Informatik Aktuell

www.informatik-aktuell.de

Alkmene Verlags- und
Mediengesellschaft mbh
Wittelsbacherallee 107
60385 Frankfurt am Main

IT-Tage 2015

Schwerpunkt: Datenbanken
14.12. - 18.12.2015
Frankfurt am Main

Maic Beher:

SQL Server 2014 – Security und Verschlüsselungsmechanismen

SQL Server 2014

Security und Verschlüsselungsmechanismen
Frankfurter Datenbanktage 2015

Maic Beher

Agenda

1. **Security**
   - Wer braucht schon Sicherheit?
2. **Verschlüsselung**
   - Ich sehe was, was du nicht siehst!
3. **Kurzer Blick in die Zukunft**
   - Was wird (vielleicht) kommen!

Security

Security

- Arbeiten mit Dienstkonten
- SPN und Kerberos
- Datenbankbenutzer
- Exkurs: Verschlüsselung
- Anmeldungen in Contained Databases
- Datenbankbenutzer mit Zertifikaten

Security– Arbeiten mit Dienstkonten

Konten zum Starten und Ausführen von SQL Server basierten Diensten

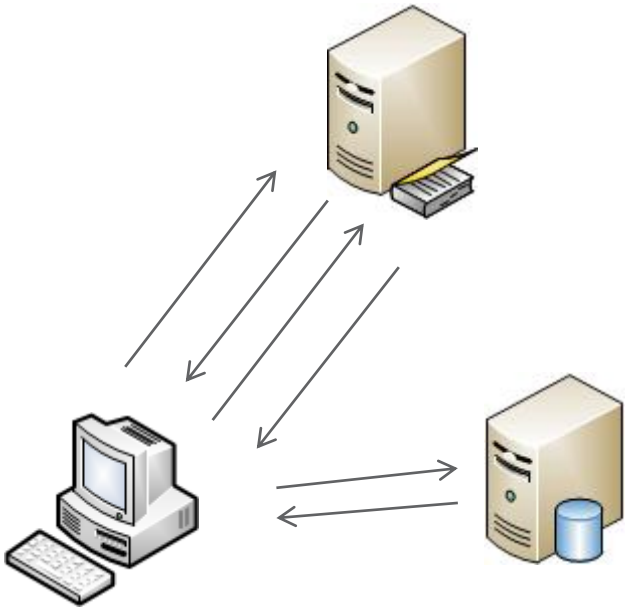
- Integrierte Systemkonten
- Virtuelle Konten
- Lokale Benutzerkonten
- Domänenbenutzerkonten
- Verwaltete Dienstkonten

Security– Arbeiten mit Dienstkonten

Verwaltete Dienstkonten

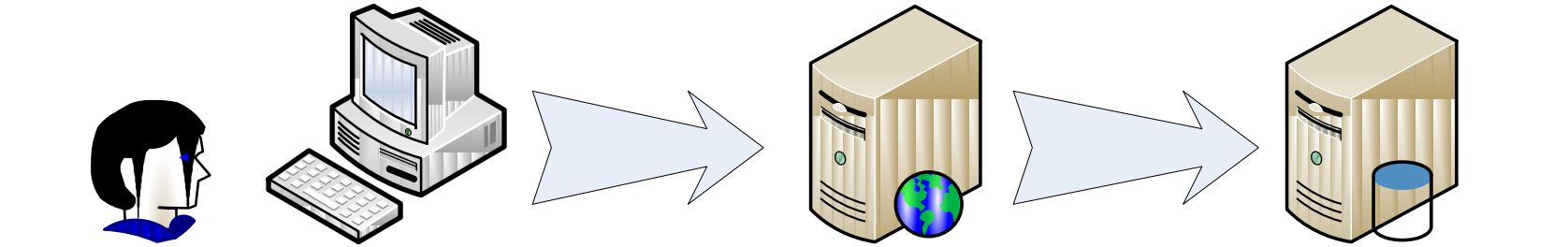
- MSA
  - Wird in der AD verwaltet
  - Kann den SPN setzen
  - Tauscht regelmäßig Kennwörter
  - Nicht für FCI geeignet
- gMSA (gruppenverwaltete Dienstkonten)
  - Wird offiziell noch nicht von SQL Server unterstützt

Security – Grundlagen Kerberos



1. Authentifizierung
2. Bestätigung /TGT + SessionKey
3. Anfrage ServiceTicket
4. Service Ticket plus ServiceSessionKey
5. Service Anfrage mit ST/SSK
6. Bestätigung des Servicezugriffs

Security – Erstellen einer KERBEROS Delegation



Security – Windows Groups Login

Neues ab SQL Server 2012

- Standard Schema für Windows Gruppen
  - es gilt die niedrigste ID
- Standardsprache auf Datenbankebene
  - nicht wirksam, wenn dem Login eine Standardsprache zugewiesen wurde

Security – ‚Best Practice' in Contained Databases

- Windowsbasierte User benutzen
  - Benutzer mit Passwörtern können kein Kerberos
- Alter any User vermeiden
- Zugriff nur auf die DB begrenzt
  - Identische User erstellen
  - Trustworthy Eigenschaft aktivieren
- Keine identischen ‚Benutzer mit Passwort' und ‚Anmeldenamen'
  - wenn vorhanden, dann an Instanz anmelden

Security – Anmeldeinformationen (Credentials)

Encryption Provider für Anmeldeinformationen

- speichert, verwaltet Verschlüsselungsschlüssel außerhalb des SQL Servers
- bietet Multi-Faktor Authentifizierung (1,2,3)
- Seperation-of-Duties
  - Securityverwaltung != Datenverwaltung
- Enterprise Feature
- Kann externe Schlüsselverwalter benutzen
  - SmartCard
  - USB Geräte
  - EKM Module

Verschlüsselung

Verschlüsselung

- Grundlagen / Begrifflichkeit
- Einsatzbereiche
- Verschlüsselungsstruktur
- Datenbankbenutzer mit Zertifikaten
- Asymmetrischer Schlüssel
- Asymmetrischer Schlüssel (Benutzer)
- Signierte Prozeduren
- TDS

Verschlüsselung - Begrifflichkeit

Symmetrische Schlüssel

- Ent- und Verschlüsseln mit dem selben Schlüssel

Asymmetrische Schlüssel

- Ent- und Verschlüsseln mit einem Schlüsselpaar
  - Privater Schlüssel
  - Öffentlicher Schlüssel

Hashalgorithmus

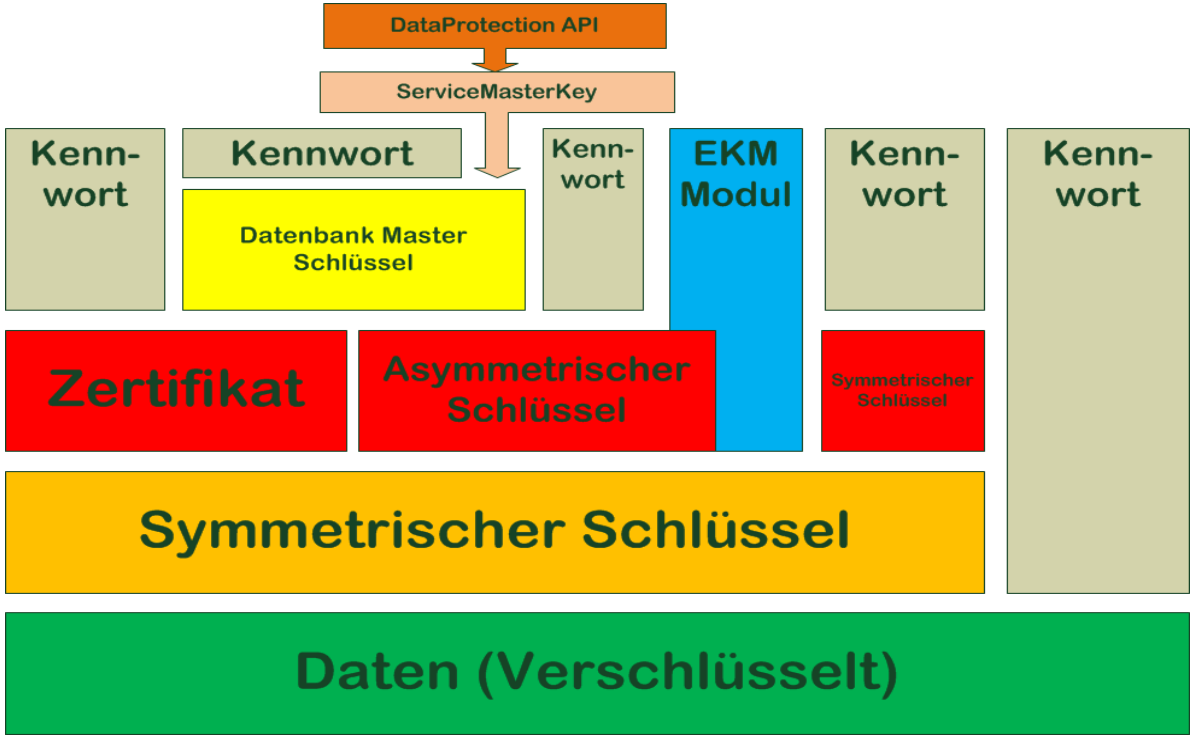
- Erzeugt eine Prüfsumme mit festgelegter Länge

Verschlüsselung - Eigenschaften

- Symmetrischer Schlüssel
  - Schnell
  - Sicher
  - Größenneutral
- Asymmetrischer Schlüssel
  - einfache Schlüsselübergabe
- Zertifikat
  - PKI bestätigter öffentlicher Schlüssel eines asymmetrischen Schlüsselpaares

PKI Vertauen kann ein Schwachpunkt sein!!

Verschlüsselung – Verschlüsselungsstruktur



Verschlüsselung – Datenbankbenutzer mit Zertifikaten

Voraussetzungen:

- Datenbank Master Key muss erstellt sein
- Zertifikat muss in zwei Dateien vorliegen
  - öffentlicher Schlüssel im CER/DER Format
  - privater Schlüssel im PVK Format
- Erstellen eines selbst-signierten Zertifikates

Tool zum Erstellen der Dateien:

- PVKConverter.EXE

Verschlüsselung – Asymmetrischer Schlüssel

Zweck asymmetrischer Schlüssel

- Schützt den symmetrischen Verschlüsselungsschlüssel
- Kann (eigenschränkt) Daten verschlüsseln
- Signiert Datenbankobjekte
- Können importiert werden

Aber:

- Können NICHT Verbindungen verschlüsseln
- Können nicht exportiert werden

Verschlüsselung –Asymmetrischer Schlüssel (Benutzer)

Benutzer auf Basis eines asymmetrischen Schlüssels

- Können sich nicht anmelden
- Können Berechtigungen erhalten
- Können Module signieren

Verschlüsselung – Signierte Prozeduren

Signierte Prozeduren

- Mehrmals signierfähig
- Ändern einer Prozedur löscht die Signierung

Kurzer Blick in die Zukunft

Kurzer Blick in die Zukunft

- Row Level Security
- Always Encrypted

SQL 2016 Angekündigte Features

Row Level Security

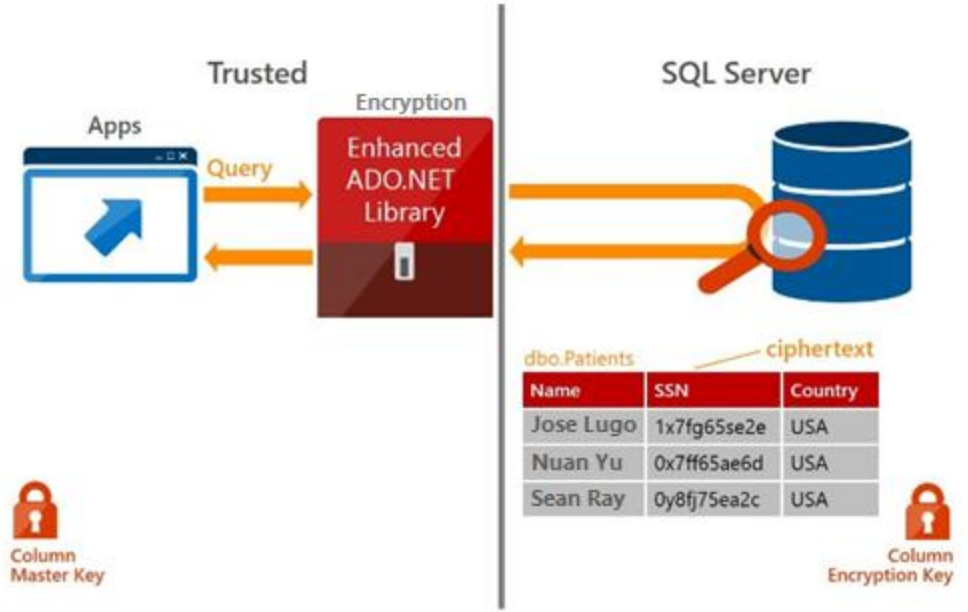
- gewährt Zugriff basierend auf
  - Gruppenmitgliedschaft
  - Ausführungskontext
- portiert Datensicherheit aus Applikationsebene auf Datenbankebene
- basiert auf ‚Sicherheitsrichtlinien' (Security Policy)
  - benötigt Inline-Tabellenwertfunktionen als Prädikat
  - Funktion muss mit Schemabindung erstellt werden
  - pro DML nur ein Prädikat

Kurzer Blick in die Zukunft

Always Encrypted

- Spaltenbasierte Verschlüsselung
- trennt Datenbesitz und Datenverwaltung
- transparent für die Applikation
- benötigt:
  - einen speziellen Treiber
  - Column Master Key
  - Column Encrytion Key

Kurzer Blick in die Zukunft



Maic Beher
Senior Consultant

maic.beher@trivadis.com

trivadis
makes IT easier.