NEXTLABS®

White Paper

Attribute Based Access Control for SAP

INTRODUCTION

Data security has become one of the most significant challenges in global businesses. Requirements are driven by a variety of sources including government compliance, lack of data identification, product development in trade restricted countries where legal protections are inadequate, data leakage beyond project teams due to mishandling, insecure or unmonitored data transfer or distribution between supply chain partners, and data lost on unprotected laptops, removable drives, or mobile devices. This guide will discuss the features and roles of functional and data access level controls and how they interoperate to address the data security challenges companies operating globally face within the context of their enterprise SAP landscape.

BUSINESS REQUIREMENTS

Large organizations are increasingly dealing with regulatory compliance issues such as CWC, FDA 21 CFR Part 11, ITAR, EAR, BAFA, DOE 810, NERC/CIP and SEC, among others. Securing intellectual property is also a major concern as growing business is often necessitated by increasing collaboration, both internal and external, such as in the areas of product and engineering, supply chain, partnerships and joint ventures. In order to support these business scenarios within a SAP environment, it is necessary to incorporate attributes such as access location, time of day, export license, user citizenship, or project/program assignment. Consider a US-based product manager of a US corporation whose product is subject to ITAR regulations, but has both government and commercial application. The business rule for compliance may be that ITAR data in SAP is onlyaccessible by US persons while in US locations. When she is on a business trip to Singapore meeting with her suppliers in their APAC regional HQ, exposing material data, CAD drawings or BOM's stored in SAP would be a violation of ITAR.

If she attempts to display information subject to ITAR on her iPad during a presentation, accessing data using SAP Netweaver Portal, location-based services can flag her location based on her IP address and should trigger a DENY message in SAP. In this example, the product manager's role serves as the functional attributes, the data elements (material/CAD/BOM) as well as the location information serve as data attributes and the business rule provides the governance for access control. Figure 1 depicts the three dimensional model of large organization system security architecture including functional access, data access, and governance.

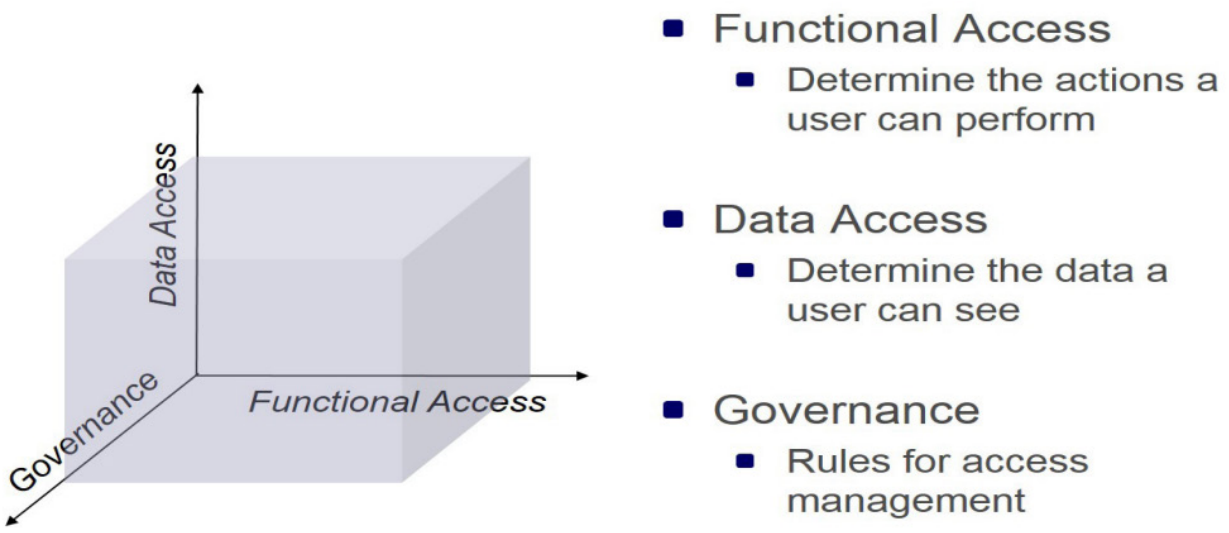

Figure 1: Three Dimensions of Business Authorization

SAP AUTHORIZATION

The SAP authorization concept is designed for role based security or Role Based Access Control (RBAC). RBAC has been the predominant approach to system security for SAP and other major IT vendors since the mid-1990's and was formalized as an ANSI/INCITS standard in 2004, based on the NIST RBAC model (Sandhu, Ferraiolo, and Kuhn) 1. SAP's security architecture contains five layers (User, Profile, Authorization, Authorization Object, Object Class) that supports functional access to the SAP system. A user may be assigned one or more profiles subject to their role responsibility within the organization, such as a buyer or payer. The buyer profile may be authorized to procure raw materials for company code "100" up to a value of $10,000 and the payer may be authorized to pay invoices from vendors for all materials in company code "100" up to a value of $50,000, for example. Governance principles and organizational best practices may dictate that the same user should not have both the buyer profile and payer profile in order to avoid potential fraud. In this simple example, SAP security is able to distinguish which user can perform a specific function by limiting their access to certain transactions, programs and services. One of the key features and benefits of SAP authorization is its ease of use in system administration and support of human resource functions such as role changes and employee turnover.

1 Ravi Sandhu, David Ferraiolo and Richard Kuhn. "The NIST Model for Role-Based Access Control: Towards A Unified Standard," 2000 <http://csrc.nist.gov/rbac/sandhu-ferraiolo-kuhn-00.pdf>

If this example is within the context of a UK multi-national chemical company setting up a joint venture with a local company in Belarus to service the emerging market, there is an additional layer of data security needed based on location in order to restrict access to recipes and intellectual property not related to the joint venture. Assuming there are 10 distinct buyer profiles in SAP, each would need to be replicated for each joint venture, plus presumably a "buyer_all" profile. If this example is further extended to include compliance requirements from the Chemical Weapons Convention for chemicals produced by the US subsidiary, each of the profiles created would need to be replicated again to account for these additional restrictions. Additional custom ABAP development is often needed to integrate the SAP authorization engine with HR-related data sourced from SAP HR or external HRIS systems to support data requirements that may be linked to an employee or contractor. This common example can quickly cause a "role explosion" within SAP authorization to manage the various factors that contribute to an "ACCESS" or "DENY" system decision. Broadly speaking, the implementation of data-based requirements results in an exponential increase in access rules compared to access variables (Figure 2). This approach often results in implementing more roles than employees and becomes an administrative bottleneck.

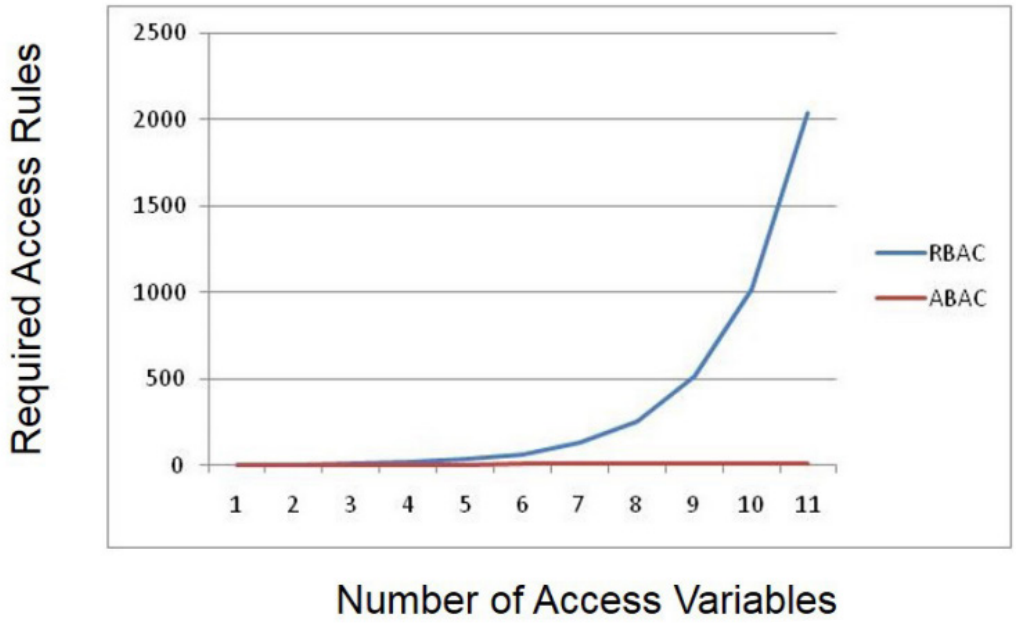

Figure 2: Role Explosion

ATTRIBUTE BASED ACCESS CONTROL

In the scenarios where data elements contribute to the access criteria, Attribute Based Access Control (ABAC) is the solution that would best support the business authorization requirements in a scalable way. Within enterprise software, XACML (eXtensible Access Control Markup Language) - a standard defined by the OASIS standards association - is becoming the defacto standard used in the enterprise software market. The basic elements of XACML architecture includes a Policy Administration Point (PAP), Policy Decision Point (PDP), Policy Enforcement Point (PEP) and Policy Information Point (PIP). The key feature of segregating these areas is the ability to quickly update authorization policies and reduction of ongoing system maintenance.

HYBRID SOLUTION

To support the needs of global businesses running on SAP, an organization will have some combination of static and dynamic access attributes. To this extent, employing a hybrid architecture of implementing SAP Authorization complemented by an ABAC system will provide the control necessary to ensure business requirements are met along with optimizing the maintenance of the authorization systems. The recommended approach is to create an authorization map to clearly identify the Functional Roles and Data Attributes for a given organization. An example of engineering collaboration with an external partner is shown in Figure 3.

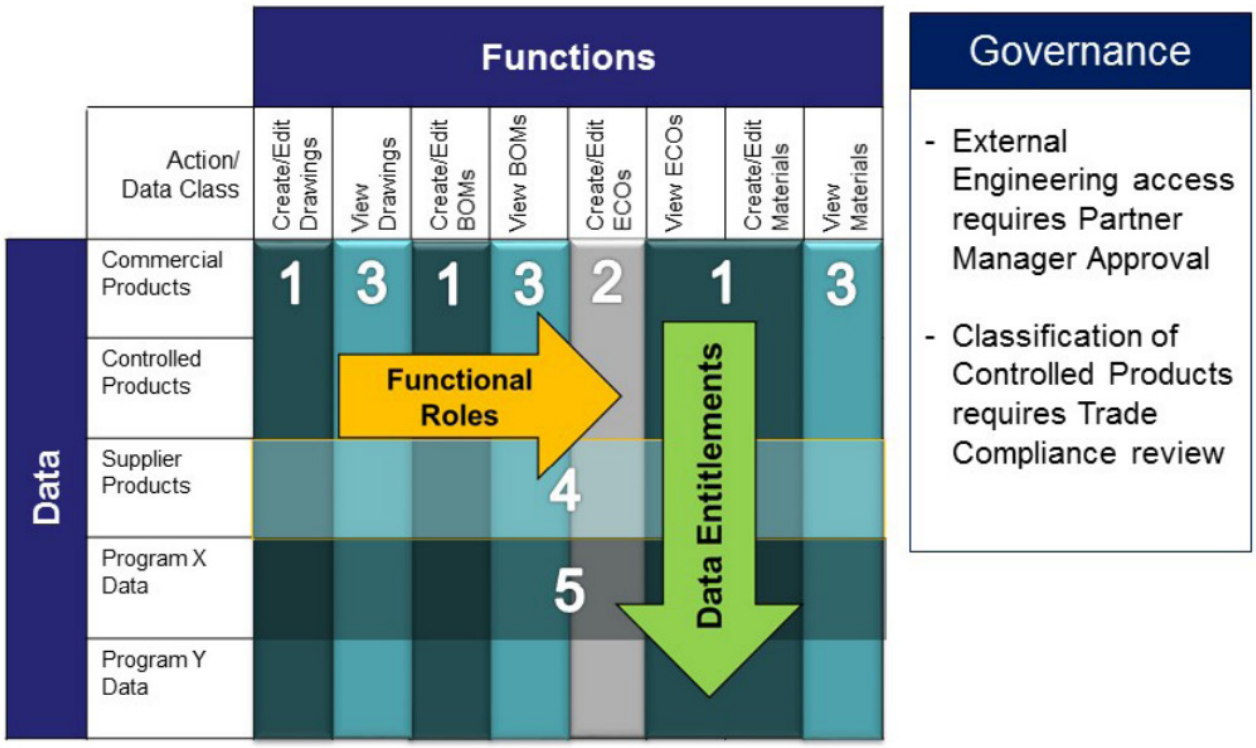

Figure 3: Authorization Map

The determination of functional roles is typically done in establishing SAP security architecture and is depicted as role 1-3 in the example. The addition of data attributes 4 and 5 can be best implemented in an ABAC layer as depicted in figure 4. The optimal approach in design is to determine which attributes are static and those that are dynamic. Static attributes such as base office location and position are best implemented in SAP authorization and dynamic attributes such as export license, project affiliation and login information are best implemented by the additional layer of an ABAC system.

The Governance layer in figure 4 represents the best practice policies govening how access is to be managed; for example: “External Engineering Access requires Partner Manager Review”. It also typically specifies Separation of Duties and other governance requirements, typically provided through SAP GRC Access Control.

By employing this hybrid approach, companies can achieve governance over system administration while maintaining their existing global production support model. This hybrid model leverage SAP GRC Access Control and SAP authorization for Governance and Functional Authorization and leverages ABAC for Data Authorization. This hybrid design combines the features and fully integrated capabilities of SAP GRC Access Control and SAP authorization,
such as ease of user assignment and role management, to efficiently supporting data attributes and avoiding the “role explosion” and custom development that would otherwise be necessary and costly.

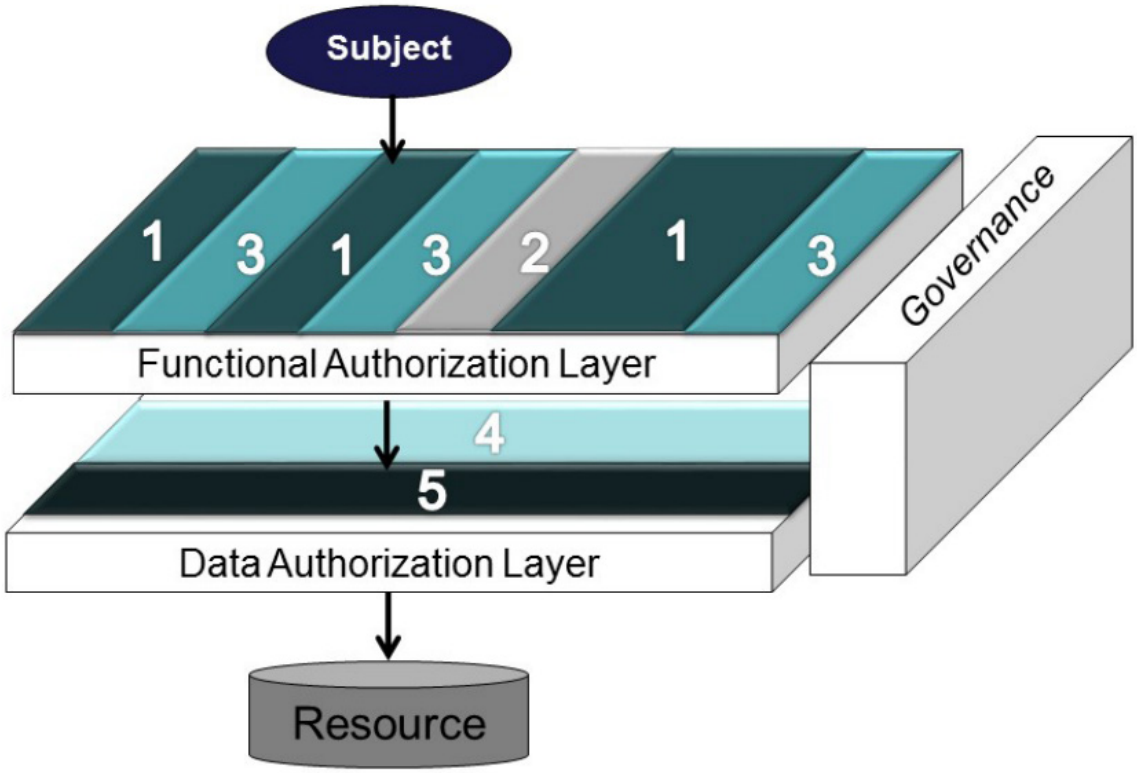

Figure 4: Authorization Layers

NEXTLABS AND SAP

NextLabs Entitlement Manager is an SAP-endorsed business solution and works with the SAP ERP, SAP Product Lifecycle Management, SAP GRC Access Control and SAP Global Trade Services applications to provide end-to-end information risk management. The NextLabs Entitlement Manager and Control Center extend SAP authorization concepts to provide attribute-based access to SAP business objects such as materials, BOMs, routings, change masters, parts specifications, CAD drawings, and documents. It can leverage SAP roles and access control contexts and combine them with other attributes for dynamic authorization decisions. The Entitlement Manager can be configured to automatically classify critical SAP data by association or inheritance or based on location of storage. This greatly simplifies the task of data classification and helps ensure that program data is properly identified for effective access control throughout its lifecycle. Finally, the Entitlement Manager works seamlessly through the SAP GUI and SAP NetWeaver® Portal and SAP Mobile Applications components to enforce data access and sharing policies. The Entitlement Manager can be extended to protect critical data after it is exported from SAP applications to provide end-to-end protection. Graphical reporting tools provide a complete audit trail of all authorization decisions.

NextLabs Entitlement Manager and Control Center work with SAP solutions to provide the following benefits:

- Automate global trade compliance and lower compliance costs associated with various export control regulations, such as ITAR, EAR, BAFA, and ECA
- Protect intellectual property while enabling global design collaboration and prevent wrongful disclosure of design and engineering specifications in compliance with proprietary information exchange agreements and nondisclosure agreements
- Prevent data breach across the global supply chain and protect supply, demand, and manufacturing data in accordance with contractor and supplier agreements
- Enhance data security and minimize the risk of SAP data spillage and contamination
- Support proper data segregation in compliance with regulatory mandates and simplify compliance reporting through centralized logging of access

The Entitlement Manager and Control Center enable safe and secure global shared service functions while providing regional policy control. By providing fine-grained authorization with centralized management, the Entitlement Manager enables global companies to automate export control, secure engineering and supply chain collaboration, and enhance data security.

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.