Name

Maha Aburahma
(Egypt)

Advisors

Dr.
Reinhard Stumptner

A.Univ.-Prof. Dr.
Josef Küng

Company

Identity and Access Management: Analysis and Conceptual Design for EVG

Identity and Access Management (IAM) is a major concept that addresses the needs for effective information security. IAM systems provide a way to abstract functionalities like administration, authentication, authorisation and audit from target systems. The use of an IAM system deployed in an organization increases the business value and reduces the operational costs and security risks.

IAM
Identity Management
Security Risks
Access Control
Information Security
Authentication

Project Motivation

Cost and Security are two major business drivers for many of the business decisions. IT managers across all enterprises aim at reducing the IT costs and complexity of managing and administrating different systems as well as enforcing company security policies and decreasing risks. Identity and Access Management (IAM) systems play a key role in increasing business value while reducing the costs and risks. IAM systems span multiple target systems to orchestrate: administration, authentication, authorisation, and audit among target systems. Deploying an IAM system within an enterprise decreases the operational cost of administrating target systems, as well as ensuring the compliance with the enterprise policies and regulations.

EV Group is a technology and market leader for wafer processing equipment. It faces some problems in managing different target systems available in the corporate. It also lacks the ability to automate the creation of security reports. Such reports ensure that the corporate information assets and privacy are well protected across all interactions with the target systems.

Project Structure

The aim of this thesis is to analyse both the impact of deploying an IAM system in EVG, and the needs behind such change. Decreasing the operational cost and time spent by the IT team at EVG is the driving force of this project, in addition to the protection of the information as it is considered as the main asset for EVG.

In order to achieve the goal of the project, the state of the art in the field of IAM systems is researched. In addition, some of the IAM suits available on the market are analysed as a reference for the functionality supported currently by IAM systems on market. The two vendors were Oracle and Axiomatics.

Oracle is one of the vendors for IAM systems on the market. Oracle Identity and Access Management products can be divided into three categories; Identity Management, Directory Services and Access Management. Oracle Identity Manager Architecture was investigated as a reference architecture for Identity and Access Management systems.

Axiomatics is a supplier of XACML-based authorisation management systems. The main advantage of using Axiomatics Policy Server is that it uses XACML which is an open standard for access control. Axiomatics Policy server was installed and the architecture was investigated as a reference for ABAC and RBAC access control policies.

The standards related to the field of IAM plays an important role in the maturity of IAM products. Thus, part of the work focused on investigation standards like: XACML, SPML, DSML and WS-BPEL. Those standards are crucial in the communication between the IAM system and different target systems.

The final step was to present an analysis of EVG requirements, which represent the main reasons for considering an IAM system. Furthermore, the work included a preliminary design of how the system should look like, pointing out the main components, classes and interactions between different objects in the system.