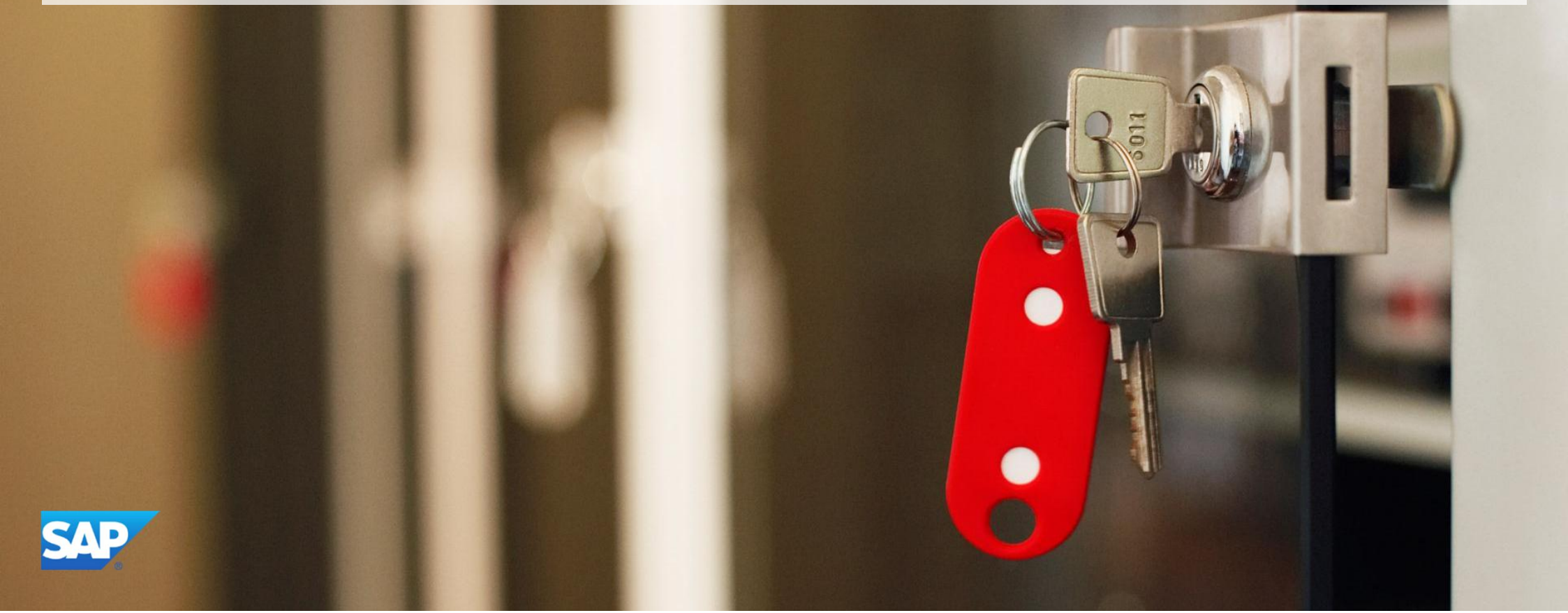
HANA Security

Christian Weide | GRC - Security
19. März 2014



Disclaimer

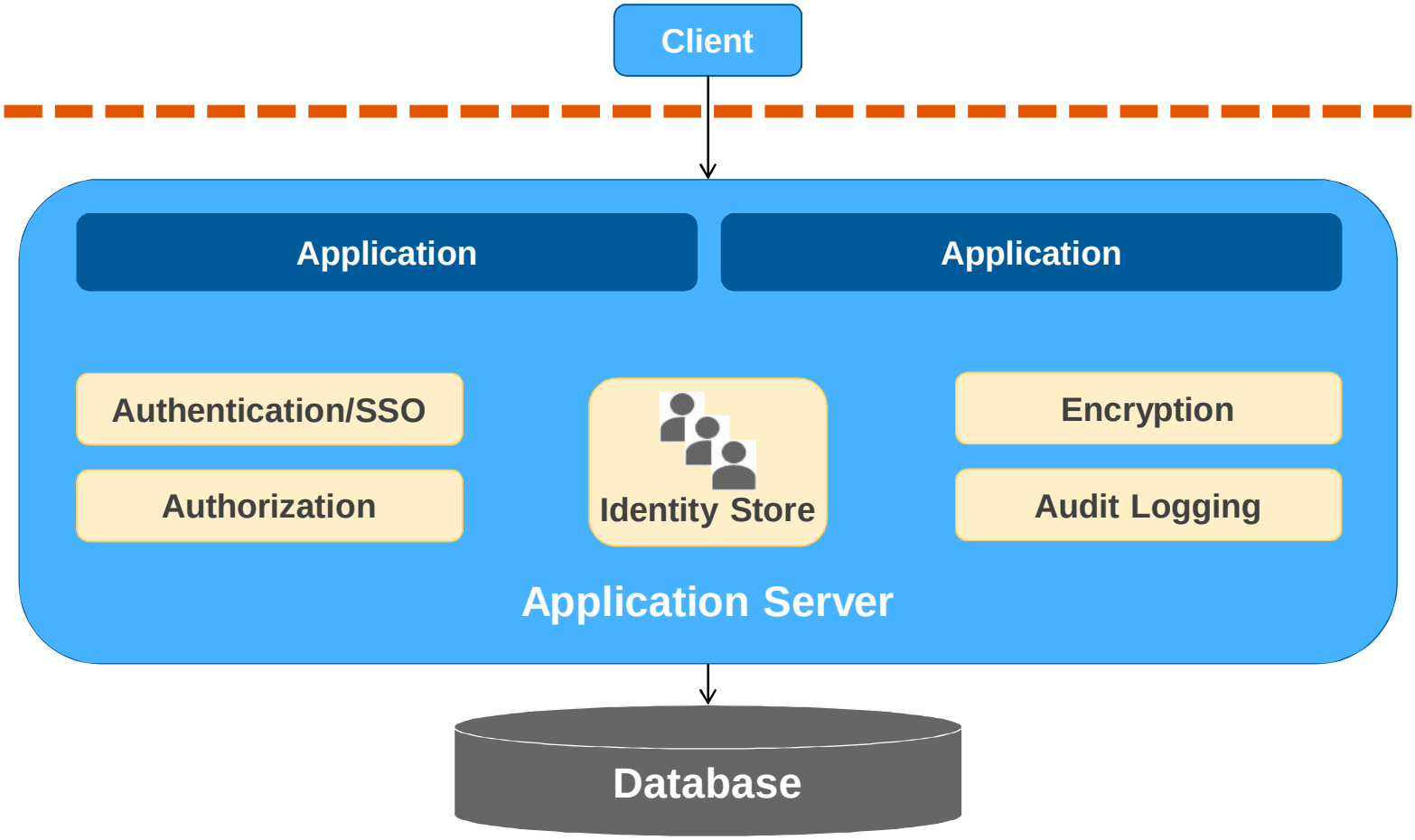
This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop 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.

1	2	3	4	5
SAP HANA scenarios and security functions	SAP HANA Authorization User Management	SAP HANA Authorization Roles Management	SAP IdM Connector GRC Access Management	Summary and Q+A

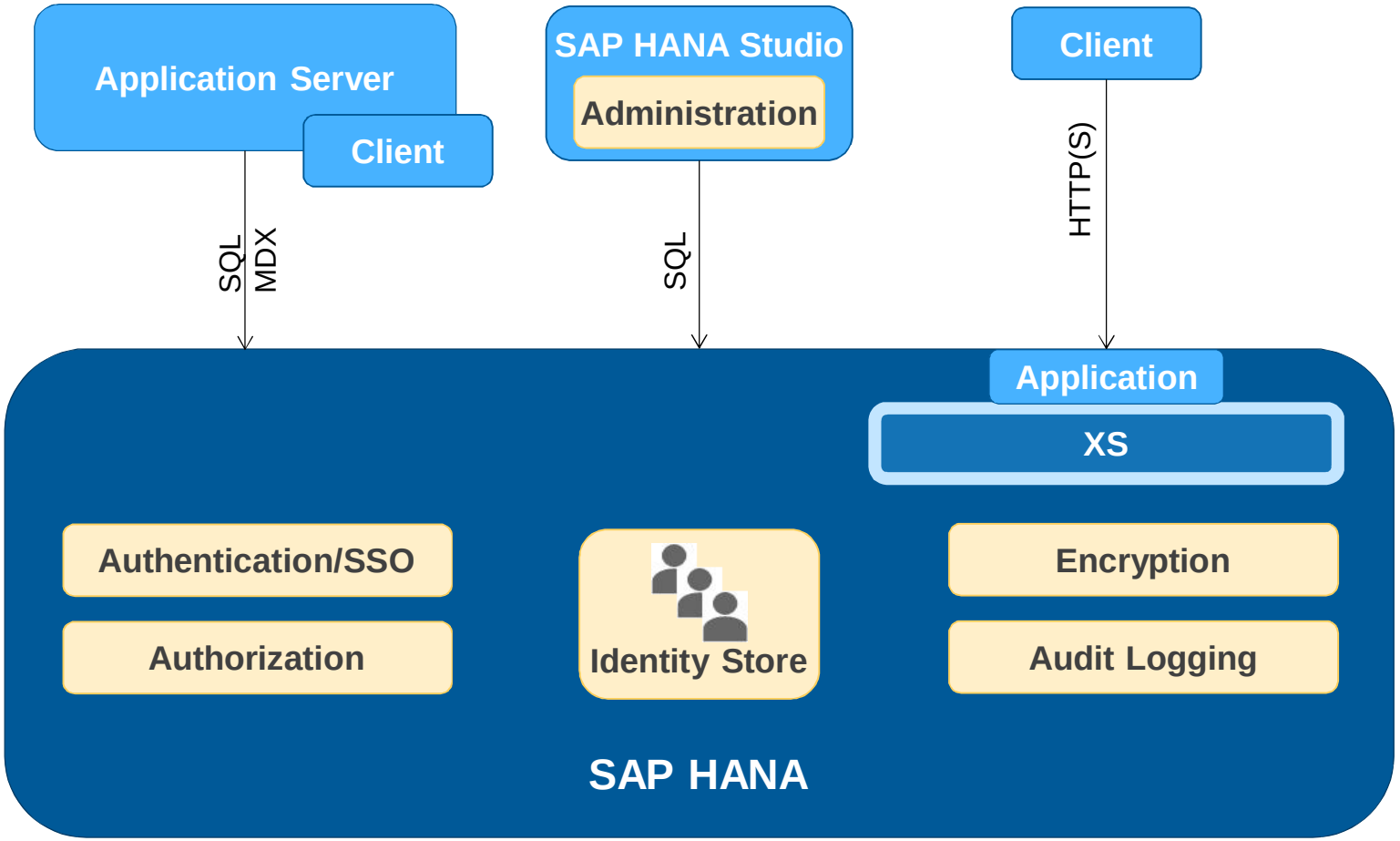
SAP HANA

Traditional Security Architecture

Traditional security architecture



SAP HANA – overview of security functions



SAP HANA – user and role management

- For logon, users must exist in the identity store of the SAP HANA database
- Roles (and privileges) can be assigned to users
- Roles are used to bundle and structure privileges
  - Create roles for specific groups of users, role hierarchies supported
- Role lifecycle: design time roles → export to production system → activate → runtime

SAP HANA – authorization

Privilege types

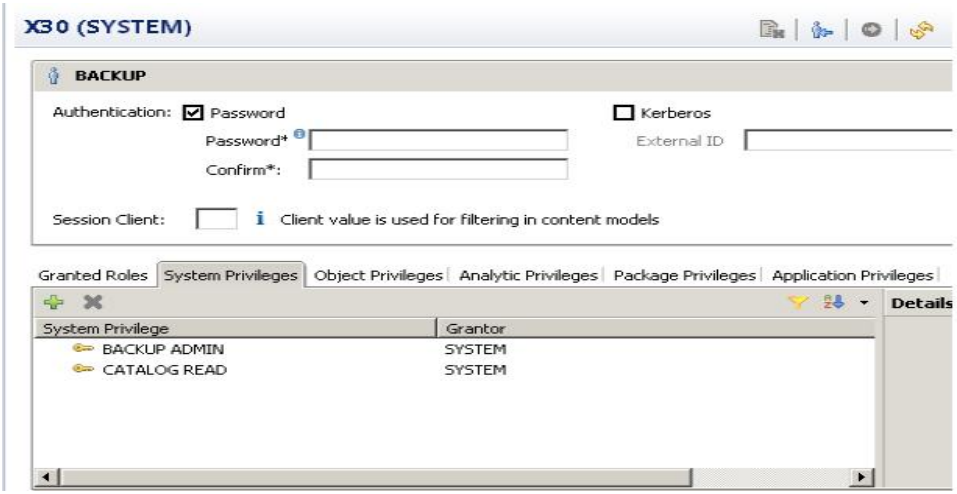
- **System** privileges: Authorize execution of administrative actions for the entire SAP HANA database
- **SQL** privileges: Authorize access to data and operations on database objects
- **Analytic** privileges: Authorize read access on analytic views at run-time, provide row-level access control based on dimensions of the respective view
- **Package** privileges: Authorize access in the repository (modeling environment) at design time
- **Application** privileges: Authorize access to SAP HANA XS application functions

HANA User Management

Via SAP HANA Studio / hdbsql

HANA User Management
via different Tools

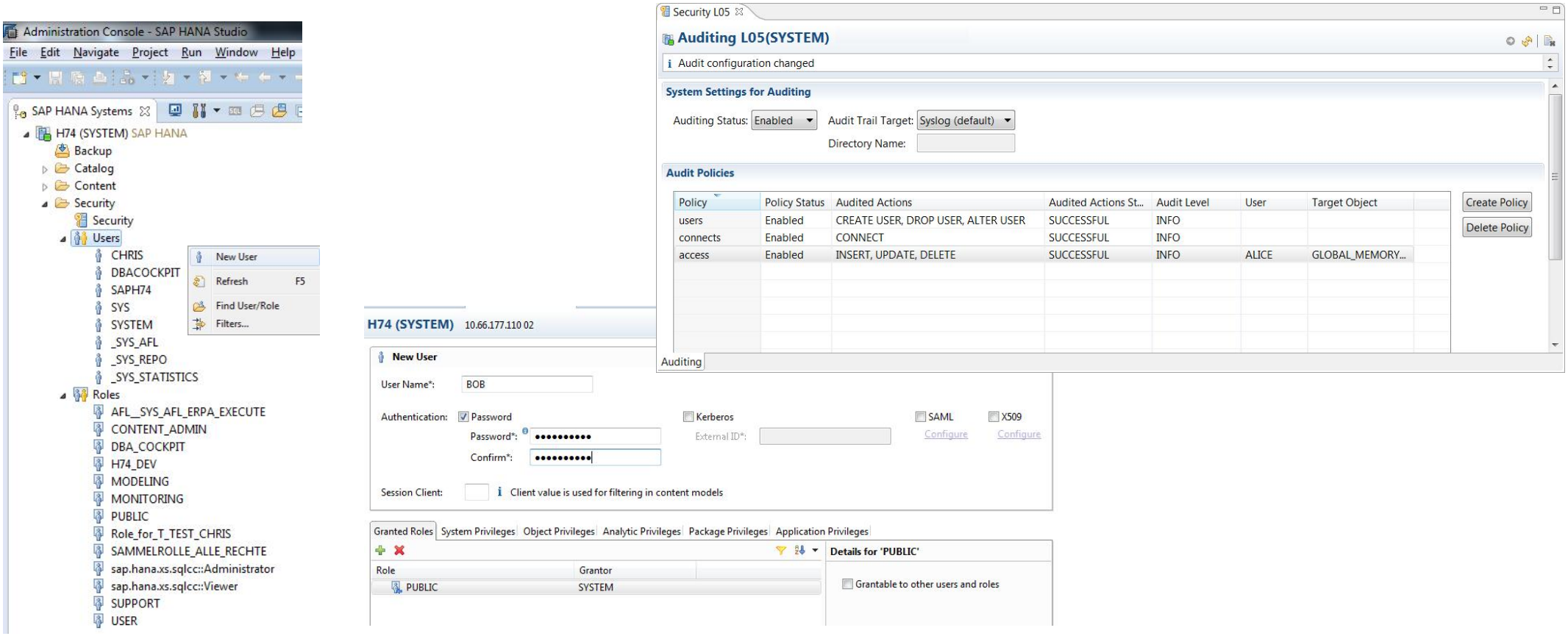
SAP HANA Studio



hdbsql

SAP HANA

Security administration with SAP HANA Studio



Demo

HANA Authorization Roles

Clarifying of terminology

HANA Authorization Roles
Current Situation

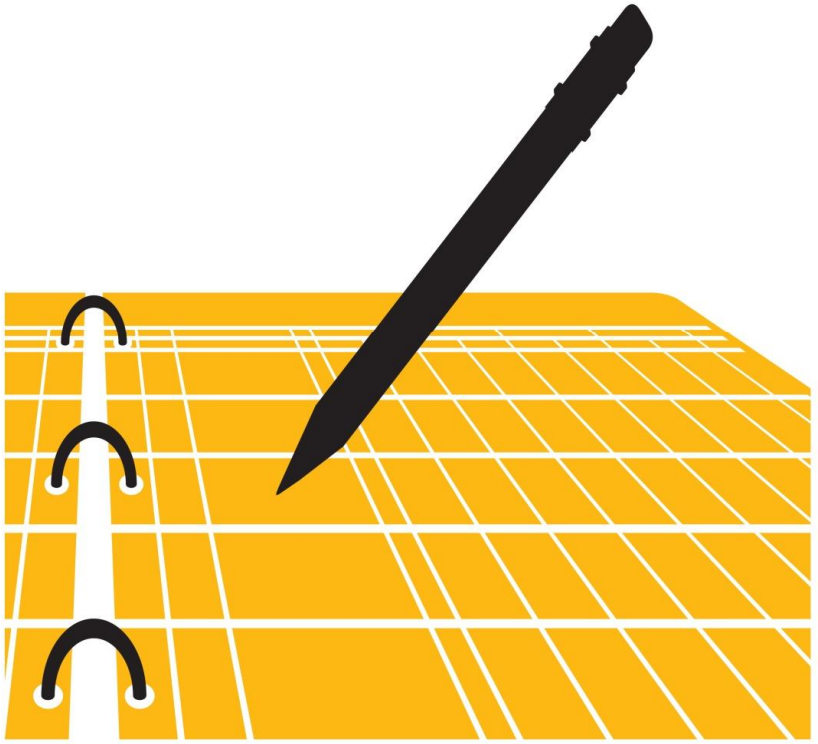
What is the current Landscape?

Which user management is implemented?

How many user will work with the SAP HANA?

Which goal will be achieved in the future?

What kind of roles are still in place?

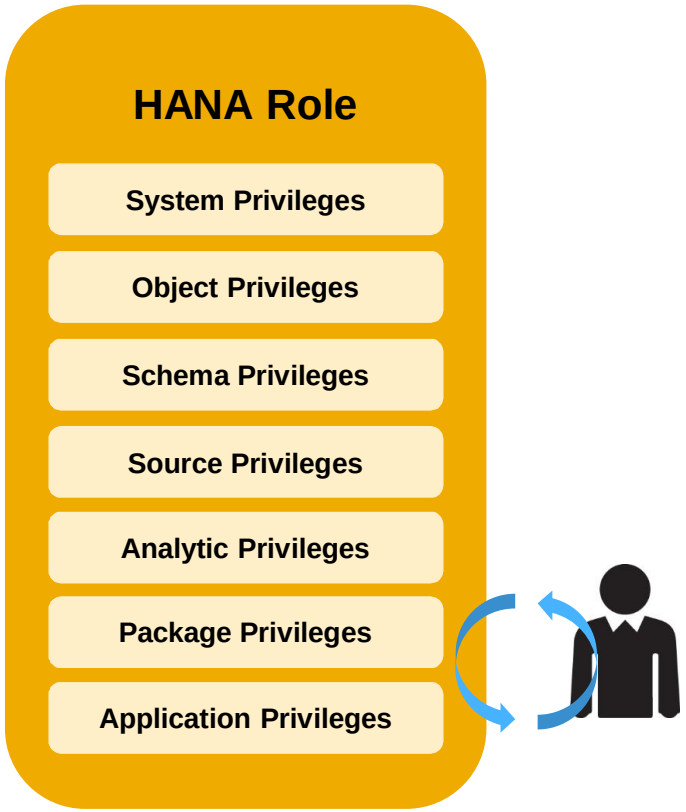


HANA Authorization Roles

What HANA Roles are

Roles:

- Are a collection of privileges
- Are the recommended practices for privilege management
- Can be granted to multiple users
- Can be used for complex role hierachies



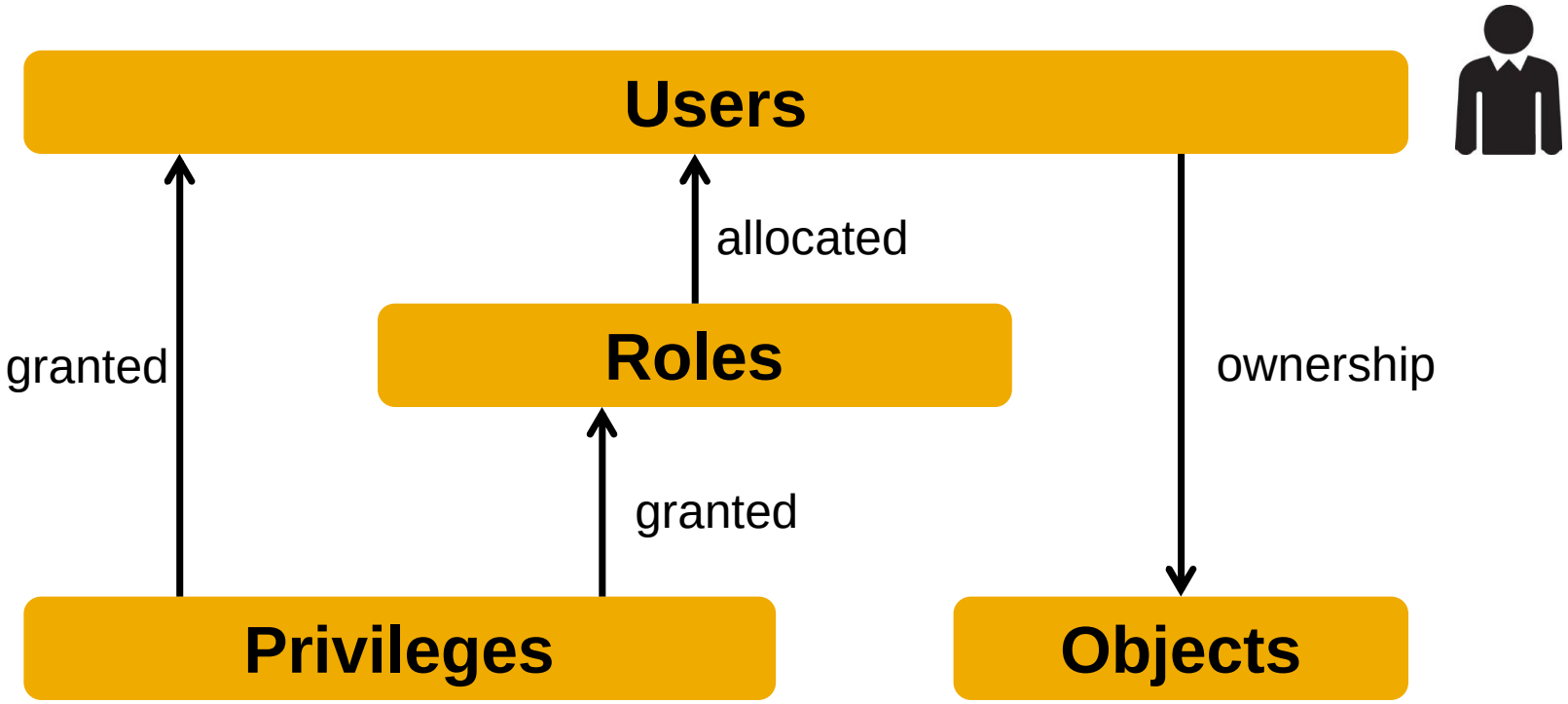
HANA Authorization

Privileges

Which Privilege…	Will be used for…
System Privilege	***Possible actions*** • *f.e..: Backup/Restore, User Administration, Instance start / stop*
Object Privilege / SQL	***Allows access to objects*** • *f.e.: SELECT, UPDATE, INSERT, DELETE of Tables, Views or Schemas* • *Objectowner can only grant access to others*
Analytical Privilege	***Allocation of row and column access*** • *f.e.: specific value ranges* • *Is required for moddeling*
Package Privilege	***Allows access to data models*** • *f.e.: Analytic or Calculation Views* • *Repository Objects*

HANA Privileges Management

Directly to Users or via Role



Demo

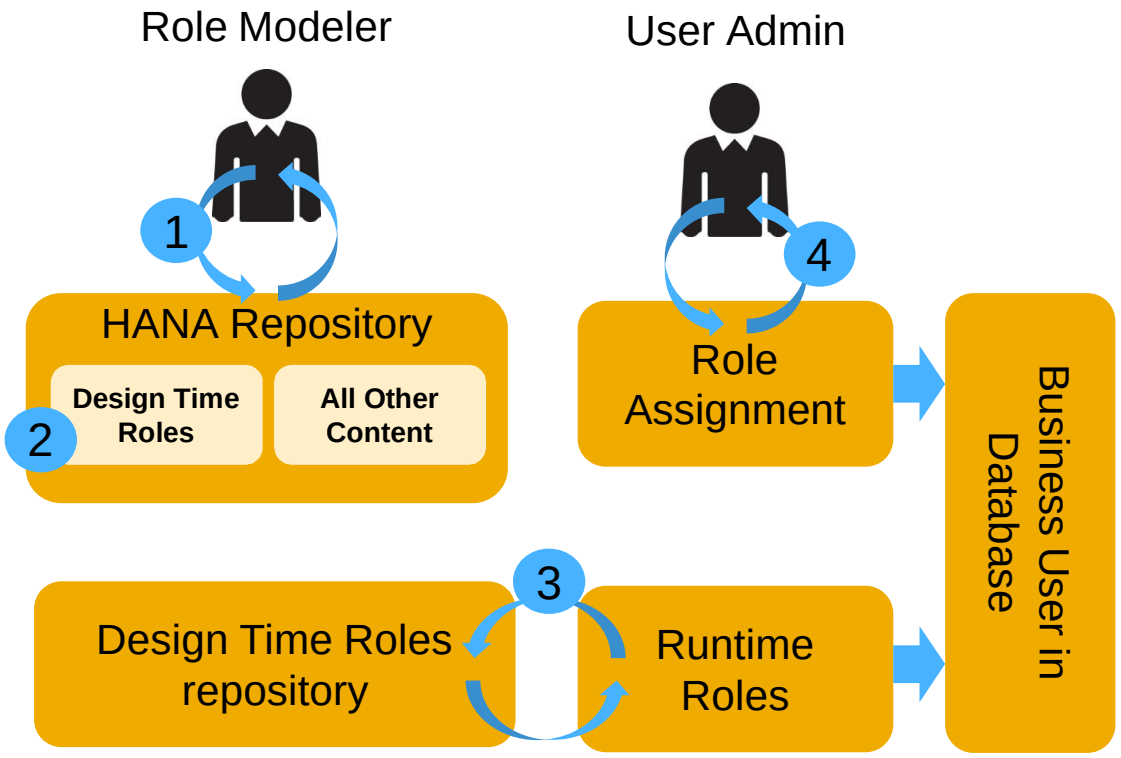
HANA Authorization Roles

Design-time roles

HANA Authorization Roles

Design-time Role

1. Design time role will be developed in the workbench of the development system
2. The role will be stored in the repository, and build in the DSL (text-based)
3. The design-time role can now be activated and become a runtime role
4. This runtime role can now be granted to an user by using the stored precudre for „GRANT_ACTIVATED_ROLE“



Demo

HANA User Management

SAP Netweaver Identity Management Connector

IdM Connector for SAP HANA
Functionality 1/2

Functions	SAP Standard HANA Konnektor	Consulting Service
Provisioning		
Create User with Password	Yes	
Password notification	No	Yes
Creating User with different authentication methods (KERBEROS, SAML,X509)	No (with next SP)	Yes
Creating User with Session Client	No	Yes
Provisioning of HANA Roles	Yes	
Provisioning of HANA Privileges	No (with next SP)	No
Deprovisioning		
Deleting Users	Yes	
Deprovisioning of HANA Roles	Yes	
Modify		
Changing of Authentication Method	No	Yes
Changing of parameters of the corresponding Authentication Method	No	Yes
Changing the Session Client	No	Yes
Lock and Unlock of Users	Yes	

IdM Connector for SAP HANA
Functionality 2/2

Functions	SAP Standard	Consulting Service
Synchronisation with HANA		
Loading of HANA Roles	Yes	
Loading of HANA Privileges	No (with next SP)	No
Loading of Users	Yes	
Mass Maintenances	No	Yes (On Basis of IdM RDS)
Reporting	No	Yes (On Basis of IdM RDS)
Managing of customer specific HANA Tables (f.e. ACL)	No	Yes (Requirements have to be clarified in the individual Project Scope)

HANA Access Management

SAP GRC Access Control

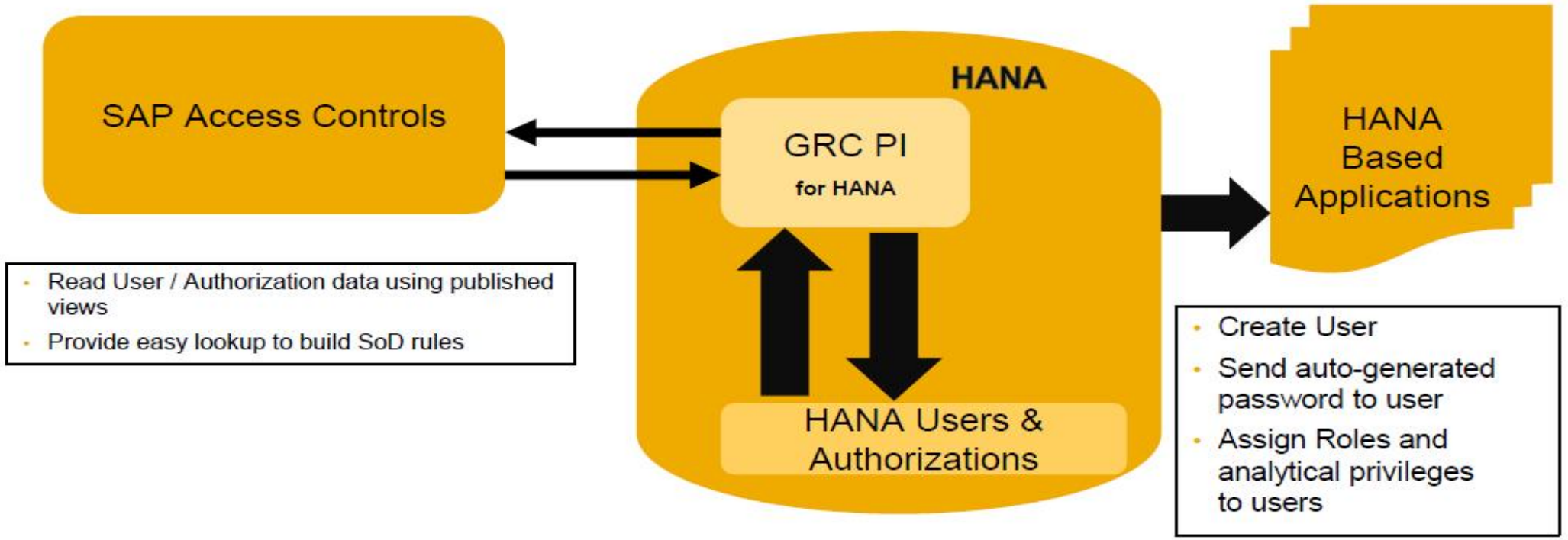
GRC for SAP HANA

What is different on pure HANA applications?

- **If you use Suite on HANA -> No change, as SU01 and PFCG care as before for non-DB related access and permissions**

- **If you use XSE-based applications like analytical applications there are 2 things no longer there:**

GRC for SAP HANA
High level Architecture



Examples for role provisioning and SOD analysis

Data Access (via Analytical Privileges)

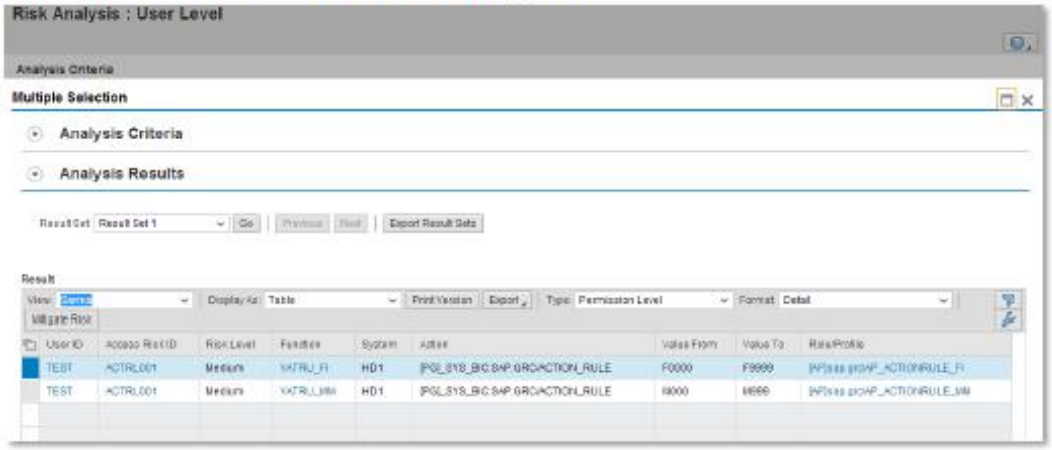
Rule

Permission Rules

Access Risk ID	Rule ID	Function ID	System	Resource	Resource Extn	Valid From	Value To	Search Type	Status
ACTRL001	0003	VATRU_FI	HD1	_SYS_BIC:sap.grc/ACTION_RULE	RISKID	F0000	F9999	AND	Active
		VATRU_MM	HD1	_SYS_BIC:sap.grc/ACTION_RULE	RISKID	M000	M999	AND	Active

Back

Access Risk from Analysis



Questions and answers

Questions

Dankeschön!

Kontaktinformation:

Christian Weide
Dipl.-Wirtsch.-Ing.
Technology Consultant | GRC / Security
SAP Deutschland AG & Co. KG | Albert-Einstein-Allee 3 |64625 Bensheim | Germany
M +49 151 446 14 261 | F +49 6227 78-47741 | E christian.weide@sap.com
www.sap.com

© 2014 SAP AG or an SAP affiliate company. All rights reserved.