

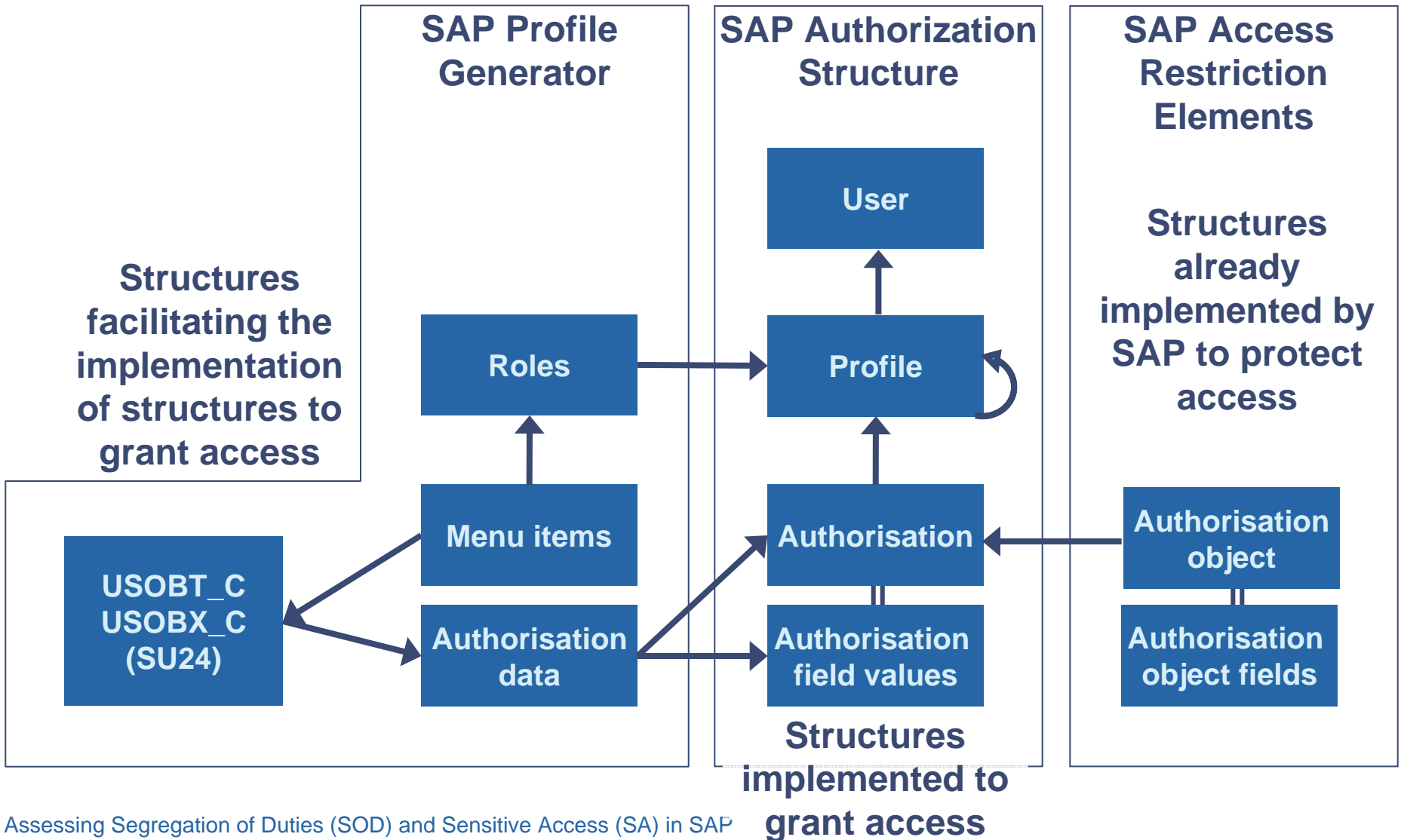
ISACA Orange County Chapter Assessing SOD and SA in SAP Wednesday November 5th, 2008



Stephan Imbach

- Managing Director at PricewaterhouseCoopers
- Located in the Orange County office
- Born in Switzerland (Basel) – moved to US in 2004
- Worked on SAP R/3 audits since 1994
- Leading global development center for ACE from 1995-2004 (ACE is PwC's access and configuration evaluation tool)
- Leading global efforts for developing and maintaining
 - SAP ITGC Practice Aids and Workprograms
 - SAP ITGC Training

SAP Authorisation Concept Structures



Examples of Backdoors in SAP Programming in Production

- Programming is one of the most powerful abilities in SAP
- If you allow somebody to program in any production client, then this person can do anything without leaving any traces
- Example:
Deleting SAP* user

Examples of Backdoors in SAP

Updating Database

- There are some functions in SAP allowing directly updating the database, e.g. via RSDD_EXEC_SQL
- If you allow somebody to execute that function, then this person can do anything without leaving any traces
- Example:
Resetting user group (or password) of an individual
- Please note:
RSDD_EXEC_SQL does unfortunately not have the correct authority check implemented by default – consider to implement an appropriate check.

Examples of Backdoors in SAP

SAP_Edit

- SAP_EDIT function allows to alter all tables via transaction SE16N
- Example: Altering table BKPF or BSEG
- Access requirements:
 - Version < 6.0: Patch to partly mitigate the risk
 - Without patch:
Object S_DEVELOP with activity 03 is necessary
 - With patch:
Object S_DEVELOP with activity 01/02 is necessary
 - Version >= 6.0: Patch is applied by default
 - See above
- Control approach:
 - S_DEVELOP with activity 01 should be restricted