

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

SAP HANA
scenarios and
security functions

2

SAP HANA
Authorization
User Management

3

SAP HANA
Authorization
Roles
Management

4

SAP IdM
Connector

GRC Access
Management

5

Summary and
Q+A

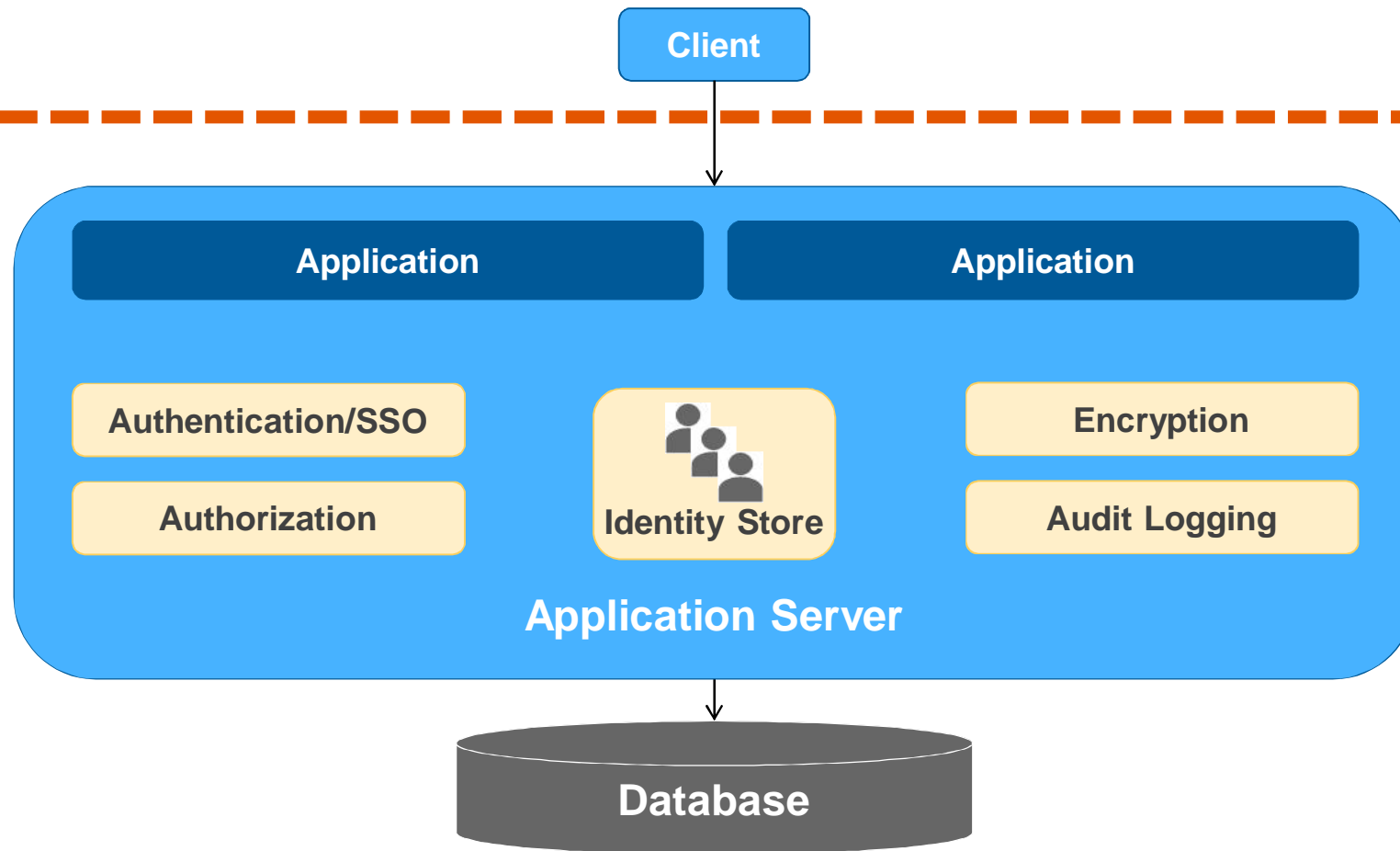


SAP HANA

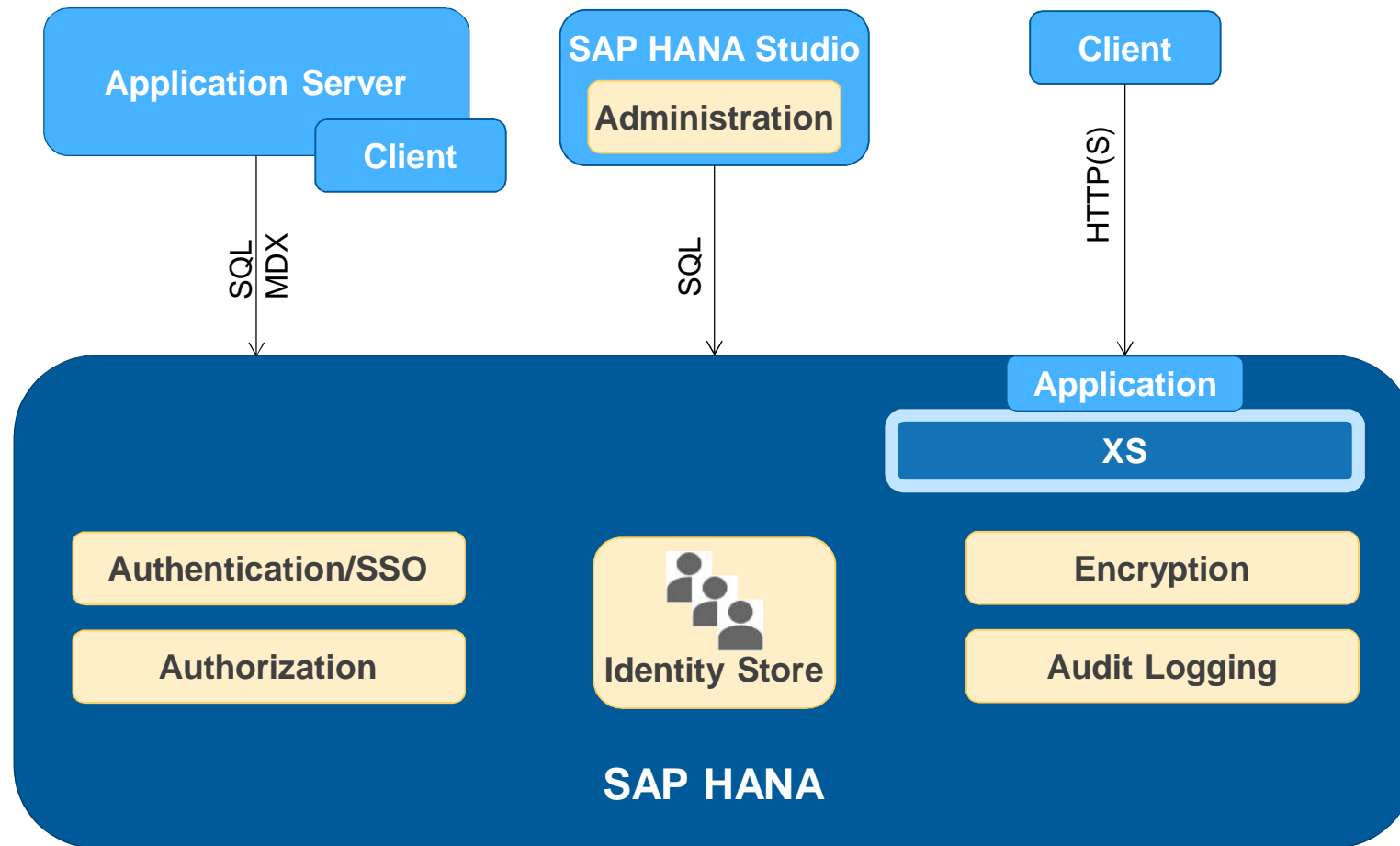
Traditional Security Architecture



Traditional security architecture



SAP HANA – overview of security functions



SAP HANA – user and role management

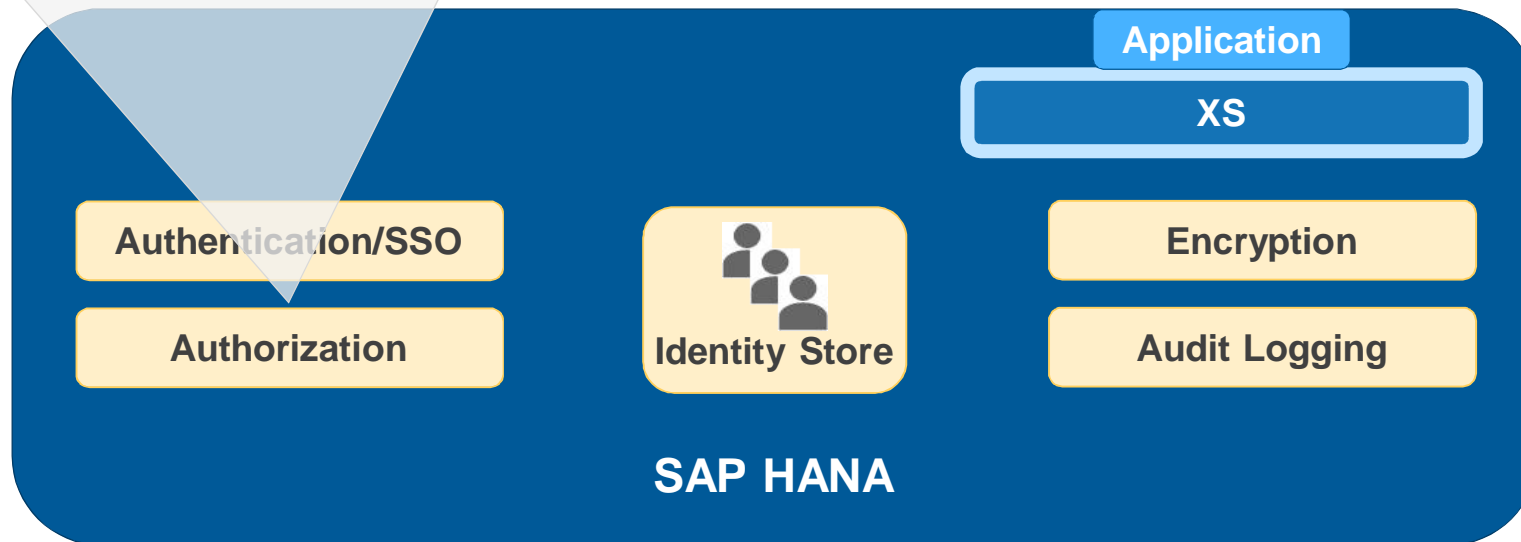
- For logon, users must exist in the identity store of the SAP HANA database
- Roles (and privileges) can be assigned to users
- Roles are used to bundle and structure privileges
 - Create roles for specific groups of users, role hierarchies supported
- Role lifecycle: design time roles → export to production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

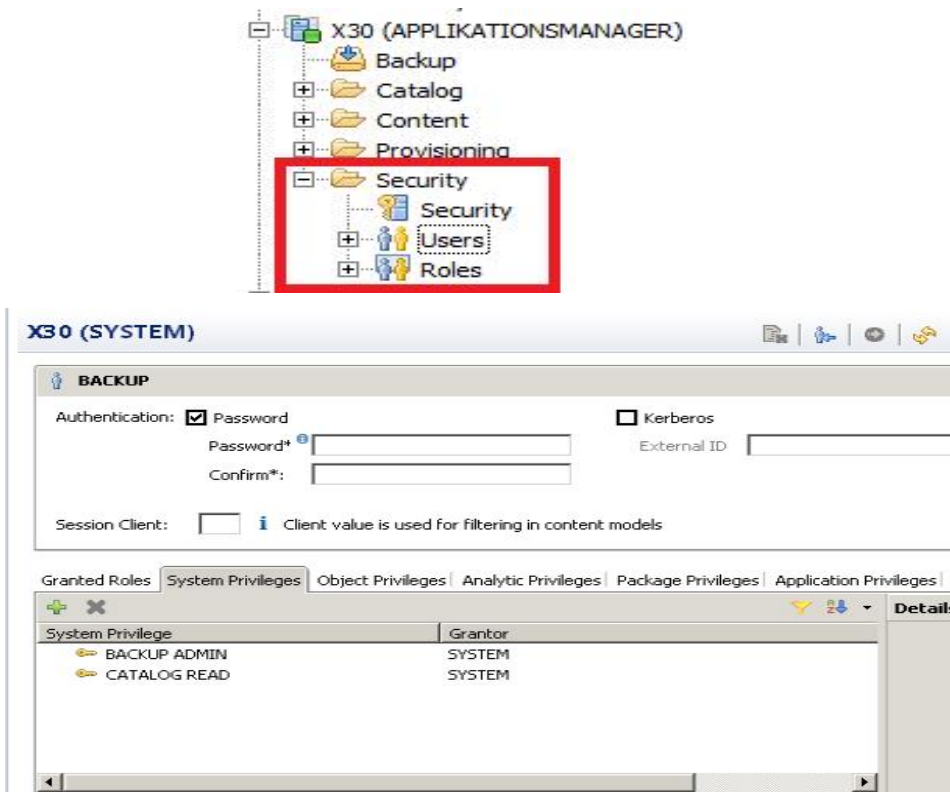
Via SAP HANA Studio / hdbsql



HANA User Management

via different Tools

SAP HANA Studio



hdbsql

```
ma-crmhana02:~ # su - x30adm
ma-crmhana02:/usr/sap/X30/HDB20> hdbsql -i 20 -u SYSTEM -p XXXXXXXXXX

Welcome to the SAP HANA Database interactive terminal.

Type: \h for help with commands
      \q to quit

hdbsql=> ALTER USER BACKUP PASSWORD TEST123
* 412: invalid password layout: minimal password length is [8] SQLSTATE: HY000
hdbsql X30=> ALTER USER BACKUP PASSWORD TEST1234
* 412: invalid password layout: password has to meet the rule ['A1a'] SQLSTATE:
HY000
hdbsql X30=> ALTER USER BACKUP PASSWORD Test1234
0 rows affected (overall time 23.694 msec; server time 20.739 msec)
hdbsql X30=>
```

SAP HANA

Security administration with SAP HANA Studio

The screenshot displays the SAP HANA Studio Security Administration Console. On the left, the 'SAP HANA Systems' tree shows the 'H74 (SYSTEM)' selected. The 'Security' folder is expanded, showing 'Users' and 'Roles'. The 'New User' dialog is open, showing the 'User Name' field with 'BOB' and the 'Authentication' section with 'Password' selected. The 'Auditing L05(SYSTEM)' configuration window is also open, showing the 'System Settings for Auditing' and a table of 'Audit Policies'.

System Settings for Auditing

Auditing Status: Audit Trail Target: Directory Name:

Audit Policies

Policy	Policy Status	Audited Actions	Audited Actions St...	Audit Level	User	Target Object	
users	Enabled	CREATE USER, DROP USER, ALTER USER	SUCCESSFUL	INFO			<input type="button" value="Create Policy"/>
connects	Enabled	CONNECT	SUCCESSFUL	INFO			<input type="button" value="Delete Policy"/>
access	Enabled	INSERT, UPDATE, DELETE	SUCCESSFUL	INFO	ALICE	GLOBAL_MEMORY...	

New User

User Name*:

Authentication: ☒ Password ☐ Kerberos ☐ SAML ☐ X509

Password*: External ID*:

Confirm*: [Configure](#) [Configure](#)

Session Client: ☐ [Client value is used for filtering in content models](#)

Granted Roles | System Privileges | Object Privileges | Analytic Privileges | Package Privileges | Application Privileges

Details for 'PUBLIC'

☐ Grantable to other users and roles

Demo





HANA Authorization Roles

Clarifying of terminology

HANA Authorization Roles

Current Situation

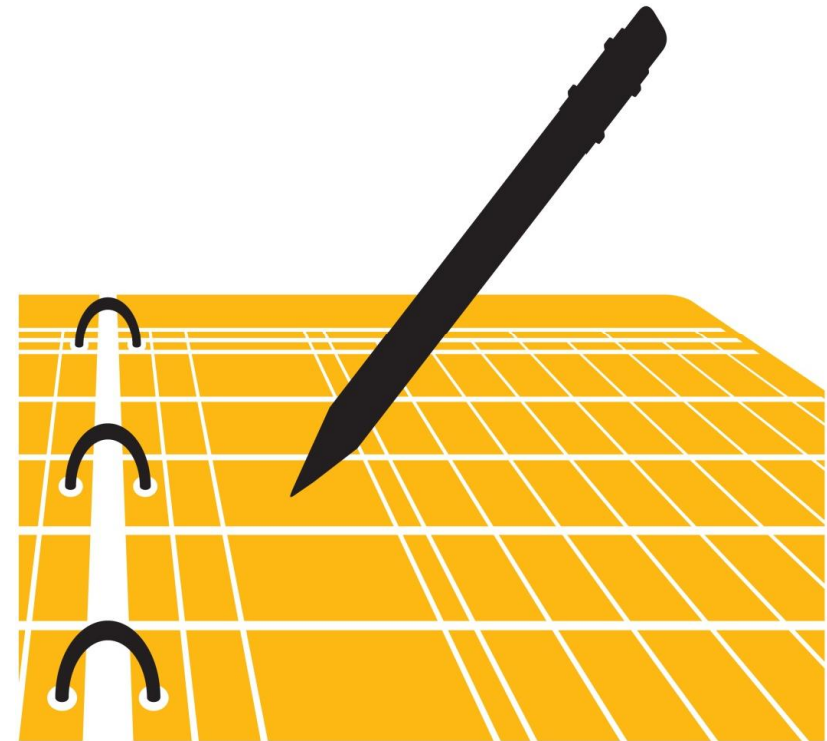
What is the current Landscape?

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?

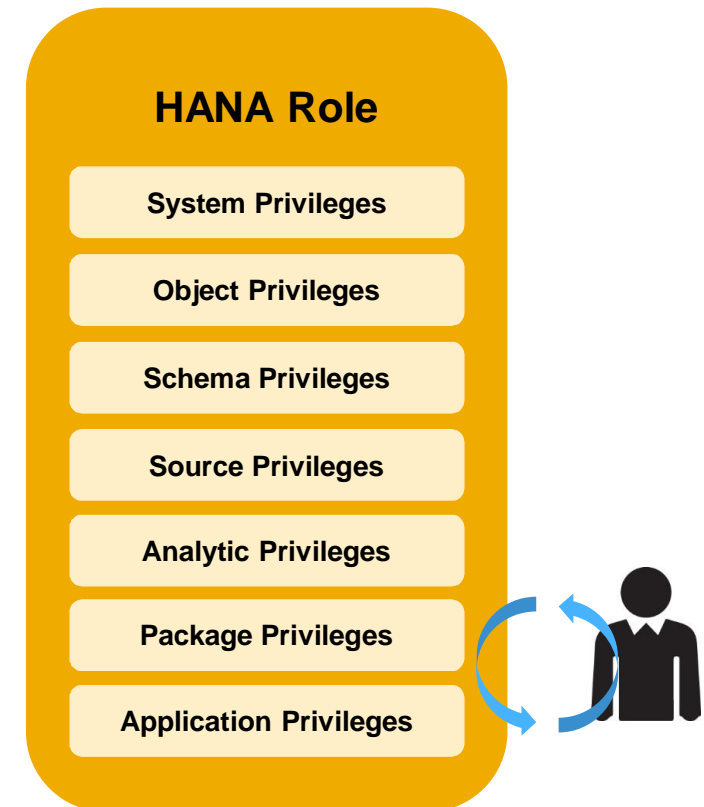


HANA Authorization Roles

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 modeling

Package Privilege

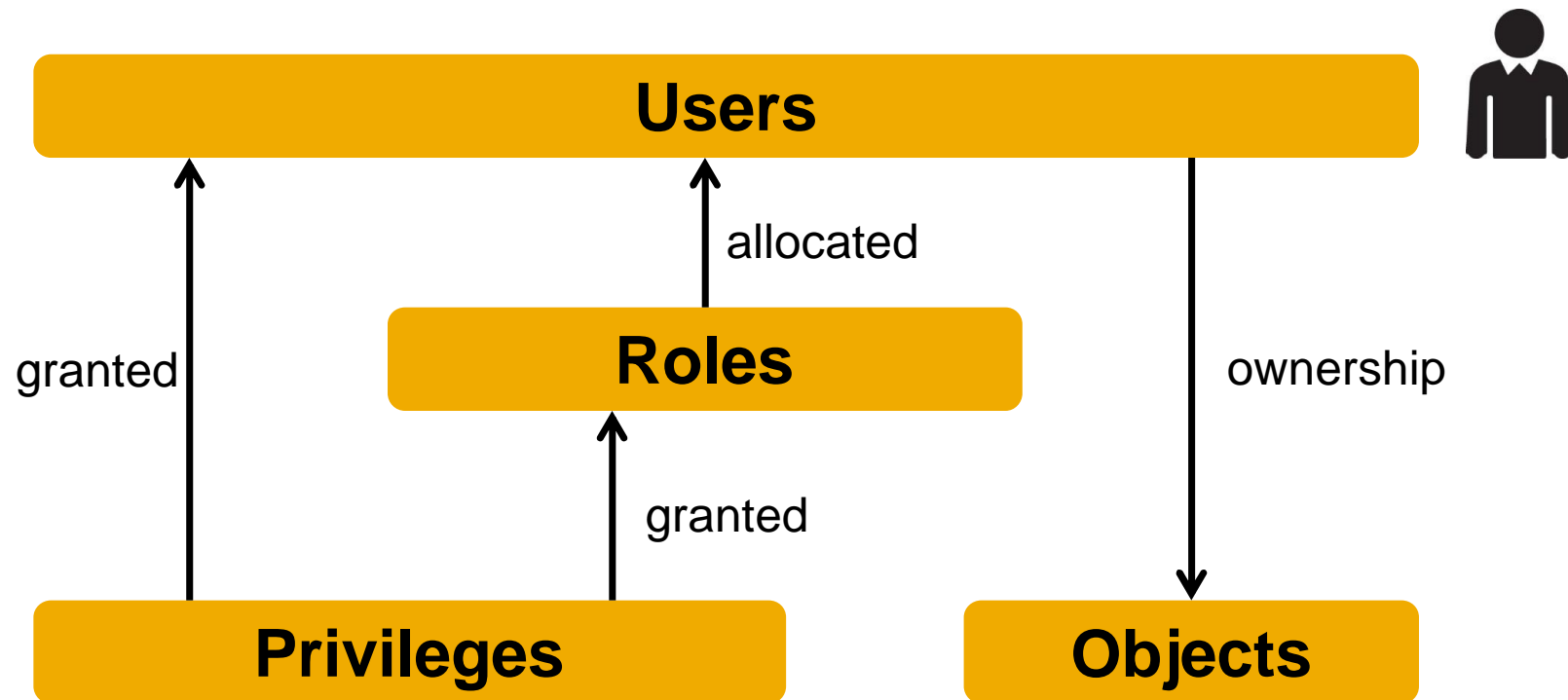


Allows access to data models

- f.e.: Analytic or Calculation Views
- Repository Objects

HANA Privileges Management

Directly to Users or via Role



Demo





HANA Authorization Roles

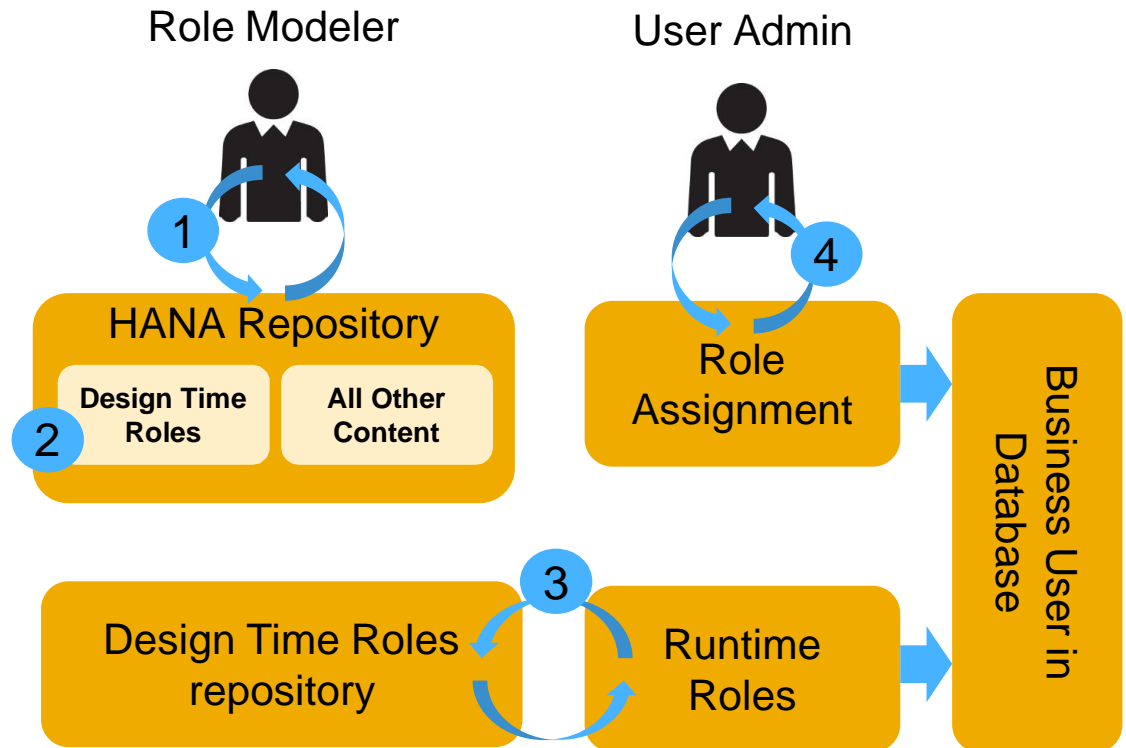
Design-time roles



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 procedure 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

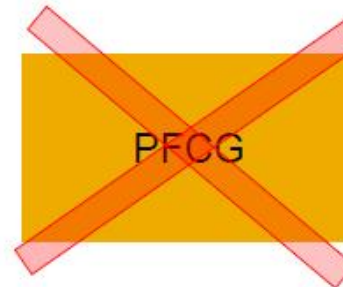
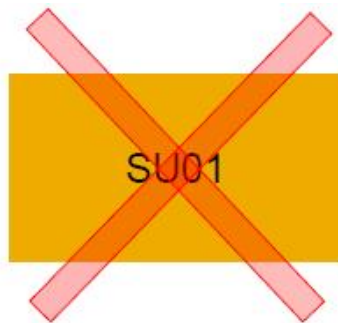
SAP GRC Access Control



GRC for SAP HANA

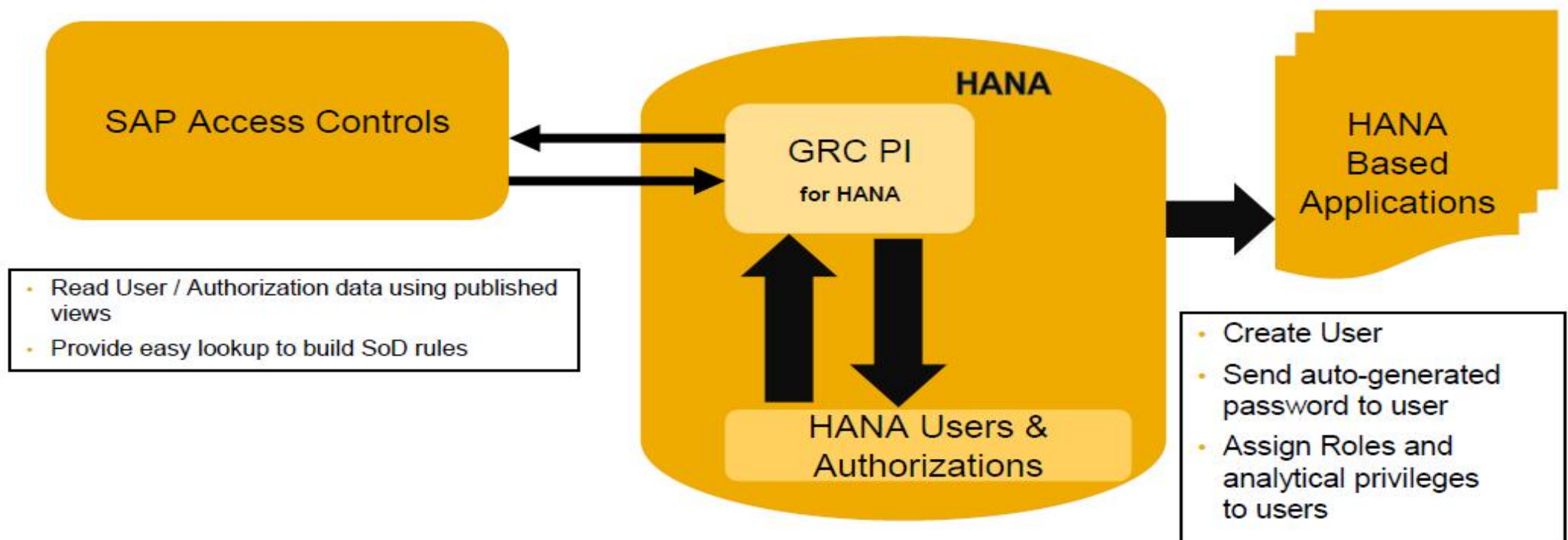
What is different on pure HANA applications?

- 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

Risk Analysis : User Level									
Analysis Criteria									
Multiple Selection									
Analysis Criteria									
Analysis Results									
Result Set: Result Set 1 Go Previous Next Export Result Set									
Result									
View: Table Display As: Table Print/Version: Export Type: Permission Level Format: Detail									
View: Table Display As: Table Print/Version: Export Type: Permission Level Format: Detail									
UserID	Access Risk ID	Risk Level	Function	System	ADP	Value From	Value To	Risk Profile	
TEST	ACTRL001	Medium	VATRU_FI	HD1	_SYS_BIC:sap.grc.ACTION_RULE	F0000	F9999	_SYS_BIC:sap.grc.ACTION_RULE_FI	
TEST	ACTRL001	Medium	VATRU_MM	HD1	_SYS_BIC:sap.grc.ACTION_RULE	M000	M999	_SYS_BIC:sap.grc.ACTION_RULE_MM	

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.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices.