SIS201
All You Need to Know About Security with SAP HANA

Andrea Kristen, Holger Mack / TIP In-Memory Platform
SAP TechEd 2012

SAP

Disclaimer

This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.

Agenda

SAP in-memory computing and SAP HANA

SAP HANA security

- Security approach
- Security architecture and functions
- Data center integration and compliance

Summary

Q&A

# SAP in-memory computing and SAP HANA

Breakthrough innovation with in-memory computing

In-memory computing is a technology that **analyzes massive quantities of data in local memory** so that the result of complex analysis and transactions is available at your fingertips – and business decisions can be executed without delay
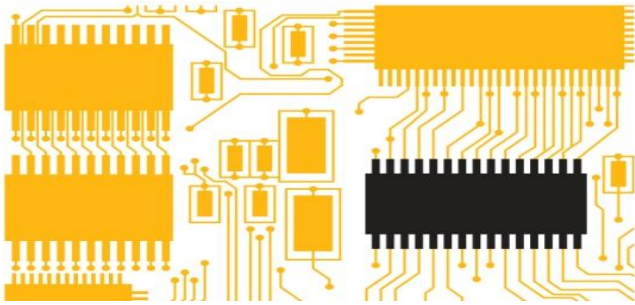
Breakthrough analytics

Deliver real-time insight and manage 'big data' with SAP HANA
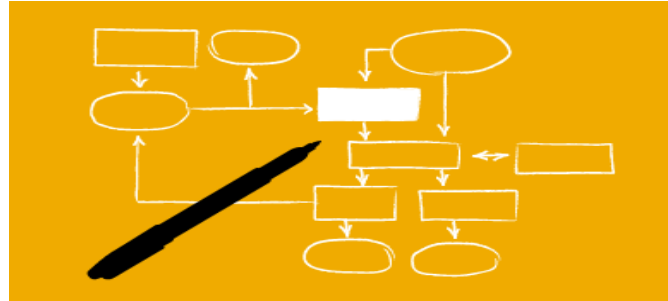
Amazing new applications

Drive rapid innovation and meet strategic challenges with a new wave of in-memory business applications
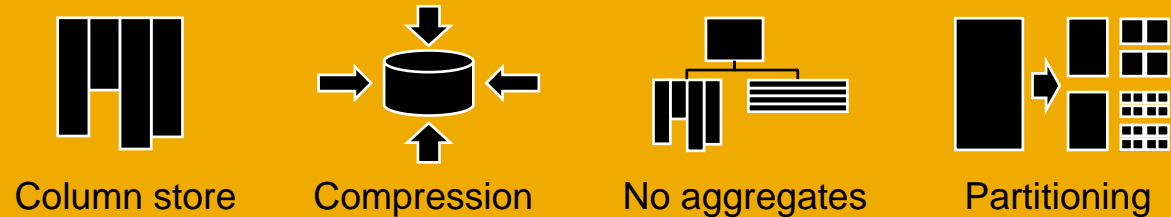
Dramatic simplification

Reduce complexity to lower cost and accelerate value delivery from IT

In-memory computing orchestrates technology innovations

Software and hardware innovations now make it possible to deliver on SAP's vision of a real-time enterprise with in-memory business applications
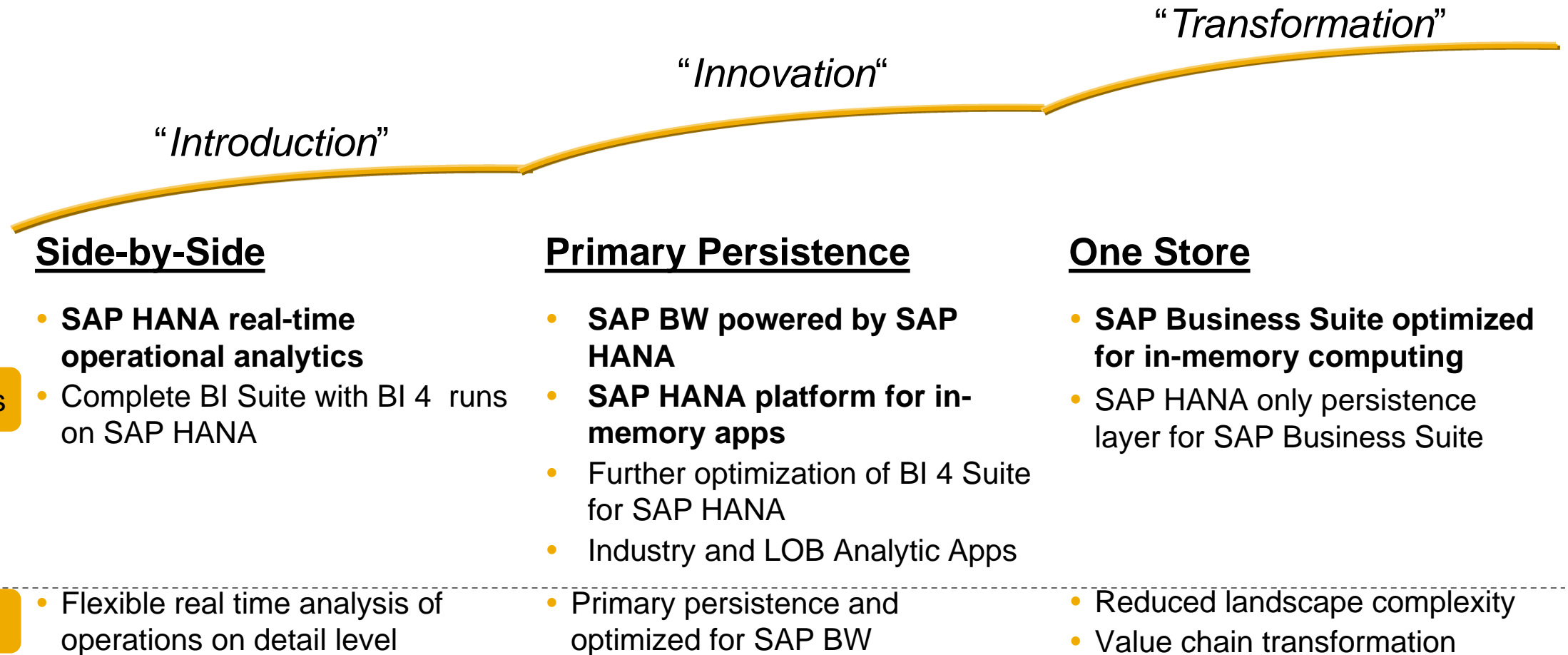
SAP software technology innovations

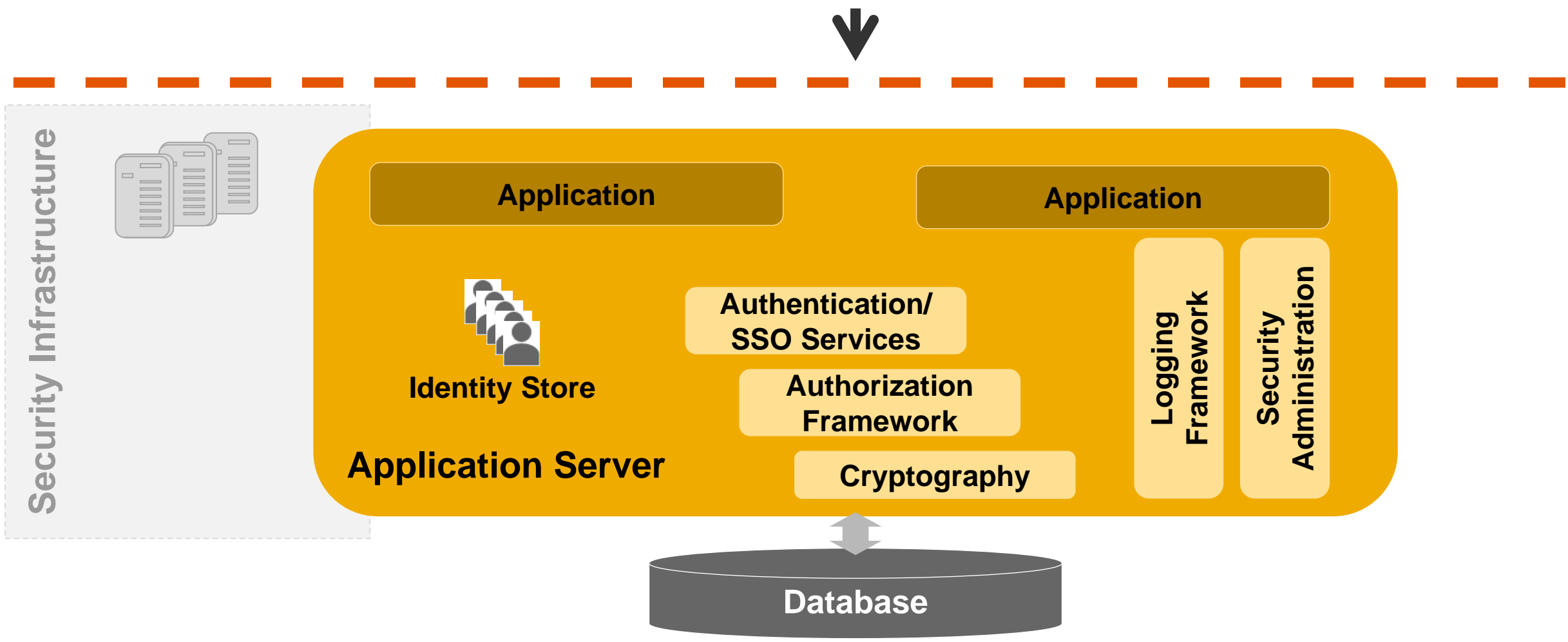| Column store | Compression | No aggregates | Partitioning |

Hardware innovations

| Memory | Multi core |

SAP in-memory strategy

"*Transformation*"

"*Innovation*"

"*Introduction*"

Side-by-Side

- **SAP HANA real-time operational analytics**
- Complete BI Suite with BI 4 runs on SAP HANA

Primary Persistence

- **SAP BW powered by SAP HANA**
- **SAP HANA platform for in-memory apps**
- Further optimization of BI 4 Suite for SAP HANA
- Industry and LOB Analytic Apps

One Store

- **SAP Business Suite optimized for in-memory computing**
- SAP HANA only persistence layer for SAP Business Suite

Capabilities

Benefits

- Flexible real time analysis of operations on detail level
- Primary persistence and optimized for SAP BW
- Reduced landscape complexity
- Value chain transformation

This is the current state of planning and may be changed by SAP at any time.

Traditional security architecture

Security Infrastructure
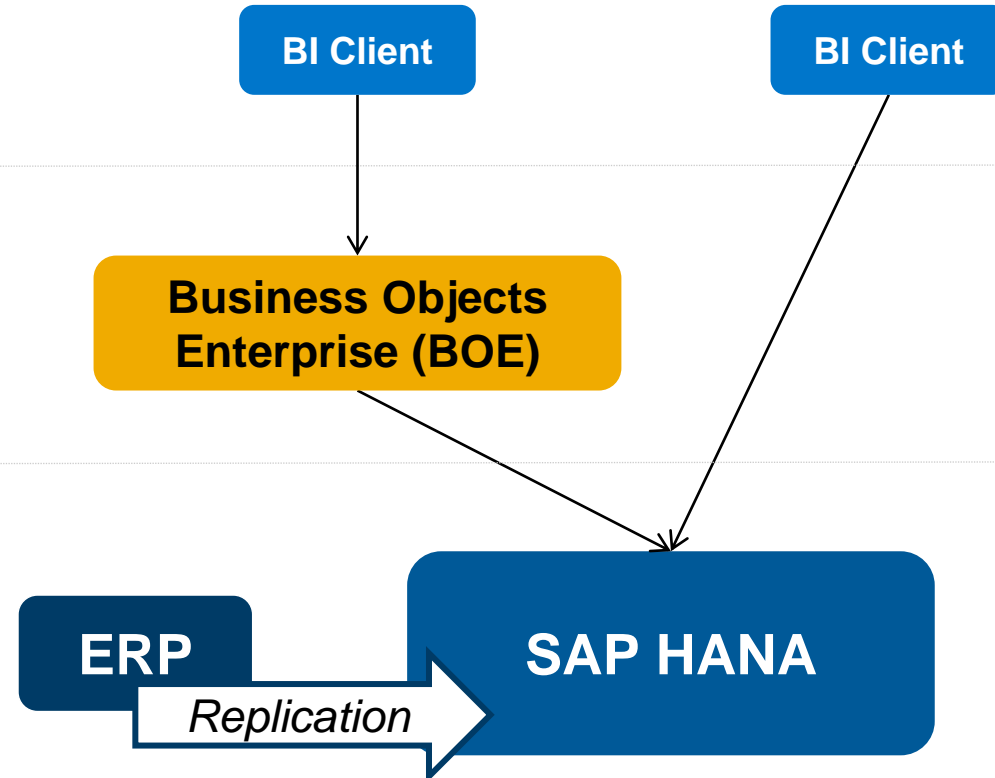
Application

Application

Identity Store

Authentication/ SSO Services

Authorization Framework

Cryptography

Logging Framework

Security Administration

Application Server

Database

SAP HANA scenarios

HANA as persistence "classical" architecture
e.g. BW on HANA

```
SAP GUI Client
      |
      v
Application Server
      |
      v
SAP HANA
```
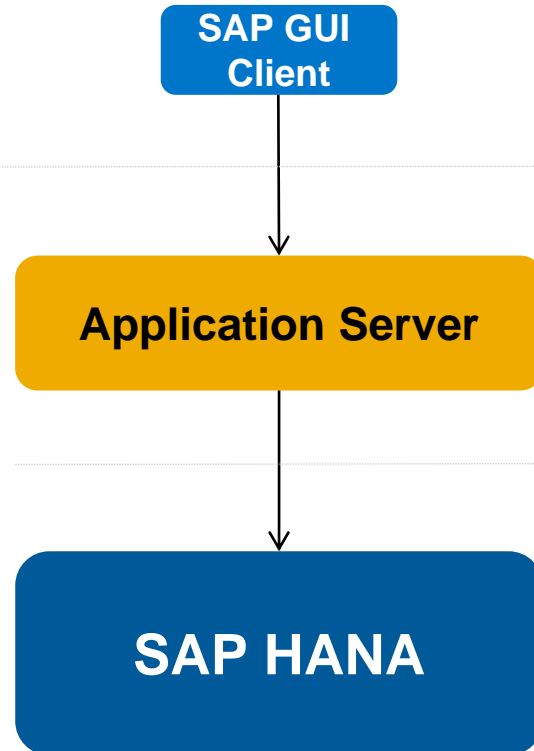
Data-mart scenarios analytics only
e.g. analytics on replicated data from ERP

```
BI Client          BI Client
   |                   \
   v                    \
Business Objects         \
Enterprise (BOE)          \
        \                  v
         \----------> SAP HANA
ERP --Replication--> SAP HANA
```

SAP HANA security

Security approach

SAP HANA – security approach
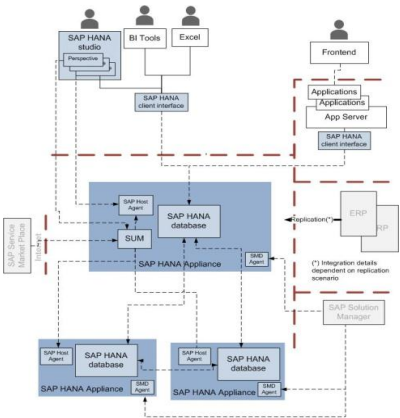
Secure SAP HANA Landscape

Secure Application Architecture

Secure In-Memory Computing

Secure In-Memory Architecture
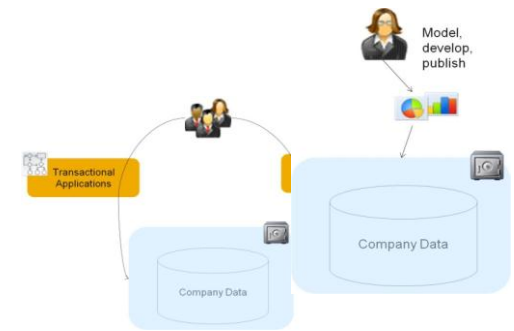
Secure Data Access and Management

SAP HANA security

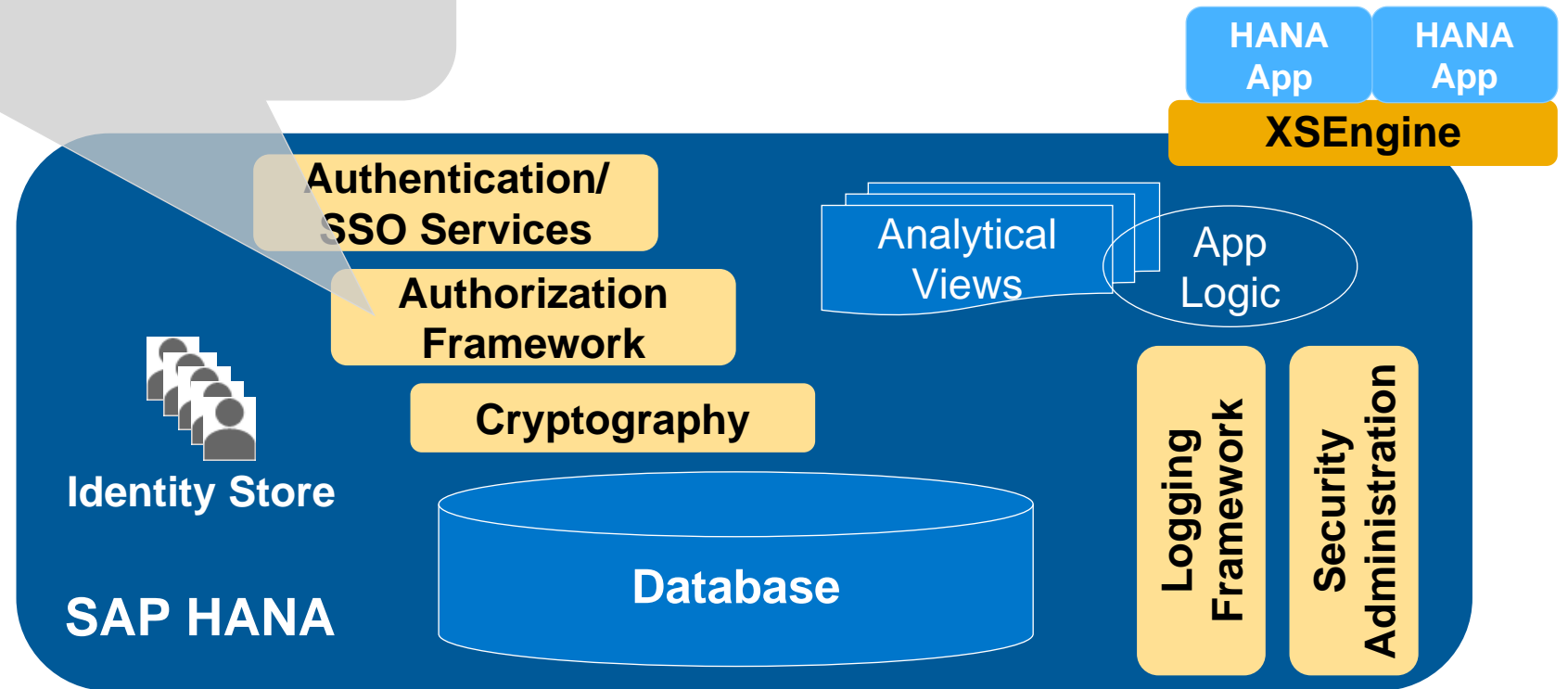Security architecture and functions

SAP HANA – security architecture
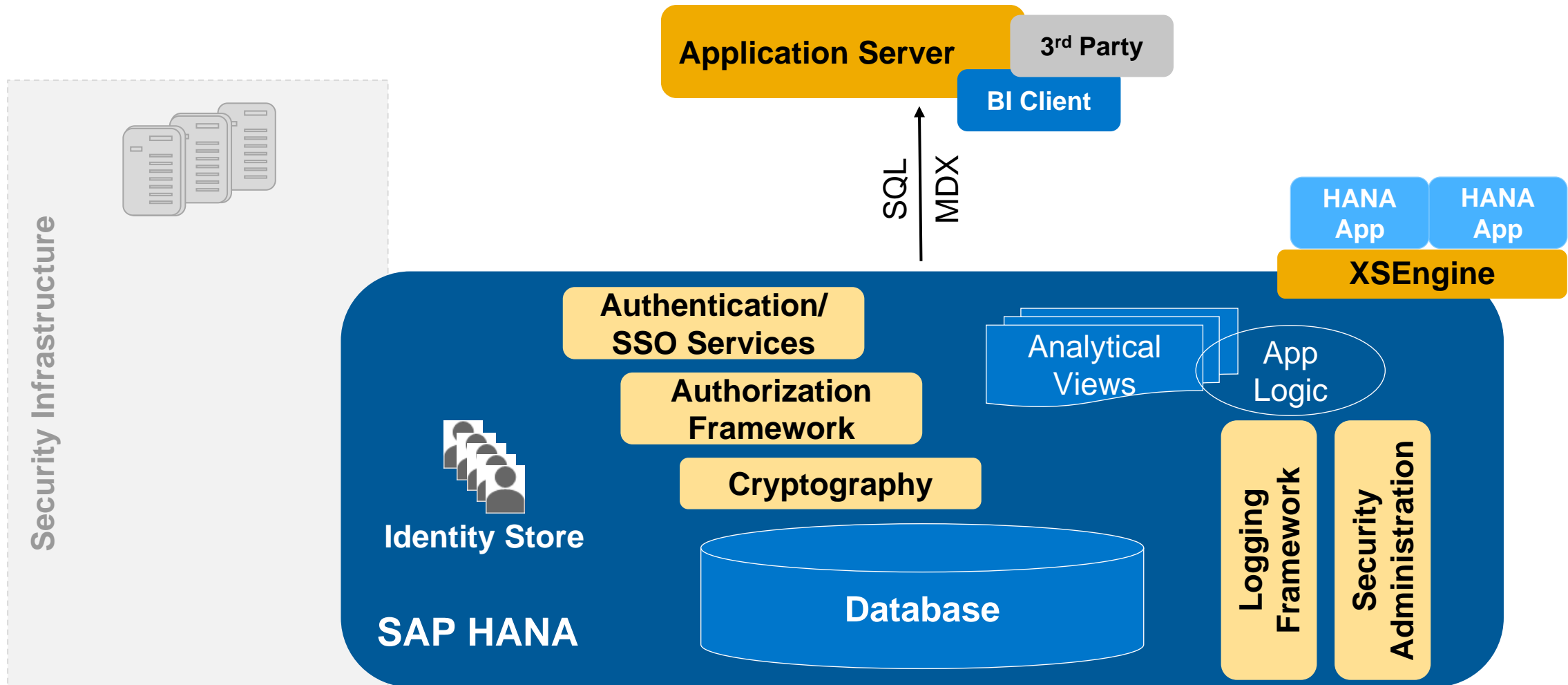
SAP HANA – authentication and single sign-on

- User name and password
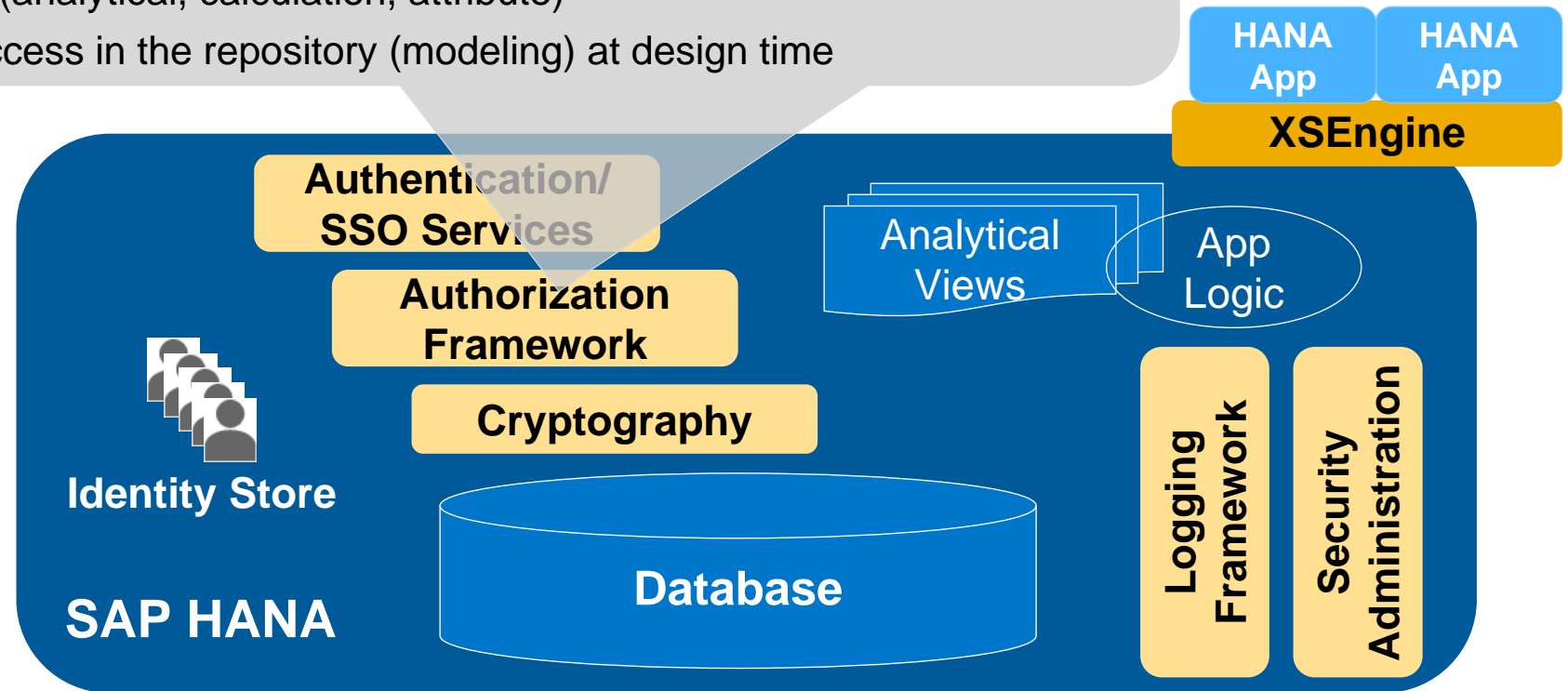 - Password policy
- Kerberos
  - Incl. delegation
- SAML
  - Bearer token

HANA App **HANA App**

XSEngine

Authentication/ SSO Services

Authorization Framework

Analytical Views

App Logic

Cryptography

Identity Store

Database

SAP HANA

Logging Framework

Security Administration
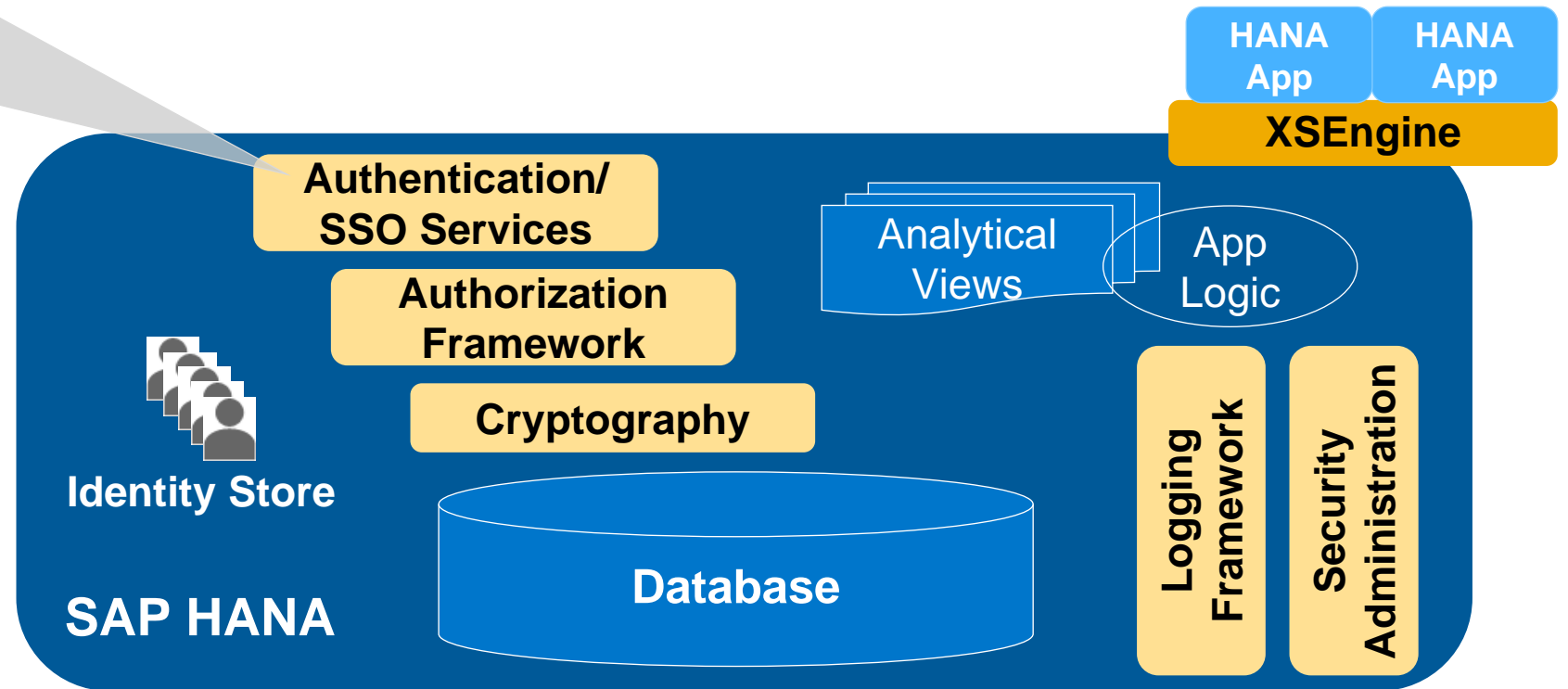
SAP HANA – user and role management

- Privileges control what users can do
- Privileges or roles can be assigned to users
- Roles are used to bundle and structure privileges
  - E.g. business roles (Modeler)
  - Role hierarchies

HANA App

HANA App

XSEngine

Authentication/ SSO Services

Authorization Framework

Analytical Views

App Logic

Cryptography

Identity Store

Database

Logging Framework

Security Administration

SAP HANA

SAP HANA – authorization framework

- System privileges: Authorize execution of administrative actions
- SQL privileges: Authorize access to data and operations on database objects
- Analytical privileges: Authorize read access on views at run-time; row-level access based on dimensions of the respective view (analytical, calculation, attribute)
- Repository privileges: Authorize access in the repository (modeling) at design time

HANA App **HANA App**

XSEngine

Authentication/ SSO Services

Analytical Views

App Logic

Authorization Framework

Cryptography

Identity Store

Database

Logging Framework

Security Administration

SAP HANA

SAP HANA – secure communication and encryption

- Communication encryption
  - SSL
- Encryption at rest
  - On the roadmap

HANA App **HANA App**

XSEngine

Authentication/ SSO Services

Authorization Framework

Analytical Views

App Logic

Cryptography

Identity Store

Database

SAP HANA

Logging Framework

Security Administration
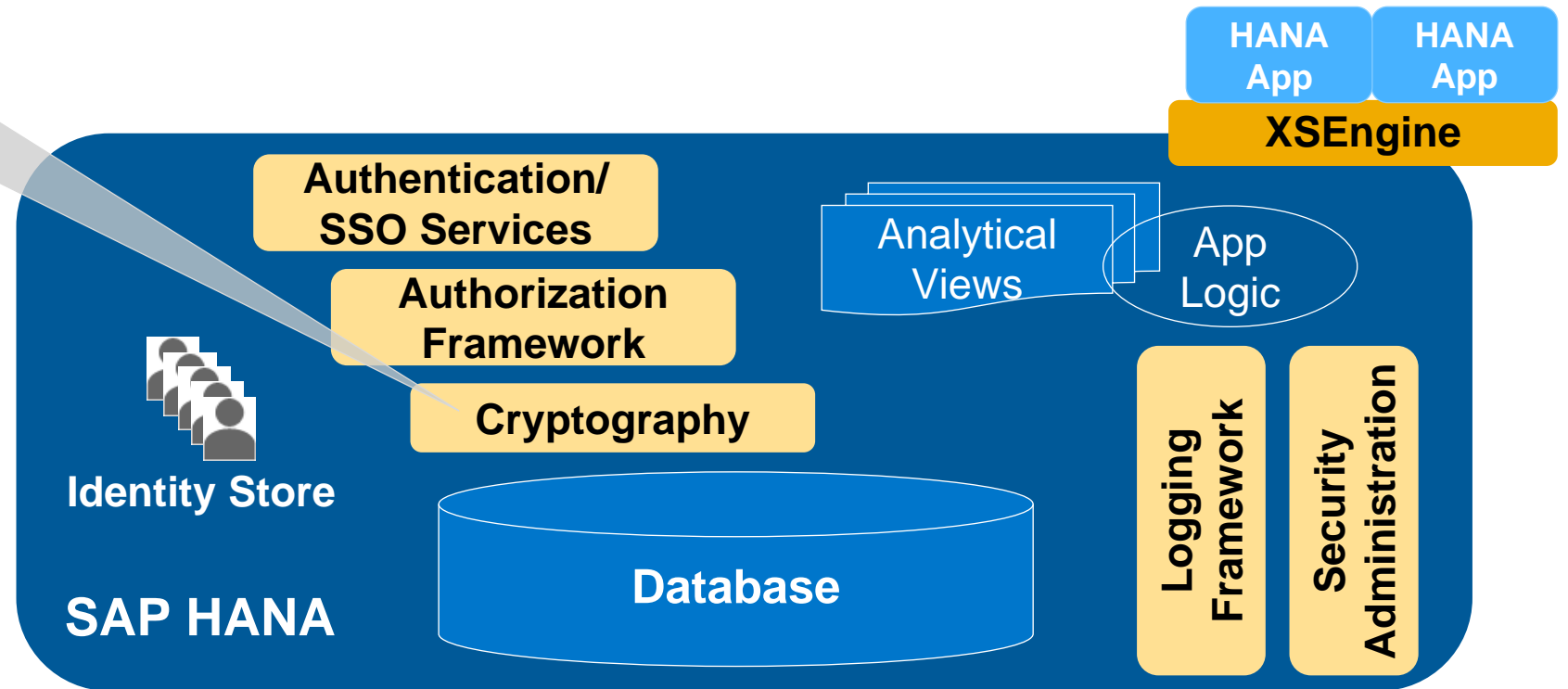
SAP HANA – audit logging (I)

- Logging of critical events for security and compliance
  - Users/roles
  - Authorization
  - Configuration
- Data access logging
  - On the roadmap

HANA App

HANA App

XSEngine

Authentication/ SSO Services

Authorization Framework

Analytical Views

App Logic

Cryptography

Identity Store

Database

SAP HANA

Logging Framework

Security Administration
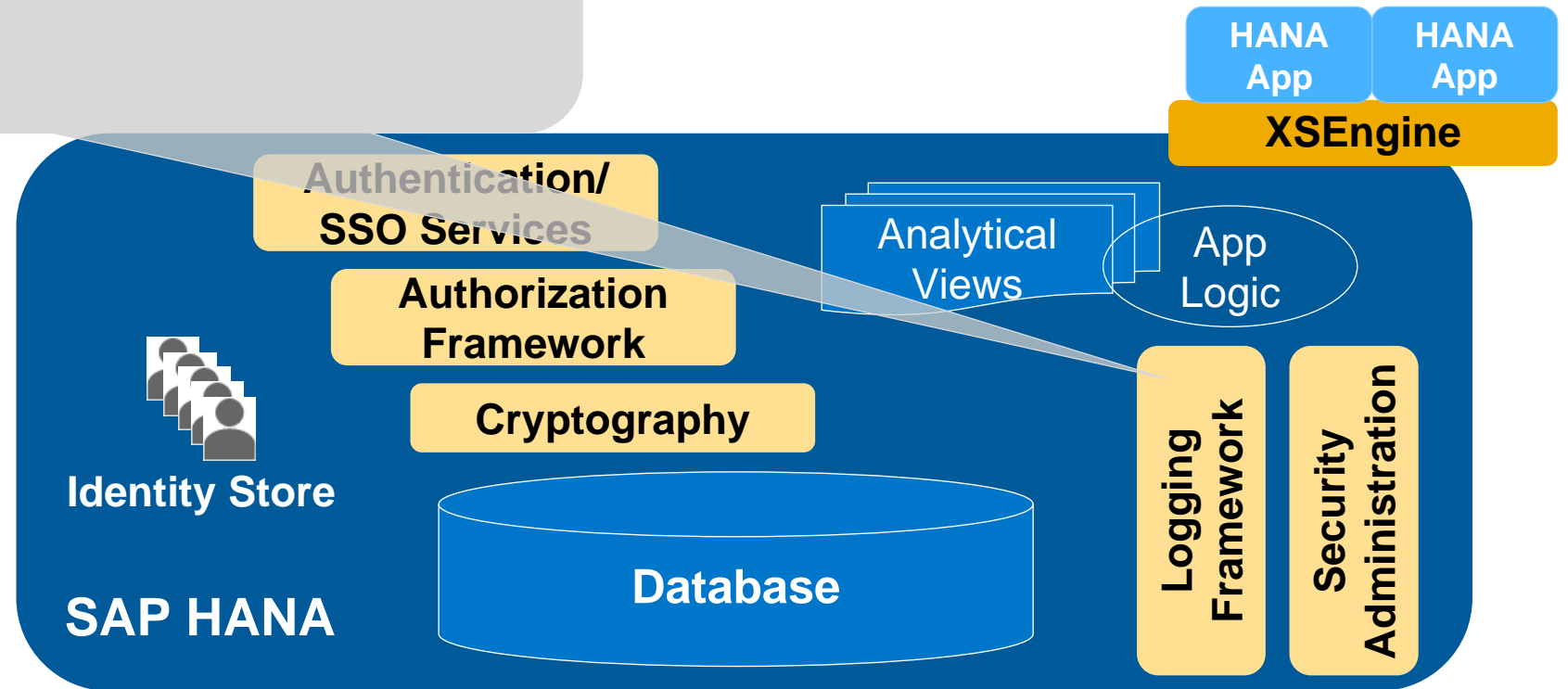
SAP HANA – audit logging (II)

Audit logging infrastructure
- Creates audit trails
  - Logging of successful and unsuccessful events
- Audit policies

Audit logging of critical events
- Create/drop user/role
- Create/drop analytic privilege
- Grant/revoke SQL/system/analytic privilege
- Grant/revoke role
- Enable/disable audit policy
- User connects to the database
- Configuration changes
- License key installation
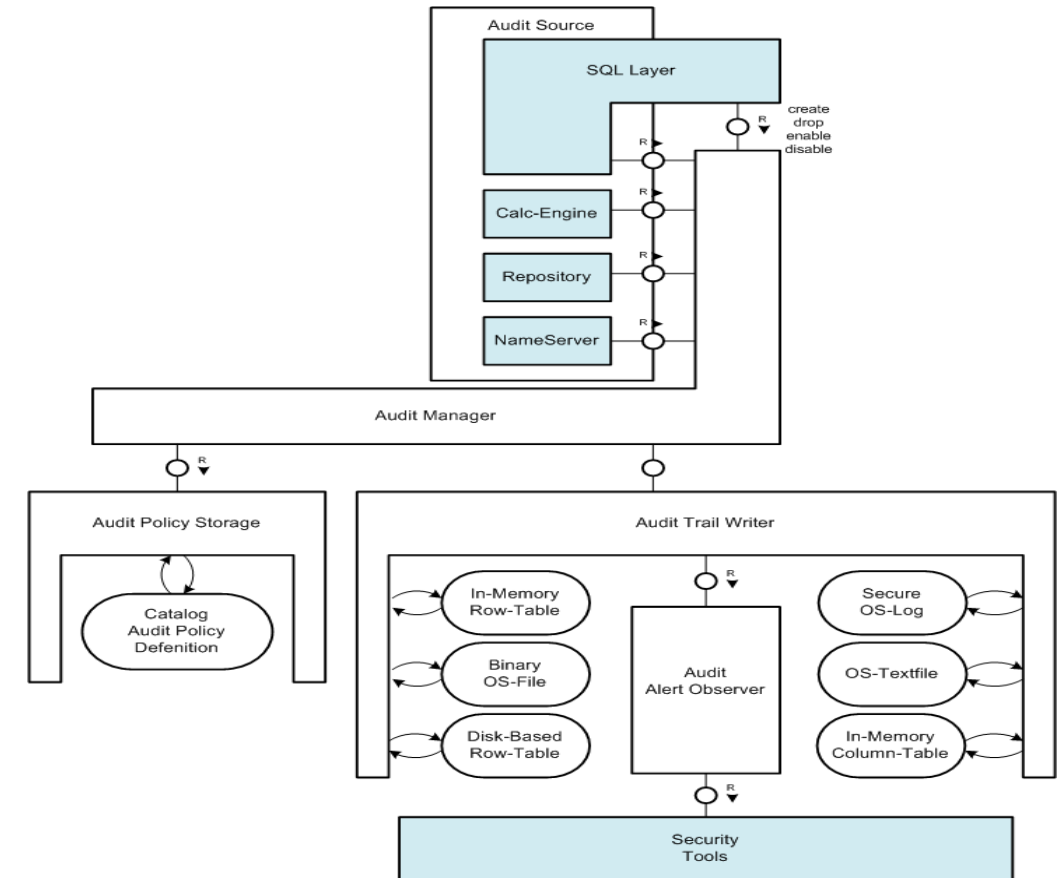
Audit logging infrastructure
(incl. examples of possible future extensions)

SAP HANA – security administration

- Security management and administration via SAP HANA Studio
  - Authentication policies
  - User/role management etc.
- SQL interface for user/role management

HANA App **HANA App**

XSEngine

Authentication/ SSO Services

Analytical Views

App Logic

Authorization Framework

Cryptography

Identity Store

Database

SAP HANA

Logging Framework

Security Administration
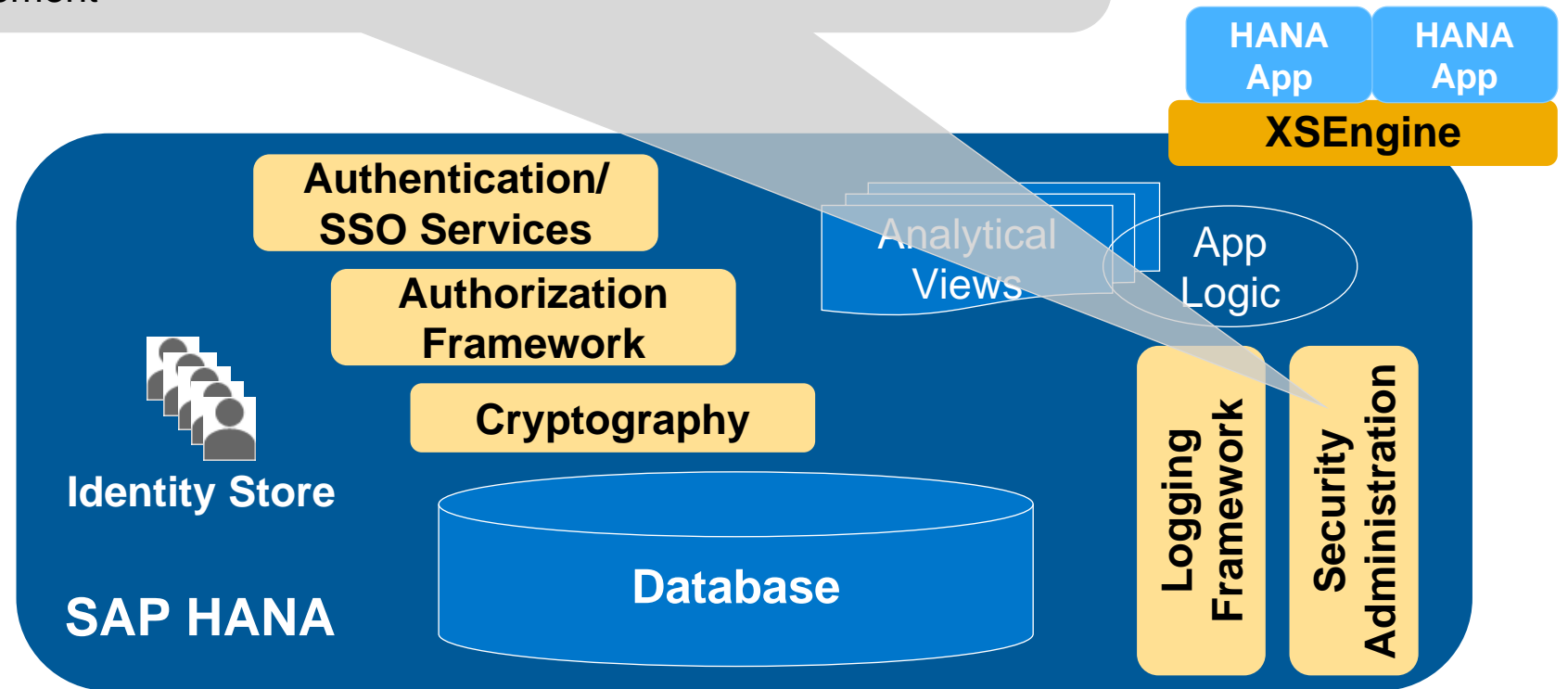
SAP HANA – application services (I)

Rationale:

Enable application development and deployment – minimize "layers"

- For applications with an http-based UI (browser, mobile apps)
- Applications run directly on SAP HANA, without an additional external application server => minimizes TCO
- Leverages the built-in strengths of the SAP HANA database for the best possible performance

HTML5 Browser

HTTP(s)

HANA App   HANA App

HANA XS
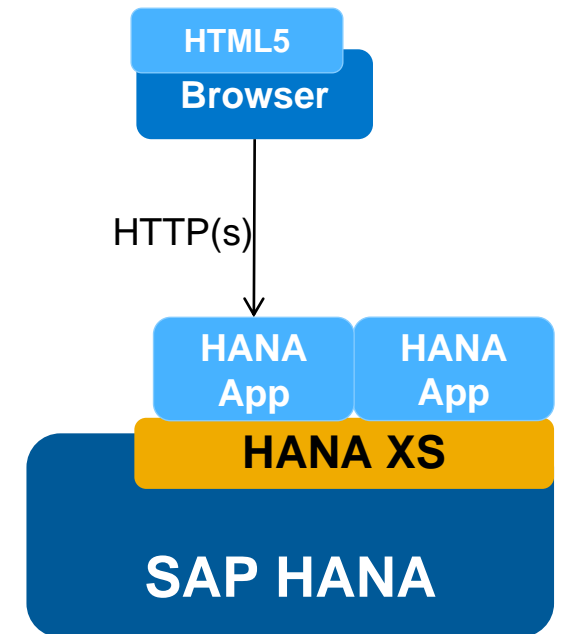
SAP HANA

SAP HANA – application services (II)

Application services security is based on the SAP HANA database security model

Authentication and single sign-on

- User name/password (HTTP Basic Authentication)
- SAML, SPNego (Kerberos) and SAP Logon Tickets on roadmap

User and role management

- Based on SAP HANA database user management

Authorization

- Based on SAP HANA database authorization system

Secure communication and encryption

- SSL support (server authentication)

SAP HANA security

Data center integration and compliance

SAP HANA – data center integration

- SAP HANA supports standard interfaces to enable integration with customer security network and datacenter infrastructures
- Secure set-up of SAP HANA appliance and network integration

Security Infrastructure

Single-Sign On Infrastructure

- Integration into standards-based SSO infrastructure, e.g. MS-ADS

Identity Management Infrastructure

Kerberos
SAML

Logging Infrastructure

SQL

syslog

SAP HANA

- Integration with existing provisioning solutions
  - Out-of-the-box connector for SAP NetWeaver IdM
  - SQL interface for integration with other IdM solutions

- Database audit trail written to standard syslog infrastructure

Summary

Summary

SAP HANA comes with security features that allow implementation of different security policies

SAP HANA is used in different scenarios

Security architecture of the scenario determines security approach

Q+A

Further Information

SAP Public Web

http://help.sap.com/hana_appliance -> Security Guide
http://experiencehana.com

Watch SAP TechEd Online

www.sapteched.com/online

Feedback

Please complete your session evaluation for SIS201.

Contact information:

Andrea Kristen (andrea.kristen@sap.com),
Holger Mack (holger.mack@sap.com)

Thanks for attending this SAP TechEd session.

© 2012 SAP AG. All rights reserved.