IBM Database Encryption Expert

Überblick

Inhalt

Zielgruppen für erhöhte Datensicherheit

Einführung in den IBM Database Encryption Expert (DEE)

Schutz von Backups (Offline policies)

Schutz der online Daten (Online Policies)

Zusammenfassung

Ansprechpartner

Weitere Infos

Wer sind die Zielgruppen für erhöhte Sicherheit?

Unternehmen oder Organisationen, welche sensitive Daten speichern und verarbeiten und/oder erhöhte Anforderungen an die Einhaltung von Datenschutzrichtlinien erfüllen müssen.

Beispiele für sensitive Daten:

Kreditkarten Daten

PCI - Payment Card Industry Data Security Standard
Einhalten zahlreicher Sicherheitsbestimmungen, vielfache Audits
Banken, Versicherungen, eCommerce

Gesundheitsdaten

Krankenkassen, Verbände, Behörden

Finanzdaten

Unternehmensberatungen, (Finanz und Steuer)-Behörden

Typische „Datensammler“

Telekom

Verbindungsdaten, Internet Communities, ...

Was wäre wenn....?

… der Datenbank Admin, der System Admin (mit lese/schreib Berechtigung auf alle Dateien) direkt auf die Platte zugreift und Datenexporte, oder Tabellenbereiche unter Umgehung der Zugriffsregeln von DB2 oder SAP auf einen USB-Stick zieht und zu Hause in Ruhe auswertet (obwohl kein Lesezugriff seitens DB2, SAP gewährt wurde)...

… ein Backup auf dem Weg (elektronisch/physisch) abgegriffen wird und die Daten ausgelesen werden...

… die Platten mit Backups, Export-Dateien oder gleich der Datenbank physisch entwendet und über Betriebssystemmittel ausgelesen und ausgewertet werden....?

Das Problem sind die unverschlüsselten Daten. Ähnlich dem Diebstahl des persönlichen Adressbuches, wenn es nicht verschlossen ist (=keine Sicherheit durch anwendungsbezogenen Zugriff (DB2/SAP/...)

IBM Database Encryption Expert V1.1.3

Schutz der Daten durch Verschlüsselung, Zugriffskontrolle und Auditing

Transparent für Datenbank und Applikationen

Schutz von Daten-Sicherungen vor Einsicht und Veränderung, auch in einem ungeschützen Bereich („unterwegs“)

Schutz von online Daten

- Datenfiles der Datenbank („Tablespaces, „Containers“)
- Extrakte (Export Files, Reports, …)
- Datenbankkonfigurationen
- Tracefiles
- ....

Automatisches Schlüssel-Management

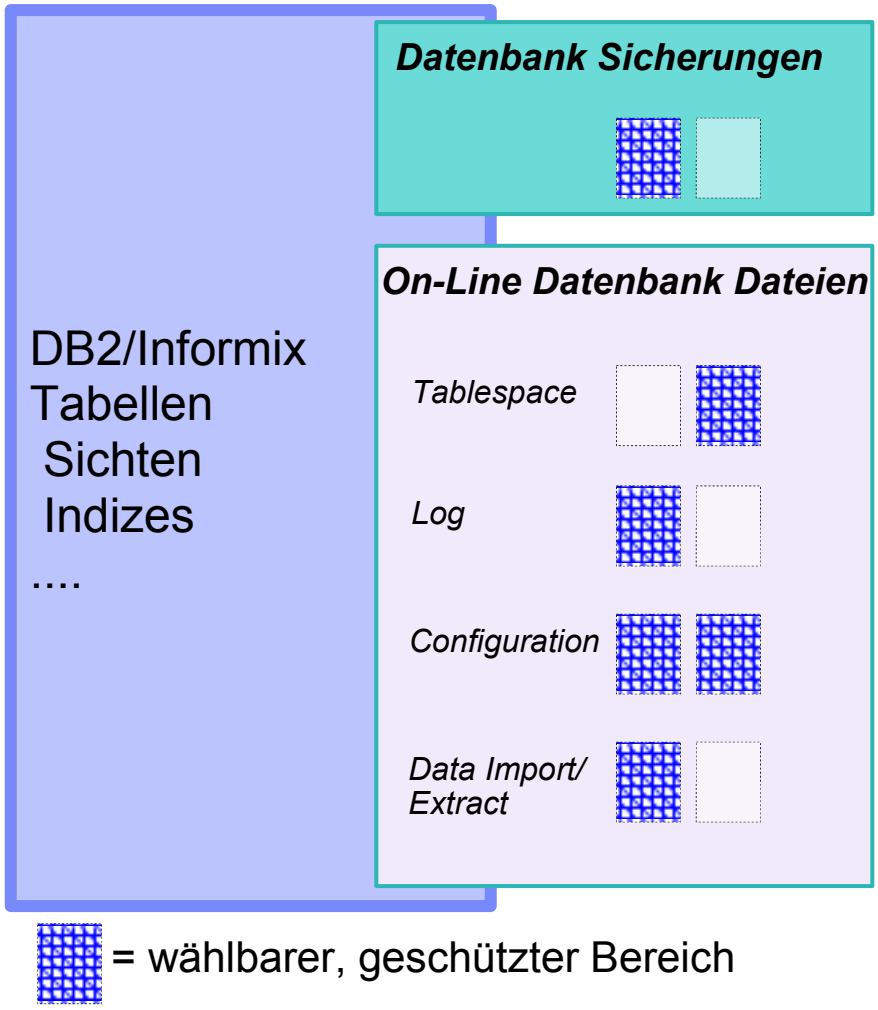
Zentralisierte, aber unaufwendige Administration

Schnell (5-12% Overhead)

DB2
- V8 Fix14+
- V9.1, V9.5

Informix
- V11.10 FC2, 11.50

Zentralisierte, feingranulare Sicherheit für DB2/Informix



Zugriffsrichtlinien

WER versucht einen Zugriff auf geschützte Daten?

Konfiguration von Benutzer(n), Guppen oder Applikationen, welche zugreifen dürfen

WELCHE Daten werden gelesen/geschrieben?

Konfiguration des Zugriffs auf Dateien/Ordner

WANN werden Daten gelesen/geschrieben?

Konfiguration von Zeitfenstern für den Zugriff

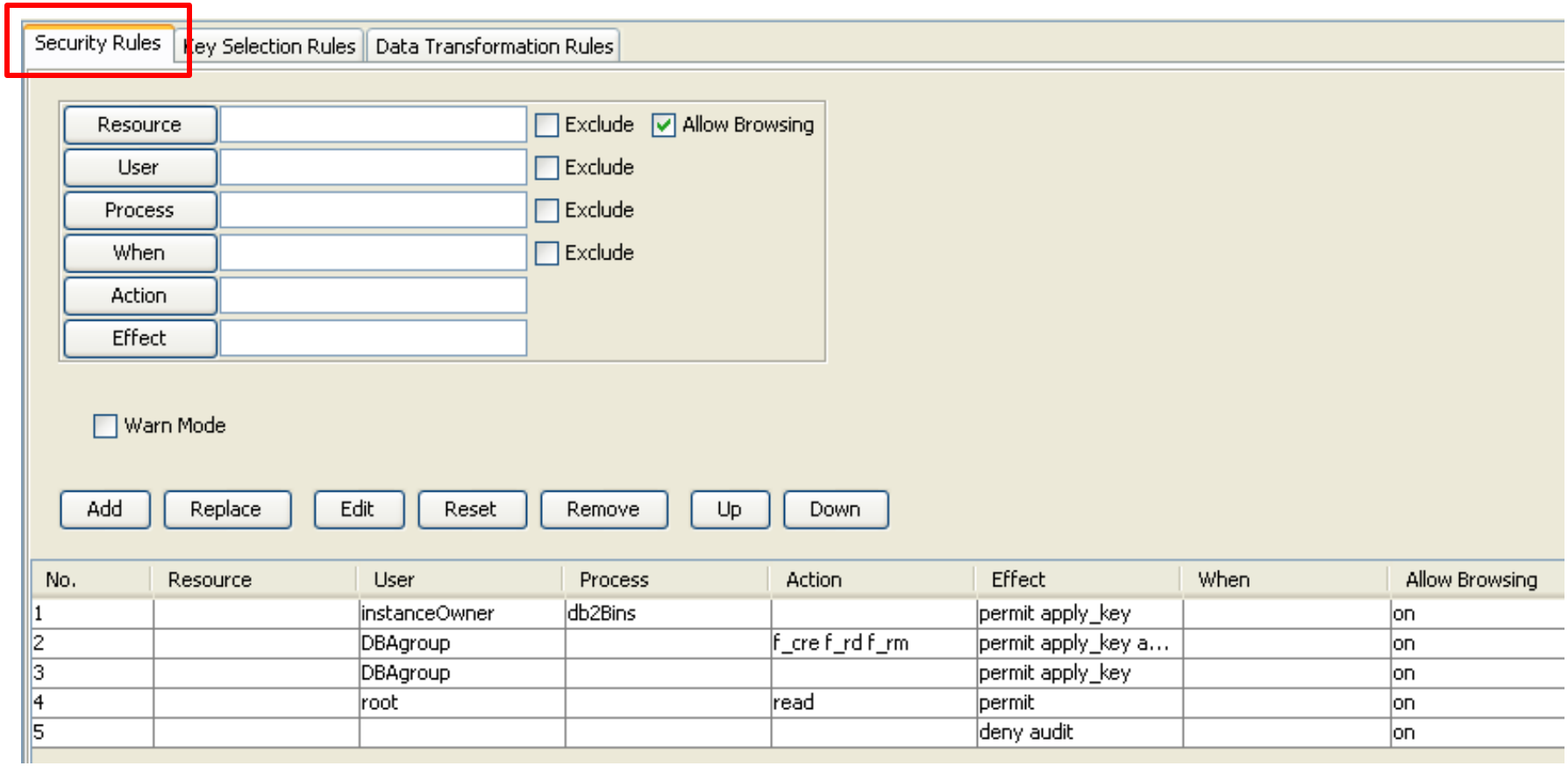
WIE wird zugegriffen?

Konfiguration der erlaubten Operationen auf Dateien/Ordnern, z.B. lesen, schreiben, umbenennen

e.g. read, write, delete, rename, etc.

WAS: Erlaube, Verbiete, Verschlüssle, Auditiere

File System Richtlinien für DB2 Security Regeln



No.	Resource	User	Process	Action	Effect	When	Allow Browsing
1		instanceOwner	db2Bins		permit apply_key		on
2		DBAgroup		f_cre f_rd f_rm	permit apply_key a...		on
3		DBAgroup			permit apply_key		on
4		root		read	permit		on
5					deny audit		on

Verschlüsselungsverfahren

Symmetrische Schlüssel

Für Online Verschlüsselung/Entschlüsselung

Für „Session Keys“ für die Verschlüsselung/Entschlüsselung von Sicherungen

AES Standard (AES128/256)

Symmetrische Verschlüsselung ist wesentlich performanter als asymmetrische

Asymmetrische Schlüssel

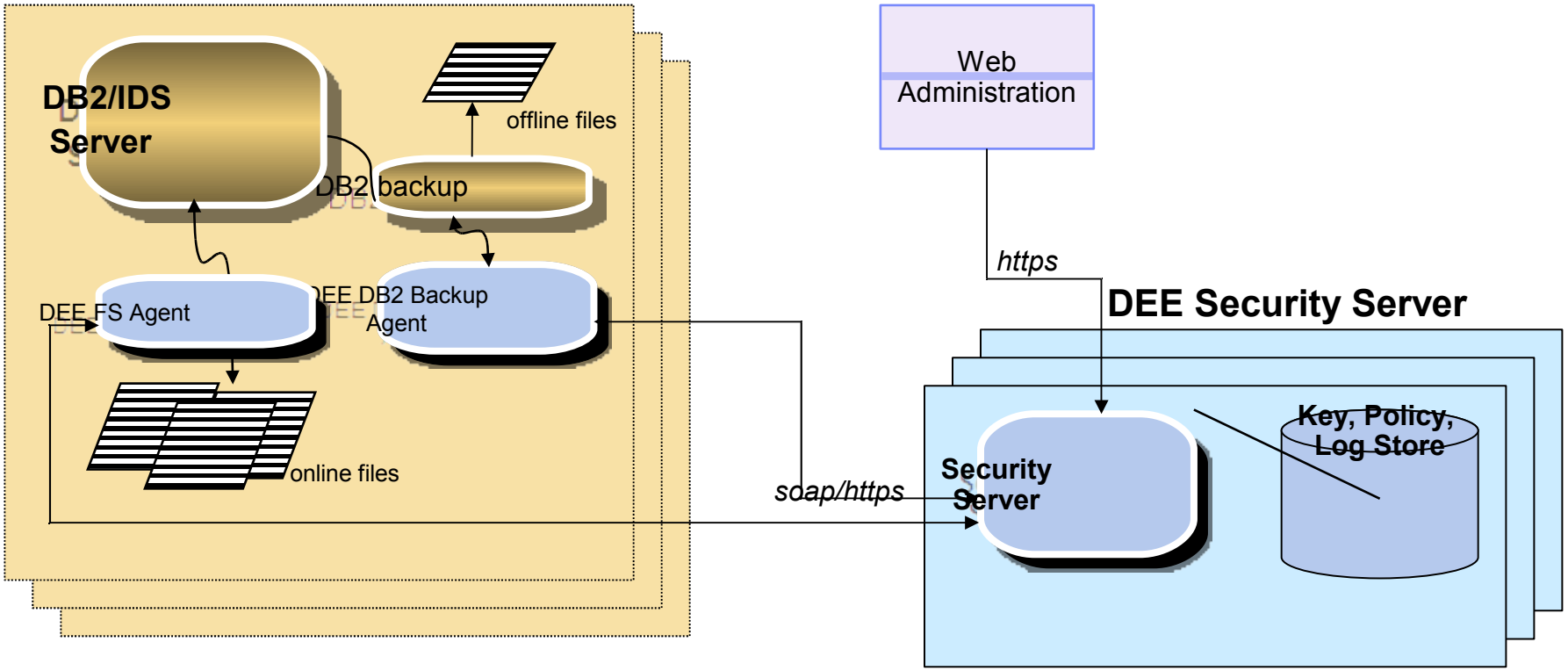
Öffentlicher Teil für die Verschlüsselung des Offline Daten “session” Keys

Privater Teil für Entschlüsselung des Offline Daten “session” Keys

RSA Standard (1024/2048/4096)

RSA – Rivest, Shamir and Adelman, first described in 1977

IBM Database Encryption Expert Architektur



EE Agenten

Kommunikation mit Security Server für das Einholen der Richtlinien (Policies)

Verschlüsselung der Daten, Auditing

Senden der Audit-Events and den Server

Security Server

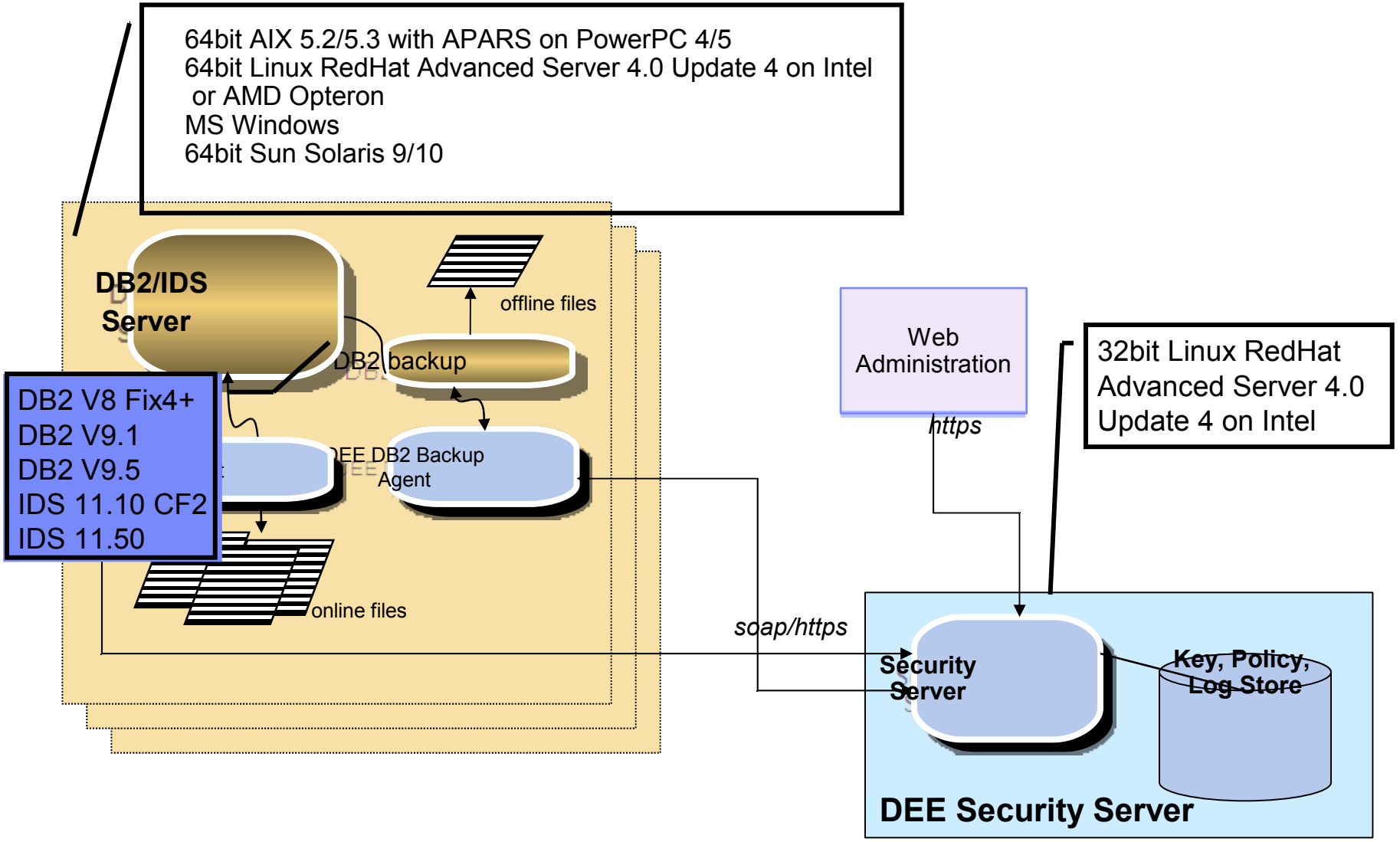
Schlüssel- und Richtlinien-Management

Zentralisierte Audit Logs

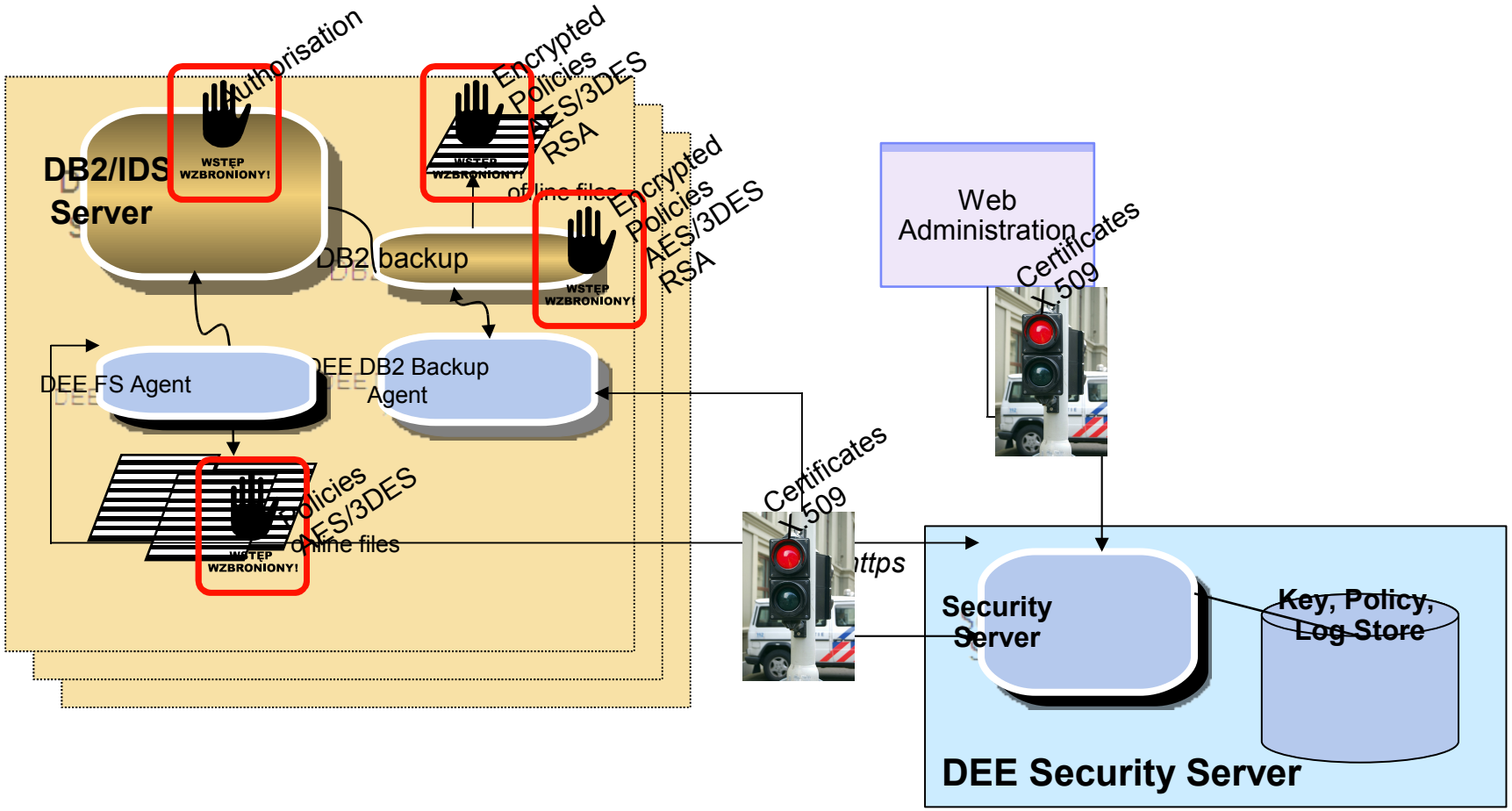
Hochverfügbarkeit (Failover Unterstützung)

Authentifiziert Agentenkommunikation

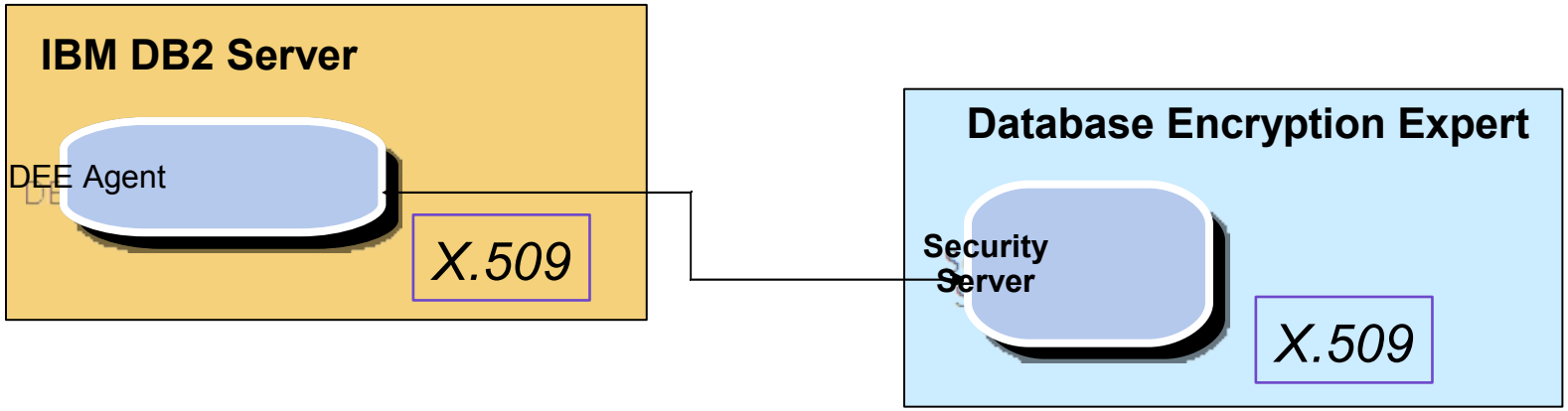
Unterstützte Plattformen



Sicherheit, Sicherheit, Sicherheit….



Agent-Server Authentifizierung

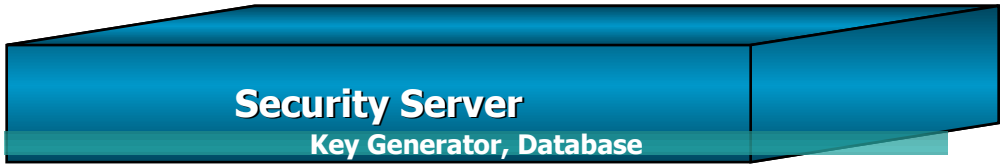


Zertifikate werden automatisch während der Installation generiert

DEE Server ist eine Certificate Authority (CA)

Gegenseitige Authentifizierung während der Richtlinien Evaluierung

Schlüssel Management

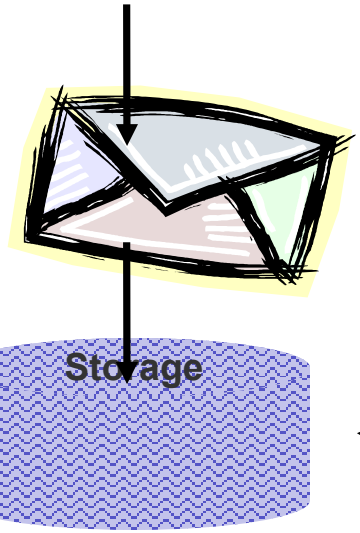


← Generiere & speichere Schlüssel
Verbinde Schlüssel mit Richtlinien

On-Line

Off-Line

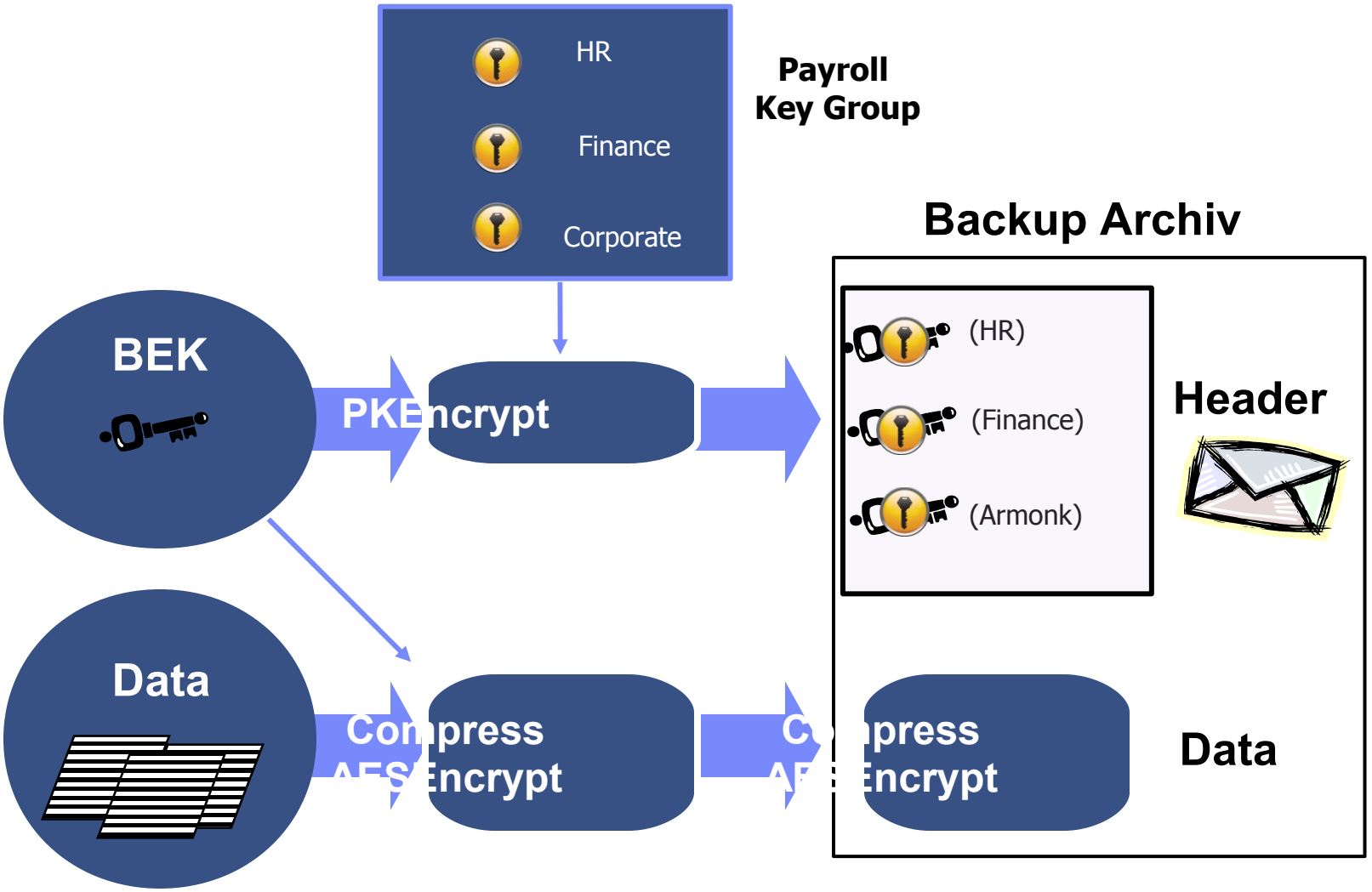
← AES 128/256 Symmetrischer Schlüssel



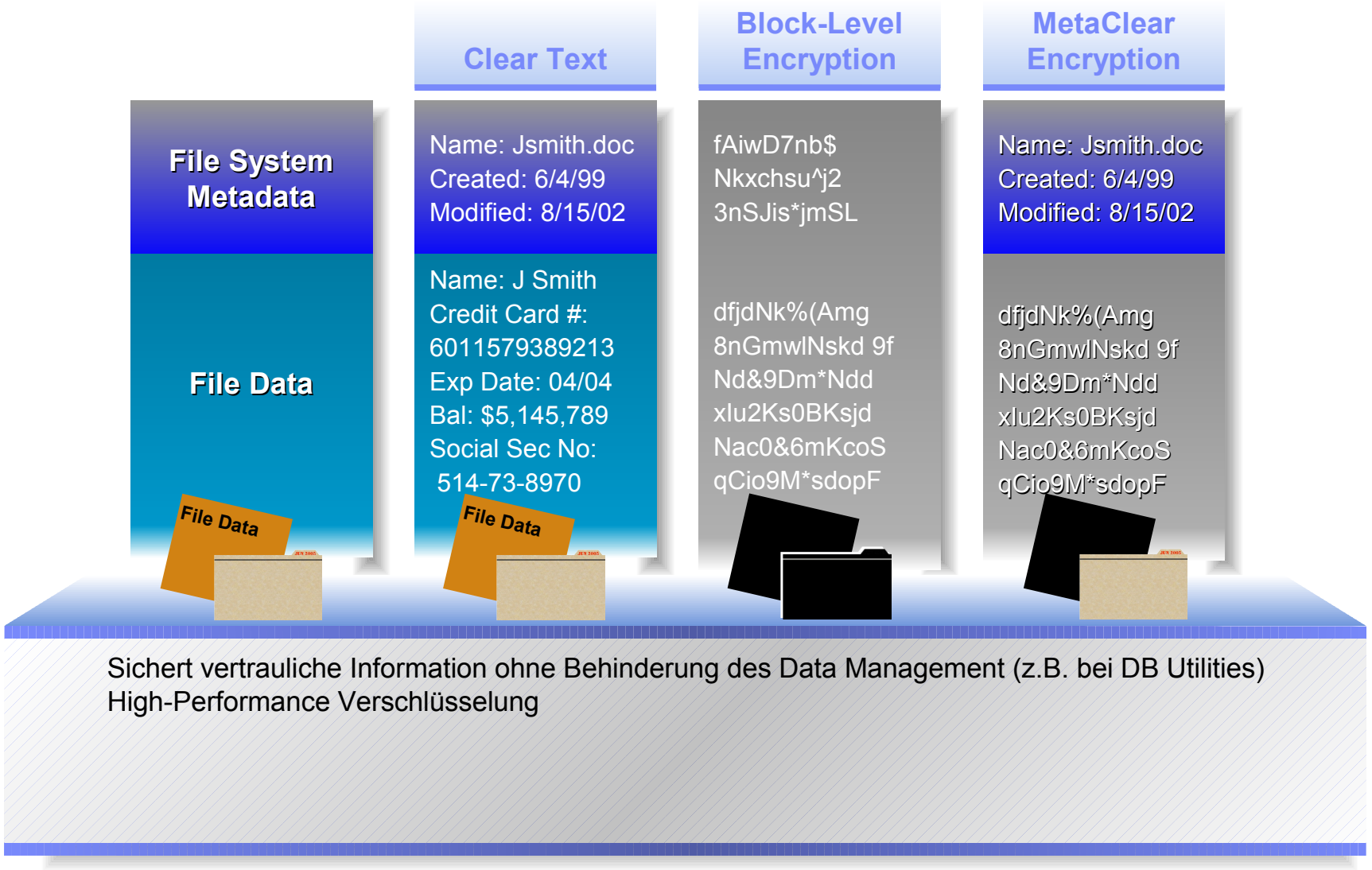
← Einpacken in asymmetrisch verschlüsselten Umschlag
RSA 1024/2096/4096

← Speichere Umschlag auf Medium

Verwendung der Schlüssel beim Backup



MetaClear™ Encryption



Sichert vertrauliche Information ohne Behinderung des Data Management (z.B. bei DB Utilities)
High-Performance Verschlüsselung

Zusammenfassung – silver bullets

IBM Database Encryption Expert ermöglicht hohe Sicherheit für:

- DB2/IDS Daten online
- DB2/IDS Daten in Datenbanksicherungen (offline)
- Sicherheit ohne Eingriffe in bestehende Applikationen oder Datenbanken
- Auditieren von dedizierten Zugriffen auf dedizierte Daten (Dateien)
- Hochverfügbares, zentralisiertes Schlüsselmanagement
- Grafische Benutzeroberfläche für die Verwaltung der Komponenten und Regeln

- DEE ist SAP zertifiziert

Weitere Infos

DEE Homepage
http://www-01.ibm.com/software/data/optim/database-encryption-expert/

DEE auf YouTube (suche dort auch nach „Encryption Expert für weitere)
http://www.youtube.com/watch?v=T5uqPORE_6I&feature=PlayList&p=BE4F5F8A5CCF227B&index=0&pla

Data Governance Blueprint
http://www-01.ibm.com/software/data/db2imstools/solutions/security-blueprint.html

SAP Zertifizierung von IBM DEE
http://imcomp.torolab.ibm.com/wiki/index.php/SAP_supports_IBM_Database_Encryption_Expert

IBM Database Encryption Expert: Securing data in DB2
ftp://ftp.software.ibm.com/software/data/db2imstools/whitepapers/IMW14003-USEN-01.pdf

Employing IBM Database Encryption Expert to meet encryption and access control requirements for the Payment Card Industry Data Security Standards (PCI DSS)
ftp://ftp.software.ibm.com/software/data/db2imstools/whitepapers/IMW14002-USEN-01.pdf