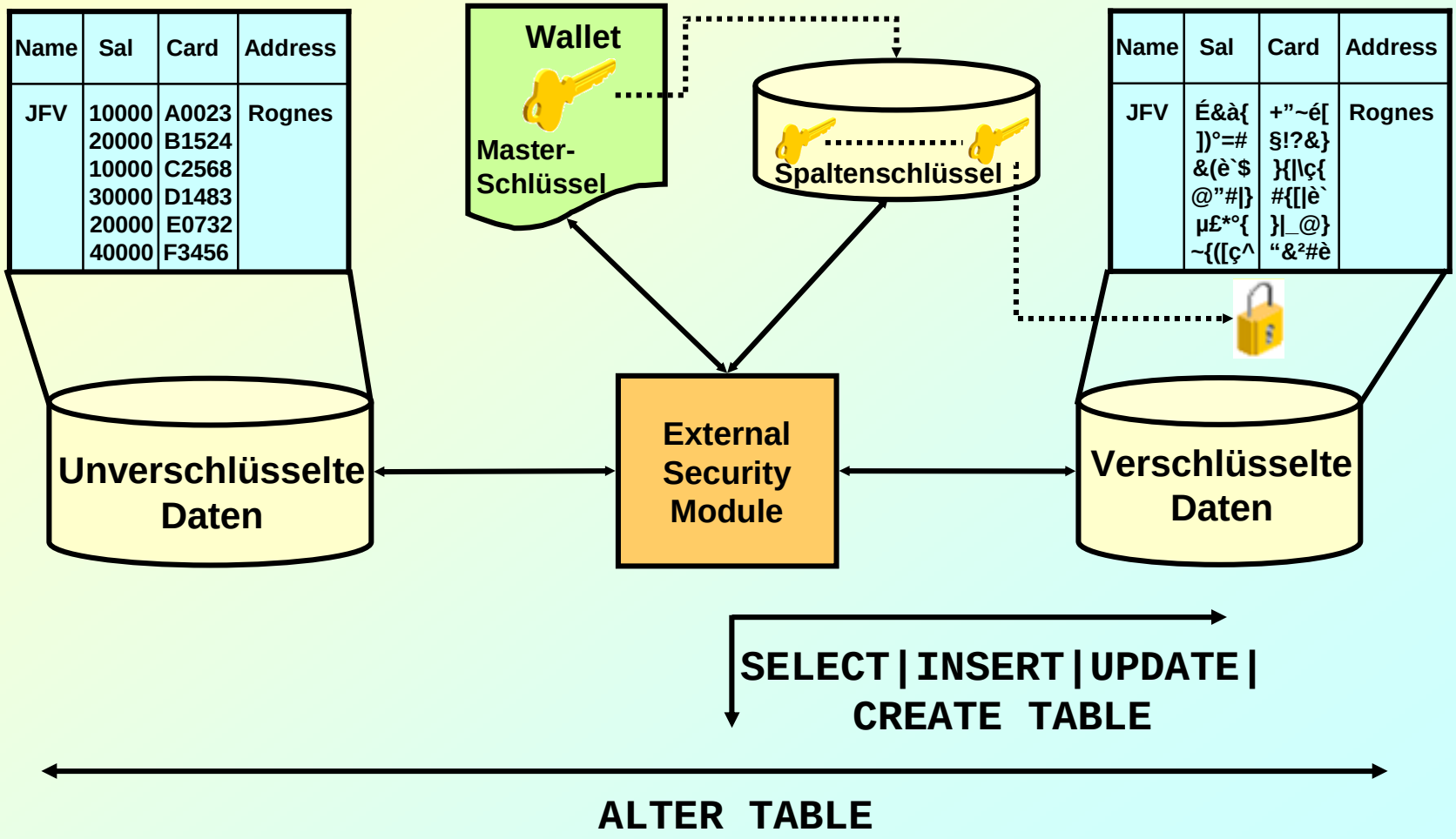
Security – Oracle Features

- **Standardauthentifizierung** – Paßwortsicherheit durch Profile
- **Standardautorisierung** – Rechtevergabe und Rollen
- **Standardauditing** – Überwachung auf den Ebenen Schemaobjekt, SQL-Anweisung und Privilegienbenutzung
- **Virtual Private Database** (VPD) – Personalisierung der Information
- **Secure External Password Store** – Paßwortspeicherung in Wallets
- **Proxy Authentification** – Authentifizierung des Client-Users bei der Datenbank in Multi-Tier-Architekturen
- **Secure Application Roles** – Schutz der Rollen durch eine Policy
- **Fine Grained Auditing** (FGA) – Überwachung des Datenzugriffs auf Zeilen- und Spaltenebene

Security – Optionen

- **Oracle Advanced Security**
  - Transparent Data Encryption (TDE) für
    - Spalten
    - Tablespaces (11*g*)
    - RMAN Backupsets
    - Datapump
    - Secure Files (11*g*)
    - Logminer (11g) → Oracle Streams und Logical Standby
  - Netzwerkverschlüsselung mit SSL
  - Starke Authentifizierung mit Kerberos and PKI
- **Oracle Label Security**
  - Zugriffskontrolle auf Zeilenebene
- **Database Vault** (im Vortrag)
- **Data Masking**
  - Maskierung der Echtdaten in nichtproduktiven Umgebungen
- **Identity Management** (Separates Produkt – früher OID)
  - Unternehmensweites Identity Management
- **Oracle Audit Vault** (Separates Produkt)
  - Unternehmensweite Konsolidierung des Auditing
  - Speicherung der Audit Trails für alle Datenbanken in einem einheitlichen Repository

Transparent Data Encryption - Spalten



TDE – Ablauf

1. Wallet anlegen (automatisch `sqlnet.ora` oder durch Wallet Manager)

```
ENCRYPTION_WALLET_LOCATION = (SOURCE = (METHOD = FILE)
        (METHOD_DATA = (DIRECTORY = ...)))
```

2. Masterschlüssel festlegen

```
ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY <password>;
```

3. Wallet öffnen

```
ALTER SYSTEM SET ENCRYPTION WALLET OPEN IDENTIFIED BY
<password>;
```

4. Spalten verschlüsseln

```
CREATE TABLE mitarbeiter (
    name         VARCHAR2(128),
    vorname      VARCHAR2(128),
    mitID        NUMBER ENCRYPT NO SALT,
    gehalt       NUMBER(6) ENCRYPT USING '3DES168',
    provision    NUMBER(6) ENCRYPT);
```

Überwachung von Datenbankaktionen

Auditing ist die Überwachung und Aufzeichnung von ausgewählten Datenbankaktionen bezüglich

- Ausgeführter SQL-Statements
- Genutzter Privilegien
- Objektzugriff

Mit dem statischen Parameter **`AUDIT_TRAIL`** kann bestimmt werden, wohin die Informationen geschrieben werden:

- `none`: Auditing ausgeschaltet (Default)
- `os`: Audits werden in das Betriebssystem geschrieben.
- `db`: Audits werden in Datenbanktabellen geschrieben
- `db,extended`: zusätzlich SQL-Text und Binds
- `xml`: XML-Dateien im Betriebssystem
- `xml,extended`: zusätzlich SQL-Text und Binds

Informationen können bei Auditing in die Datenbank mit der View **`DBA_AUDIT_TRAIL`** abgefragt werden.

Auditing – Syntax

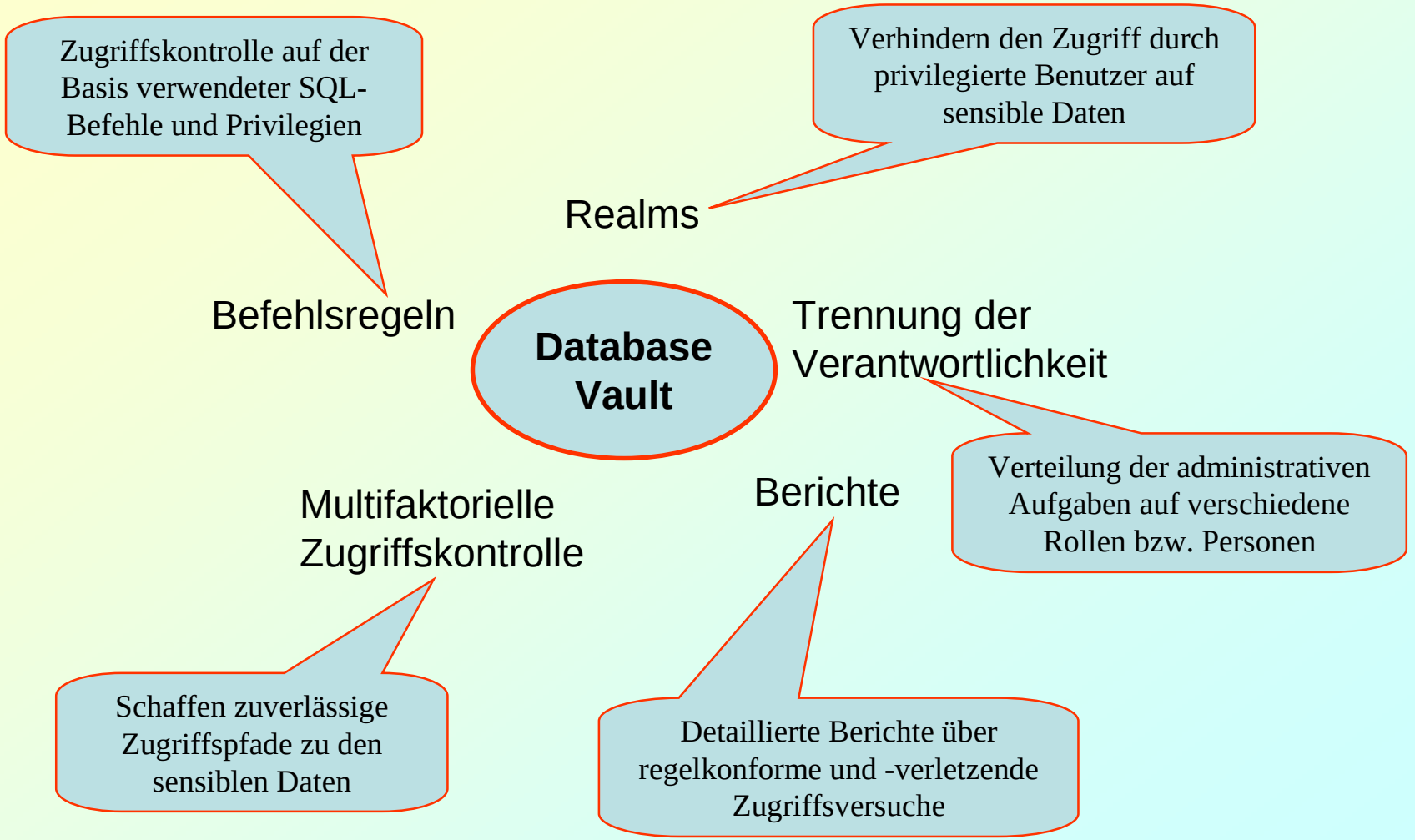
```
AUDIT { sql_statement_clause | schema_object_clause |
    NETWORK }
    [ BY { SESSION | ACCESS } ] [ WHENEVER [ NOT ]
    SUCCESSFUL ];
```

```
sql_statement_clause ::= { statement_option | ALL } |
    { system_privilege | ALL PRIVILEGES }
    [ BY { proxy [, … ] | user [, … ] } ]

schema_object_clause ::= { object_option [, … ] | ALL}
    auditing_on_clause

auditing_on_clause ::= ON { [ schema.]object |
    DIRECTORY directory_name | DEFAULT }
```

Database Vault – Übersicht



Gesetzliche Regelungen und Database Vault

Ausgewählte Gesetze und Standards:

- Sarbanes-Oxley
- Gramm-Leach-Bliley
- Basel II – Internal Risk Management
- PCI DSS (Payment Card Industry Data Security Standard
- Japan Privacy Law

Forderungen von **PCI DSS**, denen Database Vault genügt:

- Zugriff auf Kreditkartendaten nur für autorisierte Nutzer
- Beschränkung von Wartungsmaßnahmen auf bestimmte Zeitfenster
- Datenzugriff eingeschränkt auf definierte
  - IP- und Mac-Adresse
  - Applikation bzw.Service
  - Benutzer-Accounts und –gruppen
- Jede Einheit darf nur Zugang zu den Kreditkartendaten der „eigenen“ Kunden haben (Mandantentrennung)

Database Vault – Grundlagen

- Voraussetzungen
  - Datenbank mindestens 9.2.0.8
  - Label Security installiert (optional)
  - Enterprise Manager Database Control installiert und konfiguriert
- Geänderte Standardeinstellungen z.B.
  - Geänderte Initialisierungsparameter: `AUDIT_SYS_OPERATIONS=TRUE` und nicht mehr `FALSE`
  - Der User SYS hat keine Recht auf `ALTER SESSION` mehr.
  - Das Package DBMS_RLS (Label Security) gehört jetzt dem Database Vault Administrator
  - EXECUTE auf UTL_FILE nicht mehr an PUBLIC vergeben
- Neue Schemata
  - DVSYS: Eigentümer des Oracle Database Vault Schemas
  - DVF: Eigentümer der Oracle Database Vault Faktorfunktionen

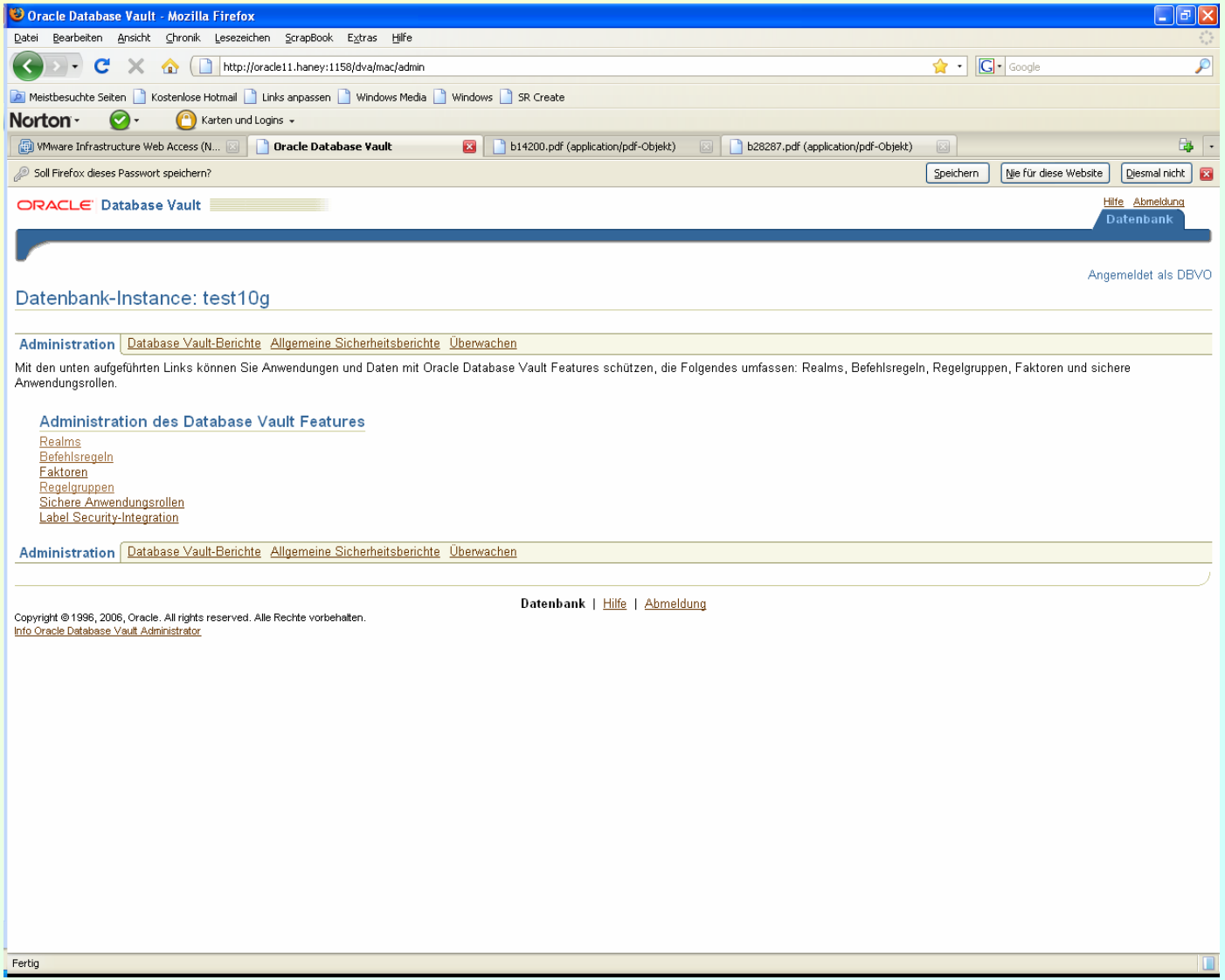
Trennung der Verantwortlichkeiten

- Neue Rollen
  - DV_OWNER: Oracle Database Vault Owner Role
  - DV_REALM_OWNER: Oracle Database Vault Realm DBA Role
  - DV_REALM_RESOURCE: Oracle Database Vault Application Resource Owner Role
  - DV_ADMIN: Oracle Database Vault Configuration Administrator Role
  - DV_ACCTMGR: Oracle Database Vault Account Manager Role
  - DV_SECANALYST: Oracle Database Vault Security Analyst Role
  - DV_PUBLIC: Oracle Database Vault PUBLIC Role
- Vertrauenswürdige Accounts
  - DV_ACCTMGR role
  - DV_OWNER role
  - SYSDBA privilege
  - SYSOPER privilege
- Accounts und Rollen nur an vertrauenswürdige Individuen vergeben
  - User mit Root-Zugriff auf das Betriebssystem
  - Eigentümer der Oracle Software
  - SYSDBA-Zugriff
  - SYSOPER-Zugriff

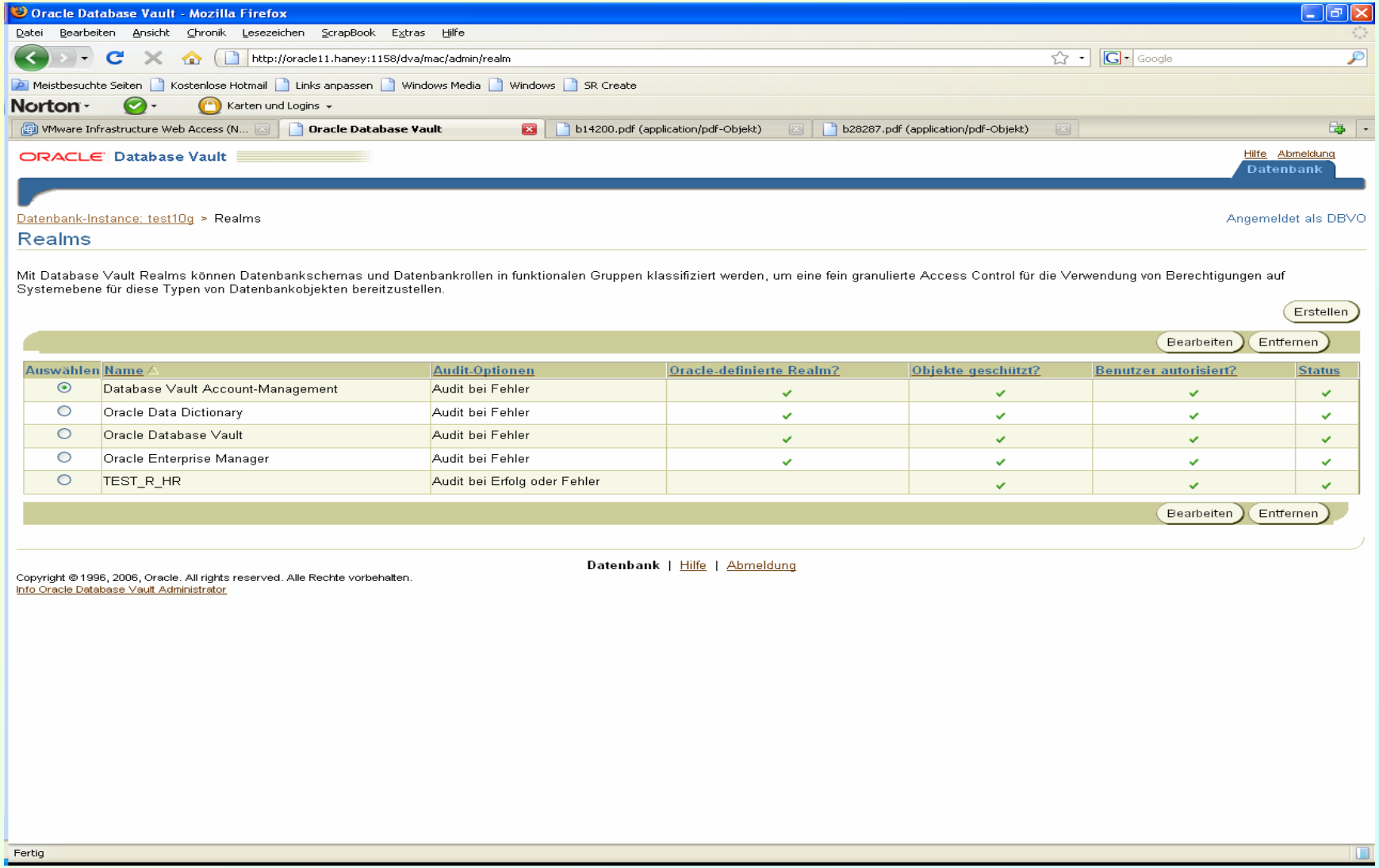
Sicherheitsrichtlinien im Umfeld von Database Vault

1. Zugriff auf die Packages UTL_FILE und DBMS_FILE_TRANSFER begrenzen
2. Eingeschränkter Zugriff auf den Recycle Bin
3. Besondere Vorsicht beim Umgang mit den Privilegien CREATE ANY JOB and CREATE JOB
4. Vorsicht beim Privileg CREATE EXTERNAL JOB
5. Unbedingt den Zugriff auf das Package LogMiner beschränken
6. Die Verwendung der Privilegien ALTER SYSTEM und ALTER SESSION beschränken
7. Vorsicht mit Java Stored Procedures
8. Vorsicht bei externen C-Programmen in der Datenbank

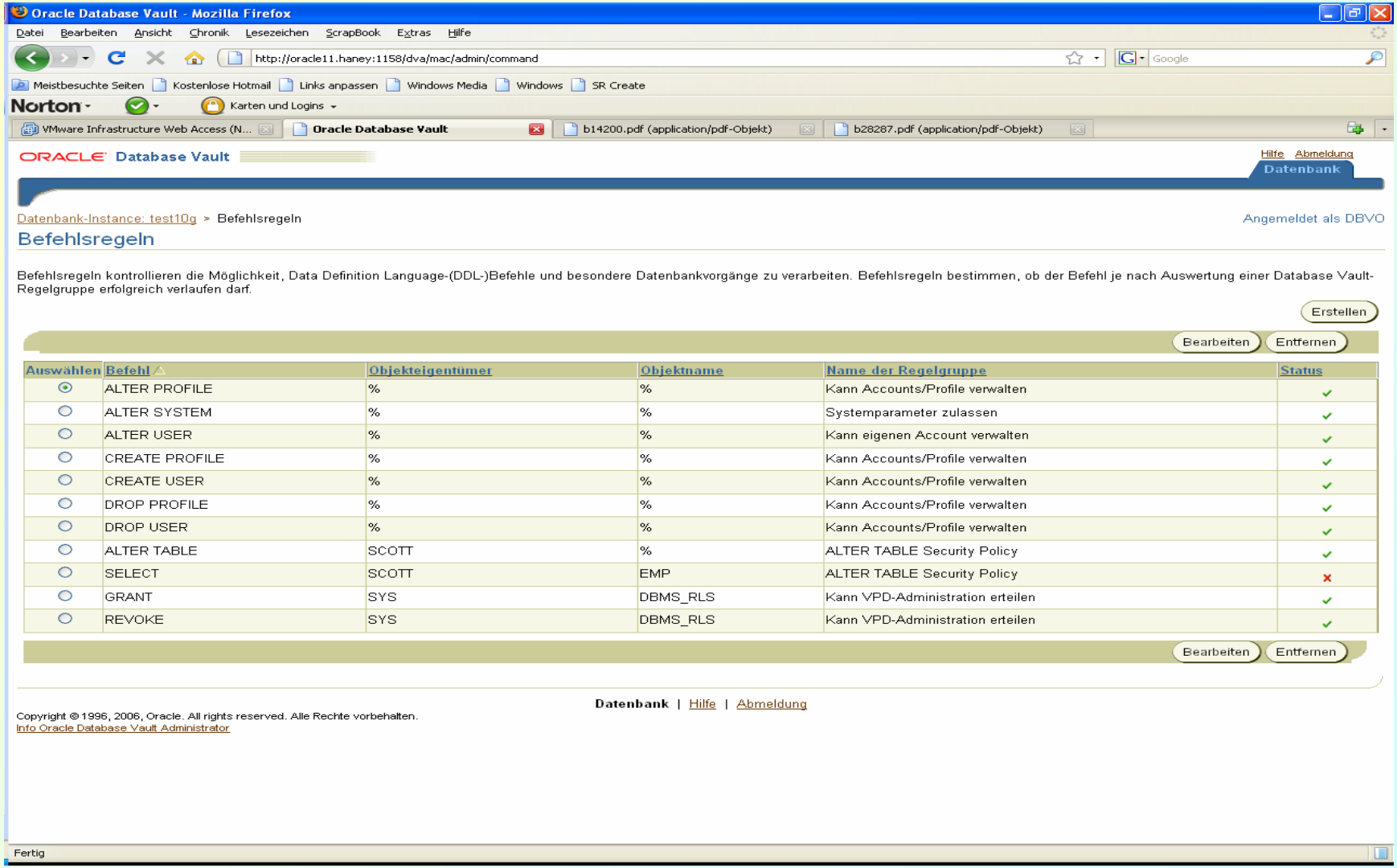
Administration mit dem DVA



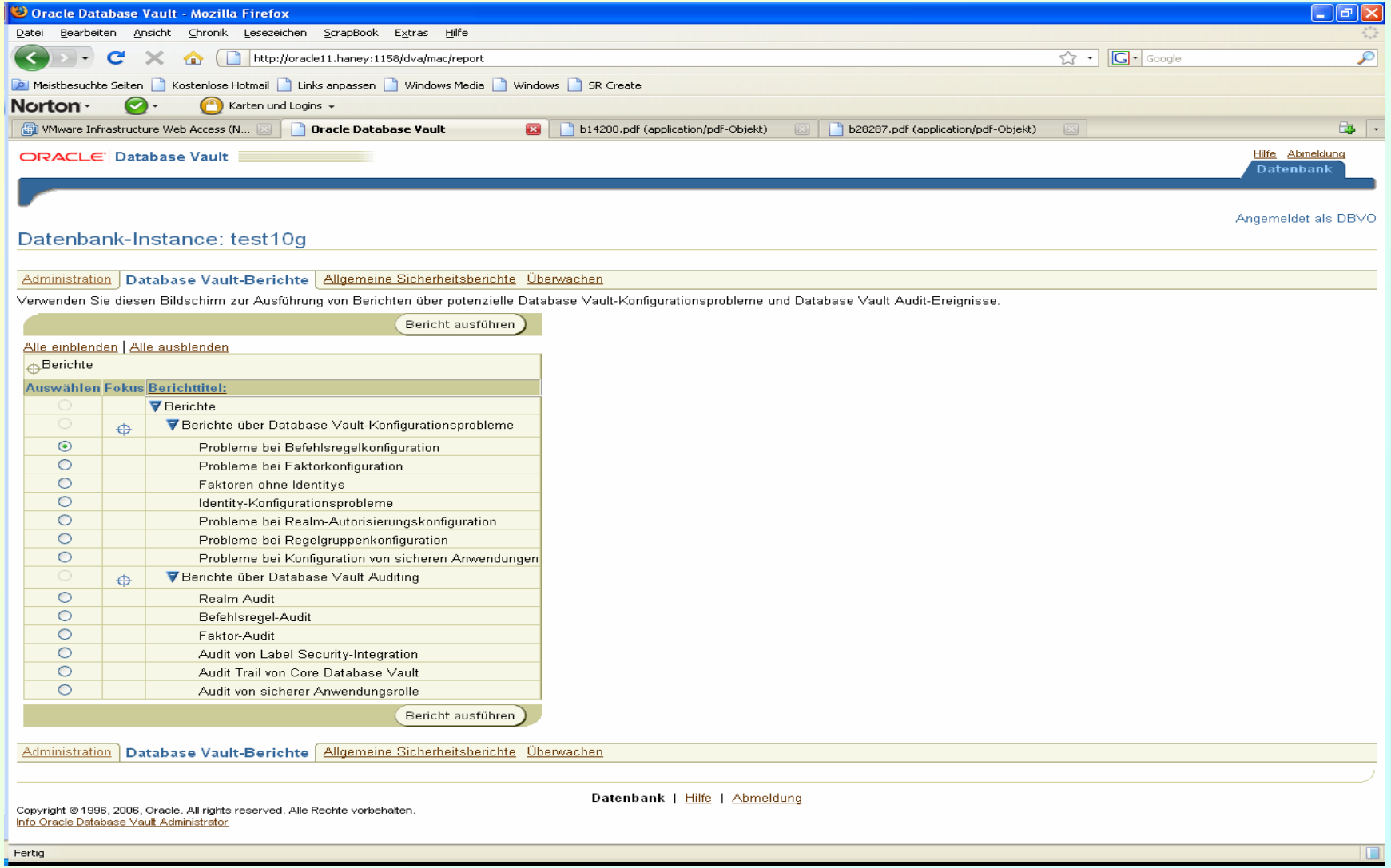
Sicherheitsbereiche (Realms) im DVA



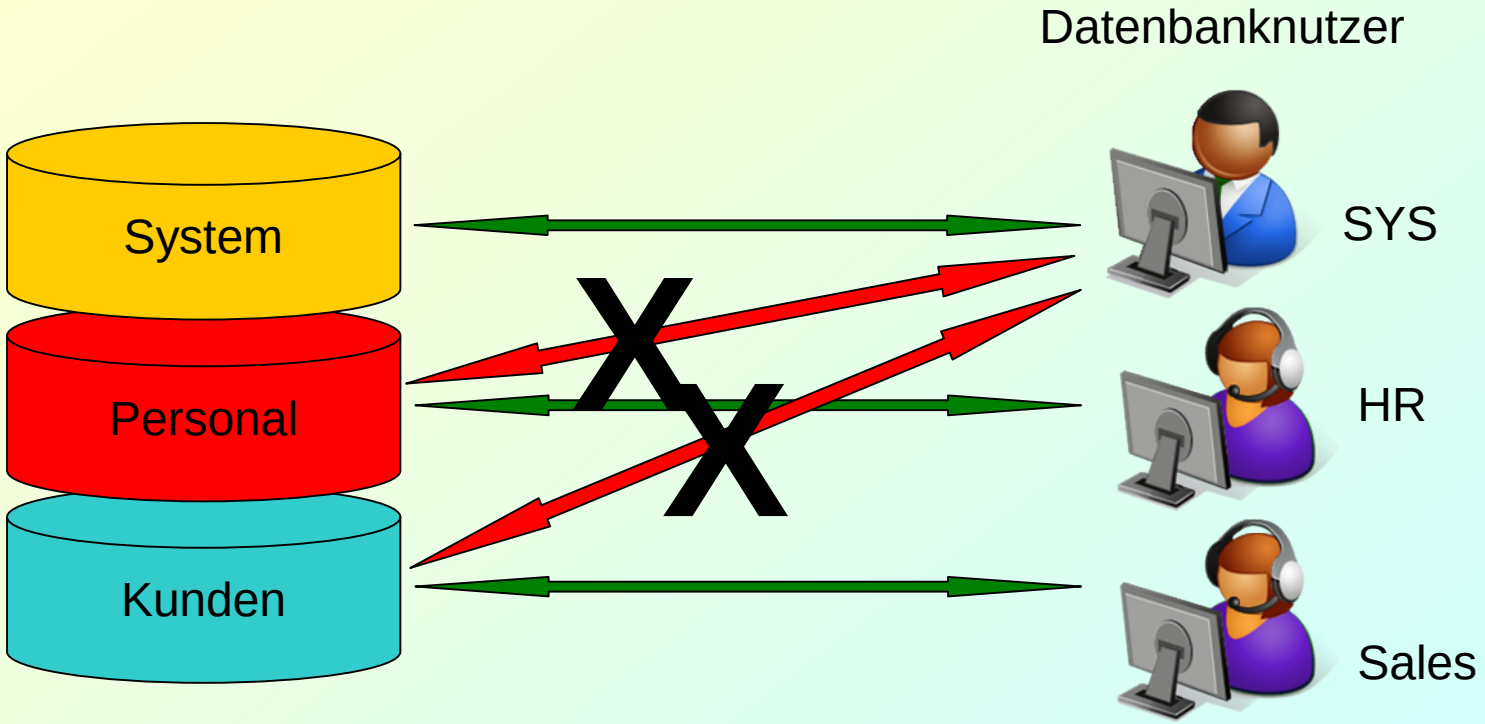
Befehlsregeln im DVA



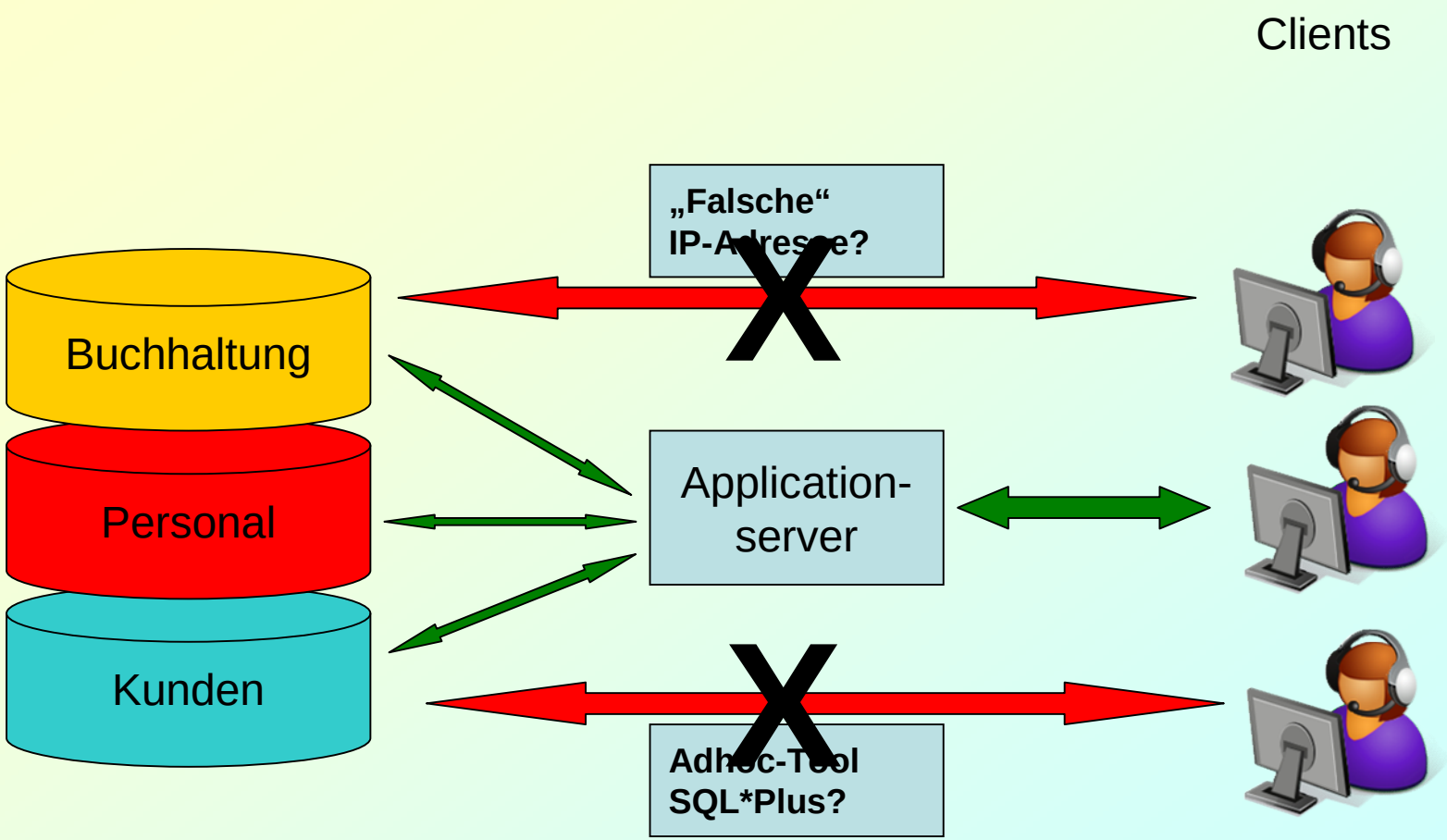
Sicherheitberichte



Oracle Database Vault Realms



Command Rules und multifaktorielle Authorisierung



Neu in Version 11 Release 2

1. Integration in den Enterprise Manager (Database Control 11.2 und Grid Control 10.2.0.5)
2. Unterstützung von Datapump
3. Unterstützung des Schedulers (Scheduler Jobs)
4. Neue Database Vault Rollen
5. Zusätzliche Standard Rule Sets
6. RMAN-Unterstützung
7. Stärkerer Schutz des Schemas DVSYS
8. Neue Standardeinstellungen, z.B. RECYCLEBIN jetzt OFF

Literatur

- OTN http://www.oracle.com/technology/deploy/security/database-security/
  - ~/maximum-security-architecture.html
  - ~/oracle-pci.html
  - ~/advanced-security/index.html
- Oracle11*g* Database Online Documentation Release 2 und 10g Release 2, vor allem folgende Teile:
  - Database Vault Administrator's Guide
  - Security Guide
  - Advanced Security Administrator's Guide

Dr. Frank Haney
info@it-haney.de
Tel.: 03641-210224