Demystifying SAP security

Marc Sel · Kristof Van Der Auwera

PricewaterhouseCoopers
marc.sel@pwc.be
kristof.van.der.auwera@pwc.be

Abstract

This article attempts to demystify the feature-rich SAP security functions, to demonstrate how they can cooperate to build a strong security posture, and how to avoid some classic pitfalls.

ERP systems continue to gain importance in the developed world, and while there are many alternatives to choose from (including competitive vendors as well as OpenSource projects such as Compierre), SAP is a major force in this field. Over the years SAP established a rich security model, including infrastructure aspects such as secure networking and separation of production and non-production environments , but more importantly they also included all relevant Identity and Access Management aspects, as well as electronic signature aspects. As a result, a SAP customer is today facing a wide range of potential safeguards to chose from, each with their own cost/benefit ratio. However, it is generally accepted that application level securty is in the end more important than infrastructure security. The SAP authorisation model is at the heart of application security in FI, CO, HR, MM etc. It evolved over the years from a fairly simple, profile-based model with capabilities towards today's model that includes identities, roles, profiles and fine-grained authorisation object management. Dedicated authorisation objects have been established for the different functional areas within SAP, and various additional software components both from SAP and from external vendors can assist with building and managing SAP authorisations. Those include e.g. Virsa FF/SAP GRC, Axl & Trax (ex-CSI) and more recent CA's ERCM. PwC also still maintains their own ACE review tool.

Under the scrutiny of the ever increasing regulatory compliance, a company has to make the right options, or will face expensive mistakes. We will in this article address both the theoretical aspects of the SAP security model, including the authorisation model, and the more practical aspects as how to organise a SAP security project and how to tackle undesired side effects when implementing a real project.

1 Introduction

1.1 The scene

Common to many organisations is that they have a limited number of core value chains such as developing a product/service, selling it and collecting due compensation, and delivering the product/service. Often technology enables these value chains or is even fully embedded in the organisation's fabric. SAP's solutions grew from offering core business applications (Enterprise Resource Planning) to a wide spectrum of solutions, embedded in the economic ecosystem. These solutions play a role in accomplishing many different and challenging tasks, including for example managing the European Commission's budget.

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2009), 1-10

1.2 Evolving functionality and technology

Originally SAP R/3 was introduced in 1992, based on a 3-tier (data, logic, presentation) architecture. It built on the concept of an enterprise model, supported by a data model, shared by all applications. The enterprise model is based on the ‘Mandant’ representing the highest organisational level of the enterprise. Within a ‘Mandant’, different organisational and legal entities can share data such as accounting ledgers, and can consolidate information. Across ‘Mandanten’, data is not shared. Through customization, SAP allows meeting the diverse compliance requirements for accounting and VAT, and supports most of the administrative business processes (Order2Cash, Procure2Pay, Treasury, HR, etc). .

Relational tables implement the data model, transactions are coded in the SAP-specific ABAP language through the ABAP workbench, screens are painted and chained with Dynpro, and end-user access is via the dedicated SAP-GUI. Transaction SE16 is the general purpose data browser, allowing you to browse all tables (assuming you have appropriate authorisations). The functional areas are structured into BC (Basis Components, client server technology, OS, DB and also security), CA (Cross-Application, euro support, document management, archiving), AC (Accounting, including FI - Finance and CO - Control, investment and treasury), HR (Human Resources), and LO (Logistics, including Materials Management, Plant Maintenance, Production Planning and Sales and Distribution). Specific modules such as APO for planning emerged. There are multiple alternatives for data exchange and integration. Within the Basis System, CTS, the Change and Transport System allows managing separate production and non-production environments.

As a next wave of integration, SAP introduced their Enterprise Portal solution, acquired from TopTier. The SAP GUI was complemented by the browser. This gave rise to the SAP login ticket, stored on the client-side as an HTTP-cookie to allow single-sign-on.

SAP introduced mySAP ERP in 2004. Under the complementary Netweaver brandname, SAP embraced Java and Web Services technology. SAP R/3 expanded from applications on a basis system into an application core, enterprise and industry extensions and collaborative functions. These are all based on Netweaver as application and integration foundation, with co-existing ABAP and J2EE logic. As such, the core financial functionality (FI-CO) migrated into mySAP ERP Financials, which included an enhanced GL. Further improvements addressed the Financial Supply Chain and its core processes (P2P, OTC, Treasury, etc), as well as reporting, planning, consolidation etc. HR enlarged into Human Capital Management.

Master Data Management was introduced to provide more integrated data views, eg producing a single view on all credits of a single debtor. Reporting was enhanced through the Business Integration functionality, and XI improved the data exchange and integration.

1.3 Fundamental safeguards

Originally, users were required to install the SAP GUI on their machine. Once authenticated with userid/password, they were provided a menu interface. Their run-time capabilities where constrained by the authorisation checks coded within the ABAP application programs. These checks verified that a user had the required authorisations in the form of Authorisation Objects (containing fields and values). This can include organisational checks (does the user belong to the appropriate part of the organisation), checks for the right to execute a particular transaction (does the user have the right to create a Purchase Order), and fine-grained checks (does the user not exceed e.g. a financial threshold). Such authorisations are granted via Profiles, which can be single or composite (composed of multiple single Profiles). This is typically referred to as a capability model, allowing fine-grained authorisation management.

For example, typical authorisation objects for transaction FB50 (GL Posting) includes the basic check for transactioncode: S_TCODE (with field TCD – transactioncode (which should then allow access to FB50)). Further objects are F_BKPF_BUK (with fields BUKRS (eg 0001) and ACTVT (01, 02, 03) – 'Buchungskreis' und 'Aktivität'), F_BKPF_BUP ('Buchungsperioden' - timeperiods), F_BKPF_GSB (with fields GSBER (eg 01, 02) and ACTVT – 'Geschäftsbereich' und 'Aktivität'), F_BKPF_KOA (with field KOART (D, K, A, S, M) and ACTVT – 'Kontoart' und 'Aktivität'). Note that modules may have their own additional complement to S_TCODE, eg the HR module has the additional P_TCODE object. SAP_ALL is probably the best-known composite profile, allowing virtually all accesses. Which authorisations are checked in which transaction is decided at customization time, and can later be managed via a.o. SU24.

It should be noted that in some situations, the model introduced undesired side-effects since AO's may be reused in different contexts. Furthermore, a complementary ACL (access control list) model was also implemented; its groups are managed via SUGR.

Management of identities and authorisations is via dedicated transactions such as SU01 (User management), SU02 (Profile management), SU03 (Authorisation management) and SUIM (InfoManagement). To find out which authorisation checks are used in transactions, you can make use of ST01 (trace) and SE38 (displays code source).

For larger landscapes SAP introduced the CUA (Central User Administration). For a good introduction refer to [SAPBRTW].

As specific applications required their own fine-grained access control, dedicated AO's such as for HR were introduced. And as the combinatory space of users, profiles, authorisation objects and authority checks increased, R/3 4.5 introduced the Profile Generator PFCG and activity groups (AGRs). It is then recommended to segregate administrative tasks into three distinct sets:

1. 'Authorisation data administrators' create activity groups and maintains authorisations;
2. 'Authorisation profile administrators' generate profiles;
3. 'User administrators' assign activity groups (or profiles) to users.

These administrators will be the only ones with the activity groups and authorisations that allow them to manage the accesses of the end user community.

As from R/3 4.6, there were approximately 900 authorisation objects, structured into some 40 object classes. Activity groups were replaced by the concept of roles, and template roles were introduced. These roles are translated into Profiles, linking the users to their authorisations.

Finally, all table updates/deletes can be logged at system level. The existing logs can be displayed with Transaction Table history (SCU3).

2 Enriching the model

2.1 SAP Basis security

SAP Basis contains the authorisation model with the authorisation objects (as introduced in the preceding section), as well as the Change and Transport System security, network security, and secure 'store and forwarding'.

2.2 Change and Transport System security

The Change and Transport System allows coordination of own developments, their migration across the SAP landscape, program upgrades, and copying of ‘Mandanten’. It is mainly composed of the Transport Organiser and the Transport Management System.

TO manages customer developments created with the ABAP workbench. What development is actually allowed is fixed at the level of the ‘Mandant’. The Transport Organiser safeguards the originals in a repository, and migrates copies through the SAP landscape. TMS allows to define which systems play a role in the landscape, and the transports between them. This allows to build a segregated production/ non-production landscape, and to control the transfer of software developments into production.

2.3 Network security – SNC and SAProuter

Secure Network Communications (SNC) was created to guarantee confidential data transfer between SAP GUI and an Application Server, particularly in an Internet and WAN setting. It relies on cryptography and is based on the well-known GSS API. Its usage was later expanded toward protection of network traffic between distributed SAP components. SNC relies on an external crypto product. In addition you can implement additional features offered by the external security product (Single Sign-On, or smart card authentication).

SAProuter is an Application Level Gateway, serving as an intermediate station (proxy) in a network connection between a SAP System and programs accessing that system. It complements traditional port and network level firewalls. SAProuter and SNC can be integrated, where the former will then decide which SNC connections can reach which applications.

Alternatively, non-SAP specific firewalls and VPNs can be used too for network security.

2.4 Http access and SSL

The ITS (Internet Transaction Server) opened access to browser-based clients. SAP also acquired Top-Tier and their portal solution, allowing access via iViews. This allowed standard browser access, with SSL/TLS possibilities where required.

2.5 Complementary smart card authentication

Furthermore, the basic userid/password authentication can be improved using third party smart card products. However, given the relative complexity of rolling out smart cards, readers and drivers, as well as a Card Management System of some form, this was not a very popular route for most customers.

3 Electronic signatures

3.1 Electronic signatures – TrustManager

Electronic signatures have been in use since the 1970’s, but got a boost by the Internet. They are typically based on a combination of two complementary transformations, signing and verifying. Most systems are based on so-called public/private key solutions, where signing happens with the private key (safely stored in e.g. a smart card) and verifying relies on the public key (published in a certificate, and made available via e.g. a public directory). Management of public keys and their certificates is typically done via a PKI (public key infrastructure). SAP provides the TrustManager to manage keys & certificates. Underlying cryptographic libraries can be obtained from vendors such as IAIK.

3.2 Application level cryptography - SSF

SAP's SSF (Secure Store and Forwarding) offers signing/verifying as well as encrypting/decrypting features. The classical signature formats are supported such as PKCS#7, XML, S/MIME, PDF and more recently the various XML formats. SSF is provided for SAP Web Application Server, for the ABAP stack and for J2EE. Integration into applications is performed with Business Add-ins (BADI), customer exits, or own modifications. Alternatively you can use SAP's Business Connector.

If required, e-signatures can also be used to secure the output of e.g. payment programs such as SAPF110S via BADI's (Business Add-In). Key management is with SAP's TrustManager or an external PKI.

4 SAP GRC suite

For various reasons, the notion of Governance, Risk and Compliance increasingly gained importance. This confirmed the relevance of Internal Control models such as COSO, which relies on Segregation-of-Duty as a fundamental control principle.

The SAP GRC suite assists in addressing access control and segregation-of-duty matters in an ABAP-based system. It evolved from the 'Continuous Compliance' toolset acquired from Virsa (and originally developed by PwC as SAFE – Security Administrator for ERP). GRC Access Control can be considered an evolution of the Profile Generator, expanded by a segregation-of-duty matrix. The matrix is structured into domains, which map to transactions, authorisation objects and similar. Furthermore it includes much-sought after functions such as self-service password reset. The Access Control product is complemented by:

- Risk Analysis and Remediation (formerly 'Compliance Calibrator') which controls violations preventively at provisioning time. Its functions are callable via Web Services too;
- Superuser Privilege Management (formerly 'Firefighter'), enabling super-users emergency access to enterprise systems without committing regulatory violations by introducing mitigating controls.
- Toolset Configuration and Business Process Enhancements for User Access Management (Compliant User Provisioning) and role administration (Enterprise Role Management).

5 Netweaver and Identity Management

5.1 Netweaver

SAP introduced J2EE-based Web Application Servers with Netweaver. In J2EE and Portal systems identities are typically based on LDAP or third party IAM systems. Netweaver's user management is based on the UME (User Management Engine), comparable to SU01 for ABAP systems. In a J2EE environment, access control comes in two different approaches: declarative and programmative. Declarative corresponds to a coarse-grained check defined in the deployment descriptor of the program, while programmative means fine-grained with checks hardcoded inside the program. Obviously, declarative controls are faster to implement and the first way to go.

Netweaver allows Web Services, program-to-program communication with service announcement, discovery, transport and all other WS features. Authentication and authorisation is now converging towards SAML and Ping Identity, with key management where required via XKMS. Key management is now receiving renewed attention, because SAML assertions about a subject may be signed too.

5.2 The identity federation challenge

Once an organisation wants to accept users from other entities with who they cooperate (‘the federation’), they are facing federation challenges. In such a federation, the key roles are the producer and consumer of assertions. A producer makes statements about a subject such as ‘authenticated by me (so if you trust me, you can let him in)’, or ‘in possession of attribute X (e.g. I confirm that he’s older than 18 years of age)’. Note that these two assertions may come from independent providers. A consumer makes use of such assertions. Furthermore, the subject may wish to select which producer to use for a specific application service he wants to access. The service provider is the one ‘consuming’ the assertions. He is also said to be the relying party since he trusts the party that endorsed the assertion. Assertions are typically expressed in XML, and digitally signed to protect their integrity.

Where SAP originally relied on their own format for assertions (‘tickets’), through cooperation with a.o. Ping Identity they moved into open federation standards such as SAML (Security Assertions Mark-up Language). Third parties such as IBM also started to offer federated identity management solutions for Netweaver.

5.3 Netweaver Identity Management

Acquiring MaxWare enabled SAP to further improve Netweaver Identity Management. It aims at managing IDs across the entire SAP landscape, with or without any existing CUA. Netweaver IM is based on the MaxWare directory concepts and services, on which provisioning scripts are based. This allows creation of high-level business roles, which can be mapped onto technical roles, containing the actual resources, which may include Profiles and other managed elements. Information available in SAP HR can either be leveraged via propagation of HR attributes into LDAP, or accessed more directly. The two core components of IM are the Identity Center (with workflow, the ID database, and event processors) and the Virtual Directory Server (creating a unified view over many physically different directory services via connectors and SPML).

Through integration, Netweaver IM can make use of all controls defined in GRC, including segregation-of-duty, allowing capitalization on investments in prior control developments.

It can be observed that where many traditional IAM vendors started from non-SAP and gradually expanded their scope towards SAP, Netweaver Identity Manager starts from SAP and reaches out towards the non-SAP sphere too.

6 Complementary tooling

Besides the SAP-supplied solutions, there are numerous additional tools. We will only discuss a small subset of relevant tools and have no objective of being exhaustive.

6.1 CA ERCM

In 2008 Computer Associates acquired Eurekify, a player in the deployment of pattern matching technology which can be used to automatically generate roles across an entire organisation, including for SAP. Furthermore, business rules could be expressed and validated over the existing or envisioned authorisations. This can be done for off-the-shelve applications, as well as home-grown developments, greatly facilitating both compliance and IAM solutions. It is particularly well suited to express segregation-of-duty constraints over all possible authorisations, both coarse and fined grained. The Enterprise Role and Compliance Management solution is now integrating with the CA IAM solutions. This allows e.g. testing a business rule such as segregation-of-duty prior to granting an authorisation.

6.2 Other

There are numerous security add-ons available for SAP. These include Virtual Forge's ABAP scanner and CodeProfiler, which reveals security defects in custom programs.Other complementary products include the product suite from Axl & Trax (formerly CSI), BizRights' Approva, and Aveksa's suite. Furthermore, despites its name, Security Weaver offers functionality similar to the SAP GRC suite, i.e. focused on traditional authorisation objects and ABAPs. Swiss-based but in India developed Conteliga also offers such functionality.

7 Tying it all together

7.1 Organising your SAP security project

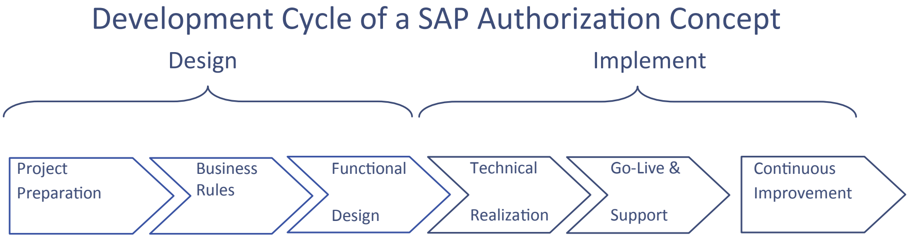
There is sufficient high-level guidance on how to organise security projects in general. However, before committing to a SAP security project, you may find it helpful to consider the various SAP safeguards from an ISO 27K perspective.

#	Security domain (aligned on ISO 27001)	Possible SAP safeguard
1	Policy 'Information Security'	May be referenced at SAP login time.
2	Organisational design, including roles & responsibilities, and horizontal and vertical segregations of power/control	'Mandant' and organisational structures reflected in Authorisation Objects SAP HR
3	Asset management	Can be handled via SAP functionality
4	Human Resources Security	SAP HR/HCM and EPP
5	Physical and environmental security	n/a
6	Communications and operations management	SAP router, SSF and SNC TrustManager (PKI) Platform hardening PUT (patches) management, SAP Notes
7	Access control	SU0x, SUIM, Role, Profiles, Authorisation Objects, Profile Generator, CUA SAP GRC suite and Netweaver IM
8	Information systems acquisition, development and maintenance	Access to ABAP Workbench, Netweaver Developer, developer key CTS - Change and Transport System
9	Information security incident management	SAP Logging – SCU3
10	Business continuity management	'High-availability' landscape
11	Compliance	SAP GRC suite
12	Independent audit and review	Various reports as well as SAP AIS

Finally, it is also relevant to consider accreditation (e.g. according to the Common Criteria) when selecting a safeguard.

7.2 SAP Authorizations

At the core of any SAP security project lies the development of an appropriate authorization concept.



Our approach is always based on a collaborative team comprising PwC and client staff. The most effective approach is to start from the business context and assess the actual situation compared to the required good practice situation (i.e. business rules based on the organisation and constraints stated in for example in regulations such as Sarbanes-Oxley). Next, we identify any discrepancies in the technical implementation, resulting from a historically grown combination / mix of SAP authorisations. The root cause of this ‘inadvertent’ access can either be poor role design & maintenance based on approved user access requests or ineffective approval procedures for requests. Conceptually:

	Business Rules	**SAP Roles**	**SAP Authorizations Challenge**
As-is	Actual functions performed by individuals Current segregation of duties and access rules in place	Actual roles assigned to individuals Degree of segregation of duties conflicts contained in current roles	Does the combination of roles lead to additional unintended access? Do the underlying SAP objects effectively support the role description?
To-be	The appropriate segregation of duties and access rules (in the form of a matrix) Required compensating controls where segregation of duties cannot be achieved	Roles required to support business rules Transactions required in each role Suitable role hierarchy and segregations	Changes required in the current authorizations of profiles? Creation of new authorisation profiles required?

We illustrate this as:

	Business Rules	**SAP Roles**	**SAP Authorizations**
As-is	Person A performs functions 1, 2 & 3 which have been approved by his manager	Person A has been granted roles which gives him access to functions 1, 2, 3, & 4	The combination of roles has allowed person A to have access to functions 1, 2, 3, 4 & 5
To-be	Person A should only be performing functions 1 & 2 Until a new resource is allocated for function 3, Person A’s manager has to monitor the performance of function 3	Person A has roles assigned which will only allow him to perform functions 1 & 2	The combination of roles does not lead to any additional unintended access

To identify all important gaps, the project team will define the to-be situation and then compare the as-is situation for business rules, SAP roles and underlying SAP authorizations with it. To analyze 'as is' authorizations, PwC developed ACE ('Automated Controls Evaluator'). ACE first extracts configuration controls and security data from a client's SAP system and copies it into a customised MS Access environment for analysis. Profile designs and user allocations can then be analyzed against SAP administrative objects, critical module transactions and combinations of transactions. ACE allows the user to complete all test cases at the authorisation level, thus the results are more representative of the client's actual security design. Complementary, data from RBE (Reverse Business Engineer) can be used to match transaction usage to users, including frequency of usage. RBE is an ABAP program that extracts data from the Performance Management system (ST03). It helps to compare transaction and system usage between R/3 installations, clients and within organizational entities. Tools such as CA ERCM can be instrumental here, even more so because they work across all applications, not just SAP.

Through the gap analysis, we identify root causes for exceptions. These may be in the area of business rules, of SAP role definitions or underlying SAP authorizations. This information is critical to plan effective remediation efforts and develop a sustainable access and authorisation maintenance policy in future.

To close the gaps, it is suggested to work with role tiers. Tier 1 contains the general roles, accesses assigned to all end users across all functional areas. Tier 2 contains common reporting and display roles within functional areas. Tier 3 contains the functional roles, allowing users to make changes to both transactional and master data. There roles contain the typical create/change/delete/block/post functionality, and are grouped e.g. into tasks. Finally, tier 4 are referred to as the enabler roles, controlling the field-level accesses. These roles do not contain transactions, only authorisation object level definitions to various organizational level fields. Where Tier 2 and 3 provide access to transactions, tier 4 enabler roles permit the accesses required to specific organisational values that allow these transactions to be executed properly.

Testing for undesired side-effects via test suites and tracing remains a key activity throughout the project.

7.3 SAP GRC projects

Also here, our approach is based on a collaborative team comprising PwC and client staff. A typical SAP GRC project would include the following five phases:

- Scoping, Planning, SAP GRC & Controls Awareness Training and Roadmap;
- Toolset Configuration and Business Process Enhancements for sensitive access and SoD (Risk Analysis & Remediation and Super User Privilege Management) including initial remediation of 'quick win' segregation-of-duty conflicts;
- Toolset Configuration and Business Process Enhancements for User Access Management (Compliant User Provisioning) and role administration (Enterprise Role Management);
- Putting into practice Security Processes; and
- Remediation of Security Design (Role Design).

The client typically provides a senior level project manager to work as a dedicated member of the project team. The purpose of this arrangement is to assist with management of the project schedule and help to efficiently coordinate the various work sessions required. As a critical success factor in this process a business sponsor at the C-level (CFO, CEO, CIO) who can set the 'tone at the top' as to the importance and relevance of the project and ensure buy-in and commitment of the right business representatives who will act as decision makers and owners of the SoD rules to be enforced.

7.4 SAP Netweaver IM projects

With Netweaver IM, the scope of SAP-based Identity Management increases significantly. We are now likely to see IM and IAM projects that will make use of the foundation of SAP HR and corporate LDAPs. It will be possible to integrate SAP HR/HCM user attributes and organisational values and use them in the Netweaver context. Most organisations start to make use of a 'business role mapped onto technical roles' model. The quality of the identities using these roles is under increasing scrutiny from regulators, as is the quality of the organisation-wide segregation-of-duty. Netweaver IM has a great role to play here. This may well be in cooperation with partners such as Ping Identity, and their toolkit for federation ('PingFederate'). This technology is converging towards SAML, WS-Trust and WS-Federation. Hence an important part of the work will be defining the high-level roles with regard to identity and attribute providers, and the types of reliance that service providers can take from these assertions. And these roles have subsequently to be implemented across ABAP and J2EE stacks.

8 Conclusion

SAP-based solutions became commonplace in the 21st century, both in private and public sector. There is a well established body of best practices and possible safeguards that can be deployed to mitigate operational, security and internal control risks. It relies on balancing security at the levels of policy, management processes, applications, and infrastructure. Alignment on the ISO 27000 family [ISO27K1] is increasingly common, because it offers a solid structure to justify security investments. At the core of it lies a well-designed and managed authorisation concept. And SAP authorisation objects and SAML assertions will work side-by-side to get the job done. Just as breaks allow a car to go faster, safeguards in terms of security and controls allow better business.

References

[ISO27K1] ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements (available from www.iso.ch)

[SAPBRTW] SAP Berechtigungswesen, IBM Business Consulting Services, ISBN 3-89842-312-3, 2003