Data Management

IBM Database Encryption Expert

Radomír Hůlka
IBM Information Management
radomir_hulka@cz.ibm.com

Why Encrypt Data? Industry Regulations

Payment Card Industry (PCI) Requirements…

1	Install and maintain a firewall	7	Restrict access to data by business need-to-know
2	Do not use vendor-supplied defaults for passwords. Develop configuration standards	8	Assign a unique ID to each person with computer access
3	Protect stored data *Encrypt cardholder number*	9	Restrict physical access to cardholder data
4	Encrypt transmission of cardholder data across public networks	10	Track and monitor all access to network resources and cardholder data
5	Use and regularly update anti-virus software	11	Systems should be tested to ensure security is maintained over time and through changes
6	Develop and maintain secure systems and applications	12	Maintain an information security policy

IBM Database Encryption Expert can help

IBM Encryptin Expert powered by Vormetric

- **The product was developed together with company Vormetric**
- **IBM closed partnership with Vormetric in 2007 and started development data security systém for IBM databases**

The Data Threats – Data at Rest & Data in Transit

- **Online – internal threats**
  - Attackers breaking through perimeter security
  - Privileged user abuse
  - Data replicates to many locations
- **Offline – theft and loss**
  - Backups typically written to portable media
  - Often stored offsite for long periods

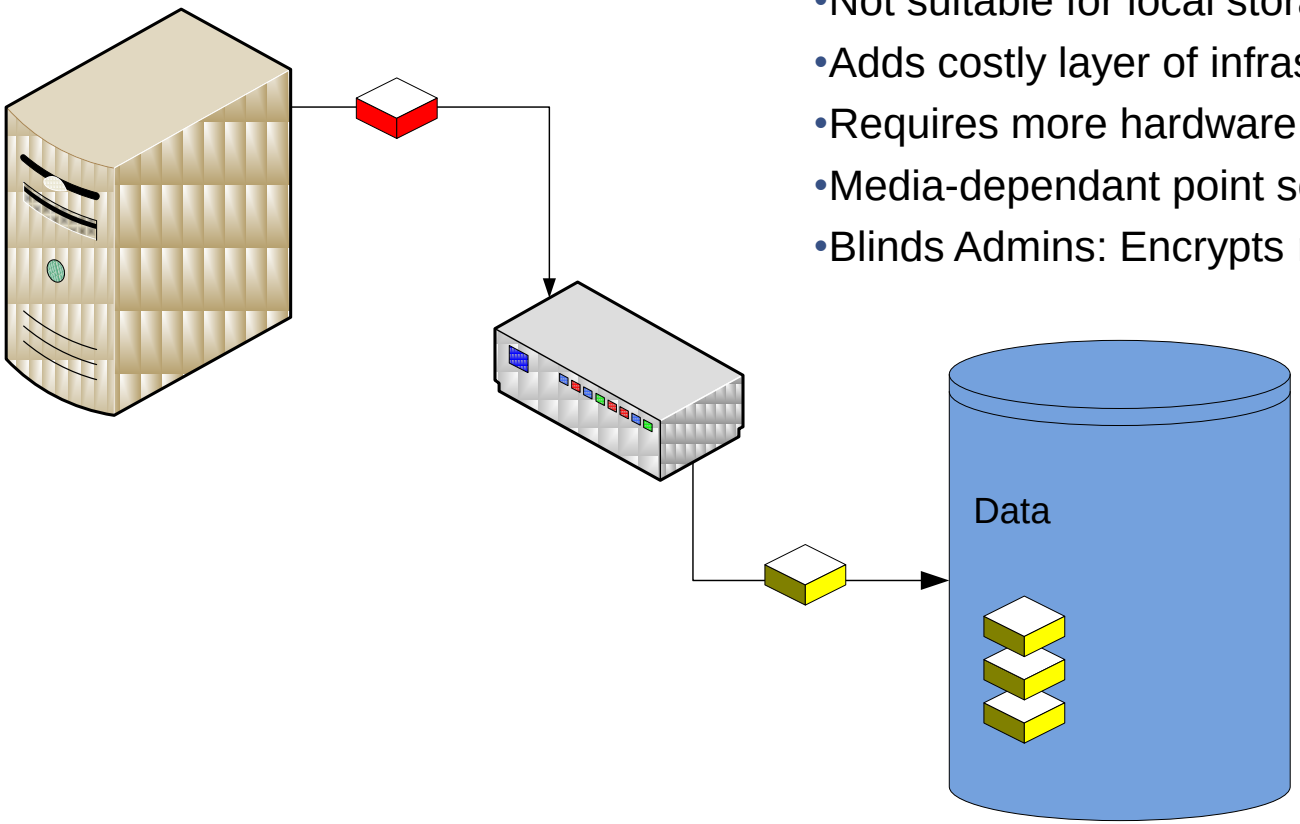
- **Onwire – internal and external threats**
  - Hackers and sniffers picking data off the network

Encryption Technologies

- **Inline Encryptors – Block device encryptors**
  - Application/Database Transparency
  - Limited threat capabilities (theft of storage device)
  - Limited key management and auditing
- **Column Encryption**
  - OS Transparency
  - Affects application development, database design, SQL Plans, and performance
  - Limited to database data only data
- **Application Encryptors**
  - Feature Rich
  - Application Intrusive (application code changes required)
  - Affects application development, database design, SQL Plans, and performance
  - Purchased Applications will not work
- **File & Tablespace & Backup Encryption**
  - Application Transparency
  - Feature Rich
  - OS Dependent
  - No DBMS security independent

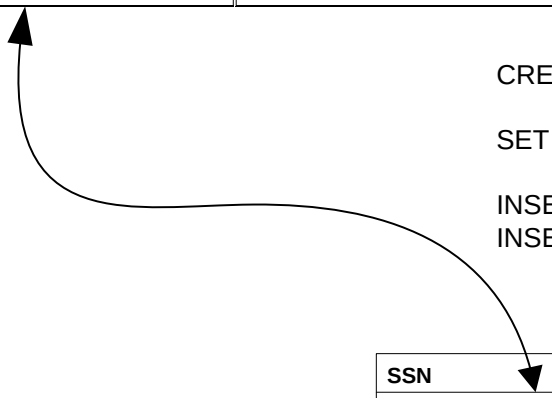
Inline Encryptors

- **Advantages**
  - Protects against physical theft
- **Disadvantages**
  - Does not address logical threats
  - Not suitable for local storage
  - Adds costly layer of infrastructure
  - Requires more hardware to scale
  - Media-dependant point solutions
  - Blinds Admins: Encrypts meta-data



Column encryption

SSN	LAST_NAME	FIRST_NAME
111-11-1111	**Shum**	Sue
222-22-2222	**Black**	Joe
333-33-3333	**Edward**	Ed
444-44-4444	**Smith**	Lawrence
555-55-5555	**Farik**	Kalib

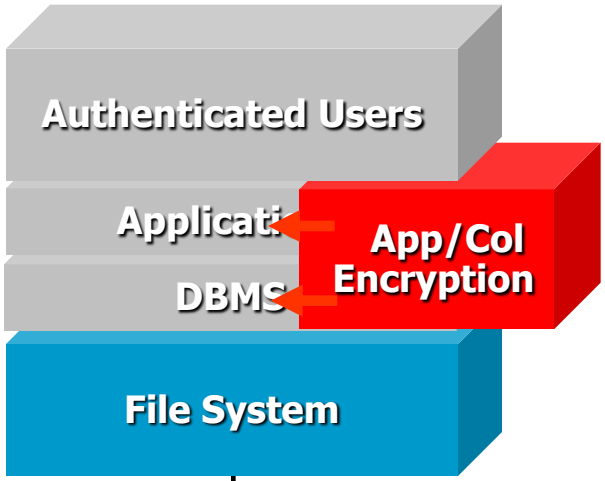


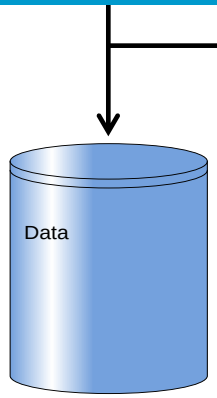
```
CREATE TABLE EMP (SSN VARCHAR(24) FOR BIT DATA,
        LAST_NAME CHAR(30), FIRST_NAME CHAR(30));
SET ENCRYPTION PASSWORD = 'Ben123';

INSERT INTO EMP(SSN) VALUES ENCRYPT('289-46-8832');
INSERT INTO EMP(SSN) VALUES ENCRYPT('289-46-8832','Ben123');
```

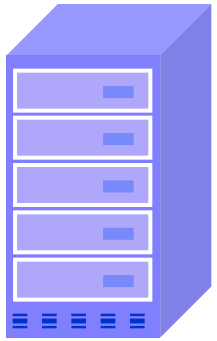
SSN	LAST_NAME	FIRST_NAME
Lk3#$%mvo@	**Shum**	Sue
#Favci?43ifno	**Black**	Joe
#Akjoi$#nsvo	**Edward**	Ed
#W$niw3.a9984	**Smith**	Lawrence
A##$fn@a40009	**Farik**	Kalib

Competition – Application/Column Encryption





Direct Attached Storage



SAN/NAS/Tape

- **Advantages**
  - Field/Column level granularity
  - Blind DBA if RDBMS access control fails
- **Disadvantages**
  - Highly Invasive - Development & Integration
  - High Performance Degradation
  - Key management and security challenges
  - What did you forget to encrypt?
  - Packaged App integration & maint. issues

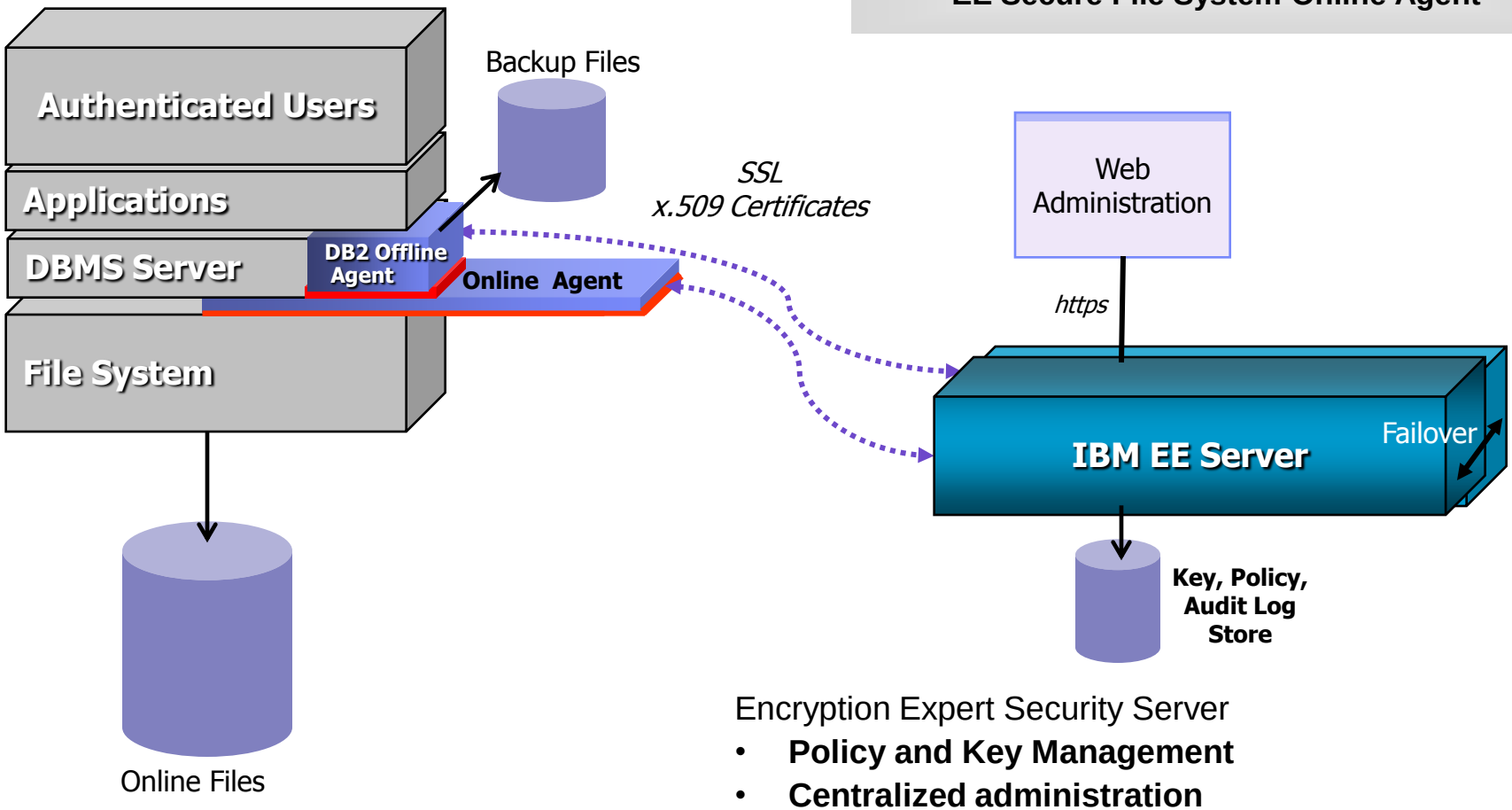
What is IBM Database Encryption Expert?

- **Data protection for your database environments**
  - High performance encryption, access control and auditing
  - Data privacy for both online and backup environments
  - Unified policy and key management for centralized administration across multiple data servers
- **Transparency to users, databases, applications, storage**
  - No coding or changes to existing IT infrastructure
  - Protect data in any storage environment
  - User access to data same as before
- **Centralized administration**
  - Policy and Key management
  - Audit logs
  - High Availability

Encryption Expert Architecture

Components:

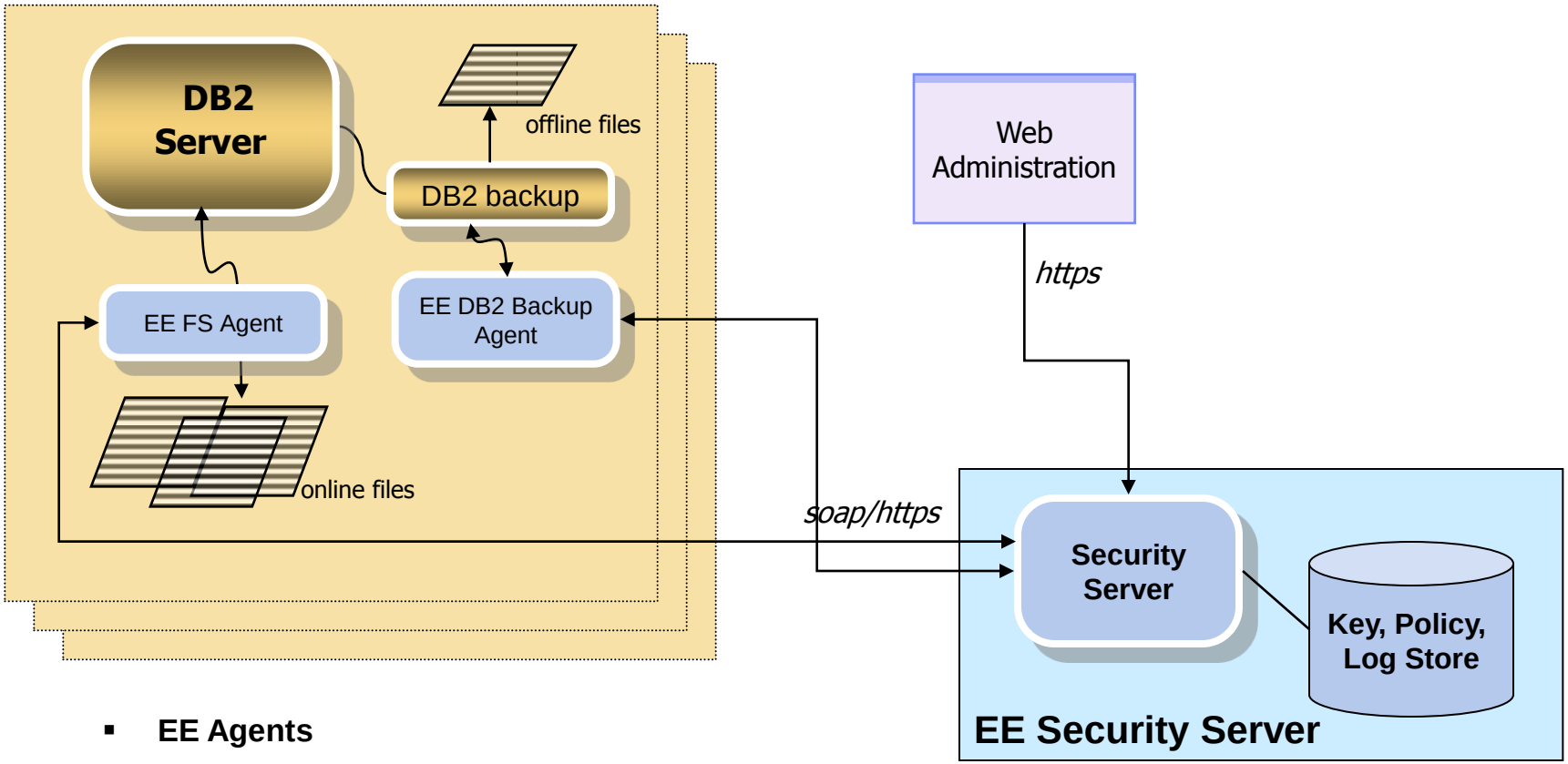
- **EE Security Server**
- **EE Secure Offline Agent**
- **EE Secure File System Online Agent**



Encryption Expert Security Server

- **Policy and Key Management**
- **Centralized administration**
- **Separation of duties**

Encryption Expert Architecture



- **EE Agents**
  - Communicates with security server to enforce policy
  - Encrypts data, controls access
  - Send audit events to server

- **Security Server**
  - Key and Policy Management
  - Centralized Audit Logs
  - High Availability (failover support)
  - Authenticates agent communication

Supported cipher algorithms

- **Symetric crypting**

  - 3DES, AES128, AES256, ARIA128, ARIA256

- **Symetric crypting**

  - RSA1024, RSA2048, RSA4096

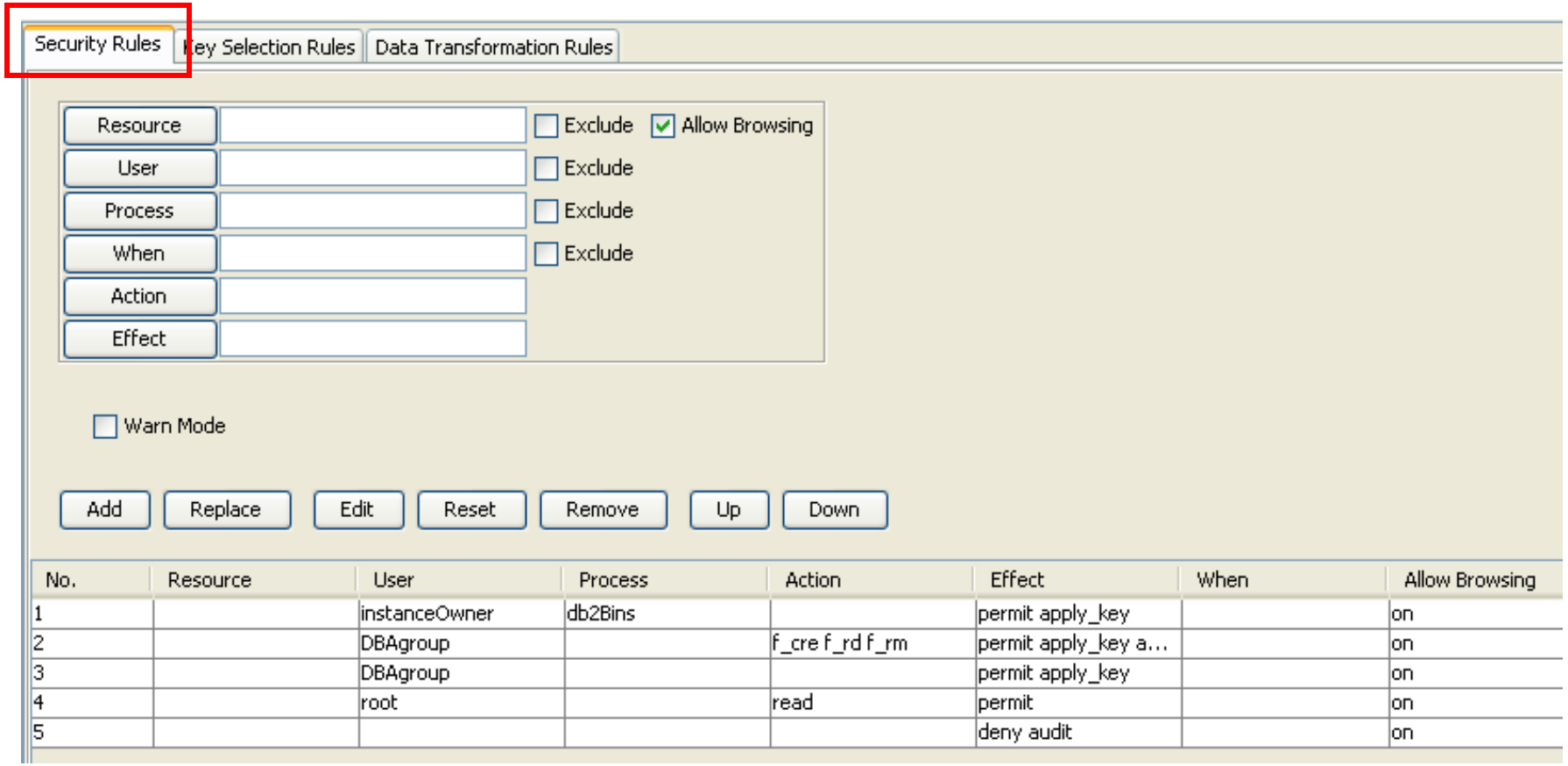
Types of Encryption Expert policies

- **Online policy**
  - **files and directories**
  - **processes**
  - **backup/restore DB2, IDS**
- **Offline policy**
  - **backup/restore DB2, IDS**

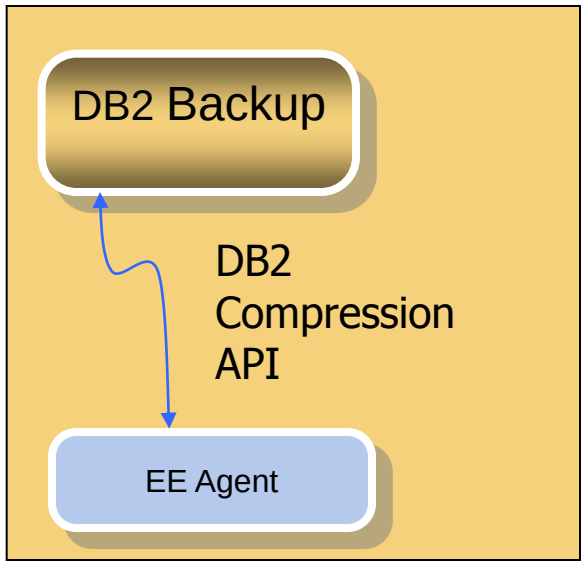
File System Policies

- A '*guardpoint'* is a mapping of a policy to a folder
- Only one policy per guardpoint
  - Can have multiple guardpoints
- The file system agent "intercepts" IO into the guardpoint and examines
  - Process
  - User/group (of process)
  - IO action (read, write, etc.)
  - Resource (what file is being accessed)
  - Time range
- Policy evaluated locally to *Permit* or *Deny*
- Controls
  - **Encryption keys**
  - **Audit**

File System Policy for DB2 Security Rules



Backup and Restore of Backup Data: Load the Agent Customized support for DB2 and IDS



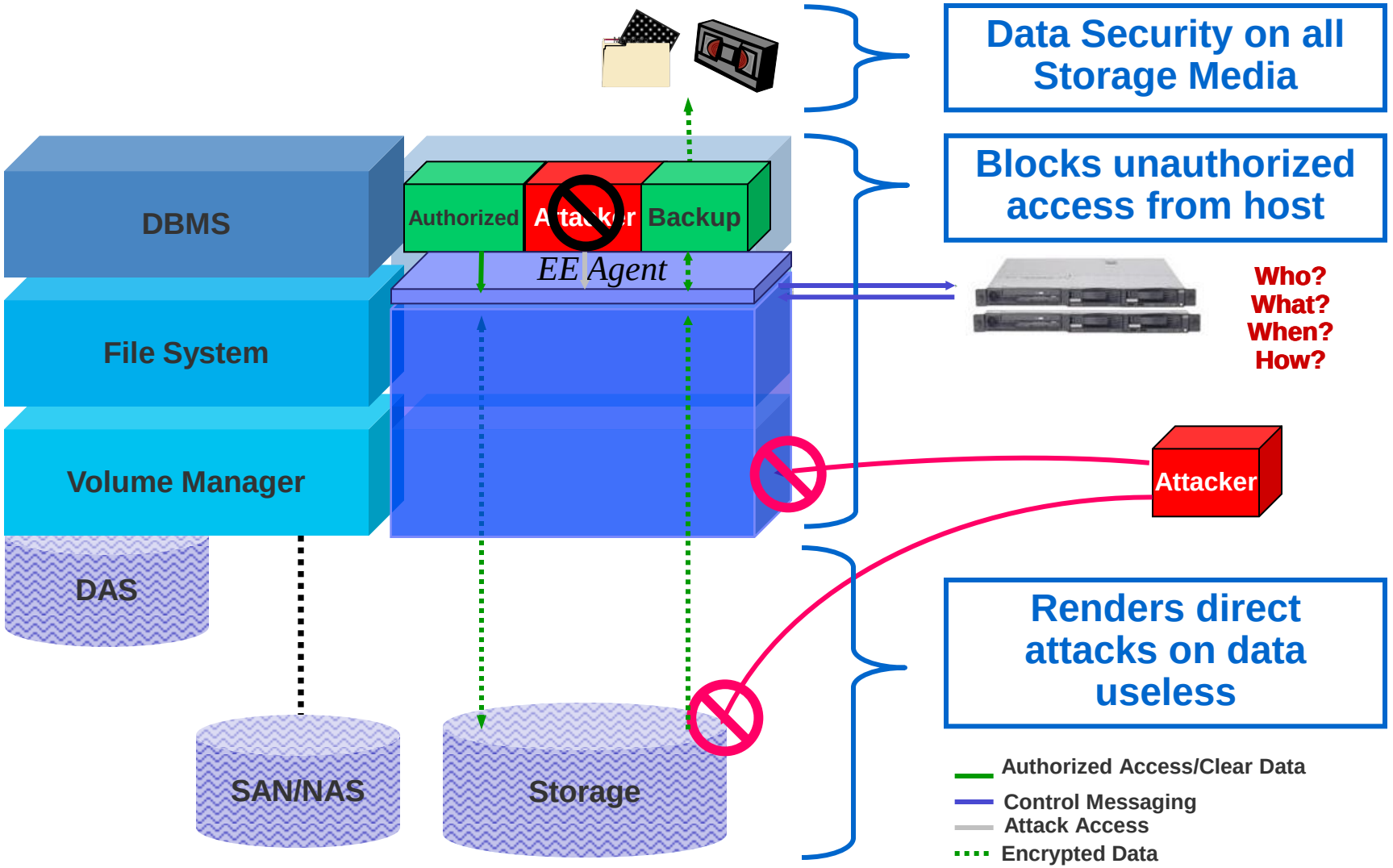
DB2 example:

- **The DB2 backup process loads the encryption expert agent**
- **The library for the agent is specified on the command line for the backup/restore operation**

example

> BACKUP DATABASE inst1 COMPRESS \ COMPRLIB /<EE install dir>/libvordb2.so

Scenarios…



Administrator Roles

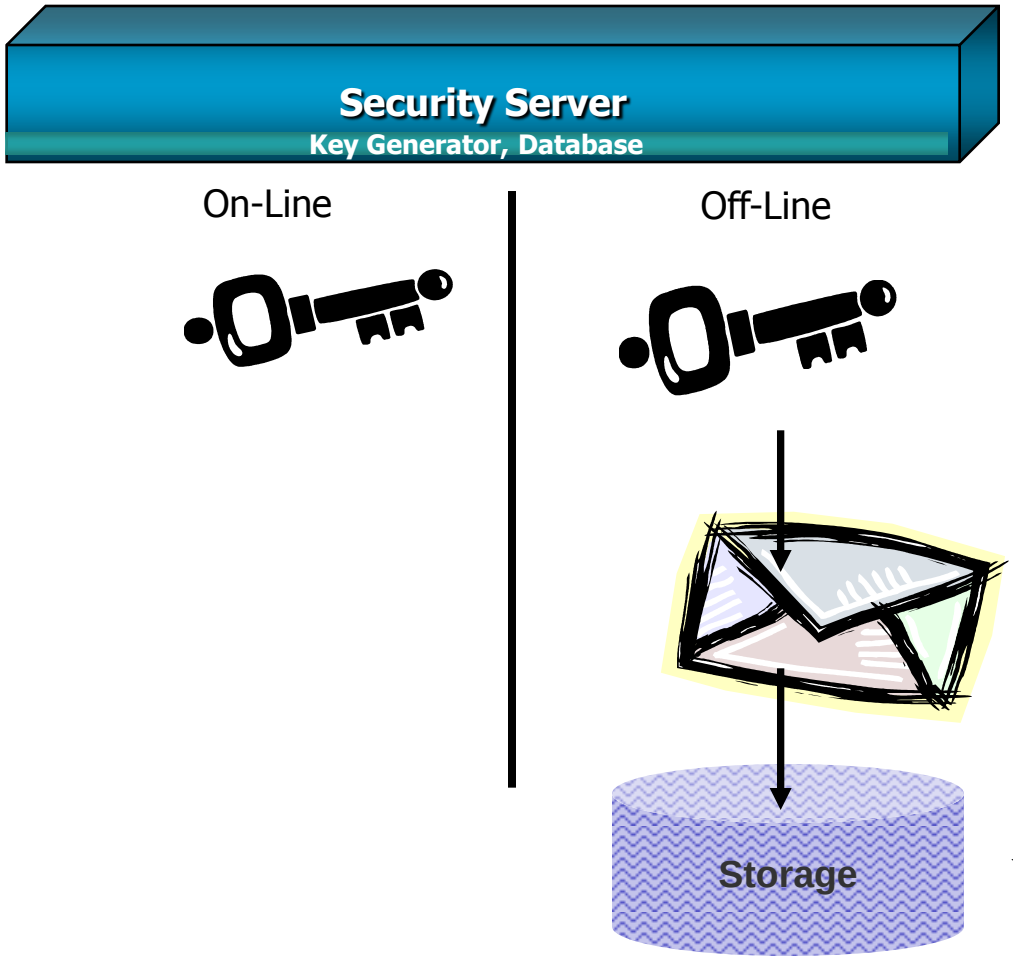
- **System administrator**
  - **creates accounts**
  - **creates domains**
  - **configures logs**
  - **configures HA**
- **Domain administrator**
  - **assignes roles to accounts**
- **Security administrator**
  - **manages policies, keys, hosts, rules**

Policy Rules

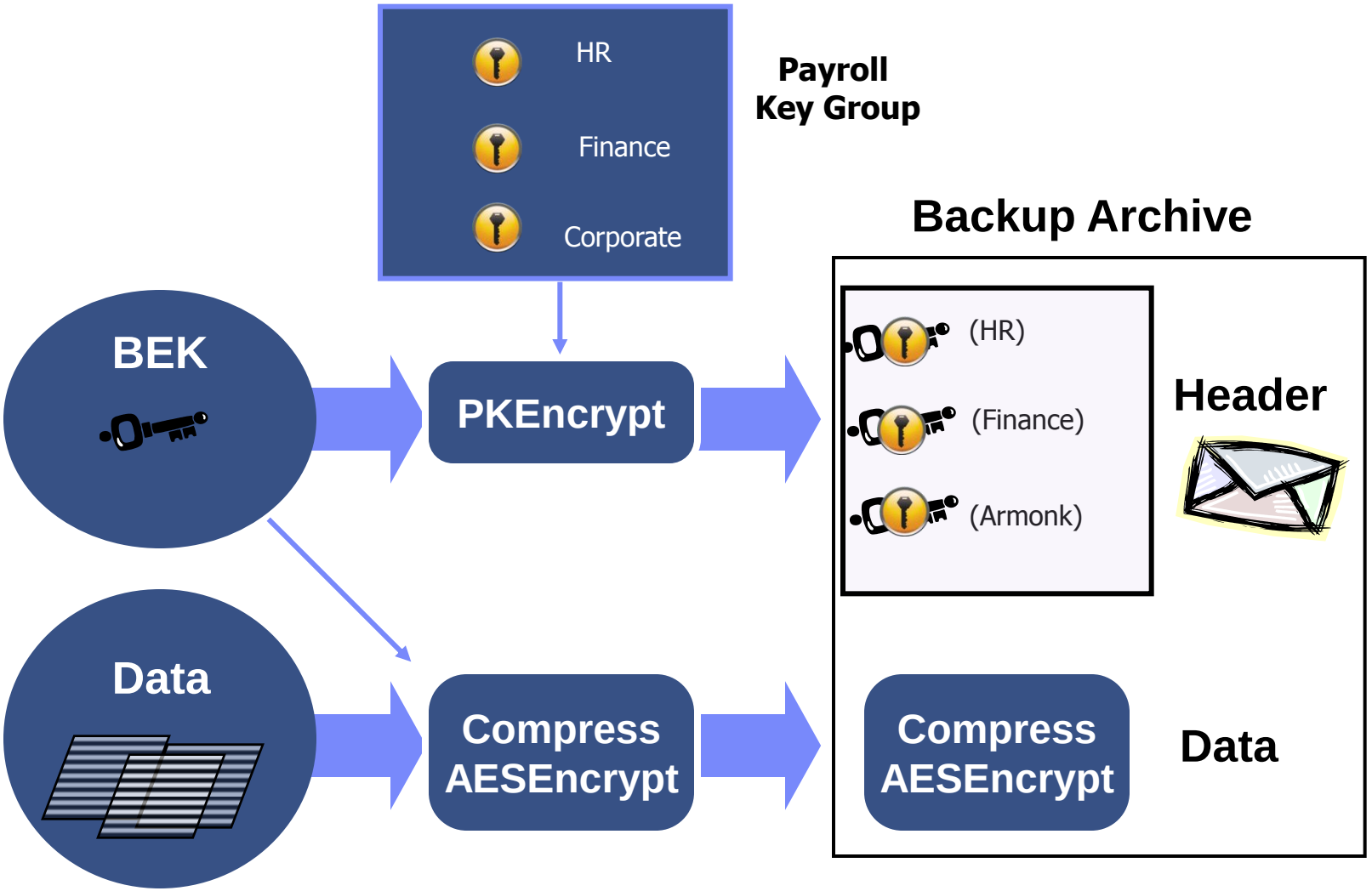
- **WHO is attempting to access protected data?**
  - Configure one or more users, groups, or applications users may invoke who can access protected data
- **WHAT data is being accessed?**
  - Configure a mix of files and directories
- **WHEN is the data being accessed?**
  - Configure a range of hours and days of the week for authorized access
- **HOW is the data being accessed?**
  - Configure allowable file system operations allowed to access the data

    e.g. read, write, delete, rename, etc.
- **EFFECT: Permit; Deny; Apply Key; Audit**

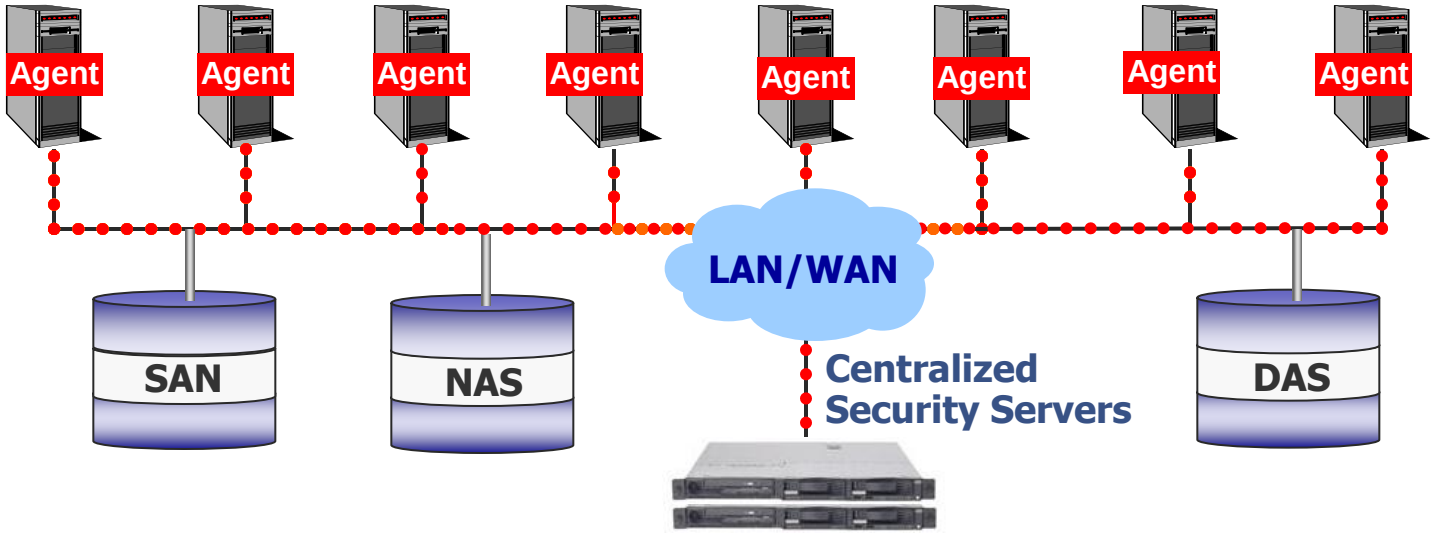
Key Management



How keys are used to create a backup



Distributed Enforcement - Centralized Management



- **Centralized Security Server:**
  - **Multiple database instances**
  - **Online and Offline**
  - **Heterogeneous databases**

Practical sample