

Securing SAP S/4 HANA guide

Illustrated by the Animalcare/Ecuphar Implementation

Christophe Decamps / Chris Walravens



Agenda

Introduction

Optimal Time to Secure Your S/4HANA

Security: Apply Best Practices

Integrated Conceptual Approach

Introduction

The AnimalCare / Ecuphar case

- S/4HANA 1709 greenfield implementation
- Embedded gateway for Fiori
- Full Fiori as front-end strategy
- Statistics

- 15 company codes
- 95 user-IDs
- 20 template composite roles
- 219 template single roles
- 156 Fiori catalogs
- 17 Fiori groups

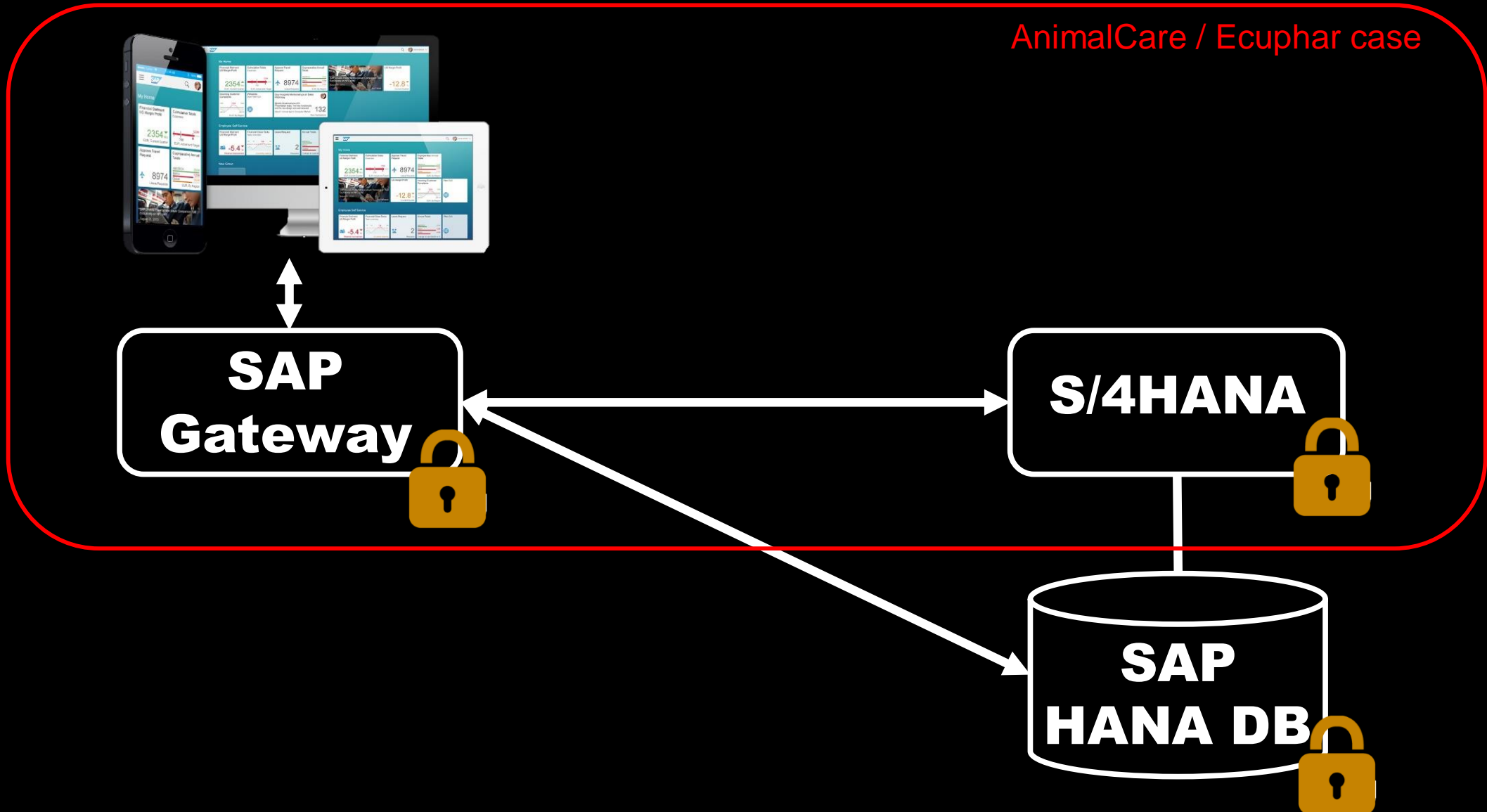
Product	Release	SP Stack
SAP FIORI FRONT-END SERVER	4.0	01 (02/2018)
NW FOR S4HANA ONPREMISE	1709	01 (01/2018)
S4HANA ON PREMISE	1709	01 (01/2018) FP
SAP FIORI FOR S4HANA	1709	01 (01/2018) FP

Composite role	Description
S4H_C_XXXX_XXXX_BUS_PRJ_MNGR	BUS - Project Manager
S4H_C_XXXX_XXXX_FIN_ACCOUNT	FIN - Accountant
S4H_C_XXXX_XXXX_FIN_CTRLR	FIN - Controller
S4H_C_XXXX_XXXX_FIN_CRD_CTRL	FIN - Credit Controller
S4H_C_XXXX_XXXX_INV_INV_MNGR	INV - Inventory Manager
S4H_C_XXXX_XXXX_INV_WH_CLERK	INV - Warehouse Clerk
S4H_C_XXXX_XXXX_IT_ADMIN	IT - Administrator
S4H_C_XXXX_XXXX_IT_ADMIN_LCL	IT - Administrator Local
S4H_C_XXXX_XXXX_IT_DEVELOPER	IT - Developer
S4H_C_XXXX_XXXX_IT_SERV_DESK	IT - Service Desk Clerk
S4H_C_XXXX_XXXX_MDM_ADMIN	MDM - Administrator
S4H_C_XXXX_XXXX_MRP_PLANNER	MRP - Planner
S4H_C_XXXX_XXXX_PUR_GR_CLERK	PUR - Goods Receipts Clerk
S4H_C_XXXX_XXXX_PUR_INV_APPR	PUR - Invoice Approver
S4H_C_XXXX_XXXX_PUR_PURCHASR	PUR - Purchaser
S4H_C_XXXX_XXXX_PUR_RELEASER	PUR - Purchase Releaser
S4H_C_XXXX_XXXX_PUR_REQUIS	PUR - Purchase Requisitioner
S4H_C_XXXX_XXXX_QM_QA_MNGR	QM - Quality Manager
S4H_C_XXXX_XXXX_SLS_CLERK	SLS - Sales Clerk
S4H_C_XXXX_XXXX_SLS_SHP_CLRK	SLS - Shipping Clerk

The screenshot shows the SAP Fiori dashboard with a navigation bar at the top containing 'Home' and several menu items: 'Purchasing - Reporting', 'Finance', 'Finance - Reporting', 'Controlling', 'Controlling - Reporting', 'Inventory Management', and 'Inventory Man...'. The main content area is divided into two sections: 'Purchasing - Reporting' and 'Finance'. The 'Purchasing - Reporting' section contains several widgets, including 'Display Purchasing Info Record', 'Display Purchase Order Price History', 'Display Purchase Order Advanced', 'Display Purchasing Documents by Supplier', 'Display Purchasing Documents by Material', 'Display Purchasing Documents by Number', and 'Display Purchase Contract'. The 'Finance' section contains widgets for 'Purchase Order Value' (73,20 M EUR), 'Print Purchase Orders', 'Spend Variance' (31,78 %), 'Purchasing report ZMR002A', 'Open Purchase Order Overview ZZ0PO', and 'Monitor Purchase Order Items' (1,86 K Overdue). The 'Create Asset Master Record' widget is also visible in the Finance section.

S/4 HANA Technical Point Of View

AnimalCare / Ecuphar case



Optimal Time to Secure Your S/4HANA

Do it right immediately

S/4HANA brownfield or greenfield implementation:

- Opportunity for improving security !
- Use that momentum to:
 - Review & optimize your historical authorizations concept
 - Ensure you start from a clean situation

Do it right immediately

For Fiori & HANA, implement security as from day 1

- Ensure your Fiori & HANA approaches are future proof
- Ensure your data are protected on database level as HANA is a platform allowing direct access
- Develop an integrated approach with your S/4 HANA, Fiori and HANA concepts

Clean-up afterwards / redesigning costs more

➤ **Start as soon as possible !**

Security: Apply Best Practices

Overall Security Objective Remains

Protect your **business processes and data !**

S/4HANA, Fiori & HANA:

- Different security mechanism
- Internal Control & SOD still applies

S/4HANA & Fiori

Technical example:

■ S_TCODE vs S_START vs S_SERVICE

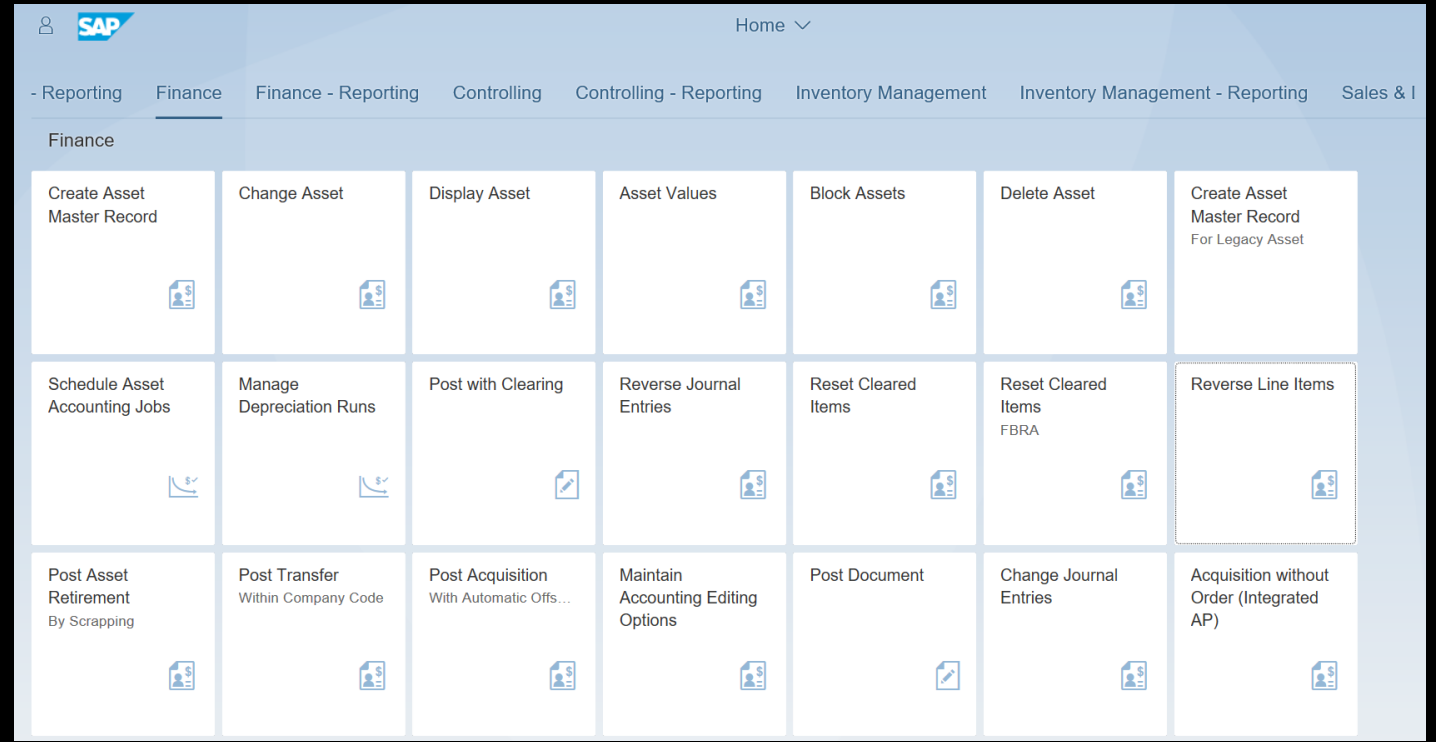
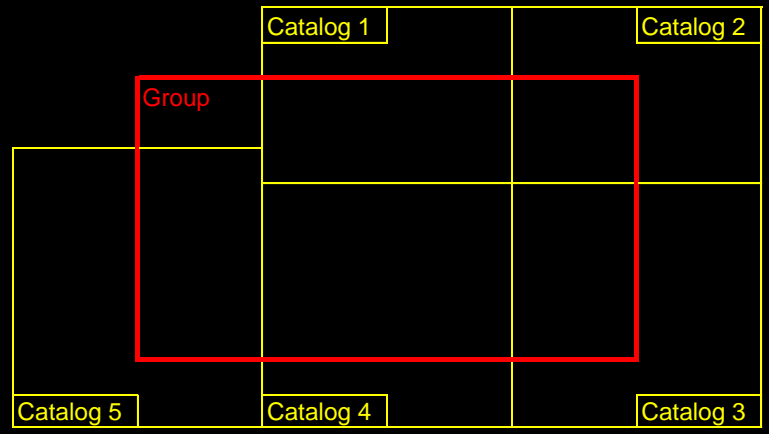
S4H_S_A_BCEU_ALLUSR		BC-EU: Basic Authorizations for all users (All)	
■	Maintained	Cross-application Authorization Objects	AAAB
■	Maintained	Authorization Check for RFC Access	S_RFC
■	Maintained	Authorization Check for RFC User (e.g. Trusted System)	S_RFACL
■	Standard	Check at Start of External Services	S_SERVICE
■	Standard	Start Authorization Check for TADIR Objects	S_START
■	Standard	Transaction Code Check at Transaction Start	S_TCODE

(*) Example from Animalcare/Ecuphar

S/4HANA & Fiori

Concept

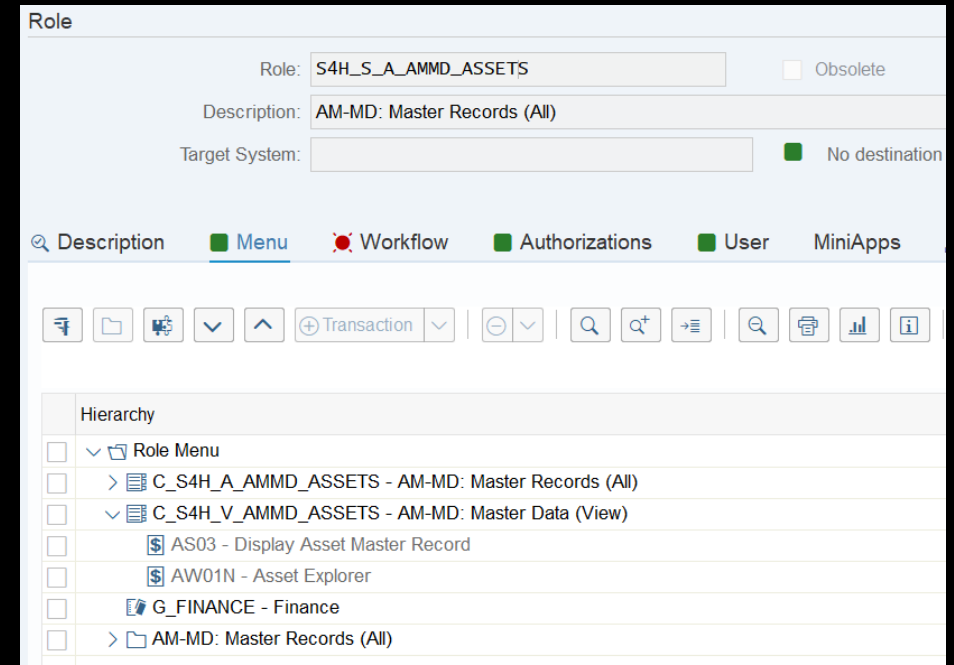
- Catalogs & Groups



S/4HANA & Fiori

Concept

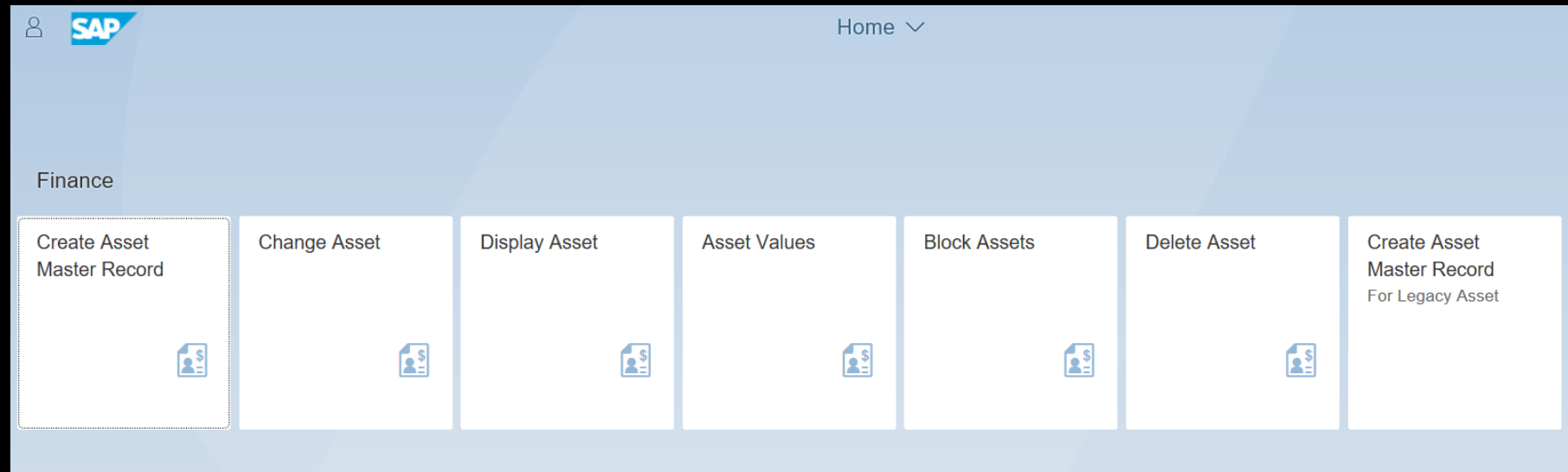
- Single roles / Tile roles
- Composite roles



The screenshot shows the SAP Role configuration interface for the role 'S4H_S_A_AMMD_ASSETS'. The role is not obsolete and has the description 'AM-MD: Master Records (All)'. The target system is set to 'No destination'. The role is configured with a menu, workflow, authorizations, and user. The menu configuration is shown in a tree view under 'Hierarchy'.

Hierarchy	
<input type="checkbox"/>	Role Menu
<input type="checkbox"/>	> C_S4H_A_AMMD_ASSETS - AM-MD: Master Records (All)
<input type="checkbox"/>	> C_S4H_V_AMMD_ASSETS - AM-MD: Master Data (View)
<input type="checkbox"/>	AS03 - Display Asset Master Record
<input type="checkbox"/>	AW01N - Asset Explorer
<input type="checkbox"/>	G_FINANCE - Finance
<input type="checkbox"/>	> AM-MD: Master Records (All)

(*) Example from Animalcare/Ecuphar



The screenshot shows the SAP Fiori Finance tile set. The tiles are arranged in a row and include: Create Asset Master Record, Change Asset, Display Asset, Asset Values, Block Assets, Delete Asset, and Create Asset Master Record For Legacy Asset. The 'Create Asset Master Record' tile is highlighted with a dashed border.

(*) Example from Animalcare/Ecuphar

HANA

Technical example:

- Privileges

Concept:

- Repository roles

- Mimic single and composite roles

The screenshot shows the SAP HANA security configuration interface. The title bar indicates the role being configured: `security.roles::SHX_S_A_BCSY_MOBAS_XXXX_MODELER_BASIC`. The 'Object Privileges' tab is selected, showing a table of granted privileges. The table has three columns: Object Name, Object Type, and Origin. The row for `models::assets` is highlighted, showing it is a VIEW with Design Time origin. To the right of the table, a 'Privileges' section lists the granted permissions: DROP, SELECT (checked), INSERT, UPDATE, and DELETE.

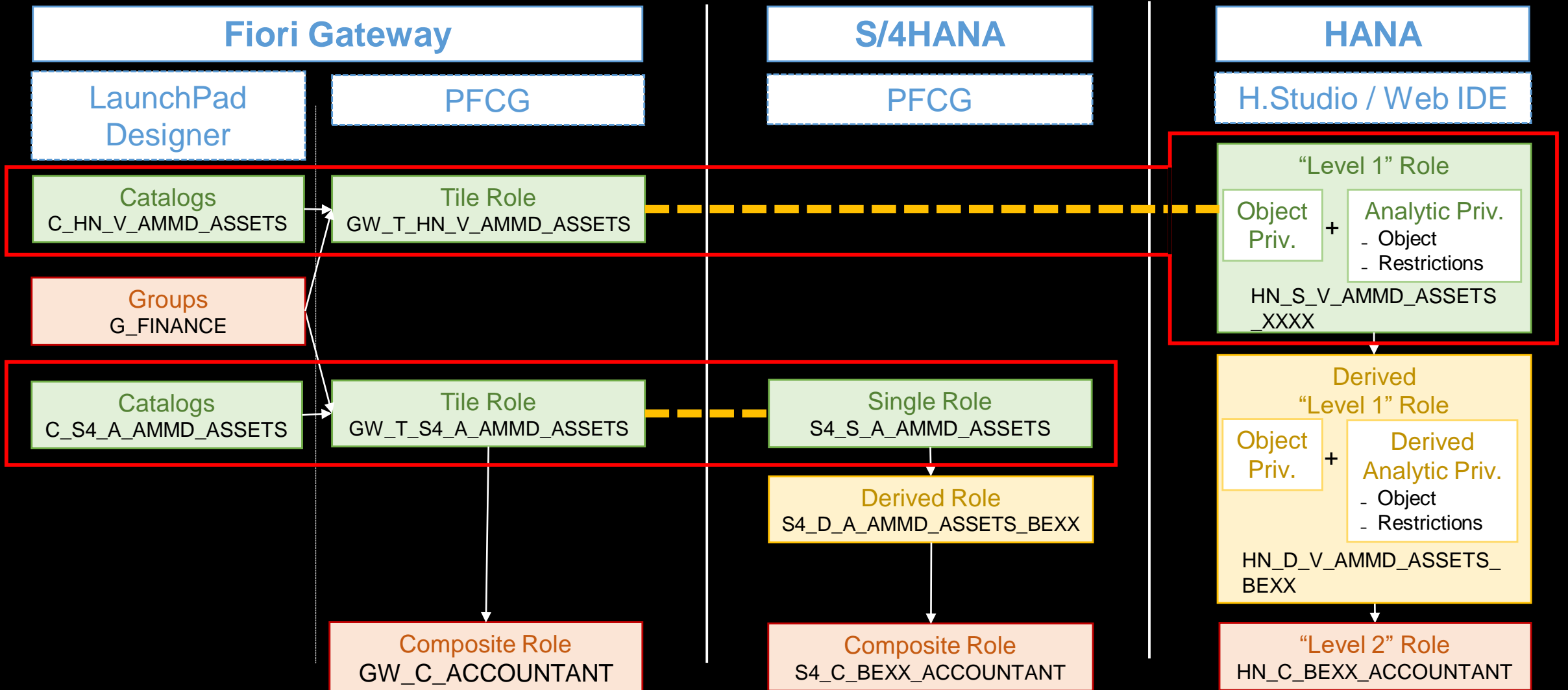
Object Name	Object Type	Origin
<code>_SYS_BI</code>	SCHEMA	Run Time
<code>_SYS_BIC</code>	SCHEMA	Run Time
<code>models::assets</code>	VIEW	Design Time

Privileges:

- DROP
- SELECT
- INSERT
- UPDATE
- DELETE

Integrated **Conceptual Approach**

Integration



Thank you.

Visit us at booth 8.3

Contact information:

Chris Walravens

GRC Community Lead & Partner

chris.walravens@expertum.net

+32 474 475 983

Contact information:

Christophe Decamps

GRC Senior Consultant

christophe.decamps@expertum.net

+32 473 720 125