SAP BI Authorization Improvement Roadmap

Bikash Mohanty
11/14/2011

Table of Contents

XYZ BI DATA USAGE SCENARIO / BACKGROUND

BI Systems

- Global BI system (B0*)
- Western Europe (B4*)
- EMEA (B7*, B0* & B4*)
- AMERICAS (B5*)
- ASPAC (B6*)

    - Each region & Global BI system has their own authorization strategy
    - Access requirement of users from different region are different
    - R/3, BI & Portal Authorization may not be in line with each other
    - There are access dependencies between different regional systems and regional-global system
        - Data restricted in Regional system should be restricted in global system as well
    - Support activities (authorization related) are handled by GSDAUTH team.
    - Report users are authorized based on their data & access requirements:
        - Data from single BI system
            - Data from multiple applications available (FIN, MKTG, OPS)
        - Data from multiple single BI system
            - Data from multiple applications available (FIN, MKTG, OPS)
        - Data from ALL BI systems through the Global BI system
            - Data from multiple applications available (FIN, MKTG, OPS)
    - Data accessed using either:
            - BEX Query directly
            - Portal reports which then connects to BW to display data

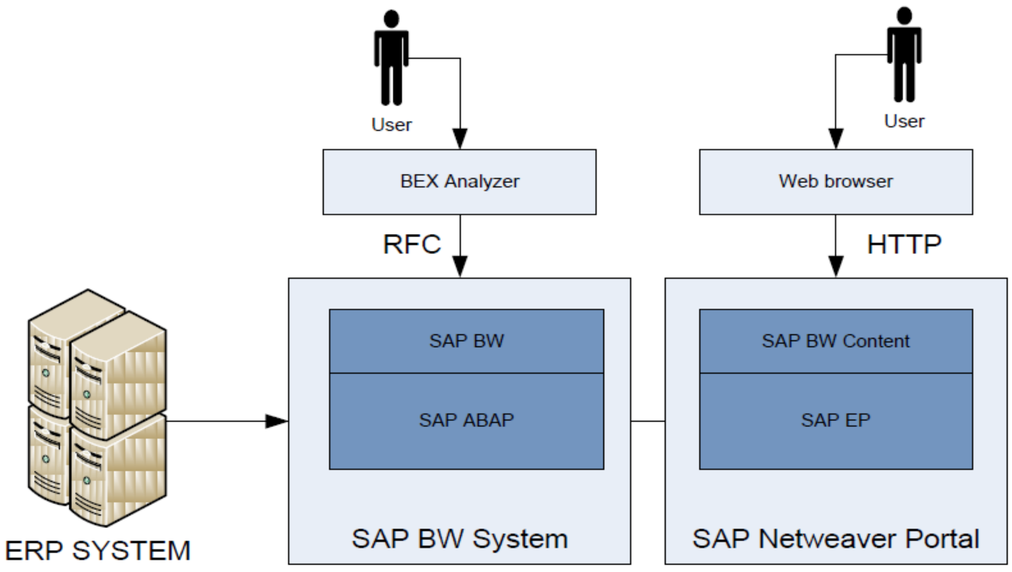
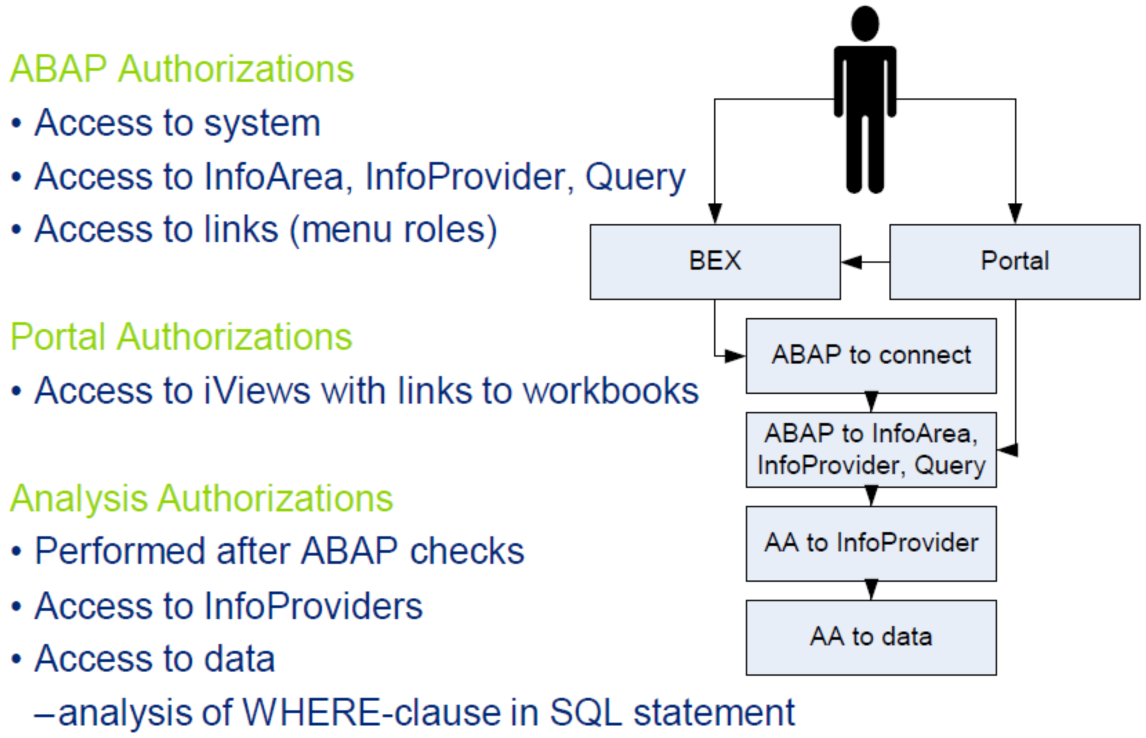


FIGURE 1: User request options to access BI data



ABAP Authorizations

- Access to system
- Access to InfoArea, InfoProvider, Query
- Access to links (menu roles)

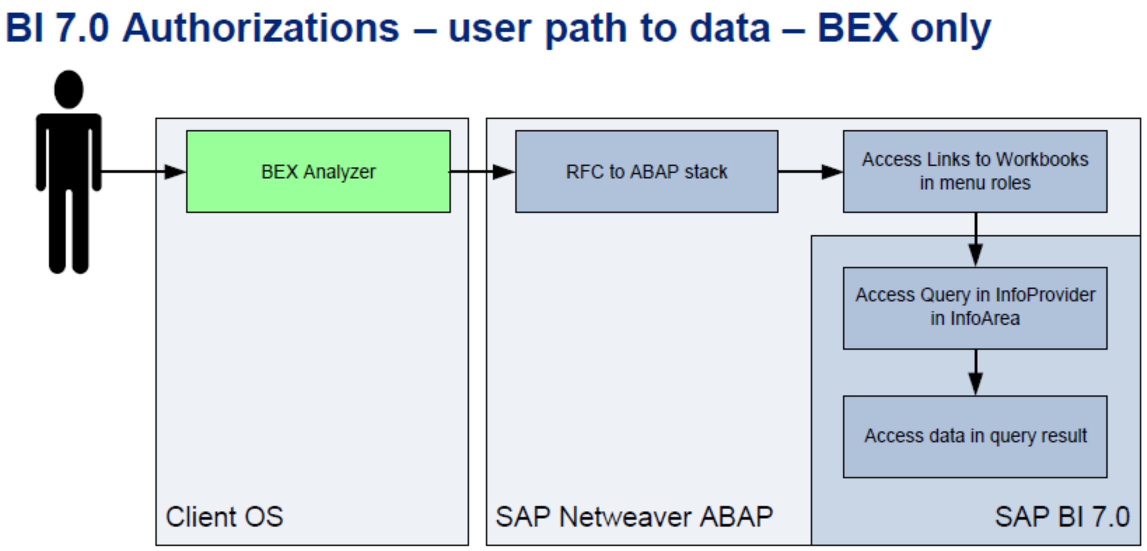
Portal Authorizations

- Access to iViews with links to workbooks

Analysis Authorizations

- Performed after ABAP checks
- Access to InfoProviders
- Access to data
  –analysis of WHERE-clause in SQL statement

FIGURE 2: Authorization request flow (User → Data → User)

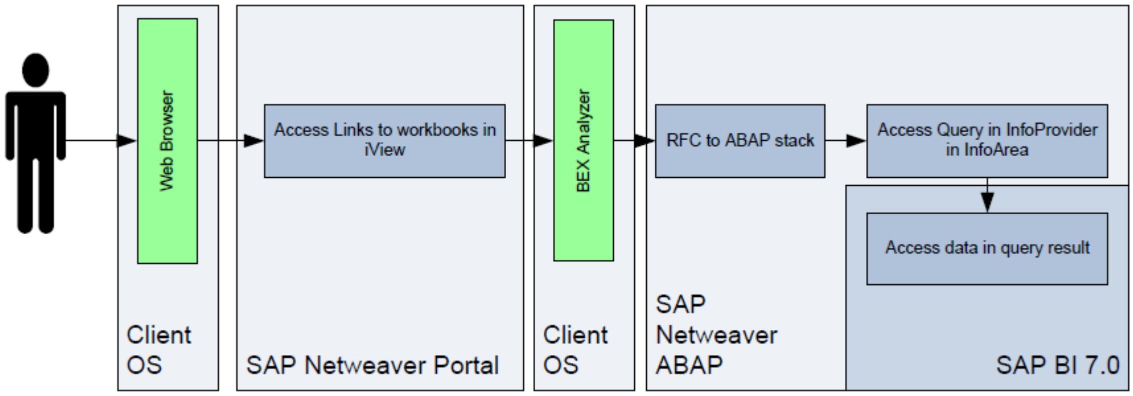


BI 7.0 Authorizations – user path to data – BEX only

BEX Analyzer
RFC to ABAP stack
Access Links to Workbooks in menu roles
Access Query in InfoProvider in InfoArea
Access data in query result
Client OS
SAP Netweaver ABAP
SAP BI 7.0

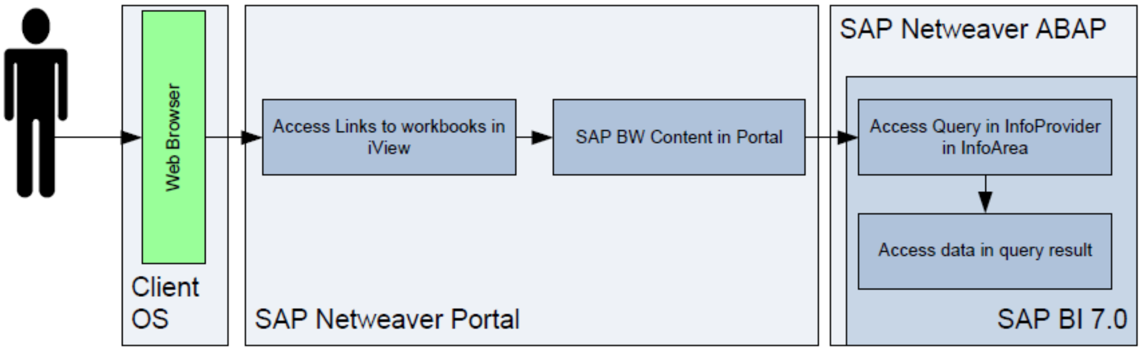
- Data Request received at client OS
- Request passed through RFC to the ABAP stack
- ABAP stack contains all the roles, which deals with the request based on the authorization it has for the requesting user.
- If the user is requesting more than what the ABAP stack has for the mentioned user in terms of role assignment – an error message is served.
- If the user is requesting within what the ABAP stack has for the mentioned user in terms of role assignment – data is displayed

BI 7.0 Authorizations – user path to data – Portal + BEX



- ❖ Data Request received at client OS
- ❖ Request passed through portal to BEX analyser and then using RFC to the ABAP stack
- ❖ ABAP stack contains all the roles, which deals with the request based on the authorization it has for the requesting user.
- ❖ If the user is requesting more than what the ABAP stack has for the mentioned user in terms of role assignment– an error message is served.
- ❖ If the user is requesting within what the ABAP stack has for the mentioned user in terms of role assignment – data is displayed

BI 7.0 Authorizations – user path to data – Portal only


Web Browser
Client OS
Access Links to workbooks in iView
SAP BW Content in Portal
SAP Netweaver Portal
SAP Netweaver ABAP
Access Query in InfoProvider in InfoArea
Access data in query result
SAP BI 7.0

- ❖ Data Request received at client OS / Web browser
- ❖ Request passed through Portal to the ABAP stack
- ❖ ABAP stack contains all the roles, which deals with the request based on the authorization it has for the requesting user.
- ❖ If the user is requesting more than what the ABAP stack has for the mentioned user in terms of role assignment – an error message is served.
- ❖ If the user is requesting within what the ABAP stack has for the mentioned user in terms of role assignment – data is displayed

CURRENT ISSUES:

Missing Objects:

- Category/List of roles by application data access***(Finance, Marketing, APO)***
- Category/List of roles by user types ***(Power / end-user / developer / support / Admin)***
- Category/List of roles by systems ***(regional and global system)***
- Category/List of roles by access / usage types ***(backend, front end, both, development, maintenance or creation, data display, data load, basis administration, scheduling, Query execution, Query maintenances.)***

If the above information were available at one place – it would be easy to pick up the most appropriate roles – when a REQUEST for user creation / modification is received.

Missing Process:

Requests for BI system access are received through an email at time. Request does not contain required information for the AUTHORIZATION team to act proactively without consulting the requester.

- BI system access should be submitted online.
- At the time of requesting access to BI system by submitting request online – the request form should have following mandatory fields.
  - BI system
  - User type (with drop-down to choose the value from)
  - Application data access (with drop-down to choose the value from)
  - Usage type (with drop-down to choose the value from)

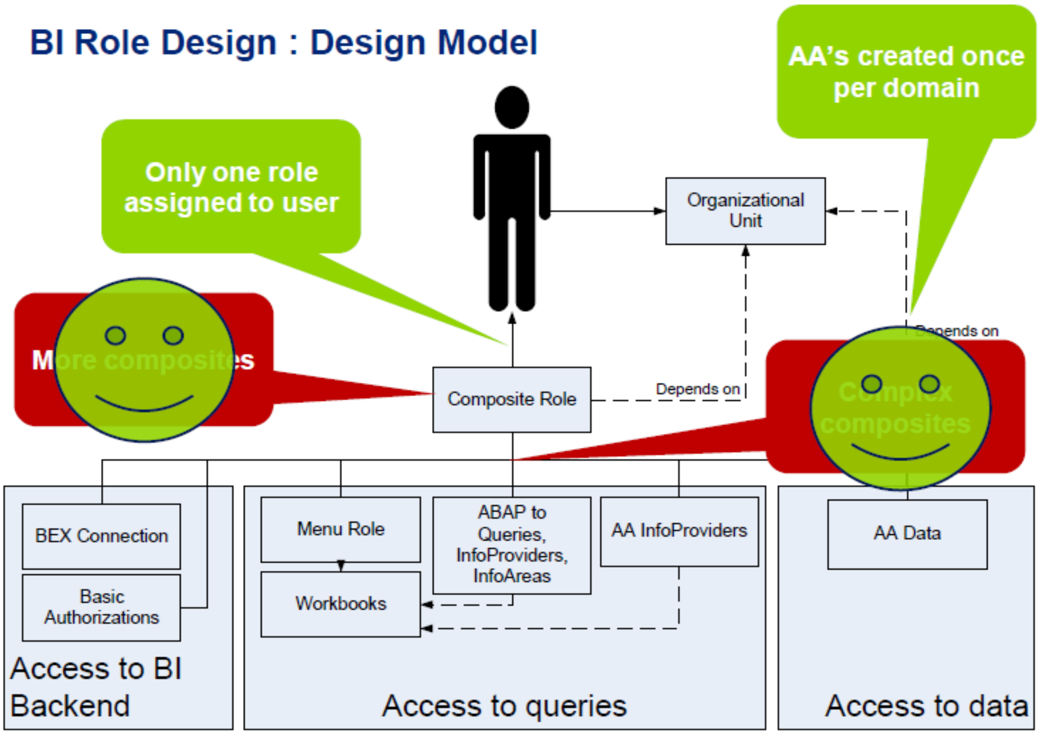
Consequences:

- Too many / unnecessary authorization or roles assigned to the user, which can decrease the report performance and hence system performance.
- Complex authorization process, which makes it difficult to analyse error and find resolution easily.

OBJECTIVES:

	Benefit	How to implement?
BI Analysis Authorization focus	• Focus is data analysis • Flexibility of reporting • Report execution time improved • System performance improved	Refer to sections ***"BI AUTHORIZATION DESIGN / MODELLING" & "BI AUTHORIZATION IMPROVEMENT - APPROACH"*** below. Following Limitations should apply to the Analysis: • Functionally • Organizationally
Simplification of authorization (role assignment) process	• Simple to implement • Simple to maintain • Simple to support	Refer to sections ***"BI AUTHORIZATION DESIGN / MODELLING" & "BI AUTHORIZATION IMPROVEMENT - APPROACH"*** below.
Simplification of error tracking procedure	• Improved response time to error resolution • Business confidence	Create a step-by-step house-keeping procedure for the support team / GSD AUTH to use
Easily available role mapping table by**:** Front-end access, back-end access and data	Readily available information. Easy to follow & compare	The mapping table need to be created. Sample format attached below.
On-line issue log	• Transparency • Can be referenced for similar errors in future	• Issues to be logged on-line • Resolution steps to be included before closing ticket • Searchable by key-word

BI AUTHORIZATION DESIGN / MODELLING:



Single layer concept
Separation of roles by:

➢ access to backend	(Development, Maintenance, Execution, Data)
➢ access to queries	(Creation, Changes, Execution, Deletion)
➢ access to functional area	(Functional Access)
➢ access to org unit data	(categorized data access by Org units)

Variations in single layered-ness

- Create composites for functional access
  - **Functional:** APO, Finance, Marketing.
  - Users can have any combination of functional area access
  - Composite roles can be maintained & re-used
- Create composites for organization unit data
  - **Organization unit:** Areas, End Markets, Region etc
  - Users can have any combination of Org units
  - Composite roles can be maintained & re-used

Organization unit - Move away from roles

- Assign Organization unit data access directly in user profile.

BI AUTHORIZATION IMPROVEMENT - APPROACH

CREATE:

- List of SINGLE roles by functional area access ***(Finance, Marketing, APO)***
- List of SINGLE roles by Organization unit access ***(Area, End market, Regions etc)***
- List of SINGLE roles by user types ***(Power / end-user / developer / support / Admin)***
- List of SINGLE roles by access / usage types ***(backend, front end, both, development, maintenance or creation, data display, data load, basis administration, scheduling, Query execution, Query maintenance etc.)***
- Create "COMPOSITE ROLES" for various combinations of SINGLE roles as per the mapping table below.
- List of SINGLE roles by systems ***(regional and global system)***
- List of composite roles by systems ***(regional and global system)***

MANAGE

- If roles are designed discretely for their purpose - It will be easy to manage, analyse and assign these SINGLE roles – in comparison to complex COMPOSITE roles which are fit for ALL purposes.
- If the above information were available at one place – it would be easy to pick up the most appropriate roles – when a USER ACCESS REQUEST is received.

ACCESS REQUEST PROCESS:

Requests for BI system access should be made through online request system. The request form should have following mandatory fields. Authorization consultant should action based on below mapping table information in place.

- BI system
- User type (with drop-down to choose the value from)
- Application data access (with drop-down to choose the value from)
- Usage type (with drop-down to choose the value from)

EXAMPLE:: MAPPING TABLE

System	**Data / Application** (Single role)	**User type** (Single role)	**Access / Usage** (Single roles / Multiple Single role)	**Composite role** (Containing all 3 single roles in the left hand side)
B4P	Finance	Power user	❖ Report Development ❖ Report execution ❖ LISTCUBE	
B4P	Marketing	Power user	❖ Report Development ❖ Report execution ❖ LISTCUBE	
B4P	APO	Power user	❖ Report Development ❖ Report execution ❖ LISTCUBE	
B0P	Finance Marketing APO	Power user	❖ Report Development ❖ Report execution ❖ LISTCUBE	
B5P	Same as B4P	Same as B4P	Same as B4P	Same as B4P
B6P	Same as B4P	Same as B4P	Same as B4P	Same as B4P

ROLE NAMING STRATEGY

Clarity needed

- Logic in naming convention
- Role mapping document

Simplify user maintenance

- User administrators want simple, easily accessible & easy to follow guide-lines

Assurance on user access

- Users get appropriate reporting access
    - Functional area access
    - Organization level access

PROJECT EXECUTION APPROACH:

Plan / Approach	**By Region** (B4, B5, B6, B7)	**By Function** (APO, MKTG, FINANCE)	**By User Category** (Power User, Admin, Developer, Report user, Support)
Short-term Plan **(Next 2 months)**	Prepare As-is	Prepare As-is	Prepare As-is
	Design to-be	Design to-be	Design to-be
	Consolidate current Issue logs	Consolidate current Issue logs	Consolidate current Issue logs
Long-term Plan **(Next 12 months)**	Prepare single roles in each system	Prepare single roles in each system	Prepare single roles in each system
	Prepare composite roles in each system	Prepare composite roles in each system	Prepare composite roles in each system
	Prepare mapping table based on usage type	Prepare mapping table based on usage type	Prepare mapping table based on usage type
	Testing using new roles & new user id	Testing using new roles & new user id	Testing using new roles & new user id
	If testing is successful – assign the new roles to the original user ids	If testing is successful – assign the new roles to the original user ids	If testing is successful – assign the new roles to the original user ids
	Prepare solution documents	Prepare solution documents	Prepare solution documents
	Prepare hand-over document	Prepare hand-over document	Prepare hand-over document
	Production cut-over	Production cut-over	Production cut-over
	GO-LIVE	GO-LIVE	GO-LIVE

RESOURCE REQUIREMENT:

Plan / Approach	From Business	From GSDAUTH	From Technology
Short-term Plan **(Next 2 months)**	1 (Part-time)	1 (Part-time)	1 part-time and 1 full-time
Long-term Plan **(Next 12 months)**	1 (Part-time)	1 (Part-time)	2 (Full-time)

PROJECT PLAN:

To be furnished – after initial project scoping

PROJECT RESOURCES:

Name	Role	Function
		Part-time
		Part-time
		Part-time
		Full-time
		Full-time